> Living in a networked world

Integrated research agenda Cyber-Physical Systems (agendaCPS)

Eva Geisberger/Manfred Broy (Eds.)

acatech STUDY

March 2015

acatech
NATIONAL ACADEMY OF
SCIENCE AND ENGINEERING

Editors:

Dr. Eva Geisberger
Technische Universität München,
Institut für Informatik
Boltzmannstraße 3
85748 Garching
E-Mail: geisberg@in.tum.de

Prof. Dr. Dr. h. c. Manfred Broy
Technische Universität München,
Institut für Informatik
Boltzmannstraße 3
85748 Garching
E-Mail: broy@in.tum.de

Series published by:
acatech – NATIONAL ACADEMY OF SCIENCE AND ENGINEERING, 2015

Munich Office
Residenz München
Hofgartenstraße 2
80539 München

T +49 (0) 89 / 5 20 30 90
F +49 (0) 89 / 5 20 30 99

Berlin Office
Unter den Linden 14
10117 Berlin

T +49 (0) 30 / 2 06 30 96 0
F +49 (0) 30 / 2 06 30 96 11

Brussels Office
Rue d’Egmont/Egmontstraat 13
1000 Brüssel
Belgien

T +32 (0) 2 / 2 13 81 80
F +32 (0) 2 / 2 13 81 89

E-Mail: info@acatech.de
Internet: www.acatech.de

Recommended citation:
Eva Geisberger/Manfred Broy (Eds.): *Living in a networked world. Integrated research agenda Cyber-Physical Systems (agendaCPS)* (acatech STUDY), Munich: Herbert Utz Verlag 2015.

Coordination: Ariane Hellinger
Edited by: Ariane Hellinger, Heinrich Seeger, Linda Treugut
Translation: Joaquin Blasco
Layout-Concept: acatech
Conversion and typesetting: Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS, Sankt Augustin

> THE acatech STUDY SERIES

This series comprises reports presenting the results of projects carried out by the National Academy of Science and Engineering. The studies are intended to provide informed assessments and future-oriented advice for policy-makers and society.

> CONTENTS

FOREWORD

BY WOLFGANG MAYRHUBER, FORMER CHIEF EXECUTIVE OFFICER OF DEUTSCHE LUFTHANSA AG AND ACATECH EXECUTIVE BOARD MEMBER

We live in the age of networks. For several centuries now, land, sea and air transport networks have helped to connect people and enable trade all around the world. Today, the dynamic development of information and communication technology has led to the emergence of an IT communications network that crisscrosses the globe like a "nervous system". The future now lies in the smart combination of the "real" and "virtual" worlds, a phenomenon known as Cyber-Physical Systems (CPS).

This study was carried out under the auspices of acatech's "Information and Communication Technology" topic network. Following on from the "Smart Objects" project, it too addresses the mega-trend of the "Internet of Things" by investigating the opportunities and challenges associated with the technological trend of Cyber-Physical Systems. Cyber-Physical Systems are systems that come about when embedded systems are connected with each other and with Web-based services. As a member of acatech's Executive Board, I have followed this project with particular interest because of the breadth of topics that it addresses and in particular the scenarios, which describe a vision of the future that focuses not only on the technological issues but also on the commercial and social aspects. The project team, which comprised a broad-based partnership between large-scale enterprises, SMEs, research institutes and professional associations, took on an extremely ambitious challenge. We are delighted to be able to present the results of their work in the shape of the first comprehensive analysis of Cyber-Physical Systems to be published in the German-speaking world. The study clearly illustrates the extent to which corporate strategies are being adapted in order to enable these complex systems to be developed and controlled.

There is a certain inevitability about this transformation, since it is being driven by a whole host of changes in customers' requirements and by the potential it offers to increase flexibility and productivity. It is therefore in the interests of businesses to incorporate this trend into their strategies.

The success of CPS technology derives from the enormous direct practical benefits that it provides by offering people more comfort, control over their own time, ubiquity, reliability, information and efficiency. There is thus huge potential to use Cyber-Physical Systems as a basis for developing new business models. For example, airlines can use CPS technology to improve the service they provide to their passengers throughout the entire service chain, by optimising travel routes or cutting waiting times. Telemedicine applications can also enhance the in-flight care or treatment options available to people requiring special care or who are taken ill during their journey.

Digital networking solutions spanning the entire supply chain also have potential in the area of smart logistics. For example, they could enable intermodal management of baggage and freight right across the logistics chain as well as providing higher customer value through real-time locating. Industry-wide standards would contribute to faster and more widespread implementation in this area. Finally, traffic management systems have a variety of potential applications, including airspace management. Optimised flight profiles would prevent delays by removing the need for aircraft to enter holding patterns, thereby cutting fuel consumption and reducing greenhouse gas emissions. Cyber-Physical Systems can make a significant contribution to efficient resource use.

Through this project, acatech has once again provided a platform for bringing together a wide range of different actors in the interests of pre-competitive collaboration. Now that the project has concluded, further interdisciplinary research projects will need to continue collectively driving forward the technological and operational competencies required for Cyber-Physical Systems. It is standard practice for forward-looking, innovation-driven airlines like Lufthansa to work closely with the scientific community on projects of this nature.

It is our belief that we now stand at a critical point in our journey. In order to guarantee the competitiveness of Cyber-Physical Systems, policymakers will need to create an appropriate framework and industry will have to flexibly and rapidly incorporate CPS into its strategies. This should be our common goal. If we are able to accomplish it, Germany will be well placed to become a leading supplier of Cyber-Physical Systems.

Cyber-Physical Systems will have a role to play in all the relevant infrastructure areas and will lead to groundbreaking developments in the fields of resource management, energy mix management and electric mobility, as well as in the shape of new service components for users. This study clearly describes the potential for innovation whilst also identifying a wide range of concrete areas for action.

As with all innovative technologies, it will also be necessary to tackle the challenge of developing marketable products and gaining the acceptance of the people who use them. This study addresses all of these issues in a clear and accessible manner – I sincerely hope that you find it stimulating reading.

Wolfgang Mayrhuber

PREFACE

BY MANFRED BROY

We are glad to see the English translation of the agenda Cyber-Physical Systems, which we finished three years ago as a German project by a German publication. In the meanwhile things have moved forward. However, the content of this agenda is as up to date as it was three years ago. It is very satisfying and encouraging to see how much our agenda Cyber-Physical Systems has already had as impact. We see quite a number of research projects that address Cyber-Physical System in Europe right now. We see that companies now understand that Cyber-Physical Systems is an important field in a spectrum of application field such as smart energy or connected production under the heading Industry 4.0. Moreover, a very fruitful discussion and collaboration has started between scientists and researchers in Europe and peers in Cyber-Physical Systems in the United States.

This all is promising and encouraging and therefore it is very useful that now the English translation appears which gives access to the results of our studies to a much larger community. We hope that this is again helpful to provide a further push in technology and research in Europe into a future where connected embedded Systems and global networks are used for the benefit of mankind.

Manfred Broy

January 2015

SUMMARY

In conjunction with microsystems technology, the sustained rapid advances in information technology and the resulting exponential increase in processing power and data capture, data transmission and data storage capacity are enabling ever more powerful peripheral, communication and control systems which are being networked more and more closely with each other. The combination of comprehensive IT systems and the Internet is leading to a continuous increase in the number, power and complexity of applications. Software-intensive systems and devices are becoming everyday commodities. By connecting them to each other in a variety of different ways and incorporating data and services from global networks, they are being transformed into integrated, comprehensive solutions that are increasingly pervading and connecting every area of our lives. Open, networked systems are emerging that use sensors to capture data about what is going on in the physical world, interpret these data and make them available to network-based services, whilst also using actuators to directly affect processes in the physical world and control the behaviour of devices, objects and services. These systems are known as Cyber-Physical Systems (CPS). They are giving rise to system landscapes and socio-technical systems with applications that are not just innovative but genuinely revolutionary.

In the future, Cyber-Physical Systems will make hitherto almost unimaginable contributions to quality of life, safety, security and efficiency, as well as to security of supply in the fields of energy, water and healthcare. They will thus help to solve some of the key challenges our society is facing. For example, modern smart health systems use sensors to record data about patients' health, connect patients, doctors and therapists with each other and provide them with access to patient data, and enable remote diagnosis and healthcare in the patient's own home. Smart Cyber-Physical Systems coordinate traffic flows, provide people with support in critical situations and cut energy consumption both in the transport system and through smart power grid management. These wide-ranging capabilities are driving rapid economic and social changes. We are witnessing a constant stream of innovations that need to be appropriately channelled. Cyber-Physical Systems require cross-domain cooperation in order to enable interactive value creation in economic ecosystems.

Targeted political, economic, technological and methodological efforts will be required to fully exploit this area of innovation. It will be necessary to resolve a variety of questions and challenges in order to enable the design and deployment of Cyber-Physical Systems and applications that meet people's needs.

Germany is a global market leader in the precursor technologies for Cyber-Physical Systems – embedded systems, integrated safety and security solutions and complex system solutions engineering. Given the huge drive for innovation in the field of Cyber-Physical Systems, Germany will only be able to maintain and develop this position if it secures its leadership in CPS innovation and extends its market leadership in embedded systems so that it can take full advantage of the potential offered by the trend towards Cyber-Physical Systems. One of the formal goals of the agendaCPS project and the integrated Cyber-Physical Systems research agenda presented in this study is to draw up a catalogue of measures that addresses the need for Germany not just to participate in the evolution of CPS and the concomitant economic and social changes but to play a major part in shaping the revolution by competing with other industries and technology centres around the world.

The rapid technological transformation induced by Cyber-Physical Systems is creating new business opportunities and is bringing about disruptive changes in the markets and business models of several key industries. It is therefore necessary to act swiftly in order to seize the moment.

Consequently, this study analyses and describes the capabilities, potential and challenges associated with

Cyber-Physical Systems, including the economic and social benefits and added value that they can bring and the technological, research, business and policy challenges that will need to be met to make Germany more innovative and competitive in this area. Its key contributions include analysing the challenges and unanswered questions with regard to the safety, security, risks and acceptance of CPS technology and its applications, as well as identifying the measures needed to meet these challenges.

There are many different challenges affecting both society and industry:

- **Society:** it is hoped that Cyber-Physical Systems will help solve some of the challenges facing our society such as the provision of care for the elderly and enabling people to lead independent and safe lives as they get older. There are a number of unresolved issues in this area with regard to data and privacy protection and human-machine interaction. These are accompanied by questions whose answers will influence the extent to which CPS are accepted, for example with regard to individual freedom, governance and fairness in systems with distributed control, as well as the self-organisation and self-management of infrastructure and utility systems.
- **Industry:** the potential of CPS is closely connected to the shift away from products and towards integrated, interactive services and solutions. The excess value that will be created in economic ecosystems will require a variety of new architectures and business models, together with open standards and platforms to ensure system interoperability.
- **Science and research:** a number of new technologies and integrated models and architectures are emerging, particularly human models and integrated models of human-machine interaction and cooperation. This requires interdisciplinary engineering and the relevant competencies for deploying and operating these technologies in order to ensure that they are properly controlled and that non-functional requirements are also met.

Based on the outcomes of these considerations, as well as the preliminary work of the National Roadmap Embedded Systems and our assessment of the current status of research and technology, the Agenda concludes with a detailed SWOT analysis that enables the priority action areas to be identified.

The study’s conclusions point towards the strategic measures and themes that can give Germany an innovative edge in the field of Cyber-Physical Systems. These can provide significant leverage and are essential in order to ensure sustainable innovativeness across the whole of the economy and to address the challenges facing our society.

The key conclusions in terms of the strategic action areas are as follows:

- It is necessary to implement a change of strategy and to rethink all levels of the value creation process, with a shift towards open, interactive markets and living spaces and the associated processes, as well as infrastructure and utility systems with integrated, interactive and networked services. This will require research to focus on specific priorities including enhanced human-machine interaction, requirements engineering, the development of requirements and domain models and innovative architectures, as well as interdisciplinary systems engineering and integrated quality assurance at all levels of the requirements and systems engineering process.
- It will be paramount to adopt an interdisciplinary approach to research, development and system design. Moreover, it will be necessary to integrate technology impact assessments, acceptance research and interactive system design into this process.

- New economic ecosystems are emerging. These will require the appropriate competitive strategies and excess-value architectures in order to foster innovation, diversity, safety, security and trust.
- It will be necessary to develop and implement models and standards for guaranteeing the quality of Cyber-Physical Systems.
- It will be necessary to ensure sustainable development of technological and operational competencies in the education and training systems and to make sure that the necessary conditions are created for industry.

Software becomes a dominant role in the control, design and use of data and services and in connecting the physical and virtual worlds. The ability to control large-scale, networked software systems with long service lives will therefore be of fundamental importance.

A variety of concrete operational recommendations aimed at policymakers and the scientific and business communities can be found in the "acatech POSITION PAPER" that was publicly launched at the 6th National IT Summit held in Munich in December 2011.

PROJECT

This study also formed the basis of the acatech POSITION PAPER *Cyber-Physical Systems. Driving force for innovation in mobility, health, energy and production* (acatech 2012).

> AUTHORS

- Dr. Eva Geisberger, fortiss GmbH
- Prof. Dr. Dr. h. c. Manfred Broy, Technische Universität München
- Dr. María Victoria Cengarle, fortiss GmbH
- Patrick Keil, fortiss GmbH
- Jürgen Niehaus, SafeTRANS e. V.
- Dr. Christian Thiel, BICCnet Bavarian Information and Communication Technology Cluster
- Hans-Jürgen Thönnißen-Fries, ESG Elektroniksystem- und Logistik-GmbH

> CONTRIBUTORS

- Theo von Bomhard, Robert Bosch GmbH
- Dr. Christian Buckl, fortiss GmbH
- Denis Bytschkow, Center for Digital Technology and Management (CDTM) and fortiss GmbH
- Fabian Dany, Center for Digital Technology and Management (CDTM)
- Stefan Greiner, acatech Office
- Jürgen Hairbucher, Intel GmbH
- Marit Hansen, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
- Dr. Christoph Krauß, Fraunhofer AISEC
- Prof. Dr. Bernd Krieg-Brückner, University of Bremen and DFKI GmbH
- Oliver Peters, Robert Bosch GmbH
- Dr. Olaf Sauer, Fraunhofer IOSB
- PD Dr. Bernhard Schätz, fortiss GmbH

> PROJECT MANAGEMENT

- Prof. Dr. Dr. h. c. Manfred Broy, Technische Universität München

> SCIENTIFIC DIRECTOR

- Dr. Eva Geisberger, fortiss GmbH

> PROJECT GROUP

- Dr. Heinz Derenbach, Bosch Software Innovations GmbH
- Prof. Dr.-Ing. José L. Encarnação, Technische Universität Darmstadt
- Prof. Dr. Otthein Herzog, University of Bremen and Jacobs University Bremen
- Prof. Dr. Wolfgang Merker
- Hannes Schwaderer, Intel GmbH
- Dr. Reinhard Stolle, BMW AG

> CONSORTIUM MEMBER

- fortiss GmbH, an associated institute of the Technische Universität München

> ASSIGNMENTS

- BICCnet Bavarian Information and Communication Technology Cluster
- Fraunhofer IOSB
- OFFIS e. V.
- SafeTRANS e. V.

> PROJECT COORDINATION

- Ariane Hellinger, acatech Office
- Dr. Christian Thiel, BICCnet Bavarian Information and Communication Technology Cluster

> PROJECT DURATION

1 May 2010 – 31 January 2012

> FUNDING

The project was funded by the Federal Ministry of Education and Research as part of the High-Tech Strategy of the German government (funding reference 01/S10032A 01/S10032B).

SPONSORED BY THE

Federal Ministry
of Education
and Research

Project administrator: Project administrator at the German Aerospace Center (PT-DLR), Software systems and knowledge technology.

acatech would also like to thank the following companies for their support: BMW AG, Intel GmbH, Robert Bosch GmbH.

This publication has been supported by the European Commission, DG CONNECT, and the fortiss GmbH.

> WE WOULD LIKE TO THANK THE FOLLOWING INDIVIDUALS FOR THEIR EXPERTISE AND VALUABLE CONTRIBUTIONS:

- Dr. Ralf Ackermann, SAP AG
- Prof. Dr. Bernhard Bauer, University of Augsburg
- Gülden Bayrak, Technische Universität München, AIS
- Klaus Beetz, Siemens AG, CT
- Andreas Beu, User Interface Design GmbH
- Ottmar Bender, Cassidian
- Thomas Benedek, BMW Car IT GmbH
- Dr. Susanne Bührer-Topcu, Fraunhofer ISI
- Anne Burger, MedVenture Partners
- Andrea Cato, Intel GmbH
- Prof. Dr.-Ing. Jana Dittmann, Otto von Guericke University Magdeburg
- Prof. Dr.-Ing. Jörg Eberspächer, Technische Universität München
- Prof. Dr. habil. Claudia Eckert, Technische Universität München
- Maximilian Engelken, Center for Digital Technology and Management (CDTM)
- Dr. Hieronymus Fischer, ESG Elektroniksystem- und Logistik-GmbH
- Axel Foery, Cisco Systems GmbH
- Dr.-Ing. Oliver Frager, teamtechnik Maschinen und Anlagen GmbH
- Dr. Ursula Frank, Beckhoff Automation GmbH
- Martin Gangkofer, ESG Elektroniksystem- und Logistik-GmbH
- Manuel Giuliani, fortiss GmbH
- Rainer Glatz, VDMA (German Engineering Federation)
- Stephan Gurke, ZVEI (German Electrical and Electronic Manufacturers' Association)
- Martin Hiller, Cassidian
- Dr. Jan Hladik, SAP AG
- Harald Hönninger, Robert Bosch GmbH
- Tobias Hoppe, Otto von Guericke University Magdeburg
- Gerd Hoppe, Beckhoff Automation GmbH
- Thomas Janke, SAP AG
- Josef Jiru, Fraunhofer ESK
- Prof. Dr. Bernhard Josko, OFFIS e. V.
- Bernd Kärcher, Festo AG & Co. KG
- Dr. Frank Kargl, University of Twente
- Dr. Ingolf Karls, Intel GmbH
- Dirk Kaule, BMW AG
- Thomas Kellerer, Intel GmbH
- Maged Khalil, fortiss GmbH
- Stefan Kiltz, Otto von Guericke University Magdeburg
- Dr. Cornel Klein, Siemens AG, CT
- Dr. Martin Knechtel, SAP AG
- Tanja Kornberger, Center for Digital Technology and Management (CDTM)
- Till Kreiler, NAVTEQ
- Frank Lafos, Intel GmbH
- Falk Langer, Fraunhofer ESK
- Prof. Dr. Ulrike Lechner, Universität der BW München

- Dr. Enno Lübbers, Intel GmbH
- Dr. Andreas Lüdtke, OFFIS e. V.
- Dr. Christine Maul, Bayer Technology Services GmbH
- Dr. Christoph Mayer, OFFIS e. V.
- Christian Menkens, Center for Digital Technology and Management (CDTM)
- Jochen Meyer, OFFIS e. V.
- Dr. Mark Müller, Bosch Software Innovations GmbH
- Dr. Stefan Ochs, Bayer Technology Services GmbH
- Claus Oetter, VDMA (German Engineering Federation)
- Dr. Josef Papenfort, Beckhoff Automation GmbH
- Christian Patzlaff, ESG Elektroniksystem- und Logistik- GmbH
- Tobias Paul, ESG Elektroniksystem- und Logistik-GmbH
- Dr. Holger Pfeifer, Technische Universität München
- Gerd Pflüger, Cisco Systems GmbH
- Prof. Dr. Dres. h. c. Arnold Picot, Ludwig-Maximilians-Universität München
- Dr. Daniel Ratiu, fortiss GmbH
- Sebastian Rohjans, OFFIS e. V.
- Benedikt Römer, Center for Digital Technology and Management (CDTM)
- Oliver Roos, Intel GmbH
- Christine Rossa, Robert Bosch GmbH
- Dr. Harald Rueß, fortiss GmbH
- Dr. Oliver Sander, Karlsruhe Institute of Technology KIT
- Andreas Schmid, Center for Digital Technology and Management (CDTM)
- Martin Schneider, ESG Elektroniksystem- und Logistik-GmbH
- Dr. Ralf Schulz, BMW AG
- Michael Schwarz, Cisco Systems GmbH
- Dr. Christian Schwingenschlögl, Siemens AG, CT
- Dominik Sojer, Technische Universität München
- Stephan Sommer, Technische Universität München
- Dr. Thomas Stauner, BMW AG
- Dr. Rainer Stetter, ITQ GmbH
- Dr. Thomas Stiffel, Bosch Software Innovations GmbH
- Prof. Dr. Peter Struss, Technische Universität München
- Carolin Theobald, ZVEI (German Electrical and Electronic Manufacturers' Association)
- Dr. Mario Trapp, Fraunhofer IESE
- Dr. Mathias Uslar, OFFIS e. V.
- Bernhard Vogel, Siemens AG, Healthcare
- Prof. Dr.-Ing. Birgit Vogel-Heuser, Technische Universität München, AIS
- Jürgen Weis, ESG Elektroniksystem- und Logistik-GmbH
- Dr. Gerhard Weiss, Maastricht University
- Dr. Kay Werthschulte, ESG Elektroniksystem- und Logistik-GmbH
- Dr. Chris Winkler, Siemens AG, CT
- Dr. Matthias Winkler, SAP AG
- Dr. Thomas Wittig, Robert Bosch GmbH
- Stephan Ziegler, BITKOM (Federal Association for Information Technology, Telecommunications and New Media)

> PROJECT ADVISORY COMMITTEE

- Dr. Reinhold Achatz, Siemens AG
- Prof. Dr. Heinrich Dämbkes, Cassidian
- Prof. Dr. Werner Damm, Oldenburg University (Spokesman of the Advisory Committee)
- Dr. Klaus Grimm, Daimler AG
- Harald Hönninger, Robert Bosch GmbH
- Prof. Dr. Peter Liggesmeyer, Fraunhofer IESE

We would like to thank Mr Johann Wiesböck for his commitment and support and for his assistance in carrying out the joint online survey in "ElektronikPraxis" magazine.

We would like to thank our technical editor Mr Heinrich Seeger for his invaluable support.

1 INTRODUCTION

The Integrated Research Agenda Cyber-Physical Systems project (hereafter abbreviated to agendaCPS) was initiated by acatech, Germany's National Academy of Science and Engineering. The project is funded by the Federal Ministry of Education and Research (BMBF) and has been carried out with extensive support from fortiss, an associated institute of the Technische Universität München.

1.1 GOALS AND STRUCTURE OF THE REPORT

Agenda Cyber-Physical Systems aims to provide a comprehensive and systematic overview of the technology trends and innovation potential associated with Cyber-Physical Systems (CPS) and draw conclusions concerning the priority areas for research and action. A number of significant fields of application are used to illustrate the economic and social importance of this topic. The goal of agendaCPS is to strengthen and develop Germany's position in the area of Cyber-Physical Systems.

Cyber-Physical Systems connect the physical world with the world of information technology. They evolve from complex interactions

- of embedded systems, application systems and infrastructures, for example controls on board vehicles, smart intersections, traffic management systems, communication networks and their connections to the Internet
- based on the networking and integration of the above
- and involving human-technology interaction in application processes.

As such, Cyber-Physical Systems are not self-contained entities, as can be seen, for example, in networked mobility *services*[1] or integrated patient telecare provided by several different service providers such as doctors, physiotherapists and pharmacies. Instead, they are open *socio-technical systems* that arise from extensive networking of the physical, social and virtual worlds and the smart use of information and communication technology. The tremendously fast development of the basic technologies and the wide range of aspects that they incorporate make Cyber-Physical Systems a complex topic to investigate – their areas of application and potential benefits are constantly developing and changing at a rapid pace. The main goal of agendaCPS is to illustrate the inherent change of the technologies and their applications. Cyber-Physical Systems open up extensive opportunities by enabling the functional connection of the physical and the software-based, virtual worlds. In the future, this will not only transform individual industries but will, in the long term, bring about a transformation of society as a whole as a result of "smart" *human-machine cooperation*.

In order to meet the overarching goals described above, the agenda aims:

- to provide a comprehensive overview of the phenomenon and knowledge field of Cyber-Physical Systems,
- to describe some of the key areas of application for Cyber-Physical Systems and their potential benefits,
- to describe the principal capabilities and features of Cyber-Physical Systems and the associated technological and social challenges,
- to describe the economic potential of Cyber-Physical Systems,
- to identify and classify the key research areas and establish where innovation initiatives are required,
- to provide recommendations for decision-makers from sciences, economy, politics and society,
- to raise awareness regarding the opportunities and challenges, both among the relevant experts and among the public as a whole and
- to contribute to the academic debate on Cyber-Physical Systems.

[1] Any terms or parts of terms written in italics are explained in the glossary.

In particular, the analysis of the issues presented in the agenda is intended to serve as the basis for comprehensive recommendations.

1.1.1 STRUCTURE OF THE REPORT

In accordance with the goals of the agenda, Chapter 2 uses a handful of selected future scenarios to look at the technology and application trends of Cyber-Physical Systems. The scenarios provide a basis for describing the nature of Cyber-Physical Systems, their capabilities and the innovation potential and potential benefits associated with them. The areas of application and application scenarios that have been selected are:

- *smart mobility* concepts featuring extensive coordination, comfort and *safety services*,
- telemedicine and comprehensive patient care, including the use of medical *application platforms* and support from online *communities*,
- *smart grids*, i.e. the distributed and semi-autonomous control of electricity generation, storage, consumption and grid equipment in electricity grids and
- smart and flexibly networked manufacturing.

A systematic analysis of these scenarios enables the key features and new capabilities of Cyber-Physical Systems to be described. These are in turn analysed in terms of the following criteria: the increasing openness of the systems, smart, semi-autonomous networking, adaptation and new forms of *human-machine interaction*.

Based on this characterisation, Chapter 3 addresses the unanswered questions and challenges relating to the future design and implementation of Cyber-Physical Systems' capabilities and potential in the context of the above-mentioned scenarios, which are analysed in depth. The key issues are as follows:

- the need for *smart infrastructures*, application architectures and communication platforms,
- challenges connected with networked acting in uncertain environments, including the systems' control, *safety* and *security*, together with *privacy* protection,
- the design of *human-system cooperation* and the challenges associated with enabling intuitively controllable, safe and secure interactions between human beings and systems and
- factors affecting the acceptance of Cyber-Physical Systems and what this means for the way they are developed.

Cyber-Physical Systems that are networked via the Internet are ubiquitous in nature. This will lead to far-reaching changes in both the public and private domains. Consequently, Chapter 4 of the agenda investigates the impact of the technology, focusing on the design of human-technology interactions. This aspect is especially important, since systems and *services* can only realise their benefits and gain acceptance if they are geared towards their users' and customers' needs and are found to be controllable and trustworthy in use. Both of these criteria are indispensable for the safe and independent use of Cyber-Physical Systems.

The results of the analysis of Cyber-Physical Systems undertaken in Chapters 2 to 4 form the basis for the identification of the key research questions and development goals. Chapter 5 identifies the relevant technologies, *engineering* concepts, research requirements and challenges relating to the design and implementation of Cyber-Physical Systems' capabilities. This allows a preliminary assessment to be made of the extent to which it will be possible to meet the research goals required for the development of the necessary key technologies.

In view of the dynamic and evolutionary nature of Cyber-Physical Systems and their applications, new interdisciplinary development methods and techniques will be required that engage users and customers in order to ensure that the systems are adapted and integrated to meet the needs of different situations. This will require systems engineering concepts to be expanded to include operation, maintenance, continued development and even strategic marketing that are all carried out in partnership between different companies. These new concepts will be implemented through cooperative networks of companies that constitute economic *ecosystems*. Based on this approach, Chapter 6 analyses the technological, methodological and economic challenges facing enterprises and their *business models*.

Chapter 7 presents a summary of the agenda's findings with regard to the potential and challenges associated with Cyber-Physical Systems and the relevant research requirements. Based on these findings and an assessment of Germany's position compared with other countries around the world, a SWOT analysis is performed with a view to finding ways of overcoming the challenges in question. Finally, the conclusions highlight the research, integrated training, policy and economy aspects where action is required.

The evolutionary development of Cyber-Physical Systems is the result of the interplay between technological advances, the resulting social and economic potentials and the possible use in economic and social processes. In order to gain an understanding of Cyber-Physical Systems, it is therefore necessary to adopt an integrated approach and to ensure *participatory development*. This interdisciplinary approach and cooperation between all the relevant actors through open innovation systems and ecosystems is indispensable if the full potential of this technology is to be unlocked. It is our hope that agendaCPS will contribute to furthering this understanding.

1.2 CYBER-PHYSICAL SYSTEMS – TRENDS AND CHARACTERISATION

Ever since it first appeared on the scene, information and communication technology (ICT) has been characterised by a continuous succession of rapid technological advances. The most striking examples are the progressive miniaturisation of integrated circuits and the continuous rapid increases in processing power and network bandwidth. In recent years, this rapid progress has led to a situation where all the performance and bandwidth we need is more or less readily available, meaning that information technology can now be used in every area of our lives. Affordable microcomputers and improved mobile network coverage have extended the reach and interconnectivity of software from beyond the traditional mainframes and home PCs to mobile end devices such as notebooks, tablets and smartphones. IT is everywhere – the vision of *ubiquitous computing* has become reality. Previously closed and proprietary embedded systems and devices and IT-based information and management systems are now becoming increasingly open and connected to other systems. This trend is leading to the emergence of open, networked, flexible and interactive systems that seamlessly connect the physical world with the virtual world of information technology. As a result of their multiple interconnections and the incorporation of data and *services* from global networks, software-intensive systems and devices are increasingly being transformed into integrated global services and solutions that are used in every area of our lives.

1.2.1 THE POTENTIAL OF CONVERGING CPS TRENDS

Cyber-Physical Systems are the product of the ongoing development and integrated utilisation of two main innovation fields: systems containing embedded software and global data networks like the Internet, featuring distributed and interactive application systems. These are enabled by a powerful infrastructure comprising *sensors, actuators* and communication networks that are employed by companies acting and cooperating at a global level.

The following technologies and trends act as the key drivers:

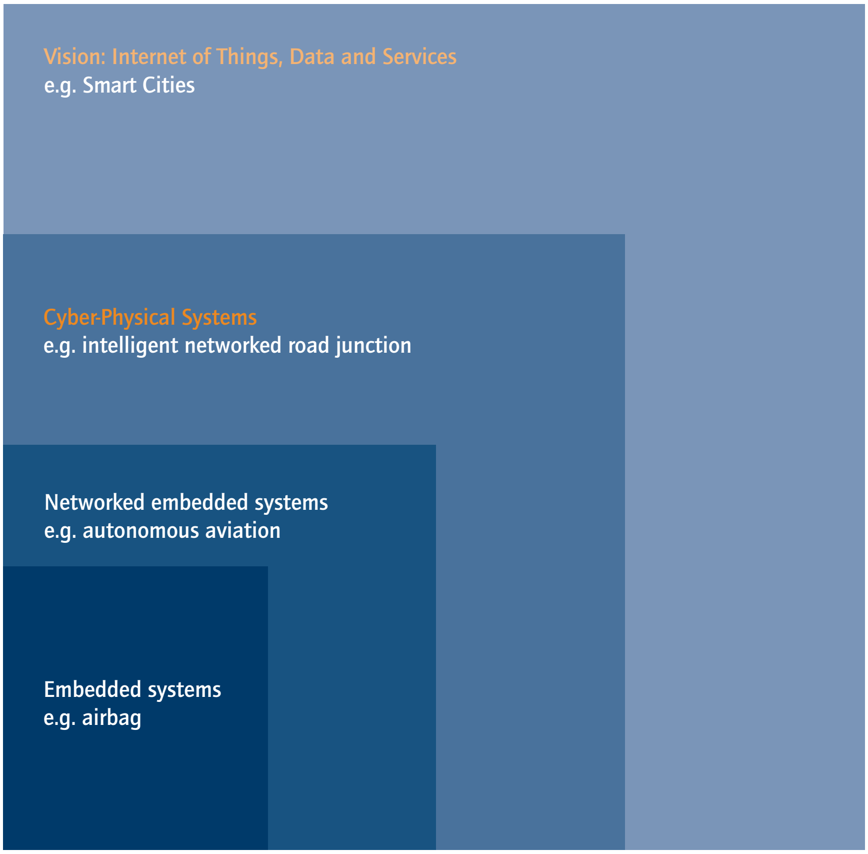
1. The use of powerful *smart embedded systems*, mobile *services* and *ubiquitous computing*:
   One of the basic key components of Cyber-Physical Systems involves powerful embedded systems that already operate in a cooperative and networked manner today, albeit as closed systems. Localised but increasingly mobile *sensor*, regulation and control *services* already exist, mainly in the automotive and aviation industries but also in manufacturing. The increasingly open networking, interaction, cooperation and use of mobility *services* and other online *services* is leading to a variety of novel alternatives and potential uses in several different fields of application and areas of our lives.

2. The use of the Internet as a *business web*, i.e. as a platform for economic cooperation, in two mutually complementary manners:
   - **a)** The use of smart, networked components fitted with *sensors* – as in *RFID* technology, for example – is particularly widespread in commerce and logistics but also occurs in other fields of application such as remote equipment maintenance. Increasingly, the status and environmental monitoring functions and "memory" of digital components are also being used for networked control, coordination and optimisation e.g. of goods flows, maintenance procedures or fleet management. Moreover, the status of and interactions between objects and *services* can increasingly be followed and interactively influenced by customers online.
   - **b)** Traditional IT and administrative tasks are increasingly being farmed out to the *cloud*, i.e. to globally distributed external service providers. This means that they are no longer dependent on local data centres. The same also applies to functions in the areas of distributed coordination, operations and billing. The *business web* makes it possible to represent the capabilities and *services* provided by Cyber-Physical Systems on the Internet and enable their use as online *services*. It forms the basis of integrated Web-based *business models*.

3. The use of the *semantic Web* and *Web 2.0* processes and the interactive design of integrated *services*:
   - **a)** The opportunities provided by user-controlled interactions and the resulting creation of knowledge and communication networks and online *social communities* is generating huge volumes of data and information that can be used to specifically target potential customers. Moreover, requirements and demand for new *services*, integrated solutions and facilities are now arising, particularly in connection with self-organising expert, application and interest groups as well as *business-to-business* applications and corporate partnerships. It is possible to provide these *services* thanks to the way that Cyber-Physical Systems connect the virtual, physical and social worlds.
   - **b)** Developer *communities* can contribute to these innovations. These *communities* tend to focus on specific development platforms and usually involve *open-source* initiatives to develop software using open-source codes. They may be self-organising or be overseen by a company or consortium. Other self-organising *communities* focus on specific fields of application, i.e. they are driven by a particular problem that has been encountered by users and customers or comprise a social network of experts in a specific field.

The interaction between these trends – and in particular the evolutionary development of open interactions with users and customers and the applications that this enables, as described in (1) and (2) above – harbours huge potential for innovation and value creation going forward. This will result in dynamic and disruptive changes to markets,

Figure 1.1: The evolution of embedded systems towards the Internet of Things, Data and Services


Vision: Internet of Things, Data and Services
e.g. Smart Cities
Cyber-Physical Systems
e.g. intelligent networked road junction
Networked embedded systems
e.g. autonomous aviation
Embedded systems
e.g. airbag

industry *models* and *business models*. Figure 1.1 illustrates this trend from the viewpoint of the embedded systems expert community.

Two things are occurring as far as the technology itself is concerned. Networked and increasingly smart *RFID* and *sensor* technology continues to be developed and is now generally referred to as the *Internet of Things* [BMW09, UHM11b]. This has implications for commerce and logistics. Meanwhile, in the realm of the *Internet of Services*, the range services and technologies in the fields of e-commerce, online *services* and media management continues to expand; see also the Theseus research programme [BMW10b].

1.2.2 INITIAL CHARACTERISATION OF CYBER-PHYSICAL SYSTEMS

The term Cyber-Physical Systems refers to embedded systems, i.e. devices, buildings, vehicles and medical equipment, as well as logistics, coordination and management processes and Internet *services* that

- use *sensors* to directly capture physical data and *actuators* to affect physical processes,
- interpret and store data which they then use as the basis for active or reactive interactions with the physical and digital worlds,
- are connected to each other via digital networks that may be wireless or wired and local or global,
- use data and *services* that are available globally,
- possess a range of *multimodal human-machine interfaces*, offering a variety of differentiated and dedicated options for both communication and control, for example using voice and gesture commands.

Cyber-Physical Systems enable a variety of novel functions, services and features that far exceed the current capabilities of embedded systems with controlled behaviour. Powerful Cyber-Physical Systems are able to directly register the situation of their current distributed application and environment, interactively influence it in conjunction with their users and make targeted changes to their own behaviour in accordance with the current situation. The systems thus provide their *services* to the relevant users and *stakeholders*

- largely independently of their location,
- but nevertheless in a context-aware manner,
- in accordance with the requirements of the current application situation
- semi-autonomously,
- in a semi-automated manner,
- multifunctionally and
- in a distributed and networked manner.

Examples include situation-based management of integrated transport solutions or online healthcare *service* coordination. A particularly significant feature of Cyber-Physical Systems is the fact that they are directly integrated into the physical world ("real world awareness").

One of the key contributions of this study consists in analysing these features and the novel capabilities of Cyber-Physical Systems as well as their different potential applications and innovations.

1.3 THE IMPORTANCE AND POTENTIAL OF CYBER-PHYSICAL SYSTEMS FOR GERMAN ECONOMY

As a result of advances in information and communication technology (*ICT*) and the way it is networked, previously separate industries are becoming connected to each other and *ICT* is becoming an integrated part of products and *services*. There are very few industries that do not now use *ICT* to improve their internal processes. Manufacturers are increasingly using embedded information technology and integrated *services* to add value to their products. The opportunities provided by networked data acquisition and interactive support for customer and user processes hold huge potential for innovation and new *business models*. More and more, information and smart information processing are becoming the key enablers of a business's competitive success. This involves putting the data and information generated by Cyber-Physical Systems to good use. It is also especially important to understand how current and future customer needs can be better met through the use of smart, networked technology. The rapid pace of these developments has huge implications for the future prospects of industries where Germany is currently a world leader.

The **automotive industry** illustrates the potential and significance of Cyber-Physical Systems perhaps better than any other. The vast majority of innovations that lead to greater safety, comfort and efficiency are now coming about thanks to Cyber-Physical Systems. Vehicles are being connected with each other, with objects in their environment and increasingly also with external information systems and mobile end devices belonging to drivers and other actors. The German automotive industry invests approximately 20 billion euros in R&D, or more than a third of all industrial R&D investment in Germany. It also employs around 715,000 people [Sta11]. It is therefore crucial to German industry as a whole that the automotive sector should play a leading role in the research, development and deployment of Cyber-Physical Systems. The link with the trend towards electric mobility[2] provides Germany with a particularly good opportunity to become established as a leading supplier of Cyber-Physical Systems. For example, route management for battery-powered cars or the integration of electric vehicles into the energy infrastructure[3] would simply not be possible without Cyber-Physical Systems. Time is running out, since the race is already well underway in the automotive industry to network vehicles[4] and provide drivers with wide-ranging support in a variety of different driving and communication situations.

Medical technology is one of the largest growth industries around the world. R&D investment in this sector accounts for some eight percent of turnover, approximately double the average for industry as a whole [BW08]. The German medical technology industry estimates that its turnover will increase by around eight percent a year between now and 2020.

In addition to remote monitoring of vital signs, implanted devices and integrated patient care, networked sensors and innovative devices also enable better diagnosis and treatment options. Furthermore, they provide a variety of opportunities to optimise healthcare delivery processes, for example emergency service responses or enhanced individual patient care in hospitals. Many of the innovations in this area are only possible thanks to the fact that devices which were formerly used in isolation are now able to communicate with each other and because data and information can now be linked up according to the requirements of each specific situation. Demographic change is going to lead to increased demand for ways of supporting older people so that they can live independently in their own homes. *AAL* solutions (*Ambient Assisted Living*, see also Chapter 2.3) can only be delivered through Cyber-Physical Systems.

Our supply of fossil fuels is dwindling and climate protection is becoming an increasingly important issue. Efficiency, usage optimisation and individual demand coverage in the generation, distribution, storage and consumption of energy are therefore key issues. This is true for the **energy industry**, for policymakers and for **consumers**, whether they be businesses, public buildings or private homes in towns and cities or rural communities. There are a number of challenges in this context – in addition to the fluctuating supply of renewable electricity and the decentralisation of energy production and distribution via *smart grids*, it is also necessary to meet a whole host of different requirements that arise as a result of consumer behaviour. Cyber-Physical Systems will play a key role in grid management, coordinating and optimising consumption and energy production planning.

The potential and challenges associated with Cyber-Physical Systems are particularly apparent in the **machinery and plant manufacturing**[5] and **automation engineering industries.**[6] Quality, optimisation and efficiency gains are enabled by sensor-based networking of smart machines and products both with each other and with global production planning, energy management and warehousing systems that may be shared between several different companies. In particular, these benefits occur as a result of the ability

[2] See e.g. [BDD+11].

[3] Without the ability to optimise charging times or coordinate the available energy supply and the times when people charge their vehicles, peak demand would quickly hit critical levels even before electric vehicles came into widespread use. In other words, it is necessary for the charging of electric vehicle batteries to be controllable either by individual users or by a service provider; for further details, see [GMF09, Sch10b].

[4] See for example [car11].

[5] At the end of 2010, some 913,000 people were employed by Germany’s machinery and plant manufacturing industry. German businesses are market leaders in several different branches of this industry. See [VDM11].

[6] See also “Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution” [KLW11].

to adapt production flexibly to customers' processes and to control globally distributed logistics processes accordingly.

Cyber-Physical Systems are capable of standardised self-description and of *self-organisation* using standard mechanisms. This enables factories and manufacturing systems – even spread across several different companies – to adapt and optimise their manufacturing and logistics processes in line with individual customer requirements. Self-organisation through goal-oriented negotiation of work-pieces, equipment and material flow systems results in these processes becoming significantly more flexible – whilst today they are based on a central planning approach, in the future they will be characterised by a decentralised optimisation approach.

Mobile communications are a key basic technology for Cyber-Physical Systems, since many applications depend on the networking and integration of mobile devices via a reliable and high-performance mobile communications infrastructure. The number of mobile Internet users in Germany as a proportion of the total population is set to rise from 21 percent to more than 40 percent by 2014.[7] There is also significant potential for growth in the fields of **positioning and navigation**. The global market for end devices with integrated GPS receivers is expected to double in size between 2009 and 2014[8]. New programs providing greater precision and simpler market access, such as the Galileo satellite system, will allow this technology to become even more widespread and enable new applications, particularly in networked systems. Furthermore, mobile communications data and geo-information can be used for a variety of applications such as route optimisation and congestion avoidance by deriving information about congestion from the current movement profiles of networked vehicles and road users.

Germany offers a unique set of conditions for developing Cyber-Physical Systems applications even before the actual infrastructure is operational, as demonstrated, for example, by the German Galileo test environment GATE [GHW10].

In the **logistics** and the goods transport sectors, it has become standard practice to use technology that is networked with the manufacturing environment in order to identify, locate and establish the status of goods. The use of Cyber-Physical Systems in logistics promises new applications thanks to smart, active objects and large-scale open infrastructure networks. These include functions such as end-to-end position tracking and *real-time* status queries that provide new opportunities with regard to the coordination, planning and control of goods transport. At the same time, this area serves as a good example of the networking and coordination challenges that will have to be met by Cyber-Physical Systems.[9]

In the field of **smart buildings and homes**, Cyber-Physical Systems enable the upkeep and maintenance of buildings, facilities, residential areas and business parks to be integrated into people's domestic and working lives. Support is provided through integrated *security* strategies and measures to increase *energy efficiency*, for example through smart management of decentralised energy generation systems such as *solar* PV.[10] Moreover, there are a number of additional applications for industrial buildings and manufacturing facilities, e.g. with regard to the interactions between building and machinery control systems. However, this will require cooperation between systems that have traditionally operated independently of each other. The smart buildings sector forecast that its sales would grow by five percent in 2011. The key growth drivers are investments in measurement, control and regulation technology and in the associated building management systems. These investments

[7] See [GS10]. The introduction and deployment of the Long-Term Evolution (LTE) mobile communications standard and the associated networks will be essential in order to enable permanent networking of end devices.

[8] See "Global Navigation Satellite Positioning Solutions: Markets and Applications for GPS" [ABI09].

[9] For further details, see e.g. the Collaborative Research Center on "modelling of large-scale logistics networks" [SFBa].

[10] This area has huge potential, since buildings account for more than 40 percent of total energy consumption in Germany [BRO11].

have a much shorter payback period than investments in other energy measures. Moreover, the technology can generate efficiency gains by interacting with manufacturing systems and vehicles.

All of the above examples illustrate the enormous potential for innovation of Cyber-Physical Systems and how they are capable of transforming industry and our everyday lives. This was also demonstrated by the cutting-edge presentations about the latest ICT- and CPS-driven *services*, applications and *business models* at the Mobile World Congress 2012 [RGH12, Sch12, Ohl12, GL12, Kes12]. One feature shared by all the examples is the way that the value creation process is transferred to networks of several different companies, often from different industries, that cooperate with each other in a variety of different ways. Companies of different sizes from many different sectors and fields of application are increasingly collaborating both with each other and with service providers, software manufacturers and telecommunications providers. The effect is to bring together the competencies needed to produce innovations across all the areas of value creation associated with Cyber-Physical Systems. Supported by a close interaction with the systems' customers and users, this is resulting in product innovations that span several different industries, shifting the boundaries of existing markets and leading to rapid convergence of markets that were previously discrete.

1.4 METHODOLOGY AND PROCESS

Figure 1.2 provides an overview of the study design and the process that was followed. The core of the project focused on the modelling and analysis of future scenarios based on the established *requirements engineering* approach of analysing use cases and scenarios.

1.4.1 SCENARIO ANALYSIS AND STRUCTURED IDENTIFICATION OF CPS CAPABILITIES AND CORE TECHNOLOGIES

A number of use case scenarios were devised in order to determine the required features and capabilities of Cyber-Physical Systems and the challenges associated with their innovative design.

1.4.1.1 Analysis methods and structural design of the agenda

Based on the description of various scenarios and the actors, components, systems and *services* involved in them, all of which were assumed to behave optimally,

- the different applications' users and *stakeholders* were identified,
- their goals and the system's operation and architecture (interactions, roles and tasks) were analysed and
  a) the benefits and value-added for the *stakeholders* and
  b) the capabilities needed by the relevant (individual and networked) Cyber-Physical Systems and associated *services* were identified.

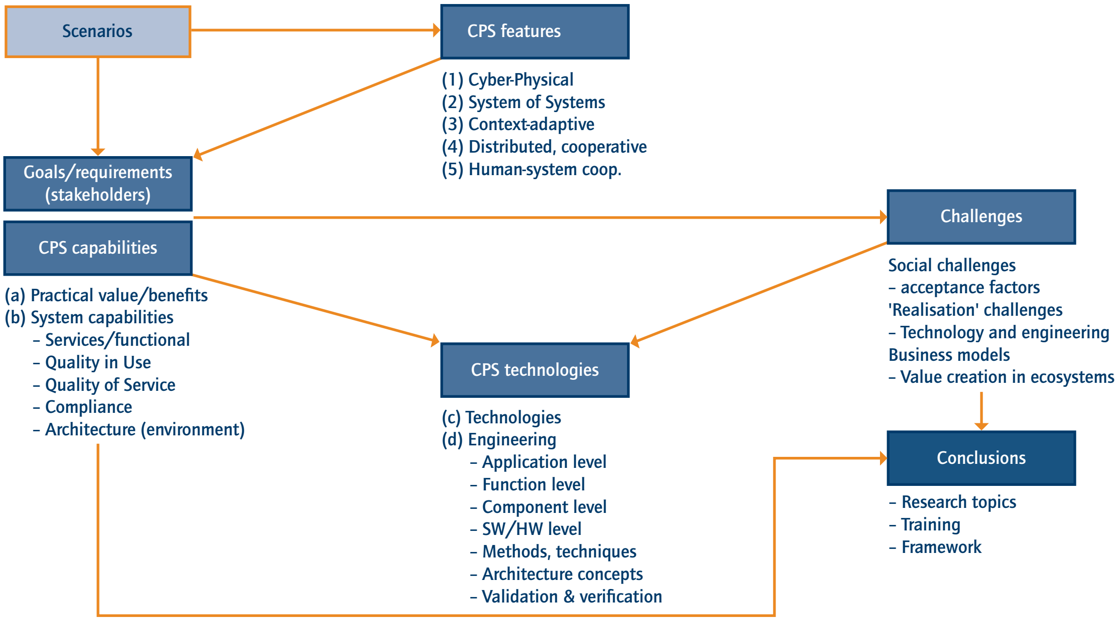
Following on from this analysis of their capabilities, the new evolutionary and revolutionary features of Cyber-Physical Systems were systematically described:

(1) merging of the physical and virtual worlds
(2) *a System of Systems* with dynamically shifting system boundaries
(3) context-adaptive systems with fully or semi-autonomous operation, active *real-time* control
(4) cooperative systems with distributed changing control
(5) extensive *human-system cooperation.*

These properties and capabilities entail a variety of opportunities and challenges with regard to the realisation and

Figure 1.2: Methodology and process employed in the agendaCPS project. CPS use scenarios [light blue] with different use goals and stakeholder requirements [blue] were used to identify characteristic Cyber-Physical Systems features [blue] and the required CPS capabilities [blue]. These were in turn used to identify the economic and social challenges [blue] and required technologies [blue]. All of the above provided the basis for establishing the action required with regard to integrated research and education [dark blue].

OVERVIEW OF THE AGENDA'S ANALYSIS METHODS AND STRUCTURAL DESIGN



control of innovative CPS *services* and applications. There are several as yet unanswered questions concerning e.g. social acceptance, conflicting goals and the need to guarantee enhanced *safety, security, dependability* and *privacy* protection. Furthermore, it is necessary to identify any gaps in the designs and solutions, the relevant technologies and the key research topics and formulate the corresponding strategies to overcome and find solutions to these problems. In order to do this, we once again draw on the use case and scenario analysis and the structured description of the core CPS technologies and *engineering* capabilities.

The trends, system transformation and dynamic nature of the innovations associated with CPS mean that traditional system developers, industries and service providers are faced with major challenges to their businesses. The system transformation referred to above and the complexity of Cyber-Physical Systems' open networks make it necessary to develop the functions and roles performed by the companies involved in them. This will require new *business models* and new forms of organisation and cooperation. The architecture of these *value networks* and *application platforms* is also addressed, based on the analysis and modelling of the CPS scenarios and their underlying system architectures.

Chapter 7 draws on the results of the analysis to provide a summary of the key challenges posed by Cyber-Physical

Systems for research, development, industry and society. It also identifies the actions that are required, particularly in the field of training and development of the necessary *engineering* know-how.

1.4.1.2 Taxonomy of CPS capabilities

The analysis of typical use case scenarios identifies and classifies Cyber-Physical Systems' capabilities based on the following four criteria:

a) Benefits

This describes the benefits and value-added that a Cyber-Physical System provides for its user groups. In addition to customers and end users, these can also include companies, organisations and social groups that are affected in a more general sense. We describe the benefits, *services* and functions that Cyber-Physical Systems provide to these groups and the value-added that accrues from their use (value/*Quality in Use, value proposition*). Examples of the benefits include efficient healthcare, enhanced overall road traffic *safety* and protection and, more specifically, improved comfort and assistance for drivers and passengers in towns and cities.

b) System capabilities

This describes the capabilities (functions, services, features) that Cyber-Physical Systems possess or provide which are required in order to deliver the benefits of CPS applications as described in (a) or to meet the challenges and threats associated with the application (*data protection, data security, loss of control*) or its interaction with other systems and actors. As in (a), we consider the capabilities required for a total system comprising the relevant application situations, processes and goals to function correctly. These include generic capabilities, such as searching for the appropriate *services* on the Internet or personal data protection, and application-specific capabilities such as route optimisation, influencing traffic flow at junctions by synchronising traffic light phases based on current measurements and in accordance with a pre-defined strategy, secure communication between vehicles and the creation of a model of the surroundings including position location.

c) CPS technologies

These include existing and as yet undeveloped components, technologies and processes (for software, electronics and mechanics) that are needed to implement CPS applications in such a way that the system capabilities described under (b) can be controlled and the benefits referred to under (a) can be delivered. Examples of CPS technologies include *pattern recognition, smart sensors, real-time* control, IP protocols as frameworks for governing Internet communication and encryption technology. The technologies concern different system levels and architectures: total systems, *human-system-environment interaction* and interfaces, networking, subsystems, software and hardware, *security* technology and communications technology.

d) Engineering capabilities

These include the necessary *engineering* capabilities and skills (principles, processes, methods, techniques and *best practices* as well as integrated multidisciplinary tooling concepts) to enable the targeted development, design, implementation, operation, evolution and sustainably profitable deployment of Cyber-Physical Systems using the capabilities and features outlined under (a) and (b). Examples of these capabilities include methods for modelling, *requirements specification*, design engineering and end-to-end quality assurance (*validation* and *verification*), as well as the use of architecture principles and concepts for meeting non-functional requirements such as *usability, dependability, safety, security* and *privacy* protection.

1.4.2 VALIDATION OF THE RESULTS

Our work was supported and accompanied by expert workshops, interviews and a systematic analysis of current academic and applied research programmes, projects and initiatives. The results and key conclusions of the project were analysed and systematically consolidated in successive rounds of workshops with our partners from industry and the research community.

The results presented in this study are intended to serve as a basis for subsequent, more in-depth investigations of core CPS capabilities and technologies, their potential, the associated challenges and the (research) work that still needs to be done. Our aim is to lay the foundations for a full and open debate on the importance of Cyber-Physical Systems to our society.

2 CYBER-PHYSICAL SYSTEMS: VISIONS, CHARACTERISTICS AND NEW CAPABILITIES

The potential of Cyber-Physical Systems can be realised in a variety of different scenarios. This is particularly true when different fields of application are combined as in the case of the "smart city". Figure 2.1 outlines an example of possible CPS application systems and how they relate to each other as components of "smart cities" and economies. Future CPS scenarios and their potential benefits could conceivably come about in many different but interconnected application areas and scenarios.

In order to describe Cyber-Physical Systems and their potential and to analyse the associated challenges, we have chosen to begin by outlining a number of key CPS scenarios:

- *smart mobility*
- remote medical care and diagnosis *(smart health)*
- *smart grids*
- smart manufacturing networks (*smart factories*).

Reader's guide to the scenarios:
The future scenarios in this section are described in the form of model future use case scenarios. They act as visions that vividly illustrate the innovation potential, novel functionality and excess value that Cyber-Physical Systems can bring to our society and economy.

In particular the first two scenarios – *smart mobility and smart health* – are used to identify and analyse the specific capabilities and potential benefits of Cyber-Physical Systems in these contexts. Their significance is described systematically and in detail in section 2.6.

Based on the analysis of the scenarios, Chapters 3 and 4 go on to take a comprehensive look at the issues and requirements connected with the technology, design and utilisation of the systems and the challenges associated with the research and development of innovative systems and applications.

In keeping with the agenda's methodology as outlined in Chapter 1.4, these results form the basis of a detailed analysis and assessment of the current state of the technology (Chapter 5) and of Germany's ability to deliver innovations in the field of Cyber-Physical Systems (Chapters 6 and 7).

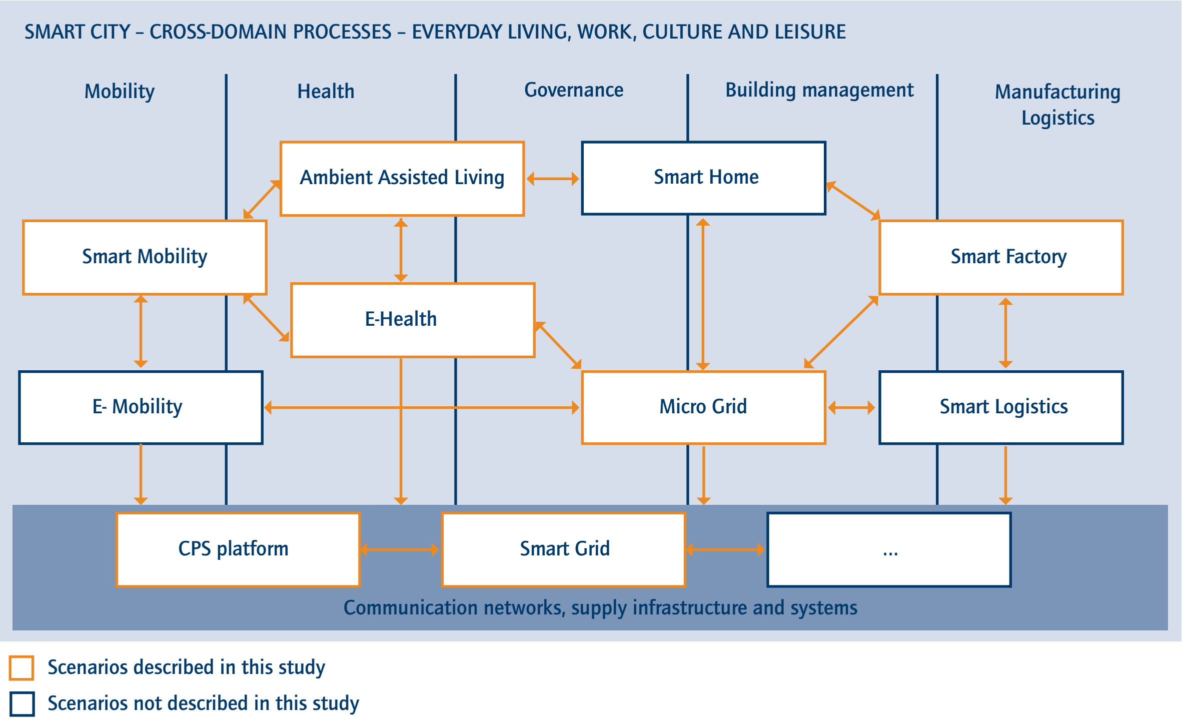
2.1 INTERCONNECTED APPLICATION AREAS

Figure 2.1 is constructed along the lines of a relational model in order to illustrate one key aspect of how things are expected to develop going forward: rather than developing in isolation from each other, the future scenarios will form part of global use case scenarios and will be characterised by numerous interconnections, interdependencies and interactions. These interactions will be so extensive that a lack of certain developments in one scenario could result in neighbouring scenarios being unable to create the conditions needed for them to maximise their potential.

The basis for the description of this relational model is an electric mobility scenario. The model illustrates its relationships and interactions with other domains.

It is apparent from the illustration that various interactions exist between electric mobility and the domains of manufacturing and logistics. Key aspects such as context-based optimisation of route planning and traffic management are especially important for electric vehicles, since it is compulsory for their route planning to take into account the locations where charging stations are available. As soon as an electric vehicle connects to a charging station it becomes integrated into the *smart grid* and can thus also be used as a peak load buffer, for example. Particularly in a grid that is heavily dependent on renewables, it is important not only to plan for electricity demand for charging vehicles in different regions and at different times but also to leverage the potential for using large numbers of electric vehicles connected to charging stations as peak load buffers.

Figure 2.1: Interconnected CPS application areas and global application processes. The scenarios are described in detail in sections 2.2 to 2.5.


SMART CITY – CROSS-DOMAIN PROCESSES – EVERYDAY LIVING, WORK, CULTURE AND LEISURE
Mobility
Health
Governance
Building management
Manufacturing Logistics
Ambient Assisted Living
Smart Home
Smart Mobility
Smart Factory
E-Health
E- Mobility
Micro Grid
Smart Logistics
CPS platform
Smart Grid
...
Communication networks, supply infrastructure and systems
Scenarios described in this study
Scenarios not described in this study

Having energy available at the right time is a key control variable for the networked and flexibly integrated manufacturing system described in the *smart factory* scenario. It is important to ensure that energy-intensive manufacturing steps are moved to times when cheap electricity is available. In the future, these times will also be flexible. By the same token, starting and stopping manufacturing steps or changing the time when they are performed has a feedback effect on the *smart grid*. Thus, the *smart factory* and the *smart grid* are closely interconnected. Meanwhile, *smart logistics* provide the link between *smart factories* and the customer. Transport costs are an important planning consideration when trying to achieve greater flexibility across several different manufacturing facilities. Ultimately, *smart logistics* are used to bring the finished goods to the customer.

In addition, private homes and companies act as nodes in *smart grids* as well as in smart logistics networks. Cyber-Physical Systems find their way into people's homes in the shape of smart meters and other *smart home sensors*, enabling a whole host of new home automation *services*. These are of particular importance to older people in the context of *Ambient Assisted Living (AAL)* – Cyber-Physical Systems can enable the elderly to live independent lives in their own homes for longer. This is done by combining Cyber-Physical Systems from the *smart home* and *E-Health* domains. An example of these systems' capabilities is the ability to trigger an alarm if they detect that a room has been empty for more than a pre-defined period of time while an oven or iron is on.

These systems can provide older people with significant support, and their benefits also extend to the domain of *smart mobility*. Future driver assistance systems will be especially beneficial for the elderly, allowing them to keep driving for longer. This is the final connection that closes the loop in the relational model.

The model also illustrates a distinction between different types of Cyber-Physical Systems. On the one hand, there are the horizontally interconnected infrastructure systems such as *smart grids*, traffic management systems or global logistics networks that are connected in *real time*. However it is also possible for *interoperable* CPS application systems and scenarios to be built on top of these systems, as in the integrated *smart home* concepts described above that include *AAL* support for the elderly or the use of smart, networked *safety* and assistance systems by individual drivers (see also 2.2).

Depending on their functions, the goals for which they are used, the contexts in which they are employed and the goals of the different actors, Cyber-Physical Systems can be said to differ from each other in the following respects:

- the degree of networking that occurs – where relevant in *real time* – and the extent of cooperation between subsystems
- the nature and extent of the *human-system interaction*. In industrial applications, this is characterised by complex operational, monitoring and coordination tasks. In the context of private use, on the other hand, the systems have to adapt interactively to the user's context, needs and capabilities, especially in the case of AAL applications. They need to be capable of adapting in this way in order to accurately interpret different situations with the aid of networked *sensor* and application data and coordinate and manage complex requirements in an appropriate and interactive manner
- the extent to which they operate openly and autonomously when resolving communication, coordination, control and decision-making tasks and their *dependability* and predictability for users and other connected systems.

The underlying infrastructure systems need to satisfy particularly exacting requirements in terms of their *dependability, safety, security* and *integrity*.

2.2 SMART MOBILITY – ASSISTANCE, COMFORT AND SAFETY THROUGH COOPERATING SYSTEMS

The subscenarios that form part of the overall *smart mobility* scenario describe how the future of mobility in our society might look if we take advantage of the rapid advances in information and communication technology. The future that they envision is based on the ability to capture comprehensive information about the environment and connect vehicles and different modes of transport, the transport infrastructure and individuals. This opens up innovative ways of taking account of both individual needs and sociopolitical considerations and contributing e.g. to accident prevention, more efficient use of limited energy resources and the reduction of environmental pollution.

> Sabine Müller is a business woman who lives with her husband and two sons in a small town in west Munich. Her home is situated in a modern part of town equipped with a modern CPS infrastructure – real-time Internet is available everywhere and objects in the district are equipped with sensors, connected to each other, and capable of exchanging data in real time.

The following sections describe three potential CPS scenarios based on different parts of a fictional day in the life of Frau Müller. A brief description is provided of how the scenarios work and the relevant new Cyber-Physical System capabilities are identified. Finally, a summary is given of the excess value and potential that Cyber-Physical Systems have to offer for users, economy and society.

The three scenarios are as follows:

- Cyber-Physical Systems as comprehensive planning and mobility assistants
- road safety improvements achieved through cooperating systems
- efficient and safe travel and the use of autonomous systems to coordinate traffic where space is at a premium.

2.2.1 CPS AS COMPREHENSIVE PLANNING AND MOBILITY ASSISTANTS

Scenario

(1) Frau Müller inputs her intention to visit her mother on Friday morning into her *mobile device*. The only information that she provides are the times and destination and a maximum cost for the entire journey. Her *mobile device* is connected to various different service providers and comes up with several options for her journey from west Munich via the city centre to pick up her children and then on to her mother's home in the east of the city. She decides to use public transport to travel to the suburban railway station near her children's school, since this is the cheapest and most energy-efficient option. Frau Müller then intends to pick up her children at the station and complete their journey to her mother's home in a car share vehicle (*CSV*). She explicitly opts for a hybrid, *autonomous driving* enabled vehicle. All the relevant travel documents such as the suburban railway ticket and the *CSV* authorisation are sent to Frau Müller's *mobile device*.

(2) Before she begins her journey, Frau Müller is informed by her *mobile device* that there has been a signal failure on Munich's suburban railway and major delays are expected. Her *mobile device* recommends booking a *CSV* to cover the first part of her journey from her home as well. When Frau Müller accepts this recommendation, her suburban railway ticket is automatically cancelled and a *CSV* authorisation for the journey from her home is sent to her *mobile device*. Soon afterwards, Frau Müller is informed that the *CSV* will be arriving at her home shortly.

(3) At the same time, her children are informed that their mother will now be picking them up outside their school in a *CSV*.

How it works

Frau Müller's *mobile device* connects her to the Internet and her own *Private Cloud*[11]. Upon request, an assistant or *"assistance app"*[12], running either locally on a *mobile device* or in the *cloud*, automatically comes up with suggestions to help the user plan their day and even makes travel arrangements on their behalf. The assistant suggests various alternatives based on information about the date, time, destination, any stop-off points on the journey and the maximum budget. In order to do this, it obtains online data on traffic volume and congestion along the entire route and on the children's school hours from service providers such as local public transport operators, *car sharing* centres or traffic management systems[13]. Once the options have been computed, they are displayed in order of how closely they meet the user's needs.

Once the user has made their choice, the assistant continually monitors the journey plan in the background and alerts the user as soon as a problem occurs or there is a change to the chosen route. If a new route is required or it is necessary to use a different mode of transport for part of the journey, and if this affects departure times or stop-off points along the route, then the assistance *service* informs everyone affected – Frau Müller and her children – as well as devising a new route and requesting or booking alternative transport.

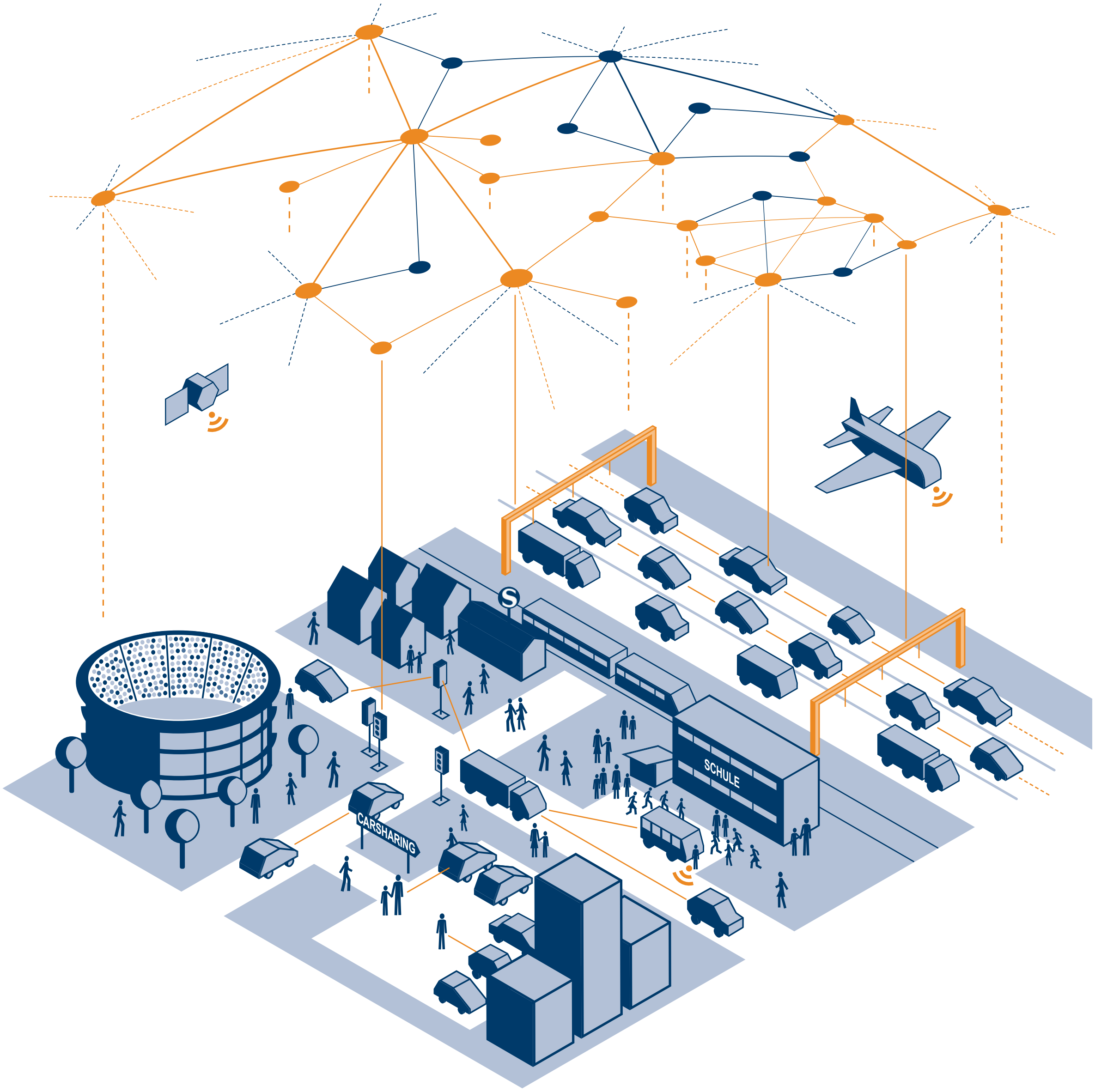
The data from the assistant are also sent to the service computer on board the *CSV* where they trigger various actions. For example, the final destination and stop-off at the school are stored in the vehicle's Sat Nav, information is requested

[11] *Private Clouds* provide access to abstracted IT infrastructures within an individual's private environment.

[12] Also known as software assistance or electronic coaches.

[13] A traffic management system may be physically built onto a particular section of a route or may only exist virtually or be distributed across all the participating vehicles. Instead of a single, central, all-embracing traffic management system, there will usually be several systems that work together.

Figure 2.2: Networked components and actors in a comprehensive assisted mobility scenario and their situation-specific coordination, symbolised by direct connections between actors and with globally networked CPS services



about predicted traffic volumes and any likely congestion along the entire route and preparations are made for the journey, e.g. by downloading films, music and up-to-the-minute information in advance in order to optimise the *CSV* passengers' journey time.

Identified services and capabilities and their excess value

Steps **(1)** and **(2)** illustrate how Cyber-Physical Systems can provide planning and coordination support to arrange a comfortable, stress-free and efficient journey whilst also taking environmental and cost considerations into account. This requires the ability to respond to new situations, since the individual systems are continually exchanging information relevant to the journey, for example about the weather, traffic situation and resources. Frau Müller's assistant coordinates and controls various different subsystems and is capable of using the information it receives to automatically suggest alternative travel arrangements if necessary. This saves Frau Müller time, since she no longer has to search for information about any changes to her travel plans.

2.2.2 ROAD SAFETY THROUGH COOPERATING SYSTEMS

Scenario

Frau Müller is en route to her children's school **(15)** in her vehicle. The vehicle is connected to a *back-end infrastructure* as well as to other road users and provides Frau Müller with significant assistance while she is driving. **(16)** For example, it automatically slows the vehicle down to keep it within the current speed limit. **(17)** As it is about to pass a stationary school bus with its hazard warning lights switched on in the immediate vicinity of the school, the vehicle suddenly performs an automatic emergency stop. Frau Müller sees a child run out in front of her vehicle from behind the school bus. The vehicle stops in time and a glance in her rear-view mirror reassures Frau Müller **(18)** that the vehicles behind her have also used autonomous braking to come to a safe halt. After the briefest of scares, Frau Müller is able to continue her journey. **(19) Once she arrives at the school, her children get in the car and** they depart the school grounds. **(20)** Shortly after setting off, the vehicle receives a notification that particulate pollution has exceeded the daily maximum and only emission-free vehicles are now allowed to continue using the roads. The vehicle checks that its battery has enough charge left and switches to electric mode. Frau Müller can thus continue her journey to her mother's home in the eastern part of Munich.

How it works

The sensors built into the infrastructure on the road to the school (e.g. streetlights, houses, pavements and the school itself) and on board moving and parked vehicles detect objects and people that pose a danger or are in danger themselves. Their position is communicated via the road infrastructure or via vehicle-to-vehicle communication. This information is always communicated instantaneously in *real time*. The assistant on board Frau Müller's vehicle processes the information and decides on the appropriate response to counter the danger, in this case opting for an emergency stop. All the other vehicles in the vicinity are simultaneously informed of this decision both via the infrastructure and via other vehicles. If necessary, nearby vehicles also take measures to counter the danger, for example the vehicles immediately behind Frau Müller also brake.

Identified services and capabilities and their excess value

Steps **(16)**, **(17)** and **(18)** illustrate how the assistants on board Frau Müller's vehicle are able to cooperate with local infrastructure (*sensors* at the roadside, at pedestrian crossings, on board the bus, etc.) and with traffic management systems in order to respond instantaneously by taking the necessary countermeasures when a dangerous situation arises. This could lead to a significant increase in road safety and a substantial reduction in the number of injuries and deaths on our roads.

The economic impact is also considerable. In Germany alone, the direct and indirect cost of road accidents comes to approximately 30 billion euros a year [BAS11]. This figure could be significantly reduced by the use of Cyber-Physical Systems.

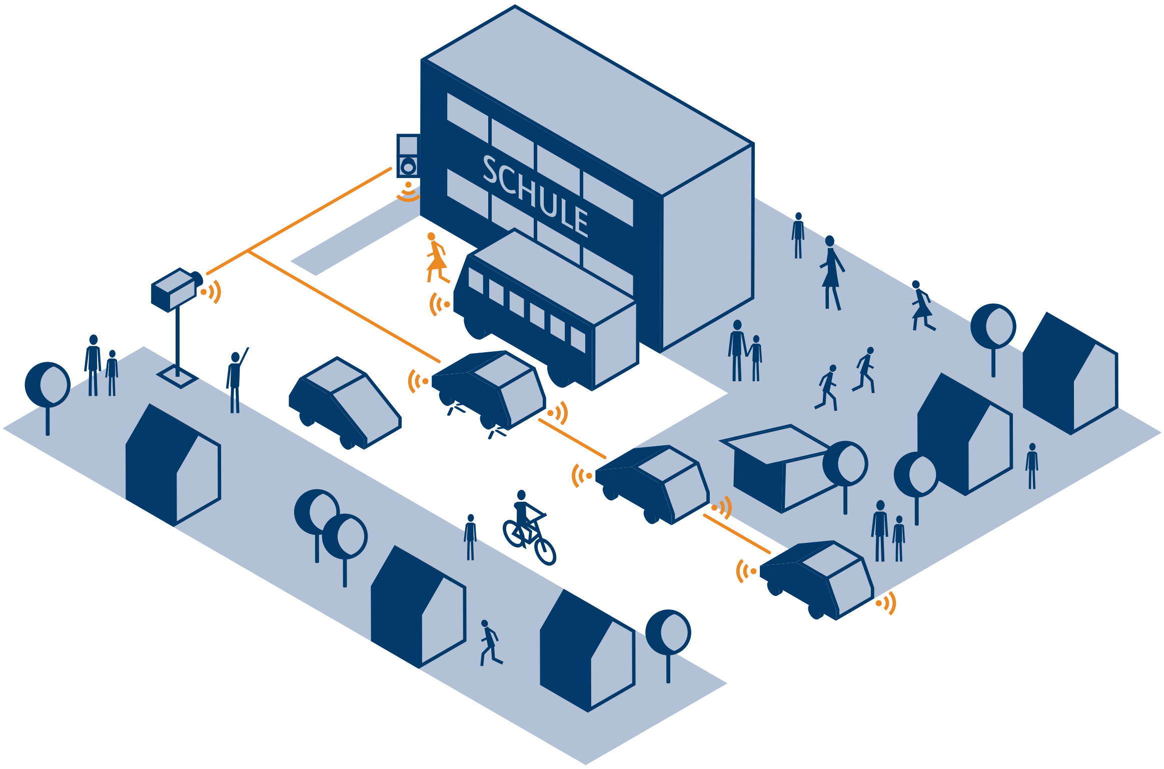
In order to counter the dangers that are described for illustrative purposes in this part of the scenario, Cyber-Physical Systems have to take decisions by themselves and implement them automatically. In our scenario, the vehicle slows down when it detects the school bus. When the child is detected running out into the road, Frau Müller's CSV performs an emergency stop while the vehicles immediately behind her also brake automatically. One important challenge is that it is not possible to assume an ideal scenario where everyone involved is connected to everyone else and all the relevant information is exchanged. It is therefore necessary to base decisions on fuzzy knowledge without this adding to the danger of the situation

2.2.3 EFFICENT AND SAFE TRAVEL AND COORDINATION IN CONFINED SPACES THROUGH AUTONOMOUS SYSTEMS

Scenario

(4) While Frau Müller is driving towards the motorway along a minor road, other cars connected with her own

Figure 2.3: Illustration of networking and adaptive real-time coordination of vehicles and smart infrastructure in a dangerous situation



vehicle inform her of an accident on the road ahead. The central traffic management system suggests an alternative route to her, taking into account the timings, destination and budget that she had previously specified. **(5)** Frau Müller switches to the alternative route and makes it to the motorway slip road with a minimal delay. **(6)** Just before she reaches the motorway slip road, Frau Müller is informed that the vehicle will shortly be switching to autonomous driving mode. Frau Müller authorises the switch and **(7)** the vehicle takes over driving responsibilities as it joins the motorway. **(8)** Since Frau Müller is now running a little late as a result of the accident on the minor road, the vehicle suggests joining the convoy of vehicles on the *premium lane*. Reservation and payment of this chargeable service are carried out automatically by the vehicle. Frau Müller grants her authorisation and the vehicle joins the convoy. **(9)** While travelling in the convoy, Frau Müller is able to use her *mobile device* to answer her e-mails and check up on the latest news. **(10)** While she is doing this, the convoy leaves the *premium lane* (a fast lane that may be used by fully autonomous vehicles upon payment of a charge) in order to let an ambulance through before subsequently rejoining it. **(11)** In order to optimise the traffic flow, Frau Müller's *CSV* is directed to take a different exit to the one that had originally been selected, requiring her to continue her journey on a road that does not support *autonomous driving*. Once again, optimal route guidance will be provided on this road **(12)**. She receives a warning that the vehicle will shortly be leaving the motorway and that it will be returning control to her. Frau Müller stops working on her *mobile device* and starts paying attention to the traffic again. She confirms that she is ready to take over control of the vehicle. **(13)** Shortly afterwards, the vehicle leaves the convoy and exits the motorway, **(14)** returning control to Frau Müller.

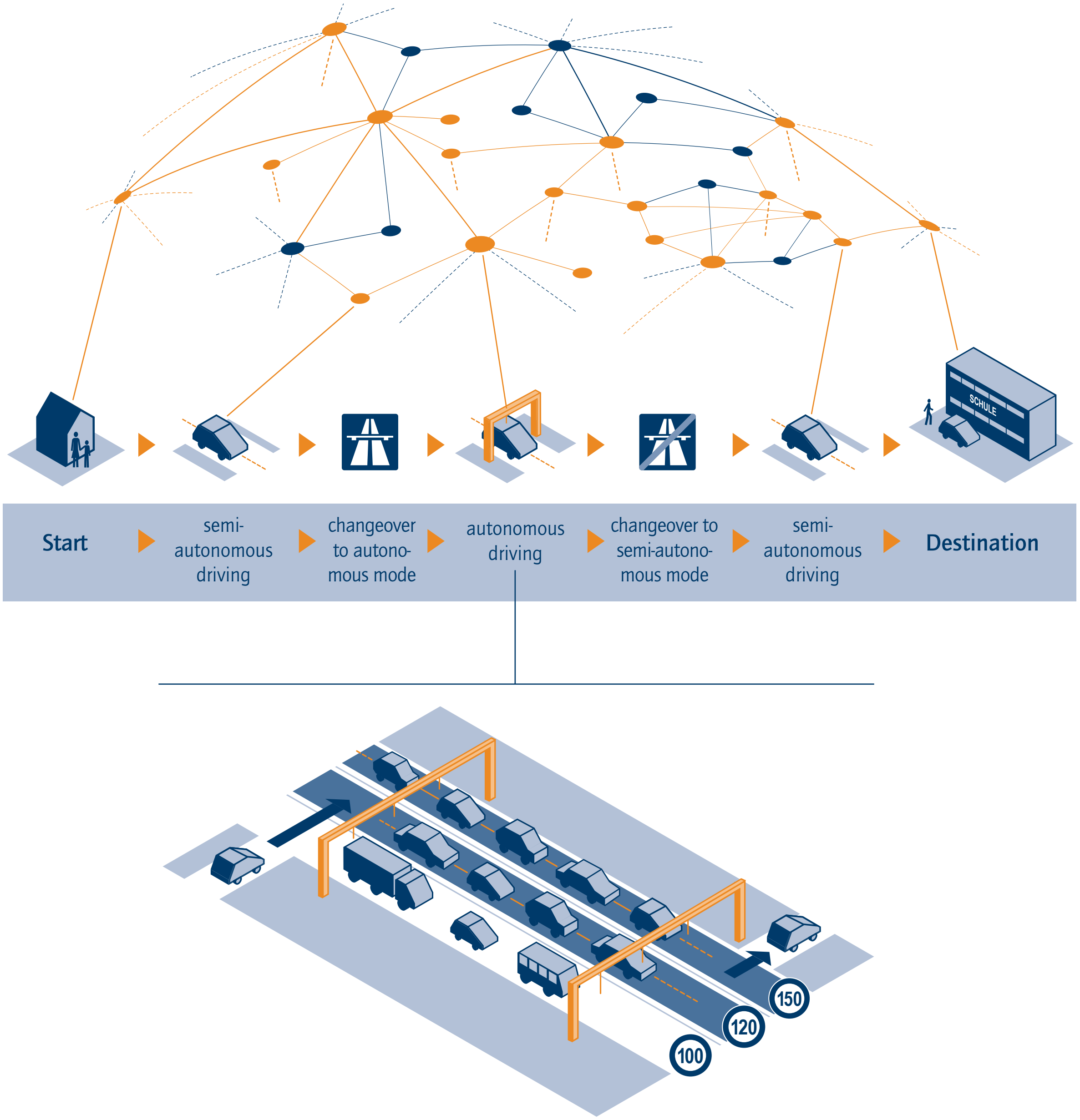
How it works

The autonomous vehicle has access to information about which sections of the existing infrastructure *autonomous driving* is permitted on. These sections must have a fully equipped infrastructure and high-resolution knowledge about the environment. The *human-machine interface* needs to guarantee a controlled and safe changeover from *semi-autonomous to autonomous* mode. Frau Müller's CSV is in communication with both the infrastructure and the other vehicles on the road. Moreover, her position is constantly updated in one or more traffic management systems that use the data provided by the infrastructure and vehicles on the motorway section to create a *virtual* global *model* of the environment. This *model* contains information on stationary and moving objects, including their speed and direction of travel, as well as planned actions, the type of object in question and its danger status. It is also important to take into account that road users who are not connected to the system or are only driving *semi-autonomous* vehicles are also allowed on the motorway.

The excess value of networked, distributed and cooperative traffic management becomes apparent on roads that are equipped with the necessary infrastructure for *autonomous* driving. Special categories of vehicle can be treated differently, as in the case of the ambulance in step **(10)**. It is given priority and the other road users that could slow it down automatically move onto other lanes so that they are not blocking its way. This requires the ambulance to report an emergency that entitles it to priority treatment. The ambulance selects its optimal route based on its starting and destination coordinates and the traffic information that it is able to call up. Meanwhile, the other vehicles on its selected route are notified that a priority vehicle is approaching. For example, the ambulance is given priority use of the *premium lane* on the motorway and the convoy is directed to temporarily leave the *premium lane* before rejoining it once the ambulance has passed through.

Only adequately networked vehicles are allowed onto the *premium lane*. Consequently, it needs to be constantly monitored by the infrastructure and the *sensors* on board networked vehicles to ensure that it is not being used by unauthorised vehicles. In the event of unauthorised use, measures need to be taken to remedy the situation. Frau Müller's *CSV* automatically pays the charge for using the *premium lane* to its operator. The speed of vehicles on the *premium lane* and the distance between them can be adjusted dynamically depending on the state of the traffic. The allocation or choice of junction to exit the motorway is based on information about traffic volumes and congestion en route to Frau Müller's destination.

Figure 2.4: Illustration of the changeover from semi-autonomous to autonomous driving mode and back (scenario steps 8 to 12)

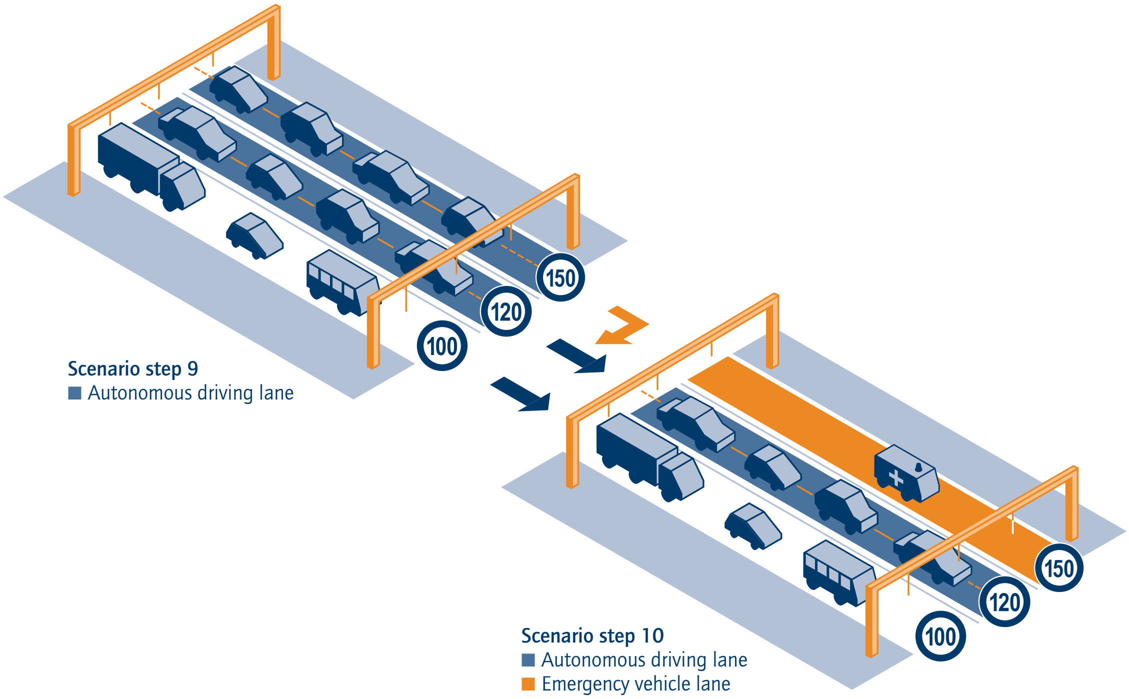


In this scenario, it is important to ensure that control of the vehicle is safely transferred during the changeover from fully to semi-autonomous mode when leaving the motorway. It is especially important to note that a failsafe procedure is in place in case the driver is unable to take over control of the vehicle due e.g. to ill health, tiredness or distraction. Acoustic and visual signals provide the driver with advance warning of the changeover.

Identified services and capabilities and their excess value

In step **(7)**, Frau Müller relinquishes control to her *CSV* which then drives *fully autonomously* on the motorway. This ensures a safe and efficient journey in traffic where space is at a premium. Vehicle networking and cooperating traffic management systems enable all of the vehicles on the road to be controlled safely. This makes it possible to achieve a dramatic reduction in the number of road accidents and the number of injuries and fatalities on the roads. Although 90 percent of road accidents are usually attributed to human error, in actual fact it is not just road users who are responsible but also people and processes involved in the design, *engineering*, organisation and communication of the different environment and system components.[14] *Autonomous driving* requires *interoperable* road infrastructures, networking of road users with each other and the associated continuous exchange of information about vehicles' current po-

Figure 2.5: Illustration of automatic lane mode change to let an emergency vehicle through



sitions and the overall traffic situation. This is supported by smart traffic management systems that can use information obtained from the infrastructure and road users to build up a virtual picture of the environment and make appropriate recommendations with a view to managing traffic volumes and congestion, as in step **(11)**. Traffic management systems thus provide significant economic and environmental excess value by helping to reduce fuel consumption and cut emissions.

In step **(8)**, Cyber-Physical Systems support the decision to travel on a *premium lane* and facilitate automatic payment of the relevant charge. This can be calculated in detail and with absolute precision thanks to the constantly updated information about the position of Frau Müller's vehicle. Since Frau Müller's assistant is connected to her *CSV* in the *Private Cloud* and thus knows her profile, the bill can be settled automatically using her credit card.

2.2.4 CPS AND POTENTIAL BENEFITS FOR THE MOBILE SOCIETY

Mobility is a key social trend and goal. Consistent deployment of Cyber-Physical Systems will provide the mobile society with the following benefits and excess value:

- improvements in road safety, e.g. through
  - detection of hazards and obstructions supported by the exchange of information with other actors
  - automatic hazard avoidance
  - congestion prevention as a result of optimal traffic management
  - *autonomous driving* allowing the prevention of driver error
- enhanced comfort for individual road users, e.g. thanks to
  - smart and autonomous assessment of information and traffic management considerations
  - improved driver assistance and even fully autonomous vehicle control
  - time savings enabled by smart assistants
- reduced environmental impact thanks to
  - less pollution as a result of improved traffic management and lower CO_2 emissions due to reduced fuel consumption
- financial benefits thanks to
  - lower costs resulting from fuel savings
  - more efficient use of the transport infrastructure and different means of transport thanks to the available information and services
  - time savings resulting from congestion avoidance
  - fewer accidents and a reduction in the associated costs.

The excess value is created by the following specific capabilities of Cyber-Physical Systems:

- networking and automatic exchange of information both with the infrastructure and among themselves, using *sensors*, objects and *actuators*
- distributed information and information processing providing a virtual picture of the overall traffic situation, thereby enabling provision of traffic management and coordination *services*
- the ability of Cyber-Physical Systems to take their own decisions and implement them automatically – for example in order to avoid a hazard – even if these decisions are partly based on uncertain data and fuzzy knowledge
- global and local data transmission in *real time*
- the context-sensitive behaviour displayed by Cyber-Physical Systems; the vehicle knows where *autonomous driving* is permitted and where it is not and is able to supply the driver with this information

[14] A number of studies have investigated human error as a consequence or symptom of underlying flaws in the system; see also [Spi63, Dör89, Rea74, Spre07]. Various current studies in the fields of aviation, nuclear power plants and medical technology, e.g. [LPS+97, Hol98], are also looking at whether and under which circumstances systems' susceptibility to errors and accidents increases as a result of complex interactions both between the different systems themselves and with human beings, as seen in Cyber-Physical Systems.

- safe changeover between *autonomous* and *semi-autonomous driving* modes
- enhancement or integration of data from different sources
- dynamic route adjustment based on local conditions such as weather, accidents or traffic volumes
- *autonomous* driving capability
- smart assistants that provide support for journey planning and execution, including automatic *billing* for *premium lane* use enabled by position location and tracking together with retrieval of payment information and automatic access to the actors' profiles in the *Private Cloud.*

However, a number of challenges will have to be overcome in order to enable these system capabilities, including

- implementation of an extensive smart infrastructure with standard interfaces,
- networking of all road users with each other and with the relevant *service* providers; it will be necessary to ensure that *safety, security* and *privacy* are included and properly addressed in this process,
- the *dependability* of systems for autonomous braking or obstruction avoidance using secure external data,
- the systems' *real-time capabilities*, particularly with regard to road safety and the implementation of *autonomous driving,*
- user acceptance and the legal framework for autonomous acting,
- achieving a suitable and accepted form of *human-machine interaction* and
- creating the legal framework and overall conditions required for the deployment of Cyber-Physical Systems.

These challenges involve a mixture of research questions and requirements with regard to the systems' design, technology and *engineering*, their organisation, the necessary infrastructure and the social and legal frameworks.

2.3 PERSONALISED AND SAFE INTEGRATED HEALTHCARE

The subscenarios that form part of the overall scenario "personalised and safe care provision, context awareness and integrated healthcare" describe how the future of healthcare in our society might look if we take advantage of the rapid advances in information and communication technology to make CPS support available in this area. The subscenarios envisage extensive networks between patients and physicians and patient health monitoring using modern *smart health systems*. These networks will enable innovative solutions for meeting individual medical needs and allow optimal support to be provided to the growing number of elderly people in an ageing population. They will also make a valuable contribution to optimising healthcare costs whilst maintaining or even improving the standard of care.

> Frau Müller's mother, Rosi Huber, is a 70 year-old pensioner who lives alone in an old farmhouse on the east side of Munich. She never learned to drive because her husband always used to drive her everywhere. Since her husband died a couple of years ago Frau Huber has suffered from mild depression. However, she is glad that she still doesn't need to take as many different medicines as her friends, who she likes to meet up with on a regular basis. She is especially proud of not being a diabetic. Although she has been managing very well on her own, she is afraid that one day she might get into difficulty when there is nobody around to help her and has therefore chosen to purchase a smart health system. The system carries out passive monitoring but also provides her with support on medical matters and will call for help in the event of an emergency. In addition to passive behaviour monitoring, there is also a module that performs daily blood pressure and weight checks, makes sure she is taking the correct medication and provides the alarm function. At the moment, these functions are only set up to cover the basic requirements, but they can be adjusted to any changes in the user's needs.

2.3.1 CPS IN TELEMEDICINE, REMOTE DIAGNOSIS AND HOME CARE SUPPORT

Scenario

(1) It is some time now since Frau Huber had the system installed in her home. The *sensors* that are built into her home have established her usual movement patterns and used them to create a profile. Frau Huber no longer even notices that these small devices are there. Her daily morning weight check in the bathroom has also become part of her routine. Moreover, the fact that the system provides her with guidance to help her get her weekly medication together means that she is no longer worried about making a mistake. At her request, she only receives a reminder to take her medication in the afternoon, since this is the only time when she doesn't have a regular meal and she always leaves her medicines on the dining table.

