Implementation Strategy Industrie 4.0

Report on the results of the Industrie 4.0 Platform

January 2016

Legal Notice

The Industrie 4.0 Platform (*Plattform Industrie 4.0 (2013-2015)*) is a joint project from the Bitkom e.V., VDMA e.V. and ZVEI e.V associations.

Published by

Bitkom e.V.
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstraße 10
10117 Berlin-Mitte

Tel.: 030.27576-0
bitkom@bitkom.org
www.bitkom.org

VDMA e.V.
Verband Deutscher Maschinen- und Anlagenbau e.V.
Lyoner Straße 18
60528 Frankfurt am Main

Tel.: 069.6603-0
kommunikation@vdma.org
www.vdma.org

ZVEI e.V.
Zentralverband Elektrotechnik- und
Elektronikindustrie e.V.
Lyoner Straße 9
60528 Frankfurt am Main

Tel.: 069.6302-0
zvei@zvei.org
www.zvei.org

Coordination, editing and proofreading

Wolfgang Dorst, Bitkom e.V.

Layout and typesetting

Astrid Scheibe, Bitkom e.V.

Graphics

Astrid Scheibe, Bitkom e.V.

Printing

Kehrberg Druck Produktion Service

Photo credits

Figure 17: Image source: Human beings orchestrating the value stream: FESTO AG & Co. KG; Figure 22: Machine image source: FESTO AG & Co. KG, image source for terminal block: PHOENIX CONTACT GmbH & Co. KG, image source for left electrical axis: FESTO AG & Co. KG, image source for right electrical axis: FESTO AG & Co. KG; Figures 24 and 31: Image source for machine 1 and 2: FESTO AG & Co. KG, image source for terminal block: PHOENIX CONTACT GmbH; Figure 25: Image source for left electrical axis: FESTO AG & Co. KG, image source for right electrical axis: FESTO AG & Co. KG; Figure 26: Sensor image source: Pepperl+Fuchs GmbH, image source for control unit: Bosch Rextoth AG, image source for left electrical axis: FESTO AG & Co. KG, image source for right electrical axis: FESTO AG & Co. KG; Figure 27: Configuration image source: FESTO AG & Co. KG, image source for manuals on left: FESTO AG & Co. KG, image source manuals on right: FESTO AG & Co. KG, image source for electrical axis, middle 1: FESTO AG & Co. KG, image source for electrical axis, middle 2: FESTO AG & Co. KG, image source for electrical axis, middle 3: FESTO AG & Co. KG, image source for electrical axis, middle 4: FESTO AG & Co. KG, image source for electrical axis, bottom 1: Pepperl+Fuchs GmbH, image source for electrical axis, bottom 2: FESTO AG & Co. KG; Figure 28: Machine image source: FESTO AG & Co. KG, image source for terminal block: PHOENIX CONTACT GmbH & Co. KG, image source for left electrical axis: FESTO AG & Co. KG, image source for right electrical axis: FESTO AG & Co. KG.

Published in April 2015

This publication is for general, non-binding informational purposes. The content reflects the view of the associations and companies participating in the "Industrie 4.0 Platform" project at the time of publication. Although the information contained herein has been compiled with the utmost care, no liability is assumed with respect to the correctness, completeness or up-to-datedness of the information. In particular, this publication cannot take into account the particularities of individual cases.

This publication, including all of its parts, is protected by German Copyright Law. Any form of commercialisation that is not expressly permitted by the German Copyright Act requires the prior consent of the publisher. This particularly applies with respect to duplication, editing, translations, microfilming as well as storage and processing on electronic systems.

Plattform
INDUSTRIE 4.0

Implementation Strategy Industrie 4.0

Report on the results of the Industrie 4.0 Platform

Umsetzungsstrategie Industrie 4.0

Ergebnisbericht der Plattform Industrie 4.0

(Translated Version)

Full Translation | Vollständige Übersetzung

Source Language: German | Ausgangssprache: Deutsch

Release Date and Place in the Original Language: April 2015, Berlin
Erscheinungsdatum und Ort in der Originalsprache: April 2015, Berlin

Translation plain text | Übersetzung Fließtext
wordic GmbH, Steindamm 103, 20099 Hamburg

Translation figures | Übersetzung Abbildungen
tsd Technik-Sprachdienst GmbH, Mittelstraße 12-14, 50672 Köln

Translation Layout and Typesetting | Layout und Satz der Übersetzung
Sabrina Flemming, Bitkom e.V.

ISBN 978-3-00-052211-6

January 2016 | Januar 2016

Sponsors of the Translation | Sponsoren der Übersetzung

KUKA

T · · Systems ·

Contents

1 Foreword 6

2 Overview of Industrie 4.0 8

2.1 Definition of Industrie 4.0 8

2.2 Strategy and goals 8

2.3 Benefit 9

2.4 Competition 10

3 Propositions from the scientific advisory board 12

4 Definition of Industrie 4.0 15

5 Research and innovation 18

5.1 Introduction 18

5.2 Topic: Horizontal integration via value networks 19

5.2.1 Methods for new business models 19

5.2.2 Value networks framework 20

5.2.3 Automation of value networks 21

5.3 Topic: End-to-end nature of engineering over the entire life cycle 23

5.3.1 Integration of the real and virtual world 23

5.3.2 Systems engineering 25

5.4 Topic: Vertical integration and networked production systems 26

5.4.1 Sensor networks 26

5.4.2 Intelligence – flexibility – changeability 28

5.5 Topic: New social infrastructures for work 29

5.5.1 Multimodal assistance systems 29

5.5.2 Acceptance of technology and organisation of working practices 31

5.6 Topic: Cross-sectional technologies for Industrie 4.0 32

5.6.1 Network communication for Industrie 4.0 scenarios 32

5.6.2 Microelectronics 34

5.6.3 Safety and security 35

5.6.4 Data analysis 36

5.6.5 Syntax and semantics for Industrie 4.0 37

5.7 The dependencies and relevance of the topics 38

6 Reference architecture, standardisation 40

6.1 Introduction 40

6.2 The reference architecture model for Industrie 4.0 (RAMI4.0) 41

6.2.1 Requirements and objectives 41

6.2.2 Brief description of the reference architecture model 42

6.2.3 The layers of the reference architecture model 43

6.2.4 Life cycle and value stream 45

6.2.5 Hierarchy levels 46

6.3 Reference model for the Industrie 4.0 component 47

6.3.1 Integration in the discussion on Industrie 4.0 47

6.3.2 Relevant content from other working groups 48

6.3.3 The "Industrie 4.0 component" 50

6.4 Standardisation 63

6.4.1 Background 63

6.4.2 Standardisation as a driving force for innovation 64

6.4.3 Cooperation between the standardisation committees 65

6.4.4 Conclusions 68

6.5 Topic roadmap 69

7 Security of networked systems 71

7.1 Introduction 71

7.2 Assumptions, hypotheses and prerequisites 73

7.3 The Industrie 4.0 world of threat 76

7.3.1 Company assets 77

7.3.2 Availability and reliability 77

7.3.3 Safety as a goal 78

7.3.4 Integrity 78

7.3.5 Confidentiality 79

7.3.6 Manipulation (intended and unintended) 79

7.3.7 Identity theft 80

7.4 Protective goals for Industrie 4.0 and security requirements 80

7.4.1 General protection targets 81

7.4.2 Security-by-design for Industrie 4.0. 81

7.4.3 Identity management 82

7.4.4 Dynamic configurability of the value networks 82

7.4.5 Security for the virtual instance 83

7.4.6 Prevention and reaction 83

7.4.7 Awareness, training, further education 84

7.4.8 Handling 84

7.4.9 Standards and guidelines 84

7.5 Examples of IT security measures 85

7.5.1 Security architecture 85

7.5.2 Identity management 87

7.5.3 Cryptography – protection of confidentiality 88

7.5.4 Cryptography – integrity protection 88

7.5.5 Secure remote access and frequent updates 89

7.5.6 Processes and organisational measures 90

7.5.7 Awareness 91

7.5.8 Company-wide coverage 91

7.6 Outlook and requirements 92

8 Appendix 95

8.1 List of sources 95

8.2 Industrie 4.0 Glossary 95

8.3 Team of authors 96

Foreword

1 Foreword

The physical and virtual worlds are increasingly merging together. An growing number of physical objects have intelligent sensor and actuator technology and are being networked through the development of the Internet of Things. The availability of all relevant information in real time through the networking of all instances involved in value creation, as well as the ability to derive the best possible value stream from data at any time is triggering the next stage of the industrial revolution known as Industrie 4.0. This will influence the evolution of technologies and have revolutionary effects on existing business processes while enabling new business models. The focus is therefore on optimising the following core industrial processes: development, production, logistics and service.

This Industrie 4.0 implementation strategy was drawn up by the Industrie 4.0 Platform (organised by the associations Bitkom, VDMA, ZVEI) in partnership with companies from German industry as well as other associations. It therefore serves to prepare Germany and its industry for the challenges of the future.

The core elements of Industrie 4.0 will be described in Chapter 4. Chapter 5, "Research and innovation", will then determine important needs for research and describe them in the form of research roadmaps and specifications. The research roadmaps offer good guidelines for the effective further development of the Industrie 4.0 topic via appropriate measures and assistance from politics and business (top clusters, demo labs, demo systems, demo plants, etc.).

A reference architecture model for Industrie 4.0 (referred to in short as RAMI 4.0) will be presented in Chapter 6. It will describe the structure of the Industrie 4.0 components and how they work. Where relevant, parts of the reference architecture model and the Industrie 4.0 components are based on existing and relevant standards so as to permit quick action. Any additional need for standardisation in connection with the implementation strategy will be identified and described when applicable.

Special security requirements arise due to increased networking and controllability of physical objects as well as the growing threat of hackers, intelligence services, espionage etc. These are outlined in Chapter 7.

The implementation strategy addresses readers from German industry, the relevant high-tech sectors, research and politics. In particular, managers, specialists and advisers are addressed as are all persons interested in or who would like to help shape the forwarding-looking vision embodied by Industrie 4.0 in Germany.

Overview of Industrie 4.0

2 Overview of Industrie 4.0

2.1 Definition of Industrie 4.0

The term Industrie 4.0 stands for the fourth industrial revolution, the next stage in the organisation and control of the entire value stream along the life cycle of a product. This cycle is based on increasingly individualised customer wishes and ranges from the idea, the order, development, production, and delivery to the end customer through to recycling and related services.

Fundamental here is the availability of all relevant information in real-time through the networking of all instances involved in value creation as well as the ability to derive the best possible value stream from data at all times. Connecting people, objects and systems leads to the creation of dynamic, self-organised, cross-organisational, real-time optimised value networks, which can be optimised according to a range of criteria such as costs, availability and consumption of resources.

2.2 Strategy and goals

The industry associations Bitkom, VDMA and ZVEI established the joint initiative Industrie 4.0 Platform to continue the activities of the German Science and Industry Research Union (Forschungsunion Wirtschaft-Wissenschaft) and to develop a coordinated, cross-sector course of action. The most important objective of the Industrie 4.0 Platform is for the associations BITKOM, VDMA and ZVEI to promote the vision of Industrie 4.0 to industry. This will secure and expand Germany's future as a manufacturing centre.

The final report of the German Science and Industry Research Union on Industrie 4.0 from April 2013 provides implementation recommendations [3], explains needs for research, and identifies eights areas for action which are listed here – supplemented with one usage aspect – to illustrate the initial situation:

1. Standardisation
   Open standards for a reference architecture
   Allows cross-organisational networking and integration via value networks.
2. Management of complex systems
   Use of models for automating activities as well as the integration of the digital and actual world.
3. Area-wide broadband infrastructure for industry
   Assurance of the requirements of Industrie 4.0 for the exchange of data in terms of volume, quality and time.
4. Safety
   The goal here is to guarantee operational safety, data privacy and IT security.
5. Work organisation and workplace design
   Clarification of implications for people and employees as planners and decision-makers in Industrie 4.0 scenarios.
6. Training and further training
   Formulation of content as well as innovative approaches for training and further training.
7. Legal framework conditions
   The goal is to create the necessary legal framework conditions for Industrie 4.0 with Europe-wide uniformity to the extent possible (protection of digital assets, contract law for contracts signed between systems, liability issues, ...).
8. Resource efficiency
   Responsible handling of all resources (human and financial resources as well as raw materials and operating supplies) as a success factor for future industrial production.

In order to transform industrial production to Industrie 4.0, a dual strategy will be pursued in Germany:

- The German equipment industry will continue to be a leader on the world market by becoming the foremost provider of intelligent production technologies through the dedicated consolidation of information and communication technology and the typical high-tech strategies they use. New leading markets for CPS technologies[1] and products must be defined and harnessed.
- At the same time, the continued development of German manufacturing by means of efficient, resource-saving production technologies will be required to make it both attractive and competitive. The goal is to expand the competitive advantages of companies in Germany through close physical proximity and active networking of users and manufacturers via the Internet. Automation, process and production technology in Germany will also benefit equally from this strategy.
- The path towards Industrie 4.0 is an evolutionary process. Existing basic technologies must be developed further to accumulate experience and gain insight with respect to optimising the entire value stream. Implementing new business models via online services has a disruptive element. Successful companies with good products or services and growing demand in their sales markets should adequately prepare themselves for change that may disrupt. Specifically, this refers to the further development of existing processes within the company as well as the development of new business models.

2.3 Benefit

This offers a broad range of benefits for participants along the entire value stream. The ability to accommodate individualised customer wishes is improved and the production of single units and very small quantities becomes more profitable. Flexibility increases through the dynamic design of business processes via the Internet in different dimensions, as well as through responsive engineering processes. The information made available by Industrie 4.0 combined with e.g. Big Data, Social Media and Cloud Computing permits optimal decision-making, early determining of design solutions and flexibility when responding to disruptions, as well as global optimisation of all resources across locations.

Production efficiency will increase – on the one hand through increased productivity and, on the other, through the efficient use of resources (machines, energy etc.).

New potential associated with new forms of value creation and employment arises; for example, downstream services, that is, services offered to users to complement the actual product after the product has left the production plant.

In view of the demographic changes, there are also benefits for structuring the way people work. Industrie 4.0 concepts can add value by supporting physical and mental abilities. In order to retain the knowledge and experience of employees with a high level of training in knowledge-based companies, Industrie 4.0 enables flexible and diverse career models in addition to management and specialist career paths. Social media will add flexibility to production and working-time planning. Production capacity will be optimised and resources will be used more effectively. It will also be possible to quickly respond to customer wishes. Last but not least, employees will be able to more effectively balance their work, family and leisure time through increased involvement in staff scheduling.

1 Definition from the implementation recommendations [3]: Cyber physical systems (CPS): CPS include embedded systems, production, logistics, engineering, coordination and management processes as well as Internet services that directly collect physical data with sensors and, using actuators, influence physical processes, are connected with one another via digital networks, use available data and services worldwide and have multimodal human-machine interfaces. Cyber physical systems are open socio-technical systems and permit a number of innovative functions, services and characteristics.

Industrie 4.0 increases Germany's competitiveness as a centre for high-wage jobs while making it possible for companies to position themselves as a leading provider, transforming Germany into the leading market for Industrie 4.0 solutions.

In Germany, our knowledge within the industrial sector, we have a decisive advantage, whether as leading companies, well established small and medium sized businesses, industry automation suppliers, IT companies, or toolmaking/machine-building – to name just a few.

2.4 Competition

Industrie 4.0 relies on secure communication and the cooperation of all participants across companies in real-time over the entire life cycle of the product; this will be made possible by Internet-based platforms. New, innovative value streams will build on these digital platforms and embody the benefits of Industrie 4.0.

The Industrie 4.0 Platform was created to address the task of jointly defining such secure "horizontal" cross-organisational communication and cooperation platforms and stipulating all framework conditions as well as further research requirements.

However, that is not all. The potential end-to-end nature of product, production and service with a respective virtual map of the physical world and its simulations have led to the development of new technologies.

Furthermore, improved vertical communication offers new possibilities for the meaningful and secure use of technologies of the "Internet of Things" in manufacturing.

The industrial companies of the Industrie 4.0 Platform, the scientific advisory board and sponsoring organisations BITKOM, VDMA and ZVEI have – in technology focused working groups – jointly evaluated necessary or suitable standards for a model of one or more reference architectures. They have also described the necessary framework conditions and identified promising fields of research. Based on knowledge generated with the Industrie 4.0 Platform to provide orientation, companies themselves can then choose to offer new value streams and innovative business models beyond the association platform, which will then compete with one another on the market.

The Industrie 4.0 Platform regularly coordinates with relevant committees and groups working on comparable topics which are relevant to individual aspects of its own work. Coordination occurs through appointed members with a relevant brief.

Propositions from the scientific advisory board

3 Propositions from the scientific advisory board

The scientific advisory board advises the Industrie 4.0 Platform on all scientific and program-related research questions while remaining in close contact with accompanying research. 16 professors from the fields of manufacturing and automation, information technology, law and the sociology of work are on the advisory board.

For the 2014 Hannover Messe (as of 3 April 2014), the scientific advisory board published its propositions [12] which are available to the public via the platform website. The propositions cited below are structured into the sections people, technology and organisation:

People

1. A wide variety of possibilities for a human-centred approach to work will arise,
   also in the sense of self-organisation and autonomy. In particular, this offers opportunities for organising working practices to account for aging and different age groups
2. Industrie 4.0 as a sociotechnical system offers the opportunity of expanding the range of tasks handled by employees, raising their level of qualifications and scope of action, and significantly increasing their access to knowledge.
3. "Learnstruments" and "communities of practice" increase productivity in both teaching and learning and new training content emerges with an increasing amount on IT skills.
4. Learning tools – practical artefacts that promote learning – automatically impart their functionality to the user.

Technology

5. Industrie 4.0 systems are easy to understand for the user, can be used intuitively, promote learning, and respond reliably.
6. Generally accessible solution strategies enable multitudes of participants to design, realise and operate Industrie 4.0 systems (Industrie 4.0 by design).
7. The networking and individualisation of products and business processes leads to complexity, which is managed by means of modelling, simulation and self-organisation. A greater scope for solutions can be analysed faster so that solutions can be found sooner.
8. Resource effectiveness and efficiency can be continuously planned, implemented, monitored and autonomously optimised.
9. Intelligent products are active information carriers, which are addressable and identifiable throughout all life cycle phases.
10. System components are also addressable and identifiable inside production means. They support the virtual planning of production systems and processes.
11. New system components have at least the abilities of the ones being replaced and are able to assume their function in a compatible manner.
12. System components offer their functions as services, which others can access.
13. A new security culture will lead to trustworthy, resilient and socially accepted Industrie 4.0 systems.

Organisation

14. New and established enhanced value networks integrate product, production and service while enabling dynamic variation with respect to the division of labour.

15. Cooperation and competition lead to new structures both at commercial and legal levels.

16. System structures and business processes can be mapped onto valid legal frameworks; new legal solutions permit new contractual models.

17. There are opportunities for arranging regional value creation – also in developing markets.

In a "Whitepaper on R&D topics", also published by the Platform for the 2014 Hannover Messe, different topics essential for the implementation of the propositions are presented both in terms of content and goals. A rough timeline for working through the topics is also described. Topics and timeline (see chapter 4 and 5) were incorporated in the work of the Platform working groups.

Implementation Strategy Industrie 4.0

4 Definition of Industrie 4.0

To strengthen Germany's position as a centre for business, the "Industrie 4.0 Platform" has the goal of drawing up an implementation strategy for Industrie 4.0. For this, a cross-sector approach to concepts for technology, standards, business and organisation models is being taken while universities, research institutes are closing ranks with small and medium-sized business as well as industrial companies, which are also pushing ahead with practical implementation .

Industrie 4.0 leads to new value streams and networks that are automated as a result of increasing digitalisation. The following areas are viewed as core components (see figure):

- Research and innovation.
- Reference architecture and standardisation.
- Security of networked systems.

These are handled by specific working groups from the Industrie 4.0 Platform. This is accompanied by:

- Creation of legal framework conditions.

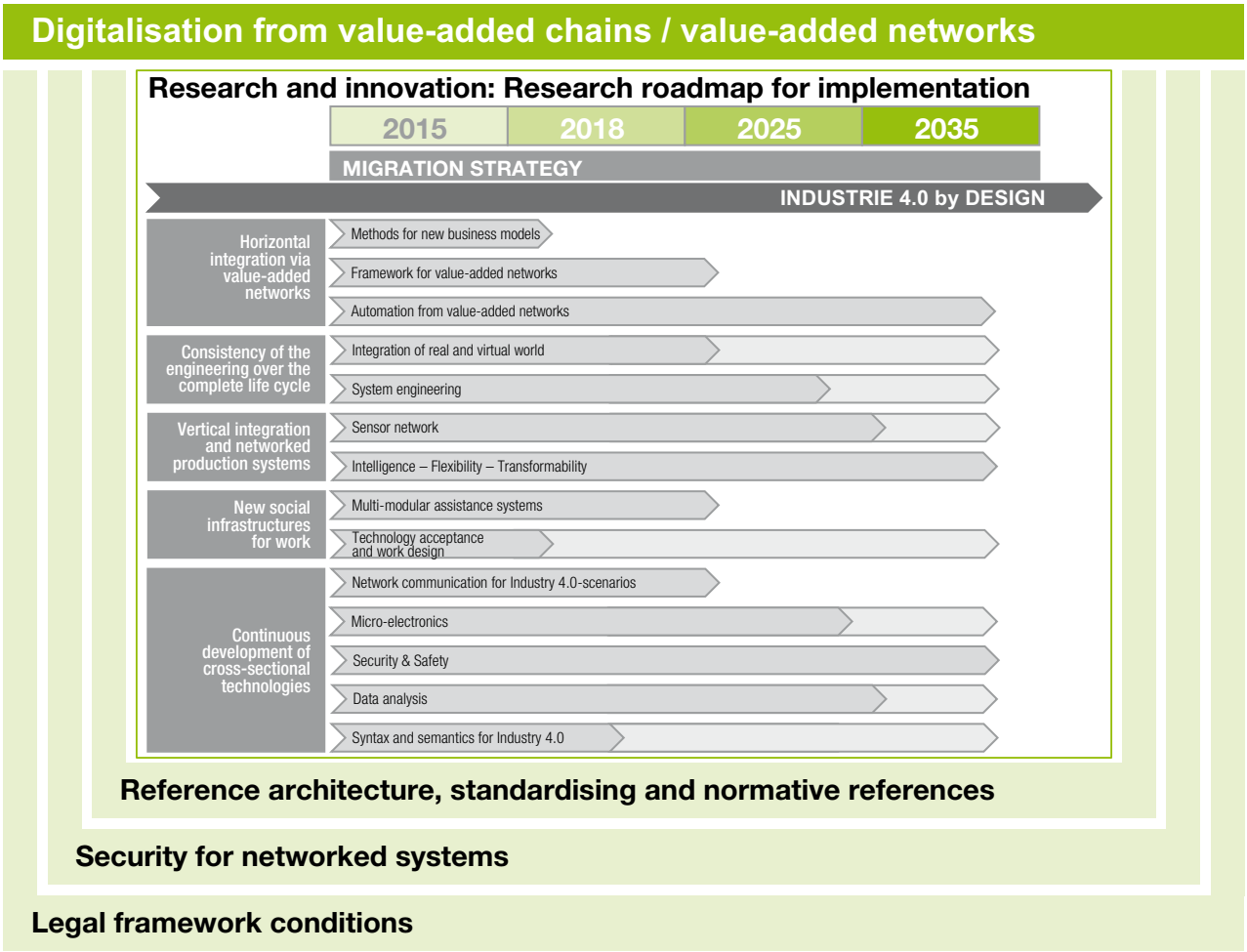


Figure 1: Core components of Industrie 4.0

This topic will not be addressed by the Industrie 4.0 Platform but dealt with specifically by working groups from the BDI.

In the field of research and innovation, the roadmap required for the implementation of Industrie 4.0 will be drawn up in coordination with the scientific advisory board; the required innovation and research activities as well as their support will be agreed and coordinated from an industry perspective. The most important topics in this respect are (see Chapter 5):

- Horizontal integration via value creation networks
  The focus lies on working out the collaboration across companies (suppliers, small and medium-sized businesses, production industry – to name just a few). This includes aspects and methods for new business models.
- End-to-end nature of engineering over the entire life cycle
  Central topics here are PLM-based engineering which links product and production design enabling consistent support along the entire value stream. This addresses technical points such as the integrated assessment of systems, engineering, modelling and simulation.
- Vertical integration and networked production systems
  The core topic in this respect is the networking of production which in many cases also entails real-time requirements. Important points here is that the necessary adaptability and production-related security requirements (e.g. redundancy and fault tolerance) are upheld and assured. This requires both the further development of the corresponding components and systems, e.g. sensor networks, as well as of methods such as predictive analytics.
- New social infrastructures for work
  The key factor for success is, and continues to be, people. As a result, ensuring that work life develops in a positive manner, supported and driven forward by all participants (unions and employer associations among others), is of crucial importance. In addition to changing and improving training and further training, there are technical aspects such as the introduction of new human-to-machine systems and assistance systems in general.
- Continual development of cross-sectional technologies
  Different technological prerequisites must be established and applied on an industrial level in order to implement Industrie 4.0. Important technologies include network communication, broadband networking, cloud computing, data analytics, cyber security, secure terminal devices as well as machine-to-machine solutions (including semantics).

The range of topics on reference architectures and standardisation concern the creation of a solution-neutral reference architecture while using and setting down standards (see Chapter 6).

With respect to the security of networked systems, work on concepts is being done using example value streams to ensure IT security within horizontal (customers/suppliers) and vertical (internal company) networking. This serves to identify general requirements and security principles (see Chapter 7). These are then worked out in an iterative process that also includes research and standardisation to contribute to the creation of an Industrie 4.0 reference architecture.

The topic of legal framework conditions addresses designs of the new production processes and horizontal business networks that adhere to legislative requirements. Challenges include contract law (dynamic conclusion in automated value streams), corporate data protection, handling digital assets, questions of liability and handling of personal data.

Research and innovation

5 Research and innovation

5.1 Introduction

The Industrie 4.0 Platform favours bundling Industrie 4.0 research activities more clearly than in the past and handling them on the basis of a structured, prioritised research agenda. The research roadmaps presented by the association platform in this chapter serve as a basis. Furthermore, a government budget is required for funding implementation of pending research work, a budget that reflects the potential of this topic and is competitive in an international comparison. It will supplement the significant resources already contributed by the participating companies and is an important prerequisite for the strategic processing of pending tasks for swift implementation of Industrie 4.0.

Political representatives must support, intensify and demand further networking and cooperation between companies and science as well as between companies of different sizes and from different sectors with suitable measures and assistance (top clusters, demo labs, demo systems, demo plants etc.).

Finally, Industrie 4.0 cannot be reached through a government managed implementation of a prescribed roadmap, mainly due to the difficulty in defining an exact vision of Industrie 4.0 because of the different interests and views of the range of businesses. Industrie 4.0 will be more the result of incremental progress on implementing specific applications (including analysis of the potential benefits and potential for value creation). It would also be desirable if the federal government considered funding such projects that have a more practice-based nature. Funding would therefore support the entire innovation path: from research into new methods and technologies and their use in university-affiliated demo systems and industry-affiliated pilot plants.

This chapter describes the research and innovation topics relating to Industrie 4.0. and is based, among other things, on the propositions of the scientific advisory board. The initial results have already been published in the "Whitepaper on R&D topics" for the 2014 Hannover Messe. Since then, work on the specifics of relevant topics has continued. The revised version of February 2015 will be documented below (more detailed fact files exist for the respective topics and go beyond the content described in this document; each fact file is updated within the Industrie 4.0 Platform working groups). At the same time, a new version of the "Whitepaper on R&D topics" will also be published in the first half of 2015 and will explore these topics in greater detail.

For each topic, the following briefly explains the (1) content of research and innovation, (2) the targeted outcomes, and the (3) key milestones.

5.2 Topic: Horizontal integration via value networks

We define horizontal integration as the integration of various IT systems for the support and/or execution of the different value processes (e.g. manufacturing, logistics, marketing, engineering, services) both within a manufacturing company as well as beyond company limits up to and including an end-to-end solution.

5.2.1 Methods for new business models

5.2.1.1 Content of research and innovation

A business model is a simplified representation on how business and value creation within a company works. It is therefore an abstract description on how money is earned, with which partners, in which markets and with which customer groups. In the context of Industrie 4.0, new business models will arise within companies based on new value processes and changing role allocations in value networks.

The following aspects to be considered are:

- Go-to-market strategies (GTMs)
- Methods for needs analysis and generation as well as the determination of potential
- Payment and billing models
- Benefit and risk assessment for each individual participant in the network
- Legal aspects
- Incentive and acceptance systems

5.2.1.2 Targeted outcomes for research and innovation

A joint understanding of the business models is a prerequisite for the long-term utilisation of potential for cross-company networking. Methods should be unified and consolidated, best practices and experiences – particularly from each of the different branches – are to be systematically documented. A transfer to production and the analysis of the resulting consequences occurs. The different roles within value networks must be considered in the process.

The following outcomes are expected:

- Examples of go-to-market strategies, derived from best practices, for the different provider roles within a network
- A business model strategy aligned with the needs of Industrie 4.0 which considers the aspects of value networks
- Examples of payment, billing and licence models
- Guidelines for the evaluation of typical benefits of Industrie 4.0 along with corresponding risks
- Guidelines for legal aspects (including liability issues, particularly with respect to service level agreements (SLAs) for software as a service (SaaS) and platform as a service (PaaS)).

5.2.1.3 Key milestones

Methodology
1.4 Principle guidelines for evaluating the Industrie 4.0 typical utilisation and the risks 1.5 Principle guidelines for legal aspects
Solutions
1.1 Best practices and experience as well as transferring to production 1.2 Exemplary Go-to-Market approaches 1.3 Exemplary methods for payment, invoicing and licensing 1.6 Business model approaches defined on Industrie 4.0 with consideration for the aspect of "value-added networks" 1.7 Piloting (new) strategies, models and processes for business
Prerequisites
2.3 Reference architecture for value-added networks for different organisational forms

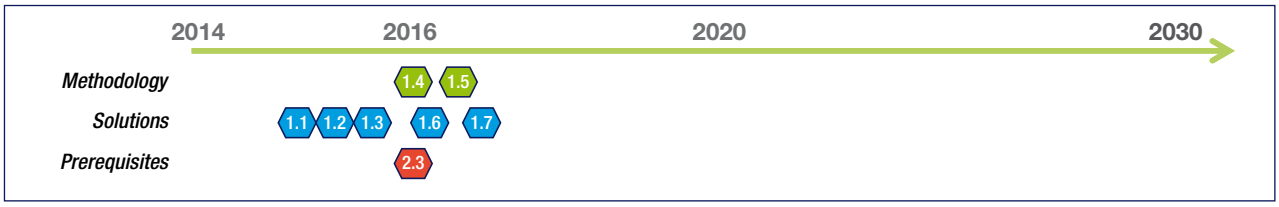


Figure 2: Milestones for research on methods for new business models

5.2.2 Value networks framework

5.2.2.1 Content of research and innovation

A value network describes a system consisting of individual value creation processes and their process-related dependency. The individual value creation processes are implemented by autonomous, legally independent participants. Complex reciprocal relationships connect them via the value network; they form a community of interests of value partners oriented towards sustainable, economical added value.

