PLATTFORM INDUSTRIE 4.0

GUIDELINES

IT Security in Industrie 4.0

Action fields for operators

Publishing information

Publisher
Federal Ministry for Economic Affairs
and Energy (BMWi)
Public Relations Division
11019 Berlin
www.bmwi.de

Editorial responsibility
Plattform Industrie 4.0
Bertolt-Brecht-Platz 3
10117 Berlin

Design and production
PRpetuum GmbH, Munich

Status
November 2016

Printed by
MKL Druck GmbH & Co. KG, Ostbevern

Picture credits
traffic_analyzer – iStock (Titel), zapp2photo – Fotolia (S. 5), Mimi Potter – Fotolia (S. 8), putilov_denis – Fotolia (S. 9), contrastwerkstatt – Fotolia (S. 13), Robert Kneschke – Fotolia (S. 14), Sikov - Fotolia (S. 19), industrieblick - Fotolia (S. 20), gen_A – Fotolia (S. 24), Maksim Kabakou – iStock (S. 25), maxsim – Fotolia (S. 29), jijomathai – Fotolia (S. 30), Kzenon – Fotolia (S. 33), Coloures-pic – Fotolia (S. 41)

This publication as well as further publications can be obtained from:
Federal Ministry for Economic Affairs
and Energy (BMWi)
Public Relations
E-mail: publikationen@bundesregierung.de
www.bmwi.de

Central procurement service:
Tel.: +49 30 182722721
Fax: +49 30 18102722721

Table of contents

1 Introduction and Management Summary

The digital networking of global production is forging ahead and will end in the fourth industrial revolution. It is currently still very difficult to estimate the extent of this development which is known as Industrie 4.0. There is a consensus between the different visions of this revolution: the far reaching networking and fundamental restructuring of production in the traditional sense will have a huge impact on society which must increasingly place confidence in the stability and functioning of these new infrastructures. However, the massive networking of industrial production can only function if there is legitimate expectation between the value-added partners. Legitimate expectation can arise if the stakeholders guarantee protection against threats (security) to the agreed extent, if this is verifiable and can be demonstrated to the satisfaction of the partners concerned. The protection objectives here are availability, integrity, confidentiality and legally compliant use (e.g. privacy) of the resources or data. In order to keep the vulnerability to attack low and to guarantee a basic stability for the new infrastructures, the security concept must be an integral part of all considerations on Industrie 4.0. Only a carefully protected production system will be able to withstand current attacks.

The introduction of IT security usually presents enormous challenges to machine and system operators: whilst recommended action and security measures are adequately covered in the traditional IT landscape, there is great uncertainty when it comes to the digitalisation of production. System operators on the path to Industrie 4.0 are confronted with a huge diversity of security issues and solutions, standards, recommendations and organisational framework conditions which cannot always be transferred to the demands of networked production. A need therefore exists for tailor-made catalogues of recommended action, particularly with a view to information security in production.

Whilst the BSI Grundschutz (Basic Protection) Manual offers general information and the IEC 62443 highlights relevant subject areas for operators, system operators in SME's still do not have clear recommendations on the first steps to be taken in the direction of secure networked production.

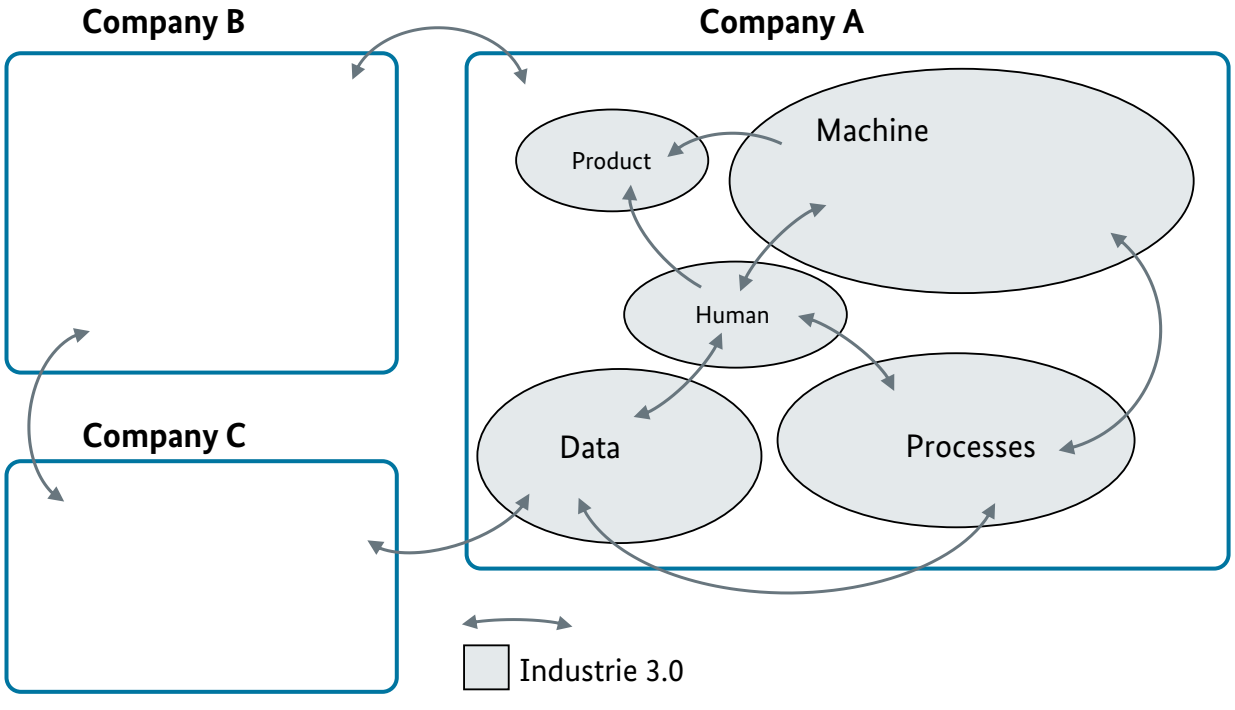
Guidelines are therefore provided in the following which describe in particular the requisite organisational framework conditions alongside the purely technical protective measures. This will assist operators of machines and systems in initially making a self-assessment, on the basis of which further areas of action may be addressed. Implementing the measures and practical information provided in the following may enable operators to satisfy possible requirements placed on the procurement of machines and systems and to address the largest risks, thereby creating the foundation for involvement in value-added networks.

2 Special features of “networked production” in Industrie 4.0

IT security risks arise from the far reaching networking of production in the context of Industrie 4.0. The special features of networked production in Industrie 4.0 will be addressed initially in order to understand the impact of networking. The aim is to create a picture of the production landscape to be expected which is as uniform as possible on the basis of which protective measures and recommended action may be provided. Three specific characterisations of Industrie 4.0 will be addressed in particular: order-driven production in added-value networks, the networking of production installations and product-machine communication.

In principle, Industrie 4.0 implies cross-company networking at all levels of traditional production. Whilst the information flows of Industrie 3.0 essentially take place within the individual companies (see Figure 1), machines, products, system components and processes communicate beyond company boundaries in Industrie 4.0 (see Figure 2).

Figure 1: Information flows of Industrie 3.0



Source: Plattform Industrie 4.0

The traditional boundaries between individual production systems are becoming increasingly blurred. The establishment and dissolution of component, process or system groups are subject to the dynamism of the value-added network. For example, distant machines can connect up to produce a small unit number of a requisite product.

2.1 Order-driven production in added-value networks

The traditional production chains with their predominantly hierarchical structures will increasingly disappear in Industrie 4.0 and will be superseded by flexible value-added networks for the production of alternating products for individual customers. The communication paths of Industrie 3.0 will essentially be maintained but will be supplemented by the networking of companies for the purpose of an agile and direct exchange of information.

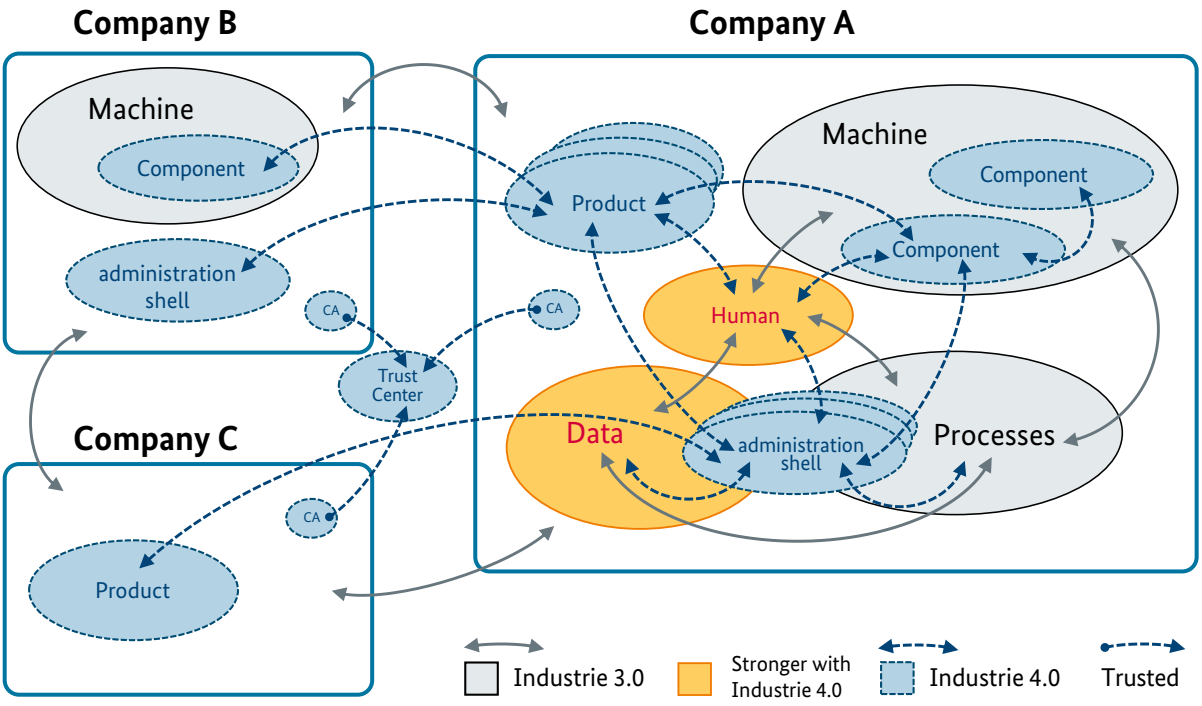
Creating value-added networks based on the intensive cross-company exchange of data can optimise corporate success through gains in efficiency. The central criterion in the formation and continuous improvement of these added-value networks will be the possibility to manufacture new and requested products and services in the desired quantity and quality with the necessary availability.