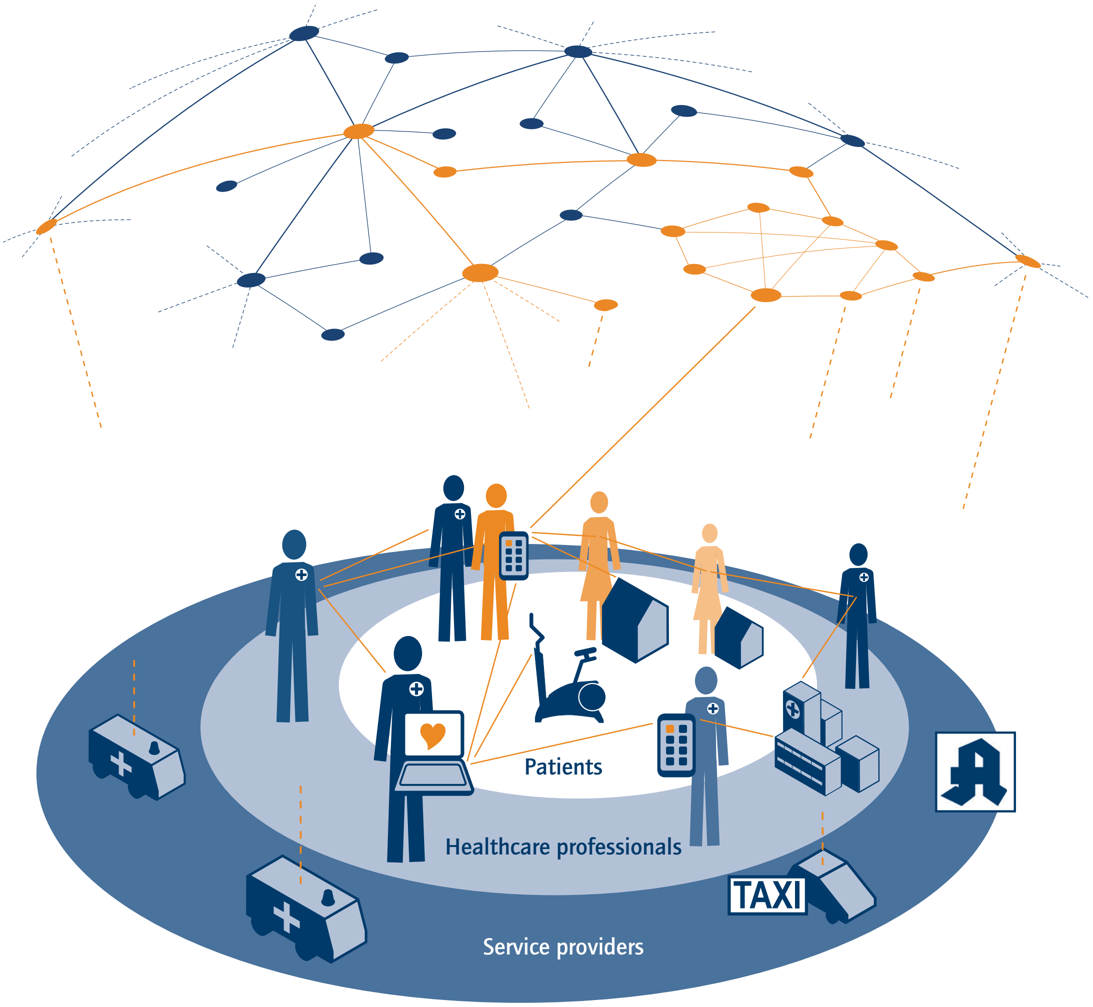
(2) Frau Huber always used to enjoy meeting up with her friends, but she has recently started skipping more and more of their get-togethers. The passive monitoring system has also detected changes in her behaviour and has recorded a noticeable reduction in her movements and an increase in her weight. Since these changes are occurring faster than would normally be expected, the system advises Frau Huber to get in touch with her GP before her next scheduled appointment. Her system makes it easy for her to make an appointment by connecting her directly to the system at her GP's practice. Her GP advises her to do more exercise and also asks her to measure her blood pressure every day when she gets up in the morning. She is able to obtain a blood pressure monitor on prescription from the chemist's and this can be easily integrated into her home system together with a wearable motion *sensor*. These devices immediately appear on her exercise system as soon as she switches them on. All she needs to do to activate them is enter the code printed on their packaging. Frau Huber can also manage her medical data. Her system can send a request to a service that will provide her with a simple overview of which details are needed by different specialists. She can then authorise access to these data, however any doctor wishing to access them will first have to provide their reasons for doing so. The camera built into Frau Huber's input device takes a picture of her that is assessed using a special function in the *cloud*. This function is also used by her entryphone so that it can display the names of people who are at the door. – After a few days, Frau Huber's condition has deteriorated and her GP refers her to an internal medicine specialist who has her admitted to an in-patient clinic so that she can be given a more thorough examination. Neither of the two doctors can explain Frau Huber's atypical movement patterns in her home over the past few days and she herself isn't even aware that anything has changed. Frau Huber has already authorised her GP to check her medical data on a regular basis. – On the same day that she is admitted to the clinic, Frau Huber suffers a minor stroke which can be treated promptly. Guidelines for what to do in an emergency are uploaded to her system. Text messages are sent to her family to inform them of the situation, her newspaper is cancelled and her home is placed under security surveillance.

How it works

In order to provide a basis for assessing the patient's medical condition, data from a variety of *sensors* are combined with evaluation and medical history data and parameters to produce a preliminary assessment using known, defined or learned *models*. In order to ensure user acceptance as well as to keep costs down and manage requirements, it is important for individuals to be able to choose the *sensors* that provide the basis for these complex assessment models. For example, largely healthy users are likelier to prefer passive monitoring systems rather than having *sensors* implanted in their bodies. The passive *sensors* in our scenario are connected to an adaptive algorithm that is capable of recognising behaviour patterns which it uses to produce individual patient profiles. This allows changes in or major deviations from their current condition to be detected. The assessment is based on data and events that have been captured in sufficient quantities by the systems being used. Moreover, Cyber-Physical Systems with integrated *data mining* functions can draw on the huge volumes of data in other systems to produce personalised results and can often even be used to predict medical events.

The information obtained in this way can be used by other systems and equipment in order to initiate or suggest appropriate interventions. These interventions may be carried out by people or systems that are able to coordinate their respective responsibilities among themselves and interact with Frau Huber in order to evaluate her medical condition. It is thus straightforward to establish interfaces with mobility *services*, pharmacies, therapists, physicians, case managers, installation engineers and service personnel.

Figure 2.6: Networked actors in an integrated telemedicine healthcare scenario



In addition to the current data that are recorded in real time, data from the patient's records may also be relevant. It is therefore necessary to ensure that any potentially significant data or information is retrieved by the distributed systems and collated in a meaningful manner.

The functions that are required to meet a system's purpose can originate from distributed systems. Generic and *domain*-specific functions can be automatically or manually combined with each other, enabling new functions to be added to systems or manual functions to be automated. Generic database-supported network functions such as face recognition enable any device with a built-in camera to identify different people. This capability can be used to open the front door to someone or to gain authorisation to access someone's data. Even simple embedded systems can acquire powerful functionality in this way. Another example is provided by portable distress signal sensors that could select which emergency service provider to alert based on their proximity to the patient. The same *sensor* could be used in a different context to select transport services such as taxis, buses or regional services based on location and time.

In all of the above contexts, *data protection* is extremely important for all the actors involved in the system. The appropriate level of protection is needed not just for patient data but also for data from doctors' practices. The system should provide patients with the support they need to ensure that they only authorise access to data if they are legally allowed to do so.

2.3.2 FOLLOW-UP CARE AND SUPPORT IN THE PATIENT'S FAMILIAR SURROUNDINGS

Scenario

(3) Frau Huber is discharged from the clinic after a few days and transferred to a rehabilitation clinic. She is very keen to return to her usual surroundings as soon as possible and get on with her life. Having discussed what to do with the doctors at the rehabilitation clinic, she decides to add a rehabilitation component to her home system so that she can carry out part of her treatment in her own home. The clinic, her GP and a physiotherapist will support her in this process. Everyone involved is granted access to the data that are relevant to them. Frau Huber's exercise equipment is delivered to her home and integrated into the system by an engineer. He is able to monitor and maintain the system remotely from his office, allowing him to respond swiftly if a fault develops. He does not get to see any of the medical data. Frau Huber's motion *sensor* is now also used to monitor and control her daily walking exercise, during which she also always has her distress alarm on her. Her scales, which were previously only used to check her weight, are now also used to help determine her diet. Since it is going to be some time before she can start meeting up with her friends again, Frau Huber is given access to an online patient portal that provides her with a range of information and tips on how people with her condition can live more independent lives. The portal also enables her to communicate with other patients who are in a similar situation. This helps her get through the lengthy rehabilitation process.

The assisted movement and coordination exercises soon achieve a positive response – in fact, rather than needing to motivate her, the main problem for Frau Huber's doctors and physiotherapists is to make sure that she doesn't overdo it. Moreover, all her readings are slightly better than the expected values calculated by the system. This means that the maintenance phase can begin sooner than expected. During this phase, Frau Huber continues to receive support to help her stick to her new dietary and exercise regimes. But it is not long before she is once again able to get together with her friends.

How it works

Cyber-Physical Systems connect technological systems and service providers to each other. This means that the systems must be able to coordinate global processes. Frau Huber can only start doing her exercises once the engineer has installed and tested the relevant systems. Escalation mechanisms need to be triggered in the event of a fault. Should a particular *service* provider become unavailable, the system needs to be able to find an alternative or refer the problem to the appropriate authority.

Healthcare services such as Frau Huber's movement and coordination exercises are highly personalised in terms of the details of what is prescribed and the assessment of the outcomes. This means that the relevant systems, which are after all required to operate in a *safety-critical* environment, must possess a high degree of flexibility with regard both to their components and the sequencing of different actions. The relevant standards ensure that data can be exchanged between subsystems and that the systems can process them automatically using the appropriate syntax and semantics.

Some of the functions described above are based on knowledge databases and knowledge *models*. Medical databases are used to compare the *sensor* data against a range of symptoms so that recommendations can be made with regard to possible diagnoses. Moreover, with the data captured during her treatment, Frau Huber is also contributing to improving overall data quality. The value of the service increases as more and more specialised databases are connected to each other within the system. For example, by adding a pharmaceutical database it would be possible to ask patients directly about the side-effects of their medication. Whilst this would of course help Frau Huber, it would also provide her doctors with valuable information.

There is one significant challenge in this area – it is older people in particular who tend to find it difficult to use telemedicine equipment. This means that their daily measurements often have to be taken by family members who are not usually able to interpret the readings or symptoms and therefore require support. Furthermore, these family members are frequently unable to attend the patient's appointments at the doctor's because of their work and are therefore in the dark as to what the doctors have decided to do. Consequently, it is necessary to find ways of including family members in the process. Until such a time as this is achieved, information portals can be used to provide people with any information they may need and answer their questions. Moderation by experienced medical practitioners would guarantee the quality and safety of the advice provided in this way. However, it is undoubtedly necessary to address the *data protection* issues that arise in connection with these portals.

As well as telemedicine, the Cyber-Physical Systems capabilities described above are also relevant to the more general context of systems that assist older people to live healthy and independent lives *(Ambient Assisted Living, AAL).* These systems comprise technology-based concepts, products and *services* geared towards providing situation-specific support to people who have specific needs in their everyday lives. An extremely important feature of these *services* is that they must be unobtrusive and should not stigmatise the people they are supporting. The goals of *AAL* are to maintain and increase the independence of people of all ages in their usual surroundings and to improve their quality of life through the provision of enhanced assistance and support *services*.

An *AAL* environment might, for example, involve the user's own home. In order to compensate for the decline in their physical or cognitive abilities as they get older, their home would gradually be fitted with the relevant user-controllable CPS equipment which would provide a variety of assistance functions. It might, for example, help them use the lights, heating, blinds, doors, beds or kitchen units and appliances. The different CPS devices communicate both with the user – via *mobile devices* or interactive voice response – and with each other. In the *AAL* context, the environment itself thus becomes a smart Cyber-Physical System that helps the user take decisions and plan ahead. For example, it might draw up a shopping list of what the user wants based on what they currently have in the house, remind them to take their medication, monitor their daily fluid intake or raise the alarm if they suffer a fall. Mobile equipment such as smart wheelchairs, wheeled walking aids or home service robots would also be incorporated into the network [KBRSG11].

2.3.3 CPS-BASED SUPPORT FOR AUTOMATIC EMERGENCY DETECTION AND PRIMARY CARE

Scenario

(4) Frau Huber goes for a walk in the woods. Suddenly everything goes black and she collapses. Her smart health system's sensors register a sudden drop in her pulse rate and a movement that resembles a fall. The *smart health system's* initial response is to emit an acoustic message requesting Frau Huber to press a specific button on her *mobile device* if she is actually all right in spite of the anomalous readings. When Frau Huber fails to respond to repeated prompts, the system activates an alarm. Frau Huber's *smart health system* is connected to the emergency response centre which is thus able to determine her location and access both the *sensor* data and her electronic medical records. The emergency response centre personnel use this data to conclude that she has probably fainted. They pass this information on to an ambulance whose crew is instructed to go and check if she is OK.

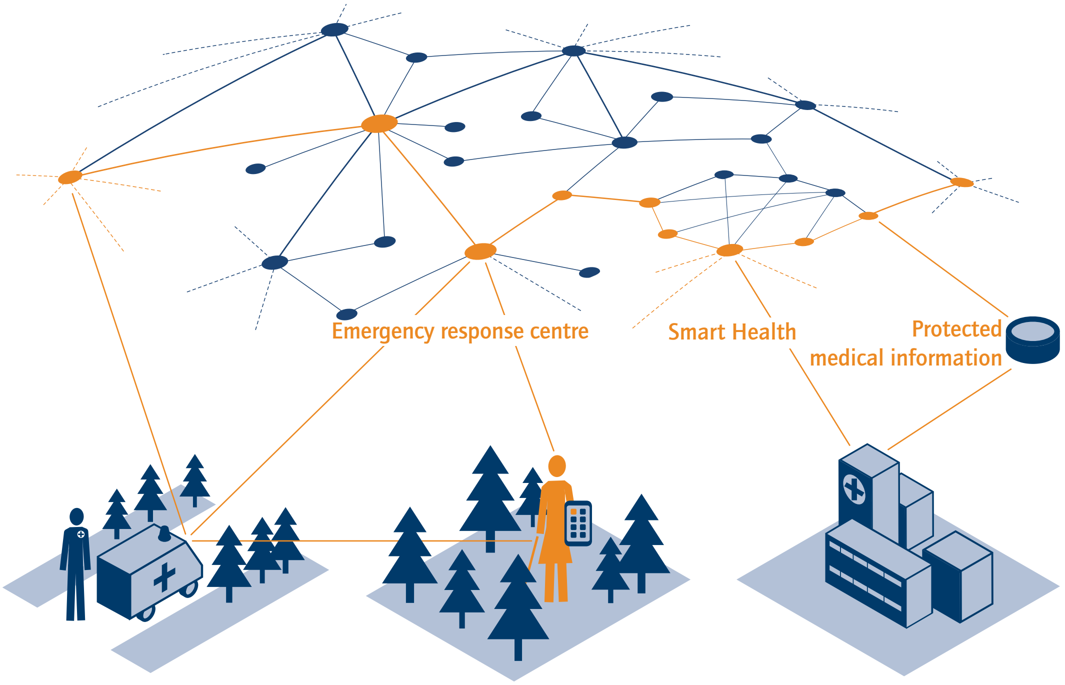
(5) The team on board the ambulance is provided with a brief overview of Frau Huber's location, her current vital signs and her medical records. A special system guides the ambulance to Frau Huber's exact location. By now, another walker has found Frau Huber and is attempting to help her. The *smart health* device provides him with guided instructions for giving her targeted first aid.

Whilst they are en route to the scene of the incident, the paramedics notice that Frau Huber's current vital signs indicate that her pulse rate is continuing to drop. This causes them to suspect that she injured herself during the fall and has lost a lot of blood. When the paramedics leave the ambulance, they therefore know to take along the necessary equipment for applying a pressure bandage. Since Frau Huber's accident occurred on a forest track that is not accessible to vehicles, the paramedics complete the last part of the journey on foot and are guided to her exact location by a *mobile device*. Once they arrive at the scene, they take over from the walker who had started administering first aid. They discover that Frau Huber punctured an artery in her leg on a sharp branch in the act of falling and is indeed losing a lot of blood. The paramedics apply a pressure bandage to her, carry her back to the ambulance and set off for the hospital. Whilst they are en route, they send her electronic medical records and current diagnosis to the A&E department. This information enables the A&E staff to identify Frau Huber's blood group and prepare a blood transfusion. When Frau Huber arrives at the hospital, everything is ready for her so that she can receive the optimal treatment without delay.

How it works

Patient *sensors* enable emergencies to be detected. Together with the patient's movement profile, a combination of different parameters such as pulse rate, blood pressure and

Figure 2.7: Illustration of coordination connections in the emergency scenario described in the text



respiratory rate allow a relatively accurate picture of their current condition to be produced. Initially, the information is collated on the patient's own *mobile device* which searches for anomalies. If the system suspects a critical situation, it begins by trying to solve the problem locally. The *mobile device* alerts the patient to the suspected problem and prompts them to rule out a false alarm. For example, just because a motion *sensor* thinks it has detected a fall, it doesn't necessarily mean that the patient is in difficulty and an alarm needs to be triggered.

However, if the patient fails to respond then the *mobile device* does activate an alarm and sends their current data to the emergency response centre together with their medical records. This information provides the centre's personnel with a sound basis for deciding how to proceed. For example, if the patient is not in a life-threatening situation, they may initially decide to ask a relative or neighbour to go and check if they are OK. The information about the patient's location obtained from the *mobile devices* of either the patient themselves or the first people to arrive at the scene can be used to find someone local who is able to provide suitable assistance and direct them to the scene of the incident via a navigation app on their *mobile device.*

If the decision is taken to send an ambulance, the relevant medical data can be sent directly to it and evaluated while the ambulance is en route. This enables the paramedics to optimise their preparations and assess the patient's condition based on the current *sensor* readings while they are travelling to the scene. The data can also be sent straight to the hospital so that the staff there can prepare to perform an emergency operation if necessary.

2.3.4 CPS EXCESS VALUE AND POTENTIAL BENEFITS

Demographic change poses huge challenges for our healthcare system. The consistent deployment of Cyber-Physical Systems can make a significant contribution to overcoming these challenges. The potential benefits and excess value are as follows:

- improvements in the quality of medical decisions, e.g. thanks to
  - the ability to draw on medically relevant *sensor* data
  - the collation of all the relevant medical information from a variety of sources in a single electronic case file held at a central location
  - optimal *availability* of the information contained in the electronic case file wherever it may be needed
  - automated analysis of the aggregated data, enabling identification of previously undetected medical conditions and the recommendation of possible treatment options
- improvements in the quality of medical care, e.g. thanks to
  - prevention of errors through increased information *transparency* throughout the chain of services provided by doctors, pharmacists, therapists, etc.
  - automatic detection of problems arising during treatment via the registering and automatic analysis of *sensor* readings
  - better *compliance* as a result of improved patient engagement
- enhanced emergency care, e.g. thanks to
  - automatic emergency detection
  - faster medical care at the scene of the emergency, thanks to the ability to perform targeted searches for people with the appropriate first-aid skills who are in the vicinity and guide them to the scene
  - enhanced care thanks to the fact that the necessary medical information is available throughout the entire emergency service chain
  - local intervention support and advice on what to do in emergencies
- efficiency gains through the use of medical services for patients, e.g.

  - less travelling thanks to the use of remote diagnosis and telemedicine
  - more efficient processes, e.g. for booking appointments or through the use of electronic prescriptions
  - the ability to find locally available specialists
- a high standard of care for patients in their own homes thanks to
  - support for patient self-management and self-monitoring
  - reassuring patients by providing them with information and feedback
  - detection of symptoms even before patients notice them themselves, enabling more cost-effective treatment options
- efficiency gains for medical service providers, e.g. thanks to
  - automated data capture by *sensors*
  - automated aggregation and analysis of medical data and recommendation of treatment options by the system
  - shorter appointment durations thanks to rapid *availability* of full patient records
  - reduction in the number of home visits thanks to the use of remote diagnosis and telemedicine
  - optimisation and digitalisation of administrative processes such as appointment booking and prescription writing and processing.

These direct benefits are augmented by indirect benefits resulting from extensive changes to healthcare provision structures. For example, several providers could work together to provide integrated patient care, thus filling in any gaps in the patient's treatment. A personalised combination of existing diagnosis and treatment service components could lead to the emergence of new treatment models; treatments could be adapted promptly and as dictated by the current situation. Furthermore, long-term follow-up would make it possible or easier to obtain evidence of a treatment's effectiveness. Finally, telemedicine procedures could improve the standard of care in areas with limited healthcare services and enable specialists from other parts of Europe to be consulted in complicated cases.

Cross-*domain* use of Cyber-Physical Systems is also a possibility. For example, the case management of people with complex treatments or living in complex circumstances could be shared across several medical facilities. Moreover, information about a patient's medical condition or disability could be used to help provide them with cross-domain services such as journey planning.

2.4 SMART GRIDS

Germany and the rest of Europe are facing major changes and huge challenges as far as their energy supply is concerned. Conventional nuclear, coal- and gas-fired power plants that produce a constant stream of energy are being partly replaced by renewable energy sources whose availability is less predictable, particularly wind and solar power. In view of the growing public awareness about environmental issues this is a politically and socially desirable change, but one that will nonetheless have major consequences.

In order to guarantee a stable energy supply, supply must always be able to meet demand in the electricity grid. As things currently stand, this stability is achieved through centralised management whereby production is adjusted to keep pace with demand. In the future, however, fluctuating and decentralised energy production will be accompanied by equally volatile demand patterns. In order to guarantee stability going forward, it will be paramount to create "smart" power grids by connecting electricity producers, storage facilities, grid management systems and consumers with each other through information and communication technology. By interconnecting all these different elements, it will be possible to build a vast energy information network or *smart grid*. In addition to guaranteeing a stable energy supply, the integrated deployment of *ICT* will enable a variety of other functions and *services* in the *smart grid*.

The high degree of interconnectedness within the smart grid makes it possible to have various different consumption and operating models for the energy supply. These include *micro grids* where networks of local producers and consumers are used to optimise the amount of electricity that is fed into the grid and consumed locally and *Virtual Power Plants* (VPPs) where several local producers come together to create a virtual power plant that delivers demand-based and secure energy distribution and increased energy efficiency. The local energy generators could be anything from *solar PV* arrays, small wind farms or biogas plants to micro CHP plants. By bringing them all together, it becomes possible to manage several small producers internally as well as helping to prevent uncontrolled fluctuations in the grid, thus contributing to the overall stability of the system.

Furthermore, research is currently being carried out into additional *smart grid* designs that would enable the integration of fixed storage facilities and electric vehicles. In order to illustrate *smart grids'* potential applications, the following section presents a use case that looks at *micro grids* from the consumer's perspective. It identifies a number of novel functions and options that *smart grids* can provide which open up innovative applications and new *business models* for small and medium-sized enterprises. The scenario describes the different actors and devices and how they interact with each other.

2.4.1 MICRO GRIDS

In the *micro grid* approach, electricity production and management of grid stability occur predominantly at a local level, e.g. within a small municipality. Inside the *micro grid,* coordination of local electricity generation facilities such as *solar PV* arrays, wind farms, fuel cells and micro CHP plants together with energy storage systems such as flywheels and batteries, smart energy consumption management systems and the grid operators ensures that local consumers' energy needs can be met without jeopardising the stability of the grid. *Micro grids* can complement the national grid by guaranteeing a partly autonomous energy supply ("supply islands") for small communities, for example. If required, their system behaviour can help increase the stability of the overall system by enabling largely autonomous supply. In an ideal *micro grid*, locally generated energy would be used in the location where it was produced in order to prevent it from having to be transported over long distances and thus avoid incurring the associated losses.

Local use of supplementary generating facilities such as micro combined heat and power (CHP) plants can, in conjunction with the appropriate storage facilities and smart consumers, help to level out the fluctuations implicit in renewable energy generation. However, in Germany this would require the deployment of large numbers of storage facilities which are currently far too expensive to be used for this purpose. Internal coordination of the *micro grid* is carried out either by a human operator or by smart software solutions also known as agents. The national grid that sits above the *micro grid* is simply treated as another producer or consumer, depending on the current energy balance between the two. Energy can thus be traded between the *micro grid* and the national grid.

The *micro grid* can be run either by institutional organisations or by small and medium-sized enterprises. However, it is important to remember that the *micro grid* approach tends to be most cost-effective for the owners of industrial facilities, large building complexes or large numbers of smaller buildings. There are a number of technological and indeed regulatory obstacles to the use of *micro grids* by private households, particularly consumers' right to freely choose their electricity supplier which means that they would be entitled to choose suppliers who did not form part of the *micro grid.*

2.4.1.1 A micro grid use case scenario

Frau Mayer recently moved into a new house in a small town near Munich. Her environmentally conscious lifestyle means that she chose a home that is equipped with the latest green technologies. These include a solar roof system (*PV* and thermal), a small energy storage system and a micro combined heat and power (micro CHP) system in the basement that provides the house with central heating. She also has several *smart household appliances* including her air-conditioning system, heating system, refrigerator, washing machine and dishwasher, as well as an electric car and a modern CPS infrastructure comprising a *smart meter* and smart *energy gateway*.

Shortly after moving into her new home, Frau Mayer hears about a service being provided by a company called Your Local Micro Grid Ltd. This medium-sized enterprise is inviting all the local residents to sign up to its *micro grid* and is offering to provide the community with an efficient supply of renewable energy so that residents can rest assured that the energy they are using is both efficient and green.

As a consumer who also owns generating equipment, Frau Mayer can join the *micro grid* as a prosumer (producer and consumer). Her home is automatically connected to the *micro grid* by Your Local Micro Grid Ltd. Standard *Plug-and-Play*-enabled technology ensures seamless integration.

Now that she is a member of the *micro grid*, Frau Mayer plans the day ahead on her *mobile device* when she gets up in the morning. She begins by telling the device that she will be at work between 8 a.m. and 6 p.m. While she is away, household appliances such as the fridge, deep-freeze and air conditioning can be controlled as smart consumers by the *micro grid* operator. In addition, Frau Mayer loaded up the washing machine and dishwasher first thing in the morning, so she can now tell her smartphone that they should both run a cycle before she gets back from work. The appliances can now run at any time while she is out of the house, providing the *micro grid* with the ability to manage electricity demand flexibly. For example, in addition to flexibility regarding the time that a wash cycle begins, it is also possible to pause it at times of peak demand, thus helping to flatten out the load curve.

How it works

The relevant settings are sent to Your Local Micro Grid Ltd via a secure communications channel. The operator uses these data to calculate how to optimise the energy load in the town on its special CPS infrastructure using smart consumption management algorithms. The exact times when the appliances run are based on Frau Mayer's instructions regarding cost, the proportion of electricity generated by her own equipment that she wishes to use and eco-friendliness. To optimise the process, the *micro grid* uses local production forecasts that take account of the current weather forecast, projected electricity prices and the grid load forecast in order to ensure stability of the local grid.

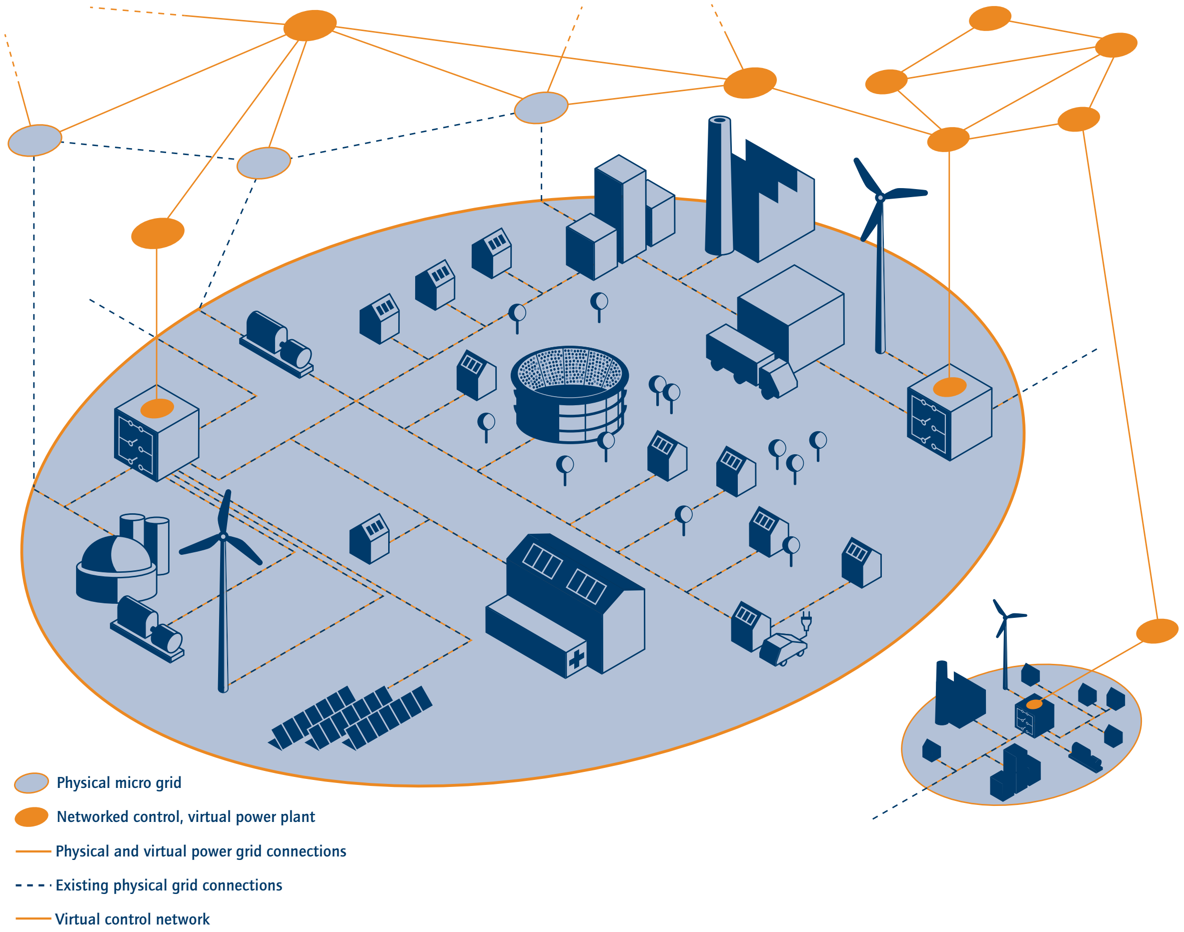
Another function provided by Your Local Micro Grid Ltd is the ability to control the temperature in Frau Mayer's home. She can input her desired settings into her smartphone and the operator then manages the controls of her air-conditioning unit and micro CHP system to ensure a comfortable temperature at all times. For its part, the *micro grid* gains another controllable consumer who can be managed by the optimisation algorithms. In contrast to a simple thermostat, this means that current electricity prices or grid load can also be taken into account when regulating the temperature in the house. The micro CHP system thus contributes to the stability of the grid and reduces the need for costly energy storage facilities. The *micro grid* operators – or an agent – can factor electricity prices and grid load into their optimisation calculations and plan and control how the micro CHP system is deployed based on these two factors, depending on whether the priority is to stabilise the grid or run the system economically. Frau Mayer can use her smartphone to view her current consumption and the amount of energy being produced by her PV systems whenever she wishes. This is made possible by her *smart meter* which is connected to the Internet and enables revenue and costs to be displayed transparently at all times. At the end of every week Frau Mayer's account with Your Local Micro Grid Ltd is settled and she is automatically credited or debited with the relevant balance.

Frau Mayer is immediately informed via her *mobile device* in the event of a fault or if her PV unit gets dirty, causing less electricity to be generated. The nature of the problem is assessed and a recommended course of action is proposed. This means that, if necessary, she can immediately call in a service provider such as an electrician to fix the fault.

Your Local Micro Grid Ltd uses its knowledge of local production and consumption to trade energy. Prices may be viewed by consumers at all times via the energy exchange or Your Local Micro Grid Ltd. Local energy surpluses can be sold on the energy market and additional energy can be bought in when there is a shortage.

Frau Mayer also connects her electric car to her local *micro grid*. While her car is parked either at home or at work, Your Local Micro Grid Ltd can use its battery to take advantage of price fluctuations on the energy market. The battery can store energy if renewable energy production is outstripping consumption. Conversely, it can feed energy back into the grid if consumption is higher than production. The *micro grid* operator can use batteries for different types of energy trading. Electric vehicles are best suited to regulating grid stability and to primary balancing on the balancing energy market, since they allow load flows to be balanced

Figure 2.8: Schematic representation of a micro grid in the networked energy supply scenario (smart grid)


Physical micro grid
Networked control, virtual power plant
Physical and virtual power grid connections
Existing physical grid connections
Virtual control network

very quickly. Electric vehicles thus enable local grid bottlenecks to be relieved rapidly and local load peaks to be balanced. Once again, Frau Mayer can use her smartphone to set the desired charge level for her car battery and the corresponding charging times. Your Local Micro Grid Ltd coordinates the management of electric vehicle charging in the local community. In doing so, it is careful to ensure that the prevention of grid bottlenecks does not impact negatively on participating car owners' ability to meet their transport requirements.

As the increased use of renewables causes energy production to become more volatile, *micro grids* are an example of a Cyber-Physical System that can help stabilise the power grid, thus removing the need for at least some of the large-scale power plants that would otherwise be necessary. Operational planning of *micro grids* is supported by the data supplied by its members and by a variety of optimisation and control algorithms. Planning is also supported by weather forecasts that make renewable energy production, particularly solar power, more predictable. It is also possible to manage consumption either via price signals or by directly accessing consumer devices and electricity storage units. It is important that new devices should be *Plug-and-Play*-enabled so that they can be added to the system without needing to be set up first – the system needs to be capable of dynamically adapting to changes in *real time*. It should also be able to respond automatically to any disruption or emergencies. Additional functions can help to solve problems by making recommendations or immediately contracting a service provider.

Since Frau Mayer's energy consumption over time is recorded very precisely, she can use her preferred end device to view details of how much energy she is using at any given moment, irrespective of her current location. Moreover, her personal energy advice agent analyses her consumption patterns and provides her with energy-saving tips.

The wide range of data available can also be accessed by the national electricity grid to help improve its stability. The grid does not have direct access to Frau Mayer's personal data, but it is able to access the aggregated data of several customers in *real time.*

Smart integration of a local energy storage unit into the system offers several advantages. In conjunction with the *PV* system, it allows Frau Mayer to consume more of the energy that she has produced herself. Furthermore, the energy storage unit can be used as a pre-charge battery to enable more rapid charging of her electric car. Finally, it helps to reduce volatility at the system level. There may be times when these three functions become incompatible with each other. Consequently, a *broker system* works together with the different units' agents to ensure that they are always operating with Frau Mayer's best interests in mind.

2.4.2 IDENTIFIED EXCESS VALUE AND SERVICES

Energy is key to some of our society's most basic needs. High security of supply and the availability of affordable energy are important drivers of economic growth. *Smart grids* will play a crucial role in the imminent energy revolution and can add value to the energy supply system in a variety of different ways. By increasing *transparency*, *smart grids* can make people more aware of how much energy they are using and thus contribute to lowering demand. They also increase consumer flexibility, thereby enabling the widespread introduction of renewable energy generating facilities without jeopardising security of supply. The benefits to our society are higher living standards and the ability to manage our natural resources more sustainably.

Micro grids are one component of *smart grids* that are particularly focused on using the available energy locally in order to prevent the losses incurred when transporting energy over long distances as well as avoiding grid use tariffs. The control of a *micro grid's* flexible components can be managed either by its operators or by automated software agents. This is supported by the use of algorithms, visualisation tools and services such as weather forecasting services as well as development and maintenance services for the energy and *ICT* infrastructures. The provision and integration of these services in the *smart grid* fosters innovative solutions that encourage the emergence of new *business models* and start-up companies. This should in turn create jobs and strengthen the German economy. Rural areas in particular stand to benefit from the installation of renewable energy generation facilities, since their operation and maintenance will create employment locally.

In addition to the advantages of greener energy production, consumers will benefit from the cheaper tariffs and lower costs enabled by renewable energy and its producers and controllable components. Controllable energy consumers and storage systems will act as a buffer against volatility and allow peak loads to be reduced. This will in turn make running the grid easier and enable more cost-effective deployment of large-scale power plants. The *micro grid*, which will operate as a public utility, will thus enable electricity to be bought far more cheaply, while the fact that it will not have to pay grid tariffs will also contribute to lower energy prices. Local suppliers will be able to use forecasts and the potential of load shifting and decentralised generation to make a profit on the energy market.

The grid will be able to evaluate the relevant data and use them for diagnosis purposes. This will enable early detection of potentially dangerous situations and allow automated responses to be triggered, preventing power failures or other threats to the reliability of customers' electricity supply. At the same time, more efficient capacity utilisation will make expansion of the grid unnecessary, allowing the price that customers pay for using the grid to be reduced.

In addition to cost savings, there are several other benefits for end users. *Smart meters* can be controlled via *mobile devices* at any time and from any location. This means that consumers will always be able to monitor their homes. For example, they will be notified imme-diately if they have forgotten to turn the oven or an iron off. In addition, certain devices' consumption patterns can provide information about their performance. For example, if a refrigerator is using more electricity than usual it will be able to send the user a message prompting them to defrost it or recommending that they purchase a new energy-saving appliance. Moreover, the fact that people's electric vehicle batteries will always be charged up to the required level while they are parked at home or at their workplace will remove the need for trips to the charging station. Finally, users will be able to analyse their own energy data and optimise their homes' energy consumption.

2.5 SMART FACTORIES – NETWORKED, ADAPTIVE AND REAL-TIME CAPABLE PRODUCTION

The two key activities of any manufacturing company are order processing and the development and production of products. These processes are illustrated by the two scenarios described below:

- the purchase of a customised kitchen, which serves to illustrate how Cyber-Physical Systems can be deployed during the ordering process and the potential benefits they can offer in this context, and
- self-configuration of production-related IT systems as an example of the potential of Cyber-Physical Systems in relation to product and production configuration.

At first sight, the scenario involving the purchase of a customised kitchen might appear to be rather trite, especially since it is taken from the b*usiness-to-consumer* domain and thus only partially describes the typical requirements of the *business-to-business* domain, such as the acquisition of a complex piece of machinery or equipment by an industrial plant operator and the associated reconfiguration of their manufacturing system. Nevertheless, this simplified use case scenario does in fact provide a useful illustration of the specific capabilities of Cyber-Physical Systems in the manufacturing environment.

In general, manufacturing is governed by the following well-known parameters [AR11]:

- the quality standards demanded by the customer, which require robust manufacturing processes to be in place,
- time and speed in relation to innovation, throughput times and equipment start-up and
- competitive manufacturing costs that allow more money to be invested in equipment and IT.

These goals can also be interpreted as restrictions on the design of manufacturing companies' IT architectures and systems. These restrictions are one of the reasons why the manufacturing environment has been slow to adopt many of the modern technologies that have long since become established in the consumer goods market. This is true, for example, of *smart end devices* such as smartphones which could be used to enable decentralised transmission of key production data and of 3D visualisations of the shop floor.

In addition to the well-known triad of quality, time and cost, a variety of new factors will also be key to successful manufacturing in the future [BBE07], for example:

- the adaptivity to manufacture several new product variants which require integration and *interoperability* of manufacturing IT systems,
- *real-time capability*, making it necessary for information to be made available rapidly to authorised users, and
- the ability to operate as part of a network in connection with a new approach based on networks of sites or companies instead of on individual enterprises.

The position of Cyber-Physical Systems at the interface between the business processes described above means that they also need to be networked across the entire product and manufacturing system life cycle and integrated with enterprises' established IT infrastructures. This will still be the case even if future manufacturing applications are obtained in the form of *cloud services.*

2.5.1 ORDER PROCESSING – SCENARIO AND SUBSCENARIOS

Scenario

(1) The Müller family wishes to purchase a new kitchen. **(2)** An assistant helps them put together their dream kitchen online based on their preferred configuration of components, kitchen units, worktop, appliances and design, plus additional factors such as price, *energy efficiency* and delivery date. **(3)** Once it has received authorisation from the family, the assistant uses the kitchen supplier's production management system to perform a direct search for production facilities belonging to the manufacturers of the relevant kitchen furniture and appliances. The results of the search indicate that all the sites that produce the family's desired kitchen furniture belong to Manufacturer A and are located in Germany, whilst all the sites that produce the worktop belong to Manufacturer B in eastern Europe. The results of the search also indicate that the kitchen can be delivered by the requested deadline and within the stipulated budget. **(4)** The Müllers therefore go ahead and place their order using the assistant. Once the order has been placed, the kitchen supplier's production management system monitors and manages the entire process with the firms that have been subcontracted to make the individual components.

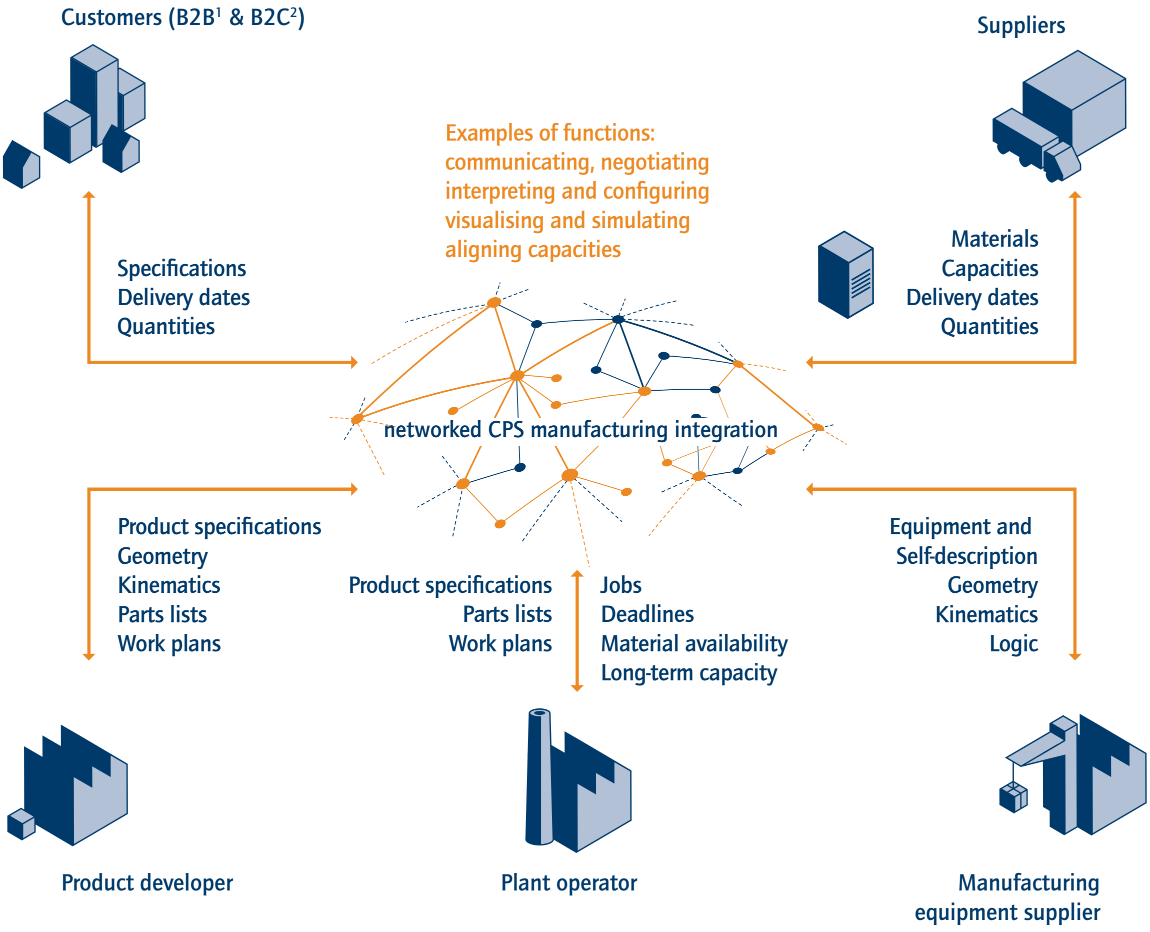
(5) Some time after ordering their kitchen – by which time the production orders have already been placed with the suppliers of the individual components – the Müllers decide that they want to change the design of their worktop. **(6)** They use the assistant to enquire about whether it is possible to change their order and if so under which terms and conditions. The assistant discovers through the production management system that the new worktop involves a different manufacturing process requiring expensive pre-treatment of the raw materials.

It searches for the manufacturing sites that are best able to meet these requirements and informs the Müllers of the changes to the price and delivery date. **(7)** The Müllers confirm the change to their order and Manufacturer B in eastern Europe is immediately informed of this mandatory change.

How it works

A customised kitchen needs to be built to a specific budget, use environmentally-friendly materials and contain appliances that conform to the desired *energy efficiency*-classes. Based on the customer's specifications with regard to dimensions, 3D configuration, components, budget and sustainability considerations such as carbon footprint and eco-taxes, the assistant uses a production management system to determine the ideal manufacturing system, cost of producing the kitchen and suggested delivery dates. In order to do this, it has to be capable of *real-time*, context-adaptive

Figure 2.9: Examples of information exchanged between actors in the manufacturing scenario



[1] Business to Business
[2] Business to Consumer

communication, networking of distributed manufacturing facilities belonging to different companies and implementation of negotiation strategies. The production management system communicates with the relevant manufacturing facilities in its network. In addition, the manufacturing facilities themselves take into account factors such as their own location, their capacity utilisation, the relevant logistics costs, the compatibility of different manufacturers' production facilities with each other (this requires horizontal networking so that different manufacturing facilities can interact with each other), the *value network* – beginning with the raw material and covering all the intermediate stages right up to the finished kitchen – and the contractual terms and conditions of the manufacturers and suppliers. Once the planning process has been completed, the best manufacturing facilities are selected even if they belong to different manufacturers in different locations. In the scenario described above, Manufacturer A in Germany is contracted to make the kitchen furniture, while Manufacturer B in eastern Europe is chosen to supply the worktop. The orders with the different manufacturers are coordinated via Cyber-Physical Systems.

Any changes to the manufacturing process resulting from changes to the order are implemented automatically by the manufacturing facilities in the network, with additional manufacturing facilities or suppliers being brought in as necessary. The end customer is notified of any increase in the final cost and can confirm that they wish to proceed with the change to their order via an assistant that communicates directly with the production management system.

Changes to the manufacturing process may be required if one of the components is unavailable. In this event, just as with changes to the order, the Cyber-Physical System reorganises itself so that the missing component can be compensated for, taking into account the relevant parameters such as delivery date, availability, cost, etc.

Identified services and capabilities and their excess value

The above scenarios require the following capabilities and *services*:

- communication through networking of manufacturing facilities and manufacturers,
- cross-facility coordination of constraints such as deadlines, capacity and materials availability,
- independent order scheduling at the level of the different manufacturing facilities,
- continuous order status monitoring including communication of any deviations in the manufacturing network,
- identification via Cyber-Physical Systems of the entities in the order fulfilment process that are affected by any changes,
- notification of the affected parties of any changes to the order,
- receipt and processing of the affected parties' feedback regarding changes to the order,
- the ability to implement changes to the order even once it has been confirmed and production of the kitchen components has commenced,
- provision of information to the end customer,
- collection of bids from different manufacturing facilities,
- evaluation of these bids based on overarching goals such as cost and deadlines,
- reassignment of production facilities to manufacturers and integration of the new manufacturing facilities into the manufacturing network,
- integration of new, supplementary manufacturing facilities during production, autonomous negotiation by Cyber-Physical Systems across different companies in order to meet the global goals of the customer order,
- adaptation, reconfiguration or evolution of manufacturing facilities, even once the manufacturing order has already been divided up (dispatched) among the different manufacturing resources,

- selection of potential alternative resources to ensure that the product is made to the specifications of the customer order,
- autonomous simulation of the entire process, including alternative resources, and interpretation of the results,
- modification of the original manufacturing sequence and rerouting of the order to alternative resources,
- integration of resources into the manufacturing network using self-description, *interoperability* and self-configuration methods,
- online link to the digital factory, data transfer and continuous alignment with planning data to enable *real-time* response to changes,
- online link to the automation level in order to ensure end-to-end vertical integration; this will require e.g. common equipment *models* based on mechatronic libraries [PLSD11],
- consistent data exchange with other Cyber-Physical Systems at the *Manufacturing Execution System (MES)* level, e.g. logistics applications, in order to enable end-to-end horizontal integration,
- global evaluation of *MES* databases using *data mining* processes in order to enable execution of manufacturing as a self-optimising system [BKS11, p. 65] where, for example, the *MES* monitors the relationships between quality data and process parameters, adjusting the latter as and when necessary,
- searches for related data across different, predominantly proprietary *MES* or factory databases so that e.g. information on a particular issue can be combined.

This in turn means that Cyber-Physical Systems will need to meet the following requirements and be supported by the following technologies and methodologies:

- an adaptable *value* chain,
- heterogeneous manufacturing facilities (different versions and manufacturers),
- vertical networking and end-to-end toolchains at the Enterprise Resource Planning (ERP) and MES levels,
- data coupling between different companies,
- horizontal networking to enable interaction between manufacturing facilities,
- *interoperability* of manufacturing facilities belonging to different manufacturers,
- scalability of manufacturing facilities,
- dynamic reconfiguration at runtime,
- configuration and consistency analysis methods,
- methods to support negotiation such as multiple goal optimisation,
- methods for implementation of *physical context* and *situation awareness.*

2.5.2 PRODUCT AND PRODUCTION FORMATION PROCESS SCENARIO

Current trends suggest that in the future there will be fundamental changes in the processes involved in planning and starting up factories and their systems and components. Manufacturing systems will be built using mechatronic components consisting of 3D geometry, kinematics and logic [PLSD11]. These smart components will know their own capabilities and which systems they can be built into. Where necessary, they will be able to autonomously change their configuration settings so that they can adapt to the current manufacturing operation and the system into which they are currently incorporated. Moreover, their own intelligence will be encrypted to ensure protection against unauthorised copying.

In the future, smart products will also be made from sensorial materials. Intermediate and semi-finished products will either have inherent sensorial properties or will contain distributed networks of several *smart sensor nodes* that will capture a variety of parameters simultaneously, pre-process data locally and detect disruption or emergencies. Even during the manufacturing process, these sensorial materials can register current parameters such as temperature, processing pressure and their position and acceleration. They can then communicate with the manufacturing machinery and transmit this data to it. Likewise, the actual processing parameters of the machinery are transmitted to the product [vTFN09, CEW09].

(1) Manufacturer A has been contracted to make the furniture for the Müllers' new kitchen. **(2)** Manufacturer A has optimised its manufacturing processes to enable a single manufacturing facility to make several product lines with different product generations. **(3)** The Müllers have chosen the latest-generation kitchen furniture in the product line. The relevant materials have to be processed using a specific technique. The materials communicate their specific properties to the manufacturing system and the relevant machines are automatically reconfigured as required. For example, the correct saw is selected and the material is given the correct pre-treatment. **(4)** Owing to the temporary unavailability of a particular raw material, one element of the Müllers' kitchen has to be made with an alternative material. Although the change has no impact on the quality or design of the Müllers' kitchen, the new raw material does need to be processed using a specific technique. **(5)** At the beginning of the manufacturing process, the alternative raw material communicates its properties to the manufacturing system. **(6)** Since the manufacturing system has never used this particular raw material before, it consults the relevant database to find out the optimal configuration for the material's specific properties. **(7)** This configuration is then uploaded to the manufacturing system, allowing the raw material to be processed without delay so that the Müllers' desired delivery deadline remains unaffected.

Identified services and capabilities and their excess value

- ability to provide a self-description in a machine-readable and - if possible - standardized format,
- autonomous definition of unmet requirements for self-configuration, including acquisition of the necessary data from the product and production configuration process,
- reading and interpretation of the self-description and self-configuration,
- autonomous change management and notification of other affected entities about changes,
- *self-organisation*, as demonstrated, for example, by the use of negotiation mechanisms between parts, machines and material flow systems in order to control production,
- extraction of knowledge, e.g. from the manufacturing process, that is then fed back into the factory planning process.
- the information contained in the components can be used to plan and monitor manufacturing and assembly processes so that production can be planned and controlled in *real time*. These new capabilities enable significant quality improvements to be delivered and costly waste to be prevented.

2.5.3 CPS EXCESS VALUE AND POTENTIAL

This section makes a number of preliminary predictions for different sectors and hierarchical levels in manufacturing industry based on the scenarios and developments in CPS described above.

Potential for plant operators in continuous and discrete manufacturing

Plant operators and their suppliers are working particularly hard to drive the development of mechanisms for creating *interoperability*. Their main aim in doing so is to enable faster integration of machines and their components into their manufacturing systems. The plant operators would also like machinery and component manufacturers' products to become interchangeable so that they would not be so tied to particular suppliers for their manufacturing equipment, ultimately enabling them to reduce their costs. These trends will only be reinforced by the fact that future manufacturing systems and components will involve Cyber-Physical Systems.

Further potential for plant operators arises from the fact that it will be possible to manage Cyber-Physical Systems and their embedded software centrally. This will allow the

IT departments of companies or networks of companies to provide their users with the precise functionality that they need to perform the relevant operations.

Competitive pressure is causing more and more plant operators to switch over to using ITIL[15] principles from the realm of commercial IT in the manufacturing IT environment, for example by employing defined Service Level Agreements. They can be expected to continue to follow these trends and demand more developments of this kind in the context of Cyber-Physical Systems. Future CPS suppliers will need to be ready for this.

Potential for systems integrators and IT system suppliers

The future scenarios described above point to new markets for independent IT service providers positioned somewhere between software manufacturers and plant operators who are more focused on maintenance, configuration and parameterisation than on programming. This trend is already becoming apparent – a recent study by Roland Berger Strategy Consultants [Ber10b] concludes that the new generation of European IT suppliers need "strong competencies at the interface between industrial/automation engineering and IT".

Potential for machinery and plant manufacturers

There is a clear trend in the machinery and plant manufacturing industry towards smart networking of manufacturing components and functional *engineering* through interdisciplinary combinations of mechanical systems, electrical equipment and software that integrate several operations. In the future, machinery and plant manufacturers will combine various mechatronic elements to create smart manufacturing systems. There are a number of new business opportunities for these companies, for example enhancement of their own systems using operational field data or preventive maintenance of their customers' systems.

There is intense international pressure in the machinery and plant manufacturing industry where Chinese manufacturers already dominate the market, principally in the low-cost segment [Ber11a]. In the mid-to-high quality and price segments, Cyber-Physical Systems offer German manufacturers an excellent opportunity to supply their customers with additional value-added services that could provide them with a competitive advantage. These include

- energy data monitoring and management using the machines' sensors and processing capabilities,
- predictive maintenance enabled by access to field data through sensors, together with the relevant life cycle models,
- Life Cycle Costing (LCC) to assist with cost management,
- customer-oriented and extremely precise system configuration for specific applications through the combination of Cyber-Physical Systems and components, thus preventing over-*engineering*,
- 24/7 worldwide system support backed up by service contracts thanks to the ability to access a machine's current status online.

Potential for automation equipment and component manufacturers

Over the next few years, automation engineering and industrial IT will be key technologies for ensuring the future competitiveness of German manufacturing industry. In all likelihood, it will be the companies in this industry that will be most affected by the trend towards Cyber-Physical Systems. The principal product groups of this industry include *sensors, actuators*, field bus systems, controllers such as PLC, NC and robot controllers, products with *human-machine interfaces* such as SCADA[16] systems and basic electrical products such as drives and controls. These automation products are used by machinery and plant manufacturers to enable the additional services referred to above. It is therefore key for automation product suppliers to take full advantage of the opportunity provided by the trend towards Cyber-Physical Systems for them to modularise their products and develop platform strategies that enable them to profitably make and deliver products

[15] Information Technology Infrastructure Library, a collection of *best practices* for IT service management.

[16] Supervisory Control and Data Acquisition (SCADA).

for several different customised applications [Ber09, Ber10a, FS09].

2.6 CHARACTERISTIC CAPABILITIES AND POTENTIAL OF CYBER-PHYSICAL SYSTEMS

The CPS scenarios from the areas of mobility, healthcare, smart energy and manufacturing that have been outlined above all demonstrate the diverse functions and valuable *services* that Cyber-Physical Systems can provide. The innovative capabilities of Cyber-Physical Systems are particularly apparent in the numerous potential applications of networked, software-based systems and *services* provided e.g. via the Internet.

This section will describe the system properties and capabilities of CPS and draw some preliminary conclusions about the associated technological requirements and *engineering* challenges.

2.6.1 CHARACTERISTICS AND NOVEL CAPABILITIES OF CYBER-PHYSICAL SYSTEMS

Using the scenario analysis methods outlined in Chapter 1.4, Cyber-Physical Systems can be described in terms of five dimensions that build upon each other as they evolve towards increasing openness, complexity and intelligence:

(1) merging of the physical and virtual worlds
(2) *Systems of Systems* with dynamically adaptive system boundaries
(3) context-adaptive systems with autonomous systems; active *real-time* control
(4) cooperative systems with distributed and changing control
(5) extensive *human-system cooperation*.

Each step in the development of Cyber-Physical Systems and their capabilities and properties involves increasing challenges in terms of user-friendly design and systems *engineering*, as well as with regard to their secure and trustworthy operation (see Chapters 3 to 5).

(1) Merging of the physical and virtual worlds

Rapid progress in miniaturisation, major increases in computing power and tremendous advances in control engineering in information and communication technology all underpin one of Cyber-Physical Systems' key capabilities: the ability to merge the physical and virtual worlds using the opportunities provided by local and global *physical awareness* and the associated *real-time* control of systems and components. One challenge, particularly as far as *engineering* is concerned, is how to combine the continuous systems of control and regulation technology with the discrete systems of information technology. Cyber-Physical Systems gather and process dedicated sensory data from their environment in a highly parallel and distributed manner, combine and interpret this data and use it to control and regulate the behaviour of the relevant *actuators* in *real time*.

The following examples are taken from the scenarios:

- In the *smart mobility* scenario, information is gathered with regard to autonomously driven vehicles' speed, their distance from other objects, the position of the edges of the carriageway and the current situation on the route (traffic, weather, road conditions, accidents, etc.). This information is combined with data on the location, destination and specifications of the vehicle – and on the driver and passengers – to enable the vehicle's behaviour to be controlled.
- In the *smart grid* scenario, both current energy generation and current energy consumption are recorded. In conjunction with forecasts and projections based on market and environmental data, this information is used to produce a global overview of the situation so that energy production, distribution and storage can be controlled in *real time*.

- In the *smart factory* scenario, the production management system and the individual production facilities belonging to the manufacturers constitute a Cyber-Physical System that is geared towards meeting individual customer requests until shortly before production commences, whilst at the same time still maximising the capacity utilisation of the relevant machinery. This is achieved by uploading new configurations from the virtual world – for example of components from specific suppliers – in *real time* during production, so that new materials can still be processed. This is an example of factories being able to adapt to changing requirements even at the logical level.[17]

Cyber-Physical Systems are thus characterised by the incorporation of numerous networked sensors, processors and machines working in parallel to gather and interpret data and use them to take decisions and control physical processes in the real world.

Capabilities

Key features of the examples described above include instantaneous data capture, networking, interaction and control or influencing of the physical and digital worlds. The systems have the ability

- to capture physical data from the environment in parallel via sensors and to merge and process this data – and to do so both locally and globally and in *real time* (physical awareness)
- to use the information that they have gathered to interpret the situation in terms of predefined goals
- to detect, interpret, deduce and forecast malfunctions, problems and threats
- to integrate, regulate, control and interact with components and functions
- to carry out globally distributed and networked control and regulation in *real time.*

The next step for Cyber-Physical Systems involves *Systems of Systems* that operate in controlled combinations of systems with dynamically shifting system boundaries.

(2) Systems of Systems with dynamically adaptive system boundaries

Services and other CPS components are deployed and integrated dynamically to enable devices and systems to be used multifunctionally. This is also true outside of the controlled domain of Cyber-Physical Systems. In other words, CPS cooperate with other systems, subsystems or services in the environment, as demonstrated by the following examples:

- In the *smart mobility* scenario, the autonomous vehicle connects dynamically with a fixed local infrastructure and with other vehicles so that together they form a Cyber-Physical System.
- In the medical emergency scenario, the Cyber-Physical System uses location-based services to guide the vehicle carrying the patient to the nearest doctor or hospital, informs them in advance of the patient's imminent arrival and medical condition and also notifies the patient's family e.g. via their *mobile devices*.
- Mobile diagnosis devices or online *services* search for new household appliances or other *smart appliances* in buildings, configure them and integrate them into the management and running of the building. They also coordinate any necessary additional steps.
- Manufacturing systems integrate the latest firmware updates of their components directly into the manufacturing CPS and, where necessary, inform higher-level IT systems of any changes, e.g. to control variables.

In these examples, the different application situations and tasks that have to be performed require targeted cooperation with known or as yet unknown *services* and systems in the local environment and on the Internet. Different Cyber-Physical Systems combine for a limited period of time to create a *System of Systems* for the particular application

[17] The adaptability of factories is defined in [WRN09, p. 121ff].

situation or task in question. In other words, they establish a temporary combination of systems geared towards fulfilling a common purpose, where the interactions between the different systems create enhanced functionality. Cyber-Physical Systems have the ability to actively build *services* and partnerships with other systems or subsystems – some of which may not even be known at the beginning of the process – and provide new or composite components and *services* in a controlled manner.

Capabilities

Cyber-Physical Systems that form part of *Systems of Systems* should possess the following capabilities:

- interpretation of environmental and situational data at different levels and in accordance with different application situations, using complex environment, situation and application *models*,
- targeted selection, integration, coordination and deployment of services in accordance with the situation, with local and global goals and with the behaviour of other relevant *services* and components,
- composition and integration, *self-organisation* and decentralised control of *services*. Depending on the application situation, conditions in the environment and the current task, Cyber-Physical Systems recognise which services, data and functions are required to complete the task. If necessary, they then actively search for them in other subsystems which may be available online – and which may, in some cases, be unknown – and integrate them dynamically into the system,
- evaluation of the usefulness and quality of the available components and *services*. In order to evaluate and guarantee the usefulness and quality of individual or dynamically created global *services*, Cyber-Physical Systems must be able to establish and evaluate the quality of new *services* and functions and calculate the impact that integrating them into the system will have on the overall quality of *service*. In addition to functional qualities, usefulness and usability, it may also be important to assess potential dangers and establish which guarantees need to be met in terms of *reliability, safety* and *security* and trustworthiness *(Quality of Service),*
- *dependability*. If the quality of a new individual service is not acceptable, the Cyber-Physical System must be able to reject it and select, coordinate and control the optimal behaviour for the user or application under the current circumstances, as well as providing guarantees with regard to the *dependability* and s*afety and security (compliance)* of the systems,
- Access protection and control for the system's native data and services.

(3) Context-adaptive and fully or semi-autonomous systems

One particularly important feature of Cyber-Physical Systems is their ability to adapt to changing environments and application requirements (context *adaptability*), allowing them to operate semi- or fully autonomously. In accordance with the requirements of their current task, they detect the environment and environmental conditions that are relevant to their application – employing the appropriate *services* as necessary –, interpret them and compute, control and coordinate a system behaviour that is useful and valuable to all the relevant actors.

This feature is especially important because it does not merely involve communication and coordination. It also incorporates the entire control domain, i.e. actuators and physical processes, as well as information and management processes via networks such as the Internet. This is illustrated by the scenarios:

- In the smart mobility scenario, when the *car-sharing* vehicle that Frau Müller has hired approaches the school bus, it possesses a detailed knowledge of the current system context, particularly the application situation and environmental conditions (position, road users, their role and their usual behaviour or how they should behave). The vehicle obtains the necessary information about the current situation and events from the networked components in the environment, for example it receives motion data from the *RFID tag* [KOT11] in the child's clothing and additional information from the smart camera system or the fixed local infrastructure. The Cyber-Physical System collates this information, assesses the situation and adapts its behaviour accordingly, in this instance by performing an automatic braking manoeuvre.

- During a car journey, the medical assistant (which is a Cyber-Physical System) detects that the driver's blood pressure is dangerously high, informs the driver, instructs the car to drive itself onto the hard shoulder and obtains information from the local infrastructure about the nearest medical centre with mobile *services*.
- In the *smart health* scenario, several mobile end devices connect both to each other and to the service providers' IT systems via a healthcare platform. Once again, this occurs dynamically and in accordance with the requirements of the current task.
- In the *smart factory* scenario, an "integrated" message is automatically generated when a component from a supplier that is identified via an *RFID* tag has approached to within a predefined distance of the end product.

These applications are all characterised by the fact that they are able to adapt the system's behaviour to changing and potentially unforeseen or previously unexperienced application situations and events. Furthermore, the systems and subsystems are able to intervene increasingly *autonomously* in various processes and take decisions about the application's subsequent behaviour. This requires Cyber-Physical Systems to possess extensive awareness, selection, interpretation, decision-making and execution capabilities.

Capabilities

In order to adapt to different contexts, Cyber-Physical Systems must possess the following capabilities:

- extensive, end-to-end context *awareness*, i.e. the ability to draw on a comprehensive *model* of the current application situation at all times,
- continuous capture, monitoring, selection, processing, evaluation, decision-taking with and communication (with systems, *services* and actors) of environmental, situational and application data, often in *real time*,
- targeted acquisition of relevant information, together with integration, coordination and control of *services*,
- adjustment, updating, coordination and control of the interaction with other systems and *services*,
- determination, analysis and interpretation of the expected behaviour of objects, systems and the current users,
- formulation of an application and *domain model* of all the actors, including their roles, goals and requirements, the available *services* and the tasks that need to be performed,
- goal-setting, including the ability to consider and weigh up the costs and risks of alternatives, together with planning and stipulation of the relevant measures in a series of execution steps,
- awareness of their own situation, including their status and the options available to them, as well as the ability to *self-organise* and coordinate, and
- the ability to learn e.g. different operational and logistics processes or patient routines and preferences in the *AAL* scenario, and the ability to adapt their own behaviour accordingly.

There are undoubtedly major differences in how open the different scenarios are, for example in terms of the restrictions on the type and number of systems and *services* that are dynamically integrated. However, it is precisely this characteristic property of Cyber-Physical Systems that allows them to fulfil their full potential. Depending on the current situation and task, different systems and *services* can be combined and integrated in order to maximise their usefulness.

Applications involving changing contexts and dynamically shifting system combinations lead to the development of increasing numbers of new partnerships and *services* that were not initially foreseen. The employment of Cyber-Physical Systems is associated with the continuous evolution of systems, applications and potential uses. It is important to clearly explain how terms that describe human behaviour are used in the context of Cyber-Physical Systems. There has been a productive debate[18] on this issue for many years in the realms of IT and *artificial intelligence* (AI) [Tur50, Wei76, Dör89], biology/neuroscience [Spi00], cognitive psychology [Fun06] and the sociology of technology [Wey06a, RS02].

(4) Cooperative systems with distributed and changing control

The CPS scenarios and the descriptions of them provided above highlight the following general components and characteristics of Cyber-Physical Systems. They comprise

- *smart embedded systems,*
- globally networked and cooperating systems (often spanning different types of services) and
- systems that operate and cooperate in different social and economic processes (spatially and socially distributed contexts).

This last aspect in particular makes it clear that Cyber-Physical Systems are not usually controlled centrally – their correct and targeted behaviour is the outcome of multiple interaction and coordination processes between fully or semi-autonomous actors. These can be software-controlled machines, systems and *services* but may also be human beings and social groups.

The scenario examples in the realm of *smart mobility* already feature control and decision-taking tasks. The application status determines what happens next based on the available information, systems, networks and communication options in the current environment. This must be done *dependably* and requires cooperation with interactive control operations, as demonstrated by the following examples:

- In the *smart mobility* scenario, the decision of Frau Müller's autonomous vehicle (which is itself a CPS) to make an emergency stop requires several coordinated actions to be performed in advance by various subsystems. First of all, the situation needs to be registered and assessed. This involves recognising the potential dangers posed by all the different actors, but also evaluating information from the camera system in the fixed infrastructure, the *smart tags* in the child's clothing and the *sensors* on board the school bus, as well as potentially also having to include other children and vehicles and the occupants of the cars behind Frau Müller's in the analysis of the situation. In addition, it is necessary to jointly coordinate the desired intervention goals and the subsequent coordinated measures (brake, swerve out of the way, warn the child, detect following vehicles). Frau Müller's *CSV* cooperates with the systems in the immediate environment (school bus sensors, smart tags in the child's clothing) and the fixed local infrastructure to detect the danger, performs an emergency stop and subsequently executes a number of additional coordinated measures such as warning the following vehicles.
- Cooperation plays an even more vital role in enabling *autonomous* and *semi-autonomous driving* of multiple vehicles on motorways or city ring roads. Numerous

[18] When modelling and developing intelligent systems, terms such as knowledge, recognition, learning and acting are generally used to describe the acting of both human beings and machines, despite the fact that autonomous machines such as robots or Internet software bots cannot be said to act like humans. In the context of the CPS scenarios and their analysis, however, the main focus is on the application, further development and limitations of technologies such as *multi-agent systems, ontologies, pattern recognition, machine learning* or approaches to robotics planning (see also the technologies for implementing CPS capabilities discussed in Chapter 5). The same applies to the topic of *human-machine interaction* (see point 5 of this section). Information technology, cognitive psychology and the natural sciences in particular share a long tradition of using each other's explanatory and design *models*, as seen for example in the information processing paradigm used in psychology, or the new sensor technology concepts that draw on the latest discoveries in biology and neuroscience, etc.

distributed cooperation and coordination tasks need to be performed in this context, particularly when unpredictable situations and events come into play or the different actors have changing or competing goals, as is usually the case in public road traffic scenarios.

Further examples of distributed control and the coordination and cooperation capabilities required by Cyber-Physical Systems include:

- shared control in emergency or disaster situations, for example in the event of an accident, in a tsunami warning system that includes evacuation and emergency aid supply logistics and in the event of a volcano eruption where it may also be necessary to coordinate air traffic depending on ash concentrations and weather data,
- in manufacturing industry, the potential automatic reconfiguration of manufacturing systems to make new product variants or distributed manufacturing and retail logistics (using *smart tags*) including adaptive online customer information and billing.

In this context, it is important to draw a fundamental distinction between *human-machine interaction, shared control* and distributed control between distributed hardware and software systems (see the following section on extensive *human-system cooperation*).

Capabilities

The examples cited above require the systems to possess the following general capabilities in order to cooperate with each other and with human beings:

- distributed, cooperative and interactive awareness and evaluation of the situation,
- distributed, cooperative and interactive determination of the necessary measures based on their evaluation of the situation, the local goals of individual actors and the overall goals of the community that these actors belong to. The final decision is negotiated among and assessed jointly by all the involved parties. Consequently, both individual and collective autonomy exist with regard to control and decision-making,
- evaluation of the quality of their own and of external *services* and capabilities,
- cooperative learning and adjustment to different situations and requirements.

(5) Extensive human-system cooperation

Cyber-Physical Systems are capable of instantaneously detecting and interpreting their users' emotional and physical condition (e.g. attention levels, agitation, etc.), making a diagnosis, measuring their vital signs or registering and interpreting their facial expression. This is enabled by a combination of specific medical *smart sensors* for detecting human movements or other parameters and interpretation technologies. Cyber-Physical Systems can use the information obtained in this way to intervene in their environment, for example by altering system responses, transport routes or living spaces, controlling vital functions or employing biofeedback methods to help a patient relax. They are thus directly or indirectly able to register the condition, behaviour and emotions of people or even groups of people and influence how they behave. In the long term, Cyber-Physical Systems will therefore lead to wide-ranging and extremely close *human-system cooperation* which in some areas will far exceed anything that we can currently conceive of today. This raises questions regarding suitable forms of interaction between humans and machines and user acceptance of this technology. These issues are addressed in Chapters 3 and 4.

(5.1) Human being as the formative element of the system's behaviour

Cyber-Physical Systems are systems where people and groups of people are passively or actively involved. Examples include

- traffic management systems that enable coordinated driving in convoys,

- *Ambient Assisted Living (AAL)* systems that assist older people to live independent lives, including the necessary smart buildings technology and integrated assistance systems,
- online social communities that include mobility or delivery *services*, for example.

These systems support human beings, carry out tasks with them and on their behalf and interactively control highly integrated applications and use and business processes in several different areas of their lives. Thanks to the extensive networking and openness of the systems and the relocation of knowledge, functions and *services* to the Internet, Cyber-Physical Systems and the *services* they enable can usually be accessed and utilised by everyone. The many different ways that Cyber-Physical Systems can be used, depending on the needs, goals and requirements of different people, enterprises and social groups, mean that they are developing into an extensive form of *human-system cooperation* with evolutionary and in some cases even revolutionary capabilities.

(5.2) Erosion of the boundaries between human and machine

The *services* provided by Cyber-Physical Systems are available to people irrespective of their location. This means that users do not have to rely on a specific device such as their personal *mobile device* in order to interact with these *services* or with their personal *software agent*. Instead, when they are in their car they can access the *services* via a centre console or head-up display[19], whereas when they are at home they can use a TV, tablet or other *mobile device*, or voice commands picked up by microphones situated in the room or worn on their collar.

In the end, rather than having the impression that they are using a dedicated Cyber-Physical Systems device, people come to regard these devices as pervasive and ubiquitous in nature. Users interact with a variety of individual devices that are integrated into the environment, conveying the impression that they are communicating with a single system. This will be especially true in smart rooms that are fitted with numerous *sensors* and other human-machine interfaces.

As far as the user is concerned, Cyber-Physical Systems are ubiquitous[20]. Users are constantly surrounded by *services* that provide them with information about alternative travel routes and means of transport, the current traffic situation or upcoming doctor's appointments, for example. At the same time, these *services* – which the user may or may not be consciously aware of – intervene in the environment on the user's behalf, for example by booking a *premium lane* on the motorway or administering insulin to them via an implant. This interactive experience causes the boundaries between man and technology to dissolve – users obtain information from any number of globally distributed services, while Cyber-Physical Systems also enable them to act globally themselves.

This will lead to **changes in our society**, for example in the realm of private transport. Teleinformation and teleaction will make some journeys unnecessary. In urban areas, close coordination of information about transport services may lead many users to decide that they no longer need to own their own vehicle. As described in the *smart mobility* scenario, the new opportunities provided by Cyber-Physical Systems will play an important part in making this possible. Moreover, *autonomous driving* will create openings for novel *business models,* e.g. in the areas of *car sharing* and fleet management.

Capabilities required for human-machine interaction

Cyber-Physical Systems also have to integrate human behaviour at the physical level. This enables them to provide human beings with support via direct integration of sensors and actuators, for example in the form of mechanical limbs. This in turn enhances people's perception and abilities, even though they may not always be aware of it.

[19] Display systems in vehicles or aircraft that project important information into the user's field of view so that they can keep their head raised.
[20] The term "Compute Continuum" has been coined to describe this phenomenon.

The ability to enable *human-machine interaction* has five broad goals:

- intuitive support through enhanced interfaces, e.g. *multimodal* active and passive control,
- enhanced human perception and abilities thanks to unrestricted and virtual system networking,
- enhanced perception and acting abilities for particular groups of people such as diabetes patients or electric vehicle drivers,
- detection and interpretation of the condition and behaviour of human beings. This includes both their emotions, needs and intentions and the ability to register the condition and environment of both human and system,
- enhanced intelligence, i.e. the ability for systems to cooperate with individuals or groups of people in order to take integrated, interactive decisions and actions, including the ability to learn.

Whilst there are some areas, such as power grids, where the *services* performed by Cyber-Physical Systems are largely invisible to the user, applications in the realms of *autonomous mobility* and *E-Health* in particular raise a number of fundamental legal and social questions in addition to the technological issues.

A table summarising the new capabilities of Cyber-Physical Systems and the associated requirements and challenges appears in Section 3.5.

2.6.2 BENEFITS AND EXCESS VALUE FOR SOCIETY AND ECONOMY

In addition to the opportunities described in the scenarios, there are several other examples of the concrete benefits of Cyber-Physical Systems. In some cases, intensive work is already underway to realise this potential:

- systems for predicting, detecting and coordinating the response to natural disasters, e.g.
  - tsunami warning systems featuring distributed tsunami detection and impact assessment, including the ability to deliver networked and coordinated warning, planning, evacuation and emergency aid supply actions and incorporating management systems for organising rescue operations and the provision of medicine, water, food, accommodation, etc.
  - autonomous robots and drones acting as specialised CPS components. In the event of chemical accidents, fires, earthquakes or other disasters, these can perform coordinated operations to investigate the scene of the incident, search for victims, locate and secure any dangerous areas or detect and remove any hazardous materials. Examples include the deployment of robots in radioactively contaminated areas following the Fukushima disaster or the annual search-and-rescue challenge for Unmanned Aerial Vehicles (UAVs) in Australia [UAV10].
- safety and security monitoring and support, e.g. at major events, featuring distributed site surveillance and monitoring for potential attacks, as well as the ability to detect and control panic situations. This includes, for example, coordination with the emergency services to assist with evacuations and provide targeted medical care to injury victims (see "*Späher, Scanner und Sensoren*" (Spying Devices, Scanners and Sensors), a programme on high-tech issues broadcast on Germany's 3sat channel on 10 October 2011 [3sa11]).
- networked service robots – highly specialised and increasingly networked robots that perform a variety of assistance and control tasks in different industrial and social areas of application. Examples include
  - autonomous and networked Automated Guided Vehicles (AGV) in container transport platforms that enable coordinated transport and loading of containers onto ships, also as part of global logistics processes

- smart wheelchairs that are networked with other systems and healthcare providers to enable the elderly to live independent and mobile lives in their own homes
- further applications such as the novel service robot applications arising from the EFFIROB study conducted by the German Federal Ministry of Education and Research (*BMBF*) [HBK11], e.g. systems for transporting hospital patients or *assistants* in the dairy cattle industry, although the latter can hardly be described as *human-system interaction*.

These capabilities enable Cyber-Physical Systems to carry out a variety of different tasks either independently or in cooperation with other systems, components or online services, but above all in conjunction with and on behalf of human beings.

All of the examples described above illustrate the challenges facing everyone involved in the research, design, development and application of smart networked technologies. In addition to addressing the technological challenges associated with *real-time* networking, physical awareness and coordinated control, it is necessary to make the most of the opportunities afforded by current technology trends to develop interactive solutions. The following goals need to be met:

- context *awareness* and coordinated context assessment geared towards the specific situation and application
- action control that it is integrated with social processes and goals
- *human-machine interaction* and *cooperation* that is designed in such a way that different actors can use the technology for their own particular goals, configuring it and deploying it safely and securely in manufacturing and business processes, in their private lives and in social contexts, and
- wide-ranging support from fully or semi-autonomous technologies for industrial, business and private applications.

Importance to the value creation of the enterprises

The descriptions of how the scenarios work clearly illustrate which components and actors and indeed which infrastructures and communication platforms need to cooperate and be coordinated with the complex networks of different services.

There is huge potential for innovation in this area, both in the development and design of the individual components or embedded systems, in the distributed *value chains* and *networks* required for their manufacture, integration, coordination and quality assurance – i.e. *validation* and *verification* – and in the interactive and *participatory design* of the application processes together with customers and users.

The opportunities and challenges associated with Cyber-Physical Systems are studied in detail in the following chapters.

3 CPS THEMATIC AREAS

The future application scenarios presented in Chapter 2 provide an indication of the thematic areas and research topics that will have to be addressed in order to make the design and control of Cyber-Physical Systems feasible. The relevant research topics include:

- the design and construction of physical, logical and commercial *smart* networked *infrastructures*, application architectures and *CPS platforms* for
  - distributed data capture and coordinated data processing and interpretation, together with the corresponding control functions (sensor and actuator technology),
  - the highest possible degree of *interoperability* both within individual and between different application *domains* and the integration of new or expanded applications,
  - the development of *domain models*, i.e. formal knowledge about applications, including requirements and function *models* and architecture *frameworks* (see 3.1),
- how to ensure the *safety* and *security* of Cyber-Physical Systems' communication and application *services* and to minimise the risks associated with their use, especially when they involve new cooperation arrangements in system landscapes and contexts of use that are open, uncertain and constantly evolving (see 3.2),
- *participatory design* of *human-machine interaction*, with transparent control structures, decision-making paths and integrated (local, regional and global) *situation* and *context awareness*, in order to ensure that the application processes are individually controllable during use and interactively designed (see 3.3, 3.4 and Chapter 4),
- ensuring that functioning CPS solutions are *dependable* and trusted by all the relevant actors through joint testing of prototypes, extensive *validation* and *verification* and the establishment of demonstration initiatives (see 3.6),
- the translation of research findings into practical innovations that will enable German enterprises to gain a global competitive advantage (see 3.6).

The open nature of the application systems, their enhanced ability to adapt and cooperate and the increasingly interactive design of Cyber-Physical Systems, initiated by and involving users and user groups with different goals, all mean that it is virtually impossible to draw up a single set of criteria that will determine the success and acceptance of Cyber-Physical Systems.

Acceptance criteria: the key acceptance criteria such as systems' *usability*, intuitiveness in use, controllability and trustworthiness are dependent on their ability to adapt to different contexts of use and be safely and securely integrated into these contexts. Moreover, the global, networked deployment of Cyber-Physical Systems and the extent and pace of change within our societies will make it extremely difficult to determine the requirements of customers and markets, especially since these will themselves be subject to constant change. These changes will furthermore be influenced by advances in *ICT*.

Evolutionary development: alongside the technological research questions relating to the capabilities of smart Cyber-Physical Systems, the other main challenges concern their *adaptability* and ability to cooperate in social contexts, as well as their evolutionary development. In general, these issues relate to all the factors where human beings are involved (*the human factor*). In order to develop usable and controllable CPS innovations (see 3.6), it will be necessary to employ interdisciplinary approaches and competencies that facilitate *participatory engineering* involving the users.

3.1 SMART INFRASTRUCTURE AND THE REQUIRED DOMAIN MODELS

The most important requirements and necessary key investments for the successful implementation of Cyber-Physical Systems are illustrated both in the analysis of the CPS scenarios provided above and in various recent studies concerning the challenges associated with future embedded systems (Nationale Roadmap Embedded Systems [ABB+09]) and studies focused on their integration into the *Internet of Things* and *Services* (recent studies and books include: [BMW08, BMW10a, AB+11, FM+05, Mat07, UHM11b]).

One key requirement will be the step-by-step construction and expansion of standardised and flexible infrastructure and communication platforms. It will be necessary to equip *interoperable* and compatible CPS components and *services* with the appropriate interfaces and protocols. This includes the development and construction of the relevant components and architectures in the physical environment, such as *smart* transport *infrastructures*, or smart barriers and blinds in contexts involving the use of autonomous robots. These will also all need to be fitted with their own sensors, communication technology and miniaturised control systems.

3.1.1 INFRASTRUCTURE FOR INTEROPERABLE AND DEPENDABLE CPS SERVICES

In addition to equipping the environment with increasingly powerful *sensors, actuators*, built-in processors and standardised interfaces and protocols, the following will also be necessary:

– a powerful *communication infrastructure* based on high-bandwidth networks, that is both *dependable* and accessible at any time and in any place and,
– based on this infrastructure, a *CPS platform* including the associated *middleware* that endows Cyber-Physical Systems with the required *interoperability*, extensibility and application integration whilst also ensuring that the coordination and cooperation *services* are fundamentally *dependable*, *safe* and *secure*.

Figure 3.1 uses the example of *Ambient Assisted Living (AAL)* to illustrate the components and protocols required to deliver comprehensive, integrated healthcare for the elderly and infirm.

A *CPS platform* needs to perform numerous generic functions such as the coordination and synchronisation of heterogeneous protocols, the integration of online *services* and the provision of basic *Quality of Service* guarantees required by the application, for example with regard to infrastructure *interoperability*, data *integrity* or *real-time capabilities.* This needs to be supplemented by the development of *domain*-specific system architectures so that the individual fields of application can be connected up with each other and integrated into the overall system.

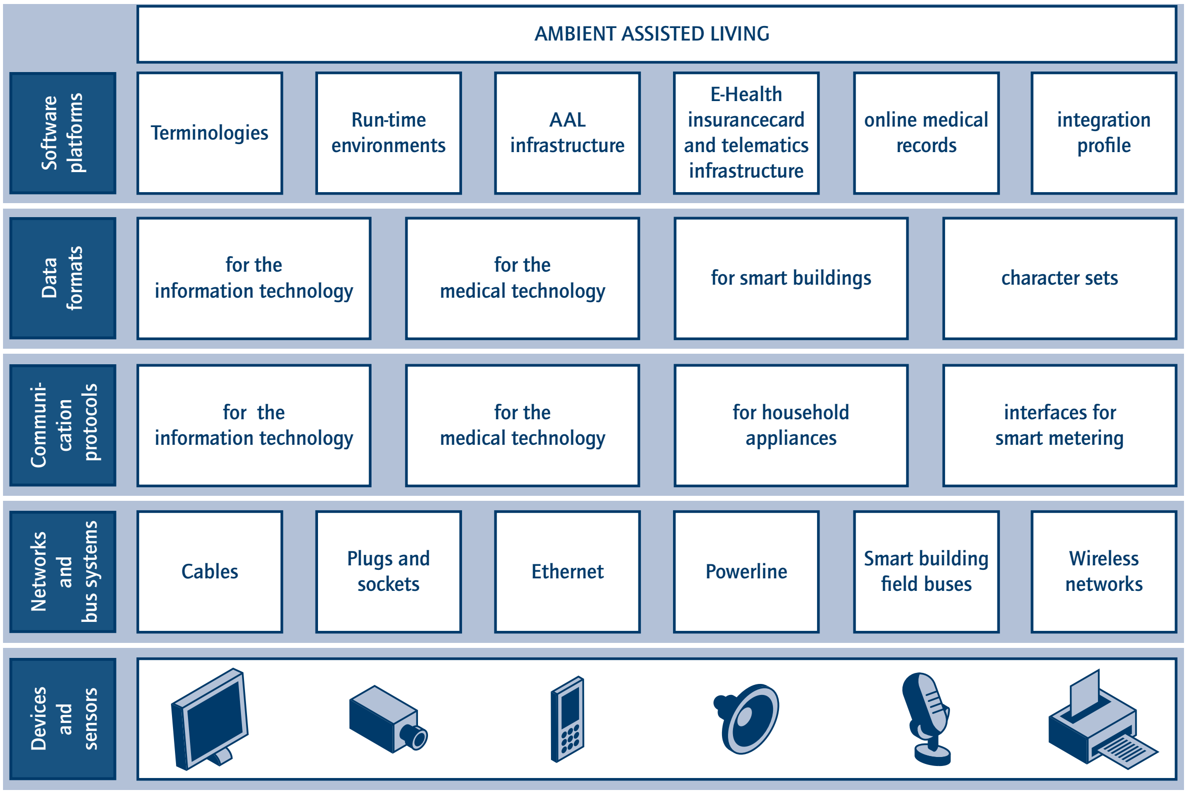
This is a mammoth task, since *smart infrastructures* will not be enough on their own to enable full implementation of Cyber-Physical Systems. For example, in order to enable vehicles to communicate simultaneously with the fixed local infrastructure and with cooperating traffic management systems whilst at the same time accessing global information, maintenance or billing services over the Internet, it will be necessary to build binding *domain-specific* and cross-*domain* standard architectures, interfaces and protocols. The particular challenge in this regard will be to design interoperable interfaces at the application *service* level and integrate them specifically in order to enable end-to-end situation- and context-sensitive usage processes[21]. These processes will need to provide the abovementioned *interoperable* and *dependable services* whilst at the same time adapting to the evolutionary expansion of CPS *services* and the associated requirements.

Current examples of efforts to meet this challenge include *domain*-specific, industry-specific and international standardisation initiatives such as:

[21] The European Telecommunication Standards Institute (ETSI) distinguishes between the following interoperability levels, each of which is built on top of the one beneath it: protocol, service, application and user-perceived interoperability [ETS94].

- the EPC Global Architecture Framework in the field of global commerce and global logistics [UHM11a, WS07],
- the standardisation and architecture framework for *smart grids* (AMI/FAN Architecture Framework [son09]),
- the standardisation initiatives in the fields of telecommunications and smart transport systems (ETSI ITS Architecture Framework [Eve10] and the “Sichere intelligente Mobilität” (Safe, Smart Mobility) project being promoted by various German ministries[22] (SimTD) [sim11]),
- the interface integration and *interoperability* initiatives in the field of *Ambient Assisted Living (AAL)* [Eic10],
- standardisation initiatives in manufacturing industry, e.g. universal interfaces between plant control systems and *Manufacturing Execution Systems* (MES; VDI 5600 and the related IEC committees) and standardisation of the self-description of manufacturing systems and their components, e.g. using the AutomationML data format (IEC project PNW 65E – 161 Ed.1 [aML11]), in order to ensure a consistent description of every stage from the engineering to the operation of manufacturing equipment.

Figure 3.1: Overview of basic components and technologies in the area of Ambient Assisted Living (AAL) (taken from [Eic10])



	AMBIENT ASSISTED LIVING					
Software platforms	Terminologies	Run-time environments	AAL infrastructure	E-Health insurancecard and telematics infrastructure	online medical records	integration profile
Data formats	for the information technology	for the medical technology	for smart buildings	character sets		
Communi-cation protocols	for the information technology	for the medical technology	for household appliances	interfaces for smart metering		
Networks and bus systems	Cables	Plugs and sockets	Ethernet	Powerline	Smart building field buses	Wireless networks
Devices and sensors						

[22] Federal Ministry of Economics and Technology, Federal Ministry of Education and Research, Federal Ministry of Transport, Building and Urban Development.

When developing and standardising this type of *architecture framework, it is important to draw a fundamental distinction between* generic and application *domain*-specific CPS components, interfaces, protocols, data and *services*. It is necessary to develop a standard *CPS platform* and *middleware* for specifying the communication, synchronisation and *interoperability* tasks of Cyber-Physical Systems as well as *services* for organising components and for the management and guaranteeing of basic *Quality of Service* requirements. In doing so, it will be important to observe the *security* standards contained in the IPv6 protocol [HV08], Universal *Plug and Play* [JW03] and Devices Profile [OAS09]. As far as possible, application services for general use – e.g. billing, payment, booking, calendar or travel *services* – should also be designed in a standard manner. The same applies to interactions between the different actors. These *services* need a standard design so that they can be used in different areas of application and be integrated into the *CPS platform*.

Furthermore, standardisation should not be confined to communication with devices, software and network components or *services* and the interactions between them. In fact, standardisation of these aspects will lead to increased standardisation of the application processes and the associated context information. Cyber-Physical Systems will be able to re-use these in similar situations in order to control systems and communicate with users. Standardisation will enable Cyber-Physical Systems to adapt to the different requirements of different application situations and is thus a key enabler of their successful deployment and acceptance.

3.1.2 REFERENCE ARCHITECTURES AND THE BUILDUP OF DOMAIN KNOWLEDGE

In order to enable them to register and interpret complex application situations and interact and cooperate with subsystems and human beings, Cyber-Physical Systems must possess a certain level of "knowledge" (in a knowledge *model*) or be able to acquire this knowledge through different *services*. This includes knowledge about specific applications in the form of *domain models* and the associated architecture concepts, components and *services*, as well as knowledge about the goals and requirements of both the application and the user

As a result, the development of Cyber-Physical Systems will not only require the establishment of domain-specific *architecture frameworks*, functions and *services*. It will also be necessary to systematically develop *domain models* comprising formal knowledge *models* that can be flexibly expanded and that incorporate the following areas:

- physical application environments, their structures and rules,
- the roles, behaviour and significance of the different components vis-à-vis the application, *stakeholders* and users,
- reference applications and requirements *models*, processes, functions and interaction patterns, application and business rules,
- the quality requirements at different application levels in order to enable consistent evaluation of *services* and the relevant cooperation and composition options.

It is important to distinguish between quality requirements

- from the viewpoint of the user, the client systems and their respective contexts of use (e.g. expanded versions of the *Quality in Use* concepts in ISO standard ISO 9126[23] [ISO10] or the expanded *usability* criteria for Cyber-Physical Systems in ISO 9241-110[24]),
- for individual *services* in terms of agreed guarantees and standards (*Quality of Service*),
- for the underlying system architectures, interfaces and protocols[25], and
- that need to be met for *compliance* purposes.

[23] This has since been expanded and incorporated into the ISO/IEC 25000 standard.

[24] EN ISO 9241 is an international standard that provides guidelines for interactions between humans and computers [ISO09].

[25] See also the system levels concept in Chapter 5.3.3.

The *domain models* incorporate strategies and concepts

- for classifying CPS situations and applications,
- for defining their roles and methods of application; for example, it is necessary to ensure compliance with *safety, security* and *privacy* protection requirements,
- for negotiations between and coordination of subsystems in accordance with agreed technical norms and standards.

This will require CPS architectures to possess specific structures and components.

3.1.3 CHALLENGES

The challenges associated with the construction and development of smart infrastructure, infrastructure systems and domain models for Cyber-Physical Systems are as follows:

- **cross-domain standardisation**, *interoperability* and context-dependent integrability, as well as composition of the architectures, interfaces and *domain models* at the different system levels; *technical, semantic* and *user-visible interoperability*,
- **the necessary vertical and horizontal interoperability** and the associated communication, coordination and integration mechanisms between the individual components and levels (see also Chapter 5.3.3.2),
- **the definition of generic CPS communication architectures** and *CPS platforms* and *middleware* with basic *interoperability*, composition, synchronisation and quality assurance *services* (see also Chapter 5.3.3 and Appendix B),
- **the definition of architecture frameworks**, *domain-specific* and cross-*domain* context, environment and requirements *models*, together with the relevant usage processes and their deployment in specific CPS applications (*tailoring*),
- **the development of appropriate methods and techniques** to enable the *adaptability*, dynamic configurability, learning and upgrading of functionalities and *services* and
- **harmonisation of the different rates of development and life cycles** of individual CPS components, systems and application *domains*, and incorporation of the viewpoints of all their respective actors into every area of the systems engineering process.

The main challenges in terms of creating the basic conditions for the deployment of fully or semi-autonomous Cyber-Physical Systems, e.g. in the field of smart mobility (see Chapter 2.2), are as follows:

- Design of the automatic *adaptation* and cooperation mechanisms and ensuring that they are legally compliant. It will be necessary to answer the following legal questions: What risks are involved? Who is liable for damage or accidents? Who provides the warranty? See also Chapter 3.2,
- Design and establishment of environmental conditions: which physical requirements and behaviour rules need to exist in the environment and the relevant *smart infrastructures* or infrastructure systems in order for the systems to achieve the necessary levels of *safety, security* and acceptance? What are the costs and benefits of carrying out this development or conversion work (in monetary and environmental terms and in terms of people's living spaces and conditions) and who will pay for them?
- the economic and social debate regarding the opportunities and risks of the new technology and its applications; see also Chapter 4.1.

3.2 NETWORKED ACTING IN UNCERTAIN PHYSICAL AND SOCIAL ENVIRONMENTS

Enabling mechanical, fully or semi-autonomous networked acting in uncertain environments is one of the key challenges associated with Cyber-Physical Systems. Hardware and software systems that were previously developed with a specific purpose in mind and acted in isolation of each other are now becoming more and more open and are increasingly working together in expanded applications and wider social contexts, resulting in the emergence of new capabilities. As a result, systems are behaving in a manner that is increasingly uncertain and unpredictable and cannot easily be controlled by technical measures alone. This behaviour also entails challenges relating to the wider *safety* and *security* of the systems, as well as the optimal forms of *human-machine interaction* and *cooperation*. The potential threats are also greater, making it necessary to answer questions pertaining to legal certainty and how to guarantee privacy and know-how protection for the companies involved in the value network.

Fully or semi-autonomous networked acting

As outlined above, Cyber-Physical Systems are characterised by the fact that they are capable of complex context and *situation awareness.* The systems interpret the physical and social environment that they have registered using *sensor* data and user input – including human behaviour, intentions, goals and processes. In order to do this, they draw on a wide range of data and information captured in a variety of different ways or provided by other systems, combining the input from all these different sources. Since it is difficult to ascertain the accuracy and *integrity* of data in the globally networked context of typical CPS scenarios, there is a heightened risk that potentially imprecise or contradictory information could lead the systems to misinterpret a given situation, causing them to take the wrong decision or having an undesirable influence or impact on their subsequent behaviour. There is a particular danger of this resulting in safety-critical behaviour.

It is thus important to ensure that Cyber-Physical Systems and their components behave as acceptably and *robustly* as possible in these situations. As such, it is essential for *safety-critical* systems to be provided with enhanced *safety* measures. Moreover, even when they are not *safety-critical,* Cyber-Physical Systems should still always behave in a way that provides users with optimal support in the pursuit of their intentions and goals and under no circumstances hinders them in this regard.

The need for correct and *reliable* networked behaviour in different application contexts and in cooperation with a wide variety of different networked systems requires both the overall system and its components to possess the following capabilities:

- the ability to register and assess situations as accurately and appropriately as possible in keeping with the application goals and contexts of the actors,
- the ability to check and, if necessary, guarantee the accuracy and quality of the information, communication and control services provided by the participating systems and components,
- the ability to form strategies – including planning, negotiation and cooperation – in order to put together the relevant *services* and ensure that they are performed to the required quality standard by the network (non-functional requirements),
- the ability to provide transparent *human-machine interactions* that can be understood and controlled by the user, in order to prevent incorrect operation or deployment of the system that could pose a threat to the environment and the actors, and
- the ability, in the event of an emergency where the situation is uncertain and the consequences of the system's acting unpredictable, to take the decision not to perform a desired function – but only if doing so will not put the user at even greater risk.

