DIN/DKE – Roadmap

GERMAN STANDARDIZATION ROADMAP

IT-SECURITY

Version 2

DIN

DKE

VDE DIN

Contents

0 Foreword to 2nd edition

In the first edition of the German Standardization Roadmap for IT security, DIN's IT Security Coordination Office (KITS) focussed on giving an overview of the current state of IT security standardization in core areas under discussion. It also presented recommendations for action based on discussions in the relevant standards bodies, predicted the new developments to be expected, and described how standardization should take these into consideration. This second edition of the Roadmap places a greater emphasis on future trends that will have an impact on standardization. Increasingly, cross-sectoral issues are coming to light that cannot be limited to one sector or domain. One reason for this is the continually progressing convergence of technologies and the associated high degree of interconnectivity. This important aspect is being given consideration at European level by the Cybersecurity Coordination Group (CSCG); the Group only gives recommendations for cybersecurity standardization in Europe, however, and does not develop its own standards. The Group has published a White Paper with recommendations on digital security. Chapter 6 of this edition of the Roadmap looks closer at general developments at European level. For ease of reading, the extensive lists of current standards have been included in a separate annex.

1 Introduction

1.1 General

The days in which the term "information technology" only meant networked micro-computers used in the office and for business purposes are long past. Over the past few years, the main challenge has been the extensive penetration of IT in diverse areas. In many areas, this development is still in

process; nevertheless, the next major task in IT security is to deal with the increasing interconnectivity of the fields which have been penetrated by ICT.

For example, "Industry 4.0" refers not only to the extreme meshing of IT with production processes, but also its role in "traditional" office technology. The "internet of things" is clearly finding its way onto the factory floor. Combining physical objects with intelligent IT systems in what is called "cyber-physical systems" - primarily via RFID transponders - is opening up new possibilities: Manufacturing blanks themselves radio messages to the production system (smart factory; material flows are controlled by the conveyed material itself. Such developments all have an impact on R&D, marketing and controlling departments.

Another trend is the use of internet-like networks in domestic households, making the home "smart". There are already a number of available products in this area, such as thermostats, light switches and shutters that are controllable by remote both inside (via radio) and outside (via the internet) the home; or washing machines whose status can be checked by smartphone. These technologies are also widely used in Ambient Assisted Living (AAL) which allows elderly persons and the disabled live independently in their own home environments.

Due to the larger address space of Internet Protocol version 6 (IPv6), it will be possible to assign IPv6 addresses to all technical devices.

The "smart grid" provides an intelligent supply of energy. Today, power consumers are simultaneously power producers - or "prosumers" - because they also produce energy, for example in their own solar power systems. Energy supply is more decentralized than ever, thanks to the wide use of solar energy and wind energy systems. But the issue of distributing electric power and safeguarding its supply is becoming increasingly complex. An important element of the smart grid is the smart meter: These components of household installations have microprocessors that allow remote reporting of energy consumption for billing purposes (e.g. per GPRS).

Another area in which data is read remotely is in electromobility: During the vehicle charging process information is transmitted for billing purposes. But electric vehicles not only communicate with utilities, but also with each other in "car2x communication" in which cars talk to each other (e.g. in case of an accident) or with a traffic system (e.g. when there is a traffic jam). Another idea being given consideration is the "smart car key" in which the user profile of the car owner can be stored (biometric verification, use of PKI certificates).

The production industry, energy, traffic, private households: All of these infrastructures are becoming more interconnected. And the enabler for this revolutionary development is information technology.

Many solutions in the areas mentioned above are still proprietary, and there is a lack of interoperability - the need for standardization is clear.

In terms of IT security, there are a number of issues that need to be dealt with:

- Is the data transfer in car2x communication sufficiently authenticated and encrypted?
- Is smart meter data protected against unauthorized access?
- How can the manipulation of the smart grid - which can threaten power supply and grid stability - be prevented?

- Is the accessibility of AAL systems ensured?
- How is sensitive and personal data protected when it is transmitted via the internet?
- Can control units in smart houses be manipulated?
- Can RFID transponders be sabotaged?
- Are interconnected networks safely operated and configured?
- How can unauthorized access be precluded in interconnected networks and the "internet of things"?

Availability, confidentiality, integrity and authenticity are all the prime goals of IT security, especially in today's complex infrastructures. There is also a great need to secure industrial systems, smart meters and vehicle controls. But not just any security measures can be used - and they must not be kept to a minimum for purely economic reasons. There is an urgent need for safe and secure products and systems, including management systems. And that is why there is a clear need for standardized requirements and solutions.

There are also other areas in which standardization is needed, such as cloud computing. The current status and need for action must also be determined for these areas.

1.2 IT Security Coordination Office (KITS)

In today's technological world in which IT security aspects must be considered for numerous processes and products, it is no longer sufficient to simply develop standards. Standards work must also be coordinated across all sectors, and the most suitable standards have to be selected for the application at hand - this is especially important in the face of accelerated technological convergence. Experts who up to now have only developed IT security standards now have to inform themselves about IT security standards in other areas on an application-by-application basis. For example, the smart grid will only be accepted by consumers if besides IT security also data protection aspects are integrated in the system architecture from the very beginning. But it is important to remember that although information about fundamental IT security standards reaches actors in various sectors, these actors are working on sector-specific solutions that are not necessarily compatible with solutions in other areas. Considering the social and political pressure being placed on the need for comprehensive, networked security for all areas, isolated sector-specific IT security solutions are no longer acceptable, because IT security itself must be interoperable. Thus, for activities that touch upon several areas, standardization must also be coordinated on a cross-sectoral level. Within DIN, this coordination is the task of the IT Security Coordination Office (KITS), a subordinate body of DIN's Presidial Committee "FOCUS.ICT", KITS' tasks are:

- Coordinating the work of various actors (standards committees, technical associations, industry experts, government agencies) relating to IT security
- Consulting standards committees working on standards that include content relating to IT security (e.g. the smart grid, informatics, and telematics in medicine)
- Maintaining an index of all standards projects relevant to IT security and which are important for German stakeholders
- Keeping the German Standardization Roadmap for IT security up-to-date

- Coordinating German influence on European and international standards work in the interests of German industry, public authorities and sciences .

Figure 1 shows the structural framework into which KITS is incorporated.

For more information on KITS go to www.din.de/go/kits.

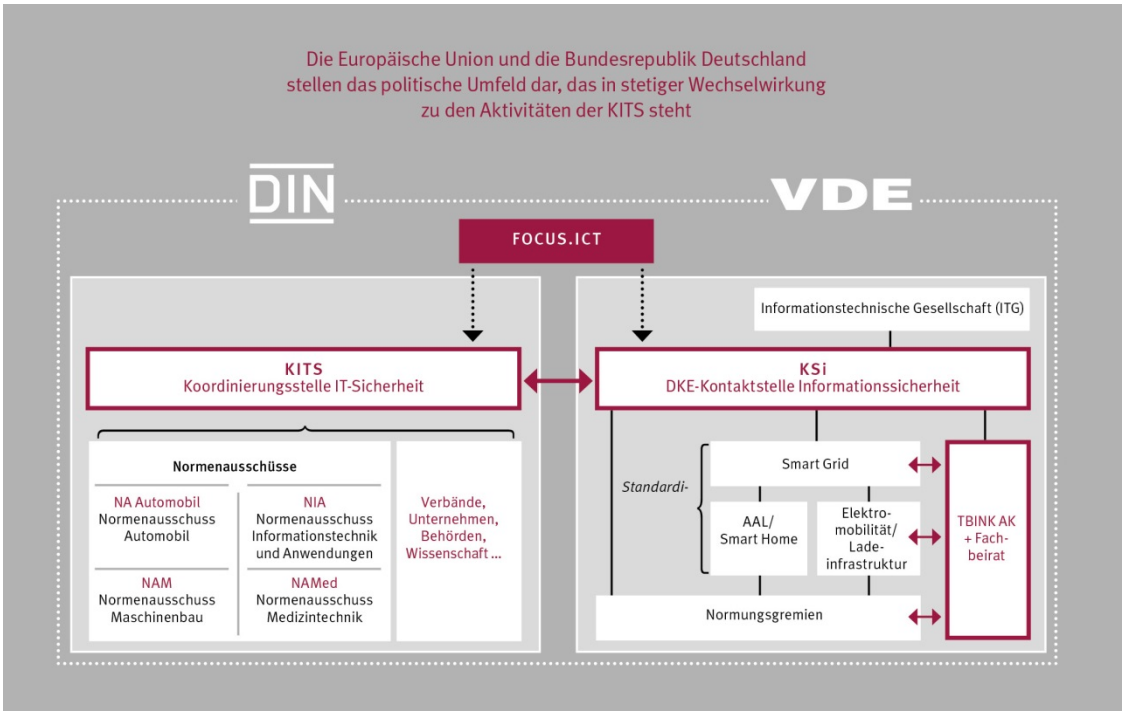

Figure 1: Structure of the IT Security Coordination Office (KITS)

2 Objective and approach of this roadmap

The objective of this roadmap is to identify areas in which the need for security solutions overlaps with for the capabilities of standardization. The aim is to help coordinate standardization activities by listing work that has already begun or that has already been completed. Discussions with experts have shown that IT can no longer be considered on a sector-by-sector basis, but rather as a cross-sectoral technology that is used across all sectors. Thus, a description of existing standards bodies and standards is the first step towards an effective coordination. The roadmap also gives recommendations for action as regards work to be done in order to meet the needs in the relevant areas. The high degree of integration in current IT trends requires such a cross-sectoral approach. In this roadmap, therefore, current topics are discussed on a cross-sectoral basis.

3 Standardization

3.1 Introduction to standardization

Standardization is officially defined as the systematic unification of material and immaterial subjects carried out by all stakeholders working in consensus for the benefit of society as a whole. One of the best known examples is the standardized A4 paper format. Standards lay down the state of the art in documents made available to the public, and provide non-discriminatory access to information on:

- Bringing innovative solutions to the market
- Opening up markets
- Knowledge transfer
- Disseminating best practices
- Interoperability
- Enhancing the reputation of the user
- Greater trust in services and products that comply with standards

According to the principles of standards work, standards are not to serve the interests of an individual party, but are to benefit society as a whole. This is the main difference between full consensus standards and consortial standards. In Germany standardization is carried out by the national standards organization, DIN, the German Institute for Standardization. According to an agreement with the Federal Republic of Germany, DIN is the only national standards organization that represents German interests in the European and International Standards Development Organisations.

In this highly networked world, a secure infrastructure used by one party also benefits other users because it can not be used for attacks. Positive network effects here become evident. Being a joint activity that networks all stakeholders, standardization is thus an excellent instrument for effectively supporting these network effects and increasing the general level of security to the benefit of all.

3.2 Areas in which IT security standards are used

Standards and specifications help increase IT security. Using standards and specifications helps increase the general level of IT security in communications within and between companies. Higher security also supports the development of innovative technologies. By laying down uniform technical and organizational measures, standards address the three main objectives of IT security: availability, confidentiality and integrity. They also facilitate:

- A greater transparency in security solutions (creating trust)
- The dissemination of best practices
- The use of applications in smaller businesses
- Descriptions of generally accepted security solutions
- Interoperability through well-defined interfaces
- Common system architectures
- Uniform terminology
- The harmonization of existing standards
- The use of existing solutions from other sectors
- The globalization of national solutions

4 Major topics

4.1 Data protection

4.1.1 Description of topic

Data protection, or privacy, is important for protecting citizens and consumers, and society as a whole, from the malicious processing of data that encroaches upon an individual or group's privacy. The extent to which a form of data processing can threaten privacy depends on the context. Therefore, data protection principles such as "privacy by design" (taking data privacy into consideration during the system design phase), or data minimization have already been laid down in standards.

IT security and privacy are closely linked. For example, IT security - e.g. in the form of encryption or access control - is essential for data protection in IT systems. However some IT security measures, such as the recording of data, can cause some problems for data privacy. Data protection standardization is also an instrument for technically implementing legal provisions. There are standards on the deletion of data, for example, or the destruction of data carriers, which help safely implement legal requirements by deleting personal data once it is no longer required.

4.1.2 Standards bodies active in this area

A number of bodies and organizations are developing standards and specifications on data protection. Often the documents do not have general applicability, but rather are intended for a specific technology, sector or domain. The most important bodies are listed in the table below.

Organization	Standards body	Title of standards body	Field of activity
ISO/IEC	JTC 1/SC 27/WG 5	"Identity Management and Privacy Technologies“	Generic data protection technology standardization
CEN	CEN /TC 225	AIDC Technologies	RFID standardization, Privacy Impact Assessment in the area of RFID
CEN/CENELEC	CEN/CLC/ JWG 8	Privacy management in products and services	Data protection management standardization
DIN	NA 043-01-27-05AK	Privacy technologies and identity management	Generic data protection technology standardization, mirror committee to TC1/SC 27/WG 5
DIN	NA 043-01-50 AA	Deletion of data carriers	Standards on secure deletion of magnetic data carriers
DIN	NA 043-01-51 AA	Destruction of data carriers	Standards on the safe destruction of data carriers
ISO	ISO /TC215	Health informatics	Health informatics, data protection in the medical sector

4.1.3 Current standardization landscape (as regards IT security)

The significance and challenges of data protection in information processing systems have already been acknowledged and have come to play a role in standardization. Data protection standardization can be divided up into three broad areas:

- **Frameworks and architectures**
- **Protection concepts**
- **Guidelines for content and evaluation**

The central problem in data protection vs IT security is that, although increased security can help protect against unauthorized access to resources such as sensitive data, it is usually necessary to collect even more data to ensure this protection. This collection of data then in turn presents an additional data protection problem. One example: Recording all access to protected data collections which helps prevent unauthorized access to sensitive data, but which in itself generates data to be protected. Another example: Identifying actors, which helps to control access to sensitive data, but which also makes it possible to record each step those actors take in detail - this information can then be used to draw up a precise personal profile with which that person can be monitored. This is why it is so important in standardization to harmonize the need to protect the personal data of individuals with the need to make an organization's IT system secure.

4.1.4 Need for action

At present, one essential need for action in data protection standardization is the coordination of activities among the different bodies. In light of the diverging approaches to data protection

technology in the increasingly convergent areas, it will be difficult to reach a common level of data protection. The greatest challenge here is dissemination of generic aspects among bodies in different domains, sectors or technologies.

In addition to the standardization of data protection fundamentals, there is an even greater need for the standardization of methods and techniques in the form of "best practices" that implement legal provisions. These provisions make it especially important that users do not consider such best practices as universal solutions. Rather, users must be aware that, in data protection, the particularities of the individual case must always be taken into consideration. Standards that fulfil these requirements create trust in legally compliant products and services, and legal security for companies who gain recognition from public authorities. A need for standardization that implements legal provisions has been identified for the following subjects:

- Documentation for products/services regarding stored personal data
- Technical procedures relating to personal rights (right to information, deletion of data, consent of use)
- Technical implementation of consent/withdrawal of consent of use
- Third party data processing
- Anonymization / pseudonymization techniques
- Privacy by design
- Data minimization technologies
- Organizational precautions and processes for the safe deletion of data

In 2013 the European Commission issued a standardization mandate to the steering bodies of CEN and CENELEC titled "Privacy management in the design and development and in the production and service provision processes of security technologies". In response to this mandate CEN and CENELEC established a Joint Working Group which began its work in January 2015. The development of European Standards on data protection management is soon to be expected. German experts can participate in the work of this JWG via the national mirror body NA 043-01-27-05 AK "Identity management and privacy technologies" within DIN's Standards Committee Information Technology and selected IT Applications. This mandate is an indication of the increased activity within the Commission in the area of IT security and data protection, often under the keyword "cybersecurity". Further mandates are expected calling on the European standards organizations to develop more standards in the area of IT security.

The European Commission is also currently working on a new regulation, the General Data Protection Regulation (GDPR). This draft regulation will replace the old Data Protection Directive, which does not deal with many current topics such as social media, cloud computing or the "internet of things".

4.2 Energy supply (smart grid)

4.2.1 Description of topic

The IT-based networking of power grid components is necessary if we want to be able to control the grid in the future. The smart grid of the future encompasses different segments and domains, including devices used commercially and in the home. Consideration needs to be given to:

- Energy management
- Smart meters
- Metering operations
- Distribution grids
- Transmission grids
- Communications grids
- Energy generation
- Storage
- Aggregators
- Electromobility
- The energy market
- Additional services ("value-added" services)

4.2.2 Standards bodies active in this area

In Germany, the DKE-Kompetenzzentrum (DKE Expertise Centre for E-Energy) and the DKE steering committee with its focus groups have been active in this area for more than three years. The aim is to coordinate smart grid standardization in DKE and DIN, and in various interest groups, incorporating this work in "e-energy projects". This not only involves the work of established standardization bodies, but also that of associations, government bodies and VDE bodies dealing with the smart grid. In addition, the DKE Expertise Centre is monitoring European (in CEN/CENELEC) and international (in IEC) smart grid standardization activities. A special focus is being placed on the "energy turnaround", i.e. the integration of renewable energies. Table 1 gives an overview of German bodies and their activities. A paradigm shift can be seen in how these bodies work: Whereas in the past, only established products and systems were standardized, now standards work is carried out even before the products are available.