Accordingly, external production resources will be incorporated flexibly and dynamically to extend own production competences or increase production capacities in the production network structures of Industrie 4.0. This will require greater expertise in terms of the product to be manufactured and the requisite production competence as well as changes in the non-productive areas such as logistics and life cycle or supplier management.

The future scenario of "order-driven production" therefore extends largely beyond the control of an order by own production facilities towards developing a best possible added-value network to produce a product for an individual customer and to control the order through this network. The entire order spectrum from single unit through to volume production can be covered here. Not every SME needs to establish a network but every SME must be in a position to participate in a network of this type if it is not to lose all its shares in business.

The initiation of this cooperation and the requisite vertical and horizontal networking of production systems of the network partners will be automated. Technical networking will be implemented on the basis of secure identities and secure cross-company communication.

Figure 2: Information flow in Industrie 4.0



Source: Plattform Industrie 4.0

The spontaneous formation of these added-value networks will create the conditions precisely for small and medium-sized enterprises to increase their production depth as required by using external production competence, to market their own production competence and capacities in new added-value networks or to take on larger orders and to "broker" their batches with a margin on virtual trading platforms. The product portfolio thus enlarged and the higher exploitation of production capacities can increase profits whilst at the same time enhancing customer satisfaction.

2.2 Networking of machines and systems

The implementation of Industrie 4.0 in small and medium-sized enterprises is accompanied by a significant increase in the degree of networking between all production systems. Communication and data transfer not only takes place between the machines of a system or between systems and entire system groups but the vertical boundaries of the traditional automation pyramid are becoming increasingly blurred.

Unlike Industrie 3.0, cross-company communication is now also taking place between the individual components of the same level of the automation pyramid which is referred to as horizontal networking. A steep increase in machine-to-machine (M2M) communication is expected in particular. Individual machines can incorporate themselves in distributed value-added networks in order, for example, to facilitate optimum load distribution. This results in a high dynamism of the system groups.

Whilst in traditional production the supply and value-added chains were still centralised, their overall inclusion is made difficult by the distributed nature of the future production landscape.

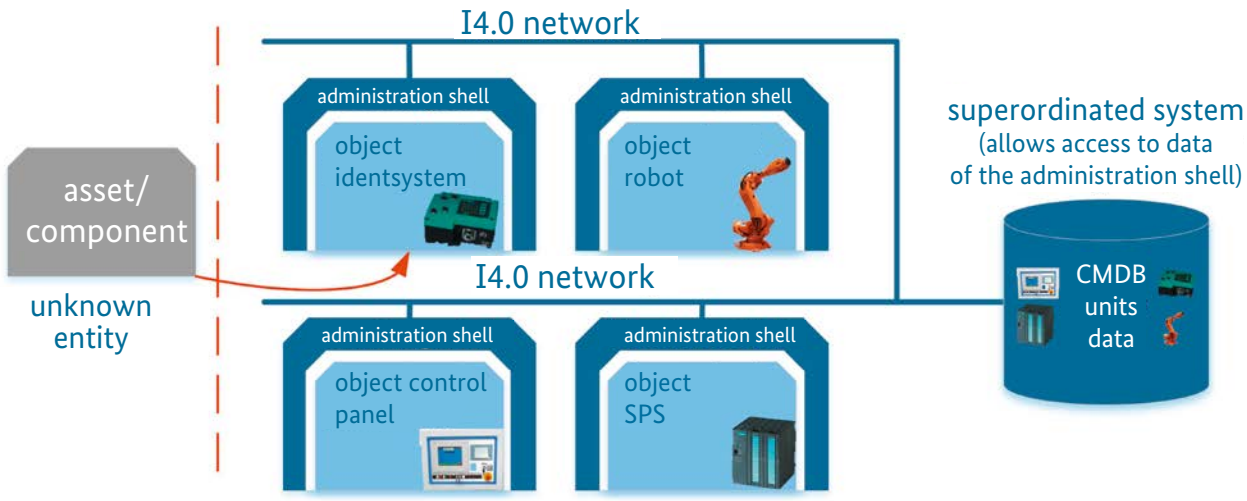
It is to be expected that the production machinery and systems will independently plan the requisite resources and forward the corresponding order processes to the productive systems. Production and material flows of Industrie 4.0 will then be controlled decentrally by the production machines involved in value creation. The planning process of material flow shifts and is organised horizontally via several systems and system groups.

Precisely the high degree of networking opens up many potential points of attack so that it is absolutely necessary to provide overarching security for all components involved in the value-added network.

2.3 Product-machine communication

Communication and data exchange takes place not only between machines but also between product and machine or the components of Industrie 4.0. For example, a virtual counterpart to every product is conceivable which passes on all requirements and parameters of the relevant production steps to the machine which processes the product. Reference is made in the context of Industrie 4.0 to the administration shell[1]: it stores the virtual image of the product that contains all data necessary for production and operation. In addition to the component data, the administration shell also offers functions and services which have been specially attuned to the product. The machine can, for example, adjust itself individually to the product-specific

Figure 3: Administration shell as a receptacle of asset information



Source: Plattform Industrie 4.0

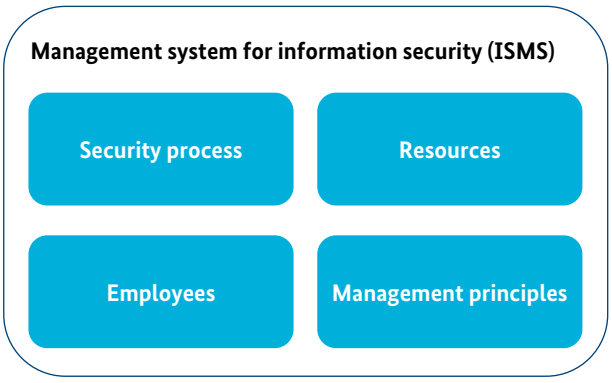
1 see ZVEI (publisher) (2015)

production processes in this way. The production process for the product can then be extended over many distributed machines and systems without the necessity for a central control of the machines involved. After completion, the transfer of further data is also conceivable. For example, the machine could send the product an early warning if a defect becomes known in a certain series and all products of the series need to be replaced. The transfer of data on the part of the product is also conceivable. If, for example, the machine receives information that a large part of the manufactured products are to be equipped with a component of a certain type, the machine could initiate a corresponding optimisation in logistics and pricing (in the case of automatic trading on digital market places).

3 Organisation, processes and responsibilities

One of the greatest current and future challenges is the creation and maintenance of a suitable IT security level. Particularly for small and medium-sized enterprises (SMEs) in industry this is hardly possible on their own. IT security is a project in which all must participate and where organisational adjustments are necessary. Furthermore, new processes must be defined and new resources and responsibilities created. This applies to traditional office IT in the same way as to production IT. Many of the necessary management principles have already been implemented for office IT whilst the IT security in production is managed typically not at all or only to an inadequate extent. The basic principles to create IT security with focus on production will therefore be outlined in the following. The recommendations from the BSI IT-Grundschutz will be followed here in the main.

Figure 4: Management system for information (ISMS)



Source: according to BSI (Publisher) (2008a), p.14

The concepts presented in the following are the same as for all management systems (e.g. quality management, environment, safety). The structures and processes presented here should therefore exist and be familiar in many other parts of the company already. These principles and processes must now be introduced and applied to security.

3.1 Information Security Management System (ISMS)

"The ISMS determines the instruments and methods with which management steers (plans, uses, conducts, monitors and improves) the tasks and activities aimed at information security." It therefore supports management so as to be able to reach the goals of information security, minimise the entrepreneurial risk and satisfy regulatory requirements. It is described as part of the BSI Standard 100-1[2] and is composed of the four components of security process, resources, employees and management principles (see Figure 4).

With the introduction of a **security process** the requisite organisational changes are initiated and aims to achieve the goals from the security strategy elaborated. In view of the higher ranking importance of the security process, it will be considered in greater detail in the following section.

