IT Security in Production Facilities

An Introduction for Small and Medium-sized Enterprises

Prof. Karl-Heinz Niemann – Hanover

Prof. Karl-Heinz Niemann
Email: Karl-Heinz@Niemann-on-line.de

In cooperation with WAGO Kontakttechnik GmbH & Co. KG

Table of Contents

1. Introduction

This document concerns IT security in production facilities. It is intended for small and medium-sized enterprises that are looking for a simple procedural model for ensuring IT security in production areas.

In order to raise readers' awareness of IT security in production facilities, security incidents are presented in section 2. It is clear that cyber attacks on production facilities in this day and age are not random, but are instead based on a targeted process.

An overview of the most important standards and recommendations on the topic of "IT security in production" then follows in section 3.

Section 4 develops a concept for setting up an IT security system for small and medium-sized enterprises (SMEs) on the basis of a ten-point plan. The focus is not only on technical measures, but also in particular on the most frequently neglected organizational measures.

Section 5 then describes the outlook for future requirements and solutions in the context of Industry 4.0.

2. The Current State of IT Security in Facilities with Automation Technology

This section gives an overview of the current state of IT security in production areas. The challenges for today's production facilities will be identified on the basis of known security incidents. The top 10 threats of the German Federal Office for Information Security (BSI) will serve as a basis for this.

2.1. Known Security Incidents in Production Facilities

The requirements on IT security in production areas are constantly changing. In the past IT security incidents in production areas were usually "collateral damage" of ordinary malware that accidentally ended up in a production facility. One of the first known incidents of this type was the attack on various Daimler Chrysler plants in 2005 by the malware "Zotob" [PAK2005]. 13 of the company's plants around the world were affected. The damage is estimated at USD 14 million [BYR2009].

More recent incidents show that malware directed explicitly against production facilities is also being used more and more. The most prominent case to date, "Stuxnet" [FAL2011] [LAN2013], was directed against an Iranian uranium enrichment facility. This case is presumed to have originated from the US and Israel [BRO2011]. Apart from this, further incidents are documented that cannot be ascribed to government intervention. For example, the German Federal Office for Information Security (BSI) reports a dedicated attack on a blast furnace in Germany, which damaged it [BSI2014e]. Furthermore, there now exists malware that attacks components of automation systems in a targeted fashion. For example, ICS-CERT describes malware that attacks OPC servers [CERT2014].

An attack on the power supply system of Ukraine on 2015-12-23 represents a new dimension of cyber attacks on automation systems and critical infrastructure [CERT2016]. Three energy providers were attacked at nearly the same time, which led to a power outage for 225,000 customers. During the attack, circuit breakers in the power grid were operated unchecked via remote access. Data on control computers was deleted at the same time.

Besides industrial automation systems, building automation components are affected in the same way. A case was documented in 2013 in which heating systems were connected to the Internet for the purpose of remote maintenance without sufficient security [EIK2013] [STA2013a]. The lack of safeguards allowed external actors to access these systems. Although the vulnerability was published in the specialist press

and corrected by the manufacturer, a large number of vulnerable heating systems were still accessible unsecured on the Internet even two years later [STA2015] The users did not install the security updates provided; the equipment remains vulnerable.

The maritime sector must also face the challenges of cyber security. Although the automation systems used on ships are bolstered and certified for this special purpose, they are still usually based on conventional automation systems. Thus the same threats face these systems as face conventional automation systems [JEN2015]. Furthermore, additional electronic systems for navigation and collision avoidance enlarge the target for potential attackers [DIR2015].

In what follows this document will address production technology systems of the process and manufacturing industry.

2.2. Future Challenges for IT Security in Production Areas

Further escalation of the threats to automation systems must be expected in the future. This is suggested by the number and development of documented attacks over time. The increase in interconnectedness that accompanies Industry 4.0 in order for this purpose of realizing horizontal and vertical integration of production processes will lead to further possibilities for attacks. In a representative survey by the Allensbach Institute, 88 % of the managers surveyed identify effective protection against cyber attacks as the greatest challenge for introducing Industry 4.0 [DEU2015].

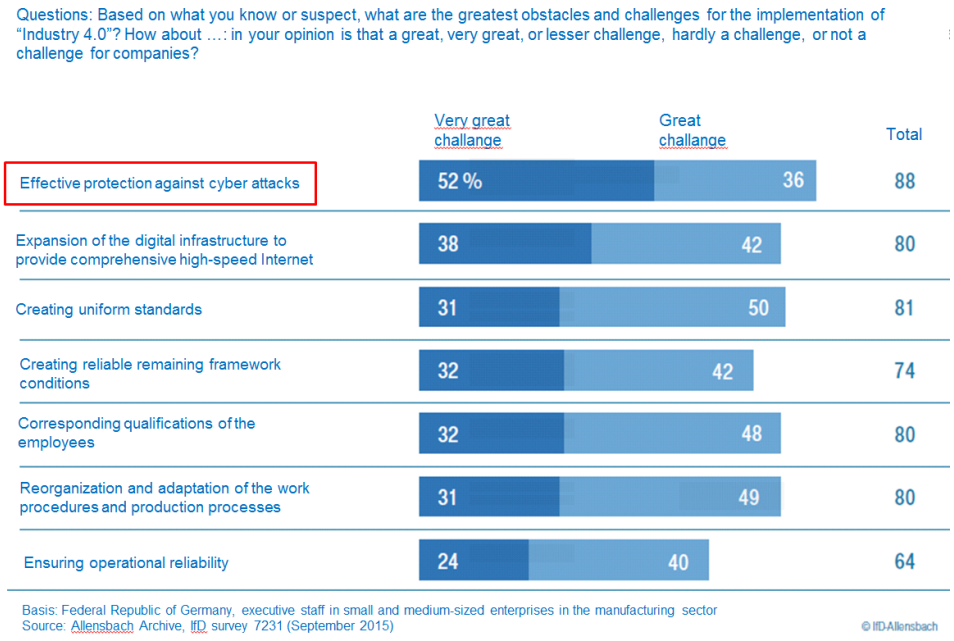

Figure 1: Obstacles and Challenges for the Implementation of Industry 4.0 [DEU2015]

The German Federal Office for Information Security publishes a list of the top 10 threats to automation systems at regular intervals. The current issue [BSI2016a] identifies the threats given in Table 1 and their ranking.

Rank	Threat	Fields of Activity
1	Social engineering and phishing	Humans, processes
2	Introducing malware via removable media and external hardware	Processes, technology
3	Infection with malware via Internet and intranet	Network, technology
4	Incursion via remote maintenance access	Processes, network
5	Human misconduct and sabotage	Humans, processes
6	Control components connected to the Internet	Network, technology
7	Technical misconduct and *force majeure*	Technology
8	Compromising extranet and cloud components	Network, technology
9	"(Distributed) Denial of Service" attacks	Networks, robustness
10	Compromising smartphones in the production environment	Humans, processes, technology

Table 1: Top 10 Threats, Augmented with Fields of Activity

It is clear that the top 10 threats given can be divided into different types of attacks with associated fields of activity. Attacks can occur through different routes, e.g. over the network or via compromised components (USB sticks, smartphones), but also through social engineering or phishing. Overloading components or networks with a flood of meaningless requests (Denial of Service, Distributed Denial of Service) also constitutes one type of attack. On the basis of the threats described, the next section will now derive the fields of activity for implementing an IT security concept for production facilities.

2.3. Fields of Activity for IT Security in Production Areas

To clarify the fields of activity, the author has added a column to Table 1 on the right with fields of activity. Individual issues can be associated with one or more fields of activity, which are described briefly below:

- **Humans:** Humans operate and monitor the production facility and should ensure its security. At the same time, humans represent a vulnerability for IT security. They may unintentionally allow third parties access to the facility via social engineering and phishing. In cases of misconduct or sabotage, humans intentionally or unintentionally compromise the IT security of the facility.
- **Technology**: The technology used (control components, network components) must be protected against attacks. Known vulnerabilities must be elimi-

nated promptly. Regular communication with the manufacturer of the components, e.g. by subscribing to security alerts, is advisable.

- **Processes**: Not all aspects of IT security can be addressed through technology. In many cases, corresponding processes (rules, regulations) must be defined in addition to the technology. Employees must be trained regularly in these processes. Compliance with the processes must be monitored, and any misconduct that occurs must be penalized. Thus this point is related to the point "Humans".
- **Network**: Although the communication network of a production facility belongs under Technology, it is listed here separately. In many cases, the network represents **the** gateway for attacks. Particular attention is necessary here in order to isolate the production network sufficiently well from the rest of the corporate network and from the Internet in particular.
- **Robustness**: "Denial of Service" attacks and "Distributed Denial of Service" attacks are usually directed against a company via the Internet and strike the outer perimeter of the company first. Even if an attack must penetrate additional perimeters in order to break through to the production facility, automation systems still must exhibit a certain robustness against overload situations.

The fields of activity described show that IT security for production facilities is not exclusively a technical problem. Besides technical problems (a vulnerability in the software; software patch not installed), other vulnerabilities may include organizational shortcomings (employees do not know that certain things are prohibited; rules on access to system components).

The following fields of activity can be derived from this state of affairs. Besides the technical aspects and network communication aspects, the IT security concept of a production facility must also take social aspects (human behavior, human misconduct) into account. Only a structured and layered approach that takes all aspects into account in an integrated way can ensure optimal protection of the facility. Such an approach is described by the term "Defense in Depth" [DHS2016b].