The extent to which users and actors are taken into account in these considerations and decisions depends on the type and field of application of the system and the tasks that it is expected to perform, as well as on the respective roles and capabilities of the people involved. For example, these roles and capabilities are distributed differently in systems that coordinate and monitor energy *services* in *smart grids* or global logistics networks compared to the field of Ambient *Assisted Living (AAL)* or the mobility scenarios such as those described in Chapter 2.2. In all these scenarios, however, the user's ability to control and co-determine the system's behaviour is key to the *safety* and *security*, quality and in particular acceptance of Cyber-Physical Systems (see also Chapter 4).

These capabilities of Cyber-Physical Systems are also reflected in their architecture, the technologies that they employ and the way that the systems are engineered (see also Chapter 5). The following sections address the challenges described above using the scenarios and a shell model of socio-technical CPS applications.

3.2.1 THE SHELL MODEL OF SOCIO-TECHNICAL CPS APPLICATIONS

Figure 3.2 uses a schematic representation of two application domains, mobility and healthcare, to illustrate the open nature of Cyber-Physical Systems and the way that they can pervade several different areas of our lives. The *model* describes the actors involved in a *domain*, i.e. systems, users and *stakeholders*, and the relationships governing their interactions in terms of the controllability, definability and predictability of their behaviour. It distinguishes between the following three realms in the meaning of fields of actions.

- **Controlled core realm (1):** this realm comprises the traditional closed embedded systems of an area of application (e.g. a building's heating system) which are characterised by controlled communication and interactions with their environment. The *safety* and predictability of the system's behaviour are guaranteed provided that it is operated correctly.
- **Specified realm (2):** in this realm, although systems and components from the application area cooperate with each other, they do so in predefined and restricted usage situations where they behave in a specified manner. However, their behaviour is uncertain in unforeseen situations that do not conform to the standard rules, for example if a child throws an item of clothing fitted with a *smart tag* into the road (see the mobility scenario in Chapter 2.2.2). Users who behave in accordance with the rules or possess the necessary training and expertise form part of this realm. Communication within realms (1) and (2) is controlled and targeted.
- **Realm of the open, networked world (3)**: this open environment includes users, actors – including groups –, systems, *services* and data – which may originate from the Internet – that may be active in one or more areas of application. As far as the inner realms – i.e. their components – are concerned, their source and the communication with them is less *dependable*. Moreover, their contexts, goals and behaviour cannot be easily classified and interpreted.[26] The key feature here is that users and components in the environment or online services interact with each other on an ad hoc basis, putting the components from the inner realms to use in their own particular context. Whilst this can potentially enable new uses, it can also involve new risks.

For example, it is already possible to use *sensors* and controllers that are globally networked over the Internet – e.g. via the online services provided through Pachube ([Pac11, PCM11]) – to monitor events in the vicinity of a holiday home and, if necessary, activate security measures and control the relevant devices, e.g. lower security barriers.[27]

Figures 3.2 and 3.3 illustrate the potential of cross-*domain* networking using the example of targeted interaction between the two sub-scenarios described in Chapters 2.3 (*smart health*) and 2.2 *(smart mobility*). In Figure 3.2, the areas shaded in

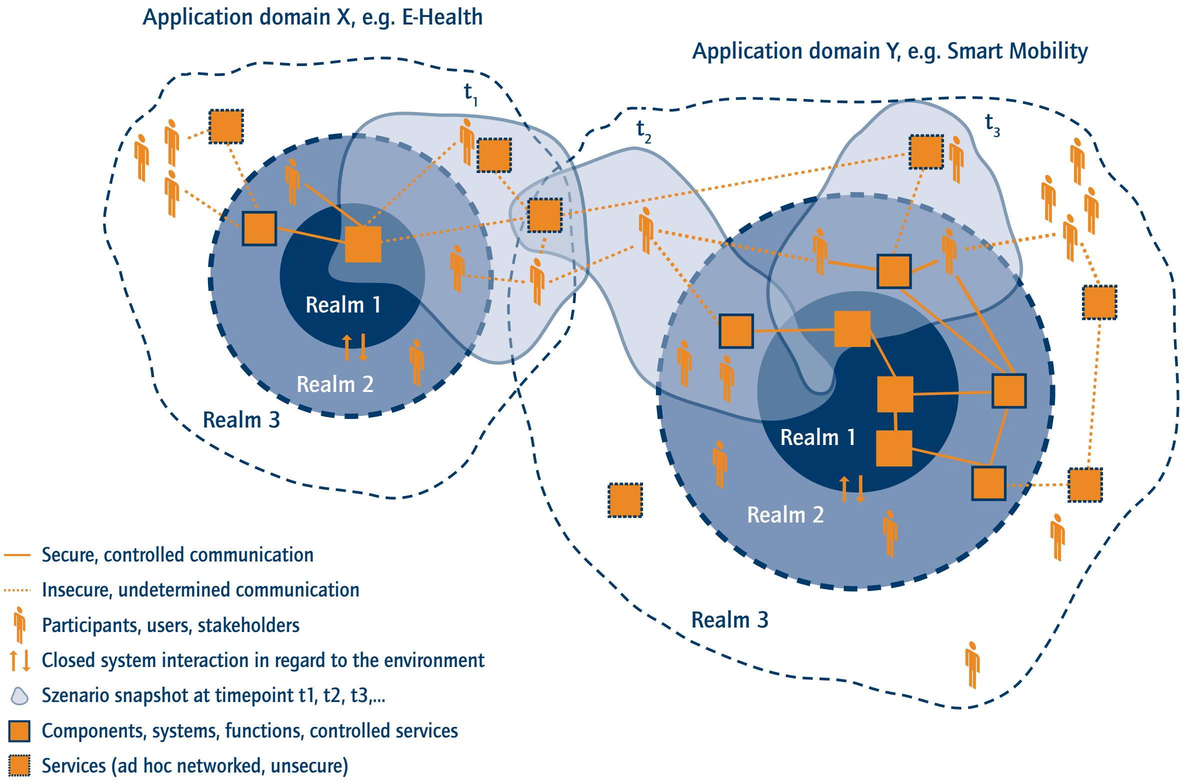
[26] From the point of view of the specified application *domains* (the inner realms).
[27] However, the security and legal position has yet to be clarified.

light blue that cut across realms 1 to 3 represent the dynamically changing sub-scenarios in the two areas of application, i.e. the operative system boundaries at a given point in time:

- **Scenario 2.3.3:** automatic detection of an emergency and provision of first aid. In this sub-scenario, after Frau Huber faints (stage 4), she receives first aid from the paramedics who have rushed to the scene (stage 5) before being taken to the casualty department of the nearest hospital.
- **Scenario 2.2.3**: CPS as a comprehensive mobility assistant. In stage (10) of this sub-scenario, the convoy with Frau Müller's *car sharing* vehicle has to leave the *premium lane* in order to let an ambulance through. This could be the ambulance that is taking Frau Huber to the hospital in the previous scenario.

The vehicles on the road adapt to the new situation. Although vehicles using the *premium lane* know that they are required to let emergency vehicles such as police cars, fire engines or ambulances through, they do not know in advance when they will have to do this or exactly which vehicles will be involved.

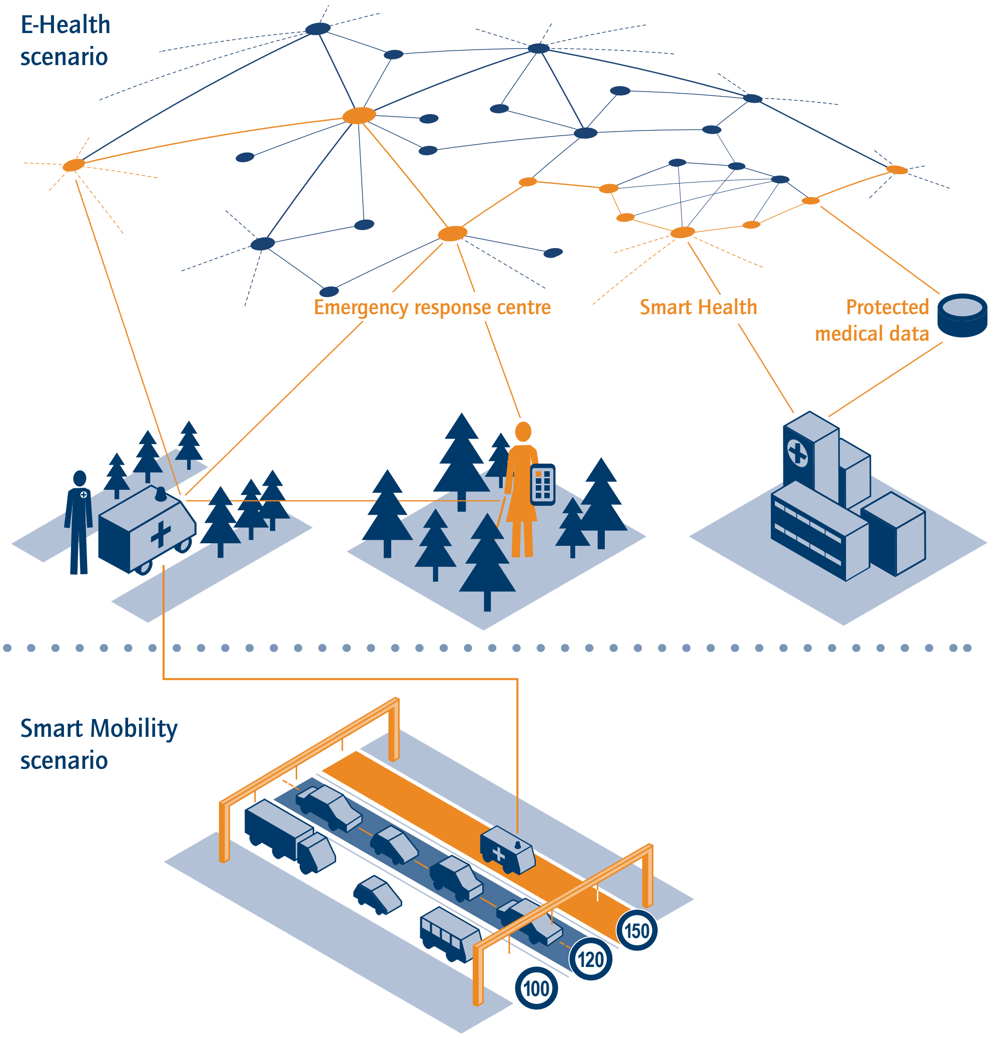
Figure 3.2: Overview of the domain structure based on the level of predictability of the behaviour of the systems and human beings involved


Application domain X, e.g. E-Health
Application domain Y, e.g. Smart Mobility
t_1
t_2
t_3
Realm 1
Realm 2
Realm 3
Realm 1
Realm 2
Realm 3
Secure, controlled communication
Insecure, undetermined communication
Participants, users, stakeholders
Closed system interaction in regard to the environment
Szenario snapshot at timepoint t1, t2, t3,...
Components, systems, functions, controlled services
Services (ad hoc networked, unsecure)

The above description of how the sub-scenarios can change demonstrates that the boundaries between CPS application scenarios are open and fluid. Depending on the situation and the acting of the relevant actors, the Cyber-Physical System configured for the sub-application in question has to be prepared to incorporate new, uncertain, changing and unpredictable actors and components.

This in turn raises the challenge of aligning the goals, intentions and behaviour of the participants. This is necessary

Figure 3.3: Cross-domain coordination example based on sub-scenarios from Chapters 2.3 (Smart Health) and 2.2 (Smart Mobility)



in order to ensure that the situation unfolds as safely as possible and to prevent or at least minimise undesirable behaviour, potential damage and danger to human beings. Appropriate strategies, concepts and technologies are required in order to do this.

3.2.2 INCREASINGLY UNCERTAIN BEHAVIOUR IN THE NETWORKED WORLD

Globally networked systems that adapt to different situations and contexts and are capable of cooperating across different *domains* are of course extremely complex. This means that there is an inherent degree of uncertainty with regard to the dangers to human beings that could arise from the behaviour of Cyber-Physical Systems and their sub-systems and *services* if they are used in an unpredictable and inadequately coordinated manner. By opening up previously closed and secure embedded systems and using them in networked applications, it is possible to trigger chain reactions that result in unforeseen consequences and may even cause damage. Furthermore, the open-ended utilisation and networking of data and services can put actors' *security* and *privacy* protection at risk in every individual application or CPS component, potentially resulting in a loss of control.

Some of the potential causes or triggers of system malfunctions are as follows:

- direct and indirect misinterpretation, misuse and erroneous propagation of data, *services*, functions and components,
- un*reliability* of distributed and networked components and *services*,
- incorrect operation and use of systems,
- unresolved or unresolvable goal conflicts and
- tampering, or attacks on systems' weak points.

In addition to failings in the systems' protection mechanisms or their adaptability during use, other causes can be associated with shortcomings in their design and development – some systems or subsystems are simply not suited to the wider uses involved in CPS scenarios. Possible shortcomings include:

- being too slow to spot or failing to correctly assess events, developments and user and customer needs and requirements in the environment or application world (realm 3 in Figure 3.2),
- flawed, inadequate or inappropriate integration and composition concepts in the systems' specification, design and development,
- flawed or inadequate needs-oriented *human-machine interaction design*. The main challenges in this regard are the ability to adapt to the user's situation and context of use with *shared control* and design of the networked behaviour of Cyber-Physical Systems.
- flawed or insecure concepts and mechanisms in the underlying *communication* and networking *infrastructures* and architectures.

There is a particularly urgent need to develop and deploy enhanced methods for *validating* and *verifying* these highly adaptive systems, such as model-based simulations, for example.

3.2.2.1 Enhanced safety – safe Cyber-Physical Systems in uncontrolled environments

Since Cyber-Physical Systems pervade every aspect of people's lives, their *safety* cannot be adequately guaranteed by the use of indirect *safety and security measures* – e.g. restricted access – or safety information such as user training. Instead, it is necessary to employ a wide range of *functional safety* strategies and measures geared towards reducing the risks to an acceptable level.

Hitherto, the *functional safety* of Cyber-Physical Systems has been based on the assumption that they will be deployed in a controlled environment from the beginning to the end of their service lives. In particular, this controlled environment involves the specification of restricted user groups, e.g. trained drivers or operators, and restricted conditions of use, e.g. authorised operating temperatures or vehicle speeds. As long as these conditions are met, the system is guaranteed safe to use. Although these are not usually closed systems, they nonetheless have clearly defined system boundaries and environments. They thus count as systems in the controlled core realm, or realm 1 in the classification outlined in Section 3.2.1. This classification is reflected in norms and standards such as IEC 61508, DO 178B and ISO 26262.

However, this rigid *model* of a category of controlled systems will in many respects no longer be appropriate for future usage scenarios. This is especially true of future system life cycles where users will replace faulty system parts with new parts of their own, for example by integrating a new *mobile device* into a vehicle's *human-machine interface.* This type of dynamic configurability is of fundamental importance to the use of CPS-type systems, since the different components can only operate in concert with each other – *telematics* functions, for example, require a smartphone to be present on board the vehicle. It is no longer possible to provide complete control over this type of system, not least because of the fact that different components are owned by different operators, raising a number of questions concerning legal liability. Consequently, it is necessary to build systems that are based on clearly defined application domains and platforms rather than controlled structures.

Binding conditions for safe use are specified in these defined *domains*, just as they are in the controlled core. However, compliance with these conditions is now largely ensured by the system itself rather than by external structures. Instead of *safety* being built into the system when it is put together (*safety* at build time), it is the system itself that endeavours to ensure *safety* during operation (*safety* at run-time). Key capabilities of such systems include the safe incorporation of system components, monitoring the system's operation to detect any dangers arising from failures or operating errors, and the deployment of comprehensive processes geared towards actively preventing threats to both the *system and to human beings (fail-safe* and *fail-operational* processes).

It is not possible to require users of these systems to have special knowledge or to undergo specific training. For example, it is unrealistic to expect every single driver to be trained to use the latest version of their route planner *services*. In order to ensure that lay users can still use the system safely, it will be necessary to develop methods that enable intuitive and transparent user interactions and ensure safe, *shared control* between human beings and the system. In addition to the system providing transparent danger alerts and guiding the user's attention, this will also require both users and machines to share the same picture of the situation in order to ensure that they act consistently (see also 3.3).

In order to enable the controlled integration of and cooperation with new, previously unknown *services* from the open, networked environment (realm 3), concepts and strategies will be required that are capable of assessing risks and dealing with them accordingly, always in direct consultation with the user.

3.2.2.2 Security threats to Cyber-Physical Systems

The open and uncertain environment also throws up new challenges with regard to *security*. The main threat to closed systems comes from insiders – they are relatively easy to protect against external attacks. They thus have little need for more extensive *security* measures. For example, the control of medical equipment is not rated as *safety-critical* from an *IT security* perspective. The equipment is therefore not protected against attacks, since it is used in controlled, non-networked environments (Level 1). The same is true of factory control systems.

Cyber-Physical Systems, on the other hand, are by definition used in uncertain, open contexts and are closely networked with an insecure environment. This entails a number of different risks. The Stuxnet worm [Lan11 provided a graphic illustration of the potential consequences of inadequate *security*. Another example involves Car2Car communication. Although the communication partners are known and controlled systems, it is conceivable that a hacker could try to use the communication process to their advantage by sending false information, for example by claiming to be an ambulance so that they can trick other vehicles into letting them through.

Figure 3.2 illustrates the open nature of the systems. Closed systems that are internally *secure* still exist (realm 1). However, the fact that these systems are now extensively networked means that they are exposed to potential attacks. Enhanced protection against external attacks is therefore necessary. This can be provided e.g. by isolating the system, protecting the network that it forms part of (perimeter protection), or by implementing dedicated and controlled cross overs to realms 2 and 3.

Cyber-Physical Systems are very different to conventional systems whose perimeters can easily be protected using firewalls, for example. In the typical attacker *models* for Cyber-Physical Systems, external attackers who try to penetrate the perimeter protection are by no means the only concern. Indeed, the main security challenge comes from internal threats such as supposedly known systems that are actually compromised and which proceed to behave maliciously. It is necessary to develop new security measures for Cyber-Physical Systems to deal with these threats.

3.2.2.3 Privacy and know-how protection

In addition to *security*, one of the other major challenges concerns the protection of the actors' *privacy*, especially since it is possible to use Cyber-Physical Systems to carry out extensive monitoring activities. It would be both socially unacceptable and an infringement of people's right to informational self-determination[28] if the observation, monitoring and tracking of people's actions were to become the norm. All it would take to cause widespread acceptance problems would be for the affected people to feel uneasy about this issue. Consequently, it is essential for all the relevant actors to have an adequate knowledge and understanding of the data processing operations that are being performed and the effects that they have. This applies equally to the systems' operators, the people whose data are being processed and any people who could be affected by decisions based on information processed by Cyber-Physical Systems.

In addition, it is also extremely important to protect companies' proprietary *know-how*. Cyber-Physical Systems operate as networks where specialised functions and services are provided and used by different actors. The partnership arrangements required for the development and networked operation of Cyber-Physical Systems mean that companies are forced to become more open vis-à-vis the outside world. Even their core business competencies can no longer be completely shielded from external entities. New technologies and statutory regulations are urgently needed in this area.

3.2.3 DISTRIBUTED ACTING IN OPEN PHYSICAL AND SOCIAL ENVIRONMENTS

The fact that open cooperation and automatic networking between CPS components can occur during operation and in *real time* raises new challenges with regard to the systems' technology and how they are used, as well as posing new risks involving a number of issues for which no solution currently exists. In view of the fact that CPS applications intervene extensively in everyday social interaction and action processes, it is particularly important to meet the relevant socio-technical design requirements and ensure an appropriate form of *human-machine interaction*. In addition to

[28] Census verdict of the Federal Constitutional Court 65, 1, 1983.

addressing the technological questions, it will also be necessary to establish common quality standards and frameworks that are supported by the aggreement on social, political and economic level. The following sections address the individual aspects of distributed acting in open environments.

3.2.3.1 System levels of networked CPS technology

The development stages of vehicle braking systems shown in Figure 3.4 illustrate the technological advances and increasing complexity of embedded systems and the new quality of the demands placed on systems as they evolve towards open Cyber-Physical Systems.

In the interests of accident prevention, the automotive industry has already been using traditional embedded systems for many years in order to improve *safety-critical* functions such as braking, and it is now increasingly also turning to Cyber-Physical Systems. One early milestone in this trend was the introduction of the ABS anti-lock braking system in 1978, which enables drivers to retain the ability to steer their vehicle while braking. Bosch then introduced its Electronic Stability Program (ESP) in 1995. This actively applies braking to individual wheels, allowing steering right up to the limits of what is physically possible. 2003 subsequently saw Honda launch its “Collision Mitigation Brake System”, an Active Brake Assist (ABA) system that applies braking automatically if the distance between a vehicle and another object falls below its minimum braking distance. These three milestones illustrate how the use of information processing has progressively enhanced basic physical functionality, from reactive optimisation (ABS) to active overriding (ESP) and finally autonomous control (ABA).

This trend has involved the complete or partial replacement of physical process chains (brake pedal – hydraulic hose – brake cylinder) by IT process chains (brake pedal – position *sensor* – *bus* line – controller – *bus* line – *actuator* – brake cylinder). As described above, this enables functionality to be significantly improved and extended. At the same time, however, it also makes the system more complex, making failure more likely and thus increasing the risks associated with using it. In addition to the extended functionality, this greater complexity is also manifested in the greater extent to which the systems are networked with and embedded in their physical environment. While an ABS system only affects wheel speed and brake force, an EPS system also influences steering and various acceleration forces. Finally, an ABA system goes one step further by detecting obstacles in the immediate vicinity of the vehicle. Current developments are focused on autonomous braking if the system detects a risk of hitting a pedestrian or adjusting the braking process if it detects that the driver has become distracted. Every increase in the degree of networking and embeddedness entails a huge increase in complexity, both in terms of registering different environments and situations in order to build up a picture of potential and actual chains of events and in terms of coordinating and controlling the response of the relevant systems and components to the current situation.

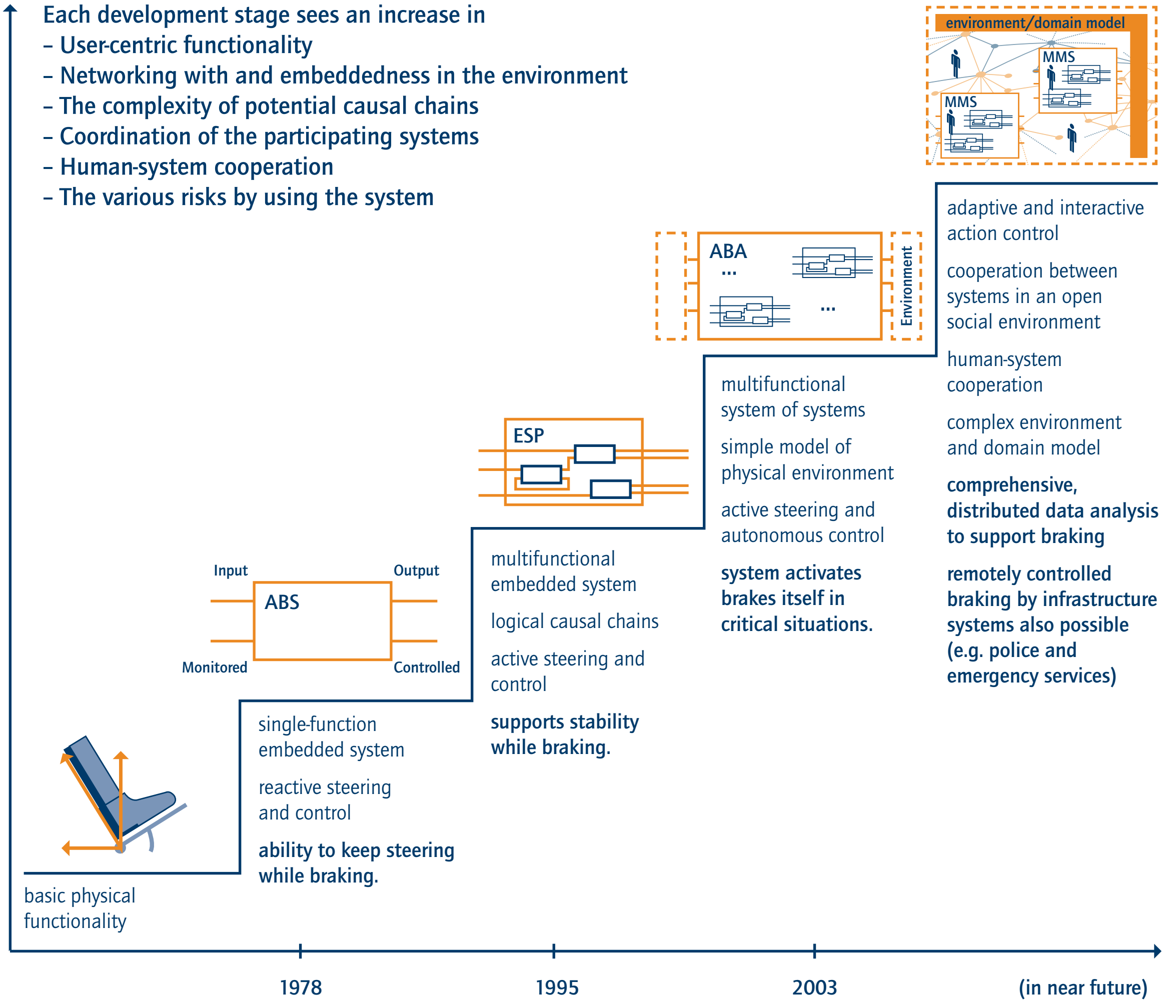
In order to meet the increased safety requirements, the latest developments are going beyond the levels of integration described above, i.e. ABS as part of a discrete braking system, the integration of EPS with the combined braking and steering system and the integration of ABA into a system incorporating the vehicle’s drive, chassis and the immediate system environment. Other parts of the environment are now also being incorporated, especially other vehicles and the *communication infrastructure*. For example, traffic data gathered from networks of vehicles can be used to respond to situations that ABA would not be able to detect. By receiving traffic flow information from the vehicles in front of them – e.g. about their speed or when they brake – and combining this with data about their current location, the following vehicles can be warned about suspected hazards, enabling them to perform an emergency stop if necessary. This also applies when the automatic brake assist is unable to detect the hazards, for example on roads where there are a lot of bends. In order to enable this kind of

Figure 3.4: Development stages of Cyber-Physical Systems as exemplified by braking systems

EVOLUTION TOWARDS CYBER-PHYSICAL SYSTEMS AS EXEMPLIFIED BY VEHICLE BRAKING FUNCTION

Each development stage sees an increase in

- User-centric functionality
- Networking with and embeddedness in the environment
- The complexity of potential causal chains
- Coordination of the participating systems
- Human-system cooperation
- The various risks by using the system



basic physical functionality

single-function embedded system

reactive steering and control

ability to keep steering while braking.

multifunctional embedded system

logical causal chains

active steering and control

supports stability while braking.

multifunctional system of systems

simple model of physical environment

active steering and autonomous control

system activates brakes itself in critical situations.

adaptive and interactive action control

cooperation between systems in an open social environment

human-system cooperation

complex environment and domain model

comprehensive, distributed data analysis to support braking

remotely controlled braking by infrastructure systems also possible (e.g. police and emergency services)

This example also illustrates the range of key non-functional features:

- Functional safety
- Dependability
- Usability, controllability (human-machine interaction, shared control)
- Valid mental model; users have an accurate idea of what the system is capable of
- Compliance – system behaves in accordance with expectations, observes rules, norms and standards, including engineering
- IT security issues associated with braking in networked systems

functionality, the functions on board the vehicle need to be complemented by the relevant infrastructure in the vehicle's environment, for example GPS and mobile communications networks capable of transmitting the necessary data.

Increased complexity also entails a greater risk of malfunctions. In order to realise the functions described above in a reliable manner, it will be necessary to ensure that the vehicles ahead report hazards accurately, that these warnings are transmitted correctly and that the affected vehicles are able to correctly perform an emergency stop.

Physical, situational and strategic awareness of the environment: the example described above clearly illustrates the growing demands in terms of systems' ability to register their environment. These demands include capturing simple physical data and fusing them to provide information about the physical environment, such as the distance between the vehicle and other objects, its position or its speed *(physical awareness).* They also encompass the ability to determine the significance of this information in the current situation (*situation awareness)*, the incorporation of extensive contextual information to help assess the situation correctly *(context awareness)* and action control, often in conjunction with other systems. In order to meet these complex requirements, it is becoming increasingly necessary for the systems' *models* of the physical environment to be accompanied by complex situation and context *models* forming part of environment and *domain models.*

As the *autonomy* of systems increases, so do users' expectations with regard to their *dependability*, posing a whole new set of challenges in terms of *human-machine interaction*. Cooperation between systems and their users requires the realisation of *shared control*. This is essential, for example, in situations where it cannot be guaranteed that the system will reliably detect every single hazard, or in complex driving situations where it may be unable to determine whether braking is the correct response. These scenarios involve a mixture of technological, social and legal considerations.

3.2.3.2 Systems with distributed risk

The scenarios in Chapter 2 provide a number of examples of the additional risks and unresolved questions regarding the development and application of the technology.

In the mobility scenario in Chapter 2.2.2, for example, Frau Müller's vehicle suddenly performs a full emergency stop in order to avert a potential collision with a child running into the road. Her vehicle's emergency stop and the automatic braking of the vehicles behind her are the outcome of networked *real-time* cooperation between *sensor* systems in the infrastructure – e.g. in road signs, cameras or smart tags/*RFID tags* in the child's clothing – and on board the vehicles. Frau Müller herself is not actively involved in the relevant communication and decision-taking processes.

Quite apart from the question of whether current legislation would permit a vehicle to perform an autonomous emergency stop on a public road without involving the driver, this example raises a number of other issues in terms of its technical feasibility, additional risks, the roles of the different people involved, the potential repercussions and problems connected with social acceptance.

From a technical point of view, it is necessary to establish exactly how much distributed context information is required in order to take a decision like the one taken in the mobility scenario. Can this information be reliably obtained using CPS technology?

Various factors need to be considered:

- is it possible that rather than the child running into the road, it is simply their smart-tagged clothing that has been thrown there? Is a second observation required, e.g. from a camera capable of interpreting what it sees?

- is it possible that the following vehicles are not equipped with CPS technology and may therefore react too late or not at all?
- or could they lack compatible technology or have different decision-taking rules, causing them to respond incorrectly or not at all?
- do the potential negative consequences of performing an emergency stop mean that it would make more sense to swerve out of the child's way? If Frau Müller was in control of the vehicle, she might have realised this and reacted accordingly.

These questions illustrate the fundamental challenges involved in correctly registering and interpreting the complex context that exists in open, networked system scenarios and using autonomous technology to respond appropriately. They also show how by focusing on a single safety goal – which in this instance involves braking autonomously to avoid hitting the child – technology-based scenarios generally tend to overlook human beings, with all their different types of doing, goals, interests and responsibilities, as well as their ability to react intelligently and prudently.

Addressing these problems will require enhanced strategies and comprehensive processes for studying, analysing and assessing risks in every area of the requirements engineering, system design, systems engineering and deployment of Cyber-Physical Systems.

3.2.3.3 Cyber-Physical Systems as agents of social actors (human beings)

In the world of open networks (realm 3 in Figure 3.2), Cyber-Physical Systems and their *services* are increasingly used in a wide variety of non-predetermined social processes and contexts. CPS *services* are networked and can take decisions or perform actions autonomously in response to different contexts. As such, they can be said to act as independent agents of social actors – i.e. individuals, groups or organisations – and represent them in their goals, interests and duties. This is illustrated by the scenarios in the fields of mobility, remote healthcare and *Ambient Assisted Living (AAL)*. In the mobility scenario in Chapter 2.2, for example, Frau Müller's vehicle is directed to leave the motorway on which it has been driving autonomously at a different junction to the one that was originally planned in order to optimise the traffic flow on the roads. Frau Müller has to continue her journey on a road that does not support *autonomous driving*, although she continues to receive optimal route guidance on this road. In this instance, the system has to weigh up Frau Müller's individual interest in reaching her destination as quickly as possible without having to drive the vehicle herself against the wider social interest of optimising traffic flows on the roads. In the healthcare scenario described in Chapter 2.3, Frau Huber's system takes a number of decisions by itself. The system draws on stored instructions for what to do in the event of an emergency and sends her family text messages informing them of the situation, cancels her newspaper and contracts a security firm to place her home under surveillance whilst it is empty.

This raises questions with regard to

- how best to register and represent human goals and intentions and their social context in the distributed information and action models of Cyber-Physical Systems and
- the application goals, target systems, potential conflicts and rules, procedures and frameworks that should apply either universally or to individual groups, organisations or societies.

In order for Cyber-Physical Systems to be usable and dependable in use, they require *domain models* containing formal application knowledge. Binding versions of these *models* must be negotiated and implemented using standard specifications, architectures and interfaces, application frameworks and *validation* and *verification guidelines, as well as comprehensive testing* procedures.

In addition to fundamental questions regarding the controllability and acceptance of these systems and the associated social issues, one of the key challenges in this area is the design of *human-machine interactions*. If human beings are to be dependent on networked technology and the *services* it provides, then it will be necessary to ensure that these systems can be operated intuitively, controlled and understood by individual users or actors (*shared control*) and behave *dependably*.

In the context of the open socio-technical applications of Cyber-Physical Systems, the actors' interests, goals, intentions and contexts are not constant and can change suddenly. Moreover, it is – possibly quite rightly – far from easy for them to be correctly identified by the *context awareness* capabilities of Cyber-Physical Systems. Finally, people's individual interests and rights must be respected including, for example, the provision of adequate *privacy* protection. Thus, supporting individuals' independent (strategic) acting is at the same time both the number one priority for Cyber-Physical Systems and the biggest challenge facing their development (see Chapter 4).

3.2.4 DEPENDABLE ACTING CYBER-PHYSICAL SYSTEMS – NEW CAPABILITIES AND CHALLENGES

The open networking of Cyber-Physical Systems and their interconnected deployment in a variety of different usage contexts means that errors and erroneous decisions can be made at any time by all of the relevant actors. One US study of "Ultra-Large-Scale Systems" [FGG+06] describes this inherent property of such systems as "normal failure". The study calls for a systematic approach to tackle this type of failure and its potential causes, in order to reduce the associated risks and negative repercussions.

In this context, a key feature of Cyber-Physical Systems is their ability to observe phenomena in the networked environment, perform calculations that enable them to predict events and actively take measures to counteract any negative consequences. For example, they are capable of

- globally networked weather data recording, predicting bottlenecks in the supply of power from solar PV arrays and dynamically adjusting the distribution of energy in *smart grids* in order to prevent shortages from occurring in individual regions, or
- networked recording of traffic volumes in towns and cities via a distributed *smart infrastructure*, predicting traffic congestion and journey time delays and dynamically controlling traffic flows and reducing congestion, for example by adjusting traffic light settings or targeted redirection of vehicles via specific routes.

The key capabilities required by Cyber-Physical Systems in order to do this include:

- **the ability to perform enhanced and wide-ranging risk analyses and assessments** that incorporate potential networking and action options,
- **the ability to plan ahead and act strategically**, including the ability to negotiate, coordinate and cooperate as required in situations where the goals and solutions are not clearly specified,
- **the ability to continuously register and assess different contexts (**context awareness) and
- **continuous learning and adaptation** of *context knowledge* (context *models*), as well as identifying and proposing the relevant options.

The key challenges involve

- **controlling and managing** the increasingly autonomous acting of this networked technology,
- **designing** *dependable* systems that act and interact in a way that can be predicted by human beings,

- **developing** the necessary, socially desirable rules, guidelines and regulations to govern systems' behaviour (*compliance* regulations, policies), obtaining the societal approval for them and subsequently putting them into force,
- **investigating the design** of *human-machine interactions* and the coordinated control and management of CPS components.

3.3 HUMAN-MACHINE INTERACTION AND SHARED CONTROL

Alongside *safety, security* and integrated control, the key enabler of successful networked Cyber-Physical Systems is the targeted adjustment of their behaviour to match the goals of their current application whilst also taking into account the functional and non-functional requirements of their users and *stakeholders*. As described in section 3.2, in open network environments these requirements will tend to be disparate and contradictory. As a rule, it will only be possible to satisfy and manage these requirements adequately through social interaction and *human-machine cooperation.* In these contexts, the usability of Cyber-Physical Systems depends on the extent to which all the actors – including the cooperating systems – are able to achieve the necessary consensus with regard to the actors' goals and how to interpret the context, and the extent to which this can then be mapped onto *domain* and *architecture models* for the relevant area of application.

In the ISO 9241-110 standard [ISO09], the International Organization for Standardization describes *usability* as:

"The extent to which a product can be used to achieve specified goals effectively, efficiently and satisfactorily by certain users in a specific use context."

ISO also outlines the following key *human-machine interaction* design criteria:[29]

- **suitability** for the task (the ability to complete the task fully and effectively, an appropriate match between the functionality provided and what is required, the effectiveness and efficiency of the support provided for the task),
- **controllability** (the ability to control the process and intervene in it at any point in time),
- **self-descriptiveness** (*transparency* of the interaction process, ease of understanding and feedback),
- **conformity** with user expectations (the conceptual alignment, compatibility, calculability and consideration of experiential knowledge),
- **suitability for individualisation** (tailoring the interaction to the user's abilities and wishes),
- **error tolerance** (prevention of serious errors and the ability to correct minor errors) and
- **suitability for learning** (learning should be rapid and easy to access, users should be encouraged to try out new functions).

These criteria go a long way towards determining the quality of the *human-machine interaction* and thus allow Cyber-Physical Systems to be controlled safely and appropriately. However, particularly with regard to the novel capabilities of Cyber-Physical Systems, they also highlight a number of unresolved questions in connection with *human-machine cooperation* and hint at some of the possible limitations of fully or semi-autonomous Cyber-Physical Systems. For example,

- does the suitability of a CPS interaction and a system's overall behaviour for performing a particular task depend on the extent to which it is able to capture the goals, intentions, action and social interaction

[29] Although this standard was originally formulated in order to define the ergonomic requirements for office work with visual display terminals, in practice it has come to be used as a guideline for interactive systems. See also the outcomes of the Federal Ministry of Education and Research partnership project "Erlebnis Automat" *(The Self-Service Machine Experience*) in [BBB+11].

processes of the actors in *domain model*s and distributed behaviour and interaction *models* that describe the continuous registering and assessment of different contexts?

- in addition to appropriate domain modelling, do the controllability and self-descriptiveness of Cyber-Physical Systems also depend on whether the *human-machine interaction* has been designed to enable cooperation and coordinated control in the *domain* and behaviour *models* of the involved CPS components in a manner that is appropriate for the relevant users and tasks as well as being sufficiently adaptable?

3.3.1 COORDINATED SITUATION AWARENESS AND CONTEXT INTEGRATION TO ENABLE INTUITIVE USE

The key enabler of all the quality criteria described above, and in particular self-descriptiveness, conformity with user expectations and the intuitive and safe use of Cyber-Physical Systems, is the development and integration of adequate application and interaction *models* and user interfaces. This is essential in order to ensure that the relevant CPS components and their users are aligned with regard to the situation, option and action models; see also the mobility scenario in Chapter 2.2.2. For this to be possible, it will be necessary to find answers to the following questions:

- Who – system, user or actor – requires what information about the situation, actors, status, *services* and capabilities – and in which data transmission format (*multimodal* interfaces and dialogues) –, so that appropriate and correct decisions can be taken?
- How should the behaviour of Cyber-Physical Systems be adapted to situations, users and conditions in order to ensure that users are provided with as much *transparency* and intuitive control as possible?
- Which aspects of the context and environment, information about the situation and user, and distributed CPS component viewpoints need to be linked to each other and integrated, how should this be done and who should be responsible for doing it?
- How explicitly, interactively and user-visibly are different contexts registered, interpreted and integrated by the system?
- How regulated, interactive or autonomous should adaptive behaviour be designed to be – e.g. by specifying operating modes – and what form should it take – e.g. the appropriate type of *multimodal* interaction – in order to ensure that it does not irritate the user?

If an intuitive, *transparent* and controllable *human-machine interaction* is to be guaranteed, then Cyber-Physical Systems need, as far as possible, to behave in a way that can be understood and predicted by human beings.

Particularly in the passive elements of *human-machine interactions*, a variety of questions arise with regard to the interpretation of contexts with the required accuracy and in a manner that is both appropriate to the current situation and desirable or acceptable for the relevant actors. Likewise, a number of questions also exist concerning the required level of autonomous or interactive control of the CPS components' behaviour. Examples include the following situations:

- camera systems located in public places that monitor e.g. the traffic situation in front of a school (see the scenario in Chapter 2.2.2), interpret the current situation and cooperate or share information with vehicles in the vicinity,
- *AAL sensors* that monitor the behaviour and health of elderly people, use these observations to draw conclusions about their intended actions and automatically open doors for them, matching the speed at which the door opens to the speed of the person's wheelchair, or automatically call for assistance if necessary,
- conference room blinds in office buildings that are not only opened and closed based on the outside weather

conditions detected by their *sensors*, but also based on whether or not the room is observed to be occupied and the activities of the people using it, e.g. presentations or conversations.

The new challenges and requirements in delivering *human-machine interaction* and coordination geared towards different users and situations become particularly apparent if we consider that Cyber-Physical Systems operate *adaptively* in changing environments, across different *domains* and on a global basis. What the user understands by an intuitive interface or an intuitive interaction is heavily conditioned by their personal experience and cultural expectations. The requirements therefore need to be adapted or completely redefined accordingly.

In addition to the questions already highlighted above, interdisciplinary research and experimental testing of *human-machine interactions* with Cyber-Physical Systems should therefore pursue the following key goals:

- **the establishment of general principles** for the intuitive and simple design of *human-machine interfaces* and *cooperation*,
- **the development of mechanisms** that enable systems to learn and adapt their behaviour to the user's needs, the current environment and the requirements of different *domains* and applications,
- **the establishment and observance of the principle of "easy-to-use multifunctionality",** ensuring that both the interaction with the user and the Cyber-Physical System's fully or semi-autonomous behaviour are kept as simple as possible and are tailored to the user's culture and experience and to the relevant social norms. Ultimately, functionality needs to be geared towards the actors' requirements and their wishes or capabilities in terms of controlling the system,
- **ensuring that the user is provided with as much flexibility** as possible to intervene in case of doubt, retaining the right to assess the situation, take decisions and control the system themselves.

3.3.2 THE CHALLENGE OF SHARED CONTROL

The aspects described above are particularly critical in applications involving *shared control*[30]. These are systems where Cyber-Physical Systems behave fully or semi-autonomously, coordinating, controlling and managing other CPS components in conjunction with human beings. Examples include:

- *shared control* and fully or semi-autonomous management of vehicles and traffic systems, as illustrated by the mobility scenarios in Chapter 2.2, or
- scenarios where humans and machines coordinate the operation and control of facilities in buildings, such as locking systems or doors, or of mobility devices and other aids, e.g. wheelchairs and walking aids in *AAL* scenarios.

In addition to researching the issues connected with ensuring that humans and CPS components register and interpret different situations and contexts in a consistent manner (*situation awareness* and *context awareness*), the key challenges relate to the interactive, coordinated evaluation and goal- and user-oriented integration of contexts, the control of systems' behaviour in everyday application situations and the use of CPS by people who have not received any special training – as opposed to pilots, for example, who have undergone specialist instruction and are trained in how to respond to critical situations. The following topics should be researched in this area:

- the mutual awareness and interpretation of systems and human beings, their condition, capabilities, operating and action modes, etc. (*"X"-Awareness*),

[30] The term "shared control" is typically used in the aviation industry, e.g. to describe the *sharing of control* between the pilots and the aircraft controls [Lev95, EBJ03].

- *self-awareness* and *self-assessment* in different contexts of use,
- *human-machine interaction, cooperation* and coordination, together with integrated action control,
- Potential *mode confusion*, or a complete or partial mismatch between the user's assessment of the system's situation, status, actions and options on the one hand, and the application's actual status and options on the other, which can lead to potentially dangerous operating errors as well as frustration and a lack of acceptance.

There a number of specific challenges associated with the assistance and comfort functions of fully or semi-autonomous CPS control in open social environments:

- **the development of methods to enable accurate interpretation** of the relevant actors' intentions, behaviour and capabilities in the case of passive *human-machine interactions,* for example when monitoring a situation *(user modelling*),
- **tackling or preventing the vigilance issues** associated with assistance and comfort functions, whereby users no longer learn how to perform potentially necessary actions and lose control in critical situations because they have become too reliant on the system. This is illustrated by the example of autonomous driving in the mobility scenarios in Chapter 2.2 (see also Chapter 4.1.1),
- **coordinating the detection and assessment** of situations with the user, including situation-dependent prioritisation and integration of CPS functions and the appropriate guidance of the user's attention. Once again, the goal here is to prevent the user from becoming irritated or being overtaxed so that they do not make mistakes. Weyer [Wey06b] and Schulz [Sch07b] use the following examples to describe the irritation, *mode confusion* and growing loss of competency experienced by drivers of hi-tech networked vehicles, even when performing very simple tasks: "Even a straightforward task like operating a windscreen wiper..." can cause *mode confusion*: "If the windscreen wiper is not operating, this can either mean that it is switched off or that it is switched on but has not detected enough moisture to activate itself automatically. Moreover, the rain sensor has [...] a genuine 'design flaw' [...]: if the vehicle's ignition is switched off, the windscreen wiper unit is also switched off without storing its current setting, leaving it turned off even though the lever is in the 'on' position. This is in marked contrast to the established convention whereby when the ignition is switched back on the windscreen wiper's setting matches the position of the lever. In vehicles fitted with a rain sensor, on the other hand, the sensor needs to be switched off and on again. In other words, it is possible for the windscreen wiper to be switched off, even if it is in the 'on' position. This is a source of irritation that is not easy to eliminate." (See [Wey06b, p. 5].)

  The existence of a large number of CPS assistance functions that are not integrated and prioritised in accordance with the requirements of complex driving situations creates a picture of the situation containing contradictory information and impressions that drivers are no longer able to properly assess or react to. Under these circumstances, it is hardly surprising that they end up losing control of the situation. For example, there is a risk of drivers becoming overwhelmed "[...] by an excessive number of assistance systems displaying uncoordinated messages and warnings that can end up causing the driver stress [...]"; see [Wey06b, p. 6; SG05].

Figure 3.5 illustrates the following aspects of the complexity of *human-machine interfaces* and *shared control*:

- coordinated display and integration of contexts and *human-machine interactions* using *multimodal* and learning-enabled interfaces. In addition to *technical* and *semantic interoperability* of *services* and functions, this also requires user-visible integration of contexts and

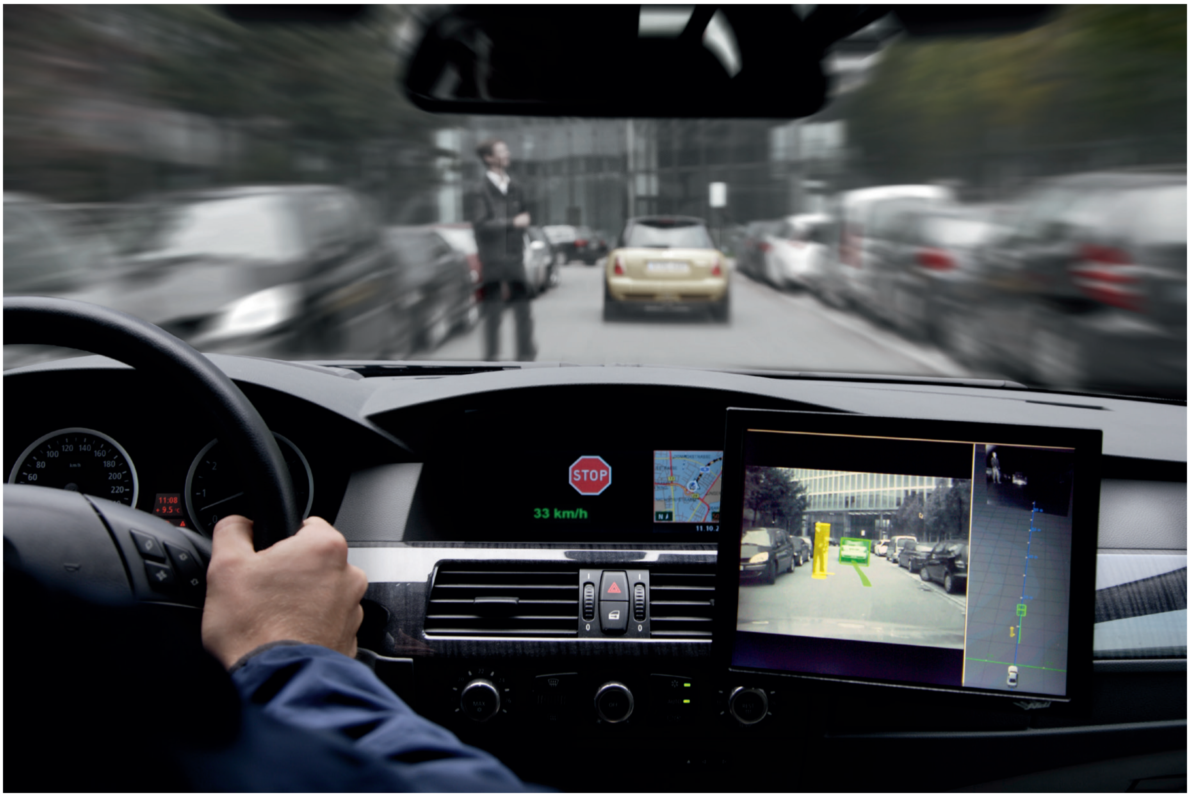
processes (see also section 3.4 on the integration of the complexity dimensions of Cyber-Physical Systems),
- ensuring that the networked technology behaves in a manner that is understandable and predictable for users in every situation.

User-centred, experimental and participatory engineering: meeting all of these challenges will require a *user-centred*, experimental and *participatory* approach to the conception, design and ongoing development of Cyber-Physical Systems and the *services* associated with them (see also *user-centred engineering* in Chapter 5.3).

In other words, the *human-machine interaction* should be designed with the abovementioned challenges in mind. This also applies to the step-by-step development, standardisation and regulation of internationally valid *domain-specific* and cross-*domain* models for the behaviour of CPS. Some of the key (social) issues in this regard are as follows:

- **Limitations**: what are the limitations of autonomous Cyber-Physical Systems in the context of controllable *human-machine interactions*?
- **Standards**: what standards, application architectures

Figure 3.5: Example of automation on board vehicles and the rising complexity of human-machine interactions



(Source: BMW AG)

(including *smart infrastructure*), environmental conditions and frameworks are required to enable fully or semi-autonomous networked acting of CPS services and the associated *human-machine interactions* in different areas of application?

It will be necessary to find answers to these questions in order to enable the safe and intuitive use of Cyber-Physical Systems (see also Chapter 4.1 on the social challenges).

3.4 ESSENTIAL ACCEPTANCE FACTORS: USEFULNESS, TRANSPARENCY, SAFETY, SECURITY AND BUILDUP OF CONFIDENCE

The following sections outline the factors that are key to the acceptance of Cyber-Physical Systems by their users and the other actors involved in the relevant application. The factors cited are derived from empirical studies and expert surveys with regard to trends and developments in the fields of *smart embedded systems*, smart automation, mobility applications and online *services*.[31] They are indispensable for the successful design, development and application of Cyber-Physical Systems in the areas of application in question.

a) *Usability* and usefulness (*services* that are integrated into their context of use, intuitive *human-machine interactions*, flexibility regarding when they are used, efficient performance of the service, permanent service accessibility and *availability*).

b) The ability for users to configure the systems in accordance with their own needs.

c) Clarity regarding *shared control* requirements.

d) User flexibility and the ability for them to act and take their own decisions independently.

e) *Safe, secure* systems that do not pose a risk to human health.

f) Availability of help if the system makes an error or fails, including help provided by human beings (e.g. service personnel).

g) Guaranteed anonymity, i.e. protection of users' personal data and *privacy*.

h) Ensuring an enjoyable user experience ("you wouldn't believe all the things it can do!").

i) In the AAL context, maintaining contact with other people.

The requirements that arise in connection with the open networking and utilisation of CPS *services* in social contexts, processes and networks are so complex that it is impossible for them to be met without the benefit of human experience and control. This is also connected to the fact that the *Quality in Use* and *Quality of Service* requirements can vary considerably in this open social context. It is therefore important that they should be accurately specified.

Certain social values and acceptance factors are also becoming increasingly important, for example

– the environmental sustainability of both the product and its behaviour,
– environmental protection issues in general and
– fair treatment of everyone involved in economic and social processes.

[31] Recent studies of trends and developments in the field of self-service machines [BBB+11], the joint Federal Ministry of Education and Research /Association for Electrical, Electronic & Information Technologies (VDE) Innovation Partnership *AAL* [Eic10, MM10], assistance systems [BK09], Vom Internet zum Outernet (*From the Internet to the Outernet*) [JS10], studies of networked services [BMW08, BMW09a, BMW10a, HW11], the Foresight Process of the Federal Ministry of Education and Research [CGW09] and the BITKOM studies on "Smart Cities" [BIT11a] and automobiles [BIT11b].

Acceptance is also determined by the attitudes and characteristics of the user, for example their age, gender or values, as well as the cultural framework or context, for example whether an application is used privately or in the workplace. These considerations should also be investigated and taken into account when designing CPS *services*.

Key success and quality enablers: the findings of the latest investigations and studies provide confirmation of the challenges facing CPS that are described above. These urgently need to be identified, specified and addressed through research and sustainable development. Cyber-Physical Systems must be useful, behave in a manner that can be understood, be capable of being tailored to individual needs and guarantee the level of *safety, security, dependability* and *privacy* protection required by the relevant social structures and regulations (*compliance*).

3.4.1 INTEGRATED SERVICES WITH CONTROLLABLE COMPLEXITY

One key feature of Cyber-Physical Systems is the fact that they operate as open networks in global physical, spatial, social political and economic structures. Whilst this holds huge potential in terms of how they can be used, it also raises the challenge of accurately selecting and interpreting contexts, goals and information. Moreover, it is essential to ensure that the right decisions are taken, irrespective of whether these decisions are taken autonomously by the system, jointly by the system and the relevant actors, or solely by the user.

Controlled CPS self-organisation: the ability to meet the requirements described above is thus at least partly dependent on the extent to which critical effects can be limited when networked technological systems operate fully or semi-autonomously in an open environment.

In the context of open, networked systems and scenarios, it is particularly important to base the structure of the relevant environments and application *domains* on local, regional and global requirements, architectures and topologies. In order to do this, the following contexts and system levels need to be taken into account and the behaviour of the relevant CPS components needs to be coordinated and integrated:

a) **the CPS application's local situation and environment:** it is primarily the local context, immediate goals and only a small number of users and actors that are relevant at this level. Examples of local use context scenarios include Frau Müller's car journey to her children's school (see Chapter 2.2.2), the scenario where she joins and subsequently leaves the motorway (autonomous convoy driving, see Chapter 2.2.3), or the mobility support and healthcare provided to the elderly and infirm in their own homes by networked CPS components and *services*, for example the control of buildings and gates, wheelchairs, media, or communication systems in *smart homes* [Eic10, MM10],

b) **spatially distributed, networked groups that share common themes, goals or problems:** these include applications in the areas of *E-Health* and *AAL* involving patients, physicians, physiotherapists and care and emergency facilities. However, they also encompass the services provided by associated healthcare and cultural entities and even *social communities* and other online interest groups. A typical application scenario would be the integrated care provided in an emergency, where it is essential to guarantee individual care, *dependability* and trustworthiness. This places high demands on the CPS *services* and on the people, organisations, components and infrastructure involved,

c) **the integrated deployment of the application systems in a) and b), taking social goals and contexts into account:** this involves integrated scenarios, such as emergency care at the scene of an accident (see scenario 2.3.3), traffic management in order to minimise the time taken to transport the patient to a hospital (e.g. by letting the ambulance through on the *premium lane* as in scenario 2.2.3), preparations for treating the patient as soon as they arrive at the hospital (scenario 2.3.3), or integrated care and mobility scenarios from the application and technology domains of *AAL, E-Health, smart homes, smart mobility,* etc. In addition to the interactive and fully or semi-autonomous coordination, prioritisation and behavioural integration of the relevant goals and contexts in accordance with agreed rules, it is also necessary to take global requirements into account, for example the safety and protection of all of the actors, environmental protection or social considerations. The latter includes integrated and fair healthcare provision and energy supply, as well as *privacy protection*; see also Chapter 4,

d) **the integration of the application scenarios** and the associated requirements in a), b) and c) into

- coherent *domain* and use *models*,
- *interoperable* architectures and platforms for CPS applications, functions and components at all the different abstraction and system levels,
- open, *interoperable* and modular architectures and platforms for infrastructure and communication.

A description of the necessary CPS functions, *services*, system architectures and infrastructure is provided in Chapter 5.3 and Appendix B.

3.4.2 DEPENDABILITY AND TRANSPARENCY – PREREQUISITE FOR CREATIVE POWER AND CONFIDENCE

All these different dimensions and integration requirements provide a clear illustration of the complexity of CPS applications. In particular, they demonstrate the importance of building *dependable* and trustworthy structures. In addition to gearing and adapting systems to widespread forms of behaviour and social norms, it is also necessary to create transparent structures for users and ensure safe and reliable acting at every level of the system.

This requires components, communication, subsystems, systems and *services* to operate *reliably* without being controlled by third parties. Moreover, the systems need to be able to reliably detect and alert people to risks, threats or potential failures and take the appropriate countermeasures if necessary.

The systematic development of *dependable* and trustworthy Cyber-Physical Systems will require strategies to ensure that:

- CPS *services* do not malfunction, maintain a high level of availability and, in the event of a partial failure, are capable of providing a working alternative that meets the required quality standard,
- Cyber-Physical Systems, their *services* and interactions – including networking and cooperation with other services – operate as expected by their users and *stakeholders*,
- Cyber-Physical Systems support their users when using new, enhanced *services* or in new situations that they have not previously encountered, for example by adapting automatically,
- Cyber-Physical Systems detect errors or malfunctions – within or outwith their own area of responsibility – and intervene in an active and coordinated manner,
- the consequences of threats, accidents or damage are kept to a minimum.

IT *security strategies* will also be required, for example

- emergency operating modes that Cyber-Physical Systems can switch to in the event of an attack. *Security* breaches cannot be allowed to have an uncontrolled impact on *safety*,

- mechanisms for guaranteeing *security*: Cyber-Physical Systems must be able to guarantee that, for example, encrypted data will remain *confidential* and that it will not be possible to hack encryption algorithms, at least for the foreseeable future. One of the problems in this regard is the fact that the frequently long life cycles of embedded systems mean that *security* measures can become outdated,
- the detection and prevention of direct attacks on the distributed components, such as unauthorised accessing of data or cryptographic keys, installation of malicious firmware or even the destruction of devices.

The *dependability* provided by the guarantees described above is one of the key requirements for Cyber-Physical Systems. In order for users and systems to trust each other, quality assurance methods and *validation* and *verification* techniques need to be accompanied by mechanisms such as certification or quality seals, as well as comprehensive organisational measures during operation.

Nonetheless, given the open nature of Cyber-Physical Systems and the fact that they operate in socio-technical contexts, it is not possible to completely prevent inconsistencies and conflicting goals. It will often not be possible for these to be fully resolved at the system level.

Compliance: In view of the above, Cyber-Physical Systems – and in particular the way that their *human-machine interactions* are *designed* – must be aligned with these different goals, interests, rules and cultural norms and be prepared for potential conflicts and situations where it is not obvious what the correct decision is. This has implications for the design and realisation of the systems' semi-autonomous acting and for the restrictions placed upon it. It is essential that the systems should behave in a way that is viewed as trustworthy and dependable by their users and the society that they are being used in.

Quality: All of the above makes it necessary to ensure that non-functional requirements are fully included in the specifications, described in detail and integrated into the systems' design. Moreover, integrated quality assurance is essential in every area of the development and deployment of Cyber-Physical Systems. The interactive collaboration of users and actors will have a key role to play in this regard.

3.5 SUMMARY OF CPS CAPABILITIES AND THE ESSENTIAL CHALLENGES ASSOCIATED WITH THEM

Figure 3.6 summarises the description of CPS provided in Chapter 2.6. The right-hand column outlines the new capabilities and key requirements that Cyber-Physical Systems will need to address in order to enable usable and innovative applications.

The realisation of these capabilities – including the formulation and establishment of the necessary framework and the creation of a social consensus – is at the heart of the research issues and general action areas that are discussed in this agenda.

In addition to research into the new capabilities and core technologies (see also Chapter 5), the implementation and control of the CPS applications that have been described will require work in the following areas:

- **the development of smart infrastructure, communication platforms and middleware** for realising integrated and interoperable CPS *services*, accompanied by guaranteed basic *Quality of Service;* see also 5.3.3 and Appendix B,

- **the development of domain models, architecture frameworks and application platforms at every level of the system** in order to enable accurate awareness and interpretation of situations and contexts, process integration and *dependable* system behaviour or control. This includes, for example,
  - *models* of the physical environment, its architecture and actors, and their tasks, roles and interactions,
  - functional and non-functional *models* for specifying the requirements of both direct and indirect actors (*stakeholders*, systems and components),
  - the design requirements for the involved systems and components,
  - application and *architecture frameworks* with process *models*, functional and *service* architectures, interaction *models* and realisation architectures. The latter include *logical architectures*, e.g. for realising specific *safety, security* or performance requirements, as well as hardware and software architectures, platforms and *communication architectures* and organisational frameworks and standards,
  - quality *models* and domain rule or business rule *models*, as well as goal *models* or company-specific *business models* for testing and *validating* CPS *services* and applications,
- **the development of norms and standards** to ensure qualified development and certification of the systems.

In addition to the different development trends and cultures of the relevant areas of application, systems, actors and disciplines, the key research themes in connection with CPS technologies and concepts are as follows:

- **the increasing loss of control that occurs in open social environments** where networked and fully or semi-autonomous systems and actors interact with each other. This in turn requires investigation of the issues, methods and concepts involved in ensuring
  - that the systems exhibit the required *dependability* in terms of enhanced *safety, security* and *privacy protection*, as well as other non-functional requirements such as performance and *energy efficiency.*
  - the required *know-how* protection in open *value networks* (CPS *ecosystems*),
- the uncertain and distributed risks associated with Cyber-Physical Systems. It is almost impossible for these to be assessed quantitatively, whilst only subjective qualitative assessments can usually be produced,
- **system and user decisions based on uncertain knowledge**, as well as the strategies and action concepts required to take such decisions,
- reasonable and fair acting of Cyber-Physical Systems when acting on behalf of social and economic actors – whether they be individuals or groups – and the resolution of goal conflicts where necessary,
- how to ensure interdisciplinary, socially inclusive specification of
  - framework conditions[32] and
  - *domain* and quality *models*, including the relevant rules and policies (*compliance* regulations), in order to regulate fully or semi-autonomous acting and decision-taking by the systems,
- **the factors connected with dependable human-machine interaction**, e.g.
  - simple and intuitive *human-machine interaction* for multifunctional *services* and alternative uses,
  - semantic and user-visible *service* integration in accordance with the situation and local, regional and global process and action contexts,
  - passive *human-machine interaction*, i.e. intentional or unintentional observation and monitoring of individuals and groups. The key here is to ensure that the Cyber-Physical System interprets this information correctly or in the desired manner,
  - vigilance issues[33], i.e. user inattentiveness and the associated loss of control.

[32] For example the infrastructure required by Cyber-Physical Systems, their *safety, security* and quality, standardisation, norms and regulatory frameworks, etc.

[33] For example driver inattentiveness due to over-dependence on the vehicle's assistance and comfort functions.

Figure 3.6: CPS characterisation and required new capabilities

(1) CYBER-PHYSICAL, SENSORS/ ACTUATORS, NETWORKED (LOCALLY-GLOBALLY), VIRTUAL, REAL-TIME CONTROL	(2) SYSTEMS OF SYSTEMS (SOS), CONTROLLED NETWORK WITH DYNAMIC BOUNDARIES	(3) CONTEXT-ADAPTIVE AND (SEMI-) AUTONOMOUS SYSTEMS
- Parallel capture (via sensors), fusion and processing of physical data from the environment, locally, globally and in real time (physical awareness) - Interpretation of situation in terms of achieving the system's goals and tasks - Detection, interpretation, deduction and prediction of disruption, obstacles and risks - Interaction, integration, regulation and control of system components and functions - Globally distributed, networked real-time control and regulation	- Interpretation of environment and situation data over several stages, depending on respective application situation - Targeted selection, integration, coordination and use of services – depending on situation, local and global goals and behaviour - Service composition and integration, decentralised control: detection of missing services, data and functions, active searching and dynamic integration - Self-organisation - Evaluation of the benefits and quality (QoS, total quality) that new components and services integrated into the application should provide – and of potential risks - Dependability in terms of guaranteed QoS (compliance) - Control of access to the system's data and services	- Comprehensive, end-to-end context awareness - Continuous capture, monitoring, selection, processing, evaluation, use for decision-taking and communication of environment, situation and application data (often in real time) - Targeted adaptation of interaction, coordination and control with/by other systems and services - Recognition, analysis and interpretation of the plans and intentions of objects, systems and the relevant users - Generation of models of the application area and domain, the actors and their roles, goals and requirements, as well as the available services and tasks - Specification of goals and actions, taking into account and weighing up the pros and cons of alternatives in terms of costs and risks - Self-awareness, i.e. knowledge of the system's current situation, status and options - Learning, e.g. of changing work and logistics processes, habits, interactions, etc., and the ability to adapt behaviour accordingly

→→ **Increasing openness, complexity, autonomy, smartness and**

(4) COOPEATIVE SYSTEMS WITH DISTRIBUTED, CHANGING CONTROL	(5) EXTENSIVE HUMAN-SYSTEM COOPERATION	KEY CAPABILITIES AND NON-FUNCTIONAL REQUIREMENTS QUALITY IN USE QUALITY OF SERVICE (QOS)
- Distributed, cooperative and interactive situation awareness and assessment - Distributed, cooperative and interactive determination of required measures based on assessment of the situation, the goals of individual actors and the goals of the communities that these actors belong to (local vs. global goals) - Coordinated processing of huge volumes of data - Coordinated appraisal and negotiation of the decision that is ultimately taken, i.e. individual and joint control and decision-taking autonomy - Decision-taking based on uncertain knowledge - Cooperative learning and adaptation to situations and requirements - Assessment of the quality of both the system's own services and capabilities and those of external entities - Self-organisation capabilities within a network	- Intuitive, multimodal, active and passive MMI support (simplified control) - Support for more extensive (in space and time) and comprehensive awareness, support for enhancing the capabilities of individuals and groups of people - Recognition and interpretation of human behaviour, including feelings, needs and intentions - Detection and evaluation of the condition and environment of humans and system (expansion of awareness and evaluation capabilities) - Integrated and interactive decisions and actions involving systems and individuals or groups of people - Ability to learn	- "X"-awareness (correct perception and interpretation) of - Situation and context - Self-awareness, third-party-awareness (status, objectives, ability to act) - Learning and adaptation (behaviour) - Self-organisation - Cooperation, bargaining/negotiation and decision-taking (within predefined parameters – compliance) - Decision-making based on uncertain knowledge - Provision and where necessary enforcement of QoS guarantees - Comprehensive safety and security strategy (dependability, safety and security) - Transparent MMI, shared control – integrated situation awareness and predictable acting - Risk management - Proactive, strategic and dependable acting - Privacy protection
evolution of systems (with disruptive effects in the relevant areas of application) →→		

Points 1 to 4 also entail the need for systems to be capable of assessing complex situations with a similar degree of prudence to a human being and prioritising, integrating and applying the required features[34].

3.6 REVOLUTIONARY AND EVOLUTIONARY SYSTEMS AND THE ASSOCIATED ENGINEERING CHALLENGES

In addition to the obvious challenge of mastering the necessary technology, *engineering* also has to address the fact that users and the environment exert an unpredictable influence on the way the systems develop. The upshot is that their development can be both evolutionary and sometimes also revolutionary. In both instances, the interconnectedness and convergence of the technologies and applications requires an integrated approach and the development of new or at least extended *engineering* concepts. Smart technologies harbour huge potential for revolutionary and disruptive CPS applications. However, it will not be possible for these to be adequately managed using traditional *engineering* concepts and methods.

The greatest *engineering* challenges in terms of the development of Cyber-Physical Systems come from opposite ends of the spectrum: on the one hand, the need to develop *dependable, safe* and *secure* systems that can add value sustainably, and on the other the need for systems, open innovation networks and procedures to be geared towards new applications and *services*. This necessitates an iterative approach, accompanied by exploratory work in value partnerships and economic *ecosystems*. This involves bringing the actors together in distributed, dynamic partnerships to address roles and tasks from every area of systems engineering and control. It affects every stage and level of systems engineering:

- development, production and utilisation,
- operation and maintenance,
- service provision, consultancy, adaptation and ongoing development,
- medium- to long-term strategic development and evolution tasks.

The above applies to companies, actors and individual parts of networks, i.e. to everyone involved in the overall systems *engineering* process. Their common challenge within their particular *ecosystems* is to develop long-term concepts and partnerships for building strategies and *application platforms*.

All these stages and tasks of CPS value creation are characterised by the fact that sustainable and disruptive or revolutionary innovations can only come about through open and wide-ranging interdisciplinary cooperation. Although they are the product of interactions and cooperation between users, actors and *stakeholders* in the different application *domains*, they also need to be coordinated across the different *engineering* disciplines involved in Cyber-Physical Systems.

3.6.1 EVOLUTION AND ENGINEERING

Different types of Cyber-Physical System evolution play a role in the open development of innovative CPS services and applications:

Autonomous evolution and adaptation at run-time: Adaptation and evolution at run-time play an important role in conventional embedded systems, particularly large-scale global systems such as the telecommunications network or civil defence systems. In order to ensure the *dependability* of these systems, adaptive mechanisms such as *self-healing* or dynamic reconfiguration in the event of a failure – for example dynamic re-routing if a subnetwork fails – are integrated into them right from the outset. Evolutionary mechanisms such as the installation of new functionality at run-time are provided in order to enable the system's service

[34] In this context, "feature" is an umbrella term encompassing *services*, functionalities and properties such as *safety, security* or performance.

life to be extended, as illustrated, for example, by the integration of new protocols into telecommunications switches.

However, the interconnectedness of different *domains* and processes that characterises Cyber-Physical Systems leads to interactions between systems and feedback effects between the systems and their use. For example, a telecommunications failure could prevent remote maintenance of the affected systems, whilst new functionality could lead to changes in the way that the CPS is used, causing additional new functions to become necessary. Since these interactions also mutually reinforce each other, *adaptive* and evolutionary mechanisms are becoming increasingly important components of CPS-type systems; see also Chapter 5.2. The above is particularly relevant at the infrastructure level.

Evolution and interactive adaptation: The second type of evolution involves the interactive adaptation and evolving use of CPS *services* by users in new application contexts, together with the coordination and adaptation of CPS functions and *services* during operation. This is primarily characterised by the CPS capabilities described in columns (3) to (5) in Figure 3.6. The evolution is determined by the interaction between the current use context – i.e. situation, tasks, goals, options and application behaviour of the relevant actors and systems – and conditions in the physical environment. The individual *adaptation* measures taken by Cyber-Physical Systems are triggered both passively – through the observations, adaptation and learning of the system – and actively by the environment and the actors themselves.

Evolution and innovation through explicit engineering processes: There is a third alternative where evolution and innovation can be controlled explicitly through interdisciplinary *engineering*, analysis of the environment and application fields with coordinated innovation and *adaptation* measures, and the employment of mechanisms for obtaining feedback from the application. These include mechanisms for enabling systematic design engineering, *validation* and *verification*. Some of the key investigation, feedback and evolution mechanisms in this regard are the experimental and exploratory use of prototypes, together with enhanced requirements *engineering* and *validation methods*. This includes the monitoring and analysis of the two other forms of evolution described above.

3.6.2 ENGINEERING TECHNOLOGY AND RESEARCH AREAS

The following six CPS *engineering* research themes can be identified based on the characteristics described both in this and the preceding sections:

3.6.2.1 User- and use-centred development – dynamics of requirements

In addition to the introduction of the technologies required to determine and realise new forms of *human-system interaction* (see also CPS *human-machine interaction capabilities*) and technologies to enable *adaptation* and cooperation at run-time (context learning, evolution and *self-organisation)*, the following *engineering* concepts and initiatives will be required in order to achieve user- and use-centred development:

- exploratory and observational procedures, the development and application of demonstration initiatives,
- testing and measurement methods for determining *Quality of Experience and Quality in Use*[35],
- user *participation* methods,
- end-to-end *user-centred* design that enables r*equirements traceability*, application integration and *validation*,
- enhanced problem-solving methods, i.e. iterative methods and techniques for defining and specifying the field and scope of the relevant tasks and research (*scoping*), as well as problems and goals,

[35] See also the ISO software quality standard ISO/IEC 9126 – which has now been incorporated into ISO/IEC 25000 [ISO10].

- involvement of users in the innovation and development process,
- *virtual* methods such as the development and utilisation of prototypes and simulation *models* for *validating* and *verifying* quality requirements,
- the development of *requirements*, environment and *domain models,* including role, *user, interaction* and *behaviour models* for identifying, *validating* and *verifying* requirements, as well as integrated *situation* and *context models* (see also 3.6.2.5),
- end-to-end methods and *models* for *tracing requirements* and how they change throughout the design and composition of networked, interconnected CPS components and *services*, in order to ensure that the requirements are met and enable the impact of changes or alternatives to be evaluated. This involves continuous *validation* and *verification* of the composition and integration of the relevant CPS components and *services*, both in terms of their quality requirements and the required guarantees for their use.

To achieve this, it will be necessary to develop end-to-end, mutually consistent processes, concepts, methods and techniques for the design, development, manufacture, maintenance and evolution of Cyber-Physical Systems and their components.

3.6.2.2 Environment and domain models with integrated application platforms

Engineering needs to address the following requirements:

- the development of generic, *domain-specific* requirements, situation, environment and quality *models* that can be used as a toolkit for putting together *interoperable*[36] components with *dependable* quality,
- *scoping, tailoring*, i.e. the selection of process components before the *engineering* process begins and the dynamic adaptation of subsequent development activities,
- expansion and integration of cross-*domain* scenarios and applications,
- platform *engineering* and the challenge posed by differences in the development and life cycles of CPS components; see also 3.6.2.5 and 3.6.2.6.

3.6.2.3 Enhanced goals and requirements engineering

In order to enable *scoping, tailoring* and situation-specific use – i.e. searching for and selecting – of CPS components, as well as to facilitate cooperation with them and alignment with the goals of the *services*, it will be necessary

- to develop goal systems as extensions of *domain models* that are capable of representing local, regional and global contexts. These contexts are represented in the *viewpoints* of all the relevant *stakeholders* – i.e. their goals, interests and relationships – which need to be depicted in a formal and structured manner.
- to undertake continuous and detailed assessment and prioritisation of the requirements with regard to risks, feasibility, compliance with guarantees, *validation* and *verification*, and
- to investigate the cost-benefit ratio and *return on investment (RoI)* of the components and *services*.

3.6.2.4 Risk engineering, enhanced safety, security and guarantees

In view of the higher risks involved in using Cyber-Physical Systems, enhanced *engineering* methods are required to enable detailed analysis and assessment of these risks, particularly with regard to technical feasibility. This includes, for example, *interoperability*, semantic integration and quality guarantees. The following risk *engineering* methods will be necessary in order to ensure *safety, security*, performance and *privacy* protection:

- standardised specification and definition of guarantee and testing concepts at every abstraction level. This includes

[36] This includes all the different levels of *interoperability, i.e. technical, semantic and user-visible interoperability* (see also 3.1).

the system and user interface requirements, architecture concepts and interaction and composition behaviour,

- the development of quality *models*, norms, standards and policies,
- the development, specification and standardisation of generic (valid for all Cyber-Physical Systems) and *domain-specific* risk constellations, i.e. *domain engineering models,*
- a standard definition of *safety and security* or threat levels/categories in uncertain environments.

This will also involve the evolutionary development and classification of quality-oriented architecture and behaviour patterns with enhanced testing and *verification* methods. The models can then be used as a basis for certification and issuing trust seals.

3.6.2.5 Interoperability: the management of open platforms, reference models and standards

The *engineering* tasks described above, and in particular the open networking of heterogeneous components and *services* via several CPS applications, will require

- the definition and creation of basic (cross-*domain* and generic) infrastructure and communication platforms for Cyber-Physical Systems, with the corresponding protocols and basic functions or services. This is also necessary in order to provide the required quality guarantees,
- the *domain-specific* development and creation of *application platforms* with function and *service* architectures, the associated requirements, architecture and quality *models* and the relevant standards and procedures.

3.6.2.6 Differences in the life cycles and character of system components and services

One of the key *engineering* challenges is how to combine the "cyber" aspects with the "physical" aspects, i.e. to integrate different types of CPS components. These include physical objects such as streets and mechanical devices, but also network infrastructure, electronic components, sensors and software, all of which have different life cycles.

The software on mobile end devices or PCs is updated almost on a weekly basis, while the end devices themselves are usually replaced every few years. Infrastructure and complex *engineering* products such as trains or aircraft, on the other hand, remain in use for several decades. This restricts their ability to cooperate with Cyber-Physical Systems and take advantage of their new capabilities. Moreover, binding quality requirements with regard to *dependability* and trustworthiness need to be complied with despite the networked and interconnected nature of CPS *services* and applications.

In addition, all of these issues make it extremely difficult to calculate the cost-benefit ratios and *return on investment* of Cyber-Physical Systems. This in turn raises a number of requirements with regard to

- version, release, configuration and compatibility management, together with design and realisation methods,
- sophisticated methods, integrated processes and procedure and process *models*,
- integration and alignment of procedures and *engineering* approaches and
- integration of heterogeneous interfaces, protocols and concepts in order to meet general or application-specific quality and guarantee requirements (see also the discussion in the previous sections of issues relating to *interoperability*, integration and standards).

The cross-domain networking and public use of open application platforms will require adjustment and continued development of the associated *models*, platforms, standards and *architecture frameworks, services* and processes. This will in turn require initiatives to ensure the support of all the *stakeholders* – involving the end users and enterprises in the *value networks* and *ecosystems* –, as well as the relevant social groups and political representatives.

4 POLITICAL AND SOCIAL CHALLENGES

At present, it is not possible to comprehensively assess the full potential of Cyber-Physical Systems. Many of the social developments that they will trigger are difficult to predict, since the particular form taken by Cyber-Physical Systems will largely depend on the technological, organisational and legal framework at both national and international level. It is therefore clear that the increased presence of networked software systems and related *services* in virtually every area of our lives is going to lead to changes that cannot be easily predicted.

The trend towards a networked world where information and communication technology plays a key role is already in full swing and would appear to be an irreversible process. There is currently much public debate regarding society's values and the extent to which they may be at risk. The topics under discussion range from closer involvement in designing the systems and their scope for shaping various aspects of our private lives to more negative aspects, including a fear that people's *privacy* will be invaded, a loss of control for individuals or even entire nations, excessive surveillance and infringements of basic human rights and freedoms, as well as the emergence of a digital divide in society [CSH04, Zil09, Sch10a[37], KR11, Sch07a, Bau09, Par11, 3sa11].

Social systems face far-reaching changes as a result of the pervasiveness of Cyber-Physical Systems and the profound impact that they will have on social interactions, processes and structures thanks to their extensive context awareness capabilities (using *sensors*) and the fact that control of their behaviour can be fully or semi-autonomous (using actuators), as well as being globally networked and integrated into everyday processes. This calls for a wide-ranging analysis of the implications of this technology and the associated *human-technology cooperation*. In addition to looking at the potential of CPS, their excess-value and the valuable *services* that they provide, there is also a need to examine and document the changes that they can be expected to bring about and their positive and negative impacts. It will also be necessary to debate their role at both the social and the policy level and to ensure that any necessary design and security precautions are taken. This task will fall in particular to the people responsible for CPS technology and its promoters.

In order to leverage their social potential and at the same time combat possible risks and develop and operate useful, acceptable and controllable Cyber-Physical Systems, it is essential to discuss the technology and its possible impact in technological, political and social terms. This means weighing up the threats, opportunities, costs and benefits, evaluating the results and taking an interdisciplinary approach to specifying the requirements and conditions for the deployment of CPS in terms of the technology and systems themselves and how they interact.

4.1 TECHNOLOGY IMPACT, SOCIAL AREAS OF CONFLICT AND ISSUES FOR INTERDISCIPLINARY RESEARCH

Cyber-Physical Systems pose a wide range of challenges for the interdisciplinary analysis of the technology's impact and design. A preliminary list of relevant issues includes:

- new safety and *security* issues for users,
- unknown risks related to changes in *human-machine interaction*,
- issues related to acceptable configuration of the technology,
- new requirements in terms of joint control of complex, open *socio-technical* systems by humans and computers.

These issues need to be tackled in a coordinated manner as part of an interdisciplinary approach to CPS acceptance research.

The selection of topics is based on the results of recent technology impact studies [ML08, Hil07] and analyses of

[37] "Plug & Pray – Von Computern und anderen Menschen" (Plug & Pray – of computers and other humans), a documentary film by Jens Schanze.

the sociology of technology [Wey06a, Wey06b, Wey06c, Wey11a, FW11]. These are complemented by the results of the *BMBF* Foresight Process “New future fields” [CGW09] and the scenario analysis methods and system characterisation described in Chapter 1.4 (see also [Hei11]).

The sections that follow outline the individual topics.

4.1.1 SAFETY AND SECURITY ISSUES FOR SMART, NETWORKED AND INTERACTIVE TECHNOLOGY

One major issue when analysing CPS scenarios and visions is the possibility that new *safety* and *security* risks may arise that cannot currently be predicted. For example, analyses of recent air and road accidents involving smart technology (see [LPS+97, Wey06b]) have demonstrated that complex chains of events, poorly understood interactions between systems’ behaviour and the immediate or more general environment and *human-machine interactions* can cause a wide variety of errors and accidents.

There is a need for detailed research into measures at the various levels of system design, development and application that could help prevent such accidents in the future. Such research should not just examine the technology itself but also aspects like organisation and training as well as standardised safety cultures and conflict resolution strategies. The main focus should be on *shared control* and possible discrepancies between human beings and their requirements on the one hand and autonomous systems[38] on the other.

Everyday use: The open, interactive nature of Cyber-Physical Systems and their use in everyday situations – in open social environments – means they have a high degree of complexity compared with the closed technologies used in the world of work – for example aviation or automation technology – and this complexity is growing as a result of the ability to network different systems (see Chapter 3.2 and 3.3). This already complex situation is exacerbated by the diverse goals and process or situational requirements of the different actors, as well as by untrained users and unknown third parties whose behaviour vis-à-vis the system cannot be predicted. These actors may well have come into contact with the technology unintentionally and found themselves forced to interact with it.

Decision-making on the basis of uncertain knowledge: Both sides – highly distributed systems and the people who use and interact with this technology – constantly have to assess the situation, make decisions and take action on the basis of uncertain knowledge.

New issues relating to controllable human-machine interaction: The use of Cyber-Physical Systems not only raises new issues concerning the controllability of technology and wider questions of *safety* and risk research as outlined in Chapters 3 and 5; there is also a wide range of issues concerning the appropriate design of the systems and the relevant *human-machine interactions* and *cooperation*, particularly in terms of their impact on the direct or indirect actors, users and *stakeholders*.

Over the last thirty years, embedded systems in the road traffic environment and in private cars have made a huge contribution towards improving passive and active *safety*. It is in no small measure thanks to such systems that the number of road casualties has been falling for many years. At the same time, the integration of a growing number of assistance and control functions into vehicle systems has changed the role of the driver and altered the relationship of driver and vehicle with the environment. Vehicles are increasingly taking over awareness, coordination and control tasks from their drivers. In addition to the problems of driver inattentiveness mentioned in Chapter 3.3, networked technology, with its wide range of usually uncoordinated[39] assistance functions, can result in drivers

[38] Thus, in [Tra09], for example, experts are quoted as saying: “Pilots only understand the aircraft superficially. Hardly anyone has an in-depth understanding of the control software anymore”.

[39] Usually developed separately and for integration into existing vehicle functions.

experiencing stress and feeling overwhelmed, particularly in unusual and critical driving situations. Drivers – and other road users such as pedestrians or cyclists – are often helpless in such situations. The fact that they have grown accustomed to receiving extensive support from assistance systems that take over responsibility for routine coordination, decision-taking and actions means that they lack the experience needed to cope with critical situations themselves; see also [Wey06b].

Vehicle systems are also increasingly open and networked with other systems in their environment, such as smart traffic lights or higher-level traffic control systems. This means that drivers are often unable to gain a clear picture of the systems or the situation. They are not able to accurately assess the systems' behaviour and capabilities because

- their behaviour is influenced by events and relationships that are not perceived by the user and do not form part of their understanding of the situation,
- they do not demonstrate the 'normal', rule-based behaviour that would be expected of social actors. **The systems' behaviour does not obey socially agreed, learned rules of interaction, but conforms to the objectives and functional rules established during system design and construction.** Figure 4.1 shows a comparison of human interactions and cooperation with conventional technology and advanced technology.

As demonstrated by the questions arising in connection with the emergency stop performed by Frau Müller's vehicle in Chapter 3.2.3.1, this can effectively mean that the driver is no longer responsible for the behaviour of the vehicle (see also [Wey06b, p. 7]); when accidents occur, it can therefore sometimes be difficult to apportion legal liability.

One question that needs to be answered concerns liability for damage or injury caused in accidents on public roads that have resulted from fully or semi-autonomous cooperation between systems. These include

- autonomous emergency stops (see Chapter 2.2.2),
- situations where the vehicle is fully controlled by autonomous, cooperating systems when joining or leaving a motorway; see Chapter 2.2.3.

Figure 4.1: Comparison of interactions between human beings and conventional/advanced (smart) technology [Wey06a]

HYBRID SYSTEMS – INTERACTIONS OF PEOPLE WITH ...

	OTHER PEOPLE	CONVENTIONAL TECHNOLOGY	ADVANCED TECHNOLOGY
Predictability	regular behaviour	completely predictable	unpredictable, irregular
Assigning capacity to act	yes	no	partly
Acting type	a) strategic b) communicative	a) instrumental (design engineer) b) strategic (user)	a) instrumental (design engineer) b) adaptive (user)

Additional engineering responsibility: These two examples alone highlight the additional technological challenges and responsibilities faced by interdisciplinary *engineering* and the planners and engineers involved in this field. If smart systems are to enjoy greater acceptance and "acceptability", it will be necessary to move away from a limited focus on technical feasibility towards interdisciplinary and *participatory design* and construction of smart, networked technology that offers extensive support whilst at the same time remaining predictable and understandable for human users and still allowing them to make their own decisions about how to proceed.

Dependencies: As well as the questions relating to the *safe* and *secure* control of CPS technology and its applications (see Chapter 3.2), various dependencies between Cyber-Physical Systems and their smart, open *infrastructures* exist in every field of application. This hugely increases the vulnerability of individuals – as well as industry and society – if the smart technology malfunctions, breaks down or is tampered with by a third party. As such, the challenges in the field of *safety* and *security* are not just connected with the *dependable* design and assuring of the systems in terms of *safety, security, privacy* protection and *know-how*, but also involve enabling every individual, and society as a whole, to act safely and independently without the need for extensive technological support.

This ultimately raises the following questions for society which have yet to be fully resolved:

- To what extent can we afford to – and do we wish to – be dependent on networked technology in different areas of our lives?
- To what extent should an understanding of technology be part and parcel of general education and training, so that people can use sophisticated technology competently?

In addition to interdisciplinary *engineering*, this calls for awareness-raising amongst users, along with a social debate on how we wish to handle the social changes and risks associated with the use of smart, networked technologies. The aim should be to identify, discuss and forge a social consensus on the requirements in terms of the systems' design and use and the framework and regulations required for their development.[40]

4.1.2 INDIVIDUAL TECHNOLOGY ACCEPTANCE AND DESIGN ISSUES

If the design of Cyber-Physical Systems is to meet the relevant needs, then in addition to the new issues of *safety* and *security*, controllability and *human-machine cooperation,* it will also be necessary to carry out an in-depth investigation of the possible impact of the technology and the related questions concerning user acceptance. This will include social values and ethical issues as well as specific user requirements and acceptance criteria amongst the individual groups or cultures for which the systems are being developed and deployed.

On the one hand, CPS technologies offer a wide range of social benefits:

- greater independence and autonomy thanks to comprehensive provision of information and assistance
- greater comfort
- close integration into social contexts through comprehensive networking
- engagement in social processes
- flexible involvement in designing the technology and how it is used through variable concepts of use.

On the other hand, the negative effects also need to be analysed and steps taken to counter them. The results of empirical acceptance research in specific application scenarios

[40] See also the demands for a social debate on the relationship between people and technology that emerged from the *BMBF* Foresight Process on "New future fields" [CGW2009].

will play an important role in establishing the relevant acceptance factors, system requirements and *human-machine interactions.* The research reveals the following possible negative effects of smart technology use for individuals and their wellbeing. These go beyond the question of *safety* and *security*:

- **Unease, stress and a excessive demand,** arising from the "cognitive dissonance"[41] that people experience when confronted with impenetrable technology and its seemingly incomprehensible acting. Smart machines undermine people's confidence because although at times they seem to operate according to familiar patterns, at other times their behaviour appears extremely erratic. This unpredictability throws the usual relationship between man and machine into doubt [Wey06a]; see also the example under 4.1.1.
- **Perceived or actual loss of freedom**, impairment of freedom of action and the ability to act strategically in a social context, and even passive-reactive behaviour. Actors who behave strategically and instrumentally include other people and their likely strategies in their plans, as well as the likely repercussions that their own actions will have for others. (see Weber's theory of social action [Web02] and [Wey06a, p. 15]). In interactions with smart technology, however, this is only possible to a limited extent, as demonstrated in 4.1.1. This highlights the challenges involved in developing *human-machine interactions* to create a technology that behaves in a way that meets human interaction requirements.

  In the *BMBF* Foresight Process on the future field of *human-machine cooperation* [CGW09], this technological challenge is encapsulated in the call for a "code of etiquette for robots" – in other words, a set of socially determined standards regulating the acting of systems and their *human-machine interactions.*
- **Surveillance and coercion:** The collection and analysis of data from different areas of our lives brings with it the danger of surveillance and coercion. In particular, CPS *sensors* will result in a considerable increase in data collection that will be largely unchecked and lacking in transparency for users, entailing the risk of infringements of people's *privacy* or freedom of action [KR11, Par11, ML08].
- **Loss of trust:** As such infringements of basic personal freedoms increase, the ubiquitous use of networked information and communication technology also leads to an erosion of trust. [Mat03]. This applies not just to trust in the technology and its manufacturers and operators, but also to trust in regulators, policymakers and society as a whole, in line with the finding that "[....] technology has generally been perceived as an embodiment of 'power' and therefore also the 'powerlessness' of the individual" [aca11a]. For example, inhabitants of the Canadian province of British Columbia are opposing plans by the state electricity utility BC Hydro to install *smart meters* in all households on the grounds that these devices would allow the utility – and therefore also the state – to gather detailed information about whether or not people are present in their homes and their patterns of behaviour. In addition, in the neighbouring province of Ontario where the devices have already been introduced, instead of falling, electricity prices have in some cases risen dramatically [Cal12].
- **Curtailment of personal freedom of action** and even forcing people to behave in particular ways. This can have many different causes such as liability concerns, a fear of surveillance and misinterpretation of one's own behaviour or even criminal use of and remote attacks on smart technology control systems such as vehicle braking systems [CMK+11] or insulin pumps implanted in people's bodies [Han11].

[41] Cognitive dissonance is used in psychology and social psychology to describe feelings that are perceived as unpleasant which are triggered by an individual having several cognitions – perceptions, thoughts, opinions, attitudes, desires or intentions – that are incompatible with one another.

The examples that follow make it clear that when it comes to these possible types of impact, the social and legal questions concerning how to handle the huge volumes of data that arise in the context of CPS use have yet to be satisfactorily addressed – for example in terms of the scope for linking the data collected to a particular person, or "collective privacy" as discussed in the examples below (for more on this, see also 4.2):

- "Green Party politician Malte Spitz went to court to demand the return of six months' of his data that had been stored by Deutsche Telekom, and subsequently made the data available to the ZEIT ONLINE newspaper. The data can be used to trace all his movements during the period in question. We also correlated the GPS data with information about the MP's life that was freely available online (via Twitter, blog entries and web sites).
- By pressing the PLAY button, you can embark on a journey through Malte Spitz's life. The speed control can be used to go faster or slower and you can stop at any point by hitting the PAUSE button. The calendar below also shows the other times when he was at this location and enables any point in time to be selected. Each of the vertical bars represents one day" [Zei11]
- Satnav manufacturer TomTom provides the police with (anonymised) speed data from its Dutch customers that enables the authorities to choose the optimum location for their speed traps [Ber11b].
- "Carrier IQ is currently facing a storm of outrage from the owners of mobile phones that use the company's program. Without their knowledge or permission, it has been scanning operations on 141 million phones and sending information on cut-off conversations, unsent text messages and power-hungry applications to the network operators in order to help them with remote diagnostics and market research. [...] Consumers in the USA have launched a class action [....] Coward comments: 'The storm in the media came as a complete surprise – up to now we weren't used to dealing with private customers – our customers are the network operators'." [SL11]
- Especially in the healthcare sector, there are a number of questions concerning the handling of collectively acquired patient data. Who do they belong to? Is a health insurance provider entitled to use data collected via a remote monitoring system – for instance the insulin readings of a diabetes patient that have been transmitted via a Cyber-Physical System – in order to check treatment compliance if it is paying for the emergency remote monitoring system? This question becomes particularly relevant in view of the fact that health insurers are already considering introducing premium reductions for patients with good treatment compliance.

In addition to questions of responsibility and liability in the case of accidents involving smart applications, there are also a variety of social and legal issues connected with the storage, accessing and utilisation of sometimes huge volumes of personal and *non-personal data*. Who do the data belong to, who is entitled to use them and for what purpose? What should it be possible to analyse using these data? And who protects the data against misuse, thereby directly or indirectly protecting the individuals involved?

4.1.3 SOCIAL CHALLENGES OF GLOBALLY NETWORKED, INTERACTIVE CYBER-PHYSICAL SYSTEMS

The complexity, degree of penetration and full extent of the impact of Cyber-Physical Systems are difficult to assess and cannot be adequately measured by any single scientific discipline. It is essential to adopt a fully interdisciplinary approach to smart, networked technology and what we know about it. It is also necessary to look beyond the confines of markets and *domains* and draw the appropriate conclusions, since the same phenomena that can be observed in financial systems – where even experts are barely able to understand them anymore – are also very much applicable to globally networked control systems such as *smart grids*.

In this context, the significance of physical-geographical space as the principle that governs cause and effect is diminished by the possibilities offered by the Internet and globally networked smart Cyber-Physical Systems. New governing principles such as topologies of technical and socio-technical networks with databases, access, utilisation and ownership rights, different actors and complex technical control and political governance systems are set to gradually become more significant than traditional control over physical space [Hil07].

In all likelihood, it will be urgently necessary to find answers to questions relating to fairness and new forms of conflict in connection with emerging networks and CPS infrastructures and their control mechanisms. These questions are particularly relevant to the global dimension of Cyber-Physical Systems. Many of the systems and networked *services* originate from countries that do not comply with German standards of *safety* and *security*, ethics and quality, but nonetheless have to be appropriately integrated to a greater or lesser extent. By the same token, the standards of other cultures also have to be complied with.

The social tensions, fears and concerns about fairness that have already been discussed in the context of the rapid development of the Internet, networks and their ubiquitous digital *services* become even more highly charged as a result of Cyber-Physical Systems' ability to capture more extensive data and exercise smart control. The relevant issues include

- the drifting apart of social strata and heightened tensions between "literates" and "illiterates", "natives" and "non-natives", "haves" and "have-nots", "drop-outs" and "refuseniks". The key issue here is the impact of the existence of Cyber-Physical Systems on groups of people who lack the technical know-how or the access required to engage with them, or who eschew them of their own volition.
- individuals or social groups losing their ability to solve problems and take action. This can result from increased use of technologies that provide support and operate autonomously and a concomitant increase in passivity and conformity.
- social groups and basic government functions becoming increasingly dependent on Cyber-Physical Systems and their coordinating services. This touches on the issue of the infrastructure required in connection with Cyber-Physical Systems; see also 4.1.4.
- basic questions and analyses relating to the impact and power of technology in shaping society, in other words in bringing about socioeconomic and institutional change [DW07][42].
- socioeconomic change that is increasingly determined by "male technology" [Dög01][43], coupled with a low proportion of women in the MINT[44] subjects and professions – something that is usually discussed in economic terms – and the current debate about the low proportion of women in the Pirate Party [Hof11].
- local and global environmental sustainability and fairness. This applies to the scarce resources and energy required to manufacture and operate the technology. Fair sourcing and distribution of these resources and energy poses a major challenge, as do economic and political tensions at both a global and a local level.