Table 2: DKE smart grid activities

Committee / Topic	Status / Activities / Plans
STD_1911 Steering Committee	• Coordination of the smart grid standardization activities in Germany, Europe (e.g. CEN/CENELEC) and at the international level (e.g. IEC) • Founding the task force "HAN-CLS Interface", which harmonizes standardization activities in the DKE standards bodies K716, K952, K461, K261 and the FNN • Working with the final report of the M/490 Smart Grid Coordination Group • Participation in BSI Task Forces • Participation in the BMWi working group "Smart meters and grids" Mirror committee to the IEC System Committee "Smart Energy"
STD_1911.1 "Grid integration, load management and decentralized energy generation“	• Further development of the use cases "DER Integration" with AK952.0.17. The compiled use cases were expanded in order to represent the flexibility concept and the traffic light model
STD_1911.2 "In-house Automation“	• Supporting the task of creating definitions for the data models shared via the HAN-CLS interface of the smart meter gateway • Collaboration with DKE AK 716.0.1 Information Security in Smart Home and Building • Coordinating with STD_1911.4 Coordination Smart Metering
STD_1911.4 "Coordination Smart Metering (KSM)"	• Supporting the development of the BSI Smart Meter protection profile • Mirroring the activities of SM-CG, and M/441 activities after the termination of the mandate • Discussions regarding definitions for the data models shared via the HAN-CLS interface of the smart meter gateway (see also STD_1911.2) • Tracking the BMWi body "Grids and Meters", particularly the group "KNA Smart Meter"
STD_1911.5 " Grid integration electromobility”	• Compiling use cases, i.e. charging at home, charging in parking spots, fast charging • Tracking the Steering Committee Emobility
STD_1911.11 "Smart grid Information Security“	• Mirroring the WG SG-IS and the four sub-groups • Link to DKE/K GAK 952.0.15 • Security in electromobility and in the industrial area • Founding the "IT security in electromobility, focusing on IT security at the charging station" (AK STD_1911.11.5)

Committee / Topic	Status / Activities / Plans
K261 "System aspects of energy generation“	• Further development of use case methodology • Micro Grids: Planning, Management • Demand Side Energy Resources Interconnection with the Grid • System aspects of elevated storage facilities • System aspects of large DER (Distributed Energy Resources) facilities
K 952 "Electricity meters“	• Evaluating IEC 61850 from the perspective of the user with an increased focus on use cases • IEC 61850, Ed. 2 99% completed, preparations for Ed. 2.2 begun • Harmonization of 61850-CIM increasingly being pushed in AK 952.0.14 "Operative power systems management" • Information security in the smart grid environment: data security in XML, Cyber Security Key Management
K 461 "Electricity meters“	• AK 461.014xxx BSI security profile data models • Tracking the BMWi body "Grids and Meters", particularly the group "KNA Smart Meter" • Implementing BSI TR 03109
FNN	• Measuring system 2020 • FNN guidelines on using IEC 61850 • FNN guidelines on storage

For example, the steering committee "E-Energy / Smart grids" coordinates national work by stakeholders via its task force "HAN-CLS Interfaces". The task force ensures the necessary exchange of information among all stakeholders, avoiding duplication of work and taking all interests into consideration. This also avoids conflicts in the scopes of the various standardizing groups. The task force is made of members from standards bodies who are directly involved in standardization and who have to implement the work results as real products. The aims of the task force are to:

- Develop a common, open architecture model that can be expanded
- Harmonize with activities at European level, taking the "traffic light concept" into consideration
- Analyse requirements: the definition of operational processes, signal processing, commissioning, availability requirements to ensure control
- Feasibility of the BDEW "traffic light concept" for all phases
- The concept must be adapted to international approaches and agreed upon by the relevant bodies in DKE and the "Forum Netztechnik/Netzbetrieb im VDE (FNN)".

4.2.3 Current standardization landscape

4.2.3.1 European Mandate M/490

IT security plays a major role in the European "Smart grid" mandate, M/490. The second phase of the mandate ended in 2014. The "Smart grid Information Security (SGIS)" working group of the CEN-CENELEC-ETSI Smart grid Coordination Group (SG-CG) presented its final report in 2014. In it the group describes how security standards can contribute to a dedicated security level in the smart grid at technical, organizational, and procedural level.

According to the group, the Smart grid Architecture Model (SGAM) [*SG-CG/M490/H_Smart grid Information Security 12/2014],* the SGIS security levels, and selected use cases play a key role in being able to define the various security requirements for each SGAM zone/domain. By relating the security standards to the SGAM, their applicability can be identified, helping system designers and integrators to select the right standards for their smart grid solution.

SGIS security levels

SGIS security levels (SGIS-SL) were defined during the first phase of Mandate M/490 to create a bridge between electrical grid operations and information security to increase grid resilience. The aim is to ensure the stability of the entire European power grid. The following figure shows the security levels with example scenarios.

Security Level	Security Level Name	Europeans Grid Stability Scenario Security Level Examples
5	Highly Critical	Assets whose disruption could lead to a power loss above 10 GW Pan European Incident
4	Critical	Assets whose disruption could lead to a power loss from above 1 GW to 10 GW European / Country Incident
3	High	Assets whose disruption could lead to a power loss from above 100 MW to 1 GW Country / Regional Incident
2	Medium	Assets whose disruption could lead to a power loss from 1 MW to 100 MW Regional / Town Incident
1	Low	Assets whose disruption could lead to a power loss under 1 MW Town / Neighborhood Incident

Figure 2: SGIS security levels

(Source: [SG-CG/M490/H_Smart grid Information Security 12/2014])

Use cases

Four representative use cases were selected and analysed to illustrate how IT security should be dealt with in various smart grid areas (see SGIS report *[SG-CG/M490/H_Smart grid Information Security 12/2014]).*

Smart grid security standards

The first phase of Mandate M/490 focussed mainly on standards for the smart grid core. The second phase also covered selected standards in related areas of the smart grid, such as industrial automation. Standards issued by ISO, IEC and IETF that deal with the implementation of security measures were also taken into account.

The SGIS divided these standards up into "requirement standards" and "solution standards". Examples of each are listed below:

Requirement standards (WHAT has to be made secure)

- ISO/IEC 15408 Information technology — Security techniques — Evaluation Criteria for IT 361 security
- ISO/IEC 18045 Information technology — Security techniques — Methodology for IT Security 363 Evaluation
- ISO/IEC 19790 Information technology — Security techniques — Security requirements for cryptographic modules
- ISO/IEC TR 27019 Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

- IEC 62443-2-4 Security for industrial automation and control systems - Network and system security - Part 2-4: Requirements for Industrial Automation Control Systems (IACS) solution suppliers
- IEC 62443-3-3 Security for industrial automation and control systems, Part 3-3: System security requirements and security levels
- IEC 62443-4-2 Security for industrial automation and control systems, Part 4-2: Technical Security Requirements for IACS Components
- IEC 62443-2-1 Security for industrial automation and control systems - Network and system security - Part 2-1: Industrial automation and control system security management system
- IEEE 1686 Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities
- IEEE C37.240 Cyber Security Requirements for Substation Automation, Protection and Control Systems

Solution standards (describe HOW elements are to be made secure)

- ISO /IEC 15118-2 Road vehicles – Vehicle-to-Grid Communication Interface, Part 2: Technical protocol description and Open Systems Interconnections (OSI) layer requirements
- IEC 62351-x Power systems management and associated information exchange – Data and communication security
- IEC 62056-5-3 DLMS/COSEM Security
- IETF RFC 6960 Online Certificate Status Protocol
- IETF RFC 7252: CoAP Constrained Application Protocol
- IETF draft-weis-gdoi-iec62351-9: IEC 62351 Security Protocol support for the Group Domain of Interpretation (GDOI)
- IETF RFC 7030: Enrolment over Secure Transport

Coverage of the smart grid field with standards

Figure 3 shows how the above standards cover the subject of the smart grid according to their scope and level of detail. The position of each standard in this diagram also illustrates its relevance for operators and market participants ("operations") and for manufacturers and service providers ("products").

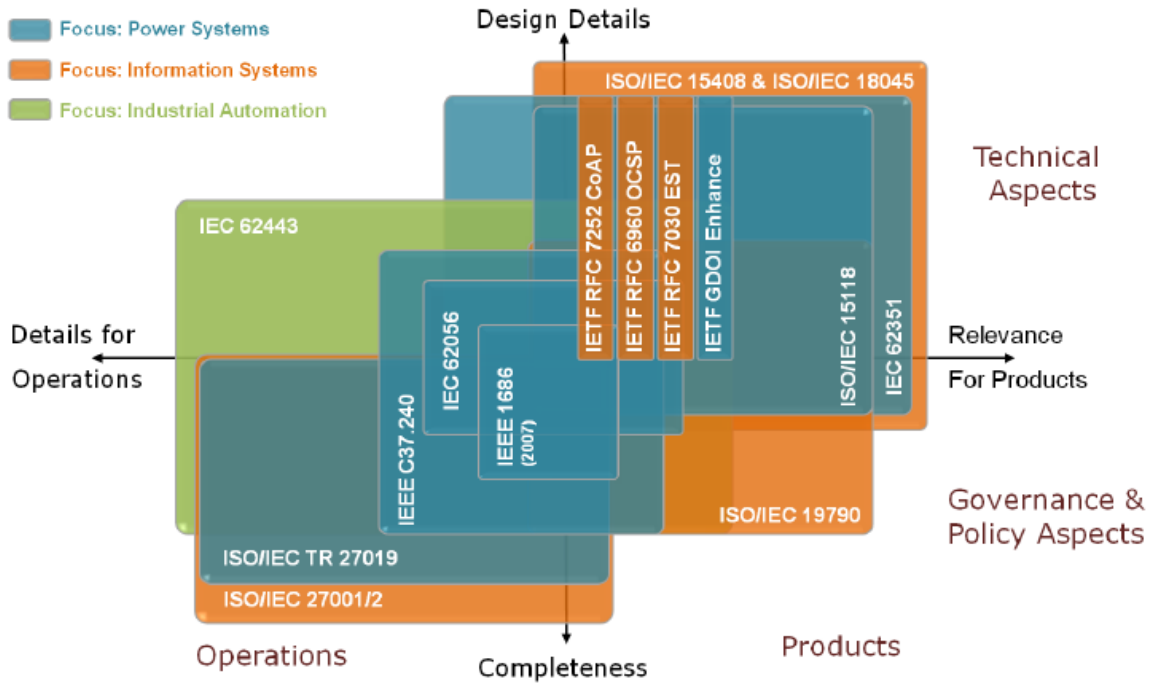

Figure 3: Smart grid standardization landscape - Classification of standards

(Source: [SG-CG/M490/H_Smart grid Information Security 12/2014])

The SGIS report effectively shows where there are gaps in the smart grid standardization landscape. Furthermore, relevant standards are listed for each of the four selected use cases to show their practical applicability.

4.2.3.2 ISO/IEC TR 27019

The Information Security Management System (ISMS) family of standards - beginning with ISO/IEC 27000 -published by ISO and IEC is an internationally recognized code of practice. Organizations in all sectors can have their Information Security Management System (ISMS) - i.e. all processes and measures taken to ensure IT security - certified to ISO/IEC 27001. The standards in the ISO/IEC 27000 family contain provisions that are either normative (i.e. requirements that must be complied with) or informative (i.e. recommendations).

The documents have different objectives and are aimed at different target groups. The central document is ISO/IEC 27001: It specifies generic minimum requirements for an ISMS. It presents over 130 security measures, called "controls", in a table in the Annex. The second main document, ISO/IEC 27002, gives guidance on how to implement the controls described in ISO/IEC 27001.

ISO/IEC TR 27019 is based on ISO/IEC 27002 but extends that standard to focus on sector-specific aspects of the energy utility industry that relate to the smart grid.

The aim is to allow energy utilities to implement a standardized information security management system (ISMS) in accordance with ISO/IEC 27001 that extends from the business to the process control level.

ISO/IEC TR 27019 was prepared by DIN and DKE and was adopted as an International Standard, using the special "fast-track procedure", by Joint Technical Committee ISO/IEC JTC 1. DKE body K 952.0.15 (mirror body to IEC TC57/WG15, see section on IEC 62351) is responsible for the security of network

control technology and initiates activities in close cooperation with the DIN mirror body to ISO/IEC JT1/SC 27/WG1 (who is responsible for the ISO/IEC 27000 standards). The SGIS group working on Mandate M/490 lends much support to this work and feels that ISO/IEC TR 27019 fills an important gap in the standardization landscape.

Thanks to the domain-specific expertise of the members of DKE body AK 952.0.15, the cooperation with the BDEW, and other liaisons in ISO and IEC, it is ensured that relevant, important aspects of process control systems will continue to be integrated into ISO/IEC TR 27019.

4.2.3.3 IEC 62351 Power systems management and associated information exchange – Data and communications security

This standard is seen in almost all international studies and investigations as a key technical standard for information security in the future smart grid. It was prepared by IEC Working Group 15 (WG 15) of Technical Committee 57 (TC 57) which has had the task of developing security standards for the communications protocols defined by TC 57 since 1999. In Germany, "DKE/GAK 952.0.15 DKE-ETG-ITG Information security in grid and station control technology" functions as the national German mirror body. In order to fulfil safety targets in critical infrastructures, information technology as a whole is seen as having "end-to-end requirements". At present, the following communication protocols are covered by IEC 62351:

- IEC 62351-3: Communication network and system security - Profiles including TCP/IP
  - IEC 60870-6 (TASE.2 / ICCP)
  - IEC 60870-5 Part 104
  - IEEE 1815 (DNP3) about TCP/IP
  - IEC 61850 about TCP/IP
- IEC 62351-4: Data and communications security– Profiles based on MMS (Manufacturing Message Specification):
  - IEC 60870-6 (TASE.2 / ICCP)
  - IEC 61850 using MMS profiles
- IEC 62351-5: Data and communications security – Security for IEC 60870-5 and derivatives:
  - IEC 60870-5, all parts
  - IEC 61850 using MMS profiles
  - IEEE 1815 (DNP3)
- IEC 62351-6: Data and communications security – Security for IEC 61850 peer-to-peer profile:
  - IEC 61850 profiles, not based on TCP/IP: GOOSE and SV

Figure 4 shows the interconnection between the above-mentioned standards

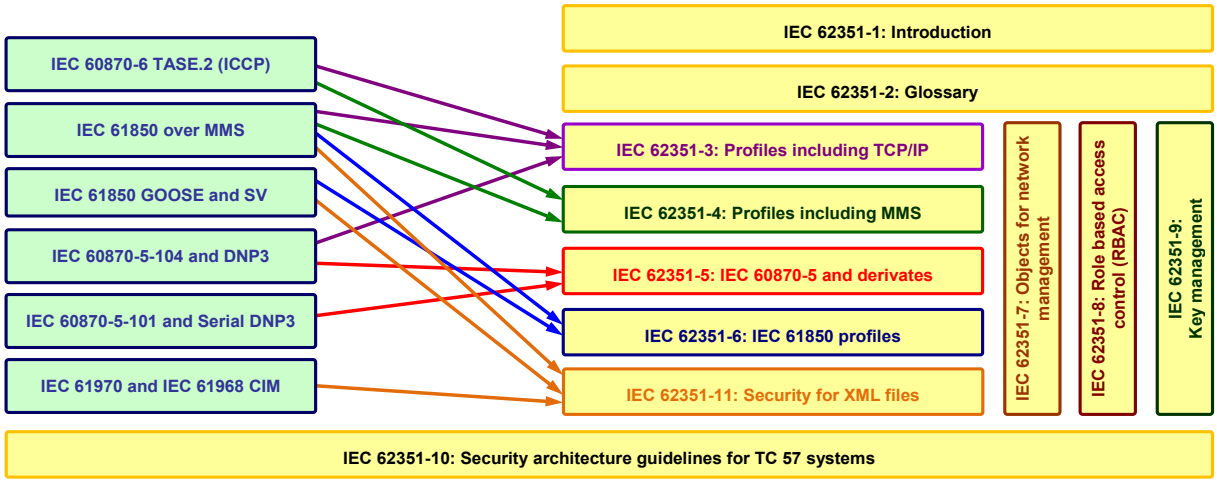

Figure 4: IEC TC 57 communications standards and their relation to the various parts of IEC 62351 [Source: IEC]

In the following section, the individual parts of this standards series are listed, with brief summaries of their contents as well as possible future developments. Most parts of the IEC 62351 series have been developed as technical specifications. Some of these parts are currently being developed into full International Standards.