2 see. BSI (publisher) (2008a)

Particular reference will be made to the responsibilities of management for the components of the ISMS **resources**. It is emphasised that in practice the persons responsible for security frequently lack the time and also the foundations to adequately come to grips with security-relevant topics (e.g. statutory requirements or technical issues). In such cases, it is recommended that use be made of external experts.[3]

The ISMS component of **employees** makes it clear that information security concerns all employees without exception and that the action of every individual can be decisive to success. All employees must therefore be incorporated in the security process. Every individual can avoid damage and contribute to success by responsible and quality-conscious action.[4]

Management principles are an indispensable foundation to satisfy internal and statutory requirements placed on information security. Since there is plenty of room for catching up here, the BSI summarises six tasks and duties at the managerial level.[5]

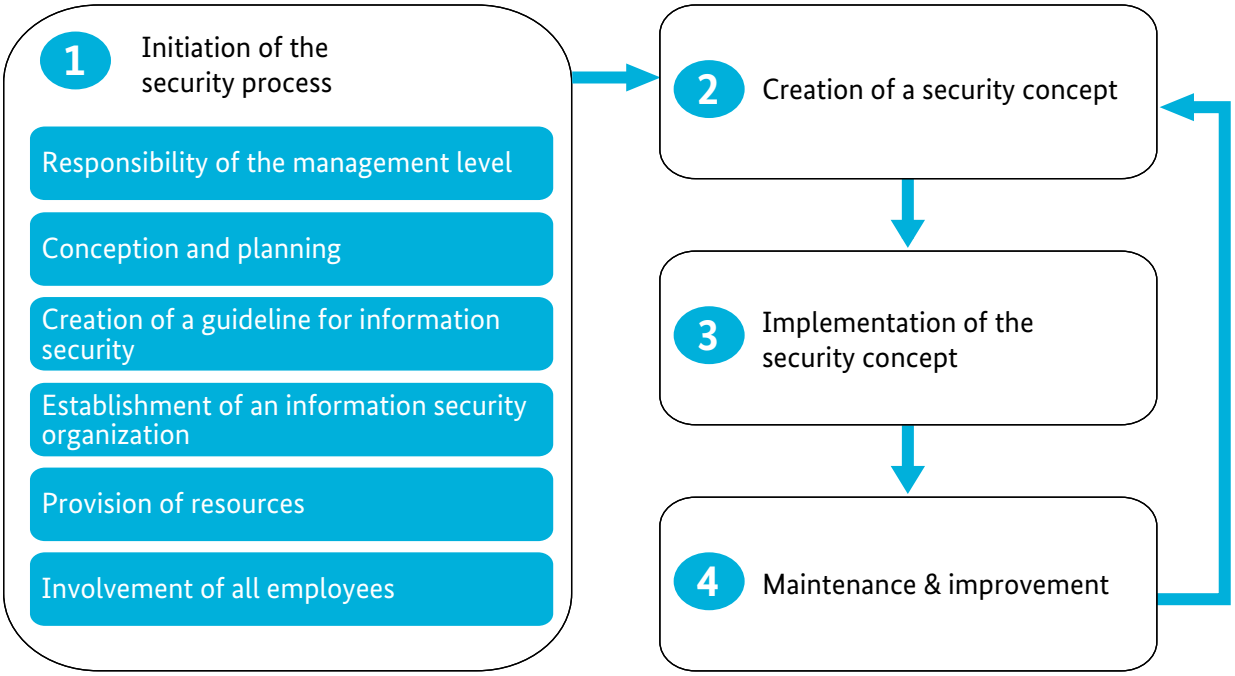
Even if an ISMS of this kind has already been implemented in a company, it is usually restricted to office IT and must be extended to production IT. In the rarest of cases are separate resources, employees, processes and management principles also available or defined for production. Companies, and in particular the operators of machines and systems, must take urgent action here.

SMEs in which management of information security (IS management) has not yet been introduced are called upon even more urgently to take action here. In this case, the special requirements of production should be taken into consideration from the outset and suitably adjusted concepts prepared.

3.2 Security process

The security process is a central element of the management system for information security and assists in the introduction and maintenance of a suitable IT security level. The four phases of the process are shown in Figure 5. In view of statutory requirements and regulations, the company management has the full responsibility for setting up the security process and guaranteeing that it is complied with.

Figure 5: Phases of the security process



Source: according to BSI (Publisher) (2008b), p.13

3 see BSI (publisher) (2008a), p. 22
4 see BSI (publisher) (2008a), p. 23
5 see BSI (publisher) (2008a), p. 17f

IT security management is to be understood as a cyclical process which comprises the phases of planning, implementation of planning, checking success and eliminating known defects and weaknesses. This PDCA[6] model is widespread and is also to be found, for example, in ISO27001 and other standards on the design of management systems. The model can also be used for individual components of the security process such as the security concept.

The main element of the security process is the security guideline using which the objectives and expectations in a company are stipulated. The security guideline must reach all employees so that they can develop the requisite sensitivity to risks in their areas of work. For this purpose, the security guideline should be set out in writing, should be worded as simply as possible and should be accessible. The security guideline is then continuously improved in accordance with the cyclical character of the security process.

The security process must be implemented throughout a company so that the aspired-to security level can be achieved. Responsible roles must be introduced in view of this overarching character.

3.3 Roles and responsibilities

Before the individual roles and responsibilities are addressed, three basic rules for the definition of roles in the context of an enterprise and its ISMS are to be listed:

1. The overall responsibility for the correct and secure satisfaction of tasks (and therefore for information security) remains at the managerial level.

2. At least one person (typically the **IT security officer**) promotes and coordinates the information security process.

3. In the context of his job and his workplace, every employee is responsible for maintaining IT security.

These basic rules refer to the implementation of the ISMS in all parts of the company, i.e. production and administration equally. A special role is assigned here to the IT security officer, who will be addressed in the following. In a second step, specific requirements for the provision of security and production in the ISMS and the requisite roles will be discussed.

3.3.1 IT security officer and information security team

IT-Grundsschutz recommends both an IT security officer and an information security team for the introduction and implementation of a security process and that they be provided with the requisite resources. The IT security officer is responsible for all questions concerning information security in the organisation. This includes production, its IT components and processes. Ideally, he is independent from an organisational point of view, i.e. implemented as a staff role. He has important tasks which include the following:

- Controlling and coordinating the security process
- Supporting management in the preparation of the security guideline
- Coordinating security-relevant projects
- Investigating security-relevant incidents
- Initiating and coordinating measures to raise awareness for, and training measures on, information security

The IT security officer is supported by the information security team which is formed from persons responsible for information security.

In smaller organisations these tasks can also be assumed by a few or by one person – in this case the IT security officer. It is important that the governance, i.e. the organisation and the administration of the information security, is uniform for production and administration and is implemented by an organisational unit in its entirety in order to achieve an equal level of security.

3.3.2 Industrial Security Officer

The previous distinction between office IT and production IT leads to measures that fail to take the impact in each other's area into consideration. It is therefore vital to overcome this silo mentality. What is needed is the ability to take a wider view, something which is becoming more urgent as the degree of networking increases.

This means there will be need for a "caretaker" who is responsible for and manages security across departments for the whole site. This role must be integrated organisationally and must have the necessary expertise.

6 PDCA is the abbreviation for Plan, Do, Check, Act.

Criteria such as company size, know-how and knowledge requirements in the respective position of responsibility will in future determine the organisation of responsibility for security.

For example, it may be worth creating a separate post for this field through a Chief (Information) Security Officer (C(I)SO), who is equally responsible for the design and implementation of security measures in both office and production IT and in production development. Such posts (or positions) have generally already been introduced in larger companies, but their focus has so far been on office IT. The areas of industrial security and/or security in product development are only rarely taken into account in this position of responsibility (see Figure 6).

Role concepts whereby a C(I)SO and a corresponding role for production, for example an industrial C(I)SO, share the aspects of responsibility are similarly conceivable.

The responsible C(I)SO may be given operational support by roles covering specific areas in office IT, production IT (Industrial Security Officer (ISO)) and product development (Product Security Officer (ProSO)). The incorporation of all specific aspects of governance and measures must be suitably ensured. However, it is likely in small and medium-sized enterprises in particular that several roles will frequently have to be combined in a single position.

The Industrial Security Officer assumes responsibility for the protection objectives in production and must have IT, IT security, engineering and management expertise as well as specific soft skills in order to design the production-specific security measures and to manage their implementation in view of the applicable governance. Further details on the organisational incorporation and the skills profile of an Industrial Security Officer are to be found in the publication entitled “Security requirements placed on the vocational and advanced training of employees in the context of Industrie 4.0” of Plattform Industrie 4.0.

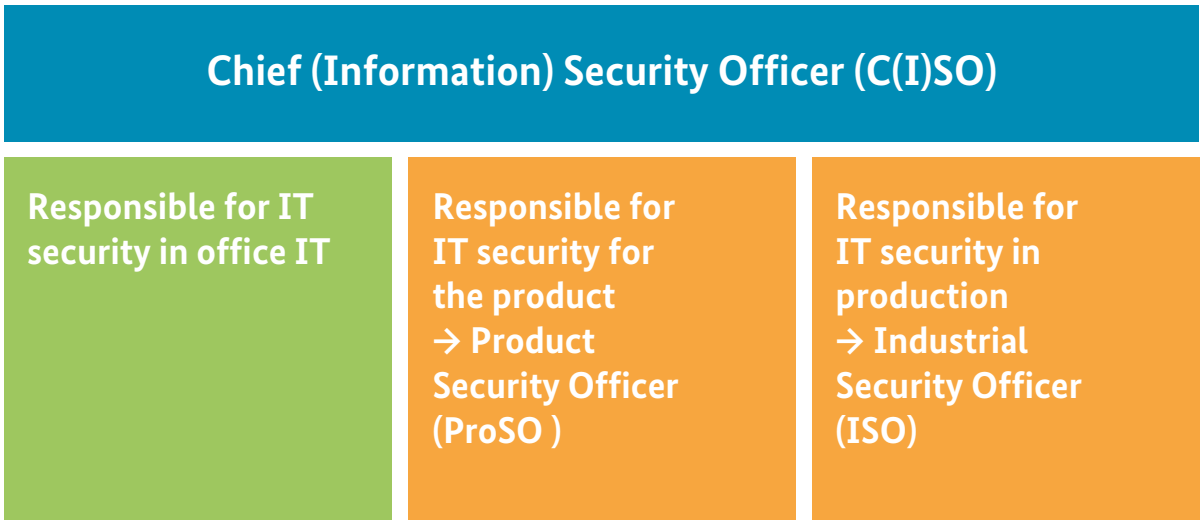
Similarly, the Product Security Officer (ProSO) assumes responsibility for the protection of the products throughout their lifecycle, starting from product concept and development, through technical service during use at the customer, for example updates of software with new, security functions, to cancellation or taking back.

3.4 Skills

The availability of the necessary (security) knowledge and expertise is essential for the introduction and assertion of an IT security concept. Each and every employee in the company must be in a position to take account of the security requirements relevant in his area of work and in the respective lifecycle phase. He must be given the opportunity to acquire and use the necessary knowledge and skills. At the same time, there must be a fundamental awareness of security and possible security risks of IT in production (see next section).