These questions and fears are counterbalanced by the potential that Cyber-Physical Systems offer, for example to improve the supply of energy and goods to areas with little

[42] It should also be pointed out that in his many contributions (300 pages) the term 'gender' does not occur; see also [Dög01].

[43] [Dög01]: Conference paper by Peter Döge which also identifies "Androcentric selectivity in the process of political technology control".

[44] MINT stands for Mathematics, Information technology, Natural sciences and Technology.

infrastructure, or the possibility of using *AAL* systems to help people with physical or mental disabilities to lead more independent and mobile lives and engage more actively in society.

4.1.4 GOVERNANCE – SOCIAL CONTROL OF OPEN SOCIO-TECHNICAL SYSTEMS

The term *governance* refers to the system for controlling and regulating a socio-political entity. Before examining the *governance* issues that arise in connection with CPS, we will begin by providing a brief introduction to the structure of the systems, since the design of the infrastructure for Cyber-Physical Systems is one of the fundamental challenges for *governance*.

Based on their typical capabilities[45], the CPS scenarios described in the previous chapters can be divided into the following types of networked *socio-technical systems*; see Chapter 2.1:

a) **large-scale first- and second-order infrastructure systems**; networked *smart sensors* for enabling *physical awareness* and needs-based control offer the greatest potential for innovation in this area.

b) **interactive socio-technical application systems** and processes in working and living environments, including virtual ones, for example in technical and social Internet *communities*; smart interactive situation and context awareness and *human-machine cooperation* tailored to users' needs are the key innovations in this context.

Appropriate design of large-scale infrastructure systems is key to the differentiated development of the application systems that use these infrastructures. [Deg02]:

> "First-order systems are open-ended and therefore functionally non-specific infrastructure systems such as traffic, transport and communications infrastructures. The term "second-order systems", by contrast, refers to superimposed inter-systemic structures in which parts of the first-order systems are combined in order to perform a specific task. These are social domains "in which, increasingly, elements of 'autonomous' technological network structures for transport, communications and data exchange, goods supply and waste disposal are recombined for the purposes of the system in question and are given their own institutional identity". Examples are cross-border disposal of toxic materials in the waste management sector, organised mass tourism structures in the leisure industry or the creation of a supraregional technological system for transplant medicine in the healthcare sector" – as well as the abovementioned large-scale logistics systems. These higher-level systems and *domains* are heavily dependent on the networked (first-order) infrastructure.

The examples discussed in [Deg02] show "that large-scale systems cut across highly differentiated functional systems (application domains) and therefore constitute a basic precondition for increased social differentiation" [Eka94].

This digression into socio-technical theory illustrates what is required for a detailed study and classification of Cyber-Physical Systems, their applications and their networked, autonomous interaction structures. It also highlights the importance of a deeper analysis of *human-technology interaction* and *cooperation* in order to answer questions relating to the technological, social and economic aspects of system and service design.

In their analysis of the *governance* and control of complex, networked "hybrid systems"[46], Weyer and Cramer use the example of road traffic [Wey06b] and large-scale logistics networks [CW07][47] to look at control-related issues in open, socio-technical infrastructure systems. For example, they discuss the extent to which the opposing concepts of central coordination and control and decentralised self-coordination of closed systems such as container terminals,

[45] See the table in Figure 3.6.

[46] The concept of a "hybrid perspective" [Ram03, p. 312] emphasises the "Involvement of technical artefacts" in hybrid constellations of actions distributed between humans and computers [RSS02, p. 13].

[47] Results of sub-project M14 "Humans in logistics" within the DFG special research field 559 "Modelling of large logistics networks" [SFBa].

which are characterised by highly disciplined actors, can be applied to an open system like road traffic where the actors are less disciplined.

If all the actors in such networks were able to communicate with each other electronically and in *real time,* then both the centralised and the decentralised, *self-organising* coordination modes would exist. Based on this assumption, the following goals and effects can be identified for large-scale infrastructure systems:

- **governance mode 1:** central coordination and control, characterised by global optimisation, hierarchical control and loss of *autonomy*; the risks involved include total control and loss of human users' ability to learn and adapt
- **governance mode 2:** decentralised self-coordination with local optimisation, for example individual use of a navigation system with dynamic route planning and decentralised negotiation. One example of this would be the "SignalGuru" green wave *app* [KPM11, Sch11], which registers local traffic light phases, passes on the information to other vehicles in the vicinity and calculates the optimal speed at which to drive in order to reach an intersection when the lights are green. Possible risks include emergent – i.e. spontaneous, and incalculable – effects, conflicts relating to fairness and loss of control over *safety, security* and quality.

Governance mode 2 – i.e. *self-organisation* – does, however, have one drawback: self-organised coordination of individual actors who all wish to gain maximum benefit from the system can result in unpredictable systemic effects which, in turn, can have unintended consequences. For example, the traffic could end up being redirected through residential areas. Even autonomous coordination between technological functional units can result in such effects, for example the random formation of container *clusters* at a terminal [CW07].

Distributed control and the fairness of Cyber-Physical Systems: Many Cyber-Physical Systems are infrastructure systems that operate semi-autonomously, for example *smart grids* or traffic management systems. In the mobility scenario in Chapter 2.2.3, for example, Frau Müller is directed to a different motorway exit from the one that constitutes the most direct route for getting to her children's school. The decision is made by the system according to the traffic situation and is based on communication, coordination and calculations undertaken by the systems involved.

In addition to the actors involved in technology and *engineering*, policymakers also have considerable responsibility for the design and distributed control of the systems and for the establishment of framework regulations and international agreements. This entails

- a trade-off between centralised and decentralised, *self-organising* system control – both for the process of social and political negotiation and establishment of the system and for technical implementation of the autonomous negotiations performed by the systems in real time and at run-time, and thus
- monitoring, controlling and handling of emergent behaviour,
- reasonable limitation of autonomous behaviour,
- fairness and
- needs-based designing of the environment and required framework, including the question of environmental sustainability.

The most important question is who has the authority to monitor and control the systems used for supplying basic energy, healthcare and mobility *services*. If they are to be accepted, it is important in both social and economic terms to ensure that access to these *services* and resources is allocated fairly. In addition, the risks must also be taken into account, i.e. curtailment of *privacy* and personal freedom and a resulting loss of trust in the systems as a whole; see also

4.1.2. In this context, the question of data sovereignty also arises: who is allowed to capture CPS-related data? Who do these data belong to? What third party access rights should exist for historical *primary* data but also for the data subsequently derived from them?

As smart networked technology develops, together with all the associated changes and the tasks and problems that CPS technology is supposed to solve, there will be more focus on issues connected with the fair and transparent management of complex *socio-technical* systems, in particular the question of who is going to control and provide support for the various *socio-technical systems* and subsystems. Such questions and changes will also arise with regard to

- existing and as yet undefined relationships and the coordination of local, regional and global goals and interests with the relevant *human-machine interactions* and technological control,
- the distribution of tasks and control and decision-making authority amongst users, social groups, enterprises, organisations, regions and states,
- the conditions required in society and the environment for needs-based design and application of Cyber-Physical Systems and
- new *business models* featuring regional and distributed corporate partnerships, together with new forms of investment and revenue sharing.

Even future open *socio-technical systems* will not be able to incorporate all the actors and their intentions electronically, for example in order to optimise traffic flows. Indeed, some actors will not even wish to be incorporated in this way. One major *engineering* challenge for the design of *socio-technical systems* and applications that are capable of being operated fairly is how to identify and **deliver the goals and requirements of all the actors on an interdisciplinary basis,** including the necessary *human-machine cooperation.* Such systems – which also raise questions relating to support for social activities – include

- traffic in cities and rural areas,
- energy and building management in residential and business districts, hospitals or airports,
- smart energy generation, networking, distribution, storage and consumption in infrastructure grids (*smart grids, micro grids*),
- extensive support in the field of *AAL*, including integration of the CPS *domains* of building management, mobility and telemedicine.

All too often, scientists and specialists in autonomous closed systems and technologies overlook the question of their social impact and the design of *human-machine interactions*. This is also demonstrated by the study “Self-organising adaptive systems – analysis of the opportunities and threats and design approaches to new ICT concepts” commissioned by the *BMBF* [EG10].

4.1.5 CONCLUSIONS FOR REFLEXIVE AND PARTICIPATORY TECHNOLOGY DESIGN AND THE ANALYSIS OF ITS IMPACT

To sum up, current analyses of the impact of technology and the challenges discussed above indicate a close interaction between the development of *human-technology co-operation* [aca11a][48] and the development of technology as a result of a “social construction process” in the sense also employed by [CW07] in [DW07]:

“Technology *per se* does not have any power to shape society; this is amply demonstrated by the many innovations that have failed or have never been realised. The

[48] [aca11a]: “Technology and society do not develop separately – they are linked together in a multiplicity of ways. The relationship between technology and society is not characterised by unilateral influence but by ‘co-evolution’.”

development of technology, however autonomously it may operate, is always a social construction process where different technologies are either used or not used. The potential that a given technological development offers is an important resource in this process, but it would be naïve to associate the emergence of a new technology directly with social change. The process is much more multi-layered than that, and it is only by closely studying the interactions between the different layers that one can identify the separate roles played by the technology and the relevant actors."

If *socio-technical systems* are to be designed in a reflexive and *participatory* manner, it will be necessary to undertake a more sophisticated and in-depth study of the interactions and cooperation between humans and computers in the fields of product and everyday technologies, work technology and *external technologies* such as chemical plants or nuclear power stations.

It is necessary to look at the vision that underlies CPS technology from all three of these perspectives, as well as to address the question of equitable distribution (see the analyses in the preceding sections). In particular, the extensively networked sensors and control logic of Cyber-Physical Systems have enabled mechanisms from the workplace to become increasingly widespread in our everyday lives in the interests of greater functionality and speed. Their unstoppable penetration of and influence over every area of our lives raises fundamental questions about *external technologies.*

As far as the development of smart networked technology in *socio-technical systems* is concerned, the findings of the analyses performed to date can be summarised as follows:

- Complex technologies were primarily used in the workplace as an instrument for increasing economic efficiency; see [aca11a]. This fact is reflected in the main goals and expected excess value in the CPS scenarios related to manufacturing, logistics, mobility and energy – and increasingly also healthcare, where the introduction of the electronic health card is expected to drive efficiency gains. Hitherto, the technology has not really been designed to meet the different goals and demands in the context of everyday social cooperation and coordination tasks such as *Ambient Assisted Living* care for the elderly in their own homes. The same goes for basic construction and business processes. For more on this, see also the current discussion about new *business models* and the disruptive impacts on the industrial sector triggered by digital technologies and their open, networked systems and services in [Fra03a, Kit09, Cus10] and the attempt to examine and explain these phenomena in Chapter 6.
- In society at large, technology is mainly experienced as a consumer good [aca11a]. Except in the world of work, it is only technologically minded people – in other words, a very small proportion of the total population – who concern themselves with the subject to any greater degree. It can therefore be assumed that many people feel somewhat helpless vis-à-vis technology, and there are indeed good grounds for concern that a social divide is opening up between "digital natives" and "non-natives". The possibility that this problem could be exacerbated by the use of smart networked technology in assistance *services* is discussed in 4.1.2.

The changes triggered by CPS technology and the interaction and cooperation between humans and machines entail a number of challenges as a result of

- the ubiquity of the technology,
- its interactive nature,
- the lack of *transparency* of networked technology and
- the need for the user to make immediate decisions based on incomplete knowledge.

If all these challenges are taken together, then the user's satisfaction with the technology – and therefore their acceptance of it – essentially depends on

- it being adapted to the user's requirements and the context of use
- it being controllable, so that people retain their role as decision-makers and problem-solvers, as well as their ability to act and configure the technology independently.

In developing new concepts for controlling open, complex *socio-technical systems (governance)*, it is therefore important to take the following considerations into account: "This ambivalent or even sceptical attitude towards a range of external technologies is largely attributable to individuals' perceived loss of control over their own lives and their ability to determine how they use their time. We know from research into happiness that nothing affects an individual's sense of wellbeing more than the feeling that their life is being governed by some outside force – whether it be in the workplace, through social inequality or as a result of technology. In this context, the term 'technology' includes the organisational forms and structures which result from the use of technology and are experienced as being coercive." [aca11a]

Implications for the development of technology

In view of the above, it is necessary for the development of technology to allow for the reflexive and *participatory design* of new kinds of *socio-technical systems* and to promote an intensive social debate about how we wish technology to develop. This applies both to the micro-level of *human-machine interaction*, networking and interconnectedness at local, regional or global level and to the macro-level of *governance* structures.

Moreover, it both determines and requires far-reaching changes in interdisciplinary research and practice, especially

- new content, goals and interdisciplinary approaches in research and training,
- new forms of interdisciplinary *engineering* of smart technology, its systems, applications, functions and associated *services* and
- the introduction and establishment of enhanced *risk* and quality *engineering*.

Starting with a preliminary empirical approach, this entails the development of new concepts of system control, as well as the coordination of *human-machine interactions* in the different application *domains* and their Cyber-Physical Systems (see also Chapter 5.3 on the challenges for *engineering*).

Extensive efforts in the field of technology education are equally necessary if we are to make full use of the potential offered by this smart technology and build and develop an economic system for Cyber-Physical Systems that is as efficient as it is sustainable.

Implications for acceptance research

[Ren05] describes how acceptance research has changed from being a means of influencing the people through targeted communication about the technologies and their risks to an empirical public *service*. Acceptance research today serves as an indicator of how general public regards technological change and the pace at which it is occurring.

However, there is now a need for a more thorough discussion of CPS te*chnology and the associated* human-machine interactions, in order to meet the challenges of assessing the risks and consequences of Cyber-Physical Systems and the systematic design of acceptable CPS technologies and applications. Acceptance research should support technology design and research into *human-system cooperation*; see also [Wey06a, FW11]. Its particular task will be to draw attention to technological change and the possibilities that it entails. This will enable acceptance research to encourage and preside over the necessary social and political dialogue and discussion with the actors involved in Cyber-Physical Systems, and to do so in a targeted manner.

Possible concerns about technological innovations and their disruptive impact require a sensitive and transparent discussion of the social impact of CPS technologies. Through conscious and *participatory* design and by taking an open approach to core issues such as the risks and how to contain them, it will be possible to achieve widespread acceptance and make full use of the potential offered by this new technology.

4.2 PRIVACY AND DATA PROTECTION

The use of Cyber-Physical Systems involves employing *sensors* to capture large volumes of data which are then exchanged and processed via digital networks. The data are used as the basis for making decisions which either enable *actuators* to directly influence physical processes or trigger further software-based processes. In this context, it is already clear today that CPS technology will have a considerable impact on our *privacy* and on *data protection*. For example, extensive data on an individual could be collected in order to provide them with better support in various different areas of their life. At the same time, however, collecting such data entails a risk that other people or organisations might use it for purposes other than those for which it was originally intended.

It is not always necessarily a question of blatant misuse of the data. However, as the ways in which it can be processed are not known in advance to the person in question – and often also not to the legislator – any use of data for purposes other than those for which they were originally intended should be viewed with a critical eye. This approach is encapsulated in the census verdict of the Federal Constitutional Court [BVe83] from as long ago as 1983, which speaks of the "right to informational self-determination".

The issue is illustrated by the following example, where Cyber-Physical Systems are ostensibly used to help people find their way on the roads, but the data gathered actually reveal a whole range of other information as well:

Information on an individual's current location that is captured for navigation purposes, for example, is also of interest to burglars who might want to check whether a house is currently unoccupied or to stalkers who are interested in a person's precise location. If the location data are monitored over a longer period of time, it is also possible to identify regular patterns of behaviour, for example the routes that people take to go to work or to visit friends and relatives, their favourite shops or the places where they pursue their leisure activities. This could be valuable information for advertisers wishing to target particular individuals as precisely as possible. For example, it might allow them to site dynamically targeted advertising boards along the relevant routes. It would then even be possible for the routes suggested by satnavs to be devised in such a way as to ensure that the target passed by the advertisements aimed at them.

Information on a person's location at different times during a journey can also be used to calculate how fast they have been driving. In conjunction with other sensor data, this can be used to establish whether they have been driving dangerously. It is possible to imagine various purposes for which this information could be evaluated. For example, it could be used to determine whether and when the Cyber-Physical System takes control of the vehicle in an emergency situation, whether an employer cautions an employee (if the car journey was relevant to their work), whether the driver's insurance premium is increased on the grounds of dangerous driving, whether statutory fines are automatically imposed or, in extreme cases, whether the person in question receives a driving ban.

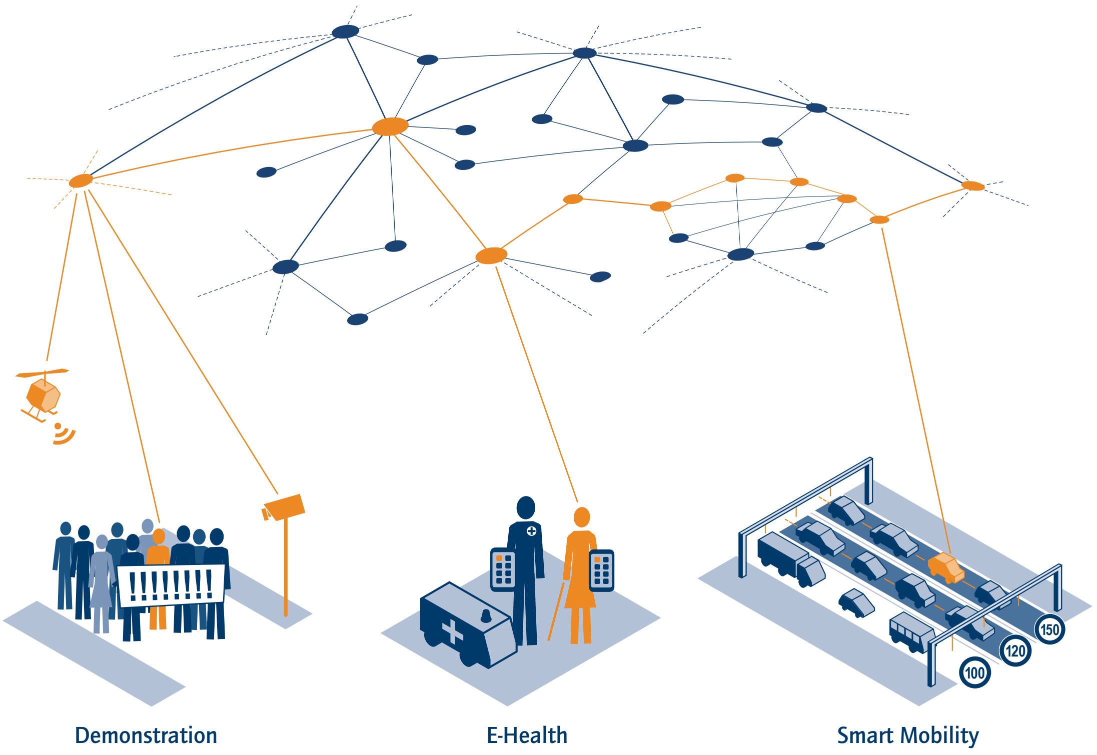
Figure 4.2. shows how the data collected by Cyber-Physical Systems can be linked and used to put together a comprehensive profile of an individual.

Privacy considerations are especially important when highly confidential data are being processed. In the healthcare sector, for example, Cyber-Physical Systems can collect and analyse medical data in order to provide *Ambient Assisted Living* support [ULD10] to the elderly in their everyday lives. Clearly this affects not just information *privacy* but also physical and spatial *privacy*. [KSWK10].

Other areas of application for Cyber-Physical Systems make very little if any use of individuals' personal data. This is the case, for example, in the fields of logistics or manufacturing. In these instances, *data protection* issues are less relevant, even though they cannot be completely dismissed. In particular, attention should still be paid to the protection of employees' personal data in the relevant fields of application.

The complexity and lack of *transparency* of Cyber-Physical Systems could, however, diminish public awareness of *data protection* issues. Social network users, for example, display a high degree of tolerance towards the use of their *personal data*. Another possible consequence could be for people to completely reject all Cyber-Physical Systems on the grounds that they give them the impression of being under constant surveillance (see Chapter 3.4, Key Acceptance Factors). The extent to which undesirable technological impacts are avoided or kept to a minimum will largely depend on the

Figure 4.2: It is possible to build up a comprehensive profile of a person by linking data from previously separate areas of their life.



Cyber-Physical Systems' specific design. The section that follows describes the principal cornerstones of a technology design approach that gives adequate consideration to *privacy* and *data protection.*[49]

After a brief description in section 4.2.1 of the legal basis for *data protection*, section 4.2.2 provides a definition of the term *privacy protection* which goes beyond the concept of *data protection* and thus more fully addresses the complex data processing performed by Cyber-Physical Systems. Section 4.2.3 then describes a possible design approach based on *protection goals*. Finally, section 4.2.4 summarises the conclusions of the preceding sections.

4.2.1 LEGAL BASIS FOR DATA PROTECTION

Legal regulation of Cyber-Physical Systems will be necessary, particularly in those fields of application where *personal data* play a significant role. This applies not just to telecommunications and telemedia regulations but also to data protection legislation at the level of central government and Germany's individual federal states. Furthermore, because of the high degree of networking involved, it also applies to the European and possibly even the international level.

Data protection in Germany is covered by various statutory regulations. However their focus is not primarily on protecting data but rather on protecting the rights of the individual. The Federal Data Protection Act (*BDSG*) states that: "The purpose of this Act is to protect individuals against infringement of their right to privacy as the result of the handling of their *personal data*" [Eur50, Eur95, Eur02, Eur09].[50]

In Germany, the key aspects of *data protection* are derived from the country's constitution and are encapsulated in two rulings of the Federal Constitutional Court regarding the "right to informational self-determination" (1983) and the "right to the guarantee of the *confidentiality* and *integrity* of information technology systems" (2008), also referred to as the "IT Fundamental Right". The processing of *personal data* in Germany is only permitted if there are legal grounds for doing so or if the individuals concerned have given their consent. Particularly in the public sector, there are thus innumerable detailed regulations governing *data protection* issues that would need to be adapted to the relevant field of application in a CPS scenario. Subordinate to these are the Federal Data Protection Act and the data protection legislation of the individual federal states. As Cyber-Physical Systems have both a telecommunications and a telemedia *services* dimension, the Telecommunications Act (*TKG*) and the Telemedia Act (*TMG*) also have to be taken into account alongside the legislation for individual fields of application.

At EU level, in addition to the right to respect for private and family life laid down in Article 8 of the European Convention on Human Rights, there are a number of harmonised *data protection* regulations that the member states are required to transpose into national law, although the details of the legislation may vary. The provisions of the EU Data Protection Directive [Eur95] were transposed into German law in the form of the Federal Data Protection Act (BDSG), while the E-Privacy Directive [Eur02, Eur09] was incorporated into the *TKG* and *TMG* acts. Harmonisation at EU level means that all the member states have an appropriate level of *data protection*, making it legally possible to transfer *personal data* between them. Thus, the regulations that apply to data transfers within a member state also apply when *personal data* are transferred to authorities in other EU member states, to other signatories to the Treaty on the European Economic Area or to the organs and institutions of the European Union. In the case of other nations,

[49] Many of these observations on the topic of *privacy* protection and Cyber-Physical Systems are being published simultaneously in [HT12].

[50] *BDSG: "Personal information* shall mean any information concerning the personal or material circumstances of an identified or identifiable natural person (data subject)."

data can only be transferred if it can be proven that an appropriate level of *data protection* exists, and this has to be verified for each individual arrangement between countries.

In terms of the legal framework for Cyber-Physical Systems, this means that care has to be taken to ensure compliance with the current *data protection* legislation in all countries in which the systems are to be used. One general problem when trying to develop systems that provide guaranteed compliance with *data protection* law is the fact that data protection is not governed by common international standards but is instead subject to regulations that generally differ from one country to another. The situation becomes even more complicated when components are networked across national borders. The legal situation in this field therefore requires even closer investigation.

4.2.2 A BROADER UNDERSTANDING OF PRIVACY PROTECTION

Current *data protection* legislation is based on the assumption that for each processing stage it is possible to unambiguously determine whether the data involved are *personal* or not, and that there is someone who is clearly responsible for the data processing and is able to fulfil this responsibility. However, both these assumptions can generate problems in the context of Cyber-Physical Systems, particularly when several operators are involved in individual components or processing stages. In many cases, the data that have been captured do not relate to a particular individual if taken in isolation. However, if they are combined, they can reveal a large amount of information about the individual concerned, even if only a small proportion of the collected data is required for the purpose in question [BDF+06]. It is also possible that the data may not just refer to individuals but may in fact affect the individual rights of entire groups of people, even though it may not be possible to attribute data to individuals [RBB+08]; see also the examples at the end of this section.

One early, much quoted definition of *privacy* does incorporate the idea of groups: "[...] the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [Wes67]. But up to now, this aspect has not been fully addressed by *data protection* legislation, which only focuses on individuals.

For every data processing operation where it not certain right from the outset whether the data could currently or at some point in the future be connected to an individual, either in its own right or in combination with other data, there is a need to go beyond the conventional understanding of *data protection* and include the actors involved in enhancing the information and all the processing stages. [ULD07]. Ultimately, decisions made on the basis of the captured and processed data affect groups as well as individuals.

It is not possible to rule out errors or inaccuracies in the process of enhancing the information and generating decisions, meaning that some people may show up as *false positives*. This can be seen from the scenarios described below, which although partly fictitious are by no means unrealistic:

– The US company YourCPS operates various Cyber-Physical Systems and related applications worldwide. When it emerges that a user of one of its systems has carried out a politically motivated attack, the company immediately blocks the user's account and informs the investigating authorities of the people he has been in contact with. It also analyses the configurations selected by the user and the usage, interest and personality profiles contained in their database. The names of all users who display an overlap of at least 75 per cent in their configurations or profiles (several tens of thousands) are also supplied both to the investigators and to the border authorities, who bar these people from entering the country as a precautionary measure.

- The effect that membership of an abstract group can have on individuals is demonstrated by the US practice of *redlining*, whereby banks refuse loans to the inhabitants of certain city districts.[51] Another example is the experience of a man from Atlanta, whose credit limit was reduced on the following grounds: "Other customers who have used their cards in shops in which you recently made purchases have had a poor repayment record with American Express in the past." [And12]

Viewed from this broader perspective, *privacy* protection goes beyond informational self-determination and includes the protection of individuals or groups of people against infringements of their *privacy* and their associated personality rights. In this context, *privacy* is the individual private domain where an individual is able to exercise his/her right to free development of his/her personality.

4.2.3 PROTECTION GOALS FOR A RISK-BASED APPROACH TO DESIGN

As described under 4.2.1, it is not enough only to apply general principles in order to ensure an application's compliance with the law. Instead, the relevant legal regulations for the particular field of application should be specifically identified and the application should then be designed in such a way as to meet their requirements. When the context of the application is not known in advance, it is seldom possible to ensure legal compliance.

However, legislation such as the Federal Data Protection Act, the data protection laws of Germany's individual federal states and the relevant media laws does contain certain general requirements for the design of technological systems, particularly with regard to data reduction, data economy and *transparency*, and these should be taken into account in system design. These general technology design requirements – as well as other basic values that are enshrined in the legislation – have influenced the discussion of special *data protection* or, to use the wider term, *privacy protection goals* that should be employed in the development and operation of IT systems.

For several decades, the field of information *security* has used the three *protection goals* of *confidentiality, integrity* and *availability*. Some years ago, three *specific privacy protection goals* were added: *transparency, intervenability* and *unlinkability* [RB11, RP09b]; see also Chapter 5.2.4.

Just like the *security* protection goals, a *privacy protection goal* establishes a basic requirement for a system such as an IT system. However, these requirements only need to be met up to a certain point. Implementing *protection goals* is often either not possible or would involve disproportionate expense. A standard approach is taken to implementing *protection goals*. Firstly, the need to protect the system and the processed data is determined based on the type and degree of damage that could result from failure to meet the *protection goal*. For *IT security*, state-of-the-art protection measures are listed, for example, in the German Federal Office for Information Security's IT baseline protection catalogues. However, since *privacy protection* goals are still a relatively recent phenomenon, there are not currently any definitive catalogues with lists of measures, although many measures can be found in the specialist literature. When selecting appropriate measures, the results of a risk analysis should also be incorporated.

The aspects addressed by the *protection goals* for Cyber-Physical Systems should include

- the individual components and the overall system made up of these components,

[51] "Access to consumer credit, both in volume and number, is negatively related to the racial composition of an individual's neighborhood." [CC08].

- the data that the system will generate or process during its entire lifetime,
- the data processing processes and
- the context, for example the spatial environment, the situation regarding voluntary use, and incorporation into a *business model*, for example with regard to billing.

This list derived from the six *protection goals* for *security* and *privacy* can be used both for assessing the impact of the technology and for making specific design choices when developing Cyber-Physical Systems and drawing up measures during their operation; see also Chapter 5.2.4.

Transparency

When referring to a system, *transparency* means that the way the system works and the effects it has should at all times be sufficiently easy to understand for its operators and the people affected by it. This includes information regarding the full life cycle of the data, from creation to deletion: which *services* are provided, which *sensors* and *actuators* are installed, where they are installed and how they are activated, which data are captured, who captures them, where they are transferred to, how they are processed, who processes them, what purpose they are analysed for, and finally, when, how and by whom they are deleted. The decisions or actions prepared or carried out by a Cyber-Physical System must also be transparent, in other words they must be predictable and understandable for the person concerned. This includes making the economic interests of the different actors visible, for example, when route planning systems guide a driver past certain shops in exchange for advertising payments.

On the other hand, *transparency* in the context of Cyber-Physical Systems does not mean that the huge volumes of data flowing between sensors, actuators and other components and the information resulting from the analysis of this data should always be communicated to everyone involved. Instead, it is necessary to enable automatic selection of the required degree of detail; see Chapter 3.3.

Intervenability

Intervenability means that rather than being powerless to influence a system, the actors should have the ability to intervene on their own initiative as and when they deem it necessary to do so.

At all times and whatever their location, the actors can independently determine the extent to which they are observed by Cyber-Physical Systems and the extent to which the systems may process any data pertaining to them. This can include the ability to intervene in the systems and, at least temporarily, deactivate those functions that affect them personally. For example, it might be desirable for actors to be able to compare and switch between personalised and non-personalised Cyber-Physical System usage modes. To reduce the complexity of such systems, the actors are often offered fewer decision-taking options in the case of personalised use, meaning that non-personalised use can provide them with greater scope for decision-taking.

It is also important to prevent user lock-in. The actors must be able to remove their data from a Cyber-Physical System and switch to alternative systems if they so wish. One current draft of the EU data protection regulation does in fact provide for this right to "portability" of *personal data* [Lük11].

Even for system operators, *intervenability* is an important requirement for controlling Cyber-Physical Systems. Every process and every component must operate in a controlled manner which the operator can influence and interrupt if necessary.

Unlinkability

Unlinkability refers to a data management requirement that calls for the separation of data and processes from different contexts. As far as possible, data should not be generated at all unless it is required – data avoidance is a necessary corollary to the protection goal of *unlinkability*. The aim is to prevent the risks connected with the accumulation of data that can be analysed in a variety of different ways and to restrict the purposes for which such data may be evaluated. *Unlinkability* also means that data from separate contexts should be kept separate and not processed as a single data chain. This can be achieved, for example, by keeping separate databases and avoiding the use of identical reference numbers or identifiers, i.e. unique data set identifiers such as telephone numbers. In addition, there should be a guarantee that data will only be used for its intended purpose – every time that data is captured, the purpose of so doing should be specified in advance and the data should then only be processed and analysed for the purpose for which it has been collected. Finally, the data should be deleted as soon as it is no longer required.

There are plenty of measures that can be taken to deliver *unlinkability* (see also Chapter 5.2.4), but many are limited in their effectiveness. Even if identifiers are continuously changed for different contexts, a third party can still link the data by monitoring the behaviour of the people who interest them in a different way. Moreover, in order to ensure the *transparency* of Cyber-Physical Systems, the actors are supposed to be provided with as consistent a picture as possible, and this is achieved by linking all the information that concerns them. The result is that *smart devices* can often accumulate a large amount of data about them.

If privacy protection goals are contravened or inadequately implemented, this generates social tensions that go well beyond traditional *data protection* issues. For example, automatic actions or decisions executed by Cyber-Physical Systems cannot be reversed if there is insufficient *intervenability*. Without *transparency*, the systems will be rejected by large sections of the public and it will not be possible to resolve the issue of liability. Without a ban on data linking, it can be expected that – partly for administrative reasons – the linking and fusion of partial identities will become increasingly common, resulting in a concentration of power.

The six *protection goals* are also useful for identifying conflicts in the areas where tensions exist, so that it is possible to work out a compromise. Thus, for example, the goals of *confidentiality* and *unlinkability* might be at odds with the goal of *transparency* because they make processes more difficult to follow.

4.2.4 CONCLUSIONS

The principle of *privacy by design* should be adhered to in the design of Cyber-Physical Systems. As far as possible, legal *data protection* requirements should be met from the very outset – in other words from the point when the technological systems, organisational procedures and *business models* are first conceived and designed. Of course, at the initial design stage it is not always possible to determine precisely which legal regulations will apply when the system is eventually deployed and it is also important to remember that the legal regulations are likely to be updated. It is therefore advisable to use the general *privacy protection goals* of *transparency, intervenability* and *unlinkability* as the starting point for designing a system.

Whereas there are already extensive lists of measures for achieving the familiar *security protection* goals of *confidentiality, integrity* and availability, measures for delivering the *privacy protection goals* are not yet part of the standard toolkit for developing, designing and operating IT systems. There is an urgent need to develop measures and to identify the interactions and possible tensions between the different *protection goals* or the measures taken to implement them. In the context of Cyber-Physical Systems, techniques for enabling *unlinkability* offer particular potential to significantly reduce the risk of data misuse – but it is difficult to bolt these on to existing systems retrospectively.

In the national and European context, there is a need – perhaps as part of a legal study or an ancillary interdisciplinary research project similar to a technology impact assessment – to verify the extent to which current legislation is sufficient to achieve an adequate level of *privacy* protection. Where this is found not to be the case, the legislative shortcomings should be identified, together with those aspects where appropriate self-regulation should be supported.

A legal or interdisciplinary study could, for example, examine the extent to which it should be permitted to accumulate linkable data in Cyber-Physical Systems, under which circumstances the informed and voluntary consent of the actors should be obtained, how the responsibility for *data protection* should be distributed amongst the operators of different interacting CPS components, how this can be communicated in an easily understood manner to the people affected and how to enable the actors to exercise their right to self-determination as comfortably, effectively and efficiently as possible – potentially also with the aid of tools or the support of the relevant organisations. This should include an investigation of the extent to which people are prepared to delegate their decisions to devices or agents and do without detailed information about how the systems function.

Methods should be developed for internal or external auditors and – at least to some extent – those affected by CPS to assess their compliance with *privacy* and *security* criteria. It will also be important to identify *best practices*, to define the state of the art as a basis for *privacy by design*, and to come up with compulsory default system settings that promote *privacy* protection, thereby complying with the principle of *privacy by default.*

5 TECHNOLOGICAL AND ENGINEERING CHALLENGES

This chapter will describe the wide range of technologies and *engineering* procedures that will be required to realise Cyber-Physical Systems. Particular attention will be paid to technologies that make a concrete contribution to investigating and enabling the specific capabilities and features of Cyber-Physical Systems and to their incorporation into interdisciplinary design and development processes.

Section 5.1 looks at some of the Cyber-Physical System technologies that already exist today. In addition to describing the different technologies and how they contribute to Cyber-Physical Systems, a brief analysis is also provided of their shortcomings in terms of the widespread realisation of the relevant CPS capabilities.

Technology will also be required to meet the key non-functional requirements of Cyber-Physical Systems and guarantee their quality. In particular, these technologies address requirements pertaining to *Quality in Use, functional safety, IT security* and *privacy protection*. Sections 5.2 and 5.3 describe the necessary technologies and discuss the *engineering* challenges associated with identifying, stipulating and guaranteeing these non-functional requirements.

Smart infrastructure and *CPS platforms* are essential to the realisation of Cyber-Physical Systems (see 3.1). Appendix B describes the key tasks and services of *CPS platforms* and *middleware*. The open, socio-technical and evolutionary nature of Cyber-Physical Systems poses major challenges with regard to their *engineering*, design and management. Section 5.3 summarises these *engineering* challenges together with the necessary integrated modelling and architecture concepts and complex system and quality management tasks. The global *human-machine interaction* and *human-system cooperation dimensions are also addressed*.

5.1 TECHNOLOGIES REQUIRED TO REALISE THE SPECIFIC CAPABILITIES OF CYBER-PHYSICAL SYSTEMS

A wide variety of different technologies will be needed in order to deliver the full range of novel capabilities that Cyber-Physical Systems have to offer (see also Chapters 2.6 and 3). The methods needed to implement some individual capabilities do not yet exist or still require further research. It is therefore impossible to provide detailed descriptions of all the necessary technologies. This chapter will describe the technologies and functional technology groups that we believe can help deliver the new CPS capabilities based on our current knowledge. We have divided them into seven fields (F1 – 7):

- **F1 – Physical awareness:** the ability to detect and recognise objects and the physical environment (*physical awareness*) is a key capability of Cyber-Physical Systems. In particular, it provides the basis for the subsequent analysis of application situations, including all of the technological and human actors involved and their condition, goals and options *("X"-awareness)*.
  Technologies: *sensor fusion* (T1), *pattern recognition* (T2), situation maps (T3)

- **F2 – Fully or semi-autonomous behaviour with the ability to plan ahead and predict the future:** Cyber-Physical Systems are able to act fully or semi-autonomously in order to fulfil goals that would typically either be set by their users or arise from their current situation. The technologies in this field are relevant to capabilities 1 – 5 described in Chapter 2.6 as well as to *"X"-awareness* and contextadaptive and cooperative behaviour.
  Technologies: *multi-criteria situation assessment* (T4), *artificial intelligence* (T5)

- **F3 – Cooperation and negotiation:** Cyber-Physical Systems cooperate with each other in order to accomplish their goals. This is witnessed both in the integration of new *services* into existing Cyber-Physical Systems and in the cooperative detection, evaluation and coordination of situations and agreement of negotiation strategies. Technologies with the ability to do this support the cooperative behaviour and *"X"-awareness capabilities.*
  Technology: *multi-agent systems* (T6)

- **F4 – Human-machine interaction:** Some of the major benefits offered by Cyber-Physical Systems lie in their ability to support the actions and intentions of human beings and perform tasks on their behalf. At the same time, they also take some decisions and perform some actions autonomously and therefore exert an influence over human behaviour and social processes. Although these capabilities offer significant benefits, there is still a huge amount of work to be done to fully master acceptable ways of enabling *human-machine interaction*. Field F4 describes existing and promising future *human-machine interaction technologies that will be required to enable* "human awareness" and *adaptation*.
  Technologies: *human-machine interfaces* and *interaction modalities* (T7) intention and *plan recognition* (T8), *user* and *human modelling*, human awareness (T9)

- **F5 – Learning:** Cyber-Physical Systems adapt their behaviour and the way they cooperate to the requirements of their current context; see the characteristic capabilities described under point 3 in Chapter 2.6. One key enabler of this capability is the ability to build up knowledge, for example with regard to particular situations and the behaviour of human beings or based on experience from previous applications and interactions with different contexts. Technologies from the field of *machine learning* could potentially be used to support the CPS capabilities of learning and *adaptation*.
  Technologies: *machine learning* and *data mining* (T10)

- **F6 – Evolution:** self-organisation and adaptation strategies. This field encompasses existing technologies that enable *self-organisation* in communication networks and manufacturing.
  Technologies: *self-organisation* in manufacturing (T11), *self-organising* communication networks (T12)

- **F7 – Basic technologies:** This field encompasses the basic technologies needed to implement Cyber-Physical Systems. In particular, these include *sensor* and *actuator* technologies, communication networks, efficient processors, distributed controllers and the *domain models* and *ontologies* that are especially important for *situation awareness* and adequate behaviour control.
  Technologies: *Domain models, ontologies* and *domain-specific languages* (T13), *sensor* and *actuator* technology (T14), *communication infrastructure* and *platforms* (T15), efficient parallel processors (T16), stable distributed controllers (T17)

Several unresolved questions also remain in the technology fields of embedded systems and communication and Internet technology, both of which are also relevant to Cyber-Physical Systems. For more on these topics, readers should refer to the relevant studies ([ABB+09, ART11, BIT08, BMW09a, BMW10a]).

5.1.1 F1: PHYSICAL AWARENESS

In order to analyse and interpret different situations and contexts, it is first of all necessary to recognise the environment (detection of real-world objects, or *physical awareness)*. Current technologies that can help to achieve this include *sensor fusion, pattern recognition* and *situation recognition* via situation maps.

5.1.1.1 T1 – Sensor fusion

Sensor fusion refers to the fusion of data from several different *sensors* in order to obtain more accurate measurements or higher-order data. *Sensor fusion* is used to detect and correct erroneous measurements made by individual *sensors*, as well as to make inferences about the system status that are only possible using several *sensors*.

Sensor fusion may be used for a variety of reasons. It is crucial for *safety-critical* systems to use several redundant *sensors* to prevent inaccurate measurements from causing incorrect decisions to be taken. In order to keep costs down, it is common practice to use several cheap but less reliable *sensors* instead of individual sensors that are more *reliable* but also more expensive.

Furthermore, in complex systems it is often simply not possible to capture the necessary information directly. Instead, it has to be deduced based on the data provided by a variety of different *sensors*. For example, how does a system decide whether or not a car driver is changing lanes intentionally? This information can only be obtained by using several different *sensors*, i.e. indicators, proximity *sensors* that detect the distance between the car and other vehicles, cameras and of course the user's own observations.

According to one study [Rab08], by 2017 there will be one thousand *sensors* for every person on the planet. For systems engineering, economic and environmental reasons, it makes sense to try and combine existing and future sensors into global *sensor* networks as soon as possible rather than simply using them in isolation in order to perform individual functions. This raises questions with regard to the trustworthiness of the *sensor* data, the specific features of the sensors and how to ensure that the decisions taken by Cyber-Physical Systems are correct.

5.1.1.2 T2 – Pattern recognition

Pattern recognition [Web02a] is an IT discipline with a strong engineering component that involves the use of algorithms and systems to recognise patterns in incoming data, compare them against known patterns and assign the detected patterns to different categories. One example would be when a front-mounted camera on a vehicle detects a person, enabling the driver to be warned and an accident to be prevented.

Pattern recognition technology is essential for registering certain situations in the physical world, since it provides the ability to extract meaning from unordered data sets (measurements), thus creating the basis for a full assessment of the situation – see T4 *multi-criteria situation assessment* and T5 *artificial intelligence.*

Tried-and-tested algorithms already exist in many areas of *pattern recognition* such as *cluster analysis,* classification, regression and sequential analysis. Algorithms from the related field of computer vision are used for processing static and moving images. The most widely established approach involves data-driven methods that use statistical models.

A number of problems remain to be solved when using this technology in complex environments. For example, at any given point in time, there are thousands upon thousands of mathematically high-dimensional measurements. However, in order to perform the current task, it is usually only necessary to analyse up to a hundred of the most significant dimensions. In order to select the right ones, algorithms are needed that are capable of solving the feature selection problem. In practice, many of these *pattern recognition* algorithms still need to be calibrated by experts in order for them to successfully perform the desired task. However, this is not a realistic proposition when it comes to the huge variety of different tasks performed by Cyber-Physical Systems. It is therefore necessary to develop self-calibrating procedures.

Another issue is that the patterns being recognised tend to drift over longer operating periods. How to recognise this drift is a problem that has yet to be solved.

5.1.1.3 T3 – Situation recognition using situation maps

The information about physical reality provided by *sensors* (T14) and *pattern recognition* algorithms (T2) is combined to create a "mental map" of the physical situation. Detected objects and subjects are recorded on this dynamic situation map at different points in time.

These maps enable the system to detect, respond to and plan for different situations. When approaching a junction, for example, the driver assistance system needs to know the number and exact position of all the other cars and pedestrians in the vicinity. The first attempts at employing situation maps have already been made in the field of autonomous robots.

A number of technological challenges have yet to be solved. One problem concerns object classification over time which is currently performed using multi-instance filtering approaches. One elegant approach might involve the use of Finite Set Statistics (FISST [Mah03]) which also addresses the categorisation problem (see T2 *pattern recognition*). However, the high cost of FISST means that it is not easy to implement and it currently only exists in the shape of approximations. The subsequent development of the situation can be projected using predictive models for physical objects such as *Kalman filters.*

Another unresolved issue is the fusion of data from distributed *sensors* for large and partially hidden objects (see T1 *sensor fusion*). Maps also need to merge data at a semantic level. In doing so, they have to take into account the varying *reliability* and accuracy of the different *sensors* and *pattern recognition* algorithms [Thi10].

5.1.2 F2: FULLY OR SEMI-AUTONOMOUSLY PLANNED AND FORSIGHTED ACTING

Based on the situation that they have detected (F1) and the user's goals (see T8 *intention and plan recognition*), Cyber-Physical Systems are able to develop strategies for delivering these goals and implement them fully or semi-autonomously. One technology that is already available today is *multi-criteria situation assessment*. However, the key technology will involve *artificial intelligence* procedures and approaches for decision-taking, planning and forecasting. The challenge is how to address goals that may be either unclear or contradictory. Any autonomous behaviour should thus always be accompanied by an assessment of its impact on society (see Chapter 6).

F7 deals with *domain models* which are a key requirement for any kind of planning or predictive behaviour.

5.1.2.1 T4 – Multi-criteria situation assessment

For Cyber-Physical Systems to be able to take fully or semi-autonomous decisions, the current situation needs to be analysed, interpreted and assessed based on a variety of criteria. All of this needs to be done in *real time*, using the currently available information. Data describing the physical situation – see F1 *situation recognition* – are combined with *domain models* (see F7) that model the various contexts and options. In complex situations, the systems have to perform numerous analyses and assessments of the actors (i.e. human beings and objects in general), their characteristics and current behaviour, and the different ways in which the situation might develop, i.e. the potential changes in the actors' actions and behaviour strategies. In the *smart mobility* scenario, for example, if a Cyber-Physical System's sensors detect a school bus, the immediate vicinity is scanned for children and their potential behaviour is analysed – are they walking slowly and safely along the pavement or are they playing with a ball?

Each scenario needs to be assessed from various different viewpoints that are relevant to the decision-taking process. It is possible that some goals may contradict each other, for example it may be necessary to weigh up the driver's safety against that of a child who has run out into the street.

One important challenge is to enable assessments to be made in *real time* so that actions can be triggered sufficiently rapidly. The processing speed of the relevant devices undoubtedly plays a role in this regard (see T16 efficient parallel processors). However, aggregated information is not always immediately available, for example it may first of all be necessary to calculate the situation map for an entire road junction. Moreover, it should also be possible to make an assessment based on uncertain information. In such cases, however, the uncertainty has to be quantified in terms of its suitability for use as the basis of a decision. A similar situation arises if the *sensors* providing the data are not all equally reliable.

One possible solution in restricted *domains* could be the development of situation-specific schemas that establish the priority to be attributed to different foreseeable factors and goals.

5.1.2.2 T5 – Artificial intelligence approaches

Artificial intelligence (AI) [RN09] is a branch of information technology concerned with the automation of smart behaviour. AI technology is needed to enable Cyber-Physical Systems to respond intelligently to their environment, pursue goals on behalf of their users and cooperate with other systems in order to do so. Examples from the scenarios in Chapter 2 include automated planning of the production of a new kitchen and the rerouting of a journey.

AI is able to take decisions by obtaining input data about the environment and using *deductive mechanisms* to draw conclusions from this data. This requires extensive formal rule systems for the different knowledge *domains* (see T13 *domain models*) which it is currently not yet possible to produce for complex situations involving unknown actors.

The uncertain knowledge that occurs in Cyber-Physical Systems for example as a result of unreliable sensors or the use of external *services* is managed using *Bayesian networks* that compare the different knowledge that is available in order to produce an overall probability distribution. The *Dempster-Shafer* theory of evidence can be employed for explicit uncertainty modelling. It enables information from different sources to be combined in order to arrive at an overall conclusion, taking into account the credibility of the different pieces of evidence.

The information gathered about a system's surroundings can be used to compute what it should do next using planning strategies. The best-known example of this approach is the Stanford Research Institute Problem Solver (STRIPS) [FN71].

Planning has also started to be used in robotics since the development of planning algorithms [PB03] that are capable of handling uncertainty and the introduction of the corresponding description languages [GMP+06] that act as an intermediate layer between high- and low-level components in embedded systems. If a plan encounters obstacles to its execution such as the unavailability of a particular component in a manufacturing context, "plan-repair" algorithms can be used to compute alternative courses of action. The distributed, cooperative formulation of plans constitutes a significant challenge.

The strength of neural networks is their ability to handle large volumes of data and to tolerate imprecise requests, e.g. thanks to the use of content-addressable memory. They thus have considerable potential in the field of CPS.

Artificial intelligence uses *multi-agent systems* (see T6) to model cooperative behaviour.

Pattern recognition (T2) and *machine learning* (T10) technology is thematically closely related to AI.

5.1.3 F3: COOPERATION AND NEGOTIATION

The ability to cooperate and negotiate enables Cyber-Physical Systems to provide distributed services and formulate problem-solving strategies in a distributed and coordinated manner and in *real time*. The goal is to enable coordinated collective behaviour. The necessary technologies are primarily to be found in the field of *multi-agent systems*. One key requirement in this area is subsystem *interoperability* both at a *technological* level (i.e. in terms of communication interfaces and protocols) and at a *semantic* and *user-visible* level (i.e. *interoperability* with regard to the meaning of data); see T13 *ontologies*.

5.1.3.1 T6 – Multi-agent systems

Agents are one of the key paradigms in *artificial intelligence*. An autonomous *agent* is a piece of software that acts independently in its environment in order to perform tasks on behalf of human beings. In *multi-agent systems,* several *agents* cooperate and negotiate with each other. Agents are able to interact with their environment through *sensors* and *actuators*. Smart *agents* are capable of task-oriented problem solving thanks to the autonomous, responsive and targeted use of the appropriate *artificial intelligence* (see T5) methods.

An example of the use of this technology is provided by Frau Müller's *assistant* in the mobility scenario in Chapter 2.

Her *agent* plans her day for her in accordance with her instructions and in doing so coordinates with calendar *agents* belonging to other users. When her travel plans have to be changed, the *agent* negotiates the cost with infrastructure *agents* and comes up with alternative routes. In the manufacturing environment [MVK06], it is possible to respond to faults locally without the need for intervention from a centralised control system. The individual units negotiate the optimal distribution of resources among themselves.

By employing large numbers of *software agents* it is possible to simulate the interactions between several networked actors [KNR+11]. This enables group behaviour to be predicted, allowing traffic flow and congestion forecasts to be made, for example.

Planners are used to come up with ways of achieving the relevant goals (see T5 above). Communication between *agents* is based on a shared vocabulary (see T13 *ontologies*).

Interactions between *agents* are complicated by the fact that each *agent* pursues its own goals. In other words, individual *agents* behave "selfishly" and lack an overview of the system as a whole. It would thus be desirable to employ criteria such as pareto-efficiency – a state in which it is impossible to make any one actor better off without making another actor worse off at the same time – and to focus on the good of the overall system (social welfare). One of the main research topics in the field of *multi-agent systems* is therefore the search for ways of interacting and rule systems that are fair to all the relevant stakeholders. The approaches that have been adopted are based on game theory [Osb03] and include concepts such as Nash equilibrium, where no player can gain anything by changing their own strategy unilaterally. The techniques employed include voting, auctions and coalitions. "General game playing" seeks to put the rules of different games into a common machine-readable language.

One of the challenges associated with *multi-agent systems* is the issue of *shared control*. Users must be able to decide how much *autonomy* they are prepared to allow their *agents*. Moreover, they must be capable of intervening at any time and understanding the decisions that have been taken.

The phenomenon of distribution is of fundamental importance to Cyber-Physical Systems. Centralised communication methods such as *blackboards* are no longer sufficient. Moreover, when several actors are involved, existing negotiation rules soon become too complex, even in purely computational terms.

In contexts characterised by open cooperation between several different partners, it becomes more difficult to prevent *agents*' decision-taking processes from being manipulated. Combined technological and economic measures are needed to address this issue [Wei00]. This includes the development of interaction rules that allow *agents* to act in their own interests while at the same time maximising the benefits for the system as a whole and maintaining its stability; see also [Woo09].

5.1.4 F4: HUMAN-MACHINE INTERACTION

In order for Cyber-Physical Systems to provide users with optimal support, new solutions will be required in the field of *human-machine interaction*. This applies to the interfaces for interactions between humans and technological systems, which will need to provide *multimodal, real-time support* for complex interactions and enable the current system status, situation and options to be conveyed in a manner that is appropriate to the current situation. In addition, it will be necessary for Cyber-Physical Systems to recognise users' intentions – in a similar way to the predictive *situation awareness* described in F2 – and anticipate human behaviour. Current technologies that could make a contribution in this regard can be found in the fields of *human-machine interfaces, intention recognition* and *user* and *human modelling*.

Other relevant technologies include *multi-criteria situation assessment* (see T4) and *machine learning* (see T10). Appropriate environment and *domain models* (see T13) also have a key role to play in this area.

5.1.4.1 T7 – Human-machine interface and interaction modalities

Interactions between humans and Cyber-Physical Systems are not confined to a single *modality* such as a keyboard. Systems may be accessed via any number of *modalities*, e.g. touch screens, voice commands or body language. For example, in the mobility scenario described in Chapter 2, when Frau Müller is asked whether she wishes to change over to the chargeable *premium lane*, she can respond with a simple nod of her head.

However, this requires the interaction logic that determines the rules governing the interaction – e.g. the number and sequence of input options – to be *modality-independent*. In other words, the logic and presentation layers need to be separate from each other.

In addition, the user interface needs to adjust to the relevant *modality* by taking into account the quantity of information and options it can display. This is an important consideration, since if a system is being operated using voice technology, for example, it is not able to present the user with the same number of options as could be displayed on a screen.

Limiting the number of options available to the user – see also F2 planning behaviour – also prevents them from feeling overwhelmed and makes them feel that they are in control of the system because they understand all of the options that they are being presented with (see also T8 *intention recognition*).

When designing interactions, it is also undoubtedly necessary to ensure behaviour patterns that are perceived as natural by the user. One model that developers might use to address this goal is the *user-centred design* process described in ISO 9241-210. However, the *model* is currently still only geared towards individual products or programs and, together with other approaches to *usability* *engineering*, it therefore needs to be expanded to include distributed networks of *services* and interaction points.

The distributed nature of Cyber-Physical Systems entails the additional challenge of having to ensure that *services* provided by different suppliers are all operated in the same way. For example, when Frau Müller switches cars, the new vehicle must also interpret her raised hand as a stop command.

The interaction *modalities* themselves have undergone rapid development in recent years. Mass-market gesture and body language interaction technologies such as Microsoft's Kinect[52] control module are now available for simple applications. Controllers that are integrated into people's everyday living environments, such as *information tables,* are currently being researched under the collective name of "tangible user interfaces" and in some cases are already being marketed. In addition to ensuring the ability to interpret non-standard ways of using them – for example if the user employs unfamiliar hand movements – and the development of new *modalities*, these technologies need to be robustly designed and capable of being used in the entire range of typical everyday situations, as occurred in the case of the iPhone.

Configuring technological systems is an expensive process that requires a lot of technical know-how and experience [Nor96]. This knowledge remains inside the heads of the relevant experts and is thus not available to others. In order to ensure that this situation does not occur with Cyber-Physical Systems, optimised parameter sets should be stored as *best practice* applications and made available to other users.

5.1.4.2 T8 – Intention and plan recognition

Intention recognition is the ability to recognise the intentions of an *agent* (in this section, the term "agent" refers to a human being or a technological system) by analysing their previous behaviour or the effect of this behaviour on the environment. *Plan recognition* goes one step further than *intention recognition* by using an agent's past behaviour to predict its future behaviour. Both of these capabilities are extremely important to Cyber-Physical Systems in order to provide users with as optimal and autonomous a level of support as possible for accomplishing their goals without necessarily requiring them to provide a detailed description of these goals via the *human-machine interface* (T7).

Research into intention recognition has been ongoing for more than thirty years [Sad11]. Significant progress has been made thanks to the use of logic- and probability-based methods. Nevertheless, new applications such as those enabled by Cyber-Physical Systems are throwing up new challenges, especially the selection of the correct intention hypothesis, how to address the issue of limited agent observability, the analysis and classification of interconnected actions where the agent has several different intentions at the same time and the recognition and classification of alternative behaviour outcomes for achieving the same goal. Furthermore, *intention recognition* for cooperating agents whose behaviour is restricted – such as people with disabilities – is currently still in its infancy.

In addition to the above technologies, *user* and *human modelling* (T9), *machine learning* (F5) and *domain models* (T13) also play an important role in intention and plan recognition.

5.1.4.3 T9 – User and human modelling, human awareness

User and *human modelling* enables the diagnosis, simulation, prediction and support of human behaviour in interactions with technological systems. Current research is focused on two applications: the "virtual test driver" and the "empathic virtual passenger".

Virtual test drivers involve *models* that assess the *safety* of different technological system designs. *Models* are linked

[52] See also the applied research in the field of *AAL* [SS11] and the support "[...] for young adults with motor disabilities" [Hua11].

to formal system designs so that large numbers of potential application scenarios can be analysed via *co-simulation*.

Current research initiatives are also attempting to apply insights from cognitive psychology and *anthropometry* to the realm of systems engineering. The aims of this approach include predicting the effect of a new system on the user's attentiveness, potential operating errors and how comfortable to use, physically accessible and easily recognised different controls are.

In CPS-based uses, *models* are employed as empathic virtual passengers in smart assistance systems in order to diagnose users' current motivation and the degree of strain that they are experiencing. This allows them to provide the user with targeted assistance for performing particular tasks, thereby offering context-sensitive support for human-machine interactions. For their input, these *models* use e.g. user behaviour (as described in T8 *intention recognition*) in conjunction with psychophysiological measurements such as eye movements, skin conductance and blinking frequency, in order to assess conditions such as stress, distraction or vigilance.

There are various technical approaches for creating *user* and *human models*, including rule-based production systems, *Bayesian networks*, mathematical control theory, Markov decision processes and various combinations of these methods.

Future research priorities include modelling and prediction of the relevant characteristics of human behaviour in interactions with *multimodal human-machine interfaces*, the integration of cognitive and *anthropometric models* and thorough *model validation*. Moreover, research is also required into the integration of the *models* into the planning of Cyber-Physical Systems' behaviour; see F2 *situation awareness*. Another major challenge concerns the definition of formal semantics for the resulting *models* and their semantic integration with formal system designs. For example, if a *human model* uses a particular definition of the word "eye", it is important to ensure that the whole system knows that this is the definition being used; see T13 *ontologies*.

5.1.5 F5: LEARNING

Adaptive Cyber-Physical Systems adapt to their users and to new situations. In other words, they learn what the user is trying to achieve in a given situation (see T8 *intention recognition*) and how they wish to operate the system (see F4 *human-machine interaction*) and they adapt to the user's language. The planning components of Cyber-Physical Systems learn which behaviours and plans succeed in specific situations and share this knowledge with each other. Moreover, machine learning methods use the large volumes of data obtained from *sensors* and cooperating systems to answer specific questions or generate new knowledge. As things currently stand, delivering this capability will require *machine learning, data mining* and *multi-agent system* technologies in addition to the technologies already referred to in F4 and F1.

5.1.5.1 T10 – Machine learning and data mining

Machine learning [Bis07] involves the use of information technology and mathematical theory to enable computers to extract knowledge from the available data. This may be done in order to find the answer to a specific question ("what does a typical traffic jam look like?") or, in the field of *data mining*, to generate completely new knowledge.

These algorithms are necessary in order to enable the data provided by Cyber-Physical Systems to be turned into something that can be used. In the field of mechanical engineering, these procedures can be used to configure the entire manufacturing process as a self-optimising system where the *Manufacturing Execution System*

(MES) identifies the optimal process parameters based on its own historical data sets [BKS11, p. 65]. In the field of healthcare, a system that has learned what the user's normal ECG readings are can alert them to any anomalous values. *Reinforcement learning* allows systems to process feedback on the success of their actions, creating a feedback loop that enables them to constantly improve the way that they adapt to the current situation and similar situations in the future.

Challenges exist with regard to the fact that many algorithms are not yet designed to handle the huge volumes of data involved. Furthermore, the relevant data are scattered across several distributed database systems. The solutions being developed include online learning procedures and *multiple classifier systems* [MCS11] that collate the knowledge from several different algorithms. Research in the field of *multiagent systems* (see T6) is investigating algorithms designed to enable distributed learning.

The majority of data do not have labels that describe what can be observed in the current measurements. Research into *partially- and semi-supervised learning* is developing ways of getting by with only a limited number of labels.

Current algorithms are not able to solve the problem if the things being searched for are unknown or poorly defined.

5.1.6 F6: EVOLUTION: SELFORGANISATION AND ADAPTATION STRATEGIES

Self-organisation and *adaptation* strategies are necessary to enable cooperation and context-adaptive, fully or semi-autonomous behaviour. Currently, this type of technology is found mainly in the realms of manufacturing, communication networks and *multi-agent systems.*

5.1.6.1 T11 – Self-organisation in manufacturing

In the realm of manufacturing, this principle has been investigated since the end of the 1990s [BS00, SB01] and is underpinned by the fundamental idea of individually identifiable workpieces that move independently through the manufacturing process, from component manufacture through to assembly. Flexible machine tools and assembly lines know what they are capable of producing and adapt independently to different tasks.

The workpieces, machinery and transport systems organise manufacturing operations locally and independently. They take the current status of production into account at all times, for example machinery failures or supply problems.

This requires products, production units and processes, their controllers and the MES functions (see 2.5) – all of which are represented by Cyber-Physical Systems – to be capable of synchronising with each other in a coherent manner. A substantial research effort will be necessary in order to develop methods, tools and software components and to enable standardisation.

Semantic interoperability will be a key requirement if these plug-and-work mechanisms are to be effective. More research is still needed in this area; see the initiatives described in [SMS11] and F3.

5.1.6.2 T6' – Multi-agent systems

As described under T6, multi-agent systems comprise independent *software agents* that pursue their own individual goals and cooperate with other *agents* and *services* in order to accomplish them. The resulting interactions give rise to a *self-organising* overall system [BCHM06] that is even capable of independently regulating access to limited resources as long as the appropriate interaction rules have been formulated.

5.1.6.3 T12 – Self-organising communication networks

CPS communication networks need to be flexible in order to guarantee trouble-free and *reliable* operation in the face of constantly changing environments and requirements.

In addition to enhancement of the existing infrastructure with technologies for addressing mobile users, additional technologies will also be required that enable network users to create *secure* communication networks among each other and operate them cooperatively so that they can exchange data. Moreover, they will have to be able to do this on an ad hoc basis, i.e. at run-time and without explicit planning and configuration. This will require technologies that enable distributed administration, configuration, control and operation, as well as the establishment of mechanisms to ensure that the cost is shared fairly among all the partners.

Given the specific quality requirements for this type of communication (see 5.2), the existing technology is unlikely to be sufficient and current approaches will need to be adapted [SAL+03]. There are a number of relevant research initiatives in the field of ad-hoc sensor networks [WS10] which are investigating proactive and reactive communication path routing protocols. The proactive protocols include the Highly Dynamic Destination-Sequenced Distance Vector Routing Protocol, whilst the reactive ones include the Ad hoc on-Demand Distance Vector. Standardisation is a key enabler of *ad-hoc communication,* since devices that have not previously worked together need a common language.

5.1.7 F7: BASIC TECHNOLOGIES

Situation awareness, planning and cooperation all require machine-processable *models* of the relevant application domains. These include *ontologies* and *domain-specific languages*.

The other basic CPS technologies include *sensors* and *actuators*, the relevant *communication infrastructure*, and devices capable of processing the large volumes of data captured by the *sensors* in real time. Among other things, this will require computers equipped with multicore processors. Moreover, the need for *real-time* processing means that it will not be possible to process the data centrally. Distributed control will therefore be essential.

5.1.7.1 T13 – Domain models, ontologies and domain-specific languages

In order to enable autonomous situation awareness (F1), planning (F2) and learning (F5), the relevant knowledge in a given application domain must be described in a *domain model.* This formal description enables cooperation between different parts of Cyber-Physical Systems (F3) and makes it possible to achieve a higher degree of *autonomy* with regard to information processing and planning.

Experts compile the relevant concepts in a particular *domain* into standard *ontologies*. These comprise descriptions of the hierarchical relationships between concepts and objects. The knowledge contained in these *ontologies* can then be exchanged – one of the fundamental principles of the *Semantic Web*. The best-known methods of describing *ontologies* are the *Semantic Web's Ontology Web Language* (OWL) and the language of the CYC project in the field of *artificial intelligence* [Len97].

Languages tailored to a particular *domain*, known as domain-specific languages (DSLs), can be used to include additional *domain* knowledge in the *models*. These are formal languages based on ontologies that have their own grammar and contain all the concepts, objects and possible actions for a narrowly-defined *domain*. There are various methods, e.g. the Meta-Object Facility Standard, and tools, e.g. the Meta Programming System [Dmi04], that can be used to develop these languages. Translation into behaviour is carried out by translators that use the information written in DSLs to create programs in a high-level computer language like C. The first attempts at doing this involve mechanisms such as OWL Profiles or Views in the Bio Portal language [RLM+06].

Every *domain* contains specific *ontologies*. For example, a Cyber-Physical System may wish to buy a ticket from a new airline whose own Cyber-Physical Systems do not recognise the term "onward journey". Communication between the two is thus only possible if the terms from the different *ontologies* can be mapped onto each other in a process known as ontology mapping, ontology mediation or ontology alignment [KS03]. This enables knowledge to be exchanged across different *domains*.

There are a number of challenges associated with producing *ontologies*. A precise definition is needed of which concepts can be included and which should be excluded from the *domain*. The translation of DSLs into behaviour can only be achieved through *domain-specific model transformation* approaches, something that very few *domains* have yet attempted.

A problem common to all technologies is that while human beings have an intuitive understanding of fuzzy concepts which can only be partially realised, they constitute a major challenge for modelling.

5.1.7.2 T14 – Sensor and actuator technology

Sensors and *actuators* allow Cyber-Physical Systems to observe and influence their physical environment. *Sensors* record qualitative or quantitative measurements of the environment's physical or chemical properties such as temperature, humidity, sound or the materials it is made of and convert these measurements into a format that can be processed digitally. *Actuators* convert digital values into mechanical movements or other physical parameters such as pressure and temperature, thereby producing an effect on the environment.

The *sensors* that can be deployed in Cyber-Physical Systems range from simple detectors that only measure one particular physical parameter to complex environment *sensors* such as video and radar, bio*sensors* that can be implanted into patients' bodies to record complex health-related processes and *sensor networks* incorporating a large number of often heterogeneous *sensors*. As illustrated by the scenarios in Chapter 2, Cyber-Physical Systems typically register their environment via a wide variety of distributed, heterogeneous sensors. These sensors are therefore fundamental to all of the technologies described in fields F1, F2 and F4.

By the same token, the *actuators* used by Cyber-Physical Systems range from simple, often mechanical controllers in control circuits, e.g. valve trains, to electromechanical and hydraulic drives and complex control systems e.g. for the longitudinal and lateral guidance of vehicles or entire traffic flows via the coordinated interaction of several heterogeneous *actuators* in *actuator* networks.

The challenges in this field (see also [GMA09b, HGZ09, MM06, HSMS07, ABB+09]) include the need to increase sensors' accuracy and speed, since these are currently often not sufficient to enable the detailed r*eal-time physical awareness* required by Cyber-Physical Systems. Furthermore, the fact that *sensors* and *actuators* will be deployed in different and often extremely demanding environments places higher demands on their *robustness* and durability as well as on their size and energy consumption. In the most extreme cases, they may even have to be energy self-sufficient. Recent years have seen the first attempts to build smarter *sensors* by increasing their processing and memory power.

The development and consolidation of this trend will benefit the realisation of Cyber-Physical Systems, since it will enable *services* such as *sensor fusion* (see T1) and object recognition (see T2) to be provided in the outer nodes of the network. Finally, other key requirements for the realisation of Cyber-Physical Systems include the development of completely new kinds of *sensors* such as bio*sensors* or *sensors* for enabling *Brain-Computer Interaction* (see [ABB+09]), together with the enhancement of *energy-efficient* wireless or wired communication. Additional challenges exist with regard to guaranteeing the *functional safety* of *sensors* and *actuators*, as well as scalability, organisation and self-configuring control concepts.

5.1.7.3 T15 – Communication infrastructure and platforms

The availability of Cyber-Physical Systems will have a significant impact on the research and development of large-scale distributed systems in areas such as electric mobility or the *Internet of Energy* and on the necessary *communication infrastructures*. As a result of information and communication technology, computers and the use of hierarchical *communication infrastructures* to network them are becoming increasingly ubiquitous. Personal Area Networks (PANs) based e.g. on the Bluetooth and Zigbee short-range radio standards are used to enable nodes to communicate with each other or with a larger network. Local Area Networks (LANs) use e.g. WiFi to enable nodes and systems to communicate with much higher data rates and over longer distances. Wide Area Networks (WANs) employing 3G, 4G and even 5G mobile communication technology cover much larger areas and enable wired and wireless communication between nodes, systems and *Systems of Systems.*

Cyber-Physical Systems will place a number of new demands on this heterogeneous and hierarchically organised *communication infrastructure* that have as yet been only partially addressed, if at all. The emergence of Cyber-Physical Systems – i.e. the trend towards spontaneous creation of new behavioural traits as a result of the interaction between different components and features – will require equally spontaneous, efficient and effective communication links to be available at both the micro and macro system levels.

Wireless data connections in particular tend to be error-prone and can suffer from latency. The *communication infrastructure* solutions for Cyber-Physical Systems will need to guarantee the most consistent and uniform *service* quality possible for all of the system's components. The CPS *communication infrastructure* data connections are susceptible to blocking, interruption and eavesdropping. In order to ensure that the data being transmitted can always be trusted, optimal data *security* must be guaranteed at the levels of individual nodes, systems and complex networks of systems. Cyber-Physical Systems are characterised by a high level of openness and *adaptability* and the *communication infrastructure* plays a key role in making this possible. In order for communication to work properly at every level, it is necessary to constantly monitor and test the *service* quality of the connections in the system and make automatic adjustments in the event of any changes to the system. Self-organising networks (SON) constitute one possible solution to this challenge.

Cyber-Physical Systems will be deployed in *dynamic real-time* environments. This will require *communication infrastructures* to be analysed, transformed, researched and re-developed in terms of their *robustness*, reconfigurability, *adaptability*, performance and access to the *cloud*.

5.1.7.4 T16 – Efficient parallel processors

Smart devices for Cyber-Physical Systems harbour huge innovation potential. In the future, it will be possible to host even more functions on a single chip, optimise their power consumption and make them even cheaper and smaller. The continued advances in electronic hardware will enable improved performance in the following areas:

- Improved performance and highly parallel architectures. In the future we will continue to see ever better and faster processor cores built onto a single chip (multicore processor approach).

- Additional hardware functions for specialised tasks (multimedia, graphics, video analysis, image processing, *real-time* capability, *security*) will result in chips with dedicated cores for specific tasks.
- I/O processing, including radio receivers, will be even more deeply integrated into the chips. There is still room for further optimisation of chips in terms of their power consumption and heat dissipation.
- New energy harvesting methods will enable the creation of Cyber-Physical Systems without an external power supply.
- Hardware-based virtualisation will enable consolidation of Cyber-Physical Systems on board vehicles, for example, without jeopardising their *real-time* capabilities, *safety and security*, functionality or performance.

Further challenges include the integration of new technologies into development processes, ensuring that the most is made of parallel processing capabilities and guaranteeing *safety* and *security*, for example. The use of multicore processors in *safety-critical* avionics applications is one example that would already be relatively easy to implement from a technical point of view, even today. However, the issue of certification of non-functional properties such as *safety* and *security* remains largely unresolved.

A summary of the challenges involved in the use of multicore processors in embedded systems is provided in the position paper [Arb11] of the Multicore Working Group of the Bavarian *ICT* cluster BICCnet.

5.1.7.5 T17 – Stable distributed controllers

Distributed controllers are control systems or networks whose signal-processing components are geographically dispersed and may even be hierarchically structured, rather than being organised centrally. This allows them to control more complex distributed systems that cannot be controlled centrally (cf. [ABB+09]), and in particular the interventions in the environment required by Cyber-Physical Systems that are based on *sensor* readings and enabled by interactions between distributed subsystems.

The distributed controllers available today are mostly confined to individual systems, e.g. in motor vehicles where individual control systems are integrated in order to provide driving stability – such as ESP and active suspension – as part of an “Integrated Vehicle Dynamics Management” system [ABB+09], or in the location detection and terrain and object recognition systems used by vehicles taking part in the DARPA “Desert and Urban Challenge” [CPS08]. In the case of Cyber-Physical Systems, however, controllers need to be networked across different systems and it is also necessary to be able to build and dismantle these control systems dynamically, e.g. to create ad-hoc control systems for cooperating systems.

Problems can arise as a result of connection failures, signal fluctuations caused by variations in communication latencies (jitter) and packet loss, which typically has a major influence on controller behaviour and can easily result in controller instability. There is therefore a need for control concepts and the associated development and analysis procedures and tools to enable the development of control algorithms that can counteract these effects in a robust, scalable and hierarchical manner and that are *adaptive* or capable of reconfiguring themselves [ABB+09].

One further fundamental problem is that the two disciplines of control engineering and information technology still largely operate separately of each other [CPS08]. Methods from both areas will therefore need to be combined.

5.1.8 SUMMARY OF THE TECHNOLOGIES REQUIRED FOR CYBER-PHYSICAL SYSTEMS

The challenges described above can be summarised as follows:

"X"-awareness is a key property of Cyber-Physical Systems, involving accurate recognition and interpretation of both situation and context (*situation awareness, context awareness*), awareness of the system's own condition and the condition and quality of CPS *services* and components and, importantly, the condition, goals and intentions of the system's users (*human awareness*). This necessitates awareness of the physical, IT and human environments and the ability to use this information to interpret and assess the situation that has been identified in terms of the goals of both the system itself and of other actors. The technologies described under fields F1, F2, F3, F4 and F7 are not currently powerful enough to provide the level of *"X"-awareness* that is required for Cyber-Physical Systems. Whilst the first challenge is to improve *sensor* technology, it will subsequently also be essential to improve awareness of complex situations together with the necessary processing and aggregation – including semantic aggregation – of large volumes of data in *real time. Further challenges will include enabling real-time* analysis and assessment of situations involving several different actors who may have conflicting goals.

Procedures and technologies for combining different perspectives when a situation is perceived and analysed by different actors and for working with uncertain knowledge will be key, as will methods for enabling the system to assess its own situation and capabilities (*self-awareness)*. The challenges with regard to recognition and interpretation of human behaviour and users' wishes, goals and intentions (human awareness) revolve around predicting human behaviour (*intention recognition*) and the design of appropriate *multimodal* interfaces for *human-machine interaction* that enable inputting of higher-order goals via any number of different *modalities* whilst at the same time providing the user with a picture of the situation that takes account of their current attention profile, the system status and the situation itself. The key challenge is to design *human-machine interactions* in a way that enables users to coordinate and control Cyber-Physical Systems as required by their current situation.

One key requirement for comprehensive *"X"-awareness* that has not yet been adequately met is the development and *validation* of appropriate *domain models*, particularly *user models*.

Context-*adaptive*, cooperative behaviour is another key feature of Cyber-Physical Systems. Even once *"X"-awareness* has been achieved, continuous context and process interactions, cooperative goal-oriented behaviour and autonomous and active context-dependent behaviour will require additional technologies, as described in fields F2, F3 and F7. The processing and communication speeds of processors and communication media will be key to the *real-time* capabilities and responsiveness of Cyber-Physical Systems. Technical and semantic *interoperability* will be equally essential. There are also a number of major challenges at the application level that are only partly addressed by current technology. These include *domain models* geared towards complex environments, the ability to pursue numerous competing goals, working with uncertain knowledge, negotiation strategies, *shared control* and fair interaction rules.

One closely related feature is the system's ability to learn and adapt its behaviour accordingly. This is necessary in order to enable targeted selection and integration of *services* – depending on the current goals, the need to adapt to changed processes and human habits and behaviour – and to adapt to the requirements of the current situation.The technologies in fields F5 and F6 and the relevant *domain* and *human models* (F7, F4) will have a particularly important role to play in this area. In addition to handling the large volumes of data generated and semantic annotation of these data, the key challenges include developing and *validating domain* and *human models* that incorporate fuzzy concepts and converting them into behaviour and learning strategies.

Coordination strategies will be necessary to enable *self-organisation* and *adaptation* to a changing physical and technological environment and new (learned or inferred) goals. Different components and *services* will need to be able to form targeted partnerships without the need for explicit planning and configuration. Some examples of possible enabling technologies are described under field F6. The greatest challenge concerns *semantic* and *user-visible interoperability* and the accompanying need for standardisation (see also 5.3.3).

5.2 TECHNOLOGIES FOR DELIVERING NON-FUNCTIONAL REQUIREMENTS – SAFETY, SECURITY AND PRIVACY PROTECTION

This section will analyse the technologies needed to deliver the non-functional requirements of *safety, security* and *privacy* protection. It will focus on the performance features of systems that can enable safe and secure operation in the face of the specific conditions and challenges associated with Cyber-Physical Systems. It will not deal with the solution-oriented *engineering* aspects such as architectures and organisational structures that can contribute to the implementation of these technologies from a design perspective – these will be described in section 5.3.

5.2.1 DEPENDABILITY

Dependability is usually taken to refer to a combination of traditional *safety* and *security* features such as *functional safety* [ALRL04], *reliability, availability, confidentiality, integrity* and *maintainability* features. Section 5.2.2 will discuss technologies for implementing the first three system features, while section 5.2.3 will address the technologies for implementing the system features of *availability, confidentiality* and *integrity*.

However, since some of the safety and security challenges discussed in section 3.2.3 are equally important or affect the system's *maintainability*, which is a particularly important aspect given the long service life of Cyber-Physical Systems, these technologies are also key to the *dependability of Cyber-Physical Systems*. The relevant issues are as follows:

5.2.1.1 Secure run-time maintenance, care and development mechanisms

Run-time maintenance and care mechanisms involve technologies that enable changes to be made to the system without having to take it offline. It is important to distinguish between three different types of changes that may be made to a system: corrective changes carried out in order to fix faults, changes made in order to enhance or expand functionality, and *adaptive* changes implemented in order to adjust to a new situation. Since the systems have to comply with exacting *safety* and *security* requirements, they need to be capable of testing themselves at run-time to ensure that their ability to meet these safety and security goals is not jeopardised by any changes to the system.

Since the changes may affect parts of the system belonging to different areas of responsibility and application *domains*, these mechanisms should also support additional procedures that enable self-reflection and self-documentation at the global system level, i.e. procedures capable of instantly obtaining information about the system's current configuration and function by interrogating the system itself.

The integration of secure run-time maintenance, care and development mechanisms into CPS-type systems makes it possible to change or swap parts of the system at run-time without jeopardising the system's *safety* and *security*. This enables the *dependability* of the entire system to be guaranteed. Since Cyber-Physical Systems are subject to constant changes while they are operating, this is a key requirement.

The run-time maintenance, care and development mechanisms that are currently available do provide procedures for replacing parts of a system without taking the entire system offline (e.g.

in the field of telecommunications). However, the majority of them do not include procedures for testing the impact of these changes on the relevant *safety* and *security* goals, i.e. they fail to address *safety*@runtime and *security*@runtime issues. Furthermore, only a limited number of current systems (e.g. in the machinery and plant manufacturing industry) possess self-reflection and self-documentation capabilities.

5.2.1.2 An integrated approach to safety and security

An integrated approach to *safety* and *security* at the systems engineering level needs to embrace the entire process, from the definition of the system's functions to their development and implementation in both software and hardware, their integration and testing and the associated processes such as system start-up and shutdown, and the adaptation of the organisational processes during use. Since Cyber-Physical Systems support a combination of technical and operational processes, it is not possible to deal with *safety* and *security* separately without jeopardising the system's overall *dependability*. Whilst unauthorised changes to data – i.e. a loss of *integrity* – can impair *safety* functions, physical disruption and the resulting failures can likewise impair data *integrity*.

Current systems engineering approaches tend to focus on just one aspect of *safety* and *security* (see e.g. the BSI handbook, Common Criteria and Orange Book which focus on *security*; and IEC 61508, DO 178B, ISO 26262 which focus on *safety*). Although the approaches adopted are often very similar, e.g. with regard to the identification of threats, the stipulation of *protection goals* and protection levels and the range of technologies employed, they have not yet been combined to create an integrated approach.

5.2.2 SAFETY AND FUNCTIONAL SAFETY

A system's *safety* is defined as the absence of unacceptable risks resulting from threats posed by the system itself. As described above, the key requirements for *safety* are the system's *functional safety* and *reliability* [ISO11]. A general definition of *reliability*, which is endorsed by the definition proposed by John. D. Musa [Mus04], is the probability of a system operating without error for a given time and in a given environment.

As well as maturity and fault tolerance (i.e. low fault rates and the ability to keep working when a fault occurs), DIN ISO 9126 demands two additional features: *robustness, or the ability to guarantee basic functionality in the event of a fault,* and recoverability, or the ability to easily restore functionality after a fault has occurred. Since *robustness* and *fault tolerance* are also generally regarded as typical features of *functional safety*, current *safety* standards such as the IEC61508 families address both aspects in their call for an integrated approach to the development of *safe* systems.

5.2.2.1 Reliable multicore processors

The parallel operation at the hardware level enabled by reliable multicore processors, i.e. processors with several processing cores, makes it possible to implement simultaneous *safety* mechanisms, e.g. through the redundant design of *safety* functions, parallel operating status monitoring or full isolation of different system-critical functions. The same applies to mechanisms for enabling *energy-efficient* operation involving e.g. turning processing cores on and off depending on the current operating status or performance requirements.

Safety cannot be guaranteed without hardware redundancy. However, CPS-type systems are characterised by a high number of controllers that may not always be very well connected to each other. Affordable, easily scalable, redundant hardware such as multicore systems is therefore essential.

Current parallel processor technology is not able to provide the necessary redundancy to cope with faults. In particular, current multicore architectures are confined to a single substrate, i.e. a single slice of silicon that houses a circuit. This means that they are unable to achieve more than the most basic Level 1 hardware *fault tolerance*. Furthermore, although current platforms have redundant processing cores, the same is not true of the key components of each input and output device, bus and memory management unit, meaning that the necessary isolation mechanisms are lacking.

5.2.2.2 Component description and testing at run-time

Technologies for describing component *safety* make it possible to test key guaranteed characteristics such as maturity – e.g. by establishing the number of errors still present in the system –, permitted application contexts or operating status when components are integrated at run-time – i.e. after delivery and installation – and in the real, functional operating environment.

These description technologies enable the system surrounding a component to ensure that it is integrated reliably. Component descriptions thus constitute binding contracts for the components in terms of both expectations and performance. This is especially important because parts of Cyber-Physical Systems may have to operate in undefined or partially defined contexts that were not fully known at the time when the system was designed or that changed at some point after it was designed.

Current approaches to describing and testing component properties at run-time tend to be confined to the components' syntactic properties such as the number and type of interface elements or simple functional properties.

5.2.2.3 Global platforms with high-order integrated safety mechanisms

Platforms with high-order integrated *safety* mechanisms can provide *safety*@runtime services that contribute to *safety* by enabling straightforward implementation of application-specific *safety* requirements. This is usually done by using generic mechanisms as system functions. These include mechanisms for monitoring operating status – e.g. via monitoring functions – that are derived from *protection goals* and consequently work towards achieving these goals. They also include mechanisms for safeguarding operating status such as automatic function replication, including the ability to switch between replicated functions. Importantly, these are cross-device platforms that thus enable topology-independent operation of *safety* functions.

As Cyber-Physical Systems grow, so does the number of software and hardware components on a platform that can provide functions. At the same time, however, extra *safety* functions also become necessary. Scalable mechanisms for fulfilling *safety* requirements are therefore necessary. It will be possible to implement scalable, *dependable* systems by making generic and user-friendly *safety services* available in platforms.

Most current platforms provide very few of the *safety* mechanisms required to implement *safety* functions. They are largely confined to hardware-oriented mechanisms such as memory *integrity* and fault containment or hardware-related mechanisms such as *virtualisation* geared towards separating functions and *services* in time and space. Higher-order *services* are not normally provided as standard.

5.2.2.4 Wider development and safety standards

Wider development and *safety* standards will need to go beyond the concepts of a system typically used by product liability law. Product liability law deals with liability issues for systems that have been created by manufacturers for a defined purpose until such a time as the system is decommissioned. In particular, these standards and technologies support the different life cycles of the system's parts, shared responsibilities and especially legal liability, and the deployment of systems and components in completely or partially undefined contexts.

Cyber-Physical Systems generally involve interactions between components made by different manufacturers and with different life cycles. It is important for regulations and standards to take this fact into account in order to enable the full range of technologies and procedures required to make the use of CPS-type systems sufficiently *dependable*.

Current *safety* standards are predominantly geared towards closed systems with limited user groups, clearly-defined responsibilities and restricted contexts of use. They thus largely fail to recognise that these restrictions are unrealistic for CPS-type systems.

5.2.2.5 Scalable safety concepts and theories

Scalable *safety* concepts and theories are capable of providing a single overview of large, extremely heterogeneous subsystems with very different *safety* goals. They enable an integrated approach to analysing the *safety* of numerous interacting subsystems.

These concepts and theories are scalable insofar as they enable the outputs of individual subsystems to be scaled up to the level of CPS-type systems. In particular, these theories and concepts support the modular and hierarchical composition of *safety* goals.

Since Cyber-Physical Systems generally involve a combination of different subsystems whose *safety goals may not be closely coordinated*, it is important to be able to map, investigate and predict the interactions between these subsystems in order to ensure the *dependability* of the CPS-type system.

Current methods for assessing system *safety* are mostly based on closed systems. Existing approaches largely overlook the fact that the subsystems in Cyber-Physical Systems interact with each other in order to accomplish a common *safety* goal. They also fail to address the fact that subsystems with conflicting *safety* goals still interact with each other.

5.2.3 SECURITY: SYSTEM FEATURES AND ENGINEERING QUESTIONS

Security is a basic requirement for Cyber-Physical Systems, as has already been described in Chapters 3.2 and 3.4. The technologies used will need to employ measures that provide protection against attacks. It will be particularly important to guarantee secure communication, since this will often occur via wireless communication interfaces. This will require technologies for ensuring that communication only takes place with *authenticated* and authorised partners. In addition, it will be necessary to guarantee the *integrity* and *confidentiality* of the data being transmitted. In other words, these data will need to be protected against tampering and eavesdropping. It will also be essential to guarantee the availability of communication. This is especially important when data need to be up-to-date and guaranteed *real-time* requirements have to be fulfilled. Moreover, when *data that can be traced back to individuals* are being processed, it will be necessary to employ technologies that protect the *privacy* of CPS users. In the *smart mobility* scenario, for example, it is important to ensure that profiles of users' movements cannot be drawn up; in particular, uncontrolled information flows need to be prevented.

In addition to ensuring secure communication, it is also necessary to provide protection for the various systems, devices and components that form part of the system, since these are often deployed in public places and are therefore highly susceptible to attacks involving physical tampering. Consequently, the data stored on these systems need to be protected against tampering, unauthorised access and destruction. This applies both to system data such as the operating system and to stored data such as measurements or the cryptographic keys used to enable secure communication. Cyber-Physical Systems often involve interactions between unknown communication partners, some of whom may harbour malicious intentions (see Chapters 3.2 and 3.4). As a result, technologies will be needed for assessing communication partners' trustworthiness.

Security needs to be addressed not only during the development stage of Cyber-Physical Systems but also once they are up and running. This will require *engineering* capabilities that enable implementation of *security concepts* for ensuring that the systems are both *Secure by Design* and *Secure during Operation*.

Delivery of these capabilities will require *security* technologies that use a variety of different approaches. The first approach is attack prevention. Encryption, for example, can be used to prevent eavesdropping as long as hackers do not have access to the relevant cryptographic keys. Meanwhile, attack detection technology can be used in situations where it is not possible to prevent attacks, as well as to assess the effectiveness of attack prevention technologies. It can also trigger appropriate responses. These technologies include Intrusion Detection Systems that detect suspicious behaviour by communication partners and attestation procedures capable of instantly recognising when a system has been tampered with. The third approach is recovery. This includes technologies such as *self-healing*, as well as the ability to tolerate attacks up to a reasonable point. The specific technologies required are described below.

5.2.3.1 Efficient and lightweight cryptographic procedures and protocols

Efficient and lightweight cryptographic procedures and protocols that are tailored to the resource limitations of the system in question can be used to enable secure communication and thus meet *protection* goals such as *authenticity, confidentiality* and *integrity*.

These procedures and protocols must be adapted to the properties and requirements of the relevant CPS components, e.g. limitations on the available resources. A further challenge is that the long service life of these components will require procedures, protocols and cryptographic keys that can either be replaced or that will remain *secure* throughout the duration of a lengthy service life.

5.2.3.2 Component protection through dedicated security hardware

CPS components are highly susceptible to attacks involving physical tampering. Effective methods are needed for protecting the relevant systems and the data that they hold against tampering and unauthorised access.

Specialised Hardware Security Modules (*HSMs*) offer one potential solution that is particularly attractive to Cyber-Physical Systems because of its affordability. *HSMs* provide secure memory and secure execution environments for *security-critical* operations. Moreover, they often include additional mechanisms for enabling detection of tampering with the systems' own system software. These mechanisms may also be used as the basis for assessing a system's trustworthiness (see below). For many CPS communication scenarios, it would be desirable to develop specialised Machine-to-Machine (M2M) modules with integrated *HSMs* or adapt existing modules to the forms of communication used by Cyber-Physical Systems. These modules would then provide the basis for enabling secure communication between individual CPS components.

The majority of *HSMs* currently in use, for example the *Trusted Platform Module* (TPM), are deployed in conventional systems such as desktop PCs. If *HSMs* are to be used with Cyber-Physical Systems, they will either need to be adapted to the specific characteristics of CPS or completely new modules will have to be developed. For example, it will be necessary to support the virtualisation technologies described below in as resource- and cost-efficient a manner as possible.

5.2.3.3 Secure execution environments

Secure execution environments isolate operations from each other in order to prevent any interaction between them. It is necessary to do this because several different operations with different *security* requirements are often carried out on CPS components.

Secure execution environments need to be adapted to the relevant Cyber-Physical Systems. For example, it will be necessary to develop *virtualisation* technologies that can be deployed in embedded systems. It is also especially important to ensure that these technologies are themselves protected against tampering. This will require secure boot processes and operating systems that use the appropriate *HSMs*. *Middleware* can also be used to provide applications with *security services* in a transparent manner.

5.2.3.4 Procedures for establishing trustworthiness

Procedures for establishing the trustworthiness of CPS components make it possible to check whether their behaviour matches their specifications.

Since Cyber-Physical Systems are employed in insecure environments, they are susceptible to being compromised by hackers. Procedures for establishing trustworthiness make it possible to detect when they have been compromised.

One approach to establishing trustworthiness is the use of behaviour-based systems that have been adapted to the requirements of Cyber-Physical Systems, for example *machine-learning* based anomaly detection supplemented by a reputation system. This approach involves monitoring the behaviour of the system in order to detect and assess any changes or potentially malicious behaviour. An alternative strategy involves lightweight attestation procedures that immediately detect when a device has been tampered with. The advantage of these procedures is that they enable the system software's status to be checked rather than being based on un*reliable* monitoring of the system's behaviour. Most attestation technologies are based on dedicated *HSMs* which act as trust anchors. Attestation procedures for Cyber-Physical Systems will need to be significantly more efficient than those used in conventional application areas. They will also need to be adapted to the new *HSMs* and, where relevant, support *virtualisation*.

5.2.3.5 Security engineering for Cyber-Physical Systems

Security engineering involves the design and development of comprehensive *security* architectures and processes.

Security engineering must be incorporated into the development of Cyber-Physical Systems right from the outset in order to ensure that protection against attacks forms an inherent part of the system. It is important to do this because it is often not possible or not effective to add on security measures after the system has been built.

Current *security engineering* procedures are focused on conventional computer systems and have yet to be adapted to the requirements of Cyber-Physical Systems. The development of CPS technologies will require secure hardware/software *codesign* as well as new *best practices* and standards for Cyber-Physical System *security engineering*. These should be based on the security process described in the "*IT-Grundschutz*" (IT baseline protection) catalogues of the Federal Office for Information Security (BSI) [BSI10]. The BSI's Protection Profile for *Smart Metering* Gateways constitutes a first step in this direction, although it does not yet take all the relevant aspects into account.

5.2.3.6 Security management

Security management enables *security* to be maintained throughout the time during which Cyber-Physical Systems are operating and to be adapted to new situations if necessary.

In order to ensure secure operation, *security* management needs to take into account the lengthy service life and life cycles of Cyber-Physical Systems. This will require *security* architectures to be developed in a way that allows procedures and algorithms to be replaced if they prove to be in*secure*. The ability to replace cryptographic keys will also be necessary in case they are compromised or become in*secure* because of inadequate key lengths. Moreover, it will be necessary to identify keys as being invalid if a user or subsystem leaves a Cyber-Physical System.

5.2.3.7 Test and analysis methods

It will be necessary to develop new test and analysis methods that take into account the specific features of Cyber-Physical Systems. *Security* test and analysis methods make it possible to check what level of *security* has been attained and whether the *security* feature requirements have been met.

The complexity of Cyber-Physical Systems often makes it difficult if not impossible to provide formal proof of *security* features' effectiveness. In many cases, the only manageable test and analysis methods are those that check the system's *security* with regard to known and, to a limited extent, unknown attacks.

5.2.3.8 Summary

Security must form an inherent part of Cyber-Physical Systems right from the outset (*Security by Design*) in order to ensure that they are protected against attacks. After all, without this protection they could not be used at all and it is also key to gaining user acceptance. *Security* also needs to be guaranteed at all times while the system is in operation (*Security during Operation*). There are several features of Cyber-Physical Systems – such as the uncertain environments in which they operate, their use of systems with limited resources and their long run-times – which make it extremely challenging to develop *security* technologies for them. Much research still needs to be done in this area.

5.2.4 PRIVACY

As described in Chapter 4.2, *privacy* protection is one of the factors that will be key to the acceptance of Cyber-Physical Systems. It is not only necessary for the technological systems to meet the *safety* and *security* requirements described in sections 5.2.2 and 5.2.3. Rather, the design of Cyber-Physical Systems should also take *privacy* considerations into account right from the outset (*Privacy by Design* [Cav09]). This concept is well-established in the global *privacy community* and involves the inclusion of *privacy* requirements in all phases of a system's life cycle, from its conception and design to its implementation, configuration and continued development. The goal, wherever possible, is to prevent any threats to *privacy* or at least to keep them to a bare minimum and to make sure that any remaining threats are clearly identified.

Usually, when a system is designed, its specific *privacy* requirements are taken from the relevant legislation for its area of application. However, since Cyber-Physical Systems constantly adapt to new requirements and cooperate with other systems, it is no longer possible to precisely define their area of application. Consequently, it is desirable to adopt an approach similar to the tried-and-tested procedures used in the fields of information *security* and IT baseline protection [BSI10], whereby the appropriate measures for meeting the relevant *privacy* requirements are selected based on the protection needs identified for the information being processed and the technological systems in question. The three traditional information *security protection goals* are *confidentiality, integrity,* and availability. These are supplemented by the three additional *privacy protection goals of transparency, intervenability,* and *unlinkability* [RP09b, RB11]; see also Chapter 4.2.

