Bundesamt
für Sicherheit in der
Informationstechnik

ICS Security Compendium

Version 1.23

Federal Office for Information Security
P.O.B. 20 03 63
D-53133 Bonn (Germany)
Phone: +49 22899 9582-5599
E-Mail: ics-sec@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of contents

1 Introduction 7
1.1 Motivation 7
1.2 Objectives 8
1.3 Target group 9
1.4 Contents 9
1.5 Safety & security 10
2 ICS bases 11
2.1 Glossary 11
2.2 Basic characteristics 12
2.2.1 Vertical integration 13
2.2.2 Horizontal integration 13
2.2.3 Life cycle 14
2.2.4 Real-time response 14
2.2.5 Functional safety 14
2.2.6 Physical separation 14
2.2.7 Software 15
2.2.8 Updates 15
2.2.9 Hardware 15
2.2.10 Standards 15
2.3 Hierarchical structure of ICSs 16
2.3.1 Level 1: Field process management 16
2.3.2 Level 2: Real-time process management 17
2.3.3 Level 3: Process management equipment 17
2.3.4 Level 4: Operational management 18
2.3.5 Level 5: Production management 18
2.3.6 Exceptions 19
2.4 Distributed control system (DCS) vs. SCADA 19
2.5 Communication processes 20
2.5.1 Communication processes in Level 1 20
2.5.2 Communication processes in Level 2 22
2.5.3 Communication processes in Level 3 24
2.5.4 Communication processes in Level 4 24
2.5.5 Communication processes in Level 5 24
3 IT Security Threats 25
3.1 Organisational threats 26
3.1.1 Insufficient rules regarding security 26
3.1.2 Inadequate documentation 26
3.1.3 Incomplete securing of remote maintenance access points 26
3.1.4 Use of standard IT components with already identified vulnerabilities 27
3.1.5 Lack of monitoring of the supporting infrastructure 27
3.1.6 Dependencies between the ICS network and IT networks 27
3.1.7 Lack of awareness 28
3.2 Human error 28
3.2.1 Inadequate protection or overly extensive networking 28
3.2.2 Poor configurations of components 28
3.2.3 Lack of backups 29
3.2.4 Portable media and laptops 29

3.2.5 Inadequate validation of input and output....29
3.3 Deliberate acts....29
3.3.1 Communication of measured and values....30
3.3.2 Determining access data by means of dictionary and brute force attacks....30
3.3.3 Systematic search for vulnerabilities via the network....31
3.3.4 Denial of service attacks (DoS)....31
3.3.5 Man-in-the-middle attacks....31
3.3.6 Phishing....31
3.3.7 Injection attacks....32
3.3.8 Cross-site scripting....32
3.3.9 Drive-by downloads....32
3.3.10 Malware on engineering workstations....32
3.3.11 Malicious software....33
3.3.12 Replay attacks....33
3.3.13 Physical attack to provoke administrative intervention....33
4 Organisations, associations and their standards....35
4.1 International standards....35
4.1.1 ISO/ IEC....35
4.2 National standards and recommendations....39
4.2.1 DIN....39
4.2.2 VDI, VDE and DKE....40
4.2.3 NAMUR....43
4.2.4 BDEW....43
4.2.5 VGB....44
4.3 Foreign recommendations....45
4.3.1 NERC....45
4.3.2 NIST....45
4.3.3 DHS....46
4.3.4 CPNI....49
4.3.5 IEEE....50
5 Best Practice Guide for Asset Owners....51
5.1 General procedure in the engineering process....51
5.2 First steps....52
5.3 Security-specific processes / policies....55
5.3.1 Security management....55
5.3.2 Technical documentation....55
5.3.3 Continuous management of all ICS components....55
5.3.4 Business continuity management....56
5.3.5 Personnel....56
5.3.6 Revision & tests....57
5.4 Selection of the used systems and components as well as of the assigned service providers and integrators....57
5.4.1 Trustworthiness....57
5.4.2 Security features of ICS components....57
5.4.3 Compatibility of the technologies used with standards....58
5.4.4 Commissioning in a secure configuration....58
5.4.5 Soft- and hardware support....58
5.4.6 Remote maintenance by the product supplier and integrator....58
5.4.7 Securing field devices....59
5.5 Constructional and physical securing....59

5.6 Technical measures 59
5.6.1 Securing of networks 59
5.6.2 Protection of services and protocols 64
5.6.3 Hardening of the IT systems 65
5.6.4 Patch management 66
5.6.5 Authentication 67
5.6.6 Access control 68
5.6.7 Protection against malware 69
5.6.8 Portable media 71
5.6.9 Backup 72
5.6.10 Logging and evaluation 73
5.7 Comparison with available standards 74

6 Methodology for audits of ICS installations 97
6.1 ICS specifics and IS revision 97
6.2 Procedure 97
6.2.1 Kick-off 98
6.2.2 Familiarisation 98
6.2.3 Coordination workshop 99
6.2.4 Test methods of the test phase 100
6.2.5 Assessment 102
6.2.6 Reporting 104
6.2.7 Implementation of the measures and recommendations 104
6.2.8 ICS revisited 104
6.3 Test phase according to subject levels 105
6.3.1 Physical security 105
6.3.2 Policies and processes 106
6.3.3 Network level 106
6.3.4 Device level 108
6.3.5 Application level 109
6.3.6 Field process management 109
6.3.7 ICS security test 109

7 Trends and resulting need for R&D 111
7.1 Current trends 111
7.1.1 Industry 4.0 111
7.1.2 Cloud architectures in the industry 111
7.2 Higher levels of security 112
7.2.1 Best practices for product suppliers, asset owners and integrators 112
7.2.2 Integration of safety and security 113
7.2.3 Tool for ICS audits 113
7.2.4 Further development of defence-in-depth strategies 113

8 Summary and outlook 115
Table of abbreviations 116
References 119

List of figures

Figure 1: Vertical integration of production plants 13
Figure 2: Horizontal integration of production plants 14
Figure 3: Hierarchical structure of an ICS 16
Figure 4: Activation of field signals 21
Figure 5: Comparison of communication concepts 23
Figure 6: Structure of the ISO 27000 series of standards in accordance with ISO/IEC 27000:2012 36
Figure 7: Overview of IEC 62443 38
Figure 8: Assignment of the IEC 62351 parts to protocols and standards (taken from [Cleveland 2012]) 39
Figure 9: Procedures according to VDI/VDE 2182 in accordance with [VDI 2182 2011] 42

List of tables

Table 1: Established audit results for the current threat scenario 8
Table 2: Comparison between SCADA systems and DCS 20
Table 3: Typical differences between production and process engineering 22
Table 4: Comparison between separated and integrated Level 2 communication 23
Table 5: Comparison between typical properties and security objectives of conventional enterprise IT and ICS 25
Table 6: Comparison of the best practices with IEC 62443, VDI/VDE 2182, NERC CIP and DHS Best Practices 83
Table 7: Comparison between the best practices and IT-Grunfschutz and ISO 27001 96
Table 8: Table for the documentation of IP network-based vulnerabilities 101

1 Introduction

To measure and control procedures, for example for automation of processes and for monitoring large systems, so-called Industrial Control Systems (ICSs) are used in many industrial sectors. They are often used in the manufacturing industry and in sectors which are counted among critical infrastructures (KRITIS), such as energy, water, food or transport and traffic.

1.1 Motivation

In the past, ICSs were physically separated from other IT systems and networks (so-called "air gap") and thus protected against external influences by other information technology to a large extent. Therefore, security was an aspect of minor importance when selecting and developing mostly proprietary software and protocols.

With the introduction of IT systems from the office environment and the increasing level of networking of the ICSs even across network boundaries (e.g. in an enterprise network), these systems are nowadays exposed to similar threats to those of conventional enterprise IT systems. The fact that these threats are real is proven by different incidents in the recent past.

Depending on the threat agents' target, the procedure of the threat agents differs slightly. In the case of systems which can be directly accessed via the Internet, attacks on the system are started in a targeted manner. This means that vulnerabilities are exploited directly. They may affect the operating system, server applications or web applications.

In the case of many attacks which have become known in the last few years, spear phishing attacks are used to enter the enterprise. In this way, a kind of "bridge head" is installed on a computer in the enterprise. This bridge head is used to spy out the network and to infect other systems. If the threat agents have reached their actual target system, they obtain the information they looked for there or manipulate it. If the threat agent achieves their goal, they will also try to cover their tracks in order to remain undetected.

This makes clear that the security design of process control systems must be reconsidered and, if necessary, adjusted to the current threat scenario.

In Table 1, typical observations made in the recent past during ICS security audits, which allow conclusions on the current threat scenario to be drawn, are listed as examples.

ICS component	Security-relevant observations
Network	• Connection of unknown systems to the backup
Firewall / router	• Rules not sufficiently restrictive • Undocumented rule entries • Data flows which are apparently no longer required • Bypass in the routing • IP forwarding on servers
Modems	• Unprotected access • Connection not documented • Permanent connection (always-on)
Remote maintenance	• Connection directly to field level
Operating systems / hardening	• Operating system components not hardened • Unneeded services offered • Unsupported new operating system version and lack of patches (patch management is a fundamental challenge in ICS)
Wireless communications	• Lack of encryption • Outdated network elements
Industrial switches	• Lack of robustness to unexpected and/or non-standard communication • Backdoors (e.g. hard-coded passwords)
Outdated network elements	• Administrative, web-based access without protection (e.g. SSL) Lack of protocol support (e.g. only 'telnet' access)

Table 1: Established audit results for the current threat scenario

Contrary to conventional IT, ICS have deviating requirements for the security objectives of availability, integrity and confidentiality. Examples of these are longer operating times and rare maintenance windows. Furthermore, the real-time requirements which are of essential importance for control must be mentioned in particular. Another important factor is warranty claims. Established security measures from the office environment can be transferred to ICSs only to a limited extent.

1.2 Objectives

Against this background, the ICS Security Compendium has the following objectives:

- The compendium is a basic reference guide for security in ICSs. It allows both security and ICS experts to easily approach security in ICSs and explains the bases of security, ICS procedures and the relevant standards which are required to consider this subject.
- A specific relationship to IT-Grundschutz was developed. After architectural, technical and organisational security measures have been developed for ICSs on the basis of existing standards, it is explained in

particular which extensions are necessary to be able to apply IT-Grundschutz in the field of ICS security and which considerations are additionally required if IT-Grundschutz is applied to the ICS infrastructure. Here, the differences and gaps of established ICS standards and especially of the IT-Grundschutz in the field of ICS security are also presented.

- Published standards and best practices for ICS security are presented and a collection of the most important measures is compiled.
- A specific, feasible methodology for ICS auditing is described.
- Finally, the compendium provides information on the current need for action and on future subjects for research and development in the field of ICS.

The ICS security compendium establishes a general framework for the different areas of application of industrial control systems. Of course, such a basic reference guide cannot address all specifics of the different industrial sectors in a detailed manner. Therefore, the compendium is to be understood as a request directed at the respective associations and organisations to create separate, sector-specific types or clarifications of the compendium and to explain the respectively applicable particularities in detail. This is the only way to describe the industry-specific bases for certain areas of application in a tailored manner.

Performing a recurring (regular and/or due to special events) risk analysis is considered mandatory. As part of the risk analysis, particularly the threats presented in chapter 3 must then be examined and assessed. The plant operator is then responsible for deriving suitable security measures which reduce the risks associated to the identified threats to an acceptable residual risk. The best practices described in chapter 5 can provide assistance in this respect.

In addition to this, the feasibility must be assessed with regard to the respective framework conditions and, if applicable, alternative security measures must be defined. For example, safety requirements can restrict the specific implementation options of a security measure. Especially in this area, the respective associations and organisations are qualified to present a possible implementation of the best practices. Therefore, these sector-specific types should address the chapters "ICS bases" and "Best practice guide for asset owners" in particular. Of course, additional contents, such as the description of the relevant vulnerabilities or the applicable standards, can also be clarified specifically for the respective sector. This results in the potential of drawing up industry-wide recommendations or guidelines which meet the respectively applicable requirements.

1.3 Target group

The compendium is primarily written for asset owners and draws attention to the subject of security. The implementation of security in the form of the developed best practices results in a risk reduction in ICSs.

System integrators and product suppliers of ICS components should be familiar with the measures and take them into account when developing and planning new components and plants.

Enterprises which test and assess the security of automation systems are another target group. Moreover, the compendium serves as a suggestion for all persons who deal with the security of automation systems in some way.

Product suppliers and integrators will be addressed to a greater extent in the update of the compendium (see chapter 8).

1.4 Contents

Chapter 2 provides an introduction to the ICS bases. It is addressed to security experts (from conventional enterprise IT) who have had nothing or only little to do with ICS so far.

The security-specific ICS bases are explained in chapter 3. They provide access to the subject of security. In addition to the general introduction to vulnerabilities and attack vectors, an explanation of ICS particularities, which is directed equally to ICS users and security experts, is given.

Chapter 4 provides an overview of national and international organisations and their standards and quasi-standards with regard to the subject of ICS security. It is intended to support all readers in classifying the available publications.

Chapter 5 defines architectural, technical and organisational measures for ICS protection. Furthermore, the best practices are compared to established standards. The best practices are primarily addressed to ICS asset owners.

Based on the measures described above, chapter 6 described a methodology for performing ICS audits.

In chapter 7, current trends from the ICS environment are considered. Possible projects and required research activities are derived from these trends.

Chapter 8 summarises the results of the study and gives an outlook on future updates.

The subject of Industry 4.0 is only considered marginally in this document. Industry 4.0 is an important future project of the German Federal Government and a driver of innovation for the German industry. The primary aim of this ICS Security Compendium, however, is to improve the security of today's plants. Today's industrial plants are not Industry 4.0 plants, since rudiments of Industry 4.0 have so far only been implemented into practice in ultra-modern plants. Altogether, the greatest need for action relates to existing plants ("Industry 3.0"). For Industry 4.0, it is not possible yet to define generally applicable best practices due to ongoing research and development. However, the bases presented in this document can and should also be taken into account and supplemented adequately when implementing the Industry 4.0 paradigm into practice.

1.5 Safety & security

At the beginning of this document, a distinction between the terms "safety" and "security" should be made. The term "safety" refers to the functional safety of the machine or plant and thus addresses the protection of the environment against abnormal operation. The term "security" describes the protection of IT-supported systems against deliberate or undesired errors. Safety systems must also be protected against attacks.

2 ICS bases

This chapter provides an introduction to the ICS bases. After the ICS areas of application have been explained, a typical ICS architecture is described. The use of ICS components based on this architecture as well as the communication technique used in ICSs are outlined. The basis of the descriptions is the common practice from the user's point of view irrespective of the product supplier. Considering the large number of different ICS applications, this document focuses on security, which is why the application-specific details are only addressed generically.

2.1 Glossary

The terms used for components and functions in the field of automation engineering are defined comprehensively in international standardisation (see IEC 60050 for example). Considering the common nomenclature in different industrial sectors, a comparison of the common terms is provided below.

German terms are often used synonymously with English terms which, however, do not necessarily have the same functionality. Unfortunately, a certain 'fuzziness' of designations cannot be avoided.

- **Anzeige- und Bedienkomponenten (ABK) [German term referring to display and operation components]**

  See Human Machine Interface

- **Actor**

  An actor, also referred to as actuator, converts a control variable into an electrical, hydraulic or pneumatic signal.

- **Beobachtungs- und Bedienkomponente (BuB) [German term referring to a monitoring and operation component]**

  See Human Machine Interface

- **Control in the Field (CiF)**

  CiF is an automation strategy in which field devices perform some of the control processes and thus contribute to a reduction in latency times. The necessary actual values are transmitted by the respective sensing elements directly via fieldbus to the field device which then performs the control tasks without including a central, higher-level control unit.

- **Distributed Control System (DCS)**

  Distributed control systems (DCSs) are used for larger process plants in most cases. They can have a large number of features, such as alarm systems, plant visualisation (curve recording of measured values), user management, central data storage as well as maintenance and development tools.

- **Engineering Workstation (EWS)**

  Engineering workstations (EWS), engineering stations (ES) as well as service computers allow the configuration and programming of ICS components.

- **Human Machine Interface (HMI)**

  These components provide display and operation functions. Functionally, they can include standard operating screens, free graphics, recipe creation and monitoring tools, alarm handling, data archiving and evaluation, system diagnoses and documentation (technical systems and production processes) as well as interactive operational support.

- **Industrial Control System (ICS)**

ICS is a generic term for automation solutions used to control technical processes.

- **Master Terminal Unit (MTU)**

  The MTU makes the information collected available to the operator via the human machine interface and transmits the control signals to remote units such as sub-MTUs, *remote terminal units* or directly to *programmable logic controllers*. In many cases, *SCADA* servers are used as MTUs.

- **Process Analytical Technology (PAT)**

  The PAT is used to optimise, analyse and control manufacturing processes in the chemical industry.

- **Programmable Logic Controller (PLC)**

  See Speicherprogrammierbare Steuerung

- **Programmiergerät (PG)** [**German term referring to a programming device**]

  See Engineering Workstation

- **Prozessleitsystem (PLS)** [**German term referring to a distributed control system**]

  See Distributed Control System

- **Prozessnahe Komponente (PNK)** [**German term referring to a process-oriented component**]

  See Speicherprogrammierbare Steuerung

- **Remote Terminal Unit (RTU)**

  Automated technical component for the collection and, if applicable, processing of process information and transmission of the information to a higher-level master terminal unit.

- **Safety Integrity Level (SIL)**

  According to IEC 61508, a safety integrity level specifies four requirement levels which are linked to the quality of the automated functions and functional integration into the material production process.

- **Sensor**

  Sensors record physical variables and convert them into a standardised signal (for example 4-20mA, 24V). There is a large number of components which belong to this class: (limit) sensors, (limit) switches or sensing elements. The communication protocols used are referred to as fieldbuses.

- **Speicherprogrammierbare Steuerung (SPS)** [**German term referring to a programmable logic controller (PLC)**]

  A programmable logic controller (PLC) is used for the automation of electromechanical processes. Digital and analogue inputs and outputs are used. Depending on the area of application, their design can be robust so that they are resistant to external influences, such as temperature, vibration etc.

- **Supervisory Control and Data Acquisistion (SCADA)**

  SCADA describes the control and monitoring of technical processes by means of a computer system. The term usually refers to systems with a decentralised database (contrary to DCS). In the case of SCADA solutions, the automated functions are realised by RTU or PLC, whereas a computer system is used for the operation, archiving and evaluation of the processes.

2.2 Basic characteristics

ICSs are used wherever processes are automated. They are used for measuring, controlling and operating industrial processes.

Examples include the process engineering, the manufacturing automation, the supply and disposal networks (e.g. energy, water, gas, district heating), die operating technology (e.g. rail and road transport) and the building automation. The individual ICS requirements are determined directly by the operational requirements of the material production processes. ICSs are usually integrated vertically and horizontally.

2.2.1 Vertical integration

Within the value-added chain of an enterprise, there is a business process between the production order and material production. Within the framework of this process,

- Production management (in which company a production order is processed),
- Operational management (are the resources required for processing a production order available) and
- Process management (are the technical parameters of the production process in the correct range)

are dealt with. After a production order has been completed, a corresponding production report is created and archived. The details of this business process can vary greatly due to individual requirements (e.g. in the area of pharmaceutical production).

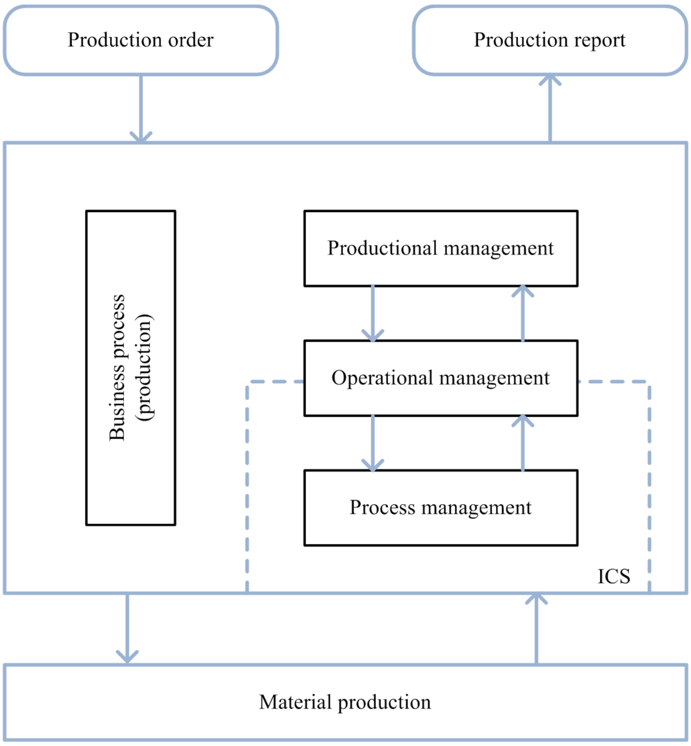


Figure 1: Vertical integration of production plants

2.2.2 Horizontal integration

Typical production processes include production steps which are divided into several levels. ICSs can be found in many of these production steps. Considering efficient production and compliance with quality-relevant regulations, information must be exchanged between the production facilities (plants, storage facilities etc.). This exchange of information can be carried out in different ways. However, the focus below is placed on communication in the sense of an electronic exchange of data.

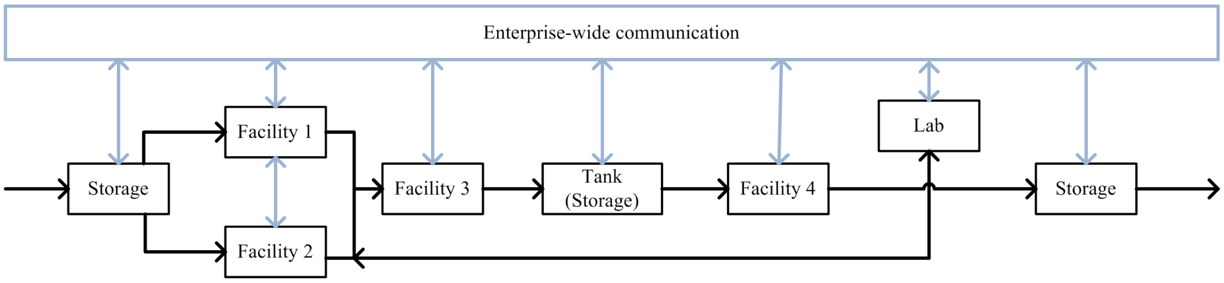


Figure 2: Horizontal integration of production plants

This structure is owing to the entrepreneurial pursuit of quality and efficiency. At the same time, it is the framework for the technical implementation of the business process.

This structure and the additional "rigid" connection to the respective material production process results in another priority sequence for ICSs than the one which is common in office IT. Therefore, the common strategies used in office IT cannot be implemented into practice without further ado (see chapter 2.2.8).

2.2.3 Life cycle

The ICS life cycle is derived from the life cycle of the associated production plants. This life cycle is significantly longer than the typical periods of time applicable to office IT. The lifespan is ten to fifteen years. Sometimes, the lifespan may even be 20 years. In office IT, the lifespan is only three to five years in most cases.

2.2.4 Real-time response

Control circuits are optimised with respect to their time behaviour. If the time behaviour of the ICS is changed due to (temporary) modifications in the software, this causes disruptions in the material production process. This may result for example in more rejects.

2.2.5 Functional safety

There are many applications in which the operation of plants is subject to official regulations (e.g. plant safety). In these cases, substantial changes, which may also include software changes in the ICSs used, require a dedicated approval process.

Due to the prescribed test process, the options for installing security updates promptly, for example, are limited and/or not available.

2.2.6 Physical separation

With respect to the ICS structure, it is common practice to also implement a physical separation of functional units, especially in terms of the infrastructure, in addition to the logical separation of individual segments.

Example:

In the field of office IT, different logical networks are usually operated on one switch. This is not common practice in the area of ICSs considering possible undesired interconnections and their potential effects. If different network segments are still combined, this must be taken into consideration within the scope of a risk assessment. The effects on the system integrity and aspects such as the possible validation of an ICS must be assessed and documented in these cases.

2.2.7 Software

Unlike office IT, ICSs are operated for longer periods of time with virtually the same user software. Changes are made within the scope of pre-planned options such as changing controller parameters, changing limit values, but also creating recipes.

2.2.8 Updates

In the field of office IT, systems are ideally improved as quickly as possible (by installing patches) after errors or vulnerabilities become known.

In the area of application of ICSs, the prescribed response times must also be complied with in addition to the functions in the case of software changes, even during the change process. Moreover, it is generally required to test the overall structure consisting of the ICS and material production process. The respective test depth depends on the respective application. For example, application-specific (e.g. in the field of pharmaceuticals production) tests, the processing of which forces a production downtime, must be carried out and documented. Therefore, updates can usually only be installed as part of maintenance activities at longer intervals.

2.2.9 Hardware

Unlike office IT, ICSs are operated for longer periods of time with the same hardware (device types).

2.2.10 Standards

In the area of ICSs, there is a large number of standards which include strict ICS requirements (e.g. IEC 61508-3 in the field of software development).

2.3 Hierarchical structure of ICSs

A hierarchy of an ICS which is typically prescribed by the business process is as follows:

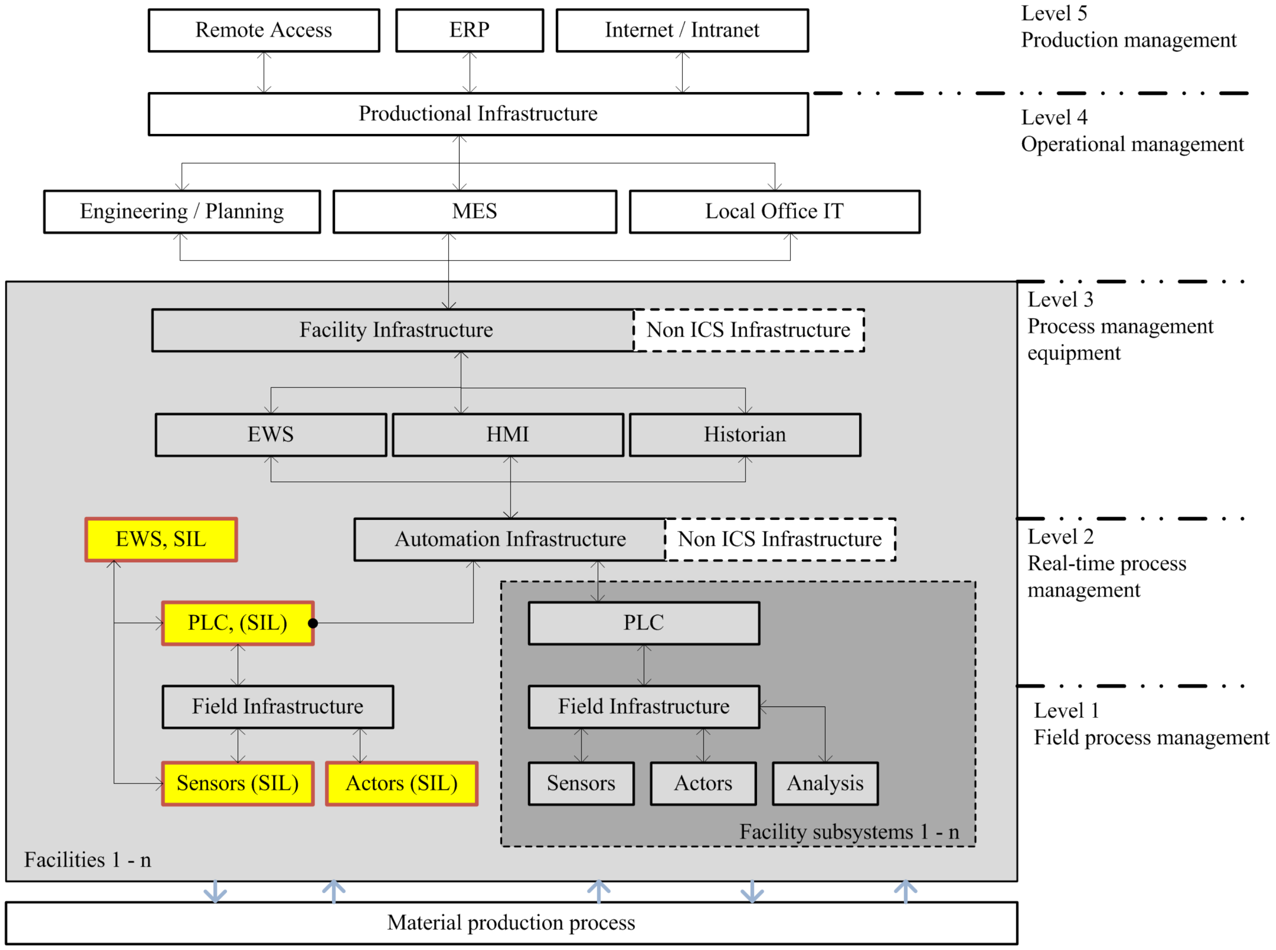


Figure 3: Hierarchical structure of an ICS

2.3.1 Level 1: Field process management

This level includes the components which are required for gaining information from the field of the material production and/or which influence the events in the field of the material production (limit switches, sensing elements, analysers, valves, actuators, motors etc.). On the one hand, these components interact directly with the material production process and, on the other, with the help of their related infrastructure, with the related information-processing units or, if applicable, also with each other (e.g. when CIF strategies are implemented). Depending on the application and technology used, the related infrastructure can include different components. In this context, examples include:

- Remote I/O (if applicable, with signal preprocessing, which is then referred to as RTU),
- Interface modules for signal conditioning,
- Switches when fieldbus solutions are used.

The process data signals in Level 1 are transmitted in real time. A disruption in the signal transmission results in the direct disruption in the material production process unless a physical (e.g. 2 of 3 interconnection in the case of sensing elements) or logical (e.g. substitute value connection in the case of a measure value failure) redundancy is available.

When using fieldbuses or devices which support the HART Protocol (Highway Addressable Remote Transducer Protocol), it is also possible to transmit diagnostic and configuration data.

2.3.2 Level 2: Real-time process management

This level includes the components which are required for the signal processing within the meaning of the presentation of the automated functions (e.g. end position reached: driver motor OFF or fill level HIGH: pump OFF). These components are typically designed depending on the plant section configuration to be automated. Depending on the automation product used and the size of the plant (section) to be automated, individual devices or networks with groups of automation products are used.

Furthermore, the technical design in detail depends very much on the design solution chosen.

In principle, there are three different versions:

1. The information from the field level is read and processed without preprocessing and the position commands are transmitted directly to the actuators. For example, the position feedback signals of a valve are monitored with respect to:
    - The static state, such as OPEN/CLOSE must not be available at the same time and
    - The logical sequence, such as the feedback CLOSE must be available within 1 second after the command termination.
2. In the field, there is a signal preprocessing (e.g. the watchdog timer of a valve) within an RTU, the Level 2 components only receive the information resulting from this, such as that the valve is open and has a runtime error.
3. Automation functions, such as control operations, are implemented in field devices such as position controllers at control valves (positioners). The related actual values are sent by the corresponding sensing elements directly (e.g. per fieldbus) to the positioners (CIF).