The following aspects to be considered are:

- Prerequisites, drivers, consequences for the creation of new value networks
- Economic role of CPS platforms as an integrator of value networks
- Possible business hazards and resulting consequences
- Organisational forms of value networks, their various components, roles and legal implementation

5.2.2.2 Targeted outcomes for research and innovation

Concepts for implementing value networks should be created and deployed in pilot projects so that topics such as (new) business strategies, models and processes can be elaborated in a practical manner with greater involvement of customers, suppliers, partners and the market. Business plans will be drawn up for specific examples and experiences in terms of "orchestration" which will also be published as future requirements on CPS platforms to support value networks.

The following outcomes are expected:

- The flexible integration of value networks in production
- Methods for analysing and evaluating economic and technological potential from the perspective of the network partners and their customers
- Mobilising, particularly small and medium-sized businesses, to cooperate in the networks

- Creation of new business opportunities
- Win-win value creation partnerships and the subsequent "integrated" business models

5.2.2.3 Key milestones

Methodology
2.1 Formal description and standards (semantics) for individual process stages in a uniform model 2.2 Formal description and standards (semantics) for interfaces and the whole network in a uniform model 2.3 Reference architecture for value-added networks for different organisational forms 2.4 Analysis and evaluation of the economic and technological potential for linked value-added networks 2.5 Principle guideline prerequisites, driving forces, consequences and approaches for implementation 2.6 Requirements for CPS-Platforms for supporting value-added networks
Solutions
2.7 Generally valid uniform model 2.8 Fundamental knowledge of conjunctions between models, prerequisites, driving forces and consequences
Prerequisites
1.6 Business model approaches defined on Industrie 4.0 with consideration for the aspect of "value-added networks"

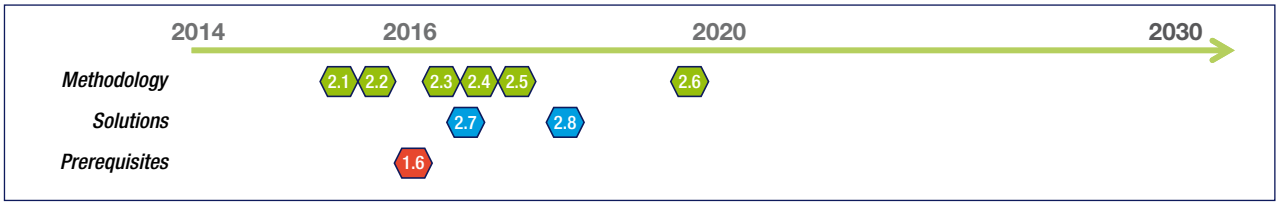


Figure 3: Milestones for research on the topic of "value networks framework"

5.2.3 Automation of value networks

5.2.3.1 Content of research and innovation

The degree of automation of horizontal integration is increased by automatic processing of the value creation stages. Prioritised here are those stages where value creation is performed automatically or in a purely "digital" world.

The following aspects to be considered are:

- End-to-end nature of information flows
- Use of methods for modelling, calculation, simulation and optimisation
- Integration of applications such as PLM, APS, MES, SCM and ERP
- Involvement of people as creative actors in the global value steam
- Design of a human-machine interface
- Dependency of qualification measures and migration processes

5.2.3.2 Targeted outcomes for research and innovation

Value creation should be performed more efficiently and flexibly; it should also be predictable. People are relieved of non-creative tasks. Increase in productivity, resource efficiency and automation are the focus. The further automation of individual sub-steps of complex planning processes optimises – in respect of globally definable targets – higher-level value streams and networks as well as operational activities.

Dependencies are considered in the process and synergy effects are generated. This will be made possible either through the integration of processes that were previously organised hierarchically and sequentially, and, in part, through synchronous or autonomous execution.

The following outcomes are expected:

- A method that describes direct and indirect relationships as well as dependencies of all corporate processes (e.g. PLM, ERP, APS, MES)
- A common system for a hierarchy of targets that references the effects of all tasks and processes for globally defined targets
- Processes and tasks that are designed in consideration of the aforementioned relationships and dependencies with respect to the most optimal compliance with global targets
- Autonomously described modules that can be applied and integrated in a simple manner
- Tools and programs that assist users through simple, intuitive presentation and continuous simulation options

5.2.3.3 Key milestones

Methodology
3.1 Optimisation methods 3.2 Strategic specifications – Objectives for hierarchy systems – Process modelling 3.3 Mastering complexities and applicability 3.4 Consistent transparency about the current and planned status of all process stages
Solutions
3.5 Piloting strategies, models and processes for business with consideration of the customers, suppliers, partners and market 3.6 consistent integration and flexible linking for added-value networks and optimal decisions
Prerequisites
2.1 Formal description and standards (semantics) for individual process stages in a uniform model 2.2 Formal description and standards (semantics) for interfaces and information flow in a uniform model 2.3 Reference architecture for value-added networks for different organisational forms 2.8 Fundamental knowledge for conjunction, models, prerequisites, driving forces and consequences

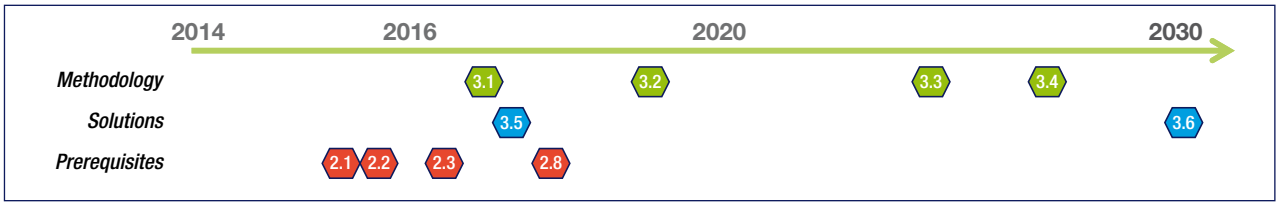


Figure 4: Milestones for research on the automation of value networks

5.3 Topic: End-to-end nature of engineering over the entire life cycle

We define the life cycle of a product as its development as well as engineering of the corresponding production system, the manufacture of the product by the production system, the use of the manufactured product by the user, and the product's recycling and/or dismantling. All information generated over this life cycle must be linked end-to-end.

5.3.1 Integration of the real and virtual world

5.3.1.1 Content of research and innovation

Industrie 4.0 is focusing to an increasing degree on the interplay of the real and virtual/digital world. All objects have a digital copy (model). In this context, the real world is generally characterised by problems to be solved and decision-making processes. The major elements of the virtual/digital world are simulations, planning and descriptive models. In addition, co-modelling essentially considers the interfaces between the two worlds on different scales.

Planning models form the basis to enable the creation of complex systems. Explanatory models permit the analysis of complex systems and therefore lead to solutions or decisions through a human transfer process. With both model strategies, the virtual world exerts a significant influence on the design of the real world. At the same time, the issues for which models are constructed, as well as the requirements or goals to be accounted for, lie in the real world and consequently influence the virtual world.

A scientific foundation, in the sense of production-related modelling theory for machine and plant building, is needed in this respect. Proven theories, descriptive tools and methods including associated basic information technologies must be renewed through appropriate adaptation, expansion and combination for widespread use in engineering disciplines. Integration – which properly addresses needs– in known, domain-specific work strategies and software tools plays a key role in this respect.

The following aspects to be considered are:

- Modelling theory must form the basis for providing in-depth answers to questions such as "What makes good models?" (including uncertainty estimates), "How do I find the right models?", "What do I implement in the digital world and in the real world?" and "How can interfaces between the virtual and real world be defined?". Existing models must be considered in the process.
- In modelling theory, concepts and main ideas such as abstraction, universality, perspectives, dependencies, type vs. instance, modularisation, modelling depth, and model-driven architectures based on defined semantics must be stipulated.
- Profitability of modelling: In addition to the resources required for creating models, the use of models offering benefits must be considered over the entire life cycle. In this respect, it is of considerable interest as to how models can "grow" over the course of their lifetime. Enhancement from existing data sources, while maintaining references for subsequent consistent assignment, also constitutes another relevant aspect.

The following concrete outcomes must be achieved:

- Modelling theory including the requirements for tools and data and/or information flows (at all levels on the automation pyramid)
- Methods for proving profitability as well as case studies
- Feasible modelling guidelines
- A general, tool-assisted meta model

5.3.1.2 Targeted outcomes for research and innovation

The required basis is a uniform understanding of models in machine-building, electrical engineering and information technology in the production environment. The long-term goal is to enable production businesses to perform profitable, beneficial and bidirectional modelling. This means that elements from virtual worlds can be linked in an interdisciplinary way to the real world on an advanced semantic level to significantly increase the efficiency of internal order processing as well as the certainty of decision making.

The following outcomes are expected:

- Modelling theory including the requirements for tools and data and/or information flows (at all levels on the automation pyramid)
- Methods for proving profitability as well as case studies
- Feasible modelling guidelines
- General, tool-assisted meta model

5.3.1.3 Key milestones

Methodology
4.1 First version of a modelling theory for complex systems including the requirements for tools 4.3 Practically workable application examples and modelling advances 4.4 Procedure for economical efficiency evidencing, single cases and/or application examples
Solutions
4.2 Identification of the "Best in Class" companies 4.5 First version of a modelling framework 4.6 General, tool-supported Meta-Model
Prerequisites
4.a Establishing a collective community 4.b Creating acceptance for modelling across the board 4.c Tools and methods for scaling the depth for models; ensuring vertical and horizontal consistency 4.d Concept for tool supporting when utilising initial reference architectures consistent with the real world

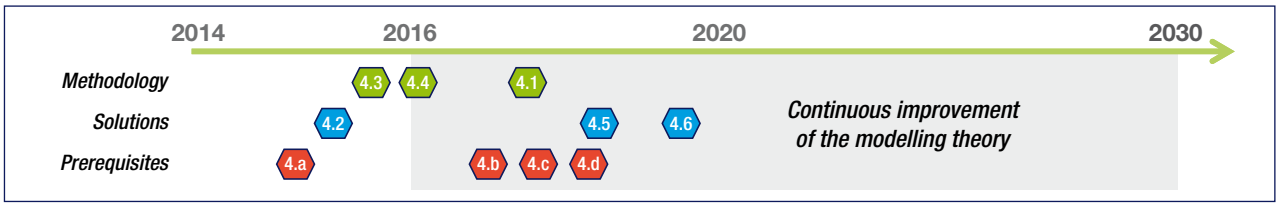


Figure 5: Milestones for research on the end-to-end nature of engineering over the entire life cycle

5.3.2 Systems engineering

5.3.2.1 Content of research and innovation

Systems engineering is a consistent, cross-disciplinary field for developing technical systems that take all aspects into consideration. It focuses on a multidisciplinary system and covers all development activities.

The following aspects to be considered are:

- Integrative development of products, processes and production systems. From the very beginning, all aspects must be developed in close interplay and continue to be developed over the product market cycle.
- Testing and validation of design decisions in "early" phases; also with respect to the intended functions which are subsequently implemented mechanically, electrically, with firmware, software or by service providers.
- Availability of all relevant data and processes external to system boundaries (sub-system, machine/process, production system, plant) and company boundaries as well as their provision in scalable systems
- Modularisation and reuse of plants and systems for managing increasing complexity and scalability
- Feedback of experience from the use of plants and systems concerning development and/or engineering and operation
- The methods used create an interoperable engineering chain which permits the secure use (exchange of data, role models, access methods) of engineering and simulation systems as well as systems used for operations, their embedding in business models (e.g. licenses, billing systems) in line with the respective versions

5.3.2.2 Targeted outcomes for research and innovation

The goal must be to have a comprehensive, interdisciplinary draft of a complex system in connection with the further determination of established development methods and the corresponding tool environments for the applicable domains such as mechanics, electrical engineering, software engineering as well as plant and process engineering.

Systems engineering – particularly for small and medium-sized businesses – should receive greater acceptance and be used in an increasingly cooperative way. The increasing complexity of Industrie 4.0 systems can then be managed to enable efficient as well as effective processing of projects in an engineering and production grouping.

The following outcomes are expected:

- Coordinated methods and coordinated tool chains and development environments
- System and location-independent use of tools
- Semantics of the applied interfaces
- Interdisciplinary, end-to-end requirement management in complex systems

5.3.2.3 Key milestones

Methodology
5.2 Practically workable guidelines as well as training and further education programmes 5.3 Continuous requirement management in complex systems throughout the vertical integration 5.6 Branch-independent reference model for developing more intelligent technical systems
Solutions
5.1 Initial jointly defined method set, initial jointly determined tool chain 5.4 System independent, mandate independent and location independent tool utilisation 5.5 Semantics for the applicable interfaces
Prerequisites
5.a Assigning technical and production-technical requirements in initial development stages 4.1 Initial modelling theory for developing complex automation and/or production-technical systems 5.c Discipline-collective modularisation for technical systems 5.d Expanding existing standards for production centralised descriptions for products

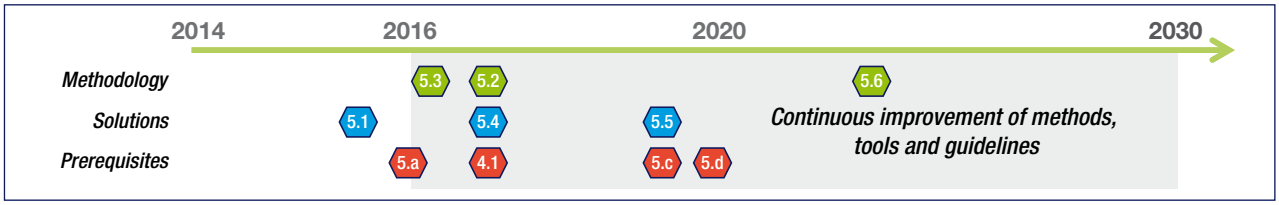


Figure 6: Milestones for research on the topic of "Systems Engineering"

5.4 Topic: Vertical integration and networked production systems

We define vertical integration as the integration of the different IT systems at different hierarchical levels of a production system (e.g., actuator and sensor, controller, production management, manufacturing, execution, and corporate planning levels) into an end-to-end solution.

5.4.1 Sensor networks

5.4.1.1 Content of research and innovation

The main motivation behind sensor data analysis is the continual collection of information via a (technical) process either as a basis for its control and regulation or for diagnosis, alerting etc. purposes. In the event, for example, of a reactive intervention, process parameters can then be adapted or, in machine-defect diagnoses, signalled.

Linking and evaluating the range of sensors (in part, under critical real-time conditions) is one of the main challenges.

The following questions must be considered:

- In practice, how can data acquisition be designed for large number of sensors?
- Where is it plausible to perform data manipulation?
- How can qualitative and quantitative relationships between the measured values and the effects that occur be recognised and transferred to a (status) model?

5.4.1.2 Targeted outcomes for research and innovation

A framework should be developed for implementing status-dependant monitoring and controls in Industrie 4.0 scenarios. Access to the main components (layers) belonging to sensor data processing should, to the extent possible, be standardised. Software architecture will be created that permits access to sensor data without requiring knowledge beyond the physical sensor level (encapsulation). In particular, the inclusion of cordless sensors must be considered. Commissioning and configuration should be implemented graphically and interactively using a plug-and-play approach. It must be made possible to analyse multiple sensor data flows according to data fusion without having to individually develop each application. In order to achieve the highest possible level of autonomy for the sensor network, the sensors are to be enriched with semantic descriptions (Semantic Sensor Network Technology).

The following outcomes are expected:

- Expanded and refined models for assessing the system/product status that make it possible to derive reliable recommendations for action
- Online regulation of a manufacturing process dependent on traced real-time data from the process as well as the quality of the process output
- Introduction of case-specific, adaptive measurement strategies in quality assurance
- Creation of a cross-industry community

5.4.1.3 Key milestones

Methodology
6.1 Transparent access to sensor data via universal interfaces / describing the sensors with meta data 6.3 Self-organising communications concept
Solutions
6.2 Inter-active commissioning process by utilising plug-and-play approach 6.4 Algorithms for decentralised data analysis (Fog-Computing), amalgamation with Cloud-Computing approach 6.5 Dynamic regulating of complex manufacturing processes, vertical integration with business economics processes
Prerequisites
6.a Local data recording, processing and saving in decentralised sensor nodes 6.b Networked production systems (Internet of Things and Services) 6.c Availability of self-sufficient energy sensors

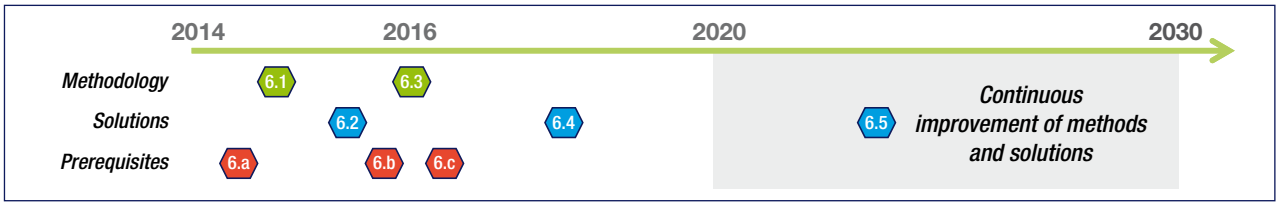


Figure 7: Milestones for research on sensor networks

5.4.2 Intelligence – flexibility – changeability

5.4.2.1 Content of research and innovation

Intelligent production systems are adaptive. This means they interact, based on integrated model knowledge, with their environment and adapt to it individually. They are robust. They also cope with unexpected situations – not necessarily considered by the developers – in a constantly changing environment without any reduction in performance levels. However, they also look ahead. They anticipate the effects of different factors based on experience-based knowledge. Finally, they are also user-friendly. They consider different behaviour patterns of users as well as the different needs for information, and independently adapt to it. Flexibility means that processes and/or systems are preconceived within defined and limited corridors in order to cover the broadest possible range of requirements. In a production environment, this corresponds to the flexible interplay of people, machines, production systems and value creation networks with respect to the production of different products and/or versions. Adaptability means shifting the limits of the flexibility corridor. As a result, processes and systems can be modified or converted in one constructive step. With respect to a machine in the production environment, this corresponds to "simple" retrofitting for the manufacture of new products and versions; with respect to a production system, this corresponds to "simply" changing the design.

The following aspects to be considered are:

- Identification, formalisation and description of the flexibility and adaptability options that directly and indirectly affect global goals
- Standardisation of interfaces and abilities of units/(modules) for creating flexible, adaptable production
- Social, ethical, ecological and ergonomic effects

Engineering and testing of autonomous systems in the production environment; the developers of autonomous systems must be properly trained and qualified

5.4.2.2 Targeted outcomes for research and innovation

Intelligence leads to new functionalities in products and production systems relieving their users as a result. Development, engineering, maintenance and life cycle management will be improved and the reliability, security and availability of products as well as production systems will be increased. Furthermore, resources such as energy and material will be used more efficiently, which enables extremely flexible, easily adaptable production processes and systems.

The following outcomes are expected:

- Identification of autonomous, reusable units (modules) within a production operation as well as derivation of requirements and potential for work models
- Robust, reliable algorithms for central and decentral intelligence
- Strategies for negotiating between intelligent systems in the production environment
- Technologies and application examples for intuitive human-machine interaction
- Migration strategies towards flexible, adaptable production

5.4.2.3 Key milestones

Methodology
7.1 Analysis for flexibility and transfer possibilities as well as their impact on working models
7.2 Migration strategies in the direction for a production that is flexible and transferable
7.3 Methods and description aids for the engineering and testing for autonomous systems
Solutions
7.4 Technological and application examples for an intuitive human-machine interaction
7.5 Standardising the cooperation between intelligent systems in the scope of production
7.6 Stable, reliable algorithms for centralised and decentralised intelligence
Prerequisites
3.2 Strategic provisions – objective hierarchy system – process modelling
9.5 Model for participation for the affected employee and the workers council in the implementation process for Industrie 4.0
3.3 Mastering complexities and applicability

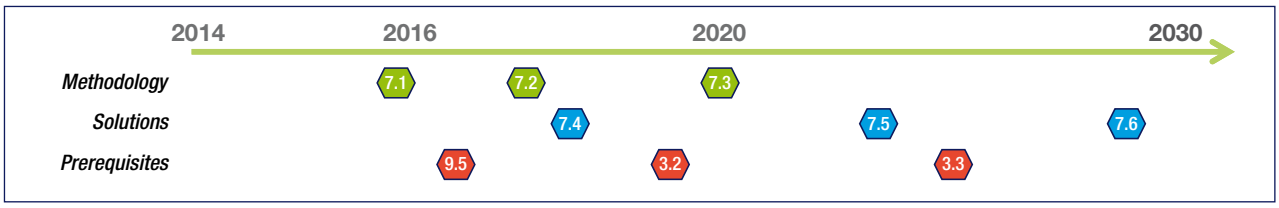


Figure 8: Milestones for research on intelligence – flexibility – adaptability

5.5 Topic: New social infrastructures for work

AG3 can only specify R&D requirements based on its expertise and experience. Topics covered in this section are therefore provided by the scientific advisory board.

5.5.1 Multimodal assistance systems

5.5.1.1 Content of research and innovation

In general, this field addresses the human-centric configuration for the human-machine interface. As part of Industrie 4.0, the basis of interaction between humans and technology will change: Machines will adapt to people – rather than the other way around. Intelligent industrial assistance systems with multimodal, easy-to-operate user interfaces can help employees with their work and introduce digital learning technologies directly to the workplace.

Aspects to be considered when devising interaction:

- Feasibility of inputs/outputs
- Perceptibility, also under unfavourable conditions
- Identifiability, disorientation-proof
- Appropriateness of tasks
- Self-explanatory capability
- Controllability
- Compliance with expectations

5.5.1.2 Targeted outcomes for research and innovation

In a factory, new forms of collaborative work will be created based on intelligent assistance systems. Methods and technologies associated with augmented reality, dual reality as well as synchronised and multiple worlds – that is, real-time synchronisation of sensomotoric and semantic factory

models with real factories – permit the collaborative teleoperation of highly complex components, e.g. when troubleshooting. As a result, how employees work together will change fundamentally. For example, cooperation and collaboration through adapted social networks and social media will also be possible beyond company and educational-level limitations. Easily adaptable interaction systems will account for heterogeneity within the workforce by being personalised and developed for special target groups.

The following outcomes are expected:

- Integration of virtual human models for supporting the simulation of automated production flows
- Prerequisites for the use and preservation of experience-based knowledge of employees as a condition for stable system operation
- Producing and assuring transparency concerning system status for employees
- Assuring qualification for all employee groups
  - Promotion of digital learning technologies
  - Further development of digital learning technologies

5.5.1.3 Key milestones

Methodology
8.1 Definition of industrial case applications for a meaningful multi-modular support for working stages 8.3 General methodology for evaluating the interaction
Solutions
8.2 Practical workable guidelines for a task-related interaction design in all stages of the production cycle 8.4 Specifying the design guidelines for a human-machine interface
Prerequisites
8.a Practical workable end-device for utilisation in an augmented reality and/or dual reality in the scope of application for the Industry 8.b Networking PLM systems and drafting engineering concepts for AR-/DR-Applications 8.c Acceptance for flexibility in employment conditions 8.d Acceptance of designs for interaction systems which will affect the heterogeneity of the staff 8.e Ensuring the access to qualifications for all employment groups

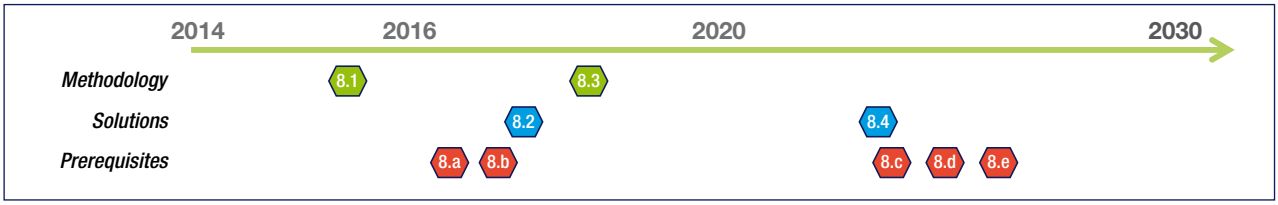


Figure 9: Milestones for research on multimodal assistance systems

5.5.2 Acceptance of technology and organisation of working practices

5.5.2.1 Content of research and innovation

Industrie 4.0 must be accepted by employees in production. This requires working conditions that permit flexibility for employees and promote their creativity as well as their ability to learn. "Multimodal assistance systems" will create the technological prerequisite for this. This topic also focuses on qualification development, work organisation and the design of work equipment in connection with Industrie 4.0 systems.

The following aspects to be considered are:

- Fundamental understanding of Industrie 4.0 as a socio-technical system where technology, organisation and personnel must be systematically coordinated with one another
- Organisation of working practices to promote acceptance, the ability to perform and develop, well-being as well as the health of working persons
- Involvement of employees and employee representation committees in the implementation process

5.5.2.2 Targeted outcomes for research and innovation

The range of tasks of employees will be expanded, their qualifications and scope for action will be increased with significantly enhanced access to knowledge. It can be assumed that innovative collaborative forms of production work will be possible and necessary for system-related reasons. As a result, Industrie 4.0 offers the chance to increase the attractiveness of production work and counteract the foreseeable skills shortage. Finally, by taking corresponding steps to re-organise working practices, conditions will be created to meet the growing challenges of an aging workforce.

The following outcomes are expected:

- Organisation of job and task structures based on acceptance, the ability to perform and develop, the health and well-being of workers
- Proposals for the integration of planning, organising, executing and controlling tasks at the workplace
- Models for an appropriate balance between less demanding routine tasks and more demanding problem-solving tasks
- Resources to promote learning to assist with work organisation
- Models for involving affected employees as well as the advisory board in the Industrie 4.0 implementation process

5.5.2.3 Key milestones

Methodology
-
Solutions
9.1 Ideas for suitable activity and task structures 9.2 Proposals for the integration of planning, organising, executing and supervisory activities 9.3 Models for reasonable relationship between tedious routine tasks and demanding tasks 9.4 Instructive working aids which support the working organisation 9.5 Models for involving the affected employee and the works council in the implementation process for Industrie 4.0
Prerequisites
-

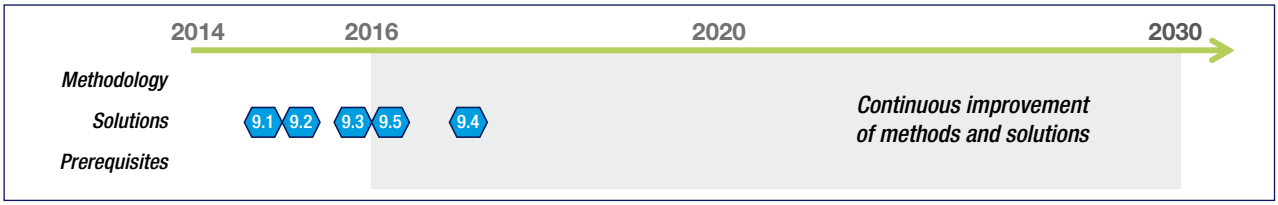


Figure 10: Milestones for research on the acceptance of technology and the organisation of working practices

5.6 Topic: Cross-sectional technologies for Industrie 4.0

The list of cross-sectional technologies in this chapter is not intended to be exhaustive and can be expanded. With respect to the addition of further technologies, it is important to clearly determine the significance of cross-sectional technologies especially for Industrie 4.0.

5.6.1 Network communication for Industrie 4.0 scenarios

5.6.1.1 Content of research and innovation

This topic addresses network communication between the stationary and mobile components involved in cyber-physical systems. These are the components, service and productive systems on the shop floor and in company background systems where data can be exchanged externally to linked supply chains and life cycle phases.

The following aspects to be considered are:

- Needs-oriented use of wireless communication in the office and shop floor environments
- Coexistence of a wide range of wireless and hard-wired communication systems and proprietary systems
- Interoperability of a wide range of wireless communication systems
- Forward-looking analysis of effects on changing system configurations
- Global use of products in the available bands
- Requirements management with respect to bandwidth, determinism and real-time
- Scalable, end-to-end use in an interoperable engineering chain
- Security and safety

5.6.1.2 Targeted outcomes for research and innovation

To fulfil the catalogue of requirements for use in Industrie 4.0 production scenarios, networking and connectivity solu-

tions for cross-industry use are to be developed and evaluated. Particular aims for this topic include requirements for data-transmission performance, robustness, security and safety as well as reliability, profitability and the capability for international rollouts.