These six *protection goals* can be seen as representing six different perspectives with regard to Cyber-Physical Systems. Since they all pull in different directions, it is necessary to try and strike a balance between them, depending on the nature of the data in question, the reasons for processing the data and the risks that are believed to be involved. The next section identifies the technologies and methodologies that can help each *privacy protection goal* to be achieved in Cyber-Physical Systems.

Transparency

The protection goal of *transparency* means that the way the system works and the effects it has should at all times be easily understood by its operators and the people affected by it. In Cyber-Physical Systems, the bulk of the data processing takes place without any direct interaction with the user. If the relevant actors are to understand both how the system works and its actual data processing operations, i.e. data flows and decisions, then these need to be presented in an accessible and understandable manner.

In order to achieve *transparency*, it is necessary to establish who is responsible for the different parts of a Cyber-Physical System, how the people with this responsibility can be contacted and which jurisdiction the data processing operations fall under. It is also necessary to check which information is held by the relevant *sensors, actuators,* and systems, i.e. what they know about the responsible authority and applicable legislation and what information they should be allowed to communicate in the event of an enquiry.

In order to ensure that actions and decisions can be traced and attributed to the actor responsible for them, it is important to establish which data should be logged in each context of use, how it should be logged and how the logged data should be handled. This can be done, for example, by defining access rights for individuals or specific functions, by implementing automatic deletion routines that are triggered after predefined periods of time or by specific events, or by protecting the logged data against unauthorised access.

One approach to providing transparency with regard to the operation and effects of a system would be for users to carry a separate device for this purpose. However, a more practical solution would be to integrate the relevant *privacy* management functions into existing *smart devices*. This type of device is already being discussed and prototypes are already being built for some contexts under the heading of "user-controlled identity management".[53]

In view of the complex interactions and data flows, it can be assumed that the majority of users will not want to deal with *privacy* issues themselves. One possible solution would be for users to independently bring in individuals, organisations, or institutions to provide them with support services. These actors could look after the user's *privacy* interests on their behalf, create clear *transparency* for them and, for example, develop and maintain layered *privacy* configuration standards. These support services could be provided by public institutions or private suppliers.

In order to enable automated processing of *privacy*-related wishes and obligations, these need to be available in a machine-readable format. This can be achieved through the use of policy description languages, although these would need to be adapted or expanded to meet the needs of CPS. Research is needed into the use of *privacy policies* in the individual CPS components to provide users with a consistent and accurate overview of data processing operations at all times. These policies could be formulated both for the CPS components and for the transmitted data. It will also be necessary to investigate under which circumstances the use of sticky policies [CMPB03] might be desirable, i.e. where the policies are permanently attached to the data even during data transmission.

Intervenability

The protection goal of *intervenability* stipulates that rather than being powerless to influence Cyber-Physical Systems, the relevant actors should have the ability to intervene on their own initiative as and when they deem it necessary to do so. This also requires the ability to enable *shared control* (see 3.3) and to meet the additional protection goal of *transparency*, since both of these factors are essential in order for targeted interventions to be possible.

All the actors and components involved in Cyber-Physical Systems must have a clear understanding of how they are able to intervene. In particular, they should be clear about

[53] E.g. in the EU projects PRIME (Privacy and Identity Management for Europe) [LSH08] and PrimeLife [FHDH+11].

when they can modify parameters, partly or completely shut systems down or switch to manual control.

Interventions often also entail changes to liability, meaning that they need to be logged. The amount of data that has to be logged depends on which details need to be assessed and the extent to which they might need to stand up in a court of law. For example, were the actors forced to use the system in the same way that airline pilots are obliged to switch to autopilot under certain circumstances, or did they have the right to switch the system off for no particular reason, e.g. if they were using it in their own home?

Data processing and storage in Cyber-Physical Systems is normally decentralised. In order to enable actors to exercise their right to amend, delete or block their *personal data*, it is necessary to provide a single point of contact that informs all the relevant CPS components of the changes.

The devices used to create *transparency* in Cyber-Physical Systems can also be used to enable intervention and configuration. Users' wishes or instructions should be stored in a standard, machine-readable language so that a separate action is not required in each individual case. Once again, individuals, organisations or institutions can be brought in to provide users with support.

Unlinkability

The protection goal of *unlinkability* combines the requirement to keep the amount of data generated to a minimum (data avoidance) with the obligation to keep data and processes from different contexts separate from each other (separation requirement). The aim is to prevent the risks arising from the accumulation of large amounts of data that could be exploited by third parties.

When designing systems and *services* it is important to ensure that they only capture and use the data that are strictly necessary to provide the *service*. Captured data should be restricted to a specific purpose, i.e. it should only be used for the purpose – or, more broadly, the field of application – for which it was originally captured. The technological support needed to restrict data use to a specific purpose can be provided by encryption and access restriction.

Various measures can be employed to implement *unlinkability*. These include physically and logically separating data that are processed for different purposes, as well as anonymising, pseudonymising or erasing them.

In terms of the erasure of data that are no longer required, it will be necessary to develop methods that also erase the relevant log data, since even knowing which *sensors* have detected certain people in a particular location makes it possible to extrapolate information about individuals.

"Private Credentials" [CL01] and "Minimal Disclosure Tokens" [Bra00] are two encryption procedures that are particularly important for data minimisation. These involve anonymous credentials whose *authenticity* and authorised use is guaranteed by a user and can be verified by other parties without needing to disclose the user's identity. Since these credentials have a different appearance for each different use, it is not possible for third parties to link them to each other. For example, users could be given digital driver's licences that appear differently every time they are read by someone else.

The huge volumes of data associated with Cyber-Physical Systems and their frequently desirable ability to intervene in people's lives mean that Cyber-Physical Systems that have not been designed with data minimisation principles in mind could pose a major threat to people's *privacy*. Statistical techniques can even be used to extrapolate personal information from *data* that were not originally connected to a particular person.[54] This issue will undoubtedly have an influence on the acceptance of Cyber-Physical Systems. Indeed, it is debatable whether it is possible to prevent such a large and uncontrolled concentration of data from being abused and whether people can be effectively stopped from using data for purposes other than those for which they were originally intended; see also Chapter 4.2.

5.2.4.1 Summary

Since safeguarding *privacy* will be key to the acceptance of Cyber-Physical Systems, it will be important to ensure that the relevant criteria are adequately incorporated into the design of the technological systems. This can be supported by the *privacy protection goals* of *transparency*, *intervenability*, and *unlinkability* that should be backed up by measures in a similar way to the *security protection goals* of *confidentiality*, *integrity*, and *availability*. Particular emphasis should be placed on technologies such as anonymous credentials, identity management systems and machine-readable *privacy policies*. A consensus needs to be reached between the society, regulators, and CPS users with regard to how much *privacy* is required for different *services*.

5.3 ENGINEERING CONCEPTS AND COMPETENCIES

The technologies and research topics addressed in sections 5.1 and 5.2 cover a significant proportion of the core CPS technologies required to deliver the novel capabilities described in the scenarios in Chapter 2 and Chapter 3.5.

In order to facilitate productive research in these areas and in particular to ensure that this research is translated into economically successful CPS applications going forward, it will be necessary to devote a substantial amount of effort to the fields of *modelling*, integration, interdisciplinary *requirements engineering* and software and systems *engineering*. This section will present a summary of the necessary research and development efforts, based on the *engineering* requirements outlined in Chapter 3.6 and a preliminary attempt at assessing the current state of both research and practice.

Significant efforts will be required in the following fields:

- *user-centred, participatory* and *virtual requirements* analysis, design and evaluation procedures
- *requirements engineering* – this is key to the conception, design, *validation* and *verification* of Cyber-Physical Systems
- comprehensive basic *human* and *system models*
- integrated and *interoperable* system architectures and *domain models*
- *domain engineering* and system management
- quality *engineering* at all stages of development
- *Living Labs* and controlled testbeds

5.3.1 USER-CENTRED, PARTICIPATORY AND VIRTUAL METHODS FOR REQUIREMENTS ANALYSIS, DESIGN AND EVALUATION

Current exploratory and *virtual* procedures for requirements analysis, iterative design and the evaluation of architecture and solution concepts can be broadly divided into two categories:

- Requirements analysis, design and *validation of* user-friendly *human-machine interaction* and *human-machine interfaces* using interactive prototypes and realistic *virtual* simulations of use.
- Modelling and simulation of designs, concepts and solutions (design space testing) for systems and components, including human behaviour *models* for the evaluation (*validation* and *verification*), selection and integration of solutions.

[54] Armed with a big enough data set and the requisite *context knowledge*, it is even possible to de-anonymise anonymised data, based on the probability of the data relating to a particular individual; see [WMKP10].

The relevant methods and procedures are to be found in the following sources and approaches:

1. *Quality of Experience, Quality in Use* [ISO10], *experience* labs and *usability engineering.*[55]

2. *User-centred design* [EBJ03, MOS08], driving and flight simulation, driver information and assistance [BK02, HAV, SANTOS, IMo, ISI, HUM].

3. *Virtual engineering (virtual* development of technological systems) in product development and *industrial engineering* [ABB+09].[56]

Cyber-Physical Systems raise new challenges regarding the development of open systems that are geared towards and capable of adapting to users' needs in globally networked and highly dynamic contexts. Meeting these challenges will require research horizons to be expanded and new problem analysis methods to be developed. It will also be necessary to align and integrate previously separate requirements and design *models* in order to enable end-to-end *validation* and *verification*.

More specifically, this will involve

– expanding the scope and depth of *human-machine interaction* testing and simulation *models* and going beyond the local and isolated contexts of use that have hitherto been addressed when it comes to analysing, aligning and combining the environment and relevant application processes, including *human-machine interaction,*
– ensuring that potential users, *stakeholders* and other actors from the application *domains* who are representative in terms of their age, gender, social and cultural background and competencies are integrated into the design process of new systems and services right from the outset. This will allow them to become active partners and help shape the development process (see also cooperative and *participatory design*),
– applying the aviation industry's experience and findings in the area of *human-machine interaction* and research into *situation awareness* and modelling to CPS applications in everyday environments and situations where the users have no special training, as well as investigating the associated requirements in terms of system design, technology and overall conditions,
– changing the current approach where users have to adapt their behaviour to operating processes and technology interfaces in favour of an approach where the systems and *human-machine interactions* adapt to their current context of use and to the user's needs, habits and abilities,
– simplifying concepts for interaction and system design and developing enhanced *safety and security* concepts and architectures, together with the identification of acceptable forms and degrees of system *autonomy* with regard to decision taking and acting,
– developing context, interpretation ("*X*"*-awareness*) and interaction *models* and the corresponding *virtualisation* and simulation procedures, so that early experience and familiarity with how the system behaves can be gained and its quality can be measured and assessed (*Quality in Use* – these criteria are critical to the system's success and acceptance[57]).
– the experimental and continuous development of formal quality *models* and the related architectural patterns in order to ensure end-to-end *Quality in Use* and *Quality of Service* at all levels of the design, integration, deployment, operation and maintenance of Cyber-Physical Systems and services.

[55] *Usability engineering* refers to the process that occurs in parallel to traditional planning and development work in order to ensure that the system will be usable. This is an iterative process, since usability experts test the extent to which the system meets the defined goals and requirements of its future users at every stage of the project. [Ram07]

[56] See also [BUl02].

[57] E.g. in terms of intuitiveness and simplicity in use, ease of understanding, *transparency*, effectiveness, etc.

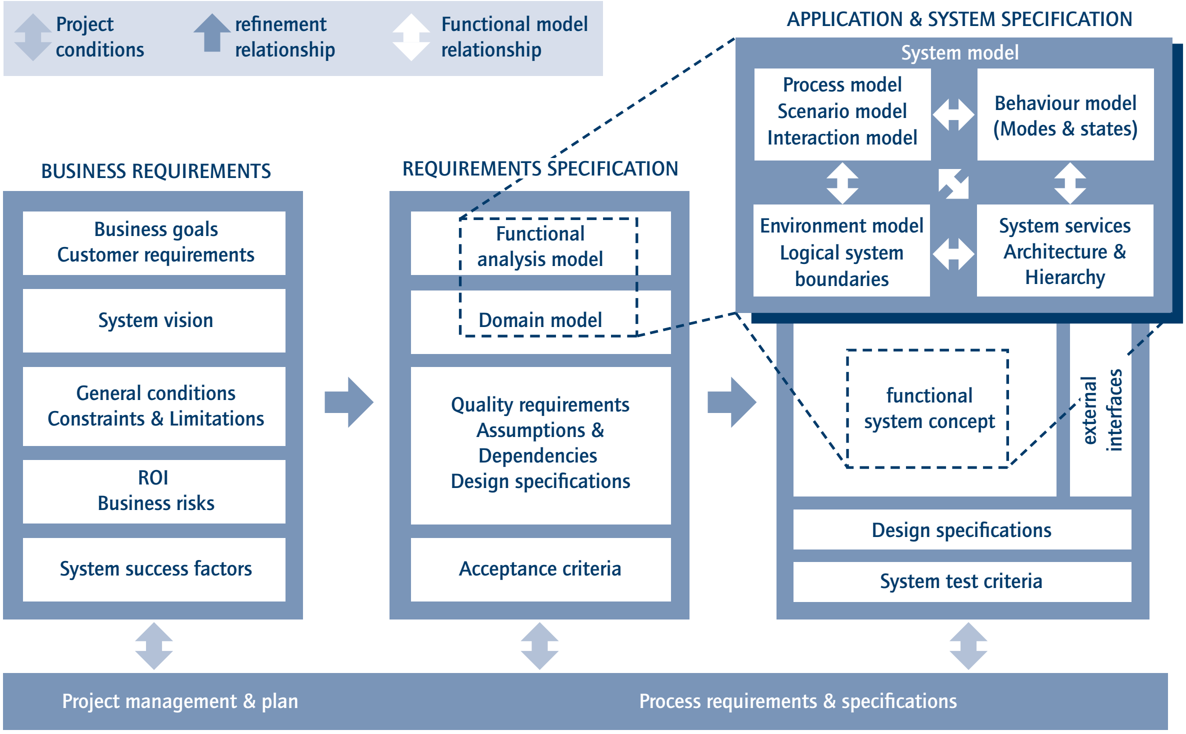
5.3.2 THE FUNDAMENTAL IMPORTANCE OF REQUIREMENTS ENGINEERING

The previous section has already illustrated the fundamental importance of *requirements engineering* (RE) to every area of systems engineering – application processes, *services*, interaction, architectures, components and platforms – and to the development phases of integration, maintenance and system evolution. The key tasks of *requirements engineering* include identifying potential problems, ascertaining business, user, customer and process requirements, setting goals and priorities, resolving conflicts and inconsistencies and establishing the relevant requirements for the system, its components and its architecture as well as the way they communicate with each other and with the outside world.

The *requirements* and system specifications have a number of key functions in this regard:

- providing a communication basis for acquiring and aligning application knowledge, requirements and solutions among the different actors involved in the system's development and use,
- specifying binding instructions and rules for finding, designing and aligning appropriate solutions and architectures at all levels of system design,

Figure 5.1: Overview of content to be specified in requirements analysis and system specification (taken from REM [BGK+07, GBB+06, GTKM11])



- specifying the basis for the selection, introduction and establishment of appropriate software development processes with quality gates,
- providing part of the content of contracts, orders and partnership agreements in *value networks*,
- stipulating the criteria and values – e.g. with regard to *availability* and service levels – needed to ensure successful operation of CPS-based applications,
- providing basic specifications with regard to the *maintenance, reuse*, upgrading, standardisation and evolution of *domain knowledge,* requirements and system *models*,
- in the case of formal r*equirements specifications* and system *models*, providing a basis for direct conversion into executable simulation models and prototypes for hands-on, interactive testing, *validation* and finalisation of requirements and design concepts (see also 5.3.1).

In order to ensure that application goals and requirements are taken into account in the system design and implemented correctly, it is essential both to understand and to carry out a qualitative appraisal of the *refinement* and design maps at all levels of the system (*traceability*).

Figure 5.1 presents a reference model of basic requirements categories and their *refinement* relationships. Its structure is based on three abstraction and design levels: customer and business requirements*, requirements specification* and the associated analysis and modelling concepts, and how these are mapped onto basic application and system specification *models* which in turn provide a fixed basis for the design of the system's components.

This reference model for *model-based requirements engineering* goes beyond current approaches to *requirements engineering*, including the methods described in Chapter 5.3.1. These are focused on the informal communication of users' requirements and on technological solutions. More specifically, they include:

- iterative, simulation-based and increasingly also exploratory establishment and *validation* of requirements,
- processes for communicating and negotiating requirements, describing and specifying them (usually informally) and allocating them to design elements such as interfaces and system functions.
- management and classification of requirements using general requirements management tools,
- modelling of *services*, interactions and data in the area of technical system specification, i.e. solutions,
- the technical communication and specification of interfaces and behaviour requirements and their *safety and security* features, especially in the field of embedded systems,
- end-to-end integration of different specification elements in the development process in tool chains. One particular challenge in this context is that the ideas associated with the requirements are unclear. The result is that the requirements can only be incompletely established and cannot be represented formally, making semantic integration almost impossible.

In view of the increasing openness, complexity and novelty of future CPS applications and the extremely wide range of possible CPS design approaches, the principal *requirements engineering* challenges will concern the identification, analysis and specification of the requirements needed to enable CPS capabilities to be designed and realised appropriately.

This will require the following research topics to be addressed:

- the adequate understanding, analysis and accurate specification of the open application context, problem space, user goals, *human-machine interaction* and targeted specification of the functional and non-functional requirements in the shape of formal requirements *models*. It will be especially important to address the evolutionary development of Cyber-Physical Systems through context-*adaptive* enhancements that provide new

functions and capabilities based on existing sub-functions, sub-services, infrastructures or platforms,
- how to structure the systemic complexity of multifunctional CPS *Systems of Systems* comprising globally networked components, devices and *services*, including how to connect them with each other and use them in different contexts. This also includes the scaling and design of concepts for the refinement of user requirements and their mapping onto system, component and communication behaviour and onto the relevant architecture concepts with their different *refinement* and design relationships,
- the specification of non-functional requirements and quality *models* – which are especially important to the design and realisation of acceptable Cyber-Physical Systems – as well as the conversion of these requirements into architecture designs and *models* at the system integration (*interoperability* and semantic integration) and architecture design levels; see also the following section.

5.3.3 COMPREHENSIVE AND INTEGRATED HUMAN, SYSTEM AND ARCHITECTURE MODELS

The scenarios, applications and potential benefits associated with CPS permeate every area of our lives. In-depth analyses will therefore be needed in order to gain a full understanding of the nature of current and future application contexts. It will also be necessary to identify and coordinate all the relevant actors and systems and the necessary *human-system cooperation*.

In order to ensure that Cyber-Physical Systems are adequately designed, configured and managed, integrated description, design engineering and system *models* and architecture concepts from the following areas will be required:

- science and engineering, in particular mechanical engineering, electrical engineering, physics, chemistry and biology,
- information and communication technology (*ICT*), embedded systems, the Internet, sensor technology, networks and system management,
- human thought, behaviour and complex problem-solving based on the *models* and findings of cognitive psychology, neuroscience and brain research,
- the social sciences, social networks and the formal study of various types of networks including networks of organisations and actors,
- deployment and integration of these concepts with IT *models*.

Description, analysis and design *models* with a formal specification language and semantics enable the targeted establishment, valid specification and systematic *validation, verification* and quality assurance of requirements and system designs; see also 5.3.2.

Research is currently ongoing in the field of *engineering* to find ways of reducing complexity and thus enabling simplified management of Cyber-Physical Systems so that additional quality, productivity and efficiency gains and cost savings can be delivered. The focus is on the following areas:

- *model*-based or *model-driven engineering*, architecture design and evaluation, testing, integration, system analysis and *verification*,
- *human-machine systems* and *human factors.* The latter is mostly confined to the use and operation of systems in the workplace,
- *virtual engineering,*
- evolutionary software development,
- *re-use* and software product lines,
- generative programming and synthesis in the field of pure software development.

5.3.3.1 The fundamental importance of integrated models and architectures

One particularly important requirement in terms of the *engineering* of CPS applications is the development of integrated description and design *models* and procedures for realisation the core CPS capabilities, together with the necessary architectures and *application platforms*. It is also necessary to verify the fulfilment of non-functional requirements in open systems and to overcome the challenges alluded to in Chapters 3.5 and 3.6. Answers need to be found to a variety of questions regarding integration at the technological level, *human-machine interaction* and business relationships, *business models*, *ecosystems* and their architectures.

It is necessary to find better ways of integrating the physical *models* used in mechanical engineering and related engineering fields with the digital *models* used in software and systems *engineering*. Numerous challenges exist, particularly with regard to control engineering, modelling techniques in software and systems *engineering* and classical *modelling*, and mechanical engineering design theory. For example, several different disciplines have contributed to the development of *smart grids. This has not only involved* experts in IT and information and communication technology but also experts on power grids and end devices, e.g. for the development of *smart metering.*

It will also be necessary to ascertain which *models*, procedures and interdisciplinary research initiatives will be needed in order to understand and analyse the far-reaching changes in *human-machine interaction* that will be triggered by Cyber-Physical Systems and information and communication technology, particularly the Internet. The wide-ranging social and political consequences will also need to be investigated and it will be important to ensure that CPS applications and services are designed to be both usable and acceptable for their users and for society as a whole.

Models from cognitive and behavioural psychology and sociology[58] have already made significant contributions to the fields of *artificial intelligence*, robotics and assistance and traffic management systems. In the context of Cyber-Physical Systems, this interdisciplinary research needs to be expanded and integrated into all aspects of *engineering*. Moreover, acceptance research should address a wider set of goals. It needs to do more than simply consider the immediate perspective of the individual user[59] and start investigating the deeper *human-system interactions* in Cyber-Physical Systems and their impact on society as a whole. This new dimension of acceptance research should furthermore be integrated into the *engineering* process.

Integration with *models* from the fields of business studies and economics will also be necessary. This will be required in order to develop *business models* and *customer value concepts*, determine the factors that are key to the technology's acceptance and deliver better quality *models* and integrated *engineering* in *value networks* and *ecosystems*, etc. This issue will also influence what businesses look like in the future, the relationships between them and the distribution of investments, sales, profits and short- and long-term *returns on investment (RoI)* among them.

5.3.3.2 Requirements-oriented, integrated architectures

In order to integrate the various ontologies and modelling concepts, *engineering* needs standard requirements *models* and architecture concepts. Their structure should be based on abstraction and system design levels and

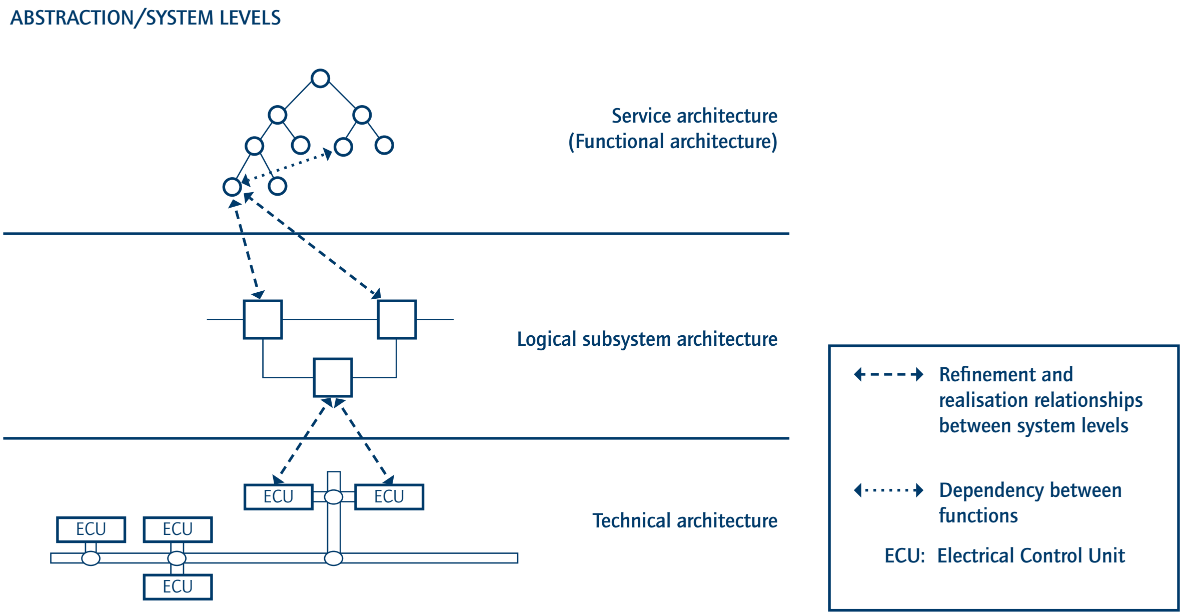
[58] See also the projects under the auspices of the DFG (German Research Foundation) Priority Programme Socionics (= sociology + IT) [FFM05, Soc07].

[59] According to [Rei82, Man83, Sim01], the goal of innovation acceptance research in the social sciences is to investigate the reasons why a particular innovation might be accepted or rejected by potential users. There are two facets to this research: (1) understanding the interactions between the introduction of an innovation and its impact and (2) creative goals - obtaining ideas for improving the design of innovations based on users' experience with them. (summary of the points made in [Qui06]).

functional modelling perspectives, as outlined e.g. in the refinement levels and system views in the functional system concept illustrated in Fig. 5.1 and in [GS07, Sch04] for embedded systems. This applies to the description and modelling of problems and their requirements, as well as to system design, integration, validation and evolution and coordination between the different *stakeholders*, i.e. customers, users and engineers from different fields. The following *architecture frameworks* have been developed:

- general systems engineering *architecture frameworks,* e.g. the TOGAF Framework [TOG09] for the development of information systems, the NATO Architecture Framework [DoD09a, NAF07] for the development of military embedded systems and the general V-Model XT[60]
- domain-specific *architecture frameworks* and standards, e.g. IMA (Integrated Modular Avionics [IMA]) in the field of avionics, the AUTOSAR standard [AUT] in the field of automotive design automation systems [Gif07, MLD10, Dra10] and the EPC Global Architecture [ABD+10] in the field of commerce and logistics. At both the *technical architecture* level and in the areas of communication networks, power grids and logistics, these *architecture frameworks* contain formal and standardised architecture and interface specifications for the *model-driven engineering* and cross-manufacturer integration and *interoperability* of components and functions.

Figure 5.2: Structure based on system and abstraction levels and their refinement relationships (simplified version of figure in [TRS+10, BFG+08]). The abstraction level of the user and application processes that use the system's functionality is not illustrated here; see also the content of the business and requirements specifications in Figure 5.1.


ABSTRACTION/SYSTEM LEVELS
Service architecture
(Functional architecture)
Logical subsystem architecture
ECU
ECU
ECU
ECU
ECU
Technical architecture
Refinement and realisation relationships between system levels
Dependency between functions
ECU: Electrical Control Unit

[60] See [FSHK09].

All the system architecture concepts are based on a structure that employs the following system and abstraction levels (see Fig. 5.2) and system views:

- **Functional level:** a structured external perspective – i.e. from the viewpoint of the user or other systems – of the functions and *services* that a system provides – *functional* or *service architecture*.
- **Logical architecture level:** a view of the system's structure, i.e. how it is broken down logically into components, interfaces and interactions in order to ensure optimal delivery of the *services* offered at the functional level. There are a number of associated requirements and questions regarding the architecture's structure, e.g.
  - whether control and coordination operations are performed centrally or distributed across several components,
  - the number of time-critical processing tasks concentrated in a single component,
  - the design of redundant architectures for *safety-critical* applications,
  - the most suitable architecture design for non-functional requirements; see also the key acceptance factors for Cyber-Physical Systems in Chapter 3.4 and the technological approaches to implementing them described in sections 5.2 *Security* and *Privacy Protection* and 5.3.5 Quality *Engineering*.
- **Technical architecture:** this describes the *technical* implementation and *architecture* of the system's functions and how they are mapped to
  - software (code architecture, run-time system and run-time elements, etc.),
  - hardware (processors, controllers, CPUs), communication links (*bus* systems),
  - sensors, actuators, *human-machine interaction* components.

  The focus is on mapping and allocating logical functions to specific software and hardware architectures, e.g. *security* mechanisms in *technical communication*, or multicore architectures.

There are also a number of architecture questions concerning the design of *smart* structures in the environment, *infrastructure* – for example with regard to the layout and appropriate control structures for the different components of a smart intersection or the distribution of healthcare centres in a remote healthcare system – and *CPS platforms* (see 5.3.3.3 and Appendix B).

Under the auspices of the SPES 2020 [SPE] partnership, partners from research and industry are working together closely to develop basic formal semantics-based architecture *models* for embedded systems using use case scenarios from the fields of healthcare, avionics, the automotive industry, power grids and automation. Their work draws on the potential of *model*-based development and end-to-end *validation* and *verification as outlined above*.

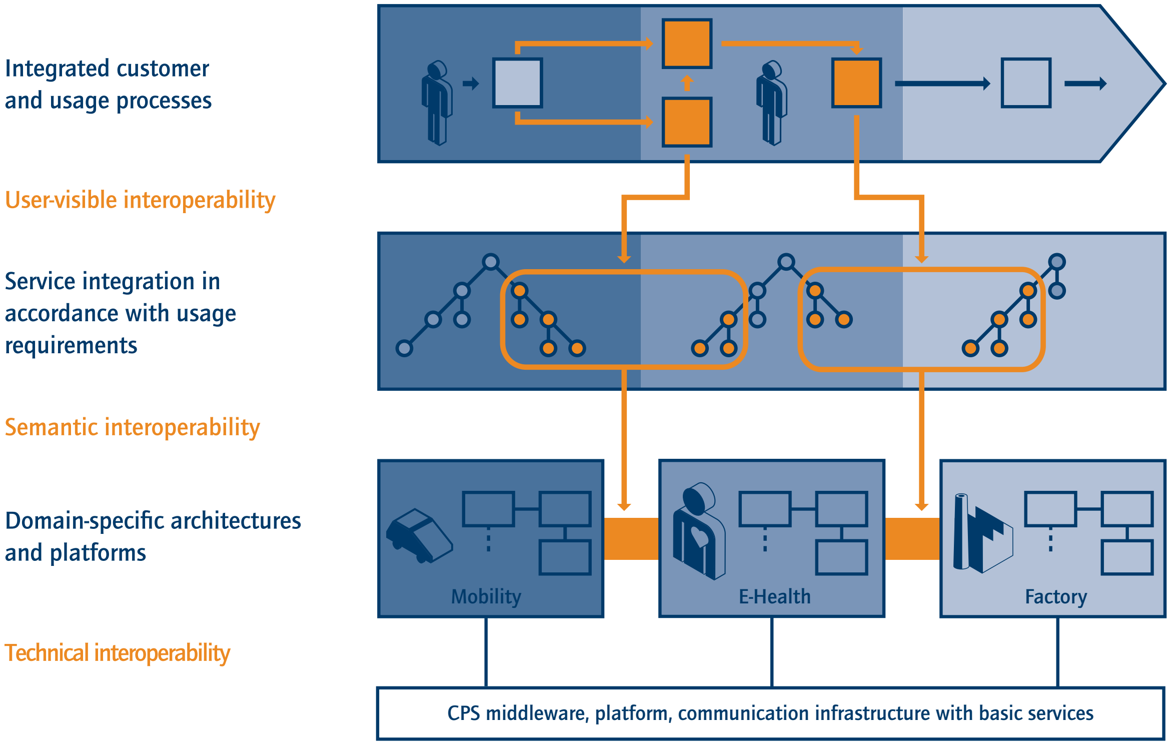
In order to provide a structured description of the user, process and environmental requirements placed on systems, the *architecture frameworks* outline the following abstraction levels:

- business architectures, including their goals systems and the relevant ontologies,
- application, utilisation process and organisational *models* and environment architectures,
- more comprehensive operational environment *models* in the field of aviation, the use of drones to gather information in the aftermath of natural disasters, or networked military systems such as the Operational and Capability Views in the US Department of Defense Architecture Framework (DoDAF).

As far as the *engineering* of Cyber-Physical Systems is concerned, the key challenges involve the investigation and development of adequate architecture models and design methods capable of reflecting the characteristics of Cyber-Physical Systems and enabling their novel capabilities. The detailed challenges are as follows:

- The architecture design for CPS components such as embedded systems needs to adopt a broader perspective that goes beyond an approach based purely on closed systems with fixed goals and predetermined application environments and requirements. Architecture and interface design needs to be adapted to open contexts of use, wide-ranging application and integration requirements and uncertain networking and adaptation needs.
- A deeper understanding of the application areas is needed at the higher abstraction levels of the problem, application and requirements domains. It will be necessary to develop and enhance behaviour patterns, *domain* and environment *models* and architectures capable of configuring and integrating CPS services and functions at all levels of the system architecture.
- It will be especially important to investigate new requirements and mechanisms for the local and global design of *services* and *functional architectures*. They will need to be capable of being employed in different contexts and combined with unknown systems and functions. Moreover, it will be important for these mechanisms to

Figure 5.3: Abstraction, design, integration and interoperability levels of Cyber-Physical Systems.


Integrated customer and usage processes
User-visible interoperability
Service integration in accordance with usage requirements
Semantic interoperability
Domain-specific architectures and platforms
Technical interoperability
Mobility
E-Health
Factory
CPS middleware, platform, communication infrastructure with basic services

be *interoperable* at all levels of the system and for them to be capable of being adapted and integrated depending on the requirements of the user and application processes. Fig. 5.3 illustrates the integration requirements and the connections at the different system levels.

- It is important to understand the complex non-functional requirements of Cyber-Physical Systems. This also applies to the requirements concerning the configuration, distributed design and open composition of *services* and components at the system's individual design and integration levels – i.e. the use process levels, functional and *service* levels and *logical* and *technical architecture* levels – and the environment.[61] It is necessary to establish concepts for interfaces and protocols and for interactive and cooperative behaviour. To do this, it will be necessary to employ *user-centred* architecture testing and evaluation techniques; see also 5.3.1.
- The key task and challenge at the *technical architecture* level involves the research and development of standard *communication* and *middleware platforms* for Cyber-Physical Systems. The priority is to create generic cross-domain network and communications structures, protocols and *interoperability* standards, as well as basic CPS *services* and quality assurance mechanisms (see 5.3.3.3 below).

All the potential CPS application fields require an in-depth understanding of the system features of the relevant CPS applications and their design. The following areas need to be investigated:

- the degree of openness, *adaptability* and *interoperability* (which is essential to enable targeted use) between the systems, as well as the ability to cooperate with unknown systems and *services* and cross-*domain* integration mechanisms,
- the required types of full or partial *autonomy* and *self-organisation*, together with the relevant architecture, communication and composition principles.

The priorities are to combine basic system modelling concepts from the relevant disciplines (see also 5.3.3.1), develop an open *CPS platform* with standard interoperability and *Quality of Service services* (see following section) and come up with a way of managing autonomous and evolutionary systems (see 5.3.3 and 5.3.4).

5.3.3.3 Open CPS platforms with basic interoperability and Quality of Service services

Open *CPS platforms* with basic *interoperability* and *Quality of Service services form a key part of the technological and strategic basis for enabling the wide-ranging innovations and evolutionary application development associated with* Cyber-Physical Systems. They provide generic basic functionality for the *secure* networking, *interoperability* and integration of CPS applications and their evolutionary development.

Appendix B uses the example of the automotive *domain* to outline the key functions that future *CPS platforms* will be expected to provide. It identifies the following *CPS platform services* based on the results of expert interviews:

- component management,
- sensors for registering the physical environment and context, as well as for data fusion and time synchronisation,
- dynamic data and *service management*, including *plug-and-play* mechanisms and load balancing and location-independent communication tasks,
- *service* interaction, contract and session management,
- monitoring, *adaptation* and communication of *Quality of Service*,
- *self-healing* and reconfiguration,
- *security services* and hardware,
- *intermodality* and translation of *ontologies*, data formats and protocols.

[61] E.g. *smart infrastructure* in the fields of transport (mobility scenarios) or buildings (*AAL* scenarios).

5.3.3.4 User-centred and user-visible interoperability – cooperation models for the different application domains

One key capability of Cyber-Physical Systems is their ability to continuously capture and integrate information about the current local, regional and global environments; see Chapter 3.4. In order to enable the different application systems and *services* of integrated CPS processes to be used, technical and *semantic interoperability* need to be accompanied at the functional level by adaptive interfaces and *models* of the different application domains' current contexts of use (*domain models*). Beginning with integrated and formal *ontologies*, it will be necessary to develop, expand and continuously validate[62] goals systems and context[63] and architecture *models* that reflect the viewpoint of the applications and their users and are mutually compatible.

This is one of the largest challenges facing the creation of *usable* and acceptable Cyber-Physical Systems. There is still huge uncertainty regarding the shape that will be taken by *human-machine interaction*. The following questions need to be answered with regard to this issue:

- How simple must the design of the cooperation, linkages and *service* integration between CPS components be for users to be able to evaluate and manage situations and systems? How much do users need to know about the networking activities and status of the relevant system?
- Should it be people, systems or subsystems that decide on the selection of and cooperation with the appropriate *services* and at which development level should this occur?
- Which operations can the system perform autonomously without consulting the user in the areas of networking, *service* quality evaluation and cooperation whilst both meeting the needs of the current situation and remaining acceptable to the individual user?
- What must the Cyber-Physical System, e.g. a digital assistant, know or learn from other systems about the situation, the context and the user's current goals and wishes in order to behave as required by the situation? How much control do users have over these networked system activities and how much control should they have?

These as yet unanswered questions are not confined to the *interoperability* of the application systems and the *domain models* and technologies required to achieve this. They are also fundamental to the nature of *human-machine interaction* in Cyber-Physical Systems, including the related social aspects; see also Chapter 4.

5.3.3.5 Requirements traceability – the key to evaluating design and cooperation decisions

Depending on how formal and complete they are, the *architecture frameworks* described above and the specific versions of them that exist in different application *domains*, including their *interoperability* and cooperation *models*, define the *refinement* and design relationships[64]. As such, they set the design and composition rules that determine development, adaptation and cooperation (at run-time) in CPS applications and networked systems of systems. These relationships between the different elements of the *requirements specification* and the system design are also known as *traceability* relationships.

Thus, in order to achieve the context integration discussed in section 5.3.3.3 and to ensure that Cyber-Physical Systems behave in a user-centric manner, it is also necessary to formalise the different user and *stakeholder* requirements and

[62] E.g. methods for testing and trialling the applications in *Living Labs*.

[63] Complex environment, process, situation and control *models*.

[64] The service for *keeping a safe distance from other vehicles* in an ACC (Adaptive Cruise Control) system is based on the logical functions *measure distance to next vehicle, calculate required speed* and *modify and control speed (engine);* The *measure distance to next vehicle* and *calculate speed functions are in turn* enabled by the relevant *sensors*, communication and computations at the technical design level. These relationships between the system's different abstraction levels are thus also referred to as refinement and design relationships.

domain and context models, as well as possible ways of mapping these requirements onto the *services* that deliver them and onto the partnerships between various CPS architectures and components. This global, end-to-end traceability, especially of non-functional requirements, enables end-to-end *validation* and verification of design and cooperation alternatives for meeting user and customer requirements. This applies equally during the system's development and during its operation.

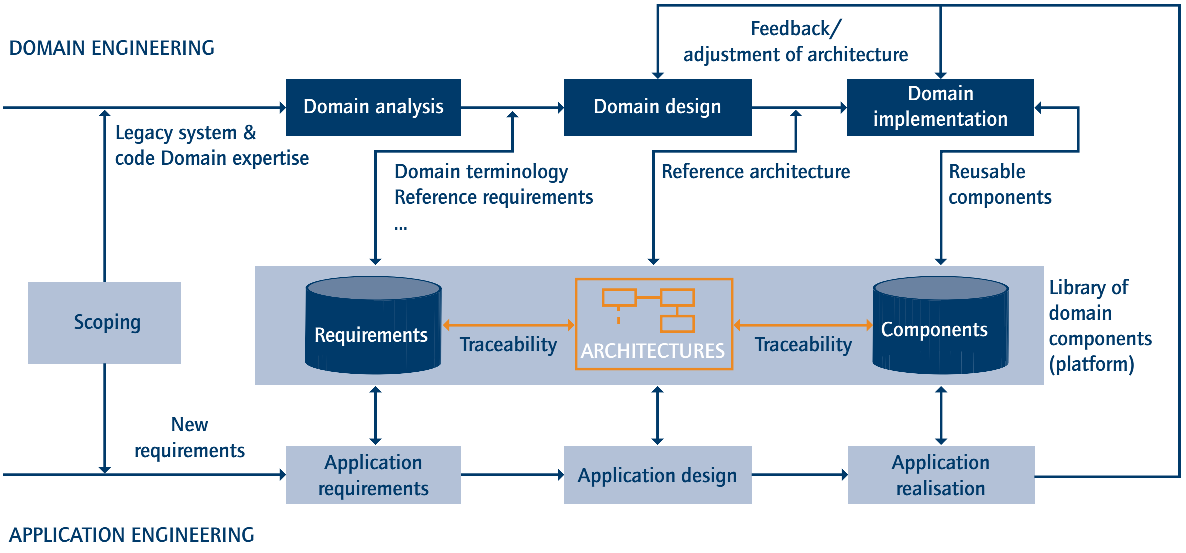
There are major failings in the current development of embedded systems with regard to the end-to-end identification, specification and verification of functional and non-functional requirements. User requirements and engineers' assumptions about the environment, application processes and involved persons' behaviour are generally not fully captured and analysed or properly specified. It is therefore almost impossible to implement, *validate* and *verify* them at the design stage [GTKM11].

The requirements placed on Cyber-Physical Systems and their design and networking relationships are subject to dynamic and evolutionary change. In conjunction with the user- and context-dependent choices and priorities in individual CPS applications, this generates a huge degree of complexity. The largest challenges with regard to the management of these systems are connected with the development of appropriate requirements and *context models*, abstraction mechanisms and scaling concepts for requirements and system management. These challenges will need to be resolved if the models are to be usable and suitable for fulfilling specific purposes.

5.3.4 DOMAIN ENGINEERING AND SYSTEM MANAGEMENT

Domain engineering refers to the acquisition of domain-specific knowledge as the basis for the development and

Figure 5.4: Reference process of the PRAISE product line approach, modified for agendaCPS (as *cited in [Ber07]*)



evolution of systems, products and services in a particular *domain*. This includes methods for analysing and modelling the requirements in the *domain*, as well as the design and modelling of generic solution architectures for product families, the development of *reusable* components, functions and *services* for the architecture and the evolution of the *domain*, architecture and implementation *models*. The sub-topics of *domain engineering* include knowledge modelling based on *domain modelling ontologies* and domain-specific program development languages.

Fig. 5.4 illustrates the basic components of *domain engineering* that have been the subject of research for many years in the field of product line development of software-intensive systems [KCH+90, Ber07]. They are also increasingly being used in the area of complex embedded systems. In order to represent the different approaches, the diagram provides an overview of the systematic development and evolution of domain-specific application and development platforms and their *engineering* components – see the library of core *domain* components in Fig. 5.4. These include, for example, *domain models,* architectural patterns and design and *validation* methods. The aim of the library is to enable the different elements to be used, reused, adapted and developed in the development of specific applications (see application *engineering*).

In order to enable the challenges outlined above to be addressed in a practical manner, domain-specific application architectures, platforms and architecture concepts and the relevant composition and integration mechanisms will need to be developed iteratively in the application areas in successive development and testing cycles; the same applies to the implementation of non-functional requirements. Although this will predominantly occur at a *domain*-specific level, the composition and integration mechanisms will nonetheless need to be capable of cross-*domain interoperability*; see the *CPS platform interoperability* and *Quality of Service services described in section* 5.3.3.

The research priorities also include the investigation and development of evolution concepts for CPS architectures, especially in terms of the interactions between *domain*-specific, cross-*domain* and generic architectures and architectural patterns. In the field of software development, these topics are being researched under the headings of evolutionary software development, *model* development, evolutionary software architectures and *reusability*. However, it remains to be seen to what extent the discoveries made in this field can be applied to the cross-*domain* and highly interdisciplinary evolution of CPS.

5.3.4.1 Domain engineering of open CPS applications and platforms

The following aspects are especially important for the *domain engineering* of Cyber-Physical Systems:

- the specification and development of appropriate *domain models*[65] including different user and *stakeholder* viewpoints and requirements,
- the development of mechanisms for selecting and scoping the aspects of the environment, problems and tasks that are relevant to a given application,
- the design of *interoperable* architectural and composition patterns for delivering non-functional requirements; see also 5.3.5 Quality *Engineering*,
- flexible *tailoring* of the development processes and life cycle and integration management of different CPS components and subsystems across different *domains* and companies, e.g. for remote maintenance or updating, replacement and evolution of components, even at run-time,
- mechanisms to enable *reuse* and tailoring, as well as variant management,
- complex management of the *application* and *domain platforms* for *engineering*, applications and tools. Their

[65] *Context knowledge*, environment *models* and architectures, user and stakeholder *models*, goals and requirements *models*, modelling principles and methods, business and technical rules, physical constraints.

development will be partly evolutionary – with effects that may occasionally not be clearly definable – and partly revolutionary, with disruptive effects in the relevant *domains*.

5.3.4.2 System management and engineering of autonomy and evolution

In addition to addressing the evolution of *CPS application* architectures and platforms, it is also necessary to develop *models*, methods and procedures for *engineering* autonomous, *self-organising*, learning-enabled systems. Answers will need to be found with regard to the following system management questions:

- the appropriate forms and degree of *autonomy* needed to deliver the new CPS capabilities and meet their requirements,
- the right choice and appropriate trade-off between centralised system management, decentralised *self-organisation* or different combinations of the two,
- the critical system properties of Cyber-Physical Systems in general and *domain*-specific applications in particular,
- risk assessment and evaluation. To what extent do the autonomous subsystems or functions of Cyber-Physical Systems produce effects that are not aligned with the goals or needs of the relevant actors?
- fundamental questions connected with operational system boundary delimitation, *autonomy* and *self-organisation,* including the relevant CPS application and system classification and characterisation.

It is important to distinguish between the following perspectives:

- system management at the application level, i.e. the management of *socio-technical systems* where human beings and social groups are networked components and actors within the application system (see also 4.1.4),
- system management of the underlying technological system level, e.g. of critical infrastructure networks such as *smart grids*; see also Interdependent Networks[66] [Uli],
- the complex interactions between these two system levels, as well as the control mechanisms and their impact on the social issues connected with *human-machine interaction*, e.g. safety and security, fairness, acceptance and the potential loss of control by human actors (see Chapter 4).

The *engineering* priorities are to establish the social and economic goals, non-functional requirements, standards and rules and to design and manage the systems in such a way as to ensure that these are implemented and guaranteed (*compliance*).

5.3.5 QUALITY ENGINEERING

Garvin [Gar84] distinguishes between five aspects of quality *engineering*:

- the transcendent quality view – quality as innate excellence.
- the product-based quality view – quality as the sum of specific product features. These features can be used to establish which characteristics define quality and how it can be measured. This makes it possible to compare the quality of products or indeed *CPS services*, e.g. based on the aspects outlined below.
- the user-based quality view – individual quality requirements and evaluation of products and their features.
- the manufacturing-based quality view – quality as the outcome of manufacturing processes. This is determined by the degree to which a product conforms to pre-established requirements or specifications.
- the value-based quality view – quality as the outcome of a cost-benefit analysis both from the customers'

[66] "There are three types of interdependent networks in today's critical infrastructure: (1) Supply Networks: transportation grids for electrical power, oil and gas; water distribution networks; transport/road tunnel systems; production flow supply chains; health care systems (2) Cyber-networks: tele-control and SCADA (Supervisory Control and Data Acquisition) networks, e-banking/finance networks, etc. (3) Managerial/organization networks where human resources supervise and/or utilize the services delivered by the above systems." [Uli, CNI06, BBB04].

and users' perspective and from the manufacturer's perspective.

In short, there is no single way of defining the quality of a product or *service* – it is always the outcome of numerous different comparisons and trade-offs between costs and benefits both in the *value chain* and on behalf of the user. Given the fluid and evolutionary nature of Cyber-Physical Systems and the way that they permeate a wide range of social and economic processes, their success will depend on the ability to accurately determine their quality and set quality standards for them, as well as to guarantee these standards in their specifications, development and integrated operation.

The previous sections have discussed a number of key quality aspects such as the *safety and security, dependability* and *usability* of CPS services, as well as the factors that are key to their acceptance, such as customisation, user freedom and compliance with *privacy* protection guarantees. Given the way that CPS components are networked and the increasingly open use of CPS *services* in new and unknown contexts, the *safety, security* and *dependability* quality requirements of Cyber-Physical Systems already constitute a major *engineering* challenge; see Chapters 3.2 and 5.2. Likewise, establishing the quality requirements for individual contexts and users and cost-effectively converting these requirements into valuable CPS products and *services* in networked CPS applications will also be extremely challenging for all the relevant actors. Consequently, it will be necessary to rethink every aspect of the *value chain* and work in a highly integrated manner in order to deliver these goals.

General quality *models* and *models* and standards for *Quality in Use* criteria – in addition to *Quality of Service* – are becoming increasingly important, as are their evaluation and the relevant *engineering* methods and processes (see e.g. the ISO 9126 standard in ISO/IEC 25000 [ISO10]). However, *domain*-specific standards for these aspects have been slow to appear, one example being the supplementary standards on ergonomic requirements in the EN/IEC 60601 [IEC10] series of standards for medical equipment.

In any case, these *models* and standards are by no means geared towards meeting the new challenges raised by the smart networked technology employed by Cyber-Physical Systems. The requirements with regard to the analysis of several different companies and *stakeholders*, alignment of their quality requirements and their implementation in *interoperable* architectures, interfaces and composition protocols or agreed *Quality of Service* guarantees have all yet to be met. The same is especially true of the need for enhanced *safety and security* and risk analysis methods for Cyber-Physical Systems (see also 5.2).

5.3.5.1 Enhanced quality models and integrated validation and verification methods

The key non-functional requirements in terms of the *usability* and manageability of Cyber-Physical Systems and the uncertainty with regard to how CPS services will be used and connected with each other in open application contexts both need to be taken into account in CPS applications' *safety* and *security* analyses. It will also be necessary to create enhanced, *valid* and binding regulations and standards. Furthermore, there will be a need for comprehensive quality *models*, methods and end-to-end procedures for the analysis, specification and guaranteeing of non-functional requirements during the design, operation and evolutionary use of Cyber-Physical Systems. These must be capable of taking into account the more extensive quality requirements of CPS. They will include interoperable *application* and *CPS platforms* with integrated architecture concepts and *best practices* for guaranteeing the required quality standards, as well as end-to-end *validation* and *verification methods;* see also 5.3.3 and 5.3.4. It will be necessary to develop appropriate and practical methods to enable the interdisciplinary analysis and modelling of quality requirements and their implementation in *interoperable* and binding *functional architecture* concepts at every level of the system's design (see Fig. 5.3).

There will also be a need for formal quality *models* that precisely specify the *Quality in Use* requirements in open and networked contexts of use. These will have to go beyond existing standards such as the supplementary standards in the EN 60601 series of standards for medical equipment [DKE10] or the ISO 26262 standard for *safety-related* electrical and electronic systems on board motor vehicles [ISO11]. Moreover, it will be necessary to provide reliable quality information backed up by *validation, verification* and certification procedures for the further development and quality assurance of Cyber-Physical Systems. This will require a wide-ranging and integrated research effort; see also the sections on enhanced *safety, security* and *privacy protection* in Chapter 5.2.

Interdisciplinary and integrated research: in view of the networking and openly interconnected use of CPS services, it will be necessary to address questions relating to *human-machine interaction* and *cooperation* at all levels of the system's design and configuration and not just with regard to the increased requirements in terms of risk analysis, *safety* and *security*. The investigation of human errors occurring during the use of CPS will need to consider the possibility of fundamental flaws in the design of the *human-machine interaction* (see also 4.1.1). It will also be important to take into account fundamental factors such as the need to ensure that Cyber-Physical Systems possess the appropriate functionality, are easy to operate and control and are both *dependable* and trustworthy, since these are key to users' acceptance of the systems which is in turn essential to their economic success. The complexity of the quality requirements that has already been alluded to at the beginning of this section means that it will be necessary to adopt an interdisciplinary approach to the *engineering* of the systems, the *domains* and their technological and business platforms, drawing on an ecosystem-based approach to *value creation*.

Fig. 5.5 outlines the tasks and importance of interdisciplinary *engineering* using integrated *model*, architecture and platform concepts. These concepts are determined by the social and economic requirements of the respective application *domains*. They require an exploratory and incremental approach to systems engineering, where the users and other stakeholders are engaged in an interactive and *participatory manner. They also require* technology assessments to be carried out at an early stage in the process.

The social debate and the interactive evolution of technology and society: *Engineering* methods require systematic support from innovation systems (see 7.1) such as *Living Labs* and testbeds. This includes a serious social, political and academic debate geared towards identifying the risks and potential negative consequences of CPS technology. It is also necessary to analyse what can be done to systematically counteract threats and unwanted disruptive effects in the economy.

Policymakers will have to use the requirements described above as the basis for developing *compliance* standards, frameworks, rules and regulations. It will also be necessary to represent these more extensive quality requirements and *compliance* standards in quality *models* for all the different system, design and organisational levels involved in the development and deployment of Cyber-Physical Systems; see Fig. 5.5.

5.4 SUMMARY OF TECHNOLOGICAL CHALLENGES

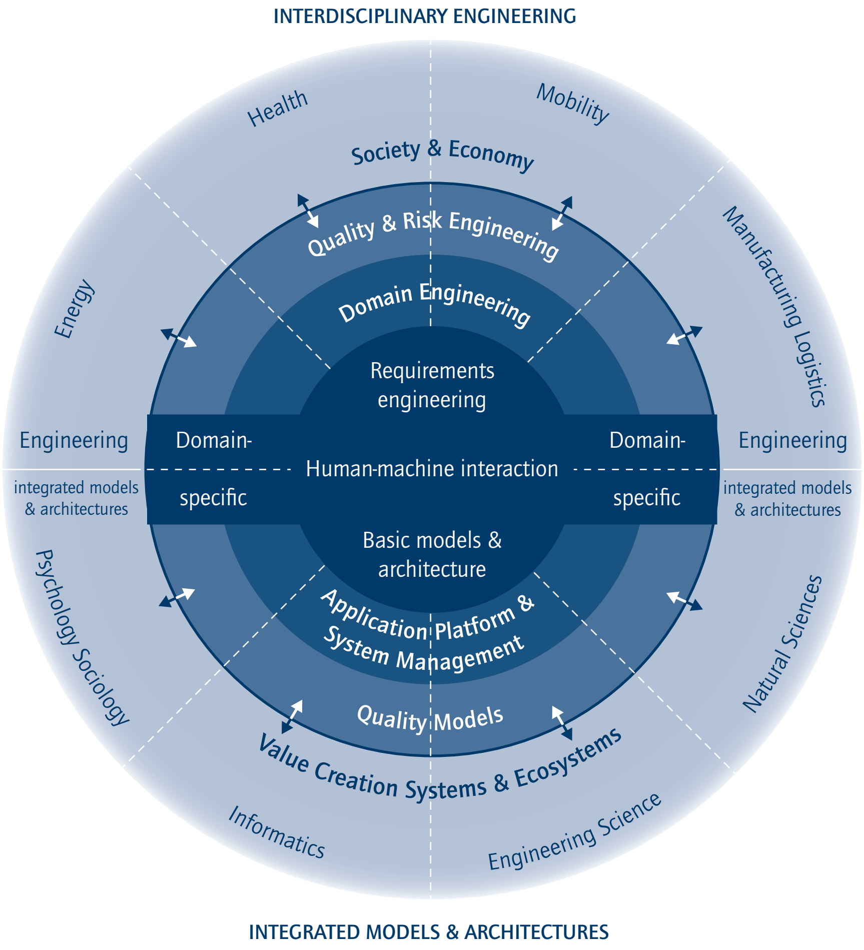
This section will present a summary of the challenges described above regarding the technologies and comprehensive *engineering* concepts required for the successful design, development and control of Cyber-Physical Systems. As far as the technologies needed to deliver the key CPS capabilities are concerned, the principal research priorities relate to the development of models, methods and techniques for

- comprehensive context detection and processing and requirements establishment and modelling,
- *human-machine interaction* and *cooperation* and
- *shared control* and *coordination in complex scenarios.*

The specific requirements include

- the establishment and validation of context and *domain models*, especially *user models* and social behaviour *models*; this will require
  - *intention recognition* models and methods,
  - action and interaction strategies for *human-machine coordination* and *shared control*,
  - conflict detection and resolution procedures,

Figure 5.5: Integrated engineering models and procedures and their interactive use in the interdisciplinary and participatory development and evolution of Cyber-Physical Systems


INTERDISCIPLINARY ENGINEERING
Health
Mobility
Society & Economy
Quality & Risk Engineering
Domain Engineering
Requirements engineering
Energy
Manufacturing Logistics
Engineering
integrated models & architectures
Domain-
specific
Human-machine interaction
Domain-
specific
Engineering
integrated models & architectures
Basic models & architecture
Application Platform & System Management
Psychology Sociology
Natural Sciences
Quality Models
Value Creation Systems & Ecosystems
Informatics
Engineering Science
INTEGRATED MODELS & ARCHITECTURES

- *models* and technologies to enable *self-analysis* and *self-diagnosis* in these complex scenarios,
- *multimodal* interfaces,
  - enhanced *sensor* technologies and networks,
  - processing and semantic aggregation of large data sets in *real time* and
  - semantic annotation of the data that have been captured and made available.

Furthermore, models, methods and techniques will be needed to enable cooperative and strategic behaviour. This may be autonomous in nature or involve *human-machine interaction.* More specifically, this will involve

- continuous context and process integration technologies; these will require
  - the establishment and *validation* of complex environment and *domain models*,
  - faster processing and communication speeds for processors and
- the establishment and *validation* of complex functional and non-functional requirements *models* together with the corresponding quality *models*,
- the development and validation of *interoperability*, architecture and composition concepts at different levels: *technical, semantic, user-visible*, controllable and manageable; see the section on *engineering* issues below.
- the development and *validation* of risk and conflict *models* together with procedures for detecting and reducing or managing risks and conflicts, including
- enhanced risk detection and assessment methods and techniques and
- decision-making strategies and mechanisms.

The list of requirements also features context-learning and behaviour adaptation *models*, methods and techniques, including

- the development and *validation* of learning, organisation, behaviour and cooperation strategies, together with planning concepts and methods and the corresponding technologies and
- the development of strategies and concepts for working with uncertain knowledge.

Integrated *models* are needed for all the relevant areas of application and scientific disciplines. These include *models* that enable networked physical awareness and control in *real time, models* of surroundings, situations, contexts, human beings, behaviours, problems and goals as well as task, behaviour and interactive control *models*. Moreover, interdisciplinary cooperation will be required to integrate system *models* from the fields of information technology, the natural sciences, engineering, cognitive psychology, the social sciences and economics; see also the section below on hybrid system and architecture *models* in *engineering*.

In terms of the technologies for detecting and fulfilling non-functional requirements, the key research topics are in the following areas:

Dependability and enhanced safety; priority issues include

- self-reflection, self-documentation and *self-healing*,
- an integrated approach to *safety* and *security*,
- *reliable multicore processors and safety architectures*,
- component description and testing at run-time so that binding contracts can be concluded. This includes the development and *verification* of *models* and techniques for describing and testing component features as well as contract mechanisms,
- development of global platforms with comprehensive, integrated *safety* mechanisms,
- enhanced development and *safety* standards,
- scalable *safety* concepts and theories,

- modular and hierarchical composition of *safety* goals, both with regard to common goals and with regard to the interactions between conflicting goals and how to manage them.

Security technology issues; the following will be required:

- technologies and procedures to enable efficient and lightweight cryptographic procedures with low resource consumption,
- *security* hardware technologies and procedures, especially *virtualisation* technologies designed to increase resource efficiency and reduce costs,
- *virtualisation technologies that enable the isolation and provision of secure execution environments, e.g. on CPS platforms*,
- procedures for assessing the trustworthiness of CPS components and
- comprehensive *security engineering* and management using concepts and technologies that enable secure hardware/software *codesign* based on *best practices* and standards. This should include life cycle management and built-in security principles such as *Security by Design* and *Security during Operation*.

Technology issues associated with *privacy protection*; the following will be required:

- Concepts, technologies, mechanisms and strategies for delivering the *privacy protection goals* of *transparency, intervenability* and *unlinkability* as well as the *security goals of confidentiality, integrity* and *availability,*
- security concepts that are built into architectures and design: *Privacy by Design,*
- procedures and technologies for guaranteeing privacy during operation and
- research and development of innovative technologies such as anonymous credentials, identity management systems and machine-readable *policies*.

The fact that Cyber-Physical Systems form part of open networks and operate in an integrated manner means that these technology issues need to be addressed as part of comprehensive interdisciplinary *engineering* questions. The key challenges and research topics in the field of *engineering* are as follows:

- *user-centric, participatory,* exploratory and *virtual* requirements establishment, design and assessment procedures,
- development of appropriate *models*, methods and procedures for establishing, configuring, *validating* and *verifying* requirements and for *tracking* them and ensuring that they are incorporated into the design and integration stages. Two particular challenges in this regard are the complexity of the requirements in an open context and problem space and the changes to requirements resulting from changes or adaptations to the context,
- establishment, scaling, structuring and formalisation of integrated *domain*, user, *stakeholder* and requirements *models*,
- development and *validation* of *viewpoint* and *scoping* concepts and the corresponding mechanisms,
- scaling of the above, including modular and hierarchical *refinement* and mapping onto *interoperable* architectures and onto interaction, composition and integrated behaviour *models*.

The particular challenges in this area concern the composition of locally and globally operating CPS *services* and architectures and the mapping and guaranteeing of non-functional requirements. This will require research into the following topics:

- development and *validation* of *interoperability*, architecture and composition concepts at the different system levels (*technical, semantic, user-visible,* controllable and manageable), i.e. the development of concepts to enable semantic composition and integration of components and *services* at these levels,

- enhanced concepts for interaction, negotiation, composition, cooperation and action,
- enhanced *refinement* and mapping concepts for implementing and complying with non-functional requirements and quality standards and
- enhanced contract mechanisms and solution and design concepts for providing *Quality in Use* and *Quality of Service* guarantees.

A variety of CPS-specific research requirements and topics also arise in more closed areas of application involving large-scale infrastructure systems such as power grids or distributed manufacturing networks, as well as the open social infrastructure networks and management systems that are superimposed on top of them, for example energy supply or traffic management in towns and local communities. They include the following:

- analysis and development of modelling and control concepts for complex, semi-autonomous systems, including ways of controlling any spontaneously occurring (emergent) effects both in the autonomous technology itself and in the relevant *socio-technical systems* and social environment,
- *security and dependability but also fairness and compliance of autonomous systems operating in social and economic contexts.*

The *engineering* challenges described above will require integrated hybrid system and architecture *models*; in this context, 'hybrid' refers to distributed

- analogue-digital control and management models,
- *human-technology interaction* and integrated behaviour *models* and
- socio-technical networks and interaction *models*.

The key requirements for realisation of these systems include the development and management of standard *domain models, interoperable application* architectures and *platforms* and cross-*domain* communication platforms and *middleware services* for Cyber-Physical Systems. Particular challenges exist with regard to modularisation, guaranteeing *interoperability* and ensuring the necessary *quality of service.*

6 BUSINESS MODELS AND ECOSYSTEMS

The trends in information and communication technology (ICT) that have been identified – i.e. the *Internet of Data, Things and Services, together with the* interactive applications and far-reaching capabilities of Cyber-Physical Systems – are causing a rapid transformation of economic processes and relationships. The process is characterised by a variety of changes in customer requirements, increased globalisation and internationalisation, market volatility[67] and growing pressure to become more flexible, cut costs and innovate. As a result, traditional economic models are shifting towards interactive forms of value creation, customer relations and problem-solving[68] that are increasingly characterised by cooperative corporate networks and *ecosystems* with new types of integrated *business models.*[69]

This chapter identifies the main factors and features connected with these changes. It also summarises the challenges for the economy and for companies and their *business models* in current and future CPS application *domains*.

6.1 STARTING BASIS AND CHALLENGES OF CHANGE

The smart capture and interactive utilisation of real-world data by Cyber-Physical Systems is revolutionising applications, uses and business processes. The global networking and cross-*domain* convergence of different sectors means that companies – whether they be large-scale enterprises or small and medium-sized enterprises (SMEs) – face considerable risks. At the same time, there are also enormous opportunities for them to develop their *business models*. This is because the *Internet of Data, Things and Services* and the new opportunities offered by Cyber-Physical Systems have created an environment for radical and disruptive *business model* innovation.

Technological developments and the ubiquity of networked *adaptive* technology have triggered a shift in products and services towards open, cooperative systems and applications based on interactive user involvement. This has boosted the pace of innovation and at the same time created greater market uncertainty. The extensive capabilities of *ICT* and CPS technology and the increase in customers' demands are causing a shift away from the traditional approach, where products are developed in isolation, towards the integrated and interactive delivery of comprehensive services tailored to particular use processes and contexts. The critical success enablers are now software competence and technology. Companies that used to focus purely on mechanical and hardware systems now have to acquire systems engineering and software competence – together with all the concomitant technological and *engineering* competencies. Many of the more traditional companies in the machinery and plant engineering sectors are finding this difficult to achieve, because their particular expertise in the past lay in the mechanical, electrical and control aspects of closed systems, and their system products were developed and marketed in well-established *domain*-specific *value chains* or networks. The sheer speed with which *ICT* has developed, and its deployment in traditional products, is already more than many companies can cope with. Not just SMEs but also many large corporations are poorly prepared for the challenges involved. In addition to rethinking their future *business models*, these companies are also having to build up software and systems *engineering* expertise and adjust their organisation to future requirements.

But business success and market share are not determined by technology alone. Technologies, particularly in the field of *ICT*, are subject to a rapid process of commodification.[70] Their development cycles are becoming shorter and they are also soon copied and made widely available to competitors.

[67] Events and the behaviour of market players; a distinction is drawn between the following types: event-related uncertainty (exogenous uncertainty) and market-related uncertainty (endogenous uncertainty).

[68] For more on the past development and forms of interactive value creation and innovation (open innovation), see [RP09a].

[69] The definitions of *ecosystem* and *business model* used in this study, as well as their components, are described in detail in 6.1.1.

[70] Nicholas Carr describes how IT thus becomes a commodity similar to people's domestic electricity supply; see [Car08].

If companies are to counteract this tendency, they have to differentiate themselves to a greater extent, for example by offering their customers even more customised solutions than is currently the case.

The changes in customer requirements brought about by Cyber-Physical Systems, and the possibilities opened up by comprehensive *context awareness*, penetration and support of processes in the workplace and in our everyday lives, require companies to acquire knowledge about customer processes and to build up a trusting relationship with the customer – irrespective of whether they are involved in manufacturing and logistics, healthcare or processes in people's private lives. The key enablers of competitiveness are now customer-oriented *business models characterised by interactive value creation in collaboration with the customer and with external problem-solvers*, as well as the use of networks of different organisations to realise innovation processes. As a result, traditional, isolated *business models* in manufacturing industry as well as the marketing of products are converging with software-driven *business models* that include the sale of licences or limited-term rights of use with maintenance contracts and service elements. Companies are thus moving from merely selling products to providing solutions and *services*. Early examples of this are the latest services offered by premium vehicle manufacturers BMW and Daimler, who are currently adding hybrid *business models* to their traditional role of selling vehicles. Under new brand names such as BMW Drive Now or Daimler car2go, they are offering mobility services that use Internet-based location, reservation and payment *services*.

Internet-based systems are also currently under development in other fields of application such as building and infrastructure management, healthcare, logistics and transport, the aim being to provide end users with comprehensive and prompt services. Examples from the healthcare sector include remote patient monitoring, *AAL* and online communities. In the field of smart homes and buildings, solutions are being developed for smart management of decentralised wind power or solar *PV* energy production systems. These examples demonstrate how companies have to develop new skills, try out new *business models* and display greater flexibility in penetrating new markets.

Cyber-Physical Systems are being jointly developed by companies of all sizes and from all industries. The "how it works" descriptions of the scenarios in Chapter 2 show how a wide range of different components, *services* and economic activities have to be integrated in the context of Cyber-Physical Systems. Communication, networking and *interoperability* are fundamental capabilities of these components at all levels within the system. Companies in different branches of industry have to expand their software and CPS competence, become more open, network their respective systems, cooperate more with software and telecommunications providers and in this way bring together the competencies required for developing and operating Cyber-Physical Systems and the associated *services*. Problems and application scenarios are analysed in collaboration with customers, and integrated solutions are developed and tested, enabling individual companies to extend their portfolios by collaborating with others. New forms of cooperation and competition are emerging within so-called *ecosystems*. In contrast to traditional value creation concepts – in which companies are organised hierarchically or in networks and focus on increasing productivity or flexibilisation – the idea here is to achieve interactive value creation and customer integration [RP09a] with the aim of becoming more innovative.

To achieve this, companies are having to operate with greater agility in development and production by developing and testing out interdisciplinary *engineering* methods; see also Chapter 5.3. The main focus is on developing concepts that offer *customer value*, identifying acceptance factors and enhanced quality *models* and cross-*domain* architecture concepts, as well as integrated *engineering* within *value networks* and *ecosystems*. This is going to have an impact on the lines of demarcation between companies and their relationships with one another – and in this context also on the question of how to share future investment, revenues and profits and indirect and long-term *returns on investment (RoI)*. It will also be necessary to align the long development cycles and life cycles of the mechanical engineering sector with the short cycles found in information and communication technology. In manufacturing industry in particular, it will be important to develop mechanisms that enable manufacturing technology and control systems to be easily adapted to the changing requirements of customers and IT without having a detrimental impact on their operation. Particular challenges arise in connection with the firmware of legacy systems and its incorporation into modified system and IT infrastructures.

The complexity of Cyber-Physical Systems and the increasingly context-dependent tailoring of products and innovations call for a greater degree of specialisation amongst companies. When highly specialised CPS components and *services* are being created, it is essential to keep in mind that their individual features should complement one another in order to ensure the required application behaviour and thus an adequate solution. In addition to the interdisciplinary *engineering* challenges related to the design and construction of *interoperable*, integrated CPS solutions and cross-company platforms, this calls for new business models that operate within *ecosystems* with a variety of organisational structures, complementary value creation architectures and open platform strategies.

Open platform strategies[71] with transparent architectures and open interfaces are required, in particular to take advantage of the extra innovative potential arising through the interactive and *participatory* engagement of customers, new, external technology-based companies or developer networks, but also in order to create *transparent*, trustworthy and *dependable* structures[72] that meet the key quality and acceptability requirements of customers in terms of individual system *usability*, protection and *safety* and *security*.

Examples of new forms of *ICT*-based *service* and platform strategies include collaborations between *mobile device* suppliers to create joint *app* stores[73] on the Internet, or Google's platform strategy with the Android operating system as cited in [Cus10]. [Fra03a] also analyses the change in forms of corporate management and organisation triggered by the Internet economy, using the example of *business webs* and technology platforms for mobile *services*.

The sections that follow focus on the future direction of the *business models* of CPS companies and the associated value creation architecture in *ecosystems*.

6.1.1 DEFINITION OF TERMS

A *business model* is a simplified representation of a company and an abstract account of how its business and value creation processes function. It provides a compact description of a company's organisational structure, value chain and products. A variety of definitions exist, but the one used here is taken from Stähler, as summarised in [Kit09, p. 31].

According to Stähler a *business model* consists of three main elements:

[71] Cusumano defines a platform strategy, as opposed to a product strategy, as follows: "[...] it requires an external ecosystem for the generation of complementary products or service innovations and the creation of positive feedback between the complement and the platform". [Cus10, p.22]

[72] See the individual and social acceptance and success enablers for Cyber-Physical Systems in Chapters 3.4 and 4.1.

[73] An online store for applications that run on *mobile devices*.

- *Value proposition*: a description of what value a customer or a partner can receive from the business. This part of a *business model* answers the question: What value does the business create?[74]
- Value architecture: a description of how the benefit to the customer is generated. It delineates the value chain, the economic agents that participate in the value creation and their roles. It answers the questions: How is the value being created and in what configuration? What is being offered and on which markets?
- Revenue model: a description of the sources of income for the firm. It answers the question: How will the business earn money?

It is this definition that provides the basis for the analysis undertaken in the remainder of this chapter. A *business model* can describe an individual company or an entire industry.

Once the analysis of value creation is extended beyond the bounds of a single company, *value creation systems* or *value networks* start to come into play. Since *value creation systems,* as opposed to *value chains*, do not necessarily have to be linear, they are better at depicting more complex structures and value creation architectures.

The particular manifestations of *value networks* that have come into existence as a result of the framework within which the Internet economy operates are referred to as *business webs*. In [Fra03], a distinction is drawn between two roles that companies can play within *business webs*: they can be so-called 'shapers', which represent the core of a *business web* and control one or more core subsystems as well as central standards and interfaces; or they can be so-called 'adapters', which create complementary products or services in line with the shapers' instructions. This distinction is frequently found, for instance, in the software industry, in which a shaper – for example the provider of an operating system – makes standards and interfaces available to market players and the latter, as adapters, develop programs for this platform.

The term *ecosystem* is borrowed from the field of biology and refers, in the economic context, to a group of market players who maintain a commercial relationship with one another, exchanging goods, information, *services* and money. The term *ecosystem* is wider and more general than the term *value creation system*. For example, non-profit actors such as education providers and research organisations as well as political entities or associations can form part of an economic *ecosystem*, whereas the term *value creation system* usually refers to the relationship between companies and to the creation of economic excess-value.

Innovation is the process of successfully introducing something new onto the market. Innovations often go through a process that starts with the identification of a problem and its potential before moving on to the generation of ideas and ending with the successful implementation and marketing of a new solution. The term innovation can refer to products and *services*, processes and procedures – and in a wider sense also to *business models*. Unlike inventions, one only speaks of an innovation when an idea has been implemented and successfully used, achieving a certain level of market diffusion. Innovative *business models* are characterised by innovation in terms of the *value proposition*, the value creation architecture or the revenue model. Such innovations have the potential to radically alter existing market structures or *ecosystems*. Examples include "freemium" *business models* on the Internet – for example the last.fm music service or the communication platform Skype – where an Internet platform offers a free service to large numbers of users. The company makes its money from the small percentage of users who are prepared to pay for a premium service.

[74] The key is not just what the supplier promises but also the benefits the customer expects from it. Kaplan and Norton [KN04] place the value proposition at the heart of corporate strategy and corporate success: "Strategy is based on a differentiated customer value proposition. Satisfying customers is the source of sustainable value creation."

A particular type of innovation, known as disruptive innovations [Chr97], have the potential to revolutionise a market by changing a product or *service* in a way that the market did not expect, thereby threatening the existence of established market players. In the past, the Internet has triggered such disruption on several occasions, resulting in dramatic changes in the market. One example is provided by the music industry, where revenues from traditional CD sales have been declining for years under the impact of digital distribution channels. Such market mechanisms can be transferred to the context of Cyber-Physical Systems and are therefore extremely significant, as illustrated in Section 6.3.

6.2 THE IMPACT AND OPPORTUNITIES OF CYBER-PHYSICAL SYSTEMS WITH REGARD TO BUSINESS MODELS AND ECOSYSTEMS

A holistic approach enables us to examine the three elements of a *business model* based on Stähler's description (*value proposition,* value architecture and revenue model) and draw up an initial description of possible CPS *business models.* It is important to understand that the final result will not be one single universally applicable *business model*. Cyber-Physical Systems can have various different niches, approaches and potential uses, but also require adjustments within the relevant companies. All we can do here is describe the mechanisms and drivers and offer some examples of the specific changes that may be necessary. Each company will have to decide what its own individual reaction to these possibilities will be, depending on the structure and maturity of the industry it operates in, as well as its past activities, its current core competencies and its strategic goals. It is thus not possible to make any universally applicable claims about the prospects of success of specific *business models.* The conclusions drawn from our analysis are summarised in Chapter 7.

All analyses and observations do have one particular conclusion in common: any future-proof propositions and *business models* will have to contain a higher proportion of software and services (even if these are delivered by human beings), because differentiation from competing products and improvement of the overall product will increasingly be based on software, configurability and customisation through interaction with the customer, frequently at runtime. The proportion of the value of the overall product attributable to mechanical and hardware components will decline – and the risk of these components becoming commoditised will increase.

The need for companies to address Cyber-Physical Systems and their demands is now generally recognised. In one survey (see Appendix C), companies were asked, among other things, for their assessment of whether Cyber-Physical Systems would have an impact on their business model. Only nine percent said this would not be the case, whereas some 38 percent believed that they would need to make adjustments but could not yet predict the precise impact that Cyber-Physical Systems would have on their business.

6.2.1 VALUE PROPOSITION

A *business model is essentially based on a value proposition,* in other words a statement of the benefits that can accrue to the customers or other partners from their relationship with the company. The key question is therefore: what value does or should the company create in order to survive in the market?

On the one hand, operational requirements and the problems encountered by users determine the excess-value that a company has to generate. On the other hand, they also determine how much customers are prepared to pay for particular products and services (see also 6.3.3). The *value proposition* – and thus the clear excess-value for the customer – plays a central role in any *business model,* irrespective of whether it is directed towards business customers or end customers. Generating this excess-value increasingly calls for companies to focus on individual customer requirements and come up with specific, comprehensible and immediate proposed solutions. The ubiquity of Cyber-Physical Systems and the rapid spread of sensors, actuators and *mobile devices* in every area of our lives opens up huge scope for the customisation of products and services.

Customer value cannot, in principle, be determined at a theoretical level. It is therefore helpful to study the market in order to gain an understanding of what customers perceive to be beneficial (see also Chapter 5.3 on the central importance of *requirements engineering*). For example, customers find concrete excess-value in:

- a proposition that meets their needs by delivering the required service at as low a price as possible (without, as often happened in the past, being given a package of services, some of which they will not use),
- simplified and accelerated processes,
- assistance, comfort and excess-value services – for example mobility and security services – as described in the scenarios in Chapter 2.
- access to a broad range of optional, combinable, personalised or personalisable additional services.

Common to all of these aspects is the fact that the *services* and products are increasingly configurable and customisable. This is technically possible because:

- more of the functionality of Cyber-Physical Systems is based on software, data and their interpretation, and software configurations and versions will in future make it possible to offer customised versions of products at an affordable price,
- the manufacturing of devices and components is increasingly controlled by software and is therefore becoming more flexible, enabling individual wishes to be directly assimilated into the manufacturing process.

For successful marketing, it is necessary to ensure a high degree of *transparency* regarding the *services* that are on offer, including all the possible combinations and extensions. As these are rapidly increasing in number, companies need to develop new marketing concepts. At the same time, there are a number of technical challenges relating to variant and configuration management and system *interoperability* and integration. The result is that software is becoming the dominant factor when it comes to using Cyber-Physical Systems. This is because it provides the key innovations that result in particular from data interpretation and application communication and control, not only in the products themselves but also in terms of their manufacture and marketing and the interaction with customers.

If they are to deliver on their *value proposition*, the companies concerned face new tasks in connection with Cyber-Physical Systems which will in turn call for new capabilities. Going forward, it will be important to make the desired information and *services* available to users at all times and irrespective of their location. This is connected with the need to control data and its transfer between the actors – for example *services* and information providers and, in some circumstances, different systems. The value created by a company in this context might, for example, come from the dynamic negotiation and automatic conclusion of contracts. What is crucial is that the company concerned should be in a position to negotiate services and cooperation agreements, adapt them to changing situations and, if necessary, bring in new *services*. The provider also has to play the role of moderator and/or adviser in order to negotiate customer goals, requirements and interests with other partner companies. Another important capability will be the ability to detect and fix faults in systems, information and *services*.

Companies from the world of embedded systems, for example, will face new challenges. Their traditional business of selling the highest possible volume of products and devices at as high a margin as possible will be supplemented or even replaced by *business models* that use the Internet as an additional medium for advertising, selling and operating as well as for interacting with customers and engaging them in networks.

6.2.2 VALUE CREATION ARCHITECTURE

A *business model* also includes the value creation architecture which describes how the customer value is generated. This architecture includes a description of the value creation stages, the economic players involved and their role in the value creation process. It provides an answer to the question: Who delivers the customer value and in what configuration?

Contextual information is resulting in customers being more closely integrated into the process of evolutionary value creation. They are no longer just users of Cyber-Physical Systems but also actively generate information and are involved in the design of the CPS *services*. This is a key aspect of Cyber-Physical Systems, as it results in a variety of network effects. Thus, for example, the quality of traffic information increases with the number of vehicles that are providing data; one example of this is the "green wave" *app* Guru (see Chapter 4.1.4, [KPM11, Sch11]), which uses car drivers' own mobile devices to network them and provide information on traffic light phases. At the same time, the willingness of car drivers and freight transport companies to pay for traffic data also increases in proportion to the data's quality and quantity. Examples of network effects can also be found in the world of IT and the Internet, for example the irresistible growth in the use of auction platforms such as eBay; sadly this is an area where German providers are falling behind other companies, especially in the US.

These types of platforms and infrastructures (see Chapter 5.3) open up new scope for collaboration between people and processes across different companies, leading to the launch of cooperative, customer-centred value creation processes. With the help of Cyber-Physical Systems, these processes will increasingly move towards intangible value creation as well as hybrid products and *business models*, ultimately strengthening the services sector.

6.2.2.1 Value creation in companies

Companies have to adapt themselves and their value creation processes to market conditions, which are changing as a result of the impact of Cyber-Physical Systems. The market is becoming more volatile and more complex, and profitability may well be reduced. Cyber-Physical Systems cause market boundaries to shift and facilitate the entry of new players. The convergence of markets resulting from the advent of Cyber-Physical Systems lowers the entry barriers to these markets, especially for niche providers. One example is the field of electric mobility, in which energy utilities, IT, software and electronics firms are all set to become players alongside traditional automotive manufacturers and their suppliers.[75]

Further shifts in the structure of industries and the distribution of market power are being caused by a wave of consolidations or horizontal mergers. The new systems suppliers will be companies that have the required technological basis to map highly integrated systems. These may be SMEs – for example in the case of highly integrated mechatronic systems – or e.g. battery manufacturers that supply highly integrated energy systems. On the other hand, large IT companies such as Apple, Google, SAP or Microsoft could become systems suppliers if they succeed in acquiring the required *know-how* to produce, for example, highly integrated software systems. Network effects mean that as long as these companies also have CPS competencies, they will be able to account for most of the value creation, and thus also receive most of the ensuing revenues. They will also

[75] See, for example, [BBD+11].

have an opportunity to integrate or link up Cyber-Physical Systems with existing in-house applications such as ERP systems.

The growing pressure to drive down costs and the need for greater flexibility is causing companies to optimise their processes. In manufacturing companies, this is usually achieved through increased automation and the deployment of IT systems. The need for integrated, flexible manufacturing systems opens up market opportunities for Cyber-Physical Systems in the fields of factory automation and logistics.

Flexibilisation of operational processes is becoming even more important for companies because

- customisation is forcing them to develop the ability to deliver new product versions and a wide range of variants with shorter development cycles,
- marketing is increasingly taking place via the Internet, so success or failure is becoming visible more rapidly,
- software is accounting for a growing proportion of the overall system, and the innovation and release cycles for software are very short.

These short cycles entail a number of additional challenges: companies have to adjust their internal development and maintenance processes and configuration management because of the wide differences in the life cycles of individual components. This calls for comprehensive information of the kind that can be captured by Cyber-Physical Systems.

A similar development can be expected for Cyber-Physical Systems to what has already been observed in the world of the Internet for many years: platforms will become established as central elements of Cyber-Physical Systems, and companies or market players who develop or operate these platforms will enjoy a correspondingly strong position in the market.[76]

The way that a company's value creation can change as a result of Cyber-Physical Systems can be illustrated using the *smart grid scenario* (see Chapter 2.4).[77] In the future, instead of the traditional electricity supplier, there will be several market players such as metering operators, operators of energy trading platforms and the underlying infrastructure, *virtual power plant* operators, etc.

This scenario also shows that value creation will not only change within companies but also within the *ecosystem* in which they are embedded. Thus, in this particular scenario, electricity customers who also generate energy (*prosumers*) are brought together to form *virtual power plants.* This creates an *ecosystem* consisting of *prosumers*, consumers, generators and storage facilities. Transactions between these actors are carried out via a trading platform. In the case of the *smart grid* scenario – as in the others – it becomes clear that Cyber-Physical Systems will in particular facilitate the long-term survival of small and medium-sized enterprises, since they often combine agility and innovation, which are two key competitive factors in the market for Cyber-Physical Systems.

6.2.2.2 Value creation in ecosystems

As Cyber-Physical Systems become increasingly complex – see for example urban mobility systems, the healthcare system and the electricity supply system – the need also arises for increasingly complex and comprehensive solutions. In the future, it will only be possible to guarantee these solutions through cooperation between different industries.

Species-rich business *ecosystems* are starting to emerge, develop, compete with and complement one another. In this context, *ecosystem* should be understood as the networked collaboration of various different company roles. The term describes strategic alliances or cooperation between groups involving considerably more actors than is normally the case in traditional corporate partnerships. Examples of such *ecosystems* that already exist are the SAP Business

[76] For an overview of business models for mobile platforms, see [JCKC11].

[77] 77 See also [LMK09].

Ecosystem or the Android *app* store. Such *ecosystems* are typically built on common platforms and standards.

Web-based Cyber-Physical Systems predominantly come about through economic *ecosystems*. Individual companies join together to form sophisticated economic *ecosystems* that are intended to be sustainable. Their creation depends on whether the companies involved can find a revenue-sharing model that is acceptable to all those concerned or whether they block each other in bilateral or multilateral negotiations. There is thus a need to further investigate the incentive systems and preconditions required for the success of such cooperative ventures. Value and revenue streams in ecosystems that enable all the participants to operate sustainable *business models* can provide a long-term source for a wide range of innovations in the future Cyber-Physical Systems market. In turn, Cyber-Physical Systems make this new type of cooperation between companies possible by removing existing, isolated silos in the *value chain* and replacing them with an open *value creation system* in which individual *ecosystems* develop into virtual marketplaces.

The most important feature of these new marketplaces will no longer be the traditional customer-supplier relationship but rather business platforms on which providers and customers can meet and interact with each other, even on an ad-hoc, context-dependent basis. Innovation is possible and necessary in all aspects of value creation, from the supplier to the end customer. This is true for development, production and commercialisation, operation and maintenance, service provision, consultancy, adaptation and ongoing development, but also in connection with medium- and long-term strategic development and evolution; see Chapter 3.6. Thus, for example, a medium-sized company that previously only positioned itself as a supplier in the value chain can now link up with other companies to deliver integrated solutions and position itself accordingly.

The networking and digitalisation of individual subsystems and partners that is an inherent feature of CPS acts as a driver of a *service*-oriented and collaborative form of value creation that can be carried out interactively between suppliers and customers across the entire *value chain*. The opening up of the architecture of the CPS marketplaces lowers the entry barriers for new companies and niche suppliers, as they are no longer forced to develop and produce complete systems in order to be able to participate in the market. In this context, the question arises as to whether vertical or horizontal integration measures within the *value chain* are required in order to develop CPS propositions. Digitalisation and networking of processes that used to be analogue and had a low level of interconnectedness provides a basis for the addition of new participants to the overall value creation process. In particular, it can be expected that software companies will make specific modules[78] or standalone components available that – in conjunction with suitable hardware and infrastructure or as additions to existing solutions – will enable new services to be provided.

Within *ecosystems*, new types of intermediaries will take over the service functions that will become possible in these new marketplaces. It is possible to envisage new service roles and functions developing in marketplaces in both the *business-to-business*[79] and *business-to-consumer*[80] markets. Overall, opportunities will arise for companies to perform new roles and functions, while existing roles will change.[81] The new CPS *ecosystems* will be characterised by the following activities:

[78] One might think, for example, of *software agents* (in the sense of standard software modules) that perform specific functions and can be integrated into existing applications by other market players or by the end user.

[79] Services related to motor car or damage insurance, logistics services, services for customers abroad, mechanical engineering industry, etc.

[80] Future car sharing centres, energy marketplaces, logistics services for individuals, etc.

[81] Many new service roles and the corresponding functions were described in the TEXO application scenario that formed part of the THESEUS Project (a research programme of the Federal Ministry of Economics and Technology “ […] with the aim of simplifying access to information, networking data on new knowledge and creating the basis for the development of new online services”); see [BMW10b] .

- supply of components and upstream products for setting up a Cyber-Physical System,
- development and production of components for creating CPS infrastructures,
  - actuators and sensors,
  - communications technology,
  - data centres,
- operation of CPS communication platforms, see Chapter 5.3 and Appendix B,
  - communication networks,
  - processing time,
- operation of Cyber-Physical Systems,
  - hardware integration,
  - provision of basic Cyber-Physical System *services* for *application* and *CPS platforms*, see Chapter 5.3 and Appendix B,
  - providing guarantees to customers, i.e. of non-functional requirements – see Chapters 5.2, 5.3.5 – and of *Quality of Service services for the CPS platform* in Appendix B,
  - structures and propositions for simple addition of services,
- CPS support *services*,
  - billing,
  - *authentication*,
  - monitoring quality in use and quality of *services*, communication and data,
  - *interoperability services,* e.g. converting between data formats and *services* – see Appendix B, Section B.3.7 – in particular between the *ontologies* of different applications and translation between standards,
- CPS marketplace operation,
  - open marketplaces under the control of a *community*,
  - closed marketplaces under the control of a company,
- provision of *services* for end customers,
  - integration and provision of CPS *services*,
  - reduction of complexity for customers,
  - creation of user-friendly interfaces for *human-machine interaction*,
- provision of CPS support *services* for end customers,
  - *service catalogue for quality assessment and information and improved searchability,*
  - certification of adherence to quality and *compliance* standards,
  - anonymisation of *service* use,
  - adaptation of external *services* to end customers' registered preferences,
  - neutral negotiator for automatically generated contractual relationships,
- provision of support for *service* providers,
  - platform for fully or semi-automated *service* brokering,
  - selling on of bundled user rights for *services* and platforms,
- provision of enhanced-value CPS *services* for *service* providers,
  - as for end *customer services, but for developers of enhanced-value services*,
  - *service* bundling,
  - data aggregation, for example for situation reports or statistical analyses.

The tasks of *service* providers can be divided into several roles that can be performed jointly and by different companies. These include development, production and commercialisation, operation and maintenance, integrated services, i.e. consultancy, adaptation and ongoing development, as well as strategic development and evolution (see Chapter 3.6), particularly in the form of *domain engineering* and the associated evolving applications and platforms; see Chapter 5.3.4.

New roles and functions were also identified in the scenarios in Chapter 2. Thus, for example, in the field of *smart mobility* there will be a need for traffic management systems as well as for integrated travel and weather *services*. Moreover, additional payment platforms like Google Wallet [WAL] will be created that will enable increased use of online and mobile payment systems. In the field of *E-Health*, there will be opportunities for healthcare platform operators. And in an e-government scenario, it is not just companies that will take on new roles and functions but customers as well. Here – as elsewhere – they will not just be CPS users but will also actively generate information and interactively influence the behaviour of the systems.

The *smart grid scenario* (see Chapter 2.4) opens up the market for metering service providers, *virtual power plant* operators or operators of energy trading platforms – both for IT infrastructure operators and providers of trading, auction and other services. New infrastructure service suppliers will also enter the market in the field of *autonomous driving.* Major traffic routes, digital networks, multi-storey car parks and parking guidance systems will be operated by private companies. *Ecosystems* will come into being as various players join forces with one another, for example *mobile device* manufacturers, weather, traffic and infrastructure information *service* providers, *app* developers, communications companies for data transmission, platform operators[82], *sensor* system and infrastructure manufacturers, *premium lane* operators, suppliers of vehicle *services* such as hiring and billing, toll collection companies or the operators of traffic guidance systems.

In future *ecosystems*, approaches from the current *Web 2.0 that have been* tried and tested in networks and *communities*, mainly in the *business-to-consumer sector,* will be adopted in the corporate environment to form so-called *business webs.* These excess-value networks where several service providers jointly generate new *services* are thus a key requirement for survival in a competitive environment.

The companies involved first have to adjust to this new form of sophisticated, evolutionary, distributed development of systems, products and *services* such as maintenance, operation, integrated services, continuous development and improvement – see Chapters 3.6 and 5.3 – and the related challenges. Firstly, the distribution of roles within such a cooperative system is complex, and secondly, the companies involved in the system will change depending on the context and with them also the constellation of partners within the *ecosystem*. These different configurations will in turn result in different life cycles for the components and *services*.

In order to deliver these *services*, it is necessary for the partnerships within the *ecosystems* to make joint investments, for example in infrastructure, open platforms, standards or training. However, this means that the costs and *RoI* models for components and *services* in the *business models* will also become more complex: more actors and products with differing life cycles will have to be taken into account. Furthermore, the components in the *value chain* differ in their significance to the companies involved.

6.2.3 REVENUE MODEL

In addition to describing the *value proposition* and the value creation architecture, a *business model* also describes what revenues the company generates and where they come from. Future income determines the revenues and value offered by the *business model* and thus also its sustainability. It answers the question: How will money be earned? This part of the b*usiness model* is called the revenue model.

Many software manufacturers or *service* providers already offer free basic functionality as part of freemium propositions so that users become accustomed to using a product and will subsequently be prepared to pay for additional functionality or premium *services*.

Cyber-Physical Systems make further revenue models possible, as well as enabling changes to existing payment

[82] See for example [Oct].

models. In the future, providers will be able to operate in the market as suppliers of fully integrated systems or as specialised service providers for individual components. In addition, there will also be platform suppliers who make their money from the use of the platform. Cyber-Physical Systems will make it possible for billing of data and information *services* to be based on individual units of information. *Business models* with information at the core of their value creation processes will thus become the key to success for many suppliers. In addition, prices will become increasingly variable. In the future, billing will be based on time, location or usage profile. This will be possible because there will be more and more usage-based billing models and payment will become even simpler.

6.3 THE DISRUPTIVE INNOVATIVE POTENTIAL OF CYBER-PHYSICAL SYSTEMS

This section describes the potential offered by Cyber-Physical Systems for triggering disruptive innovations. A disruptive innovation has two fundamental phases. First, a new market player (disruptor) occupies a new market niche by serving customers who have a different requirements profile from the customers of the established players (incumbents) in an existing large-scale market. At this stage, the established players ignore the niche because it would be unprofitable for them to serve such a small market and they would rather concentrate on more profitable projects. This gives the disruptors time to further develop their technology and customer base.

The time then comes when the disruptors have learned how to reduce their manufacturing costs and the product itself has reached a level of maturity that allows the disruptor to leave the niche market and enter the incumbents' market, offering cheap products which possess the features required by the market.

This forces the incumbents to adjust their product portfolio or to develop their own products using the new technology. But because they have a different technology base and different cost structures, they have no chance of catching up with the disruptor, who has already gone through several learning loops with the new technology. The result is that the established player increasingly focuses on the high-end market and loses market share to the disruptor.

Disruptive innovations are thus fundamentally strategic as well as technological. Disruptiveness is not actually a property of a technology but rather the effect that technology triggers in an existing market. A technology only has a disruptive impact if it is ignored by the existing market players in its early stages. One example of a disruptive innovation was the car. It initially had no impact on a transport market dominated by horses and railways. In a context that was at the time characterised by high prices and inadequate infrastructure, it was initially unattractive to the mass market. Consequently, it was at first sold as a luxury item to a limited number of customers. It was only with the advent of the cheap, mass-produced Ford Model T that the car started to be used more widely, triggering a disruption of the transport market. Another example is the replacement of sailing boats by steamships. Initially the poor *reliability* of the latter meant they were unsuitable for long voyages and were thus only used on inland waterways. However, a process of continuous improvement eventually enabled the steamship to compete with sailing boats, triggering a disruption.

E-Health

Expensive and capital-intensive equipment is frequently required in the field of healthcare. However, there is scope for achieving revolutionary - possibly even disruptive – innovations by networking less complex pieces of medical equipment. Many types of medical technology are set to be taken from their usual setting in healthcare institutions and transferred into the home environment. Equipment such as electronic scales and blood pressure monitors are already available for domestic use. The increasing use of sensors and smart systems for measuring vital parameters will make it possible to continuously monitor patients with critical health conditions in their homes. This will enable decisions on when to admit an at-risk patient to hospital to be made with greater accuracy. The result will be better levels of utilisation of expensive, more sophisticated hospital equipment and more efficient patient care, whilst also creating gaps in the market for low-end medical equipment. This trend displays a disruptive pattern. However – in contrast to an unregulated market – *business models* cannot be freely established in this sector. The highly complex funding structure of the healthcare sector, with its many different actors, makes it more difficult to change processes and as a result hinders business and product innovation.