This information is processed deterministically, which means that a predefined response time must be ensured for proper overall functioning. Non-compliance with this requirement results in the direct disruption in the material production process.

The systems to reduce the operational risk if special reliability requirements are imposed on them (e.g. SIL) have a special role in the field of the Level 1 and Level 2 applications. Depending on the sector-specific application, addition requirements up to the physical separation of the systems (see IEC/EN 61511-1 section 9.5.1) are imposed on these systems.

Furthermore, special attention must be paid to components for the operation of which specific quality requirements, such as GMP (Good Manufacturing Practice) or GAMP (Good Automation Practice) requirements, must be met. In these cases, specific risk analyses, if necessary, must be carried out and documented.

2.3.3 Level 3: Process management equipment

In Level 3, the equipment which is required for the process management, but which does not process data in real time can be found. In this context, examples include:

- HMI/BUB,
- Product-related engineering and maintenance stations
- Measured value and process data archive servers etc.

These components are important for the process management. Their behaviour is less critical than that of the Level 1 and 2 components both with respect to the time behaviour and, in many cases, often also with regard to their availability. On the one hand, this is due to the fact that, for example, inherent redundancies are often available in the field of control stations, since there are several control stations, for example, so that the failure of one control station results in a loss of convenience, but not in the direct disruption in the material production process. The same applies to archive servers, for which a short failure is tolerated by most automation systems, because process data is stored in the real-time components until they have been archived.

Irrespective of these circumstances, Level 3 components are treated restrictively with respect to software updates, because both the interaction between the Level 3 components and the Level 1 and 2 components, and the interaction of the Level 3 components with each other are absolutely necessary for the proper management of the material production process and a potential error on the level of the software used can affect all Level 3 components at the same time.

2.3.4 Level 4: Operational management

The components which can be found in Level 4 fulfil the operational management functions. They can typically be divided into the following categories:

1. Manufacturing execution system (MES)

   In operational management, the MESs map the data transfer between automation engineering on the one hand and economic data processing on the other. In addition to the actual communication processes, this data transfer also includes the aggregation of data. It is necessary, since the equipment in Level 3 processes the process data in second intervals, whereas data processing in Level 4 is performed at significantly longer time intervals (e.g. on a daily basis).

2. Engineering/planning

   System-independent engineering and planning tools can be found in Level 4. They are required to create and maintain technical documentation (circuit diagrams, architectural drawings, process descriptions etc.).

3. Local office IT

   Moreover, the production-oriented office IT can be found in Level 4. On the one hand, the office IT is used by the operating personnel for activities which are not related to production (e-mail, drafting documents, extraordinary analyses etc.) and, on the other, these components often have read access to Level 3 components in order to extract and analyse process data from the archive server, for example, or to display the plant operating screens on the workstations.

2.3.5 Level 5: Production management

In Level 5, the software solutions with the aid of which the comprehensive enterprise-wide business organisation is supported can be found.

Typically, the following functions can be found in Level 5:

- ERP connection
  Production orders and production reports are transmitted via this connection. Moreover, it is also often used to transmit performance-relevant comparative data. Normally, the ERP communicates with the MES (Level 4).

- Internet/Intranet access
  From the ICS's point of view, Internet and Intranet are an equal, untrusted environment. For processing the tasks in Level 4, however, such a connection is required in most cases.

- Remote access equipment
  Specific access points are often used for maintenance purposes. As regards technology, they usually use the Internet (telephone connections must also be considered as Internet connections). These connections differ from the connections mentioned above in that they are usually not required permanently.

2.3.6 Exceptions

Irrespective of the hierarchical structure described here, there are applications in which the postulated hierarchy cannot be implemented into practice.

Examples include devices which combine the signal processing, monitoring and operation and activation of the material production process in one device. If these functions are projected onto the hierarchical model described here, these devices can thus be found in Levels 1 to 3. In practice, these devices are usually integrated into the ICSs on Level 2 provided that they control package units, for example. If they control autonomous systems, for example in the field of smaller applications, however, these systems are operated as independent ICSs.

Specific quality measurements are another example. In different applications, sensors which record quality-relevant data are connected directly to registering systems which can be found in Level 3 by bypassing Level 2. Since specific requirements must be met in these cases, logically and physically separated networks are set up for these application in most cases.

2.4 Distributed control system (DCS) vs. SCADA

In principle, the automation functions presented in this document can be realised both with DCS and with so-called SCADA solutions.

DCSs are characterised in that they are equipped with central data storage for all parameters. All components of a distributed control system access this data. The communication processes required for the operation of the distributed control system are established automatically as specified by the individual configuration without the user having to worry about it. The engineering for distributed control systems takes place centrally using an integrated engineering tool.

SCADA solutions have a heterogeneous structure. They consist of different components between which there are usually no preconfigured communication channels. All communication processes required for the realisation of an automation task must be planned and configured individually. For the engineering of the individual components, different engineering tools might be necessary.

From the plant operator's point of view, equivalent applications can be realised with both solutions. However, the work required for developing a certain solution differs extremely. This can be illustrated by means of the following example:

In a system, an additional alarm is to be generated from an existing analogue input.

Working in a SCADA system	Working in a DCS
• Opening the configuration tool of the source PLC (the PLC which processes the analogue value) • Inserting and configuring an alarm module • Testing the alarm module • Defining a communication variable for the alarm • Assigning the communication variable to a communication process • Reloading the PLC application • Opening the configuration tool of the SCADA solution • Defining a communication variable • Assigning the communication variable to a communication process • Defining the message text • Testing the data transmission	• Opening the central engineering tool • Activating the measuring point • Switching on the alarm function • Updating the documentatio

Table 2: Comparison between SCADA systems and DCS

If the plant size is the same, this advantage in terms of the operating convenience might be weighed up against the significantly higher purchase price of the DCS.

2.5 Communication processes

The communication processes required for ICS operation can be realised with many different technological solutions which have comparable results. Furthermore, this field is subject to an intensive development process. For this reason, essential technical requirements and no individual solutions are taken into consideration below.

The consideration is based on the system presentation according to 3. The level on which a communication process takes place is used a criterion for differentiation. Communication processes within the individual level are considered first.

2.5.1 Communication processes in Level 1

In general, it is necessary for the communication in Level 1 to transmit the process data by complying with deterministic conditions. In addition, diagnostic and configuration data must be transmitted if required. Moreover, anti-falsification mechanisms and (e.g. remote control technology) encryption are required depending on the specific requirements (e.g. SIL). In general, three different versions are available:

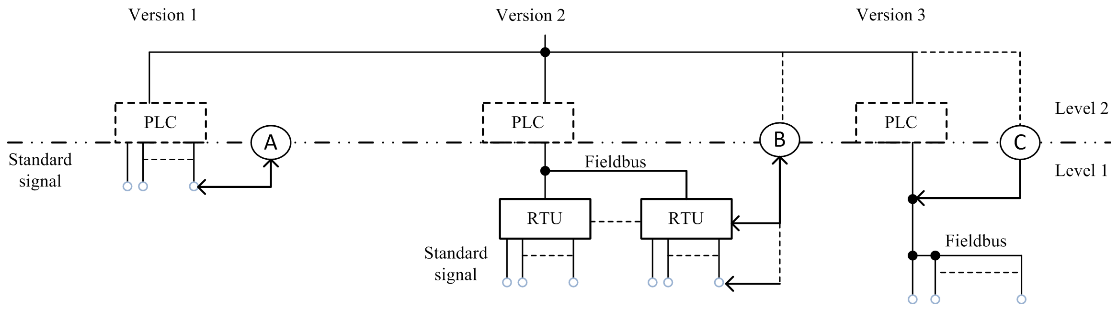


Figure 4: Activation of field signals

- Version 1
  - The field devices are connected to the PNKs using standardised signals as part of a point-to-point wiring.
  - Maintenance devices are typically connected according to A.
- Version 2
  - The field devices are connected to the RTUs using standardised signals. They communicate by means of a fieldbus with the related PNKs.
  - Maintenance devices are typically connected according to B, with the field devices possibly being connected to the RTU (e.g. in the case of EX applications).
  - Solutions where the maintenance connection leads to communication connections between Level 2 and Level 1 (e.g. HART multiplexers) require special consideration.
- Version 3
  - The field devices are connected to the PNKs by means a fieldbus.
  - Maintenance devices are typically connected according to C, with the connection being possibly established at the PNK (e.g. in the case of EX applications).
  - Solutions where the maintenance connection leads to communication connections between Level 2 and Level 1 (e.g. fieldbus monitoring systems) require special consideration.

In the area of fieldbuses, there is a large number of different products. According to IEC 61158, the following fieldbus systems are currently (version 2013)available:

- FOUNDATION Fieldbus,
- CIP (Common Industrial Protocol),
- PROFIBUS and PROFINET,
- P-NET,
- WorldFIP,
- INTERBUS,
- SwiftNet,
- CC-Link,
- HART[1],
- VNET/IP,

[1] The HART Protocol is generally not a fieldbus in the strict sense, because digital communication is modulated on conventional, point-to-point wired 4-20 mA signals and/or used in parallel.

- TCnet,
- EtherCAT,
- ETHERNET Powerlink,
- EPA (Ethernet for Plant Automation),
- Modbus (RTU and/or ASCII but also TCP),
- SERCOS,
- RAPIEnet,
- SafetyNet p
- MECHATROLINK.

In addition to this, there is a version (multidrop), for which a function which is similar to a bus can be created. Furthermore, there is a wireless version (WirelessHART) which is available for setting up encrypted wireless networks for the transmissions of measured data. Details in this respect are defined in IEC 62591:2010. Other common types of transmission are ZigBee or Bluetooth.

With respect to the requirements for fieldbuses, there are basic differences between production engineering and process engineering.

Production engineering	Process engineering
Many binary signals	Many analogue signals
No impact of the configuration work on the data transmission in terms of time	Explosion protection
Highspeed data transmission	High availability
	Power transmission per bus cable

Table 3: Typical differences between production and process engineering

2.5.2 Communication processes in Level 2

On Level 2 of an ICS, there are both real-time connections (e.g. between the PNKs) and connections which are not critical in terms of the transmission time (e.g. engineering access). Therefore, protocols with different stacks (e.g. Industrial Ethernet in the case of new systems) are often used. Typically, the layers 1, 2 and 7 of the OSI reference model are used. In the case of distributed control systems, the functions of layer 7 are usually not disclosed.

For example, OPC (OLE for process control) and/or OPC UA (Unified Architecture) or DDE (Dynamic Data Exchange) are used as software interface.

Considering the consequences of a failure of the Level 2 communication, redundant structures can frequently be found here.

For the communication between the PNKs which must meet special requirements (e.g. SIL), specific security procedures which make it possible to detected random transmission errors an den data (e.g. CRC checksums) are additionally used.

For SCADA solutions in particular, the same protocols as in Level 1 are often used.

Plants for which transmission media and the related infrastructure, which are not an exclusive part of the ICS, are used for the communication described here require special consideration. This applies in particular to remote control systems and/or ICS, with which geographically separated plant sections are operated (e.g. gas, power and water / wastewater disposal).

Moreover, applications for which switches, routers and fibre optic cables are to be used as part of a Level 5 IT site network for the Level 2 communication must also be considered specifically.

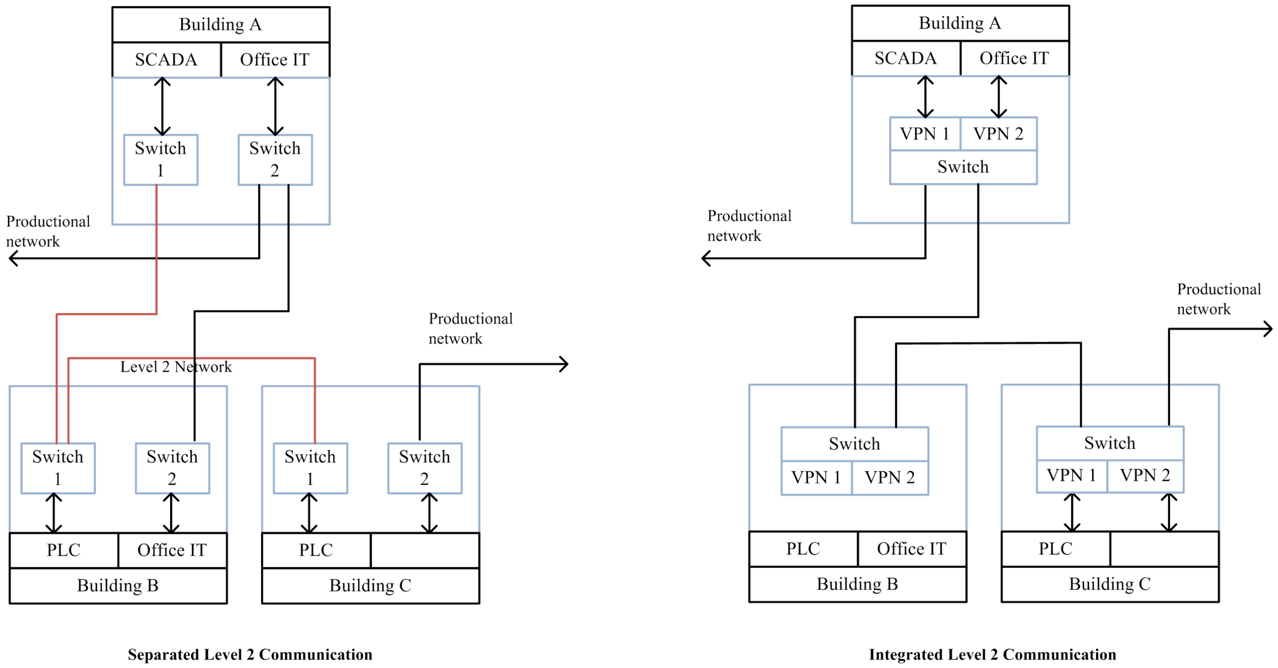


Figure 5: Comparison of communication concepts

In these cases, separate consideration of the risks resulting from this architecture is required.

Separated Level 2 Communication	Integrated Level 2 Communication
• Separated communication infrastructure • Changes to office IT switches do not have an impact on ICSs • No undesired cross communication • Separated patch management for switches possible • Life cycle of the office IT switches does not have an impact on ICSs • Where necessary, reasonable redundancies can be implemented	• Shared communication infrastructure • Changes to office IT switches must be assessed with respect to their impacts on ICSs (data, transmission times etc.) • The communication possibilities between the different VPNs must be assessed • Patch management must be assessed, e.g. in the case of GMP requirements • Life cycle of the office IT switches has an impact on ICSs • Redundancy requirements cannot be implemented completely in some cases.

Table 4: Comparison between separated and integrated Level 2 communication

In principle, wireless transmission protocols can also be applied to Level 2, as they are available, for example, with WLAN according to IEEE 802.11. Considering the special requirements of industrial environments (e.g. EMC, failures due to steel constructions etc.), these solutions, however, must be assessed critically for these areas of application irrespective of possible security risks.

2.5.3 Communication processes in Level 3

The data transfer between the actual ICS and the higher-level functions and/or stations is handled via Level 3 of an ICS application. Level 3 is the external perimeter of the actual ICS application (except for special cases with integrated MES functionality). Data is typically transmitted using Ethernet technology. Typically, the layers 1, 2, 3, 4 and 7 of the OSI reference model are used.

As software interfaces,

- DDE to access predefined data areas
- OLE (Object Linking and Embedding) to access (external) software elements
- ODBC (Open Data Base Connection) to access databases

or similar technologies are used. Wireless transmission protocols are used on Level 3. Here, examples include the connections between maintenance computers which are connected to the ICS and portable devices which are used for maintenance purposes. For example, WLAN according to IEEE 802.11 is typically used.

2.5.4 Communication processes in Level 4

In Level 4, the entire range of communication technology is used.

For ICS operation, the functions implemented in Level 4 are of particular importance, since security functions with external effects can be found in this level. For many users, the systems in Level 4 are administered by the IT department of the respective plant operator. With regard to the protection requirements, there are the same requirements as are common for office IT. The typical security strategies from the area of office IT can be applied to the applications on Level 4.

On Level 4, the security functions which protect an ICS against external threats which use external communication processes as a basis are established.

2.5.5 Communication processes in Level 5

For Level 5, no ICS requirements are provided.

The only exception in this case is maintenance access (remote access) which is dedicated exclusively for the respective ICS. For these applications, the entire range of the available technology including GSM, UMTS and LTE with transmission rates of approx. 100 KBit/s up to 1 GBit/s is used.

3 IT Security Threats

The perception of ICS security has changed in the recent past. For a long time, the installations were compartmentalised systems based on proprietary technologies without any networking with third-party systems. Networking with the Internet or existing office communication networks was not taken into account or could not be realised due to technological barriers.

Because of the increased use of software and protocols from the office IT as well as the increasing level of networking and sharing of resources (see chapter 2.5), ICSs are exposed to the same threats as office IT. Due to other framework conditions, however, there are not always the same possible solutions.

These framework conditions include, amongst other things:

- The high availability requirements which make it difficult to import updates as in office IT (see chapter 2.2.4)
- The long life span (see chapter 2.2.6 and chapter 2.2.9)
- The fact that, in the past, security aspects were not taken into account when designing the protocols used. The only exceptions in this case include recently adopted protocol specifications.
- Specifications for approvals and the operation of the plants or components (e.g. SIL)

Category	Conventional enterprise IT	ICS
Performance	• No guaranteed processing times • High latency acceptable under certain circumstances	• Guaranteed processing times • Latency in some cases very limited
Availability	• Rebooting of productive systems not unusual • Maintenance processes arranged at short notice (e.g. patch) • Maintenance downtimes only result in low costs	• Rebooting in the productive environment not acceptable • Maintenance cycles only with a long lead time • Maintenance downtimes result in high costs
Assessment of risks	• The confidentiality and integrity of data have priority • Significant risks concern the lasting disruption of business processes	• The protection of people and the environment has priority • Significant risks concern the inadequate protection of people and the destruction of production capacities. Effects on the environment are possible
System resources / dedicatedness	• Systems have free resources which, for example, allow security tools to be installed on the system	• Installation of third-party software components on the systems is not provided or only after approval, e.g. anti-virus programs, programs for video linking
Life span of the components	• A few years	• Up to 20 or 25 years

Table 5: Comparison between typical properties and security objectives of conventional enterprise IT and ICS

Several threats relevant to ICS with respect to security are listed below. They also occur in enterprise IT. For detailed information, references to the threats from IT-Grundschutz are provided.

In this respect, it must be taken into account that this is not a listing in the order of importance. Vulnerabilities are assessed in combination with a risk analysis which must also take the potentially exposed people and objects into consideration.

3.1 Organisational threats

3.1.1 Insufficient rules regarding security

The subject of security must be considered holistically. If the responsibilities for identifying and updating information technology processes are not defined, the documentation becomes obsolete or is not created at all. Involving the specialised departments is also necessary for complete identification and implementation.

Rules regarding the subject of security influence many areas, from the purchasing of new components, to the employment of new personnel, up to the operation and the disposal of devices (see [BSI GS] T 2.1).

Different knowledge levels in the field of security or ICS may cause implementation problems. On the one hand, specifications which cannot be implemented in the ICS area because of the technology can be made by the office security. On the other hand, the ICS experts may not be familiar with certain security aspects. This results in friction losses in the communication and implementation.

However, only drawing up rules is useless if they are not communicated adequately to the staff ([BSI GS] T 2.2) and controlled ([BSI GS] T 2.4).

3.1.2 Inadequate documentation

Documentation covers a very wide field ([BSI GS] T 2.27). It includes, among other things, an updated image of the network cabling ([BSI GS] T 2.12) as well as of the entire information system ([BSI GS] T 2.136) with all components, the services operated on individual components and the approvals in the firewall.

Furthermore, the documentation provides the basis for a risk analysis and the implementation of the security measures.

If the documentation is inadequate, error diagnosis and elimination may be delayed considerably or rendered completely impossible after a damage event as a result of the occurrence of a hardware failure or software malfunction.

Furthermore, the lack of documentation may give a false sense of security. Thus, decisions or statements which are based on a false level of information are made. This may affect, for example, the networking of the office and ICS network so that a clear separation is assumed, although there are connections to individual components.

3.1.3 Incomplete securing of remote maintenance access points

ICSs are often monitored or operated via remote maintenance access points. Different public and private networks, such as the telephony network, wireless network, mobile phone network and increasingly the Internet are used as transmission media (see chapter 2.5.2, chapter 2.5.4, chapter 2.5.5). If these access points are planned inadequately, configured incorrectly or are not monitored ([BSI GS] T 2.128, T 2.129, T 2.130, T 2.131), threat agents may thus access individual ICS components and the ICS infrastructure via these access options in an unauthorised manner and so bypass the security mechanisms at the perimeter.

In addition to a central remote maintenance access points, remote maintenance access points can be found on Level 2 or 3 (see chapter 2.5.2, chapter 2.5.3) and can thus be found directly at the control unit. Existing security mechanisms used to protect the ICS network can thus be bypassed (e.g. modem dial-up option without security mechanisms such as authentication). Especially in existing plants, there are unprotected modem connections, and so a threat agent could possibly attack the ICS using this access point.

3.1.4 Use of standard IT components with already identified vulnerabilities

In addition to ICS-specific IT components, components, technologies and office IT software are increasingly used in ICS solutions. These components, so-called commercial off-the-shelf (COTS) products, have vulnerabilities (like virtually every software). They are often documented and publicly known.

Moreover, corresponding attack tools are often freely available and may also be used by inexperienced threat agents. Since COTS products are widely used, threat agents are also very interested in finding other vulnerabilities in these products. By using COTS products, old and new vulnerabilities from the office IT are thus transferred into the ICS environment (see ([BSI GS] T 0.28).

Since the COTS products are most commonly used, threat agents are not only interested, for example, in detecting new vulnerabilities, but also in developing specifically tailored malware for these products. Furthermore, unlike the procedure in conventional office IT, it is not always possible to operate anti-virus protection in the ICS network and it is therefore more difficult to implement protection against malware.

Typical areas in which COTS products are used are, for example, operating and engineering systems or routers, switches and modems.

3.1.5 Lack of monitoring of the supporting infrastructure

The monitoring of production states is an essential function of ICS solutions. Warnings concerning the production (e.g. if fill levels are fallen short of) and technical parameters (e.g. temperatures, valve positions) are usually shown. On the other hand, there is often a lack of adequate monitoring of the supporting IT infrastructure (see [BSI GS] T 2.22, T 2.160).

If unusual or security-relevant events requiring monitoring are not monitored by ICSs or are monitored inadequately, for example, attempted attacks, bottlenecks in the network architecture or foreseeable failures cannot be detected at an early stage. These events include unsuccessful and successful authentications, an increased utilisation of the network at nodes and incorrect attempts to read from a hard disk.

Moreover, the poor, confusing presentation of the events may also mean that warnings and errors are detected too late.

3.1.6 Dependencies between the ICS network and IT networks

Meanwhile, ICS networks are no longer operated continuously autonomously. If there are dependencies with other systems, networks or services, failures or security incidents outside the ICS network might also affect the ICS environment (see chapter 2.5.2).

Especially if these systems and networks are not under the control of the ICS asset owner, this may lead to severe adverse effects on the production and the availability of the ICS installation. Furthermore, the incident or error might only be remedied with restricted possibilities.

Example of dependencies with other systems and networks include Internet connections (both using a cable connection and using mobile radio), shared infrastructure components (see chapter 2.5.2) or the increasing use of cloud services.

3.1.7 Lack of awareness

The staff makes a major contribution to the security in an enterprise. If they are not aware of the threats, there are increased risks. Examples include the selection of weak passwords or also the opening of e-mail attachments.

For example, there is often a widely held view that the internal network is already secure and that there are thus no risks. This gives a false sense of security. Due to the careless handling of the IT used, security measures might be bypassed or ignored, which makes it easier for the threat agents to carry out attacks.

3.2 Human error

3.2.1 Inadequate protection or overly extensive networking

If unnecessary communication channels into the ICS network are set up, a threat agent can use these possibly inadequately secured access routes to access the ICS and compromise systems (see [BSI GS] T 2.60, T 3.29).

If, for example, a member of staff sets up a data connection from their office workstation into the ICS network for monitoring of an ICS, the office network (e.g. with a connection to the Internet) is linked to the ICS network ([BSI GS] T 3.78). Thus, the ICS network is exposed to the same threats as the office network (e.g. attacks and malware from the Internet).

In addition to the connections mentioned above, data connections are also required for production control, where data must be exchanged between the ICS network and office network. It may occur that the approvals are too general or that the segmentation of the network is implemented inadequately already in the planning phase ([BSI GS] T 2.45). This also opens unnecessary communication channels.

Accessing the Internet from the ICS network is also a threat. Using this channel, data can leak or malware can be downloaded.

Furthermore, ICS components can, for example, have connections in different levels of the example architecture (see 3) (so-called multi-homing). By means of these connections starting from one of the networks, a threat agent might be able to access another segment in an unauthorised manner (e.g. in the case of activated bridge or routing functionality). Possible security measures on the network level are thus bypassed.

3.2.2 Poor configurations of components

In the default configuration of software or components, security measures are not always activated. This makes it considerably easier for a threat agent to gain unauthorised access (see [BSI GS] T 3.28, T 3.38, T 4.49, T 4.53, T 4.70). If software or components are operated in an insecure configuration, they are also a security risk for other IT systems with a connection to this system.

The following examples illustrate possible, security-related threats of a default configuration:

- Unnecessary programs and activated services, if applicable, with known vulnerabilities,
- Default users and passwords,
- Deactivated security functions (e.g. firewall),
- Unprotected administration accesses.

3.2.3 Lack of backups

Regular backups and/or backups performed after changes were made allow prompt replacement of defective or failed components by importing the last backup on the new component. Operations can be resumed immediately in this manner.

During day-to-day operations, this backup is often not performed, and so there are no or outdated data for restoration when actually needed. Another problem can be the storage of the backups, which might not be in a central place, but in different and undocumented places. In some cases, there is also the lack of possibilities for the creation of backups and/or their restoration.

3.2.4 Portable media and laptops

Several administrative activities cannot be performed via remote maintenance access points (see chapter 3.1.3), which makes it necessary for a maintenance technician to come to the site. In this case, a maintenance technician uses portable media (e.g. USB sticks) or their own laptops which are connected to the ICS network or the affected ICS component.

There is the risk of malware being on these devices and that it spreads throughout the network or infects the component (see [BSI GS] T 5.23, T 5.142).

For example, the maintenance technician usually also uses the hardware in other ICSs and can thus distribute the malware among different plants. If there is malware on the hardware and if the maintenance technician connects the hardware to the ICS, malware can lodge itself on the hardware and is transported from one ICS to the other.

Malware (e.g. worms, viruses, Trojan horses) is any kind of software which was developed for the purpose of executing harmful undesired/unintended functions (among other things, data theft, deletion of data). Numerous infections caused by malware are already known in the ICS environment (see also chapter 3.1.4).

Furthermore, maintenance laptops have different communication interfaces (e.g. Ethernet, WLAN, Bluetooth, infrared, mobile phone networks such as UMTS). If, for example, there is already an Internet connection via UMTS and the laptop is connected to the ICS network at the same time, this is a network interconnection. This way, direct access from Internet into the ICS network is possible.

3.2.5 Inadequate validation of input and output

If applications receive input for processing or return data without checking it adequately for validity, a threat agent can be able, for example, to insert malicious code to be executed on the system (e.g. by means of buffer overflows) or force output in such a way that malicious code is transmitted by the application to the recipient (e.g. cross-site scripting in the browser). When developing applications, the validation of input and output data is often dispensed with (see [BSI GS] T 4.84). The same applies to proprietary development tools. Here, attention is often only paid to the functionality and error control routines are not taken into account (in most cases, due to lack of time).

This is a risk which must already be taken into consideration during the development and procurement phase.

3.3 Deliberate acts

Common to all of the following threats is the fact that the threat agents require less and less expertise in many cases. There are various tools available on the Internet which can be used for such purposes.

3.3.1 Communication of measured and values

The systems in ICSs communicate with each other using different network protocols and technologies. In addition to protocols and technologies from the office IT (e.g. Ethernet, TCP/ IP, WLAN, GSM), ICS-specific protocols are used. They have mainly been developed without taking security into account and therefore offer no or only limited security mechanisms.

The information transmitted is, for example, measured and control values. The transmission is often performed in plaintext and, in this case, is protected only insufficiently against manipulation. A threat agent with physical access to the ICS network is thus able to read or modify these values or to load new values (e.g. to control a machine or to forge sensor data; see [BSI GS] T 0.14, T 0.15, T 0.43, T 5.7, T 5.8, T 5.24).

If, for example, incorrect sensor data is faked by a threat agent, the operators of the system can no longer read reliable, sensor data and might be badly mistaken as to the actual system state. The manipulation of sensor data which is based on fully automatic control (closed-loop control) systems might result in incorrect control commands and can therefore have a direct impact on the process.

In the case of insecure wireless communications in particular, the transmitted data can be accessed easily. By means of deliberate overlaying, it is possible to install or modify data as well as to interfere with the entire communication.

This type of attacks can lead to three problems (see also chapter 3.3.4):

- Loss of view,
- Manipulation of view and
- Loss of control.

For example, sensor data (e.g. fill level, temperature, pressure) can be falsified to prevent shut-down or control operations and to influence the production process in this way. It could also be possible that production parameters (e.g. frequencies, rotations, duration of a welding process) are forged to cause production errors in a targeted manner. The incorrect production parameters might only be recognised during the quality control, since the parameters shown in the visualisation do not correspond to the parameters actually set by the threat agent.

Moreover, safety mechanisms might be triggered or interfered with (e.g. automatic shut-down when a pressure is exceeded or a fill level is fallen short of or automatic shut-down is suppressed).

3.3.2 Determining access data by means of dictionary and brute force attacks

If accessing systems requires authentication by means of access data, a threat agent can try to guess it. To do this, automated attack tools which try to determine passwords (see [BSI GS] T 5.18) based on different data are usually used.

In the case of a brute force attack, all possible combinations of characters are tested for the password (e.g. alphabet with numbers and special characters). Here, the effort increases exponentially with the length of the password. Therefore, a brute force attack is often very time-consuming and characterised by a large number of unsuccessful login attempts.

Due to the inefficient procedure in the case of a brute force attack with all possible combinations for a password, the data basis to determine the passwords is often limited to a defined dictionary. Such an attack is referred to as a dictionary attack. It is thus a version of a brute force attack. Contrary to the brute force attack described above, however, the success of a dictionary attack largely depends on the quality of the dictionary. Such dictionaries with frequently used passwords are therefore actively exchanged on the Internet.

Especially default access data (see chapter 3.2.2) and passwords that are insufficiently complex, trivial and too short can be determined by means of these attack techniques efficiently and within a short period of time (see [DUD 2009], [BSI 2008]).