The planning, implementation, and ongoing operation of a "Defense in Depth" concept is no easy task for small and medium-sized enterprises in particular. A large amount of know-how is required in order to set one up. The resources required for this are usually scarce in the company, or the necessary training in this special domain is lacking. Therefore future concepts are needed that provide solutions for SMEs that are economical but still secure.

3. Standards, Guidelines, and Laws

A number of standards and series of standards are available to companies in the area of IT security. The standards specify the state of the article and thus make a standardized procedure possible for the design, implementation, operation, and certification of IT security systems.

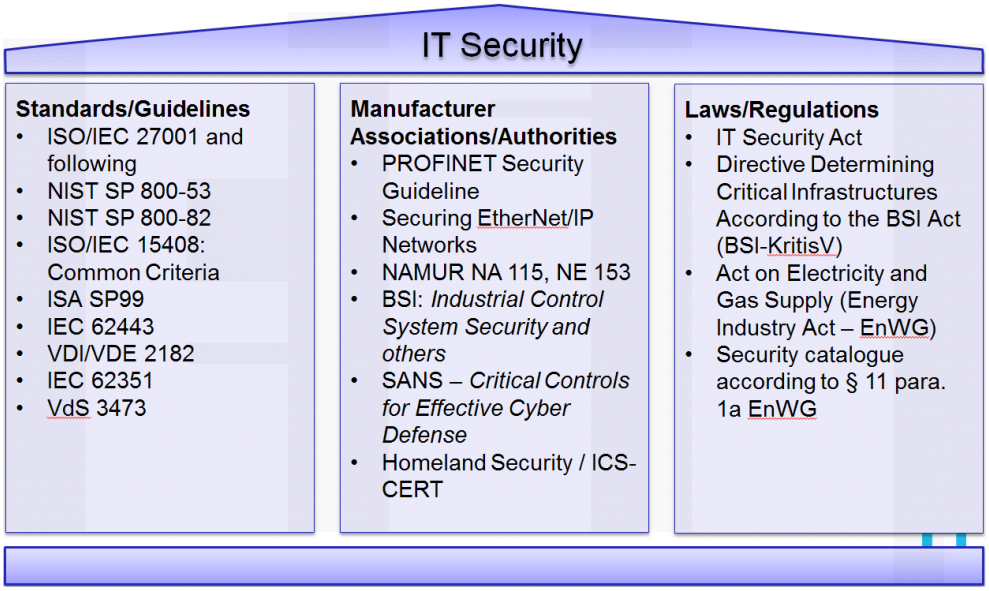

Figure 2: Overview of IT Security Standards

Figure 2 gives an overview of IT security standards. Besides standards for the office area (ISO 27000 series, IEC 15408, BSI basic protection catalogue [Grundschutzkatalog]), standards that address production areas in particular (ISA SP99/IEC62443, IEC 62351, VDI/VDE 2189) are also listed. The list is supplemented with a series of standards of manufacturer/user associations (PROFINET, EtherNet/IP, NAMUR) and authorities (BSI, Homeland Security).

The following sections provide an overview of the state of standardization. It first examines the general IT security standards. There then follows an overview of special standards for automation technology and recommendations of manufacturer organizations. The section ends with future prospects of the IT Security Act.

3.1. Standards for Office Areas

IT security in office areas has been specified through corresponding standards for many years. The ISO 27000 series of standards provides a comprehensive set of standards that, besides the technical aspects, also describe the associated processes.

An overview of the series of standards can be found in [KER2016], for example. IT security systems can also be certified correspondingly according to the standard. The certification procedure can be found in [KER2013], for example. Certification according to the ISO 27000 series of standards is considered complex and laborious. Therefore, it is primarily companies that are considered especially exposed (banks, payment service providers) that are certified. SMEs usually do not have ISO 27000 certified IT security systems.

On the basis of the ISO-27000 series of standards, the German Federal Office for Information Security specifies a series of basic protection catalogues (Grundschutzkatalogen) [BSI2016c] that allow easier access to the standard. The BSI also provides appropriate checklists and data entry forms. This gives SMEs easier access to the topic of IT security.

With the [VDS_3473] guidelines, the VDS offers principles for cyber security in office areas tailored to the needs of small and medium-sized enterprises. Certification according to this standard is possible. The level of effort is tailored to the needs of small and medium-sized enterprises and significantly less than for certification according to the ISO-27000 series of standards.

3.2. Standards for Production Areas

The standards described in section 3.1 address IT security in office areas. This means the IT of a company that has no production facilities (e.g. banks), or the part of a company in which no production facilities are located (e.g., administration, sales, human resources, etc.). The requirements in office areas are prioritized as follows: confidentiality, integrity, and availability. Figure 3 shows the prioritization of these security objectives for office areas on the side.

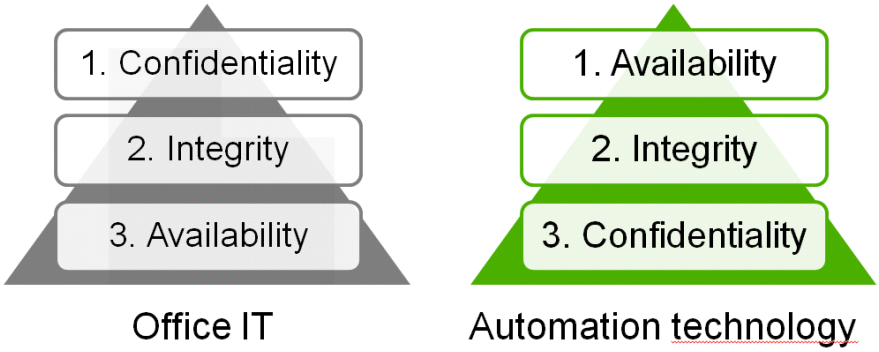

Figure 3: Prioritization of the Security Objectives for Office IT and Automation Technology

The prioritization in the production area is different. As can be seen on the right side of Figure 3, the availability of the production facility has the highest priority, followed by the integrity of the facility. Confidentiality follows in third place.

Due to this prioritization and the real-time behavior required in many areas for production facilities, the standards described in section 3.1 are inapplicable to the production area, or only applicable to a limited extent. For this reason a series of standards that take the requirements of production into account is being developed. The following sections introduce the most important of these standards.

3.2.1. IEC-62443 Series of Standards

The IEC 62443 series of standards is being developed by the International Electrotechnical Commission (IEC) and the International Society of Automation (ISA). The initial work on the standard began in working group ISA SP99 and is currently being continued in a cooperation between IEC and ISA. Therefore, many documents still contain references to ISA working groups and documents.

On the basis of the models and requirements of the ISO-27000 series of standards, the special requirements of IT security in production areas are taken into account in the IEC-62443 series of standards. Figure 4 shows the structure of the series of standards.

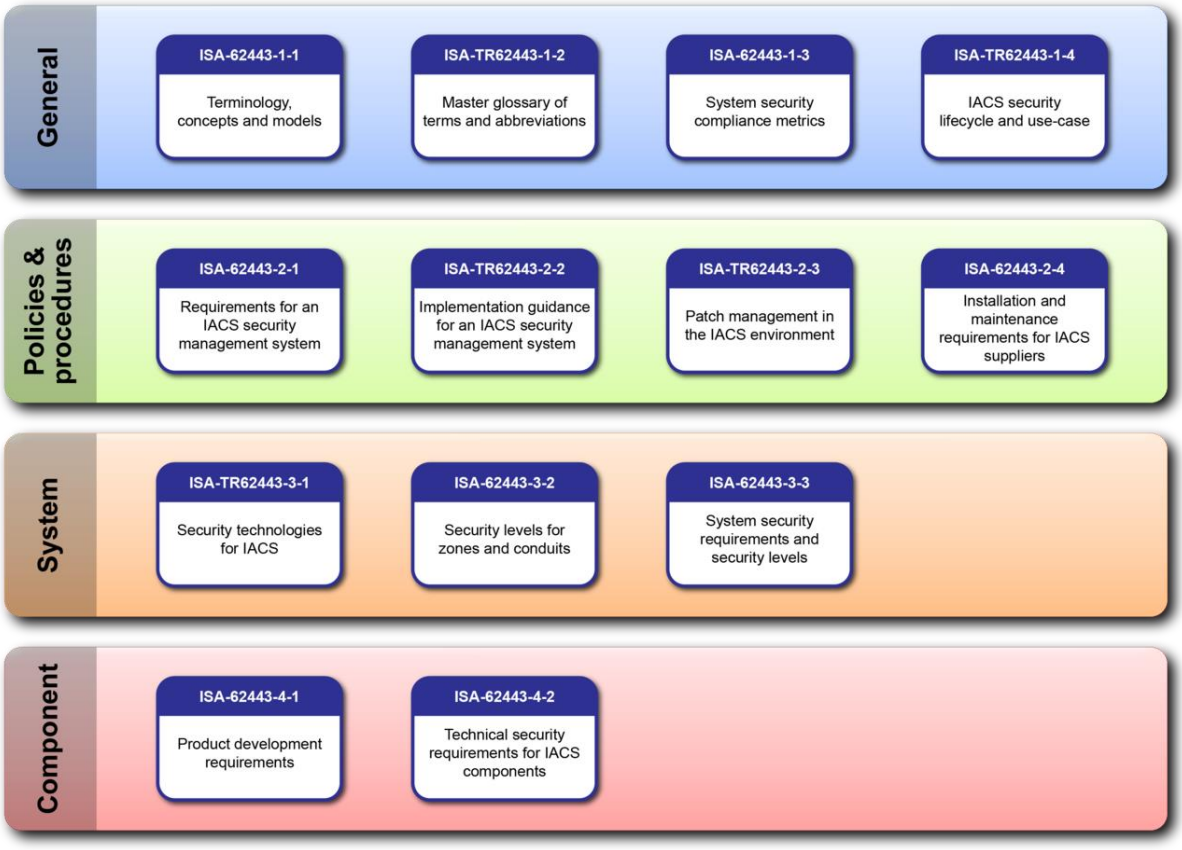

Figure 4: Parts of the IEC 62443 [Image Source: Wikimedia Commons]

The IEC 62443 series of standards consists of four main areas that are presented below, including the associated standards:

- The **"General"** section of [IEC_62443_1_1] first defines terms, concepts, and models. The [IEC_62443_1_2] section defines all terms used in the standards. The [IEC_62443_1_3] section defines metrics for assessing IT security; section [IEC_62443_1_4] describes the security lifecycle and application cases.