The following outcomes are expected:

- Cost-efficiency and acceptance of Industrie 4.0 with standardised solutions whose standards take into account the goals of interoperability, scalability, cost sensitivity (e.g. including expensive sensors in small batches) as well as acceptance of requirements. Standards must be classified by mechanisms that can be applied to regular developmental processes and which do not contain cost-increasing certificates (which are neither technically nor spatially driven). Open methods such as the CE "Self-declaration of manufacturers" are therefore to be pursued.
- Evaluation of options for current and future
  - public networks in the context of Industrie 4.0
  - WLAN technologies and possible alternatives such as Bluetooth in an Industrie 4.0 context
  - Near-field technologies in the context of Industrie 4.0
- Identification of requirements for specific
  - wireless solutions, network technologies for public networks, proprietary solutions and identification of possible alternatives
  - Application fields such as buildings, process technology or infrastructure (energy, water, transportation)

5.6.1.3 Key milestones

Methodology
10.1 Redesigning public networks, deriving new radio technologies & frequency planning in public-private partnership 10.3 Standardising SDN-based virtualisation for network resources 10.5 Evolutionary development for radio standards, near field technologies and adaptable aerial systems
Solutions
10.2 100 Gbit/s 5G Network infrastructure in public networks is available 10.4 SDN in productive utilisation 10.6 Utilising new radio standards, near field technologies and adaptable aerial systems in I40 applications
Prerequisites
10.a Design and standardising of the 5G Network infrastructure as well as new radio standards and near field technologies 10.b Availability of standard hardware for SDN-based network virtualisation 10.c Industrialising new aerial technology for a flexible radio signal network 10.d Standardising new co-existence procedures including interference detection, interference suppression and preventing

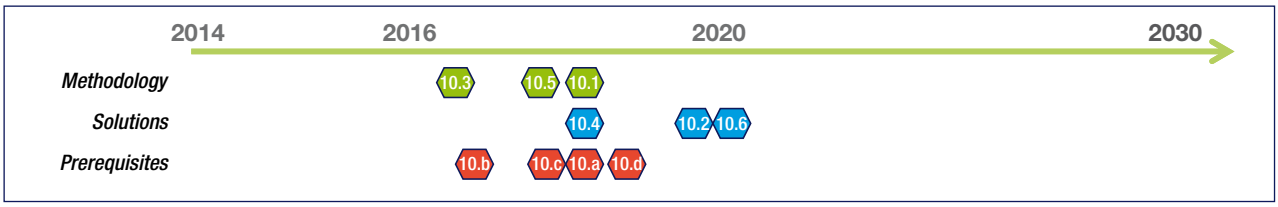


Figure 11: Milestones for research on network communication for Industrie 4.0 scenarios

5.6.2 Microelectronics

5.6.2.1 Content of research and innovation

Microelectronics is the basis for CPS hardware for intelligent control monitoring and identification of production and logistics processes in Industrie 4.0. It provides a comprehensive modular system for gradually implementing the elements of Industrie 4.0 scenarios. In this context, microelectronics stand both for "Moore" as well as for "More than Moore" technologies which receive special significance because technologies for system integration (e.g. 3D integration at the level of wafers, capacity for self-diagnostics, energy efficiency) play a key role here.

The most important research topics are:

- Micro-electro mechanical systems (MEMS) including sensors and actuators
- Embedded systems on chip including special processors, special real-time capable microcontrollers and high-tech storage offering high performance and minimal power consumption as well as multi-core architectures
- Power electronics for efficient running actuator systems
- Radio communication (low power, low latency)
- Energy harvesting with the greatest possible yield
- System integration
- Embedded IT security architecture
- Robustness and resistance to aging

5.6.2.2 Targeted outcomes for research and innovation

Microelectronics are one of the key technologies for achieving the Industrie 4.0 objectives such as flexibility, increased productivity and cost reduction. An optimised interplay of special electronic hardware and intelligent software is a prerequisite for this. The implementation of Industrie 4.0 scenarios depends on the availability of suitable microelectronic components and systems. As a result, there is a need for continual research and development in order to develop new components of micro-electronics and to adapt existing ones to the concrete requirements in the Industrie 4.0 environment.

5.6.2.3 Key milestones

Methodology
11.1 System integration 11.2 Stability and ageing resistance 11.3 Energy harvesting with the highest possible yield 11.4 Embedded systems on chip, special real-time capable micro-controller and high-technology storage
Solutions
11.5 Micro-electro-mechanical system (MEMS) including sensors and actuators 11.6 Embedded IT-Security 11.7 Power electronics for efficiently working actuator systems 11.8 Radio signal communication (low power, low latency)
Prerequisites
5.1 Initial jointly defined method set, initial jointly determined tool chain 10.5 Evolutionary development for radio standards, near field technologies and adaptable aerial systems

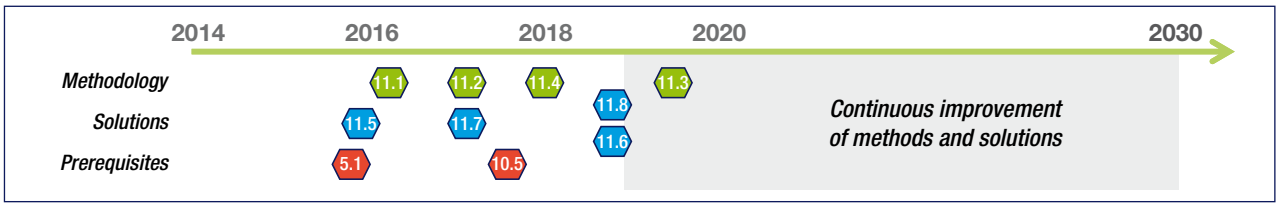


Figure 12: Milestones for research on micro-electronics

5.6.3 Safety and security

5.6.3.1 Content of research and innovation

Security ("information security") with respect to the availability, integrity and confidentiality of information in Industrie 4.0 facilities and systems. For security, the goal is to ward off risks that could affect a system and/or its functioning. This includes, in particular, intentional and non-intentional attacks. Information security must be assured for all functionalities, for operational functions as well as for monitoring and protective functions (e.g. safety).

Safety ("functional safety") for systems means ensuring, by taking suitable measures, that the function of a machine or a facility does not pose a risk for people or the environment. Safety is part of the protective functions for operational safety.

The following protection objectives must be considered for products, components and Industrie 4.0 systems:

- Availability and integrity
- Operational safety
- Expertise protection
- Data protection

Secure verification of identity is of crucial importance for Industrie 4.0.

The following aspects to be considered are:

- Measurement methods for threat potentials and risks including a cost/benefit analysis of security measures
- Protection of interfaces in external and internal dealings
- Protection of communication systems within the facility
- Effect of security loopholes on risks for operational security
- Correlation with legal requirements, e.g. concerning data protection
- Security by design
- Long-term feasibility of security solutions
- Detection and analysis of attacks

The following framework conditions must be considered in this respect:

- Alignment of security assessments to the affected horizontal and vertical value networks
- Alignment to specific use cases and real-time transfer to applicable events to demonstrate practical suitability
- Consideration of the "human factor": Transparency, usability, user acceptance, data protection

5.6.3.2 Targeted outcomes for research and innovation

A wide range of standards and technologies already exist today. However, to date these have been implemented only to a limited extent in an industrial environment. There are many reasons for this but the main purpose of automation solutions is not security functions. Security-related processes, development and production are becoming more expensive for providers and now require expertise that often does not exist. For operators, security concepts often pose corresponding hurdles with respect to expenditure and acceptance on the part of the operating personnel.

In order to achieve a high level of acceptance by all parties, solutions must be realised, which are user-friendly, have tools to aid developers and provide efficient methods for security evaluation.

The following outcomes are expected:

- User-friendly security methods
- Scalable security infrastructures for industrial domains
- Easy-to-use methods and measurement procedures with respect to the security characteristics of individual components and their combination to form an Industrie 4.0 facility "Plug&Operate" as well as the autonomous, dynamic configuration must be observed in the process

- Methods for the dynamic determination and evaluation of the safety functions of a facility while considering the effect of the achieved security level with respect to the residual risks in the sense of safety
- Preparation of security standardisation
- Creation of suitable catalogues of measures in the event security loopholes, e.g. in accordance with CERT methods

5.6.3.3 Key milestones

For the long-term planning of research on the topic of "Security and safety", milestones have not yet been defined for methods, solutions or the necessary prerequisites.

5.6.4 Data analysis

5.6.4.1 Content of research and innovation

On one hand, the main motivation for data analysis is the possibility of generating (new) knowledge. On the other hand, an "actionable" data analysis serves as a decision-making aid as well as autonomous decision-making (which information is provided to whom and when), which in turn helps companies to increase the quality of their products and the efficiency of their production as well as to quickly identify any undesirable developments. This also serves as a basis for new business models. Predictive analysis methods are used for this. They span a multitude of basic techniques from statistics, machine-based learning and data mining. Current and historical measurements as well as "unstructured" data such as data from social networks is analysed in order to identify unknown correlations (descriptive analytics) or also to derive estimates regarding future system behaviour and/or effects (predictive analytics). The newly acquired knowledge ultimately makes it possible to evaluate different action alternatives and, as a result, continual optimisation of systems, processes and strategies (prescriptive analytics). The actual challenge is the derivation of recommendations for action or direct measures based on data analysis.

The topic "data analysis" contains the following aspects:

- Data manipulation
- Status detection
- Prognostic assessment
- Advisory generation

5.6.4.2 Targeted outcomes for research and innovation

A catalogue of criteria is to be developed for the use of data analyses which permits implementation of the following principles:

- Access to data without knowledge of the specific (physical) origin (encapsulation and/or virtualisation)
- Inclusion of new data sources via standardised interfaces using the plug&use approach (semantic description)
- Use of data in a cross-industry value network
- A broad process basis that can be continually expanded will be created to make it possible to derive new applications
- Legal security (who has which rights to which data and the resulting findings)

Principles should also be developed which make it possible for software architecture and the corresponding interfaces to evaluate multiple data flows in the form of data fusion at a meta level without each application having to be individually developed.

- Models for describing statuses are to be developed which permit the prediction of future statuses
- Procedures and algorithms are to be developed which are capable of effectively and efficiently analysing continually increasing data quantities

5.6.4.3 Key milestones

Methodology
13.2 Application guideline for utilising data analysis in the production environment 13.4 Analytics technologies for on-line adjustment and optimising production processes
Solutions
13.1 Technology and application examples for data analysis 13.3 Algorithms for decentralised data analysis (Fog-Computing), amalgamation with Cloud-Computing approach 13.5 Dynamic regulating of complex manufacturing processes, vertical integration with business economics processes
Prerequisites
13.a Legal clarification for property rights and utilisation conditions for the data 13.b Theoretical fundamentals for descriptive, predictive and prescriptive analytics

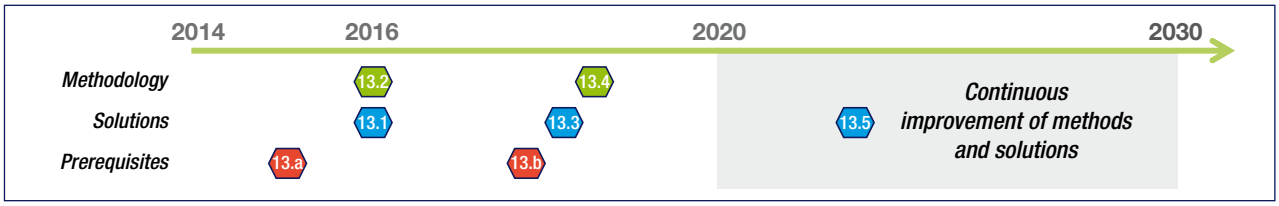


Figure 13: Milestones for research on the topic of "Data analysis"

5.6.5 Syntax and semantics for Industrie 4.0

5.6.5.1 Content of research and innovation

Realising Industrie 4.0 scenarios requires interpretation, i.e. identification and understanding, of the objects involved (e.g. machines, machine components, product and product descriptions or resources in the form of the digital factory) by the acting subjects (e.g. people, software tools, software agents, control systems, software services). This requires description of the relevant properties of the objects in the form of features in a model and of the tasks of the objects in relation to roles. The information models are the basis for this. In order for them to be processed in computers requires (data) models, model systems, explanatory models, planning models as well as component models in the production environment.

The syntax describes valid symbols that may be used for describing documents and data (e.g. letters, numbers, special characters, graphical symbols) and how these characters are correctly linked with one another into symbol chains.

The semantics creates a relationship between the symbols and models so that the symbol chains and/or data are provided with meaning, transforming the data into information. Such a relationship is, for example, the agreement that a certain string of characters in one file describes a certain feature of a model, the attributes this feature describes, and the manifestations these attributes may have. The interdependencies between the features and the attributes also have to be described.

5.6.5.2 Targeted outcomes for research and innovation

The goal is to develop a formal, computer-processable form of the description as common semantics for Industrie 4.0 and consequently to define a domain-specific "language" at the application and usage levels which can use all objects, subjects and their links (that is, processes, communication and value networks) in the group. At the same time, the task is to ensure the end-to-end nature of information flows in and between the value streams and to base them on the aforementioned existing standards, continue to develop them and fill any loopholes in standards that are found.

- Semantics and syntax form a substantial basic prerequisite for multi-manufacturer interoperability of data storage, data transfer and data processing
- Standardised semantic descriptions form the basis for self-optimising behaviour and the automation of value streams
- This permits the integration of models in the complete life cycle (because the description of the product, process and resources is in place in engineering as semantics)
- Generic tools and/or tool functionalities can be created with the help of syntax and semantics
- Semantics and syntax enable plug-and-produce functionalities for Industrie 4.0 components and as a result, flexibility and adaptability

The challenge will be, on one hand, to rapidly generate results when designing syntax and semantics for Industrie 4.0, and at the same time, to attain the greatest possible domain of applicability (in the form of an industry footprint).

5.7 The dependencies and relevance of the topics

The different research topics are not stand-alone in nature, but rather result in dependencies between the research findings. As a result, new findings in a field of research affect research in another field. In cooperation with the scientific advisory board, the AG3 is currently working on an analysis of the reciprocal influence and relevance of topics. In this respect, the methods of scenario analysis by Prof. Gausemeier are being used. The results of this analysis are to be published during the course of the year. However, it is already possible to determine that the research findings for the following topics have a considerable influence on other research findings:

- "Flexibility, intelligence and changeability"
- "Sensor networks"
- "Framework value networks"
- "Security and safety"

5.6.5.3 Key milestones

Methodology
14.8 Application guidelines with regard to utilising syntax and semantics with Industrie 4.0
Solutions
14.1 Actual value analysis for standardising/normative references in the scope for syntax and semantics 14.2 Actual value analysis for relevant concepts in the scope for syntax and semantics 14.3 Industrie 4.0-Requirement catalogue for syntax and semantics 14.4 Nominating research subjects on the basis of application cases and value-added chains 14.5 Loopholes in standards and assigning the relevant need for standardisation in standardising and normative reference roadmaps 14.6 Implementing selected inter-operability demonstrators 14.7 Integration concept in existing communication standards, conceptional expansion of software tools
Prerequisites
14.a Requirements for data and information models derived from application cases and value-added chains

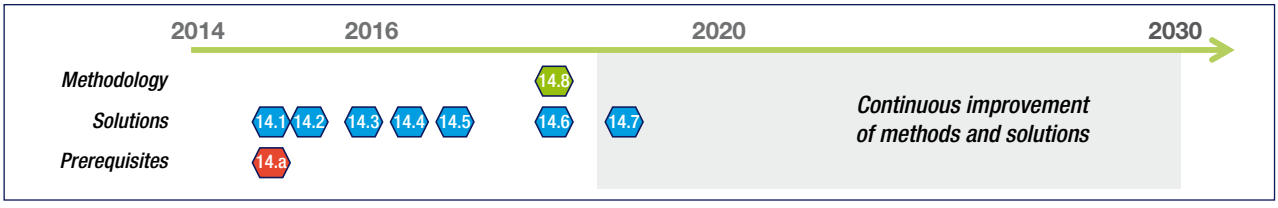


Figure 14: Milestones for research on syntax and semantics for Industrie 4.0

Reference architecture, Standardisation

6 Reference architecture, standardisation

The findings obtained in cooperation with multiple institutions[2] with respect to the underlying reference architecture for Industrie 4.0 as well as the derived needs for standardisation are summarised in this chapter.

The Industrie 4.0 Platform therefore had the role of coordinating activities in the numerous sub-boards and maintaining a consistent line. As such, the platform has fulfilled the task assigned to it of ensuring that a concerted approach is taken by a wide range of organisations and associations. The broad range of results presented below are therefore an important step towards upholding the competitiveness of German industry.

6.1 Introduction

One of the fundamental ideas regarding the reference architecture of Industrie 4.0 is the grouping of highly diverse aspects in a common model. Vertical integration within a factory describes the networking of means of production, e.g. automation devices or services. The inclusion of the product or workpiece is also a new aspect in Industrie 4.0, The corresponding model must reflect this aspect. But Industrie 4.0 goes considerably further. End-to-end engineering throughout the value stream means that the technical, administrative and commercial data created around the means of production or of the workpiece are kept consistent within the entire value stream and can be accessed via the network at all times. A third aspect of Industrie 4.0 is horizontal integration via added value networks extending beyond individual factory locations and facilitating the dynamic creation of such added value networks. The task to be performed was to represent these aspects in a model. Ultimately, closed loop control circuits with polling rates in milliseconds were to model dynamic cooperation between multiple factories within a common added value network with the inclusion of commercial factors. This required understanding of the perspectives of different application domains, identification of the fundamentals and unification in a common model.

Before work could commence on the reference architecture model RAMI4.0, it was therefore necessary to establish an overview of the existing approaches and methods. It rapidly became clear that there was already a series of existing and usable approaches but which, as a rule, only addressed partial aspects of the holistic view of Industrie 4.0 outlined above. The following individual aspects were considered in greater detail:

Approach for implementation of a communication layer

- OPC UA: IEC 62541 basis

Approach for implementation of an information layer

- IEC Common Data Dictionary (IEC 61360Series/ ISO13584-42)
- Characteristics, classification and tools to eCl@ss
- Electronic Device Description (EDD)
- Field device tool (FDT)

Approach for implementation of a functional and information layer

- Field device integration (FDI) as integration technology

2 The VDI and VDE experts working in the Society for Measurement and Automation Technology (GMA) served as excellent partners for developing the strategies. In particular, experts from the technical committees 7.21, "Industrie 4.0", and 7.20, "Cyber-Physical Systems" warrant mention.
At the same time, the SG2 mirror committee, which has also contributed to the group in terms of content, was formed in the ZVEI. The DKE (Deutsche Kommission Elektrotechnik) was also included in all work with corresponding representatives in the SG2 so that standardisation was also part of the group.

Approach for implementation of a functional and information layer

- AutomationML
- ProSTEP iViP
- eCl@ss (characteristics)

The first step was a fundamental examination of whether these approaches match the reference architecture model presented in the following chapter. It was found in principle that they do, although the concepts and methods considered still require more detailed examination.

6.2 The reference architecture model for Industrie 4.0 (RAMI4.0)

Highly divergent interests meet in the discussion concerning Industrie 4.0: Sectors ranging from process to factory automation with entirely differing standards, information and communication technologies and automatic control, the associations Bitkom, VDMA, ZVEI and VDI and the standardisation organisations IEC and ISO with their national mirror committees in DKE and DIN.

In order to achieve a common understanding of what standards, use cases, etc. are necessary for Industrie 4.0, it became necessary to develop a uniform architecture model as a reference, serving as a basis for the discussion of its interrelationships and details.

The result is the reference architecture model for Industrie 4.0 (RAMI4.0).

It contains the fundamental aspects of Industrie 4.0, and expands the hierarchy levels of IEC 62264 by adding the "product or workpiece" level at the bottom, and the “connected world” that extends individual factory boundaries at the top. The left horizontal axis is used to represent the life cycle of systems or products, also establishing the distinction between “type” and “instance”. Finally, the six layers define the structure of the IT representation of an Industrie 4.0 component.

The special characteristics of the reference architecture model are therefore its combination of life cycle and value stream with a hierarchically structured approach for the definition of Industrie 4.0 components. Maximum flexibility for the description of an Industrie 4.0 environment is provided in this way. The approach also permits encapsulation of functionalities where appropriate.

By means of the reference architecture model, the conditions have thus been created for the description and implementation of highly flexible concepts. In this context, the model permits gradual migration from the world of today to that of Industrie 4.0, and the definition of application domains with special stipulations and requirements.

The reference architecture model RAMI4.0 has been put forward for standardisation as DIN SPEC 91345.

6.2.1 Requirements and objectives

Objectives

Industrie 4.0 is a specialisation within the “Internet of Things and Services”. Around 15 industries have to be involved in the deliberations. Using the reference architecture model, tasks and workflows can be broken down into manageable parts. In this way, the subject matter is to be made so accessible that a productive discussion, e.g. on standardisation issues, becomes possible. The existing standards which come into question can then be identified, revealing where there may be a need for additions or amendments, or where standards are missing. Overlaps will also become transparent and open to discussion. If consideration of the model reveals that there are several standards for the same or similar matters, a preferred standard can be discussed within the scope of the reference architecture model.

The aim is to cover the issues with as few standards as possible.

Compliance with standards

The concepts and methods described in the standards selected are to be reviewed to ascertain the extent to which they are suitable for applications in the Industrie 4.0 environment. Implementation of a partial standard may be sufficient for an initial Industrie 4.0 application. This would speed up the implementation and introduction of non-proprietary solutions which are essential for Industrie 4.0, and would also enable smaller companies to adapt to Industrie 4.0 and master its challenges more rapidly.

Use cases

The reference architecture model also provides an opportunity to locate Industrie 4.0 use cases, for example, to identify the standards required for the relevant use case.

Identification of relationships

Various topics can be represented as subspaces of the reference architecture model. Industrie 4.0 essentially depends upon the ability to detect and process relationships, e.g. those between these subspaces, electronically.

Definition of higher-level rules

The reference architecture model permits a derivation of rules for the implementation of Industrie 4.0 applications at a higher level.

Overview of objectives:

- A simple and manageable architecture model as a reference
- Identification of existing standards
- Identification and closure of gaps and loopholes in standards
- Identification of overlaps and the setting down of preferred solutions
- Minimisation of the number of standards involved
- Identification of a standard's subsets for rapid implementation of partial content for Industrie 4.0 ("I4.0 ready")
- Identification of use case contents
- Identification of relationships
- Definition of higher-level rules

6.2.2 Brief description of the reference architecture model

A three-dimensional model is best suited to represent the Industrie 4.0 space. The basic features of the model reflect those of the Smart Grid Architecture Model (SGAM[3]), which was defined by the European Smart Grid Coordination Group (SG-CG) and is accepted worldwide. It was adapted and extended to meet Industrie 4.0 requirements.

Layers are used in the vertical axis to represent the various perspectives such as data maps, functional descriptions, communications behaviour, hardware/ assets or business processes. This corresponds to IT approaches where complex projects are split up into clusters of manageable parts.

A further important criterion is the product life cycle with the value streams it contains. This is displayed along the horizontal axis. Dependencies, e.g. constant data acquisition throughout the life cycle, can therefore also be well represented in the reference architecture model.

The third important criterion, represented in the third axis, is the location of functionalities and responsibilities within factories/ plants. This concerns a functional hierarchy and not the equipment classes or hierarchical levels of the classical automation pyramid.

3 CEN/CENELEC/ETSI SG-CG, Overview of SG-CG Methodologies, Version 3.0, Annex SGAM User Manual, 2014

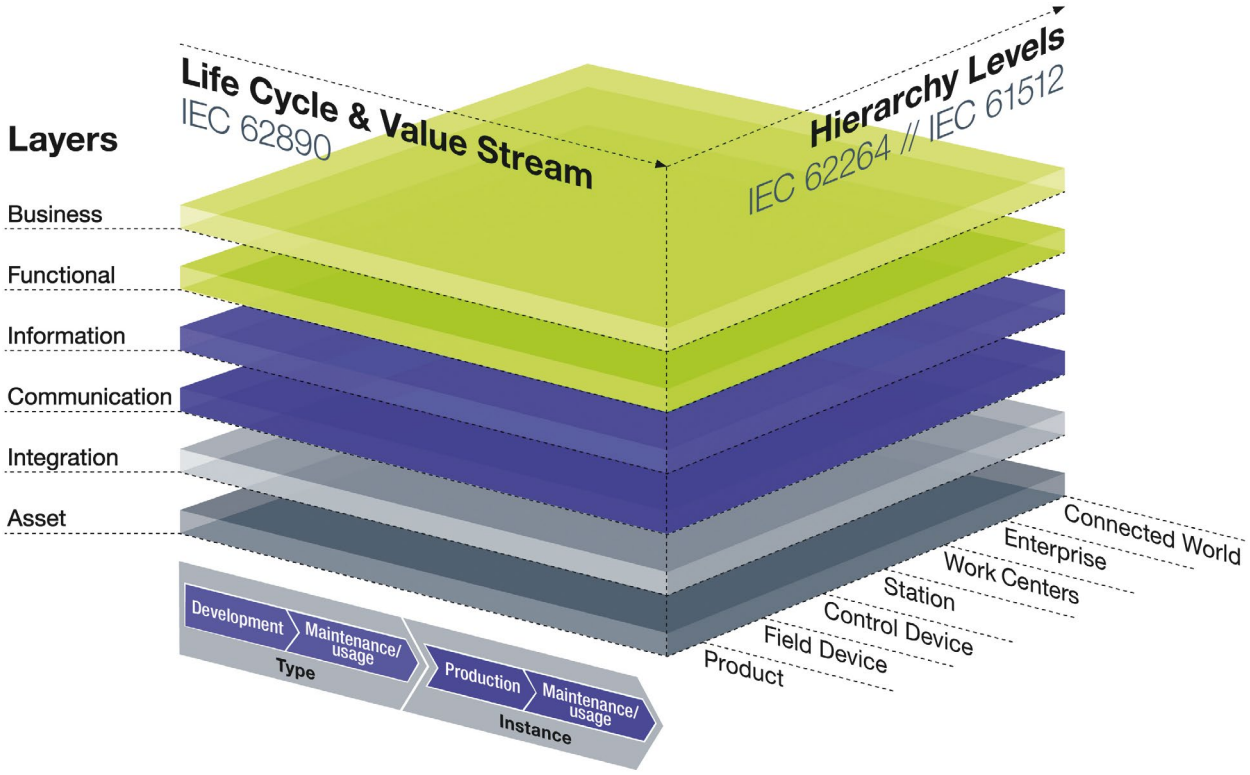


Figure 15: Reference Architecture Model Industrie 4.0 (RAMI 4.0)

6.2.3 The layers of the reference architecture model

The Smart Grid Architecture Model (SGAM) is a good starting point to describe the situation on hand. It deals with the electricity grid, from generation and transmission through to supply to the consumer. Industrie 4.0 focuses on product development and production scenarios. Consequently, it is necessary to describe how development processes, production lines, manufacturing machinery, field devices and the products themselves are configured and how they function.

For all components, no matter whether they are a machine or a product, it is not only the information and communication functionality which is of interest. In the simulation of a system, e.g. a complete machine, its cables, linear drive and also its mechanical structure are also considered. They are part of the reality without being able to actively communicate. Their information needs to be available as a "virtual representation". For that purpose they are, for example, passively connected to a database entry via a 2D code.

To enable an improved description of machines, components and factories, SGAM's component layer has been replaced by an asset layer at the bottom of the model with the newly inserted integration layer above. This permits digitisation of the assets for virtual representation. The communication layer deals with protocols and the transmission of data and files, the information layer contains the relevant data, the functional layer all the necessary (formally defined) functions, and the business layer maps the relevant business processes.

Note: *A high level of cohesion is to prevail within the layers, with loose connections between them. Events may only be exchanged between two adjacent layers and within each layer.*

Several systems are grouped together to form larger overall systems. Both the individual systems and the overall system must follow the reference architecture model. The contents of the layers must be compatible with each other.

The individual layers and their interrelationships are described below:

6.2.3.1 Business layer

- Ensuring the integrity of functions in the value stream.
- Mapping business models and the overall process emerging from it.
- Legal and regulatory framework conditions.
- Modelling of the rules the system has to follow.
- Orchestration of services in the functional layer.
- Link between different business processes.
- Receiving events for advancing of the business processes.

The business layer does not refer to actual systems such as ERP. The functions of ERP in a process context are typically located in the functional layer.

6.2.3.2 Functional layer

- Formal description of functions.
- Platform for horizontal integration of the various functions.
- Runtime and modelling environment for services which support business processes.
- Runtime environment for applications and technical functionality.

Rules and decision-making logic are generated within the functional layer. Depending on the use case, these can also be executed in the lower layers (information or integration layers).

Remote access and horizontal integration take place only within the functional layer. This ensures the integrity of information and conditions within the process and integration of the technical level. The asset and integration layers may also be accessed temporarily for maintenance purposes.

Such access is used in particular to call up information and processes which are relevant only to subordinate layers. Examples include flashing of sensors/actuators or the reading of diagnosis data. This maintenance-related temporary remote access is not relevant to permanent functional or horizontal integration.

6.2.3.3 Information layer

- Run time environment for (pre-) processing of events.
- Execution of event-related rules.
- Formal description of rules.
- Context: Event preprocessing.

Rules are applied here to one or more events to generate one or more further events, which then initiate processing in the functional layer.

- Persistence of data representing the models
- Assurance of data integrity.
- Consistent integration of different data.
- Obtaining new, higher quality data (data, information, knowledge).
- Provision of structured data via service interfaces.
- Receiving of events and their transformation to match the data which are available for the functional layer.

6.2.3.4 Communication layer

- Standardisation of communication, using a uniform data format, in the direction of the information layer.
- Provision of services for control of the integration layer

6.2.3.5 Integration layer

- Provision of information on the assets that can be computer-processed (physical components/hardware/documents/software, etc.
- Computer-aided control of the technical process.
- Generation of events from the assets.
- Contains the elements connected with IT, such as RFID readers, sensors, HMI, etc.

Interaction with humans also takes place on this level, for instance via the Human Machine Interface (HMI).

Note: Each significant event in the real world points to an event in the virtual world, i.e. in the integration layer. If the reality changes, the event is reported to the integration layer by suitable mechanisms. Relevant events can trigger events signalled to the information layer via the communication layer.

6.2.3.6 Asset layer

- Represents reality, e.g. physical components such as linear axes, metal parts, documents, circuit diagrams, ideas, archives etc.
- Human beings are also part of the asset layer and are connected to the virtual world via the integration layer.
- Passive connection of the assets with the integration layer via the QR code

6.2.4 Life cycle and value stream

Life cycle

Industrie 4.0 offers a great potential for improvement throughout the life cycle of products, machines, factories, etc. In order to visualise and standardise relationships and links, the second axis of the reference architecture model represents the life cycle and the associated value streams.

The draft of IEC 62890 is a good guideline for considering the life cycle. The fundamental distinction between type and instance is of central importance in those considerations.

Type:

A type is always created with the initial idea, i.e. when a product comes into being in the development phase. This covers commissioning, development and testing up to the initial sample and prototype production. The type of the product, machine, etc. is thus created in this phase. On conclusion of all tests and validation, the type is released for series production.

Instance:

Products are manufactured industrially on the basis of the general type. Each manufactured product then represents an instance of that type, and, for example, is assigned a unique serial number. The instances are sold and delivered to customers. For the customer, the products are initially once again only types. They become instances when they are installed in a particular system. The change from type to instance may be repeated several times.

Improvements about a product reported back to the manufacturer from the sales phase can lead to an amendment of the type documents. The newly created type can then be used to manufacture new instances. Similar to each individual instance, the type is therefore also subject to use and updating.

Example:

The development of a new hydraulic valve represents a new type. The valve is developed, initial samples are set up and tested, and finally a first prototype series is manufactured and validated. On successful completion of validation, the hydraulic valve type is released for sale (material number and/or product designation in sales catalogue). At that point, series production also starts.

In series production, each hydraulic valve manufactured is, for example, provided with its unique identification (serial number) and is an instance of the previously developed hydraulic valve.