3.3.3 Systematic search for vulnerabilities via the network

If a threat agent can access ICSs via the network, they can identify available services and determine any known, existing vulnerabilities by means of different techniques via the network. To do this,freely available programs which automate the process can be used.

Using a so-called port scan, the accessible services can be determined via the network (e.g. TCP and UDP scan). Afterwards, a so-called vulnerability scanner can check the identified services for vulnerabilities. For this purpose, test vectors which check the services for specific, known vulnerabilities (e.g. buffer overflows, SQL injection, broken authentication or improper session management (see [OWASP Top10]) are stored in vulnerability scanners.

3.3.4 Denial of service attacks (DoS)

Denial of service attacks pursue the goal of restricting the availability of systems or offered services. If, for example, a threat agent ties up resources through a large number of simultaneous requests in a targeted manner, it might no longer be possible for other users to access the component due to the load. This attack can also be carried out on the network level (e.g. overloading the transmission capacity) or on the application level by frequently executing resource-intensive operations. Moreover, exploiting software-based vulnerabilities (e.g. buffer overflow) may also result in the failure of the system or service and are thus used for a DoS attack (see [IX 2013], p. 64-67).

If the communication takes place via a wireless connection, a threat agent can interrupt it by targeted overlays.

The attack can also be performed via a distributed infrastructure, for example a bot network. In this case, it is referred to as a Distributed Denial of Service (DDoS).

3.3.5 Man-in-the-middle attacks

When conducting a man-in-the-middle attack (MitM attack), the threat agent takes a position between two communication partners in order to, for example, read or manipulate the transmitted data (see chapter 3.3.1 and [BSI GS] T 5.143). This can take place physically, e.g. by separating a line and the direct connection to the two communication partners or logically by feigning the identity of the respective other communication partner so that the threat agent is mistaken for the respective other partner.

In the ICS environment, ARP[2] spoofing in particular plays an important role as an MitM attack technique due to the common Ethernet use and communication via the IP protocol.

3.3.6 Phishing

In the case of a phishing attack, the threat agent pretends to be a trusted person or entity (e.g. administrator, colleague, ICS product suppliers) towards the user. They thus try to obtain information such as access data or to cause the user to perform certain actions (e.g. changing a configuration relevant for security, installation of malware in the e-mail attachment). The threat agent thus tries to exploit the user's trust relationships (see [BSI GS] T 5.157, T 5.158).

Usually, these phishing attacks are conducted using forged websites and sending e-mails or messages in social media. By sending these e-mails as bulk mails, phishing attacks can be extended to a large number of users.

In addition to the widely distributed sending of messages, there is a trend of conducting targeted attacks. Here, for example, information from public sources or social network is used to address the victims as

[2] Address Resolution Protocol

personally as possible. This increases the probability that the victim opens an attachment or clicks a link which refers to a website which is infected with malware.

3.3.7 Injection attacks

When carrying out an injection attack, a threat agent transmits prepared input data to an application and thus tries to execute commands. This mainly applies to processing services and is based on the poor validation of input data (see chapter 3.2.5). Examples include SQL injection attacks, in which specifically designed data is transmitted to a web application, and this data is intended to execute a command on the database. If the data is not checked adequately for plausibility, the contents in the database can be manipulated (see [BSI GS] T 5.174 and T 5.131), since they are interpreted as a command.

Other examples include LDAP[3] injection, mail command injection, OS command injection, SSI[4] injection, Xpath injection or code injection.

3.3.8 Cross-site scripting

Cross-site scripting attacks (XSS attacks) are directed against the users of a web application. Here, a threat agent tries to send malicious code (usually scripts such as JavaScript that can be run on the browser side) indirectly to the client of the user of the web application.

If the input and output data of a web application are not validated adequately (see chapter 3.2.5), then a threat agent can smuggle in malicious code into the web application (e.g. within a comment to an item) and so spread it. If an infected website is called up by the user, the client (for example, browser) executes the inserted malicious code. From the user's perspective, the malicious code comes from the web application and is thus classified as trusted. Therefore, the malicious code is interpreted within the security context of the web application and the threat agent is able to execute commands within the context of a possibly existing session of the affected user.

3.3.9 Drive-by downloads

Due to vulnerabilities in browsers and their extensions, only visiting a website which was prepared with malicious code can cause the computer to be infected with malware. This type of attack is called drive-by download (also referred to as drive-by exploit). No further interaction with the user is required in this case (see [BSI 2012]).

3.3.10 Malware on engineering workstations

Engineering workstations (EWSs) are used for the configuration and programming of ICS components. If the EWS is infected with malware:

- The programs on the PLC can be changed. This may result in changes in the presentation, additional control commands or the like. Thus, the threat agent can make changes to the production and/or automation process.
- The programs and processes on the PLC can be stolen and transmitted to the threat agent.

For threat agents, this attack vector is particularly valuable, since not only the PLC can be compromised and production can be disrupted. At the same time, the visualisation of the control state is influenced as intended by the threat agent. As a consequence, the operating personnel might not notice the impact of the attack,

[3] Lightweight Directory Access Protocol

[4] Server Side Includes

does not become suspicious and continues production unabatedly. Affected systems may then be sabotaged over a long period of time without being noticed.

3.3.11 Malicious software

In addition to the targeted infection with malware, versions which are actually aimed towards the enterprise IT can be responsible for damage in the ICS (collateral damage). This may result in crashes, changed run times or an increase in the network traffic which, in turn, cause failures. Possible ways of infection have already been described in 3.2.4, 3.3.6 or 3.3.9.

3.3.12 Replay attacks

If a threat agent can record the network traffic (e.g. the execution of a command with privileged rights), they might be able to perform the recorded action again in an unauthorised manner by re-installing this data in the network. This requires that the protocol used for data transmission cannot distinguish between data which is sent several times. In this case, data which has been transmitted legitimately for the first time cannot be differentiated from the copy of the previously transmitted data and rejected if necessary. This technique is referred to as replay attack.

The threat agent can thus put correctly formatted and also encrypted or signed data into circulation, which the recipient processes as authentic information, for example, without having to disable the encryption or find out a password beforehand.

For example, a switching command (e.g. activation of a pump) or the transmission of parameters (e.g. definition of a set temperature of a furnace) to an ICS component can be recorded by a threat agent and repeated at a later point in time at which damage is to be expected.

3.3.13 Physical attack to provoke administrative intervention

Depending on the area of application of the ICS installation, a threat agent can physically manipulate one of the components (e.g. external sensor or actuator) to provoke a response of the operating personnel. In this way, a threat agent can influence certain actions, such as the realisation of administrative activities, and exploit them afterwards, for example for conducting further attacks.

For example, a temperature sensor can be heated to trigger an alarm and, as a consequence, cause a certain response of the operating personnel. This is in the interest of the threat agent, for example, if they can assume that

- There is a maintenance access for which a password is transmitted insecurely (recording of the password at a network component),
- A control command (e.g. restart or emergency shut-down) which the threat agent needs for a subsequent replay attack is sent or
- An insecure remote maintenance access point is activated, because the provoked disruption requires the interventions of supplier staff and the threat agent can then use this access for themselves.

This attack vector therefore combines knowledge of the productive system itself with the existing vulnerabilities of ICS components.

A similar procedure is continuous alerting. The threat agent repeatedly triggers an alarm (e.g. interruption of a light barrier). If administrative intervention is required several times and if it is not possible to identify a cause, the operating personnel might assume a false alarm which was triggered by a malfunction, and the alarm is deactivated for the time being. In this way, the actual attack, which would trigger the same alarm, can be prepared.

4 Organisations, associations and their standards

This chapter provides an overview of national and international organisations as well as their standards and recommendations with regard to the subject of security in ICS. The focus is on the security-relevant standards; safety-specific standards are not included.

The objective, target groups, contents and areas of application of the standards and quasi-standards are shown in the overview.

4.1 International standards

4.1.1 ISO/ IEC

The International Organization for Standardization (ISO; http://www.iso.org) develops internationally applicable standards in all areas. Together with the International Electrotechnical Commission (IEC; http://www.iec.ch), which is responsible for the field of electrics and the electronics, and the International Telecommunication Union (ITU), which is responsible for the telecommunication sector, these three organisations are the World Standards Cooperation (WSC).

4.1.1.1 ISO/ IEC 27000 series regarding information security

The ISO/IEC 27000 [ISO/IEC 27000] series of standards is reserved for the subjects of information security. The series of standards is developed by the technical committee JTC 1 (joint technical committee) SC 27 (subcommittee) (see [ISO Standards 2013]).

The goal of the ISO/IEC 27001 is to define general requirements for an information security management system (ISMS) within a process approach. An ISMS is characterised by a risk management which aims at taking suitable technical and organisational measures against identified risks. The generic requirements can be applied to all organisations. They are mainly process-oriented and have a low technical level of detail [BITKOM/DIN 2007]. The target group of the ISO/IEC27001 and ISO/IEC 27002 are asset owners in particular in the ICS environment. Integrators and product suppliers can provide the information required for certification.

The ISO/IEC 27002 is part of the general guidelines and defines the framework and general principles for an ISMS in an organisation. It is used as a guide to implementing an ISMS and covers the following subjects:

- Risk assessment and response,
- Security policy,
- Organisation of information security,
- Management of the organisation's own assets,
- Personnel security,
- Physical and environment-related security,
- Operational and communication management,
- Access control,

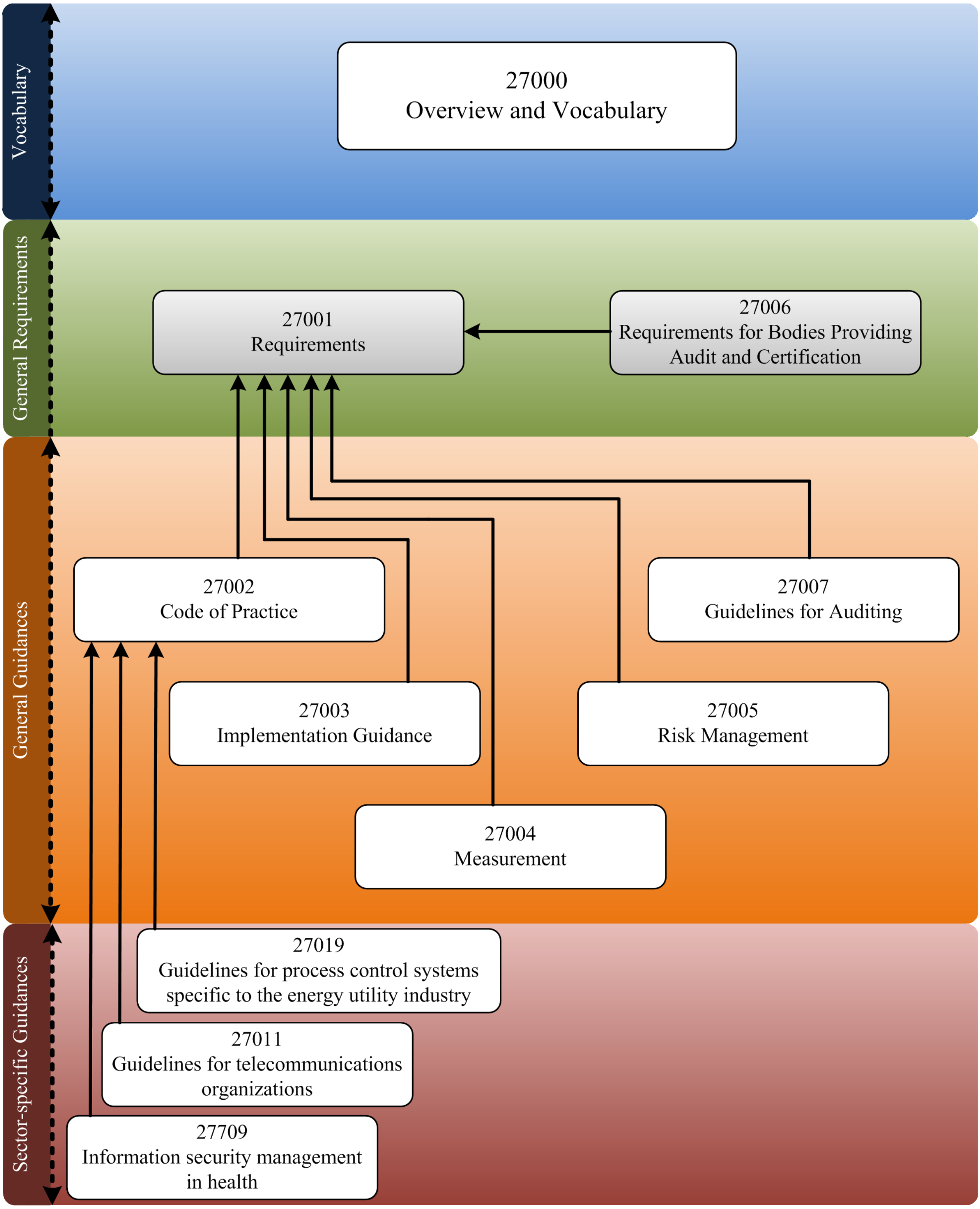


Figure 6: Structure of the ISO 27000 series of standards in accordance with ISO/IEC 27000:2012

- Purchasing, development and maintenance of information systems,
- Handling of information security incidents,
- Securing of business operations and
- Compliance with requirements.

Other general guidelines cover, fro example, the following subjects:

- ISO/IEC 27003: Implementation guidelines,
- ISO/IEC 27004: Measurements,
- ISO/IEC 27005: Risk management and
- ISO/IEC 27007: Audits.

Moreover, there are sector- and subject-specific guidelines, e.g. ISO/IEC 27011 "Information security management guidelines for telecommunications organizations based on ISO/ IEC 27002". These interrelations are shown in 6.

The national standard DIN SPEC 27009 (see chapter 4.2.1) was introduced by means of fast track at JTC 1 as ISO/IEC TR 27019 "Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy market" in June 2012. The English translation of DIN SPEC 27009 is adopted as ISO/IEC DTR 27019.

4.1.1.2 IEC 62443 – Industrial communication networks – Network and system security

The IEC 62443 series of standards is developed by the working group 10 of the technical committee 65 IEC TC 65 WG 10). The national mirror committee is the DKE UK 931.1 subcommittee at the German Commission for Electrical, Electronic & Information Technologies (DKE).

The IEC 62443 series of standards "Industrial communication networks – Network and system security" puts requirements for establishing security for industrial automation and control systems (IACSs). It covers functional requirements for automation solutions, systems and components as well as process-oriented procedural models for the operation, system integration and product development. The standard is written for product suppliers, integrators and asset owners.

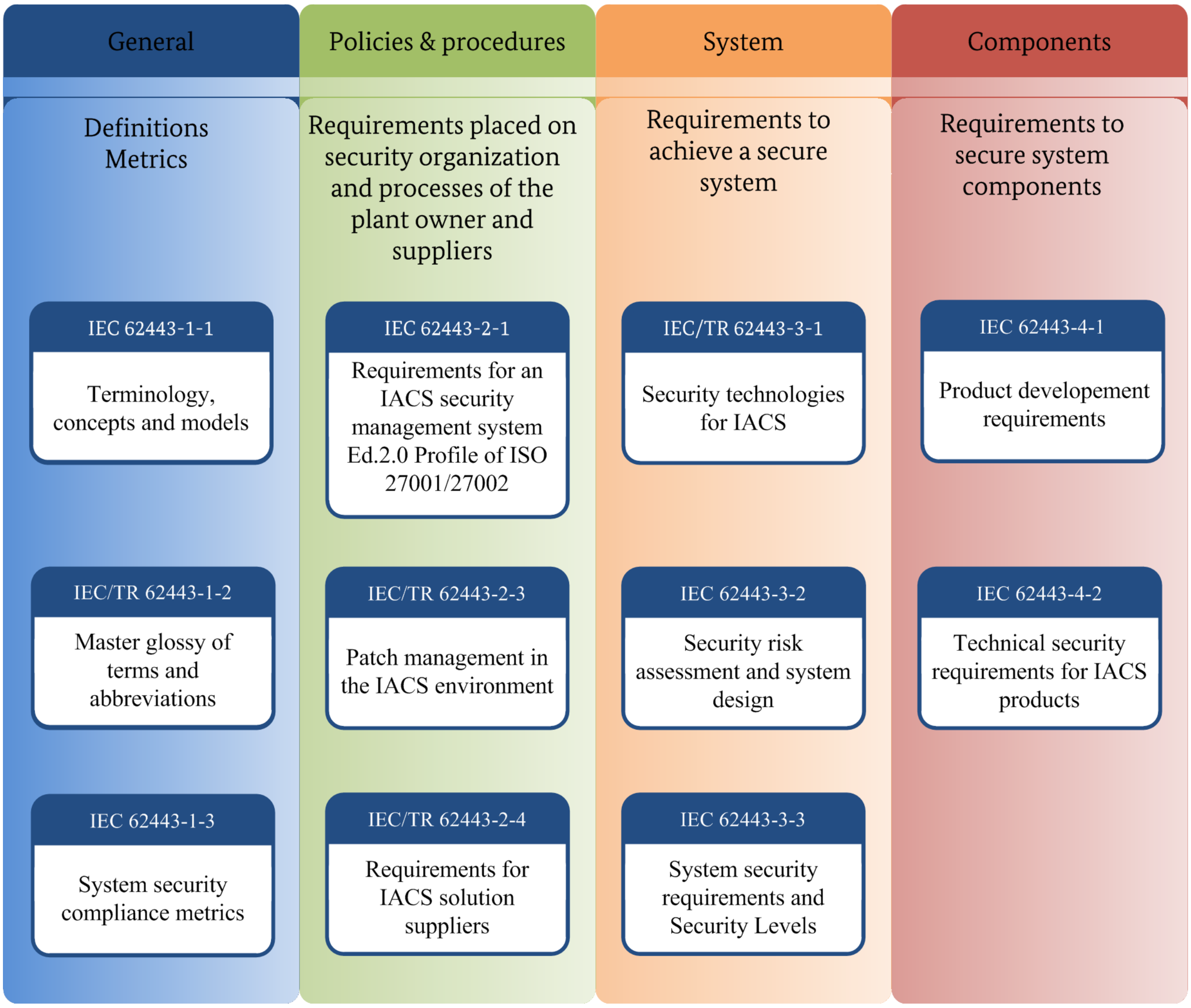

General
Policies & procedures
System
Components
Definitions
Metrics
Requirements placed on security organization and processes of the plant owner and suppliers
Requirements to achieve a secure system
Requirements to secure system components
IEC 62443-1-1
Terminology, concepts and models
IEC 62443-2-1
Requirements for an IACS security management system Ed.2.0 Profile of ISO 27001/27002
IEC/TR 62443-3-1
Security technologies for IACS
IEC 62443-4-1
Product developement requirements
IEC/TR 62443-1-2
Master glossy of terms and abbreviations
IEC/TR 62443-2-3
Patch management in the IACS environment
IEC 62443-3-2
Security risk assessment and system design
IEC 62443-4-2
Technical security requirements for IACS products
IEC 62443-1-3
System security compliance metrics
IEC/TR 62443-2-4
Requirements for IACS solution suppliers
IEC 62443-3-3
System security requirements and Security Levels

Figure 7: Overview of IEC 62443

The development of the IEC 62443 series of standards has been promoted together with the International Society of Automation (ISA) since 2009. It publishes standards, best practices and technical reports which define the procedures for the secure implementation of ICSs and for the assessment of security measures.

4.1.1.3 IEC 62351 – Power systems management and associated information exchange – Data and communication security

The IEC 62351 [IEC 62351] standard is developed by the working group 15 of the technical committee 57 (IEC TC 57 WG 15) and covers the securing of the communication protocols used in power engineering at the technical level. The goal is to develop security measures for communication protocols developed by IEC TC 57, especially for the IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970 and IEC 61968 series of standards. The standard primarily addresses the members of the working groups developing the corresponding communication protocols. Moreover, the product suppliers of products in which these communication protocols have been implemented are the target group of the standard 8 shows the structure of the standard and the reference to the different communication standards.

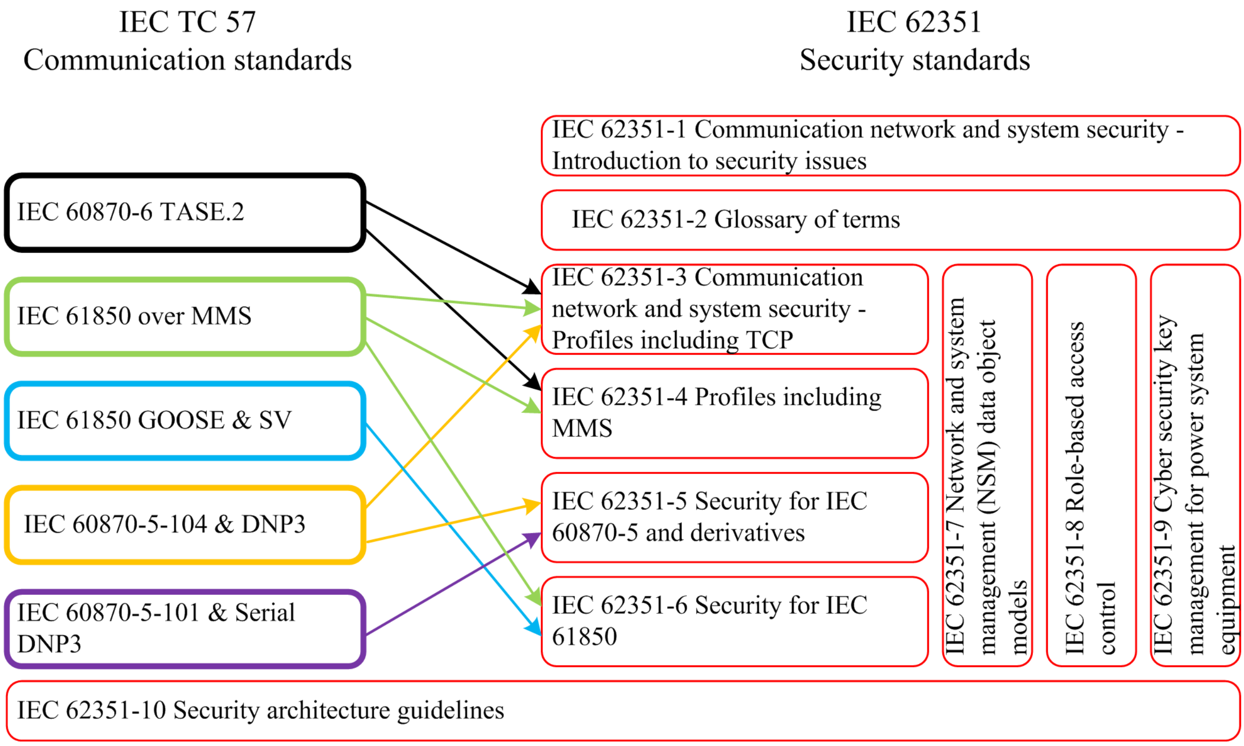

IEC TC 57
Communication standards
IEC 62351
Security standards
IEC 62351-1 Communication network and system security - Introduction to security issues
IEC 62351-2 Glossary of terms
IEC 60870-6 TASE.2
IEC 61850 over MMS
IEC 61850 GOOSE & SV
IEC 60870-5-104 & DNP3
IEC 60870-5-101 & Serial DNP3
IEC 62351-3 Communication network and system security - Profiles including TCP
IEC 62351-4 Profiles including MMS
IEC 62351-5 Security for IEC 60870-5 and derivatives
IEC 62351-6 Security for IEC 61850
IEC 62351-7 Network and system management (NSM) data object models
IEC 62351-8 Role-based access control
IEC 62351-9 Cyber security key management for power system equipment
IEC 62351-10 Security architecture guidelines

Figure 8: Assignment of the IEC 62351 parts to protocols and standards (taken from [Cleveland 2012])

4.2 National standards and recommendations

4.2.1 DIN

The Deutsche Institut für Normung e. V. (DIN, http://www.din.de) is the best known national organisation for standardisation in Germany.

4.2.1.1 DIN SPEC 27009 - Guidance for information security management of power supply control systems based on ISO/IEC 27002

DIN SPEC 27009 describes a guide to implementing a sector-specific information security management system in the same way as ISO/IEC 27001 for power system control applications in the power supply sector. The measures from the ISO/IEC 27002 were supplemented by sector-specific requirements.

At the DIN, it is maintained by the standards committee (NA) 043 "Informationstechnik und Anwendungen" [Information Technology and Applications] (NIA) in the working committee NA 043-01-27-01 AK - "Anforderungen, Dienste und Richtlinien für IT Sicherheitssysteme" [Requirements, Services and Policies for Security Systems] (see [DIN SPEC 27009 2013]).

The standard is primarily written for asset owners of energy supply process control systems as well as for the competent persons responsible for information security. Furthermore, the standard is of interest to product suppliers, integrators and auditors. The standard focuses on systems and networks for the control and monitoring of the generation, transmission and distribution of power, gas and heat in combination with controlling supporting processes. This includes

- The distributed control and automation systems,
- The security and safety systems as well as

- The measuring technology including the related communication and remote control technology.

Collectively, these systems are referred to as process control systems [DIN SPEC 27009 2012]. The structure of the DIN SPEC 27009 is similar to that of the ISO/ IEC 27002 [TeleTrusT 2012]:

1. If the measures (controls) are applied as they are, the corresponding ISO/IEC 27002 section is referred to.
2. If the corresponding measures are supplemented, the original ISO/ IEC 27002 content applies with additional specific contents in the categories
    1. Implementation guidance for the power supply sector
    2. Additional information for the power supply sector
3. Additional measure objectives and controls were integrated into the corresponding ISO/IEC 27002 chapters.
4. In the appendix, the BDEW white paper (see chapter 4.2.4.1) is referred to and the measures of the DIN SPEC 27009 are compared to the corresponding security requirements of the white paper.

DIN SPEC 27009 covers the following contents. In addition, the number of sector-specific supplements as compared to ISO/IEC 27002 is provided:

- Chapter 5 – Security policy: no supplements,
- Chapter 6 – Organisation of information security: 5 supplements,
- Chapter 7 – Management of the organisation's own assets: 3 supplements,
- Chapter 8 – Personnel security: 3 supplements,
- Chapter 9 – Physical and environment-related security: 11 supplements,
- Chapter 10 – Operational and communication management: 9 supplements,
- Chapter 11 – Access control: 6 supplements,
- Chapter 12 – Purchasing, development and maintenance of information systems: 2 supplements,
- Chapter 13 – Handling of information security incidents: no supplements,
- Chapter 14 – Securing of business operations: 2 supplements and
- Chapter 15 – Compliance with requirements – 1 supplement.

4.2.2 VDI, VDE and DKE

The Association of German Engineers (Verein Deutscher Ingenieure e.V., VDI; http://www.vdi.de) is an association of engineers, scientists and information scientists in Germany, which supports standardisation, among other things. The German Association for Electrical, Electronic & Information Technologies (Verband der Elektrotechnik Elektronik Informationstechnik e.V., VDE; http://www.vde.com) is a technical and scientific association in the field of electrical and electronic technologies.

The German Commission for Electrical, Electronic & Information Technologies (Deutsche Kommission Elektrotechnik Elektronik Informationstechnik, DKE) in DIN (see chapter 4.2.1) and VDE develops standards in the field of electrical, electronic and information technologies. The DKE (http://www.dke.de) is supported by the VDE and is a standards committee in DIN. The DKE is also a member of the IEC and CENELEC. Furthermore, the DKE is the German national standardisation organisation (NSO) of the European Telecommunications Standards Institute (ETSI).

4.2.2.1 VDI/ VDE – Technical Rule 2182 IT-security for industrial automation

In Technical Rule 2182, the VDI and the VDE describe a procedural model for the implementation of specific security measures using practical examples. Due to the process-oriented, cyclic approach, the entire life cycle and the collaboration of product suppliers, integrators and asset owners are taken into account. This applies particularly to the exchange of information between the three parties.

The Technical Rule was developed by the technical committee FA 5.22 "Security" of the VDI/VDE-Society for Measurement and Automatic Control (GMA) and consists of six parts. In Part 1 "IT-security for industrial automation - General model", the basic procedure is explained. It covers the following contents:

- Scope,
- Terms and definitions,
- Method,
  - Dependencies,
  - Roles,
  - Structure analysis,
  - Trigger,
  - Documentation and
- Procedure description [VDI 2182 2011].

In addition to the interlocking of the three life cycles, an important aspect was the downsizing of ISO 27000 and IT-Grundschutz approaches when drafting the Technical Rule. Figure 9 graphically shows the procedure description (see [VDI 2182 2011]).

Examples of use from different perspectives of the product suppliers, integrators and asset owners are explained in the following parts (see [VDI/VDE Richtlinien 2013]):

- VDI/VDE 2182 Part 2.1 IT-security for industrial automation - Example of use of the general model for device manufacturer in factory automation - Programmable logic controller (PLC),
- VDI/VDE 2182 Part 2.2 IT-security for industrial automation - Example of use of the general model in factory automation for plant and machinery installers - Forming press,
- VDI/VDE 2182 Part 3.1 IT-security for industrial automation - Example of use of the general model for manufacturers in factory automation - Process control system of an LDPE plant,
- VDI/VDE 2182 Part 3.2 IT-security for industrial automation - Example of use of the general model for integrators in process industry - LDPE[5] reactor,
- VDI/VDE 2182 Part 3.3 IT-security for industrial automation - Example of use of the general model for plant managers in process industry - LDPE plant.