- The **"Policies & Procedures"** section describes the IT security management system and thus specifies the organization of IT security, followed by implementation aids. The part [IEC_62443_2_1] describes requirements on IT security management systems, e.g. the definition of security procedures. The part [IEC_62443_2_2] provides notes on how and in which domains these procedures must be implemented. Updating automation system software – patching – is especially significant, since an incorrect procedure can lead to malfunctions. Therefore, the standard gives patch management its own [IEC_62443_2_3]. The part [IEC_62443_2_4] addresses the use of service providers for commissioning and service from the point of view of IT security.

- The **"System"** part describes the technical procedure. The part [IEC_62443_3_1]first describes the underlying technologies such as authentication, encryption, filtering, and logging. Part [IEC_62443_3_2] describes structuring a facility into zones (isolated areas) and conduits (secure connections between the areas). In this way a facility with automation technology should be divided into sub-areas, which are in turn isolated from each other. Part [IEC_62443_3_3] defines a metric for assessing the security condition achieved by assigning the implemented solution a security level.

- The **"Component"** part describes the requirements on the components and the associated development cycle. This part is aimed at the manufacturers of automation systems. Part [IEC_62443_4_1] specifies the development process that must be taken into account when developing components for automation technology. Topics such as "Security Management Process", "Security Requirement Specification", "Secure Architecture Design", and "Security Risk Assessment and Threat Modeling" are parts of the standard. Part [IEC_62443_4_2] describes the technical requirements for components of automation systems, applications, and functions.

The standards have only been published in part so far. However, all parts of the series of standards are available in draft form at least. The current state of the work and the release status of the parts of the standard can be viewed at [ISA2016]. [KOB2016] gives an overview of the IEC 62443 series of standards and explains the relationships between the parts of the standards. The standards/draft standards described currently comprise 1,018 printed pages (version of Nov. 2016).

3.2.2. VDI/VDE-2182 Series of Standards

The VDI/VDE 2182 series of standards clarifies the topic of IT security for production facilities with practical examples for the manufacturing and process industry. The prospects for manufacturers, integrators, and operators are addressed in the process.

Part 1 of the [VDI_2182_1] standard first defines the essential terms of IT security for production facilities:

- User
  - Person or application that can interact with the object of consideration.
- Asset
  - All material and immaterial values of automation equipment, automation systems, machines, or production facilities that can be threatened and are worth protecting
  - Examples: SPS, formulas, interface functions, firmware
- Threat
  - A situation or event that can lead to damage
- Risk
  - Combination of probability and extent of damage
- Risk reduction
  - Reduction of the probability of damage or level of damage by taking security measures
- Vulnerability
  - Deficiency that allows a threat to become effective for the object of consideration
- Originator
  - Authorized or unauthorized users whose actions can have intended or unintended negative effects on security objectives of an object of consideration

The standard then defines a procedural model with associated roles as shown in Figure 5.

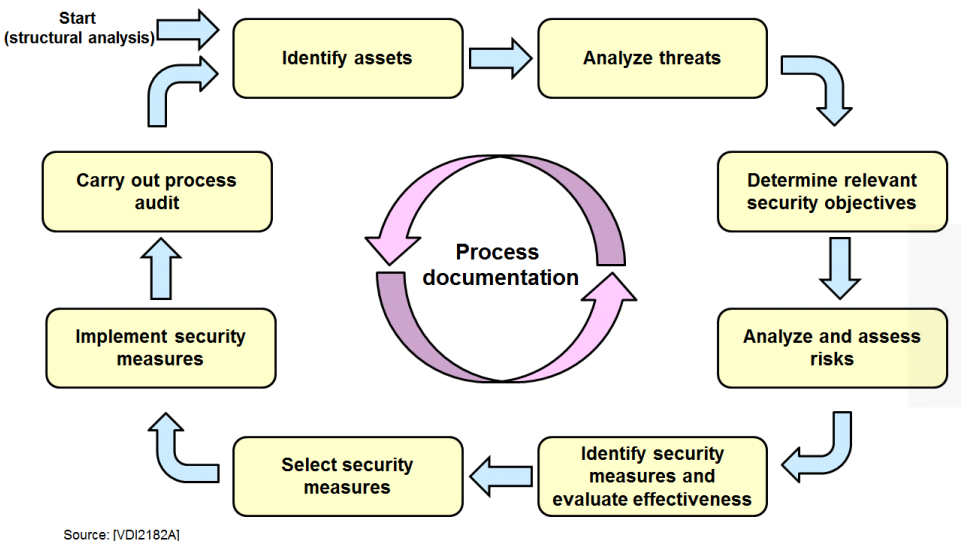

Figure 5: Procedural Model According to [VDI_2182_1]

The procedural model of VDI/VDE 2182 is based on a so-called "Plan–Do–Check–Act cycle" (PDCA).

1. In an initial step, the assets of the facility, especially automation components, computers, etc., are identified and recorded. The result is a list of identified assets.
2. The cycle next requires identifying the threats that affect the assets. Threat scenarios are considered and documented in the process. VDI/VDE 2182 provides corresponding templates.
3. As the third step the standard requires determining the relevant security objectives. The security objectives are derived from the threats, determined, and documented.
4. The fourth step of the procedural module now provides for a risk assessment. Based on the threats and the identified security objectives, the probability of occurrence of the identified threats and associated potential damage are now described. An associated risk can be determined from the combination of probability of occurrence and level of damage.
5. The result of the risk assessment identifies areas in which the existing risk is unacceptable. Risk reduction measures, so-called security measures, must be provided here and evaluated in terms of their effectiveness and economic viability.
6. The security measures are now selected on the basis of the considerations from step 5. The goal of this selection is to implement security measures to an economically reasonable extent while simultaneously achieving the necessary risk reduction.
7. The following step provides for the implementation of the selected security measure.
8. An audit of the described process is then conducted on the basis of the preceding steps. The documents created and the effectiveness of the described

security measures are determined in the process. The audit should be conducted by persons who were not involved in the preceding steps.

Since external events can alter the threat situation for a production facility, this process should be repeated at specified intervals.

SW tools that support recording and evaluating the assets are available to support the described process. For example, the German Federal Office for Information Security provides the LARS tool [BSI2014a] . Homeland Security offers the CSET tool [ICS2016]. The INSA research project [GLA2015] is pursuing an an approach to automated threat analysis.

The VDI/VDE-2182 series of standards specifies the process with respect to three roles:

- Manufacturer: The manufacturers develop and sell the system components. They are responsible for the maintenance and service of the supplied components (e.g. SW updates to eliminate security gaps) at the same time.
- Integrator: The integrator is a service provider hired by the operator and is responsible for the planning and commissioning of a facility. Operators of facilities often do not have sufficient resources for the planning and commissioning of new facilities or for carrying out the modifications to the facility. Thus use of integrators is frequently common practice.
- Operator: The operator is responsible for the operation and maintenance of the facility. The operator may delegate maintenance tasks to maintenance service providers.

Parts 2 and 3 of VDI/VDE 2182 follow the described role concept. Part 2 describes the tasks according to the procedural model described in Part 1 for the roles of manufacturer [VDI_2182_2_1], integrator [VDI_2182_2_2], and operator [VDI_2182_2_3] on the example of a production facility in the area of manufacturing automation. Part 3 does this in the same way for a process automation facility [VDI_2128_3_1] [VDI_2128_3_2] [VDI_2182_3_3].

The VDI/VDE-2182 series of standards provides manufacturers, integrators, and operators with a basis for viewing the described PDCA procedural model with a focus on the respective responsibilities. The respective parts guide the reader through the process on the basis of an actual example and show what form documentation of the results can take by providing checklists.

3.2.3. VdS 3473-1– Part 2

The guide to the interpretation and implementation of VdS 3473 for Industrial Automation Systems, VdS 3473-1 adresses specifically small and and medium-sized enter-

prises and represents a supplement to the existing directive [VDS_3473]. Part 2 is addressed to SMEs that operate production facilities. The criteria necessary for implementation of an IT security strategy in production areas are described in a brief and perspicuous form.