Feedback on the hydraulic valves sold in the field (instances) may for example lead to minor adjustments to the mechanical design and the relevant drawing, or to corrections in the firmware for the valve. These are modifications to the type, i.e. they are included in the type documentation, undergo re-approval and then emerge as new instances of the modified type in production,

Value streams:

Digitisation and linking of the value streams in Industrie 4.0 provides huge potential for improvements. Cross-linking of different functional areas is of decisive importance in this connection.

Logistics data can be used in assembly, and intralogistics organise themselves on the basis of the order backlog; purchasing sees inventories in real time, and knows where parts from suppliers are at any point in time; the customer sees the completion status of the product ordered during production, and so on. The linking of purchasing, order planning, assembly, logistics, maintenance, the customer and suppliers, etc., provides huge potential for improvements. The life cycle therefore has to be viewed together with the value-adding processes it contains – not in an isolated fashion focusing on a single factory, but rather in a collective of all factories and all parties involved, from engineering and component suppliers through to the customer.

With regard to the value streams, attention is also drawn to the publication on value streams by the GMA Technical Committee 7.21 (VDI/VDE) [1].

6.2.5 Hierarchy levels

The third axis of the reference architecture model describes the functional classification of various circumstances within Industrie 4.0. The issue here is not implementation, but rather functional assignment only.

For classification within a factory, this axis of the reference architecture follows the IEC 62264 and IEC 61512 standards (see figure). For a uniform consideration covering as many sectors as possible from process industry to factory automation, the terms “Enterprise”, “Work Unit”, “Station” and “Control Device” were selected from the options listed there and used.

For Industrie 4.0, not only the control device (e.g. head controller) is decisive, but also considerations within a machine or system. Consequently, the "Field Device” has been added below the Control Device. This represents the functional level of an intelligent field device, e.g. a smart sensor.

Furthermore, not only the plant and machinery for the manufacture of products is important in Industrie 4.0, but also the product to be manufactured. It has therefore been added as “Product” at the bottom level. As a result, the reference architecture model enables a homogeneous view of the product to be manufactured, the production facility and the interdependencies between them.

An addition has also been made at the upper end of the hierarchy levels. The two previously mentioned IEC standards represent only the levels within a factory. Industrie 4.0, however, goes a step further and also describes the group of factories, and the collaboration with external engineering firms, component suppliers and customers, etc. For observations above and beyond the enterprise level, the “Connected World” has therefore been added.

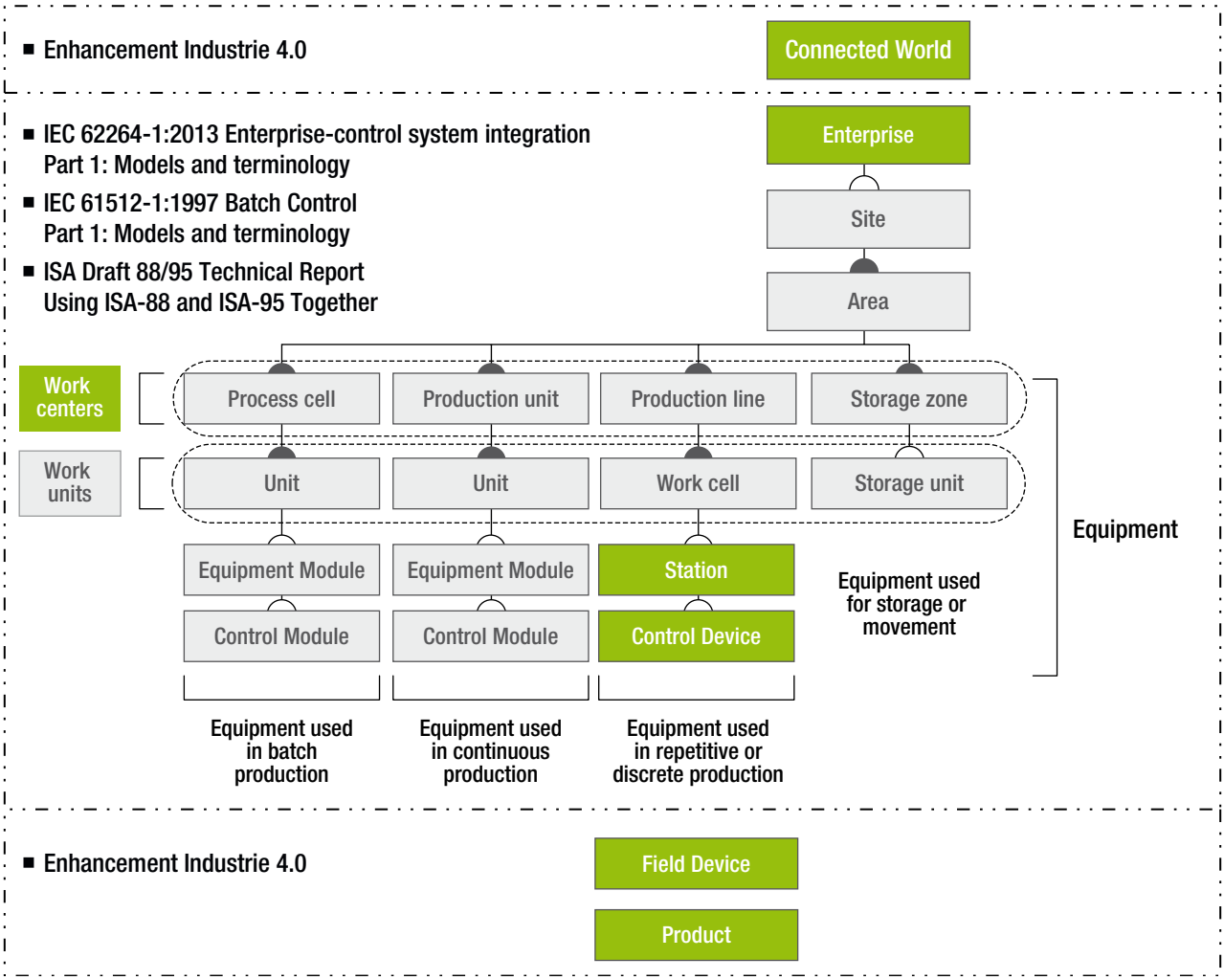


Figure 16: Derivation of the hierarchical levels of the reference architecture model RAMI 4.0

6.3 Reference model for the Industrie 4.0 component

Version 1.0 of the "reference model for Industrie 4.0 components" described below is intended to be the first of several enhancements to be published at intervals of less than one year. In a further step, sections with more precise definitions are therefore to follow and formalisation with UML is planned.

Care is taken in the text to identify precisely where texts/quotations from other sources are adopted in the Industrie 4.0 environment (e.g. VDI/VDE GMA 7.21).

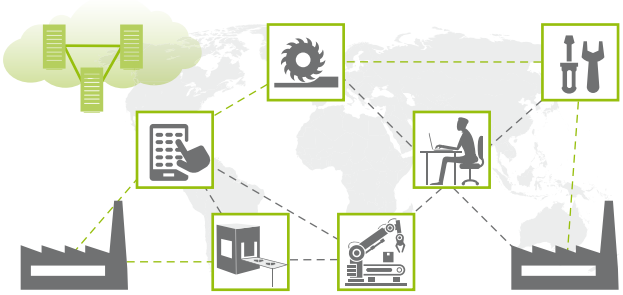
In the final version, the terms used and their definitions are to be identical with those of the GMA Technical Committee 7.21. Examples are also explicitly identified in order to avoid exclusions not explicitly named in the example.

6.3.1 Integration in the discussion on Industrie 4.0

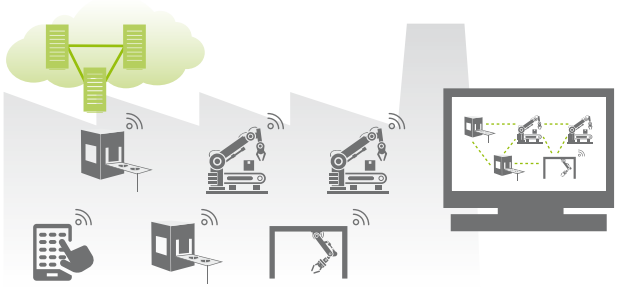
The discussion on Industrie 4.0 can be roughly understood as the interaction between four aspects, as illustrated in the following figure from [3]

4 Source: IEC 61512, IEC 62264, ISA Draft 88/95 Technical Report, Industrie 4.0 Platform

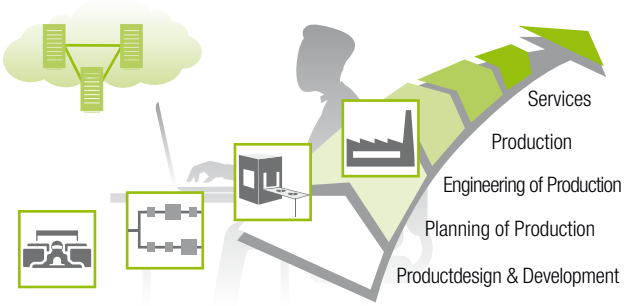
Horizontal integration via value-added networks



Vertical (integration and networked production systems)



Digital consistency for the engineering throughout the whole value-added chain



The human being as a conductor for added value

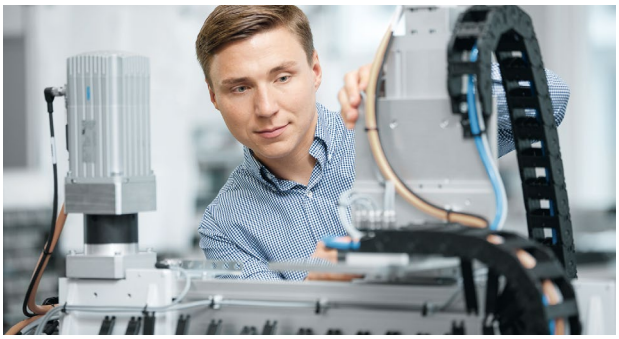


Figure 17: Four important aspects of Industrie 4.0[5]

According to the above images, these four aspects are:

- Industrie 4.0 aspect (1)
  Horizontal integration through value networks
- Industrie 4.0 aspect (2)
  Vertical integration, e.g. within a factory/ or production shop
- Industrie 4.0 aspect (3)
  Life cycle management, end-to-end engineering
- Industrie 4.0 Aspect (4)
  Human beings orchestrating the value stream[6]

The Industrie 4.0 component described in this text provides a flexible framework on the data and functions that can be defined and made available to facilitate and promote the Industrie 4.0 aspects listed above.

The concepts described in this text currently address in particular Aspect (2), and take account of some of the requirements from Aspect (3).

6.3.2 Relevant content from other working groups

VDI/VDE GMA 7.21: Industrie 4.0: Objects, entities, components

For definitions from VDI/ VDA GMA 7.21, reference is made to the previous chapters.

Types and instances

Attention is briefly drawn here to the state of the art indistinctions between types and instances in Industrie 4.0.

5 based on [3], figure on the bottom right source: Festo

6 According to Prof. Bauernhansl

Life cycles

According to Dr. Carmen Constantinescu and Prof. Thomas Bauernhansl of Fraunhofer IPA, life cycles in various dimensions are of relevance to the operation of a factory in Industrie 4.0.

- **Product:** A factory produces several products. Each product has its own life cycle.
- **Order:** Each order for manufacturing runs through a life cycle and its specifics necessarily have an impact on the production facility during performance of the order.
- **Factory:** A factory also has a life cycle:
  It is financed, planned, constructed and recycled.
  A factory integrates production systems and machines from different manufacturers.
- **Machine:** A machine is ordered, designed, commissioned, operated, serviced, converted and recycled.

  The manufacturer of a machine purchases individual supplier parts, referred to in this paper as objects. The supplier (usually a component manufacturer) also puts supplied parts through a life cycle.
- **Component:** From planning and development, rapid prototyping, construction, production and use through to servicing.

Figure 18 illustrates this.

Linking of life cycles

The reason why it is necessary to distinguish between types and instances is the interaction of different business partners and their individual life cycles with planning processes. During planning, various hypotheses and alternatives are considered. Planning proceeds on the basis of potential objects, and refers to them as “types”:

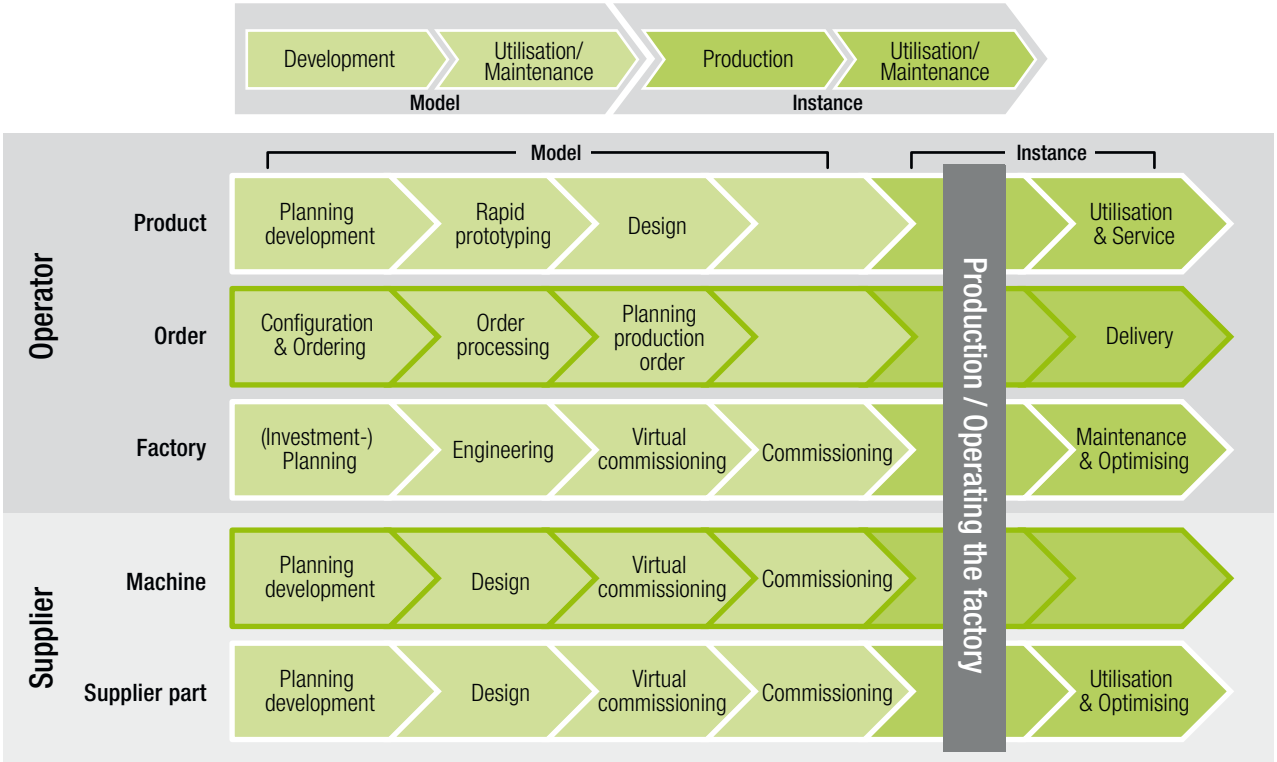


Figure 18: Relevant life cycles for Industrie 4.0 components[7]

7 Source: Martin Hankel, Bosch Rexroth; Prof. Thomas Bauernhansl, Fraunhofer IPA; Johannes Diemer, Hewlett-Packard

- **The component supplier** refers to them as "part types": Only manufacture and the subsequent delivery to the customer (machine manufacturer) “creates” an instance, which the machine manufacturer uses as a bought-in component.
- **The machine manufacturer** discusses "machine types" with his customer, and designs them. Construction of a specific machine creates an instance which is then used by the factory operator.
- **The factory operator** also initially develops a product as a product type. Only receipt of an order initiates production and implements the manufacture of concrete product instances which are then delivered.

It is noticeable in this context that during the design and planning of each type a large amount of data and information is generated, and can be drawn upon by the downstream business partner in the added value network by using the relevant instance. Further information is added during production of a particular instance (e.g. tracking data and quality data). The reference model for Industrie 4.0 components therefore deals with types and instances as being similar and equivalent.

Reference architecture model for Industrie 4.0 (RAMI4.0)

With regard to the definitions in the "Reference Architecture Model for Industrie 4.0 (RAMI4.0)", attention is drawn to the preceding chapters. The "Industrie 4.0 component" presented here is located within the layers of RAMI4.0. It can adopt various positions in the life cycle and value stream, and occupy various hierarchical levels: A final assignment is only possible in the case of an actual instance.

6.3.3 The "Industrie 4.0 component"

6.3.3.1 An initial, generally recognised definition of an Industrie 4.0 component is derived in this chapter. Demarcation of the Industrie 4.0 components between "Office floor" and "Shop floor".

In order to achieve a clear assignment of responsibilities, companies usually distinguish between “office floor” and “shop floor”. In modern businesses, however, these areas are increasingly interlinked. If the focus is on automation systems, the relevance of the office floor decreases, while more and more requirements of the shop floor become relevant. The same also applies in reverse.

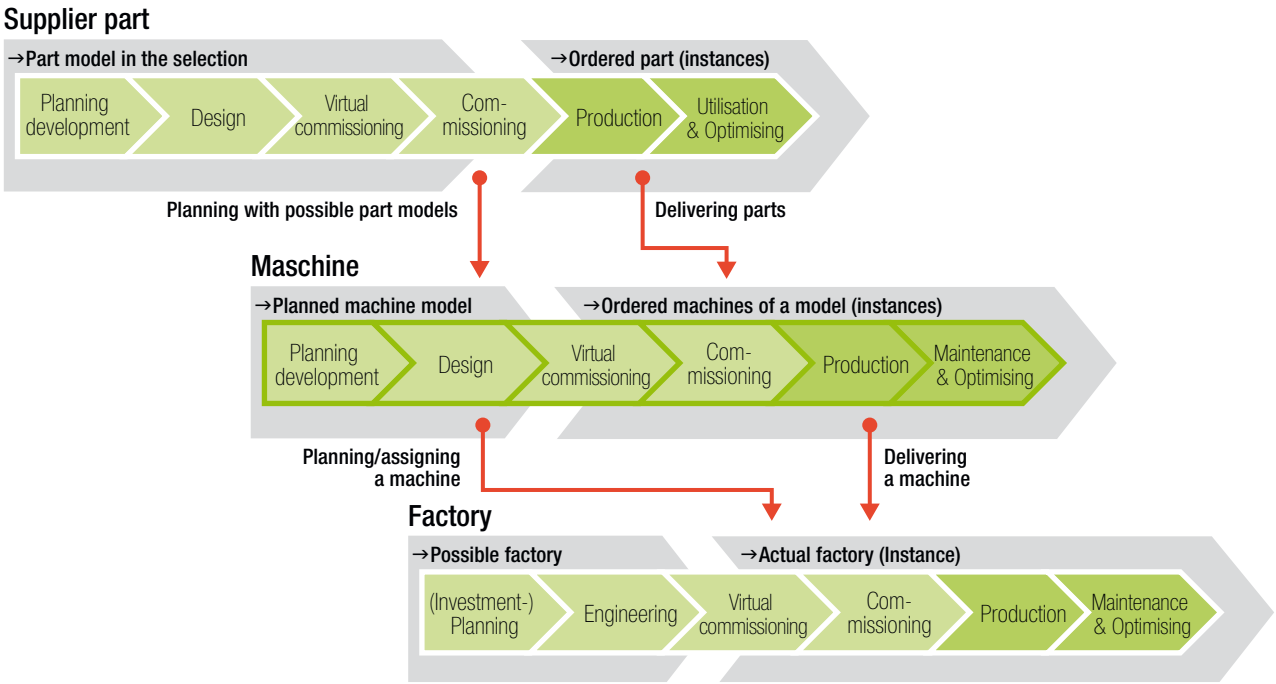


Figure 19: Types and instances in the life cycle

Because of connectivity requirements to any end point and a common semantic model in the following figure, components must have certain common properties independently of the levels. They are specified in the form of the Industrie 4.0 components.

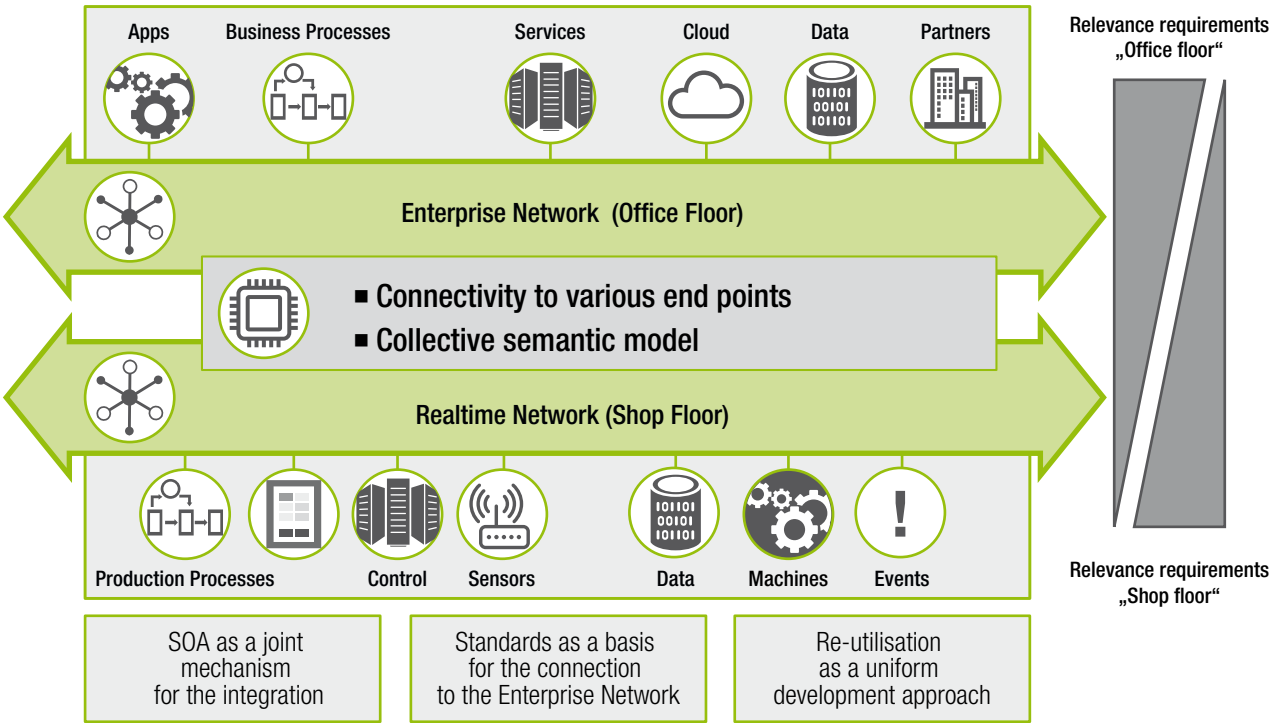


Figure 20: Demarcation between "office floor" and "shop floor"

An Industrie 4.0 component can be a production system, an individual machine or station, or an assembly within a machine. Each Industrie 4.0 component, however different they may be, therefore moves along the life cycle of the factory in dynamic relevance to the office and shop floors, and in contact with such central and significant factory systems as PLM (Product Life Cycle Management), ERP (Enterprise Resource Planning) and Industrial Control and Logistics systems.

Requirement:
A network of Industrie 4.0 components must be structured in such a way that connections between any end point (Industrie 4.0 components) are possible. The Industrie 4.0 components and their contents are to follow a common semantic model.

Requirement:
It must be possible to define the concept of an Industrie 4.0 component in such a way that it can meet requirements with different focal areas, i. e. “office floor” or “shop floor”.

6.3.3.2 From the object to the Industrie 4.0 component

In the following section, the individual findings of the Society for Measurement and Automatic Control (GMA) are to be referenced to each other to arrive at a definition of an Industrie 4.0 component:

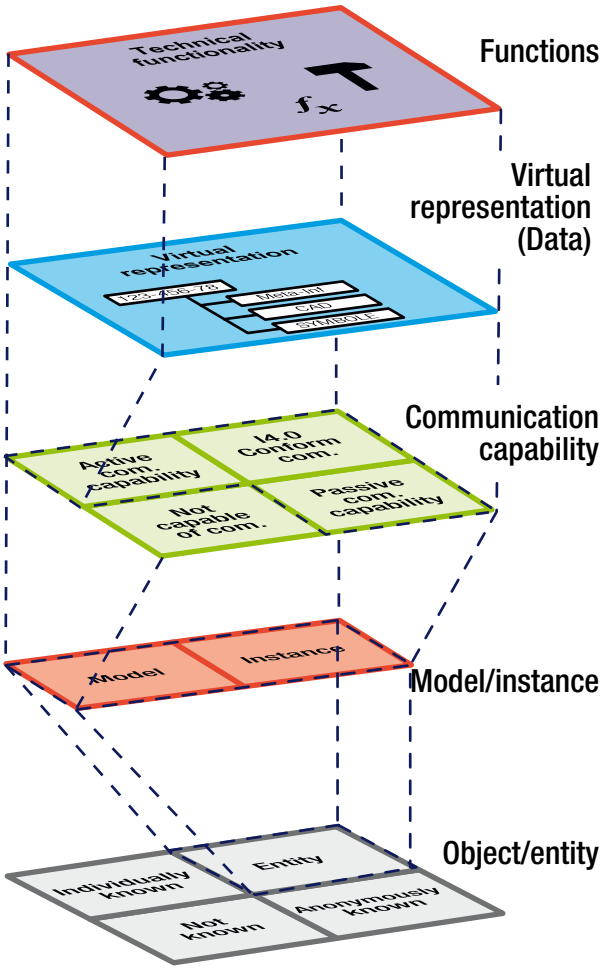


Figure 21: Levels of an 4.0 component in accordance with GMA 7.21

Classes of objects:

- GMA names four classes of objects:
- Unknown
- Anonymous
- Individually known
- Entities

In order to link data and functions to an object, it must take the form of an entity. Software, which in the conventional sense can be delivered physically or non-physically, is also an object. Ideas, archives and concepts are also objects within the meaning of the word here.

Note 1:
As it is one of the objectives of an Industrie 4.0 component to provide data and functions within an information system, individually known objects as defined by GMA automatically undergo a transition to becoming an entity.

Note 2:
The term object is used below whenever an object/entity is referred to.

Type/instance

Objects may be known in the form of a type or an instance. An object in the planning phase, for example, is known as a type, and if the order information for a planned object is known, it can be regarded as an individually known type. Instances, for example, are all objects in an actually existing machine. No special consideration is currently given to those apparent instances which arise from multiple instantiation of a type for purposes of countability (batches). In such cases, instantiation should be performed as a concrete process and a reference to the type established.

Communication ability

If the properties of an Industrie 4.0 component are to be made available, at least one information system must maintain a connection with the object. This therefore requires at least passive communication ability on the part of the object, which means that an object does not necessarily have to have the ability of Industrie 4.0 compliant communication as set out by GMA Technical Committee 7.21. In consequence existing objects can be “extended” to constitute Industrie 4.0 components. In this case, a higher level IT system takes on part of the Industrie 4.0 compliant communication by way of a service oriented architecture and a deputy principle.

An identifiable terminal strip, for example, or a ProfiNet device (identifiable by its I&M data) can become an Industrie 4.0 component in this way.

Virtual representation

Virtual representation contains data on the object. These data can either be kept on/in the Industrie 4.0 component itself and made available to the outside world by Industrie 4.0 compliant communication, or they can be stored in a (higher level) IT system which makes them available to the outside world by Industrie 4.0 compliant communication.

In the reference architecture model RAMI4.0, virtual representation takes place in the information layer. Industrie 4.0 compliant communication is thus of great importance.

Requirement:
Industrie 4.0 compliant communication must be performed in such a way that the data of a virtual representation of an Industrie 4.0 component can be kept either in the object itself or in a (higher level) IT system.

One important part of the virtual representation is the "manifest"[8] which can be regarded as a directory of the individual data contents of the virtual representation. It therefore contains what is termed meta-information. Furthermore, it contains obligatory data on the Industrie 4.0 component and used, among other purposes, for connection with the object by the corresponding identification capability.

Possible further data in the virtual representation include data which cover individual life cycle phases such as CAD data, terminal diagrams or manuals.

Technical functionality

Apart from data, an Industrie 4.0 component can also possess technical functionality. This functionality may, for example, comprise the following:

- Software for "local planning" in connection with the object. Examples: Welding planning, software for labelling terminal strips, etc.
- Software for project planning, configuration, operator control and servicing.
- Value-added to the object.
- Further technical functionalities which are relevant to the implementation of the business logic.

Technical functionality takes place in the functional layer of the reference architecture model RAMI4.0.

6.3.3.3 An "administration shell" turns an object into an Industrie 4.0 component

As the section above indicates, different objects with different communication abilities can be implemented as an Industrie 4.0 component. This section is intended to describe these various implementations in greater detail using examples. The various implementations are of equal value for the purposes of the "Industrie 4.0 component" concept.

Figure 22 shows that an object, no matter what kind it is, is not initially an Industrie 4.0 component. Only when that object, which must be an entity and at least have passive communication ability, is surrounded by an "administration shell", can it be described as an Industrie 4.0 component.

Within the context of the section above, the administration shell includes both the virtual representation and the technical functionality of the object.