IEC 62351-1: Introduction

This part of the standard provides an overview and background information on the topic of information security in the energy domain and the particularities that apply here. In addition, relevant safety targets (Confidentiality – Integrity – Availability – Non-Repudiation) and necessary measures to prevent specific threats are broadly introduced, as seen in the following flowchart:

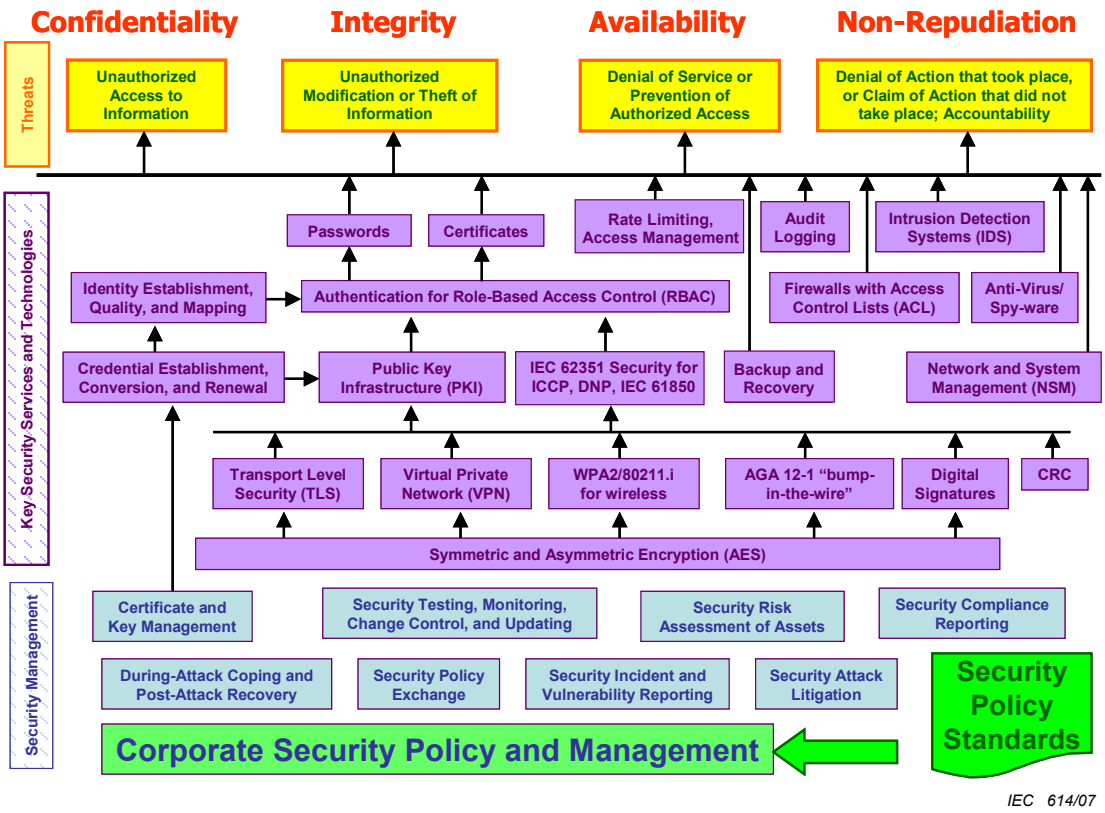

Figure 5: Security requirements, threats, counteractive measures and management [Source: IEC 62351-1]

IEC 62351-2: Glossary of terms

This part includes all relevant terms and abbreviations found in this standards series.

IEC 62351-3: Communication network and system security – Profiles including TCP/IP

Part 3 of the standard deals with telecontrol protocols that make use of TCP/IP as a message transport layer. It specifies how to provide message level authentication, confidentiality, and integrity protection using Transport Layer Security (TLS): For example, optional TLS components are made obligatory and special requirements for are laid out for network control technology on the certificate to be used. This part of the standard is currently under revision (will be released as a 2nd edition). With this revision, additional TLS mechanisms will be added and the cipher suites updated.

IEC 62351-4: Data and communications security– Profiles including MMS

Part 4 specifies procedures, protocol extensions and algorithms to facilitate securing ISO 9506 (Manufacturing Message Specification) based applications. MMS is used in network control technology with messaging systems that have real-time demands. Part 4 also defines TLS based procedures at the transport and application layers based on the profile in Part 3. Currently, corrections which have arisen due to interoperability tests are published as supplements. Edition 2 of this part of the standard is planned.

IEC 62351-5: Data and communications security – Security for IEC 60870-5 and derivatives

Part 5 of the series takes into consideration the special aspects of serial communication. It defines security measures which ensure the integrity of the serial connections using a Keyed-Hash Message Authentication Code (HMAC). It is currently planned that Part 5 will include a separate key management specification; the exact mechanisms to be used are still under discussion.

IEC 62351-6: Data and communications security – Security for IEC 61850 peer-to-peer profile:

IEC 61850 specifies three peer-to-peer multicast protocols, that are not to be routed in a substation LAN. The most prominent of these is the GOOSE (Generic Object Orientated Substation Events) protocol, which was developed for the secure transmission of messages between intelligent controllers within 4 milliseconds. Under such difficult real-time conditions, only limited security measures can be implemented, because they have a significant impact upon the processing functions. Part 6 includes digital signatures to protect multicast messages; however, they are difficult or even impossible to employ with the typical field device hardware. An alternative solution is currently being developed in Technical Report IEC 61850-90-5 that would use a group key to gauge the integrity value instead of a device-specific digital signature. This approach is now being gradually incorporated into the further development of different parts of IEC 62351.

IEC 62351-7: Network and system management (NSM) data object models

Part 7 focuses on network and system management (NSM) data object models specific to the infrastructure of power system operations. WG 15 defined abstract NSM data objects for the control and monitoring of both the network and connected devices in order to work out which information is necessary at a control centre to manage the information infrastructure just as dependably as the energy infrastructure systems. Typical management protocols like SNMP can be combined with this information. With a monitoring system of the network in place, attacks should be recognized quickly, allowing fast countermeasures to be taken.

IEC 62351-8: Role-based access control

The central focus of Part 8 is on role-based access control (Role-Based Access Control, RBAC) for enterprise-wide use in power systems. Integration into the entire energy supply domain is essential, because authentication and traceability are imperative in protection systems and control areas. Part 8 describes three different access token formats, supported as three different profiles, to transport information. Two of them are X.509 Access tokens and the third is a software token similar to Kerberos.

IEC 62351-9: Key Management

Part 9 of the series, still under development, specifies how digital certificates and encryption keys are best generated, distributed, revoked and processed in order to protect digital information and communications. In addition, the scope of this standard covers the safe handling of symmetric keys (pre-shared and session keys). Part 9 describes both protocols and technologies typically employed for key management and a number of use cases that utilize these technologies.

IEC 62351-10: Security Architecture

Part 10 lays out security architecture recommendations for the entire IT infrastructure based upon fundamental security measures (components, functions and their interaction It is intended to support system integrators in using the relevant standards to operate power systems and energy transmission and distribution centres securely. The following flow chart shows the fundamental architecture upon which IEC TC 57 communication standards and security measures are based.

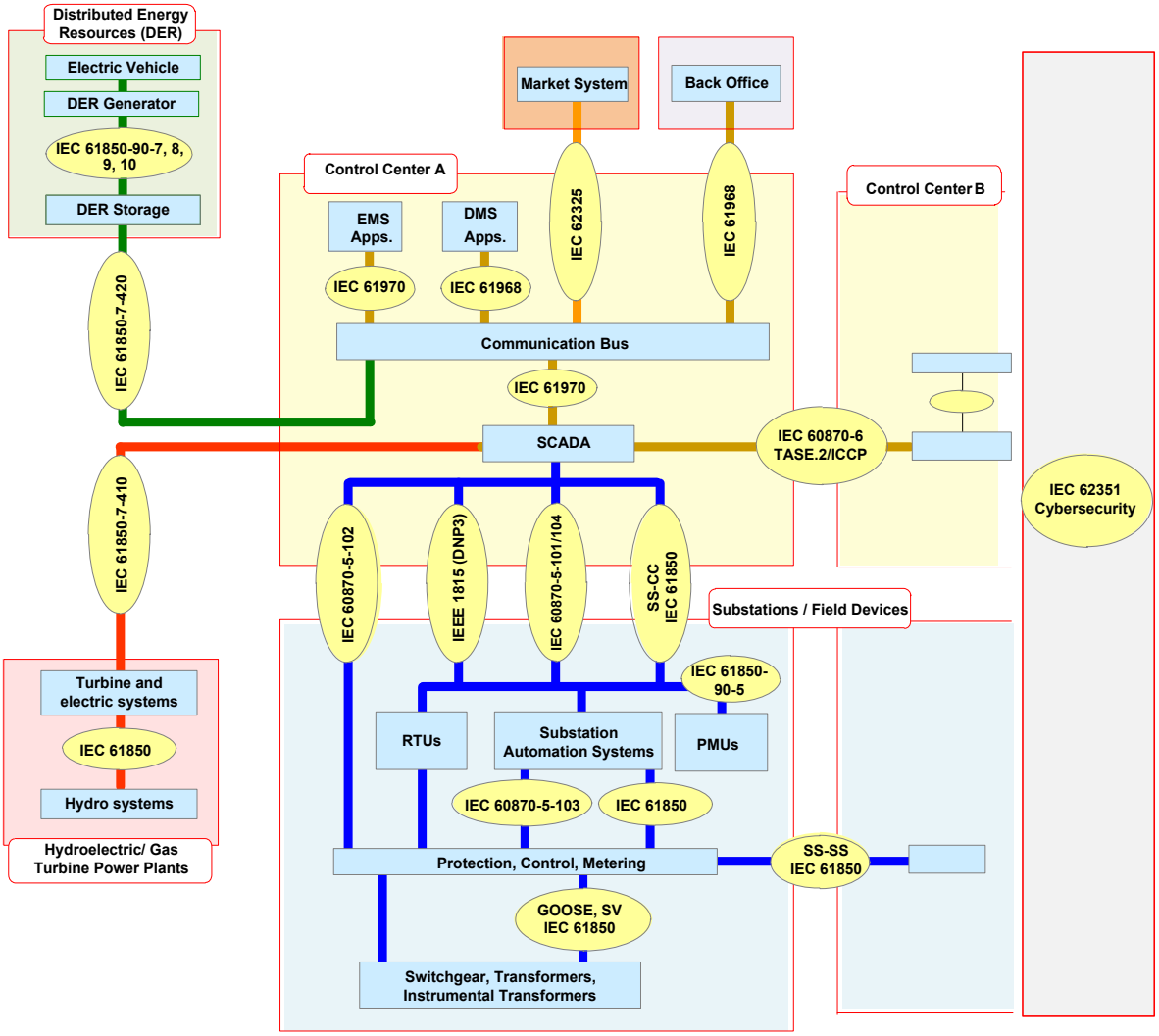

Figure 6: IEC TC 57 Architecture of communications standards [Source: IEC 62351-10]

IEC 62351-11: Security for XML files

The work on part 11 began in the summer of 2012 and has not yet been completed. The main objectives of this part are:

- Definition of a mechanism that can authenticate the XML source file, and in particular, to classify the sensitivity of the transported data (tagging). This should help the person processing the information to handle the file appropriately based on its level of sensitivity, addressing the data protection not only during the communication, but also during the local processing and saving.
- Definition of a mechanism that recognizes manipulation attempts
- Definition of security measures, ensuring that maximum compatibility with the present formats (CIM, SCL and other SML formats) is reached

4.2.4 Conclusions and need for action

In its final report, the SGIS states that standards are already available that lay down the foundation for IT security in the smart grid. However, it also points out the necessity of continually expanding existing standards in order to integrate IT security requirements specific to the smart grid, and new technologies, architectures and use cases.

Particular attention should be paid to making the standards and guidelines for implementation as easy to use as possible.

The SGIS report [*SG-CG/M490/H_Smart Grid Information Security 12/2014]* describes the standardization gaps to be filled.

In 2014 it was widely agreed that the SGIS should continue its activities beyond the end of Mandate M/490. Cooperation with US organizations is encouraged.

In Germany, DKE/UK STD_1911.11 "Smart Grid Information Security“ - which is part of the DKE-Kompetenzzentrum (DKE Expertise Centre for E-Energy) is proactively supporting this work.

4.3 Industrial production (Industry 4.0)

4.3.1 Description of topic

Today's production industry is becoming increasingly automated by means of networked computers, measuring and control systems. This means that not only is business software (e.g. SAP, Windows, etc.) a central focus for IT security, but production systems are as well. Technologies that once were independent of each other are becoming more closely networked. In addition, automation technology is increasingly making use of "COTS" (commercial-off-the-shelf) and generic hardware and software, and open standards such as TCP/IP are being used for communications. However, TCP/IP security mechanisms commonly used in the business world are not necessarily appropriate for the production industry. This is one reason Industry 4.0 involves complex security issues that are difficult to foresee, due to the interaction between office IT systems and production IT systems (similar to the smart grid). Such issues need to be addressed and re-evaluated. Standards play a decisive role in this, because they help identify not only the security needs in production and manufacturing, but also the relevant threats. This makes it easier to develop effective measures and a strategic, holistic standardized IT security concept.

Industry 4.0 is bringing new areas and new systematic approaches to the forefront. Concepts going across levels and domains must be developed and standardized. It is not sufficient to set up a higher level over all; rather, a comprehensive, holistic approach is needed, as are efforts to go beyond the usual work of standardizing bodies in order to effectively support these developments with standards and specifications. Key aspects of Industry 4.0 are:

- Automation technology
- Functional safety (FS)
- Information and communications technology (ICT)
- IT security

4.3.2 Standards bodies active in this area

The development of full consensus-based standards is a long-term task carried out in Germany by DKE and DIN, in Europe by ETSI, CENELEC, CEN and internationally by IEC and ISO. In addition to these officially mandated bodies, other groups are drawing up specifications and guidelines for standardizing Industry 4.0. The table below gives an overview of some bodies active in Industry 4.0 standardization relating to IT security:

Organization	Standards body	Title of standards body	Field of activity
DIN	NA 043-01-27 AA	IT Security Techniques	Mirror committee to ISO/IEC JTC 1/SC 27
DKE	DKE/GK 914	Functional safety of electric, electronic and programmable electronic systems (E, E, PES) for protection of persons and the environment	Mirror committee to IEC TC65/SC 65A/WG 14

Organization	Standards body	Title of standards body	Field of activity
DKE	UK 931.1	IT security for industrial automation systems	Mirror committee to IEC TC65/WG 10
CEN	TC251	Health informatics	IT security for industrial automation systems
ISO/IEC	JTC 1/SC 27	IT Security Techniques	Generic IT security / Information Security Management Systems
IEC	TC65	Industrial-process measurement, control and automation	Medical informatics
ETSI	TC Cyber	Technical Committee (TC) Cyber Security ETSI	Develop and maintain the standards, specifications and other deliverables to support the development and implementation of cyber security standardization within ETSI
ISA	ISA 99	Industrial Automation and Control Systems Security	IT security of production control systems

4.3.3 Current standardization landscape (as regards IT security)

The IEC 62443 series of standards play an important role in the IT security standardization landscape. However, the extent to which these standards cover all necessary subjects must still be investigated in detail.

Key documents are described in more detail below.

4.3.3.1 IEC 62443 Industrial communication networks - Network and system security

The IEC 62443 standards series, which is currently under development, is of major importance for IT security in Industry 4.0.

This series is being developed by IEC/TC 65 working closely with the US organization "International Society of Automation (ISA)", who had published the ISA 99 standards upon which the IEC standards are based. The standards cover the implementation of electronically secure Industrial Automation and Control Systems (IACS), including critical infrastructures such as power systems. The ISA 99 standards are being agreed upon within the international standards body IEC - for the most part, they are identical with the IEC 62443 standards (except for IEC 62443 Part 4).

The European standards organization CENELC has decided to adopt the IEC 62443 series in the future.\\BLNS9B4X.DINGRUPPE.NET\proj\SD\Übersetzungen außer Normen\DIN\Roadmap KITS-DIN-DKE-IT Security\ - True The DKE body UK 931.1 "IT-Sicherheit in der Automatisierungstechnik" expects this series to be published in Europe as EN 62443 standards starting from 2015 - in Germany,

the standards will be published as the DIN EN 62443 (VDE 0802) series. The standards will not only apply to automation technology, but will also be important for network control technology and control systems for critical infrastructures.

As mentioned above, IEC 62443 is based on the ISA 99 standards published in the United States. Thus, ISA 99.00.01 corresponds to IEC 62443-1-1. The following parts of the standards series have either been published or are planned:

- IEC/TS 62443-1-1, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models; status of development: IEC/TS 62443-1-1, edition 1.0 (2009-07), revision planned

Subclause 1.2 "Included functionality" explicitly states that the scope of the technical specification not only covers industrial automation systems, but also systems that are commonly used by organizations that operate in critical infrastructure industries, such as electricity transmission and distribution, or gas and water distribution networks. (see also section 4.2.4 of this roadmap). Subclause 5.3 of the IEC specification lists the "Foundational requirements":

a) Identification and authentication control (IAC): Monitoring use of selected devices, information or both as protection against unauthorized access;
b) Use control (UC): Monitoring use of selected devices, information or both as protection against unauthorized use;
c) System integrity (SI): Ensuring integrity of data in selected communication channels, thus providing protection against unauthorized exchange of data;
d) Data confidentiality (DC): Protecting selected communication channels from listening/tapping in order to ensure the confidentiality of particular data;
e) Restricted data flow (RDF): Restricting the data flow in communication channels as protection against the passing on of information to unauthorized data sinks;
f) Timely response to events (TRE): Responding immediately to IT security breaches by notifying the responsible bodies, requesting that the necessary evidence be secured, and at the right time, making sure corrective measures are taken in critical situations or situations that are critical to safety;
g) Resource availability (RA): Ensuring the availability of all network resources as protection against denial-of-service attacks.

Other concepts introduced in this document are Defence in Depth, Threat and Risk Assessment (TRA), the IT security program maturity, IT security policies, zones and conduits (for segmenting and isolating subsystems), and security levels (SL).

The security levels describe the effort an expected attacker will make :

- SL 1: casual or coincidental misuse,
- SL 2: intentional misuse using simple means,
- SL 3: intentional misuse using sophisticated means,
- SL 4: intentional misuse using sophisticated means with extended resources.

There are three different types of security levels:

- SL-T (SL target): target security level for a zone or conduit (result of a threat and risk assessment),

- SL-C (SL capability): inherent security level capability of devices or systems (when correctly implemented and configured),
- SL-A (SL achieved): achieved security level (for the entire system).