3.2.4. Guidelines of the German Federal Office for Information Security (BSI)

The German Federal Office for Information Security offers a series of guidelines in the domain of IT security for production facilities. The BSI publishes the top 10 threats to automation systems at regular intervals [BSI2016a]. In addition the BSI offers the ICS compendium [BSI2013] as an introduction to IT security of production facilities for facility operators. The document "Requirements on Network-compatible Industrial Components" [BSI2014c] is addressed to the manufacturers of automation components and specifies requirements on components of automation systems. Besides these basic documents, the BSI publishes case studies at regular intervals which address special issues. For example, there are case studies for attacks [BSI2014d], an example for employing service technicians, [BSI2014b] and one for IP cameras [BSI2016b]. In addition, the BSI offers LARS-ICS [BSI2014a] as a software tool that supports the PDCA cycle described in section 3.2.2.

The topic of remote service and remote diagnose is particularly significant, since communication links to third parties here can be operated from the automation domain. The BSI devotes a separate document [BSI-CS_108] to this topic.

3.2.5. Guidelines of Manufacturer Organizations

Industrial communication systems such as PROFINET or EtherNet/IP represent an important part of automation infrastructure. For this reason the various manufacturer organizations have addressed the topic of IT security in production facilities and published corresponding guidelines. For example, the PROFIBUS user organization offers guidelines for PROFINET [PNO2013]. A comparable document from ODVA is available for EtherNet/IP [ODV2011]. An IT security section has already been incorporated into the current edition of the standard for the BACNET bus protocol [ISO16484-5] used in building automation. In addition there is a security model for OPC UA in the form of a technical report of the IEC [IEC_62541-2]. The German Federal Office for Information Security has evaluated this concept and given a basically positive assessment [BSI2016d], [WIC2016].

3.2.6. Industry-specific Standards

Besides the manufacturer associations, user associations are also addressing the topic of IT security. The User Association of Automation Technology in Process Industries (NAMUR) has published both recommendations for IT security [NA_115] in existing

facilities and an outlook for future requirements [NE_153] related to IT security in automation systems of the process industry.

Industry-specific standards are also available for the maritime sector in the form e.g. of standards of the American Bureau of Shipping (ABS) [ABS2016] and of the Baltic and International Maritime Council (BIMCO) [BIM2016].

The standards of the North American Electric Reliability Corporation can be referenced for the "power supply and power distribution" sector. A series of cyber security standards are available here [NERC2016]. It should be noted that the power supply sector in particular is also characterized by national statutory regulations.

It is only possible to provide a limited outlook for industry-specific standards here, which makes no claim to completeness.

3.2.7. Summary of Standards

All the documents described above are based on the "Plan–Do–Check–Act cycle" (PDCA cycle). As described in section 3.2.2, the assets are recorded, the threats are identified, the risks are assessed, and the necessary measures are derived, implemented, and verified in a structured process. A further shared criterion is establishing an IT security strategy in the company, which requires an integrated and comprehensive view. Besides technical issues, organizational and personnel issues in particular must also be taken into account.

In terms of the technical implementation, the existing standards take a Defense-in-Depth strategy as the starting point. A series of supplemental measures protect the assets by sealing them off against threats from outside.

The existing concepts will have to be expanded and improved with the introduction of Industry 4.0. [NIE2014_1] specifies a series of additional challenges which must be addressed in future in connection with IT security in production areas. In particular these are:

- Protection against internal perpetrators
- Increasing communication even beyond the boundaries of the company
- Network access control
- Securing communication by cryptographic means

Section 5 will address and discuss this issue once again.

3.3. The IT Security Act

The IT Security Act (IT-Sicherheitsgesetz) [ITSichG2015] legislates requirements on the IT security of critical infrastructures (KRTIS). The definition of critical infrastructures is governed by a separate ordinance [BSI-KritisV]. The following infrastructures fall under the law in the current edition of this ordinance: power supply, gas supply, fuel and heating oil supply, district heating supply, wastewater disposal, and drinking water supply. The ordinance specifies threshold values for the supply services. For example, sewage treatment plants with a population equivalent of 500,000 or above and power plants with a nominal capacity of 420 MW or above fall under the ordinance. It is to be expected that the ordinance will expand the group of infrastructures addressed in the future.

Within the scope of the IT Security Act, a reporting office for incidents is established at the German Federal Office for Information Security (BSI) and a reporting obligation specified for critical incidents.

The law also stipulates the following:

> *"Operators of critical infrastructures are obligated to take organizational and technical precautions within at most two years of the effective date of the ordinance according to §10 paragraph 1 to prevent disruptions of the availability, integrity, authenticity, and confidentiality of their information technology systems, components, or processes that are critical for the functionality of the critical infrastructures they operate"* [ITSichG2015].

Furthermore, the operators of critical infrastructures are obligated to establish a contact point and must demonstrate compliance with the requirements. In addition, [ITSichG2015] summarizes a series of further requirements on other laws that relate to the issue of critical infrastructures and IT security.

The legal framework will mean that the operators of critical infrastructures will increasingly turn to their suppliers in order to obtain information and, in some cases, technical improvements to bolster components.

4. Measures for the Implementation of IT Security in Production Areas

Section 3 provides an overview of the relevant standards in order to derive a corresponding procedure from them. However, the problem for SMEs is that these sets of standards are very extensive and still incomplete in some cases. Therefore, it is hard for SMEs to reach an assessment in connection with their own companies. A quick check (e.g., www.vds-quick-check.de), which provides an initial classification of the company in terms of IT security, can provide a first estimate. There is one check available for office areas and one for production areas.

To allow an easy entry point into IT security in production areas for SMEs, a 10-point plan is proposed below for establishing IT security in production areas. These ten points are:

1. Management commitment
2. Organization of the responsibilities and processes
3. Creating guidelines
4. Training staff
5. Acquiring and providing knowledge
6. Identifying, evaluating, and protecting the assets
7. Regulating external access to production facilities
8. Data backup
9. Handling malfunctions and failures
10. Handling IT security incidents

The following sections will address these ten points and describe measures necessary for establishing an IT security process in production areas. The literature usually has a strong focus on points 6 and 7. However, it should be noted that IT security must be viewed as an integrated process incorporating all these points.

4.1. Management Commitment

IT security must be established in the company as a top-down process. Implementation in the company only makes sense with corresponding commitment from the management. For this purpose the management should prepare an IT security strategy for the company (or have one prepared) that includes the office and production areas. The strategy should define clear objectives and corresponding responsibilities.

It is advisable to define a project for the initiation of the process and provide it with the necessary internal and, if applicable, external resources. The procedure described here is comparable to the introduction of a quality management process.

4.2. Organization of the Responsibilities and Processes

After the start of the project, the management should define corresponding responsibilities. Since the technical systems in the office and production areas are often administered separately, one IT security officer should be appointed for the office area and one for the production area. A single person can handle this task if necessary. However, in that case it is necessary to ensure that this person has the necessary knowledge of the office and production areas. The two officers should form the information security team together with additional employees and a management representative. This team is responsible for the implementation of the IT security strategy and for handling malfunctions, failures, and IT security incidents.

Corresponding staff should be assigned to this topic/project in order to ensure continuous work. The reporting channels must be defined. Rules should also be established for the delegation of tasks and involvement of the top management. It should be noted that suppliers and system integrators must also be included in the processes.

4.3. Creating Guidelines

The company should address the topic of IT security in corresponding guidelines that impose basic rules of conduct on the staff. Only if the staff know what is expected of them in connection with IT security can they behave accordingly. This includes specifying the conduct of employees in connection with (non)use of private devices.

For automation systems, especially the installation of software, the introduction of software updates, and the prior verification of software updates must be defined, and the scope of the security equipment (failsafe systems) must be described.

The guidelines should also describe the information flow when staff are absent and the sharing of access codes. It should also make clear that abuse will be monitored and that penalties should be expected for misconduct. As in section 4.2, specifications should also be made for suppliers and integrators.

4.4. Training Staff

Staff are a decisive factor for IT security. Adequate know-how and training of staff can make a decisive contribution to IT security in the company.

Employees should sign confidentiality agreements when joining the company. In the onboarding phase, new employees should be given instruction on the IT security guidelines and additional guidelines if applicable. The staff's knowledge should be kept up to date with training and instruction.

Corresponding measures should be taken when employees leave the company. VPN access of these employees should be locked and passwords changed. This also applies to shift access.

4.5. Acquiring and Providing Knowledge

A report in the specialist press in 2013 indicated vulnerabilities in components of automation systems that are accessible via the Internet [STA2013b]. A reexamination two years later revealed that a large proportion of the systems remain unsecured [STA2015]. The software updates provided by the manufacturer were not installed in the system. This case makes clear that it is essential for the operators of automation systems to inform themselves of known vulnerabilities of their systems and correct them.

For this reason, a process that ensures acquisition of corresponding, up-to-date information for the company should be established in the company. Possible sources for acquiring information on vulnerabilities may include:

- Information from the manufacturers of the automation systems. For example:
  - ABB [ABB2016]
  - Siemens [SIE2016]
  - WAGO: [WAG2017]
- Information from ICS-CERT (US Homeland Security) on known vulnerabilities of automation systems [DHS2016a]
- Databases of known vulnerabilities. For example:
  - CVE Common Vulnerabilities and Exposures [MIT2016]
  - Open Indicators of Compromise (Open IOC) [MAN2016]

It must be ensured that the knowledge is up to date. In some cases it is possible to subscribe to alerts (notifications from the manufacturer about vulnerabilities that have been discovered) via an email distribution list for certain systems. Individuals

who evaluate these notifications and derive measures from them for the company should be designated in the company.

Besides specific knowledge concerning known vulnerabilities, employees' general knowledge should be established and kept up to date through awareness-raising, training, and further education.