[5] Low-Density Polyethylene

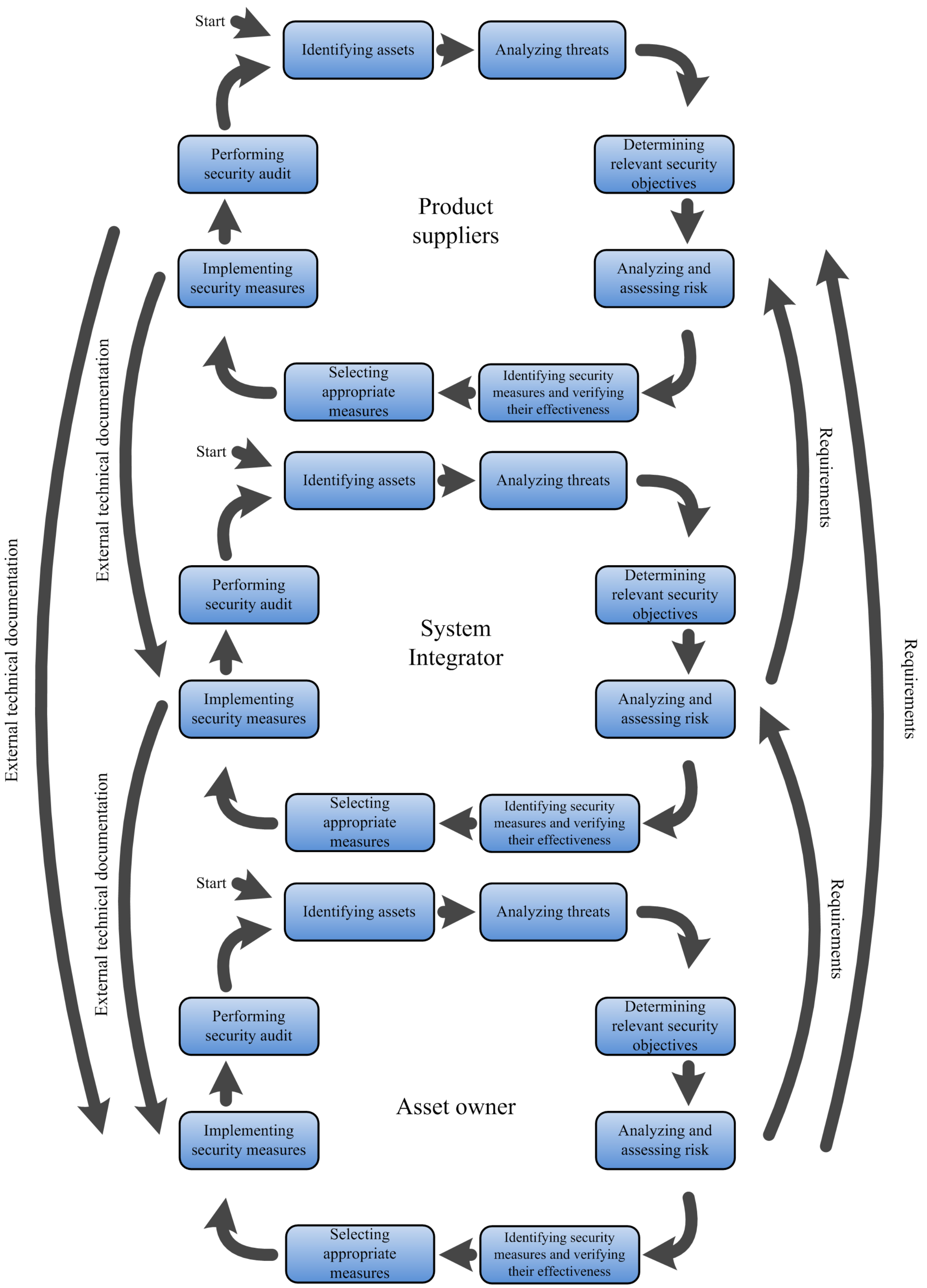

Start
Identifying assets
Analyzing threats
Determining relevant security objectives
Analyzing and assessing risk
Identifying security measures and verifying their effectiveness
Selecting appropriate measures
Implementing security measures
Performing security audit
Product suppliers
Start
Identifying assets
Analyzing threats
Determining relevant security objectives
Analyzing and assessing risk
Identifying security measures and verifying their effectiveness
Selecting appropriate measures
Implementing security measures
Performing security audit
System Integrator
Start
Identifying assets
Analyzing threats
Determining relevant security objectives
Analyzing and assessing risk
Identifying security measures and verifying their effectiveness
Selecting appropriate measures
Implementing security measures
Performing security audit
Asset owner
External technical documentation
External technical documentation
External technical documentation
Requirements
Requirements
Requirements

Figure 9: Procedures according to VDI/VDE 2182 in accordance with [VDI 2182 2011]

4.2.3 NAMUR

The Normenarbeitsgemeinschaft für Meß- und Regeltechnik in der chemischen Industrie (NAMUR, http://www.namur.de) is an international user association of automation technology in process industries. The association's activities include, among other things, participating in national and international standardisation.

4.2.3.1 NA 115 IT-Security for Industrial Automation Systems

In 2006, NAMUR published Worksheet 115 [NA 115 2006] which describes the framework conditions of automation engineering for security products from the user's perspective. On the one hand, the Worksheet is written for product suppliers who should take the specific framework conditions in the process industry into account when drafting new systems. On the other, integrators should implement security mechanisms according to these conditions. Furthermore, users should use the criteria from the document as a basis for future purchasing decisions. After the security objectives of conventional IT and the automation engineering have been distinguished, basic measures for the securing of existing systems are discussed. In the next chapter, the most important requirements for the development of future systems are explained. The individual criteria are formulated in a concise and generally valid manner.

4.2.4 BDEW

Approx. 1,800 enterprises are organised in the Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW, http://www.bdew.de) [German Association of Energy and Water Industries]. It represents the interests of its members to political representatives, experts, the media and public.

4.2.4.1 BDEW white paper "Requirements for Secure Control and Telecommunication Systems"

For power industry enterprises and organisations, a white paper specifying essential security measures for control and telecommunication systems with regard to ISO/IEC 27002 (see chapter 4.1.1) was published in 2008. The goal is to protect the systems adequately against security threats in daily operations. The security measures defined in the white paper are recommended for all new control or telecommunication systems. The aim of the white paper is to have a positive effect on product development regarding security aspects and to establish a common understanding in the industry sector for the protection of these systems. Security requirements are defined both for the asset owner and for the product supplier.

During the planning phase of a new control or telecommunication system, the protection requirements must be determined as early as possible. The process of determining the protection requirements is described, for example, in [BSI 100-2]. If this determination process results in normal protection requirements, it is sufficient to implement the requirements of the white paper. In the case of high or very high protection requirements, a supplementary risk analysis must be carried out.

The white paper focuses on requirements for systems and components as well as on the corresponding development and maintenance processes. The white paper is primarily provided for tendering procedures. After the end of the planning phase the determined final security requirements are integrated into the requirements specification with the following documents:

- A copy of the current white paper,
- If necessary, detailed requirements and additional measures as well as implementation requirements arising from the results of the risk analysis,
- The tolerable exceptions or workarounds [BDEW 2008].

Security requirements are defined for the following subjects:

- General information/organisation,
- Base system,
- Networks/communication,
- Application,
- Development, test and rollout as well as
- Backup/data restoration and contingency planning.

4.2.4.2 Requirements for Secure Control and Telecommunication Systems – BDEW White Paper

In 2012, Oesterreichs Energie (http://oesterreichsenergie.at) and the BDEW (https://www.bdew.de) have jointly published a practical guide for the white paper "Anforderungen an sichere Steuerungs- und Telekommunikationssysteme” [Requirements for Secure Control and Telecommunication Systems]. The goal of these *Ausführungshinweise* [English equivalent would be "implementation instructions", since there is no official English translation of this document] is to provide implementation examples and application instructions for the individual requirements of the BDEW white paper with respect to the different technology areas in the field of process control in the power supply sector. The *Ausführungshinweise* are used as a supplement to the requirements of the BDEW white paper [OE BDEW 2012].

4.2.5 VGB

The VGB PowerTech e.V. (http://www.vgb.org) is a European technical association for power and heat generation and a voluntary association of companies for which power and heat generation and thus the power plant operation and the related technology are an important basis.

4.2.5.1 Guideline R175: IT Security for Generating Plants

The VGB guideline published in 2006 [VGB R 175] is intended to provide power plant operators with information and recommendations to improve security. The introductory chapters explain basic terms in the field of security and describe typical threats arising from the operation of power plants. To counter these threats, a collection of best practices resulting from organisational and technical measures is provided in the chapters below. The individual measures are described in different levels of detail.

At the moment, the guideline is revised by a VGB working group. After its revision, it will probably be published with the title VGB – Standard S175 IT Security for Generating Plants.

4.3 Foreign recommendations

This section includes ICS-specific recommendations from several countries. They can be used as source of information. When implementing the measures described there, the different regulatory requirements in these countries and in Germany must be observed. To implement these recommendations and measures in Germany, adjustments may therefore be necessary to comply with the law. Foreign recommendations should thus be considered as supplementary sources of information which do not have a normative character for Germany.

4.3.1 NERC

The North American Electric Reliability Corporation (NERC, http://www.nerc.com) is responsible for the coordination of the electrical power supply systems and the securing of the electrical power supply in North America.

4.3.1.1 NERC CIP: Cyber Security Standards Critical Infrastructure Protection

The Cyber Security Standards are developed by the NERC to protect critical infrastructures with the aim of securing electrical power supply. With the confirmation of the Federal Energy Regulatory Commission (FERC) in 2006, this Critical Infrastructure Protection (CIP) series became mandatory for the users and asset owners of power supply systems in the USA, Canada and parts of Mexico. The CIP standards consist of several documents with requirements and security measures with respect to different subjects and are updated on a regular basis. This means that there are various revisions of each standard. The standards cover the following subjects [NERC CIP]:

- CIP-001 Sabotage Reporting
- CIP-002 Cyber Security - Critical Cyber Asset Identification
- CIP-003 Cyber Security - Security Management Controls
- CIP-004 Cyber Security - Personnel & Training
- CIP-005 Cyber Security - Electronic Security Perimeter(s)
- CIP-006 Cyber Security - Physical Security of Critical Cyber Assets
- CIP-007 Cyber Security - Systems Security Management
- CIP-008 Cyber Security - Incident Reporting and Response Planning
- CIP-009 Cyber Security - Recovery Plans for Critical Cyber Assets.

Each standard is basically divided into five sections, which are introduction, requirements, measures, compliance and regional differences. The documents have a fixed structure which is characterised by enumerations.

4.3.2 NIST

The National Institute of Standards and Technology (NIST, http://www.nist.gov) is a federal authority of the United States of America and, among other things, responsible for standardisation.

4.3.2.1 SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations

In the draft of the Special Publication 800-53 Rev. 4 [SP 800-53] from 2012, the NIST describes security mechanisms for the security of information systems of the US authorities. The aim is to support the US authorities in selecting and implementing adequate security mechanisms by means of a risk management which takes the organisation, process and information level into account. The defined and recommended security measures from the document are thus intended to be implemented as part of a risk management process. In Appendix I, specific ICS security mechanisms are explained.

4.3.2.2 SP 800-82 Guide to Industrial Control Systems Security

With the Special Publication 800-82 [SP 800-82] from 2011, the NIST provides terms and definitions as well as best practices for the implementation of security measures to ensure the secure operation of ICSs and is thus written for asset owners and integrators. After the general terms have been defined and the functions of ICS components described, typical threats and vulnerabilities of ICSs are explained. To counter the resulting risks, the steps required to develop an ICS security program are described on the basis of a business case. In the following chapters, possible security measures are listed with references to more detailed NIST documents. The security measures sometimes include technically very specific recommendations, such as with respect to protocol-specific firewall settings.

4.3.2.3 NIST IR 7628 Guidelines for Smart Grid Cyber Security

With the conversion of the power transmission grid into an electronic smart grid, significant changes to the infrastructure are planned. The conventional electrical grid is to be converted into a decentralised, digital infrastructure which allows two-way communication for the transmission of information and for the control of the ICS components as well as of the distribution of power. The Guidelines for Smart Grid Cyber Security [NISTIR 7628] from 2010 provide the organisations involved, such as grid operators and product suppliers of electric vehicles and charging stations, with an analytical framework in a three-part report. Using this framework, effective security strategies which are tailored to smart grid characteristics, risks and vulnerabilities of the specific area of application are to be developed.

4.3.3 DHS

The main task of the United States Department of Homeland Security (DHS, http://www.dhs.gov) is to protect the American population and territories against terrorist and other threats.

The most important DHS publications as part of the Control Systems Security Program (CSSP) are explained below. Best practices and recommendations for securing ICS plants can be found at http://us-cert.gov/control_systems/practices/Recommended_Practices.html.

4.3.3.1 Cyber Security Procurement Language for Control Systems

The Cyber Security Procurement Language [DHS CSPL 2009] of the DHS from 2009 serves the asset owners of automation and control technology as a basis for tenders. The focus is on the security features which the systems of the product suppliers must comply with. The long-term aim is to integrate security into the automation and control technology life cycle. In the document, examples of tender texts which asset owners can derive specific requirements from are provided for basic security features (e.g. system hardening, auditing and logging, firewall) of ICS components. These examples are to be integrated into the contacts entered into between the contract partners and are to ensure an adequate security level in automation and control technology.

4.3.3.2 Cyber Security Assessments of Industrial Control Systems

The Good Practice Guide "Cyber Security Assessments of Industrial Control Systems" [DHS Assessment 2010] of the DHS and CPNI (see chapter 4.3.4) from 2010 points out the particularities of a security assessment in ICS environments. Furthermore, a methodology and a procedural model for performing an ICS security assessment are presented for asset owners. After a brief introduction to the differences between conventional penetration tests and an ICS assessment, a procedure and the process of such an ICS assessment with the individual, required phases are explained. In this respect, the aspect of reporting with specific examples is an integral part of the chapter. The dependencies and possible influencing factors which determine the scope and type of the assessment (e.g. existing source text, budget) are explained briefly below. Finally, different assessment methods (e.g. interviews, checking of documents, technical tests in the production environment or test environment) are presented and discussed.

4.3.3.3 Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies

The "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies" [DHS DiD 2009] of the DHS from 2009 provides asset owners and integrators with assistance in developing a holistic defence strategy. Based on well-known vulnerabilities, the possible solutions are shown. The "Defense-In-Depth" paradigm of structuring the security of the system in different layers and thus making it more difficult for a threat agent to penetrate the systems is explained.

4.3.3.4 Recommended Practice for Patch Management of Control Systems

The "Recommended Practice for Patch Management of Control Systems" [DHS PM 2008] of the DHS from 2008 is to give asset owners assistance in developing a patch management program for automation and control technology. In this respect, the DHS recommends best practices for the patch management and their implementation in automation and control technology. After a brief overview of the main elements of a patch management program (e.g. patch management plan, patch testing), methods on the basis of which vulnerabilities and the resulting risk can be assessed are presented. Possible need for action can then be derived from the determined risk level.

4.3.3.5 Recommended Practice for Securing Control System Modems

On the one hand, the "Recommended Practice for Securing Control System Modems" [DHS Modem 2008] of the DHS from 2008 describes methods and tools to identify and analyse modem connections. On the other hand, mainly technical measures are recommended to secure modem connections.

4.3.3.6 Configuring and Managing Remote Access for Industrial Control Systems

The document "Configuring and Managing Remote Access for Industrial Control Systems" [DHS Remote 2010] of the DHS and CPNI (see chapter 4.3.4) from 2010 provides asset owners and integrators with recommendations on how to secure ICS remote access points. The roles involved are defined and the risks explained by using examples. Moreover, measures for the securing and operation of remote access points are described.

4.3.3.7 Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments

The draft "Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments" [DHS ZigBee 2007] of the DHS from 2007 is intended to support asset owners and integrators in the secure installation and operation of ZigBee wireless networks in the ICS environment. The document has been written from a technical point of view and, in addition, to basic information on the wireless standard, covers essential design principles and best practices as well as the available security mechanisms. Here, the particularities in the ICS environment with possible solutions are referred to in a separate chapter.

4.3.3.8 Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability

In the DHS publication "Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability" [DHS IR 2009] from 2009, asset owners of ICS plants are guided in the development of processes for the handling of security incidents. In this publication, the DHS gives recommendations on how asset owners of ICS plants can prepare themselves for and respond to security incidents. For example, this includes the analysis of the incident and the restoration of the operating environment after security incidents have occurred. The contents are quite general so that further literature is referred to in many cases, highlighting particularities of ICSs.

The document is divided into the following four main chapters:

- Cyber Incident Response Planning,
- Incident Prevention,
- Incident Management and
- Postincident Analysis and Forensics.

4.3.3.9 Catalog of Control Systems Security: Recommendations for Standards Developers

Since sector-specific standards are not always mutually consistent and comparable due to their focus areas, for example, with respect to the level of detail, this comprehensive DHS catalogue [DHS Standards 2009] from 2009 tries to offer a selection of proven, sector-independent security measures for ICSs which make the differences between the standards clear. The catalogue is aimed at supporting standardisation bodies in developing sector-specific standards. Moreover, the catalogue is intended to provide asset owners of ICSs with an framework for the development of a cyber security program. The measures from the catalogue should be taken into account when implementing best practices, guidelines and standards for ICSs.

4.3.3.10 Using Operational Security OPSEC to Support a Cyber Security Culture in Control Systems Environments

The draft in Version 1.0 [DHS OPSEC 2007] of the DHS from 2007 addresses managers and security specialists who are to be supported in developing an operational security (OPSEC) program for automation and control technology. By applying methods from operational security, processes and policies which increase security in daily operations and promote a culture for cyber security are to be developed. In this respect, essential cyber security key elements of automation and control technology (e.g. access control, risk assessment, compliance) are described briefly. The document covers the subjects on an abstract level and thus does not replace any sector-specific security standards.

4.3.3.11 Personnel Security Guidelines

The aim of the DHS "Personnel Security Guidelines" [DHS Personnel 2004] from 2004 is to provide assistance when selecting and preparing personnel and raising their awareness. For this purpose, specific measures which are intended to prepare the personnel adequately for their work in an ICS enterprise and raise the required awareness for security are listed. Operation-specific measures can be derived from these recommendations. The recommendations regarding personnel-related security is divided into the following three topics:

- Trustworthiness,

- Capability and
- Secure Environment.

The suggested measures are provided as concise requirements and, in many cases, supplemented by lists with examples or aspects to be taken into consideration. In this respect, different legal framework conditions between the USA and Germany must be taken into account if applicable.

4.3.4 CPNI

The Centre for the Protection of National Infrastructure (CPNI, http://www.cpni.gov.uk) is an authority of the United Kingdom with the task of protecting critical infrastructures. To achieve this, recommendations regarding physical and personnel security as well as cyber security are given.

4.3.4.1 Good Practice Guide – Process Control and SCADA Security

With the Good Practice Guide from 2008 [CPNI 2008], the CPNI aims at providing asset owners of ICSs with proven, fundamental security principles for control technology. For this purpose, a framework including the following seven subject areas is presented:

- Understand the business risks,
- Implement secure architecture,
- Establish response capabilities,
- Improve awareness and skills,
- Manage third party risks,
- Engage projects,
- Establish ongoing governance.

For each subject area, there is a separate document in which recommendations are given in an abstract form and the respective basic principles for application are explained.

4.3.4.2 Good Practice Guide – Firewall Deployment for SCADA and Process Control Networks

In the Good Practice Guide [CPNI 2005] published in 2005, the CPNI makes recommendations for firewall architectures, the configuration and the management of firewalls for securing ICSs and is thus addressed to asset owners. In this respect, the different firewall components and technologies are described and the fundamental architectures compared to each other and assessed. Moreover, information for a secure firewall rules is provided, solutions for possible problem cases are suggested and basic activities for the management of the components described up to the protocol level.

4.3.5 IEEE

The Institute of Electrical and Electronics Engineers (IEEE; http://www.ieee.org is the world's largest professional association of engineers and information scientists.

4.3.5.1 IEEE 1686-2007 - IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities

The IEEE standard defines security functions which are to be made available by IEDs. The standard is aimed at product suppliers of IEDs.

5 Best Practice Guide for Asset Owners

This chapter provides an overview of several architectural, technical and organisational best practices for the asset owners of ICS. These best practices are a collection of reasonable measures which have proven to be successful in practice on the one hand and, on the other, can be derived from the existing standards ISO 27000/IT-Grundschutz, IEC 62443 and VDI 2182. They are put into relation to the best practices.

The explanations in this chapter cover the aspects as widely as possible. Therefore, there are no detailed technical descriptions.

At this point, it should be emphasised that the best practices described here are only intended to give an introduction to an organised security process within an ICS and/or an entire enterprise. The goal should be to establish a functioning information security management on the basis of ISO 27000, IT-Grundschutz or IEC 62443.

When implementing the measures described, it must be ensured that the following measures in particular should be implemented first:

1 Establishment of a security organisation

2 Creating and maintaining the documentation

3 Establishing a security management

4 Network plan

5 List of IT systems and installed applications

6 Administration and user manuals

They are used to gain an overview of the organisation's own systems and the infrastructure, to define responsibilities and to become aware of the existing risks. To collect inventory data, the methodology described in chapter 6 can also be used for audits, since many of the relevant questions are addressed there.

The risks and the security measures derived from them are specific to each individual ICS installation. Due to previous experiences with the ICSs, however, there are still best practices the implementation of which is suitable to increase the security level of the ICS and cope with the current threat scenario. For the appropriate selection and implementation of the measures, however, an individual risk analysis is absolutely necessary (see chapter 1.2).

Implementing all measures without taking the existing risks into consideration may lead to measures which are not necessary being implemented or the threats not being considered.

When implementing the measures, the size of the company and the organisational form may also result in specific deviations or in the decision that a measure will not be implemented. Here, the costs, benefit and remaining risk must be weighed up. However, this should be a conscious decision with the consequence that the remaining risks are explicitly taken.

With this procedure, it should be ensured that first a defined process is established for the subject of security. Afterwards, there should be suitable perimeter protection and multi-layer security measures should be taken on the network level. Then, the protection at the components themselves should be improved. In the case of new plants, this should already be taken into account in the planning phase.

In the following sections from 5.2, the best practices are grouped in terms of content and numbered.

5.1 General procedure in the engineering process

Since large parts of ICSs can be designed individually according to the requirements of the respective material production process, the related engineering processes are of critical importance. General procedures are laid down in international standards such as IEC 62337 (milestones) or IEC 62382 (loop check).

Furthermore, there are application-specific requirements, such as EN 50156 (furnaces), EN 61511 (the process industry sector systems) or EN ISO 13849 (machinery) for the design of engineering processes for the field of security technology.

In the field of security, IEC 62443 provides information on security aspects with regard to ICSs. Moreover, there are sector-specific determinations in the form of the BDEW white paper "Requirements for Secure Control and Telecommunication Systems" (chapter 4.2.4.1) and the VDI/VDE 2182 "IT-security for industrial automation" (chapter 4.2.2.1).

The basic tenor of these documents with respect to security is as follows:

1. Defining which units under consideration are to be examined and which threats are relevant to the respective units under consideration.

   Example:

   > If a plant is equipped with a crane for performing maintenance work, it must be checked if and to what extent the crane control must be examined with respect to security.

   It must be specified which threats are relevant to an application. An ICS application without remote maintenance access, for example, does not have to be assessed regarding possible consequences in this respect. However, it must be ensured that, for example, the temporary setup of such an access is examined directly prior to its setup at the latest.

2. Defining which risks can be derived from the threats

   The undesired publication of process data in a pharmaceutical application, for example, must be assessed differently than in a sewage treatment plant.

3. Defining which measures are (can be) taken for countering risks

   When defining these measures, the economically reasonable framework and, especially in the case of existing plants, the technically feasible measures must be defined. If necessary, a specific iteration process is required to coordinate wishes, resulting requirements and necessary measures.

   Example:

   > From a functional point of view, many ICSs do not require a permanent Internet or Intranet connection. Dispensing with this connection can help to minimise security risks.

4. Implementing these measures on all levels of the ICS (defence in depth)

   The measures taken must be implemented on all levels of the ICS. Here, the effectiveness of the complete package depends both on the individual measures and on their staggered structure.

5. Checking the compliance with and effectiveness of the taken measures at regular intervals

   The goal of these checks (audits) is to ensure that, on the one hand, the measures taken are complied with throughout the entire service life of an ICS. On the other, it must be verified that the measures taken are sufficiently effective. These checks are particularly important with respect to the security of ICSs, since the threat scenarios in this context can often change.

VDI/VDE 2182 describes a comprehensive process in addition to the type and scope of the exchange of information and the entities to be involved (product suppliers of devices, system integrators and asset owners).

5.2 First steps

1. Establishment of a security organisation

The asset owner should establish a security organisation which manages and controls the roles and responsibilities for the security of ICS components. The security organisation should take into account all parties involved in the operation of ICS components (e.g. product suppliers, outsourcing partners, third-party vendors, specialists for physical security, production and maintenance managers).

The management should commit to the security program.

Persons responsible should be appointed for plants and components. It has proven useful to appoint persons responsible for specific system groups or network areas, for example, divided into the individual management levels (see 3).

There should be close cooperation between the ICS and the security experts to mutually benefit from each other, pursue a common objective and avoid planning mistakes.

2. **Creating and maintaining the documentation**

Documents and information on the security of ICS components (e.g. risk and vulnerability analyses, network plans, network management, configuration, security program and organisation) should be included in the requirements for solution providers, created, maintained and protected adequately against unauthorised access (if necessary, by encryption).

In a security policy regarding document management, a process should describe the life cycle of the documents. This includes the classification, maintenance, archiving and destruction of the documents. Consequently, the confidentiality levels for the classification of these documents should, for example, also be defined in the security policy (e.g. public, restricted, confidential).

It should be checked at regular intervals if the security policy is up-to-date. If necessary, it must be revised.

3. **Establishing a security management**

An information security management system (ISMS) should be established for the operation of the ICS. The goal of an ISMS is to permanently control, check, maintain and continuously improve information security.

In this respect, the most important task is the risk management. This includes taking all functional and security-specific components of an ICS into account. Within the framework of the risk management, comprehensive considerations regarding the security design, prioritisation of security measures and assessment of residual risks are made.

For the integration into an already existing ISMS, the technical particularities of an ICS must be taken into account. Applying the requirements from the office IT without reflection does not lead to the desired results due to the specific framework conditions and cannot be implemented in most cases.

Requirements and information with regard to the structure of an ISMS and risk analysis can be found, for example, in [VDI 2182 2011], [IEC 62443], [ISO/IEC 27000] and [BSI GS].

4. **Network plan**

The structure of the network should be documented in a physical and a logical network plan. The physical plan shows the locations and the infrastructure of the ICS, e.g. cables, building, wireless communications. The plan should at least include:

- IP network addresses and net masks, e.g. 192.168.1.0/24,
- IP addresses of all connected network interfaces, e.g. 192.168.1.54,
- MAC addresses,
- Computer name and functionality of the systems,
- (If any) DNS name,
- (If any) FQDN (FullyQualifiedDomainName) and
- The technical documentation should be updated and maintained throughout the entire life cycle (starting with the requirements for suppliers and planners).

The logical network plan does not describe the physical conditions, but focuses on the structure and the security zones.

5. List of IT systems and installed applications

To avoid incompatibilities and inconsistencies of software in specific versions as well as configurations (e.g. IP address conflicts), the configuration of the individual ICS components should be documented in a list. Furthermore, ICS components can thus be identified quickly if new updates are available or configuration changes are required. Even if updates are not possible, the potential state of being affected can be assessed on the basis of such a list in a timely manner.

The list can document, for example, the following properties:

- Functional name,
- Computer name,
- Responsible administration personnel with stored contact data (if necessary, also service times),
- Physical installation site,
- MAC address(es),
- IP address(es),
- DNS designation,
- FQDN,
- Operating system,
- Installed applications and services by specifying ports and used protocols,
- Patch status of each software with the date of installation of the patch,
- Date of the last virus scan (e.g. daily automated scan, manual scan on 23 January 2013) and
- Backup interval (complete and incremental), scope of the backup and last backup.

6. Administration and user manuals

For secure and uninterrupted operation, it is necessary that the service and maintenance personnel as well as the administrators are familiar with all functions of the ICS and are able to operate them. If there are staff shortages (e.g. due to illness or dismissal), it should be ensured that the required information is still available in the enterprise and can be accessed by the staff.

Therefore, an administration and user manual should be available for all ICSs and applications. The documents should cover the following security aspects:

- Required firewall rules (including service, protocol and port),
- Instructions for the hardening of specific applications,
- Instructions for secure configuration,
- Specific risks (e.g. when activating a specific configuration),
- System recovery (for contingency planning, see chapter 5.3.4).

5.3 Security-specific processes / policies

5.3.1 Security management

7. Development and integration of individual software

ICSs are delivered as a system of hard- and software. The adjustment to the individual circumstances and requirements is realised by the configuration. In a few particular cases, it may be necessary to develop proprietary software (e.g. scripts, batch files for batch processing) in order to subsequently integrate specific automatic procedures or functions. If proprietary programs or also scripts are developed, both the secure creation (secure coding guidelines) of the programs and the secure integration into the existing environment should be governed by an internal software development policy.

8. Disposal of hardware

Before a defective device is handed over to a third-party vendor for repair or maintenance, it should be ensured that no confidential information or configurations are stored on the device (e.g. hard disk or internal memory). For example, storage media with confidential information should have been removed or deleted in a secure manner beforehand.

Trusted service providers should be commissioned to dispose of the hardware. The defective devices should be stored until they are collected in such a way that they are protected against unauthorised access (e.g. storage in locked cabinets).

5.3.2 Technical documentation

9. Audit reports

The results of the performed audits should be documented in the form of audit reports. Information on the structure and contents of audit reports is explained in chapter 6. The contents of the documents are highly sensitive. The reports must be classified according to their security classification level and handled correspondingly (see measure 2).

5.3.3 Continuous management of all ICS components

10. Definition of the operational tasks of asset owners, integrators and product suppliers

The respective operational tasks of the asset owner, integrator and product supplier should be defined and documented in writing. This may apply, for example, to the administration of components in the field up to the application development or patch management.

11. Change management

For changes to the ICS, a change management system should be established. Roles should be separated so that it is not possible that the person who release a change can also implement this change. All planned changes should be checked by qualified persons as to whether they have security-relevant effects on the ICS.

12. Security monitoring

If security-relevant events are identified at an early stage, they can be responded to in a timely manner and possible damage can thus be averted. Therefore, a strategy as to how security-relevant events can be detected and identified, which response actions are required and how a secure state can be recovered should be developed in a security incident response plan in advance. The security incident response plan should take the phases of planning, response and recovery into account and define processes, e.g. for the classification of the events, reporting/notification, documentation, examination of the event and the actions derived from them.

In particular, the responsibilities and roles (see measure 1) as well as the further procedure (e.g. notification of authorities or publication) should be defined. The data protection officer of the enterprise should be involved in particular.

It should be tested and checked at regular intervals and at least every year whether the plan is up-to-date. If necessary, it must be revised.

5.3.4 Business continuity management

13. Business continuity plan for sensitive assets

In a business continuity plan, it should be defined how essential functions in the ICS can be resumed after a significant disruption. Actions which ensure that production is restarted within a reasonable time after a production disruption or a security incident occurred should be derived in advance. This includes, for example, backup processes, restoration and the regular testing of backups, system recovery procedures, repair of defective components and provision of spare parts as well as alternative communication and control options in the case of failures.

It should be checked at regular intervals and at least every year whether the plan is up-to-date. If necessary, it must be revised.

5.3.5 Personnel

14. Training of the personnel

The personnel (e.g. staff, contract partners and third parties) should refresh and extend the technical qualification at regular intervals in security-specific qualification and training programmes to perform their assigned activities. In this way, it should be ensured that the personnel does not make poor decisions, for example due to ignorance or lack of qualification.

In addition to the qualification programmes, the personnel should be informed about possible threats and vulnerabilities in regular awareness training courses and made aware of them. In particular, changes to already existing policies should be presented (see also measure 3, measure 12, measure 13).

The training courses should enable the service and maintenance personnel as well as administrators to identify and assess possible vulnerabilities as well as to counter them by taking adequate countermeasures.

15. Personnel security

To reduce the risk caused by human error (e.g. poor technical decisions, theft, fraud), the following aspects should be taken into consideration in human resources management.

In an employment policy, the prerequisites for employment should be defined. Applicants should be assessed, for example, with respect to their capability for their job on the basis of a previously defined and precise job description. Moreover, mentioned qualifications and references can be verified.