- IEC 62443-1-2, Industrial communication networks - Network and system security - Part 1-2: Glossary. Status: In development
- IEC 62443-1-3, Industrial communication networks - Network and system security - Part 1-3: System security compliance metrics. The Draft Technical Specification (DTS) was rejected by IEC in the first quarter of 2014
- IEC 62443-2-1, Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program. Status: IEC 62443-2-1:2010 (DC 10/12):

  This standard has been developed by IEC TC 65. It specifies the necessary elements for the implementation, management and operation of an IACS security system. These elements include guidelines, procedures, practical implementation and human resources. The standard also gives guidance on developing these elements, which is to be seen as an example that must be adjusted to suit each individual case.
- IEC 62443-2-2, Industrial communication networks - Network and system security - Part 2-2: Implementation guidance for an industrial automation and control system security program. Status: planned
- IEC 62443-2-3, Industrial communication networks - Network and system security - Part 2-3: Patch Management. Status: Technical Report (TR) for the first quarter of 2015
- IEC 62443-2-4, Industrial communication networks - Network and system security - Part 2-4: Requirements for IACS solution providers. Status: International Standard (IS) for the second quarter of 2015.

  This standard specifies requirements for IT security regarding policy, procedures, practice and personnel, which can be applied by suppliers of industrial automation systems throughout the life cycle of their products.
- IEC 62443-3-1, Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems. Status: IEC/TR 62443-3-1:2009-07. Revision planned

  This part of the standard describes and evaluates various IT security techniques, for example authentication, authorization, filtering, blocking, access control, encryption, validation, auditing and measuring, monitoring, and operating systems.
- IEC 62443-3-2 Industrial communication networks - Network and system security - Part 3-2: Security levels for zones and conduits. Status: Committee Draft for Vote (CDV) in the second quarter of 2015.
- IEC 62443-3-3 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels. Status: IEC 62443-3-3:2013.

This document provides detailed technical control system requirements (SRs) for each of the seven foundational requirements (FRs) defined in IEC 62443-1-1. For some SRs, a number of even more detailed "requirement enhancements" (RE) are given. For example, twelve system requirements are defined for FR 2 "Use Control (UC)". In addition, several "requirement enhancements" are given for SR2.1 "Authorization enforcement", e.g. SR 2.1 RE 2 "Permission mapping to roles". This specifies that an authorized user or role must be able to define and modify the mapping of permissions to roles for all human users. System requirements (SR) and requirement enhancements (RE) are defined in terms of control system capability security levels (SL-C), which is a security level that the system is capable of reaching when it is correctly configured. IEC 62443-3-3 thus makes it possible, for SL-C, to adjust the requirements to the system technology, or to define the achievable SL-C when requirements are met. This document also describes conditions that are typical for industrial automation and control systems, such as maintaining real-time characteristics when an IT security event is identified, maintaining security functions, or continuing to operate during a denial-of-service event..

- IEC 62443-4-1 Industrial communication networks - Network and system security - Part 4-1: Product development requirements Status: Document for Comment (DC) planned for first quarter of 2015
- IEC 62443-4-2 Industrial communication networks - Network and system security - Part 4-1: Technical requirements for industrial automation and control system components Status: Document for Comment (DC) planned for first quarter of 2015

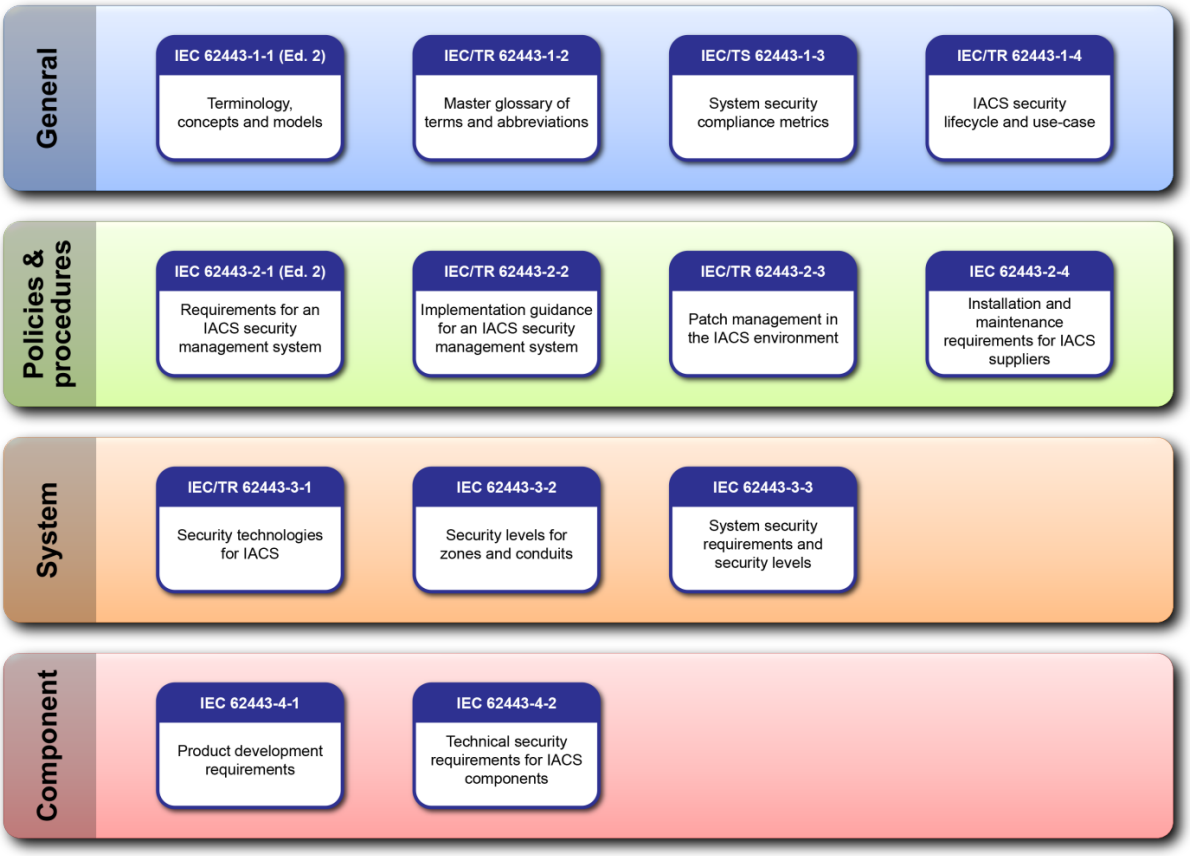

Figure 7: Structure of the IEC 62443 series

4.3.3.2 - NAMUR Worksheet NA 115 - "IT-Security for Industrial Automation Systems - Constraints for measures applied in process industries"

NAMUR, the "User Association of Automation Technology in Process Industries" published its worksheet NA 115 in 2006. This document includes reports of experience gained by and working documents for the chemical and pharmaceutical industries. It is not a standard or guideline, but rather describes state-of-the-art technological developments. The protection targets in IT security for the process industry are listed in order of priority: 1. Availability, 2. Integrity, followed by authenticity, confidentiality, non-repudiation and controllability. Over the past few years IT security has increasingly become important for industrial automation. Reasons for this include expanded system functionality in comparison with earlier systems, along with a greater integration of these systems in the IT landscape of companies, and the transition from proprietary systems to systems based on standard hardware and operating systems. The greater integration of systems not only increases the possibility of attacks, the use of standard IT components also means that these attacks have a higher chance of success. In fact, modern automation technology is just as vulnerable as are classical IT systems. The purpose of this NAMUR worksheet is to illustrate the framework conditions associated with IT security products in automation engineering from the point of view of the user. It is intended for manufacturers and system integrators, and provides them with information on framework conditions specific to the process industry as regards the implementation of security measures and/or design of new systems. It also addresses users, giving them relevant criteria to consider when making a purchasing decision. This NAMUR worksheet addresses measures that are indispensable for current systems, as well as the development of future industrial automation systems from the point of view of IT security.

4.3.3.3 VDI/VDE 2182

This VDI/VDE Guideline was developed by Fachausschuss 5.22 "Security" of the VDI/VDE Society for Measurement and Automatic Control (VDI/VDE-GMA). The aim was to provide a basis for discussion - from the German standpoint - that at the time (2011) was lacking at both national and international level.

The guideline describes how specific measures can be implemented in order to guarantee the IT security of automated machines and installations; aspects of the automation devices, systems and applications used are taken into consideration. Using a common terminology that has been agreed on by manufacturers and users (e. g. machine vendors, integrators, plant management), a uniform, practical procedure for ensuring IT security throughout the entire life cycle of automation devices, systems, and applications is described. For the purposes of the guideline, "life cycle" encompasses the development, integration, operation, migration, and decommissioning phases.

Part 1 defines a simple, iterative eight-step model procedure for the development and description of IT security. This document is by-and-large a "best practice" that consists of open "to do" points and experience gained by the members of the issuing organization. Drawn up not only by the VDI/VDE Society for Measurement and Automatic Control, but also with the contribution of other German technical associations such as NAMUR, ZVEI, and VDMA, Part 1 does not apply to any specific applications, such as the smart grid. Other parts - Parts 2.1, 2.2, 3.1, 3.2, 3.3 - give examples of how automation is used in the production and process industries. The focus of Fachausschuss 5.22 was not on the smart grid or energy issues.

Fachausschuss 5.22 has decided to make its results and knowledge open to the public for discussion. For example, a number of related documents have been published and there were many forums, workshops and discussions at trade fairs. There has also been cooperation with DKE bodies such as DKE/GAK 952.0.15 DKE-ETG-ITG "Information security in grid and station control technology" and DKE/UK 931.1 "IT security in automation technology". The Fachausschuss 5.22 regularly reports on its work in joint meetings, with the aim of bringing the concepts laid down in VDI/VDE 2182 to international standardization. The DKE body DKE/AK 952.0.15 has discussed publishing a further part of this series that will deal with energy.

4.3.3.4 Industrial Control System Security Compendium

In 2013 the German Federal Office for Information Security (BSI) published a "compendium" on the IT security of industrial control systems (ICS). This document serves as a basis for discussions between IT and cyber security experts and industry specialists. It includes a best practice guide for operators, an audit methodology for ICS installations, an overview of R&D that still needs to be carried out, and the standardization landscape. The aim is to synchronize the sector-specific know-how in the international standards bodies with the work of the Federal Office for Information Security to keep national and international activities from going in different directions.

In 2014 the Federal Office for Information Security also published an "ICS Security Compendium" addressed to manufacturers of components. It provides guidance on establishing a "security by design" approach to component development, using IT security tests and measures for avoiding weaknesses.

4.3.4 Need for action

4.3.4.1 Functional security - IT security

A central aspect of IT security in Industry 4.0 is the relationship between "functional" security and IT security when networking automation and production systems.

Currently, many different groups are working intensively on effectively establishing IT security in safety-relevant systems in various industrial sectors, although there are many diverging opinions, approaches and terminologies. This makes an exchange of information essential for the development of uniform, standardized solutions. In DKE a cross-sectoral working group ("TBINK ad-hoc working group IT security") has been set up to deal with these issues. Experts from several standardization bodies are working together to produce quick results that can be integrated into current standardization activities.

4.3.4.2 Current standardization landscape

Essential functions of any IT system are protecting information - a valuable asset - from loss and misuse, ensuring timely access to this information for authorized users, and maintaining the integrity and confidentiality of this information. Virtualization, increasing flexibility, and the linking of company production and field networks with global networks are presenting numerous new challenges for information security. In Germany, information on activities in this area - including requirements, legal provisions and recommendations - can be obtained from a number of sources, such as the "Landesdatenschutzbeauftragten" (Data Protection Commissioner of the German

Länder), the BSI (Federal Office for Information Security), national and international standards organizations (e.g. DIN, DKE, IEC) and relevant technical associations (BITKOM, VDE, VDI, GMA).

It is absolutely essential that a roadmap be drawn up describing the fields, requirements and available IT security solutions relating to industrial production.

4.4 Medical technology

4.4.1 Description of topic

Medical technology is developing from a world of individual devices for patients to the wide-spread use of IT-supported systems. For example, in operating theatres and intensive care units there is a trend towards presenting digital information on monitors so that doctors can react quickly when carrying out complex treatments. This IT networking of diagnoses, communications and therapies presents the medical technology sector with new challenges in terms of IT security. This is particularly so because the protection of personal data and the availability of such - sometimes vitally important- data are highly sensitive protection targets. However, these targets can also sometimes contradict each other due to legal implications.

The broad scope of privacy and data security standardization in the health and social services sectors therefore encompasses the specification of methods and systems which ensure and improve the confidentiality, integrity and availability of health information. It also covers the protection of systems from negative impacts on patient safety, the protection of personal data containing health information, and ensuring that system users can still carry out their responsibilities in terms of the health information system.

One particular aspect of healthcare and social services (and thus also medical technology) is the high regional fragmentation of processes and organizations, which makes traditional standardization more difficult, even at the technical and procedural levels. This is reflected in information technology for medical care processes, which likewise makes traditional standardization difficult.

To effectively address this issue, it has proven useful to focus on the standardization of infrastructure elements and fundamental processes, which are then generically specified. This approach allows regional or specialist groups to draw up concrete technical standards based on common architectures and services, achieving an interoperability that nevertheless can only go so far as the consensus reached at specialist level.

Although this criticism of the lack of interoperability among healthcare IT systems is technically correct, it also ignores the core issue, which is the lack of processes that cooperate with one another, together with a lack of technical consensus at application level.

This means that to ensure IT security in this sector, users who are standards setters must always take into consideration organizational frameworks and relevant technical processes, if a useful implementation guideline (which is the actual technical standard specification) is to be drawn up from the diverse standards described below. For IT systems used in healthcare and medical technology, then, it is not only important to focus on the technical "building blocks" of IT security, but also on models and methods which are to be used in specific cases. For this reason, reference is repeatedly made to models at different abstraction levels, and to modern design methods and the realization of services, terminologies, (object) databases and registers.

Not only are domain-specific requirements, functional models, and service functional models described, but infrastructure services (directory services, terminology services, policy representations, etc.) and basic definitions such as ontologies, terminologies and vocabularies are standardized as well. Domain-specific supplements to existing cross-domain specifications are also drawn up.

Taking data security into consideration - which at international level normally includes data protection - a differentiation can be made between communications security and application security. (see Figure 8)

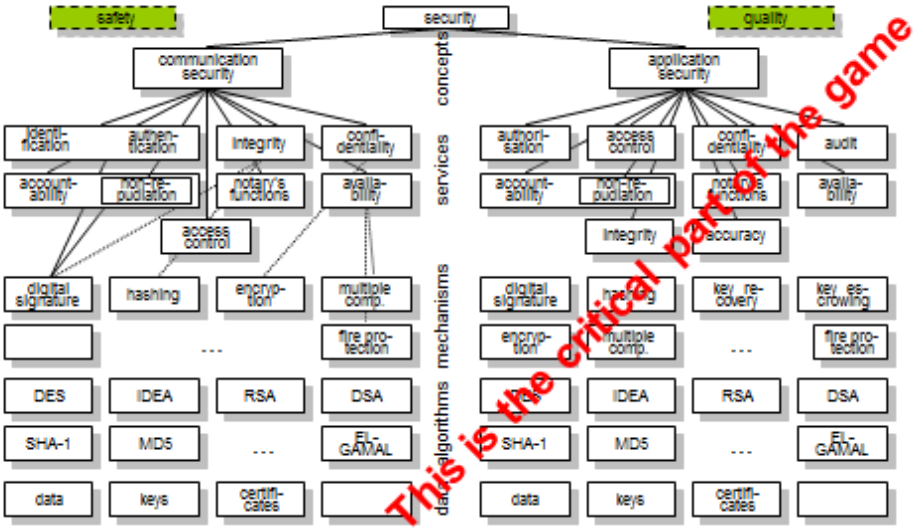

Figure 8: Security Concepts (Blobel B, Roger-France F (2001) A Systematic Approach for Analysis and Design of Secure Health Information Systems. International Journal of Medical Informatics 2001; 62 (3): 51-78)

Communications security services are not domain-specific and thus existing specifications and solutions from other domains (such as finance, telecommunications, administration) can be used. However, application security services regarding privileges management, access control, and the use of personal health information are affected by domain-specific rules (laws, regulations, rules laid down by bodies such as governments, self-governing organizations, professional organizations, etc.). ISO 22600 refers to such rules as "policies".

4.4.2 Standards bodies active in this area

The following standards bodies are working on standards relevant to IT security in the medical sector:

Organization	Standards body	Title of standards body	Field of activity
DIN	NA 063-07-04 AA	Medical informatics — Security	Security in medical informatics
DKE	UK 811.3	Security of networked devices, systems and installations used for medical purposes	Operating medical devices in IT or medical networks

CEN	TC251	Health informatics	Medical informatics
ISO	TC215	Health informatics	Medical informatics

4.4.3 Current standardization landscape (as regards IT security)

Particular focus is placed on promoting data protection and security in communications and cooperation between organizations that are directly or indirectly involved in health and welfare (intersectoral communication and cooperation). Standardization will encompass the necessary infrastructure services (identification, authentication, directory services, etc.), privileges management and access control on the basis of explicit policy specifications, role definitions, data protection and data security attributes in the context of information and document exchange, but also the transfer of extracts from electronic health records. Standardization activities in the health sector carried out to ensure application security focus on privileges management and access control, including related aspects such as taking patients' wishes into consideration, limiting the use of the data and using them only for the specified purpose(s).

The health telematics infrastructure defined in Germany is oriented towards smart card technologies, and thus specific card standards.

Because acceptance of a solution is decisive for its successful implementation, these standards have to meet the requirements and needs of the most important stakeholders, and bring them clear benefits. Thus, medical services such as electronic health records (EHR) must be given sufficient priority.

Many countries in Europe and beyond are much further than Germany in establishing standardized ICT services for the healthcare and social services sectors.

It is generally acknowledged that medical equipment - especially equipment that has been on the market for a long time - can be targeted by hackers. Equipment operators are playing an increasingly important role in IT security, because they configure component networks on site using a number of different components.