8 Selection due to the .JAR file, see manifest [11].

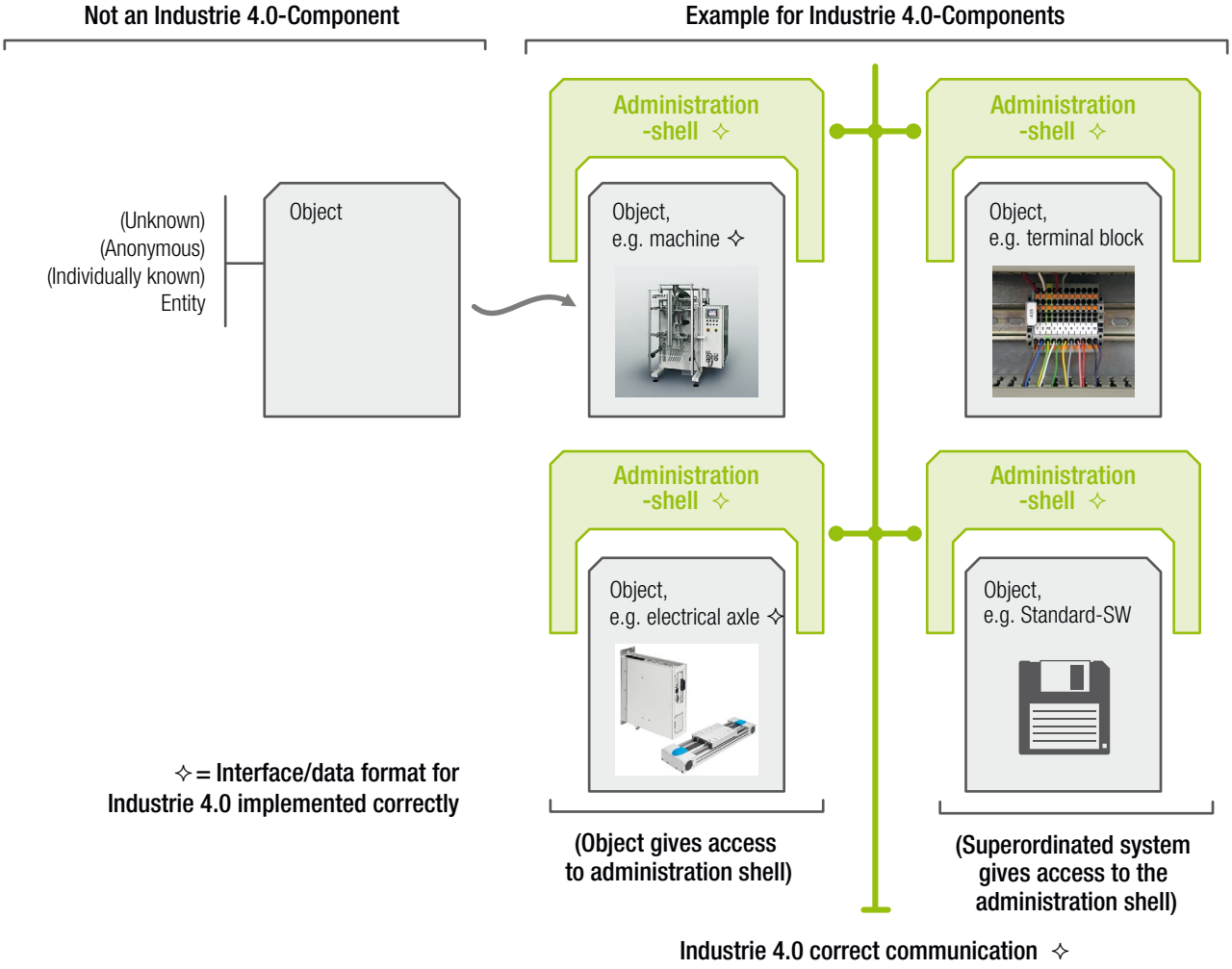


Figure 22: An object becomes an Industrie 4.0 component

The above figure provides four examples of a possible object:

1. An entire machine can be implemented as an Industrie 4.0 component, above all as a result of its controller. This implementation of the Industrie 4.0 component is, for example, undertaken by the machine manufacturer.
2. A strategically important assembly[9] from a supplier can also be regarded as an independent Industrie 4.0 component, so that it can, for example, be registered separately by asset management and maintenance systems. This implementation of the Industrie 4.0 component is, for example,undertaken by the component manufacturer.
3. It is also possible to regard individual composite parts in the machine as Industrie 4.0 components. For example, for a terminal block it is important to retain the wiring with individual signals and keep it up to date throughout the life cycle of the machine. This implementation of the Industrie 4.0 component is, for example, undertaken by the electrical design engineer and electrician.
4. Finally, the software supplied can represent an important asset in a production system, and thus be an Industrie 4.0 component. Such standard software could, for example, be an independent planning or

9 to avoid the term component

engineering tool which may be important now or in the future for operation of the manufacturing system. It is also conceivable that a supplier may wish to sell a library which provides extended functions for his products as separate software. This implementation of the Industrie 4.0 component would then, for example, be undertaken by the software supplier; distribution among individual IEC 61131 controllers would be effected by the various Industrie 4.0 systems.

Figure 22 shows how logically an administration shell belongs to each object. From the point of view of deployment, the object and the administration shell may by all means be decoupled. For example, in objects which possess passive communication ability, the administration shell may be provided[10] by a higher level IT system. The connection between the object and the administration shell is maintained with the aid of the object's passive communication ability and the Industrie 4.0 compliant communication regime of the higher level IT system. The same applies when the object has active, but not Industrie 4.0 compliant, communication ability. Only with Industrie 4.0 compliant communication ability can the administration shell be hosted "in" the object (it is, for example, stored in the controller of a machine and supplied via the network interface). For the purposes of the "Industrie 4.0 component" concept, these alternatives are to be regarded as equivalent.

One object may have several administration shells for different purposes.

Requirement:

A suitable reference model must be established to describe how a higher level IT system can make the administration shell available in an Industrie 4.0 compliant manner (SOA approach, deputy principle).

10 hosted

Requirement:

A description is required of how the administration shell can be "transported" from the originator (e.g. component manufacturer or electrical designer) to the higher level IT system (e.g. as an attachment to an email).

6.3.3.4 Further disambiguation

The following figure provides a further disambiguation of the terms:

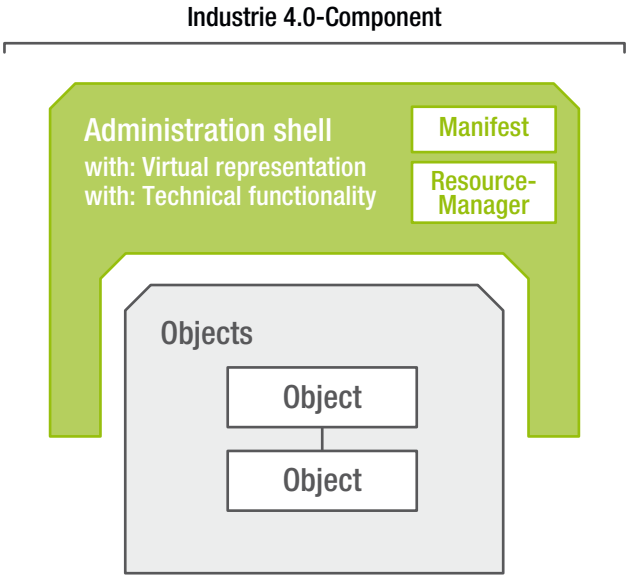


Figure 23: Industrie 4.0 component:

From a logical point of view, an Industrie 4.0 component comprises one or more objects and an administration shell which contains the data for virtual representation and the functions of the technical functionality. The manifest, as part of the virtual representation, details the necessary administrative details about the Industrie 4.0 component. The "resource manager", as defined by GMA Technical Committee 7.21, is also part of the administration shell. With the resource manager, IT services have access to the data and functions of the administration shell and make them externally available.

The administration shell and its contents can be hosted within one of the objects of an embedded system (active, Industrie 4.0 compliant communication ability) or distributed among one or more higher level IT systems (deployment view).

Requirement:
Depending on the nature of the higher level systems, it may be necessary for the administration objects to allow for deployment in more than one higher level IT system.

Cyber-physical system

The Industrie 4.0 component constitutes a specific case of a cyber-physical system.

6.3.3.5 Industrie 4.0 components from the point of view of deployment

The section above makes it clear that from a logical point of view an administration shell belongs to each object of an Industrie 4.0 component. It is however also emphasised that situationally and from a deployment point of view, the administration shell can be relocated into a higher level system.

Industrie 4.0 component mapped in a repository

For a better understanding, a representation of a repository conforming to the "digital factory" and in harmony with the concepts outlined can be shown.

Industrie 4.0 component mapped by an object

If one of the objects in the Industrie 4.0 component has Industrie 4.0 compliant communication ability (CP34 or CP44 in accordance with [2]), it is appropriate to portray the Industrie 4.0 component by the object:

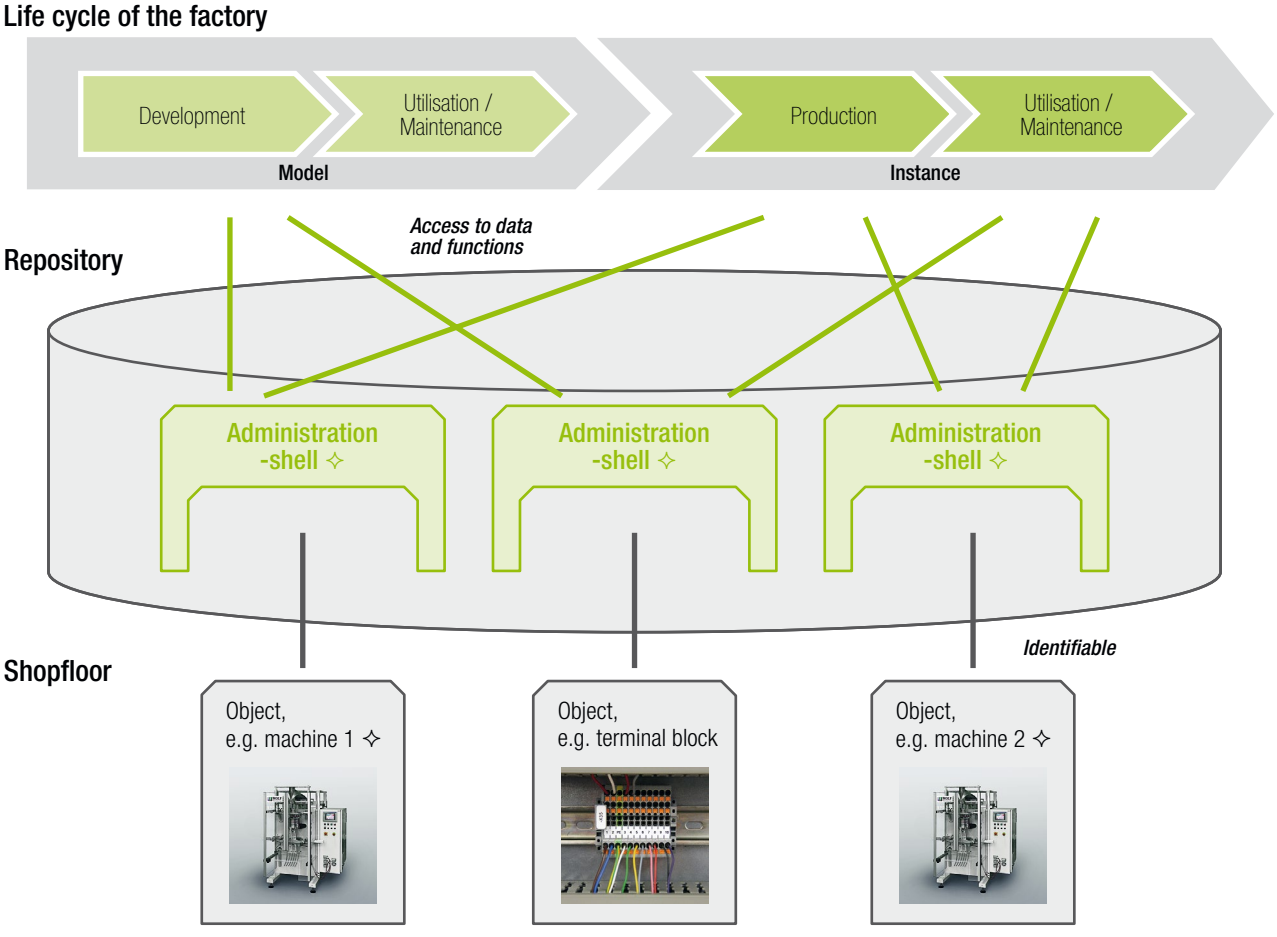


Figure 24: Repository

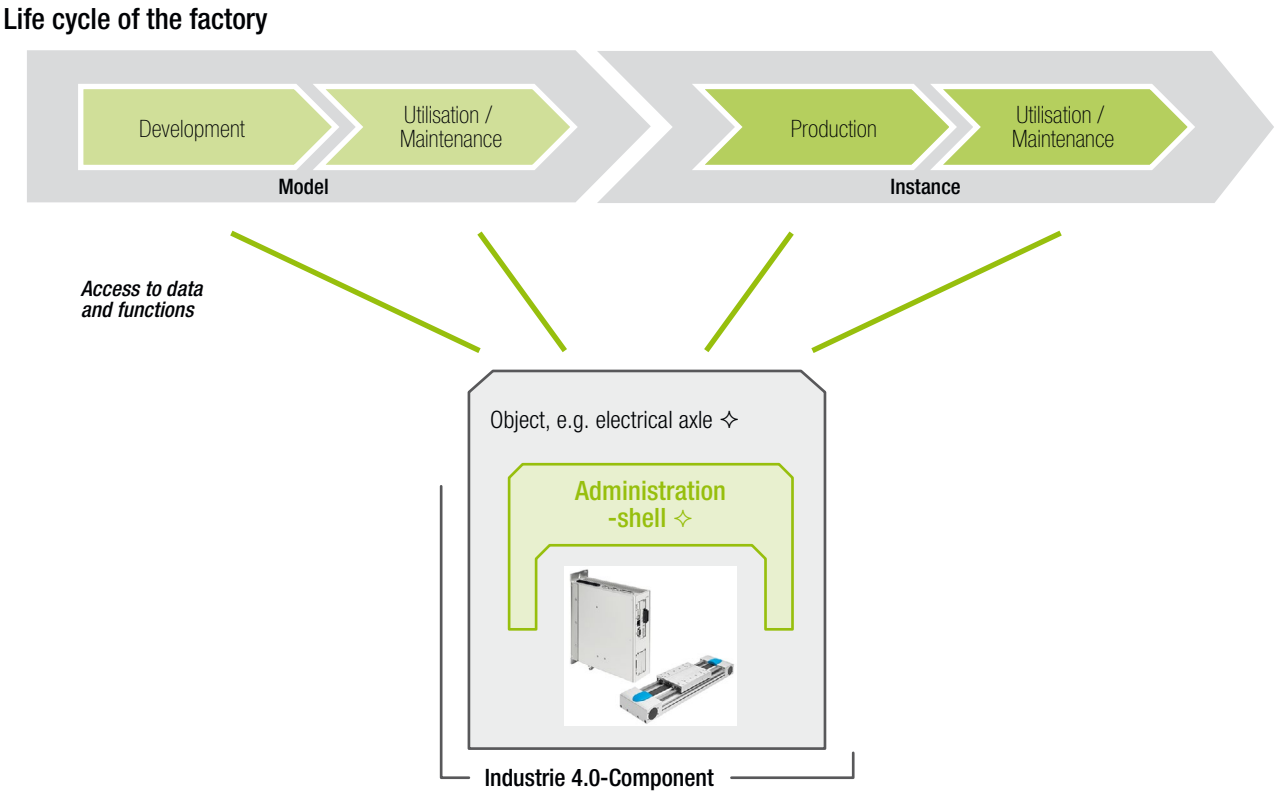


Figure 25: Life cycle of the factory

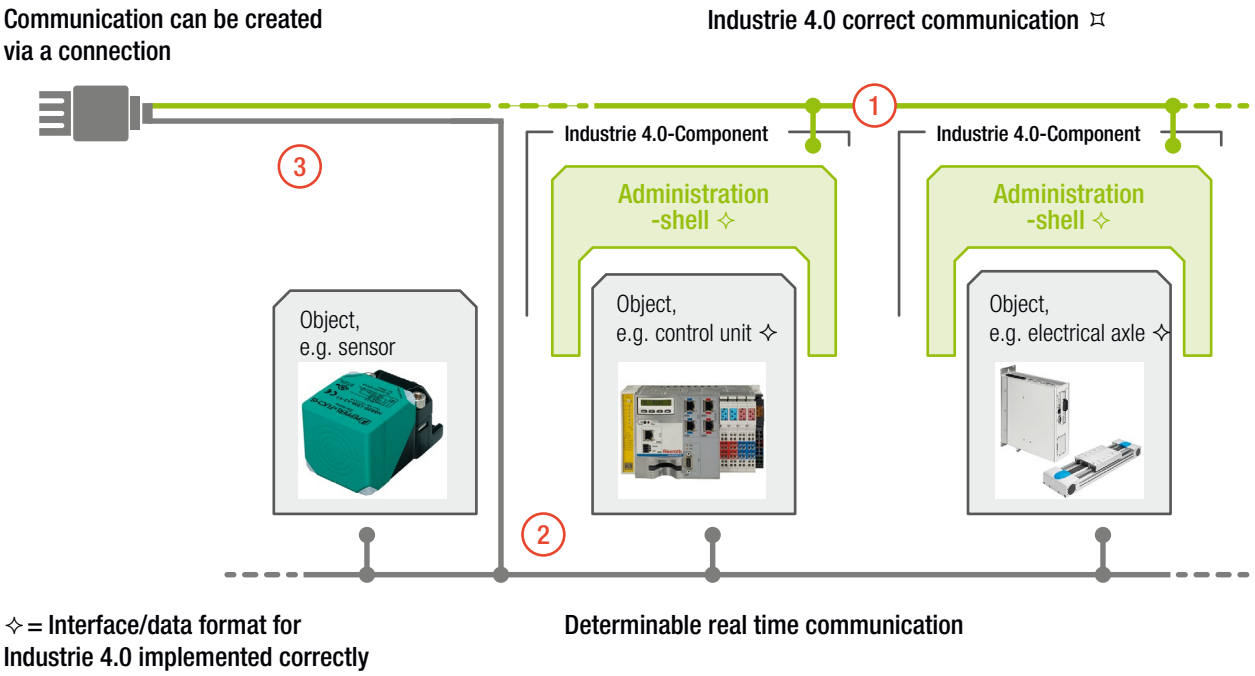


Figure 26: Separability and networking of an Industrie 4.0 component

6.3.3.6 The Industrie 4.0 component is separable

The Industrie 4.0 component is to be intentionally capable of entering into and initiating all possible cross-connections within the Industrie 4.0 factory (figure 26, no. 1). But this networking must not lead to a restriction of the core functionality (figure 26, no. 2). The ability to keep this core area free from faults, even when the "external" network is experiencing disturbances, is designated by SG2 (ZVEI Mirror Committee on Reference Architecture) and SG4 (ZVEI Mirror Committee on Security) as "separability".

Requirement:

The Industrie 4.0 component, and in particular the administration shell, its inherent functionality and the protocols concerned are to be "separable".

The present concept fulfils this requirement in that the administration shell is implemented as an independent data/function object. Access to the data and functions it contains is to be provided for in accordance with the principle of "Separation of Concerns" (SoC)[11], so that influencing of workflows critical for production can, according to state-of-the-art technology, be excluded.

It follows from the application of this principle that Industrie 4.0 compliant communication does not necessarily have to completely replace the Ethernet-based field buses currently used in production (migration scenario).

However, Industrie 4.0 compliant communication and a possible deterministic or real-time form of communication should be brought into line with each other, and, for example, the same (physical) interfaces and infrastructures used wherever possible. Consistency between the two communication channels must be ensured.

With regard to the reference model described in this paper, this argument means that Industrie 4.0 compliant communication does not have to implement all the properties of deterministic or real-time communication itself, but can delegate them to existing technologies.

Requirement:

The aim of the Industrie 4.0 component is to detect non-Industrie 4.0 compliant communication relationships leading to or from the object's administration shell and to make them accessible to end-to-end engineering.

The current real-time Ethernet protocols make it possible to effect both forms of communication via the same communications infrastructure (connectors, plugs and intermediate stations) (figure 26, no. 3). According to the principle of "Separation of Concern", however, both types of communication are to remain logically separated.

6.3.3.7 An Industrie 4.0 component can contain several objects

This section uses an example to show that an Industrie 4.0 component can contain not only one, but also several objects.

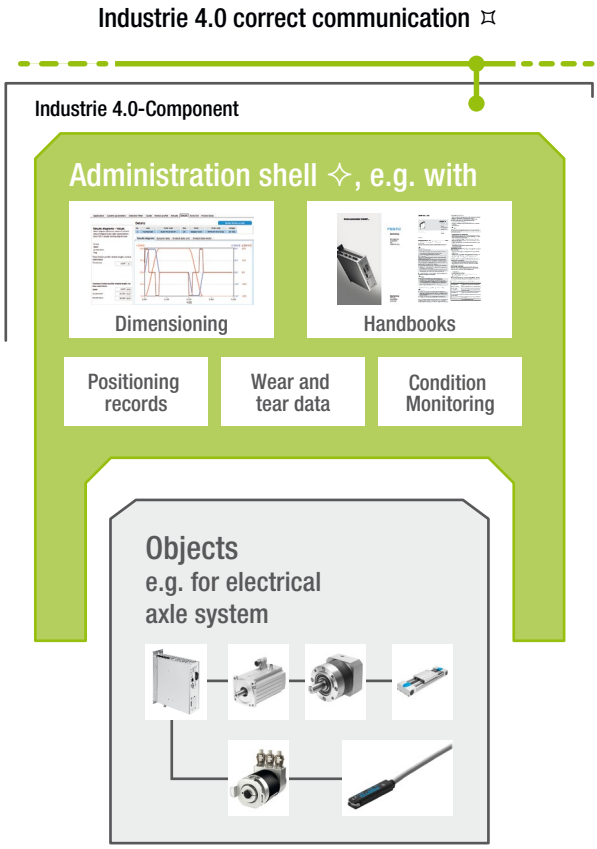


Figure 27: Industrie 4.0 component consisting of several objects

11 http://en.wikipedia.org/wiki/Separation_of_concerns

The objects in figure 27 in combination form an example of an electrical axis system. Design software from one manufacturer resulted in the individual partial systems being combined into a single system during the engineering phase. Configuration software also exists with which the system as a whole can be put into operation. Traversing blocks, recorded wear data and condition monitoring need to link the individual parts of the system to each other (e.g. with regard to the maximum traversing length).

From an Industrie 4.0 view, it is therefore appropriate to manage these individual objects as a system and portray them as one Industrie 4.0 component. A breakdown into individual Industrie 4.0 components would necessitate the portrayal of many different interrelationships by one or possibly even more higher level Industrie 4.0 systems, and unnecessarily complicate the process.

6.3.3.8 An Industrie 4.0 component can be logically nestable

Industrie 4.0 demands the modularisation of production systems for order-related reconfiguration and re-use of (corporate) assets[12] under the terms of Industrie 4.0 Aspect, "Vertical Integration". The concept therefore provides for an Industrie 4.0 component to encompass other components in logical terms, to act as a unit and perform logical abstraction for a higher level system.

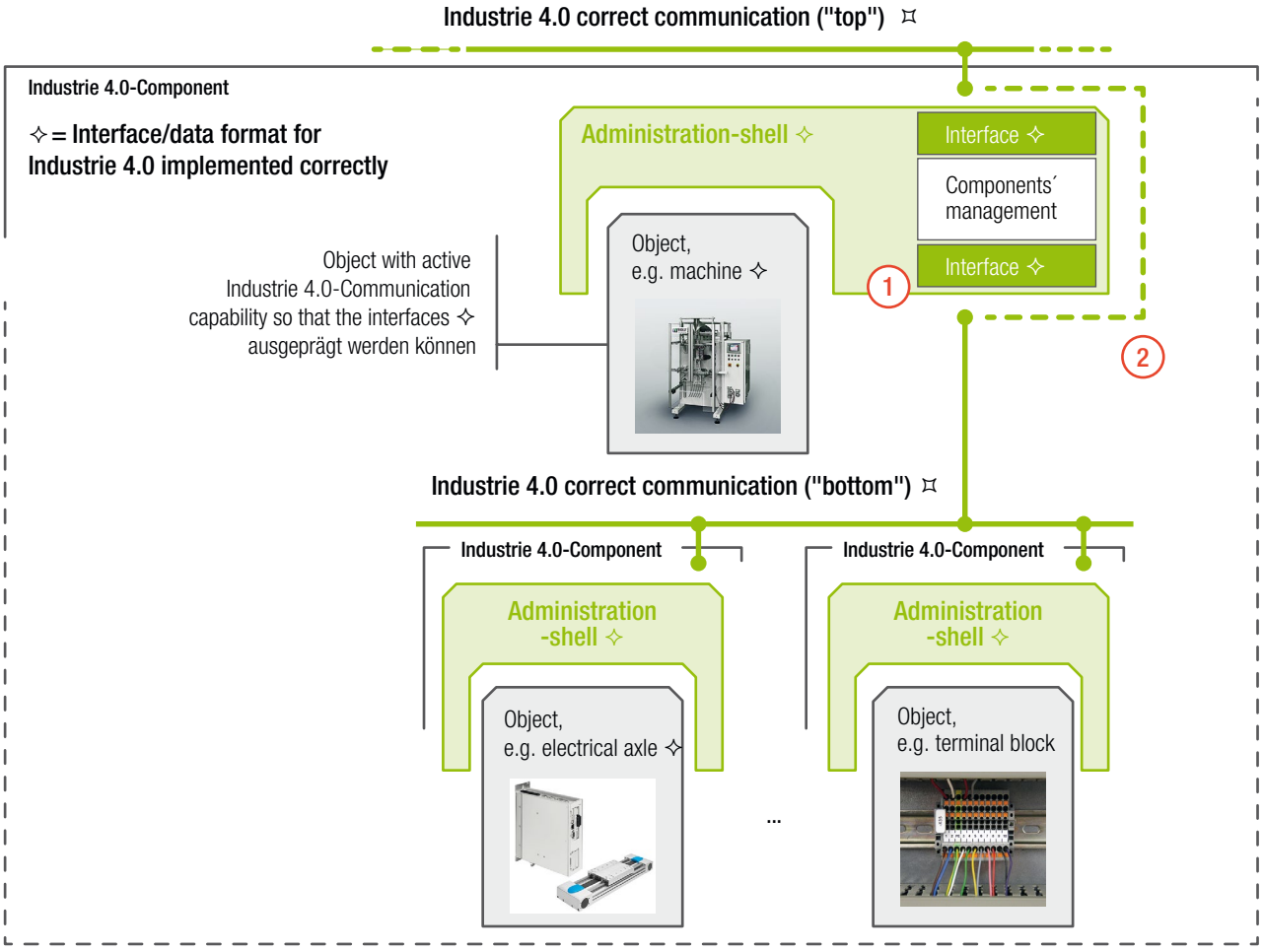


Figure 28: Nestability of Industrie 4.0 components

12 see [3]: "In addition, modularisation and reuse concepts are also a prerequisite for ad-hoc networking and the reconfigurability of production systems in combination with suitable intelligent system capability descriptions."

In addition, Industrie 4.0 Aspect requires “end-to-end engineering” with further data and engineering planning available online for as many objects in a production system as possible. The administration shell provides for data –which can be unambiguously assigned to the objects in the Industrie 4.0 component – to be also available in such a distributed manner. Such distributed data are advantageous for distributed engineering and for rapid reconfiguration.

The concept for an Industrie 4.0 component should therefore enable other Industrie 4.0 components to be logically assigned to an initial Industrie 4.0 component (e.g. an entire machine), in such a way that there is (temporary) nesting.

From a technical point of view, this can be done in such a way that the higher level object (e.g. a machine) develops two Industrie 4.0 compliant communication interfaces, so that there is clear logical and physical separation between higher and lower level Industrie 4.0 components (figure 28, no. 1). A further method is to have the Industrie 4.0 compliant communication physically unified at the “top” and “bottom” but logically separated (figure 28, no. 2).

The administration shell can have a suitable “component management” system to manage such a logical assignment of “subordinate” Industrie 4.0 components. This can, for example, provide support in the reconfiguration of a machine, or provide a suitable portrayal of the status of the machine to the higher level.

Requirement:
It should be possible to logically assign other Industrie 4.0 components to one Industrie 4.0 component (e.g. an entire machine) in such a way that there is (temporary) nesting.

Requirement:
Higher level systems should be able to access all Industrie 4.0 components in a purpose-driven and restrictable manner, even when these are (temporarily) logically assigned.

6.3.3.9 Status model

The status of an Industrie 4.0 component can always be accessed by other subscribers of an Industrie 4.0 compliant communication. It then follows a defined component status model.

As Industrie 4.0 components can be organised hierarchically, a suitable method of portraying sub-statuses within a status should be defined (“What happens to the machine when a part is not ready to operate?”).

In addition, the component status model should also be complemented with a larger number of status variables which permit a more detailed view of virtual representation and technical functionality statuses. This permits a consistent view of the status of an Industrie 4.0 component at time “t”, e.g. for statistically correct data analysis.

6.3.3.10 General characteristics of the “Industrie 4.0 component”

GMA 7.21 [2] defines the term “component” in the context of Industrie 4.0 as follows:

The term “component” is a general term. It designates an object in the physical or information worlds which plays a particular role in its system environment or is intended for such a role. A component can be, for example, a tube, a PLC functional module, a lamp, a valve or an intelligent drive unit. The important thing is that it is considered as a unit and that it has a relationship with the role (function) which it is to perform or already performs in a system. What we call an Industrie 4.0 component is a special type of component. Industrie 4.0 components are notable for fulfilling certain requirements with regard to the classification characteristics set out above. Even in an Industrie 4.0 system, there are many components which do not fulfil these requirements and are therefore not Industrie 4.0 components.

The concept presented here also permits objects with a passive or active communication ability which is nevertheless not Industrie 4.0 compliant. The following therefore applies to an Industrie 4.0 component within the meaning of this document:

- It is either a CP24, CP34 or a CP44 component in terms of CP classification.
- It has an administration shell which can be communicated in such a way that it becomes a fully fledged service system subscriber in the Industrie 4.0 network

The following section is a refinement on the GMA definition [2] and therefore presents the concepts in greater detail. In complete accord with [2], the following features (requirements) are needed from an Industrie 4.0 component as a service system subscriber in the Industrie 4.0 network:

Identifiability

It is unequivocally identifiable in the network and its physical objects are identified by means of a unique identifier (ID). If it is a CP34 or CP44 component, it can be reached via a communication address (e.g. IP address).

Industrie 4.0 compliant communication

The Industrie 4.0 components communicate with each other at least in accordance with the SOA principle (including common Industrie 4.0 compliant semantics).

Industrie 4.0 compliant services and statuses

It supports the generally standardised (and loadable) service functions and statuses for an Industrie 4.0 system.

Virtual description

It supplies its virtual description, including its dynamic behaviour. This description is established by the virtual representation and the manifest.

Industrie 4.0 compliant semantics

It supports the Industrie 4.0 compliant semantics standardised for an Industrie 4.0 system.

Security and safety

It provides sufficient protection (security) for its functionality and data appropriate to the task. Applications may also require functional safety and machine safety measures.

Quality of services

It possesses the Quality of Services (QoS) properties necessary for its function. With regard to applications in automation systems, these include characteristics such as real time capability, fail safety and clock synchronisation. These properties may correspond to a profile.

Status

It provides information on its status at all times.

Nestability

Every Industrie 4.0 component can consist of other Industrie 4.0 components.

Industrie 4.0 components in the context of this document stand for production systems, machines, stations and conceptually important parts or assemblies in machines.