4.6. Identifying, Evaluating, and Protecting the Assets

This section describes how the assets of a production facility are systematically recorded, evaluated, and secured if necessary. The procedure here follows the VDI 2182 series of standards. The IEC 62443 series of standards describes a comparable procedure. The steps shown in Figure 5 are taken for the analysis of the automation system. Section 3.2.2 describes the "Plan–Do–Check–Act cycle" (PDCA) and the necessary steps.

The result of this analysis is:

- List of all assets
- Breakdown of the threats that affect the assets in the form of a threat matrix
- List of all relevant security objectives in the form of a threat matrix with relevant security objectives.
- List of the assessed risks that affect the assets
    - The VDI 2182 series of standards provides suggestions for compiling such lists.
- List of possible security measures and assessment of their effectiveness and costs
- List of the selected security measures to be taken
- Report on the implementation of the security measures
- Results of the process audit for evaluating the effectiveness of the selected measures

Typical security measures that result from the process described usually follow from a so-called Defense-in-Depth concept [DHS2016b].
The following figures show examples of selected components of a Defense-in-Depth concept.

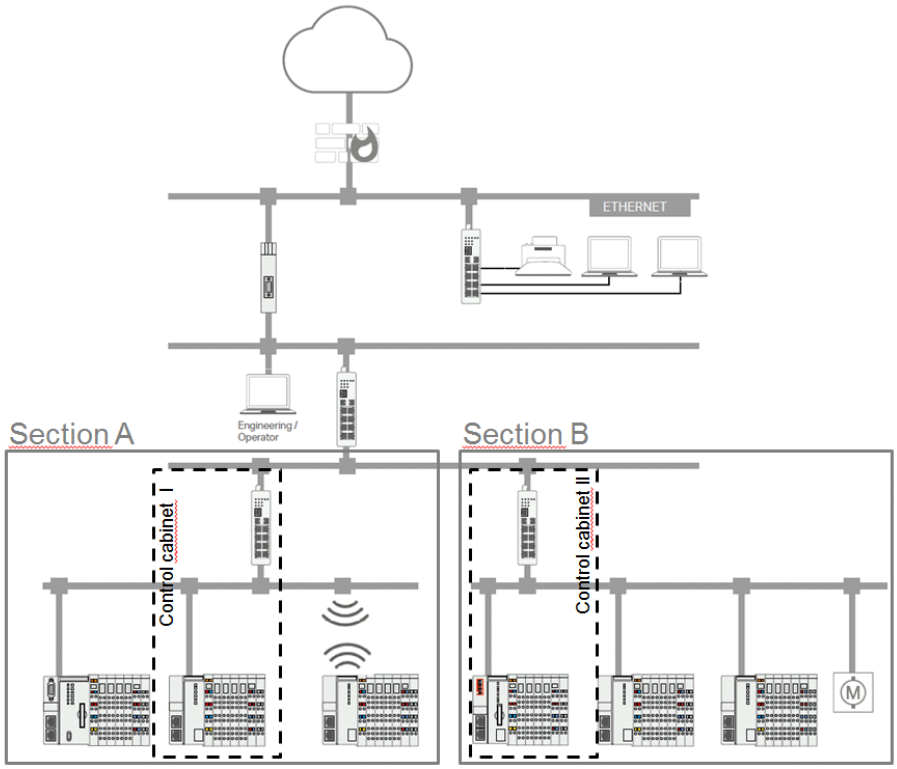

Figure 6: Example Facility with Office and Production Areas

Figure 6 shows a production facility consisting of two parts. The control room area is located above the production facility. The office area is shown above that. The company is assumed to be separated from the Internet by a firewall. An Internet connection is required for acquiring software updates or storing data in the cloud, for example.

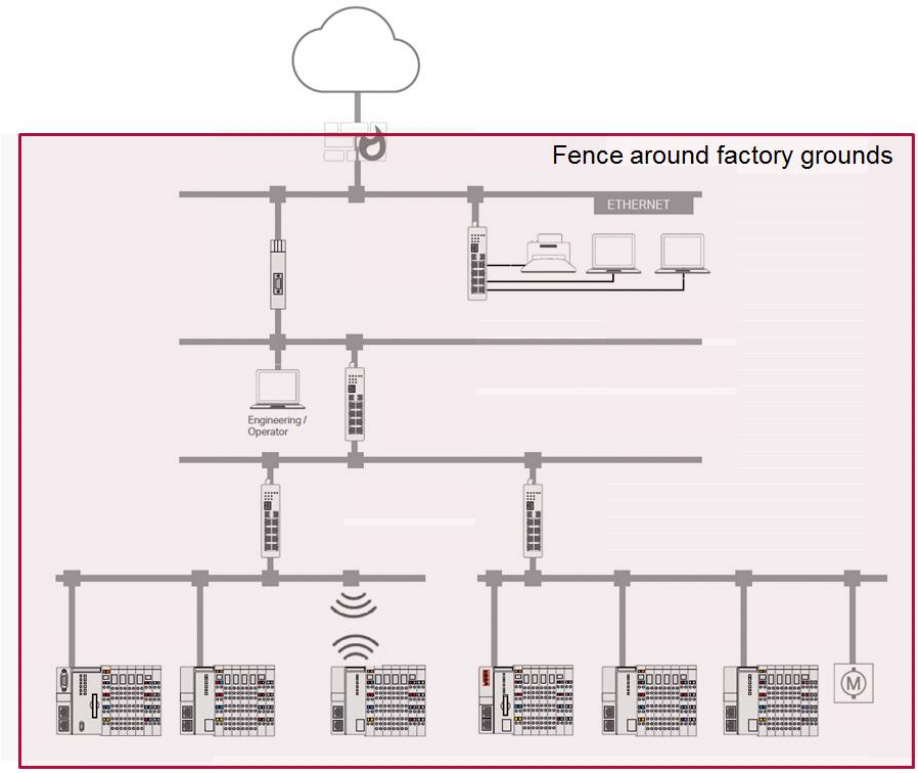

Figure 7: Perimeter Security

As the first measure taken, the entire premises can be secured against intrusion from outside, e.g. with a fence Figure 7. This measure prevents unauthorized individuals from accessing the factory grounds and represents the initial barrier against attackers. However, in one known incident a cyber attacker was able to get over a double fence and cripple a power plant with a cyber attack [PAN2008] This means that the fence must be only one of many interconnected measures.

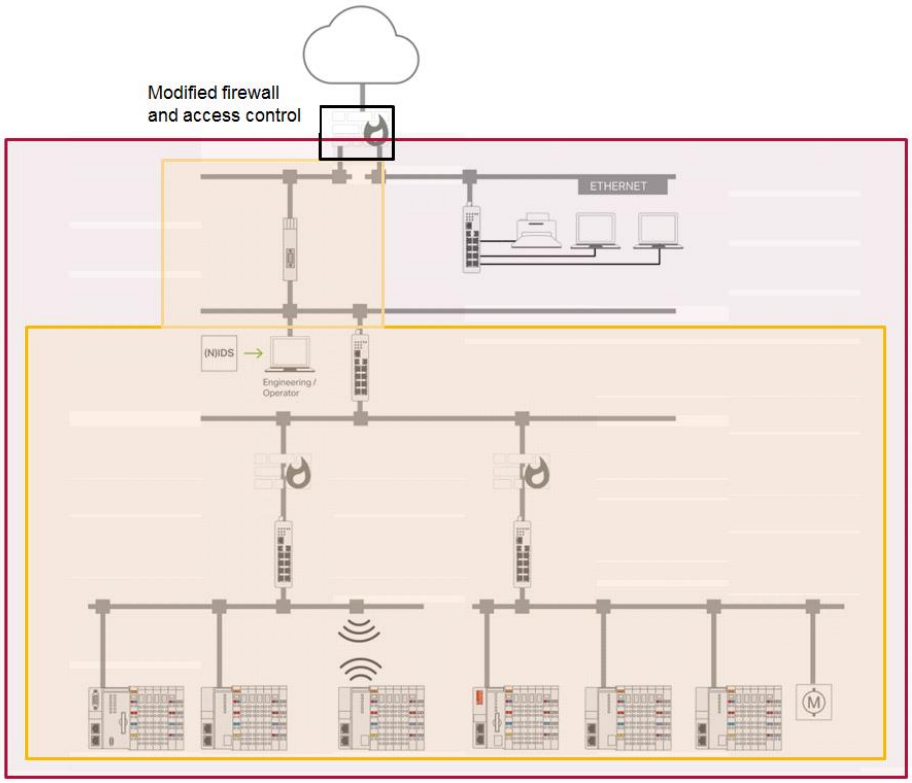

Figure 8: Modified Firewall and Building Access Monitoring

Figure 8 shows a modified firewall configuration as the next security measure. This is now configured in such a way that no access to the automation system is permissible from outside the company. At the same time necessary connections for the office area are permitted for the operation of the facility. Access monitoring for the building in which the production facility is located is installed as an additional measure. These measures provide a data barrier between the production area and both the office area and the Internet. In addition to the fence around the factory grounds, a second, narrower access control is implemented.