Security aspects can only assessed in connection with the system, taking the following protection targets into consideration: effectiveness, data and system security, and patient safety. Each of these targets has a different significance depending on each medical treatment use case (for example, it is important that doctors always have access to data regarding the patient they are treating, especially in emergency situations). Critical IT systems in the healthcare sector must thus have a risk management program in place that takes into consideration each of the three protection targets in the relevant socio-technical context, ensuring the quality of medical treatment and patient safety. When evaluating systems, not only must normal operations be considered, but also exceptional cases such as mass casualty incidents, catastrophes or terrorist attacks.

IEC 80001-1 describes the risk management of IT networks incorporating medical devices, which serves to assess the three protection targets (called "key properties" in the IEC standards), safety, effectiveness and data and system security, and ensuring optimal patient treatment.

In the case of medical devices, there is a legal obligation to report adverse incidents in order to prevent (further) harm to patients due to the same error. Knowledge gained from incident reports is

incorporated into the risk assessment programs of the manufacturers and operators of the devices. However, this does not apply to information systems that do not lie within the scope of the Medizinproduktegesetz (German Act on Medical Devices), or for critical events - with or without harm to patients - that occur due to incorrect use.

4.4.4 Need for action

Paradigm shifts in technology and other aspects of healthcare and social services - such as ubiquitous healthcare, mobile technologies, the use of social media and big data analytics - present new challenges for data protection, data security and IT security. To face these challenges, new standardized solutions must be developed. Another growing aspect of data security which must be taken into consideration (e.g. in accordance with Germany's Medizinproduktegesetz) is the integration of biomedical technologies and new pharmaceutical applications. The number of SOA-based specifications is also growing. Wherever possible, projects should be proactive rather than reactive.

However, most standard solutions, and even standardized ICT drafts and architectures, pose two major issues in today's networked healthcare system: the ICT protection targets themselves, and the responsibility for maintaining these targets when implementing partial solutions at component or functional level. An assessment of the suitability of the IEC 62443 series - which is so relevant to Industry 4.0, as discussed earlier in this roadmap - for clinical/medical ICT is urgently needed, especially because it has been recognized by the US FDA as a cybersecurity standard, although responsibilities are not described. Using the IEC 62443 series, or parts thereof, as a basis and then adapting it to suit German conditions in the healthcare sector is desirable, because this would provide legal security, transparency and trust for all involved.

It is recommended that more human and financial resources be invested In health telematics and health informatics standardization in Germany. Closer cooperation with standards bodies such as ISO, CEN, ETSI and CENELEC, and standards-setting organizations such as OMG, OASIS, HL7, IHE, etc. would be of great advantage. Existing activities should be supported. An integrative structure similar to that of the formally accredited Standards Collaborative in Canada, which brings together national bodies in the Canadian SDOs, would also be of great value. More and more countries are following this example.

IT security in medical technology is being faced by very special challenges. The availability and usability of devices and services are clearly of prime importance. In day-to-day clinical operations, however, it is difficult to make clear the loss of usability due to security measures. The concept that IT security incidents threaten the usability of IT systems has not yet seeped through to all levels, including the user level. Standards and specifications can create greater acceptance of security solutions if usability is taken into consideration as early as their design phase. This applies both to incident control and incident avoidance. Users must be aware of the condition of the system they are using in order to be able to turn to alternatives, for example in the case of a corrupted system. Due to the close connection between medical technology and information systems in the healthcare sector, it is recommended that work be in line with DIN EN 62366. Because of the heterogeneity of the socio-technical environment when operating critical IT systems, and the resulting risks to the healthcare system, it is important to learn from such incidents. That is why setting up or using existing incident reporting systems for IT-associated treatment errors or adverse effects on patients

is desirable. This should include operating errors in order to gain information for the further development of usability standards.

The integration of mobile devices presents another great challenge - there are not yet any standardized requirements for integrating them into the security architecture. Above all, the international standards organizations are called upon to develop standards and specifications that are as generic as possible so they can be used worldwide. Also, a closer integration of AAL applications will be necessary, in order to ensure the treatment of persons in their own homes.

4.5 Electromobility

For Germany to improve on its competitive edge in the international electromobility market, and to ensure that the development and added value of this technology remains in this country, a major focus must be placed on furthering and bundling these developments, and the interests behind them, at an early stage. If German industry is to position itself successfully, it is essential that the positive effects of standardization be incorporated into the development process right from the start so that they can be fully exploited.

Standardization in the field of electromobility is characterized by several features distinguishing it from previous standardization processes. Here, the challenge lies in coordinating and integrating diverse activities in different sectors in order to effectively meet demands. Electromobility is a breakthrough innovation that requires a new, cross-sectoral systemic thinking. Up to now, standards in the electrical engineering/energy technology and automotive technology domains have been dealt with separately. So far there has been little attempt to view them in an integrated manner, although this would be an important approach, particularly because these domains are merging, resulting in new points of contact and interfaces.

Electromobility will result in a large amount of information that will be collected and stored at various points and exchanged via various communications interfaces between the involved parties. Ensuring adequate security of these data and of the data processing systems is therefore of great importance. Where this data is of a personal nature, ensuring comprehensive data privacy is particularly important for the wide-spread acceptance of electromobility. Data security and data protection are thus cross-sectorial issues that must be dealt with for all individual systems and communication interfaces.

The German Standardization Roadmap for Electromobility – Version 3.0 (December 2014] is an update of the roadmap originally published in Fall of 2010. It addresses current developments and framework conditions in electromobility, and describes current standardization activities as well as work that must still be carried out. This Electromobility Standardization Roadmap reflects the general agreement among all actors in the electromobility sector - including automobile manufacturers, the electrical industry, energy suppliers/grid operators, communications grids operators, technical associations and public authorities. As such, the roadmap represents the German strategy for electromobility standardization.

Political action is needed at European and international level

The close networking of research and development, and of regulatory and legislative frameworks with standardization is necessary. National standardization and regulation carried out by certain countries must not impede harmonization at an international level.

Standardization must be timely and international

At present, national and international standardization concepts compete with one another. However, since road vehicle markets are international, efforts must aim towards developing international standards right from the start. The same applies to interfaces between electric vehicles and the infrastructure. Standardization at national or European level alone is considered to be inadequate. It is therefore essential that national standards proposals be processed quickly and that German results be transferred to international standardization as soon as possible.

Coordination and focus are absolutely essential

Because e-mobility involves so many actors and sectors, collaboration among all relevant bodies, and coordination by DIN's Electromobility Office and the steering committee EMOBILITY (DKE/NA Automobil) are important to avoid duplication of work. New bodies should not be created; instead, the existing committees within DIN and DKE are to be strengthened.

Standards must be clear and unambiguous

To encourage innovation, standards should be function-related and should avoid the definition of specific technical solutions (i.e. they should be performance-based rather than descriptive). Nevertheless, some technical solutions need to be defined in interface standards to ensure the necessary interoperability (e.g. between vehicles and the network infrastructure).

A uniform worldwide charging infrastructure is necessary (interoperability)

It must be possible to charge electric vehicles “everywhere, at any time”: The interoperability of vehicles of different makes with various operators’ infrastructures - and a sufficient IT security - must be ensured. The standardization of charging techniques and billing / payment systems must ensure the development of a charging interface that is user-oriented, uniform, safe and easy-to-operate. User interests must have priority over the interests of individual companies.

Existing standards must be used and further developed without delay

There are already a number of standards in the automotive technology, ICT and electrical engineering sectors. These must be appropriately utilized and made known. Providing information on these standardization activities and their status are an important part of Version 3.0 of the German Standardization Roadmap for Electromobility.

Moreover, the necessary work should focus less on initiating new standards projects than on expanding/adapting existing standards and specifications to the needs of electromobility. Cross-sectoral cooperation at international level is required particularly for the standardization of interfaces and IT security.

Participation in European and international standardization is essential

In order to achieve our aims – and to ensure our active influence - a greater participation at national and international level is needed. This means that German companies must play a greater part in German, European and international standards work. Standards work is to be seen as an integral component of R&D projects and thus eligible for funding.

Standardization is a central factor for disseminating electromobility, in addition to road vehicle engineering, energy supply, and the associated information and communication technologies.

The automotive engineering, electrical engineering/energy technology, information and communication technology (ICT) and IT security domains, which up to now have largely been considered separately, need to converge if electromobility is to be a success. This calls for a long-term strategy that takes national interests into consideration while at the same time giving German industry access to the expanding international market. Version 3.0 of the German Standardization Roadmap for Electromobility is part of this strategy and embraces immediate standardization needs at one end of the scale and long-term standardization activities at the other, as well as the need for research.

System components, domains and subsectors relating to electromobility standardization are shown in Figure 9. Product safety and communications are cross-cutting topics which affect all system components. Standardization requirements can be divided into the following main areas.

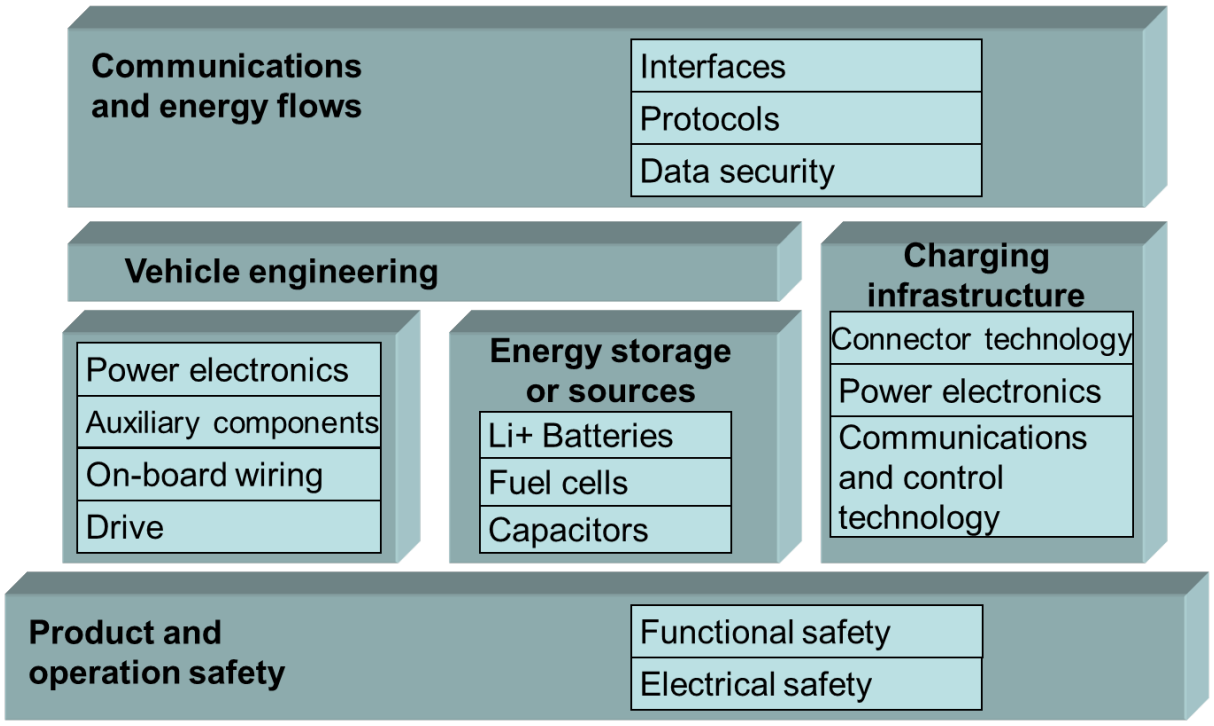

Figure 9: Standardization of relevant system components and domains [Source: The German Standardization Roadmap for Electromobility – Version 2.0A, DIN/DKE May 2013]

4.5.1 Standardization activities: Data security and data protection

Electromobility will result in a large amount of information that will be collected and stored at various points and exchanged via various communications interfaces between the involved parties. Ensuring adequate security of this data and of the data processing systems is therefore of great importance. Where this data is of a personal nature, ensuring comprehensive data privacy is particularly important for the wide-spread acceptance of electromobility. Data security and data protection are thus cross-sectorial issues that must be dealt with for all individual systems and communication interfaces. The essential aspects of these subjects, and the provisions of the Energiewirtschaftsgesetz - EnWG (German Energy Law) are of prime importance.

Owing to the many types of communication interface between the various systems, a number of data security threats and data protection violations are possible and must be taken into consideration. Examples of such threats are:

- Attacks on central systems for energy trading transactions and payment settlement, with the objective of compromising and manipulating the system.
- Attacks on central systems for controlling energy supply grids and/or attacks on the smart grid infrastructure with the aim of manipulating it, and particularly of disrupting the operation of energy supply networks.
- Attacks on central systems for services (fleet management, vehicle maintenance etc.).
- Attacks on distributed systems in the charging infrastructure, for instance with intent to manipulate or gain unauthorized access to billing data.
- Attacks on terminal devices in vehicles, for instance to manipulate billing data or possibly to gain unauthorized access to vehicle movement data.
- Attacks on other underlying vehicle systems (control units, driver assistance systems, communications systems, value-added services) possibly via the vehicles' internal communication networks.
- Other violations of data protection laws not mentioned above.

Luckily, there are already many internationally accepted and widely applied standards concerning information security which can also be used to ensure data security, data privacy and protection in the electromobility environment. In this context, particular reference is made to the following standards:

- The ISO/IEC 27000 family of standards
  The basic standard ISO/IEC 27001 describes an information security management system which is generally suitable for the appropriate handling of information security issues and for the implementation of suitable measures. Application of this standard is therefore recommended for all relevant sectors and operators of information technology systems related to electromobility. Furthermore, the recommendations made in ISO/IEC 27001 for the implementation of the ISO/IEC 27001 controls can be applied directly to trading platforms and commercial systems and their associated communication networks and interfaces. We do not consider that any further standardization is necessary in these areas.
- Protecting communications with grid control systems
  Some mechanisms for protecting communications between grid control networks are already provided in the communication protocols used (especially in IEC 61850) or are additionally defined in supplementary standards (e.g. IEC 62351). Some of the many activities currently being undertaken to further develop existing energy supply networks into "smart grids" are the efforts being made to apply and amend these standards. We do not consider that any further standardization is necessary from the security aspect.

- The ISO 15118 series specifies a communication protocol for automatic load management and automatic payment procedures in the vehicles. Basically, these standards describe the communication between the vehicle and the charging infrastructure (grid) as they negotiate charging profiles and a dynamic charging process. Services for safe billing, value-added serves and key provisioning are also defined. From the very start, IT security was incorporated into this standard in the form of known technologies for protecting exchanged data: Thus, the standard includes protocols such as TLS for the communication layer, or XML security measures for the application layer. Primarily requirements for the following areas have an impact on the infrastructure (secondary actors):
  - key formats (data formats, algorithms)
  - key provisioning (generation of key material and revocation information)
  - signed charge data records

Important components of the charging infrastructure other than the vehicle and charging station ("primary actors") are called "secondary actors" (e.g. customer, charging station operator, clearing houses, electricity providers, vehicle-to-grid public key infrastructure (PKI), etc.) and are covered in ISO 15118.

4.5.2 Need for action

To supplement the existing standards listed above, we consider that additional standardization activities are needed in the following areas specifically for the electromobility sector:

- Protection of communications interfaces specifically used in electromobility: The communications interfaces defined as part of electromobility standardization activities should have inherent security features and mechanisms. These include methods for the reliable authentication of communication partners, ensuring the confidentiality and integrity of exchanged data, and ensuring the traceability of transactions. The relevant interfaces include, for example, communication interfaces between vehicle and charging station (IEC 61851-23/24), and vehicle-to-supply grid interfaces (ISO 15118). It should be discussed whether separate standards are needed for such protection or whether the protection mechanisms can be dealt with directly in current standards. Since cryptographic methods are normally used for protecting communication interfaces and these require the provision of key material for all communications partners, it must also be examined whether additional standards are required for providing and distributing key material to all participants.
- ISO 15118 does not cover the protection of communications between the charging station and the back end or grid. DKE body STD 1911.11.5 on IT security for electromobility intends to fill this gap. Their focus is not only on IT security for grid integration into electromobility, but also the standardization of various role definitions in this area. A common, standardization understanding of roles is necessary for defining the relevant relationships in communications and to draw up the necessary protection measures. In Germany, STD 1911.11.5 functions as a central contact partner for IT security in the charging infrastructure, including sector-specific and cross-sectoral standardization needs.

- To ensure the safe connection of charging stations to the smart grid (back end), there are several existing and planned standards projects relating to ISO 15118, IEC 61850 and IEC 62351, as well as the work of the German Federal Office for Information Security, BSI, on protection profiles and its Technical Guideline TR 3109 for smart metering systems. The definition of "protection profiles" according to "common criteria" (as specified in the ISO/IEC 15408 series) has proven to be a good method of defining the security features of devices. In particular, these permit a neutral verification and certification of systems made by different manufacturers.

4.6 Smart Home

The concept of a "smart home" includes all privately used living and working spaces (rented or owned, in apartment buildings or houses, old or new). It thus also covers dwellings in large buildings wherever private use is involved and occupants have a need for safety, comfort and energy efficiency. One major difference between the commercially used "smart building" and the "smart home" is that with the former, the focus is on the building itself, whereas with the latter the needs of the private individual take precedence. Nevertheless, signalling mechanisms should be the same in both cases. Volume 1 in a series on home networking published by the German association BITKOM (Glasberg & Feldner, 2008) gives the following definition:

The terms "connected home", "electronic house", "intelligent living", "smart home", "smart house" etc. all refer to a number of approaches to new ways of living and working in private dwellings. One thing these terms all have in common is that they cover the need to provide occupants with systems that help meet their individual needs for comfort, safety and energy efficiency.