The personnel should be made aware of their duties to comply with the security policies (see measure 1). This may also be part of the employment contract (e.g. also in the case of service providers). For example, a non-disclosure agreement should be part of the contract (see measure 19).

The personnel (e.g. staff, contract partners and third parties) with authorisations for site or data access to the ICS should be entered in a list. The list should be checked and updated at regular intervals with respect to the required authorisations of the individual employees and, if necessary, authorisations should be re-assigned or withdrawn.

It should be checked at regular intervals if the policies for the personnel and job descriptions are up-to-date. If necessary, they must be revised.

Information on the subject of insiders can be found in [BSI CS-061].

16. Processes for the engagement, changes and retirement of personnel

Processes which ensure that the system, site and data access authorisations of the affected persons correspond to the new situation in the case of new recruitments, in the case of changes of the role and/or area of responsibility within the enterprise and in the case of retirements of staff should be established.

5.3.6 Revision & tests

17. Auditing

Audits of the security of networks and other components of an ICS should be carried out at regular intervals. In complex systems, it is absolutely essential to establish specialised teams for the identification and assessment of possible attack scenarios. A methodology for performing audits in ICS installations is described in chapter 6.

18. Component testing

When selecting components, defined (functional and security-relevant) requirements should be tested. The test item can be individual components up to the entire ICS.

5.4 Selection of the used systems and components as well as of the assigned service providers and integrators

5.4.1 Trustworthiness

19. Non-disclosure agreement with the product suppliers, solution providers and external asset owners

The asset owner should enter into non-disclosure agreements with contract partners (product suppliers, solution providers or external asset owners). They should particularly take staff of the contract partner with security-relevant information and knowledge of the ICS of the asset owner into account (e.g. for the case that staff of the contract partner changes the position or company).

Furthermore, there should be rules on how the operation of the ICS can be maintained if the contract partner no longer offers maintenance services or other services (e.g. due to the insolvency of the contract partner). The asset owner should, for example, still have the required access to these systems and adequate documentation should be available for the maintenance and operation of the ICS.

If a contract partner closes down their business, it should be contractually agreed that confidential information is returned to the asset owner.

5.4.2 Security features of ICS components

20. Notifying the system integrator of the security requirements

The system integrator should be notified of the asset owner's security requirements for the ICS, which result from the risk analysis. This should be part of the requirements specification.

The requirements should be formulated on the basis of specific applications. The requirements may relate to necessary properties or information. No solutions, but requirements should be described.

21. Taking the system integrator's security specification into account

The asset owner must take the security specification provided by the system integrator for an ICS into account in the risk analysis cycle. On the basis of the information made available by the system integrator, additional measures can be defined by the asset owner.

22. Robustness of products

In addition to the hardware (e.g. industrial computer), the software (e.g. protocol stack, ICS applications) should also respond to invalid input in a robust manner. For example, invalid network packets should not result in the crash or errors of the software, but be ignored by the protocol stack and logged if necessary.

The robustness of the components should already be ensured by the product suppliers. This requirement should already be specified when the asset owner purchases new components.

5.4.3 Compatibility of the technologies used with standards

23. Compatibility

The ICS to be purchased and their components should implement common standards of the respective technology and be compatible with other systems according to these standards. This particularly includes the support of the security mechanisms.

5.4.4 Commissioning in a secure configuration

24. Dispensing with superfluous product functions

If ICS components have services or interfaces which are not required by the asset owner, they should be removed or at least deactivated if possible. The changes made to the ICS should be documented in a comprehensible manner.

25. Individual access data

The access data of the ICS and applications should be changed individually during commissioning so that it cannot be seen in the publicly available documentation (see also measure 46). Another possibility is to create random access data which is assigned individually per device.

26. Activated security mechanisms and current patch status

The ICS components should have a current patch status during commissioning so that they do not have any relevant vulnerabilities in the delivered state. Available security functions should be activated and configured restrictively (e.g. firewall). Correspondingly, the ICS should be hardened to the greatest possible extent and require explicit user access releases by the integrator prior to commissioning.

5.4.5 Soft- and hardware support

27. Ensuring security in the long term

During the planning phase, asset owners, system integrators and product suppliers should already develop a strategy as to how long the security of the plant can be ensured. The same applies to the entire lifespan of the plant. This also includes the continued use of discontinued software. Therefore, alternative security measures should already be taken into account at an early stage.

28. Support of anti-virus solutions

If necessary, the ICSs to be purchased should be equipped with an anti-virus program or at least support the operation of anti-virus programs. Usually, the product supplier supports selected products of anti-virus solution providers (see also chapter 5.6.7).

5.4.6 Remote maintenance by the product supplier and integrator

29. Secure remote maintenance

The systems with which remote maintenance is carried out should have the same level of protection as the ICS network. The security policies of the ICS network should be in accordance with those of the remote maintenance systems.

Establishing the connection should at least require two-factor authentication (e.g. token and password) and the data should only be transmitted in encrypted form (see measure 68).

If the connection for remote maintenance is to be established externally, no direct connection to the ICS should be established. The connection to the ICS network should rather be established by means of a so-called jump server/proxy server in a DMZ (see measure 32). It is able to establish a corresponding connection to the ICS. At the same time, it can record all activities.

As an alternative to the jump server, the connection can be established internally from the ICS network instead of externally. The ICS thus connects to the product supplier. In this way, incoming connections are avoided and no additional services offered to the outside.

The remote maintenance access possibility for the product supplier should only be activated if needed and otherwise be deactivated by the asset owner. This reduces the risk of possible attacks. Moreover, the operator should confirm that the connection has been established before the ICS can be accessed.

5.4.7 Securing field devices

30. Requirements for field devices

Securing field devices (e.g. sensors and actuators) is important, among other things, to counteract threat agents with physical access to these devices. If these devices are equipped with security mechanisms, such as authentication, encryption, access control or logging, asset owners should insist that they are used. Particularly older components, however, have often purely functional design and are not equipped with integrated security mechanisms if they can be addressed via higher protocols. In this case, accompanying physical, organisational or additional technical measures should be used. This includes, for example, security appliances filtering the transmitted data traffic, which have been designed particularly for use in industrial environments.

5.5 Constructional and physical securing

31. Physical securing

The ICS must be secured against unauthorised physical site, system and data access. This applies to buildings, rooms and cabinets.

Site access should be controlled, monitored and logged. It should be possible to lock housings and cabinets. Unauthorised site and data access should be detected promptly, e.g. by the triggering of alarms.

5.6 Technical measures

When implementing the technical measures, the requirements specified by the product suppliers and/or the product documentation must be observed. Product suppliers often provide descriptions or restrictions for the implementation of the listed measures.

5.6.1 Securing of networks

32. Network segmentation

An ICS network should consist of several network segments with individual protection requirements. The data traffic between the different levels (see 3) should be limited to the operationally required extent by means of data flow control, e.g. firewall.

If the protection requirements are correspondingly high, a demilitarised zone (DMZ) should be included between the production management and the operational/process management. A DMZ is an intermediate network located between the Intranet and the Internet, but not included in either network. It is a separate network not protected as strongly as the network actually to be protected. It consists of two physically separated firewalls and an application level gateway. Proxy services with filtering options up to layer 7 should control and monitor the data traffic.

In addition to the network segmentation with different functionalities (for vertical integration, see 1), networks at all geographic sites or generally organisationally independent machines/plants should also be segmented among each other (for horizontal integration, see 2). This prevents, for example, malware from spreading to all machines in an unhindered manner.

The connection should always be established from the network segment with the higher protection requirements into the network segment with the lower protection requirements.

The network segmentation must not be bypassed by means of undocumented connections. Uncontrolled connections to network segments with different protection requirements should not be allowed in particular.

33. Securing of electronic, external interfaces

All external interfaces to the ICS network should be identified and documented (e.g. in a network plan; see measure 4). In addition to obvious interfaces such as the connection to the office network via a DMZ, this also includes less obvious, external communication channels such as wireless networks and serial connections, e.g. between buildings in the case of geographically distributed systems and lines.

A process which requires regular examination of the documentation and, in the case of changes, timely updating should be defined (see measure 2).

If external interfaces are required, direct access from outside to the ICS network should be avoided (e.g. direct modem connections to an ICS, administration via a direct connection from the Internet). On the other hand, all external connections in the DMZ to the ICS network should be established via a proxy service and thus via an additional security level. Access to the ICS network is thus only possible via this service and not to the ICS network directly. Remote access is such a possibly required external access (see measure 29).

In the case of external interfaces, the following security measures in particular should be taken into account to prevent the ICS network from being accessed from outside in an unauthorised manner:

- Access via external interfaces should require strong authentication (e.g. callback of the modem to a preconfigured telephone number, exclusive connection to a configured IP address, hardware key in the modem).
- Connection attempts and access should be logged and monitored (e.g. in the case of modem connections by means of a telephone system; see also measure 73).
- External interfaces (e.g. remote access points) which are not needed for a longer period of time must be switched off. The devices should only be switched on again (electrically) if needed.
- Security-relevant data should not be transmitted (e.g. access data, critical and privileged commands).
- Data (engineering data, production data) should only be stored in the ICS environment, but not on external systems.
- Wherever possible, remote maintenance access points should only allow read access.

34. Static network configuration

Especially in the case of a manageable number of ICSs, static assignment of the network configuration should be preferred to dynamic assignment. This includes the static assignment of IP addresses, subnet masks and routing within the ICS network. The configuration of WINS/DNS servers may also be required if names are to be resolved with them.

When assigning IP addresses, prevailing conventions should be complied with if possible. Routers should be assigned the first available IP addresses in the network segment (e.g. 192.168.0.1) and switches and gateways the following IP addresses (e.g. 192.168.0.2), followed by ICSs with other functions.

The addressing of the systems must be documented (see also measure 5). Furthermore, it should be ensured that an IP address is not assigned several times.

If a static network configuration of the ICS is carried out, the DHCP client software should be uninstalled or at least deactivated on the ICSs. An unintentional DHCP packet does thus not override the static network configuration.

35. Same security measures for ICSs in one network segment

All components in a network segment (e.g. process management, see 3) should meet the same security level. If, for example, an ICS with a lower security level is compromised by a threat agent, this system is a threat to all other ICSs in the same network segment and this in the same security zone. Starting from this compromised system, a threat agent can perform further attacks to other systems and possibly exploit trust relationships between the systems. Therefore, all ICSs in the same security zone and thus with the same trust relationship among each other should also be secured in a comparable manner.

36. Independent operation of network segments

If the connection between two network segments in the ICS network is lost, this should not affect production or should affect it only to a small extent. Therefore, dependencies between networks should be avoided. Possible effects of a network segment failure are thus reduced to the greatest possible extent.

37. Securing of wireless technologies

Using wireless technology requires careful planning. Since this is a so-called shared medium, the transmission medium can usually be accessed by the threat agent even from large distances and from outside the organisation’s property and it is very difficult to restrict such access.

The range of wireless networks should therefore be restricted as far as possible. Security functions (e.g. passwords, PIN input) should be activated and differ in the configuration from the default settings in the initial installation.

Wireless technologies should not be used for purposes which require high availability requirements (e.g. a wireless connection can be interrupted again and again or restricted severely due to interfering signals). Moreover, the technologies used should have adequate security mechanisms in accordance with the state of the art so that unauthorised access to the data transmitted is not possible (e.g. encryption of the data traffic).

Security in the case of wireless networks should not only be based on the security features of the technology used, but additional security mechanisms on the network level should also be implemented. It should be ensured that not only one security wall, but several hurdles are established. This includes, for example, the network segmentation and the additional use of cryptographic algorithms when transmitting data (in this respect, see also measure 32, measure 43, measure 58). Accordingly, wireless networks should preferably not be connected directly to the ICS network, but communicate with the ICS via proxy services in the DMZ due to the different security level (see measure 33).

Available logged data of the devices should be checked at regular intervals for irregularities (e.g. communication with unknown devices).

A detailed description with respect to this subject can be found in the brochure "Drahtlose Kommunikation und ihre Sicherheitsaspekte" [Equivalent English translation of the title would be: "*Wireless communication and related security aspects*"][6].

38. Use of firewalls

For the logical separation of network segments, a firewall which controls the data flow between the segments as a filter component should be used (see also measure 32).

In this respect, a distinction can be made between the following categories of firewalls on the network level (host-based firewalls are covered in measure 39):

- Packet filter (filtering for IP address and port),
- Stateful inspection firewall (filtering for IP address, port and connection status),

[6] https://www.bsi.bund.de/DE/Publikationen/Broschueren/drahtloskom/index_htm.html

- Application level gateway (additional filtering up to the application level).

Firewalls should preferably be used as dedicated hardware. Trained personnel should be responsible for the configuration and operation of the firewalls. The following aspects should be taken into account when configuring a firewall:

- The firewall should be configured restrictively and therefore generally prohibit everything in accordance with the white list approach so that connections and access must be activated explicitly.
- Only connections which are absolutely necessary for the operation of the ICS should be enabled.
- Connections from the ICS network to external networks (e.g. office network) should only be made via proxy services in the DMZ. Direct connections between the networks must be avoided. The communication with other networks should be disabled completely.
- Incoming connections from external networks into the network of the ICS should preferably be disabled completely. If this is not possible, the contents of the connections should be filtered and checked for conformity.
- Filtering should be as fine-grained as possible. If possible, access should therefore be restricted to individual IP addresses or to a small defined address range.
- Only the absolutely necessary ports for TCP or UDP should be enabled.
- Both incoming and outgoing data traffic should be filtered.
- The place holder ANY should be avoided.
- The last filter rule should always prohibit everything (DENY ALL, PERMIT NONE).

Moreover, the logged data of the firewall should be checked at regular intervals for irregularities. In this respect, it must be pointed out that only installing a firewall does not provide additional protection if there is no careful and restrictive configuration of the rules and corresponding monitoring.

The procurement criteria differ from case to case. Depending on the type of applications, functions for the filtering and monitoring of the protocols can be used. It is recommended that not only IP addresses and ports are filtered, but also the protocols themselves.

39. Host-based firewalls

A host-based firewall is a software used for the filtering of the network traffic from and to a computer. Unlike a network firewall, a host-based firewall is installed on the computer to be protected. In many cases, these firewalls are part of the operating system.

Wherever possible, a host-based firewall should be installed and used on all ICSs.

40. Data diode (one-way gateway)

A data diode allows that data transmission is only possible in one direction. There is no return channel, which results in certain restrictions. If a return channel is required for acknowledgements, the individual connections should be terminated in the gateway, the protocol should be checked and only then should the connection be redirected.

Depending on the direction of the data diode, different objectives can be pursued. Thus, it is possible to prevent, for example, control commands from a network with low protection requirements (e.g. office network) from being transmitted to a network with high protection requirements (e.g. ICS network). On the other hand, confidential information from a network with high protection requirements can be prevented from outflowing in the case of the reverse positioning.

In this case, the restrictions also apply to obtaining updates and configuring the components via the network. Establishing connections past the data diode for this purpose bypasses the function and must be avoided.

If the communication has to take place in both directions, there are solutions which offer filters and control options. Thus, conformity and the possibly transmitted values and commands can be checked for the respective area or validity.

41. Suitable logical separation and VLAN

VLANs can be used for the logical separation of network segments. To separate network segments with different protection requirements, physical separation is required on the device level.

When using VLANs, the default VLAN should be deactivated. Unused ports at the switch should be assigned a separate VLAN.

42. Implementing intrusion detection and/or intrusion prevention systems

Using intrusion detection systems (IDS) and intrusion prevention systems (IPS), attack attempts can be identified at an early stage so that the administrator is alerted in time (e.g. by means of an IDS) or an automated response to the attack has already been initiated (e.g. by means of an IPS).

To this end, IDS/IPS work on the basis of heuristics in order to distinguish attack attempts from usual, desired behaviour and data. Accordingly, these heuristics must be updated at regular intervals. Moreover, the heuristics must be adapted to the ICS and its individual circumstances. Typical incidents and events which can be identified by such a system include, for example, unauthorised access to systems and the unauthorised installation of software or manipulations of data. Furthermore, unintended and accidental changes (e.g. in configuration files) can also be detected.

An IDS/IPS can monitor individual servers (host-based IDS/IPS; HIDS/HIPS) or check the data traffic in the network using sensors (network-based IDS/IPS; NIDS/NIPS).

If an NIDS/NIPS is used, the sensors in the network should in particular be positioned at the external interfaces (e.g. DMZ) for the monitoring of the data traffic. Higher threats by attacks (e.g. Internet) usually emanate from external interfaces. An HIDS should also be installed on all ICSs. The logged data of the HIDS should be integrated into central logging (see measure 73).

IDS/IPS should be considered as an additional security measure and do not replace the monitoring of the systems and network (e.g. by means of a security information event management (SIEM) system).

Using and operating an IDS can only be recommended to larger companies, since creating, maintaining and examining the messages (especially in the initial phase) involve considerable expense and effort. In smaller plants, the cost and benefits must be checked in advance and, if necessary, alternative hardening and security measures must be implemented.

When implementing an IPS, it must also be taken into account that very special situations are also taken into account in the planning phase to ensure that these legitimate transmissions are not prevented. Before activating these functions, a very careful test phase should be completed.

The effectiveness of an IDS/IPS strongly depends on an adapted and individual configuration. This effectiveness can be impaired, for example, by a large number of recurring false positives. IPSs in particular should be used with deliberation. Priority is given to live operation which might be disturbed by incorrect intervention of the IPS.

Therefore, not only the initial configuration of the IDS/IPS requires trained specialist personnel, but a person must be able to distinguish between a reported attack attempt and a false positive also during operation in an emergency situation. It should be possible that this person can be contacted at all times so that corresponding countermeasures, if necessary, can be initiated after the message has been classified.

For additional information on IDS/IPS, corresponding literature should be referred to (e.g. [BSI IDS]).

43. Use of secure protocols

For administrative and security-critical tasks (e.g. logging in to the component or configuration), the confidentiality and integrity of the data should be ensured. The use of insecure protocols (e.g. Telnet, FTP, HTTP) should therefore be avoided. Weak protocols should be replaced by secure protocols (e.g. SSH, SFTP, HTTPS) or secured by additional cryptographic procedures (e.g. SSL/ TLS).

In the case of real-time data, encryption can be dispensed with if the confidentiality of the information is to be given lower priority. However, measures should still be taken to be able to ensure authenticity and integrity as well as to detect and/or avoid the installation of messages.

For newer plants, it should be taken into account that secure protocol versions are used.

If weak protocols cannot be secured or replaced by secure alternatives (e.g. in the case of proprietary, ICS-specific protocols), additional security measures should be taken to protect the data transmitted against unauthorised access (e.g. positioning of the affected ICS in a separate network and restrictive filtering of the data traffic between the network segments).

5.6.2 Protection of services and protocols

44. Name resolution (DNS)

The Domain Name System (DNS) resolves the names of the computers into their IP address in IP networks and is thus required for the communication of the ICSs among each other.

Dedicated DNS servers which are operated separately from DNS servers in other networks (e.g. office network) should be responsible for the ICS network. If there is a connection to other networks, a filter component (e.g. firewall) should prevent the DNS server from being accessed from outside the ICS network.

The DNS service should only be responsible and configured for the name and address space of the specific ICS installation and thus only manage and store zone information for computers from the ICS network.

The ICS network should preferably be compartmentalised so that names of external computers do not have to be dissolved. If this is still necessary, the names should only be resolved via the DNS server in the ICS network which, in turn, contacts a DNS server, for example, behind the firewall in the office network as a kind of representative. Name resolution requests should under no circumstances take place directly on external DNS services.

The availability of DNS servers should be ensured by means of a redundancy, e.g. in the form of master/slave pairs. In this case, a DNS service manages the zone information as a master and backs it up at regular intervals by means of so-called zone transfers on a slave computer.

The transmission of zone transfers should be restricted as far as possible, since the information provides a potential threat agent with an unnecessary insight into the structure of the ICS network. Therefore, static IP addresses should preferably be assigned in the ICS network for the computers so that the DNS entries are not changed at regular intervals and, as a result of this, no excessive zone transfers are required (see also measure 34).

Zone transfers should only be possible between trusted systems and require previous authentication (e.g. by means of cryptographic signatures; see also [RFC 2845 2000]).

The IP address should be assigned statically (see measure 34). If the IP address has to be assigned dynamically, only change notices of the IP address should be processed by DNS servers if they come from trusted computers.

Moreover, security measures against cache pollution and cache poisoning should be taken into account when securing the DNS service.

45. Time synchronisation

In ICS environments, a large number of processes, but also administrative activities are based on an exact and harmonised time (e.g. traceability of distributed logged data, adding additives in production at the right time). Due to the application requirements, it must be considered carefully how the time is synchronised.

For synchronisation, Network Time Protocol (NTP) or IEEE 1588 can be used.

The time signal for the server should be provided by a trusted source. The clients on the ICSs should interpret the time in a uniform, standardised format (e.g. by taking time zones, standard time and daylight savings time into account).

5.6.3 Hardening of the IT systems

46. Default user accounts and passwords

Default user accounts and passwords on systems and in applications are often known globally and documented, for example in manuals. Therefore, default users should at least be deactivated, or preferably deleted. Default passwords in systems and applications should be changed to secure passwords during the installation.

Prior to changing default users and passwords, it must be checked if the systems and applications can still perform the functions assigned to them after default users and passwords have been changed. If, for example, the SNMP community string is changed on routers, this change must also be known to the server.

Changing passwords must be preferred to other measures. Only in exceptional cases (e.g. in the case of permanently set passwords in the program code), should the asset owner accept that the password is not changed. Depending on the risk, accompanying measures should be taken. They include, for example, connections to a VPN via a security appliance.

47. Individual user accounts

If possible, each member of staff should have their own user account and only use their own account to log in to the operating system and applications.

This is often not possible in ICS environments so that several members of staff share one user account in many cases. As a result, performed actions cannot be assigned to one person and the password is known by a larger group of people.

In such cases, it should be checked by means of a risk analysis to what extent the existing security measures are adequate to prevent the ICSs from being accessed in an unauthorised manner (e.g. locked doors in the control centre). Moreover, the passwords should be different for those group accounts at least in each network segment. This applies to user accounts both on the operating system level and on the application level.

48. Removing unnecessary software and services

If programs and services are installed or activated on ICS components and if they are not required for the operation of production, they should be removed or at least be deactivated. In many cases, such a software is pre-installed when the ICSs is delivered and automatically activated during the start procedure of the computer possibly without being noticed.

A listing of the required software and network services should be taken from the product supplier's documentation or requested from the product supplier. If only local or explicit access of selected systems to services is required, the availability of these services should be restricted, for example, by means of a local firewall (see also measure 39).

49. Adjusting the default settings

The default settings can have vulnerabilities when the ICS hard- and software is delivered so that, for example, security measures are only activated and set inadequately. Therefore, the configuration should be checked and, if necessary, adjusted especially after the delivery or changes of the system (e.g. software updates, new software) or the infrastructure (e.g. new connections to network segments).

The following examples illustrate possible, security-related settings of a default configuration:

- Deactivated security functions (e.g. firewall),
- Less restrictive firewall rules limiting the data traffic,
- Unprotected administration accesses,

- Default users and passwords (see also measure 46),
- Unnecessary programs and activated services with vulnerabilities if applicable (see also measure 48).

50. Adjusting the hardware configuration

Hardware which is not required for productive operation should be removed or at least deactivated. This includes local interfaces such as USB ports, CD / DVD drives and other storage medium devices.

Deactivation can be achieved, for example, by means of a mechanical locking device, in a software-controlled manner or by means of seals, e.g. at USB ports. If these devices are used in an unauthorised manner despite the securing measure, this should be traceable for the administrator of the system (e.g. broken locks or seals or protocol entries in the system).

In the case of a software solution, the administrator should be able to deactivate and unset the locking mechanism for a short period of time for maintenance purposes so that the hardware can be accessed.

51. Access to the Internet within the ICS network

Especially when surfing the Internet, there is the risk of infection with malware caused by drive-by downloads. Therefore, free access to the Internet from the ICS network should be disabled.

If, for example, access to the Internet is still possible in Level 4, the data traffic should be checked by a virus scanner and active contents filtered out.

5.6.4 Patch management

52. Handling of patches

Errors in software are a serious problem in ICSs. Due to the vulnerabilities resulting from this, a threat agent can gain access to the system or interfere with the software process. The general rule is that these errors should be eliminated.

A patch process with role-specific responsibilities should be defined, which also takes additional third-party software into account (e.g. office applications, PDF reader) in addition to the patches and updates approved by the product supplier. The process should contain the following elements at a minimum:

- Regular examination for new vulnerability messages at the product suppliers of the ICS components or third-party software
- Assessing the criticality of patches, for example with the Common Vulnerability Scoring System (CVSS)[7],
- Obtaining the patches and updates,
- Testing,
- Approval process,
- Handling product supplier approvals of patches and
- Handling the patching of additional software.

Sources of supply for the notification of vulnerabilities are the product suppliers or also CERTs.

The CVSS is a methodology used to assess and classify vulnerabilities depending on the individual risk of the individual operation. The so-called Base Score includes, among other things, how the vulnerability can be exploited (e.g. locally or remote) and what are the consequences (e.g. denial of service or execution of codes). A second value (the so-called Temporal Score) assesses framework conditions which may change in the course of time. This includes, for example, the availability of exploit code. A third component establishes the reference to the user's local environment. This user must evaluate on the basis of their environment what this vulnerability means for them. The first two pieces of information are made available on different

[7] http://www.first.org/cvss

websites about vulnerabilities (e.g. CVE MITRE, Secunia, Qualys). A detailed description of the procedure can be found on the website of the Forum of Incident Response and Security Teams (FIRST)[8].

Installing patches and updates usually requires the approval of the ICS product supplier. Therefore, usually patches and updates which are already available on the Internet, for example, cannot installed by the asset owner, since a loss of function would be possible and the product supplier would not assume any guarantee.

For this reason, the asset owner should contractually agree together with the product supplier upon periods of time for the approval and provision of patches and updates or alternative workarounds for vulnerabilities. The periods of time should be chosen as short as possible, since the system concerned is exposed to a higher risk due to the vulnerability in this time window.

Where possible, the asset owner themselves can perform tests prior to the installation. As an alternative, the updates should be installed and tested sequentially. In this respect, the updates should be installed first on redundant systems. Prior to installing patches and updates, it is recommended to perform a backup for each ICS. This applies particularly to ICSs which are required for production. ICS of no or very little importance for production might also be patched after confirmation by means of a risk analysis without prior backup and comprehensive tests.

Moreover, it should be checked if a restart is performed after the patch or if it is required. This must be taken into consideration when planning.

Altogether, the installation of patches should be integrated into the operating cycles of the plant. Thus, maintenance windows at the plant can be used to install patches. If the components have a redundant design, a step-by-step procedure might be chosen in order not to postpone the time of the installation for too long.

If no patch is available, alternative measures should be considered and taken as part of a risk analysis to prevent the vulnerability from being exploited. As an alternative measure, it is for example possible to position the ICSs concerned in a separate network segment and to filter the data traffic to this network segment by means of a firewall (see measure 32 and measure 38).

53. Handling the end of support

If the end of support has been reached for ICS components or software used in them, these components are an increased risk from a security perspective. This applies in particular to software from the IT environment (e.g. operating systems). In these cases, it is possible that vulnerabilities are still identified, but they are not closed any more. In this case, additional security measures might have to be taken, e.g. the migration to a new software version.

For this purpose, a risk analysis should be carried out and, on the basis of this, adequate security measures should be identified depending on the function of the ICSs and its importance for production. For example, separating ICSs with unpatched vulnerabilities into their own network segment and a restrictive firewall for the filtering of the data traffic can thus protect the systems.

The long-term goal should be to replace the ICSs concerned with components supported by the product supplier. Without the product supplier's support, errors and failures occurring in the future may have a strong impact on production, since developing solutions without the help of the product supplier are more complex and costlier.

In the procurement phase in particular, it should be ensured that no components which have already been discontinued by the product supplier are used.

5.6.5 Authentication

54. Technical authentication measures

[8] http://www.first.org

Wherever possible, using all ICSs should require the authentication of the users and services so that the systems can only be operated in an authenticated condition (see measure 46, measure 47). In addition to conventional computers, this also includes routers, switches and PLCs.

For authentication, different procedures and characteristics can be used. A distinction is made between the authentication characteristics such as knowledge (e.g. password, PIN), ownership (e.g. token, smartcard, certificate) and physical characteristics (e.g. fingerprint, iris recognition).

In addition to one characteristic, it is also possible that several characteristics are used for authentication and thus a higher security level can be established (e.g. two-factor authentication by means of token and password). Here, characteristics from different classes (knowledge, ownership, biometric features) should be combined.

When selecting the authentication methods, a risk analysis must be performed. They must be compared to other requirements (e.g. Hazardous Incident Reporting Ordinance) and organisational framework conditions (e.g. access restrictions) to reach an appropriate selection.

55. Password distribution and management, password policy

A password policy taking the following aspects into account should be drawn up and implemented. Both technical solutions and organisational measures can be defined.

- The user should be prevented from choosing weak passwords due to complexity requirements (e.g. length, alphabet including numbers and special characters).
- The password should only be valid for a pre-defined period of time. The user should then be asked to choose a new password which differs from the old password.
- The number of failed login attempts should be limited (e.g. temporary blocking of the user account).

The mentioned requirements should preferably be managed by means of a central management solution (e.g. in a directory service within the ICS).

Not all measures can be applied comprehensively to all ICSs. For example, a threat agent can block the user account by means of provoked, failed login attempts. Thus, the affected system could no longer be accessed by the legitimate user. Therefore, the increase in security gained by the respective measure and possible restrictions of other requirements for the ICS (e.g. required, immediate access) must be weighed against each other.

56. Avoiding misuse

Unauthorised access to systems should be prevented. It should be recognisable and documentable which user was active.

There are certain operating situations which require immediate operating access to the ICS. In this respect, logout or a screen lock are not acceptable. In these cases, the systems should be protected against unauthorised access by compensating security measures (e.g. staffed control centre).

In less critical areas, operation should be locked and only current information displayed. In this way, monitoring is still possible, but unhindered access prevented.

For authentication, solutions using chip or RFID cards should be used to avoid the entering of passwords.

5.6.6 Access control

57. Authorisation

Wherever possible, only the respectively required access rights should be assigned on all ICSs depending on the user logged in. Accordingly, the assignment of authorisations, e.g. to the file system, should be based on the so-called principle of least privilege. A user or service should thus only be assigned those rights which are required to perform their activities.

Usually, access rights are assigned on the file system level (reading, writing, executing and deleting files) and on the network level (access to networks and network services).

When managing users, groups and authorisations (e.g. in Windows networks), it is recommended to allocate user accounts to groups and to assign authorisations for these groups. Thus, a so-called role-based access control (RBAC) concept is implemented into practice.

58. Use of suitable cryptographic algorithms

If cryptographic algorithms (e.g. hash function, symmetric and asymmetric encryption) are used, they should be in accordance with the state of the art (e.g. BSI TR-02102).