Even in the area of standard IT, it is frequently hardly possible for small and medium-sized enterprises to keep up

Figure 6: Duties of a Chief (Information) Security Officer



Source: Plattform Industrie 4.0

with the growing requirements placed on specialisation and qualification, which is why recourse is made to support from external specialists and service providers. In addition to developing internal skills, service providers can also be incorporated by framework agreements or request services, for example.

3.4.1 Expertise of employees

The "human factor" is elementary in the overall establishment of IT security, which means that expertise in correct behaviour and the handling of IT security must be trained accordingly. To ensure that all employees of a company are able to act in accordance with their area of responsibility, the foundations of information technology and information security must be trained throughout the company. In addition, employees in corresponding roles and functions must be able to provide evidence of extended knowledge and possibly also expertise on IT security, network security and the special features of IT and IT security in the area of production.

This is also associated with the demand that established professional fields be extended accordingly and aligned with the requirements of Industrie 4.0.[7] Corresponding further training measures are also required in development to qualify employees at a contemporary level.

3.4.2 Training methods

In the context of training, it is important to prepare content and select suitable training methods in line with the target groups. The different expertise of employees and their areas of work in the company must be taken into consideration when making this choice.

The training activities should also be designed such that they are obligatory, demonstrable and documented. The content of training must also be part of an overall security process and must be improved on a regular basis.

The training content should be prepared and coordinated in close cooperation between HR department, IT security officer and the management of the company. The HR department is to be incorporated primarily due to its mandate to look after personnel and its further training but should also accompany corresponding qualification measures within the greater context of Industrie 4.0.

Depending on the qualification and leeway afforded in the preparation of materials, training can then be conducted by internal employees, in cooperation with externals or entirely by externals. The implementation is essentially in line with the requirements and possibilities of the company.

7 Discussions are underway with the Chambers of Industry and Commerce, for example, as to whether the professional field of a cyber mechatronic is to be defined as an apprenticed trade.

4 Risk management

In order to sensibly and sustainably engage in risk management, it is necessary to know the corporate values to be protected. In the security context, the corporate values to be protected are referred to as assets. Without a list of assets (process know-how in terms of production parameters or formulations) it is not possible to correctly prioritise the measures for more IT security. It is therefore necessary to recognise the critical value-adding processes, to document the components and information involved and then to derive the protective requirement of specific assets, i.e. the corporate values to be protected. A threat analysis is then conducted which distinguishes between the irrelevant threats and those which can have an impact on the critical assets. Finally, the possible weak points are considered which endanger the assets and the associated threats. The likelihood of incidence must then be factored in so as to be able to derive the risk values.

4.1 Corporate values (assets) to be protected as a basis for the risk analysis

The knowledge of the information to be protected, of the (information) assets, provides the basis for all assessments. The following sections outline the tasks of asset management as a basis for risk management.

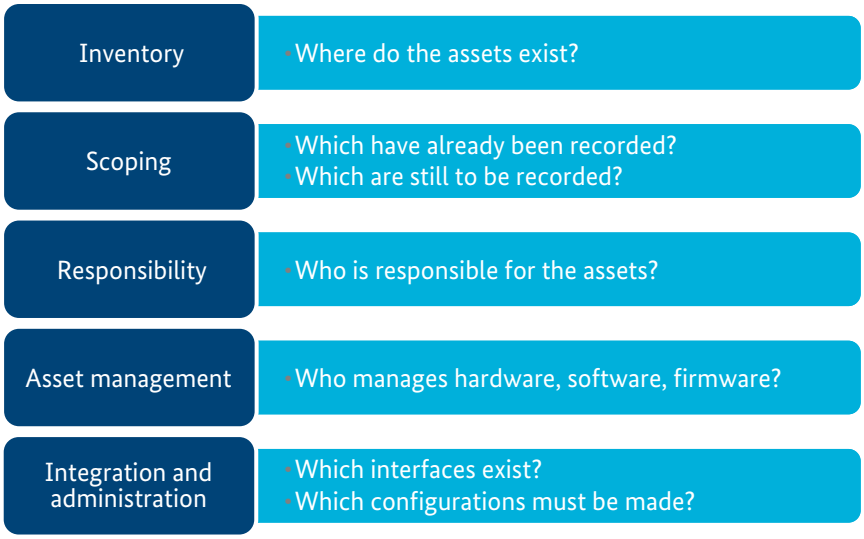
4.1.1 Definition of assets to be protected

The term 'assets' refers to all corporate values to be protected: it covers both physical objects and also intellectual property such as secret formulations or knowledge about specific production processes and their parameters. Secret formulations and processes have always been strictly protected by storage in safes (paper) or by encrypted storage. As far as hardware assets are concerned, it is already standard in office IT to list all existing devices in an assets database before their first use (Configuration Management Database (CMDB)). The devices are typically assigned an asset ID and an initial classification is made. Technical detailed information can and should also be deposited here. This form of asset management provides companies with an idea of the existing equipment and the existing IT infrastructure. On the basis of this outline, a risk assessment of the existing assets can be made at any time. Considering the existing assets and their risk classification, decisions must be made on the level of protection to be provided and corresponding measures derived. The focus here must be placed on protecting the core competences and critical data. This may be process instructions, product data or production technologies, for example.

4.1.2 Asset management: challenges in production

An overview of the existing assets is present only very rarely in production. It is therefore absolutely necessary for the components in production to be recorded in detail so as to be able to prepare an adjusted protection concept in the first place. In detail this means that a production system, for example, can no longer be recorded as only one system but that a breakdown into its components is necessary. For example, it must be documented which system components have which communication possibilities from the system. Many weak points and therefore threats to IT security are associated with the increasingly networked IT components contained in a system because the IT components (which are partially obsolete on delivery) are already insecure or could quickly become so through the lack of updates. It is

Figure 7: Basic information to manage assets



Source: Plattform Industrie 4.0

therefore necessary to precisely record the individual (IT) components of a system and to document them in detail so as to be able to take targeted measures should gaps in security arise. The first approach here is provided in the Information Technology Infrastructure Library (ITIL) and in the description of systems and components in IEC62443.

Since a list of the IT components is frequently not provided in the usual scope of delivery or the documentation, IT assets must usually be recorded manually. The activities required by asset management must urgently be described in processes and must be actively driven by the newly created responsibilities in production.

4.1.3 Procedure for the management of assets

In order to facilitate a suitable management of assets, they must be assigned corresponding information such as responsibilities, i. e. a corresponding inventory must first be made. All information must be documented accordingly and must be updated at regular intervals. On introduction of asset management, the following steps must be conducted and the corresponding questions answered (see Figure 7).

4.1.4 Inventory of the existing assets

The inventory of assets is the first step in the process of asset management or in the management and administration of the existing IT components. Various tools are in principle available in IT for the automated recording and storage of these components. However, only few of these are also suitable for the recording of production assets because so far they frequently lack the requisite interfaces. The use of agents for asset recording is usually rejected by system integrators for reasons of stability. It is therefore a good idea to request a comprehensive directory of the components used from the supplier when a system is delivered or to define it as an acceptance condition. For existing systems, the manual recording and documentation in own databases – or initially at least in EXCEL tables – is the only alternative. In order to be able to easily recognise changes at least in IP-based networks, passive monitoring tools are suitable which recognise both new IP and also MAC addresses and send the corresponding messages.

4.1.5 Configuration administration

One way of documenting assets is nomenclature in “Configuration Items” (CI) as used for processes of the IT Infrastructure Library (ITIL). All operating resources of IT are understood by configuration items in ITIL. Access to configuration items and their configuration can be managed using databases which are referred to as Configuration Management Database (CMDB). A CMDB serves to bring together all information which is available for one configuration item. Frequently, available information – particularly on production assets – is distributed over different databases in a company. The CMDB offers the possibility to bring together information without it necessarily having to be stored centrally (federated database management).

4.2 Data (flow) analysis and data classification

For a risk analysis it is necessary to know not only the critical assets but also the relevant communication relationships and the components involved and to record the different data flows on the basis of which production processes run. For this purpose, it is necessary to know and document the connections between the components, the data exchanged and the protocols used. The use of network analysis tools is a good way of obtaining an overview.

As soon as the data flows have been clearly recorded, they should be classified in order to derive information about possible zones or protection needs. Unfortunately, many established classification systems and automated tools are based on the assumption that confidentiality is the primary protection goal. This is derived from the origin of the classification stages from data protection.

However, for production it is necessary that the requirements placed on run times (real time requirements), integrity and authenticity are also recorded and shown per classification. The capture of data and their classification in production is becoming increasingly more relevant for IT security as the degree of networking and the complexity of machines and systems grow because an increasing number of communication partners are incorporated, which automatically leads to greater vulnerability to attack.

When implementing an IT security concept, it is a good idea to classify data particularly in terms of their value or sensitivity and the resultant protection worthiness. The individual protection requirement is usually stipulated in a risk analysis.

In the context of Industrie 4.0 a cross-company and standardised classification of data is called for so as to be interoperable in terms of classification and prevent misunderstandings. One proposal for a uniform and simple classification scheme is made in the working results document “Secure cross-company communication” from Plattform Industrie 4.0. (see Figure 8).

4.3 Risk analysis in production

The question to be asked in a risk analysis is how large the possible damage within a company would be if the protection goals (availability, integrity, confidentiality, authenticity) of critical assets in production were to be impaired. In a security incident of this nature, certain types of data could be stolen, manipulated or production processes altered, for example.

For a sustainable risk management and a protection concept based on it, the three following principles apply which clarify the significance and tasks of asset management once again:

- Only those things can be protected if they are known to exist!
- Only if the weak points and relevant threats are known can sustainable protective measures be taken!
- Only if assets, weak points and location/owner are known can a correct reaction be given to attacks and failures!