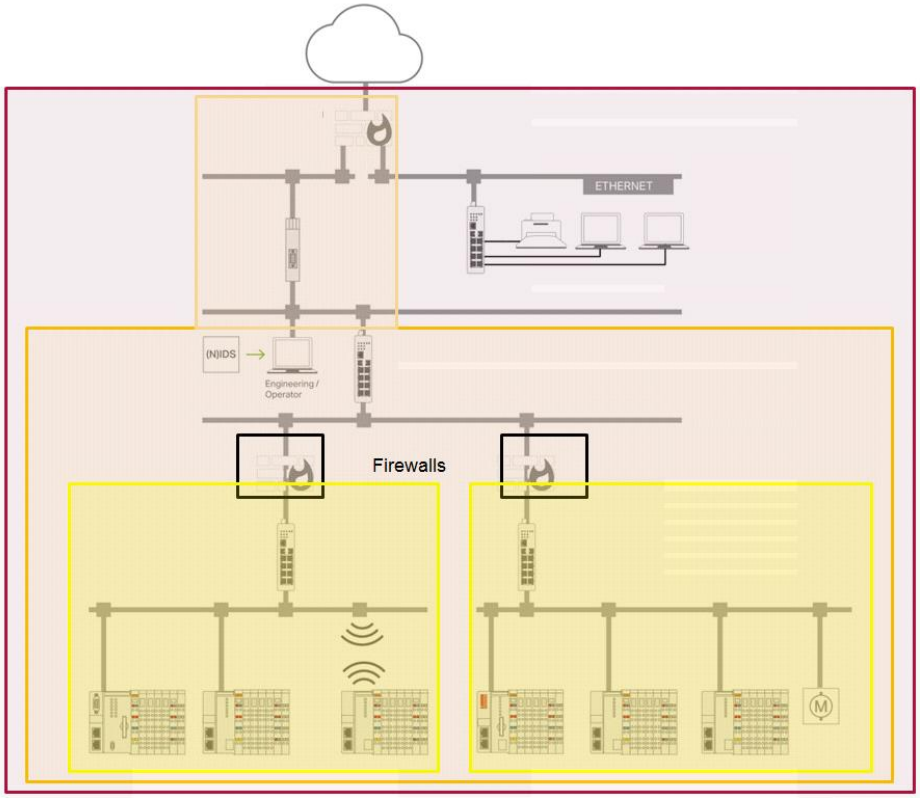

Figure 9: Isolating the Production Area

Figure 9 shows a further subdivision of the production facility. The production facility is divided into two sub-areas (yellow background). Each of these areas is itself isolated from the maintenance area (ocher-colored background) by a firewall. In addition, the components in the sub-areas could be further secured by installing them in a locked switch cabinet, for example.

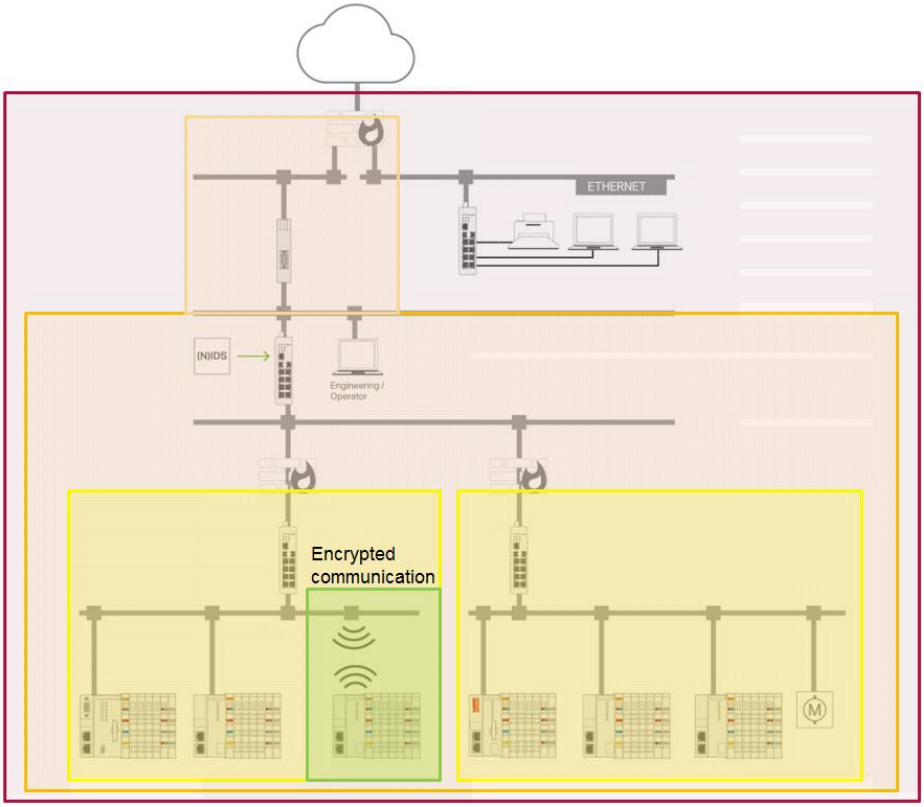

Figure 10: Encryption of the Communication

Figure 10 shows the security measure for a wireless access point through encryption. Even if off-the-shelf WLAN access points offer standard encryption, it it is important to select a sufficiently secure procedure and sufficiently strong passwords.

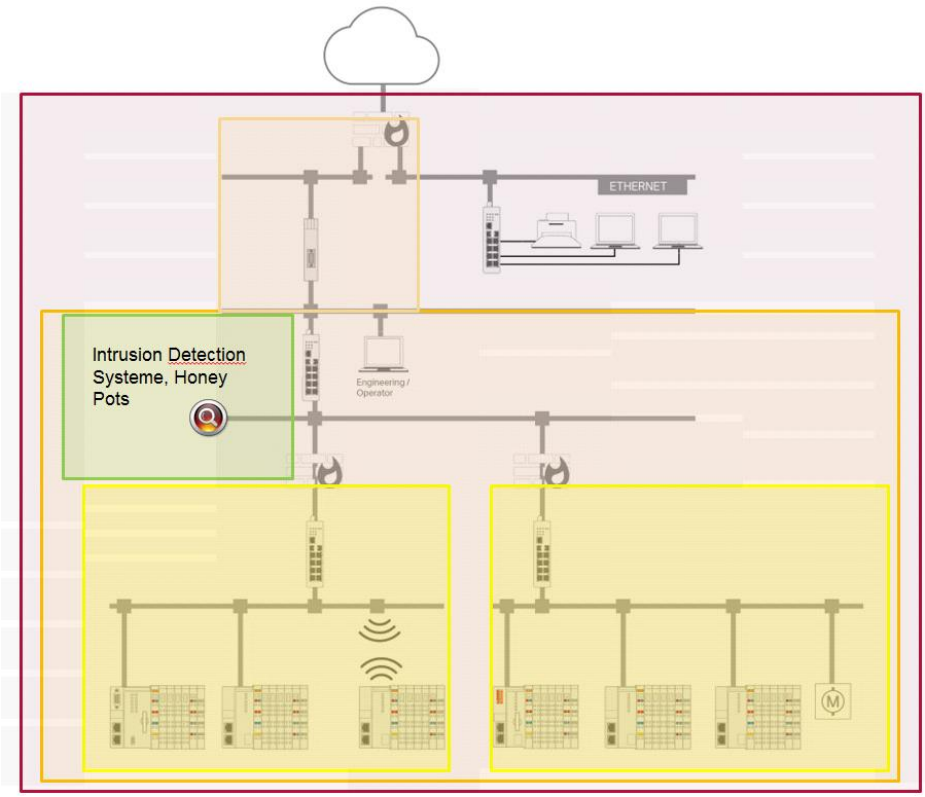

Figure 11: Network Monitoring

Figure 11 shows monitoring, e.g. via a honey pot or a network monitoring system, as the final measure. The honey pot is a monitoring system that masquerades as an easy victim, lures in possible attackers, and documents attacks. A network monitoring system (Network Intrusion Detection System – NIDS – or Intrusion Detection System – IDS) monitors the network traffic for anomalies.

The measures presented here represent a few examples. Further measures exist which we will not go into here for reasons of space. Examples include:

- Virus protection
- Application whitelisting
- Access restriction for portable media
- Setting up demilitarized zones (DMZs) for introducing software updates
- Authentication of network participants
- Restricting access to the network by turning off unused network ports

Although this part of the 10 point program is the most laborious, the other points should not be neglected in comparison with this part.

4.7. Regulating External Access to Production Facilities

External access to production facilities for remote diagnosis and remote maintenance purposes is an especially critical process from the point of view of IT security. For this reason, this topic is described in a separate section.

Known incidents of this type trace back to the use of remote access [BYR2009] [SAN2016]. For this reason special security measures apply to such access. [BSI-CS_108] provides a good orientation. In it the BSI describes the basic procedures for setting up remote access. The BSI's basic guidelines are:

- Setting up a uniform solution. This standardizes the hardware and processes used, reducing the administrative effort.
- Locating the remote maintenance components in an upstream zone (DMZ).
- No blanket access to an entire (sub)network, but rather only to dedicated end-points.
- Establishing the connection from the company to the outside
- Using dedicated systems that can only be used for this purpose
- Current versions of established protocols such as IPsec, SSH, or SSL/TLS are used exclusively in order to establish a tunnel between two end-points/networks.
- The connection between the company and diagnosis point must be encrypted. Sufficiently strong cryptographic processes are used for encryption.
- Only one user should be provided per account. It is essential to avoid group accounts.
- Use of multi-factor authentication method
- Appropriate specifications should be created and followed for use of pass-words.
- Mechanisms for detection of attacks on password-based authentication meth-ods should be used.
- Performing a risk analysis
- Following the minimality principle (as few connections as possible)
- Establishing processes for enabling and blocking access
- Specifications for staff who perform remote maintenance, e.g. prohibition on performing remote maintenance via mobile phones
- Restricting access to a specified timeframe; automatic disconnection after a certain time span
- Switching on and evaluating protocol functions

The document referenced contains even more information. This document merely reproduces the essential points.