Re feature (1): Identifiability

The objective of the Industrie 4.0 approach is to be able to access all the relevant data in real time. The Industrie 4.0 components represent an important part of an expansion in infrastructure relative to the present day. This applies throughout the life cycle of the production system. Industrie 4.0 components therefore play a central role in ensuring a consistent and uniform exchange of information in all Industrie 4.0 value streams [1] and all their value adding processes.

An active Industrie 4.0 component can perform Industrie 4.0 compliant communication itself; for a passive Industrie 4.0 component, this is handled by the necessary infrastructure.

There is a need for communication which fulfils the requirements of industry. As production systems are increasingly working in networks, and in such a context great distances sometimes have to be overcome, the connection of local area networks by wide area links is constantly gaining in importance.

Requirement:
The wide area networks used in the connection of Industrie 4.0 components should function in such a way that local area networks can communicate via a long distance link without restrictions.

This concerns the availability of such connections, their security and their on-time performance. Even if streaming technologies and other mechanisms could constitute a basis for appropriate solutions, fundamental work is still required in this field.

At one level higher, connections have to ensure that stable and reliable communication is ensured over long periods. In this context, existing protocols are to be examined for usability in Industrie 4.0 applications. A distinction is to be made between the addressing of the Industrie 4.0 component and the addressing of its (application) objects. The latter are addressed by means of a unique, global and non-proprietary ID. As regards handling of IDs, attention is drawn to [4] and [5] and other standards.

Requirement:
A distinction is to be made between the addressing of the Industrie 4.0 component and the addressing of its (application) objects.

Re feature (2):
Industrie 4.0 compliant communication

Self-disclosure by an Industrie 4.0 component is achieved on the basis of a service-oriented architecture (SOA) with services corresponding to a service model (Resource Manager). A corresponding profile of the Industrie 4.0 component can regulate how such services can be implemented technologically (e.g. via OPC-UA basic services).

Re feature (3):
Industrie 4.0 compliant services and statuses

As different applications have to be operated on the shop and office floors, there must be the option for Industrie 4.0 components to operate the various application levels with different protocols.

Requirement:
Protocols and application functions should therefore be loadable as options.

Re feature (4): Virtual description

The information for description of the characteristics, including the relevant dynamic behaviour, of an Industrie 4.0 component is generated in an Industrie 4.0 data format from the virtual portrayal of the real component. This portrayal is termed a “virtual representation”; one part of the virtual representation is the manifest, which must have unequivocal semantics. The specification of features plays an important role.

The following, for example, are parts of the manifest:

- Characteristic features of the real components
- Information on relationships between the features
- Relationships between Industrie 4.0 components which are relevant to production and production processes
- Formal description of relevant functions of the machine and its workflows

The following, for example, are parts of the virtual representation:

- Commercial data
- Historical data, e.g. service history
- And so on...

The demarcation between the manifest in particular and administration objects in general is that the manifest contains information which must be publicly known and have unequivocal semantics for the realisation of an “Industrie 4.0 compliant network” in accordance with the Industrie 4.0 aspects. Administration objects can also contain such information, although here the manufacturer may decide independently what is to be revealed and in what form.

Re feature (5): Industrie 4.0 compliant semantics

The exchange of information between two or more Industrie 4.0 components requires unequivocal semantics. These must be stipulated throughout Industrie 4.0 by means of the characteristics set out under [4]. According to [4], it appears helpful to classify the features according to the following fields:

- Mechanics
- Functionality
- Location
- Efficiency and
- Business conditions

On dealing with features, attention is drawn to [4], [5] and [6].

Re feature (6): Security and safety

Each Industrie 4.0 component has a minimum infrastructure to ensure security functions. As security is only ensured when the production processes concerned are directly involved in the security considerations, the security infrastructure of an Industrie 4.0 component provides necessary, but by no means sufficient, functionality. If functional and machine safety have to be ensured, this has an impact on the characteristics of the individual Industrie 4.0 components. Additional features need to be recorded, assessed and passed on to higher level systems in this context.

Requirement:
The minimum infrastructure must satisfy the principles of Security by Design (SbD).

Re feature (7): Quality of services

The use of an Industrie 4.0 component in a particular environment determines the requirements placed upon it. The properties demanded in the relevant environment (QoS) must therefore already be taken into account in the selection of the components for a machine or system. Especially for automation environments, these are properties such as:

- Duration of real time for production communication, e.g. determinism with real time capability of D1ms.
- Maximum fail-safety of the surrounding network infrastructure (robustness)
- Clock synchronisation
- Interoperability
- Diagnosis and engineering on the basis of uniform rules
- Establishment of ad-hoc connections

Re feature (8): Status

As every Industrie 4.0 component represents part of a group with certain functions, and these functions must be performed in processes in a coordinated manner, the status of every Industrie 4.0 component must be accessible at any time to other subscribers in an Industrie 4.0 compliant communication network. This information is used for the local administration of other Industrie 4.0 components and the global administration for coordination of the workflows.

Re feature (9): Nestability

Industrie 4.0 components may be grouped together in a single Industrie 4.0 component. In this way, for example, a machine can constitute an Industrie 4.0 component. It can itself consist of independent Industrie 4.0 components, e.g. as a modular machine. The individual machine modules may for their part also be structured from individual Industrie 4.0 components.

6.4 Standardisation

6.4.1 Background

In accordance with the German Standardisation Strategy, "Normung" ("standardisation", "formal standardisation", "consensus-based standardisation") is defined as the development, on the basis of full consensus, of rules, guidelines and characteristics for activities for general or repetitive application by an approved organisation – and "Standardisierung" ("informal standardisation", "limited consensus standardisation" or "consortial standardisation"), the process of drawing up specifications.

There are, for example, several types of document, e.g. a VDE application guide, DIN SPEC (DIN Specification), PAS (publicly available specification), TS (technical specification), ITA (industry technical agreement) and TR (technical report).

The "DKE Industrie 4.0 Roadmap", the first version of which was published the previous year and which is currently being reviewed, is very helpful in this respect. The aim behind this document was to draw up a strategic, technically oriented roadmap which, taking special account of the recommendations from the Industry and Science Research Union and the corresponding assistance from the BMWi and BMBF, presents the requirements for standards and specifications for Industrie 4.0, identifies areas where action is necessary and issues corresponding recommendations. In addition, it provides an overview of the standards and specifications in this field.

The standardisation roadmap is intended as taking stock as well as a means of communication between the parties involved from the various technological sectors such as automation, information and communications technology and manufacturing technology.

6.4.2 Standardisation as a driving force for innovation

Standards create a secure basis for technical procurement, ensure interoperability in applications, protect the environment, plant and equipment and consumers by means of uniform safety rules, provide a future-proof foundation for product development and assist in communication between all those involved by means of standardised terms and definitions.

Standardisation is of central importance for the success of the future Industrie 4.0 project. Industrie 4.0 requires an unprecedented degree of system integration across domain borders, hierarchy borders and life cycle phases. This is only possible if it proceeds from standards and specifications based on consensus. In the Industrie 4.0 Platform, close cooperation between research, industry and the standardisation bodies is required to create the necessary conditions for sweeping innovation: methodical soundness and functionality, stability and security of investments, practicability and market relevance (see fig. 29). For rapid implementation in industrial practice, the concepts need prompt stabilizing by a standardisation process based on consensus and accompanying research.

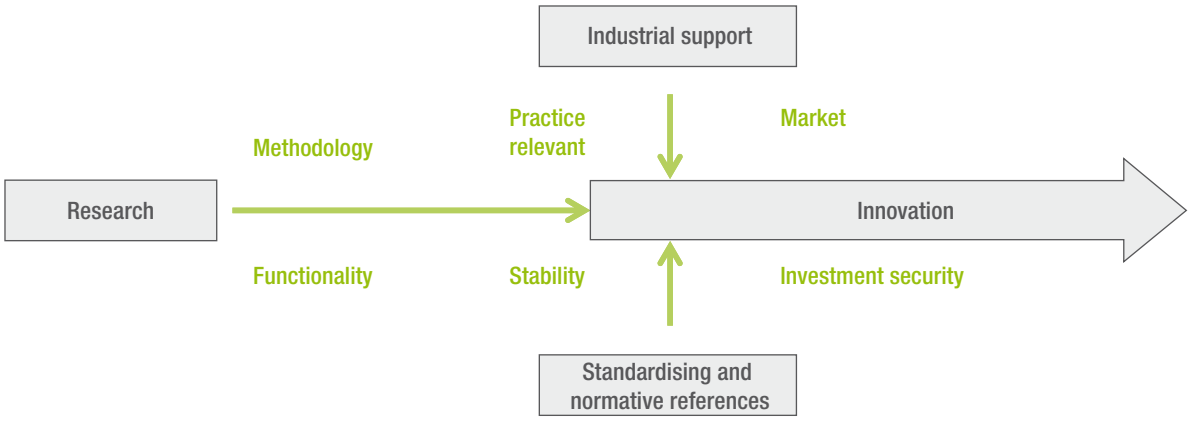


Figure 29: Innovation through standardisation (based on [10])

6.4.3 Cooperation between the standardisation committees

The stipulation of technical requirements in globally valid standardisation systems is of especial importance to an export-oriented German industry and its global operations. The aim must be to gradually set down in international standards all the stipulations essential for uniform technical functionality and usability. The major relevant target standardisation bodies are the IEC and ISO.

For information technology, the globally accepted standards of the IETF and W3C consortium play a central role. The objective of standardisation for Industrie 4.0 is, on one hand, to improve interopereability at the application level and. on the other, network quality.

Consensus-based standards can be established in different ways. Figure 30 presents a diagram of the typical procedures. The starting point is the identification of a particular need for standardisation. This can emerge from feedback from practical applications, from the creation of new technologies, from the results of research or from new regulations.

Considering the path leading to an international standard (ISO3, IEC4), distinctions can be made between three typical routes:

- Direct stipulation within the responsible standardisation committees. In this case, the stipulations to be standardised are compiled and developed within the responsible international committee and its national mirror committees. One example is the development of IEC 61131-3, “Programmable controllers” in IEC/SC 65B/WG 7 and in Germany in the Working Group DKE/AK 962.0.3, “SPC languages”.
- Direct adoption of consortium specifications. In this case, the specification is compiled within a consortium and then adopted essentially unchanged as a standard. Examples include the adoption of the batch control specification ISA S 88 (ISA) in IEC 61512, the OPC UA specification in IEC 62541 and the PROLIST specification in IEC 61987.
- Consensus-based development in national committees with subsequent further development in the responsible standardisation committees. In this case, the fundamental stipulations are prepared within professional associations and published as guidelines or national specifications and then, in a second step, developed into international standards by the responsible standardisation committees.

The alternative routes are shown in figure 5.4.2. 90 % of national standards in the field of electrical engineering are now based on international standards from IEC. IEC standards are agreed in parallel during the compilation process at the European (CENELEC5) and international levels, and then adopted nationally in Germany as DIN standards (Dresden Agreement). There is a comparable procedure at ISO and CEN7 under the terms of the Vienna Agreement.

It has become apparent in recent years that the development and elaboration of proposals for and content of standards by the responsible standardisation committees themselves is increasingly reaching its limits. In many cases, the time available to the voluntary members of the committees is insufficient. For that reason, the alternative route of extensive preparation of standards by consortiums and professional associations has become established in many areas. The Industrie 4.0 Platform will take this approach with respect to partial results relevant to this subject matter.

The committees responsible for standardisation are increasingly taking on the functions of reviewing, facilitation, support, consultation and integration. They ensure that the interested groups are informed of the contents and the planned procedures, and that the standardisation process is based on consensus. Together with these functions and the day to day administrative and editorial tasks, standardisation committees are increasingly taking on an important role in analysing the existing standardisation landscape and initiating and coordinating standardisation projects in strategically important areas. In this respect, they were very helpful from the beginning of work in connection with the Industrie 4.0 Platform project. They are also essential when it comes to pending questions regarding the utilisation of results.

Comparing the objectives of consortiums and professional associations in standardisation, one fundamental difference

can be found: Consortiums attempt in their stipulations to define a complete solution, while professional associations aim to compile guidelines or to standardise individual aspects of a solution. Both approaches will be required around Industrie 4.0. There are a number of relevant technical associations on the national level. In many cases, the associations have a broad set up and are internally organised on a consensus basis so that their publications can be regarded as the common opinion of the relevant professional community and thus constitute a particularly stable and reliable basis both for the further standardisation process and for immediate industrial use. The platform makes use of this. A procedure may be termed consensus-based in this context when the following conditions are fulfilled:

- The specifications are compiled in committees which any professional can join. Membership in an organisation is not required. If the number of members has to be limited, selection is made by a transparent and non-discriminatory procedure.
- The results of the committee's work are published at an early stage as a draft for comment. They can be obtained and commented on by anyone, irrespective of membership in an organisation.
- Prior to being published as a specification, an objection's procedure is available for anyone to raise an objection. The committee decides in open discussion on acceptance of the objection.

When adopted, the specification is published and is available to all those interested, irrespective of membership in an organisation.

With consensus-based specifications, a sound standardisation foundation can therefore be promptly provided, initially at a national basis, for development processes within businesses. These specifications then provide a good starting point for international standardisation. To this extent, the development of the concept for Industrie 4.0 – including in the form of a reference model within the Industrie 4.0 Platform – and its application to international standardisation is consistent.

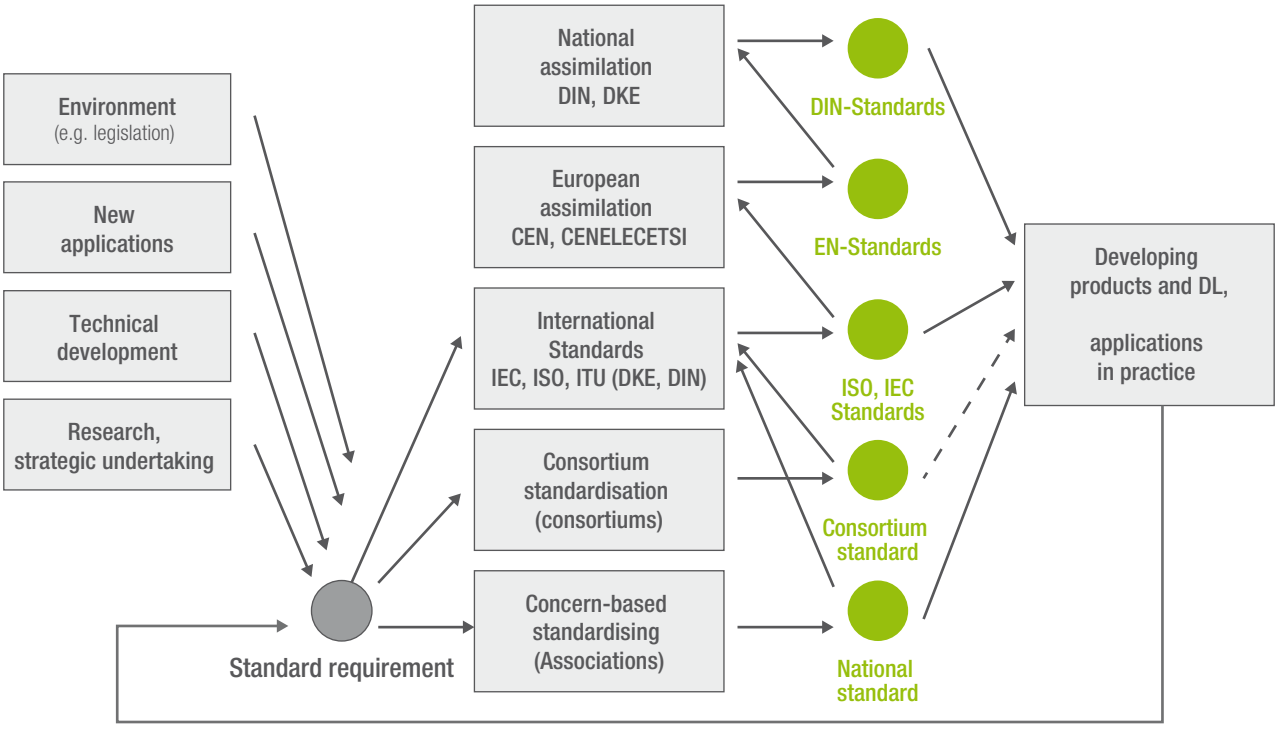


Figure 30: From the need for standardisation to the standard (corresponds to [10])

Document number	Title	Committee
ISO/IEC 62264	Enterprise-control system integration	IEC TC65
IEC TR62794	Industrial-process measurement, control and automation – Reference model for representation of production facilities (Digital Factory)	IEC TC65
IEC 62832	Industrial-process measurement, control and automation – Reference model for representation of production facilities (Digital Factory)	IEC TC65
IEC 62541	OPC Unified Architecture	IEC TC65
IEC 61360-1 IEC 61360-2	Standard data element types with associated classification scheme for electric items	IEC SC3D
ISO 13584-42	Industrial automation systems and integration – Parts library – Part 42: Description methodology: Methodology for structuring parts families	ISO TC184
IEC 61987	Industrial-process measurement and control – Data structures and elements in process equipment catalogues	IEC TC65
IEC 62683	Low-voltage switchgear and controlgear – Product data and properties for information exchange	IEC TC17B
IEC 61804-1 IEC 61804-3	Function blocks (FB) for process control – General requirements Function blocks (FB) for process control – Part 3: Electronic Device Description Language (EDDL)	IEC TC65 IEC TC65
IEC 62453	Field device tool (FDT) interface specification	IEC TC65
IEC 62769	Devices and integration in enterprise systems; Field device integration	IEC TC65
IEC 62714	Automation ML	IEC TC65
ISO/IEC 2700x	Information technology – Security techniques – Information security management systems – Requirements	ISO/IEC JTC1
ISO 15926	Industrial automation systems and integration – Integration of life-cycle data for process plants including oil and gas production facilities	ISO TC184
ISO 8000	Data quality	ISO TC184
IEC 62439	Industrial communication networks – High availability automation networks	IEC TC65
IEC 62443	Industrial communication networks – Network and system security	IEC TC65
ISO 15926	Industrial automation systems and integration – Integration of life-cycle data for process plants including oil and gas production facilities	ISO TC184
IEC 61158	Industrial communication networks – Fieldbus specifications	IEC TC65
IEC 61784	Industrial communication networks – Profiles	IEC TC65
IEC 62591 IEC 62601 EN 300328	Industrial communication networks – Wireless communication network and communication profiles – WirelessHART™ Industrial communication networks – Fieldbus specifications – WIA-PA communication network and communication profile Electromagnetic compatibility and radio spectrum matters (ERM) - Wideband transmission systems - Data transmission equipment operating in the 2.4 GHz ISM band and using wide band modulation techniques	IEC TC 65 IEC TC65 ETSI

Document number	Title	Committee
IEC 62591 IEC 62601	Industrial communication networks – Wireless communication network and communication profiles – WirelessHART™ Industrial communication networks – Fieldbus specifications – WIA-PA communication network and communication profile	IEC TC 65 IEC TC65
IEC 61984	Connectors – Safety requirements and tests	IEC TC65
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems	IEC TC65
IEC 61511	Functional safety – Safety instrumented systems for the process industry sector	IEC TC65
IEC 62061	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems / This document and its separate amendments continue to be valid together with the consolidated version	IEC TC44
VDMA 24582	Fieldbus neutral reference architecture for Condition Monitoring in production automation	VDMA
ecl@ss V9.0	Database with product classes and product properties	ecl@ss
IEC CDD	IEC Common Data Dictionary	IEC SC3D
PROFIBUS International Profile 3.02	Profile for Process Control devices	Profibus International
Sercos	Function specific profiles	Sercos International
Recommendation 5th Edition 2008	XML	W3C
Recommendation 5th edition 2014	HTML5	W3C
VDI 5600	Production management systems	VDI
…..	…..	…..

Table 1: Open list of standards classified as relevant for Industrie 4.0

6.4.4 Conclusions

The development of consensus-based standards is supported sustainably and in the long term by the organisations responsible. These are in particular DKE and DIN in Germany, ETSI, CENELEC and CEN in Europe, and IEC and ISO at the international level. In addition to these mandated standardisation bodies, the consensus-based standardisation committees together with industry associations in the Industrie 4.0 Platform provide particular impetus to standardisation work by developing specifications and proposals for standards. This at the national level, e.g. the VDI/Society for Measurement and Automatic Control (GMA). The established cooperation between these different bodies assists with the customary transfer of the findings of the Industrie 4.0 Platform.

With Industrie 4.0, however, the focus shifts to new subject areas and in particular to a system-oriented procedure. Cross-level and cross-domain strategies have to be developed and subsequently standardised. Based on the results of the work to date, Industrie 4.0 can build on a host of concepts from existing standards. Of course, some of them have to be modified, others expanded, and new standards have to be created. The existing standards domain will support the migration from Industry 3.0 to Industrie 4.0 over the long term. The table provides an open list of potentially relevant standards. This list is, among other things, gradually expanded with ICT standards and is published in the new edition of the standardisation roadmap "Industrie 4.0" from DKE and DIN as a revised version.

6.5 Topic roadmap

The creation and discussion of the reference architecture model 4.0 (RAMI4.0) and Industrie 4.0 components mean that the foundation for further work has been laid. Important pending topics are described below. An important objective in this respect is, on one hand, to improve interopereability at the application level and, on the other, network quality in accordance with requirements of Industrie 4.0.

Identification

Identification is an essential prerequisite to enable the things to locate one another independently. Initial discussions have shown that identification in connection with the movement of goods, identification of the location and identification within the network are required. Different standards exist here; in some cases, supplements offering new technical possibilities are also being discussed.

Semantics

The information layer is an important layer in RAMI4.0. It contains, among other things, the data. Uniform semantics including syntax for the data are needed for the non-proprietary exchange of data. Initial considerations are already being made; the task is now to draw up a concept for a complete arrangement including standardisation. The specification of features in eCl@ss, for example, lends itself as the basis for a comprehensive definition of features for "Industrie 4.0".

Quality of services (QoS) for Industrie 4.0 components

Important characteristics of Industrie 4.0 components are therefore defined. They can be configured and/or accessed. Agreements concerning service qualities between the components should also be possible. With regard to applications in automation systems, these are characteristics such as real time capability, fail safety and clock synchronisation. These characteristics may be described in profiles.

Industrie 4.0 communication

There are already numerous communication connections and protocols in automation technology. There are also new methods from the area of telecommunications and information technology. All of them must be evaluated in terms of their suitability with respect to the requirements of Industrie 4.0 communication and adapted as necessary. The communication layer from RAMI4.0 lends itself here to structuring. The procedure for identifying suitable standards can be effectively explained based on the communication. With respect to establishing standards, all suitable candidates, for example, will be entered in the layer. Overlaps will be discussed and preferred protocols defined. Any gaps will be filled.

Standard functions:

A greater challenge lies in embodying non-proprietary standard functions, which are portrayed on the functional layer of RAMI4.0.

Uniform basic functions must be defined for the simple exchange of information and for interoperability between manufacturers. Therefore, basic functions essential for the exchange of information must be specified in an open manner. This significantly reduces the costs associated with interface adaptation for the user in his machines/systems/factories. The VDMA guideline concerning the definition of conditions monitoring is an example. It defines non-proprietary standard functions as well as a model that every manufacturer can integrate (encapsulate) its own functions in. At the same time, exchanging data and linking condition-monitoring functions continues to be easily possible.

Security of networked systems

7 Security of networked systems

7.1 Introduction

Security is the "enabler" for Industrie 4.0 value networks. Transforming linear value streams into value networks is essential for the development process leading towards Industrie 4.0. The resulting complete networking of all value partners means that more participants will be integrated to an as yet unknown extent and with greater depth as well as, in some cases, on an ad hoc basis in company and production processes. In order to achieve the endeavoured efficiency and productivity gains, the partners must be able to exchange sensitive production and process data with one another. This can only occur on the basis of trust between the partners because central expertise – i.e. the core asset of every company – must be shared, at least partially. Trust is established when it is shown that information and data can be exchanged securely and correctly between authorised partners. Ensuring this is the task of security in Industrie 4.0. If security in office and production systems is not assured, Industrie 4.0 will not be implemented because trust cannot emerge for the sensitive communication processes.

An additional challenge for security is to design not only secure but also user-friendly and easy-to-use implementations to ensure acceptance among customers. Customers ultimately want a plug and operate approach. Furthermore, coordinating with customers in connection with Industrie 4.0 means their wishes will have a greater direct influence on the production process (e.g. see batch size 1 in automotive manufacturing). If the required close B2B and B2C communication is unable to progress in a secure, correct and legally secure manner, it will be difficult to implement the envisioned business models. Security measures form the basis for fulfilling the requirement.

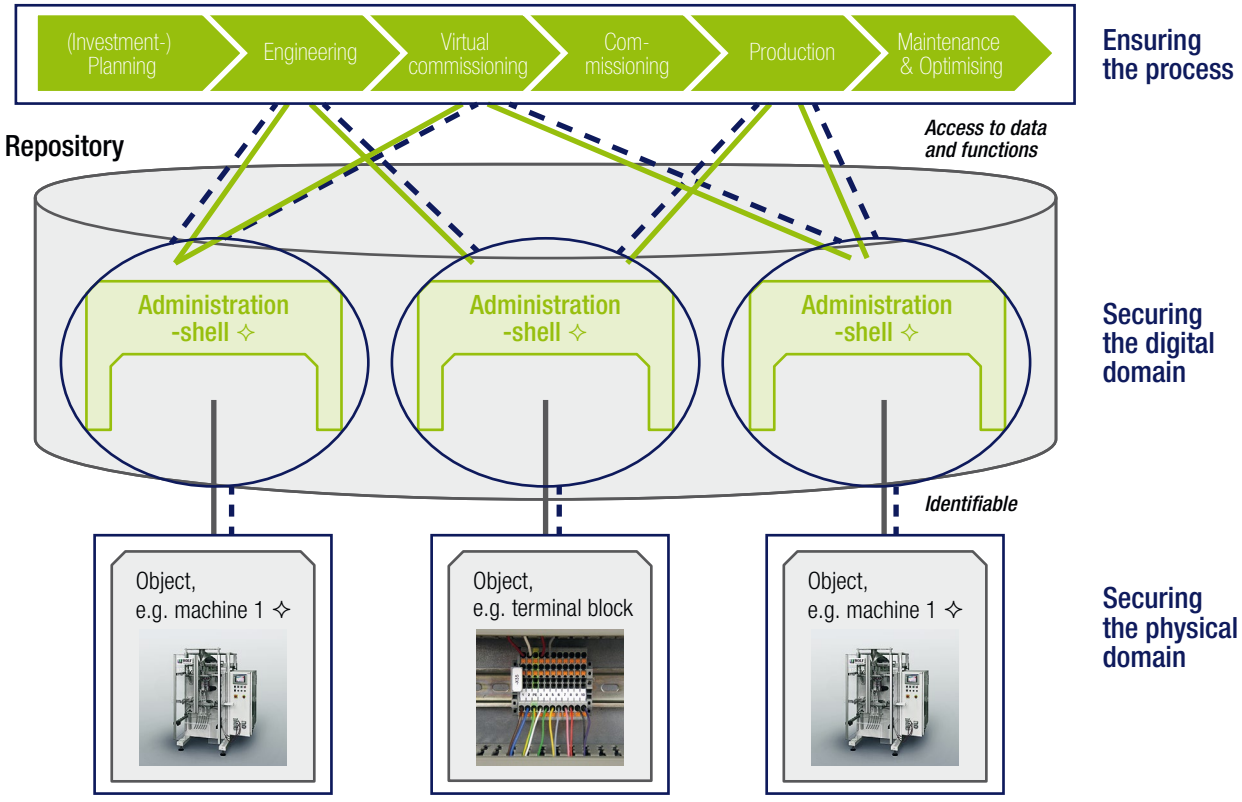


Figure 31: Security requirements

Applied at the technical level of the current Industrie 4.0 development, the following principle applies:

Security that spans the physical and digital domain, the respective processes as well as communication between these areas is a prerequisite for the success of Industrie 4.0. Security that is implemented only in an isolated way is easily bypassed and would be ineffective.

Security is everybody's business

Companies face the challenge of managing multidimensionality both internally and externally. Internally, a "silo mentality" – in the sense of a static linear organisational set up – will no longer be possible with Industrie 4.0. It is conceivable that production processes, for example, will become an integral part of the ERP level (referring to production networks increasingly becoming an integral part of the enterprise network). In the long-term, this development leads to a merger of office IT and production IT and therefore becomes a necessary task for static-linear company organisation. As a result, more tasks will have to be managed and integrated as issues cutting across all areas. End-to-end, ongoing risk and security management in the company will become essential with Industrie 4.0. Multi-dimensionality arises as these management tasks are no longer broken down into "internal" and "external" tasks. Risk and security management must reflect the changes associated with Industrie 4.0, as a result of which external participants will be able to influence to a greater degree traditionally internal processes. The classic "fenced in" and consequently determinable corporate area will cease to exist. In a value network, the boundaries between internal and external corporate domains will be fluid and vary over time.

Against this backdrop, a company will no longer be able to manage its security alone. Even when it takes every conceivable precaution, it cannot be considered secure. Due to the close affiliation with customers and suppliers, where corresponding interfaces could serve as points of attack, security management by customers and suppliers also affects the company's own level of protection. In future, the weakest link will affect the security of the entire value network to a much greater extent.

As a result, one of the principles must be that security is everybody's business in Industrie 4.0. Security is a shared responsibility that cannot be provided by any one participant alone – regardless of how big the respective company is.

Security is a moving target

The need for a multi-dimensional analysis of security in Industrie 4.0 is based on a technical principle that already applies today but which will become increasingly more relevant due to the growing number of interfaces. Security must be viewed as a moving target. The essential questions of "What do I have to be prepared for?" and "What measures have to be taken?" will have to be repeatedly re-evaluated because any security strategy leads to the creation of a corresponding counter strategy, which in turn affects the security strategy. Technical progress also affects methods and opportunities for attacks. Every technical and HR measure can be worked around with enough effort in the form of corresponding technical and HR measures. Security therefore represents an every-changing, dynamic threat that demands constant adaptation. It is impossible to effectively implement a security plan in the sense of "set up and forget". This is, among other things, also a basic difference to the principles of safety/operating safety (= protection of people from machines). Safety provisions are based on fixed and in part legally prescribed provisions and statistically verifiable assumptions.