Figure 8: Classification of data in terms of sensitivity

1 Public

- No secrecy required, no protective measures
- Information and services are not worthy of protection or deliberately available publicly
- e. g. machine movement data or sensor data if these are uncritical for a publication

2 Confidential business partners (new in Industrie 4.0 scenarios)

- Average protection worthiness
- Cross-company information exchange essential for Industrie 4.0
- Correct handling of business information and documentation of the correct handling is fundamental
- Applies, for example, to the automatic exchange of production information

3 Confidential internal

- Absolute protection worthiness
- Data or services may not exceed company boundaries
- e. g. confidential product data, technology data or not yet published patents

Source: according to BMWi (publisher) (2016a), p. 15f

An individual risk analysis on the basis of the recorded and classified IT components and data flows is essential. Sensible measures can be derived from the results of the risk analysis so as to appropriately diffuse the identified risks.

The process of risk analysis is to be regularly conducted so that the changes in threat scenarios are recorded and corresponding measures initiated. The BMWi study on IT security in Industrie 4.0 writes as follows: "The special features of industrial systems require [...] an approach that goes beyond the pure threat and risk analysis and can be rather described as constantly updated IT security documentation. The main reason for this is the lifecycle of industrial systems which may extend over several decades." Amongst others, the BSI standard 100-3: Risk analysis on the basis of IT-Grundschutz describes a suitable approach to risk analysis. Internal responsibilities and competences should already have been created before a risk assessment is made.

A uniform picture for analysis of risks and security requirements of different Industrie 4.0 applications is to be elaborated as part of the national reference project "IUNO – IT security in Industrie 4.0"[8].

4.3.1 Weak point analysis

As soon as the important assets have been identified, the existing weak points of these assets must be determined. The supplier can and should be included in this fundamental weak point identification and assessment process. A context diagram on the network communication and the protocols used as well as the presentation of the software components used provide the basis for the weak point analysis. A number of aids are available from IT using which the assessment of any weak points is simplified.[9]

In addition to these assessment systems, every operator must decide for himself how critical a weak point is in his own environment.[10]

Ultimately, the operator must also consider those weak points which may be known only to himself, such as additional remote accesses or concealed authorisations in the system which become active only under certain circumstances. The special features of the operating situation must also be considered. If outside workers and temporary staff are used to an increasing extent, the usual safeguarding measures will not always be effective and visible operating parameters at critical equipment become a weak point.

4.3.2 Threat analysis

Depending on the type of asset, it must be assessed which attack vectors can impact which protective objectives that can impair the function or the value of the assets. This may firstly be the loss of confidentiality of a secret production method or changes in the integrity of the control or test values in a continuous process. It is important that the asset is viewed as closely as possible in its context. A completely autonomous production island (an individual press, for example) without networking cannot, of course, be attacked through the network and the corresponding threats will not be relevant!

4.3.3 Risk assessment

In practice, a risk assessment is frequently made using an assessment by internal and external experts. Risks are jointly derived on the basis of the goods identified to be worthy of protection, the data analysis and the weak points and threats. The risks derived are then assessed in terms of their likelihood and the extent of damage. Assessment scales can be determined individually, whereby five-step or three-step scales are frequently used. A possible three-step categorisation of the extent of damage may take the following form, for example:

- High: great impact on the organisation through to destruction which is difficult to compensate for
- Medium: noticeable impact on the organisation
- Low: low impact on the organisation which can be absorbed without problem

The combination of likelihood and extent of damage indicates a risk level for every individual risk. This can then be set out in a table with possible protective measures, as Figure 9 shows by way of example. Tables of this type are also suitable as a simple tool to track risk over time if these risks are numbered with a risk owner and a date for the implementation of the measure.

8 See http://www.iuno-projekt.de/

9 The Common Vulnerability Scoring System (CVSS) and the Common Configuration Scoring System (CCSS) permit the comparability of weak points from the area of software development (Buffer Overflows or Privilege Escalation) during configuration (such as use of obsolete algorithms in SSL/TLS).

10 The so-called Environmental Factor (EF) is consulted here as a multiplier for weak points. It is derived from the exposure of the system to possible attack vectors.

This will then permit such risks to be identified which are beyond the risk appetite to be defined by management and which are to be reduced to an acceptable level using counter-measures. Measures should be concentrated on which, in particular, strengthen the protection of the critical assets. However, it should not be forgotten that a strong defence in one direction will be useless if attacks elsewhere can easily be successful.

4.3.4 Defining protective measures

A balance of measures can only be achieved from the perspective of the overall risk and the individual risks. The prioritisation of the measures must consider both the individual protective objective and the entirety of the protective objectives of an asset because in some cases measures for one protective objective may have a negative impact on other protective objectives. For example, creating external storage of a backup of the critical production parameters at the same time risks them becoming known because the parameters are no longer in the relative safety of the shielded system. If the system is destroyed by an accident, however, these parameters will be urgently required for a fast restoration of production capability. Against the background of such interdependencies, measures should always be planned and considered following an overall risk analysis.

4.4 Emergency management and restoration

In terms of the demand for greater production resilience – i. e. resilience to attacks and a rather more elastic behaviour in the case of damage – the consideration of emergency management, restoration processes and the sensible use of backup technologies is attributed greater significance in risk management.

The total material loss of systems can be compensated for by corresponding insurance. Unfortunately, the loss of the "configured know-how" in the system is far more difficult to compensate for. In terms of emergency management, it must be ensured that configuration data, operating parameters and tool settings, for example, are correctly documented and that this documentation can also be used to restore the production capability at a different location. Since in a normal case, no company has an alternative production centre, the question always remains as to how the secured data can be transferred to a new system. A simulated environment or a graded transfer of the secured configuration to individual segments of the system can be tested only at considerable expense (in service windows, for example).

Figure 9: Example of a simple asset/risk table

Asset	Possible threat	Likelihood	Expected extent of damage	Risk level	Possible protective measure
Main frame computer (HMI)	Infection with malware	Medium (occurs several times a year)	Medium (production impaired for up to 4 hours)	Medium	Deactivate USB Install AV[11] Freeze system

Source: Plattform Industrie 4.0

11 Anti-virus software

As long as no adequate technical and financial leeway exists for simulation, test and restoration in such failure scenarios, a backup or a recording of data should nevertheless be made. Since these data at the same time reflect the company's expertise, corresponding data carriers should be prepared and transported only after maximum physical security precautions have been taken. The encryption of such records is a good idea from the aspect of confidentiality but practice shows that the restoration process is complex enough and encryption would only complicate it further. Measures such as transportation in especially safe boxes and storage in safes may be suitable here.

5 Segmentation of equipment, systems and networks

In order to achieve an appropriate level of security despite the increasing networking of production, zones with similar protective needs must be identified and separated from each other using technical means. This must happen such that the separation of the individual system areas does not essentially restrict production processes. Communication between the zones can continue to take place if the transitions are clearly defined and secured accordingly. A careful zoning with corresponding identification and securing of information flows can, therefore, guarantee a high level of security also in the highly networked system landscapes of Industrie 4.0.

5.1 Separation of office and production

The fluent transition between office IT and the lower levels of production (such as the operational control level, process control level, control level, field level and process level) in particular frequently presents a direct point of access for attackers. A compromised system at the operating level without sufficient segmentation can, for example, cause great damage in the networked production system. Conversely, attacks from a compromised component of production on sensitive data and processes in the ERP of an unprotected system are realistic. Office IT and the downstream production systems must therefore be separated from each other to an adequate extent. In a first step, it must first be clarified which components are actually to be attributed to office IT. Any such zone definition should ideally be based on the identification of the risk-based need for protection.

The assets identified as being worthy of protection in the risk analysis and the assigned protection objectives are assigned a corresponding protection need using a threat analysis. Components with similar protection needs are then brought together in a zone. However, since it is frequently the case that an appropriate risk analysis cannot be made by small and medium-sized enterprises, direct zoning on the basis of a rough threat analysis is also possible. For example, all computers of office IT which have access to the internal email system and which are therefore exposed to special risks can be brought together in one zone. Network segments with components of comparable protection need therefore result both in office IT and in the production systems. In a second step, the zones of the operating level can then be separated from the zones of the production level by technical means.

5.2 Separation of system sub-networks

Whilst segmentation in office IT and production describe a vertical separation, system sub-networks can also be separated horizontally in the same way. This is necessary to counter any further compromising of upstream and downstream installations and systems following a successful attack on sub-systems of production. The necessity for horizontal separation becomes directly visible if the production system is considered in the context of Industrie 4.0. Actual production extends over a large number of systems and system groups, the components of which transfer not only data but entire functions in some cases. An individual compromised component in any such group can have significant

effects on the entire production – particularly if the attacker gains unimpeded access to neighbouring systems and can successfully penetrate the system group in this way. In order to counter any such scenarios, the system sub-networks must be divided into zones and separated from each other using suitable technical isolation measures. This separation is intended to counter cascade effects and may not at the same time restrict the horizontal and vertical communication with neighbouring system components in a way as to impair function. To guarantee this, special zone transitions will be described in the next section.

5.3 Zone transitions

In order to segment the identified zones, special transitions should be established between them. The entire communication between two zones is then channelled through a zone transition of this type. Concentrating the communication channels makes filtering, monitoring and generally the securing of communication between zones considerably easier: the systematic implementation of zone transitions has the advantage of substantially reducing the complexity to be considered because instead of the communication channels between individual components, merely the zone transitions between zones of component groups need to be considered. From a technical point of view, zone transitions of this type can be realised using appropriately configured routers and switches. The zone transitions themselves can be suitably isolated. Added to this are firewalls and data diodes to filter communication. Where necessary, zone transitions can also be equipped with special modules for attack recognition (see section 5.9 here). Hardware and software solutions are available on the market for these filter functions whereby hardware solutions are to be given preference for particularly critical zone transitions whilst software solutions frequently represent a less costly alternative. How to subdivide into zones and establish zone transitions is described in detail in the ISA/IEC 62443 standard.