Smart mobility

This scenario illustrates the significant potential threats to established market players. The scenario analyses intermodal transport options for private mobility – in other words, the use of various modes of transport such as cars, trains, aircraft, etc., which are integrated into an overall mobility system. Individuals are thus able to optimise the duration and cost of their journeys and minimise their environmental impact by using a smart system that suggests the best route based on their instructions and preferences. The first initiatives providing Internet platforms offering this type of comfortable travel arrangements already exist today: Deutsche Bahn railways already links train information with bus and tram information on its online booking site. Meanwhile, Citroen goes one step further by having an Internet platform that offers end customers a choice between travelling in their own car, by train or by air. Tamycar, on the other hand, provides private cars for hire, thereby competing with established car hire firms and *car sharing schemes*. These technological solutions are part and parcel of a general trend away from private car ownership and towards car sharing or car hire. The expansion of electric mobility also entails the possibility of further disruption.[83] It is a technology that could potentially replace the internal combustion engine and open up opportunities for new market players in the global *value network* of the automotive industry.[84]

Smart factories

The examples of order processing given in this scenario are very similar to the *virtualisation* of sales channels in e-commerce: logistics suppliers or online marketplaces such as myhammer.de and eBay are able to coordinate collaboration between different companies and create a joint customer interface. This allows specialist companies to emerge that no longer actually make anything but instead use information technology to coordinate manufacturing companies and provide a customer interface. These central companies or corporate partnerships can thus build up a network of manufacturing facilities, enabling a more flexible response to customer requests. As such, they could represent a threat to manufacturing-based companies which can process large orders but are unable to respond flexibly to changing requirements.

When it comes to product and production development, machinery, plant and component manufacturers can succeed in the market if they equip their components with open, standardised interfaces that enable various types of equipment from different manufacturers and different owners to be combined (“plug and work”), rather like the use of USB sockets on PCs. These components can be installed in any system, unlike proprietary components where a new interface has to be defined and implemented for every new installation. This underlines the need for *interoperability* between software or Internet technology and the hardware used by manufacturing facilities.

[83] By 2017, Pike Research estimates that there will be 13.9 million electric vehicles on the road. North America will account for the greatest number, with 4.9 per cent of all light duty vehicles being electrically powered by that date [Pik11].

[84] See [BBD+11].

Autonomous driving

This scenario primarily investigates the exchange of information between two vehicles in order to enable *autonomous driving*. Irrespective of whether information is exchanged from vehicle to vehicle or indirectly via a *back-end infrastructure,* this is a field that offers huge potential for innovation. Provided that the systems can be made safe enough and there is an adequate infrastructure – including both the mobile communication network and the fixed local infrastructure – autonomous vehicle convoys could compete not only with conventional cars but also with other means of transport. In particular, they have the potential to revolutionise *car sharing* services.

6.4 SUMMARY

Cyber-Physical Systems offer considerable innovative potential in all the areas examined – in some cases with disruptive consequences for established market players. One feature common to all the scenarios is the fact that the new competitors can come from other industries, in particular from the *ICT* and software sectors. New entrants to the market with experience in software development and the operation of *service* portals and server centres have sufficient expertise to develop and operate high-availability Internet applications. Commissions and cooperative ventures with companies in various different sectors can enable them to acquire enough application and *domain* knowledge to be able to subsequently market their own *services* and products in the markets in question.

An analysis of future *business models* leads to the conclusion that there will not be one single *business model* that fits all markets and all companies. On the contrary, Cyber-Physical Systems allow for many different niches, approaches and potential opportunities, although these do also require adaptation on behalf of the companies concerned. The scenarios that have been described and the potential changes that they imply underline the huge differences between the various areas of application in terms of innovations and the changes that are required in their *business models*. For this reason, it is only possible for the present study to describe the contexts, mechanisms and drivers and provide a few examples of specific changes that can be expected to occur. The biggest changes can be expected in all those cases where Cyber-Physical Systems trigger disruptive innovations. It is therefore important to tap into the far-reaching potential of Cyber-Physical Systems and control their disruptive impact on the market and on application systems. For this reason, it is essential to systematically establish sustainable innovations in regionally and globally networked *ecosystems*, thereby creating the capability to develop integrated and interactive CPS solutions.

Heterogeneous innovation networks that bring together actors encompassing a wide variety of competencies, roles and company sizes are an important part of these *ecosystems*. Operating as cooperative ventures and value creation partnerships, they serve to integrate CPS component innovation cycles that evolve differently and have different durations, as well as different innovation and development cultures. Their interaction can give rise to mutually complementary innovations, strategies, *business models* and *business model* innovations; see also [Che06]. Stähler [Stä02] differentiates between value innovation, architecture innovation and innovations related to revenue models and coordination mechanisms.

What is required is a combination of technology-based start-ups, established SMEs that have close relationships with their customers and large global companies with the durability to strengthen the network's stability and trustworthiness. Together, these players will have the ability to develop targeted products, *services* and integrated solutions for users and open markets. To ensure innovation in the long term, it is also important to involve companies that have the ability to manage heterogeneous networks and the systematic development of integrated CPS technologies, as well as complex *application platforms* and their evolution.

Particularly in Europe, *Living Labs* are being used to develop the innovative capabilities of different regions and industries. These build up innovation and development networks and open them and the related processes up to users, thereby creating networks of scientists, practitioners, developers and users. *Living Labs* thus act as testbeds for the interactive development and testing of complex CPS innovations. However these instruments – i.e. both the labs and the testbeds – have to be customised for each application context.

One important requirement for encouraging and implementing networked CPS innovations are open platforms, *communication infrastructures* and standards, with a particular emphasis on the *interoperability* and quality of CPS applications and services (see Chapter 5.3). These platforms can drive innovation and the sustainable evolution of Cyber-Physical Systems and serve as a basis for economic *ecosystems*. It is particularly important in this context for interactive value creation and development processes and architectures to be of high quality and to operate on an interdisciplinary basis – including the *models*, methods and tools that are used.

One key capability in this context is comprehensive software competence. Software is of central importance to many of the systems' key features: it ensures the *interoperability* of data and services and has a decisive impact on their functionality, adaptability to new requirements, quality and longevity.

The future challenges for industry and research can be summarised as follows:

- appropriate value creation architectures, collaboration platforms, organisational forms and roles in *ecosystems*,
- new, mutually complementary *business models* and their integration, including harmonisation of the different life cycles of products and components,
- appropriate forms of cooperation and competition and the resulting interactions and business relationships, including
- *revenue-sharing models,* even for the medium to long term, and *models* for calculating the *return on investment (RoI)* in distributed investment and revenue models.

Policymakers and businesses face a number of equally important challenges: a legal framework has to be created, a basis for standardisation needs to be established, and the relevant economic and financial infrastructures and frameworks need to be developed. Moreover, all of this will have to be adapted to different requirements; see also the *model* of a research and innovation system in Figure 7.1.

7 POSITION DECISION, ANALYSIS AND CONCLUSIONS

The analysis undertaken in this agenda provides a clear indication of the opportunities and numerous potential benefits that Cyber-Physical Systems and the associated software-based technologies can bring to the table both for the society and for economy. We have outlined the fundamental changes in system evolution and *human-technology interaction* – and in the way that they are designed and developed – that result from the open networking and utilisation of the systems' new capabilities, as well as the new risks and challenges that they entail for enterprises and society as a whole.

It will be important to take the following key findings of this agenda into consideration in order to facilitate the development of innovative CPS *services* and applications:

1. We are witnessing a shift away from products and towards hybrid systems, interactive *services* and integrated solutions.

2. Innovation is driven by technology and our interactions with it. The quality of Cyber-Physical Systems is determined by their ability to understand the relationships between data, things and *services* in the human environment and the context of the relevant application processes.

3. High-quality CPS *services* are characterised by three factors: extensive interaction, the establishment of *safety, security* and trust, and customisation. They need to be geared towards the needs of demanding and knowledgeable users.

4. Extensive software skills are a key capability, since software plays a central role in enabling functionality, the ability to adapt to new requirements, quality and lastingly innovative system solutions.

5. Communication, networking and *interoperability* are basic capabilities required by all the components, subsystems and applications of Cyber-Physical Systems. Open standards and *CPS platforms* with basic *interoperability*, brokering and *Quality of Service services* are a key driver of diverse and dynamic CPS evolution.

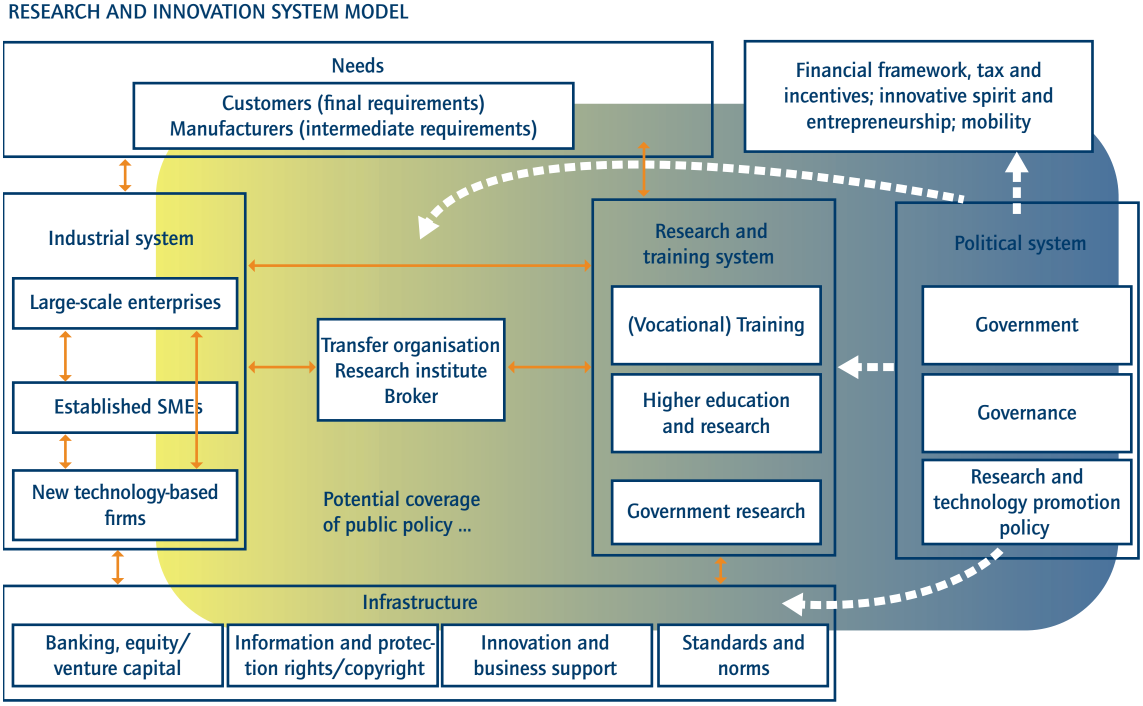
6. Cyber-Physical Systems require an interdisciplinary approach, value creation strategies and *business model* innovations in economic *ecosystems* that are capable of meeting the challenges described above and delivering global leadership. As far as industry is concerned: "The culture shift must occur primarily on the supply side. It is suppliers who must be prepared to implement radical changes to their business processes and even their business models. If they are forced to do so by the market, then in most cases it will already be too late." [HW11]

These findings make it clear that if Germany wishes to take full advantage of the potential offered by Cyber-Physical Systems in order to secure a long-term competitive advantage, it will be necessary for policymakers and the business, research and scientific communities to work together in an integrated manner. The following sections systematically present a number of conclusions based on the findings of this agenda in conjunction with a detailed SWOT analysis.

7.1 THE NECESSARY INTEGRATED INNOVATION EFFORTS

Figure 7.1 provides an overview of the research and innovation system *model* developed by the Fraunhofer ISI (Institute for Systems and Innovation Research) [AKvdMo1]. The description that this *model* provides of the key actors and roles involved in the innovation process serves as a basis for structuring the conclusions and recommendations of the Integrated Research Agenda Cyber-Physical Systems outlined in section 7.2.3.

Figure 7.1: Research and innovation system model; Source: [AKvdMo1], augmented by Kuhlmann (Fraunhofer ISI)


RESEARCH AND INNOVATION SYSTEM MODEL
Needs
Customers (final requirements)
Manufacturers (intermediate requirements)
Financial framework, tax and incentives; innovative spirit and entrepreneurship; mobility
Industrial system
Large-scale enterprises
Established SMEs
New technology-based firms
Transfer organisation
Research institute
Broker
Potential coverage of public policy ...
Research and training system
(Vocational) Training
Higher education and research
Government research
Political system
Government
Governance
Research and technology promotion policy
Infrastructure
Banking, equity/ venture capital
Information and protection rights/copyright
Innovation and business support
Standards and norms

The following three subcategories of future economic *ecosystems* – i.e. the business and innovation partners involved in *value networks* and architectures – can provide a useful basis for structuring the recommendations: enterprise systems and networks (industrial systems), research transfer and commercialisation organisations (transfer organisations, research institutes) and innovative, sustainable research and training systems and their sub-structures (training and research system).

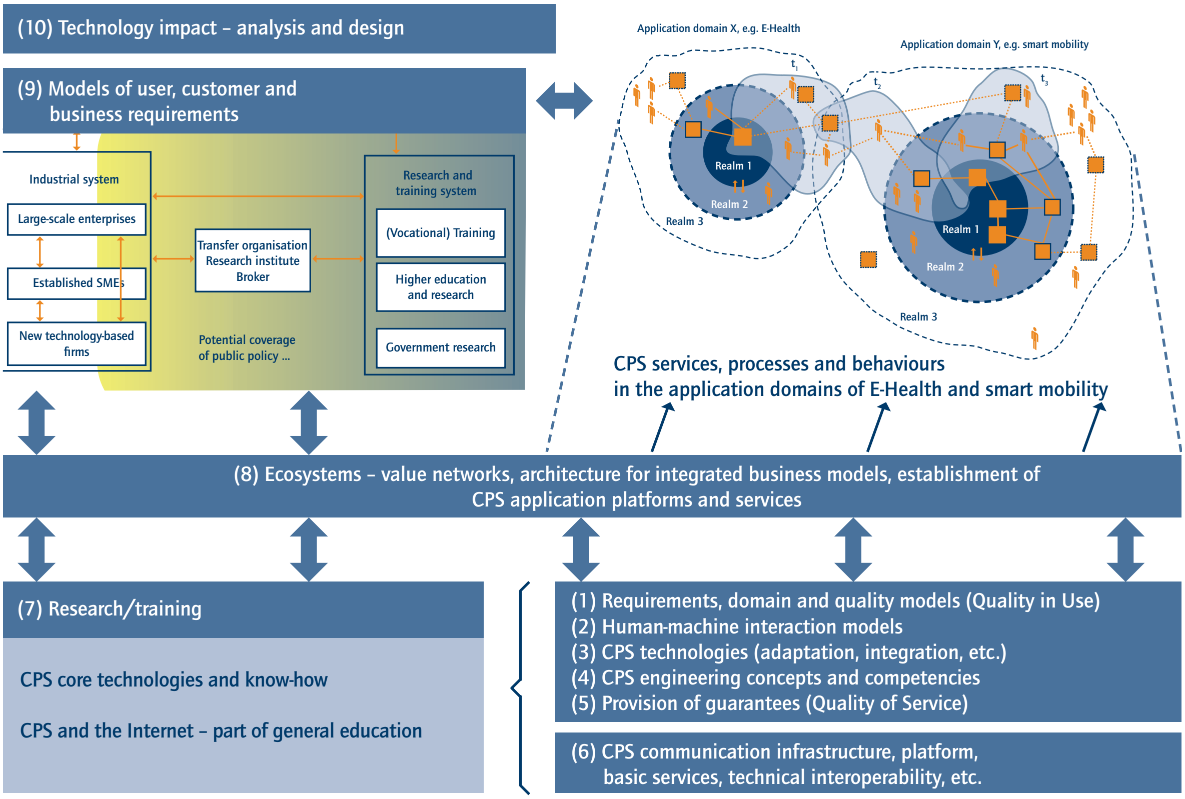
Figure 7.2 illustrates the relationships between these three categories and provides an overview of the required innovation initiatives with regard to:

- CPS application *domains* (Figure 3.2 from Chapter 3, based on sub-scenarios from the *domains of E-Health* and *smart mobility*) and the associated technological requirements and user-centred design,
- CPS core technologies and
- the components of the innovation systems and *ecosystems*.

Coordinated action is required in the following areas:

- **CPS core technologies (1 – 6):** integrated, interdisciplinary research into CPS core technologies – see the summaries of the capabilities, challenges and core technologies provided in Chapters 3.5 and 5.5 – and initiatives to promote the creation and deployment of Cyber-Physical Systems in innovation systems and *ecosystems*,

Figure 7.2: Overview of required coordinated innovation initiatives in the field of Cyber-Physical Systems


(10) Technology impact – analysis and design
(9) Models of user, customer and business requirements
Industrial system
Large-scale enterprises
Established SMEs
New technology-based firms
Transfer organisation
Research institute
Broker
Potential coverage of public policy ...
Research and training system
(Vocational) Training
Higher education and research
Government research
Application domain X, e.g. E-Health
Application domain Y, e.g. smart mobility
t_1
t_2
t_3
Realm 1
Realm 2
Realm 3
Realm 1
Realm 2
Realm 3
CPS services, processes and behaviours
in the application domains of E-Health and smart mobility
(8) Ecosystems – value networks, architecture for integrated business models, establishment of CPS application platforms and services
(7) Research/training
CPS core technologies and know-how
CPS and the Internet – part of general education
(1) Requirements, domain and quality models (Quality in Use)
(2) Human-machine interaction models
(3) CPS technologies (adaptation, integration, etc.)
(4) CPS engineering concepts and competencies
(5) Provision of guarantees (Quality of Service)
(6) CPS communication infrastructure, platform, basic services, technical interoperability, etc.

- **interdisciplinary research and training (7)** and the development of core competencies among everyone involved in the innovation process, as well as general public education initiatives to ensure that everyone is capable of using CPS technology and the Internet competently and independently; see also Chapter 4,
- **economic *ecosystems* (8)** where the partners in CPS *value networks* concentrate on their respective core competencies, in accordance with the innovative *business model* and *ecosystem* concepts and challenges addressed in Chapter 6; see also the platform strategies in Cusumano [Cus10]. This will involve
- companies and networks concentrating on their respective core competencies and capabilities in the field of CPS technology,
- thinking and acting along the lines of modular *application platforms* and CPS *services* that can be flexibly integrated and adapted to different applications,
- establishing corporate networks and *ecosystems*. This will involve developing the relevant value creation architectures and networks and integrated *business models* to enable the creation of *CPS application* architectures and *platforms* and integrated solutions.

- **the requirements of users, customers and businesses (9)**, along with social requirements and conditions,
- **participatory technology design and impact assessment (10):** analysis and evaluation of CPS scenarios and joint design of critical CPS applications based on societal dialogues and negotiation processes for obtaining their support.

Overview of the agenda's findings

Figure 7.3 summarises the individual themes of the innovation initiatives described above and provides an overview of the agenda's findings, including

- a description of the changes that are taking place, together with the factors that are driving them and the key features of Cyber-Physical Systems,
- a detailed description of CPS in terms of their application *domains* and their required capabilities and features; see the summaries of CPS capabilities and challenges provided in Chapters 3.5 and 3.6,
- a summary of the social acceptance issues and factors connected with the changes, together with the associated technological requirements in terms of the political, legal and organisational frameworks; see also the findings presented in Chapters 3.4 and 4.1,
- a summary of the associated technology and *engineering* issues; see also the summary provided in Chapter 5.5, and
- a summary of the resulting challenges for businesses and their *business models*; see Chapter 6.5.

7.2 SWOT ANALYSIS

The SWOT analysis presented below addresses the agenda's key findings, identifies various specific strengths and weaknesses of both Germany and the European Union and relates them to the opportunities and threats, with a view to developing and strengthening innovation in Germany.

The opportunities and threats comprise the external influences on the analysis connected with the specific characteristics of CPS. The strengths and weaknesses refer to the internal capabilities of research and industry in Germany and Europe (see Figure 7.3 and the following sections).

Identification of strategic action areas

The centre of the SWOT analysis diagram in Figure 7.4 is divided into four quadrants:

- SO strategies (expand): use strengths in order to exploit opportunities
- WO strategies (catch up): eliminate weaknesses in order to exploit opportunities
- ST strategies (consolidate): use strengths in order to prevent threats
- WT strategies (reduce): eliminate weaknesses in order to reduce threats

The strengths and weaknesses are set against the opportunities and threats in order to identify areas where action is required in order to develop an integrated CPS action strategy. The SWOT analysis focuses on the new challenges connected with the networking and opening up of the systems. The findings of the *Nationale Roadmap Embedded Systems* [ABB+09] are also included in the analysis, since embedded systems and the associated technologies make up an important part of Cyber-Physical Systems.

The strengths, weaknesses, opportunities and threats identified in Figure 7.4 are summarised in sections 7.2.1 and 7.2.2 below. Section 7.2.3 subsequently addresses the areas identified as requiring strategic action in the middle quadrants of the SWOT diagram.

7.2.1 STRENGTHS AND WEAKNESSES OF GERMANY AS A CENTRE FOR INNOVATION IN THE FIELD OF CYBER-PHYSICAL SYSTEMS

This breakdown of the technological and business strengths and weaknesses of Germany and the European Union in the field of Cyber-Physical Systems is based on the latest studies and market analyses[85], the overview of the current state of research and technology presented in Appendix A and the analysis of the technology and *engineering* challenges provided in Chapter 5.

Strengths

Position and framework

- strongly positioned in embedded systems:
  - *safety-critical* systems, *real-time* systems, *security*, systems *engineering*, system integration, *sensor* technology, mechatronics, robotics
  - architectures, protocols
  - development and manufacturing processes
- leadership in key industries that use embedded systems:
  - automation, manufacturing, automotive, energy technology, logistics, aviation, healthcare
  - strong client industries with high demand for innovation in Germany
- comprehensive local *value chain* coverage
- high-performing, innovative corporate networks in the field of embedded systems that include SMEs
- high-quality and comprehensive c*ommunications infrastructure*
- strong in the field of SCADA[86] systems and the required network technology
- pronounced awareness among the people and policymakers of environmental issues, sustainability, *data protection* and *privacy protection*

Engineering, research and training

- strong research and *engineering* in the field of embedded systems
  - close cooperation between research and industry in certain disciplines and fields of application, for example automotive, medical technology, automation technology
  - *architecture frameworks*
  - *model*-based development, quality assurance, *verification*
  - *safety and security* technology, certification
  - modelling, *model*-based development, *validation* and *verification*
- leadership in basic research on individual CPS technology topics
- high standard of training in embedded systems and conventional *engineering*

Weaknesses

Position and framework

- lack of market competence in consumer products that use embedded systems and the associated software, and a correspondingly weak position with regard to end devices and innovative user interfaces
- failure to adequately take users, use processes and application problems into account, for example in terms of *human factors* and living spaces. This situation is characterised by
  - a weak services industry[87]
  - a strong focus on technology *per se*, without considering the consequences of using it
  - industry's obsession with industry-specific *Business-to-Business processes* and their optimisation
- a lack of market-leading Internet companies and software platforms, meaning that there are hardly any major players capable of establishing *de facto* IT standards

[85] E.g. [BMW08, COS+09, BMW09a, BMW09b, ABB+09, AG09, BMW10a, BIT11a, BIT11b, IDC11, aca11b].

[86] Supervisory Control and Data Acquisition; computerised monitoring and control of technological processes.

[87] See the final report of the Innovationsrat Baden-Württemberg (Innovation Council of Baden-Württemberg) [AG09].

Figure 7.3: Overview of agendaCPS findings – description of the technological and social changes triggered by Cyber-Physical Systems and the associated challenge

ICT, (REAL-TIME) NETWORKING, PHYSICAL AWARENESS, WEB 2.0 (PUSH) ⟵

CHANGES : OPEN SYSTEMS, UBIQUITY, INTERACTIVE CONTEXT ADAPTATION

CPS DESCRIPTION AND REQUIRED CAPABILITIES	QUESTIONS & CHALLENGES ASSOCIATED WITH CHANGES
CPS characterisation based on social and spatial network structures (topologies) a. industrial infrastructure systems and services (controlled realm) b. social infrastructure systems and services (defined realm) c. social application systems and services – including businesses; differentiated areas, cross-domain, open to d. individual application systems and use processes **Features that build on each other** **(1)** Cyber-Physical, networked (locally-globally), virtual, active control in real time **(2)** System of Systems, controlled network with dynamically adaptive boundaries **(3)** context-adaptive and fully or semi-autonomous systems **(4)** cooperative systems with distributed, changing control **(5)** extensive human-system cooperation **CPS require the following capabilities:** • "X"-awareness and context integration • learning and adaptation of their behaviour • transparent and predictable human-machine interactions • dependable and transparent acting • cooperation and strategic acting • risk, goal and quality analysis • guaranteed Quality of Service (QoS)	**Individual and social acceptance** • individual usability, controllability and configurability in the current context • transparency and dependability • safety, security and privacy protection • fairness • environmental sustainability • intellectual property protection **New technological challenges** • enhanced human-machine interaction and cooperation • user-visible and user-controllable semantic interoperability and cooperation • strategic acting in social contexts • redetermine non-functional requirements • enhanced risk analysis and assessment • more demanding quality requirements for CPS components and smart infrastructure systems • stipulation of compliance rules and Quality of Service guarantees **Unresolved questions** • debate on costs and benefits for society • establishing needs and policy guidance locally • design of environmental and other conditions required for application • determination of legal framework for – development, application, operation – economic parameters – standardisation and quality standards

es for technology, businesses and society

(PULL) CONTEXT AWARENESS, HUMAN-MACHINE INTERACTION AND COORDINATION

AND PROCESS INTEGRATION, USERS INVOLVED IN DESIGN (ACTIVITIES, MONITORING, COORDINATION)

TECHNOLOGICAL AND ENGINEERING CHALLENGES

Requirements and domain models

- formalised and integrable requirements, environment and domain models
- models of human-machine interactions and shared control, integrated interaction and acting concepts in complex application situations
- hybrid (system) models and integrated architecture and composition concepts
- models for cooperative and strategic acting

Enhanced quality models (non-functional requirements – NFR)

- targeted structuring and mapping at system levels (Quality in Use, Quality of Service), architecture and composition concepts
- conflict and coordination models (rules)
- CPS capabilities and required technologies
- intuitive and dependable (transparent) operating, interaction and control concepts
- human models, situation and intention recognition
- learning and adaptation technologies and procedures
- sensor and actuator technologies and networks
- semantic web technology
- efficient processors and communication
- Self-X and safety and security technologies – enhanced safety and security methods
- CPS platforms and middleware inc. quality guarantees

Interdisciplinary engineering

- participatory requirements analysis and design
- model-based exploration, simulation, validation and verification
- enhanced quality and risk engineering
- ensuring NFR are met in design and composition
- forms of self-organisation and controlled autonomy
- privacy protection goals and Privacy by Design
- domain engineering, development of application architectures and platforms

Standardisation

CHALLENGES FOR BUSINESSES AND THEIR BUSINESS MODELS

Development of value networks and business platforms (ecosystems)

- strategic goals, creation of sustainably stable structures
- wide range of competencies, sizes and roles
- new forms of CPS business platforms and leadership in their development by large-scale global enterprises
- questions regarding suitable architectures, core competencies and roles
- forms of cooperation and competition
- SMEs as innovators and integrators who understand users and customer problems
- innovation and research systems systematically develop integrated CPS technologies and competencies
- integrated product and life cycle models for CPS components with different life cycles
- development of software skills in traditional SMEs

Wide range of integrated business models

- value proposition – now oriented towards several different customer benefits (cf. enhanced quality models)
- integrated business models, that address e.g. unresolved questions re. revenue sharing and return on investment (RoI) in distributed investment and revenue models

Legal framework

- liability and IP, patent and ownership rights
- national, international

Research and innovation systems

- frame conditions
- (de facto) standardisation

- inadequate competencies and infrastructure in a number of key areas:
  - inadequate competencies with regard to Internet and *cloud* technology
  - inadequate software know-how among established SMEs and CPS component suppliers
  - inadequate technology and software know-how among trades and service providers, e.g. in the fields of building services and architecture
- in places, inadequate *communication infrastructure*, in particular a lack of broadband coverage in rural areas, preventing businesses from locating there
- a unaware attitude towards technology among the general public
- shortage of skilled labour, many skilled workers continue to go abroad
- Germany is not an attractive location for people and (particularly small) businesses from abroad:
  - setting up new organisations and companies involves a lot of red tape
  - inadequate social infrastructure; for example, a lack of support to help foreign citizens integrate into German society, as well as insufficient assistance with childcare, language classes or dealing with the authorities
  - inflexible or non-existent regulatory frameworks
  - a general reluctance to experiment and take risks
  - insufficient venture capital, reluctance to invest

Engineering, research and training

- highly fragmented research in individual disciplines, isolated research topics
- no sustainable development of interdisciplinary research fields
- weaknesses in individual key research areas:
  - requirements management; a lack of requirements analysis methods, e.g. for identifying requirements, modelling application *domains* and prioritising and tracking requirements throughout the design stage
  - *human-technology interaction, usability*
  - inadequate integration of sociology and psychology with IT and technology
  - non-functional requirements and quality *models*
- weaknesses in terms of the consistent translation of research findings into innovations
- rigid and hierarchical development stages and supply structures. There is little communication with potential users and customers. As a result, their requirements are not adequately taken into account in the design of systems and subsystems.
- a lack of interdisciplinary training

7.2.2 OPPORTUNITIES AND THREATS OF GERMANY AS A CENTRE FOR INNOVATION IN THE FIELD OF CYBER-PHYSICAL SYSTEMS

Various opportunities and threats in the field of Cyber-Physical Systems are outlined below, in terms of the economic and social innovations and sustainable excess-value that they can offer society and the environment. They were identified based on the research and analysis undertaken as part of this study and also incorporate the findings of the studies referred to in 7.2.1.[88]

Opportunities

Potential (for society, industry and the market)

- Living spaces and growing needs, contribution to meeting social challenges
  - smart cities, transport, mobility services, people's everyday private lives, *smart homes, smart buildings,* green IT, assistance
  - *AAL, E-Health,* integrated remote healthcare, enabling the elderly and infirm to live independent lives and play an active part in society
- infrastructure and utility systems, integrated service delivery, organisation, supply and monitoring

[88] [BMW08, VI09, CvONS+09, BMW09a, BMW09b, ABB+09, AG09, BIT11a, BIT11b, KPCv11, aca11b].

Figure 7.4: Overview of the SWOT analysis and the strategic CPS action areas that it identifies

	SWOT ANALYSIS	INTERNAL CAPABILITIES	
		Strengths • embedded systems, industries and entire value chain • innovative SMEs in field of embedded systems • research in field of CPS technology • systems engineering and integration • ...	**Weaknesses** • insufficient focus on users and user contexts • weak services industry • inadequate software know-how in established SMEs • highly fragmented research • inadequate CPS training and technology education • no global Internet companies • ...
EXTERNAL INFLUENCES	**Opportunities** • living spaces • smart cities • utility systems and infrastructure • expansion of embedded systems via networking • ...	**SO strategies (expand)** • vertical, cross-domain research clusters and testbeds • systematic development and standardisation of interoperable, safe and secure smart systems providing needs-oriented living space solutions, including integrated services • establishment of innovation clusters, formation and testing of economic ecosystems • integrated research into the economic challenges arising from the emerging ecosystems • creation of platforms for ecosystems • strengthening, promoting, engaging and supporting SMEs	**WO strategies (catch up)** • reorientation of development and innovation strategies towards living spaces and social application processes • embedded systems: need rethinking at every level of the value creation process • research priorities: human-machine interaction, requirements analysis, goal, domain and quality models • interdisciplinary, integrated research structures & concepts, training and CPD • local CPS advice & support centres • creation of internationally competitive conditions for businesses • strengthening Internet skills
	Threats • emergence (internal and external influences) • tampering, attacks • need to clarify legal situation • new competitors • ...	**ST strategies (consolidate)** • models and standards for system quality demanded by the society (quality and engineering models) • leading privacy protection competence centre	**WT strategies (reduce)** • devise strategies to prevent "commercial wars" (IP, patent and legal disputes) • social dialogue, technology design and technology impact analysis • research and competence centre for platforms and technologies in the Internet and CPS environment • practical skills development, CPS technology to form an integral part of general education

  - energy, water
  - *governance*, needs-based, integrated control of energy and water supply and of traffic in towns and cities
  - healthcare, integrated (remote) medical care
- integrated security surveillance and safety monitoring and the associated strategies, e.g. for panic or fire prevention, as well as for general technological processes at events in public buildings or towns and cities
- integrated services for all of the above, delivered using CPS technology

Technology and engineering

- requirements and *domain models,* enhanced quality *models*, architecture and composition concepts
  - integrable requirements, environment and *domain models*
  - *models of human-machine interactions* and *shared control*
  - integrated interaction and behaviour concepts
  - hybrid *models* for systems and networks, as well as integrated architecture and composition concepts
  - *models* for cooperative and strategic behaviour
  - integrated technologies and methods for delivering the required CPS capabilities
  - intuitive, *dependable* and *transparent* concepts for operation, interaction and control and for *usability, multimodal* interfaces and communication
  - *human models*, situation and *intention recognition*
  - techniques and procedures for learning and *adaptation*
  - sensor and actuator technologies and networks
  - Internet technology, especially semantic technology
  - efficient processors and communication
  - *Self-X* and *safety* and *security* technologies, enhanced *safety* and *security methods*
  - *CPS platforms* and *middleware*, including quality assurance *models*
- interdisciplinary *engineering*
  - *requirements engineering, participatory* requirements analysis and design
  - model-based exploration, simulation, *validation* and *verification*
  - enhanced quality and *risk engineering*
  - ensuring that non-functional requirements are met in design and composition
  - *domain engineering*, creation of *CPS application* architectures and *platforms*
  - *self-organisation* and controlled *autonomy*
- concepts for technologies, *engineering*, architectures and guarantees geared towards *privacy* protection, for *Privacy by Design* – i.e. the incorporation of personal data protection considerations right from the very beginning of a product's or service's development – and for *privacy protection goals*
- Green IT, energy and resource efficiency

Industry

- evolution towards and breakthrough into a new generation of technology
  - potential for a whole host of innovative products, systems and *services*
  - sustainable innovation diversity through creation of networks and *ecosystems*
- the opportunity to carry out all aspects of the research, development, manufacture and integration of Cyber-Physical Systems in Germany, thereby ensuring Germany's market and technology leadership
- development of the relevant cross-sectoral standards and of *models*, architectures and modelling languages that facilitate new innovations

Threats

Technology

- the complexity and resulting internal and external emergence (the spontaneous coming about of new be-

haviours as a result of system components interacting with other system components or with the social environment) of Cyber-Physical Systems and their applications
  - lack of predictability and controllability
  - increased risks as a result of inadequate *safety* and *security*
- higher risk of tampering and attacks owing to the open and ubiquitous nature of the systems
- inadequate *security* and protection of embedded systems and critical CPS infrastructures

Society and economy
- surveillance society
- digital divide
- individual and social dependence on correct operation of Cyber-Physical Systems
- restriction of individual flexibility and freedom
- disruption of *business models* in key industries
- non-transparent control of the Internet and communication by state and private actors, e.g. Google, Facebook or the secret services
- threats to know-how advances, e.g. from espionage[89]
- threats arising from inadequate legal framework, e.g. inconsistent, inflexible or non-existent IP and patent regulations
- inadequate networking between manufacturers of individual components, resulting in pronounced technological heterogeneity and solutions that have been developed in isolation of each other
- fragmented technology, failure to standardise, preventing system *interoperability*

7.2.3 STRATEGIC ACTION AREAS

The recommendations presented below bring together the key strategic areas identified in this study as requiring action in order to strengthen and develop innovation and industry in Germany in the field of Cyber-Physical Systems. They correspond to the four quadrants at the centre of the SWOT diagram in Figure 7.4 and serve as a basis for prioritising research topics and interventions. The topics that have been selected are those that are expected to have the greatest impact in terms of the required changes and long-term innovation. The position paper based on this study [aca11d] drew on the agenda CPS findings in order to formulate a number of initial specific recommendations that include recommendations for horizontal and vertical project and research consortia.

(1) A change of strategy

Realignment of innovation and development strategies so that they are geared towards open markets and environments, openly integrated applications and processes – including over the Internet – and the associated problems, the requirements of public and private *stakeholders* and the networked economy; see the list of chances and opportunities under 7.2.2., particularly in the fields of smart cities and *E-Health*

Infrastructure and utility systems, integrated services for organisation, supply and monitoring in the energy and water sectors and for *governance* – i.e. control of the energy and water supply and of traffic in towns and cities –, and in the field of healthcare and medicine; see 7.2.2.

Embedded systems: rethinking every level of the value creation process – including research and training – based on participatory, interdisciplinary and integrated concepts and principles. This will in turn generate new requirements, for example in terms of the protection of CPS infrastructure and components against tampering and attacks, as well as new *safety* concepts, methods and analysis procedures.

[89] See, for example, reports on how competition has been hindered by lengthy patent suits concerning complex technological products [Ber11], industrial espionage in the wind power industry [Wer11] and the legal risks associated with *cloud* applications [Gra11].

Research priority: human-machine interactions in socially networked CPS applications and environments; this will require integrated system *models*.

Research priority: requirements engineering and analysis, development of *domain* and quality *models*, including enhanced methods for goal-oriented evaluation and prioritisation of requirements and solutions and for strategic marketing.

Research priority: methodically integrated, interdisciplinary software and systems engineering, including end-to-end architecture *models, requirements refinement* and *traceability* and *model*-based quality assurance (*validation* and *verification*).

(2) Interdisciplinary research

Interdisciplinary research and training in every area of the value creation process, including trades and service providers

Interdisciplinary and interdepartmental research strategies, also at a policy level

Interdisciplinary research structures and strategies incorporating scientific disciplines, users, *stakeholders* and value creation partners, e.g. research centres and testbeds

- to enable early exploration of requirements, preconditions and risks and to answer questions relating to acceptance, the impact of the technology, the legal, economic and policy frameworks and the technology's limitations,
- to facilitate the development of integrated *models* of the relevant scientific disciplines incorporating *human-machine interactions,*
- to improve the core technologies and gain a better understanding of CPS *engineering*,
- to enable targeted interdisciplinary research geared towards developing, testing and controlling new technologies,
- to develop and acquire CPS *engineering* competencies,
- to facilitate the establishment of competence centres that can also provide local advice and support.

Research into the impact of the technology and the associated acceptance issues – i.e. the sociology of technology –, focused on the investigation of the technology, analysis, description and of the *human-machine interactions* involved in Cyber-Physical Systems. This will also involve occuring and moderating a social discourses on these issues.

(3) Clusters, economic ecosystems and competitive strategies

Vertical and cross-*domain* research clusters and testbeds, Living Labs for developing **cross-*domain*** solutions, e.g.:

- CPS application systems for social and individual use – see c) and d) in Figure 7.3 –, for example smart city applications or other living space applications from the list of opportunities described in 7.2.2
- These application systems will also determine the requirements and the structure and architecture standards for CPS application systems involving industrial or social infrastructure systems, e.g. in the field of traffic management or local energy supply via *smart grids* or *micro grids,* including integrated concepts for services such as remote maintenance, support and diagnosis.

The systematic development and standardisation of interoperable, high-quality, *safe and secure smart infrastructure* and utility systems providing needs-oriented solutions for people's living spaces, *governance* structures and regulations that place the highest possible degree of control and configurability in the hands of users and customers.

The establishment of open CPS platform and interoperability standards, including **cross-*domain*** brokering and *Quality of Service services.* This is essential to enable open innovation and innovation leadership in the field of Cyber-Physical Systems.

The establishment of innovation clusters, the formation and testing of economic *ecosystems* and *value networks;* this includes

- **the development of application architecture** and *CPS platforms* and the definition of *interoperability* standards; see the opportunities listed under 7.2.2,
- the strengthening, engagement and promotion of SMEs,
- the promotion of CPS transfer organisations through Private-Public Partnerships,
- the creation of more favourable conditions for starting up and developing businesses in CPS value networks.

Integrated research into the economic challenges arising from the emerging ecosystems and *business models;* see Figure 7.3.

Devising strategies to prevent commercial wars from breaking out, for example over intellectual property (IP) in the form of patents or over strategically important business and system data, as well as strategies to protect and support SMEs.

Extensive measures to promote regional and supra-regional innovation systems, including social infrastructure projects, measures to make locations more attractive to businesses and initiatives to strengthen and promote SMEs by making research funding available to them and incorporating them into innovation clusters and regional innovation systems.

(4) Models and standards to ensure that systems meet the quality standards demanded by the society

Dialogue with the society, design of the technology and analysis of the technology's impact. It will be necessary to address cost-benefit ratios, legal questions, regulations, frameworks, the threats arising from extensive dependence on technology and the measures that can be taken to counter this phenomenon, as well as the democratic and *participatory design* of the systems and the relevant aspects of the environment. Standards, regulations and *policies* should be developed for all of these goals.

The development of new and enhanced quality standards for Cyber-Physical Systems. This includes quality *models*, quality measurement and assurance methods, *engineering* standards for non-functional requirements including new *usability* concepts, methods and analysis tools, with a particular focus on controllable *human-machine interactions, safety* and *security* and the control and limitation of semi-autonomous behaviour.

(5) Capacity building through comprehensive advice and support

The creation of a research and competence centre for platforms and technologies in the Internet and CPS environment. Alongside commercial Internet applications (*business web*), *cloud* technology and semantic technologies, this organisation would also address technological approaches to enabling *IT security* and user confidence, as well as intellectual property protection and standardisation.

The establishment of a *privacy* protection competence centre that treats this issue as an opportunity and develops high-quality technologies, quality standards, advice concepts and audits, as well as privacy protection seals.

The creation of research-based advice centres that provide users – i.e. businesses, local authorities, SMEs, tradesmen, service providers, etc. – with local support and advice with regard to the deployment and use of Cyber-Physical Systems.

(6) Development of practical skills, creation of favourable conditions for businesses

Making sure that CPS technology forms an integral part of general school education in order to ensure that people are taught the practical skills that they will need to use Cyber-Physical Systems.

The creation of globally competitive conditions for attracting venture and equity capital in order to promote business start-ups and attract skilled labour by providing job offers with long-term prospects, creating the relevant social infrastructure for workers' families and carrying out and promoting international interdisciplinary research.

The SWOT analysis identifies a number of priority action areas that are described below. The goal of these actions is to maintain and develop Germany's position as a leading innovator in embedded systems and, going forward, also in Cyber-Physical Systems:

(I) A change of strategy and direction is required with regard to Cyber-Physical Systems research. Research needs to be translated into practical applications much more quickly, so that Germany can draw on its strengths in the development of complex systems in order to respond to the way that the systems and the associated challenges are changing. This provides an opportunity to develop solutions in a variety of application areas that are useful, integrated, safe, secure and dependable for the relevant actors. It also offers a chance to share expertise and pool the innovative capacity of SMEs through interdisciplinary and *participatory* partnerships and *ecosystems*. Furthermore, *human-machine interaction, requirements engineering* and integrated *modelling* will need to be established as research priorities. The basic principles, results and *know-how* already exist in the individual research disciplines. However, the necessary framework and the desire among researchers to adopt a joint interdisciplinary approach are still lacking.

(II) Since Cyber-Physical Systems will pervade every area of our lives, their acceptance and *participatory design* by users from the society and economy will be key to their commercial success. It is therefore essential to involve people locally in use scenarios at every level of the systems engineering process, in order to engage them in the design of the systems and enable their exploratory development and testing in testbeds. An intensly social and political debate encompassing all the affected areas of our society will do much to promote engagement, confidence and acceptance, thus creating the conditions for sustainable success. The highest quality standards should also be applied to *data protection, privacy* and fairness, and the appropriate consensus-based quality standards and models and binding *compliance* regulations should be developed. These regulations will serve to clarify the legal situation and promote the development of acceptable CPS solutions and sustainable *business models.*

(III) The successful long-term evolution of software systems and the IT and software development expertise needed to make this possible are key to the design of Cyber-Physical Systems and successful innovations in this field. The functionality of CPS systems and applications will be fundamentally determined by the software that enables data to be analysed and interactions and behaviour to be controlled. The key challenges in this regard are to be found in the field of IT. They involve opening up the application areas and their requirements and system *models*, ensuring *interoperability* and guaranteeing the key quality parameters. Meeting these challenges will require an interdisciplinary and methodologically integrated approach to software engineering. There are many reasons why it will be important to improve the overall level of software know-how: in addition to the fact that software is a feature of all the different application domains and plays a key role in enabling the systems' functionality, networked software and the Internet also enable extremely flexible operational scaling of applications. It is therefore essential to ensure that companies' software and software *engineering* competencies are strengthened, integrated and developed at every level.

(IV) Heterogeneous innovation and *value networks (ecosystems)* based on the open technological and business *application platforms* of Cyber-Physical Systems will have an especially important role to play. It will therefore be necessary to implement measures to promote the development of these platforms and to build *ecosystems* comprising actors that cover a wide range of competencies, roles and company sizes. Networks for promoting innovation should be established, incorporating start-ups, traditional SMEs and large-scale industrial enterprises. The members of these networks will need to cooperate in order to tackle the constant changes that are implicit in CPS, as well as to address the demanding quality, *safety* and *security* requirements placed on the systems. To do this, it will be necessary to get different corporate and scientific cultures working together. In order to ensure the *interoperability* of the platforms, thereby enabling open innovation and the required level of *safety* and *security*, it will be essential to develop architecture framework, quality assurance and *compliance* standards for CPS applications.

(V) It will be necessary to develop and enhance a wide range of competencies in matters relating to Cyber-Physical Systems. This will necessitate the involvement of various public entities in order to facilitate interdisciplinary research, training and CPD and to provide local advice and support in the different areas of application. As part of this process, it will be necessary to support the development and organisation of regional innovation systems, including the promotion of CPS transfer organisations through Private-Public Partnerships and ensuring that SMEs are appropriately involved.

It will be paramount to strengthen the development of Internet skills in connection with CPS applications. Ubiquitous data acquisition and enhanced control options in utility supply structures (*governance*) mean that it will be especially important to establish a competence centre for the relevant subjects. This would address the full range of issues pertaining to the Internet, the technology, the applications, the market and the economic potential, as well as the social, political and ethical aspects. This institution should engage leading experts from the fields of information technology, engineering and mechanical engineering, sociology, neuroscience, the natural sciences and psychology in order to provide collective interdisciplinary advice to industry, policymakers and non-governmental organisations. It would be particularly important for this body to address the necessary competencies in the fields of *security* and *privacy* protection.

At the policy level, it will be necessary to implement initiatives for promoting sustainable interdisciplinary research structures, establish innovation and transfer systems and create the appropriate conditions to facilitate purposeful management of the field of Cyber-Physical Systems and provide security for businesses. In so doing, it will be crucial to take the rapid pace of innovation into account.

(VI) There are a number of specific challenges in connection with education. It is necessary to build capacity, not just in order to develop Cyber-Physical Systems, but also to enable people to use them independently and beneficially in every area of their professional and private lives. Particular effort should be devoted to improving Internet, media and system skills. Education will need to pay much more attention to these aspects and it will be necessary to create the conditions for sustainable capacity building at every level of the education system.

APPENDIX A: CURRENT STATUS OF RESEARCH AND TECHNOLOGY

This Appendix presents a review of the current status of research and technology in the field of Cyber-Physical Systems. The first section compares programmes and research priorities from around the world, whilst the second focuses on the advances made in Germany that are relevant to the implementation of Cyber-Physical Systems.

A.1 REGIONAL PROGRAMMES AND PRIORITIES

This section will begin by describing the programmes that currently exist in Germany, before going on to look at programmes in the rest of Europe, the US and finally the BRICS[90] countries and Asia.

A.1.1 GERMANY

A.1.1.1 ICT2020 and the High-Tech Strategy

The High-Tech Strategy [BMB06] of the Federal Ministry of Education and Research (*BMBF*) was published in 2006 as a national strategy for supporting innovation in a variety of different technology areas. Its three main goals are as follows: (a) the establishment of priorities and the creation of leading markets in technology areas that are important to Germany, (b) promoting innovation through the development of closer links between the business and scientific communities and (c) improving the conditions for innovation in industry. The revised strategy published in 2010 is known as the High-Tech Strategy 2020 [BMB06]. It identifies five priority areas (climate and energy, health and nutrition, mobility, security and communication) as well as 17 innovation areas for delivering goal (a). These are divided into the following themes: (1) Healthcare and Safety, (2) Communication and Mobility and (3) Cross-cutting technologies.

1 HEALTHCARE AND SAFETY:	1.1 Healthcare Research and Medical Technologies
	1.2 Safety Technologies
	1.3 Plants
	1.4 Energy Technologies
	1.5 Environmental Technologies
2 COMMNICATION AND MOBILITY:	2.1 *ICT*
	2.2 Automotive Technologies
	2.3 Aeronautic Technologies
	2.4 Space Technologies
	2.5 Maritime Technologies
	2.6 Services
3 CROSS-CUTTING TECHNOLOGIES:	3.1 Nanotechnologies
	3.2 Biotechnology
	3.3 Microsystem Technology
	3.4 Optics Technologies
	3.5 Materials Technologies
	3.6 Production Technologies

In order to deliver the second goal of promoting an innovation-friendly environment by fostering closer ties between the business and scientific communities, the Leading-Edge Cluster Competition [BMW07] and the Excellence Initiative for Cutting-Edge Research at Institutions of Higher Education [EXC] have been launched to support leading-edge clusters that promote collaboration between industry and science. In addition, there are a variety of special programmes for supporting innovation by SMEs, for example the Central Innovation Program SME (*ZIM*) [BMW11b] and *KMU innovativ* (Innovative SME) [KMU].

The High-Tech Strategy's third goal of improving the conditions for innovation in industry is being addressed through improved funding for innovation, more favourable condi-

[90] BRICS is the acronym for Brazil, Russia, India, China and South Africa.

[91] The lead innovations are: initiative for automotive electronics, networked intelligent objects in logistics, communication technology for safe mobility and *ICT* for healthcare.

[92] Technology alliances have been established for: digital product memory, standards for communication of the future, virtual technologies and real products and ambient intelligence for autonomous networked systems.

[93] The service platforms relate to: *ICT* for services and the provision of services and flexible modules for communication services.

tions for start-ups, better intellectual property protection and improvements in higher education.

Although embedded systems and Cyber-Physical Systems do not constitute one of the High-Tech Strategy's innovation areas in their own right, they do play a key role within the 17 innovation areas that it identifies. This can be seen, for example, in the BMBF's 'ICT 2020 – Research for Innovation' programme. This programme, which is geared towards implementing the High-Tech Strategy in the area of *ICT* research, has the following goals: consolidating and expanding Germany's leadership in the field of *ICT*, boosting its competitiveness in the realms of research and manufacturing and making Germany a more attractive place to work, and facilitating access to technological *know-how* for small and medium-sized enterprises.

The ICT 2020 programme draws on a range of strategic instruments that include lead innovations[91], technology alliances[92] and service platforms[93]. Furthermore, ICT 2020 identifies four basic technologies: electronics and microsystems, software systems and knowledge processing, communication technology and networks and future developments. The programme concentrates on the following application areas: (a) automotive and mobility, (b) automation, (c) healthcare and medical technology, (d) logistics and services and (e) energy and environment.

A number of innovation alliances between representatives of science and industry are being forged under the auspices of ICT 2020, including the Software Platform Embedded Systems 2020 (SPES 2020). This involves what are known as vertical cooperation initiatives that focus on fields of application in the different *domains* in order to accelerate the pace of technological innovation. At the same time, horizontal cooperation initiatives are also being implemented in the shape of technology alliances where science and industry cooperate in the pursuit of technological goals.

The programme is due to run from 2007 to 2020. Between 2007 and 2011, it received approximately 380 million euros of funding from the German government. The funding for the period from 2012 to 2020 has not yet been announced.

A.1.1.2 National Roadmap Embedded Systems

The National Roadmap Embedded Systems (NRMES, see [ABB+09]) was published on the occasion of the National IT Summit in 2009 and focuses on embedded systems as a key component of Cyber-Physical Systems. The networking of embedded systems with each other and with global IT *services* is repeatedly cited as a key new feature and plays an important role in some of the innovations and research priorities identified in the roadmap. Nevertheless, the NRMES also often uses the term 'embedded systems' in the traditional sense. It identifies a number of social challenges – ageing society and healthcare, mobility, safety (divided into *functional safety* and public safety), environment and energy, the knowledge society, globalisation and urbanisation – and describes the capabilities that will be required to meet these challenges. These include both system and developer capabilities. Finally, it identifies the technology and process innovations that will be needed to deliver these capabilities. These are divided into two groups of nine:

- Technology innovations: smart devices of the future, resource-optimised technologies, *architecture frameworks* for embedded systems, safe, secure and protected embedded systems, networked control systems, *functional safety* for embedded systems, cognitive embedded systems, innovative interaction interfaces and cooperative embedded systems
- Process innovations: *requirements engineering*, architecture design and evaluation, system analysis, *model-driven development*, systematic *re-use, human-centred design,* life cycle management, process automation and process organisation

The identified capabilities are grouped into research priorities and assigned to one of three timeframes (pre-2015, pre-2020, post-2020). The NRMES is not a funding programme as such and consequently does not have a fixed funding budget.

A.1.1.3 Internet of the Future

In Germany, new *services*, technologies and infrastructure for the Internet of the Future are primarily funded through the Federal Ministry of Economics and Technology (*BMWi*). The priority themes are as follows:

(I) Internet of Services. Theseus is a 100 million euro programme that ran from 2007 to 2012, geared towards creating the *services* and knowledge infrastructure for the Internet of the Future. It investigated basic technologies such as automatic recognition of content and semantic relationships, as well as developing application scenarios for different market segments such as mechanical engineering and healthcare. It also funded accompanying research projects, in particular with a view to benchmarking the approaches developed under Theseus against other European and international initiatives and establishing connections with actors outside Germany who are also working in this field.

'Trusted Cloud – Secure Cloud Computing for small and medium-sized enterprises and the public sector' is a 50 million euro ideas competition running from 2011 to 2014, aimed at promoting initiatives for innovative, efficient cloud structures and services.

(II) Internet of Things. The technology competition 'Autonomics – autonomous, simulation-based systems for small and medium-sized enterprises' concluded in early 2009. The resulting projects (running from 2009 to 2013) have received a total of 55.3 million euros of funding and address the development of prototype systems and solutions for context-adaptive, autonomous mechanical engineering systems for small and medium-sized enterprises. Meanwhile, the Next Generation Media programme ran between 2005 and 2009 and made a total of 36.9 million euros of funding available for collaborative research and development projects focused on the development, testing and application of new technologies and standards for smart objects and their networking in the application fields of consumer electronics in networked systems, smart logistics networks, smart manufacturing system networking and smart healthcare systems.

Building on the Service Centric Home (SerCHo) project, some 3.5 million euros of funding was made available between 2010 and 2012 for the two projects *Serviceorientierte Heimautomatisierungsplattform zur Energieeffizienzsteigerung* (Service-Oriented Home Automation Platform for Increased Energy Efficiency – SHAPE) and Service Enabled Devices for Intelligent Connected Media Assistance (SEDICMA). These projects aimed to develop new and forward-looking smart home networking methods, together with the corresponding sustainable business models.

(III) Internet of Energy. The programme *E-Energy – Informations- und kommunikationstechnologiebasiertes Energiesystem der Zukunft* (E-Energy – Information and Communication Technology-Based Energy System for the Future) ran from 2008 to 2012 and provided a total of approximately 40.2 million euros of funding for the following projects: eTelligence (Intelligence for Energy, Markets and Networks), E-DeMa (Development and Demonstration of Decentralised, Networked Energy Systems for the E-Energy Market of the Future), MEREGIO (Development of Minimum Emission Regions), MoMa (Model City Mannheim in the Rhine-Neckar Metropolitan Region), RegModHarz (Regenerative Model Region Harz) and Smart W@TTS (Improving The Energy System's Self-Regulatory Capability by Establishing an Internet of Energy). These were complemented by accompanying research projects.

The programme ICT for Electric Mobility provided a total of 53.7 million euros of funding over three years (2009 to 2011) for seven projects in the following areas and model regions: Interurban Integration of Electric Vehicles Into Energy Systems (Grid Surfer), *ICT*-based Integration of Electric Vehicles into Future Energy Grids (e-mobility), Smart Electric Mobility in the Model Region of Aachen (Smart Wheels), Minimum Emission Regions Mobil (MEREGIOmobil), Efficient Electric Mobility & Tourism (eE-Tour Allgäu), Integration of Electric and *Plug-in Hybrid Vehicles* into Commercial Vehicle Fleets (Future Fleet) and Deployment of Electric Mobility (HARZ.EE-MOBILITY).

'IT2Green Energy-Efficient ICT for SMEs, the Administration and the Home' is a joint programme of the Federal Ministry of Economics and Technology and the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety providing 27.5 million euros of funding between 2011 and 2014 for projects to develop and test systemic approaches for increasing the e*nergy-efficiency* of *ICT* systems and applications (technology, organisation, *business models* and *services*).

(IV) Mobile Internet. SimoBIT – *Sichere Anwendung der mobilen Informationstechnik in Mittelstand und Verwaltung* (Secure Application of Mobile Information Technology in SMEs and Government) is a programme that ran between 2007 and 2011, funding a total of twelve research projects geared towards the development, testing and wide-ranging deployment of innovative, safe and secure mobile multimedia applications for improving productivity and quality in industry and government.

A.1.2 EUROPE

It is the stated aim of the European Commission to strengthen the European Union (EU) in the field of research and development of innovations and new technologies. It has created a number of funding instruments to this end. The main current EU research funding instrument is the Seventh Framework Programme for Research and Technological Development (FP7). This is complemented by the Eureka Programme, where a current total of 39 countries plus the EU fund international research projects.

A.1.2.1 Framework Programme

The Seventh Framework Programme and Horizon 2020

Running from 2007 to 2013, the Seventh Framework Programme is the European Union's largest publicly funded research programme. It is divided into five overarching themes. The 'Cooperation' programme provides support to international research projects through the deployment of structural policy instruments. It has ten thematic areas where the EU wishes to become a leader or strengthen its current leadership position. These include information and communication technologies, health, transport and energy. The structural policy instruments include the Joint Technology Initiatives (JTIs, see below).

The total budget for the Seventh Framework Programme comes to 53.2 billion euros, approximately 61 percent of which (32.365 million euros) is allocated to the Cooperation programme. In order to ensure that the funds are awarded to high-calibre projects, regular 'Calls' are announced in the individual research areas that focus on different key themes and challenges. The following challenges – all of which are relevant to Cyber-Physical Systems – have currently been specified for the information and communication technologies (ICT) thematic area:

- Pervasive and Trustworthy Network and Service Infrastructures
- Cognitive Systems, Interaction, Robotics
- Components, Systems, *Engineering*
- Digital Libraries and Content
- Towards Sustainable and Personalized Healthcare
- ICT for Mobility, Environmental Sustainability
- ICT for Independent Living, Inclusion and *Governance*

These challenges are addressed by specific research goals that comprise the key content of the Calls. The goals and outcomes to be delivered by the research and development projects are stipulated for each of these goals.

Work began in early 2011 on the content of the Eighth Framework Programme, dubbed Horizon 2020, which is due to begin in 2014.

Joint Technology Initiatives

The EU's Seventh Framework Programme established European Technology Platforms (ETPs) comprising industry-driven alliances of industrial and academic actors in specific thematic areas. There are more than 35 ETPs, including ACARE (Advisory Council for Aeronautics Research in Europe) in the aviation industry, ENIAC (European Nanoelectronics Initiative Advisory Council) in the nanoelectronics sector and ARTEMIS (Advanced Research and Technology for Embedded Intelligence and Systems) in the field of embedded systems. Some of the ETPs have established what are known as Joint Technology Initiatives (JTIs). These are research funding programmes through which the European Union and the member states support research projects that are aligned with the Strategic Research Agenda (SRA).

JTI ARTEMIS – Advanced Research and Technology for Embedded Intelligence and Systems

Following the establishment of a Strategic Research Agenda (SRA) for the field of embedded systems in 2006, the ARTEMIS initiative was launched in February 2008. A Call for Project Proposals has been issued every year since 2008. Between 2008 and 2013, the funding available through ARTEMIS amounted to more than 2.4 billion euros.[94] The recently published updated version of the SRA refers to three societal challenges: (I) Smart Buildings and *Communities* of the Future, (II) Green, Safe, and Supportive Transportation and (III) Affordable Healthcare and Well-being. These provide the basis for converting the inherent technological questions in the field of embedded systems into research strategies that can be applied to the individual fields of application.

This ensures that projects aligned with the ARTEMIS SRA deliver practical outcomes and help to address social and economic challenges. Aspects connected with the networking of embedded systems – both with each other and with digital networks and services – play a far more important role than in the original 2006 version of the SRA. As such, ARTEMIS is now highly relevant to the field of Cyber-Physical Systems at European level. Rather than basing the structure of the topics covered by ARTEMIS on application *domains*, the SRA adopts a structure comprising three horizontal research *domains*: (I) Reference Designs and Architectures, (II) Seamless Connectivity and Interoperability and (III) System Design Methods and Tools. These research *domains* are supplemented by newly identified technology fields, including open Internet; robustness, autonomy, mixed critical systems; self-organising and autonomous systems and *Systems of Systems.* In addition to identifying the research topics, the 2011 ARTEMIS SRA also provides advice on supporting and implementing innovations. To this end, ARTEMIS seeks to foster the creation of an innovation-friendly environment, standardisation, tool platforms, support for SMEs, international cooperation and an enhanced intellectual property *policy*.

ARTEMIS funds R&D projects in eight subprogrammes that embody and prioritise the research topics specified by the SRA:

- Methods and Processes for *Safety*-relevant Embedded Systems
- Embedded Systems for Healthcare
- Embedded Systems in Smart Environments
- Manufacturing and Production Automation
- Computing Platforms for Embedded Systems
- ES for *Security* and Critical Infrastructures Protection
- Embedded Technology for Sustainable Urban Life
- Human-centred Design of Embedded Systems

[94] However, current estimates suggest that this sum will not be taken up in its entirety, meaning that the overall figure is likely to be lower.

JTI ENIAC – European Nanoelectronics Initiative Advisory Council

The ENIAC nanoelectronics initiative is a 3 billion euro programme running to 2013. ENIAC projects are also aligned with an SRA that focuses on the "grand challenges" in different areas of application:

- **Automotive and Transport:** Intelligent Electric Vehicle, *Safety* in Traffic and Co-operative Traffic Management
- **Communication and Digital Lifestyles**: Internet Multimedia Services, Evolution To A Digital Life Style, Self Organizing Network, Short-Range Convergence
- **Energy Efficiency:** Sustainable and Efficient Energy Generation, Energy Distribution and Management – *Smart Grid*, Reduction of Energy Consumption
- **Health and the Ageing Society:** Home Healthcare, Hospital Healthcare, Heuristic Healthcare
- **Safety and Security**: Consumer and Citizens *Security*, Securing the European challenging Applications, Enabling Technologies for Trust, *Security* and *Safety*
- **Design Technologies**: Managing Complexity, Managing Diversity, Design for Reliability and Yield
- **Semiconductor Process and Integration:** *Know-how* on Advanced and Emerging Semiconductor Processes, Competitiveness through Semiconductor Process Differentiation, Opportunities in System-in Package
- **Equipment, Materials and Manufacturing:** Advanced CMOS – 1X nm and 450mm, More than Moore, Manufacturing

A.1.2.2 Public-Private Partnerships

The Economic Recovery Plan adopted by the European Commission and European Council in 2008 establishes Public-Private Partnerships (PPPs) for the development of new technologies in the manufacturing, construction and automotive industries. While these industries remain extremely important to Europe's economy, they suffered a major fall-off in demand as a result of the global economic crisis. The aim of the PPPs is to link the short-term economic and financial measures of the Recovery Plan to "smart" longer-term investments in research and development in order to create a strong basis for securing the competitiveness of European industry going forward. The PPPs provide support for the key themes of the three industries referred to above. An additional PPP was established in 2009 in order to implement the European Future Internet Initiative.

PPP Factories of the Future (FoF) – value 1.2 billion euros

Of the four strategic *domains* that comprise the PPP FoF, the most relevant to Cyber-Physical Systems is that of ICT-Enabled Intelligent Manufacturing. The R&D projects in this *domain* address the following themes: (a) Smart Factories: ICT for Agile Manufacturing and Customisation, (b) Virtual Factories: Value Creation, Global Networked Manufacturing and Logistics and (c) Digital Factories: ICT for better Understanding and Design of *Manufacturing Systems*.

PPP Energy-efficient Buildings – value 1 billion euros

Cyber-Physical Systems play a relatively peripheral role in the PPP Energy-efficient Buildings. Nevertheless, certain horizontal technological themes are relevant to CPS, for example Energy Management Systems and Diagnosis and Predictive Maintenance.

PPP Green Cars – value 1 billion euros

The objective of the European Green Cars Initiative is to support R&D on technologies and infrastructures that are essential for achieving breakthroughs in the use of renewable and non-polluting energy sources, safety and traffic fluidity. This includes research on trucks, internal combustion engines, biomethane use and logistics. The main focus is on the electrification of mobility and road transport.

PPP Future of the Internet (FoI) – value of the three calls for projects to date: 300 million euros

The PPP FoI was launched in 2009 by a consortium of companies including Alcatel-Lucent, Ericsson, Telekom, Nokia, Orange, SAP, Tahales and Siemens. The main objective of this PPP is to provide support for the implementation and introduction of future Internet *services* up to 2015 and the establishment of *smart infrastructures* in European markets.

A.1.2.3 Eureka

EUREKA is an initiative that supports international research within Europe through individual programmes focused on specific themes. Calls for projects are issued under these programmes and the project proposals received are assessed by a European evaluation committee. If the assessment is favourable, the project is endorsed with the Eureka label. Funding is awarded at national level – in other words, there is no central budget for allocating funds, this is done through the member states' national or regional funding instruments. EUREKA programmes facilitate international applied R&D projects for civil purposes. Since the projects' content is not governed by an overarching strategy, EUREKA project calls are extremely flexible.

Examples of EUREKA programmes include CELTIC in the field of telecommunications, EURIPIDES in the field of smart systems, ACQUEAU in the field of water technologies and ITEA and CATRENE (see below).

A.1.2.4 ITEA

ITEA (Information Technology for European Advancement) is a European programme that supports pre-competitive applied R&D projects in the field of software-intensive systems and *services*. ITEA 2 is an industry-driven strategic EUREKA cluster programme in the field of information and communication technology. Running for eight years, from 2006 to 2013, ITEA 2 is a continuation of the original ITEA programme (1998 to 2005), whilst ITEA 3 is planned for the period 2014 to 2021.

The programme is characterised by being highly flexible in terms of the research topics that it supports. Projects are initiated by the project partners – it is they who define the content, scope, nature and duration of the partnership, without being constrained by the terms of a call for projects. The key criteria for awarding an R&D project the ITEA label are its innovative potential and marketability. Every four years, the ITEA 2 Community – comprising the 15 founding partners plus several other major industrial enterprises and academic institutions – publishes the ITEA roadmap, which is intended as a source of inspiration for new projects.

The roadmap takes a dual approach, describing applications in the different *domains* and the basic technologies and innovations required to enable these applications. The fourth roadmap will be published in 2013.

In total, more than 3 billion euros (2009) have been invested in ITEA 2.

A.1.3 USA

A.1.3.1 National Science Foundation (NSF)

A joint Cyber-Physical Systems research programme [CPS08, RLSS10] has been launched by the NSF's Directorate for Computer and Information Science and Engineering (CISE) and Directorate for Engineering (ENG). The programme promotes the following three themes

- basic principles,
- research on methods and tools and
- components, run-time substrates and systems

by providing three categories of research grants:

- up to 200,000 US dollars a year over three years for small projects,
- up to 500,000 US dollars a year over three years for medium projects and
- up to 1 million US dollars a year over five years for large projects.

In total, funding was provided for 58 projects in FY 2009 and more than 43 in 2010. In order to carry out focused, disciplinary research in the field of embedded and hybrid systems within the Computer Systems Research Program (CSR), the strategy for FY 2011 is to sustain the multidisciplinary CPS programme using the research outcomes from core discipline programmes. Discussions are also ongoing with government and industry, in particular the transportation sector (NRC, FAA, NASA, AFRL, FHA, USN, Boeing, GM, Ford, SRI) and the energy and healthcare/medical sectors (NIH, ARPA-E, NIST, NSA, DHS, FDA, CIMIT, SRC). The call for projects for FY 2011 continues to provide support for the same three themes, but only for medium and large projects. An evaluation and assessment of testbeds and platforms is also planned. 144 projects worth a total of 72.5 million US dollars were ongoing as of 7 July 2011.

A.1.3.2 Defense Advanced Research Projects Agency (DARPA)

DARPA funds 13 projects under the META Program, which is itself part of the Adaptive Vehicle Make (AVM) portfolio of programmes. Funding has been allocated to the following enterprises and research institutions:

- Adventium Enterprises (Minneapolis)
- BAE Systems (Minneapolis)
- Boeing (St Louis)
- IBM Haifa Research Lab (Haifa, Israel)
- MIT, Dr. Donna Rhodes (Cambridge, Massachusetts)
- MIT, Prof. Karen Willcox (Cambridge, Massachusetts)
- Rockwell Collins (Cedar Rapids, Iowa)
- Smart Information Flow Technologies (Minneapolis)
- SRI (Menlo Park, California)
- United Technologies Research Center (East Hartford, Connecticut)
- Vanderbilt University, Dr. Theodore Bapty (Nashville, Tennessee)
- Vanderbilt University, Dr. Sandeep Neema (Nashville, Tennessee)
- Xerox PARC (Palo Alto, California)

The goal of the META Program is the model-based design and *verification* of complex systems, using novel design and development processes to ensure functional correctness from the moment that the systems are constructed (Correct-by-Construction). Over a twelve month period, the beneficiaries of the funding were charged with developing:

- a metalanguage for representing highly heterogeneous cyber-electromechanical systems that is capable of expressing all the features required to verify functional correctness,
- a *model*-based design flow suitable for producing systems such as ground combat vehicles,
- a *verification* approach for issuing "probabilistic certificates of correctness" for different designs and
- practical, observable metrics for complexity and adaptability that can serve as guidelines for design optimisation.

General contractors have a whole host of ideas for solving the relevant challenges, ranging from basic technology research to revolutionary concepts for solving the key technological challenges and their integration into existing design tool suites.

A.1.3.3 Networking and Information Technology Research and Development (NITRD)

The NITRD program is the primary federal government mechanism for coordinating R&D investment in non-classified networking and information technology. It officially comprises 14 research funding agencies, but collaborates with a number of other agencies, too. These agencies work together to develop a broad spectrum of advanced network and IT capabilities and to promote the US' scientific, technical and technological leadership and economic competitiveness. This serves to increase the overall effectiveness and productivity of the R&D investments, leveraging strengths, avoiding duplications and increasing the *interoperability* of networking and IT products. The agencies' activities are divided into eight research areas that span a broad spectrum of IT domains and capabilities:

1. High-end Computing Infrastructure and Applications (HEC I&A)

2. High-end Computing Research and Development (HEC R&D)

3. *CyberSecurity* and Information Assurance (CSIA)

4. *Human-Machine Interaction* and Information Management (HMI and IM)

5. Large-Scale Networking (LSN)

6. High-Confidence Software and Systems (HCSS)

7. Software Design and Productivity (SDP)

8. Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW)

The last research area is not relevant to this study, while the penultimate research area is only of limited relevance.

In realising the goal of creating a framework for research and development strategies that focus on game-changing technologies, the NITRD Program has led a series of public-private activities that culminated in the definition of initial strategic themes for transforming cyber-*security*: (a) Tailored Trustworthy Spaces, (b) Moving Target and (c) Cyber Economics and Incentives.

The budget for the first six research areas described above was 3,520 million US dollars in 2010 and is expected to be 3,384 million US dollars in 2011. The budget applied for in 2012 is 3,557 million US dollars. The National Science Foundation (NSF) receives the largest proportion of the funding, with 952 million, 942 million and 1,081 million US dollars respectively in the three years referred to above. The second largest amount goes to the National Institutes of Health (NIH), followed by the Office of the Secretary of Defense (OSD) and the Department of Defense (DOD), the Department of Energy (DOE) and DARPA, in that order. Meanwhile, the most heavily funded research area is High-end Computing Infrastructure and Applications, with 1,281 million, 1,266 million and 1,259 million US dollars, followed by *human-machine interaction* and Information Management, which receives approximately two thirds of these amounts.

A.1.4 BRICS COUNTRIES AND ASIA

The BRIC or BRICS countries (Brazil, Russia, India, China and South Africa) are carrying out a range of activities relevant to the field of Cyber-Physical Systems, albeit often under a different name or as part of wider funding programmes. Whilst it is not easy for third parties to obtain information about these initiatives, it is clear that there is a lot of activity and that significant support is being provided by government and the relevant funding agencies.

A.1.4.1 Brazil

Several projects are underway in Brazil to investigate the opportunities provided by Cyber-Physical Systems. Ciberfloresta, for example, is a Cyber-Physical System that uses environmental *sensors* to detect events such as fires and rain or to determine when the conditions are favourable for sowing or harvesting crops in the forest. Biodigestor Inteligente is a Cyber-Physical System used to control a biogas plant that produces biogas and biofertilisers from animal manure. Meanwhile, the LOGBOT (LOGistic Mobile RoBOT) project has designed a prototype mobile robot for the development of the Amazon rainforest. The robot can be used for telemetry and remote data acquisition as well as for autonomous navigation in indoor environments.

Brazil has had 'smart buildings' that employ *sensors* to respond rapidly to changes in climate since as long ago as the 1970s. They went one step further during the 1980s by establishing functional connections between individual building systems. Today, home and building automation is standard practice in the Brazilian construction industry. The features on offer include energy-saving measures such as active and passive solar energy systems, efficiency and comfort measures, security alarm systems, alarms for medical emergencies, communication systems, remote maintenance and a variety of other functions.

Brazil has also launched a project known as Cidade Inteligente Búzios. The aim is to make the city of Búzios on the Atlantic coast a flagship for smart energy consumption management in Brazil and potentially for the whole of Latin America. The project hopes to enable more efficient energy use by upgrading the city's electricity grid so that it can be controlled automatically. Advances have also been made in the field of smart health. Projects to fully automate hospitals allow integration of *mobile devices* such as smartphones and tablets belonging to both staff and patients, whilst technical systems can be controlled remotely over the Internet. Navigation systems and sensors are also being employed in the automotive sector.

A.1.4.2 India

In India, a project entitled Cyber-Physical Systems Innovation Hub has been launched under the auspices of the Ministry of Communications & Information Technology, Government of India. The project aims to investigate the following topics: Smart Grid Systems, Smart Cellular Networks, Green ICT, Smart Buildings, Smart Healthcare Systems, Humanoid Robots and Search and Rescue Robots. In addition, the Ministry's Department of Information Technology is working on a legal framework for the new technologies. It has devised a strategy for cyber-security in India which is currently being implemented. Cyber-laws provide legal recognition of electronic documents and a framework to support legally binding electronic documents (e-filing) and legally binding online business transactions (e-commerce transactions), as well as for combatting cyber-crime. R&D to develop domestic cyber-*security* solutions is funded through projects run by well-known organisations. The programme supports basic research, technology surveys, proofs of concept, test-bed projects, prototypes and advanced training for people working in the field. Other subsections of interest include the Cyber Appellate Tribunal, the Indian Computer Emergency Response Team and the Controller Of Certifying Authorities.

The Centre for Infrastructure, Sustainable Transportation and Urban Planning (CiSTUP) was established by the Indian Institute of Science (IISc). In conjunction with acatech, CiSTUP organised a symposium entitled Smart Mobility and Energy Concepts for Megacities as part of the German-Indian Partnership for IT Systems (GRIP IT) project. Funded by the Federal Ministry of Education and Research (*BMBF*), this project is intended to act as a catalyst of research and development cooperation between science and industry in the two countries. The symposium focused on the topic of smart cities, and in particular mobility and energy in urban environments.

Meanwhile, Bosch has established the Centre for Research in Cyber-Physical Systems at the IISc in Bangalore. Both the Fraunhofer-Gesellschaft and several top Indian research centres are participating in this project in an advisory capacity. The partnership, which is funded to the tune of 22.8 million euros, aims to create an optimal research and working environment for the IT specialists of the future. Going forward, support will also be provided to industry and the research community, for example through research contracts.

The Indo-US workshops on "Developing a Research Agenda in Pervasive Communications and Computing Collaboration (PC3)" were initiated in response to the rise of globalisation and the growing interconnectedness of countries around the world. Their aim is to plan specific joint research projects in the fields of pervasive computing, communication and e-infrastructure. The workshops identified the key issues and discussed the research agenda and cooperation models and mechanisms. The first workshop took place in New Delhi in March 2011, while the second was held in the US in the summer of 2011. The workshops focused on CPS topics such as smart environments, embedded systems, *sensor networks* and their applications – e.g. agriculture, water and weather –, *reliable* computing (system *security*, homeland security, *data protection*), energy and sustainability (smart grids, environmental and home monitoring), healthcare (personalised, smart healthcare technologies) and how citizen science can be enabled by smart devices such as smartphones that possess the relevant *sensors* and processing power.

A.1.4.3 Russia, China, South Africa

Whilst these countries are undoubtedly active in the field of Cyber-Physical Systems, very little information is available about what they are doing. We do know that Russia's Southern Federal University in Rostov-on-Don is home to the A. B. Kogan Research Institute of Neurocybernetics, while smart buildings are being built in South Africa.

In 2009, a research group was established in the School of Software at China's Dalian University of Technology to address everything from the theoretical principles, design and implementation of Cyber-Physical Systems through to applications and training. The technologies being investigated are networks, protocols, algorithms and software platforms. The research is focused on the *domains* of healthcare, energy, consumer electronics, transport, automation technology and education.

A.2 CURRENT STATUS OF RESEARCH AND TECHNOLOGY

This section will review the current status of research and technology in Germany. It will describe the research projects that are relevant to CPS capabilities in Germany as well as those European projects where there is German involvement.

Germany has several research projects in the field of 'cognitive systems'. These projects are investigating methods, processes and technologies relating to different aspects of the capabilities required for *"X"-awareness*, learning and behaviour adaptation, *human-machine interaction* – including *shared control* –, planning and autonomous, active behaviour. The projects include *Sonderforschungsbereich Transregio* (SFB/TRR) 62, A Companion Technology for Cognitive Technical Systems [SFBb] which was established in 2009. This project focuses on cognitive abilities: the ability to recognise and detect situations and human needs and emotions, interactions and communication between human beings and technological systems in accordance with the current situation, as well as joint planning and decision-taking by people and technological systems.

Since 2003, researchers working on the SFB/TRR 8 project (Spatial Cognition – Reasoning, Action, Interaction) have been investigating the question of how people and robots acquire and process knowledge about their spatial environment, how they find their way around and how they are able to exchange information about their environment. One of the areas where they have been applying their research findings is in the field of *AAL* applications [BAA]. Meanwhile, various projects at the University of Hannover are working on navigation of autonomous systems in outdoor environments [NAV]. Research into *self-diagnosis* is being carried out in different contexts in a variety of European projects. These projects are currently being supported by the EU-funded Coordination Action Awareness [AWA] (Self-Awareness in Autonomic Systems).

In addition to basic research, there are also a number of applied research projects in the field of *situation awareness* and *modelling* that are strongly focused on individual *domains*. The Ko-FAS (Cooperative Sensor Systems and Cooperative Perception Systems for Preventive Road Safety [KOF]) research initiative aims to develop new technologies, components and systems that use cooperative sensor systems and perception systems to provide road users with a comprehensive view of the traffic around them, as well as new safety measures for road users that make use of these sensor data.

In the field of *artificial intelligence,* Germany has a number of high-level research groups whose numerous R&D projects address issues relating to knowledge management, robotics and manufacturing technology, cognitive systems, learning and adaptation, planning and behaviour, agents, virtual reality and intelligent user interfaces. The most prominent of these include the DFKI (German Research Center for *Artificial Intelligence*), which has facilities in Kaiserslautern, Saarbrücken and Bremen, the Research Group on the Foundations of *Artificial Intelligence* at the University of Freiburg, the Neuroinformatics and Cognitive Robotics Lab at the TU Ilmenau, the Cognitive Robotics Working Group at Berlin's Humboldt University and the Cognitive Systems Group at the University of Bremen. One example of the projects that these groups are involved in is the EU-funded CogX project that aims to develop robots capable of working in complex environments where they have to deal with novelty, uncertainty and change. In such environments, robots need to be able to assess the limitations of their own abilities and knowledge (*self-awareness*) and extend these abilities and knowledge based on their experience and goals (self-extension).

Manufacturing technology is one of the areas where research projects are investigating self-organising and self-configuring systems. The KARIS project [KAR] is focused on novel, intelligent and autonomous functional modules for object transportation with a view to optimising material flows in factories. The SFB 653 project (Gentelligent Components in their Lifecycle – Utilization of Inheritable Component Information in Product Engineering) is investigating methods and processes for the *self-organisation* and self-configuration of manufacturing systems using components that intrinsically store information about themselves. The Federal Ministry of Economics and Technology's (*BMWi*) Autonomics programme is concerned with innovative approaches for developing a new generation of smart tools and systems that are independently able to network via the Internet, identify situations, adapt to changing operating conditions and interact with users. The programme's projects address numerous topics that are relevant to Cyber-Physical Systems, for example *sensor fusion* (AutASS project), performance assessment (LUPO project), mobile, cooperative robots (Marion project), autonomous vehicles and robots (SaLsA and Robo Gas Inspektor projects) and self-configuring systems (smartOR and viEMA projects).

A wide range of projects exist in the field of continuous context and process interactions and integration. These are focused on monitoring and controlling goods flows and product life cycle management. Some of the key initiatives include the SemProM [SEM] project, which forms part of the *BMBF's* Digital Product Memory Initiative, the ICT 2020 leading innovation Aletheia [ALE] and the Alliance Digital Product Flow (ADiWa [ADI]). At European level, the ebbits [EBB] project is driving progress on the semantic integration of data from the Internet of Things in enterprise systems and business applications, while the SOCRADES research project is focused on the deployment and *engineering* of service-oriented architectures (SOAs) for networking automation components, industrial wireless communication in the field and integration with the management level.

Numerous projects on *autonomous* driving also exist in Germany, investigating issues in connection with situation recognition, cooperation, *shared control* and autonomous behaviour, as well as concepts, methods and processes for developing *autonomous driving* systems. The Department of Planning and Controlling of Warehouse and Transport Systems [FTS] at the Gottfried Wilhelm Leibniz University in Hannover is running various projects to investigate autonomous vehicles in restricted, controlled environments such as driverless transport systems and automated guided vehicles. Research is also ongoing at vehicle testing facilities into potentially dangerous *autonomous driving* manoeuvres (the *Fahrautomat* (Automatic Vehicle) project [FAM] at Heilbronn University) and fully autonomous vehicle parking in car parks [PAR]. Furthermore, *autonomous driving* in more complex situations, albeit in specific sets of circumstances, is being investigated e.g. by BMW, who are developing an emergency stop assistant as part of their Smart Senior [SEN] project. This system is capable of performing a fully automatic stop when it detects an emergency situation (when the driver becomes incapacitated as a result of a sudden medical emergency). At European level, the Prometheus project [Cir11] is also working in this area. Other projects, such as SATRE [SAT], are investigating *autonomous convoy driving*, while the CyberCars-2 Initiative [CYB] and Citymobil project [CIT] address *autonomous driving* in connection with specific forms of urban transport. Meanwhile, the Stadtpilot [STA] project at the Technische Universität Braunschweig is attempting to achieve fully *autonomous driving* in a real-life road traffic environment.

Applied R&D projects on the topics of cooperation, negotiation and decision-taking are often *domain*-specific in nature. One example in the field of mobility is the Aktiv (Adaptive and Cooperative Technologies for Intelligent Traffic [AKT]) research initiative, which comprises three projects on traffic management, active safety and cooperative cars. Robocup Rescue Simulation [RES] is a project of the international Robocup Association that investigates disaster response strategies using *multi-agent systems*. The ELROB Trial [ELR] is researching the deployment of cooperating robots in hazardous environments.

The following projects focus on innovative *human-machine interactions*. A group at the TU Darmstadt's Institute of Automotive Engineering is working on the Conduct-by-Wire[95] concept which involves a manoeuvre-based driving approach where the driver is largely relieved of stabilising operations such as keeping the vehicle within its lane and is only required to select the general driving manoeuvre that he or she wishes to perform. The NIMITEK (Neurobiologically Inspired, Multimodal Intention Recognition for Technical Communication Systems [NIM]) cluster project funded by the State of Saxony-Anhalt is investigating the basic principles of the processing of *multimodal* input. In the automotive sector, the H-Mode [HMO] project is developing a new and intuitive *multimodal* operating concept for steering vehicles. Meanwhile, in the manufacturing technology sector, the SiWear [SIW] project, which is funded through the Federal Ministry of Economics and Technology's simoBIT initiative, is developing wearable information systems for applications in commissioning, service and repair that integrate people's natural gestures, haptics and speech into work processes and use them for communication purposes. The HaveIT [HAV] project developed *situation awareness* processes and *safety* concepts, in particular new methods for interactions between people and assistance systems and for *shared control.*

Under its *Human-Technology Interaction* [MTi] programme, the Federal Ministry of Education and Research (*BMBF*) is funding a range of projects, some of which have already concluded, to develop technologies that enable communication and the exchange of information between people and IT systems using a variety of different methods such as speech, gestures, facial expression and haptics. However, so far the projects have largely focused on supporting human behaviour through technological systems such as imaging processes for operations and radiotherapy in the field of medical technology (FUSION and DOT-MOBI projects), autonomous manipulator control for rehabilitation robots (AMaRob project), the development process for ambient intelligence systems (AmbiComp project) or support for medical equipment management (AIMES project). Finally,

[95] See [WHB+06].

the DESIRE (German Service Robotics Initiative) project investigated the technological questions associated with *"X"-Awareness*, mobile manipulation and mechatronics, as well as learning and *human-machine interaction*.

The integration of human behaviour *models* into the development of Cyber-Physical Systems is being researched in a number of projects, including IMoST [IMo], isi-Padd-as [ISI], Human [HUM] and D3COS [D3C]. The aim is to make the systems accessible to formal analysis and *verification* techniques.

A whole host of initiatives are being promoted under the German government's ICT strategy that are also relevant to Cyber-Physical Systems, especially in terms of the required infrastructure, platforms and *middleware*. These include the Cloud Computing Initiative and Trusted Cloud technology competition [BMW10d], the Broadband Strategy [ZBB], various programmes connected with the *Internet of Things* (Theseus [BMW10b]) and the *Internet of Services* (Autonomics [BMW11a], Connected Living [CLV], next-generation media [NGM]) and a raft of measures aimed at improving cyber-*security* both in terms of the technology and the overall framework.

The SimoBIT (Secure Application of Mobile Information Technology) programme supports a wide range of projects across four competence fields, including projects for developing a telemedicine platform for the emergency services (Med-on@ix), a platform for remote maintenance of manufacturing equipment *(mobile Servicewelten)* and for integrating semi-autonomous processes and mobile devices into business and service models (R2B, Robot to Business [R2B]).

At European level, too, there are several projects with German involvement to create platforms in different fields of application. These include projects to build *sensor network* platforms such as WASP [WAS] and the ITEA project Vitality [VIT] in the field of healthcare.

The research project sim^{TD} (Safe and Intelligent Mobility, Testfield Germany) is researching and testing car-to-X communication and its applications, for example recognition of traffic obstructions and other hazards. To this end, realistic traffic scenarios are being tested in a large-scale test field infrastructure around the city of Frankfurt am Main in the state of Hesse. The project will also pave the way for the political, economic and technological framework required for the introduction of car-to-car and car-to-infrastructure networking. AIM (Application Platform for Intelligent Mobility [AIM]) is a project of the German Aerospace Centre (*DLR*) to develop a research laboratory for smart transport and mobility *services* that is embedded in a city's real transport environment. It allows new road safety measures and technologies to be developed and tested in a real-life context.

The Hydra project [HYD] is aimed at investigating, developing and validating *middleware* for networked embedded systems in order to enable developers to develop cost-effective, high-performance Ambient Intelligence (AmI) applications for heterogeneous physical devices. The CHROMOSOME *middleware* [CHR] developed by the fortiss institute is an o*pen-source* solution that provides a *communication infrastructure* and execution platform for distributed applications. Platform standards for specific fields of application include e.g. the AUTOSAR standard in the automotive sector [AUT] and the IMA architecture (Integrated Modular Avionics [IMA]) in the avionics industry.

The G-Lab project [GLB] is working to create a basis for the Internet of the future. The 32 partners are investigating the interactions between new requirements and new applications, whilst also providing safe and *reliable* testing facilities for testing the feasibility, scalability and performance of new applications and technologies such as routing and address technologies.

Several of the projects referred to above are also developing processes and methods for *engineering* the specific applications that they are working on. Projects with a specific focus on processes and methods often also pay particular attention to the provision of *Quality of Service* guarantees, especially with regard to *functional safety*. In the field of basic research, the SFB/TRR 14 AVACS [AVA] project that has been running since 2004 addresses the automatic verification and analysis of complex systems. It is investigating automatic methods of safety analysis and formal verification of the *safety* features of networked embedded systems and even open, hybrid systems (Cyber-Physical Systems). Another major national project focused specifically on *model*-based approaches to the development of such systems is the SPES 2020 (Software Platform Embedded Systems 2020 [SPE]) innovation alliance, which is developing solutions for cross-*domain*, *model*-based development of embedded software. *Model*-based processes with a sound mathematical basis allow efficient development of embedded systems, from the initial customer requirements, through design and implementation, right up to the systems' *verification* and certification.

At European level, one project that deserves a particular mention in this area is CESAR (Cost-efficient Methods and Processes for Safety-relevant Embedded Systems [CES]). This project is investigating methods and processes for cost-efficient development and certification of embedded systems – including support from interoperable tools – in the three *domains of* automotive, avionics and rail. In addition, the ITEA project Verde [VER] is working to improve *validation* and *verification* in the development process, while the ARTEMIS project MBAT (Model-Based Analysis and Testing) is focused on improving integration of the testing process. Finally, the SAFE [SAF] project is working on development methods and tools specifically for *safety-critical* automotive applications based on the AUTOSAR standard.

Thanks to a wide range of national projects and extensive involvement in European projects, Germany is extremely well-placed overall in many of the areas that are relevant to Cyber-Physical Systems, particularly in basic research and system development and integration. Nonetheless, the results that have been achieved to date are still a long way off what is needed to deliver the capabilities required for Cyber-Physical Systems. While there are also several projects focused on applied R&D, almost all of them concentrate on individual fields of application. Cross-*domain* and interdisciplinary projects are the exception rather than the rule in this area. Together with the technological challenges (see also Chapter 5), this lack of cross-*domain* initiatives is one of the greatest hurdles that will need to be overcome before Cyber-Physical Systems can be implemented.

APPENDIX B:INTEROPERABILITY AND QUALITY OF SERVICE PLATFORM SERVICES AS ILLUSTRATED BY THE VEHICLE DOMAIN

This study has shown the major increase in functionality and complexity associated with Cyber-Physical Systems compared to the systems that are prevalent today. This is due to the factors described in Chapter 2.6, including increasing convergence of computer systems with their environment (cyber-physical), increased networking of formerly independent systems (*Systems of Systems*), context-*adaptability* and *autonomy*. The advance is so great that it will no longer be possible to achieve cost-effective and reliable development of such systems using traditional methods and technologies. As described in Chapter 5.3.3, in order to manage this complexity some of the functionality will need to be standardised and delivered by an underlying platform.

B.1 INTRODUCTION

The term *CPS platform* refers to the processing and communication hardware, operating system and *middleware*. In recent years, the word '*middleware*' has acquired a whole host of additional meanings, and even more can be expected to come about in connection with Cyber-Physical Systems. In this appendix, *middleware* is used as a generic term for the software layer that sits above the firmware and operating system and provides operating system-related functionality. By taking care of the standard functionality, the platform allows developers to concentrate on the application-specific functions.

Avionics is a good example of a *domain* where this type of standardisation and abstraction have enabled a significant reduction in complexity. Integrated Modular Avionics provide standardised computing hardware, transferring functions that were formerly implemented in the application logic to the underlying operating system.

However, the drawback of current solutions, in terms of both their hardware and their operating systems and *middleware*, is the fact that they focus on specific *domains*. Tailoring individual solutions to a specific class of applications makes them completely unusable for other applications. This approach clearly needs to be altered, making cross-*domain* integration one of the key challenges facing Cyber-Physical Systems. *Domain*-specific hardware and operating system/*middleware* solutions will need to be replaced by modular concepts that allow custom solutions to be delivered – including the ability for these solutions to subsequently be modified in response to changing system conditions – whilst still reducing complexity through standardisation.

In view of the above, this chapter will discuss the capabilities and *services* that any future *CPS platform* will need to provide.

When addressing the requirements for a *CPS platform architecture*, it is important to begin by defining the specific focus. The different levels of a *CPS platform* architecture are therefore briefly described below:

- Hardware and communication level: at this level, the architecture addresses the structure of the processing and communication hardware. In general, it can be said that in the field of embedded systems, the hardware for *sensor* and *actuator* nodes (i.e. *smart sensors* and *actuators*) is becoming increasingly specialised. At the same time, there is a growing need for standardisation of node hardware, i.e. individual processors used to perform computations without interactive input and output *(cloud computing*, mainframes),
- *Middleware* and operating system level: this level relates to the *services* that are implemented in software so that they can be flexibly configured, whilst at the same time being generic enough to be deployable in different application scenarios.

- Functional level: this is the level where application-specific functionality is implemented; this level forms the interface with the logical levels of the *architecture frameworks* referred to in Chapter 5.3.3.2.

There is now a general trend for non-specific functions that are re-used in several different applications within a *domain* to migrate from the functional level where they used to reside to the *middleware*/operating system level. Furthermore, the hardware is now providing basic functionalities – e.g. memory management, memory protection and hardware time stamping – that simplify their implementation in the *middleware*.

Before describing a technology platform's architecture, it is first of all necessary to define the context in which it will operate. For example, a platform can help developers to integrate several different applications onto a single processing unit. The iPhone *application* and technology *platform* is one example of this.

For *safety-critical* systems, *CPS platforms* allow processes of different criticalities to be kept separate in time and space on a single node (Mixed Criticality Systems). This context will hereafter be referred to as the node perspective.

The next context up in terms of size is the system perspective. In this chapter, the term 'system' describes a group of nodes that work together in a predominantly static manner in order to deliver a fixed functionality. A *CPS platform* can be used to integrate different computers into a largely static system. In the medical technology scenario, for example, this might involve combining various pieces of medical equipment and other devices from different manufacturers to create a healthcare CPS. Finally, the most complex perspective is referred to in this chapter as the *System of Systems* perspective. In the abstraction/system levels model in Chapter 5.3.3.2, this equates to the logical architecture levels of the application systems. The individual systems can of course perform their individual functions independently of each other. However, dynamic coordination at runtime with other systems – even ones that were previously unknown – allows these functions to be performed more effectively. *Services* supporting brokering and coordination are included in this perspective.

B.2 CHALLENGES

As discussed at the beginning of this chapter, future technology platforms comprising hardware and operating systems/*middleware* will enable modular integration of individual *services* so that they can meet the requirements of different application scenarios while still being usable by systems with limited resources. This will require open standardisation in order to reflect the cross-*domain* nature of Cyber-Physical Systems. Although the majority of the platform functionalities described below are already implemented in different applications today, researchers and developers nonetheless face a number of challenges, the most important of which are as follows:

- **cross-domain standardisation:** in the future, *services* that currently already have specific implementations for individual *domains* will need to be developed generically so that they can operate across different *domains*. It will be necessary to determine which aspects of the relevant service's functionality are only relevant to a specific *domain* and which aspects can be implemented generically.
- **modularisation of existing platforms** and the need to guarantee technical and increasingly also s*emantic interoperability*: today's platforms generally have monolithic structures. Cyber-Physical Systems are characterised by the heterogeneity both of their requirements and of their hardware, which can range from the tiniest microcontrollers to complex *cloud computing resources*.