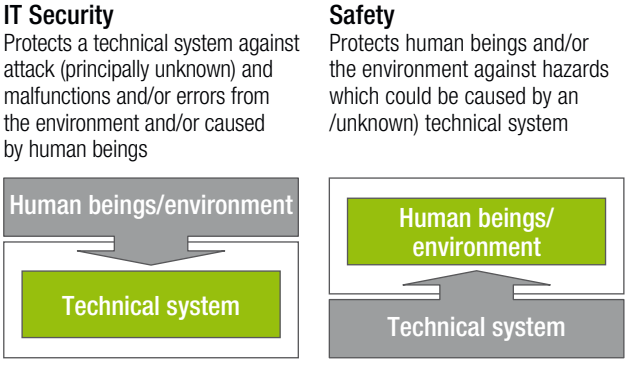


Figure 32: IT security vs. safety

The highly dynamic security environment of Industrie 4.0 value networks demands efficient, adaptable use of security resources. Knowledge of a company's own assets and their need for protection is the basis for this. Alone for reasons of profitability, security measures must not only be adaptable, but made-to-measure. Not all assets require, for example, a high level of security. Company management can only implement the required combination of measures by means of continual risk management. Clarification is required on the basis of what needs to be secured, what is the resource requirement and what is the need for security. The results of an evaluation provide guidelines for all other measures and should be reviewed regularly at extended intervals.

There is no such thing as 100 percent security for Industrie 4.0.

The dynamic nature of the "moving target" as well as technical progress mean that security must be understood as (1) unifying technology, people and processes as well as (2) a specific, on-site analysis of individual cases. Security is not a ready-made product. The required security measures are highly specific to the company. Therefore, a universally applicable security solution does not exist.

7.2 Assumptions, hypotheses and prerequisites

Even if the individual architectures, models and systems of Industrie 4.0 are not yet set in stone, one can assume a certain technical trend: an increase in automated, cross-organisational communication between individual industrial components. From a security view point, this will have multiple consequences. It will be increasingly difficult to establish a "closed factory" unit. It will become increasingly difficult to clearly demarcate between internal and external areas of responsibility. This applies both in a physical and digital/IT-related sense. When very tightly knit communication processes exist in an Industrie 4.0 value network between suppliers and manufacturers, any production-relevant decisions made under real-time conditions mean that a supplier can, under certain circumstances, directly influence the manufacturer's processes. Disruptions to processes may therefore have a reciprocal effect. The ability to control and manage internal flows will decline and mutual interdependence will increase. The decisive sphere of influence that directly effects the company's corporate areas goes beyond one's own capacity to act.

A factory's premises now extend beyond the factory fence. Until now, entry and exit could be monitored both with respect to the physical domain (fence + gatekeeper/watch duty) as well as the IT domain (separation of Intranet and Internet, introduction of DMZs). The classic zone concept will, however, have to change with Industrie 4.0 such that it can be defined dynamically and, when applicable, ad hoc.

Security hypotheses

Together with the core statements described in section 7.1, these developments lead to five security hypotheses. Concepts on future architectures and models for Industrie 4.0 should from the outset take these hypotheses into consideration:

1. The value network itself is a potential attack vector

   The company itself may be protected by a variety of means at the communication and production levels but this may all be in vain if the systems of suppliers and customers are also not effectively secured. In an Industrie 4.0 environment, it must be expect that attacks and failures may be brought about by the systems of external partners. A purely "internal analysis" of the areas under self-control is no longer sufficient. Particularly in cases where, for example, supplier partners change, appropriate precautions, security coordination and audits should be part of business agreements and relationships. Mutual (contractual) agreements concerning security precautions are required for this.

2. Safety functions are becoming increasing vulnerable

Due to the increasing degree of networking at all levels of industrial production, the number and severity of opportunities for manipulation and sabotage rise accordingly. Unauthorised infiltration into the actual functional control of machines is becoming increasingly possible. In an extreme case, no area will be free from potential manipulation.

If digitalisation in Industrie 4.0 reaches the deepest functional controls of machines and systems, possibly also encompassing safety functions (e.g. emergency deactivation, clamping protection, electrical shielding, burn protection etc.), these also become open to attack. To date, safety functions have been separate and in some cases, set up as redundant to ensure the highest level of availability and reliability. Networking in the Industrie 4.0 environment can now lead to more technical interfaces and "points of contact" between safety devices and other devices. Systems therefore theoretically become more accessible. This means that in the event of a security event (e.g. external attack by a hacker), a safety event can be triggered (e.g. manipulation of the light barrier control of a clamping and crushing protection system of a metal press). The intentional separation or encapsulation of safety and other systems that has existed up to now will disappear. To achieve flexibility, it will be increasingly difficult to uphold the imperative for fault-free operation.

This becomes particularly controversial in areas where people work closely with machines such as in robot-assisted manufacturing. As a result, the areas that have up to now tended to be regarded as separate from one other – and currently standardised only in terms of safety – are to be increasingly considered as interdependent with a corresponding adaptation of protection concepts.

3. Detection and response capabilities are part of the basic setup

The analysis of different security events makes it clear that any protective measure can be circumvented if enough effort is invested. The core statement "there is no such thing as 100 percent security" means that any product or measure is unable to offer fool-proof security. Today, the average time needed to detect an attack amounts to several hundred days while at the same time an increasing number of attacks are going undetected by affected companies.

Even the combination of various technical and organisational measures is reaching its limits when potential attackers have ample time not to mention research and security expertise (so-called APT attacks). Such strategic, persistent attacks aim to remain undetected by conventional security measures.

Government funded organisations are taking a similar approach, but their opportunities for attack, on processes such as relationships based on trust, people and technologies, are again much more far-reaching. Preventing such an attack, depending on how professional it is, is not economically feasible.

With respect to conventional attacks and cyber crime, the level of capability is also increasing. Sooner or later, an incident will occur. The firewall that can keep everything out will no longer exist. This means that capabilities must also be available on an as-needed basis in order to detect incidents, respond to them and resolve them as quickly as possible. The robustness of security measures as an interplay between preventative and reactive measures (detection capabilities are implicitly included) will be decisive for the security of Industrie 4.0 under the aforementioned assumption. In future, it will probably not be possible to detect professional attacks swiftly let alone in real-time. Particularly for small and medium-sized businesses, it will become more common for companies to learn of a security breach or new forms of attack after the fact and from external parties.

The necessary strengthening of capabilities for detection and response permits, however, detecting APT attacks during or after they happen, or at least to accurately analyse the scope and severity post-attack and improve response measures. As a result, companies are put in a position to detect more, which will likely increase awareness, but also to respond in a more effective and consequently more cost-efficient manner.

4. Detection capabilities within the office domain must be developed and made available for the production realm

The current focus is on securing office communication systems. This is attributed to the situation that common attack vectors and vulnerabilities have to date concerned office systems (e.g. operating systems, browsers, Internet-based communication, data storage devices etc.). As a result, conventional protective measures focus on exactly these areas (e.g. virus scanners, e-mail and hard-drive encryption, monitoring of data traffic and data access etc.). Widespread implementations such as "intrusion detection systems" do not exist for industrial communication within the production domain. Industrial attacks such as Stuxnet show that such programs can be active for months or years before being detected.

For reasons of protecting expertise, companies have a considerable interest in being informed and ready to take action. As a result, such "blind spots" on the security map must be identified and systematically resolved. This also means that organisational, HR and technical security investments must be made in fields that have not been considered to date.

5. With Industrie 4.0, distributed data storage will become one of the main challenges in terms of security

Many services may emerge in Industrie 4.0 through the application of big data, predictive analytics and intelligent sensors. The involvement of data experts and analytical programs will achieve the potential for efficiency gains (e.g. reduction of material scrap in metal pressing through the data-supported adaptation of the punching process). Very specific process, machine and system expertise will be necessary for the analyses. This means that operators may, when applicable, submit their data to external service providers and/or the manufacturers for analysis and/or integrate them in data traffic via interfaces. Cloud and other data platforms also enable location-independent industrial control and production.

Data generation, transfer and processing in production will, under certain circumstances, occur digitally and using external platforms. This will increasingly confront operators with technical, security-related and legal challenges. The company will, when applicable, use an additional critical infrastructure, involve an additional external participant and will only be able to control this participant's influence on the data to a limited extent. If the provider of the data platform is beyond the company's own jurisdiction, contractual provisions and sanctions are more difficult to implement. Due to the required, permanent technical accessibility of such platforms corresponding to requirements of a value network with vertical and horizontal networking, a multitude of potential attack vectors exist. If data protection and information security is not thoroughly assured, achieving distributed data storage under Industrie 4.0 will be unlikely.

The principle of security development: Security will be implemented as migration and depending on the initial situation within the company.

Development of hypotheses will be based on the relevant context and not be independent of the current initial situation. All security concepts will build on existing systems and plants. The fundamental shift from security as a subordinate, follow-up topic towards the security-by-design approach will gradually unfold across the different system and component generations. The same applies to the further development of security standards. In many areas, existing rules need to be adapted rather than the creation of entirely new standards. Security features will also continue to be incorporated purely as a cost factor in company decision making. Accordingly, larger companies, due to

economies of scale, will have an easier time making such investments and replacing systems in order to implement new security levels. Particularly small and medium-sized businesses will not be able to make any comprehensive investment in security.

Developments such as intelligent sensors combined with big security data will also lead to the introduction of new opportunities for security measures in areas which today still remain isolated and proprietary, and where manipulation therefore often goes undetected.

7.3 The Industrie 4.0 world of threat

It can no longer be disputed that IT in office and production realm is exposed to threats. Last year in particular, a large number of vulnerabilities were disclosed in applications and systems. This was accompanied by various successful attacks on companies which have since become public. One such attack constituted the "Havex" malware that became public in 2014. It strategically collects information on industrial monitoring and control systems. In the process, this data may concern production instructions or infrastructure-related data that could be used for future attacks. There is the possibility of loading additional modules that could damage a system.

In connection with this attack, the websites of numerous system manufacturers were manipulated. If a system connects with the manufacturer site in order to perform a software update, the communication undergoes attack. From the customer's standpoint, the attack appears to be a plausible and legitimate communication between the system and the manufacturer and presumably does not at first attract attention. As other modern attacks are also concealed by legitimate access operations, companies face new challenges when it comes to detecting security incidents. In many cases, it is only possible to detect such incidents – if at all – after the fact. This can be much more cost-efficient than completely reinstalling the entire infrastructure. It must be assumed that a significant dark number exists with respect to other attacks on companies. In this respect, damage ranges from data theft and blackmail through to operational and production process manipulation.

This should make it clear that threats to production systems already exist today which companies need to adapt to. With the trends described above, Industrie 4.0 offers new opportunities in terms of productivity as well as process and system improvements. This also includes administration shells for the Industrie 4.0 components. Through increasingly dynamic communication and participating service providers, there will unfortunately also be new opportunities for attack that will give rise to new threats. These threats apply equally to both the administration and automation networks.

In many cases, systems warranting special protection cannot not be accessed from the Internet; this commonly holds true for the production realm. Attackers use a two-pronged technique here: They start by attacking a computer where malware has been installed in an area with less protection. Additional attacks that infiltrate deeper into the company are then carried out from this computer. This type of infiltration often follows a long-term strategy with minimal invasiveness and is therefore only detected late or after the fact. Corresponding strategic attacks, e.g. Stuxnet, are known as Advanced Persistent Threat "APT". The so-called "air gap" no longer constitutes an adequate security measure.

There are commonly three types of attackers: Intelligence services, cyber criminals and cyber activists. Cyber criminals want to earn money illegally through their activities. They do so by blackmailing companies or private persons, threatening to delete certain data or to shut down systems. Cyber activists pursue political or ideological objectives. They range from the theft and publication of internal company information and extend through to DDoS attacks and the deactivation of systems. The task is to protect one's own company from these two groups. In the case of attackers from intelligence services, it is practically economically unviable for a company to rule out all attack routes due to the virtually unlimited resources available to such attackers.

In addition to such targeted attacks, companies should also protect themselves against unintentionally caused problems such as human error or attacks without a particular motive – so-called "rive-by attacks[13]". This may involve the distribution of harmful programs between the administration and automation networks, but also the unwanted incorrect configuration of systems.

The development of attack software is becoming increasing professional and is noticeably and increasingly targeting the area of automation. The goal is initially to spy. One example of this is the "BlackEnergy" malware: It targets HMI systems from certain manufacturers and, once modified, goes unnoticed as it misuses affected systems for further analyses. The current malware has been revised and improved several times since 2008 and can now be supplemented with additional functions on the basis of modules. It is attributed to an espionage group[14], which had recently targeted vulnerabilities in programming software for HMI and SCADA systems.

It can also be assumed that an upstream espionage phase occurred before the attack on the blast furnace of a German steel mill [8] – in any case, the absence of findings regarding the events of the attack suggest this.

7.3.1 Company assets

In order to explore threats to a greater extent, what is of value to a company must be considered. In the context of security, a system, part of a system, but also an alloy or recipe data or a service may be the core asset to a company.

To date, primary focus has been on the availability of a production system. With respect to recipes, the focus lies on confidentiality. These are only two examples of assets of existential importance to a company because extensive resources can be invested in research and development in this area. Further assets in the form of services also exist due to emerging trends and new techniques being introduced or integrated in production. Such assets may be IT systems (for accepting orders or production coordination), which did not play a central role in the past, didn't exist at all or which were previously operated in isolated areas. Examples are the digital identities of products and components or the legally-secure issue and management of electronically negotiated contracts.

The new threats in connection with trends and developments will be explored in greater detail below.

7.3.2 Availability and reliability

Company processes are supported by systems. A system may be a machine, a section of plant, but also an IT system. An administration shell for an Industrie 4.0 component also falls under this area. With Industrie 4.0, it is expected that there will be a further increase in systems required for operations as well as interfaces for cross-organisational communication and increasingly dynamic operating processes.

If these systems or their interfaces are not available, it affects, to a greater or lesser degree, company processes, value creation and therefore financial aspects. Critical disruptions to production or other services pose a direct threat to a company. Other threats are also possible which give rise to the need for the coordinated deactivation of systems – for example, to prevent physical damage.

Distributed-Denial-of-Service (DDoS) attacks pose a risk for every externally accessible interface and are difficult to safeguard against. They involve submitting a large number of requests, for example to overload the recipient with requests or take up the entire available network bandwidth making it impossible to process legitimate requests. There are already a number of examples of companies being driven to bankruptcy by a persistent DDoS attack associated with access to their systems [8].

With Industrie 4.0, there are more time-critical processes and services leading to additional points of attack for DDoS.

13 Attacks where a user is directed to a prepped website where a vulnerability in the web browser is used to compromise the user's systems.

14 "Sandworm"

If work occurs almost in real time in industrial environments with highly dynamic data, there is little room for the corrective measures customary in office IT security. At the same time, the data to be processed not only has to be exact, it must also be received and processed by different systems synchronously. SCADA systems calculate different process data received from different systems, automate them and forward control commands based on the calculation. A communication error affecting the data required for calculating control commands could become a challenge in a dynamic Industrie 4.0 environments (example from the energy sector).

7.3.3 Safety as a goal

The aforementioned increasing degree of networking and collective use of resources within a company is also occurring to a limited extent with safety components. As a result, they are being operated to an increasing degree with other systems within a common network. This means that safety components are also exposed to the same attacks via the network as other components. At the same time, attacks on the safety function as well as indirect attacks on availability are possible.

Indirect attacks on availability

Attacks on safety functions pose the threat of emergency shutdowns of systems or machines. This can happen, for example, by overloading of the component by a large number of requests, by overloading of the network in use, or by a software error in the component which causes a designated safety function to activate. The actual function of the safety component remains in tact in such cases so that there is no risk to people or the environment; nonetheless, this results in impairments to the production process.

Attacks on the safety function

In a worst case scenario, the exploitation of vulnerabilities in a safety component may lead to manipulation of the function – e.g., threshold values are changed. This leads to functional safety (including safety and security) no longer being assured. In such cases, harm to people and the environment can only be assured by further protective measures, such as a mechanical system. As the relevant protective functions are prescribed by legal guidelines (e.g. the Machine Directive), the integration of security requirements for the fulfilment of safety requirements is already being worked out in standardisation committees.

7.3.4 Integrity

The integrity both of the data used for production as well as the recorded data is of utmost importance.

Attacks on data used for production negatively affects the quality of the manufactured products. In an extreme case, safety-relevant characteristics of the product could, for example, be modified resulting in subsequent injury to persons or property.

The integrity of records for tracing production processes is also relevant because, depending on the sector or product, of questions of liability or regulatory guidelines such as those in the pharmaceutical industry.

For the reasons described above, nearly all sectors prioritise integrity, if only implicitly with reliability being viewed as the most important aspect by those involved.

In the cross-organisational value networks in Industrie 4.0, integrity is supplemented with the additional question of authenticity[15].

As adequate synchronisation is needed for the coordination of processes in Industrie 4.0, the integrity of time also becomes relevant.

7.3.5 Confidentiality

Already today, certain information – in many cases, time-limited information – requires confidential treatment. This includes recipes, design data or control programs. This data constitutes a substantial asset for a company due to the resources and knowledge expended to obtain it.

The term "data theft" is normally used for the undesired outflow of information. But it lacks accuracy because data is not actually stolen but rather copied leaving the original in place. A major challenge around "data theft" is that it can easily go unnoticed.

A particular problem in data theft or unauthorised access to data is the lack of options to reverse the process or to take protective measures. From the first instance of data loss, the company loses complete control over further instances of unauthorised access. There is no fall-back position as with safety. It is therefore recommended to consider relevant measures during planning and above all, to ensure that data of critical importance to the company is labelled as such and that proper handling of such data has been formulated.

To date, the company itself is responsible for preventing information from being stolen or published. In Industrie 4.0, this responsibility also extends to affiliated companies. It is therefore important to define appropriate contractual rules for labelling, handling and responsibilities to ensure that critical data is treated in a confidential manner. When classifying data, it should be considered that some data, for example as a finished product or a machine, is already beyond a company's control. The dimensions of a finished product can be determined by a competitor; in such a case, confidentiality prior to disclosure is particularly important, but later reconstruction based on the product is very easy.

An example of processing of sensitive data is a transfer of design data to a contract manufacturer who is to manufacture a certain quantity of products. It must be ensured that the contract manufacturer only manufactures the requested quantity of products and is not able to use the information further.

Another example concerns remote access for maintenance work. In this respect, the machine builder may have extensive access to a machine or production network. In this way, data concerning the level of utilisation and production can be extracted from the system as can other data from the production network when adequate protection is absent.

Independent of sensitive data is personal information. Particularly with respect to the batch size 1 aimed at by Industrie 4.0, it must be excepted that personal information concerning production orders is also processed. In this case, legal obligations must also be considered and protection must be assured.

7.3.6 Manipulation (intended and unintended)

Sabotage and human error represent a known problem. They commonly occur today. Based on increasing networking within companies and the resulting cross-organisational value streams, the consequences may be further-reaching and less controllable. This particularly applies when insufficient responsibilities and forms of communication as well as (on a technical level) insufficient network segmenting or access control occur due to more dynamic requirements (at a procedural level).

15 See "Identity theft" threat

The greater number of potential access points further increases the risk of unauthorised access by intruders. The access points at risk include unmanned stations, open or unsecured network access as well as connection points to other companies (e.g. for maintenance or order processing). A new quality will emerge with Industrie 4.0 from increasingly dynamic, cross-organisational networking. Attacks targeting contract partners are increasingly likely from affiliated companies. To analyse attacks, there will be increasing reliance on security management at the contractual partner's establishment.

The outflow of information is particularly at risk; it is, however, also plausible that manipulated order or production data is uploaded. Consequences could involve unauthorised access to sensitive information or manipulation of machines and system parts including their deactivation or destruction.

7.3.7 Identity theft

Relationships based on trust play a critical role with respect to safety measures: If, for example, a website is visited, the user trusts that the address transmitted will not lead him to an entirely different, harmful website – which may have been manipulated for this purpose. The web service in turn trusts that the logged-in user is also who he claims to be. This relationship based on trust applies both in private dealings and in business dealings and is generally supported by safety measures (confidential login data, token key and unique biometric data).

The risk of identify theft now occurs with an attacker claiming to be an entirely different person and obtaining this person's legitimate access rights. Authentication in access protocols can not then differentiate the attacker from the real, legitimate user. There are a range of methods for curtailing the risk. Publicly accessible services (e.g. Gmail) can determine where a user is located physically – and alert the user of multiple logins from different countries. If the actual user logs onto the system, he is informed of the potential security breach and is able to confirm or deny it. In many cases, interaction with the applicable person is required for confirmation. Following feedback, the verification process can be further improved and at some point fully automated.

In Industrie 4.0, identity theft poses a serious threat to the availability of systems and confidentiality of information for two reasons:

The constellation of persons, services,, systems and sensors involved is capable of dynamic change. This means a large number of identities and a large number of possible attack vectors. Furthermore, machines are unable to be flexible in decision making. This makes it difficult to recognise, improve and automate security measures. The problem here has less to do with machine-to-machine identification and more to do with an attacker claiming to be a machine. It is expected that a central surveillance body is needed which records the range of identity factors such as login data, communication behaviour or data volumes exchanged, and passes on cases involving potential identity theft for investigation.

7.4 Protective goals for Industrie 4.0 and security requirements

Industrie 4.0 with horizontal and vertical value streams is significantly driving forward the networking of machines and systems as well as closer linking between company IT and the Internet. Protection against outside attacks and protection against manipulation by so-called insider intruders must take into account the increased requirements from Industrie 4.0.

For Industrie 4.0, smooth cooperation between industrial security (security in production) and IT security (office) are a fundamental prerequisite. This interplay must be organised with the goal of a common, secure and standardised IT infrastructure.

7.4.1 General protection targets

Current protection targets within the production realm have the same high priority within Industrie 4.0:

- Availability
- Integrity
- Protection of expertise/confidentiality

In addition to these are:

- Authenticity
- Integrity of time, particularly with respect to value networks that extend beyond company limits
- Traceability
- Legal security

Authenticity is an essential characteristic in a value network, particularly if communication occurs beyond company limits. The need for traceability also results from data protection requirements as soon as personal data is processed, e.g. from employees and customers. Overall, technical assistance on privacy/data protection in the form of security mechanisms takes an important role.

These protection objectives apply equally to operational functions, surveillance functions and protective functions (e.g. safety). Safety ("functional safety") for systems means ensuring, by taking suitable measures, that the function of a machine or a facility does not pose a risk for people or the environment. In this respect, freedom from retroactive effects of security must be ensured in every special profile.

7.4.2 Security-by-design for Industrie 4.0.

For the implementation of Industrie 4.0, prompt consideration of measures for protecting information security is imperative. Rather than retrospective integration of technical mechanisms for security, an integrated approach associated with product development and processes is needed for the protection of systems and infrastructure.

The goal is to implement the required security functions as an integrated part of a product and/or solution. In addition to clearly setting down, from the very beginning, security in the appropriate standards, there are consequences for manufacturers and operators of systems.

Comprehensive supplements to existing processes will become necessary.

Existing development processes must be adapted. To effectively apply security requirements, threat and risk analyses are needed that particularly consider the relevant applications for producing the product. Protection objectives for security measures for a product are based on the manufacturers' assets requiring protection, the integrators and operators and, when applicable, the (in many cases, country-specific) regulatory guidelines from authorities, for example, for scenarios associated with critical infrastructures.

The security design must consider the life cycle of production systems – which in many cases exceed 10 to 15 years.

Following identification of assets requiring protection, a threat and risk analysis is performed. Possible security measures are selected based on the identified risks. Economic aspects also play an important role in this respect. Security measures are only accepted in the market if they match the business model of the target architecture, and any associated financial expenditure is manageable.

When selecting cryptographic components, export guidelines and the associated processes must be considered. This concerns in particular functions for the encryption of data; dedicated authentication or integrity mechanisms are less critical.

If products with integrated security are to be used in a range of areas, this may result in a range of measures (profiles) for implementation which must also support different security levels.

Current security analyses often focus on functions in connection with network security such as firewalls, VPNs, remote access to the network, etc. This will change with Industrie 4.0: Complex, distributed applications must contain a priori security measures with security by design. Security profiles must be "agile", i.e. it must be possible to dynamically adapt and negotiate them. Fast (re)configuration must permit inclusive security.

Traditional quality measures must be supplemented with typical security measures. Included here are:

- Vulnerability tests, penetration testing
- Integrity assurance of production processes, particularly with respect to security protocols and crypto functions
- The required certifications (e.g. in accordance with IEC 62443) which, depending on the intended security level, lead to time-intensive effort and substantial additional costs for specific cases

In addition to the management of explicit security functions at a procedural level, the secure implementation of software-based applications must also be ensured. Training by the software engineers involved as well as strategic quality testing of findings on vulnerabilities are necessary for consistent implementation. Information emerging from quality tests must be analysed and incorporated in the design process.

7.4.3 Identity management

A necessary and essential characteristic of a participant (machine, user, product) in an Industrie 4.0 value network is a distinct identity resistant to forgery and represented by a digital certificate. In addition to authentication codes, digital certificates contain the necessary information for encryption and decryption.

Reliable and trustworthy storage mediums are required for the recording information relating to security. Security protocols and applications with integrated security must be supplied with the required login data. The prerequisite for this is an identity infrastructure (with one or more instances depending on the complexity), along the value network which guarantees the unambiguous and consistent identification and attribution of the identity of a participant and supports the authentication and awarding of rights on the basis of identities.

Trustworthy certification authorities (CA) are needed as administration instances for digital identities (certificates) of all participants in an Industrie 4.0 value network.

To ensure efficient identity management, security login data/codes for participants must be personalised with secure identities and/or paired with the device.

Identity management must provide end-to-end support for the protection of intellectual property (IP protection). This includes, among other things, product and production models. A system of digital management of rights that is user acceptable and applicable is an important prerequisite for this.

7.4.4 Dynamic configurability of the value networks

Efficient value networks require dynamic configuration/reconfiguration of the Industrie 4.0 system. Security management must support the dynamic nature of the Industrie 4.0 system. A description of the security characteristics of an Industrie 4.0 component (security profiles) with a standardised language (security semantics) is necessary which also contains a clear description of the communication interfaces/protocols and their security characteristics.

The security characteristics must be part of the semantics of the reference architecture.

The description must highlight which security capabilities the Industrie 4.0 component has and which methods the required security level can achieve in the value network.

In general, security functions in components must support different security levels in order to accommodate current requirements for a value network. These prerequisites must make it possible to evaluate the resulting security level of an Industrie 4.0 system through the aggregation of security profiles of Industrie 4.0 components.

The security profiles must be capable of supporting the required flexibility from the dynamically changing value networks with adequate protective functions. This leads to a substantial standardisation requirement for the heterogeneous system landscape of Industrie 4.0 (cf. KITS Roadmap – standardisation roadmap IT security, DIN/DKE, 17 February 2015).

Overall, the classic analysis (communication and network-centric security) will defer to a complex security architecture for the application level.

7.4.5 Security for the virtual instance

The "virtual instance" of production plays an important role in Industrie 4.0. In addition to the physical implementation of security requirements, appropriate security for the virtual representation is also required at the same time.

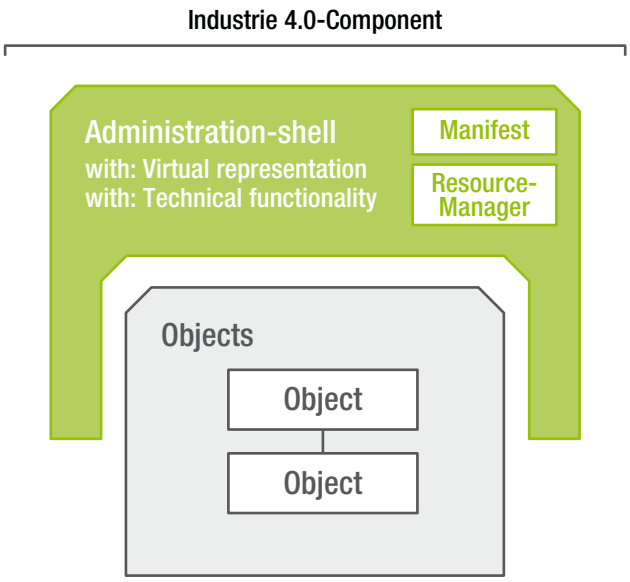


Figure 33: Industrie 4.0 component:

From a logical point of view, an Industrie 4.0 component comprises one or more objects and an administration shell which contains the data for virtual representation and the functions of the technical functionality.

Requirement:
Depending on the nature of the higher level systems, it may be necessary for the administration objects to allow for deployment in more than one higher level IT system.

Depending on the distribution of the "virtual instance" (office platform and/or in the cloud), different security framework conditions may arise than for its physical implementation. Of course, interaction with the physical level must be designed to be secure and traceable. Complex security architectures are therefore required for the application level. Protection of expertise and integrity are particularly important requirements in this respect. Classic domain boundaries for security are not simply portrayed in the "virtual model". End-to-end security will become an important aspect. A "virtual instance" in connection with recovery functions may make a very positive contribution to implementing security architecture because the virtual instance should also contain all the information needed for restoring the physical environment following a security incident.

7.4.6 Prevention and reaction

Prevention and response are equally necessary: Complete Industrie 4.0 security solutions cannot exist without further action being possible.

Attacker expertise and equipment continue to grow. As a result, attack vectors are continually changing and require ongoing development of effective countermeasures.

In addition to preventative protective measures, response mechanisms are also very necessary (monitoring and event handling, incident management). Standardised semantics for security messages with rule-based analysis may create the prerequisites for active response management. Bundling activities in a security operation centre (SOC) with 24h availability 365 days a year provides the operational prerequisite for the focused documentation, analysis and evaluation of all security aspects.

Security is not a "one-off topic": Security cannot be achieved by taking action on just one occasion; the threat situation is constantly changing due to new technical possibilities for potential attackers or the discovery and disclosure of vulnerabilities in standard products and components. Manufacturers and operators must be able to respond to them with patches and updates; possibilities for implementing new security versions must be identified and incorporated in the planning process. The costs for security are substantial both for manufacturers as well as for operators; therefore committed efforts must be made in all processes to prevent over-engineering.

The implementation of comprehensive security architecture remains the priority. At the same time, overall architecture and all processes must be considered in connection with standardisation, development, production and management.

Security is and continues to be, for the most part, a process topic and is not assured by an individual security chip.

Adaptation of the IT structures must be pursued taking the special framework conditions of the production environment into consideration.

7.4.7 Awareness, training, further education

Organisational measures play a key role. Training of the personnel to raise the awareness of security measures and their necessity must be established in every organisation involved (manufacturers, plant manufacturers and operators). This facilitates understanding of the measures and enhances the quality of implementation.

Infrastructures and personnel must be provided with relevant training on security management functions and processes (key management, audit functions, event handling). User guidelines provided by the manufacturers of products and solutions must be integrated in the processes. This includes the handling of passwords, data and data storage devices, regular data backup etc.

7.4.8 Handling

It must be possible to operate the industrial security function without detailed prior knowledge. This applies particularly to rectifying problems in connection with maintenance and other services. In particular, plug & operate must be pursued for security solutions.