5.4 Radio technologies

The described concept of zones and zone transitions should also be systematically transferred to radio technologies. This means in particular that all transmitters should at least be assigned one zone and the defined zone transitions are also to be realised via corresponding wireless gateways. The secure configuration of the radio technologies used plays a central role here. As low as possible ranges should be achieved by shielding and adjusting the signal strength. The selected radio technology should also guarantee a vulnerability to faults which is as low as possible (e.g. by means of frequency hopping). Due to the exposed nature of the radio network, strong authentication of the participants should be installed at all access nodes. Even a simple access restriction such as MAC filtering can be sensible here, particularly if weak older terminal devices are used which do not support stronger procedures. More recent systems also support modern methods such as Network Admission Control (NAC)[12], which, however, may also make investments necessary in current network technology and access points. If relay stations are used in zone transitions in order to connect geographically distant systems, insecure communication channels (without cryptographical protection) must be tunnelled through secure protocols.

5.5 Remote access

Remote access connections, for example for remote servicing by the integrator, can also be incorporated in the defined zones and their transitions. Remote access should always be implemented through at least one zone transition, whereby this should be protected from failure by the use of redundant gateways. In the case of larger systems, several zone transitions with independent hardware are also conceivable. For example, all M2M connections from distant systems can be routed via a separate transition.

At the start of every session, a strong authentication of the communication partners must take place. Irrespective of any further possible authentication on the target machine, this should already happen in the gateway of the zone transition. All external communication via insecure networks must be protected cryptographically. At least the integrity and authenticity of the transferred data should be secured, and data without special real time requirements should also be encrypted where possible. The use of cryptographically protect high quality VPN solutions is recommended here amongst other things. This has the practical advantage that commercially available VPN gateways are already equipped with a firewall in many cases. A firewall is essential to filter incoming inquiries. The encapsulation in OPC UA is a further option, as described in section. Even the essentially possible conversion of the configuration and virtualisation accesses to https provides basic security which should not be foregone. Secured REST-APIs as an alternative should also be given consideration in terms of a dissemination of M2M communication.

12 The protocol 802.1x is used here which permits authentication of the clients at level 2 – i.e. before use of IP.

Special rules for the setting-up, course and termination of a session should be defined for every zone transition (for remote access). Session rules include, for example, requirements as to the duration and functional scope of the session, permitted servicing intervals and IP address areas as well as the scope of the recorded session data. If these predefined session rules are violated, the connection must be cut automatically. The rules for remote access can be adjusted flexibly here to the defined roles. For example, customised session rules are a good idea for servicing, use, update, backup, M2M communication.

In frequent cases, machine and services cannot be reached directly but only via several zone transitions. In this case, it is necessary to satisfy the session rules for every transition used. If, for example, a machine connects with a machine of a remote system via three zone transitions, it may well be that the machine needs to authenticate itself three times. All session rules for the three zone transitions used then apply to this connection.

5.6 Internal and external networking of the production systems

As mentioned in the introduction, Industrie 4.0 systems are characterised by a high degree of networking. Not only is a high degree of internal networking between the individual machines to be observed but also between the automation levels. Machines and planning systems of distant installations are also brought together into groups. Here too, the primary objective should be the separation of communication and networks for which zones are once again suitable. It is advisable, for example, to conduct communication on the operating level and the M2M communication of the field equipment via different zone transitions. As mentioned in section 5, different gateways are quite conceivable for every zone transition envisaged. This will facilitate the selection of protective mechanisms and forms the logical separation of the zones communicating with each other also on the hardware side. Where two zones are connected to each other in the long term (also of distant systems), it is advisable to set up a site-to-site VPN tunnel. All communication of the two zones is channelled directly through the assigned VPN gateway. This can be realised easily using IPsec or SSL VPN. It is not a good idea to set a VPN for short-term connections. The communication partners should take the described path of predefined zone transitions here. For example, a site-to-site tunnel would not be set up for a machine which sends an individual query to an external database once a month. The boundaries here are blurred, however, and zones are conceivable which extend over several distributed systems. To maintain an overview here, the system operator requires a clear picture of the zone architecture.

Machines within a zone usually communicate via suitable field busses. Frequently, they do not have any security at all and can guarantee neither authenticity not integrity to say nothing of confidentiality of the communication. In view of the real time requirements, some of which are high, an encryption at field bus level is not always a good idea. However, within the Industrie 4.0 context authenticity and integrity should at least always be guaranteed. Field busses can be tunnelled through secure channels for M2M communication between distant systems. The encapsulation of modbus in OPC UA is an example here in order to connect remote zones with each other at the field level. The direct vertical integration of production into production planning and the handling of orders of modern ERP systems is also realised through such tunnels.

5.7 Cryptography

Many of the protective mechanisms already mentioned are based on cryptography. In order to guarantee secure communication, strong authentication or data confidentiality and data integrity, mathematical procedures are used which provide adequate protection in accordance with the current state of the art. Already researched and standardised procedures should be used exclusively here. Even if proprietary developments appear to be the more direct and simple path in individual cases, this is urgently advised against because they are usually broken within a short period of time.

Therefore, public authorities make recommendations on secure procedures and corresponding parameters which are not only publicly accessible but are also adjusted constantly to the current threat situation. The recommendations of the BSI[13, 14], of the NIST[15] and of the Federal Network Agency[16], in particular, provide a good and current overview of secure cryptography.

In practice a discrepancy between the public recommendations and the components available on the market can be recognised. Ideally, all cryptographic parameters of the operator can be set after purchase and the components securely configured. When purchasing system components,

13 See BSI (publisher) (2012)

14 See BSI (publisher) (2015)

15 See NIST (publisher) (2014)

16 See Bundesnetzagentur (2015)

the operator should ensure that the components support the replacement and therefore the updating of the cryptographic procedures used. Only in this way can the system withstand the highly dynamic threat situation even over a longer duration of use.

5.8 Operator's public key infrastructures (PKI)

Ideally, the system operator will already have a public key infrastructure (PKI) for office IT using which he will also be able to generate certificates for his systems and modules and for the network equipment. In this case, it is important that new system components can be integrated into the existing PKI. If the operator does not as yet possess a PKI, this should be planned, prepared and operated in close cooperation with office IT since these tasks belong to traditional IT security. An operator model is to be aspired to here in which office IT provides production merely with its own issuing CA but operates it together with the remaining confidential hierarchy and the accompanying technologies.

The operator should, in particular, pay attention to whether the certificates (e.g. X.509) can be processed by the components and whether adequate memory exists for the storage of root certificates. Many pieces of equipment from the embedded environment are also designed too weakly to satisfy the usual requirements placed on algorithms and key lengths. An adjusted policy must be drawn up in cooperation with office IT. The operator should also use a Certificate Lifecycle Management (CLM) tool to manage the certificates. Ideally, the certificates of all system components can be managed using this tool and also be updated during ongoing operations. The system is frequently subject to high component fluctuation: not only are the components within the system replaced frequently but temporary component networks can also arise with other systems. If certificates are then declared invalid to a large extent, they must also be marked accordingly. The standard procedure for this is the rather static Certificate Revocation Lists (CRLs) for the publication of invalid certificates. Incidents in the recent past show, however, that this technology is reaching its limits.[17] In order to take account of the increased dynamism, the use of the Online Certificate Status Protocol (OCSP) is advisable. In this case, the validation of certificates of the components is outsourced to a validation service instead of generating very long CRLs which may already be obsolete if a problem arises. Even with OCSP, security problems have recently arisen which have currently not yet been conclusively remedied. In the absence of alternatives, the user currently has no other choice than OCSP.

5.9 Control of network communication

Whilst the previous chapter dealt with methods and approaches to separate in communication networks, aspects of control and maintenance of network communication will be explained in this section.

5.9.1 Monitoring

As already intimated in section 5.2, zone transitions are suitable points in the network infrastructure to record system communication and examine it for any unusual features. Commercially available monitoring systems so far only offer the recognition of possible malware on the basis of signatures or behaviour-based recognition of protocol anomalies. However, these procedures can only be implemented with a certain amount of work for production because the corresponding configurations and learn phases require great expertise and knowledge of the local environment in many cases.

An anomaly here is understood to be behaviour that deviates from normal operations and which can be recognised, particularly at the field level, by relatively identical communication patterns. Whilst solutions of this type do not offer complete protection against attacks via the network, they do frequently cover them to an adequate extent. In view of the high dynamism of the attack patterns, the Intrusion Detection Systems (IDS) used and the Intrusion Prevention Systems (IPS) must always be kept up to date. Only with the most recent signatures can harmful anomalies be reliably recognised. The data recorded should be centrally stored, at least temporarily, for the purposes of possible forensic examination. The scope of the data recorded should be adjusted to the security requirements of the zone transition: from recording and analysis of individual measurement data at the field level through to the complete recording of identities of all communication partners, time and duration of communication as well as spoken protocols of all sessions can be adjusted flexibly using suitable monitoring systems. Sensitive data should, however, be excluded from recording.