A "smart home" is thus more than just a conglomeration of individual intelligent devices:

1. Numerous sensors and smart devices help provide intuitive controls to meet the needs of occupants.
2. The information gathered is processed taking both current and anticipated conditions into consideration.
3. Action is then taken in response to this information and its interpretation. This is done by means of a sophisticated connected home network that makes possible the simple and safe interaction of devices in many areas (consumer electronics, ICT, household appliances (stove, refrigerator, etc.), building services such as alarm systems, heating and lighting controls, etc.) via interfaces, software etc. using wired and wireless technologies.

In the past, the subject of security in the smart home was often neglected, although it has recently received more attention due to an increasing networking of devices, etc. Today, the secure collection, storage, processing and transmission of data and information has become an essential prerequisite for a modern, sustainable and heavily networked smart home system - especially in terms of market acceptance. In standardization, functional and other requirements from areas such as security, comfort, automation, HVAC, energy management and AAL are brought together by the relevant standards bodies working in close cooperation. Requirements on all levels of a smart home system need to be taken into consideration, from the individual sensor to the cloud management system.

Standardization is presented with a special challenge in that diverse technologies and individual solutions need to be brought together to create an overall solution that is as interoperable and

secure as possible. Such a solution must apply to a wide range of use cases from the point of view of the consumer, manufacturer and service provider. Interoperability among the various technologies in a smart home should be provided by middleware/gateway technology. In terms of IT security, the WAN interface of such gateways is of special importance, because it must provide a safe way for local devices to communicate via the WAN. Existing standards (e.g. from the smart grid sector such as IEC 62351, IEC 27002, IEC 27019 and the results of the CEN-CENELEC-ETSI "Smart grid Information Security" working group, SGIS) need to be given consideration. German and European data protection laws also need to be given particular consideration, because the data involved can be sensitive information such as that on personal presence in the home, diagnostics or TV viewing habits.

The aim is to develop group- and application-specific security requirements and standards for all aspects of the smart home, in order to effectively address threats associated with an increasingly networked and interoperable application environment.

Requirements for selected security mechanisms for communications inside and outside the smart home focus on the main objectives of IT security: confidentiality, integrity and availability, whereby a differentiation is to be made in the different use cases: For example, in the case of personal data, confidentiality takes precedence, while integrity and availability are more important for safety-relevant data.

4.6.1 Communications security

One aspect of IT security in the smart home is communications security, i.e. requirements for all measures and systems involved in the transmission of data between two devices. This can relate to the encryption of the data transmission path as well as the reliability of the transmission itself. There are a number of standards and specifications on the encryption of transmission paths for different kinds of communication: In key management of wired systems it is essential that keys can be changed if the key is lost or discovered so that the communication system can be returned to a secure state.

The reliability of communications must cover the following aspects:

- susceptibility of the communication to interference by wanted participants
- susceptibility of the communication to interference by unwanted participants
- means of transmitting information when the transmission path is disrupted
- means of identifying and reporting a break in communications or loss of connection (in radio communications, a connection is made only for direct transmission and is then disconnected when the transmission is completed. In this case suitable measures such as heartbeats or lifechecks are needed to regularly check availability).

Depending on the security level and application, certain measures need to be taken and dealt with in smart home standardization.

Existing standardization results, particularly from the areas of fire protection, break-in prevention, energy and automation, need to be taken into account and modified as needed.

4.6.2 Communications across technologies

As mentioned above, one of the major objectives of standardization is ensuring interoperability, which is decisive for the success of smart home technology. In order to break down the technological barriers of individual solutions, a secure "bridge" in the form of middleware and gateways is needed to ensure secure transmission between different technological domains. In terms of security, the various communications technologies need to be qualified for certain security levels. Standardization must take careful consideration of the bridge between WAN and LAN in order to protect local networks from attacks via the WAN interface. For example, the connections to cloud and other services, and remote access to home services via the internet are use cases in which the WAN interface needs a high level of protection. In addition, end-to-end security plays a major role in remote access via devices such as a smartphone.

4.6.3 Protection profile for a smart meter gateway

[Source: BSI (German Federal Office for Information Security)]

The increasing decentralized supply of renewable energies presents a major challenge for future energy supply systems. For one thing, the supply of renewable energy leads to unpredictable time schedules; for another, at certain times of the day energy consumption can reach very high peak loads.

The European Union sees the smart grid as a good solution for making a flexible yet safe energy supply possible. Such smart grids also involve smart metering systems on the consumer side. The use of such systems gives consumers greater transparency regarding their own energy consumption, and makes it possible to lower energy costs.

But there is also a great need for data protection and data security, because personal data is processed and consolidated in measuring systems, and there are possible adverse effects on the security of the energy supply. Hacker attacks on smart metering systems, such as those in the US, and new threats such as the computer worm "Stuxnet" illustrate the urgent need for safe solutions for introducing smart metering systems in Germany.

In implementing its energy policy, the German Federal Government will gradually introduce the "smart" connection of energy consumers and generators to the grid. The goal is to increase the percentage of green energy to at least 35 percent by 2020, and to at least 80 percent by 2050.

In the face of possible threats, the government sees a great need for legally binding requirements on the security architecture of smart grids, to ensure that data protection and data security are ensured from the very start. This is why, in September 2010, the German Federal Ministry for Economic Affairs and Energy (BMWi) mandated the German Federal Office for Information Security (BSI) with the development of a protection profile and a series of technical guidelines (the TR-03109 series) on communication units for a smart meter gateway. The aim is to create a uniform technical security standard for all market participants. Both the German Energiewirtschaftsgesetz - EnWG (German Energy Law) and the "energy package" adopted by the German Bundestag in June 2011 call for such a protection profile and such technical guidelines. Since the start of 2011, the Federal Office for Information Security has been working closely with the Federal Commissioner for Data Protection and Freedom of Information, the German national metrology institute (PTB), and the Federal Network Agency on a draft protection profile for a smart meter gateway communication unit. Technical associations from the telecommunications, energy, IT, housing and consumer protection

sectors have taken part in the development process. In terms of standardization, several DKE bodies have been established to work on the technical guidelines, and to harmonize work on requirements regarding metrological aspects of energy management in the smart home with work at international level. This important national work is well under way. There is also a move towards using the smart meter gateway as an anchor for developing value-added services (e.g. AAL) from the smart home domain.

The DKE body AK 716.0.1 "Informationssicherheit im Smart Home und Building" is also working together with other DKE bodies, such as K952, K461, K261 and the FNN, to draw up recommendations for integrating the smart meter gateway into smart homes. Because the smart home area is incongruous with the smart meter gateway, any interfaces between a gateway and a smart home must be secured, as must the WAN/gateway interface; the communications interface must also be restricted to non-critical use cases. DKE AK 716.0.1 has already defined an isolation module that ensures a secure isolation between the system operator and the smart home at the HAN-CLS interface.

4.6.4 Security architecture with privacy zones

A large amount of data that is processed and stored in relation with the smart home is personal in nature. Thus, a smart home data protection concept is absolutely necessary in order to make sure information on occupant behaviour is not revealed. The "privacy by design" principle, and thus confidentiality, must be a major objective of any design. This is not only essential for user acceptance, it is also legally required.

To reduce the complexity of any security design, it is recommended that the security architecture be divided up into data protection zones. For private living quarters, especially those in non-residential buildings and rented dwellings, the responsibility for operating such systems does not always lie with the user. Thus, a differentiation is to be made between the user and responsible parties (e.g. for data protection).

Data protection zones include:

- Rooms
- Dwellings
- Buildings (residential, non-residential ....)
- Business areas which require protection for cloud services (e.g. the storage and processing of personal data).
- Application software modules within a device

Communications between data protection zones must take place via secure channels. One operator takes responsibility for each protection zone, ensuring availability, data protection, etc. For dwellings this can be the owner, a third party or the occupant. Environmental conditions can be described for data protection zones that can then be used as assumptions during risks analysis.

DKE STD 1711.0.2 is working on a reference model architecture for homes and buildings that is along the lines of the European Smart grid Architecture Model (SGAM). In this architecture, existing reference models can be used for the home and building domains. The aim of DKE AK 716.0.1 is to

carry out a differentiated security analysis for the home and building domain that goes across all areas.

This analysis is being carried out at every layer (organization/policy, service/function, information, communication, log./phys., components).

This model should be flexible enough so that data protection in virtualized functions (cloud) can also be considered. To this end integration zones for data processing have been introduced:

- Environmental interactions zone (persons, sensors, actors)
- Near-field zone
- Local zone
- External/far-field zone
- Business zone
- Market zone

The "near-field zone" can be pre-processing near a sensor.

In the "local zone", data is still directly influenced or controlled by the data object (dwelling, building).

For example, for the data object there can be a need for anonymization / pseudonymization after data integration and when it leaves the integration zone.

4.6.5 Security considerations for the operation of smart home components

Since 2014, DKE AK 716.0.1 has been working on a code of practice that describes IT security needs when operating networked components in the smart home. This code is a kind of best current practice recommendation, which includes recommendations for action.

One particular aspect of the smart home is that the user and owner (and thus operator) are often identical, so that organizational measures are often only voluntarily carried out. However, there are also cases where third parties take over the responsibility for operations (e.g. planners, installers, sub-contractors, landlords).

5 Future fields of standardization

5.1 Ambient Assisted Living - AAL

The area of AAL is constantly under development, in which new perspectives, responsibilities and needs are identified and contribute to the general heterogeneous environment. Today AAL is a topic of much discussion, with numerous activities taking place at national, European and international level. AAL refers to the use of technological solutions to help persons of any age remain active in all environments, increasing the quality of life for all ages and situations. AAL applications are extremely diverse and cross-generational. This means that partners from several different areas - such as healthcare, technology, social services, gerontology and business - have to interact with one another. Not only must the human actors learn to understand and respect each other, the different technical systems and components must also adjust to and be interoperable with one another. There are thus already a large number of specifications for individual systems that can be used.

But the existing specifications do not sufficiently address the special needs of AAL systems and products. First, it is necessary to identify those existing specifications that are actually relevant to AAL systems. Next, it is important to fill any gaps, especially as regards the integration and interoperability of individual systems, and regarding the training and qualification of specialists.

An infrastructure is needed for the AAL environment that in many areas will overlap with the smart home infrastructure. G. Demiris et al. describes smart homes as "residences equipped with technology that enhances the safety of patients at home and monitors their health conditions" (G.Demiris et al., "Older adults' attitudes towards and perceptions of 'smart home' technologies: A pilot study", Medical Informatics 29 (2004), p. 88), clearly illustrating the connection between AAL and the smart home. Thus, close cooperation between actors in the two domains is necessary. Suitable public relations work can also bring synergies. In smart home technologies, sensors and actors are used to reach a high level of energy efficiency, security, comfort and a high quality of life. Technologies can be modified and retrofitted to achieve a sustainably high level of energy efficiency, security and comfort. Several technological concepts can be networked for greater effect.

An example of joining assistive technology with smart home applications is adding sensors to entertainment applications (e.g. for gesture control) allowing those who are restricted in movement to control their devices and home environment.

"Assistive technology" is basically technology that makes it easier for users to perform tasks and movements which they otherwise would not be able to perform, or could do so only with difficulty. Sensors installed in the home can record activities and request any necessary support.

One typical aspect of AAL is that the applications are not limited to the domestic environment, but can involve external areas, for example when the person leaves their home. AAL methods increase independence, security and thus the quality of life. Although one major focus of AAL is on the elderly due to current demographic developments, all generations can benefit from AAL. For example, IT-supported systems can help families care for their small children .

AAL technology thus not only helps meet the challenges of an ageing population, but also fulfils increasing demands for great comfort and security. Because the AAL user group is so heterogeneous, there are a number of different functional and non-functional user requirements that need to be considered from the very start. In Germany, the relevant legal provisions are laid down primarily in data protection laws and the Medizinproduktegesetz (Act on Medical Devices). AAL functions can be easily integrated into existing smart home environments, and adjusted to meet changing needs. It is expected that smart home technologies and AAL applications will soon gain more attention on the market. Innovations in these areas must thus be now seen as bringing competitive advantages for SMEs.

5.1.1 Privacy and AAL

AAL technologies and services involve the processing of sensitive data, such as vital parameters, social contacts, domestic activities and healthcare information. As such, legal requirements relating to personal data protection, informational self-determination, and the Medical Devices Act also apply to the AAL sector. In some cases, laws already exist, such as those regarding patient-related data processing: e.g. the European Data Protection Directive, 95/46/EC, and the German data protection laws implementing the directive at Federal and State level. Other relevant German laws include the Criminal Code, Social Security Code and the Basic Law. Principles of data avoidance and data

minimization should be followed in AAL as well. It should also be possible to choose between centralized and decentralized data storage.

The difference between data protection and data security should also be made clear. Clear data security concepts must be laid down as early as the design phase. Furthermore, data protection should be integrated into all processes by the manufacturer and service provider.

Further work in this area is being carried out by the Unabhängiges Landeszentrum für Datenschutz in Schleswig-Holstein (ULD). They have drawn up a preliminary study on legal issues in AAL. Here, abstract models are used to identify current legal relationships, analyse data flows and processing methods, and evaluate legal ramifications. The extent to which the German Medical Devices Act applies to AAL systems and products still needs to be discussed.

In addition, international data protection specifications are being drawn up in various ISO working groups.

Because AAL needs a high level of security to be successful, it is essential that security issues be addressed as early as the design stage, and a security architecture is needed for the AAL environment.

5.1.2 Current standardization landscape for AAL IT security

In 2014, the working bodies in DKE dealing with AAL were integrated into the body Fachbereich 8 for medical technology, electroacoustics, ultrasound and lasers. In Germany there are currently 11 groups working on AAL standardization. Figure 1 gives an overview of the DKE bodies currently working on AAL.

The DKE "excellence cluster" on AAL supports technological developments, guides and coordinates various AAL standardization activities within DKE, DIN and other groups, and promotes a continual exchange of information between specialists and the working groups.

Figure 10: DKE bodies currently working on AAL

The DKE working group "Sicherheit und Datenschutz im Kontext von AAL" deals with data protection and security in the AAL context.

Their aim is to ensure that IT security is considered from the very start in AAL system architectures (security by design).

The particularities of private life, as well as any future storage and processing of sensitive data in the cloud need to be taken into account.

This architecture should also serve to identify any gaps in standardization that can be filled by work within DIN and DKE.

Another aspect being dealt with is the work of the Federal Office for Information Security (BSI) in smart metering. In September 2010, the German Federal Ministry for Economic Affairs and Energy (BMWi) mandated the German Federal Office for Information Security (BSI) with the development of a protection profile and a series of technical guidelines (the TR-03109 series) on the communication unit for a smart meter gateway. The aim is to create a uniform technical security standard for all market participants. Developed on the basis of a threat analysis, the protection profile specifies the essential minimum requirements for a secure operation that ensures data privacy. The smart meter gateway should serve as an anchor for developing AAL, a value-added service, from the smart home domain. The requirements laid down by the Federal Office for Information Security (BSI) regarding HAN (home area network) and WAN (wide area network) interfaces will be taken into consideration, and the results documented in the form of standards and specifications.

The next step for the DKE working group will be to gather use cases and user stories in AAL, to consolidate them, and then to identify roles, actors and assets on the basis of the gathered information. A "user story" is a written text that is later used to draw up use cases. A standard use case template as in IEC 62559-2 is used for this to ensure interoperability with the smart home domain. The work will continue as follows: After assets have been derived from the use cases, a threat analysis will be carried out and security targets defined, which will be used as a basis for security functions (e.g. authentication); this will be followed by a risk analysis. The results of this process will be described in a normative technical specification (VDE code of practice).

At international level, various ISO/IEC working groups (such as JTC1/SC27/WG5) are developing international data protection specifications that are also important for AAL (see also Chapter 4.1):

- ISO/IEC 29100, "Information technology—Security techniques—Privacy framework", defines data protection requirements for processing personal data in IT systems all over the world.
- ISO/IEC 29101: "Information technology—Security techniques—Privacy architecture framework" gives best practices for technically implementing data protection principles
- ISO/IEC 24760-1 "Information technology—Security techniques—A framework for identity management—Part 1: Terminology and concepts" defines the framework for a secure, reliable identity management.

5.2 Smart cities

Global urbanization and the corresponding depopulation of rural areas present new challenges for the development of structures, resources, products and services in settled areas in Germany and throughout the world. New integrative IT solutions which are being used in all areas of life have led to the coining of the term "smart city", which refers to intelligent (mostly IT) technologies that are helping to improve processes in urban life. Today, the concept of a "smart" city also includes non-technical aspects such as civic engagement, sustainability, and the use of public spaces.

Nevertheless, IT plays a key role in smart city developments. Due to developments in ICT and greater integrability, and through the networking of single solutions, new intelligent solutions are now possible in a number of areas. This has led to new integrated technology, services and process solutions with a great need for interface management.

To address this need, DIN and DKE have set up a special organizational structure for dealing with standardization in urban development.