7.4.9 Standards and guidelines

For this reason, industrial security, particularly with respect to Industrie 4.0, is currently a topic of discussion in associations and standardisation committees.

The international standard IEC 62443 "IT security for industrial control systems – network and system protection" creates a framework with assessment criteria for industrial security based on four security levels. Seven fundamental requirements for IT security from industrial automation systems (foundational requirements, FR) are detailed in system requirements (SR) and requirement enhancements (RE). A security level (SL 1.4) is based on a set of SR and RE.

When integrating components into a system, the security capabilities of the components must be taken into consideration according to the required security level. At the same time, processes must be designed to permit the achievement of the required security level.

It is expected that the IEC 62443 will be used in the future for certification.

The process model for information security in industrial automation, which is known from VDI Directive 2182, interconnects with the activities of the component manufacturers, the machine-builders and operators. The operator identifies and evaluates potential vulnerabilities as part of a risk analysis. The manufacturer must by default make the necessary information (including the relevant network characteristics) available for the integrator/machine-builder and/or operator to determine security concepts and solutions. This directive has been incorporated in IEC 62443.

The ability of the organisation to establish and implement security processes can be determined with appropriate benchmarks.

The demand from Industrie 4.0 value networks for dynamic configuration is orthogonal to valid regulatory and normative guidelines, which will lead to a loss of certification/operating license in the event of change. Therefore, a set of rules that accounts for the dynamics is required. Consistent self-protection by all participants with security mechanisms free from retroactive effects is a prerequisite.

7.5 Examples of IT security measures

The examples of measures that are presented in this chapter must be understood as a generic tool kit that serves to present selected approaches for determining the direction in which IT, technical departments and/or central departments such as a security competence centre can develop and implement effective measures for improving IT security in a company. Such strategies are described in particular which are, from today's standpoint, expected to be highly relevant tomorrow, but are not currently widely disseminated and implemented. As such, the descriptions represent an excerpt from the current discussion concerning the transformation of industrial security that must occur for Industrie 4.0, and do not represent a conclusive catalogue of measures. Further development on a conceptual level up to series production demands much more detailed requirements.

7.5.1 Security architecture

There are multiple measures at the architectural level, which must be considered with respect to the conception of security for Industrie 4.0 (security by design).

The segregation / separation of duties currently takes place in production usually only between administrative and user authorisations. The components are typically operated using a super user administrative log-in with full rights, who often has rights that also go beyond the boundaries of the production domain. This is due to the fact that in production, the focus has, for understandable reasons, been on the goals of protecting the availability and integrity of data and less on confidentiality and authenticity. This will (has to) change with Industrie 4.0 as the probability of a successful cyber attack on an unprotected component connected to the Internet is very high. The effects are all the greater when such a component is also operated with full administrative rights extending beyond the limits of its own domain. To the extent the protective goals of confidentiality and authenticity are neglected, this may – e.g. by means of a cyber attack over the Internet – also have short, medium or long-term effects on the availability and integrity of the data. This example makes it clear that the division of the system design – i.e. from modules, machines and entire production systems through to value networks – is a necessary architectural measure in multiple areas separated from one another. Separation here may be of a logical and/or physical nature, and may also refer to the existence of information assets in saved or transferred form or to domains separated according to access, which results in domain boundaries for authentication. These separations can in turn be vertical (administrator- versus operator-login in the same module) or horizontal (segregated administrator and operator accounts for different modules). This refers to the installation of isolation limits in the right areas of the design following analysis, particularly in combination with differentiation of known critical aspects e.g. safety-relevant parts. In a – likely impracticable – maximised form, each function represents its own security domain and has its own access controls, rights and other security functions.

Network segmentation is clearly associated with this and is a regular topic in security: the clearly defined differences between "inside" and "outside" and/or between different trustworthy network areas or zones requiring various degrees of protection blur to an increasing degree in Industrie 4.0 scenarios in favour of fine, granular differentiation at the (sub)-component level. Firewalls are either permeable due to the numerous systems having to communicate via the Internet, or so complex that hardly anyone is capable of gaining an overview of the numerous rules, which poses the risk of some rules cancelling each other out.

Even in the case of effective rules, their number increases so much that prompt inspection of ongoing communication becomes increasingly difficult. This trend continues to grow with Industrie 4.0 as advancing automation increases the overall density of temporal flows. This leads to perimeter protection – in the form of firewalls and structural safety measures – becoming increasingly less effective and consequently less important. It is therefore crucial that the prerequisites that are to change with Industrie 4.0 are in future considered in the design of individual components and workflows. A more important measure is to organise separation at the communication level so that it is significantly more granular, and at the same time to move from a formally implemented separation – in the form of firewalls with relatively static rules – to a system that combines the following methods: Firewalls with more generous rules which define non-negotiable barriers for communication – in this case, everything that is absolutely not permitted in Industrie 4.0 production is inhibited, e.g. intervention from a higher-level external control centre attempting to control an internal, decentral actuator. A further supplementary method involves separating different modes of production units from one another by permitting or suppressing rules of communication depending on the mode. For example, a classic remote maintenance situation where communication with other production units is prevented while remote maintenance is performed. This approach to refining communication management can be expanded to other dimensions; the details depend on the requirements of future production communication networks.

"Defense in depth", as an architectural measure breaks, on the one hand, with the habit of viewing the production location as an isolated island where steps must be taken to protect it against external access and, on the other hand, with the assumption that the required level of protection can be achieved with a single countermeasure. Instead, every component and ultimately every information asset is considered a stand-alone component warranting protection and is to be protected, for example, by means of authentication or encryption.

At the same time, it is taken into account that different attackers and attack capabilities exist and, based on defence in depth, every intruder type, in the best case scenario, ideally fails to clear the corresponding hurdle of measures as early as possible. Therefore, combinations of suitable countermeasures are used at different levels to arrange the most suitable protection in a cost and performance-efficient manner. As well as infrastructure, this also covers transmission paths and the protocols used for data transmission. "Defense in depth" can begin with the encryption of data that is processed within the component and (temporarily) saved, and range from special data transmission protocols and authentication / authorisation of access to data and extend up to end-to-end encryption. It is therefore immaterial whether the attempt at access comes from a human or machine. The combination of measures that provides the best overall protection must be determined in individual analyses accompanied by a uniform overall strategy.

Strict implementation of rules with simultaneous flexibility is expected to be a necessary architectural paradigm. This means that there will be non-negotiable "barriers" which are to be strictly implemented as security policy in production. For example, area-wide encryption of information accessible to persons (operators) will, for reasons of data protection, always represent a necessary minimum measure regardless of the size, region etc. of the company. However, a high degree of flexibility (see "Dynamic configurability" in the protection objectives above) is needed within the defined playing field as defined by these barriers. In the above example, this means, for example, depicting (legal) regulations that differ from region to region concerning personal data that may be collected, saved, transferred (where to) and stored (how long). It is also expected that both the protection level of measures (i.e. increasing resistance to attacks through, for example, multi-factor authentication versus a basic password, but also through increased implementation quality) and temporal requirements of security measures as well as many other manifestations of security vary in large areas depending on the application.

Furthermore, there will, due to the autonomic and late (requested task-) changes, also be fluctuations with respect to events and communication that cannot be predicted. This kind of dynamic in the production environment is unusual today and confronts security measures with new challenges. A plausible way of implementing flexible security is with a security administration network that is independent from the actual production communication and where security-relevant reconfiguration occurs during run-time. A corresponding risk analysis is needed to commercially evaluate such methods in order to compare the resource requirement with the risk assessed.

Likewise, rules with static configuration and/or hardware can – unlike in a dynamic configuration – be implemented in software algorithms by means of (reconfigurable) rules.

7.5.2 Identity management

Only if it is known which user has and may have access to which machine, can unauthorised instances of access be effectively identified and prevented. This leads to identity management.

The blanket introduction of electronic identities – for persons and technical entities associated with the developing authentication and authorisation procedures –implements the above required separation of duties and/or their access as well as the security principles of mandatory access control and least privilege: Each access attempt must be authenticated and authorised with the least privilege required by the application.

As part of increasing Industrie 4.0 automation and autonomy, the described measures must also be introduced for systems, machines and plants, particularly when they can control other units.

Prerequisites for such end-to-end authentication of access operations are a directory of all identities for people and machines across a production network who have approved access to resources in the examined process as well as the modelling of differentiated roles and rights that depict the required activities.

Finally, a system-wide policy must be available and in place which defines the currently valid access rules. This confronts large internationally operating corporations with genuine challenges as the sheer number of processes, roles, rights and identities is often much too large to be kept and managed within a single site. Locations distributed around the world and access to this directory imply that a central solution is impossible. In order to be able to assign company-wide unique identities, a verification mechanism must be in place that is capable of accessing all identities used within the company to, for example, determine whether a newly created identity already exists within the company when assigning a new, unique identifier. At the same time, it is highly plausible that multiple decentralised databases exist where identities are managed. With this decentral version, it must be ensured that when assigning new and managing existing identities it is possible to check all existing databases as to whether the applicable identity already exists or where administration is needed. The decentral version requires high-availability architecture with integrated load balancing and failover mechanisms to ensure that all databases used are available at all times. Time-frames for maintenance should also be considered to ensure access to identities within one's own company so that, for example, a company can issue, verify and revoke company ID's and certificates. The challenges described also apply comparatively for the other data mentioned; a method can, for example, be implemented to organise roles and rights that differ regionally while still monitoring and documenting them centrally. It is to be expected that the number of identities for systems and their components will soon significantly exceed those for people.

Company ID's, for example, document the identity of a person in a company and can, depending on its design, control access to rooms and buildings as well as access to software. When creating company ID's, the identity of the person is authenticated based on official documents (personal ID card, passport, etc.) and the ID card number is linked with the unambiguous company-wide identity assigned to the person. Entry and access authorisations can be awarded by means of a separate authorisation process and, depending on the design of the company ID, the relevant authorisation certificates can be saved on its chip. In general, certificates are only valid for a limited amount of time to ensure, for example, that regular evaluation (re-certification) occurs. Based on the authorisations linked with the identity, approved authorisations can be revoked for each identity, for example, at the end of an employment relationship. It is also possible for authorisations to be withdrawn or fully blocked from the respective company ID in the event of its loss. This should be performed via a central platform in each company and used for the issue, verification and revocation of identification.

The separation and division of authorisations to multiple users in the system design, each of whom only have the rights relevant to their work (least privilege, separation of duties) is yet another hurdle in the event an external attacker attempting to access (encrypted) information.

7.5.3 Cryptography – protection of confidentiality

It must be assumed that, with respect to the vast majority of classified information saved electronically on a data storage device, there are corresponding specific interests in obtaining unauthorised knowledge of such information. However, one can make access to such information significantly more difficult for an unauthorised third part by, for example, ensuring adequate end-to-end encryption. Good encryption algorithms offer increased protection for the confidentiality of information by significantly increasing the resources required for unauthorised decryption (without a key). Data transmission often occurs via multiple centres. Even if the individual transmissions are encrypted and temporary storage occurs in plain text, there is a risk of data theft or data manipulation by unauthorised third parties. End-to-end encryption makes data manipulation and data access in the event of unauthorised access and/or data theft ("secure the weakest link") more difficult, but does not, however, prevent it from happening. Data, with the recipient's public key, is encrypted by the sender – in asymmetrical cryptography, for example – and is transmitted encrypted and stored encrypted. How asymmetrical and symmetrical cryptography is used is defined by concepts that consider the specifics of the application. The case of replaceable manufacturer recipes in production machines serves as an example. The encrypted transmission here from the manufacturer to the user and onto the machine must take place to prevent disclosure of the increasingly value-generating and/or cost-incurring recipes for the user in Industrie 4.0. As the user typically has administrator rights to the machine, saving the recipe in the machine must also occur in encrypted form (or a memory area that can only be read by the manufacturer or a manufacturer-certified code). On the question of whether and how the program sequence based on the recipe is to be encrypted, risks such as run time analyses as well as external intruders must be evaluated by the user on whether additional safeguards (which require more resources) are justified. If symmetrical cryptography is used, a reasonably secure memory for the local private key and corresponding infrastructure is needed, which soon then requires a special hardware security element. Additionally or alternatively, the effect of an attack can be limited by the use of machine-specific keys. The latter also makes it possible to restrict the use of recipes on individual machines by using licence management.

7.5.4 Cryptography – integrity protection

Cryptography is ideal for protecting integrity by using appropriate forms of test values in combination with signatures. As an Industrie 4.0 measure, it effectively protects both integrity and authenticity. The protection of basic system software (embedded operating systems) of embedded systems is an example.

Designing embedded systems only makes sense with secure boot processes in all areas. An initial software component that cannot be modified in the field (non-writeable memory, TPM or similar) first checks the integrity of the next higher software code with a hash and signature before it is started. This can occur at multiple levels if necessary, and results in a trustworthy code basis in operations. A hardware protection module provides confidence in resistance to attacks. For Industrie 4.0, the task is to clarify how this measure can be implemented area-wide, particularly in areas where it requires a large amount of resources (e.g. with basic sensors).

In the recipe example above, asymmetrical cryptography can be used if the requirements on the processing time are low (conventional symmetrical methods are calculated faster and offer comparable strength compared to the asymmetrical ones) and/or if no suitable secure storage location is available locally (for the confidential key required for symmetrical methods) and recipe authenticity is the priority compared to confidentiality. The manufacturer's public key is sufficient for verifying authenticity and, being public, it does not require a secure storage area.

The encryption methods and the encryption algorithms used for individual cases depend on a range of criteria including on the required duration of protection, available resources (calculation performance), availability and ability to introduce local confidential memory for key storage versus central infrastructure (public key infrastructure), availability of online connections (central management, revocation), detected attacks etc.

Though cryptography facilitates the task of providing protection as a whole, it requires key material to be handled with care. If keys are lost, there is a risk of data loss and if the key ends up in the wrong hands, undetected access to the encrypted data is possible.

However, it is easier to protect keys in a smaller number of locations as opposed to area-wide protection without cryptography. Established methods such as PKI are available for this purpose. Dedicated hardware components – security chips with comprehensive security functions and a high level of protection against a range of attack methods – are also available. However, cryptography only unleashes its full potential if the concept is adapted to the application and risk situation.

7.5.5 Secure remote access and frequent updates

It is a common practice in production operations for manufacturers to have machines and robots remotely maintained via the Internet. In this respect, the manufacturer's technician directly accesses the machine in the company that requires maintenance via the Internet to perform firmware updates or adjust settings to improve performance. The cooperation of different companies – when applicable via shared platforms – poses the considerable challenge of correctly authenticating different users; own employees can generally be unambiguously identified through personnel systems but this does not apply to employees from cooperation partners, customers and manufacturers. Though each of the involved companies has its own identity management, the cooperating companies normally do not have an established trust-based relationship based at the technical level.

Such a position of trust can be created with so-called Federated Identity Management (FIM). An external identity broker, who (must) be trusted by all involved companies, checks whether the requested identity (it is immaterial whether this is a person or a machine) is the one it claims to be. This check can take place by means of multi-factor authentication using a combination of two or more of the following factors: Possession (dongle, smart-card, tokens), knowledge (passwords, key phrases) and/or biometry (finger print, iris scan). Once authentication is complete, it can be checked in the company in a second step whether and (if yes) which authorised access operations exist for this identity and whether the desired system may be accessed. Universal standards will become imperative at the latest at this point.

The same question of trust is relevant with respect to the computer systems used. To ensure, for example, that no malware/viruses or even backdoor risks are caused by a manufacturer's system used for remote maintenance and unverified by the user, standardised virtualisation technologies can be used (de facto). The user and the manufacturer can jointly define and check the image approved for use because the VM interface and the availability of the required maintenance tools in the VM runtime environment are relevant for the manufacturer while the user is primarily interested in avoiding risks to his production. As Industrie 4.0 evolves towards continual services for the monitoring, care and analysis of production systems, this measure must be continually developed. An example here is checking of the outflow of operative data from production.

Frequent updating and/or options to bridge software gaps are required in networked systems that are becoming increasingly software-dependent. In the production environment, this creates conflict with certification, e.g. for operational security. Possible countermeasures include the encapsulation of certified systems vis-à-vis networks with security gateways, the scope of whose functions may vary greatly but in essence address the visibility and consequently the vulnerability of the encapsulated system. Regarding further modularisation, this requires a downsizing of gateways while at the same time more widespread support for industry-relevant protocols and protective mechanisms. A shift must take place regarding limitations on real-time communications testing for the increasing numbers of protocol and ISO/OSI layers while at the same time avoiding failures. Methods are also needed that permit updating in the field despite certification, which along with appropriate modularisation may make it possible to at least disconnect and update visible and consequently vulnerable parts of the certification core.

Authentication mechanisms ensure that only entitled user names have access to the protected data. However, conventional single-factor authentication by means of a password or possession only checks whether the user name is authorised and not whether the correct user is also using this user name.

As long as it is assured that the private key of the recipient has not been compromised, only the desired recipient can decrypt and read the message. Though it is in principle possible to crack the key, according to the current status of technology, this requires a relatively large amount of resources and can only be achieved in specific cases and not area-wide.

The use of end-to-end encryption requires that both the sender and the recipient have and use the respective valid keys for a certification centre and that an encrypted transmission as well as encrypted data storage are technically possible with the infrastructure being used. This includes the use of appropriate protocols, hardware and software to maintain at a reasonable minimum the increased computing power needed for encryption and the subsequent drops in performance.

This not only applies for processes in the company, but also for processes and data flows within the manufactured products.

7.5.6 Processes and organisational measures

Ideally, the management of information security risks in a company is supported by appropriate, comprehensive security management which includes risk and incident management systems. The task of risk management is to identify and handle existing risks so as to make them transparent and to permit the organisational portrayal of such risks in cooperation with the technical departments and in consideration of compliance. In general, there are 4 options for dealing with identified IT security risks: acceptance, mitigation, elimination and transfer.

IT security risks must be identified to adequately counteract them. Only an identified risk can be effectively addressed. To avoid participating departments and areas of the company from an uncoordinated definition of their own responsibilities – which risks individual topics remaining not being addressed or interdisciplinary topics being neglected – requires the establishment of cross-sectional functions at an organisational level and clear, company-wide definitions of existing responsibilities and roles. If not yet in place, it is recommended that dedicated positions are created for this purpose ("Chief Information Security Officer", "Production Information Security Officer") whose tasks are to consider IT security as a holistic process within the entire company based on very close coordination and cooperation.

In general, the first actions of such central positions is to develop and implement a comprehensive monitoring concept. Existing monitoring measures can, if applicable, continue to be used and/or aggregated. Many areas relevant to security, which in the past have often been neglected such as documentation and analysis of access controls for security-relevant central systems (central key store) particularly for administrators, must be newly created because they do not generally exist, at least in production.

Furthermore, with Industrie 4.0, it is imperative that solutions for cooperation at process levels extending beyond company and country limits can, when applicable, be found through a shared platform which permits the independent analysis of incidents as well as their identification and documentation.

Only after established security management, as a measure for achieving transparency, is in place is it possible to detect and document anomalies and to bring about a production-wide, positive increase in security.

7.5.7 Awareness

Finally, it is imperative that both the workforce and management are aware of the importance of IT security and the effects of, for example, potential data loss or data manipulation and that they understand IT security guidelines in order to comply with and observe them. A lack of understanding can lead to intentionally bypassing IT security measures as security measures often do not facilitate or accelerate the work process. Regular and further training of the entire workforce is therefore an important measure.

7.5.8 Company-wide coverage

IT-security does not, however, begin with production but rather begins with the planning and procurement of production components. In order to set up a secure IT environment for production, planning, procurement and production must closely collaborate with one another. IT security guidelines can only be complied with if the procured products are also able to achieve this technologically. To gain familiarisation about the technological requirements of the components to be procured, production, planning and purchasing must engage in a dialogue. Without specific guidelines from customers, manufacturers often see no need to implement security features in the products due, under certain circumstances, to their association with higher production costs and performance loses. Without a relevant offer from manufacturers, customers often find themselves confronted with a market situation seemingly without alternatives. This vicious circle results in IT security measures currently being implemented at a very slow pace only in manufacturers' products. Therefore, the minimum requirements, entrenched in purchasing guidelines, on manufacturers' products should be revised and adapted on a regular basis.

All example measures presented serve to incrementally improve IT security within the company. It should and must be determined in individual cases which of these measures will be effectively implemented and/or adapted in a particular case based on best practice.

7.6 Outlook and requirements

Industrie 4.0 connects the information worlds ranging from office to sensors and extending beyond company limits. The security of these information worlds can only be assured by eliminating the separation of responsibilities that often exist today for information processing and security between office IT and automation.

Standards already currently exist for the area of office IT and they address numerous issues ranging from information security (ISO 27000 series) and infrastructure management (ITIL) through to business-relevant IT measures (Cobit). In the area of automation technology, there is – despite a multitude of sector-specific recommendations[16] – an even greater pent-up need to raise awareness regarding risk detection and the implementation of security measures.

In the short-term, a procedural model for information security in industrial automation –the VDI Directive 2182 – can be used as it considers the interlinking of manufacturers, integrators and operators.

Due to the increasing consolidation of all company networks as well as entire value networks on the one hand and different protection requirements and opportunities on the other, the coordination and harmonisation of security measures in the entire company and of service providers is of critical importance. IEC62443[17], which is still under development, pursues the goal of efficiently and securely connecting a procedural model and measures for administrative IT (in the form of the ISO 27000 series) with special aspects for automation (based on ISA-99[18]). The new requirements and measures for Industrie 4.0 must be developed accordingly in standards. Whether this can be implemented more effectively with new standards or through the revision and supplementation of existing standards requires evaluation in the context of other standardisation topics relating to Industrie 4.0.

Harmonisation in this respect also means that security management of office IT and automation technology must converge. Movement must occur on "both" sides for this.

The fact that there are automation guidelines without an equivalent in office IT is evidenced, for example, by the Machine Directive 2006/42/EC: It represents a regulatory framework for protecting people and the environment at the European level. In addition to assuring operational security and reliability, ensuring risk-free function in connection with the dynamic value networks in Industrie 4.0 poses a unique challenge for an updated Machine Directive.

The assurance of risk-free function using corresponding components requires suitable integration measures and tests. Applied to information security, suitable methods and mechanisms must be developed, which achieve the endeavoured level of security and maintain it in value networks subject to dynamic change.

The creation of trustworthy certification centres and unique, forge-proof identities are the prerequisites for an identity infrastructure along the value network. These prerequisites guarantee definite and consistent identification as well as the allocation of a participant's identity and support the identity-based authentication and award of rights.

Security must be an integral part of the product creation process (security by design).

Even if the specific requirements and framework conditions differ in the areas, they can be dealt with using collective methods and concepts. Consolidating the expertise from office IT and automation offers considerable synergy effects.

16 for example, ISA99, NIST SP800-82, NERC CIP, CPNI Good Practice Guide (all in English)

17 See https://www.dke.de/DE/STD/INDUSTRIE40/Seiten/IEC62443.aspx

18 See https://www.isa.org/isa99/

Opening up the subject matter and further training on the part of office IT is just as necessary for automation requirements as expanding IT expertise and especially security know-how in automation.

The security situation will never be a static one; the threat situation will always be constantly changing. Therefore, it is imperative that security is understood as a continual process and, at least at the beginning, is viewed as a time-limited project. All participants must find a way to deal with new security challenges, which, among other things, were unknown when the product was created and commissioned.

A special challenge will be an arrangement that considers the needs of small and medium-sized businesses. A viable security landscape can only be established if products and services are offered whose standardised security characteristics have already been considered and for which relevant infrastructures exist for easy incorporation into company processes. Possible steps in this direction involve a uniform communication and security datasheet for automation products, and standardised reports on security events using standardised semantics to make centralised documentation and analysis easier.

Information and networking become central assets in the new value networks. Sharing or providing information will create new opportunities. At the same time, there exists the questions of ownership of the information, the roles and the legally secure responsibilities of the involved parties. The added value from the analysis of information that occurs with partners and suppliers must be weighed against the possible outflow of expertise.

Appendix

8 Appendix

8.1 List of sources

[1] VDI/VDE Society for Measurement and Automatic Control: Statusbericht; Industrie 4.0; Wertschöpfungsketten (Status report; Industrie 4.0; value streams). Düsseldorf: VDI e.V., April 2014

[2] VDI/VDE Society for Measurement and Automatic Control: Statusbericht; Industrie 4.0; Gegenstände, Entitäten, Komponenten (Status report, Industrie 4.0; Objects, Entities, Components). Düsseldorf: VDI e.V., April 2014

[3] Acatech Studie, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, Abschlussbericht des Arbeitskreises Industrie 4.0 (Acatech Study, Implementation Recommendations for the Future Industrie 4.0 Project, Final Report of the Industrie 4.0 Working Group). http://www.bmbf.de/pubRD/Umsetzungsempfehlungen_Industrie4_0.pdf

[4] IEC TR62794: Industrial-process measurement, control and automation – Reference model for representation of production facilities (Digital Factory), 2012

[5] IEC CD 62832 Digital Factory

[6] IEC 61987-10

[7] GMA definitions: http://www.iosb.fraunhofer.de/servlet/is/48960/

[8] German Federal Office of Information Security: Die Lage der IT-Sicherheit in Deutschland 2014 (The State of IT Security in Germany 2014). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

[9] www.iosb.fraunhofer.de/?Begriffel40

[10] https://www.dke.de/de/std/informationssicherheit/documents/nr%20industrie%204.0.pdf

[11] http://docs.oracle.com/javase/7/docs/technotes/guides/jar/jar.html#JAR_Manifest

[12] http://www.plattform-i40.de/sites/default/files/140326_Broschuere_Industrie_0.pdf

8.2 Industrie 4.0 Glossary

In connection with Industrie 4.0, the languages of and ICT (information and communication technology) are merging together. However, there are historically based differences and uncertainties with important terms surrounding Industrie 4.0. The working group "Terms" in the VDI/VDE-GMA 7.21 "Industrie 4.0" technical committee led by Dr.-Ing. Miriam Schleipen of the Fraunhofer IOSB is endeavouring to work out a common "basis" (terminology) for Industrie 4.0 in the sense of linguistic and intellectual constructs. Work is also being performed in close cooperation with the committees responsible (e.g. DKE/UK 921.1) of the DKE's technical department 9 (e.g. DKE/UK 921.1) and is also coordinated with the AG2 "Reference architecture" of the Industrie 4.0 Platform.

The goal is a common understanding of fundamental terms! Work also builds on existing standards from the areas of ICT and production.

In the Industrie 4.0 environment, terms and concepts from different domains are adopted (for example, from the area of ICT, the orchestration of services in a service-oriented environment). Some terms, however, have different meanings in the applicable domains (for example, service in the area of ICT versus in production). Other terms also have different meanings or are imprecise within a domain (such as component). This linguistic and conceptual differences and discrepancies as well as the need for explanations of concepts beyond known subject areas are an obstacle with respect to the development of interdisciplinary complex technical solutions for Industrie 4.0 as well as in standardisation.

The glossary therefore provides a common basis for terms in connection with Industrie 4.0 and accounts for the different perspectives and requirements. This serves to facilitate cooperation beyond the limits of companies and sectors and is a prerequisite for standardisation.

The current definitions can be found under [9].

8.3 Team of authors

The technical input for this implementation strategy was provided by the working groups from the Industrie 4.0 Platform. The authors named below composed the written summary in the form of this report.

Team of authors Chapters 1- 4:

- Wolfgang Dorst (BITKOM e.V.)
- Carsten Glohr (Detecon International GmbH)
- Thomas Hahn (Siemens AG)
- Frank Knafla (Phoenix Contact Electronics GmbH)
- Dr. Ulrich Loewen (Siemens AG)
- Roland Rosen (Siemens AG)
- Thomas Schiemann (T-Systems International GmbH)
- Friedrich Vollmar (IBM Deutschland GmbH)
- Christoph Winterhalter (ABB AG)

Team of authors Chapter 5:

- Dr. Bernhard Diegner (ZVEI e.V.)
- Johannes Diemer (Hewlett Packard GmbH)
- Dr. Mathias Dümmler (Infineon Technologies AG)
- Stefan Erker (Huber + Suhner GmbH)
- Dr. Werner Herfs (RWTH Aachen, WZL – Chair for tool machines)
- Claus Hilger (HARTING IT Services GmbH & Co. KG)
- Dr. Lutz Jänicke (Innominate Security Technologies AG)
- Prof. Dr.-Ing. Jürgen Jasperneite (Institut für industrielle Informationstechnik / inIT, OWL University of Applied Sciences, Lemgo and Fraunhofer IOSB-INA)
- Johannes Kalhoff (Phoenix Contact GmbH & Co. KG)
- Prof. Dr. Uwe Kubach (SAP AG)
- Dr. Ulrich Löwen (Siemens AG)
- Georg Mattis (Huber + Suhner GmbH)
- Georg Menges (NXP Semiconductors Germany GmbH)
- Frank Mildner (Deutsche Telekom AG)
- Mathias Quetschlich (MAN Truck & Bus AG)
- Ernst-Joachim Steffens (Deutsche Telekom AG)
- Dr. Thomas Stiedl (Robert Bosch GmbH)

Team of authors Chapter 6:

- Dr. Peter Adolphs (Pepperl+Fuchs GmbH)
- Dr. Heinz Bedenbender (VDI e.V.)
- Martin Ehlich (Lenze SE)
- Prof. Ulrich Epple (RWTH Aachen)
- Martin Hankel (Bosch Rexroth AG)
- Roland Heidel (Siemens AG)
- Dr. Michael Hoffmeister (Festo AG & Co.KG)
- Haimo Huhle (ZVEI e.V.)
- Bernd Kärcher (Festo AG & Co.KG)
- Dr. Heiko Koziolek (ABB AG)
- Reinhold Pichler (VDE e.V. DKE)
- Stefan Pollmeier (ESR Pollmeier GmbH)
- Frank Schewe (Phoenix Contact Electronics GmbH)
- Thomas Schulz (GE Intelligent Platforms GmbH)
- Dr. Karsten Schweichhart (Deutsche Telekom AG)
- Dr. Armin Walter (Lenze SE)
- Bernd Waser (Murrelektronik GmbH)
- Prof. Dr. Martin Wollschlaeger (TU Dresden)

Team of authors Chapter 7:

- Dr. Lutz Jänicke (Innominate Security Technologies)
- Michael Jochem (Bosch Rexroth AG)
- Hartmut Kaiser (Secunet Security Networks AG)
- Marcel Kisch (IBM Deutschland GmbH)
- Dr. Wolfgang Klasen (Siemens AG)
- Jörn Lehmann (VDMA e.V.),
- Lukas Linke (ZVEI e.V.)
- Jens Mehrfeld (BSI)
- Michael Sandner (Volkswagen AG)

ISBN 978-3-00-052211-6