5.6.7 Protection against malware

59. Installation and operation of anti-virus programs

If the installation and the unrestricted operation of anti-virus programs is possible on an ICS and approved by the product supplier, these systems should be supplied automatically with current virus signatures (e.g. via a local virus signature distribution service in the DMZ; see measure 62).

The following ICS components are usually approved by the product supplier for the unrestricted installation and operation of the anti-virus software:

- EWS,
- Systems for process data processing and visualisation,
- Operating and monitoring systems,
- Engineering systems,
- Asset management systems and
- Systems for the configuration of the field devices.

60. Suitable alternatives in case anti-virus programs are not possible

There are cases in which no or only a restricted installation of an anti-virus program is possible on an ICS (e.g. no virus scanner is available). This usually concerns control systems, PLCs and field devices. In this case, additional compensating security measures must be implemented to protect the systems adequately against malware. The following listing includes several sample criteria for the identification of such systems:

- The product supplier has not approved anti-virus programs.
- Only restricted operation of the anti-virus protection is possible so that there is no sufficient increase in security.
- The virus signatures cannot be updated in a timely manner (e.g. daily updates).
- There is too high a risk that the availability is impaired.

Based on individual risk analyses for each ICS, an adequate combination of compensating security measures should be identified. This includes the following security measures, among others:

- Use of an "airlock" for removable media if removable media are connected to the device (see measure 67),
- If possible, regular scanning of the ICS from a boot medium or USB device with a current anti-virus program and current signatures, for example during a planned maintenance window (an infection can thus be identified and then eliminated, although with some delay)
- Separation of the affected ICS into their own network segment with a filter component (see measure 64)
- Application whitelisting (see measure 65)
- Deactivation of file shares in the network.

61. Secure configuration of anti-virus programs

Due to the high availability requirements in ICS environments, adjusted configuration for anti-virus programs should be used under certain circumstances in the case of critical systems. Settings which may lead to an unintended impairment of production (e.g. due to a high system load caused by a scanning process) should be deactivated. Product suppliers often only approve those restricted configurations for the operation of anti-virus programs on the ICSs.

Anti-virus programs can usually operate in two different modes. On the one hand, scanning can generally take place before applications or files are accessed or the scanning process is initiated manually or automatically at specific times. Usually, the anti-virus program should automatically scan in the case of every access.

The selection should be made depending on the recommendation of the product supplier of the anti-virus program and the ICS component. If continuous examination is not possible (e.g. for performance reasons), additional alternative security measures should be taken.

Moreover, a complete scan of all data should be performed at regular intervals. An additional, complete scan with current signature should be carried out after the initial installation and after changes have been made to the system.

In general, the following settings should be taken into account when configuring the anti-virus programs:

- Manual scans should only be carried out and documented when production has come to a standstill.
- Only local media should be checked. Network drives should not be scanned to avoid parallel scans by several computers.
- Only the administrator should be authorised to configure or deactivate the anti-virus program.

The installation process as well as the configuration should be documented for each ICS.

62. Central virus signature distribution service

The ICS network should be operated autonomously wherever possible and only allow absolutely necessary connection to other networks. If connections to other networks are required, they should not be established directly, but always via a proxy server.

Therefore, the signatures for the anti-virus program should not be obtained directly from the Internet, but via a central virus signature distribution service in the DMZ. This services downloads the current signatures from the Internet as a kind of representative and makes them available to the ICSs. Thus, no direct connections of the ICSs to the Internet are required.

63. Prompt updating of virus signatures

Prompt updates of the virus signatures and the anti-virus programs are often not possible in ICS environments. For this reason, the following aspects must be taken into consideration.

The ICSs should be subdivided into groups according to their possible update intervals. In addition to this, ICS components with a redundant design should be assigned to different groups in order to be able to, for example, respond immediately to the distribution of incorrect virus signatures in the production environment (e.g. false positives).

The virus signatures should be distributed in the groups with redundant ICSs with a time delay (e.g. 12 hours) in order to be still able to maintain the operation with the second system in the case of problems.

Due to the high availability requirements, only signatures which have been approved by the ICS product supplier and classified as uncritical should be distributed.

64. Anti-virus program on the firewall (virus wall)

A virus wall examines the data traffic between two networks for malware. In this way, it can check the data transmitted as a kind of representative for ICSs with no or with a restricted anti-virus program. To do this, these ICS are positioned in a separate network segment and the data traffic to and from this network is filtered by an application level gateway (ALG) with an installed anti-virus program and examined for malware.

It should be taken into account that widely available ALG products usually do not support ICS-specific protocols. In this case, it is not possible to check the data transmitted via this protocol. Nevertheless, especially collateral damage caused by non-targeted malware can be avoided to a large extent.

65. Application whitelisting

It is possible to monitor and restrict the execution of programs by means of special security software for application control. Unlike conventional anti-virus programs, instead of trying to block undesired software, only desired programs are allowed to execute.

Consequently, a distinction can be made between two different approaches to identify and prevent applications and undesired behaviour of a system (e.g. in the case of malware). In the case of the blacklisting approach of conventional anti-virus programs, this is achieved on the basis of known signatures and heuristics of undesired applications. This approach has several vulnerabilities, for example that new malware may change independently in each new copy and thus have a new, still unknown signature. Successful protection depends on the currency and availability of the signatures.

In the case of application whitelisting, only those applications and such behaviour which was approved explicitly are allowed. Everything else is prohibited. In this way, there is no dependency on current signatures. This procedure is suitable particularly in the case of systems as in the ICS environment which are only subject to minor changes by software installations. Therefore, application control should always be based on the whitelisting approach, wherever possible.

To prevent unauthorised software from being executed, such a protection software can use the following different attributes:

- Certificates (signing of trusted software e.g. by a central entity),
- File system path (certain areas are declared to trusted),
- Hashes (applications and possible unauthorised changes are identified based on a hash of the files),
- System and user behaviour (e.g. use of certain TCP ports, operation only at specific times).

At the moment, application whitelisting is not considered to be an equivalent replacement for an anti-virus program.

5.6.8 Portable media

66. Handling of removable media

For the use of removable media, rules for the respective handling should be set up and made known.

On the components, the use should be limited to specific devices (device control). In most cases, this can be achieved with functions of the operating system or via additional software.

67. "Airlock" for removable data (quarantine PC)

A quarantine PC can examine storage media for malware as a kind of representative for ICSs. For this purpose, the staff must be instructed to examine storage media from an untrusted source (e.g. USB sticks) by means of the quarantine PC for malware, before such media are integrated into the ICS network or an ICS with no or with a restricted anti-virus program can be connected.

The quarantine PC should have a current patch status of the anti-virus programs and current malware signatures should be installed on it. The signatures of the quarantine PCs should therefore be updated at least on a daily basis.

In addition to a possibly automated examination of the storage media by means of the quarantine PC, the medium should also always be scanned manually.

68. Use of notebooks for maintenance purposes

In applications, notebooks are often used as portable maintenance devices. With respect to the security level, they must be assessed as Level 4 (provided that they are under the control of the asset owner) or Level 5 devices (provided that they are under the control of an external service provider) from the ICS point of view.

In both cases, using these devices requires particular measures. In general, it must be defined prior to each use which tasks must be carried out and the member of staff must be able to perform these tasks due to their training and knowledge. When carrying out work at plants with particular protection requirements (SIL, GMP etc.), it might be necessary to ensure by means of additional measures that undesired changes are performed.

Technical security measures (e.g. protection of the configuration data of the field device using a corresponding bridge) or, as an alternative, organisational measures (two-man-principle) must be applied.

Internal devices:

By taking organisational measures, it must be ensured that only software which is required for maintenance purposes is installed on these maintenance devices. System hardening as for the Level 3 devices should be carried out. Moreover, these devices should be patched at regular intervals and examined for malware.

External devices:

For the use of external maintenance devices, it is recommended to first conclude a corresponding contract with the external provider, in which the security aspects (particularly codes of conduct for external staff) are contractually agreed upon.

Before using an external maintenance device, an inventory must be performed. In this context, the following aspects must be clarified:

- Which software is installed (incl. the operating system and patches)
- Which interfaces are available and active (GPRS!)
- What protection against malware has been installed (Are current signatures available?)

If this inventory has been completed and not given negative insights, an examination for malware using anti-virus protection which complies with the asset owner's requirements must be performed.

If this test has been completed successfully, access to the productive system can be granted.

In this context, using individual firewalls (USB-powered compact devices) has proven successful in the case of different users. They are connected between the respective PNK and the maintenance device and should prevent undesired activities.

69. Activated BIOS password and restricted boot options

By changes to the BIOS configuration of the ICSs, the interface for portable data storage media can be activated and the setting for the boot medium changed (e.g. USB port, CD / DVD drive). In this way, the ICS can be booted from external media and a threat agent can obtain full access to the system.

Therefore, the password protection of the BIOS should be activated on all ICSs and, in addition, the ICS only boot from the required medium (e.g. internal hard disk) in the default configuration of the BIOS. Other boot options should be deactivated (e.g. USB port, CD/DVD drive).

70. Deactivation of the autorun function

The autorun function should be deactivated on all ICS. If this function is activated, programs, for example on portable media, can be started without being noticed after they have been identified by the operating system. In many cases, malware uses this function to spread via portable media.

5.6.9 Backup

71. Backups of systems

To reduce the risk and the consequences of a loss of data (e.g. caused by unintended changes to the data, hardware defects), it should be considered to perform backups on all IT systems at regular intervals.

The underlying backup strategy should implement different backup levels. Therefore, a backup should be stored locally on the IT systems for quick access and an additional backup should be carried out on a central system.

Depending on aspects such as the availability requirements or changes to the data in the case of IT systems, the interval and the scope of the backup may vary. For example, the configuration of switches only changes rarely. In such cases, the backup strategy cam thus be adjusted to the corresponding application scenario so that backups can be performed, for example, based on events.

The following aspects should be taken into account when drawing up a backup concept:

- The backup should include both incremental and complete backups. If possible, the local backup should be performed on a daily basis. For this purpose, a second hard disk, for example, can be installed.
- The data used for ensuring the integrity should be included in the backup so that unauthorised changes or defects can be identified.
- The scope of the backup (e.g. incremental, complete) should be documented for each IT system with the date of the backup performed last.

The backup should generally include all data on the media of the IT system. Such precautions include, for example:

- Operating system and firmware,
- Configurations (e.g. routers, switches, applications, firewall rules),
- Applications,
- Databases,
- Production data,
- Other data (e.g. logged data).

Backups should be carried out sequentially in the case of the IT systems. Moreover, backups should preferably be performed when production has come to a standstill so that the backup process does not affect production adversely.

72. Storage of backups

To ensure the integrity, confidentiality and availability of the data, the backup should be stored according to the following requirements:

- The storage media should be stored in a fire-proof safe with an adequate protection class and in a different fire zone separated from the secured IT systems.
- Physical access to the storage media should be avoided by organisational and technical site, system and data access controls (e.g. two-man principle, locked safe).
- In an emergency situation, it should be ensured that the backups can be accessed immediately.
- The storage place should meet the climate-related requirements regarding long-term storage, since storing the backups under improper conditions may shorten the lifespan of the media.

5.6.10 Logging and evaluation

73. Logging / Monitoring

Logging is used to detect errors and security-relevant incidents such as unauthorised access attempts to data or the identification of transmission bottlenecks at an early stage

The logged data should be stored on a central server. Thus, the logged data of the distributed systems and components can be collected, analysed and associated centrally.

In an ICS, at least the following events should be logged and collected centrally provided that they are available:

- Local events, e.g. of the operating systems,
- Events of domain controllers,
- Firewall/router/switch/server events,
- Events of the anti-virus programs,
- Events of the IDS/IPS.

In addition to the events mentioned above, the following data should be recorded:

- Date and time,
- Description of the event,
- Criticality,
- Source of the event, e.g. application, operating system.

Further information can be found in [BSI LogDaten]. Furthermore, the applicable privacy policies must be complied with. The data should be monitored by a central system. On On the basis of occurring events and limit violations in the case of monitored values, an alarm which informs the administrator about this should be triggered.

The following list illustrates possible examples of these events and patterns:

- Conspicuous behaviour which is typical of malware (e.g. increased network traffic, decrease in performance, increasing number of errors in applications and integrity violations),
- Hardware defects such as defective sectors in the case of data storage media (e.g. hard disk) or failing components due to hardware errors,
- Loss of the network connection,
- Unusual increase in the CPU load and memory usage.

5.7 Comparison with available standards

6 shows to what extent the aspects of the best practices are covered by the standards

- IEC 62443 (see chapter 4.1.1.2),
- VDI/ VDE 2182 (see chapter 4.2.2.1),
- NERC CIP (see chapter 4.3.1.1) and
- DHS Best Practices (see chapter 4.3.3)

.

ff	IEC 62443	VDI/ VDE 2182	NERC CIP	DHS Best Practices
1 Establishment of a security organisation	2-1 chapter A.3.2.3 2-1 chapter 4.3.2.3 2-1 chapter 4.3.2.3	Part 1 chapter 3.2 Part 2.1 chapter 4.2		
2 Creating and maintaining the documentation	2-1 chapter A.3.4.4 2-1 chapter 4.2.3.13	Part 1 chapter 3.1 Part 1 chapter 3.5 Part 2.1 chapter 7 Part 2.1 chapter 8 Part 3.3 chapter 4.1.3 Part 3.3 chapter 4.1.4		
3 Establishing a security management	Complete 2-1	Part 1 chapter 3 Part 1 chapter 4	CIP-002-1 CIP-002-2 CIP-002-3 CIP-002-3a CIP-002-3b CIP-002-4 CIP-002-4a CIP-002-5 CIP-003-1 CIP-003-2 CIP-003-3 CIP-003-4 CIP-003-5	
4 Network plan	2-1 chapter A.3.4.2.3.3 2-1 chapter 4.2.3.5	Part 1 chapter 3.3 Part 1 chapter 4.1 Part 2.1 chapter 4.3		PL chapter 12.2
5 List of IT systems and installed applications	2-1 chapter 4.2.3.4 3-1 chapter 8.7	Part 1 chapter 3.5.1 Part 1 chapter 4.1 Part 2.1 chapter 4.3.1 Part 3.3 chapter 4.1.4		

ff	IEC 62443	VDI/ VDE 2182	NERC CIP	DHS Best Practices
6 Administration and user manuals	2-1 chapter A.3.3.5	Part 1 chapter 3.5 Part 2.1 chapter 7 Part 2.1 chapter 8		
7 Development and integration of individual software	2-1 chapter 4.3.4.3.1 2-1 chapter 4.3.4.3.3 2-1 chapter 4.3.4.3.4 2-1 chapter 4.3.4.3.5	Part 1 chapter 4 Part 2.1 chapter 5.5 Part 2.1 chapter 5.7		PL chapter 5
8 Disposal of hardware	2-1 chapter 4.3.3.3.9		CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	
9 Audit reports		Part 1 chapter 4.8		
10 Definition of the operational tasks of asset owners, integrators and product suppliers				
11 Change management	2-1 chapter A.3.4.3.6 2-1 chapter 4.3.4.3.2			
12 Security monitoring	2-1 chapter A.3.4.5 2-1 chapter 4.3.4.5 2-1 chapter 4.3.3.3.8	Part 2.1 chapter 4.4	CIP-001-0 CIP-001-1 CIP-001-1a CIP-001-2a CIP-008-1 CIP-008-2 CIP-008-3 CIP-008-4 CIP-008-5	PL chapter 6.2
13 Business continuity plan for sensitive assets	2-1 chapter A.3.2.5 2-1 chapter A.3.4.3.8		CIP-009-1 CIP-009-2	

ff	IEC 62443	VDI/ VDE 2182	NERC CIP	DHS Best Practices
	2-1 chapter 4.3.2.5 2-1 chapter 4.3.4.3.9		CIP-009-3 CIP-009-4 CIP-009-5	
14 Training of the personnel	2-1 chapter A.3.2.4 2-1 chapter 4.3.2.4		CIP-004-1 CIP-004-2 CIP-004-3 CIP-004-3a CIP-004-4 CIP-004-4a CIP-004-5	
15 Personnel security	3-1 chapter 10.3, 2-1 chapter A.3.3.2 2-1 chapter 4.3.3.2		CIP-004-3 CIP-004-3a CIP-004-4 CIP-004-4a	
16 Processes for the engagement, changes and retirement of personnel	2-1 chapter 4.3.3.2			
17 Auditing	2-1 chapter A.3.4.2.5.4 2-1 chapter 4.2.3.10 2-1 chapter 4.4.2.2	Part 1 chapter 4.8 Part 2.1 chapter 5.8		
18 Component testing	2-1 chapter A.3.4.3.5 2-1 chapter A.3.4.2.4.2 2-1 chapter A.3.4.2.4.3 2-1 chapter 4.3.4.3.1		CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	
19 Non-disclosure agreement with the product suppliers, solution providers and external asset owners				PL chapter 4.7
20 Notifying the system integrator of the security requirements	2-1 chapter A.3.4.2.4 2-1 chapter A.3.4.3	Part 1 chapter 3.1 Part 1 chapter 3.5		

ff	IEC 62443	VDI/ VDE 2182	NERC CIP	DHS Best Practices
		Part 2.1 chapter 6 Part 2.1 chapter 4.1.1 Part 3.3 chapter 4.1.1 Part 3.3 chapter 4.1.2		
21 Taking the system integrator's security specification into account	2-1 chapter A.3.4.2.4 2-1 chapter A.3.4.3	Part 1 chapter 3.1		
22 Robustness of products	2-1 chapter A.3.4.2.4.2			
23 Compatibility				
24 Dispensing with superfluous product functions			CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	PL chapter 2.1
25 Individual access data	2-1 chapter A.3.3.5.3.13			
26 Activated security mechanisms and current patch status		Part 3.3 chapter 4.1.4		
27 Ensuring security in the long term			CIP-009-1 CIP-009-2 CIP-009-3 CIP-009-4 CIP-009-5	
28 Support of anti-virus solutions				
29 Secure remote maintenance	2-1 chapter A.3.3.6.5.3 3-1 chapter 7.4			PL chapter 10 PL chapter 12.2
30 Requirements for field devices				PL chapter 9
31 Physical securing	3-1 chapter 10.2 2-1 chapter A.3.3.3		CIP-006-1 CIP-006-1a	PL chapter 11

ff	IEC 62443	VDI/ VDE 2182	NERC CIP	DHS Best Practices
	2-1 chapter 4.3.3.3		CIP-006-1b CIP-006-1c CIP-006-2 CIP-006-2a CIP-006-2b CIP-006-2c CIP-006-3a CIP-006-3c CIP-006-3d CIP-006-4c CIP-006-4d CIP-006-5	
32 Network segmentation	2-1 chapter A.3.3.4 2-1 chapter A.3.4.2.3.3 2-4 chapter 4.3.3.4		CIP-005-1 CIP-005-1a CIP-005-2 CIP-005-2a CIP-005-3 CIP-005-3a CIP-005-4a CIP-005-5	PL chapter 12
33 Securing of electronic, external interfaces	2-1 chapter A.3.3.6.5.3		CIP-005-1 CIP-005-1a CIP-005-2 CIP-005-2a CIP-005-3 CIP-005-3a CIP-005-4a CIP-005-5	PL chapter 10 PL chapter 12.2
34 Static network configuration				
35 Same security measures for ICSs in one network segment	2-1 chapter A.3.4.2.3.3			
36 Independent operation of network segments				
37 Securing of wireless technologies				PL chapter 13

ff	IEC 62443	VDI/ VDE 2182	NERC CIP	DHS Best Practices
38 Use of firewalls	3-1 chapter 6.2			PL chapter 3.1
39 Host-based firewalls	3-1 chapter 6.3			
40 Data diode (one-way gateway)				
41 Suitable logical separation and VLAN	3-1 chapter 6.4			
42 Implementing intrusion detection and/or intrusion prevention systems	3-1 chapter 8.4			PL chapter 2.2 PL chapter 3.2
43 Use of secure protocols				PL chapter 4.2 PL chapter 10.3
44 Name resolution (DNS)				PL chapter 8.1
45 Time synchronisation				
46 Default user accounts and passwords	2-1 chapter 3.3.5.3.9 2-1 chapter 4.3.3.5.5 2-1 chapter 4.3.3.5.7 2-1 chapter A.3.3.5.3.13		CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	PL chapter 4.1
47 Individual user accounts	2-1 chapter A.3.3.5.3.7 2-1 chapter 4.3.3.5.2			PL
48 Removing unnecessary software and services			CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	PL chapter 2.1
49 Adjusting the default settings	2-1 chapter A.3.3.5.3.13			PL
50 Adjusting the hardware configuration				PL chapter 2.4

ff	IEC 62443	VDI/ VDE 2182	NERC CIP	DHS Best Practices
51 Access to the Internet within the ICS network				
52 Handling of patches	2-1 chapter A.3.4.2.4.3 2-1 chapter 4.3.4.3.7 2-1 chapter 4.3.4.5.3 2-1 chapter A.3.4.2.3.5	Part 2.1 chapter 4.4	CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	PL chapter 2.6 PL chapter 6.1 PL chapter 6.2
53 Handling the end of support	2-1 chapter A.3.4.2.3.5			
54 Technical authentication measures	2-1 chapter A.3.3.6 2-1 chapter 4.3.3.6 3-1 chapter 5.3 3-1 chapter 5.4 3-1 chapter 5.5 3-1 chapter 5.6 3-1 chapter 5.7 3-1 chapter 5.10		CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	
55 Password distribution and management, password policy	3-1 chapter 5.9		CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	PL chapter 4.3
56 Avoiding misuse				
57 Authorisation	2-1 chapter A.3.3.5 2-1 chapter A.3.3.7 2-1 chapter 4.3.3.5		CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	PL chapter 2.3 PL chapter 4.5

ff	IEC 62443	VDI/ VDE 2182	NERC CIP	DHS Best Practices
58 Use of suitable cryptographic algorithms	3-1 chapter 7.2 3-1 chapter 7.3 3-1 chapter 7.4 3-1 chapter 5.2			PL chapter 4.2
59 Installation and operation of anti-virus programs	3-1 chapter 8.3 2-1 chapter 4.3.4.3.8		CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	PL chapter 7
60 Suitable alternatives in case anti-virus programs are not possible				PL chapter 7
61 Secure configuration of anti-virus programs				PL chapter 7
62 Central virus signature distribution service				
63 Prompt updating of virus signatures	2-1 chapter A.3.4.2.4.2		CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	PL chapter 7
64 Anti-virus program on the firewall (virus wall)				
65 Application whitelisting				
66 Handling of removable media				
67 "Airlock" for removable data (quarantine PC)				
68 Use of notebooks for maintenance purposes				
69 Activated BIOS password and restricted boot options				

ff	IEC 62443	VDI/ VDE 2182	NERC CIP	DHS Best Practices
70 Deactivation of the autorun function				
71 Backups of systems	2-1 chapter 4.3.4.3.9			
72 Storage of backups	2-1 chapter A.3.4.3.8			
73 Logging / Monitoring	3-1 chapter 8.2 3-1 chapter 8.6 3-1 chapter 8.7 3-1 chapter 8.8 2-1 chapter 4.3.3.5.8 2-1 chapter 4.3.3.6.4		CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	PL chapter 4.4

Table 6: Comparison of the best practices with IEC 62443, VDI/VDE 2182, NERC CIP and DHS Best Practices

7 shows the coverage of the best practices by existing measures of the IT-Grundschutz Catalogues (12th version), where these measures are referred to as "safeguards". In the table below, it is indicated in the column "Coverage" (Cov) as follows:

- "O" Best practices are covered one-to-one by the IT-Grundschutz safeguard.
- "S" Best practices are covered by several IT-Grundschutz safeguards together.
- "P" Best practices are covered in part by the IT-Grundschutz safeguard. (Supplement here: in which parts, see column "Notes")
- "-/-" Best practices are not covered by any IT-Grundschutz safeguard.

In table 7, this also applies to the degree of coverage by the requirements of the standard ISO/IEC 27001 (see chapter 4.1.1.1 by the respectively assigned controls of the ISO/IEC 27002 into account. The above-mentioned indication with "O", "S", "P" and "-/-" is applied accordingly for controls according to ISO/IEC 27001 and ISO/IEC 27002 as well as for chapters from the management framework of the ISO 27001.

Note: If the word "here" is used in the notes of the table below, it refers to the respective best practice (first column) as it is included in this document.

	IT-Grund-schutz	Cov	Notes	ISO 27001	Cov	Notes
1 Establishment of a security organisation	S 2.193 S 2.336	S	The security program should be covered correspondingly by a security concept according to IT-Grundschutz.	A.6.1.1 A.6.1.2 A.6.1.3	S	
2 Creating and maintaining the documentation	S 2.201	O		4.3.2	O	
3 Establishing a security management	BSI 100 M 1.0 M 1.16	S		4.1 4.2	S	
4 Network plan	S 2.139	O	Note: Also according to BSI 100-2, chapter 4.2.3	A.7.1.1 A.10.6.1	P	The requirement for a network plan is implicitly derived from the controls. There are no specific requirements for a physical and a logical network plan and their contents.
5 List of IT systems and installed applications	M 4.2 S 2.168 S 2.171 S 2.25 S 2.10	S	Note: Also according to BSI 100-2, chapter 4.2.2 and 4.2.4	A.7.1.1		
6 Administration and user manuals	S 2.25 S 2.111 S 2.219	S		A.10.1.1	O	Note: The control generally requires documented operating processes.
7 Development and integration of individual software	S 2.378	O	Is also supported additionally by S 2.379	A.12.5 A.12.5.2	P	ISO 27001 does not require an explicit policy for the development of software.

	IT-Grund-schutz	Cov	Notes	ISO 27001	Cov	Notes
8 Disposal of hardware	M 1.15	S	Within this module, especially S 2.13, S 2.431, S 2.436	A.9.2.6	O	
9 Audit reports	S 2.119	O		6	O	
10 Definition of the operational tasks of asset owners, integrators and product suppliers	S 2.1 S 2.225	P	The measures cover responsibilities and authorisations only generally, but not specifically for the parties involved which are mentioned here.	A.6.1.3 A.6.2.3	P	These controls also cover the assignment of the responsibility for information security to different roles and/or parties (only) generally.
11 Change management	M 1.14	S		A.10.1.2 A.12.5.1	S	
12 Security monitoring	M 1.8 S 6.60 S 6.65	S	Part: Reporting of security incidents in general. Here, however, the explicit notification of the competent authority is required.	A.6.1.6 A.13 A.13.1.1 A.13.2.1	S	Part: Reporting of security incidents in general. Here, however, the explicit notification of the competent authority is required.
13 Business continuity plan for sensitive assets	M 1.3 M 1.4	S		A.10.5.1 A.14 A.14.1.3 A.14.1.4 A.14.1.5	S	
14 Training of the personnel	M 1.13 S 3.45 S 3.51	S		5.2.2 A.8.2.2	S	

	IT-Grundschutz	Cov	Notes	ISO 27001	Cov	Notes
15 Personnel security	M 1.2 S 2.30 S 2.220	P	Protection of people against the danger to life and limb Safety is not covered	A.8.1.1 A.8.1.2 A.8.1.3 A.8.2.1 A.6.1.5 A.11.2.4	P	Protection of personnel Safety is not covered
16 Processes for the engagement, changes and retirement of personnel	S 3.6	O		A.8.3.1 A.8.3.2 A.8.3.3	S	
17 Auditing	S 2.199	O	Note: Moreover, the subject of auditing is generally covered in BSI 100 and, with respect to technology, in various modules with individual measures, such as S 4.81, S 4.298, S 4.368, S 2.360 ...	6 A.6.1.8	S	
18 Component testing	S 2.199	O	Note: Testing prior to approval is covered, for example, in S 4.65	A.15.2.2 A.10.3.2	S	
19 Non-disclosure agreement with the product suppliers, solution providers and external asset owners	S 3.55 S 2.307	S		A.6.1.5 A.6.2.3	P	

	IT-Grund-schutz	Cov	Notes	ISO 27001	Cov	Notes
20 Notifying the system integrator of the security requirements	S 2.80	P	Part: In S 2.80, a requirements catalogue is generally required. This best practice, however, specifically relates to the ICS asset owner's requirements for the system integrator. Note: In general, services rendered by third parties are covered in M 1.11.	A.12.1.1	P	Part: According to A.12.1.1, requirements for information systems must generally be specified. This best practice, however, specifically relates to the ICS asset owner's requirements for the system integrator. Note: In general, services rendered by third parties are covered in A.10.2.1.
21 Taking the system integrator's security specification into account	-/-	-/-		-/-	-/-	
22 Robustness of products	-/-	-/-	Note: As in the best practice above, product features are covered here. This is not covered by ISMS requirements in such a manner.	-/-	-/-	
23 Compatibility	-/-	-/-		-/-	-/-	
24 Dispensing with superfluous product functions	-/-	-/-	Note: Product features are covered here; the measure S 4.95 only relates to a minimum operating system.	-/-	-/-	
25 Individual access data	S 4.7	O	Note: Also in S 4.201 (for routers and switches)	A.11.5.2	P	Part: Personal (individual) access data. Changing default passwords upon delivery is not required explicitly in A.11.5.2.

	IT-Grund-schutz	Cov	Notes	ISO 27001	Cov	Notes
26 Activated security mechanisms and current patch status	S 2.318 S 4.237 S 4.95	S		-/-	-/-	Note: A.10.3.2 requires the acceptance of systems before they are used in production, but not, as is the case here, the explicit currency and activation of security functions.
27 Ensuring security in the long term	-/-	-/-	Note: There are various (module-)specific measures with regard to maintenance or contracts. S 2.4, S 2.27, S 2.213, S 2.369, S 2.253 ... However, the subject of the "end of support" is not covered explicitly.	-/-	-/-	
28 Support of anti-virus solutions	M 1.6	P	Part: Protection against malware generally in M 1.6. Here, however, the capability of supporting the ICS anti-virus solutions is focused on.	A.10.4.1	P	Part: Protection against malware generally in A.10.4.1. Here, however, the capability of supporting the ICS anti-virus solutions is focused on.
29 Secure remote maintenance	S 5.33 M 4.4	P	Part: Here, two-factor authentication and the two-man principle are required. S 5.33 does not required this explicitly	A.11.4.2	P	Part: Here, two-factor authentication and the two-man principle are required. A.11.4.2 does not required this explicitly
30 Requirements for field devices	-/-	-/-	Note: In principle, a security concept for end devices is required here.	-/-	-/-	

	IT-Grund-schutz	Cov	Notes	ISO 27001	Cov	Notes
31 Physical securing	M 2.1 M 2.9 S 1.55 S 1.13 S 2.17 S 1.73 S 1.49 S 2.6 S 1.29	S		A.9.1.1 A.9.1.2 A.9.2.1	S	
32 Network segmentation	M 4.1 S 5.61 S 5.62 S 5.77 S 2.141	S	Note: The requirements for network segmentation are generally covered. Here, however, the ICS network in particular is considered.	A.11.4.5 A.10.6.1	S	Note: The requirements for network segmentation are generally covered. Here, however, the ICS network in particular is considered.
33 Securing of electronic, external interfaces	M 4.1 M 4.3 M 4.4 M 4.5 M 4.6 M 3.301 S 2.139 S 2.204 S 5.150 S 5.141 S 4.81 S 5.39	S		A.10.6.1 A.10.6.2 A.11.4.2 A.11.4.3 A.10.10.1 A.10.10.2	P	Note: The requirements for the securing and monitoring of external interfaces are generally covered. Here, however, special interfaces (e.g modem) in the ICS network are also considered.