4.8. Data Backup

[ZET2016] and [SAN2016] describe the attack on the Ukrainian power grid in 2015. This attack included making the hard drives of control systems unusable with the help of the "KillDisk" program. Triggering a total data loss is thus a method of attack already known today. Therefore data backup takes on particular significance in production areas.

A concept for handling a catastrophic data loss (deletion of all data pools including operating systems) should be developed. Regular full backup of all data pools of the automation system is part of a data backup concept. The recovery routines should be documented and tested.

In view of the further spread of ransomware such as Locky [MC 2016], the backup systems should only be connected to the computer network for the duration of the backup. Furthermore, it should not be possible to modify or delete the data of the backup system from the computer network.

4.9. Handling Malfunctions and Failures

It is necessary to handle malfunctions and failures rapidly and efficiently in order to resume operation quickly after such an incident. It is essential to define the term clearly. The alert type and alert channels should be determined and documented. It is necessary to specify which types of incidents fall under this category. A plan for communication with the outside should also be drawn up. The reactions to malfunctions and failures should be specified, and procedural models (recovery plans) are necessary for handling such incidents.

When incidents occur, restoring proper operation initially has the highest priority. After that, the causes are investigated, the damage is documented, and follow-up to prevent future incidents is performed.

4.10. Handling IT Security Incidents

To begin with, the malfunctions described in section 4.9 can be of a general nature. The IT security incidents form a sub-category of these incidents that require special treatment. First of all, the procedure described in section 4.9 applies to IT security incidents as a general rule. In addition, preventive measures to detect and avert IT security incidents are advisable. In a survey by the SANS Institute [SAN2015], 15 % of

the companies surveyed said that they had needed more than one month to detect an attack.

For this reason, further measures such a network access monitoring, analysis (possibly automatic) of log files, honey pots, or network monitoring systems (Intrusion Detection Systems) make sense. In any case, an internal company reporting system should be set up to record and handle IT security incidents.

5. Outlook

The 10 point action plan presented in section 4 offers an initial approach to implementation of IT security in the production area. Although it is appropriate for implementing sufficient protection for a production facility, there are still some deficiencies that will emerge more prominently in the context of Industry 4.0.

State-of-the-art measures have the following deficiencies:

- The concepts focus heavily on defence against the "outside." [HAR2015] shows that employees represent the largest group of perpetrators, accounting for 25 % of the incidents. Therefore, future concepts must concentrate more than they have on protection against internal perpetrators.
- Any attacker who has access to an unsecured network switch can introduce a device into the network and participate in the communication. [LIN2014] contains an impressive description of how an attacker was able to get control of an automation system through unsecured network access.
- The increase in horizontal and vertical integration in the context of Industry 4.0 will mean that the classic security measures will only remain effective to a limited degree. The number of network nodes will grow; the effort for ensuring IT security will increase.

In [NE_153], NAMUR described requirements on future automation systems. The fundamental principle is the "Security by Design" approach. Instead of sealing the devices off, in the future security functions will be integrated into the devices that will permit secure communication even under real-time conditions. Essential requirements for such a concept can be found in [NIE2014_1] or [NIE2014_2].

However, for implementing IT security today, the established measures should be taken, especially "low-hanging fruit" – goals that can be achieved with limited effort. A significant increase in security can be achieved with minimal effort in such cases.

6. List of Figures

7. List of Tables

8. Literature List

[ABB2016] ABB Asea Brown Boveri Ltd: Cyber security alerts and notifications. http://new.abb.com/about/technology/cyber-security/alerts-and-notifications, 29.11.2016.

[ABS2016] American Bureau of Shipping: Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations - Volume 1: Cybersecurity. http://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/221_Guidance_Notes_Cyber_Safety_Principles_Maritime_Operations/Cyber_Security_v1_GN_e.pdf, 08.03.2016.

[BIM2016] BIMCO: The Guidelines on Cyber Security onboard Ships. https://www.bimco.org/News/2016/01/~/media/AEEEE215CBE3421F8F7493A6A1B0E521.ashx.

[BRO2011] Broad, William J.; Markoff, John, Sander, David E.: Israeli Test on Worm Called Crucial in Iran Nuclear Delay. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=3&sq=stux.

[BSI2013] Bundesamt für Sicherheit in der Informationstechnik: ICS-Security-Kompendium. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile, 05.06.2014.

[BSI2014a] LARS ICS. Light and Right Security ICS - Ein Werkzeug für den leichtgewichtigen Einstieg in industrielle Cyber-Security -Benutzerhandbuch, Bonn, 2014a.

[BSI2014b] Bundesamt für Sicherheit in der Informationstechnik: Empfehlung IT in der Produktion. Fallbeispiel Schwimmbad. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/materialien/fallbeispiele/BSI-CS_095a.pdf?__blob=publicationFile, 29.07.2015.

[BSI2014c] Bundesamt für Sicherheit in der Informationstechnik: Anforderungen an netzwerkfähige Industriekomponenten. https://www.bsi.bund.de/ACS/DE/_downloads/techniker/hardware/BSI-CS_067.pdf;jsessionid=320A5E59D3035F5560291B16C049C738.2_cid286?__blob=publicationFile, 15.06.2014.

[BSI2014d] Bundesamt für Sicherheit in der Informationstechnik: Fallbeispiel Servicetechniker. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/materialien/fallbeispiele/BSI-CS_095c.pdf?__blob=publicationFile, 29.07.2015.

[BSI2014e] Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2014. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2014/bsi-lagebericht-it-sicherheit.pdf%3F__blob%3DpublicationFile, 12.01.2015.

[BSI2016a] Bundesamt für Sicherheit in der Informationstechnik: Top 10 Bedrohungen und Gegenmaßnahmen 2016. Industrial Control System Security. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf?__blob=publicationFile&v=4.

[BSI2016b] Bundesamt für Sicherheit in der Informationstechnik: Sicherheit von IP-basierten Überwachungskameras. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_128.pdf?__blob=publicationFile&v=5.

[BSI2016c] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzkataloge. 15. Ergänzungslieferung. https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf.

[BSI2016d] Bundesamt für Sicherheit in der Informationstechnik (BSI): Sicherheitsanalyse OPC UA. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/OPCUA/OPCUA.pdf?__blob=publicationFile&v=2.

[BSI-CS_108] Bundesamt für Sicherheit in der Informationstechnik: Fernwartung im industriellen Umfeld. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_108.pdf?__blob=publicationFile&v=3, 15.01.2015.

[BSI-KritisV]: Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung). BSI-KritisV, 2016.

[BYR2009] Byres security lnc.: Daimler Chrysler Cyber Security lncident case Profile. Virus shuts down 13 plants; loss estimated at $14 million. https://www.tofinosecurity.com/sites/default/files/CP-104-Case_Profile-Daimler_Chrysler-rev1.pdf.

[CERT2014] The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): Alert (ICS-ALERT-14-176-02A). ICS Focused Malware (Update A). https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A, 13.11.2014.

[CERT2016] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): Cyber-Attack Against Ukrainian Critical Infrastructure. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[DEU2015] Deutsche Telekom /T-Systems: Cyber Security Report 2015. Ergebnisse einer repräsentativen Befragung von Abgeordneten sowie Top-Führungskräften in mittleren und großen Unternehmen. https://www.telekom.com/static/-/293656/2/Cyber-Security-Report-2015-si, 22.11.2015.

[DHS2016a] Department of Homeland Security: ICS-CERT Alerts. https://ics-cert.us-cert.gov/alerts, 29.11.2016.

[DHS2016b] Department of Homeland Security: Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

[DIR2015] DiRenzo, Joseph; Goward, Dana A.; Fred S. Roberts: The Little-known Challenge of Maritime Cyber Security: 6th International Conference on Information, Intelligence, Systems and Applications (IISA), 2015.

[EIK2013] Eikenberg, Ronald: Vaillant-Heizungen mit Sicherheits-Leck. http://www.heise.de/security/meldung/Vaillant-Heizungen-mit-Sicherheits-Leck-1840919.html, 12.02.2016.

[FAL2011] Falliere, Nicolas; Murchu, Liam O.; Chien, Eric: W32.Stuxnet Dossier. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, 21.08.2014.

[GLA2015] Glawe, M. Fay, A.; Tebbe, C.; Niemann, K.-H.; Schewe, F.: Wissensbasierte Methoden zur Erstellung von IT-Sicherheitsanalysen automatisierter Anlagen. In (VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik Hrsg.): Automation 2015 - Benefits of Change – the Future of Automation. VDI-Verlag GmbH, Düsseldorf, 2015; S. Ohne Seitenzählung.

[HAR2015] Harp, Derek; Gregory-Brown, Bengt: The State of Security in Control Systems Today. http://www.sans.org/reading-room/whitepapers/analyst/state-security-control-systems-today-36042, 29.07.2015.

[ICS2016] ICS-CERT: Downloading and Installing CSET. https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET, 30.11.2016.

[IEC_62443_1_1] IEC- International Electrotechnical Commission IEC/TS 62443-1-1: Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models, 2009.