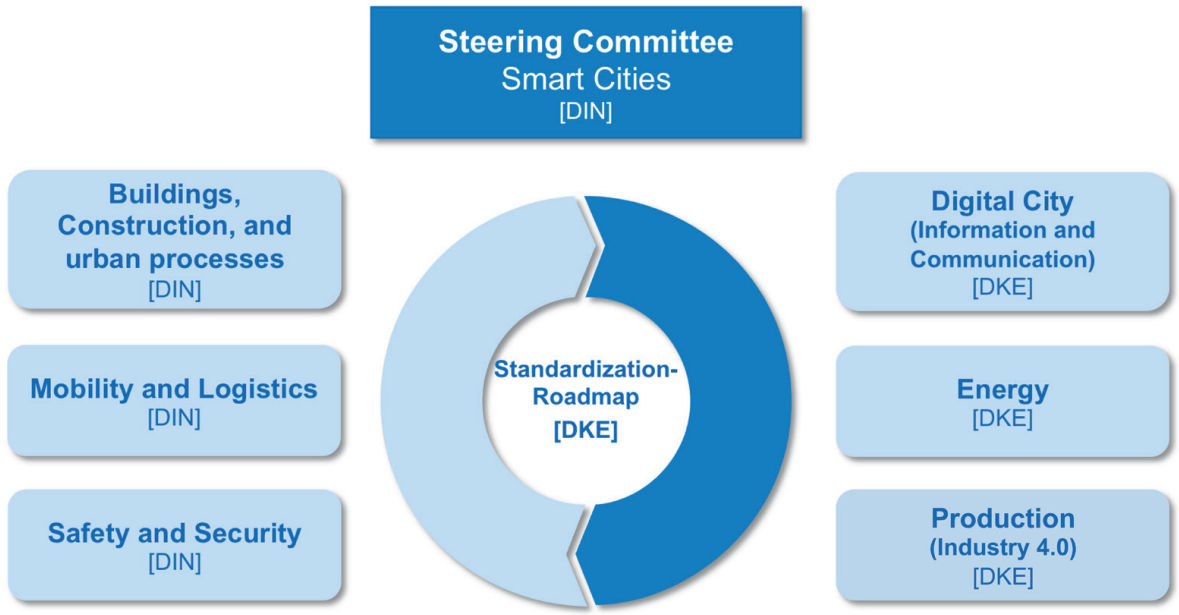

Figure 12: Organization of smart city standardization in DIN and DKE

In 2014, the DIN/DKE steering body on smart cities published a definition for the term "smart "city:

"A 'smart city' is a settled area which utilizes systemic (in terms of ecological, social and economic aspects) and sustainable products, services, technologies, processes and infrastructures, in most cases supported by highly integrated and networked information and communications technologies."

The intention is to help society as a whole take advantage of the opportunities these changes are bringing, while at the same time developing mechanisms to protect society and the individual. One particular area of focus is data security.

Although it is unavoidable that information will be passed on to ensure functionality, individual privacy still needs to be protected. This requires systems that simultaneously ensure a high level of privacy, security and safety, a low level of vulnerability, and the ability of a society to respond to threats, survive catastrophes, etc. (resilience). Standards work must thus deal with fundamental security and safety mechanisms.

In order to take advantage of new functions, services and business models, it is necessary to develop new standardized, automatic communication processes for the essential interfaces between systems and infrastructures of a settled area. New, secure IT architectures need to be defined in order to deal with potential risks due to greater networking, such as violations of privacy, new forms of vulnerability of critical infrastructures, and new forms of cybercrime.

Until recently, standards bodies have dealt with subjects separately in the various responsible standards committees; however, this approach is not suitable for a cross-sectoral topic such as the smart city. Here, there are no individual products or product groups, but complex systems with numerous interfaces. DIN/DKE is aware of this situation, and in response have set up the joint working bodies mentioned above. The joint body on safety and security, especially, is addressing not only the resilience of cities, but also the security of communications and data.

The boundaries between the various technological areas are becoming increasingly blurred and can no longer be represented in a "silo" structure. For example, discussions regarding mobility in the smart city must not only include architects, traffic planners, and urban planners, but also manufacturers of telematics systems and vehicles, as well as public transport operators. Until now, these areas were largely considered on an isolated, individual basis. But a system-oriented approach is necessary in order to effectively deal with highly complex subjects with a growing number of interfaces - even in the area of standardization.

DIN and DKE are working towards bringing such a systematic approach to activities at national as well as international (in ISO/IEC) level. For more information on smart cities standardization, go to the DIN website at

6 European activities in the area of cybersecurity standardization

In 2011 the Cyber Security Coordination Group (CSCG) was created to provide strategic advice under the lead-management of CEN, CENELEC and ETSI. The main task of the CSCG is to bundle existing European standardization expertise in this field and to coordinate the relevant recommendations, taking international developments into consideration to encourage exchanges of information with bodies outside Europe. On 2 April 2014, a delegation of the CSCG handed over a White Paper with nine recommendations on digital security to the EU Commissioner for the Digital Agenda, Neelie Kroes. The following recommendations were made:

1. The European Commission (EC) should mandate the CSCG to create a governance framework for the coordination of Cyber Security standardisation within Europe.
2. The EC should establish a clear and common understanding of the scope of Cyber Security, based on an initiative the CSCG plans to launch to clarify the key terms and definitions used in the standardisation of and communication related to Cyber Security within the European Union.
3. The EC should mandate CEN/CENELEC/ETSI to launch an initiative to re-establish the trust of the European citizen in the European digital environment, coordinated by the CSCG and aimed at

producing standards to create the most trustworthy environment in the world; this should include privacy and harmonised objectives for education and awareness.
4. The EC should mandate CEN/CENELEC/ETSI to establish an initiative to produce standardised mechanisms for a strong, interoperable, trustworthy and transparent European Public Key Infrastructure and strong cryptographic capabilities for all participants in the European Digital Single Market.
5. The EC should authorise the CSCG to coordinate the standardisation work for a high-level European Cyber Security Label for information and communication technologies (ICT) to protect the European consumer (objective 4 of the EU Cyber Security Strategy).
6. The EC should mandate CEN/CENELEC/ETSI, with the CSCG coordinating appropriate harmonisation with the European regulatory bodies, to extend existing European Cyber Security requirements and evaluation frameworks to ensure adequate Cyber Security throughout the full ICT value chain and to establish an initiative for risk-based standardisation.
7. The EC should authorise the CSCG to create a high-level interface between the CSCG and the European research community to ensure alignment between standardisation and research including industrial research.
8. The EC, with the support of the CSCG, should engage in an industrial forum to harmonise Cyber Security Standards with key international players and stakeholders according to European requirements.
9. The EC, with the support of the CSCG, should launch a targeted global initiative to promote standards appropriate to European requirements for the development of trustworthy ICT products and services as well as Cyber Security solutions.

The White Paper can be downloaded for free at the CEN/CENELEC website
.

These recommendations are fundamental in nature and aim at facilitating an effective, targeted and harmonized standardization in the cybersecurity field. They thus also relate to all national topics discussed in this roadmap. In 2015 the CSCG plans to draw up detailed plans and measures to implement these recommendations.
Another current development within Europe that impacts IT security standardization is the foundation of a new ETSI technical committee, "TC CYBER". The committee will develop ETSI specifications as well as EN Standards on cyber security. The activities of TC CYBER include the development of standards in the following areas:

- Cybersecurity
- Security of infrastructures, devices, services and protocols
- Security advice, guidance and operational security requirements to users, manufacturers and network and infrastructure operators
- Security tools and techniques to ensure security
- Creation of security specifications and alignment with work done in other ETSI committees

7 Critical infrastructures

The Federal Ministry of the Interior's proposed IT security act was adopted by the German Bundestag on 17 December 2014. The act took effect in July 2015. The act obliges "operators of critical infrastructures" to apply sector-specific IT security standards, and to some extent prove

compliance with these standards by means of certification. The Act addresses critical infrastructures in the following sectors:

- Food
- Energy
- Finance and insurance
- Health
- Information technology and telecommunication
- Media and culture
- Transport and traffic
- Water

The Act stipulates and/or allows the use of minimum standards and sector-specific security standards, referring to the state of the art. These standards are to be developed by industry itself and are not set down in the Act. Existing standards - as a rule, international standards - should be used to describe the state of the art. In some of the sectors mentioned above there are already structures and standards that can be used to implement the Act's provisions. A short overview of these is given below.

Food

At present there are no standards bodies for the food industry that deal explicitly with IT security. There are also no sector-specific IT security standards for the food industry. Because standard IT components are mainly used in the food trade, it is presumed that commonly used generic IT security standards will apply. In food production, automation technology solutions can be adopted. The extent to which there are IT security aspects particular to the food industry has not yet been widely discussed by stakeholders along the value added chain.

Energy

See Chapters 4.2 and A.2 regarding existing standards bodies and standards.

Finance and insurance

DIN's Standards Committee Information Technology and selected IT Applications (NIA) deals with the standardization of IT security aspects in banking and finance in its Working Committee NA 043-03-02 AA "Financial services". The committee also mirrors the international subcommittee ISO /TC 68/ SC 2 "Financial Services, security", which deals with this topic at international level.

Health

See Chapters 4.4 and A.4 regarding existing standards bodies and standards.

Information technology and telecommunication

There are a number of bodies and standards dealing with ICT. At national level, telecommunications standardization is carried out by the DKE, while fundamental IT standardization is carried out by DIN's Standards Committee Information Technology and selected IT Applications (NIA). In Germany the telecommunications sector is heavily regulated, for example by the German Telemedia Act. Also

important are the "IT security catalogue" issued by the Federal Network Agency, which only apples within the context of the Energiewirtschaftsgesetz - EnWG (German Energy Law).

Media and culture

Up to now, aspects of IT security particular to the cultural and media landscape have not been much discussed, although IT in this area has gone through some major changes. Information is exchanged via the "social media", news published on diverse platforms is disseminated to the public and contributes to the opinion-forming process. Manipulated or false information provided on compromised trustworthy sources presents a serious threat. A greater focus must be placed on securing IT-supported communications channels and preventing identity theft. A thorough analysis should be made regarding the use of existing standards, and it is recommended that sector-specific standards and specifications be developed by an appropriate standards body, which has yet to be founded.

Transport and traffic

This sector covers road, rail and air traffic, and traffic at sea. DIN's Standards Committees Road Vehicle Engineering, Railway, Aerospace, and Shipbuilding and Marine Technology are responsible for standards work in this area.

There is already an aerospace standard dealing with IT security: DIN EN 16495 Air Traffic Management - Information security for organisations supporting civil aviation operations.

The IT security of electric train signals have been dealt with in DIN EN 50159 and DIN VDE V 0831-102, but largely only in terms of safety-relevant electronic systems which use a transmission system for digital communication. The subject of "vandalism and unreasonable human behaviour" is excluded from the scope of DIN EN 50126, in both its current and draft editions. However, recent incidents have shown that the vulnerability of IT systems in electronic train signal systems to malicious attacks has possibly been underestimated. Although these attacks have not led to a full shutdown of these systems, it cannot be denied that there is great potential for damage due to such attacks, at least where preventative hazard control measures are not taken in time. For railway signalling systems, not only is longevity of prime importance, but the large area covered by such systems is also an important aspect. Current technological trends and new threat scenarios are making it all the more necessary to address IT security to a greater extent:

- commercially available systems - especially operating systems and transmission protocols - are increasingly being used in railway signalling systems,
- applications are increasingly networked, especially over open networks,
- over the past few years the number of attacks on IT systems has grown considerably, especially were tools for such attacks are readily available and there is a market for such activities,
- the privatization and opening of markets has led to a complex situation, particularly in terms of the number of people and/or organizations involved in business processes.

Unfortunately, general requirements for the IT security of electric signalling systems exist in only a few isolated cases. But without such general requirements there is a danger that unsuitable requirements that only apply in single cases will be specified. Such unsuitable requirements can be so

strict that they threaten the economic efficiency of railroad operations, or can impair such operations considerably. Another external motivation for drawing up standards on this subject is the fact that the railway system is a "critical infrastructure" and as such, there has been a call for application-specific IT security technical rules on the part of bodies such as the German Federal Government and the European Commission. The question is, therefore, whether a body of technical rules should be drawn up specifically for the IT security of electrical train signalling systems, or whether existing technical rules should be used. Studies have shown that standards from the industrial automation sector, such as the IEC 62443 series, cover the same subjects to a high degree. Therefore, there should be no individual attempts to draw up technical rules on IT security in signalling systems, but instead, the approaches being set down in IEC 62443 should be integrated in existing rules such as DIN EN 50129 or EU VO 402/2013. This is done in DIN VDE V 0831-104 "Electric signalling systems for railways - Part 104: IT Security Guideline based on IEC 62443", for example.

Water

The water supply infrastructure is very similar to that for energy supply. In 2008 the German Association of Energy and Water Industries (BDEW) has published a white paper which is based on ISO/IEC TR 27019. The extent to which ISO/IEC TR 27019 can also be applied to the water industry should thus be examined.

8 Summary

This overview of standardization activities in various areas of IT security shows that a number of standards and specifications are under development. These areas are well covered in terms of standards work. However, a closer look at these documents also shows that the number of common standards used in many different sectors remains relatively small, although the subject matter - the transmission of information - is the same in all sectors. This is partly due to the special requirements for this area, especially at organizational level, but it could also be an indicator for the unclear or insufficient separation of generic and sector-specific aspects in standardization. The heterogeneity of the standardization landscape makes an evaluation regarding IT security difficult. However, different system architectures in different areas can also enhance security, because the likelihood that a system weakness would pose a threat for several areas at once is thus minimized. These two opposing effects need to be looked at more closely if conclusions regarding future IT security standardization are to be made. The IT Security Coordination Office (KITS) is continuing and encouraging discussions on this matter.

A further need for action is the integration of IT security in new areas of standardization from the very start. It should be ensured that new areas profit from experience gained and work already carried out in IT security standardization, and that new security solutions are compatible with existing solutions, at least for economic reasons. KITS will therefore continue to make efforts to bring representatives from different areas together.

Annex A Overview of existing standards

A.1. Data protection

Frameworks and architectures

- A Framework for Identity Management (ISO/IEC 24760, IS, CD, WD)
- Privacy Framework (ISO/IEC 29100, IS)
- Privacy Architecture Framework (ISO/IEC 29101, FDIS)
- Entity Authentication Assurance Framework (ISO/IEC 29115, IS)
- A Framework for Access Management (ISO/IEC 29146, CD)
- Telebiometric authentication framework using biometric hardware security module (ITU-T X.1085 | ISO/IEC 17922, WD) (formerly X.bhsm)

Protection concepts

- Biometric information protection (ISO/IEC 24745, IS)
- Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191, IS)

Guidelines for content and evaluation

- Authentication Context for Biometrics (ISO/IEC 24761, IS)
- Privacy Capability Assessment Model (ISO/IEC 29190, CD)
- Code of practice for data protection controls for public cloud computing services (ISO/IEC 27018, CD) -> Code of practice for PII protection in public clouds acting as PII processors
- Identity Proofing (ISO/IEC 29003, WD)
- Privacy impact assessment – Methodology (ISO/IEC 29134, WD)
- Code of practice for the protection of personally identifiable information (ISO/IEC 29151, WD)

The interrelation between relevant projects and standards in the privacy area (mostly from ISO-IEC/ITC1/SC 27/WG 5) is shown in Figure A1.

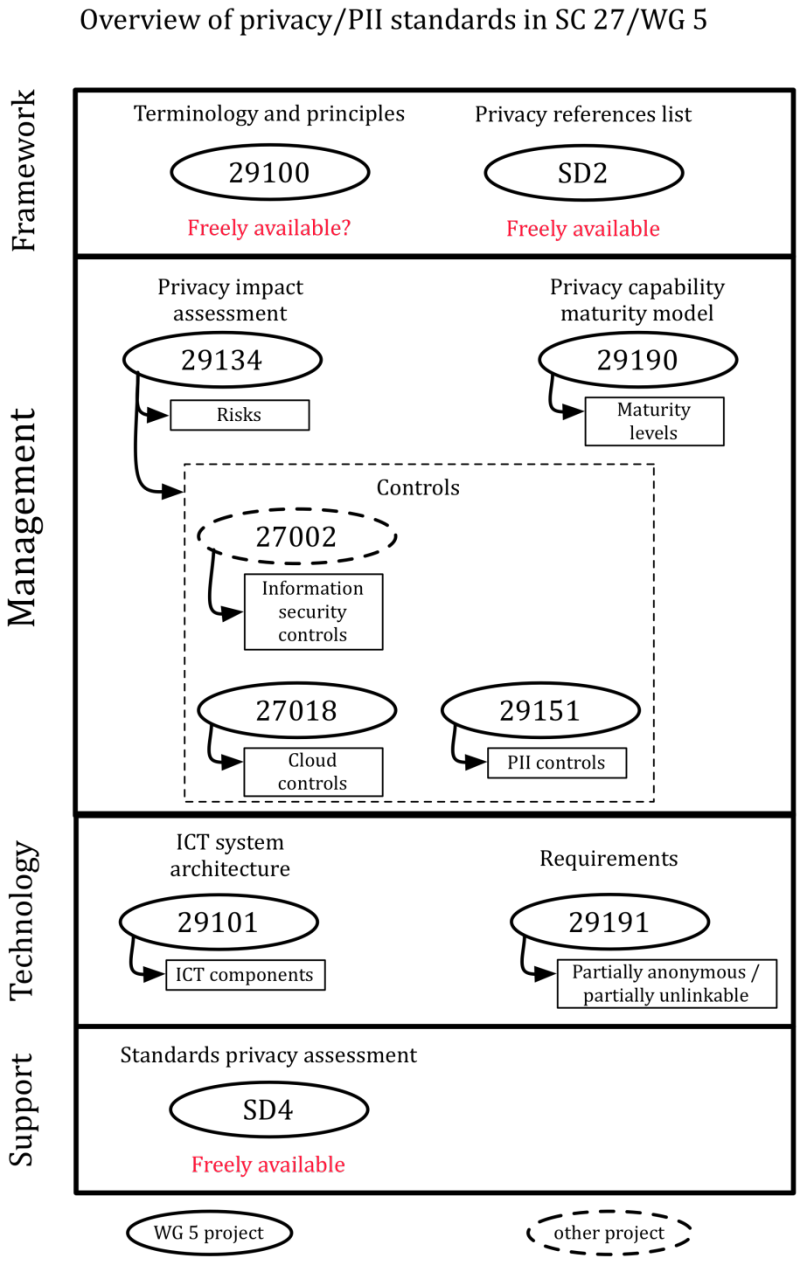

Figure A1: The interrelation between relevant projects and standards in the privacy area (mostly from ISO-IEC/ITC1/SC 27/WG 5) [Source: Roadmap ISO/IEC JTC 1/SC 27/WG 5 "Identity Management and Privacy Technologies"]