A modular platform is therefore essential, so that the modules required for the current application can be selected. The development of appropriate interfaces will be absolutely key to the implementation of such a platform.

– **secure integration of modules into platforms**: the modular platform trend will, however, also involve huge variability in the instances of a platform. It will be necessary to develop methods to ensure the correct functioning of the different variants in open and cross-*domain* applications, particularly as far as their non-functional features are concerned. One especially challenging aspect is that the various platforms will themselves need to be dynamically adapted in order to be able to respond to the changing requirements of open, networked CPS applications.

One key consideration is the extent to which platforms support the rapid and reliable performance of *services* so that the tasks and challenges described in Chapter 3.5 can be met.

B.3 DESCRIPTION OF THE SERVICES

A series of expert interviews were used to identify the functionalities that future *CPS platforms* will need to deliver in order to ensure that the application *services* provide the *interoperability* and *Quality of Service* required by CPS. These platform functionalities are modular and consist of numerous incrementally developed *services*. In this context, *services* are logical units with clearly defined semantic and syntactic interfaces that are configured individually for applications and can be reused in any number of other applications. A *service-oriented architecture* concept describes the design and implementation of an application using *reusable services*. Depending on the abstraction level and degree of *autonomy*, a *service* may be able to describe its own capabilities and features.

Figure B.1 shows the potential *CPS platform services* identified by the experts in this study. In the following sections, these services are grouped together under different themes.

B.3.1 COMPONENT MANAGEMENT

In order for the platform to automatically manage these *services* and the application components, component management *services* are required. This section will focus on the management of static components, while section B.3.3 will consider the additional aspects involved in supporting dynamic system behaviour.

B.3.1.1 Services and system management

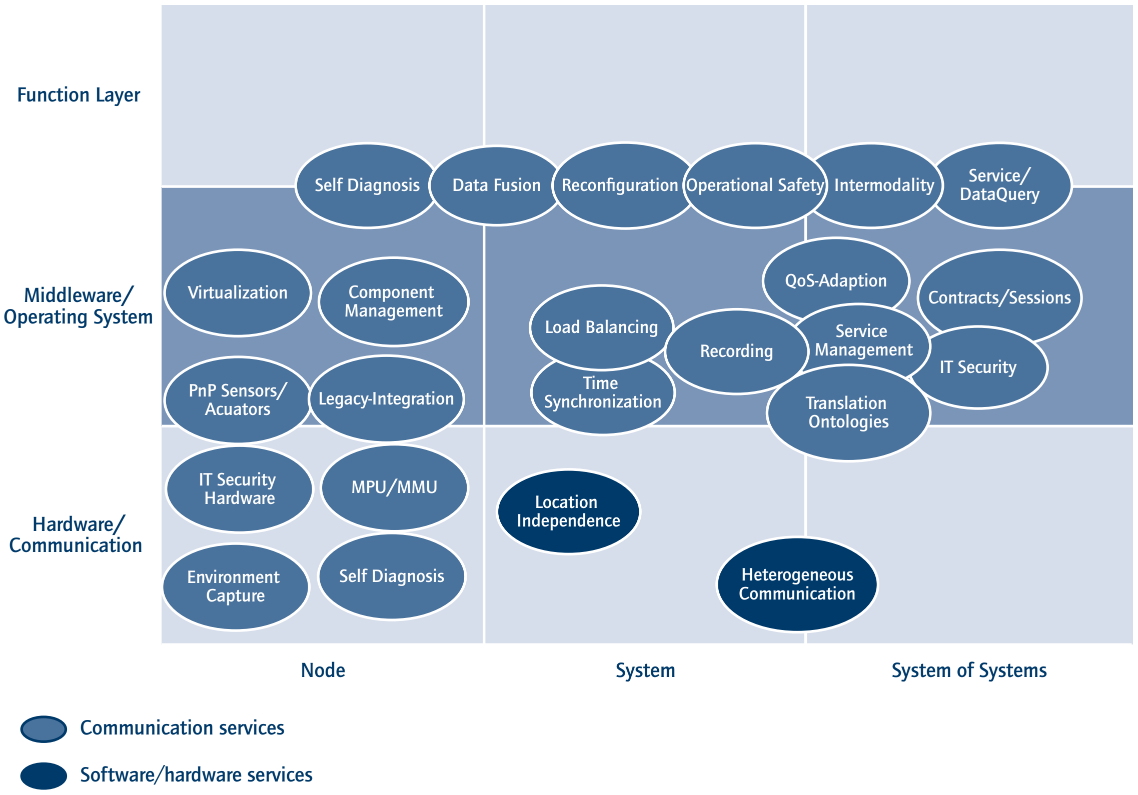
Services are managed on a distributed *service* management platform and communicate using standard communication technologies such as the Internet/Web and telecommunications. Various different functions are required to manage them:

Service life cycle management allows a *service* to be managed throughout its life cycle, from its design, implementation and installation to its execution on the platform and maintenance (e.g. updates), right up to the moment when it is removed and uninstalled.

Service composition allows different *services* to be combined in order to perform tasks or map processes that involve more than one *service*. *Services* are combined via their interfaces in conjunction with application-specific program code and sequences can be defined. *Service* composition manages and monitors the execution of the composition and makes it available as an abstract service via service publication.

Service binding transformation ensures that different *services – as well as services* and applications from different companies **that use different implementation and**

Figure B.1: Generic *CPS platform services* identified by the experts



communication technologies – are able to exchange data on a distributed *service* management platform. In order to make this possible, the different bindings to protocols and technologies for a given *service* are transformed into the required bindings to protocols and technologies for its partner *service*. For the *services*, this occurs in a completely transparent manner, meaning that they do not need to be adapted to each other and that the transformation can be performed automatically on the platform; see Enterprise Service Bus (ESB).

Service message routing allows *services* on a distributed *service management platform* to be addressed and makes it possible to ensure that messages and data exchanged between the providers and consumers of the *service* can be delivered securely. This function is performed e.g. by the Enterprise Service Bus (ESB) in the field of smart homes.

In current systems, system management, i.e. global management of the composition of several components, is still implemented in a highly domain-specific manner. However, it is set to play a far more important role going forward. Some of the key questions relate to the control and management of the overall system. Striking the right balance between centralised system management and decentralised or *self-organising* approaches constitutes an ongoing challenge for Cyber-Physical Systems and in many other areas, too.

B.3.1.2 Application component management

For systems to be able to respond to changing scenarios and tasks, they need to be dynamically adapted to the relevant requirements, irrespective of whether they are deployed as an isolated system of as part of a complex Cyber-Physical System. To this end, it is extremely important to be able to install new software components and update the components that have already been installed. Performance of this *service* requires cooperation between several different components, for example *QoS* monitoring and adaptation or *self-healing* and reconfiguration. This is key to ensuring that there is no detrimental impact on the *services* being provided and that the new *services* do not pose a *security* risk to the entire system.

In the *smart mobility* scenario in Chapter 2.2, this *service* can be used to update or upgrade the vehicle's or control unit's software while it is at a service centre. A precise knowledge of the local node – in this instance, the control unit – and its requirements enables the application management *service* to ensure that the new or additional software components do not place too great a load on the node.

B.3.2 PHYSICAL ENVIRONMENT AND CONTEXT AWARENESS

In addition to platform *service* and application component management, Cyber-Physical Systems need to be capable of recognising their environment and the physical system context, as discussed in Chapter 2.6.1.

B.3.2.1 Sensor technology for environment and context awareness

In the *smart mobility* scenario in Chapter 2.2, various different *sensors* are employed to ensure that the Müllers have a smooth journey. *Sensors* on board the car and in the infrastructure enable the Müllers' vehicle to detect a child running out into the road.

B.3.2.2 Data fusion service

Data fusion has a variety of uses in Cyber-Physical Systems. The deployment of different, redundant sensors is absolutely key in *safety-critical* systems in order to prevent incorrect decisions based on inaccurate *sensor* data. A further factor is the widespread use of several cheap, redundant but less reliable *sensors* instead of extremely expensive but more *reliable individual sensors*. Furthermore, in complex systems it is usually not even possible to measure the necessary information directly.

Although the actual data fusion is application-specific, certain generic basic functions are performed by the platform, for example redundant data fusion or the stitching together of a single image from several cameras with overlapping fields of view. The application also ensures application-specific interpretation of the data, e.g. to determine whether a driver is leaving his lane intentionally. This assessment can only be made with sufficient certainty by using several different *sensors* – for example indicators, proximity *sensors* and cameras – and by drawing on the relevant application knowledge as contained in *domain models*, for example.

B.3.2.3 Time synchronisation services

Cyber-Physical Systems involve two essentially opposing trends: the ongoing increase in the distributed execution of *services* and applications on the one hand, and the increasing requirements in terms of data fusion and coordinated execution on the other. As a result, it is important that the platform should provide time synchronisation *services*. This allows data fusion and the implementation of *fault tolerance* to be significantly simplified. Unlike in traditional closed systems, CPS time synchronisation will also have to work in heterogeneous networks.

The *smart mobility* scenario provides a simple illustration of the importance of time synchronisation for data fusion. In order to achieve successful fusion of the data from different *sensors* such as radar and cameras, it is essential for the *sensors* to be very accurately synchronised with each other.

Time synchronisation is enabled by *services* at the different levels. The hardware level requires extremely accurate clocks and the ability to generate time stamps for specific events such as the sending of messages. In order to support time synchronisation in heterogeneous networks, it will be necessary to make increased use of devices with external – e.g. GPS-based – time synchronisation. At the *middleware* level, the time synchronisation algorithms need to be converted into *services*, whilst also taking *fault tolerance* aspects into account.

B.3.3 DYNAMIC MANAGEMENT

In the future, Cyber-Physical Systems will need to use their context and environment awareness capabilities to adapt semi- or fully automatically to changing circumstances. This may also require them to be capable of fully or semi-autonomous behaviour, as described in Chapter 2.6.1. A range of *services* will be needed to make this possible.

B.3.3.1 Service and data publication and search services

Cyber-Physical Systems are made up of *services* from different providers – the full range of providers and available *services* is not usually known at the time of their design. *Service* and data publication and searching enables *services* to be combined flexibly in spite of this uncertainty.

Service publication enables providers to inform potential users about their *services* using distributed, globally available catalogue-style directories. Entries in these directories should at the very least comprise a description of the *service* and its interfaces, as well as a *service* contract. Semantic information should also be stored using standardised technologies for the semantic description of *services*. This allows information about the *service* to be processed automatically and means that the *service* can be dynamically integrated into different applications. Publication can be carried out centrally via a directory *service* or on a peer-to-peer basis – for instance, when the Müller's car communicates with the transport infrastructure.

The same applies to *service* search facilities. These enable applications to search the distributed directory for *services* that can meet specific requirements. This can be done during the application's design and implementation stage, or dynamically, during execution time, using semantic information about the relevant requirements and *services*.

It would not be possible to adequately adapt a monolithic solution to the required functionality to enable its use with embedded systems. One possible alternative approach might be a hierarchical implementation along the lines of DNS servers on the Internet. One application in the field of *smart mobility* could involve roadside units that provide information about the condition of the road surface or the volume of traffic on the road. During the journey, the vehicle's onboard electronic systems would search for *services* providing information relevant to its route. The *service* search facility would allow these *services* to be identified, located, assessed for relevance and incorporated into the system. Since the vehicle's position will be constantly changing, so too will the composition of this *System of Systems*. New *services* will be added, whilst others will be removed. Additional *interoperability services* will be required in order to enable communication with the relevant *services* and ensure that they all interpret the data in the same way, both syntactically and semantically. *Quality of Service* (QoS) evaluation is particularly important when it comes to choosing *services*.

B.3.3.2 Services for providing sensors and actuators with Plug and Play capability

In addition to providing the ability to incorporate new software components, systems will also need to support the integration of sensors and actuators. One of the main reasons for this is the long service life of *CPS platforms* and their substantial cost, making it important that they should be easy to expand, even by the end user. This will require *services* that allow the node to incorporate new sensors and actuators at run-time and make them available to the applications without needing to reprogram them. These *services* will allow new capabilities to be added to nodes in a flexible manner without making any active interventions in the system. Once the new hardware has been connected, its functionality is immediately available to the node and ultimately to the overall system.

This capability can be put to use at several different points in the *smart mobility* scenario. For example, it means that an infrastructure that only possesses basic functionality when it is first installed can gradually have additional functions added to it over time. This allows it to be simply and cost-effectively adapted to new or changed requirements, as well as enabling its quality to be improved. One possible application in the *smart mobility* scenario, for instance, might involve automatic integration of a touch-sensitive screen for the back seats into the vehicle's infotainment system as soon as it has been physically installed.

B.3.3.3 Load balancing and energy efficiency

The dynamic changes implicit in Cyber-Physical Systems will require equally dynamic adjustment of the processing and communication load by moving software components around, as well as appropriate configuration of communication. This is essential, both in order to prevent congestion and to ensure *energy efficiency*. The load balancing function can be developed by the platform both as a *service* provided to the outside world and as an internal mechanism that runs transparently – i.e. invisibly – for the application.

Cyber-Physical Systems must be capable of using a variety of load balancing media both for internal communication with CPS nodes and for external communication with other Cyber-Physical Systems and the required *services*. This applies to both incoming and outgoing data. These media should include radio communication standards such as WiFi, WiMAX, GSM, GPRS, EDGE, UMTS, HsxPA, LTE, Bluetooth, NFC, FM Radio, etc. It will be key to ensure that these media can be used in parallel whilst simultaneously being prioritised or weighted, both for outgoing and incoming communication. In the *smart mobility* scenario, for example, a person might simultaneously use the private WiFi in their garage at home for uploading the entertainment or navigation system and GSM/LTE for gathering *sensor* data. The vehicle's outgoing data streams are especially important in this regard and will need to be smartly distributed based on the available bandwidth, the security of the media or the cost of the connection. Other factors that will need to be taken into account include data compression, encryption and *authentication*. The system will also need to work with location-independent communication.

B.3.3.4 Location-independent communication

Communication, networking and *interoperability* are some of the basic *services* provided by nodes, systems and *Systems of Systems*. It is important to draw a distinction between internal/local and external/global communication. Internal communication refers to communication between nodes or systems that are part of a single entity – i.e. if they are in the same location or form part of the same object. An example of internal communication in the *smart mobility* scenario is the interaction between the car's on-board *sensors* and the navigation system.

External communication, on the other hand, refers to communication between nodes or systems at different locations or between different objects. Since in this case direct communication is not possible, it is necessary to transfer data between different networks via IP transport (routing). However, the fact that routing will usually always follow the address (identity, EID[96]) of the node or system means that location-independent communication is not possible, since this requires the identity of the node or system to be separate from its location. The location (routing locator, RLOC) describes how and where a system or node is connected to the network, while the identity (EID) defines the node or system with its IP address.

One example of location-independent communication in the *smart mobility scenario* is vehicle network roaming via different connection technologies such as WiFi, GSM and LTE. If the vehicle is using the home WiFi connection while it is parked in the garage, its current location is defined by the home WiFi IP address. However, when the vehicle drives out onto the road, it is defined by the IP address of the mobile communications connection. This means that the vehicle's network is always connected to the Internet and its Cyber-Physical Systems or nodes can therefore communicate with other external Cyber-Physical Systems or nodes. Appropriate IP address mapping enables seamless communication.

Additional benefits of decoupling location and identity include not being tied to a particular Internet protocol (IPv4 or IPv6) or transport protocol (IPv4 or IPv6). Furthermore, when the EID is registered, as well as its location (IP address), additional information about the Cyber-Physical node or system can also be stored in the database. This might include e.g. geographic coordinates, the properties of the node or system, a description of the connection with the aid of *security* measures, *virtualisation* techniques and encryption, and much more besides.

B.3.3.5 Energy management services

Mobile nodes and systems that in principle do not need to be permanently connected to an electricity supply are a key component of Cyber-Physical Systems. Examples include the nodes in a wireless *sensor network* and electric vehicles. In these scenarios, it is necessary to ensure that the power available to the node or system is used optimally, and this in turn requires an energy management *service*. This *service* collaborates with other *services*, e.g. reconfiguration *services*, to ensure that the most important system functions are supplied with power for as long as possible. In order to do this, it may be necessary for certain subsystems to be switched off or placed into power saving mode.

In the *smart mobility* scenario, for example, this *service* might deactivate certain comfort functions in the Müllers' vehicle if the vehicle's battery charge fell below a critical threshold and it was not possible to get to a charging point before the battery went flat.

B.3.4 SERVICE INTERACTION

The fact that *services* from different providers are combined dynamically means that the interactions between them need to be regulated by contracts. Some of the technologies that could be used to do this are discussed under B.3.2. The following *services* will be required in this context:

B.3.4.1 Contract and session management

Whenever several independent systems wish to interact with each other without their operators having previously signed explicit contracts or agreements, there is a need for mechanisms capable of negotiating the terms of the co-operation at run-time. These can include the required *Quality of Service* and the relevant fee.

Consequently, *Systems of Systems* require *services* that can select the service that best meets the user's requirements from among those that are available and negotiate the conditions of use. They will often also need to strike a balance between cost and *Quality of Service*. In addition to searching for and negotiating the terms of new communication relationships, this *service* is also responsible for managing

[96] Endpoint Identifier.

existing contracts. For example, it may select a more suitable *service* or one that is equally suitable but cheaper, all at runtime. In order to evaluate individual contracts and sessions, it is necessary to use information obtained from other *services*, for example *Quality of Service monitoring services.* In the context of *smart mobility*, this *service* can be used in order to negotiate contracts for the use of the *services* found by the *service* search facility. The driver might, for example, select a radio station that plays a particular kind of music. As long as the vehicle can pick up the station's signal, it can tune into the station free of charge over the radio. However, when the vehicle can no longer pick up the signal directly and the reception quality starts to deteriorate, it can switch to a fee-based online music *service*. The switch from the free *service* to the fee-based *service* can be carried out by the contract management *service*. Moreover, the system can then switch back to the free service as soon as it becomes available again.

B.3.4.2 Service interaction logging service

Since applications from different providers will often be involved, it is necessary to have a means of monitoring and legally documenting the interactions between the different *services*. This is essential, not only for accurate billing, but also to establish who was responsible in the event of an error.

In the *smart mobility* scenario, Frau Müller uses several services that can be paid for using a billing function in the *middleware*. For example, she books a hire car, a train journey and a hotel room. Moreover, since Frau Müller also has an airline loyalty card, the billing function in the CPS *middleware* needs to be flexible enough to offer different customers different prices for the same *service*.

B.3.5 QUALITY OF SERVICE

Since a Cyber-Physical System's functions are experienced directly, it is extremely important to ensure that *Quality of Service* (QoS) is monitored and guaranteed, as illustrated by the *services* described below.

B.3.5.1 QoS monitoring and adaptation

In the field of Cyber-Physical Systems, systems are created at the *System of Systems* level which involve a large number of contracts containing the relevant guarantees as opposed to being coordinated and controlled by a single person or business. It is therefore important to ensure that the guaranteed features are actually delivered. Typically, these QoS parameters would relate to bandwidth, latency and reliability of communication.

QoS should also incorporate the quality of the *service* that indicates how accurate the data are, for example by quantifying the accuracy of the measurements made by temperature *sensors*. Based on the content of the contracts and the quality assurances given by the *service* provider, the QoS monitoring *service* can ascertain whether the promised quality has been delivered or whether it is necessary to *adapt* the *System of Systems* in order to achieve an adequate quality standard. In addition to this type of *Quality of Service* evaluation, user-oriented quality evaluation (*Quality in Use, Quality of Experience*) is also becoming increasingly important in the field of Cyber-Physical Systems.

In the *smart mobility* scenario, the QoS monitoring *service* can be used to monitor external *services* such as route planners and make sure that they deliver the promised *service* quality, e.g. with regard to response times. A soon as it detects that a QoS guarantee has been breached, it can assess whether to adapt the system by checking if alternative route planning *services* with more dependable QoS guarantees are available. If necessary, it can then switch to the alternative *service*.

B.3.5.2 QoS-enabled communication

The typically distributed configuration of Cyber-Physical Systems means that communication plays a particularly important role in ensuring the desired *Quality of Service*. Communication *Quality of Service* (QoS) means that the required communication connections with the specified features are available to the user at all times, irrespective of their location. In the case of Cyber-Physical Systems, a number of other key features need to be added to this definition, as described below.

QoS-enabled communication for Cyber-Physical Systems requires different end devices to establish communication with each other automatically, effectively, in accordance with the needs of the current situation and in *real time, as well as to exchange* context-related data securely, *reliably* and efficiently. This will necessitate the investigation and development of robust, *secure* and powerful communication platforms, protocols and standards that are compatible with the existing *ICT* infrastructure. These must be capable of adapting to systems' requirements and be suitable for building future hierarchical, heterogeneous Cyber-Physical Systems. It will be necessary to develop technologies that enable autonomous, failsafe and secure communication and that continue to perform critical functions at all times and under all circumstances, irrespective of any accidental or malicious damage or interference.

For example, if Frau Müller's children are watching a video on a *mobile device*, a minimum bandwidth needs to be guaranteed, irrespective of whether the device is still communicating with the wireless LAN at their nursery school or with the video server via UMTS.

B.3.5.3 Self-healing and reconfiguration service

As has already been discussed, Cyber-Physical Systems have a lengthy service life, which means that they will potentially also have longer service intervals. As a result, such systems will require *self-healing* and reconfiguration capabilities at the functional level, since it is inevitable that they will suffer failures or experience a deterioration in their *Quality of Service* over the course of time; see also the *self-organisation* technology referred to in Chapter 5.1, B6. This will require *services* that monitor individual components, adapting the configuration as necessary. This could involve rule-based component replacement, switching over to use free system resources, or even deactivating non-essential components in order to guarantee minimum functionality.

In the *smart mobility* scenario, for example, the electronic systems on board the Müllers' vehicle will comprise a small number of powerful control units rather than the large numbers of less powerful controllers that are currently still the norm. If a *safety-critical* subsystem such as the Steer-by-Wire system develops a fault during a journey, the infotainment system could be automatically deactivated, thus freeing up resources to allow the *safety-critical* functionality to be maintained. Another example involves switching from radio to Internet reception mode, as described above in the context of QoS monitoring.

B.3.6 SAFETY AND SECURITY

Because of the open nature of Cyber-Physical Systems and the fact that they intervene directly in the environment, both *safety* and *security* are extremely important issues. They are enabled by a wide variety of platform *services*.

B.3.6.1 Security services and hardware

Security services are a range of *services* that afford the node, system or *System of Systems* protection against attacks. It is necessary to adopt an integrated approach to *security* so that there are no weaknesses for potential attackers to exploit. Consequently, Cyber-Physical Systems *middleware* should provide these *services* for systems and *Systems of Systems* as well as for individual nodes.

At the level of the individual node, *security services* need to provide protection against attackers who try to compromise the node either through direct physical interventions or via the communications interface. *Security services* must ensure that attackers cannot tamper with the node's software and prevent unauthorised access to stored data. The *security services* can do this by using a hardware security module (*HSM*) that provides secure memory and a secure execution environment for cryptographic operations. It is also necessary to provide protection for communication between the individual nodes within a system. It is important to ensure that only authenticated and authorised nodes can communicate with each other, as well as to guarantee the *integrity, confidentiality* and *availability* of this communication. Cryptographic protocols may be used for *authentication* or encryption, for example.

Since individual nodes within a system can behave maliciously, e.g. if they have been compromised by an attack, additional processes are needed in order to identify the attackers. For example, CPS *middleware* can provide network-based intrusion detection systems or employ attestation processes to verify the platform integrity of individual nodes. This allows any nodes within a system that have been tampered with to be identified and countermeasures to be taken, for example by excluding the relevant nodes; see also the aspects discussed under B.3.5.3. At the *System of Systems* level, the *middleware* needs to provide protection for communication between the system and other, unknown and potentially malicious systems. There is a particular need for mechanisms to evaluate the trustworthiness of the other systems with which communication is taking place.

The implementation of the *middleware* also needs to pay special attention to the relationship between *safety* and *security*. *Security services* should have no impact on certain *safety* requirements. For example, it is important to ensure that cryptography *services* do not consume so many resources that *real-time* requirements can no longer be met. At the same time, it is of course also true that *security services* can have a positive impact on safety by preventing attacks on *safety-critical* functions. For instance, *security services* can protect a vehicle system against external attacks aimed at remotely seizing control of or tampering with the vehicle's steering system.

A whole host of different *security services* can be employed in the *smart mobility scenario*. For example, Sabine Müller uses her *mobile device* to identify and authenticate herself to her hire car. Once she has authenticated herself vis-à-vis her *mobile device* by entering her PIN number, the *mobile device* then uses an integrated *HSM* to provide secure *authentication* vis-à-vis the vehicle.

By virtue of being a highly networked system, the hire car is also exposed to numerous risks. The hire car system can be protected by protecting the vehicle's individual control units using e.g. *HSMs* and other measures, and by protecting the communication between these control units using cryptographic protocols. The *smart mobility* Cyber-Physical System's *safety and security* is heavily reliant on the *authentication*, integrity and *confidentiality* of communication between the individual component systems, i.e. mobile phones, vehicles, booking systems, etc. These need to be protected by authentication, integrity assurance and encryption *services. Services* are also required to provide protection for communication with unknown and potentially malicious systems. Special attention should be paid to the relationship between *security* and *safety* in this scenario. Attacks on *security services* cannot be allowed to have a negative impact on *safety*-critical operations; see the example given above with regard to the resources consumed by cryptographic *services*.

B.3.6.2 Safety services

Platform *safety services* are a range of *services* that enable the system to protect its users from danger. They can be subdivided into *services* for the prediction, detection, prevention, fixing and tolerance of faults. One key feature of Cyber-Physical Systems is that they are highly integrated, meaning that *safety-critical* and non-critical systems are executed on a common platform. In order to enable Cyber-Physical Systems to be developed within a reasonable timeframe and as cost-effectively as possible, the platform should support application-independent mechanisms for guaranteeing *fault tolerance* and separation. In the hardware layer and at the node level, these include support for memory separation mechanisms or dual-channel architectures that include fault detection, whereas at the *middleware* and system levels they involve redundancy management and status monitoring *services*. Finally, application-specific responses for ensuring *safety* and *security* are implemented in the application layer. It will be important to ensure that, for the foreseeable future, *safety* is first and foremost addressed and guaranteed at the system and application levels, particularly because of liability issues.

There are numerous *safety services* that could potentially be used in the *smart mobility* scenario. For example, the semi-autonomous driving function of the Müller's hire car could be designed to be redundant at the hardware level in order to prevent any danger to the vehicle's occupants in the event of a hardware failure. Redundancy management can be performed by the *middleware* and the redundancy mechanisms can be implemented generically. In the event of a fault, there is always the option of disabling comfort functions in order to guarantee safe performance of *safety-critical* functions. Should this happen, the driver would need to be informed of the reason for this reduced functionality and how it can be restored.

B.3.6.3 Virtualisation, memory management and memory protection services

The ever greater processing power of individual *compute nodes* means that several different applications can be executed on a single hardware component in Cyber-Physical Systems. In this context, it is important to ensure that *safety-critical* or *confidential* applications can be executed separately. This can be achieved by keeping them separate in time and space (*virtualisation*) in the *middleware*. Separation in time can be implemented exclusively in software by means of scheduling, using a rotating time slice with dedicated sectors for each application.

On the other hand, separation in space on the relevant hardware is reliant on memory protection and management *services* such as Memory Protection Units (MPUs) and Memory Management Units (MMUs).

In the *smart mobility scenario,* this separation is evident within the vehicle *domain* in relation to networked functions in the Müller's hire car. The vehicle has a small number of powerful control units that perform a range of functions. The consequences of their failure vary from one function to another – while failure of the infotainment system is non-critical, if the Steer-by-Wire system were to fail the consequences could be fatal. These functions must therefore be executed reliably with the aid of *middleware services* and should be allocated separate memory areas for storing their data. Furthermore, access to these memory areas should be monitored by a hardware *service* such as a Memory Protection Unit.

B.3.6.4 Self-diagnosis service including sensors and actuators

In order to ensure their *functional safety*, Cyber-Physical Systems need to be able to monitor themselves at the node level, since in certain applications the individual CPS nodes are difficult or even impossible to access. Moreover, Cyber-Physical Systems may contain huge numbers of nodes, making manual diagnosis impractical. It is to some extent possible for the *middleware* to carry out *self-diagnosis* tasks, since many hardware tests, for example, are not tied to specific functions. However, in other cases application knowledge is absolutely critical, e.g. in order to ensure that diagnosis function scheduling does not impair any of the system's hard *real-time* requirements. Furthermore, dedicated *actuators* and *sensors* are required for diagnosing faults in the system's *sensors* and *actuators* by stimulating the *sensors* and testing the *actuators*.

In the *smart mobility* scenario, the Müllers use a car from a *car sharing* pool. Since the people using this car are constantly changing, it is essential for it to be equipped with automated *self-diagnosis* functionality so that its *reliability* can be guaranteed. At the functional level, it should be fitted with sensors for checking e.g. that the headlights are working properly. Meanwhile, the *middleware* should also provide diagnosis functions for checking that the built-in controllers are operating correctly.

B.3.7 INTERMODALITY AND INTEROPERABILITY

The pervasiveness of CPS *services* in every area of our lives means that inter*modality*, *interoperability* and the associated *services* will become increasingly important. This also applies to the *multimodal human-machine interfaces* required to enable intuitive *human-machine interactions* as described in Chapter 3.3.1.

B.3.7.1 Intermodal user input and information display

The interaction options that Cyber-Physical Systems offer their users are fundamentally different to the user interfaces of traditional information processing systems. Cyber-Physical Systems pervade every area of the environment and people's everyday lives. Users will therefore interact with Cyber-Physical Systems in a variety of different situations, for instance on local public transport, when engaging in sport or in their homes. As a result, Cyber-Physical Systems need to provide their users with more than just a manual user interface – they need to offer intermodal control via speech, cameras or input devices. Moreover, the system's responses also need to be provided inter*modally*. The *services* required to achieve this should be delivered by the *middleware* and include e.g. hypertext interpreters and text-to-speech systems; see Chapter 5.1, T7: *Human-machine interface*.

In the *smart mobility* scenario, these *services* might be employed to enable Frau Müller to read today's newspaper on a business trip involving various different means of transport. Since the planning of her route is automated, Frau Müller doesn't know which means of transport she will be using until her journey begins. However, this doesn't prevent her from getting to read her newspaper, since the CPS *middleware* sees to it that she can read the paper on a tablet PC while she is on the train and have it read to her by a text-to-speech system while she is in her car.

B.3.7.2 Translation of ontologies, data formats and protocols

In order to ensure that different *services* can be combined flexibly, it is essential for them to interpret the relevant data and application contexts in the same way. Furthermore, each *service* needs to understand the data formats and protocols of the other relevant services. Systems from different manufacturers and *domains* are unlikely to be able to do this by default, meaning that *translation* services will be required. In the case of *ontologies*, this might involve *services* capable of mapping one *ontology* onto another; see Chapter 5.1, T13. The mapping can then either be stored by a platform *service* or used as a translation. Data formats and protocols can be dealt with in a similar manner. It possible to imagine *services* that are capable both of converting data formats and acting as a proxy for other systems in order to translate the necessary protocols. This also facilitates the integration of legacy systems and components.

In the field of *smart mobility, these services* could be used to integrate *sensors* that have already been installed in and around the streets so that they can be used by new systems. These might include *sensors* that measure the ground temperature or how slippery the road surface is, for example. The information provided would enable the vehicle to warn the driver of hazardous conditions on the road ahead or suggest an alternative route if necessary.

APPENDIX C: RESULTS OF SURVEY OF SMALL AND MEDIUM-SIZED ENTERPRISES

This appendix presents a summary of the responses to the online survey "Future Technology Trends: Cyber-Physical Systems", that was carried out in July 2011 as part of the agendaCPS project, in conjunction with "Elektronik Praxis" magazine [aca11c].

The 126 small and medium-sized enterprises that responded to the survey – the majority of which came from the industrial electronics, automotive, medical technology and healthcare sectors – assessed the technological, economic and social opportunities and challenges associated with Cyber-Physical Systems as well as the research support provided by government. The companies in the survey indicated that although they expect to benefit from Cyber-Physical Systems, they believe that there is a shortage of skilled labour with interdisciplinary training. They also called for greater government support.

The full list of the questions in the survey is given below, accompanied by summaries of the answers received.

I. Technological challenges (1)

Question: *Networking is a key feature of Cyber-Physical Systems. In the future, it will be necessary to ensure interoperability of very different subsystems in order to enable comprehensive networks to be established. Listed below are six technology areas where key research questions have yet to be resolved. On a scale of 1 – 5, please identify the areas that you consider to be the most challenging.*

Answers:

- Core technologies and infrastructure were considered to be less problematic.
- Sustainability, *safety* and *security* were regarded as the most difficult issues.
- *Human-machine interaction*, system adaptability, methods and techniques (*engineering*) and norms and standardisation also tended to be viewed as challenging topics.

II. Technological challenges (2)

Question: *In which of these areas do you regard SMEs as the most important source of expertise?*

Answers:

- It appears that SMEs believe that they are the most important source of expertise in the field of system adaptability. This includes e.g. exploratory processes for ad hoc establishment and application of compatibility, *adaptation* concepts and *self-healing.*
- The next highest-ranked areas were sustainability, *safety* and *security* and methods and techniques (*engineering*).

III. Technological challenges (2) ctd.

Question: *Please give the reasons for your answer:*

Answers:

- SMEs believe that their flexibility and close relationships with their customers mean that they have particular expertise in the field of *human-machine interaction.* They view their flexibility as a core competency in the fields of "system adaptability" and "methods and techniques".

IV. Economic challenges (1)

Question: Owing to their highly networked nature and the open architecture that they ideally seek to employ, *Cyber-Physical Systems could potentially have a disruptive effect on traditional business models. For example, the services in a Cyber-Physical System can no longer be exclusively delivered by a single provider – they can only be provided collaboratively by combining various existing technologies, services and solutions. Do you expect Cyber-Physical Systems to have an impact on your business model?*

Answers:

- Most of the respondents believed either that Cyber-Physical Systems will tend to have a positive impact on their *business model*, or that it is still too early to predict their impact.

V. Economic challenges (2)

Question: *In which areas do you think future Cyber-Physical Systems will provide the greatest opportunities for your business?*

Answers:

The following areas, listed in order of importance, were considered to offer the greatest opportunities:

- introduction of new services based on Cyber-Physical Systems
- introduction of new products based on Cyber-Physical Systems
- enabling the company to tap into new markets/ business areas
- benefitting from synergies arising from networking, standardisation and interoperability
- increasing global competitiveness
- delivering time and cost savings
- *human-machine interaction* as a specific future market

VI. Economic challenges (3)

Question: *The increased networking will lead to closer cooperation between different companies. Has your business given any thought to new forms of cooperation (open source, open innovation, the use of swarm intelligence, etc.), and if so, how have these been implemented operationally?*

Answers:

- *Open source* is widely used, although attitudes towards it are nonetheless often rather negative.
- Some companies are also starting to implement partnership models, e.g. with higher education institutions, and are using open innovation as a strategic innovation tool.

VII. Economic challenges (4)

Question: *Studies are always claiming that although Germany is good at developing cutting-edge technologies (e.g. the development of MP3 technology by the Fraunhofer Gesellschaft), it is not as successful as US companies (e.g. Apple) when it comes to marketing these technologies as products. Do you agree with this view? If you do, what do you consider to be the greatest general and specific obstacles for your business in terms of successfully transforming technologies into winning products?*

Answers:

- most respondents agreed with the view expressed in the first part of the question
- the following areas were considered to constitute the main obstacles to innovation:
  - reluctance to take risks, lack of entrepreneurship and fear of failure
  - too much perfectionism and obsession with technology for technology's sake, products not good enough in terms of customer orientation and *usability*
  - inadequate venture capital landscape
  - lack of technology acceptance in the market
  - insufficient networking of SMEs with the research community and global players
  - German engineers are not good enough at thinking in an interdisciplinary manner.

VIII. Social challenges (1)

Question: *In addition to the technological and economic challenges, the issues of social acceptance and an appropriately trained workforce will also be fundamental to* *the success of future Cyber-Physical Systems. The development of user-friendly human-machine interfaces and an interdisciplinary approach to education policy are regarded as key enablers in this regard. Which skills would you consider to be essential for your employees if they are to help shape the future of CPS?*

Answers:

- interdisciplinary approach to training and the ability "to adopt a broader perspective"
- broad-based knowledge of basic principles, general education
- ability to work as part of a team
- ability to see things from the user's perspective

IX. Social challenges (2)

Question: What concrete measures are you taking in your business to encourage your employees to acquire these skills?

Answers:

- In addition to the usual training, seminars and CPD programmes, several respondents also said that they were cooperating with external organisations and encouraging their employees to work in interdisciplinary and intercultural teams.
- Efforts are also being made to adopt an integrated approach that links up the individual stages of the innovation cycle.

X. Social challenges (3)

Question: *What, if anything, needs to change in Germany's training system so that your employees can acquire these skills?*

Answers:

- interdisciplinary, broad-based training programmes should teach people to think in a networked manner (one respondent called for: "... more cc rather than just rpm").
- more focus on the MINT (mathematics, IT, natural sciences and technology) subjects and an increase in the proportion of women studying them
- a more practical focus in higher education

XI. Social challenges (4)

Question: *How or in which direction do you think that the methods of interaction between humans and computers need to change in order to achieve public acceptance of future Cyber-Physical Systems?*

Answers:

- the majority of respondents called for improvements to the systems' intuitiveness, *transparency, safety, security* and *usability*. They felt that they should ideally be developed in a *user-centred* manner by interdisciplinary teams of developers
- respondents complained about the lack of standards in the field of *human-machine interaction*
- this lack of standards also leads to problems with *interoperability*
- people should always have the choice to opt in or out of using *multimodal* systems
- the most important point expressed by the respondents was that "people shouldn't be aware that they are interacting with a machine."

XII. Research support (1)

Question: *The German government is seeking to use its High-Tech Strategy to further strengthen Germany's leadership in the field of technology and drive the transfer of research findings into commercial applications. A targeted funding policy forms an important part of this approach by providing the basis for future innovations. Has your SME ever been involved in a government-funded research project?*

Answers:

- yes: 24.6 percent
- no: 38.9 percent

XIII. Research support (2)

Question: *Which targeted government measures would you like to see to help German SMEs prepare for Cyber-Physical Systems?*

Answers:

- although some respondents were either sceptical about or completely opposed to government subsidies, several others called for
- support for partnerships, particularly between SMEs and higher education institutions,
- implementation-oriented funding schemes that support successfully implemented initiatives and don't just spread the funding around indiscriminately.

XIV. Research support (3)

Question: *In your opinion, how should support measures be targeted to provide SMEs like yours with the best possible support throughout the innovation cycle (from the original idea right through to the final product)?*

Answers:

- There was a clear desire for easier access to the knowledge of higher education institutions and more opportunities to cooperate with them and with partners from industry.
- This mainly affects the area of research and development.
- Other demands included cutting red tape and assistance with legal matters.

GLOSSARY

AAL; see ***Ambient Assisted Living***.

Actuator: a software, electronic and/or mechanical component that takes electronic signals such as commands from a control computer and converts them into mechanical movements or other physical parameters such as pressure and temperature in order to carry out control operations in a control system.

Adaptability: a system's ability to adapt its behaviour to a given situation. The prerequisite for adaptability include ***situation*** and ***context awareness***.

Ad-hoc communication: communication that is not based on a fixed infrastructure but is instead independently organised by the individual communication partners at run-time.

Ad-hoc sensor network: a system comprising ***sensor nodes*** that self-organise at run-time without a fixed infrastructure, in order to monitor their environment via ***sensors*** and communicate the captured data, which in some cases may also be pre-processed.

Agent; see ***software agent.***

Ambient Assisted Living (systems that assist older people to live healthy and independent lives): technology-based approaches, products and services geared towards providing unobtrusive, situation-based support (i.e. support that does not stigmatise the users) to assist people with specific needs in their everyday lives.

Anthropometry: the science of measuring the human body and finding applications for these measurements. Its principal uses are in ergonomics, where it facilitates workplace design, vehicles, tools, furniture and occupational health and safety.

App; see ***application***.

Application: software that provides additional functionality that can be easily integrated (e.g. downloaded) by users into their systems (e.g. ***mobile devices***).

Application platform: a technical and organisational operating and development platform on which different ***services***, technologies and processes work together under a particular architecture to enable an application or ***domain-specific*** group of applications. The principles of modularity and ***reusability*** are applied to the design of application platforms in order to enable tailoring and variant management. An application platform usually involves several actors forming part of an economic ***ecosystem*** who cooperate with each other based on their own strategic considerations. Examples of application platforms include ***smart health systems*** or integrated regional transport services.

Architecture framework: a terminological and methodological structure that provides a standard basis for describing and specifying system architectures. The purpose of architecture frameworks is to create a common structure and language for describing architectures and to provide a methodology for describing concrete architectures.

Artificial Intelligence (AI): a branch of information science concerned with the automation of intelligent behaviour. AI technology enables Cyber-Physical Systems to respond intelligently to their environment, pursue goals on behalf of their users and cooperate with other systems in order to do so. Examples from the scenarios include automated planning of the production of a new kitchen and the rerouting of a journey.

Authentication: the act of establishing ***authenticity***.

Authenticity: the genuineness of an object or subject. This can be verified using its unique identity and characteristic features.

Autonomous driving: the ability of a vehicle to use active networking to drive to a pre-established destination without the driver's active assistance and usually also without direct external steering commands. Within predefined parameters, the vehicle is able to make its own decisions on which route to use and which speed to drive at and is also capable of responding to unforeseen events in a targeted and ***dependable*** manner; see also ***semi-autonomous driving***.

Autonomy: a system's ability to take decisions and behave independently.

Availability: a property of processes and data according to which they should be available for their intended use whenever required. Authorised users should not be prevented from accessing the relevant information and systems.

Back-end infrastructure: servers and the associated software that process large volumes of data, including data from mobile sources, and make the processed information available, e.g. by sending it to (potentially mobile) storage media (data sinks). The back-end infrastructure is a subsystem of the CPS infrastructure and can be implemented in the ***cloud***.

Bayesian network: a probability modelling-based method for dealing with uncertain knowledge; Bayesian networks are used to describe as compactly as possible the common probability distribution of all involved variables by using known conditional independencies. The process is used e.g. in the field of medical diagnosis and for calculating and predicting the movements of objects in the field of robotics. A ***Bayesian network*** is a directed acyclic graph where the nodes represent random variables and the edges represent conditional dependencies between the variables. Each node in the network constitutes a conditional probability distribution for the random variable that it represents, based e.g. on historical ***primary data***.

Best practice: a proven, optimal or exemplary method or approach.

Billing: refers to the invoicing process in service contracts, particularly in telecommunications and similar markets. Billing incorporates all the steps from receipt of the usage data to drawing up of the invoice.

Blackboard: a centralised communication mechanism used by several ***software agents*** to post partial results when working iteratively to solve a problem.

Brain-computer interaction: the direct flow of information between a human brain and a technological system via a brain-computer interface which is often made up of specialised ***sensors and actuators.*** These interfaces are often used to restore or enhance motor and cognitive skills, e.g. to restore a person's hearing or control prosthetic limbs.

Broker: an agent such as an energy trader on the energy market.

Broker system: a trading system on the market.

Bus: a system for transmitting data between different technical components using a shared transmission medium.

Business model: a business model is a simplified representation of a company and an abstraction of how it does business and creates value. It provides a compact description of a company's organisational structure, value chain and products. The development of a business model forms part of a company's business strategy.

Business to Business: commercial relationships between at least two businesses, as opposed to ***Business to Consumer.***

Business to Consumer: the relationships between businesses and the end customer, as opposed to ***Business to***

Business. Business to Consumer also includes the online sale of goods and services to end consumers.

Business Web: a network of businesses that produce value-added parts of services independently of each other but which are mutually complementary. The commercial success of each of these businesses is tied to the others, since the integrated solution provided to the customer comprises a system product produced by the ***entire value network***. It is this system product that competes with other products on the market.

Car sharing: the organised, collective and flexible use of one or more cars. Rather than owning their own cars, users hire cars for a limited period of time from a car sharing provider. They are normally billed based on how long they used the vehicle for and the number of miles driven.

Cloud: abstracted, ***virtualised*** IT resources such as data storage, processing power, applications or services, that are managed by service providers and delivered via a network, usually the Internet.

Cloud Computing: the use of IT resources from the ***cloud***.

Cluster: a group of values or data objects with similar properties.

Cluster analysis: a process for calculating what to include in a ***cluster***. Examples include K-Means and hierarchical clustering.

Co-design: integrated hardware and software design.

Communication infrastructure: this includes both communication networks and ***services*** such as the postal service, radio, TV, telephony and e-mail, and the technology needed to implement these networks, such as broadcasting technology, mobile communications technology, undersea cables, the Internet and communications satellites. It is possible for one communication infrastructure to be built on top of another one – for example, Voice over IP (VoIP) enables Internet Protocol computer networks to be used for making telephone calls. A communication protocol defines the rules governing the connections and data exchange between two parties and may also include processes for ***authentication*** and for detecting and correcting errors.

Community: a group of individuals with common interests, goals, activities, etc.

Compliance: the features of systems, ***services*** or processes that ensure observance of legal and regulatory requirements.

Compute node: a computer that forms part of a network, has its own unique address, and can send, receive and relay information. Some compute nodes are allocated specific tasks.

Confidentiality: the requirement that only authorised persons should have access to processes and data. Confidential information should not be viewed or communicated by unauthorised persons.

Context awareness: a system's ability to register, identify and process information about its context – i.e. the physical context, context of use and the context of a given situation in terms of time and its historical or strategic context; see also ***situation recognition, situation awareness.***

Co-simulation: a method of simulating technological systems where the individual components of an overall system are simulated simultaneously using separate specialised simulators for each component's specific features that exchange all the relevant information with each other.

CPS, Cyber-Physical Systems: this term refers to ***embedded systems***, logistics, coordination and management processes and online ***services*** that use ***sensors*** to directly capture physical data and ***actuators*** to influence physical processes. They are connected to each other via digital networks, ***use data and services from around the world*** and are equipped with ***multimodal human-machine interfaces***. Cyber-Physical Systems are open ***socio-technical systems*** that enable a whole host of novel functions, services and features which go far beyond the capabilities of current embedded systems exhibiting controlled behaviour.

CPS platform (CPS communication platform, CPS middleware): a platform that incorporates the hardware, software and communication systems with basic, standardised CPS brokering, interoperability and ***Quality of Service*** (QoS) services for the implementation and management of Cyber-Physical Systems and their applications. Since they provide the basic functionality for the implementation, dependable operation and evolution of Cyber-Physical Systems, CPS platform services form an integral part of domain-specific CPS ***application platforms***. They guarantee overall cross-domain functionality and quality at the technical system level, for instance by providing QoS-based communication, security services or ***self-diagnosis, self-healing and reconfiguration services***.

CSV: (car sharing vehicle): a vehicle belonging to the fleet of a ***car sharing service provider***.

Customer value: the actual benefits, and thus also the value, that a business or a business' products and services deliver to customers. The term is usually used to distinguish between the actual value and the promised value (***value proposition).***

Data mining: processes geared towards identifying specific patterns in large data sets. Data mining draws on techniques from the fields of ***artificial intelligence***, ***pattern recognition*** and statistical learning, supported by data warehouses.

Data protection: the protection of the individual against infringement of their individual rights in relation to ***personal data***.

Data security: security of data: the basis of ***data protection***.

Deductive mechanisms: rules for inferring additional information from information specified in formal logic.

Dempster-Shafer theory: a mathematical framework for calculating uncertainty; a generalisation of approaches such as ***Bayesian networks***.

Dependability: a combination of traditional safety and security features ***such as functional safety, reliability, availability, confidentiality, integrity and maintainability.***

Domain: subject area, area of knowledge, field of application.

Domain engineering: the development, maintenance and management of the formation and evolution of ***domains***, i.e. areas of knowledge that use common concepts for describing phenomena, requirements, problems, capabilities and solutions that are of interest to a particular ***stakeholder*** group. Domain engineering is studied, researched and used in many different fields such as software product line engineering (SPLE), ***domain-specific language*** engineering (DSLE) and conceptual modelling & knowledge engineering (CMKE).

Domain model: the conceptual ***model*** of a ***domain***, also often referred to as a "problem domain", that describes the domain's concepts, features, roles, relationships and limitations, i.e. the factors that determine the model's ***integrity*** and define the domain's boundaries. Suitable modelling tools include ***ontologies***, system modelling languages such as ***UML*** and ***domain-specific languages***. A domain model can be used to validate the understanding of a domain and verify that it does not contain any inconsistencies; it can also serve as a tool to facilitate communication between different stakeholders and project partners.

Domain-specific language (DSL): a formal language for describing a ***domain*** or problem area. DSLs are designed to enable a high degree of problem specificity to be attained and to ensure that the language is capable of representing all the problems in its particular domain. The opposite of a domain-specific language is a universal programming language such as C or Java, or a universal modelling language such as ***UML***.

Ecosystem: in economics, an ecosystem is a system comprising market players who have a commercial relationship with each other and exchange goods, information, ***services*** and money. The term ecosystem is wider and more general than the term ***value creation system***. Education providers, research organisations, political entities and associations all form part of economic ecosystems, whereas ***value creation systems*** are exclusively made up of companies.

E-Health; see ***smart health system.***

Embedded system: hardware and software components that are integrated into a larger product in order to provide product-specific functional features.

Energy efficiency: a system's ability to use as little energy as possible in the performance of its functions.

Energy gateway: a customer communication and ***service*** platform that enables communication with external services and helps provide ***security for prosumers***.

Engineering: an interdisciplinary systematic approach to design, develop and implement complex technical systems accordingly to the requirements.

Experience Lab: an experimental research approach where teams comprising members from different disciplines, including psychologists, sociologists and designers, observe people and the way they behave and interact when using innovative technologies in order to gain valuable insights for the technology's future development. Experience Labs are one of the key approaches used in user-centred systems engineering and design; see also ***Living Lab***.

External technology: the sociology of technology distinguishes between everyday, workplace and external technologies. External technology, also referred to as "technology as a neighbour", includes things such as chemical plants, waste incineration plants, power plants or genetic engineering laboratories. Decisions concerning external technologies are the outcome of interactions between business, policymakers and the public.

Fail-operational: a property of systems which means that they are able to continue to operate when their control systems fail. This property is necessary if an application is in an unsafe condition immediately after the failure of a component. Examples include lifts, the gas thermostats in domestic ovens and passively safe nuclear reactors. Systems in fail-operational mode are not necessarily also ***fail-safe at the same time.***

Fail-safe: fail-safe systems continue to be safe even when they are no longer able to operate. Medical systems often fall into this category. For example, if an infusion pump stops pumping, it need not pose a threat to the patient's life as long as the pump informs the nurse that it is no longer working and as long as it is designed to remain safe for long enough to enable a human being to respond to the situation. Similarly, when fail-safe mode is activated, it is safe for an industrial or domestic combustion controller to stop working, i.e. to shut down combustion, if it detects a fault. Railway signalling technology is also developed to be fail-safe.

Fairness: a concept used in data processing and operating systems, whereby the available processing time is shared out among the different processes. In computer networks, the term "fairness" refers to the fact that all the participants in the network are equally entitled to the same access to the available resources.

False positive: the incorrect assignment of a positive outcome to an object or subject in the results of an analysis.

Fault tolerance: a system's ability to maintain its functionality when faults occur.

Functional architecture (functional view): a description of a system's functionality, how the system is broken down into different functions and the usage view of the interactions between these functions.

Functional safety: the absence of unacceptable risks resulting from hazards caused by faults in a system.

Governance: the system for controlling and regulating a political, social or organisational entity.

HSM: (Hardware Security Module): a cryptographic coprocessor that provides secure memory, e.g. for cryptographic keys, and a secure execution environment for cryptographic operations.

Human-machine interaction: a branch of information science concerned with the user-friendly design of interactive systems and their ***human-machine interfaces***. In addition to the field of information science, it also draws on knowledge from the fields of psychology, occupational science, cognitive science, ergonomics, sociology and design. Some of the key sub-disciplines in human-machine interaction include ***usability engineering***, interaction design, information design and context analysis. The latter is particularly important in Cyber-Physical Systems, in order to ensure that the interaction is optimally tailored to the current user in every situation.

Human-machine interface: the interface between human users and computerised systems; see also ***human-machine interaction.***

Human factor: a collective term for the psychological, cognitive and social factors that influence ***socio-technical*** and ***human-machine systems.***

Human model: a formal ***model*** that represents an aspect of human behaviour and allows it to be analysed. This enables human behaviour to be diagnosed, simulated and predicted. The aspects of human behaviour represented by these models are focused on specific applications – for example they may be restricted to how human beings interact with a new assistance system on board a car – and parameterizable, for instance with regard to the age of the person being modelled, whether their behaviour matches that of a defensive or aggressive driver, or their reaction times.

Human-system cooperation: cooperation between human users and computerised systems, based on ***human-machine interaction***.

Human-technology cooperation; see ***human-system cooperation***.

ICT: information and communication technology.

Industrial engineering: a combination of disciplines involved in the design, enhancement and installation of integrated systems incorporating human beings, technological components, materials, information, equipment and energy. It draws on specialist know-how and skills from the realms of mathematics, physics and the social sciences, together with the principles and methods of technical analysis and design, in order to specify, predict and evaluate the results delivered by integrated systems.

Information table: a table whose surface comprises a (usually touch-sensitive) screen for displaying information.

Integrity: a condition referring to the intactness, transparency and completeness of the data from different processes; integrity requires accurate information and a correctly functioning system.

Intention recognition: a system's ability to recognise the intentions of a human being. Intention recognition and intention modelling incorporate findings from psychology and cognitive science.

Internet of Energy: comprehensive digital networking and optimisation of energy supply systems through the use of the latest ***ICT***. For example, private customers' energy consumption is fed back via the Internet in order to effect changes in consumer behaviour. To this end, ***smart meters*** are installed in consumers' homes so that they can monitor their electricity usage. In addition, Germany's E-Energy project is geared towards striking a balance between volatile electricity generation that fluctuates e.g. in accordance with weather conditions and fluctuating electricity demand, so that wind- and solar-powered electricity production can be more effectively integrated into the overall energy supply system.

Internet of Services: a part of the Internet that represents services and functionalities as granular, web-based software components. These are made available on the Internet by different providers for on-demand use. Internet service technologies enable the individual software components or services to be integrated with each other. Businesses can orchestrate the individual software components in order to create complex but flexible solutions (***service-oriented architecture***). ***Cloud***-based development platforms make it extremely easy for different market players to develop and supply online services. Furthermore, service platforms are created where customers can find a full range of needs- and process-oriented services instead of having to search for, compare and combine several different individual services themselves. As a result, the Internet becomes a service tool kit for ***ICT*** applications, infrastructure and services.

Internet of Things: where uniquely identifiable physical objects (things) are linked to a virtual representation on the Internet or a similar structure. Automatic identification via ***RFID*** is often regarded as the key enabler of the Internet of Things. Other technologies such as sensors and actuators provide ***enhanced functionality by enabling detection of the environment and performance of actions.***

Interoperability: the ability of separate, heterogeneous systems to cooperate as seamlessly as possible so that they can exchange information efficiently and effectively, work together and provide users with ***services***, without there being a need for any special arrangements between the relevant systems; see also technical interoperability, ***semantic interoperability and user-visible interoperability.***

Intervenability: a privacy protection goal intended to ensure that the processes in digital systems enable the relevant actors to exercise the rights to which they are entitled. Intervenability means that rather than being powerless to influence a system, the actors should have the ability to intervene on their own initiative as and when they deem it necessary to do so.

I/O: the communication of systems with users or other systems by reading and writing data.

Kalman filter: a statistical algorithm that takes a series of measurements observed over time which contain uncertainties or noise and produces aggregated "clean" values.

Know-how: knowledge acquired by people or businesses through learning, experience or research, that they can use in order to achieve a specific technical or commercial outcome.

Living Lab: a research methodology that adopts a ***user-centred open innovation approach*** to developing products and services. Operators, developers, users and researchers engage in parallel R&D processes. The Living Lab approach tends to be used in a single laboratory, city, cluster or region – it is less common for Living Labs to be spread across several different locations; see also ***Experience Lab.*** Living Labs are usually funded through Public-Private Partnerships.

Logical architecture view: a description of how a system is broken down into logical units (subsystems, components), as well as the associated interfaces and signal flows between the units and the environment.

Logical component architecture; see ***logical architecture view***.

Machine learning: a general term for any technology that enables computers to turn experience into knowledge. Systems learn from examples and at the end of the learning phase they are able to make generalisations, i.e. identify patterns in the learned data. This then allows the system to evaluate data that it has never seen before. Machine learning draws on ***pattern recognition*** and ***data mining*** techniques.

Maintainability: the ability of a system to be modified or upgraded. The aim is to isolate and eliminate problems and faults and to equip the system to meet new requirements so that it can operate in a changed environment.

Manufacturing Execution System (MES): the process-oriented level of a multiple-level production management system.

Micro grid: self-contained regional energy systems and grids that incorporate local energy producers and consumers and in some instances also storage facilities.

Middleware: software that acts as a link between hardware and software applications. Middleware provides generic functions to the application. Applications often need the functions provided by the middleware in order to communicate.

Mobile device: a device that can access communication and information ***services*** irrespective of its location, e.g. a smartphone or tablet.

Mobile Internet: access to the World Wide Web and other online ***services*** via ***mobile devices***.

Modality: a means of registering sensory information ***via an input channel*** and of outputting signals and information. Similarly to human beings, devices such as computers can use sensors – which in this instance act as an input device – to receive input from human beings via a touch-sensitive screen, keyboard or microphone, for example. In ***human-machine interactions***, the information flows in both directions, meaning that the device also outputs signals and information.

Mode confusion: an inaccurate understanding of the mode, operation or abilities of a system that can lead the user to operate it incorrectly.

Model: a simplified, goal-oriented representation of the function of the subject of a study or behaviour of a system which is used to enable or facilitate the study or investigation in question. Models are key software development artefacts; they represent systems at different abstraction levels (analysis, design, implementation), system components (user interface, data base, business logic, system administration), dimensions ***(safety and security,*** performance, robustness), and tasks (testing, deployment), usually by employing modelling concepts.

Model-based requirements engineering: an approach to ***requirements engineering*** where formal and informal ***models*** are used to help establish, analyse and produce structured specifications for the requirements relating to a system, its deployment and the associated business and development information. Depending on how complete and formal they are, the models enable ***requirements and system specifications*** to be tested for completeness, consistency and accuracy; see also ***refinement, verification***.

Model-driven engineering (MDE): the description of software systems using, as far as possible, fully or partly formal ***models***, so that as many system artefacts as possible can be derived generatively from the models. Examples include the Object Management Group's (OMG) "Model-driven Architecture" and Microsoft's "Software Factory" initiatives, model interpreters such as "Executable ***UML***" and, more generally, modelling approaches that use ***domain-specific languages and*** generative programming.

Model transformation: automatic generation of a target ***model*** (expressed in a modelling language) from a source model (expressed in the same or a different modelling language), according to a transformation definition, i.e. a set of transformation rules. A transformation rule is a description of how one or more constructs in the source language can be transformed into one or more constructs in the target language. Model transformation is a ***model-driven engineering*** method geared towards ensuring the compatibility and consistency of families of models; see also ***refinement***.

Multi-agent system: a system comprising several distributed ***agents*** that cooperate and communicate with each other in order to accomplish a goal.

Multi-criteria situation assessment: assessment of a situation in ***real time*** using multiple criteria, based on the analysis and interpretation of the available information; see also ***situation awareness***.

Multimodal: using several modalities.

Multiple-classifier system: a system with multiple classifiers. A classifier is a computer program capable of assigning a measurement to a particular category (for example, is the lung pictured in an X-ray diseased or healthy?). In a multiple-classifier system, several classifiers work in parallel and their responses are combined to produce a more accurate and ***robust*** result. The individual classifiers use different recognition algorithms or obtain data from different ***sensors***, for example they may use speech and video to recognise emotions.

Network model: a formal, schematic representation of a network. A network's underlying structure can usually be modelled mathematically as a graph.

On-demand: adjective applied to services, goods, etc., indicating that requirements can be met whenever the user or customer wishes. ***On-demand*** systems and processes are often tied to real-time requirements.

Ontology: in information science, an ontology is a formal, structured representation of a set of concepts, their properties and the relationships between them. Upper ontologies represent basic, generally applicable knowledge, whereas domain ontologies represent the knowledge pertaining to a particular ***domain***. Ontologies are used to convert knowledge into a formal, digitised format so that it can be shared between application software and ***services***. Unlike taxonomies, which only provide a hierarchical breakdown, ontologies represent information networks with logical relationships. Ontologies may contain inference and ***integrity*** rules, i.e. rules that enable conclusions to be inferred and their validity to be guaranteed. Ontologies form part of the ***artificial intelligence*** field of knowledge representation; see also ***Ontology Web Language***.

Ontology Web Language (OWL): a language designed for authoring ***ontologies***. OWL was developed to be compatible with the World Wide Web in general and the ***Semantic Web*** in particular.

Open source: the human-readable program code (source code) of open-source software can be viewed by any member of the general public and used, modified or disseminated under an open-source licence.

Partially- and semi-supervised learning: a branch of ***machine learning*** focused on learning from large data sets where only a small percentage of the training data is labelled. "Supervised learning" refers to cases where all the data is labelled, while "unsupervised learning" refers to cases where none of it is labelled.

Participatory design: a process for designing innovative systems where (putative, potential or future) users and other stakeholder groups cooperate with designers, researchers and developers.

Pattern recognition: the ability of algorithms and systems to recognise regularities, repetitions, similarities and patterns in incoming data.

Personal data: data that are associated or could be indirectly associated with a particular natural person. This includes data that could be used to infer an association with a particular person, even if the information tying the data to this person is not in the public domain. The only thing that matters is whether or not it is reasonably possible to associate the data with a particular person.

Photovoltaics (PV): a technology for converting solar energy into electrical energy.

Physical awareness: a system's ability to use the data from ***sensor fusion*** or other information sources in order to draw additional conclusions about the physical environment; see also ***situation recognition, situation awareness.***

Plan recognition: a technology that takes ***intention recognition*** one step further by enabling the recognition of actors' plans, i.e. sequences of actions including actions that will not be performed in the immediate future. This technology is also used to design and develop ergonomic ***human-machine interfaces*** and human-robot interfaces.

Plug and Play: a technology that enables devices or subsystems to be integrated into other devices or systems so that they are able to start working immediately, without requiring users to intervene by installing drivers or setting parameters, for example.

Plug-in hybrid vehicle (also plug-in hybrid electric vehicle, PHEV): a motor vehicle with a hybrid propulsion system featuring a battery that can be charged externally by connecting it to the electricity grid as well as via the vehicle's internal combustion engine. Plug-in hybrid vehicles usually have bigger batteries than standard hybrid vehicles. They thus fall somewhere between a standard hybrid and an electric vehicle.

Policy: framework regulation, rule, guideline.

Premium lane: a lane on a road where, upon payment of a charge, vehicles are given priority over the vehicles in other lanes.

Primary data (raw data): the data captured directly from a source; referred to as ***measurements*** in the case of physical data; cf. ***secondary data***.

Privacy: the non-public domain where individuals are entitled to exercise their right to behave as they wish without external interference. The right to privacy is a human right that is enshrined by all modern democracies.

Privacy by Default: a principle used in the development of technological systems and organisational processes, whereby products and services default to ***data protection*** friendly settings at the time of their delivery or when used for the first time. Only data that are absolutely essential to their use are recorded, processed and communicated. Any use of the data for other purposes requires an explicit decision on behalf of the user, for example the decision to change their ***data protection*** settings.

Privacy by Design: a principle used in the development of technological systems, organisational processes and ***business models***, whereby ***data protection*** law requirements are, as far as possible, implemented right from the outset, i.e. during the conception and design stages.

Privacy policy: a description of the rules governing the handling of ***personal data***. Policies may simply reflect the terms and conditions stipulated by a service or service provider, but may also reflect users' wishes. Although they can exist as a written document, some may only be available in a machine-readable format.

Privacy protection goal: a basic requirement of IT systems. The extent to which it is implemented depends on the required level of protection that has been determined for the system in question. The established privacy protection goals that exist today are ***transparency, intervenability and unlinkability.***

Private cloud: a version of ***cloud computing*** that provides access to IT infrastructure within a clearly demarcated environment. Although this will usually be a particular company, it may also be an association, family or even an individual. Private cloud ***services*** are usually provided over private networks or networks with special security arrangements and not over the open Internet.

Prosumer: individuals who are both producers and consumers of goods at the same time; this includes intangible goods such as energy.

Protection goal: a requirement with regard to the way that data are processed and services are performed that, among other things, is designed to ensure a system's security. The technical and organisational measures for delivering protection goals need to be state-of-the-art, meaning that they must be updated regularly. Examples of protection goals include ***confidentiality, integrity and availability.***

Public cloud: a cloud with publicly ***available*** infrastructure systems and ***services*** that are usually accessed over the Internet.

Quality in Use: the quality of a system or ***service*** during use – based on its intended purpose and context of use – as seen from the perspective of its human users or any other systems that may be using it.

Quality of Experience: a subjective measure of the experience that the user has when using a particular service; see also ***Experience Lab.***

Quality of Service: a measure of the quality of ***services*** and their cooperation and composition options based on the extent to which they meet agreed quality guarantees and standards.

Real-time capability: a system's ability to provide guaranteed response and reaction times.

Redlining: a term coined in the 1960s to denote the practice employed by US banks of refusing to grant loans to people who lived in certain districts that were delineated with a red line on the banks' in-house maps. The term would subsequently come to refer to discrimination against members of particular social groups, irrespective of geography.

Refinement: a process used in information science that takes an abstract description such as a formal specification or ***model*** and transforms it into a more concrete description or executable program. The concrete description produced by the refinement process preserves the specific features of the abstract description. A formally verifiable accuracy relationship exists between the two descriptions. This is also known as the "refinement relationship".

Reinforcement learning: an umbrella term embracing ***machine learning methods*** where ***software agents*** evaluate how successful the outcomes of different actions are so that they can subsequently be optimised. In order to do this, the ***agents*** have to observe the effects and benefits resulting from their actions and explore the world in which they are able to operate.

Reliability: a capability or behavioural characteristic of a system that describes how ***reliably*** it performs its intended functionality over a given period of time.

Requirements engineering: a process for determining the requirements placed on a system or service. It is aimed at providing a full description of a particular problem requiring a solution, establishing the business, user, customer and process requirements, setting goals and priorities, resolving conflicts and inconsistencies, specifying the requirements pertaining to systems, components, architecture and communication in the requirements and system specifications and monitoring the extent to which these are implemented in the system's design; see also ***requirements traceability.***

Requirements specification: establishes a system's requirements from the viewpoint of the user and other ***stakeholders***, provides a communication basis for acquiring and aligning application knowledge and solutions among the different actors involved in the system's development and use, and specifies instructions and rules for finding, designing and aligning appropriate solutions and architectures at all levels of the system's design and specification.

Requirements traceability: a branch of ***requirements engineering*** and system management; the ability to monitor and ensure compliance with the requirements specified in the design, implementation and subsequent development (evolution) of systems, sub-systems and components. In the area of ***requirements and system specifications***, requirements traceability enables the analysis, testing and qualitative evaluation of specifications, alternative architecture and solution concepts and change requirements; see also ***refinement, validation, verification.***

Return on Investment (RoI): a ***model*** for measuring the return on a business activity or project based on the ratio between profit and capital invested.

Re-usability: a property of software components that allows them to be used successfully for purposes other than those for which they were originally designed, thus preventing the same thing from unnecessarily being developed more than once.

RFID (Radio Frequency Identification): the identification of objects using readers that can interpret the electromagnetic waves transmitted by RFID transponders – also known as RFID tags – that are attached to the objects.

Risk engineering: a structured process for identifying shortcomings in systems' design and implementation which could result in a variety of different risks, such as malfunctions or a lack of acceptance.

Robustness: a system's ability to respond to errors and unforeseen circumstances without malfunctioning.

RoI; see ***Return on Investment.***

Safety (German: Betriebssicherheit): ***safety*** in terms of the operation of a system. The term primarily refers to ***functional safety***, but also includes ***reliability*** – the absence of unacceptable risks while the system is operating. Safety is ensured both by functional safety measures and e.g. by limiting the user's options (indirect safety) and user training. The German version of this study distinguishes between Betriebssicherheit (safety), IT-Sicherheit (security) and Sicherheit (an umbrella term that includes both safety and security)

Safety and security (German: Sicherheit): a system's ability to promise problem-free and safe operation. At a technical level, safety and security depend on how they have been defined or the degree of danger and insecurity that is deemed acceptable for the use of the technical function in question. The IEC 61508 standard defines safety as "freedom from unacceptable risk" and uses the term ***functional safety*** to refer to what it describes as part of the overall safety of a technological system. The German term "Sicherheit" (as used in the original version of this study) includes both (operational) safety (German: Betriebssicherheit) and ***(IT) security*** (German: IT-Sicherheit).

Safety-critical: describes systems where there is the potential for risk or danger during their operation or use; see also ***safety and security***.

Scoping: the definition and specification of a particular task or study's topics and scope.

Secondary data: data derived from ***primary data***.

Security (German: IT-Sicherheit): the protection of data and services in digital systems against abuse such as unauthorised access, tampering or destruction; see also data protection, privacy protection. The German version of this study distinguishes between Betriebssicherheit (safety), IT-Sicherheit (security) and Sicherheit (an umbrella term that includes both safety and security)

Security by Design: a system's built-in security. Security mechanisms are built into the overall architecture and system design from the earliest stages of its development. Since it is assumed that attacks are inevitable, the relevant protective mechanisms and countermeasures are built into the system to deal with security vulnerabilities or invalid user input. ***Security during Operation mechanisms are also already specified at this stage***.

Security during Operation: a system's ability to ensure the necessary level of ***security***, detect and analyse vulnerabilities and implement countermeasures, all during operation. This may, for example, involve replacing algorithms that have been found to be insecure without interrupting the system's operation.

Self-analysis; see ***self-diagnosis***.

Self-awareness: a term taken from the field of psychology that is also used in robotics. It is not only human beings who are capable of self-awareness – technological systems can also possess this ability; see also self-diagnosis. The opposite of ***self-awareness*** is external awareness, i.e. the perception of a person or robot by others.

Self-diagnosis (self awareness): the ability of a system or process to analyse its own status.

Self-evaluation; see ***self-diagnosis***.

Self-healing: the ability of a system or process to fix problems by itself.

Self-organisation: the transition from a disordered to an ordered state. During this process, certain structures (communication and functional structures) are formed spontaneously. The patterns of order that arise in self-organisation cannot be attributed to external organising agents.

Self-X: the ability of technological systems to react autonomously to problems during operation. This makes them more ***robust*** and reliable; see also ***self-diagnosis*** and ***self-healing***.

Semantic interoperability: the ability of computer systems to exchange information with each other and interpret the exchanged data in a consistent manner.

Semantic Web: a concept for developing the Internet, and in particular the World Wide Web, so that it can achieve a semantic understanding of the information contained in texts. In order to do this, every single word must be assigned a unique meaning; this is achieved via semantic networks; see ***ontology***.

Semi-autonomous driving: a driving mode where, although the vehicle is still driven by a human being, Cyber-Physical Systems provide support for a number of routine activities such as keeping the vehicle within its lane. If necessary, the system will also intervene actively to control the vehicle. The decision as to whether or not to make such an intervention is based on fixed rules that in some cases are supplemented by learned rules; see also ***autonomous driving***.

Sensor: a technological component that can record physical or chemical properties either qualitatively or quantitatively in the shape of a measurement.

Sensor fusion: a targeted combination of the measurements made by several different ***sensors***. Data are combined from several sensors that may be different or identical to each other and which will often be interdependent. This allows more highly aggregated values to be calculated which are correspondingly more reliable.

Sensor network: a system made up of ***sensor nodes*** that cooperate either as part of an infrastructure-based or self-organising ***ad-hoc sensor network*** in order to monitor their environment via ***sensors*** and transmit the data that they record. In some cases they may also pre-process the recorded data.

Sensor node: tiny (the size of a mote of dust) to relatively large (the size of a shoebox) autonomous ***sensors*** that communicate using radio waves.

Service: an abstract term referring to the functions and facilities provided by systems and human beings.

Service-oriented architecture (SOA): a software architecture concept where functions realised in software are designed as discrete ***reusable*** components (specialised ***services***). These can be combined in order to perform more complex tasks.

Shared control: when control of a highly automated global system such as an aircraft is shared between human beings and the system itself.

Situation awareness: a capability that is required to enable systems to mirror human beings' temporal and spatial awareness of their environment and the elements that it contains and imitate their ability to infer the significance of this information and draw conclusions from it that can be used for taking decisions; see also ***context awareness***. More advanced systems are able to use situation awareness to ascertain the current state of their human users and to direct their attention in such a way as to prevent ***mode confusion***.

Situation recognition: a system's ability to recognise or determine the status and significance of an application situation. In order to do this, it must be capable of ***physical awareness***. Situation recognition has various applications in the field of robotics; see also ***context awareness***.

Smart buildings: a technology used in buildings where monitoring, management, control and optimisation systems automatically perform operational functions in a coordinated manner in accordance with preset parameters or simplify these operations and the monitoring of the building. The goal is to reduce energy consumption and staffing requirements.

Smart device: a device – i.e. a physical object with an embedded processor, memory and network connection – that performs smart assistance functions in a manner not unlike a ***mobile device***. It will usually possess a user interface and the ability to interact with its physical environment.

Smart embedded system: an embedded system that possesses ***adaptive*** or autonomous capabilities.

Smart factory: a partnership of several companies that uses ***ICT*** to coordinate manufacturing facilities and customer interfaces in order to enable a more flexible response to customer requests.

Smart grid: a smart, ***ICT***-based network comprising producers of electrical energy that fluctuates in terms of its availability, storage facilities for this energy, grid management components and energy consumers, geared towards ensuring that supply always meets demand.

Smart health system: an ***ICT***-based partnership of systems, components, human experts and the ***services*** they provide in order to enable integrated patient healthcare and 24/7 monitoring of patients' health, catering for both their individual healthcare needs and for situations such as medical emergencies that require an urgent response.

Smart homes: a branch of ***smart buildings*** technology focused on private dwellings and the specific requirements of their occupants. Its aim is to provide enhanced comfort and safety and to enable monitoring of more than one residence.

Smart infrastructure: technological infrastructure components and systems such as transport, energy and ***communication infrastructures***, that are increasingly equipped with smart networked sensors and actuators and embedded control components for monitoring and analysing complex processes. For instance, smart infrastructures can be used to identify inefficiencies, optimise operating procedures or collect tolls.

Smart logistics: ICT-driven measures designed to optimise or reduce freight transport and warehousing requirements through the use of smart measurement and control technologies.

Smart meter: an electronic domestic meter. Rather than simply recording overall consumption, smart meters can record and store the times when energy is consumed and communicate this information to customers or third parties.

Smart mobility: the deployment of state-of-the-art ***ICT*** to optimise the use of existing transport services and enable ***energy-efficient***, low-emission, ***safe***, comfortable and affordable mobility.

Smart sensor: a sensor that combines the function of taking measurements with local processing of the captured data (***data fusion***) and signal processing, all in a single unit.

Smart sensor node: a node in a wireless ***sensor network*** that is capable of capturing and processing sensory information and transmitting it to other nodes connected to the same network.

Smart tag: an ultra-thin passive ***RFID*** transponder which, together with its antenna, can be housed on a strip of film which can then be treated as if it were a piece of paper. They can also be integrated into smart cards.

Socio-technical system: functional cooperation between human beings or groups of human beings and technology.

Software agent: a computer program capable of some form or other of autonomous behaviour. ***Agents*** have applications in fields such as e-commerce, information searches, simulations, performance of routine tasks and ***autonomous*** systems. They usually focus on one particular area, e.g. smart behaviour in a networked manufacturing environment or ***IT security.***

Stakeholder: natural or legal persons or interest groups affected by the potential development, deployment and operation of a system and who therefore have an interest in the process and outcome of the system's development and deployment.

System of Systems: a structured system comprising several subsystems that are usually organised hierarchically and all operate independently.

Tailoring: adaptation to a particular requirement or application.

Technical architecture: a representation of the concrete technical dimensions, implementation and structure of a system.

Technical interoperability: the ability of computer systems to exchange data with each other. Technically interoperable systems share a clearly defined communication protocol and an established ***communication infrastructure***.

Telematics: the combined use of telecommunications and IT technology.

Traceability: in systems management, the ability to trace the requirements of a system function back to all of the elements that execute this function, either on their own or together, and thus meet the requirements in question; see also ***requirements traceability***.

Transparency: a privacy protection goal that stipulates that the way a system works and the effects it has should at all times be sufficiently easy to understand for its operators and the people affected by it. It should be reasonably simple to understand, check and evaluate how ***personal data*** have been captured, processed and used.

Trusted Computing Module (TCM): a type of ***HSM*** whose functions are stipulated in a specification formulated by the Trusted Computing Group (TCG).

Trusted Platform Module (TPM); s***ee Trusted Computing Module.***

Ubiquitous computing: this term refers to the presence of computerised information processing in every area of our lives. It transcends the ***human-machine interaction paradigm associated with PCs and laptops***, describing instead a scenario where information processing capabilities form an integral part of everyday objects and activities. The Internet of Things supports people in their everyday lives, in some cases without them even being aware of it.

UML (Unified Modeling Language): a graphic modelling language for specifying, constructing and documenting software and other systems. It is a standardised language (ISO/IEC 19501) that was developed by the Object Management Group (OMG). UML defines the majority of terms that are important for modelling and establishes possible relationships between these terms. In addition, graphical notations for the terms are defined. This also occurs for models of static structures and of dynamic processes that can be formulated with these terms. Additionally, it describes a format for enabling models and diagrams to be exchanged between different tools.

Unlinkability: a privacy protection goal that states that it should not be possible to link data and entities with each other to infer private information. Unlinkability combines the requirement to maximise data avoidance with the obligation to keep data and processes from different contexts separate from each other, in order to prevent the risks arising from the accumulation of large amounts of data that could be exploited by third parties.

Updatability: a system's ability to implement data and code updates in order to ensure that it has the latest technical and content versions.

Usability: a capability and quality feature of a system or service that is essential as far as its human users are concerned. The ISO 9241-110 standard stipulates the following system usability sub-criteria: suitability for the task, controllability, self-descriptiveness, conformity with user expectations, suitability for individualisation, e***rror tolerance and suitability for learning***; see also ***Quality in Use.***

Usability engineering: a process that occurs in parallel to traditional planning and development work to ensure that a system, and in particular its ***human-machine interface***, will be usable. This is an iterative process, since experts test the extent to which the system meets the defined goals and requirements of its future users at every stage of the project; see also ***User-Centred Design.***

User-Centred Design (UCD): a development method based on the ISO 13407 standard that pays special attention to user needs and involvement. The development methodology involves a series of iterative cycles comprising four stages: (1) analysis and requirements gathering, (2) implementation, (3) testing and (4) evaluation. The outcomes of the evaluation stage in the previous cycle are fed into the requirements stage of the next cycle; see also ***participatory design***.

User-centred engineering: technological systems engineering that involves and pays special attention to the user; see also ***user-centred design.***

User model; see ***human model***.

User-visible interoperability: the ability of interoperable systems to make their interactions and communication and cooperation behaviour options visible and understandable to the user, thereby affording users the opportunity to intervene interactively in the behaviour of the usage process.

Validation: testing of the explicit or implicit requirements of a system during or at the end of the development process, in order to check whether the system meets the expectations and needs of its ***stakeholders***.

Value chain: a value creation model comprising a sequential, step-by-step series of activities and/or processes ranging from development through to production, marketing and service delivery.

Value creation system: a partnership between companies that have a commercial relationship with each other and exchange goods, information, ***services*** and money; see also ***ecosystem***.

Value network: a decentralised, polycentric network characterised by complex reciprocal relationships between autonomous, legally independent actors. It involves a pool of potential value creation partners who engage in common processes as and when necessary. The establishment of value networks is geared towards the creation of sustainable economic value-added. Specific instances of value networks are referred to as ***business webs.***

Value proposition: a statement of the value that a business can offer customers or other partners. A company's value proposition forms the basis of its ***business model***.

Verification: the act of checking that the results of a development phase match the relevant specifications, i.e. the requirements that were initially specified.

Viewpoint: a structuring concept used in systems ***engineering*** for specifying requirements and system knowledge from the point of view of the relevant ***stakeholders*** and their goals in terms of the system's application and development.

Virtual engineering: the science of engineering virtual products. It involves the computer-based, integrated ***modelling*** of a product's entire life cycle in a virtual reality technology-enabled projection and working environment. Virtual engineering enables developers, suppliers, manufacturers and customers to address all aspects of future products, from their specification through to their ***maintenance*** and recycling entirely in the virtual domain, allowing them to carry out realistic assessments of their features and functions.

Virtualisation: production of a virtual (as opposed to physical) version that is not tied to concrete resources such as a hardware platform, operating system, storage medium or network resources.

Virtual Power Plant (VPP): a collection of several small, decentralised electricity producers who are connected up to each other in order to provide a source of energy that can be accessed centrally by consumers.

Web 2.0: an umbrella term that covers a range of interactive and collaborative aspects of the Internet. In Web 2.0, users are providers of content as well as consumers, flexibly combining content from a variety of sources.

"X"-Awareness: the ability to accurately register and interpret situations and contexts, including the condition, intentions, goals and purpose of the actions of any humans or systems involved; see also ***situation recognition and context awareness.***

XML (Extensible Markup Language): a language for representing hierarchically structured data as written text. XML's uses include the platform- and implementation-independent exchange of data between computer systems, especially over the Internet.

REFERENCES

[3sa11].
3sat: *Späher, Scanner und Sensoren – Kann Technik uns vor Terrorismus schützen?* (Report on the German television programme "hitec"), first broadcast 10 October 2011. [In German]

[ABB+09].
Achatz, R./Beetz, K./Broy, M./Dämbkes, H./Damm, W./Grimm, K./Liggesmeyer, P.: *Nationale Roadmap Embedded Systems*, Frankfurt/Main: ZVEI (Zentralverband Elektrotechnik und Elektronikindustrie e. V. – *German Electrical and Electronic Manufacturers' Association)*, Kompetenzzentrum Embedded Software & Systems 2009. [In German]

[ABB+11].
Appelrath, H.J./Behrendt, F./Bognar, K./Mattern, F./Mayer, C./Weiss, M.: *Forschungsfragen im „Internet der Energie"* (acatech MATERIALIEN, No. 1), Munich 2011. [In German]

[ABD+10].
Traub, K. (Ed.)/Armenio, F./Barthel, H./Dietrich, P./Duker, J./Floerkemeier, C./Garrett, J./Harrison, M./Hogan, B./Mitsugi, J./Preishuber-Puegl, J./Ryaboy, O./Sarma, S./Suen, K./Williams, J.: *The EPC global Architecture Framework.* (Technical Report, GS1, Final Version 1.4), 2010. URL: http://www.gs1.org/gsmp/kc/epcglobal/architecture/architecture_1_4-framework-20101215.pdf [Accessed: 12.01.2012.].

[ABI09].
Allied Business Intelligence (ABI): *Global Navigation Satellite Positioning Solutions: Markets and Applications for GPS, Galileo, GLONASS, and Beidou* (Research report), 2009. URL: http://www.abiresearch.com/research/1003224-Global+Navigation+Satellite+Positioning+Solutions [Accessed: 12.01.2012].

[aca11a].
acatech (Ed.): *Acceptance of Technology and Infrastructure: Observations on a contemporary social phenomenon* (acatech TAKES A POSITION, No. 9), Heidelberg inter alia: Springer Verlag 2011.

[aca11b].
acatech (Ed.): *Smart Cities: German High Technology for the Cities of the Future. Tasks and Opportunities* (acatech TAKES A POSITION, No. 10), Heidelberg inter alia: Springer Verlag 2011.

[aca11c].
acatech (Ed.): *Umfrage Cyber-Physical Systems: Mittelstand wünscht sich Interdisziplinarität und Benutzerfreundlichkeit* (acatech press information and news), 31 August 2011. URL: http://www.acatech.de/de/aktuelles-presse/presseinformationen-news/news-detail/artikel/umfrage-cyber-physical-systems-mittelstand-wuenschtsich-interdisziplinaritaet-und-benutzerfreundli.html [Accessed: 12.01.2012. In German].

[aca11d].
acatech (Ed.): *Cyber-Physical Systems. Driving force for innovation in mobility, health, energy and production* (acatech POSITION PAPER), Heidelberg inter alia: Springer Verlag 2011.

[ACW11].
Agrawala, A./Corner, M./Wetherall D. (Ed.): *9th International Conference on Mobile Systems, Applications, and Services* (MobiSys'11, Proceedings, ACM), 2011.

[ADI].
ADIWA: ADIWA - *Alliance Digital Product Flow*. URL: http://www.adiwa.net/ [Accessed: 12.01.2012].

[AG-09].
Innovationsrat Baden-Württemberg: AG-I: *Baden-Württemberg 2025: Wirtschaft, Gesellschaft und industrieller Wandel- Endbericht*, 2009. URL: http://www.baden-wuerttemberg.de/fm7/1899/Endbericht%20der%20Arbeitsgruppe%20I%20Baden-W%FCrttemberg%202025.pdf [Accessed: 12.01.2012. In German].

[AIM].
Deutsches Zentrum für Luft- und Raumfahrt (German Aerospace Center – DLR): *Anwendungsplattform Intelligente Mobilität* (AIM). URL: http://www.dlr.de/fs/desktopdefault.aspx/tabid-6422/10597_read-23684/ [Accessed: 12.01.2012. In German].

[AKT].
AKTIV: *aktiv – Adaptive and Cooperative Technologies for Intelligent Traffic*. URL: http://aktiv-online.org/ [Accessed: 12.01.2012.].

[AKvdM01].
Arnold, E./Kuhlman, S./van der Meulen, B.: *A singular council: Evaluation of the Research Council of Norway* (Report to the Royal Norwegian Ministry of the Church, Education and Research Affairs), technopolis 2001. URL: http://www.technopolisgroup.com/resources/downloads/reports/243_RCN_Synthesis.pdf [Accessed: 12.01.2012].

[ALE].
ALETHEIA: *Semantic Federation of Comprehensive Product Information.* URL: http://www.aletheia-projekt.de/ [Accessed: 12.01.2012.].

[ALRL04].
Avizienis, A./Laprie, J.C./Randell, B./Landwehr, C.: *Basic Concepts and Taxonomy of Dependable and Secure Computing.* In: IEEE Transactions on Dependable and Secure Computing, 1(1) 2004, pp. 383–396.

[aML11].
Automation ML: *Erfolge innerhalb der IEC-Standardisierung* (openautomation.de), February 2011. URL: http://www.openautomation.de/2069-0-automation-ml-erfolge-innerhalb-der-iec-standardisierung.html [Accessed: 12.01.2012. In German].

[And12].
Andrews, L.: *Wie die Datensammel-Industrie hinter Facebook und Co. funktioniert,* Süddeutsche Zeitung, 10 February 2012. URL: http://www.sueddeutsche.de/digital/auswertung-persoenlicher-informationen-wie-die-datensammel-industrie-hinter-facebook-und-co-funktioniert-1.1280573 [Accessed: 10.02.2012. In German].

[AR11].
Abele, E./Reinhart, G.: *Zukunft der Produktion: Herausforderungen, Forschungsfelder, Chancen,* Carl Hanser Verlag 2011. [In German]

[Arb11].
BICC *(Bavarian Information and Communication Technology Cluster): Arbeitskreis Multicore: Multicore-Technologien für Embedded Systems: zur Bedeutung, Bestandsaufnahme und Potentialermittlung für den Industrie- und Forschungsstandort Deutschland.* URL: http://bicc-net.de/aktivitaeten/aktivitaet/arbeitskreis-multicore/ [Accessed: 12.01.2012. In German].

[ART11].
ARTEMIS Industry Association: *Strategic Research Agenda 2011: Technical report, 2011.* URL: http://www.artemis-ia.eu/publication/download/publication/541 [Accessed: 12.01.2012].

[ASP08].
ASP-DAC (Ed.): *13th Asia South Pacific Design Automation Conference* (ASP-DAC'08, Proceedings), Los Alamitos: IEEE Computer Society Press 2008.

[AUT].
AUTOSAR: *AUTOSAR – Automotive open system architecture.* URL: http://www.autosar.org/ [Accessed: 12.01.2012].

[AVA].
AVACS: *AVACS – Automatic Verification and Analysis of Complex Systems.* URL: http://www.avacs.org [Accessed: 12.01.2012].

[AWA].
A.W.A.R.E.: *Awareness – Self Awareness in Autonomic Systems.* URL: http://www.awareproject.eu/ [Accessed: 12.01.2012].

[BAA].
BAALL: *Bremen Ambient Assisted Living Lab.* URL: http://baall.informatik.uni-bremen.de/de/index.php/Hauptseite, [Accessed: 12.01.2012.].

[Bal00].
Balzert, H.: *Lehrbuch der Software-Technik – Software-Entwicklung,* Spektrum Akademischer Verlag 1997–2000, vol. 1. [In German]

[Bal11].
Balser, M.: *Wenn ein Stadtwerk systemrelevant wird,* Süddeutsche Zeitung, 19 October 2011. [In German]

[BAS11].
Bundesanstalt für Straßenwesen (Federal Highway Research Institute): Volkswirtschaftliche Kosten durch Straßenverkehrsunfälle 2009. BASt aktuell, p. 2, 2011. URL: http://www.bast.de/cln_031/nn_957200/DE/Publikationen/BASt-aktuell/Downloads/BASt-aktuell-2011-02,templateId=raw,property=publicationFile.pdf/BASt-aktuell-2011-02.pdf. [Accessed: 12.01.2012. In German].

[Bau09].
Baum, G.: *Rettet die Grundrechte! Bürgerfreiheit contra Sicherheitswahn – Eine Streitschrift,* Kiepenheuer & Witsch Verlag 2009. [In German]

[BBB04].
Brown, T./Beyeler, W./Barton, D.: *Assessing infrastructure interdependencies: The challenge of risk analysis for complex adaptive systems.* In: International Journal of Critical Infrastructures, 1(1) 2004, pp. 108–117.

[BBB+11].
Beinhauer, W./Bierkandt, J./Block, M./Büllesfeld, E./Link, J.: *Trendstudie – Auszug der Studie: Trends und Entwicklungen im Umfeld von Automaten* (Technical report, Fraunhofer-Institut für Arbeitswirtschaft und Organisation [Fraunhofer IAO]), 2011. URL: http://www.erlebnis-automat.de/cms/images/documents/auszug_trendstudie.pdf. [Accessed: 12.01.2012. In German].

[BBD+11].
Bernard, M./Buckl, C./Doricht, V./Fehling, M./Fiege, L./Grolman, H. von/Ivandic, N./Janello, C./Klein, C./Kuhn, K./Patzlaff, C./Riedl, B./Schätz, B./Stanek, C.: *Mehr Software (im) Wagen: Informations- und Kommunikationstechnik (IKT) als Motor der Elektromobilität der Zukunft* (Abschlussbericht des vom Bundesministerium für Wirtschaft und Technologie geförderten Verbundvorhabens "eCar-IKT-Systemarchitektur für Elektromobilität"). In: Antriebstechnik, Fahrzeugtechnik, Speichertechnik (2. Automobiltechnisches Kolloquium, Proceedings). VDI Verlag 2011. [In German. English Summary: The Software Car. Information and Communication Technology (ICT) as an Engine for the Electromobility of the Future. Summary of the results of the "eCar ICT System Architecture for Electromobility" research project sponsored by the Federal Ministry of Economics and Technology. URL: http://download.fortiss.org/public/ikt2030/ikt2030en.pdf]

[BBE07].
Bischoff, J./Barthel, H./Eisele, M.: *Automobilbau mit Zukunft: Baustein und Konzepte für Produktion und Logistik.* LOG X 2007. [In German]

[BBLR11].
Beinhauer, W./Bierkandt, J./Link, J./Ringbauer, B.: *Qualitätsmerkmale – Auszug des Leitfadens „Entwicklung und Bewertung von Automaten"* (Technical report, Fraunhofer-Institut für Arbeitswirtschaft und Organisation [Fraunhofer IAO]), 2011. URL: http://www.erlebnis-automat.de/cms/phocadownload/2011_07_21_auszug_leitfaden%20qualittsmerkmale.pdf. [Accessed: 12.01.2012. In German].

[BCHM06].
Bernon, C./Chevrier, V./Hilaire, V./Marrow, P.: *Applications of self-organising multi-agent systems: An initial framework for comparison.* In: Informatica (Slovenia), 30(1) 2006, pp. 73–82.

[BDF+06].
Bizer, J./Dingel, K./Fabian, B./Günther, O./Hansen, M./Klafft, M./Moller, J./Spiekermann, S.: *Technikfolgenabschätzung: Ubiquitäres Computing und Informationelle Selbstbestimmung* (study commissioned by the Federal Ministry of Education and Research, Technical report, Independent Centre for Data Protection Schleswig-Holstein (ULD) and the Institute of Information Systems at the Humboldt-Universität zu Berlin (HU)), 2006. URL: http://www.taucis.hu-berlin.de/_download/TAUCIS_Studie.pdf. [Accessed: 12.01.2012]. [In German]

[Ber07].
Berger, T.: *Softwareproduktlinien-Entwicklung – Domain Engineering: Konzepte, Probleme und Lösungsansätze* (Undergraduate dissertation), Leipzig University 2007. [In German]

[Ber09].
Roland Berger Strategy Consultants (Ed.): *Global Automation Industry Study 2015* (Technical report), 2009.

[Ber10a].
Roland Berger Strategy Consultants (Ed.): *Automation: Time to find your true north – Global view on the automation industry* (Technical report), 2010. URL: http://www.rolandberger.com/media/pdf/Roland_Berger_taStudy_Automation_20100706.pdf [Accessed: 12.01.2012].

[Ber10b].
Roland Berger Strategy Consultants (Ed.): *IT-Anbieter einer neuen Generation: Der Europäische Weg* (Technical report), 2010. URL: http://www.rolandberger.com/media/pdf/Roland_Berger_IT_Anbieter_einer_neuen_Generation_20101025.pdf [Accessed: 12.01.2012]. [In German]

[Ber11a].
Roland Berger Strategy Consultants (Ed.): *Production Systems 2020: Global challenges and winning strategies for the mechanical engineering industry* (Technical report), 2011. URL: http://www.rolandberger.com/media/pdf/Roland_Berger_Production_Systems_2020_20110419.pdf [Accessed: 12.01.2012].

[Ber11b].
Bergert, D.: *TomTom verkauft Geschwindigkeits-Daten an die Polizei,* PC-Welt 28 April 2011. URL: http://www.pcwelt.de/news/Navigation-TomTom-verkauft-Geschwindigkeits-Daten-an-die-Polizei-1544623.html [Accessed: 12.01.2012. In German].

[Ber11c].
Bernau, V.: *Foulspiel*. Süddeutsche Zeitung, 30 September 2011. [In German]

[BFG+ 08].
Broy, M./Feilkas, M/Grünbauer, J./Gruler, A./Harhurin, A./ Hartmann, J./Penzenstadler, B./Schätz, B./Wild, D.: *Umfassendes Architekturmodell für das Engineering eingebetteter Software-intensiver Systeme* (Technical report,TUM-I0816, Technische Universität München), 2008. URL: http://www4.in.tum.de/publ/papers/TUM-I0816.pdf [Accessed: 12.01.2012. In German].

[BGK+ 07].
Broy, M./Geisberger, E./Kazmeier, J./Rudorfer, A./Beetz, K.: „Ein Requirements-Engineering-Referenzmodell". In: *Informatik Spektrum* 30(3) 2007, pp. 127–142. [In German]

[BHGZ09].
Brand, L./Hülser, T/Grimm, V./Zweck, A.: I*nternet der Dinge: Übersichtsstudie* (Technical report, Zukünftige Technologien Consulting der VDI Technologiezentrum GmbH), 2009. URL: http://www.vdi.de/fileadmin/vdi_de/redakteur/dps_bilder/TZ/2009/Band%2080_IdD_komplett.pdf [Accessed: 12.01.2012. In German].