	IT-Grund-schutz	Cov	Notes	ISO 27001	Cov	Notes
34 Static network configuration	-/-	-/-	Note: Individual measures such as *S 4.294 Secure configuration of access points* require static IP, but only in a specific context	-/-	-/-	
35 Same security measures for ICSs in one network segment	S 5.77 S 2.141	P	Part: The Grundschutz safeguards require the positioning of applications and systems with the same protection requirements in one zone. Here, however, (vice versa) the same security measures are required for all ICSs of one zone.	A.11.4.5	P	Part: This control requires the separator of networks (see Grundschutz). Here, however, the same security measures are required for all ICSs of one zone.
36 Independent operation of network segments	-/-	-/-		-/-	-/-	
37 Securing of wireless technologies	M 4.6 M 4.8 S 2.381 S 4.133 S 4.293 S 4.294 S 4.298 S 5.77	S		A.11.4.2	P	Part: The securing of wireless networks is only covered in ISO 27002 and this only generally.
38 Use of firewalls	M 3.301	S		A.11.4.5 A.11.4.6 A.11.4.7	S	
39 Host-based firewalls	S 4.238	O		-/-	-/-	Note: No controls explicitly regarding host-based firewalls

	IT-Grund-schutz	Cov	Notes	ISO 27001	Cov	Notes
40 Data diode (one-way gateway)	-/-	-/-		-/-	-/-	
41 Suitable logical separation and VLAN	S 4.202 S 4.203 S 5.6.2	O	Note: S 4.203 only provides the checklist suitable for S 4.202.	-/-	-/-	Note: No controls explicitly regarding VLAN
42 Implementing intrusion detection and/or intrusion prevention systems	S 5.71	O		-/-	-/-	Note: IDS is only referred to as further information or indirectly in the controls.
43 Use of secure protocols	S 5.39	O	Note: Avoiding insecure protocols is also additionally covered in several other measures.	-/-	-/-	Note: No controls explicitly on how to avoid insecure protocols
44 Name resolution (DNS)	M 5.18 S 2.451	S		-/-	-/-	Note: No controls explicitly regarding DNS
45 Time synchronisation	S 4.227	O		A.10.10.6	O	Note: This control does not require explicitly an NTP service in the organisation's own (ICS) network.
46 Default user accounts and passwords	S 4.7	O	Note: Also in S 4.201 (for routers and switches)	A.11.5.2	P	Part: Personal (individual) access data. Changing default passwords upon delivery is not required explicitly in A.11.5.2.
47 Individual user accounts	S 2.220 S 2.30	S	Note: Furthermore, this is also covered, for example, in S 4.244 and S 2.322	A.11.5.2	O	

	IT-Grundschutz	Cov	Notes	ISO 27001	Cov	Notes
48 Removing unnecessary software and services	S 4.95 M 3.301	S		A.11.4.6	P	Part: Only the network control, but not the removal of unnecessary software and services is covered.
49 Adjusting the default settings	S 4.237 S 4.82	S	Note: Furthermore, this is also covered in other object-specific measures, among others, in S 4.201, S 4.244	A.12.5.3	P	Part: The control only covers the change control, but not the actual adjustment of the default settings themselves.
50 Adjusting the hardware configuration	S 4.4 S 4.200	S		-/-	-/-	Note: No controls explicitly regarding the removal of unnecessary hardware (interfaces).
51 Access to the Internet within the ICS network	S 5.69	O		A.10.4.2	P	Part: This control also allows the controlled handling of active contents. Here, however, preventing the execution is generally required.
52 Handling of patches	M 1.14 S 2.35 S 2.273	S O P	Part: Prompt installation of security-relevant patches and updates is covered in S 2.273, and the patch management generally in M 1.14. Approval by third parties (avoiding the loss of warranty etc.) is not covered.	A.10.1.2 A.12.6.1	S O	

	IT-Grund-schutz	Cov	Notes	ISO 27001	Cov	Notes
53 Handling the end of support	-/-	-/-		-/-	-/-	
54 Technical authentication measures	S 4.15 S 2.7	P	Part: Authentication is required in the control, but not two-factor authentication.	A.11.5.2	P	Part: Authentication is required in the control, but not two-factor authentication.
55 Password distribution and management, password policy	S 2.11	O		A.11.3.1	O	
56 Avoiding misuse	S 4.2	O		A.11.3.2	O	
57 Authorisation	S 2.8 S 2.30	S		A.11.2.2 A.11.6.1	S	Note: The best practice of working with group authorisations is not covered by the controls.
58 Use of suitable cryptographic algorithms	S 2.164	O	Note: The measure does not include any reference to BSI TR 02102 (although both documents come from the BSI)	A.12.3.1	P	Part: The control requires risk assessments regarding the strength and quality of the algorithms used. Result must not correspond to the state of the art.
59 Installation and operation of anti-virus programs	M 1.6	S		A.10.4.1	O	
60 Suitable alternatives in case anti-virus programs are not possible	S 2.224	P	Part: Only preventive measures against malware, which, however, are not considered to be alternatives.	-/-	-/-	

	IT-Grund-schutz	Cov	Notes	ISO 27001	Cov	Notes
61 Secure configuration of anti-virus programs	S 4.3	P	Part: The configuration of the anti-virus programs is covered generally in the measure. Here, however, further specific requirements for the production environments must be met.	-/-	-/-	
62 Central virus signature distribution service	-/-	-/-	Note: S 2.159 requires anti-virus programs and signatures used to be updated, but no central virus signature distribution service.	-/-	-/-	
63 Prompt updating of virus signatures	M 1.6 S 2.159	P	Part: S 2.159 requires anti-virus programs and signatures to be updated in a timely manner. Here, however, the delayed distribution of signatures in groups after extensive testing is required.	-/-	-/-	
64 Anti-virus program on the firewall (virus wall)	-/-	-/-	Note: S 4.3 requires the examination for malware in the case of data transmission in general, but no "virus wall"	-/-	-/-	
65 Application whitelisting	-/-	-/-		-/-	-/-	
66 Handling of removable media	S 4.4	O	Note: Generally also in M 5.14	A.10.7.1	P	Part: The control covers removable media generally, but does not necessarily require technical inspections.

	IT-Grund-schutz	Cov	Notes	ISO 27001	Cov	Notes
67 "Airlock" for removable data (quarantine PC)	S 2.235	O		-/-	-/-	
68 Use of notebooks for maintenance purposes	-/-	-/-		-/-	-/-	
69 Activated BIOS password and restricted boot options	S 4.84	O		-/-	-/-	
70 Deactivation of the autorun function	S 4.57	O	Note: Also in other safeguards such as S 4.280 and S 4.339	-/-	-/-	
71 Backups of systems	M 1.4	O		A.10.5	O	
72 Storage of backups	M 1.4	O		A.10.5	O	
73 Logging / Monitoring	M 1.8 M 4.2 S 4.225 S 5.9 S 4.312 S 2.157 S 4.205 S 2.133 S 2.140	S	Note: Further measures cover the monitoring under specific aspects (e.g. S 4.276, S 2.365 in the case of Windows Server 2003; S 4.321 for VPNs; S 6.130 for the detection of security incidents	A.10.3.1 A.10.6.1 A.10.10.1 A.10.10.2 A.10.10.3 A.10.10.4	S	Note: The requirement for a loghost is implicitly derived from A.10.10.3. Part: The controls focus on the monitoring of the system and data access attempts as well as system alarms. The focus is less on the monitoring of regular conditions.

Table 7: Comparison between the best practices and IT-Grunfschutz and ISO 27001

6 Methodology for audits of ICS installations

This chapter describes a methodology for performing audits in ICS installations. Methodological principles for the auditing are presented and the phases of an ICS audit are described over the course of time. These principles describe comprehensive and holistic auditing (maximum requirements) which should be adjusted and reduced depending on the applicable framework conditions.

6.1 ICS specifics and IS revision

The VDE Technical Rule 2182 presented in chapter 4.2.2.1 describes a specific procedural model for the implementation of security measures and considers the entire ICS life cycle. Audits are described as a time- or event-driven measure which must be carried out at regular intervals. Audit results must be documented in order to detect shortcomings and deviations.

The information security revision (IS revision) on the basis of IT-Grundschutz focuses on the holistic review of the information security in an enterprise or an administration. All levels from the establishment of an information security organisation to personnel aspects up to the configuration of systems are examined[9]. However, ICS specifics are not taken into account by the IS revision, since it focuses solely on the IT infrastructure of an organisation.

Based on the VDE Technical Rule 2182 and the concept of the IS revision, supplemented by ICS-specific system properties, an audit methodology for ICS is described below. This is a success control method and is used to review the security concept and organisation and the implementation of the measures.

When planning and carrying out audits in the area of ICSs, it must particularly be taken into account that the persons in charge (especially external service providers) not only have the required technical knowledge in the field of security, but also have the respectively applicable industry-specific qualifications enabling them to handle the respective plants.

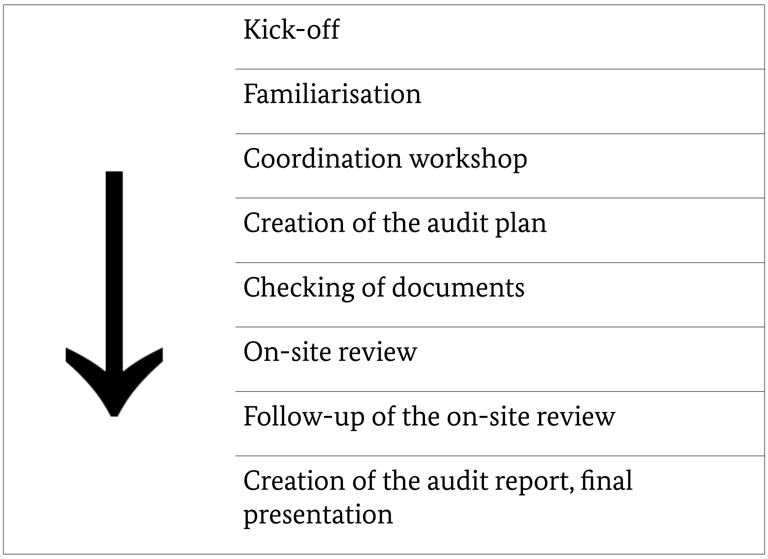
Audits are an important element of secure ICSs and should therefore be implemented. The specific scope of an audit must be chosen adequately for the respective enterprise, especially with regard to the enterprise size and the available financial resources. Both test width (which systems) and test depth (type and scope of the test methods) must be assessed.

An obligatory element of audit is a risk analysis in which possible consequences of the performed tests (interactions, functional consequences etc.) in particular are considered. This results, among other things, in strict limitations with respect to the possible tests.

6.2 Procedure

The auditing procedure can be divided into the following eight phases.

[9] For information security revision, see [IS 10]



Kick-off

Familiarisation

Coordination workshop

Creation of the audit plan

Checking of documents

On-site review

Follow-up of the on-site review

Creation of the audit report, final presentation

6.2.1 Kick-off

The preparation of the audit starts with an initial meeting (kick-off), in which the parties involved are informed about the further procedure and their respective tasks are defined. Necessary consents of the parties involved are given in the kick-off meeting or obtained following the meeting after consultation in decision-making bodies (e.g. on the part of the management or supervisory board). It is mandatory to involve especially those persons who bear the operational responsibility for the respective plants in addition to the persons responsible for IT from the start

The audit team is introduced to the other parties involved. The project manager explains the planned procedure both from a technical and organisational point of view and answers directly arising questions. Any concerns on the part of the system administrators (operational responsibility) should be raised during the meeting so that they can be identified as framework conditions to be taken into account at a later point of time and included in the minutes. Technical experts of the team and corresponding specialists responsible on the part of the asset owner (e.g. PLC specialists, network specialists) should be able to meet in person and build up direct communication channels. The next steps should be scheduled roughly. Prior to the kick-off, corresponding milestone plans have already been communicated in advance so that the parties involved are able to prepare themselves and to identify collisions with other time-critical projects.

The documentation required for the following phases is described and requested from the specialists responsible. Mutual obligations to provide information must be set out and communicated to all parties involved who are not present in person in the initial meeting.

The aim of the kick-off is to clarify the rough framework conditions for the auditing and to define the responsibilities.

6.2.2 Familiarisation

If the documentation and outstanding consents have been made available, the audit team can start with the familiarisation. The audit team gains an overview of the components to be audited and their technical and organisational interaction in the enterprise. Queries regarding technical aspects can be clarified directly with the specialists responsible.

The completeness, quality and currency of the submitted documentation must be assessed. For successful audit planning, at least the following documentation is required:

- ICS security concept and security concepts of subsystems which include all personnel, organisational and technical measures with respect to ICS security,

- Organisational chart,
- Description of the production area and the test systems (where audited),
- Network plans, communication relations, system configurations,
- Listing of critical production processes,
- Policy on information security and
- Audit reports of the last five years.

Missing or incomplete documents must be requested. If it turns out that documents do not exist, they should now be created. If necessary, interview minutes with specialists responsible must be included in the collection as a replacement document. For further planning, at least an advanced draft of each document must be submitted to ensure that subsequent audit results can refer to the documentation in a reasonable manner.

The audit team reviews the documentation by clarifying the following questions:

- Is the documentation complete (are all subsystems, networks, physical locations included)?
- Does the comparison of the threats with the measures show any coverage gaps or superfluous measures?
- Which residual risks remain? Are they acceptable for the management according to the records?
- Are the prescribed measures described in a comprehensible, practically feasible and understandable manner and are they adequate?

The team creates a detailed audit plan based on the available documents and information collected from the parties involved. This audit plan refers to the measures which cannot be assessed solely on the basis of checking the documentation. In the case of a large number of individual measures, a reasonable measure sample which is to be compared to previous audit reports must be selected. A risk analysis with respect to the tests to be carried out, which must be performed in close coordination with the persons in charge, is of particular importance. This is the only way to minimise the risk of possibly critical impacts of tests on the plants.

After this phase, the audit plan comprises the following elements:

- Listing of all components to be tested according to priorities and the respective measures to be tested,
- Definition of a test method for each measure,
- Listing of the components for which vulnerabilities are searched for,
- Listing of the organisational roles and, as far as possible, the interview partners and parties involved in the test resulting from them as well as
- Suggested detailed scheduling.

The audit team must be supported adequately in performing their tasks. A separate lockable room near the systems or system administrators should therefore be made available to external teams and access to the office infrastructure (printers, copiers, office material) should be ensured.

6.2.3 Coordination workshop

The workshop is used to analyse the prepared audit plan together with the system administrators and determine the feasibility of the plan. To ensure that the subsequent test phase can be carried out successfully, necessary system and site access rights for the auditors must be granted and approved by the system administrators.

For the productive areas, safety provisions must be referred to and compared to the planned test methods. Individual test methods which potentially affect safety-critical systems or may interfere with the system behaviour of hazardous components must be checked for feasibility. If necessary, additional securing measures should be defined during the auditing (e.g. evaluation of production areas during a test). The external auditors must be briefed about the safety regulations with the start of the test phase at the latest.

The main goal of the coordination workshop is to define mandatory, so-called "rules of engagement". These rules specify which subsystems or interfaces of invasive examinations must be excluded, who must be informed before and after the test methods to be determined, who provides an on-call service during the test phase and which members of staff must be present during which tests. Mandatory limits for the auditors are part of these rules of engagement:

- Which test methods are taboo?
- Which systems or local production areas should under no circumstances be affected in the test phase?
- Who has decision-making powers in the case of unclear interpretations of rules during the test phase?

Clear and detailed rules and regulations facilitate the further procedure both for the auditors and for the customer and prevent disputes regarding questions of liability from arising in the case of unplanned losses of production.

The results of the workshops must be documented and have been assigned a coordinated test concept. This concept lists all components and associated test methods and specifies the respectively mandatory rules of engagement. A schedule refined in accordance with the workshop results must be added to the test concept.

6.2.4 Test methods of the test phase

In the test phase, test methods which can be divided into the following three categories are applied: penetration tests, on-site review and interviews. These categories are described first. For the application of test methods on different subject levels, possible questions are presented in 6.3.

6.2.4.1 Penetration tests

External and internal penetration tests can be included in the audit plan. These tests are optional and should be used with caution. They make sense especially within the scope of factory acceptance tests or site acceptance tests. The problem of penetration tests is that components may enter into an undefined state when vulnerabilities are found. This may result in control problems. For this reason, these tests should only be performed in the maintenance window. Moreover, penetration tests can be restricted to selected components (e.g. engineering workstations). In general, it is recommended to restrict penetration tests to those systems which are not directly related to productive operations. In several areas of application, it is absolutely essential to dispense with penetration tests to a large extent and to be confined to carrying out passive examination methods instead.

The penetration tests particular cover the vulnerability areas mentioned in chapter 3

- Use of standard IT components with already identified vulnerabilities,
- Inadequate input validation,
- Lack of securing of default configurations,
- Incomplete securing of remote maintenance access points,
- Negligent setup of network access points,
- Local access via control messages and
- Undesired, extensive networking

, but are not limited only to these typical vulnerabilities.

For the systems to be tested within the agreed scope of the audit, a list of potential vulnerabilities is determined and documented. This list must be assessed over the course of this audit. The documentation should have a defined structure to ensure that penetration test results from different audits can be compared. Thus, vulnerabilities which were determined via IP network access points, can be documented, for example, in a table with the following column structure:

ID	IP address	ICS component	service	Description
1	10.1.1.3	MTU m13	http/ TCP 80	Web server service apached with known software vulnerabilities (outdated version).
(...)				

Table 8: Table for the documentation of IP network-based vulnerabilities

Relevant industrial standards (e.g. [VDI 2182 2011], Part 2) specify examples of requirements for the tabular documentation of vulnerabilities and their analyses.

When assessing the vulnerabilities, they must be assigned to the security objectives formulated in the ICS security concept (e.g. the availability of an MTU or confidentiality of production parameters) and the extent of the impairment determined. The assessment and effort estimate to eliminate the vulnerability is carried out on the respective subject level.

6.2.4.2 On-site review

The on-site review starts with an opening meeting with the main parties involved. This opening meeting is followed by interviews (see chapter 6.2.4.3) and an inspection of the production area including a visual inspection of the systems as well as a preliminary evaluation (see [BSI IS-Revision 2010], section 4, performing an IS revision).

During the on-site review, the following test methods are applied.

- Visual inspection of ICS components and premises
  - Do the components correspond to the inventory list and the documented function?
  - Are there any interfaces which are not intended (e.g. network cabling)?
  - Are the rooms equipped with access control systems according to the documentation? Are there undocumented modifications or deviations from room layout?
  - Are systems designated clearly and assigned to production areas?
  - In inaccessible areas, the visual inspection can be replaced by camera movements, records or indirect monitoring.
- Observations
  - Accidental perception of relevant events by the audit team
  - Understanding the particularities of the production process
  - Clear desk and clear screen status
- Technical checks
  - Alarm system, access control function, locked states

  - Operation of plants and HMIs by competent personnel
  - Testing of automated switch-off processes
  - Test triggering of sensors (e.g. light barrier, vibration, heat, water, smoke)
- Inspection of data (e.g. log files, HMI access, printed protocols)
  - Identifying security-relevant events in the records
  - Verifying taken measures (adequacy, completeness)
  - Verifying the documentation requirements
- Working through checklists

The on-site review is completed with a final meeting, in which the main observations are reflected to the parties involved and suggestions for eliminating identified vulnerabilities or deviations from the documentation are collected.

6.2.4.3 Interviews

The opening meeting with the main parties involved can be followed by interviews conducted with the personnel in the production area within the scope of the on-site review. The statements made during the interviews must be documented:

- Recording security-relevant observations made by the parties involved,
- Checking the level of knowledge with respect to policies, rules and instructions,
- Determining the training level of the personnel,
- Recording of procedures which have not been documented so far or procedures deviating from the documentation,
- Comparing job descriptions and actual job characteristics.

The audit plan may require to request written interviews (e.g. completing questionnaires) in advance to prepare the interviews.

6.2.5 Assessment

The audit team assesses the determined situations with respect to the formulated requirements from the ICS security concept and the comparison to the submitted documentation.

The completeness, quality and currency of the submitted documentation must already be assessed during the familiarisation phase. In this phase, it should be possible to subsequently improve the documentation in order to supplement any missing documents. The status of each partial document (advanced draft, final version, outdated version) and the quality (e.g. complete, only partially complete, incorrect; clarity, adequate description depth) must be determined as part of the assessment and documented in the audit report.

With regard to the security measures to be tested, the following scheme can be applied in accordance with the BSI IS revision[10] in order to determine the implementation status:

- Measure has been implemented
- Measure has been implemented partially

[10] https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/ISRevision/isrevision_node.html

- Measure has not been implemented
- Measure can be dispensed with (e.g. because other measures have adequate effects)

In the case of measures which have not or only partially been implemented, the security deficiency must be assessed. A suitable simple scheme has two stages: "security deficiency" or "serious security deficiency".

Deviations of the actual state from the documentation must be listed in detail. For each deviation, the following assessment must be carried out:

- Is there a deviation which can be eliminated solely by updating the documentation?
- Does the deviation indicate that one or several measures have not been implemented? (In this case, this deviation can be assessed according to the scheme for measures which have been implemented partially or not all.)
- Does the deviation indicate that specified requirements from the ICS security concept are not complied with? (In this case, the specified requirement must be designated and the non-compliance assessed with regard to the security concept.)

The vulnerabilities identified in the course of the auditing must be assessed by the auditors unless they have already been taken into account and assessed in the security concept:

- Which ICS components are affected by the threat? Which production areas are affected?
- Which (cross-component) function is affected by the vulnerability?
- Can the vulnerability be exploited? Which efforts are assumed to achieve this?
- Which objectives contrary to the security concept can a threat agent achieve by exploiting the vulnerability?
- Which physical effect and which damage can be achieved by exploiting the vulnerability?
- Which efforts to eliminate or mitigate the vulnerability are assumed according to available information?
- Are there indications that the vulnerability has already been exploited or is known by potential threat agents?

The assessment based on all of the mentioned aspects cannot be performed yet at the time the audit is completed, because additional information must be obtained (e.g. information provided by product suppliers) or because the test coverage was not complete according to the audit plan. To what extent an additional analysis of a vulnerability is required is covered as part of the recommendations to be made.

After the vulnerabilities have been assessed, the measures to be carried out and recommendations for the customer are formulated.

- The measures which have been implemented only partially or not all are listed unless it has turned out that they can be dispensed with.
- New measures which seem to be required due to the vulnerabilities determined with respect to the objectives specified in the security concept are listed.
- Recommendations regarding the adjustment of the security concept are formulated in the light of the identified situations (e.g. identification ineffective measures, re-assessment of risks due to technical progress, classification of assets).
- Recommendations as to how the detected vulnerabilities can be eliminated and which procedure is adequate are formulated.

6.2.6 Reporting

The customer must be notified of the audit report including the reference documents in writing. The report and its key results should be explained to the persons responsible in more detail as part of a presentation. The presentation should take place around the same time as the report is delivered. The type and scope of the audit report must already be defined in the coordination workshop.

The report should address the specifics of the ICS installation and describe the situations in the context of the production environment. The report should cover the following aspects:

- Members and management of the audit teams
- Contact persons of the customer, who have been involved in the audit
- Underlying documentation
- Audit plan and rules of engagement
- Explanation of the test methods
- Test results and protocols
- Listing of identified and assessed vulnerabilities
- Reportable events during the auditing
- Measures and recommendations
- Brief summary of the audit result

After the presentation, feedback talks may take place either in the entire group or in smaller groups with the parties involved. Praise and criticism can be addressed with respect to the procedure of the audit team and the support provided by the customer. Furthermore, test methods and results can be discussed with the technical experts with regard to the determined results.

6.2.7 Implementation of the measures and recommendations

After the audit has been completed and the audit report discussed, the formulated measures and recommendations are implemented as specified by the senior management.

Measures can relate to the mere re-configuration of a component (e.g. adjustment of a configuration file, change in the network topology for network segmentation), the updating of the software on the components (e.g. installation of a security update, installation of a newer version) or the installation and commissioning of a new security component (e.g. introduction of a firewall as an additional network component).

The implementation efforts therefore differ greatly. Whereas a re-configuration can be completed within a working day, the commissioning of an additional component might result in the planning of a long-term rollout project. The prioritisation of the measures and recommendations therefore has a significant impact on the planning and realisation of complex measures and must be performed in advance by the senior management.

6.2.8 ICS revisited

At a defined time after the completion of the audit, a re-audit can be performed to promote an iterative implementation process with respect to the measures and recommendations. Within the scope of a shortened procedure, the status of the audited areas is reviewed and both the deviation from the audited state and the deviation from the state aimed at determined. The audit team can verify the implementation of individual measures and recommendations and provide assistance in re-assessing the actual state. In the case of implementation difficulties or new technical developments, alternative measures and recommendations making it easier for the customer to achieve their security objectives can be formulated.

6.3 Test phase according to subject levels

6.3.1 Physical security

The auditing of the physical security includes reviewing the physical security plan referred to in chapter 5.5.

In this respect, the audit team checks both the documented concept and, where possible, the construction plans for completeness and suitability with respect to the designated security objectives and their implementation on site. The audit plan may require that only a segment (e.g. implementation check) is audited within the scope of the on-site review.

As part of the on-site review, especially passive security measures can be audited. Typical questions include:

- Do the existing walls, fences, ditches, windows and ducts comply with the defined security perimeters?
- Are existing access lines and communication connections protected physically?
- Are doors equipped with the documented access control function and does it function properly?
- Does the presence of the assets within security zones separated by perimeters comply with the security concept?
- Were ICS components with comparable security requirements summarised in zones?
- Are there unmanned production areas with a correspondingly defined security zone?
- Are the components, materials and media located in locked housings or security cabinets?
- Is access to ICS control mechanisms restricted according to role assignment?
- Are the access control systems maintained at regular intervals?

Active security measures are audited depending on the circumstances both on site in the production area and in a central place (e.g. gatekeeper area):

- Are doors and gates opened (only) after the authorisation has been verified?
- Are controllable barriers or other obstacles to vehicles included in the security concept? How are the mechanisms used?
- How is access in emergency situations controlled?

Supporting security measures are audited both on site and in a central place:

- Are available video cameras and motion sensors included in the security concept? Do they cover the area to be protected?
- How is recorded picture information managed? Is short-term access to a record specified for the test case possible?
- What reporting chain is available for different incidents and/or alarm situations in the production area? Was it complied with in the past?

6.3.2 Policies and processes

The subject level of policies and processes refers to the best practices defined in chapter 5.3 and goes beyond. The organisational framework conditions are checked. Such a list typically includes the following aspects:

- Has a security policy been drawn up and a security management established?
- Was a security organisation established? Do responsibilities and roles exist for all ICS components? Are qualified specialists assigned to the roles?
- Is the security concept documented for the production area and are the persons responsible familiar with this concept?
- Is the information related to the security of the ICS components (e.g. plans, organisation charts) maintained and protected against unauthorised access?
- Were the operational tasks of the asset owner, integrator and product supplier defined and complied with?
- Are there non-disclosure agreements with integrators and product suppliers? Are they still valid?
- Does a policy for the secure remote maintenance of components exist? Is a remote maintenance access possibility available and activated for product suppliers or integrators at the time of the audit? Who is responsible for the (de)activation?
- Are the administration and maintenance of the ICS components subject to a role concept? Can it be also implemented into practice under production conditions? (Deviations must be documented.)
- Does a software development policy or a configuration policy exist? How are they implemented?
- Are there rules for the disposal of hardware? Was a relevant policy applied?
- How is the patch and change management managed? Have the changes to the ICS prior to the audit been carried out as planned?
- Is a process which assesses new vulnerabilities which become known with respect to the ICS components in place? Were vulnerabilities which became known responded to adequately in the past?
- Is a business continuity plan available for a defined list of assets? Are the accompanying measures (e.g. backup) actually implemented into practice?
- Is an employment policy available? Does the operative personnel comply with this policy in the ICS environment?
- Are processes in place for when personnel change their position and leave the enterprise? Were these processes applied to the procedures prior to the audit?
- Is a qualification program established for the personnel with respect to security-relevant knowledge? How is the qualification status?

To determine the situations described in this checklist, both an on-site audit and carrying out interviews as well as a combination of test methods from both categories is suitable.

6.3.3 Network level

The auditing on the network level can start with examining the configuration of routers, switches and firewalls. This may include reading out and collecting the current configurations or reading them out directly from the individual devices.

To perform the security analysis on the network level, network sniffers are used. These tools record the network traffic in the individual subnetworks and, as a result, provide a file with the recorded network traffic, which can be used for further analysis. Since hubs which allow the direct recording of the entire data traffic at a free physical port are rarely used, other measures must be taken. The switch administrator can set up a so-called "mirror port" on the switch. On this mirror part, the entire data traffic of one or several other ports can be provided as a copy. Moreover, the data traffic can be recorded by means of a so-called "network tap" (a "T-piece" at the bottom network level) at the respective network connections. Both methods result in significant interference with the network and should therefore be used only with caution.

Based on the recorded data, the following aspects can then be checked as part of the audit:

- Are the end points of the detected data connections documented correctly in the network plan?
- Are the data connections provided in the communication infrastructure? (Deviations may include misconfigurations, poor quality of the documentation or a specific indication of malware.)
- Are there connections to office workstations or ERP systems?
- Are data transmissions encrypted?
- Does the data volume meet the expectations according to the component description?
- Can VPN and remote maintenance access be detected?
- Is the physical separation of networks or systems ("air gaps") complied with?
- Do the transmitted messages which are monitored allow a replay or a man-in-the-middle attack?

In addition to the tethered networks, wireless networks must also be tested as part of the audit. By means of corresponding scanners, the presence of the respective wireless network technologies can be determined and compared to the network plan. Furthermore, corresponding access data of undocumented networks can be determined under favourable conditions in order to apply active test methods in these networks as part of further audit steps.

Whereas the security analysis using the network sniffers without accompanying man-in-the-middle attacks is a passive test method which does not affect the ICS components apart from the additional load on the switch due to a mirror port, active test methods can identify vulnerabilities during the audit and cause incalculable problems. They should therefore be dispensed with wherever possible.

Active methods in the productive areas must be documented explicitly in the audit plan and must be covered by the rules of engagement agreed upon. The possible consequences should be considered before carrying out the methods, because components may fail!