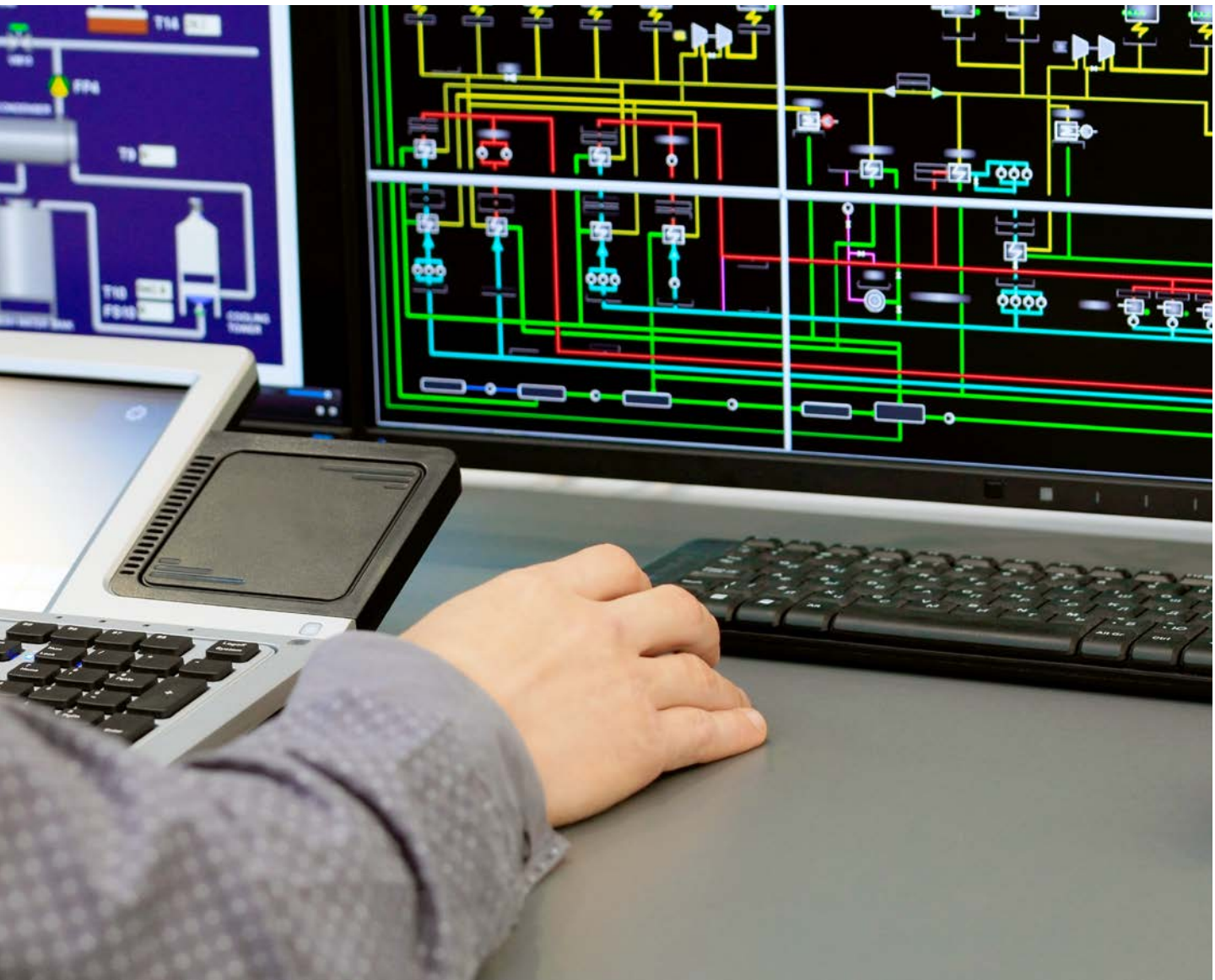
In addition to data recording at the zone transitions, monitoring systems can also be integrated directly into the control panel. Depending on network infrastructure, the advantage of this is that security-relevant events can be reacted to directly and centrally. Operator and integrator should carefully consider whether the network infrastructure is able to withstand the communication load with a

17 See here the steeply risen network load after the heartbleed weak point became known in the OpenSSL Library and the mass revocation of certificates.

possibly very high data throughput to the central control panel. A communication situation with anomaly recognition as an additional information source will be essential here in future. Centralised log management should be initially established for the centralised recording and secure storage of log data. This will prevent the subsequent manipulation of logs by privileged users and will facilitate central analyses following security incidents. The Security Information and Event Management solutions (SIEM) are a tool which have so far only be used in the group environment for the further harmonisation of logs, their analysis and correlation of data from different security concepts. Using these solutions, the operator has an overview of the condition of all security-relevant components and can react to recognised incidents in real time and in a centrally controlled manner. The security components used must be compatible if they are to be correctly integrated in the SIEM system. SIEM solutions are the crowning glory of IT security measures under strict consideration of standards and the selection of suitable source systems because their implementation frequently requires man years and they must be constantly adjusted to changes in the source systems. This means that SIEM should primarily be used in the sense of a “managed service” because SMEs have neither the requisite resources nor can they provide the requisite operating staff or trained incident managers.

5.9.2 Isolation of incidents

If the operator recognises an attack or infection with malware at an early date, the network segments concerned must be isolated from the network infrastructure in order to prevent it spreading. Here too, the described zoning of the network infrastructure benefits the operator: if a subnetwork is affected by a fault which threatens to spread to the adjacent network areas, it is sufficient to cap the corresponding zone transitions and therefore to isolate the fault from the entire system. This can be realised quickly and simply by the integration of a few filter rules into the respective firewalls at short notice. Once the fault has been isolated, the network area concerned can be restored to a trustworthy condition. The use of Software-defined Networking (SDN) technologies - which are already established amongst the operators of computer centres and cloud servers – can be given consideration in future also for the production networks. SDN permits the central storage and automated configuration of the network topology.



6 Secure identity management

Plattform Industrie 4.0 already established in the working paper “Secure identities” as follows:

> ***“Secure identities are the starting point for security chains that protect data capture, transport and processing at the hardware, software and process levels. They are a pre-requisite for many other protection measures. When an attacker succeeds in assuming an identity on an unauthorised basis, all other constructive measures, such as access protection, make no sense. The primary aim of secure identities is to start a chain of trust in automated communication.”***

The use of clear secure identities is essential both to safeguard authenticity, preserve integrity and above all transparency.[18] Working on the basis of secure identities has already become standard in the office IT systems. For Industrie 4.0 the relationship between man and machine (for example their identities) plays an important role. This will be eclipsed in future by identities for systems, machines and work pieces in machine-to-machine communication (M2M). The following sections provide an overview as to which functions of established identity and authorisation management can also be used for production and where new processes and functions must be created.

One of the most important tasks in the secure design of production systems is to ensure the authenticity of the respective operator. In the area of pharmacy, foods and the chemical industry great attention has been paid to this aspect for many years because organisations such as the Food and Drug Administration (FDA) in the USA and the European Regulation REACH (Registration, Evaluation, Authorisation and Restriction of Chemicals) from 2007 have led to considerable rules in these areas which, in their turn, imply transparency with respect to the question of “who worked when with which batch of the substance during which production step”. Consequently, the personal login of a worker to a machine of the chemical industry is quite usual whilst similar approaches have not been implemented in the forwarding industry, primarily due to intervention from works councils due to alleged monitoring of workers or due to technical problems.

It is a fact that the transparency of actions and personal assignability can only be achieved by using personal user accounts in systems and machinery as well as operating computers. This then requires the management of a far greater number of accounts (which so far have distinguished only between “fitter/repairer” and “operator”). This personalisation of the user accounts leads in its turn to the need to efficiently manage them parallel to each other on a large number of systems and machines or at least to facilitate the personal assignability at the level of technical application if the access to the operating systems cannot be or is not to be personalised for technical reasons.

18 See BMWi (publisher) (2016b), p. 11

6.1 User accounts in operating systems and application

A distinction must firstly be made between a login (identification) of the user to the operating system and the application. It has so far been the case that systems and machines could only be used in the context of a user created locally in the operating system. The following section shows that in future only user accounts managed centrally in a directory (generally referred to as "AD"[19] accounts) are to come into question for the login to the operating system. It must be noted that many software programs which are currently used do not permit the use of such accounts because a local system account is expected for execution. A further problem in the use of such accounts is that it may be necessary to support the directory service 24/7 to secure usability. This is necessary to enable any "locked out" users to access their accounts again, something which at least requires interaction with the service desk. An alternative here is the use of system accounts which automatically log in for the start of the operating system and a complete focus on the management of user accounts in the applications of the production. This, in its turn, will usually require the use of centrally controlled provisioning solutions which facilitate the creation and deletion of user accounts on the basis of rules and threshold values or limit values.

In addition to the centrally managed "AD accounts", user accounts for production applications[20] should be individually assignable to the employees and be centrally managed. An interface to the central Identity and Authorisation Management (IAM) system is necessary here.[21] Writing access to the user account database is similarly conceivable which requires an insight into the table structures, however.

6.2 Life cycle of user accounts

As described in the above section, corresponding user accounts must exist to use an application. However, they must first be applied for and approved. These processes are the core processes of identity and authorisation management and use can largely be made here of the known interfaces and established workflows of IT identity management. However, it is not sufficient to merely apply for and approve and then generate a user account (roughly granular). Firstly, the technical implementation of the provisioning must be correct – which will not usually function without the cooperation of the supplier or the manufacturer of the software – and secondly, the necessary authorisations and functions in the application must be assigned to the user account as a next step (Entitlement Management). This finely granular coordination and stipulation of "what the user may do in the application", is frequently a rather complex chain of functions within the application and can only rarely be directly implemented using the IAM system. It may possibly be necessary to continue to have a qualified person to manually assign the authorisations as soon as the account has been automatically generated.

The function of automated generation is not adequate on its own. In particular, great importance will be attached in future to the fast deactivation or sustainable deletion of accounts because so-called "orphaned accounts" without an assigned person (after dismissal or in parental leave or in the case of death) represent a high potential for abuse (see here 6.7 Managing privileged accesses). Consequently, the IAM system must offer the function centrally as must the application itself to deactivate or delete user accounts quickly and easily via interfaces or the user interface.

6.3 Logs: auditability of user accounts and accesses

Ultimately, it cannot be ruled out that irregularities or evidently abusive use of systems and applications will arise at a given time. It must be possible here to track in detail who had access when and where, and who made modifications when and where. This will require the application to store detailed log messages and to keep them in an unalterable form where possible over lengthier periods of time. Functions for the direct, access-protected storage of logs on a separate (Syslog) server would be desirable for log centralisation as is usual in IT. The heeding or the compliance with or orientation to standard formats as provided by Syslog, LEAF or CEF, for example, would be ideal here.

This facilitates the central analysis and correlation of messages and permits a definition of central thresholds such as alerting Security if unsuccessful access attempts have been made on various pieces of equipment within a short space of time using one user account (primarily by using so-called Security Information & Event Management SIEM solutions).