[Bie11].
Bielicki, J.: *Städte unter Strom.* Süddeutsche Zeitung, 7 October 2011. [In German]

[Bis07].
Bishop, C.: *Pattern Recognition and Machine Learning* (Corr. 2nd printing.), Springer: New York 2007.

[BIT08].
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Federal Association for Information Technology, Telecommunications and New Media) (Ed.): *Studie zur Bedeutung des Sektors Embedded-Systeme in Deutschland* (Technical report, BITKOM), 2008. URL: http://www.bitkom.org/files/documents/Studie_BITKOM_Embedded-Systeme_11_11_2008.pdf [Accessed: 12.01.2012. In German].

[BIT11a].
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Federal Association for Information Technology, Telecommunications and New Media) (Ed.): *Smart Cities – Grüne ITK zur Zukunftssicherung moderner Städte* (Technical report, BITKOM), 2011. URL: http://www.bitkom.org/files/documents/Smart_Cities_Studie_Mai_2011.pdf [Accessed: 12.01.2012. In German].

[BIT11b].
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Federal Association for Information Technology, Telecommunications and New Media) (Ed.): *Studie Automobil – ITK im Auto und Elektromobilität* (Technical report, BITKOM), 2011. URL: http://www.bitkom.org/files/documents/BITKOM_Studie_Automobil_-_ITK_im_Auto_und_Elektromobilitaet.pdf [Accessed: 12.01.2012. In German].

[BJ94].
Braun, I./Joerges, B.(Ed.): *Technik ohne Grenzen,* Frankfurt/Main: Suhrkamp 1994. [In German]

[BK02].
Buld, S./Krüger, H.: *Wirkungen von Assistenz und Automation auf Fahrerzustand und Fahrsicherheit* (Technical report, Interdisziplinäres Zentrum für Verkehrswissenschaften (IZVW) Universität Würzburg [IZVW – Centre for Traffic Sciences at the University of Würzburg), Projekt Effort-Management und Performance-Handling in sicherheitsrelevanten Situationen (EMPHASIS) (Project: Effort Management and Performance Handling in Safety-Relevant Situations [EMPHASIS]), final report, 2002. URL: http://lexikon.kfz.tuberlin.de/apsn/uploads/media/Emphasis_Abschlussbericht.pdf [Accessed: 12.01.2012. In German].

[BKS11].
Brecher, C./Kozielski, S./Schapp, L.: *Integrative Produktionstechnik für Hochlohnländer.* In: Gausemeier, J/Wiendahl H. [GW11]., pp. 47–70. URL: http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/acatech_diskutiert/acatech_diskutiert_Wertschoepfung_WEB.pdf [Accessed: 12.01.2012. In German].

[BMB06].
Bundesministerium für Bildung und Forschung (Federal Ministry of Education and Research) (Ed.): *Die Hightech-Strategie für Deutschland* (Technical report, Public Relations Division, BMBF), Bonn/Berlin 2006. URL: http://www.bmbf.de/pub/bmbf_hts_kurz.pdf [Accessed: 12.01.2012. In German].

[BMB07].
Bundesministerium für Bildung und Forschung (Federal Ministry of Education and Research) (Ed.): *Deutschlands Spitzencluster: Mehr Innovation, Mehr Wachstum, Mehr Beschäftigung*, 2007. URL: http://www.bmbf.de/de/10726.php [Accessed: 12.01.2012. In German.].

[BMB10].
Bundesministerium für Bildung und Forschung (Federal Ministry of Education and Research) (Ed.): *Ideas. Innovation. Growth. High-tech Strategy 2020 for Germany* (Technical report, Innovation Policy Framework Division, BMBF), Bonn/Berlin 2010. URL: http://www.bmbf.de/pub/hts_2020.pdf [Accessed: 12.01.2012].

[BMW08].
Bundesministerium für Wirtschaft und Technologie (Federal Ministry of Economics and Technology) (Ed.): *Zukunft & Zukunftsfähigkeit der deutschen Informations- und Kommunikationstechnologie – Abschlussbericht der ersten Projektphase* (Technical report), 2008. URL: http://www.bmwi.de/Dateien/BMWi/PDF/IT-Gipfel/studie-zukunftsfaehigkeit-der-deutschen-ikt,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf [Accessed: 12.01.2012. In German].

[BMW09a].
Bundesministerium für Wirtschaft und Technologie (Federal Ministry of Economics and Technology) (Ed.): *Internet of Things. A guide to technical, organisational, legal and safety-related aspects of implementing new RFID-supported processes in industry and government* (Documentation 581), 2009. URL: http://www.bmwi.de/English/Redaktion/Pdf/documentation-581-internet-of-things,property=pdf,bereich=bmwi2012,sprache=en,rwb=true.pdf [Accessed: 12.01.2012].

[BMW09b].
Bundesministerium für Wirtschaft und Technologie (Federal Ministry of Economics and Technology) (Ed.): *Zukunft und Zukunftsfähigkeit der Informations- und Kommunikationstechnologien und Medien – Internationale Delphi-Studie 2030* (Executive Summary and Methodology, Technical report), 2009. URL: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Studien/zukunft-und-zukunftsfaehigkeit-ikt-medien-executive-summary-methodik,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf [Accessed: 12.01.2012. In German].

[BMW10a].
Bundesministerium für Wirtschaft und Technologie (Federal Ministry of Economics and Technology) (Ed.): *Das Internet der Dienste. Innovationspolitik, Informationsgesellschaft, Telekommunikation,* 2010. URL: http://bmwi.de/BMWi/Redaktion/PDF/Publikationen/Technologie-und-Innovation/internet-derdienste,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf [Accessed: 12.01.2012. In German].

[BMW10b].
Bundesministerium für Wirtschaft und Technologie (Federal Ministry of Economics and Technology) (Ed.): *The THESEUS Research Program. New Technologies for the Internet of Services,* 2010. URL: http://theseus-programm.de/ [Accessed: 12.01.2012].

[BMW10c].
Bundesministerium für Wirtschaft und Technologie (Federal Ministry of Economics and Technology) (Ed.): *Offen für die Zukunft – Offen in die Zukunft* (Technical report), 2010. URL: http://www.muenchner-kreis.de/typo3conf/ext/naw_securedl/secure.php?u=0&file=fileadmin/dokumente/Download/Offen_fuer_die_Zukunft_Offen_in_die_Zukunft.pdf&t=1288951855&hash=5276553976a47ee360991db68a9094de [Accessed: 12.01.2012. In German].

[BMW10d].
Bundesministerium für Wirtschaft und Technologie (Federal Ministry of Economics and Technology) (Ed.): *Sichere Internet-Dienste — Sicheres Cloud Computing für Mittelstand und öffentlichen Sektor* (Trusted Cloud), 2010. URL: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Technologie-und-Innovation/sichere-internet-dienste-sicheres-cloud-computing,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf [Accessed: 12.01.2012. In German].

[BMW11a].
Bundesministerium für Wirtschaft und Technologie (Federal Ministry of Economics and Technology) (Ed.): *Autonomik – Autonome und simulationsbasierte Systeme für den Mittelstand,* 2011. URL: http://www.autonomik.de [Accessed: 12.01.2012. In German].

[BMW11b].
Bundesministerium für Wirtschaft und Technologie (Federal Ministry of Economics and Technology) (Ed.): *Central Innovation Program for SMEs* (Funding modules ZIM-KOOP, ZIM-SOLO, ZIM-NEMO), 2011. URL: http://www.zim-bmwi.de/ [Accessed: 12.01.2012].

[BN97].
Brandenburger, A./Nalebuff, B. (Ed.): *Co-opetition: 1. A revolutionary mindset that combines competition and cooperation, 2. The Game Theory strategy that's changing the game of business,* Currency Doubleday 1997.

[Bra00].
Brands, S. (Ed.): *Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy,* Cambridge: MIT Press 2000.

[Bro10].
Broy, M. (Ed.): Cyber-Physical Systems: *Innovation durch softwareintensive eingebettete Systeme* (acatech DISKUTIERT), Heidelberg inter alia: Springer Verlag 2010. URL: http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/acatech_diskutiert/acatech_diskutiert_CPS_einseitig_ol.pdf [Accessed: 12.01.2012. In German].

[BRO11].
Bundesregierung (German government) : *Höhere Energieeffizienz bei Gebäuden* (Nachrichten, Regierung online), 2011. URL: http://www.bundesregierung.de/nn_1272/Content/DE/Artikel/2011/04/2011-04-07-energieeffizienz.html [Accessed: 12.01.2012. In German].

[BS00].
Bussmann, S./Schild, K.: *Self-Organizing Manufacturing Control: An Industrial Application of Agent Technology,* (Fourth International Conference on MultiAgent Systems, Proceedings), 2000, pp. 87–94.

[BSI10].
Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security) (Ed.): *Leitfaden Informationssicherheit – IT-Grundschutz kompakt.* (Technical report BSI-Bro10/311, Referat 114 Sicherheitsmanagement und IT Grundschutz), 2010.URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf? blob=publicationFile. [Accessed: 12.01.2012. In German].

[Bul02].
Bullinger, H.: *Virtual Engineering und Rapid Prototyping,* (Entwicklung und Erprobung Innovativer Produkte – Rapid Prototyping, Forschungsforum 2002). University of Stuttgart 2002. [In German]

[BVe83].
Bundesverfassungsgericht (Federal Constitutional Court): Volkszählungsurteil (Census Verdict), BVerfGE 65, 1, 1983. URL: http://www.bfdi.bund.de/DE/GesetzeUndRechtsprechung/Rechtsprechung/BDSGDatenschutzAllgemein/Artikel/151283_VolkszaehlungsUrteil.html;jsessionid=238890526283F442781F95A15E49CBA8.1_cid134?nn=1236576 [Accessed: 12.01.2012. In German].

[BW08].
Bräuninger, M./Wohlers, E.: *Medizintechnik in Deutschland: Zukunftsbranche Medizintechnik – Auch im Norden ein Wachstumsmotor,* (Technical report, Hamburgisches Welt-WirtschaftsInstitut [HWWI], Study commissioned by HSH Nordbank AG), 2008. URL: http://www.hwwi.org/fileadmin/hwwi/Publikationen/Partnerpublikationen/HSH/Medizintechnik-Studie.pdf [Accessed: 12.01.2012. In German].

[Cal12].
Calonego, B.: *Der Feind in meiner Steckdose.* Süddeutsche Zeitung, 16 January 2012. [In German]

[Car03].
Carr, N.: *IT doesn't matter.* In: Harvard Business Review, 81(5) 2003, pp. 41–49.

[Car08].
Carr, N.: *The Big Switch: Rewiring the World – from Edison to Google,* W. W. Norton & Company 2008.

[car11].
carIT: *Modernisierungswettlauf: Audi setzt auf Vernetzung.* 2011. URL: http://www.car-it.automotiveit.eu/modernisierungswettlauf-audi-setzt-auf-vernetzung/id-0025678 [Accessed: 12.01.2012. In German].

[Cav09].
Cavoukian, A.: *Privacy by Design* (Technical report, Office of the Information and Privacy Commissioner, Ontario), 2009. URL: http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf [Accessed: 12.01.2012].

[CC08].
Cohen-Cole, E.: *Credit Card Redlining* (Quantitative Analysis Unit (QAU) Working Paper QAU08-1), Federal Reserve Bank of Boston 2008. URL: http://www.bos.frb.org/bankinfo/qau/wp/2008/qau0801.pdf [Accessed: 12.01.2012].

[CES].
CESAR – Cost-efficient methods and processes for safety relevant embedded systems. URL: http://www.cesarproject.eu/

[CES10].
CESAR: *Definition and exemplification of RSL and RMM. Deliverable D SP2 R2.1 M1, Cost-efficient methods and processes for safety relevant embedded systems* 2010. URL: http://www.cesarproject.eu/fileadmin/user_upload/CESAR_D_SP2_R2.1_M1_v1.000.pdf [Accessed: 12.01.2012].

[CEW09].
Constantinescu, C./Eichelberger, H./Westkämper, E.: *Durchgängige und integrierte Fabrik- und Prozessplanung (Grid Engineering for Manufacturing: Continuously and integrated factory and process planning – grid engineering for manufacturing).* In: wt Werkstattstechnik online, 99(3) 2009, pp. 92–98. [In German]

[CGW09].
Cuhls, K./Ganz, W./Warnke, P. (Ed.): *Foresight Process on behalf of the German Federal Ministry of Education and Research. New Future Fields,* Karlsruhe: Fraunhofer Verlag 2009. URL: http://www.bmbf.de/pubRD/Foresight-Process_BMBF_New_future_fields.pdf [Accessed: 12.01.2012].

[Che06].
Chesbrough, H.: *Open Business Models: How to Thrive in the New Innovation Landscape.* Harvard Business Press 2006.

[CHR].
CHROMOSOME Middleware. URL: http://www.fortiss.org/de/forschung/projekte/chromosome-middleware.html [Accessed: 12.01.2012].

[Chr97].
Christensen, C.: *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail,* Harvard Business School Press 1997.

[Chr03].
Christensen, C.: *The Innovator's Dilemma: The Revolutionary Book that Will Change the Way You Do Business,* (Collins Business Essentials), Harper Paperbacks 2003.

[Cir11].
Cirino, Zheng (Ed.): *Eureka Prometheus Project.* Civ, May 2011.

[CIT].
CityMobil – Towards Advanced Road Transport for the Urban Environment. URL: http://www.citymobil-project.eu [Accessed: 12.01.2012].

[CL01].
Camenisch, J./Lysyanskaya, A.: *An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation.* In: Pfitzmann, B. (Ed.): Advances in Cryptology – International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT'01, Proceedings, volume 2045 of Lecture Notes in Computer Science), Springer 2001, pp. 93–118.

[CLV].
Connected Living. URL: http://www.connected-living.org [Accessed: 12.01.2012].

[CMK+11].
Checkoway, S./McCoy, D./Kantor, B./Anderson, D./Shacham, H./Savage, S./Koscher, K./Czeskis, A./Roesner, F./Kohno, T.: *Comprehensive Experimental Analyses of Automotive Attack Surfaces.* In: 20th USENIX Security Symposium (Proceedings), 2011, pp. 77–92. URL: http://www.autosec.org/pubs/cars-usenixsec2011.pdf [Accessed: 22.02.2012].

[CMPB03].
Casassa Mont, M/Pearson, S/Bramhall, P.: *Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services.* In:14th International Workshop on Database and Expert Systems Applications (DEXA'03, Proceedings), pp. 377–382. IEEE Computer Society 2003. Long version. URL: http://www.hpl.hp.com/techreports/2003/HPL-2003-49.pdf [Accessed: 12.01.2012].

[CNI06].
International Workshop on Complex Network and Infrastructure Protection (CNIP'06, Proceedings), 2006.

[CPS08].
Cyber-Physical Systems Summit: *Holistic Approaches to Cyber-Physical Integration* (Report, CPS Week), 2008. URL: http://iccps2012.cse.wustl.edu/_doc/CPS_Summit_Report.pdf [Accessed: 12.01.2012].

[CSH04].
Capurro, R./Scheule, R./Hausmanninger, T. (Ed.): *Vernetzt gespalten: Der Digital Divide in ethischer Perspektive*, Paderborn: Wilhelm Fink Verlag 2004. [In German]

[Cus10].
Cusumano, M.: Staying Power: *Six Enduring Principles for Managing Strategy and Innovation in an Uncertain World,* Oxford: Oxford University Press 2010.

[CvONS+ 09].
Cave, J./Oranje-Nassau, C./Schindler, H./Shehabi, A./Brutscher, P./Robinson, N.: *Trends in connectivity technologies and their socioeconomic impacts – Final report of the study: Policy Options for the Ubiquitous Internet Society* (Technical Report TR-776-EC, RAND Europe), 2009. URL: http://ec.europa.eu/information_society/activities/foi/library/docs/final-report-nosec-clean.pdf [Accessed: 12.01.2012].

[CW03].
Christaller, T./Wehner, J. (Ed.): *Autonome Maschinen*, Wiesbaden: Westdeutscher Verlag 2003. [In German]

[CW07].
Cramer, S./Weyer, J.: *Interaktion, Risiko und Governance in hybriden Systemen.* In: Dolata/Raymund W. [DW07]. pp. 267–286. URL: http://www.techniksoziologie-dortmund.de/Mitarbeiter/Cramer/K%C3%B6lnpdf.pdf [Accessed: 12.01.2012. In German].

[CYB].
Cybercars-2. URL: http://cybercars2.paris-rocquencourt.inria.fr/ [Accessed: 12.01.2012].

[D3C].
Artemis Industry Association, D3COS. URL: http://www.artemis-ia.eu/project/index/view/?project=27 [Accessed: 12.01.2012].

[Dav92].
Davis, A.: *Operational Prototyping: A New Development Approach.* IEEE Software, 9 1992, pp. 70–78.

[Deg02].
Degele, N.: *Einführung in die Techniksoziologie,* Berlin inter alia: UTB/W. Fink 2002. [In German]

[DKE10].
Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (DKE German Commission for Electrical, Electronic and Information Technologies of DIN and VDE): *Medizinische elektrische Geräte – Teil 1-6: Allgemeine Festlegungen für die Sicherheit einschließlich der wesentlichen Leistungsmerkmale – Ergänzungsnorm: Gebrauchstauglichkeit* (Technical report, DIN EN 60601-1-6; VDE 0750-1-6:2010-10), 2010. URL: http://www.dke.din.de/cmd?artid=133687070&contextid=dke&bcrumblevel=1&subcommitteeid=70724983&level=tpl-art-detailansicht&committeeid=54738887&languageid=de [Accessed: 12.01.2012. In German].

[Dmi04].
Dmitriev, S.: Language Oriented Programming: *The Next Programming Paradigm (Jetbrains)*, 2004 URL: http://www.jetbrains.com/mps/docs/Language_Oriented_Programming.pdf [Accessed: 12.01.2012].

[DoD09a].
Department of Defense Chief Information Officer: *Department of Defense Architecture Framework Version 2.0 (DoDAF V2.0) – Volume 1: Introduction, Overview, and Concepts – Manager's Guide* (Technical report), 2009. URL: http://cio-nii.defense.gov/docs/DoDAF%20V2%20-%20Volume%201.pdf [Accessed: 12.01.2012].

[DoD09b].
Department of Defense Chief Information Officer: *Department of Defense Architecture Framework Version 2.0 (DoDAF V2.0) – Volume 2: Architectural Data and Models – Architect's Guide* (Technical report), 2009. URL: http://cio-nii.defense.gov/docs/DoDAF%20V2%20-%20Volume%202.pdf [Accessed: 12.01.2012].

[DoD09c].
Department of Defense Chief Information Officer: *Department of Defense Architecture Framework Version 2.0 (DoDAF V2.0) – Volume 3: DoDAF Meta-model, Physical Exchange Specification – Developer's Guide (*Technical report), 2009. URL: http://cio-nii.defense.gov/docs/DoDAF%20V2%20-%20Volume%203.pdf [Accessed: 12.01.2012].

[Dog01].
Döge, P.: *Männlichkeit, Technik, Politik: Androzentrische Selektivitäten im Prozess der politischen Techniksteuerung. In: Kultur-, Geschichts- und Sozialwissenschaften* (1. Tagung AIM Gender (Arbeitskreises für interdisziplinäre Männerforschung), Tagungsband), 2001. URL: http://www.ruendal.de/aim/pdfs/Doege.pdf [Accessed: 12.01.2012. In German].

[Dor89].
Dörner, D.: *Die Logik des Mißlingens: Strategisches Denken in komplexen Situationen,* Rowohlt Taschenbuch Verlag 1989 [In German. Available in English as *The Logic of Failure: Recognizing and Avoiding Error in Complex Situations,* Basic Books 1997].

[Dra10].
Drath, R. (Ed.): *Datenaustausch in der Anlagenplanung mit AutomationML: Integration von CAEX, PLCopen XML und COLLADA* (VDI-Buch), Heidelberg inter alia: Springer 2010. [In German]

[DW07].
Dolata, U./Werle, R. (Ed.): *Gesellschaft und die Macht der Technik: Sozioökonomischer und institutioneller Wandel durch Technisierung.* In: Schriften aus dem Max-Planck-Institut für Gesellschaftsforschung Köln (Max Planck Institute for the Study of Societies Cologne), No. 58, Frankfurt inter alia, Campus Verlag 2007. [In German]

[EBB].
ebbits – Business-based Internet of Things and Services. URL: http://www.ebbits-project.eu/, [Accessed: 12.01.2012].

[EBJ03].
Endsley, M./Bolte, B./Jones, D.: *Designing for Situation Awareness: An Approach to User-Centered Design*, CRC Press, July 2003.

[EG10].
Erben, M./Günther, W.: *Rechtsexpertise zu selbstorganisierenden adaptiven IT Systemen.* In: Selbstorganisierende adaptive Systeme [IÖ 10]., Appendix III. [In German]

[Eic10].
Eichelberg, M.: *Interoperabilität von AAL-Systemkomponenten Teil 1: Stand der Technik*, VDE-Verlag 2010. [In German]

[Eka94].
Ekardt, H.: Unter-Gestell. *Die bautechnischen Fundamente großer technischer Systeme.* In: Braun, I./Bernward, J. [BJ94]., pp. 166–211. [In German]

[ele11a].
elektroniknet.de: 2017: *Weltweit 13,9 Mio. elektrifizierte Fahrzeuge,* 23 August 2011. URL: http://www.elektroniknet.de/automotive/news/article/81468/ [Accessed: 12.01.2012. In German].

[ele11b].
elektroniknet.de: *Verbrauch neu zugelassener Pkw sinkt um 5 Prozent*, 10 August 2011. URL: http://www.elektroniknet.de/automotive/news/article/81193/ [Accessed: 12.01.2012. In German].

[ELR].
ELROB – The European Robot Trial. URL: http://www.elrob.org/catalogue.html [Accessed: 12.01.2012].

[EPC07].
GS1: *Electronic Product Code (EPC): An Overview* (Technical Report, DTR/MTS-02003-1, ETSI Doc. Number ETR 130), 2007. URL: http://www.gs1.org/docs/epcglobal/ an_overview_of_EPC.pdf [Accessed: 12.01.2012].

[ETS94].
European Telecommunications Standards Institute (ETSI): *Methods for Testing and Specification (MTS); Interoperability and conformance testing: A classification scheme* (Technical Report, DTR/MTS-02003-1, ETSI Doc. Number ETR 130, April 1994). URL: http://www.etsi.org/deliver/etsi_etr/100_199/130/01_60/etr_130e01p.pdf [Accessed: 12.01.2012].

[Eur50].
European Convention on Human Rights: *Article 8 "Right to respect for private and family life"* (last amended by the provisions of Protocol No. 14 of 13 May 2004, effective as of 1 June 2010), 4 November 1950. URL: http://www.echr.coe.int/Documents/Convention_ENG.pdf [Accessed: 12.01.2012].

[Eur95].
European Community: *Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Official Journal of the European Union, (L 281):31–50, 23 November 1995. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= CELEX:31995L0046:en:HTML [Accessed: 12.01.2012].

[Eur02].
European Community: *Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector* (Directive on Privacy and Electronic Communications). Official Journal of the European Union, (L 201):37–47, 31 July 2002. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML [Accessed: 12.01.2012].

[Eur09].
European Community: *Directive 2009/136/EC of the European Parliament and of the Council of 25th November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. Official Journal of the European Union,* (L 337):11–36, 18 December 2009. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF [Accessed: 12.01.2012].

[Eve10].
Evensen, K.: *Architecture and Cross Layer. In 2nd Workshop on Intelligent Transport Systems* (ETSI TC ITS'10, Proceedings), 2010. URL: http://docbox.etsi.org/Workshop/2010/201002_ITSWORKSHOP/3_TCITS_WORKINGGROUPS/EvensenWG2_Architecture.pdf [Accessed: 12.01.2012].

[EXC].
Excellence Initiative for Cutting-Edge Research at Institutions of Higher Education. URL: http://www.bmbf.de/en/1321.php [Accessed: 12.01.2012].

[FAM].
Fahrautomat für autonomes Fahren in der Kfz-Prüftechnik. URL: http://zentrix-t1.te1.hs-heilbronn.de/T1_MST/fue-aktivitaeten/fdgdfgdf [Accessed: 12.01.2012. In German].

[FFM05].
Fischer, K./Florian, M./Malsch, T.(Ed.): Socionics: *Scalability of Complex Social Systems.* In: Computer Science volume 3413, Lecture Notes, Berlin: Springer 2005.

[FGG+ 06].
Feiler, P./Gabriel, R./Goodenough, J./Linger, R./Longstaff, T./Kazman, R./Klein, M./Northrop, L/Schmidt, D./Sullivan, K./Wallnau, K.: *Ultra-Large-Scale Systems: The Software Challenge of the Future* (Technical report, Carnegie Mellon Software Engineering Institute (SEI)), 2006. URL: http://www.sei.cmu.edu/library/assets/ULS_Book20062.pdf [Accessed: 12.01.2012].

[FHDH+ 11].
Fischer-Hübner, S./Duquenoy, P./Hansen, M./Leenes, R./Zhang, G. (Ed.): *Privacy and Identity Management for Life* (6th IFIP/PrimeLife International Summer School 2010, revised selected papers, volume 352 of IFIP Advances in Information and Communication Technology), Berlin: Springer 2011.

[Flo05].
Florkemeier, C.: *EPC-Technologie – vom Auto-ID zu EPCglobal.* In: Fleisch, E./Mattern, F. [FM05]., pp. 87–100. [In German]

[FM05].
Fleisch, E./Mattern, F. (Ed.): *Das Internet der Dinge: Ubiquitous Computing und RFID in der Praxis – Visionen, Technologien, Anwendungen, Handlungsanleitungen,* Berlin: Springer 2005. [In German]

[FN71].
Fikes, R./Nilsson, N.: STRIPS: *A new approach to the application of theorem proving to problem solving.* In: Artificial intelligence 2(3-4)1971, pp. 189–208.

[Fra03a].
Franz, A.: *Management von Business Webs: Das Beispiel von Technologieplattformen für mobile Dienste. Markt- und Unternehmensentwicklung,* Wiesbaden: Deutscher Universitätsverlag 2003. [In German]

[Fra03b].
Franz, G.: Digitales Fernsehen: *Herausforderungen für TV-Forschung und TV- Werbung.* In: Media Perspektiven 2003(10):462–469, 2003. http://www.media-perspektiven.de/uploads/tx_mppublications/10-2003_Franz_neu.pdf [In German]

[Fre07].
Frey, U.: *Der blinde Fleck: Kognitive Fehler in der Wissenschaft und ihre evolutionsbiologischen Grundlagen,* Ontos 2007. [In German]

[FS09].
Frost & Sullivan: *EMEA Automation and Control Solutions Services Market* (Technical Report M370-01), 2009. URL: http://www.frost.com/prod/servlet/report-toc.pag?repid=M370-01-00-00-00 [Accessed: 12.01.2012].

[FSHK09].
Friedrich, J./Sihling, M./Hammerschall, U./Kuhrmann, M.: *Das V- Modell XT – Für Projektleiter und QS-Verantwortliche kompakt und übersichtlich (Informatik im Fokus),* Berlin: Springer 2009. [In German]

[FTS].
FTS-Kompetenzseiten (AGVS competence section). URL: http://www.pslt.uni-hannover.en/fts.html [Accessed: 12.01.2012].

[Fun06].
Funke, J.: *Denken und Problemlösen* (Volume 8: Enzyklopädie der Psychologie, Themenbereich Theorie und Forschung, Serie Kognition), Göttingen: Hogrefe – Verlag für Psychologie 2006. [In German]

[FW11].
Fink, R./Weyer, J.: *Autonome technische Systeme als Herausforderung der soziologischen Handlungstheorie.* In: Zeitschrift für Soziologie 40(2) 2011. [In German]

[GBB+ 06].
Geisberger, E./Broy, M./Berenbach, B./Kazmeier, J./Paulish, D./Rudorfer, A.: *Requirements Engineering Reference Model (REM)* (Technical Report, TUM-I0618), Technische Universität München 2006.

[GHW10].
Heinrichs, G./Loehnert, E./Wittmann, E.: *User RAIM Integrity and Interference Mitigation Test Results with Upgraded German Galileo Test Range GATE.* In: 5th ESA Workshop on Satellite Navigation Technologies (NAVITEC'2010, Proceedings), 2010. URL: http://www.gate-testbed.com/fileadmin/gate/publications/Paper_ESA-NAVITEC-2010_GATE.pdf [Accessed: 24.02.2012].

[Gif07].
Gifford, C. (Ed.): *The Hitchhiker's Guide to Manufacturing Operations Management* (ISA-95 Best Practices Book 1.0), ISA 2007.

[GL12]
Graf, A./Laube, H.: *Android – mehr Masse als klasse.* In: Financial Times Deutschland, 28 February 2012. URL: http://www.ftd.de/it-medien/computer-technik/:apple-rivale-android-mehr-masse-als-klasse/60174849.html [Accessed: 02.03.2012. In German].

[GLB].
G-Lab. URL: http://www.german-lab.de/ [Accessed: 12.01.2012].

[GMA09a].
VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (Association of German Engineers [VDI]/VDE Society of Measurement and Automatic Control) (Ed.): *Automation 2020: Bedeutung und Entwicklung der Automation bis zum Jahr 2020 – Thesen und Handlungsfelder* (Technical report, GMA), 2009. URL: http://www.vdi.de/fileadmin/vdi_de/redakteur_dateien/gma_dateien/AT_2020_INTERNET.pdf [Accessed: 12.01.2012. In German].

[GMA09b].
NAMUR/VDI/VDE- Gesellschaft Mess- und Automatisierungstechnik (NAMUR/Association of German Engineers [VDI]/VDE Society of Measurement and Automatic Control) (Ed.): *Roadmap „Prozess-Sensoren 2015+".*(Technical report, GMA), 2009. URL: http://www.vdi.de/fileadmin/vdi_de/redakteur_dateien/gma_dateien/Prozess-Sensoren_2015+.pdf [Accessed: 12.01.2012. In German].

[GMF09].
Gerbracht, H./Most, D./Fichtner, W.: *Elektromobilität – Auswirkungen auf das Energiesystem.* In: Energiewirtschaftliche Tagesfragen 59(11) 2009, pp. 66–69. [In German]

[GMP+ 06].
Geib, C./Mourão, K./Petrick, R./Pugeault, N./Steedman, M./Krueger, N./Worgötter, F.: *Object Action Complexes as an Interface for Planning and Robot Control* (Humanoids'06 Workshop Towards Cognitive Humanoid Robots, Proceedings), 2006.

[Gra11].
Graf, A.: *Vorsicht, Ihren Daten fehlt die Ausreiseerlaubnis* Financial Times Deutschland, 2 December 2011. URL: http://www.ftd.de/it-medien/it-telekommunikation/:rechtsrisiko-cloud-ihren-daten-fehlt-die-ausreiseerlaubnis/60136904.html [Accessed: 12.01.2012. In German].

[Gro99].
Grove, A.: *Only the Paranoid Survive: How to Exploit the Crisis Points That Challenge Every Company,* Crown Business 1999.

[GS07].
Geisberger, E./Schätz, B.: *Modellbasierte Anforderungsanalyse mit Auto-RAID.* In: Informatik – Forschung und Entwicklung 21(3–4) 2007, pp. 231–242. [In German]

[GS10].
Graumann, S./Speich, A.: *Monitoring-Report Deutschland Digital – Der IKT-Standort im internationalen Vergleich 2010.* (Fifth National IT Summit, Federal Ministry of Economics and Technology), Berlin November 2010. URL: http://www.bmwi.de/BMWi/Redaktion/PDF/I/it-gipfel-monitoring-deutschland-digital-langfassung-2010,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf [Accessed: 12.01.2012. In German].

[GTKM11].
Geisberger, E./Teufl, S./Khalil, M./Mou, D.: *Experience with content-based requirements engineering assessments* (19th IEEE International Requirements Engineering Conference Proceedings), 2011.

[GW11].
Gausemeier, J./Wiendahl, H. (Ed.): *Wertschöpfung und Beschäftigung in Deutschland* (acatech diskutiert), Heidelberg inter alia: Springer 2011. URL: http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/acatech_diskutiert/acatech_diskutiert_Wertschoepfung_WEB.pdf [Accessed: 12.01.2012. In German].

[Han11].
Handelsblatt: *Lebensretter mit Hacker-Schwachstellen,* 9 August 2011. URL: http://www.handelsblatt.com/technologie/forschung-medizin/medizin/lebensretter-mit-hacker-schwachstellen/4480014.html [Accessed: 12.01.2012. In German].

[HAV].
HAVEiT – Highly Automated Vehicles for intelligent Transport. URL: http://www.haveit-eu.org [Accessed: 12.01.2012].

[HBB+ 03].
Hilty, L./Behrendt, S./Binswanger, M./Bruinink, A./ Erdmann, L./Frohlich, J./Kohler, A./Kuster, N./Som, C./ Würtenberger, F.: *Das Vorsorgeprinzip in der Informationsgesellschaft – Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt (*Technical report TA46/2003, TA-SWISS), Zentrum für Technologiefolgen-Abschätzung (Centre for Technology Assessment), Berne 2003. URL: http://www.ta-swiss.ch/?redirect=getfile.php&cmd[getfile].[uid].=542 [Accessed: 12.01.2012. In German].

[HBK11].
Hägele, M./Blümlein, N./Kleine, O.: *Wirtschaftlichkeitsanalysen neuartiger Servicerobotik-Anwendungen und ihre Bedeutung für die Robotik Entwicklung* (Technical report, Fraunhofer Institutes for Manufacturing Engineering and Automation (IPA) and for Systems and Innovation Research (ISI) on behalf of the Federal Ministry for Education and Research, Ref. 01IM09001), 2011. URL: http://www.ipa.fraunhofer.de/fileadmin/www.ipa.fhg.de/Robotersysteme/Studien/Studie_EFFIROB_72dpi_oI.pdf [Accessed: 12.01.2012. In German].

[HEG11].
European Commission: *High-Level Expert Group on Key Enabling Technologies* (Final Report, Technical report), 2011. URL: http://ec.europa.eu/enterprise/sectors/ict/files/kets/hlg_report_final_en.pdf [Accessed: 12.01.2012].

[Hei11].
Heidenreich, M.: *Regionale Netzwerke.* In: Weyer, J. [Wey11b], pp. 167–188. [In German]

[Her11].
Andreas Herkersdorf (Ed.): *Ein Multicore-Ökosystem für Embedded Systems – Positionspapier zur Bedeutung, Bestandsaufnahme und Potentialermittlung der Multicore-Technologie für den Industrie- und Forschungsstandort Deutschland (BICCnet - Bavarian Information and Communication Technology Cluster),* Munich, December 2011. [In German]

[Hil07].
Hilty, L.: *Risiken und Nebenwirkungen der Informatisierung des Alltags.* In: Mattern, F. [Mat07]., pp. 187–205. [In German]

[HMO].
H-Mode – Ein intuitives Kontrollinterface zu einem intelligenten Fahrzeug, II. URL: http://www.lfe.mw.tum.de/de/research/projects/h-mode [Accessed: 12.01.2012. In German].

[HMPR04].
Hevner, A./March, S./Park, J./Ram, S.: *Design Science in Information Systems Research.* In: MIS Quarterly 28(1) 2004, pp. 75–105. URL: http://misq.org/design-science-in-information-systems-research.html?SID=lsp77n0v8pq6njos2df1fqbua5 [Accessed: 12.01.2012].

[Hof11].
Hofmann, N.: *Piratinnen aller Länder vereinigt euch!* Süddeutsche Zeitung, 26 September 2011. URL: http://www.sueddeutsche.de/kultur/netz-depeschen-piratinnen-aller-laender-vereinigt-euch-1.1149182 [Accessed: 12.01.2012. In German].

[Hol98].
Hollnagel, E.: *Cognitive reliability and error analysis method,* Elsevier Science & Technology 1998.

[HSMS07].
Hirvonen, J./Sallinen, M./Maula, H./Suojanen, M.: *Sensor Networks Roadmap* (Research notes 2381, VTT Tiedotteita), 2007. URL: http://www.vtt.fi/inf/pdf/tiedotteet/2007/T2381.pdf [Accessed: 12.01.2012].

[HT12].
Hansen, M./Thiel, C.: *Cyber-Physical Systems und Privatsphären-Schutz.* In: Datenschutz und Datensicherheit (DuD) 36(1) 2012. [In German]

[Hua11].
Huang, J.: *Kinerehab: a kinect-based system for physical rehabilitation: a pilot study for young adults with motor disabilities.* In: 13th international ACM SIGACCESS conference on computers and accessibility (ASSETS'11, Proceedings), pp. 319–320, 2011.

[Hug11].
Hug, P.: *Gebäudeautomationsbranche rechnet mit weiterem Wachstum in 2011* (German Engineering Federation – VDMA, Press release), January 2011. URL: http://www.vdma.org/wps/wcm/connect/vdma/Home/de/Branchen/G/AMG/Presse/AMG_A_20110106_IMB_Pressemitteilung_Wirtschaftliche_Lage_2011_1_de?pagedesign=-SEITENENTWURF-Artikel_Druck [Accessed: 12.01.2012. In German].

[HUM].
Human – Model-based Analysis of Human Errors during Aircraft Cockpit System Design. URL: http://www.human.aero/[Accessed: 12.01.2012].

[HV08].
Hogg, S./Vyncke, E.: I*Pv6 Security: Information assurance for the next generation Internet Protocol,* Indianapolis: Cisco Press 2008.

[HW11].
Heuser, L./Wahlster, W. (Ed.): *Internet der Dienste* (acatech DISKUTIERT), Heidelberg inter alia: Springer 2011. URL: http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/acatech_diskutiert/acatech_Diskutiert_Internet-der-Dienste_WEB_02.pdf [Accessed: 12.01.2012. In German].

[HYD].
Hydra – Networked Embedded System Middleware for Heterogeneous Physical Devices in a Distributed Architecture. URL: http://www.sit.fraunhofer.de/de/kompetenzfelder/projekte/hydra.html [Accessed: 12.01.2012].

[IMA].
Integrated Modular Avionics. URL: http://de.wikipedia.org/wiki/Integrated_ Modular_Avionics [Accessed: 12.01.2012].

[IMo].
IMoST – Integrated Modeling for Safe Transportation. URL: http://imost.informatik.uni-oldenburg.de/ [Accessed: 12.01.2012].

[IÖ 10].
Institut für ökologische Wirtschaftsforschung (Institute for Ecological Economy Research – IÖW): *Selbstorganisierende adaptive Systeme – Analyse der Chancen und Risiken sowie der Gestaltungsansätze neuer IKT-Ansätze* (Final report, Technical report, recommendation of the "Innovations- und Technikanalyse" (innovation and technology analysis) of the Federal Ministry of Education and Research (BMBF), Duration: 03/2008–06/2009), 2010. URL: http://www.kanzlei-dr-erben.de/fileadmin/PDF/Selbstorganisierende_Adaptive_Systeme_Endbericht_Teil_I.pdf und http://www.kanzlei-dr-erben.de/fileadmin/PDF/Selbstorganisierende_Adaptive_Systeme_Endbericht_Teil_II.pdf [Accessed: 12.01.2012. In German].

[ISI].
ISI-PADDAS – Integrated Human Modelling and Simulation to support Human Error Risk Analysis of Partially Autonomous Driver Assistance Systems. URL: http://www.isi-padas.eu/ [Accessed: 12.01.2012].

[ISO09].
International Organization for Standardization (ISO) (Ed.): *Ergonomics of human-system interaction – Part 110: Dialogue principles* (Technical Report ISO 9241-110:2006), 2009. URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38009 [Accessed: 12.01.2012].

[ISO10].
International Organization for Standardization (ISO) (Ed.): *Software Engineering – Software product Quality Requirements and Evaluation (SQuaRE)– Guide to SQuaRE* (Technical Report ISO/IEC 25000:2005), 2010. URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35683 [Accessed: 12.01.2012].

[ISO11].
International Organization for Standardization (ISO) (Ed.): *Road vehicles – Functional safety – Part 1: Vocabulary* (Technical Report ISO 26262-1:2011), 2011. URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43464 [Accessed: 12.01.2012].

[JCKC11].
Janssen, M./Charalabidis, Y./Kuk, G./Cresswell, T. (Ed.): *Special Issue on E-government Interoperability, Infrastructure and Architecture: State-of-the-art and Challenges.* In: Journal of Theoretical and Applied Electronic Commerce Research 6(2) 2011. URL: http://www.jtaer.com/portada.php?agno=2011&numero=2 [Accessed: 12.01.2012].

[JM05].
Jürgens, U./Meißner, H.: *Arbeiten am Auto der Zukunft – Produktinnovationen und Perspektiven der Beschäftigten,* Berlin: Edition Sigma 2005. [In German]

[JS85].
Janson, M./Smith, L.: Prototyping for Systems Development: A Critical Appraisal. In: MIS Quarterly 9(4) 1985, pp. 305–316. URL: http://misq.org/prototying-for-systems-development-a-critical-appraisal.html?SID=lsp77n0v8pq6njos2df1fqbua5 [Accessed: 12.01.2012].

[JS10].
Jánszky, S./Schildhauer, T.: *Vom Internet zum Outernet: Strategieempfehlungen und Geschäftsmodelle der Zukunft in einer Welt der Augmented Realities* (Technical report, 2b AHEAD ThinkTanks and the Institute of Electronic Business at the Berlin University of the Arts), 2010. URL: http://www.2bahead.com/fileadmin/content/janszky/pdf/PDF_broschueren/WhitePaper_Vom_Internet_zum_Outernet.pdf [Accessed: 12.01.2012. In German].

[JW03].
Jeronimo, M./Weast, J.: *UPnP Design by Example: A Software Developer's Guide to Universal Plug and Play,* Intel Press 2003

[JWW08].
Jovane, F./Westkämper, E./Williams, D.: *The ManuFuture Road: Towards Competitive and Sustainable High-Adding-Value Manufacturing.* Heidelberg: Springer 2008.

[JZSB10].
Jian, C./Zhekova, D./Shi, H./Bateman, J.: *Deep Reasoning in Clarification Dialogues with Mobile Robots.* In: 19th European Conference on Artificial Intelligence (ECAI'10, Proceedings), Amsterdam: IOS Press 2010, pp. 177–182.

[KAR].
Kleinskaliges Autonomes Redundantes Intralogistik System – KARIS. URL: http://www.ifl.kit.edu/mitarbeiter_1312.php [Accessed: 12.01.2012. In German].

[KB05].
Krieg-Brückner, B.: *Selbstadaptation Kognitiver Service-Roboter* (Symposium Feldafinger Kreises, Presentation), 2005. URL: http://www.feldafinger-kreis.de/WS1_Impulsref_Krieg-Brueckner.pdf [Accessed: 12.01.2012. In German].

[KB08].
Kündig, A./Bütschi, D. (Ed.): *Die Verselbständigung des Computers*, Zürich: vdf Hochschulverlag 2008. [In German]

[KBRSG11].
Krieg-Brückner, B./Rofer, T./Shi, H./Gersdorf, B.: *Mobilitätassistenz im "Bremen Ambient Assisted Living Lab"* (BAALL). In: Altern und Technik (Altern in Deutschland Vol. 6), Nova Acta Leopoldina N. F., 104(368) 2011, pp. 157–174. [In German]

[Kes12]
Kessler, G.: *Daniel Hechter – Paris in Unterfranken.* In: Financial Times Deutschland, 28 February 2012. URL: http://www.ftd.de/unternehmen/handel-dienstleister/:markenrechte-daniel-hechter-paris-in-unterfranken/60175024.html [Accessed: 02.03.2012. In German].

[KGK10].
Kladroba, A./Grenzmann, C./Kreuels, B.: *FuE-Datenreport 2010 – Analysen und Vergleiche: Forschung und Entwicklung in der Wirtschaft* (Report on the R&D Surveys 2007/2008). (Technical report, Wissenschaftsstatistik GmbH im Stifterverband für die Deutsche Wissenschaft), 2010. URL: http://www.stifterverband.org/publikationen_und_podcasts/wissenschaftsstatistik/fue_datenreport/fue_datenreport_2010.pdf [Accessed: 12.01.2012. In German].

[Kir97].
Kirsch, W.: *Wegweiser zur Konstruktion einer evolutionären Theorie der strategischen Führung.* In: Münchner Schriften zur angewandten Führungslehre, Vol. 80, Herrsching, 1997. 2. revised and expanded edition. [In German]

[Kit09].
Kittl, C.: *Kundenakzeptanz und Geschäftsrelevanz: Erfolgsfaktoren für Geschäftsmodelle in der digitalen Wirtschaft.* In: Mobile Computing, Vol. 80, Gabler Edition Wissenschaft 2009. [In German]

[KLW11].
Kagermann, H./Lukas, W./Wahlster, W.: *Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution.* (Technical report, VDI Nachrichten [Association of German Engineers News]), April 2011. URL: http://www.vdi-nachrichten.com/artikel/Industrie-4-0-Mit-dem-Internet-der-Dinge-auf-dem-Weg-zur-4-industriellen-Revolution/52570/1 [Accessed: 12.01.2012. In German].

[KMU].
KMU-Innovativ: *Vorfahrt für Spitzenforschung im Mittelstand.* URL: http://www.bmbf.de/de/10785.php [Accessed: 12.01.2012. In German].

[KN04].
Kaplan, R./Norton, D.: Strategy Maps: *Converting Intangible Assets into Tangible Outcomes,* Harvard Business School Press 2004.

[KNR+ 11].
Krewitt, W./Nienhaus, K./Roloff, N./Weeber, R./Reeg, M./Weimer-Jehle, W./Wassermann, S./Fuchs, G./Kast, T./Schmidt, B./Leprich, U./Hauser, E.: *Analyse von Rahmenbedingungen für die Integration erneuerbarer Energien in die Strommärkte auf der Basis agentenbasierter Simulation* (Final report, Technical report) Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR German Aerospace Center), Interdisziplinärer Forschungsschwerpunkt Risiko und nachhaltige Technikentwicklung (ZIRN Interdisciplinary Research Unit on Risk Governance and Sustainable Technology Development), Thomas Kast Simulation Solutions, Institut für ZukunftsEnergieSysteme (IZES), (funded by the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety; funding reference no. 0325015), 2011. URL: http://www.dlr.de/Portaldata/41/Resources/dokumente/st/AMIRIS-Pilotvorhaben.pdf [Accessed: 12.01.2012. In German].

[KOF].
Forschungsinitiative KO-FAS. URL: http://www.kofas.de/ [Accessed: 12.01.2012. In German].

[KOT11].
KO-TAG: *Protecting Children*, 2011. URL: http://www.iis.fraunhofer.de/en/bf/ln/referenzprojekte/amulett.html [Accessed: 12.01.2012].

[KPCV11].
Krawczyk, S./Pétrissans, A./Cattaneo, G./Veronesi, L. (Ed.): *Special Study: European Union Embedded Systems Engineering Strategy 2020* (Workshop Report, International Data Corporation (IDC) and European Commission June 2011. Unpublished.

[KPM11].
Koukoumidis, E./Peh, L./Martonosi, M.: *SignalGuru: leveraging mobile phones for collaborative traffic signal schedule advisory.* In: Agrawala, Ashok inter alia. [ACW11]., pp. 127–140.

[KR00].
Kittler, J./Roli, F. (Ed.): *1st International Workshop on Multiple Classifier Systems* (MCS'2000, Proceedings, volume 1857 of Lecture Notes in Computer Science), Springer: Berlin 2000.

[KR11].
Kurz, C./Rieger, F.: *Die Datenfresser: Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen,* Frankfurt/Main: Fischer 2011. [In German]

[KS98].
Kotonya, G./Sommerville, I.: *Requirements Engineering: Processes and Techniques;* Wiley 1998.

[KS03].
Kalfoglou, Y./Schorlemmer, M.: *Ontology mapping: The state of the art.* In: The Knowledge Engineering Review 18(1) 2003, pp. 1–31.

[KSWK10].
Konings, B./Schaub, F./Weber, M./Kargl, F.: *Towards territorial privacy in smart environments* In Genesereth, M./Vogl, R./Williams, M. (Ed.): Intelligent Information Privacy Management Symposium (AAAI Spring Symposium, Proceedings, Technical Report SS-10-05), Stanford University 2010, pp. 113–118. URL: http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1043/1496 [Accessed: 12.01.2012].

[Lan11].
Langner, R.: *Robust Control System Networks: How to Achieve Reliable Control After Stuxnet,* Transatlantic Publishers 2011.

[Len97].
Lenat, D.: *From 2001 to 2001: Common Sense and the Mind of HAL.* In: Stork, David [Sto97]., pp. 305–332.

[Lev95].
Leveson, N.: *Safeware: System Safety and Computers,* Addison-Wesley 1995.

[LGK+ 09].
Legler, H./Gehrke, B./Krawczyk, O./Schasse, U./Leheyda, N./Rammer, C./Sofka, W.: *Die Bedeutung der Automobilindustrie für die deutsche Volkswirtschaft im europäischen Kontext* (Technical report), Zentrum für Europäische Wirtschaftsforschung (Centre for European Economic Research – ZEW) und Niedersächsisches Institut für Wirtschaftsforschung (Lower Saxony Institute of Economic Research – NIW) 2009. Final report to the Federal Ministry of Economics and Technology (BMWi Project No. 29/08). URL: ftp://ftp.zew.de/pub/zew-docs/gutachten/AutomobEnd-Bericht_final.pdf [Accessed: 12.01.2012. In German].

[LM08].
Lheureux, B./Malinverno, P.: *Magic Quadrant for B2B Gateway Providers* (Research ID Number: G00157460), Gartner, Inc. 2008. URL: http://www.trustlink.co.za/content/sterlingIntegrator.pdf [Accessed: 12.01.2012].

[LMK09].
Lorenz, M./Menkens, C./Konrad, N. (Ed.): *E-Energy – Trend Report 2009/2010* Center for Digital Technology and Management (CDTM), Munich 2009.

[LPS+ 97].
Leveson, N./Pinnel, L./Sandys, S./Koga, S./Reese, J.: *Analyzing Software Specifications for Mode Confusion Potential,* Workshop on Human Error and System Development (Proceedings), 1997, pp. 132–146. URL: http://sunnyday.mit.edu/papers/glascow.pdf [Accessed: 12.01.2012].

[LSH08].
Leenes, R./Schallaböck, J./Hansen, M.: *PRIME White Paper* (Technical report), The PRIME (Privacy and Identity Management for Europe) Project 2008. URL: http://www.rolandberger.com/media/pdf/Roland_Berger_IT_Anbieter_einer_neuen_Generation_20101025.pdf [Accessed: 12.01.2012].

[Lük11].
Lüke, F.: *EU-Datenschutzverordnung: Gegen den unkontrollierten Datenstrom* (Technical report). In: c't magazin, 7 December 2011. URL: http://www.heise.de/ct/artikel/EU-Datenschutzverordnung-Gegen-den-unkontrollierten-Datenstrom-1391778.html [Accessed: 12.01.2012. In German].

[Mah03].
Mahler, R.: *Multitarget Bayes filtering via first-order multitarget moments.* In: IEEE Transactions on Aerospace and Electronic Systems 39(4) 2003, pp. 1152–1178.

[Man83].
Manz, U.: *Zur Einordnung der Akzeptanzforschung in das Programm sozialwissenschaftlicher Begleitforschung – Ein Beitrag zur Anwenderforschung im technisch- organisatorischen Wandel,* Munich: Florentz Verlag 1983. [In German]

[Mat03].
Mattern, F. (Ed.): *Total vernetzt: Szenarien einer informatisierten Welt* (7. Berlin Colloquium of the Gottlieb Daimler- und Karl Benz-Stiftung, Proceedings, Xpert.press), Heidelberg: Springer 2003. [In German]

[Mat07].
Mattern, F. (Ed.): *Die Informatisierung des Alltags: Leben in smarten Umgebungen.* Heidelberg: Springer 2007. [In German]

[MB07].
Mediratta, B./Bick, J.: *The Google Way: Give Engineers Room,* The New York Times, 21 October 2007. URL: http://www.nytimes.com/2007/10/21/jobs/21pre.html [Accessed: 12.01.2012].

[MCS11].
International Workshop on Multiple Classifier Systems (MCS, Proceedings, Lecture Notes in Computer Science). Springer 2000–2011.

[MGS+ 11].
Mutter, F./Gareis, S./Schätz, B./Bayha, A./Grüneis, F./Kanis, M./Koss, D.: *Model-Driven In-the-Loop Validation: Simulation-Based Testing of UAV Software Using Virtual Environments.* In: 18th IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS'11, Proceedings), IEEE Computer Society 2011, pp. 269–275. URL: http://www.fortiss.org/fileadmin/user_upload/FB1/Schaetz/MBD2011.pdf [Accessed: 12.01.2012].

[MKRW11].
März, L./Krug, W./Rose, O./Weigert, G. (Ed.): *Simulation und Optimierung in Produktion und Logistik: Praxisorientierter Leitfaden mit Fallbeispielen,* Berlin inter alia: VDI-Buch Springer 2011. [In German]

[ML08].
Mattern, F./Langheinrich, M.: *Eingebettete, vernetzte und autonom handelnde Computersysteme: Szenarien und Visionen.* In: Kündig, A./Bütschi D. [KB08]., pp. 55–75. [In German]

[MLD10].
Mahnke, W./Leitner, S./Damm, M.: OPC *Unified Architecture* Heidelberg: Springer 2010.

[MM06].
Marron, P./Minder, D.(Ed.): *Embedded WiSeNts Research Roadmap,* Berlin:Logos Verlag 2006. URL: ftp://ftp.informatik.uni-stuttgart.de/pub/library/ncstrl.ustuttgart_fi/BOOK-2006-03/BOOK-2006-03.pdf [Accessed: 12.01.2012].

[MM10].
Meyer, S./Mollenkopf, H.(Ed.): *AAL in der alternden Gesellschaft: Anforderungen, Akzeptanz und Perspektiven – Analyse und Planungshilfe,* VDE-Verlag 2010. [In German]

[MOS08].
Deutsches Zentrum für Luft- und Raumfahrt (German Aerospace Center – DLR): *Pilot gaze performance in critical flight phases and during taxiing* (Technical report), Results from the Project MOSES (More Operational Flight Security through increased Situation Awareness), 2008.URL: http://www.dlr.de/fl/en/Portaldata/14/Resources/dokumente/abt27/MOSES_results.pdf [Accessed: 12.01.2012].

[MS95].
March, S./Smith, G.: *Design and natural science research on information technology.* In: Decision Support Systems 15 1995, pp. 251–266.

[MTI].
Mensch Technik Interaktion. URL: http://www.pt-it.pt-dlr.de/de/1862.php [Accessed: 12.01.2012. In German].

[Mü10].
Müller, O.: *Zwischen Mensch und Maschine: Vom Glück und Unglück des Homo faber,* (Volume 29 Reihe edition unseld), Berlin: Suhrkamp Verlag 2010. [In German]

[Mus04].
Musa, J.: *Software Reliability Engineering: More Reliable Software Faster and Cheaper,* 2nd edition, Authorhouse 2004.

[MVK06].
Monostori, L./Váncza, J./Kumara, S.: *Agent-Based Systems for Manufacturing.* In: CIRP Annals – Manufacturing Technology 55(2) 2006, pp. 697–720.

[NAF07].
North Atlantic Treaty Organization (NATO): *NATO Architecture Framework Version 3.0* (NAF V2.0) (Technical report), 2007. URL: http://www.nhqc3s.nato.int/ARCHITECTURE/_docs/NAF_v3/ANNEX1.pdf [Accessed: 12.01.2012].

[NAV].
Navigation autonomer Systeme im Outdoor-Bereich. URL: http://www.rts.uni-hannover.de/index.php/Navigation_autonomer_Systeme_im_Outdoor-Bereich [Accessed: 12.01.2012. In German].

[NGM].
Next Generation Media. URL: http://www.nextgeneration-media.de/en/index.php [Accessed: 12.01.2012].

[NIM].
NIMITEK – Neurobiologisch inspirierte, multimodale Intentionserkennung für technische Kommunikationssysteme URL: http://wdok.cs.uni-magdeburg.de/nimitek [Accessed: 12.01.2012. In German].

[Nor96].
Norman, D.: *Dinge des Alltags: Gutes Design und Psychologie für Gebrauchsgegenstände*, Campus Verlag 1996. [In German]

[OAS09].
Organization for the Advancement of Structured Information Standards (OASIS): *Devices Profile for Web Services (DPWS) Version 1.1* (Technical report), 2009. URL: http://docs.oasis-open.org/ws-dd/dpws/1.1/os/wsdd-dpws-1.1-spec-os.pdf [Accessed: 12.01.2012].

[Oct].
Octo Telematics. http://www.octotelematics.com/de [Accessed: 12.01.2012. In German].

[Ohl12]
Ohler, A.: *Telekomkonzerne entern Gesundheitsbranche.* In: Financial Times Deutschland, 1 March 2012. URL: http://www.ftd.de/it-medien/it-telekommunikation/:mobile-world-congress-telekomkonzerne-entern-gesundheitsbranche/60176147.html [Accessed: 02.03.2012. In German].

[OPT05].
Osterwalder, A./Pigneur, Y./Tucci, C.: *Clarifying Business Models: Origins, Present, and Future of the Concept.* In: Communications of the Association for Information Systems 16(1) 2005, pp. 751–775. URL: http://aisel.aisnet.org/cais/ vol16/iss1/1, Article 1 [Accessed: 12.01.2012].

[Osb03].
Osborne, M.: *An Introduction to Game Theory,* Oxford University Press 2003.

[OyG49].
Gasset, J.: *Betrachtungen über die Technik (translated from Spanish by Fritz Schalk),* Stuttgart: Deutsche Verlagsanstalt 1949. [In German. Available in English as Thoughts on Technology (translated by H. Weyl). In: Mitcham C./Mackey R. (Ed.): Philosophy and technology. Readings in the philosophical problems of technology. New York: Free Press 1972]

[Pac11].
Pachube API Documentation (Technical report), 2011. URL: http://api.pachube.com/ [Accessed: 12.01.2012].

[PAR].
Vollautonomes Einparken von Fahrzeugen auf Parkplatzgeländen. URL: http://zentrix-t1.te1.hs-heilbronn.de/T1_MST/fue-aktivitaeten/vollautonomes-einparken-von-fahrzeugen-auf-parkplatzgelaenden, [Accessed: 12.01.2012. In German].

[Par11].
Pariser, E.: *The Filter Bubble: What the Internet Is Hiding from You,* Penguin Press 2011.

[PB03].
Petrick, R./Bacchus, F.: *Reasoning with Conditional Plans in the Presence of Incomplete Knowledge.* In: ICAPS03 Workshop on Planning under Uncertainty and Incomplete Information (Proceedings), Università di Trento 2003, pp. 96–102.

[PCM11].
Pletikosa Cvijikj, I./Michahelles, F.: *The Toolkit Approach for End-User Participation in the Internet of Things.* In: Uckelmann, D. et al. [UHM11b]., pp. 65–96.

[Pik11].
Cumulative Plug-in Electric Vehicle Sales to Reach 5.2 Million Worldwide by 2017, Pike Research Newsroom, 22 August 2011. URL: http://www.pikeresearch.com/newsroom/cumulative-plug-in-electric-vehicle-sales-to-reach-5-2-million-worldwide-by-2017 [Accessed: 12.01.2012].

[PLSD11].
Prinz, J./Lüder, A./Suchold, N./Drath, R.: *Beschreibung mechatronischer Objekte durch Merkmale.* In: atp-edition53(7/8) 2011, pp. 62–69. [In German]

[PS06].
Picot, A./Schmid, M.: *Wettbewerbsstrategien von Internet-TV-Plattformen und Business Webs.* In: Information Management & Consulting 21(3) 2006, pp. 30–40. [In German]

[Psy11].
YouGovPsychonomics AG (Ed.): *ComparisonCheck Finanzen 2011 – Finanzportale im Vergleich* (Technical report), 2011. URL: http://www.psychonomics.de/filemanager/ download/2483 [Accessed: 12.01.2012. In German].

[Qui06].
Quiring, O.: *Methodische Aspekte der Akzeptanzforschung bei interaktiven Medientechnologien.* In: Münchner Beiträge zur Kommunikationswissenschaft 6, December 2006. URL: http://epub.ub.uni-muenchen.de/archive/00001348/01/mbk_6.pdf [Accessed: 12.01.2012. In German].

[R2B].
Robot2Business. URL: http://www.agrardienstleistungen.de/r2b/ [Accessed: 12.01.2012. In German].

[Rab08].
Rabaey, J.: *A brand new wireless day.* In: ASP-DAC'08 [ASP08]., p. 1.

[Ram03].
Rammert, W.: *Technik in Aktion: Verteiltes Handeln in soziotechnischen Konstellationen.* In: Christaller, T./Wehner, J. [CW03]., pp. 289–315. [In German]

[Ram06].
Rammert, W.: *Technik in Aktion: Verteiltes Handeln in soziotechnischen Konstellationen.* In: Rammert, W./Schubert, C. [RS06]., pp. 163–195. [In German]

[Ram07].
Rampl, H.: *Handbuch Usability,* 2007. URL: http://www.handbuch-usability.de/usability-engineering.html [Accessed: 12.01.2012. In German].

[RB11].
Rost, M./Bock, K.: *Privacy By Design und die Neuen Schutzziele.* In: Datenschutz und Datensicherheit (DuD) 35(1) 2011, pp. 30–35. [In German]

[RBB+ 08].
Roussopoulos, M./Beslay, L./Bowden, C./Finocchiaro, G./Hansen, M./Langheinrich, M./Le Grand, G./Tsakona, K.: *Technology-induced challenges in Privacy & Data Protection in Europe* (Technical report, Ad Hoc Working Group on Privacy & Technology), European Network and Information Security Agency (ENISA) 2008. URL: http://www.enisa.europa.eu/act/rm/files/deliverables/technology-induced-challenges-in-privacy-data-protection-in-europe/at_download/fullReport [Accessed: 12.01.2012].

[Rea94].
Reason, J.: *Menschliches Versagen: psychologische Risikofaktoren und moderne Technologien,* Spektrum Akademischer Verlag 1994. [In German]

[Rei82].
Reichwald, R. (Ed.): *Neue Systeme der Bürotechnik – Beiträge zur Büroarbeitsgestaltung aus Anwendersicht,* Berlin: Erich Schmidt Verlag 1982. [In German]

[Ren05].
Renn, O.: *Technikakzeptanz: Lehren und Rückschlüsse der Akzeptanzforschung für die Bewältigung des technischen Wandels.* In: Technikfolgenabschätzung – Theorie und Praxis 14(3): 2005, pp. 29–38. [In German]

[RES].
Rescue. URL: http://www.informatik.uni-freiburg.de/~rescue/ [Accessed: 12.01.2012].

[RGH12]
Ruch, M./Graf, A./Hucko, M.: *Ford warnt vor Verkehrsinfarkt.* In: Financial Times Deutschland, 27 February 2012. URL: http://www.ftd.de/it-medien/it-telekommunikation/:interview-mit-aufsichtsratschef-ford-warnt-vor-verkehrsinfarkt/60174749.html [Accessed: 02.03.2012. In German].

[RLM+ 06].
Rubin, D./Lewis, S./Mungall, C./Misra, S./Westerfield, M./Ashburner, M./Sim, I./Chute, C./Solbrig, H./Storey, M./Smith, B./Day-Richter, J./Noy, N./Musen, M.: *Advancing Biomedicine through Structured Organization of Scientific Knowledge (National Center for Biomedical Ontology OMICS).* In: A Journal of Integrative Biology 10(2) 2006, pp. 185–198. URL: http://www.liebertonline.com/doi/pdf/10.1089/omi.2006.10.185 [Accessed: 12.01.2012].

[RLSS10].
Rajkumar, R./Lee, I./Sha, L./Stankovic, J.: *Cyber-physical systems: the next computing revolution.* In: Sapatnekar, S. (Ed.): 47th Design Automation Conference (DAC'10, Proceedings) ACM, 2010, pp. 731–736.

[RMM11].
Müller, R./Kijl, B./Martens, J.: A *Comparison of Inter-Organizational Business Models of Mobile App Stores: There is more than Open vs. Closed.* In: Marijn J. inter alia. [JCKC11]., Journal of Theoretical and Applied Electronic Commerce Research 6(2) 2011, pp. 63–76. URL: http://www.jtaer.com/portada.php?agno=2011&numero=2 [Accessed: 12.01.2012].

[RN09].
Russell, S./Norvig, P.: *Artificial Intelligence: A Modern Approach* (3rd edition), Prentice Hall 2009.

[RNR+ 11].
Reeg, M./Nienhaus, K./Roloff, N./Wassermann, S./Weimer-Jehle, W./Hauser, E./Leprich, U./Kast, T.: *Analyse von Rahmenbedingungen für die Integration erneuerbarer Energien in die Strommärkte auf der Basis agentenbasierter Simulation.* In: 7. Internationale Energiewirtschaftstagung an der TU Wien (IEWT'11, Proceedings), 2011. URL: http://eeg.tuwien.ac.at/eeg.tuwien.ac.at_pages/events/iewt/iewt2011/uploads/fullpaper_iewt2011/P_249_Reeg_Matthias_9-Feb-2011,_14:11.pdf [Accessed: 12.01.2012. In German].

[Roß07].
Roßnagel, A.: *Datenschutz in einem informatisierten Alltag,* Berlin: Friedrich-Ebert- Stiftung 2007. URL: http://library.fes.de/pdf-files/stabsabteilung/04548.pdf [Accessed: 12.01.2012]. [In German]

[RP09a].
Reichwald, R./Piller, F.: *Interaktive Wertschöpfung: Open Innovation, Individualisierung und neue Formen der Arbeitsteilung* (2nd completely revised and extended edition), Gabler Verlag 2009. URL: http://www.open-innovation.de/Reichwald-Piller_IWS-2009_Auszug_2auflage.pdf [Accessed: 12.01.2012]. [In German]

[RP09b].
Rost, M./Pfitzmann, A.: *Datenschutz-Schutzziele revisited.* In: Datenschutz und Datensicherheit (DuD) 33(6) 2009, pp. 353–358. [In German]

[RS00].
Rosenkranz, D./Schneider, N. (Ed.): *Konsum: Soziologische, ökonomische und psychologische Perspektiven* Opladen: Leske + Budrich Verlag 2000. [In German]

[RS06].
Rammert, W./Schubert, C. (Ed.): *Technografie: Zur Mikrosoziologie der Technik,* Frankfurt/Main: Campus Wissenschaft 2006. [In German]

[RSM+ 11].
Romer, B./Sußmann, J./Menkens, C./Lorenz, M./Mayrhofer, P. (Ed.): *Smart Grid Infrastructures – Trend Report 2010/2011,* Munich: Center for Digital Technology and Management (CDTM) 2011.

[RSS02a].
Rammert, W./Schulz-Schaeffer, I. (Ed.): *Können Maschinen handeln?* In: Soziologische Beiträge zum Verhältnis von Mensch und Technik Frankfurt/Main: Campus Wissenschaft 2002. [In German]

[RSS02b].
Rammert, W./Schulz-Schaeffer, I.: *Technik und Handeln – Wenn soziales Handeln sich auf menschliches Verhalten und technische Abläufe verteilt.* In: Rammert, W./Schulz-Schaefer, I. [RSS02a]., pp. 11–64. [In German]

[RWJ+ 11].
Richling, J./Werner, M./Jaeger, M./Mühl, G./Heiß, H: *Autonomie in verteilten IT-Architekturen*, Oldenbourg Wissenschaftsverlag 2011. [In German]

[Sad11].
Sadri, F.: *Logic-Based Approaches to Intention Recognition.* In Chong, N./Mastrogiovanni, F. (Ed.): Handbook of Research on Ambient Intelligence and Smart Environments: Trends and Perspectives, IGI Global 2011, pp. 346–375.

[SAF].
SAFE – Safe Automotive soFtware architecture. URL: http://www.itea2.org/project/index/view/?project=10108 [Accessed: 12.01.2012].

[SAL+ 03].
Stankovic, J./Abdelzaher, T./Lu, C./Sha, L./Hou, J.: *Real-time communication and coordination in embedded sensor networks.* In: Real-Time Systems (Proceedings of the IEEE) 91(7) 2003, pp. 1002–1022.

[SAT].
The SARTRE project. URL: http://www.sartre-project.eu [Accessed: 12.01.2012].

[SB01].
Sundermeyer, K./Bussmann, S.: *Einführung der Agententechnologie in einem produzierenden Unternehmen – Ein Erfahrungsbericht.* In: Wirtschaftsinformatik 43(2) 2001, pp. 135–142. [In German]

[SB10].
Schleipen, M./Bader, T.: *A concept for interactive assistant systems for multi-user engineering based on AutomationML.* In: Computer-Aided Production Engineering Conference (21st International CAPE, Proceedings, Paper 014), 2010.

[Sch00].
Schneider, N.: *Konsum und Gesellschaft.* In: Rosenkranz, D./Schneider, N. [RS00]., pp. 9–22. [In German]

[Sch04].
Schätz, B.: *AutoFocus – Mastering the Complexity.* In: Kordon, F. Lemoine, M. (Ed.): Formal Methods for Embedded Distributed Systems: How to master the complexity (chapter 7), Kluwer Academic Publishers 2004, pp. 215–257.

[Sch05].
Schoch, T.: *Middleware für Ubiquitous-Computing-Anwendungen.* In: Fleisch, E./Mattern, F. [FM05]., pp. 119–140. [In German]

[Sch07a].
Schaar, P.: *Das Ende der Privatsphäre: Der Weg in die Überwachungsgesellschaft,* C. Bertelsmann 2007. [In German]

[Sch07b].
Schulz, A.: *Driving without awareness – Folgen herabgesetzter Aufmerksamkeit im Straßenverkehr,* VDM Verlag Dr. Müller 2007. [In German]

[Sch10a].
Schanze, J.: *Plug & Pray.* (Film, 91 min., produced in Germany), 2010. URL: http://www.plugandpray-film.com/ [Accessed: 12.01.2012]. [In German with English subtitles]

[Sch10b].
Schill, W.: *Electric Vehicles in Imperfect Electricity Markets: A German Case Study* (Discussion papers 1084), Deutsches Institut für Wirtschaftsforschung (German Institute for Economic Research – DIW) 2010. URL: http://www.diw.de/documents/publikationen/73/diw_01.c.364293.de/dp1084.pdf [Accessed: 12.01.2012].

[Sch11].
Schwan, B.: *Grüne Welle dank Smartphone* (Technical report), Technology Review, 7 October 2011. URL: http://www.heise.de/tr/artikel/Gruene-Welle-dank-Smartphone-1353408.html [Accessed: 12.01.2012. In German].

[Sch12]
Schlüter, N.: *Intel drängt ans Steuer.* In: Financial Times Deutschland, 1 March 2012. [In German]

[SDL03].
Scheer, C./Deelmann, T./Loos, P.: *Geschäftsmodelle und internetbasierte Geschäftsmodelle – Begriffsbestimmung und Teilnehmermodell.* In: Working Papers of the Research Group Information Systems & Management 12, Johannes Gutenberg-University Mainz 2003. URL: http://wi.bwl.uni-mainz.de/publikationen/isym012.pdf [Accessed: 12.01.2012. In German].

[SE07].
Sauer, O./Ebel, M.: *Plug-and-work von Produktionsanlagen und übergeordneter Software.* In: Koschke, R./Herzog, O./ Rodiger, K./Ronthaler, M. (Ed.): INFORMATIK 2007: Informatik trifft Logistik Volume 2 (Beiträge der 37. Jahrestagung der Gesellschaft für Informatik e. V. GI [Papers from the 37th annual conference of the German Informatics Society]), Volume 110 of Lecture Notes in Informatics) GI 2007, pp. 331–338. URL: http://subs.emis.de/LNI/Proceedings/Proceedings110/gi-proc-110-058.pdf [Accessed: 12.01.2012. In German].

[SEM].
Semantic Product Memory – SEMPROM. URL: http://www.semprom.de/semprom_engl/ [Accessed: 12.01.2012].

[SEN].
Smart Senior – Independent, safe, healthy and mobile. URL: http://www.smart-senior.de/enEn [Accessed: 12.01.2012].

[Sep08].
Seppänen, M.: *Business Model Concept: Building on Resource Component*s (PhD thesis, Faculty of Business and Technology Management), Tampere University of Technology 2008. URL: http://dspace.cc.tut.fi/dpub/bitstream/handle/123456789/5/seppanen.pdf?sequence=1 [Accessed: 12.01.2012].

[SFBa].
TU Dortmund (Sonderforschungsbereich 559) (Ed.): *Modellierung großer Netze in der Logistik.* (Technical report, Sonderforschungsbereich 559, Project funded from 07/1998–06/2008.). URL: http://www.wiso.tu-dortmund.de/wiso/Medienpool/dokumente/medien_sonstiges/sfb559.pdf [Accessed: 12.01.2012. In German].

[SFBb].
Universität Ulm (Ulm University) (Sonderforschungsbereich/ Transregio 62): *Companion Technology.* URL: http://www.uni-ulm.de/en/in/sfb transregio-62.html [Accessed: 12.01.2012].

[Sim01].
Simon, B.: *Wissensmedien im Bildungssektor – Eine Akzeptanzuntersuchung an Hochschulen* (Dissertation), Wirtschaftsuniversität Wien (Vienna University of Economics and Business Administration) 2001. [In German]

[sim11].
Sichere Intelligente Mobilität – Testfeld Deutschland (simTD) (Ed.): *fakten* (Technical report), 2011. URL: http://www.simtd.de/index.dhtml/484ea960514a731976nm/object.media/deDE/7265/CS/-/backup_publications/Informationsmaterial/simTD-informationsbltter_2011_DE.pdf [Accessed: 12.01.2012. In German].

[SIW].
SiWear – Sichere Wearable-Systeme zur Kommissionierung industrieller Güter sowie für Diagnose, Wartung und Reparatur. URL: http://www.siwear.de [Accessed: 12.01.2012. In German].

[SL11].
Schlüter, N./Laube, H.: *Vom schicken Startup zum schöden Schnüffler,* Financial Times Deutschland, 7 December 2011. [In German]

[SMS11].
Schleipen, M./Münnemann, A./Sauer, O.: *Interoperabilität von Manufacturing Execution Systems (MES): Durchgängige Kommunikation in unterschiedlichen Dimensionen der Informationstechnik in produzierenden Unternehmen.* In: Automatisierungstechnik 59(7) 2011, pp. 413–425. URL: http://www.iosb.fraunhofer.de/servlet/is/4893/auto.2011.0936.pdf?command=downloadContent&filename=auto.2011.0936.pdf [Accessed: 12.01.2012. In German].

[Soc07].
Journal of Artificial Societies and Social Simulation: Special section: Socionics 2007. URL: http://jasss.soc.surrey.ac.uk/10/1/contents.html [Accessed: 12.01.2012].

[son09].
sonoma innovation (Ed.): *Smart Grid Communications – Architectural Framework*, 2009. URL: http://www-users.cselabs.umn.edu/classes/Fall-2009/seng5861/project/a1ueNt4L.pdf [Accessed: 12.01.2012].

[SPE].
SPES 2020 – Software Plattform Embedded Systems. URL: http://spes2020.informatik.tu-muenchen.de/ [Accessed: 12.01.2012. In German].

[Spi63].
Der Spiegel: *Unfall-Ursachen: Erzwungene Versager*, 22 May 1963. URL: http://www.spiegel.de/spiegel/print/d-45143500.html [Accessed: 12.01.2012. In German].

[Spi00].
Spitzer, M. (Ed.): *Geist im Netz: Modelle für Lernen, Denken und Handeln.* (corrected edition), Spektrum Akademischer Verlag 2000. [In German]

[SS11].
Stone, E./Skubic, M.: *Evaluation of an Inexpensive Depth Camera for Passive In-Home Fall Risk Assessment.* In: 5th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth'11, Proceedings), pp. 71–77, 2011. URL: http://eldertech.missouri.edu/files/Papers/StoneE/Evaluation%20of%20an%20Inexpensive%20Depth%20Camera.pdf [Accessed: 27.02.2012].

[STA].
Stadtpilot. URL: http://stadtpilot.tu-bs.de/en [Accessed: 12.01.2012].

[Stä02].
Stähler, P.: *Geschäftsmodelle in der digitalen Ökonomie: Merkmale, Strategien und Auswirkungen* (Volume 7 of the Electronic Commerce series, 2nd edition) Lohmar: Josef Eul Verlag 2002. [In German]

[Sta11].
Statistisches Bundesamt (Federal Statistical Office) (Ed.): *Produzierendes Gewerbe: Beschäftigung und Umsatz der Betriebe des VerarbeitendenGewerbes sowie des Bergbaus und der Gewinnung von Steinen und Erden* (August 2011) (Technical report Fachserie 4 Reihe 4.1.1), Wiesbaden 2011. URL: http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Publikationen/Fachveroeffentlichungen/ Produzierendes_20Gewerbe/VerarbeitendesGewerbe/Konjunkturdaten/Monatsbericht-M2040411111084,property=file.pdf [Accessed: 12.01.2012. In German].

[Sto97].
Stork, D. (Ed.): *HAL's Legacy: 2001's Computer as Dream and Reality*, Cambridge (MA): MIT Press 1997.

[Thi10].
Thiel, C.: *Multiple classifier systems incorporating uncertainty*, Munich: Verlag Dr. Hut 2010.

[TOG09].
The Open Group (Ed.): *TOGAF Version 9, Enterprise Edition* (Technical report), 2009. URL: https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?catalogno=g091 [Accessed: 12.01.2012].

[Tra09].
Traufetter, G.: Captain Computer. In: Der Spiegel, 27 July 2009. URL: http://www.spiegel.de/spiegel/print/d-66208581.html [Accessed: 24.02.2012. In German].

[TRS+ 10].
Thyssen, J./Ratiu, D./Schwitzer, W./Harhurin, A./Feilkas, M./Thaden, E.: A *System for Seamless Abstraction Layers for Model-based Development of Embedded Software.* In: Engels, G./Luckey, M./Pretschner, A./Reussner, R. (Ed.): Software Engineering Workshops 2010 (Proceedings, volume 160 of Lecture Notes in Informatics, Gesellschaft für Informatik [German Informatics Society]), 2010, pp. 137–148. URL: http://www4.in.tum.de/~schwitze/Envision2020.pdf [Accessed: 12.01.2012].

[Tur50].
Turing, A.: *Computing Machinery and Intelligence.* In: Mind, LIX(236), 1950, pp. 433–460. URL: http://mind.oxfordjournals.org/content/LIX/236/433.full.pdf [Accessed: 12.01.2012].

[UAV10].
UAV Challenge – Outback Rescue 2010, 2010. URL: http://www.uavoutbackchallenge.com.au/2010/ [Accessed: 12.01.2012].

[UHM11a].
Uckelmann, D./Harrison, M./Michahelles, F.: *An Architectural Approach Towards the Future Internet of Things.* In: Uckelmann, D. et al. [UHM11b], pp. 1–24.

[UHM11b].
Uckelmann, D./Harrison, M./Michahelles, F. (Ed.): *Architecting the Internet of Things,* Heidelberg: Springer 2011.

[ULD07].
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) (Ed.): *Verkettung digitaler Identitäten* (Technical report, funded by the Federal Ministry of Education and Research as part of the Innovation and Technology Analysis), 2007. URL: https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf [Accessed: 12.01.2012. In German].

[ULD10].
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD): *Vorstudie: Juristische Fragen im Bereich Altersgerechter Assistenzsysteme* (Technical report, commissioned by VDI (Association of German Engineers)/VDE Innovation + Technik GmbH as part of the BMBF funding priority "Altersgerechte Assistenzsysteme für ein gesundes und unabhängiges Leben – AAL"), 2010. URL: http://aal-deutschland.de/deutschland/dokumente/20110215-Juristische%20Fragen%20im%20Bereich%20altersgerechter%20Assistenzsysteme.pdf [Accessed: 12.01.2012. In German].

[Uli].
Ulieru, M.: *eNetworks in an Increasingly Volatile World: Design for Resilience of Networked Critical Infrastructures* (Unpublished). URL: http://independent.academia.edu/MihaelaUlieru/Papers/394260/ENetworks_In_An_Increasingly_Volatile_World_Design_for_Resilience_of_Networked_Critical_Infrastructures [Accessed: 12.01.2012].

[VDI07].
VDI (Association of German Engineers) Fachbereich Informationstechnik (Ed.): *Fertigungsmanagementsysteme* (Manufacturing Execution Systems, MES), (VDI-Richtlinie: VDI 5600 Blatt1), Beuth 2007.

[VDI08].
VDI (Association of German Engineers) Fachbereich Fabrikplanung und –betrieb (Ed.): *Digitale Fabrik: Grundlagen* (Digital factory: Fundamentals), (VDI-Richtlinie: VDI 4499 Blatt 1), Beuth 2008.

[VDI11a].
VDI (Association of German Engineers) Fachbereich Fabrikplanung und –betrieb (Ed.): *Digitale Fabrik: Digitaler Fabrikbetrieb* (Digital factory: Digital Factory Operations), (VDI-Richtlinie: VDI 4499 Blatt 2) Beuth 2011.

[VDI11b].
VDI (Association of German Engineers) Fachbereich Informationstechnik: Fertigungsmanagementsysteme (Ed.): *Logische Schnittstellen zur Maschinen- und Anlagensteuerung* (Manufacturing Execution Systems, MES: Logic interfaces for machine and plant control), (VDI-Richtlinie: VDI 5600 Blatt 3.) Beuth 2011.

[VDM11].
Verband Deutscher Maschinen- und Anlagenbau (VDMA German Engineering Federation) (Ed.): *Maschinenbau in Zahl und Bild 2011* (Technical report), Frankfurt/Main 2011. URL: http://www.vdma.org/wps/wcm/connect/c6ce3800467e8f3284d0965629cf6c64/MbauinZuB2011.pdf? MOD=AJPERES&CACHEID=c6ce3800467e8f3284d0965629cf6c64 [Accessed: 12.01.2012. In German].

[VER].
ITEA-Project VERDE – Validation-driven design for component-based architectures. URL: http://www.itea-verde.org/ [Accessed: 12.01.2012].

[VI09].
Verein Deutscher Ingenieure e. V. (VDI) und Institut der deutschen Wirtschaft Köln (IW Köln) (Association of German Engineers and the Cologne Institute for Economic Research) (Ed.): *Ingenieurarbeitsmarkt 2008/09 – Fachkräftelücke, Demografie und Ingenieure 50Plus* (Technical report), 2009. URL: http://www.vdi.de/uploads/media/2009-04-20-Studie_VDI-IW2_01.pdf [Accessed: 12.01.2012. In German].

[VIT].
Vitality – Monitoring & Managing your Health and Well-being. URL: http://www.itea2.org/project/index/view/?project=10071 [Accessed: 12.01.2012].

[vTFN09].
Thiel, B. van/Frädrich, T./Nyhuis, P.: *Maintenance Driven by Component Status.* In: Life Cycle Engineering in the Sustainability Age (LCE'09, Proceedings), 2009, pp. 472–477.

[WAL].
Google Wallet. URL: http://www.google.com/wallet/ [Accessed: 12.01.2012].

[WAS].
WASP – Wireless Accessible Sensor Populations. URL: http://www.wasp-project.org [Accessed: 12.01.2012].

[Web02a].
Webb, A.: *Statistical Pattern Recognition* (2nd edition), John Wiley & Sons 2002.

[Web02b].
Weber, M.: *Wirtschaft und Gesellschaft: Grundriß der Verstehenden Soziologie* (5th revised edition), Tübingen: Mohr Siebeck 2002. [In German. Available in English under the title Economy and Society: An Outline of Interpretive Sociology, University of California Press 1992.]

[Wei76].
Weizenbaum, J.: *Computer Power and Human Reason: From Judgement to Calculation,* W. H. Freeman & Co Ltd. 1976.

[Wei00].
Weiss, G. (Ed.): *Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence,* MIT Press 2000.

[Wer11].
Werner, K.: *Sturm über Klagenfurt.* Financial Times Deutschland, 22 September 2011. [In German]

[Wes67].
Westin, A.: *Privacy and Freedom,* New York: Atheneum 1967.

[Wey06a].
Weyer, J.: *Die Kooperation menschlicher Akteure und nicht-menschlicher Agenten – Ansatzpunkte einer Soziologie hybrider Systeme.* In: Soziologische Arbeitspapiere 16, Universität Dortmund (TU Dortmund University), 2006. URL: http://www.wiso.tu-dortmund.de/wiso/is/Medienpool/Arbeitspapiere/ap-soz16.pdf [Accessed: 12.01.2012. In German].

[Wey06b].
Weyer, J.: *Die Zukunft des Autos – das Auto der Zukunft. Wird der Computer den Menschen ersetzen?.* In: Soziologische Arbeitspapiere 14, Universität Dortmund (TU Dortmund University), 2006. URL: http://www.wiso.tu-dortmund.de/wiso/is/Medienpool/Arbeitspapiere/ap-soz14.pdf [Accessed: 12.01.2012. In German].

[Wey06c].
Weyer, J.: *Modes of Governance of Hybrid Systems: The Mid-Air Collision at Ueberlingen and the Impact of Smart Technology.* In: Science, Technology & Innovation Studies 2(2) 2006, pp. 127–149.

[Wey11a].
Weyer, J.: *Netzwerke in der mobilen Echtzeitgesellschaft.* In: Weyer, J. [Wey11b]., pp. 3–38. [In German]

[Wey11b].
Weyer, J. (Ed.): *Soziale Netzwerke: Konzepte und Methoden der sozialwissenschaftlichen Netzwerkforschung* (2nd revised and updated edition), Munich: Oldenbourg Wissenschaftsverlag 2011. [In German]

[WHB+06].
Winner, H./Hakuli, S./Bruder, R./Konigorski, U./Schiele, B.: *Conduct-by-Wire: ein neues Paradigma für Entwicklung der Fahrerassistenz.* In: Stiller, C./Maurer, M. (Ed.): 4. Workshop Fahrerassistenzsysteme (FAS'06, Tagungsband), Freundeskreis Mess- und Regelungstechnik Karlsruhe e.V. (fmrt): 2006, pp. 112–134. URL: http://www.iad.tu-darmstadt.de/forschung_15/forschungsschwerpunkte_1/fahrzeugergo_1/conductbywire.de.jsp [Accessed: 17.02.2012. In German].

[WMKP10].
Wiedersheim, B./Ma, Z./Kargl, F./Papadimitratos, P.: *Privacy in Inter-Vehicular Networks: Why simple pseudonym change is not enough.* In: 7th International Conference on Wireless On-demand Network Systems and Services (WONS'10, Proceedings), IEEE Computer Society Press 2010, pp. 176-–83.

[Woo09].
Wooldridge, M.: *An Introduction to MultiAgent Systems* (2nd edition), John Wiley & Sons 2009.

[WR08].
Wahlster, W./Raffler, H.: *Forschen für die Internet-Gesellschaft: Trends, Technologien, Anwendungen* (Technical report), Feldafinger Kreis 2008. URL: http://www.feldafinger-kreis.de/Feldafinger-Kreis_Studie_2008.pdf, Trends und Handlungsempfehlungen 2008 [Accessed: 12.01.2012. In German].

[WRK10].
Weiner, N./Renner, T./Kett, H.: *Geschäftsmodelle im „Internet der Dienste" – Trends und Entwicklungen auf dem deutschen IT-Markt* (Technical report), Fraunhofer-Institut für Arbeitswirtschaft und Organisation (Fraunhofer IAO), 2010. URL: http://wiki.iao.fraunhofer.de/images/studien/geschaeftsmodelle_im_internet_der_dienste_trends.pdf [Accessed: 12.01.2012. In German].

[WRN09].
Wiendahl, H./Reichardt, J./Nyhuis, P.: *Handbuch Fabrikplanung: Konzept, Gestaltung und Umsetzung wandlungsfähiger Produktionsstätten*, Munich: Carl Hanser 2009. [In German]

[WS07].
Wright, S./Steventon, A.: *Smarte Umgebungen – Vision, Chancen und Herausforderungen.* In: Mattern, F. [Mat07]., pp. 17–38. [In German]

[WS10].
Wood, A./Stankovic, J.: *Security of Distributed, Ubiquitous, and Embedded Computing Platforms.* In: Voeller, J. (Ed.): Wiley Handbook of Science and Technology for Homeland Security, John Wiley & Sons 2010.

[WSB+ 10].
Wollschläger, M./Schrieber, R./Birkhofer, R./Winzenick, M./Kalhoff, J./Kleedorfer, C./Mühlhause, M./Niemann, J.: *Life-Cycle-Management für Produkte und Systeme der Automation: Ein Leitfaden des Arbeitskreises Systemaspekte im ZVEI Fachverband Automation*, ZVEI Services 2010. [In German]

[ZAM10].
Zott, C./Amit, R.,/Massa, L.: *The business model: Theoretical roots, recent developments, and future research* (Working papers WP-862, IESE Business School), University of Navarra 2010. URL: http://www.iese.edu/research/pdfs/DI-0862-E.pdf [Accessed: 12.01.2012].

[ZBB].
Zukunft Breitband für eine flächendeckende Breitbandversorgung. URL: http://www.zukunft-breitband.de [Accessed: 12.01.2012]. [In German]

[Zei11].
Zeit Online: *Verräterisches Handy.*, February 2011. URL: http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten [Accessed: 12.01.2012. In German].

[Zil09].
Zillien, N.: *Digitale Ungleichheit: neue Technologien und alte Ungleichheiten in der Informations- und Wissensgesellschaft* (2nd edition), VS Verlag für Sozialwissenschaften 2009. [In German]

[ZPS+ 01].
Zerdick, A./Picot, A./Schrape, K./Artopé, A./Goldhammer, K./Heger, D./Lange, U./Vierkant, E./Lopez-Escobar, E./Silverstone, R.: *Die Internet-Ökonomie: Strategien für die digitale Wirtschaft* (Volume 7 in the European Communication Council Report series, 3rd extended and revised edition), Heidelberg inter alia: Springer 2001. [In German. Available in English under the title E-conomics. Strategies for the Digital Marketplace, Heidelberg inter alia: Springer 2000]

LIST OF ILLUSTRATIONS

ABOUT THE AUTHORS

Dr. Eva Geisberger studied computer science and psychology at the Technische Universität München and gained a doctorate in requirements engineering for embedded systems. In addition to her involvement in a variety of interdisciplinary research partnership projects, she acts as a consultant on model-based requirements and systems analysis and strategic development for a number of global enterprises. Since 2009, she has been head of the Department of Software and Systems Engineering at the fortiss GmbH research institute, an associated institute of the Technische Universität München. Ms Geisberger was the scientific director of the BMBF project Integrated Research Agenda Cyber-Physical Systems.

Prof. Dr. Dr. h.c. Manfred Hans Bertold Broy is Professor of Computer Science at the Faculty of Computer Science of the Technische Universität München where he holds the Chair of Software & Systems Engineering. Professor Broy has been awarded the Leibniz Prize, the Federal Cross of Merit and the Konrad Zuse Medal for his outstanding contributions in the field of computer science. Professor Broy is a Fellow of the Max Planck Society, a Member of the National Academy of Science and Engineering and a Member of the German National Academy of Sciences "Leopoldina". His main research interest is the role of software in a networked world.

Dr. María Victoria Cengarle studied computer science at the University of Buenos Aires and the Escuela Superior Latinoamericana de Informática (ESLAI) in Argentina, before obtaining a doctorate from the Ludwig-Maximilians-Universität München. She has worked as a research fellow at several different research institutes and has been involved in numerous national and international basic and applied research projects, as well as transfer projects. Some of the projects she has worked on are the standardisation of the Lisp programming language, Principles of Systems Engineering and the formal semantics of the UML and OCL modelling languages.

Patrick Keil studied economics and computer science at the Ludwig-Maximilians-Universität München. He is a research fellow at the Department of Software & Systems Engineering of the Technische Universität München and fortiss GmbH, and has been involved in numerous research and industrial projects. These include research into IT trends for the European Commission and the Federal Office for Information Security and a study of the IT system architecture of electric vehicles.

Jürgen Niehaus studied computer science and began his career as a research fellow and project leader at the University of Oldenburg. He has been CEO of the university's Research Center Safety-Critical Systems since 2004. In addition, since becoming CEO of the SafeTRANS Competence Cluster in 2006, he has been working on processes, methods and tools for the development of safety-critical systems.

Dr. Christian Thiel has a degree in computer science and obtained a doctorate in machine learning and pattern recognition from the University of Ulm. After working as a data mining and bid management expert for a start-up company in Passau, Mr Thiel moved to his current post of cluster project manager at BICCnet, the Bavarian Information and Communication Technology Cluster. In addition to organising working groups and events on a variety of topics, he is also responsible for the management of major projects such as agendaCPS.

Hans-Jürgen Thönnißen-Fries has a degree in computer science and is head of the Center of Competence Systems Engineering IT at ESG Elektroniksystem- und Logistik-GmbH in Fürstenfeldbruck. The Center's work focuses on system and software architectures, process modelling and engineering methods. In 2007, he also took up a position as the company's Corporate Technology Manager, with responsibility for technology and innovation management.

> THE FOLLOWING TITLES HAVE PREVIOUSLY BEEN PUBLISHED AS PART OF THE ACATECH STUDY SERIES AND ITS PREDECESSOR ACATECH REPORTS AND RECOMMENDS:

Appelrath, Hans-Jürgen/Kagermann, Henning/Mayer, Christoph (Ed.): *Future Energy Grid. Migration to the Internet of Energy* (acatech STUDY), Heidelberg inter alia: Springer Verlag 2012.

Spath, Dieter/Walter Achim (Ed.): *Driving German Innovation. The role of incubator organisations in the promotion of high-tech academic spin-offs* (acatech STUDY), Heidelberg inter alia: Springer Verlag 2012.

Hüttl, Reinhard. F./Bens, Oliver (Ed.): *Georesource Water – The Challenge of Global Change* (acatech STUDY), Heidelberg inter alia: Springer Verlag 2012.

acatech (Ed.): *Organic Electronics in Germany.* (acatech REPORTS AND RECOMMENDS, No. 6), Heidelberg inter alia: Springer Verlag 2011.

acatech (Ed.): *Monitoring of motivation concepts for technology students* (acatech REPORTS AND RECOMMENDS, No. 5), Heidelberg inter alia: Springer Verlag 2011.

acatech (Ed.): *Economic development of spin-offs from non-university research institutes* (acatech REPORTS AND RECOMMENDS, No. 4), Heidelberg inter alia: Springer Verlag 2010.

acatech (Ed.): *Recommendations on the Future of the Engineering Doctorate. Strategies for the further improvement and strengthening of the engineering doctorate at German universities* (acatech REPORTS AND RECOMMENDS, No. 3), Stuttgart: Fraunhofer IRB Verlag 2008.

acatech (Ed.): *Bachelor- und Masterstudiengänge in den Ingenieurwissenschaften. Die neue Herausforderung für Technische Hochschulen und Universitäten* (in German) (acatech REPORTS AND RECOMMENDS, No. 2), Stuttgart: Fraunhofer IRB Verlag 2006.

acatech (Ed.): *Mobility2020. Perspectives for tomorrow's traffic* (acatech REPORTS AND RECOMMENDS, No. 1), Stuttgart: Fraunhofer IRB Verlag 2006.

> acatech – NATIONAL ACADEMY OF SCIENCE AND ENGINEERING

acatech represents the German scientific and technological communities, at home and abroad. It is autonomous, independent and a non-profit organisation. As a working academic institution, acatech supports politics and society, providing qualified technical evaluations and forward-looking recommendations. Moreover, acatech resolves to facilitate knowledge transfer between science and industry, and to encourage the next generation of engineers. The Academy counts a number of eminent scientists from universities, research institutes and companies among its Members. acatech receives institutional funding from the national and state governments along with third-party donations and funding for specific projects. It organises symposiums, forums, panel discussions and workshops to promote new technologies in Germany and to demonstrate their potential for industry and society. acatech publishes studies, recommendations and statements for the general public. The Academy is composed of three bodies, the Members, organised in the General Assembly, the Senate, whose well-known figures from the worlds of science, industry and politics advise acatech on strategic issues and ensure dialogue with industry and other scientific organisations in Germany, and the Executive Board, which is appointed by the Members of the Academy and the Senate, and which guides the work of the Academy. acatech's head office is located in Munich while offices are also maintained in the capital, Berlin, and in Brussels.

For more information, please see www.acatech.de