Using a ping sweep and a port scan, the components accessible via the network and their respective network services can be requested actively in order to make a comparison with the network plan possible (see chapter 3.3.3). By means of an ARP scanner, the replies to ARP broadcast messages can be used to find components which block the ICMP packets and remain hidden in the case of ping sweeps. Using these tools makes it therefore possible to additionally check the following aspects:

- Are the network components documented in the network plan present and are the documented services available?
- Are there network components or services which are not documented?
- Are services blocked by the firewall (as documented)?
- Does the router and switch configuration comply with the network plan?

In this respect, the audit team must take into account that a communication attempt which deviates from the usual behaviour can already lead to undefined system states in the productive system. Two examples from the audit environment are referred to by the NIST (see [SP 800-53]): A ping sweep to an ICS network, which would have resulted in a ping reply of each connected device according to the protocol, surprisingly triggered a 180° rotation of a robot arm with a length of 3°m. Another sweep in an ICS network caused the standstill of a control unit within the production line of a chip production enterprise, which resulted in the loss of $ 50,000 worth of wafers. The ICMP echo request used in the case of these sweeps is an element of the (standardised) IP protocol and should be responded to correctly or ignored by a conform target system. In the case of (in some cases proprietary) network protocols used in the industrial environment, however, deviations from communication protocol standards must be taken into account.

6.3.4 Device level

The device level refers to all types of ICS components. HMIs, sensors and PLCs are particularly focused on. The examination on the client level starts with host-specific tests which are performed on the network level. Therefore, initial test data includes: IP address(es), open ports, operating system parameter as well as offered services of the host in the different subnetworks. This data must be compared to the documentation. Deviations must be documented.

Using vulnerability scanners, the vulnerabilities which can potentially be exploited via the network can be determined automatically. They relate to known vulnerabilities in the software which provides a service, old versions/missing updates in the case of server services, default passwords or weak passwords and misconfigurations on the operating system or service level (e.g. approvals). Several vulnerabilities can only be identified if the scanner can authenticate as a user or if access takes place via a certain subnetwork. These parameters must be taken into account in the audit plan (e.g. leaving a user account to the auditors, permission to use undocumented network access points which were identified during the examination on the network level).

The test results of the vulnerability analysis are used to review the following aspects:

- Are there outdated software versions (operating system components, server services, applications) on the system, for which vulnerabilities are known?
- Are there software security updates which are not installed (but recommended by the product suppliers) for the system?
- Does the installed software comply with the documentation?
- Does the system have insecure user access points (e.g. anonymous access, weak password, empty password, default password, terminal access which is no longer required etc.)?
- Are there different user roles on the system (e.g. user versus administrator) and are the privileges properly assigned to the roles?
- Are there remote administration tools or central software distribution mechanisms which correspond to a documented security policy?
- Are security-relevant system events recorded? Are the records from the past fully available?

On the security-specific network components (firewalls, routers, modem access), the following aspects must be checked especially in the case of host-based auditing:

- Is access via wireless networks secured in such a way that only connections documented in the network plan are possible?
- Do the firewall rules and routing tables correspond to the documented logical network connections?
- Is the VPN and modem access restricted to a whitelist of approved access points?
- Is VPN and modem access logged? Does the evaluation of the protocols show any irregularities?

For an identified potential vulnerability, an exploit can be developed for the further assessment of the exploitability by the audit team (see chapter 3.3.3). This exploit uses the vulnerability in order to show a possible system penetration. A reason for the development may be that the ICS asset owner would like to have a proof of the actual exploitability in order to be able to justify expensive measures and losses of production in the production environment. Moreover, the system behaviour can be tested in the case of an attack by means of the exploit code and the risk which is present by the vulnerability can thus be assessed more precisely.

6.3.5 Application level

In the ICS environment, an examination on the application level is particularly required for HMI system, data historian, historian database, engineering workstation and master terminal unit components. Compared to other components, they have a high system complexity which justifies breaking the analysis down into different logical levels. Furthermore, they have a direct network connection to the devices in the process management as part of the real time process management and the process management within the DMZ of the ICS.

The analysis can refer both to default applications (e.g. telnet, ftp, web server) and particularly be carried out with respect to applications tailored to the use of ICSs, such as web and database applications for data processing of the environmental data and production parameters measured in the ICS.

On the one hand, vulnerability scanners which have already been mentioned in the sections above (they can also be used in order to detect vulnerabilities such as SQL injection or cross-site scripting) are used for the examination on the application level. On the other hand, semi-automatic and manual analyses (e.g. test of individual functions, code review) are also required to include applications which are not or only inadequately covered by the vulnerability scanners in the analysis.

Within the framework of the audits on the application level, the following aspects can be checked:

- Are there remote access options to the component? Do they correspond to the documented condition?
- Is access allowed via protocols fraught with vulnerabilities, such as ftp, telnet, or an outdated SSH implementation? Are they restricted to the required communication relations?
- Is backup software installed on the system? Does it have vulnerabilities which can be exploited?
- Are there web-based vulnerabilities such as cross-site scripting?
- Are there vulnerabilities in the SSL implementation, such as self-signed certificates?
- Are there vulnerabilities as part of poor input validation, such as SQL injection or buffer overflows?
- Is authentication at the application level ensured? Are the documented user roles and privileges assigned?

6.3.6 Field process management

For ICS components in the field process management, the following aspects should be checked:

- Are the communication relations documented in the network plan?
- Are security mechanisms (such as the signing of messages and encryption of the transmitted user data according to OPC UA) applied according to the documentation?

6.3.7 ICS security test

The security functions themselves are audited by means of functional tests. The audit plan can list a subset of security functions which must be tested during the audit.

Depending on the presence of different security mechanisms, functional security tests can relate to the clarification of the following aspects.

- Is the authentication of the user forced in the case of tethered and wireless network access, modem access or VPN access?
- Is the user assigned the documented rights?
- Are unauthorised access attempts prevented and recorded in a log file? Are security-related events recorded reliably?
- Are the recorded log files evaluated automatically and is a suitable alarm generated if there are corresponding irregularities?
- Is access protection active?
- Is the alarm actually triggered in the case of alarm-relevant events?
- Are the virus definition files up to date? Is the anti-virus program used in accordance with the security concept?
- Is port security activated in the case of switches?
- Is an IDS active? Are alarms generated in case of relevant events?
- Are only dedicated DNS and active directory servers used and queried for the ICS components?
- Is the time synchronisation carried out by means of a dedicated NTP service?
- Are backup procedures complied with? Does the restoration process function properly?
- Are screen locks activated after a timeout period (if necessary)?

The test method applied with respect to these functional tests is regular, manual testing of the functionality based on a checklist.

7 Trends and resulting need for R&D

7.1 Current trends

7.1.1 Industry 4.0

The term "Industry 4.0" is characterised by the future project of the German Federal Government with the same name (see [BUND_2012]). This project deals with the trend towards increasing networking and performance of the industrial components used in production. The number four refers to a new, future level of industrialisation, i.e. the 4th industrial revolution. In this respect, this development joins in the ranks of the development stages of mechanisation, industrialisation and automation. In the development stage of Industry 4.0, the so-called "Internet of Things" has found its way into the factory in the form of a smart factory. It is characterised by networked, intelligent production components which exchange information independently, trigger actions and automatically and mutually control themselves.

With these new communication relations and the increasing transfer of intelligence to the production components result in the following potentials, among other things:

- Small-scale series from individual customer wishes can be produced economically up to a batch size of one.
- The use of resources can be optimised and processes can be designed more efficiently.
- Current characteristic figures can be obtained throughout the entire production process at all times.
- Short-term and flexible response to incidents as well as changes to the configuration are possible.
- New business models may arise.

With increasing complexity and communication infrastructure, this trend is also associated with risks, for example caused by an increased attack surface and networking beyond the limits of trust (e.g. for the integration of customers and business partners in the production process).

The following subjects will play an essential role in the design, structure and operation of the required infrastructure, among other things, with respect to this trend:

- Drawing up standards for the smart factory (e.g. a reference architecture) which take security aspects into account.
- Developing secure tools for the control of the increasingly complex and intelligent systems which also implement security functions.
- Securing production plants against the misuse and unauthorised access by people (in addition to the protection of people against the production plants). Therefore, security aspects should already be considered in the design phase of new infrastructure components (e.g. by means of an integrated security architecture).

7.1.2 Cloud architectures in the industry

Cloud computing is a technological paradigmatic change, summarising IT infrastructures such as software, server systems or services in a centralised structure (cloud) in a freely scalable manner, which can be accessed via a network. Unlike in publicly accessible cloud infrastructures for storing and sharing files or using resources via smartphones, cloud service providers and users can belong to the same organisation (so-called private clouds). However, the infrastructure in such a private cloud can be operated in the computer centre of the organisation or a third-party organisation.

An emerging trend towards cloud computing in the industry concerns the enterprise resource planning (ERP) with regard to materials management, logistics and business intelligence. In this respect, the cloud section "Software as a Service" (SaaS) plays an important role: The software provided via the cloud is then accessed only using Internet-capable PCs in the enterprise and limited to a browser as regards the requirements for the clients. Only the ERP resources which are also actually used by industrial enterprises are reimbursed (so-called pay-per-use). In a service level agreement, the services of which the industrial enterprise are assured by the service provider are contractually agreed upon. The administration of the ERP software as well as services such as updates, maintenance, backups) is performed centrally. The enterprise using the cloud infrastructure expects major cost savings in the field of IT components which otherwise are to be provided and maintained locally.

Another cloud-based innovation concerns carrying out remote maintenance tasks. Thus, individual communication solutions between components suppliers and operators can be developed. *"In the future, specialists will no longer connect manually to machines. The production systems automatically connect to their cloud-based telepresence platform as social machines and search for the required experts depending on the respective situation"* (see [DAT 2013]). The ICS components then extend their functionality independently by automatically reloading required configurations and data. Whether this future vision will actually become a trend cannot be foreseen yet. However, these future visions illustrate the substantial potential which also develops for industrial and previously non-IT production areas due to the spreading of cloud infrastructures.

In a benchmark paper, the BSI has drawn up recommendations for secure cloud computing which primarily address cloud service providers (CSPs) and offer a basis for the discussion between CSPs and cloud customers (see [BSI 2012]). The recommendations relate, among other things, to aspects such as computer centre security, server security, network security, application and platform security, data security and cryptographic mechanisms.

With increasingly widespread use, cloud services become interesting for threat agents especially if critical resources related to industrial production are stored in central computer centres and can be attacked. Therefore, international standards are required for cloud security in the medium term, on the basis of which service providers can be evaluated and certified.

7.2 Higher levels of security

7.2.1 Best practices for product suppliers, asset owners and integrators

In different phases of the product life cycle, different parties influence an ICS (e.g. product suppliers, integrators, asset owners). For the secure production, integration and operation of ICSs, security guides are therefore required for all parties involved. This applies particularly against the backdrop of the previously historically subordinate role of security for ICSs.

In the past, recommendations and measures regarding the security of ICSs were covered in standards primarily for asset owners and thus almost exclusively for secure operation. In the last few years, more and more requirements were additionally drawn up by asset owners for ICS product suppliers (e.g. [DHS CSPL 2009], [WIB 2010], [BDEW 2008]), which should be used as procurement criteria for ICS.

Against the backdrop of frequent security incidents in the last few years, best practices for product suppliers should also be collected in addition to the requirements from asset owners. In this manner, for example, vulnerabilities caused in production can be detected and eliminated at an early stage, which otherwise may only be compensated with difficulties during subsequent operation by means of additional security measures.

Therefore, future close collaboration between the parties involved in the product life cycle, i.e. product suppliers, integrators, asset owners, is absolutely necessary for the secure production, integration and operation of ICSs. In a manner comparable to chapter 5, best practices could be useful for product suppliers in this respect. Furthermore, the BSI has already provided product suppliers with information on the different subjects mentioned above at "http://www.allianz-für-cybersicherheit.de".

7.2.2 Integration of safety and security

For historical reasons, the widely recognised industry standards primarily cover risks arising from the production plant (safety). However, security aspects to protect the production plant against people and thus aspects of misuse or unauthorised access are not taken into account or taken into account to a little extent (security). Safety and security requirements have been combined in the world of standards up to now at most rudimentarily.

As described in chapter 4, there are several standards, some of which have far-reaching requirements for ICS security. In the future, these security requirements must be brought into line with safety requirements and safety and security requirements must be integrated into the world of standards. To achieve this, there are initial efforts with respect to standardisation and the revision of standards.

7.2.3 Tool for ICS audits

In the past, audits regarding the security of ICS plants were not carried out or were performed very differently due to the absence or lack of information in the industry sectors. As a result of the ever-increasing awareness of the subject of security, checking conformity according to recognised industry standards is becoming more and more important. In this respect, chapter 6 describes approach to be followed until a comprehensive ISMS has been established.

To carry out standardised ICS audits, both the procedure and the examined contents and the test depth should be comparable. A tool for ICS audits can support the auditors in performing their tasks and ensure comparability.

In the USA, for example, there is a freely available tool developed by the DHS, which supports the auditors in carrying out the audits. The so-called Cyber Security Evaluation Tool (CSET®, see [ICSCERT CSET 2013]) helps to determine and access the IT assets to be protected in a systematic procedure. This is based on pre-defined questions and the comparison to recognised industry standards (e.g. from the NIST, NERC, DoD and ISO). As a result, the auditor is provided with a listing of recommendations from the standards and best practices, which are sorted according to priority. This tool, however, cannot be applied to plant operators in Germany due to the supported standards.

Asset owners of ICS plants lack a tool which can be applied to small and medium-sized enterprises (SMEs) in particular which do not have the financial and personnel resources to implement an information security management system according to ISO/IEC 27001 (see chapter 4.1.1.1) or BSI IT-Grundschutz. A lightweight possibility which allows a cost-efficient and fast introduction to ICS security especially for SMEs is therefore required. The asset owner could, for example, be guided by means of a defined set of questions regarding security in order to obtain answers with respect to the threat scenario and the protection requirements. On the basis of these answers, the asset owner is provided with information for possible security measures and specific implementation measures.

7.2.4 Further development of defence-in-depth strategies

The defence-in-depth approach is a concept that provides securing on the different layers of an architecture so that a redundancy becomes active only on one level or only a few levels if the security architecture fails.

The threat agent is thus forced to break through security barriers throughout several levels and so are hindered in their progress or at least slowed down.

With respect to IT security of ICSs, this results in the requirement to develop security measures on the field process management further so that their security does no longer depend on their physical inaccessibility and the security of the control level. An effective defence-in-depth strategy would also ward off a threat agent who has direct access to the field process management. For example, unauthorised access via an unprotected maintenance access is possible. Additional barriers can then also prevent a threat agent from finding further attack routes within the field process management and being able to attack the realtime process management via RTU and PLC.

Elements for implementing the defence-in-depth strategy include fieldbus firewalls, secure fieldbus protocols and automated anomaly detection in the fieldbus communication.

8 Summary and outlook

For a long time, ICSs have already been essentially necessary for the measurement and control of processes, for example for the automation of processes and for monitoring large networks and systems. The trend which started several years ago towards increasingly networking these system and using standard IT products now makes it necessary to also consider security aspects from conventional IT for ICSs. The fact that security will play an increasingly important role in control and automation plants in future has already been shown by various incidents which particularly have an adverse impact on the security objectives of availability and integrity, but also that of confidentiality.

This compendium is the starting and connection point for all further technology-oriented projects and developments of the BSI in the context of security of control and automation plants. Together with future projects, an ICS security standard reference work is thus created.

The compendium is to be supplemented successively by additional information and also adjusted to new conditions and circumstances. The next goal is to make best practices available to product suppliers, mechanical engineers and integrators, which provide them with information and support for the development of secure products.

Particularly a generally stronger implementation of security measures in ICSs, it is necessary to counteract the threats for ICSs. On the one hand, this requires enhanced cooperation of conventional IT and ICSs and, on the other, an integration of security aspects in safety requirements (security for safety). In addition to the asset owners who are primarily addressed in this compendium by means of the best practices, integrators and product suppliers must make a necessary contribution to increase the ICS security level, for example, by increased tests of the ICS products.

Table of abbreviations

Abbreviation	Full designation
ABK	*Anzeige- und Bedienkomponente* (German term referring to display and operation components)
ALG	Application level gateway
BDEW	*Bundesverband der Energie- und Wasserwirtschaft* [German Association of Energy and Water Industries]
BUB	*Beobachtung- und Bedienkomponenten* (German term referring to monitoring and operation components)
CENELEC	Comité Européen de Normalisation Électrotechnique
CERT	Computer Emergency Response Team
CIF	Control in the Field
CIP	Common Industrial Protocol
COTS	Commercial-off-the-Shelf
CPNI	Centre for the Protection of National Infrastructure
CSSP	Control Systems Security Program
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DCS	Distributed Control System
DDE	Dynamic Data Exchange
DHS	Department of Homeland Security
DIN	*Deutsches Institut für Normung* [German Institute for Standardization]
DKE	Verband der Elektrotechnik Elektronik Informationstechnik [German Association for Electrical, Electronic & Information Technologies]
DMZ	Demilitarized Zone
DNS	Domain Name System
EOS	End of Support
EPA	Ethernet for Plant Automation
ERP	Enterprise Resource Planning
ES	Engineering Station
ETSI	European Telecommunications Standards Institute
EWS	Engineering Workstation
FIRST	Forum of Incident Response and Security Teams
HMI	Human Machine Interface
IACS	Industrial automation and control systems
ICS	Industrial Control System

Abbreviation	Full designation
IDS/IPS	Intrusion Detection/Prevention System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISA	International Society of Automation
ISMS	Information security management system
ISO	International Organization for Standardization
KMU	*Kleine und mittlere Unternehmen* (German term referring to small and medium-sized enterprises (SMEs))
KRITIS	*Kritische Infrastrukturen* (English term: Critical Infrastructures)
MES	Manufacturing Execution System
MitM	Man-in-the-Middle
MTU	Master Terminal Unit
NAMUR	Normenarbeitsgemeinschaft für Meß- und Regeltechnik [International user association of automation technology in process industries]
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
ODBC	Open Database Connectivity
OLE	Object Linking and Embedding
PAT	Process Analytical Technology
PG	*Programmiergerät* (German term referring to a programming device)
PLC	Programmable Logic Controller (German term: Speicherprogrammierbare Steuerung)
PLS	*Prozessleitsystem* (English term: Distributed Control System)
PNK	*Prozessnahe Komponente* (German term referring to a process-oriented component)
RBAC	Role Based Access Control
RIO	Remote I/O
RTU	Remote Terminal Unit
SaaS	Software-as-a-Service
SCADA	Supervisory Control and Data Acquisition
SFTP	SSH File Transfer Protocol
SIEM	Security Information Event Management
SIL	Safety Integrity Level
SNMP	Simple Network Management Protocol
SPS	*Speicherprogrammierbare Steuerung* (English term: Programmable Logic

Abbreviation	Full designation
	Controller)
VDE	Verband der Elektrotechnik Elektronik Informationstechnik [German Association for Electrical, Electronic & Information Technologies]
VDI	*Verein Deutscher Ingenieure* [The Association of German Engineers]
XSS	Cross Site Scripting

References

BSI GS Federal Office for Information Security (BSI): IT-Grundschutz Catalogues 12th version. Bonn: Federal Office for Information Security (BSI) 2011

DUD 2009 Fox, Dirk: Mindestlängen von Passwörtern und kryptographischen Schlüsseln. [Equivalent English translation of the title would be: *Minimum length of passwords and cryptographic keys.*] Datenschutz und Datensicherheit Nr. 10 [Equivalent English translation of the title would be: *Data protection and data security No. 10*] (October 2009): 620-623. Wiesbaden: Springer Gabler Verlag 2009

BSI 2008 Federal Office for Information Security (BSI): S 2.11 Provisions governing the use of passwords. IT-Grundschutz Catalogues 12th version. Bonn: Federal Office for Information Security (BSI) 2011

OWASP Top10 Open Web Application Security Project: OWASP Top Ten Project. Version 2010. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project (11 June 2013)

IX 2013 Waibel, Stefan: Gezielte Abwehr: Wie man sich vor Denial-of-Service-Angriffen schützt. [Equivalent English translation of the title would be: *Targeted defence: How to protect against denial of service attacks.*] iX No. 5 (May 2013): 64-67 Hanover: Heise Zeitschriften Verlag GmbH & Co. KG 2013

BSI 2012 Federal Office for Information Security (BSI): Security Recommendations for Cloud Computing Providers. Bonn: Federal Office for Information Security (BSI) 2012

ISO/IEC 27000 International Organization for Standardization; International Electrotechnical Commission: ISO/IEC 27000 series "Information technology – Security techniques"

ISO Standards 2013 International Organization for Standardization: Standards catalogue. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306 (11 June 2013)

BITKOM/DIN 2007 BITKOM; DIN: Kompass der IT-Sicherheitsstandards. [Equivalent English translation of the title would be: *Compass of security standards*.] Version 3.0. Berlin: BITKOM, DIN 2007

BMWi 2009 OFFIS - Institut für Informatik, SCC Schwarz Communication Consulting, mpc management project coaching: Untersuchung des Normungsumfeldes zum BMWI-Förderschwerpunkt "e-Energy - IKT-basiertes Energiesystem der Zukunft". [Equivalent English translation of the title would be: *Examination of the standardisation environment for the major funding project of the German Federal Ministry of Economics and Technology (BMWi) "E-Energy: ICT-based energy system of the future".*] http://www.e-energy.de/documents/Zusammenfassung-2009-02-23_Untersuchung_des_Normungs-_und_Standardisierungsumfeldes__E-Energy%281%29.pdf (11 June 2013)

IEC 62351 International Electrotechnical Commission: IEC 62351 Power systems management and associated information exchange – Data and communication security

Cleveland 2012 Cleveland, Frances: IEC 62351 Security Standards for the Power System Information Infrastructure. http://xanthus-consulting.com/Publications/documents/IEC%20_TC57_WG15_White_Paper.pdf (11 June 2013)

DIN SPEC 27009 2013 Deutsches Institut für Normung e. V. [German Institute for Standardization]: DIN SPEC 27009. http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&subcommitteeid=54742877&artid=151100155&bcrumblevel=2&languageid=de (12 June 2013)

DIN SPEC 27009 2012 Deutsches Institut der Normung e.V. [German Institute for Standardization]: DIN SPEC 27009:2012-04 Guidance for information security management of power supply control systems based on ISO/IEC 27002. Berlin: Deutsches Institut der Normung e.V. 2012

TeleTrusT 2012 Kasper, Rolf-Dieter: DIN SPEC 27009 Informationssicherheit in Energienetzen. [Equivalent English translation of the title would be: *Information security in energy grids*.] http://www.teletrust.de/uploads/media/TeleTrusT-Infotag_SmartGrid_Kasper.pdf (11 June 2013)

VDI 2182 2011 Verein Deutscher Ingenieure; Verband der Elektrotechnik, Elektronik, Informationstechnik [German Association for Electrical, Electronic & Information Technologies]: VDI/VDE 2182 IT-security for industrial automation. Berlin: Beuth Verlag GmbH 2011

VDI/VDE Richtlinien 2013 VDI e. V.: VDI Guideline: VDI/VDE Manual "Automation". http://www.vdi.de/7776.0.html?&tx_vdirili_pi2[showUID]=89690 (12 June 2013)

NA 115 2006 Normenarbeitsgemeinschaft für Meß- und Regeltechnik in der chemischen Industrie [User Association of Automation Technology in Process Industries]: IT-Security for Industrial Automation Systems Constraints for measures applied in process industries. NAMUR Worksheet 115. 1st edition. Leverkusen: NAMUR (c/o Bayer Technology Services GmbH) 2006

BSI 100-1 Federal Office for Information Security (BSI): BSI-Standard 100-1: Information Security Management Systems (ISMS)

BSI 100-2 Federal Office for Information Security (BSI): BSI-Standard 100-2: IT-Grundschutz Methodology

BDEW 2008 BDEW Bundesverband der Energie- und Wasserwirtschaft e.V. [German Association of Energy and Water Industries]: White paper "Requirements for Secure Control and Telecommunication Systems". Version 1.0. Berlin: BDEW 2008

OE BDEW 2012 Oesterreichs Energie; BDEW: Anforderungen an sichere Steuerungs- und Telekommunkationssysteme: Ausführungshinweise zur Anwendung des BDEW Whitepaper. [Equivalent English translation of the title would be: *Requirements for Secure Control and Telecommunication Systems: Implementation instructions for the application of the BDEW white paper.*] Version 1.0. Vienna: Oesterreichs E-Wirtschaft, Berlin: BDEW 2012

VGB R 175 VGB PowerTech e.V.: VGB-R 175 Guideline: IT Security for Generating Plants. 1st edition. Essen: VGB PowerTech e.V. 2006

NERC CIP North American Electric Reliability Corporation: Critical Infrastructure Protection Standards. http://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx (11 June 2013)

SP 800-53 National Institute of Standards and Technology: Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. Version 4. Gaithersburg (Maryland, USA): NIST 2013

SP 800-82 National Institute of Standards and Technology: Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security. Gaithersburg (Maryland, USA): NIST 2011

NISTIR 7628 National Institute of Standards and Technology: NISTIR 7628 Guidelines for Smart Grid Cyber Security. Gaithersburg (Maryland, USA): NIST 2010

DHS CSPL 2009 Department of Homeland Security: Cyber Security Procurement Language for Control Systems. Washington (District of Columbia, USA): Department of Homeland Security 2009

DHS Assessment 2010 Department of Homeland Security; Centre for the Protection of National Infrastructure: Cyber Security Assessments of Industrial Control Systems.

Washington (District of Columbia, USA): Department of Homeland Security 2010

DHS DiD 2009 Department of Homeland Security: Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies. Washington (District of Columbia, USA): Department of Homeland Security 2009

DHS PM 2008 Department of Homeland Security: Recommended Practice for Patch Management of Control Systems. Washington (District of Columbia, USA): Department of Homeland Security 2008

DHS Modem 2008 Department of Homeland Security: Recommended Practice for Securing Control System Modems. Washington (District of Columbia, USA): Department of Homeland Security 2008

DHS Remote 2010 Department of Homeland Security; Centre for the Protection of National Infrastructure: Configuring and Managing Remote Access for Industrial Control Systems. Washington (District of Columbia, USA): Department of Homeland Security 2010

DHS ZigBee 2007 Department of Homeland Security: Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments. Draft. Washington (District of Columbia, USA): Department of Homeland Security 2007

DHS IR 2009 Department of Homeland Security: Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability. Washington (District of Columbia, USA): Department of Homeland Security 2009

DHS Standards 2009 Department of Homeland Security: Catalog of Control Systems Security: Recommendations for Standards Developers. Washington (District of Columbia, USA): Department of Homeland Security 2009

DHS OPSEC 2007 Department of Homeland Security: Recommended Practice: Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Systems Environments. Version 1.0 (draft). Washington (District of Columbia, USA): Department of Homeland Security 2007

DHS Personnel 2004 Department of Homeland Security: Personnel Security Guidelines. Washington (District of Columbia, USA): Department of Homeland Security 2004

CPNI 2008 Centre for the Protection of National Infrastructure: Good Practice Guide - Process Control and SCADA Security. CPNI 2008

CPNI 2005 Centre for the Protection of National Infrastructure: Good Practice Guide - Firewall Deployment for SCADA and Process Control Networks. CPNI 2005

IEC 62443 International Electrotechnical Commission: IEC 62443 series of standards "Industrial communication networks - Network and system security"

BSI CS-061 Federal Office for Information Security (BSI): Cyber security recommendation: Industrial Control System Security: Innentäter [Equivalent English translation of the title would be: *Insiders*]

BSI IDS Federal Office for Information Security (BSI): BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen. [Equivalent English translation of the title would be: *BSI guide for the introduction of intrusion detection systems.*] https://www.bsi.bund.de/DE/Publikationen/Studien/IDS02/index_htm.html (11 June 2013)

RFC 2845 2000 Network Working Group: Request for Comments 2845: Secret Key Transaction Authentication for DNS. Fremont (CA, USA): Internet Engineering Task Force 2000

BSI LogDaten Federal Office for Information Security (BSI): Studie über die Nutzung von Log- und Monitoringdaten im Rahmen der IT-Frühwarnung and für einen sicheren IT-Betrieb. [Equivalent English translation of the title would be: *Study on the* *use of log and monitoring data as part of IT early warning and for secure IT operation.*] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Logdaten/logdatenstudie_pdf.pdf?__blob=publicationFile (11 June 2013)

IS 10 — Federal Office for Information Security (BSI): Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz. [Equivalent English translation of the title would be: *Information security revision - A guide for IS revision on the basis of IT-Grundschutz.*] Version 2.0. Bonn: Federal Office for Information Security (BSI) 2010

BSI IS-Revision 2010 — Federal Office for Information Security: Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz. [Equivalent English translation of the title would be: *Information security revision - A guide for IS revision on the basis of IT-Grundschutz.*] Version 2.0. Bonn: Federal Office for Information Security (BSI) 2010

BUND_2012 — Federal Ministry of Education and Research: Industrie 4.0. [Equivalent English translation of the title would be: *Industry 4.0.*] http://www.hightech-strategie.de/de/59.php (10 May 2013)

DAT 2013 — Deutsche Akademie der Technikwissenschaften [German National Academy of Science and Engineering]: Recommendations for implementing the strategic initiative INDUSTRIE 4.0. http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Projekte/Laufende_Projekte/Industrie_4.0/Bericht_Industrie_4.0_barrierefrei.pdf (13 May 2013)

WIB 2010 — Werkgroup voor Instrument Beoordeling: M 2784-X-10 Process Control Domain - Security Requirements for Vendors. Version 2.0. Den Haag (NL): WIB 2010

ICSCERT CSET 2013 — Industrial Control Systems Cyber Emergency Response Team: Cyber Security Evaluation Tool (CSET), http://ics-cert.us-cert.gov/Assessments, accessed on 10 May 2013

Yang 2006 — Yang, Dayu; Usynin, Er; Hines, J. Wesley: Anomaly-Based Intrusion Detection for SCADA Systems. 5th International Topical Meeting on Nuclear Plant Instrumentation. 2006

Tsan 2005 — Tsang, Chi-Ho; Kwong, Sam: Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction. IEEE International Conference on Industrial Technology (2005): 51–56 IEEE 2005

ISCdiary 2012 — Pelaez, Manuel; Santander, Humberto: Snort 2.9.2 now supporting SCADA protocol checks. http://isc.sans.edu/diary/Snort+2.9.2+now+supporting+SCADA+protocol+checks/12346 (13 May 2013)

Gao 2010 — Gao, Wei; Morris, T.; Reaves, B.; Richey, D.: On SCADA control system command and response injection and intrusion detection. eCrime Researchers Summit (2010): 1–9. eCrime 2010

Vald 2009 — Valdes, A.; Cheung, S: Intrusion Monitoring in Process Control Systems. 42nd Hawaii International Conference on System Sciences (2009): 1–7. HICSS 2009

Gold 2013 — Goldenberg, Wool: Accurate Modeling of Modbus/TCP for Intrusion Detection in SCADA Systems. 7th Annual IFIP Working Group. ICCIP 2013