A.2. Electrical energy supply

List of select cyber security standards, specifications and guidelines with Smart Grid relevance:

Advanced Security Acceleration Project – Smart Grid (ASAP-SG):

- Development of security requirements for the Smart Grid at the system level (e.g. for Smart Metering, distribution automation) in the form of security profiles:
- Third Party Data Access
- Advanced Metering Infrastructure (AMI)

- Third Party Data Access Distribution Management
- Wide-Area Monitoring, Protection, and Control (WAMPAC)
- Substation Automation (under development)

International council on Large Electric Systems, CIGRE B5/D2.46:

- Implementation and management of cyber security measures for protection and control systems

Department of Homeland Security (DHS):

- Catalog of Control Systems Security
- Cyber Security Procurement Language for Control Systems

Department of Energy (DOE) / Department of Homeland Security (DHS):

- Electric Sector Cyber Security Risk Management Maturity Initiative

Department of Energy (DOE) / National Institute of Standards and Technologie (NIST) / North American Electric Reliability Corporation (NERC):

- Electricity Subsector Cyber Security Risk Management Process Guideline[1]

CEN / CENELEC:

- EN 62056-5-3: describes the COSEM application layer, including security

European Telecommunications Standards Institute (ETSI):

- ETSI TCRTR 029, Security Techniques Advisory Group (STAG); A directory of security features in ETSI standards
- ETSI ETR 332, Security Requirements Capture
- ETSI ES 202 382, ETSI ES 202 383, Security Design Guide; Method and proforma for defining Protection Profiles
- ETSI EG 202 387, Security Design Guide; Method for application of Common Criteria to ETSI deliverables
- ETSI TS 102 165-1, Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis
- ETSI TS 102 165-2, Protocol Framework Definition; Methods and Protocols for Security; Part 2: Counter Measures
- ETSI EG 202 549, Design Guide; Application of security countermeasures to service capabilities
- ETSI TR 185 008, Analysis of security mechanisms for customer networks connected to TISPAN NGN R2
- ETSI TR 187 012, Report and recommendations on compliance to the data retention directive for NGN-R2
- ETSI TS 187 016, NGN Security; Identity Protection (Protection Profile)
- ETSI TR 102 419, Security analysis of IPv6 application in telecommunications Standards
- ETSI TS 101 456, ETSI TR 102 437, ETSI TS 102 042, ETSI TR 102 572, ETSI TS 102 573, Electronic signatures
- ETSI TS 102 689, M2M service requirements
- ETSI TS 102 690, M2M-Functional architecture
- ETSI TS 102 921, M2M-mIa, dIa and mId interfaces

[1] risk-management-process-guideline

- ETSI TR 103 167, Threat analysis and counter-measures to M2M service layer
- ETSI TS 100 920, Communication, information for mobile (3GPP, GSM, CDMA …) telecommunication infrastructures
- ETSI TS 133 203, Access security for IP-based services (3GPP TS 33.203 version 8.8.0 Release 8)
- ETSI TS 133 210, Network Domain Security (NDS); IP network layer security (3GPP TS 33.210, version 5.2.0 Release 5)
- ETSI TS 133 234, Wireless Local Area Network (WLAN) interworking security (3GPP TS 33.234 version 6.4.0 Release 6)
- ETSI TS 133 310, Network Domain Security (NDS); Authentication Framework AF) (3GPP TS 33.310 version 10.5.0 Release 10)
- ETSI TS 102 225, Communication, information for mobile (3GPP, GSM, CDMA …) telecommunication infrastructures. Secure packet protocol for remote administration of security element
- ETSI TS 102 226, Communication, information for mobile (3GPP, GSM, CDMA …) telecommunication infrastructures. Remote administration of Security element
- ETSI TS 102 484, Communication, information for mobile (3GPP, GSM, CDMA …) telecommunication infrastructures. Local Secure Channel to security element
- ETSI TS 187 001, Communication, information for fixed (IP based …) telecommunication infrastructures. Security Requirements
- ETSI TS 187 003, Communication, information for fixed (IP based …) telecommunication infrastructures. Threat Analysis
- ETSI TR 187 002, Communication, information for fixed (IP based …) telecommunication infrastructures. Security Architecture
- W3C XML Digital Signature, Provide security features for XML encoded data
- W3C XML Encryption, Provide security featuresz for XML encoded data

International Electrotechnical Commission (IEC)

- Standards series "IEC 62351 Parts 1-11 – Power systems management and associated information exchange – Data and communications security (see below for details)
- Standards series "IEC 62443 – Industrial communication networks – Network and system security"
  (see below for details)
- IEEE 1686-2007 – IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities”
- IEEE 802.11i Wireless security
- IEEE 802.1X Port based network access control
- IEEE 802.1AE MAC security
- IEEE 802.1AR Secure Device Identity

The Internet Engineering Task Force (IETF):

- IETF Cyber Security RFCs:
- RFC 2617 HTTP Authentication: Basic and Digest Access Authentication
- RFC 2759 EAP MS-CHAP2
- RFC 2865 RADIUS (Remote Authentication Dial In User Service)
- RFC 3711 Secure Real-time Transport Protocol (SRTP)
- RFC 3748 EAP Base Protocol (includes EAP MD5)
- RFC 4101, RFC 4102, RFC 4103 Base standards for IP Security (IPSec)
- RFC 4301, RFC 4302, RFC 4303 IPSec
- RFC 4764 EAP PSK (Pre-Shared Key)

- RFC 4962 Authentication, Authorization, and Accounting (AAA)
- RFC 5054 Using the Secure Remote Password (SRP) Protocol for TLS Authentication
- RFC 5106 EAP IKEv2
- RFC 5216 EAP TLS
- RFC 5246 Transport Layer Security (TLS)
- RFC 5247 Extensible Authentication Protocol (EAP) Framework, Key Management Framework
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Basis specification for the X.509 certificate and certificate processing
- RFC 5281 EAP TTLSv1.0
- RFC 5289 TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)
- RFC 5652 Cryptographic Message Syntax (CMS) is used by BSI for content data encryption in the Smart Meter Gateway (TR-03109 v1.0)
- RFC 5746 Transport Layer Security (TLS) Renegotiation Indication Extension
- RFC 6066 Transport Layer Security (TLS) Extensions
- RFC 6090 Fundamental Elliptic Curve Cryptography Algorithms
- RFC 5746 Transport Layer Security (TLS) Renegotiation Indication Extension
- RFC 6272 Internet Protocols for the Smart Grid (identifies RFCs that can be used in the Smart Grid)
- RFC 6347 Datagram Transport Layer Security (DTLS), alternative to TLS in UDP based networks
- RFC 6407 Group Domain of Interpretation (GDOI), is used, for example, to implement the Key Management Framework found in IEC 61850-90-5
- RFC 6749 The OAuth 2.0 Authorization Framework
- RFC 7027 Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS)
- RFC 7250 Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)

International Society of Automation (ISA):

- ISA 99 Standards Framework

International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC):

- ISO/IEC 27000 series (see below for details)

North American Electric Reliability Corporation (NERC), Critical Infrastructure Protection (CIP) Program:

- NERC-CIP Standards 002 to 011

National Institute of Standards and Technologie (NIST):

- FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION (FIPS) 140-2: Security Requirements for Cryptographic Modules
- Special Publication (SP) 500-267 Security profile for IPv6
- Special Publication (SP) 500-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths”
- NIST SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations (rev 4 as draft)
- NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security

- NIST Special Publication 1108: NIST Framework and Roadmap for Smart Grid Interoperability Standards
- NIST Special Publication 800-39: Managing Information Security Risk: Organization, Mission and Information System View
- NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems
- NISTIR 7628 US-Guidelines for Smart Grid Cyber Security
- NISTIR 7823: Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework (Draft)

A.3. Industrial production

Selection of IT security standards, specifications and directives with Industry 4.0 relevance:

- IEC 62443 – Industrial communication networks – Network and system security
- ISO/IEC 27000 series Information technology – Security techniques – Information security management systems (ISMS)
- IEC standards series IEC 62541 Part 1-10, in particular:
  IEC/TR 62541-2 OPC Unified Architecture - Part 2: Security Model
- OPC UA (OLE for Process Control – Unified Architecture
  (OPC UA was also published as IEC standards series IEC 62541)
- ISA99: ISA 99 series Manufacturing and Control Systems Security
- NERC CIP: Cyber Security Standards Critial Infrastructure Protection
- NIST SP 800-82 Guide to Industrial Control Systems Security
- NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations
- Department for Homeland Security
- VDI/VDE – Directive 2182 Information security in industrial automation
- NAMUR NA 115 IT Security for Industrial Automation Systems
- WIB - Process Control Domain-Security Requirements for Vendors
- CPNI Good Practice Guide – Process Control and SCADA Security
- CPNI Good Practice Guide – Firewall Deployment for SCADA and Process Control Networks
- BSI (Federal Office for Information Security) - ICS Security Compendium
- BSI (Federal Office for Information Security) - ICS Security Compendium - Testing recommendations and requirements for component manufacturers

A.4. Medical technology

ISO TC 215 “Health Informatics”, Working Group 4 “Security, Safety and Privacy”

Standards

- ISO/TS 14441:2013 Health informatics -- Security and privacy requirements of EHR systems for use in conformity assessment
- ISO/NP TS 14441-2 Health informatics - Security and privacy requirements for compliance testing of EHR systems -- Part 2: Protection profile for small scale patient health record Systems
- ISO/TS 14265:2011 Health Informatics - Classification of purposes for processing personal health information

- ISO 17090-1:2013 Health informatics -- Public key infrastructure -- Part 1: Overview of digital certificate services
- ISO 17090-2:2008 Health informatics -- Public key infrastructure -- Part 2: Certificate profile
- ISO 17090-3:2008 Health informatics -- Public key infrastructure -- Part 3: Policy management of certification authority
- ISO 21091:2013 Health informatics -- Directory services for healthcare providers, subjects of care and other entities
- ISO/TS 21298:2008 Health informatics -- Functional and structural roles (DIS ballot underway)
- ISO/TS 21547:2010 Health informatics -- Security requirements for archiving of electronic health records -- Principles
- ISO/TS 22600-1:2006 Health informatics -- Privilege management and access control -- Part 1: Overview and policy management (IS ballot underway)
- ISO/TS 22600-2:2006 Health informatics -- Privilege management and access control -- Part 2: Formal models (IS ballot underway)
- ISO/TS 22600-3:2009 Health informatics -- Privilege management and access control -- Part 3: Implementations (IS ballot underway)
- ISO 22857:2013 Health informatics -- Guidelines on data protection to facilitate trans-border flows of personal health data
- ISO/TS 25237:2008 Health informatics – Pseudonymization
- ISO 27789:2013 Health informatics -- Audit trails for electronic health records
- ISO/TS 27790:2009 Health informatics -- Document registry framework
- ISO 27799:2008 Health informatics -- Information security management in health using ISO/IEC 27002

Technical Reports

- ISO/TR 11633-1:2009 Health informatics -- Information security management for remote maintenance of medical devices and medical information systems -- Part 1: Requirements and risk analysis
- ISO/TR 11633-2:2009 Health informatics -- Information security management for remote maintenance of medical devices and medical information systems -- Part 2: Implementation of an information security management system (ISMS)
- ISO/TR 11636:2009 Health Informatics -- Dynamic on-demand virtual private network for health information infrastructure
- ISO/TR 21548:2010 Health informatics -- Security requirements for archiving of electronic health records -- Guidelines

Infrastructure-related Documents

- ISO/TS 22220:2009 Health Informatics -- Identification of subjects of health care
- ISO/TS 27527:2010 Health informatics -- Provider identification

Safety-related Documents

- ISO 11238:2012 Health informatics -- Identification of medicinal products -- Data elements and structures for the unique identification and exchange of regulated information on substances

- ISO 11239:2012 Health informatics -- Identification of medicinal products -- Data elements and structures for the unique identification and exchange of regulated information on pharmaceutical dose forms, units of presentation, routes of administration and packaging
- ISO 11240:2012 Health informatics -- Identification of medicinal products -- Data elements and structures for the unique identification and exchange of units of measurement
- ISO 11615:2012 Health informatics -- Identification of medicinal products -- Data elements and structures for the unique identification and exchange of regulated medicinal product information
- ISO 11616:2012 Health informatics -- Identification of medicinal products -- Data elements and structures for the unique identification and exchange of regulated pharmaceutical product information
- ISO/NP TS 16279 Health Informatics - Alert information in health records
- ISO/TS 22224:2009 Health informatics -- Electronic reporting of adverse drug reactions
- ISO 31000:2009 Risk management – Principles and guidelines
- ISO/HL7 10781:2009 Electronic Health Record-System Functional Model, Release 1.1
- ISO/HL7 NP 16527 Personal Health Record System Functional Model, Release 1 (PHRS FM)
- ISO/TR 22790:2007 Health informatics -- Functional characteristics of prescriber support systems
- ISO/TS 25238:2007 Health informatics -- Classification of safety risks from health software
- ISO/TR 27809:2007 Health informatics -- Measures for ensuring patient safety of health software
- ISO/HL7 27953-1:2011 Health informatics -- Individual case safety reports (ICSRs) in pharmacovigilance -- Part 1: Framework for adverse event reporting
- ISO/HL7 27953-2:2011 Health informatics -- Individual case safety reports (ICSRs) in pharmacovigilance -- Part 2: Human pharmaceutical reporting requirements for ICSR
- IEC 62305:2006 Medical device software – software life cycle processes
- IEC 80001-1:2010 Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities
- IEC/TR 80001-2-1:2012 Application of risk management for IT-networks incorporating medical devices -- Part 2-1: Step by Step Risk Management of Medical IT-Networks; Practical Applications and Examples
- IEC/TR 80001-2-2:2012 Application of risk management for IT-networks incorporating medical devices -- Part 2-2: Guidance for the communication of medical device security needs, risks and controls
- IEC/TR 80001-2-3:2012 Application of risk management for IT-networks incorporating medical devices -- Part 2-3: Guidance for wireless networks
- IEC/TR 80001-2-4:2012 Application of risk management for IT-networks incorporating medical devices -- Part 2-4: General implementation guidance for Healthcare Delivery Organizations

A standards series which is important for German infrastructure

- ISO 21549-1:2013 Health informatics -- Patient healthcard data -- Part 1: General structure
- ISO 21549-2:2004 Health informatics -- Patient healthcard data -- Part 2: Common objects (revised version ballot underway)
- ISO 21549-3:2004 Health informatics -- Patient healthcard data -- Part 3: Limited clinical data (revised version ballot underway)
- ISO 21549-4:2006 Health informatics -- Patient healthcard data -- Part 4: Extended clinical data (revised version ballot underway)

- ISO 21549-5:2008 Health informatics -- Patient healthcard data -- Part 5: Identification data (revised version ballot underway)
- ISO 21549-6:2008 Health informatics -- Patient healthcard data -- Part 6: Administrative data (revised version ballot underway)
- ISO 21549-7:2007 Health informatics -- Patient healthcard data -- Part 7: Medication data (revised version ballot underway)
- ISO 21549-8:2010 Health informatics -- Patient healthcard data -- Part 8: Links

CEN TC 251 "Health Informatics", Working Group 3 "Security, Safety and Quality"

Standards

- EN 13606-4:2007 Health informatics - Electronic health record communication - Part 4: Security
- CR 14301:2002 Health informatics - Framework for security protection of healthcare communication
- CR 14302:2002 Health informatics - Framework for security requirements for intermittently connected devices
- EN 12251:2004 Health informatics - Secure User Identification for Health Care - Management and Security of Authentication by Passwords
- EN 14484:2003 Health informatics - International transfer of personal health data covered by the EU data protection directive - High level security policy
- EN 14485:2003 Health informatics - Guidance for handling personal health data in international applications in the context of the EU data protection directive
- EN ISO 10781:2009 Electronic Health Record-System Functional Model, Release 1.1 (ISO 10781:2009)
- ENV 13608-1:2000 Health informatics - Security for healthcare communication - Part 1: Concepts and terminology (resolved to withdraw)
- ENV 13608-2:2000 Health informatics - Security for healthcare communication - Part 2: Secure data objects (resolved to withdraw)
- ENV 13608-3:2000 Health informatics - Security for healthcare communication - Part 3: Secure data channels (resolved to withdraw)

Safety-related Documents

Standards

- CEN/TS 15260:2006 Health informatics - Classification of safety risks from health informatics products

Technical Reports

- CEN/TR 15253:2005 Health informatics - Quality of service requirements for health information interchange
- CEN/TR 15299:2006 Health informatics - Safety procedures for identification of patients and related objects
- CEN/TR 15300:2006 Health informatics - Framework for formal modelling of healthcare security policies
- CEN/TR 15640:2007 Health informatics - Measures for ensuring the patient safety of health software
- CR 13694:1999 Health Informatics - Safety and Security Related Software Quality Standards for Healthcare (SSQS)