[IEC_62443_1_2] IEC- International Electrotechnical Commission ISA-TR62443-1-2: Security for industrial automation and control systems - Master Glossary.

[IEC_62443_1_3] IEC- International Electrotechnical Commission IEC/TS 62443-1-3: Security for industrial process measurement and control – Network and system security – Part 1-3: System security compliance metrics, 2014.

[IEC_62443_1_4] IEC- International Electrotechnical Commission ISA-62443-1-4: Security for industrial automation and control systems Life Cycle and Use Cases, 2013.

[IEC_62443_2_1] IEC- International Electrotechnical Commission IEC 62443-2-1-2010: Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program, 2010.

[IEC_62443_2_2] IEC- International Electrotechnical Commission ISA 62443-2-2: Security for industrial automation and control systems - Implementation Guidance for an IACS Security Management Systems, 2013.

[IEC_62443_2_3] IEC- International Electrotechnical Commission IEC/TR 62443-2-3: Industrial communication networks – Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment., 2014.

[IEC_62443_2_4] IEC- International Electrotechnical Commission IEC 62443-2-4: Security for industrial automation and control systems – Network and system security – Part 2-4: Requirements for IACS solution suppliers., 2014.

[IEC_62443_3_1] IEC- International Electrotechnical Commission ISA 62443-3-1: Technical Report Security Technologies for Industrial Automation and Control Systems, Rev. 2, 2007.

[IEC_62443_3_2] IEC- International Electrotechnical Commission IEC 62443-3-2: Industrial communication networks - Network and system security – Part 3-2: Security assurance levels for zones and conduits, 2013.

[IEC_62443_3_3] IEC- International Electrotechnical Commission ISA-62443-3-3 (99.03.03): Security for industrial automation and control systems Part 3-3: System security requirements and security levels, 2013.

[IEC_62443_4_1] IEC- International Electrotechnical Commission IEC/NP 62443-4-1: Industrial communication networks – Network and system security – Part 4-1: Product development requirements, 2013.

[IEC_62443_4_2] IEC- International Electrotechnical Commission IEC/NP 62443-4-2: Industrial communication networks – Network and system security – Part 4-2: Technical security requirements for IACS components.

[IEC_62541-2] IEC- International Electrotechnical Commission IEC TR 62541-2:2016: OPC unified architecture - Part 2: Security Model, 2016.

[ISA2016] ISA - The International Society of Automation: ISA99 Committee - Work Product List. http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx.

[ISO16484-5] DKE-Deutsche Kommission Elektrotechnik, Elektronik Informationstechnik DIN und VDE, DIN Deutsches Institut für Normung e. V DIN EN ISO 16484-5: Systeme der Gebäudeautomation – Teil 5: Datenkommunikationsprotokoll (ISO 16484-5:2014); Englische Fassung EN ISO 16484-5:2014. Beuth Verlag GmbH, Berlin, 2014.

[ITSichG2015]: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 2015.

[JEN2015] Jensen, Lars: Challenges in Maritime Cyber-Resilience. In Technology Innovation Management Review 04, 2015; S. 35–39.

[KER2013] Kersten, Heinrich; Reuter, Jürgen; Schröder, Klaus-Werner; Wolfenstetter, Klaus-Dieter: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz. Der Weg zur Zertifizierung. Springer, Wiesbaden, 2013.

[KER2016] Kersten, Heinrich; Klett, Gerhard; Reuter, Jürgen; Schröder, Klaus-Werner: IT-Sicherheitsmanagement nach der neuen ISO 27001. ISMS, Risiken, Kennziffern, Controls. Springer Vieweg, Wiesbaden, 2016.

[KOB2016] Kobes, Pierre: Leitfaden Industrial Security. IEC 62443 einfach erklärt. VDE Verlag, Berlin, Offenbach, 2016.

[LAN2013] Langner, Ralph: To kill a centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve. http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf, 13.11.2014.

[LIN2014] Lindner, Felix: Licht aus! Sicherheit kritischer Infrastrukturen im Test. In c't Magazin für Computertechnik 9, 2014; S. 150–155.

[MAN2016] Mandiant: Open IOC. http://openioc.org/.

[MC 2016] Mc Affee Labs: Threat Report September 2016. http://www.mcafee.com/de/resources/reports/rp-quarterly-threats-sep-2016.pdf.

[MIT2016] Mitre Corporation: Common Vulnerabilities and Exposures. https://cve.mitre.org/, 29.11.206.

[NA_115] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V: NA115: IT-Sicherheit für Systeme der Automatisierungstechnik: Randbedingungen für Maßnahmen beim Einsatz in der Prozessindustrie, 17.11.2016.

[NE_153] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V NE 153: Automation Security 2020 – Design, Implementierung und Betrieb industrieller Automatisierungssysteme, Leverkusen, 2015.

[NERC2016] North American Electric Reliability Corporation (NERC): Critical Infrastructure Protecion (CIP) Standards. http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx, 19.03.2016.

[NIE2014_1] Niemann, Karl Heinz: IT Security Konzepte. Anforderungen im Kontext von Industrie 4.0. In (VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik Hrsg.): Automation 2015. Smart X - Powered by Automation. VDI-Verlag GmbH, Düsseldorf, 2014; S. 489–506.

[NIE2014_2] Niemann, Karl Heinz: IT-Security-Konzepte für die Prozessindustrie. Anforderungen im Kontext von Industrie 4.0. In atp-edition 7-8/2014, 2014, Jahrgang 56; S. 62–69.

[ODV2011] ODVA Inc.: Securing EtherNet/IP Networks. http://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00269R0_ODVA_Securing_EtherNetIP_Networks.pdf, 28.04.2014.

[PAK2005] Pakalski, Ingo: Computerwurm befällt CNN, DaimlerChrysler und Walt Disney. http://www.golem.de/0508/39902.html.

[PAN2008] Pany, Thomas: Saboteur schaltet Turbine des britischen Kohlekraftwerks Kingsnorth aus. https://www.heise.de/newsticker/meldung/Saboteur-schaltet-Turbine-des-britischen-Kohlekraftwerks-Kingsnorth-aus-188799.html?view=print.

[PNO2013] PROFIBUS Nutzerorganisation e.V.: PROFINET Security Guideline7.002. http://www.profibus.com/download/specifications-standards/.

[SAN2015] SANS Institute: The State of Security in Control Systems Today. http://www.sans.org/reading-room/whitepapers/analyst/state-security-control-systems-today-36042, 19.07.2016.

[SAN2016] SANS Institute: Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[SIE2016] Siemens Aktiengesellschaft: ProductCERT Security Advisories. http://www.siemens.com/cert/de/cert-security-advisories.htm, 29.11.2016.

[STA2013a] Stahl, Louis-F.; Eikenberg, Ronald: Fünf nach zwölf. Die „Gefahr im Kraftwerk" ist noch nicht gebannt. In c't Magazin für Computertechnik 15, 2013a; S. 16–17.

[STA2013b] Stahl, Louis-F.: Gefahr im Kraftwerk. Industrieanlagen schutzlos im Internet. In c't Magazin für Computertechnik 11, 2013b; S. 78–82.

[STA2015] Stahl, Louis-F.; Benz, Benjamin; Eikenberg, Ronald: Risiko verdrängt und vergessen. Industriesteuerungen nach über zwei Jahren noch verwundbar. In c't Magazin für Computertechnik 21, 2015; S. 86–87.

[VDI_2128_3_1] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) VDI/VDE 2182 Blatt 3.1: Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Hersteller Prozessleitsystem einer LDPE-Anlage. Beuth Verlag, Berlin, 2013.

[VDI_2128_3_2] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) VDI/VDE 2182 Blatt 3.2: Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Integratoren LDPE-Reaktor. Beuth Verlag, Berlin, 2013.

[VDI_2182_1] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) VDI/VDE 2182 Blatt 1: Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell. Beuth Verlag, Berlin, 2011.

[VDI_2182_2_1] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) VDI/VDE 2182 Blatt 2.1: Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Hersteller Speicherprogrammierbare Steuerung (SPS). Beuth Verlag, Berlin, 2013.

[VDI_2182_2_2] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) VDI/VDE 2182 Blatt 2.2: Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Maschinen- und Anlagenbauer Umformpresse. Beuth Verlag, Berlin, 2013.

[VDI_2182_2_3] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) VDI/VDE 2182: Informationssicherheit in der industriellen Automatisierung Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Maschinen- und Anlagenbauer Umformpresse. Beuth Verlag, Berlin, 2011.

[VDI_2182_3_3] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) VDI/VDE 2182 Blatt 3.3: Informationssicherheit in der industriellen Automatisierung Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Betreiber LDPE-Anlage. Beuth Verlag, Berlin, 2013.

[VDS_3473] VdS Schadenverhütung GmbH: Informationssicherheit in kleinen und mittleren Unternehmen (KMU). Anforderungen. http://www.vds.de/fileadmin/vds_publikationen/vds_3473_web.pdf.

[WAG2017] WAGO Kontakttechnik GmbH & Co. KG: Wago Security-Hinweise Automatisierungskomponenten. http://www.wago.de/produkte/produktkatalog/automatisierungskomponenten/security-hinweise/index.jsp, 02.02.2017.

[WIC2016] Wichmann, Andre: Sicherheitsanalyse von OPC UA für Industrie 4.0. In atp edition 07-08, 2016, Jahrgang 58; S. 40–45.

[ZET2016] Zetter, Kim: Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, 05.03.2016.