19 Active Directory

20 As in a production information system or Manufacturing Execution System (MES) or Production Planning and Control System (PPS).

21 By Simple Provisioning Markup Language (SPML) or Simple Cloud Identity Management (SCIM).

6.4 Identification, (strong) authentication and authorisation

Industrial IT essentially uses the traditional "user name/password" model. For this purpose, the user provides the operating system or application with his user name as a means of identification. He identifies himself to the system or asserts that he is the user "John_Smith" (by providing his user name). To prove this assertion that he is "John_Smith", he also provides the password belonging to the account. Once this authentication has been successful, the user is given access to the functions assigned to him or approved for him (authorisation). These purely knowledge-based procedures have proven to be inadequate many times in the past because users tend to write down passwords or even actively pass them on. In order to counter abuse, multifactor procedures have been used for some time. They combine the knowledge of a user name with the possession of a token or a smartcard or the comparison with biometric characteristics such as fingerprint or retina pattern or facial form and other features. In production, these procedures frequently encounter difficulties of implementation because the efficiency of these authentication technologies may be restricted by protective clothing or dirt. Only the use of stable tokens on the basis of active or passive RFID/NFC technology has proven reliable. Tokens of this nature are used ("electronic key system" eks from Euchner, for example) particularly for the "administrative access" of maintenance staff or fitters for machine controls. This extends explicitly also to control equipment as recognised on specific software modules of the manufacturers for the integration of hardware (such as the Siemens Device Manager).[22]

In addition to these procedures, the certificates on the basis of x.509v3 are becoming more important both for users and for machines and servers. This well-known technology, which comes from the area of webservers in eCommerce, is also used to secure web interfaces for systems and SPCs.

However, mention must be given here to the similarly growing need for enterprise key and certificate management because it would appear to be impossible to manually manage the considerable quantity of cryptographic material in Industrie 4.0 production.

6.5 Machine-to-machine communication

Particularly in the case of communication between systems and machines, recourse is made to the already described use of certificates. They are also frequently used to execute authentication of both sides in order to be able to provide clear identification to the counterpart and where required to also be able to establish encrypted communication (a symmetrical key for the actual data transfer is exchanged here using the existing asymmetrical keys of the certificates). New protocols have become established in addition to the certificates, particularly from the environment of secure communication beyond company boundaries and the use of apps[23]. OAuth 2.0 is particularly used for small mobile applications (so-called apps) which permit the access to resources without having to provide credentials (such as user name or password) directly to the providing resource. Complex accesses to the resources of third parties can be provided using these protocols as will be usual in the environment of Industrie 4.0.

6.6 Authorisation management

The management of authorisations within an application or the assignment of authorisations to user accounts is generally referred to as authorisation management. Ideally, authorisations are combined to produce logically matching bundles of rights which are usually used by assigning a role or group. This is usually subsumed under role-based rights management.[24] The type of assignment can also be on a discrete base, however, by explicitly determining for every resource which subject may access it,[25] and which possibilities of access are permitted.[26] In the worst case innumerable direct relationships between objects and subjects result so that a larger number of resources or users can quickly lead to intransparent solutions.

The military area has procedures which divide resources into classes (Public|Internal|Confidential|Secret or as shown in Figure 8)[27] and assign people the corresponding approvals[28, 29].

22 See Siemens AG (publisher) (2010)

23 Such as the Security Assertion Markup Language (SAML2.0) for federating, OAuth 2.0 for API authorisation and OpenIDConnect (OIDC) as identity layer.

24 RBAC – Role-based Access Control

25 DAC – Discretionary Access Control

26 Reference is usually made to CRUD – Create|Read|Update|Delete.

27 Data classification is one of the most difficult and complex tasks in IT security.

28 Clearance

29 MAC Mandatory Access Control is a very strict principle which has not proved successful for use in industry.

Consequently, a modified role-based approach has become largely established: a number of the most important and usual rights is classified and assigned by roles whilst a small number of individual rights is assigned discreetly.

In order to achieve a high degree of security whilst at the same time granting more flexibility, procedures are used which do not assign persons to groups or roles but which check a number of attributes which the subject must satisfy as part of the authorisation check.[30] The context of the access can also be incorporated if, for example, a subject is to be given access according to his roles or group classification but the access is refused because the access is made from an unknown device at an unusual time.[31] This context-based authentication can therefore be seen as a supplement to roles and discrete rights because it subjects the access to further restrictions or checks.

6.7 Managing privileged access

A special challenge to security is presented by the highly and most highly privileged accounts. These "administrative accounts" or "superusers" are able to make substantial changes to the systems and are frequently able at the same time to conceal their activities by manipulating the system. In production, the accounts of the fitter, maintenance and frequently those of the service providers and suppliers are particularly privileged because these persons or roles are required to make adjustments to the system. By comparison with the "root" accounts on Linux or the domain administrator in the Microsoft Active Directory, such important authorisations are potentially dangerous. Added to this, is the fact that for reasons of efficiency or serviceability, the account name-password combination (generally referred to as "credentials") is kept identical in many production systems and known to a number or individuals (usually all fitters or maintenance personnel). This automatically leads to an overall unsafe situation because neither traceability nor confidentiality can be adequately protected. For systems with network connection and rudimentary protocol support (SSH – Secure Shell or https), it is now advisable to conduct the access of such privileged accounts using a central system. These tools are referred to as Privileged Access|Identity|User Management[32] and have functions for the secure storage of a large number of credentials whilst also facilitating the fast and intensive rotation of the passwords. The latter is facilitated by an automatic mechanism which alters the password in the system after a user session has been completed, stores the new value in the internal database and releases it for the next user for the duration of his access. Ideally, the system starts these sessions directly and injects the password so that the users never learn of the credentials.

6.8 Directory services for the management of identities

Even now, the networked components of production are larger in number than the IT components used operationally in office IT. Even if hundreds or even thousands of employees have a digital identity in the company so as to be able to have access to their IT systems, the number of the system components, control systems, sensors and actors which are individually identifiable will soon require an almost unmanageable number of secure identities. In a first approach, it would be conceivable for these identities to be kept as a part of the asset database. The identities also help to identify assets clearly and securely. A great part of communication in Industrie 4.0 should be secure, however, i.e. primarily "authenticated" and this in its turn generates a need for frequent and fast request of ID information. Databases are suitable to only a certain extent for the many millions of such requests per second with a huge number of entries. Directory services play a decisive role here. Unlike databases which are designed for the efficient storage without doublets, directories offer multiple storage of similar data sets at various places in the hierarchical tree. This permits requests on the same identity in different contexts to be answered considerably faster. The data of the telephone and cable companies serve as a comparison for Industrie 4.0 here. The customer data for the provision of services have always been stored in directories in order to accelerate fast recurrent requests and guarantee the satisfaction of the highest demands placed on availability.

30 Attribute Based Access Control (ABAC)

31 Context Based Access Control (CBAC)

32 PAM/PIM/PUM – depending on manufacturer and emphasis, the solutions are termed Privileged User Management, Privileged Access Management or Privileged Identity Management. Their functionalities have converged, however, for some time now.

7 Security of software in production

Industrie 4.0 and the strong networking of production systems require robust, reliable and trustworthy software. From ERP and MES systems, process management and SCADA systems through to stored programmable controls (SPCs), software covers security-critical processes. The system operator is confronted with a highly heterogeneous software landscape: he has the choice between a multitude of technologies, providers and implementations. The system operator should know the main parameters of secure software development in order to be able to request a secure development process from suppliers. Only with this knowledge can the operator ensure that his system can withstand the threat situation. In addition, there are operators who adapt components available on the market to own needs and circumstances using their own software developments. Here too, the criteria and methods of secure software development play a decisive role. This chapter describes the main steps and criteria which must be considered in the development, servicing and compiling of the software used.

7.1 Software security

A decisive criterion in deciding whether a software module can be assessed as secure is a secure software development process. Rough parameters can be established even if it is frequently not possible for the operator to determine the underlying criteria of the software development process of suppliers in detail. As already mentioned, these aspects should be taken into consideration. Even at the software design and planning stage, the later application environment will play an important role. Software which is exposed to a greater attack environment (e. g. availability such as in the case of Distributed Denial of Service (DDoS) via external interfaces) must be specially adjusted to the expected threat situation. For this purpose, a rough risk analysis should be made (see section 2.4): security requirements to be placed on the software result from the assets defined as worthy of protection and a vulnerability analysis. If, for example, the software processes sensitive or security-critical data, this must be taken into consideration in the software design (for example in the form of corresponding cryptographic modules to encrypt these data). A system operator will then be able to decide whether the security requirements placed on the third party software are in line with the protective requirements of the system.

The identified security requirements are then incorporated in the design of the software. The aim here is to minimise the area of vulnerability for particularly critical areas. If, for example, a complex data structure is read in, this process can frequently be very vulnerable to errors. Attackers frequently make use of weak points during the parsing of such data structures in order to smuggle malcode into the attacked system. In this case, it would be advisable to firstly check the origin of the file, possibly also by checking a digital signature. Then at least only files from a trustworthy origin are passed on to the actual input and processing process. Basically, the principle of the smallest possible privileges should be implemented systematically and logically. Every module, whether process, user or additional program, may only have access to those functions and data for which it possesses the requisite rights. The distribution of rights is to be approached as conservatively as possible. A triple consecutive security procedure can be recognised in the above example: first of all, the software checks the origin of the data using a digital certificate. It then uses the access rights to check whether the data may be further processed and

only then is the actual processing commenced. This principle of "defence in depth" should be systematically used in the software design process in order to reduce the vulnerability of critical software modules to a minimum. The functional scope of the software should also be largely restricted. The operator should adapt purchased components himself by deactivating software modules and functions which are not required on the condition that the components offer a configuration option of this type.

Suitable development environments should be selected for implementation. Even the choice of the programming language can rule out many known gateways from the outset. Some security aspects can also be realised simply through compiler settings. Recourse should also be made in development to software libraries which are as secure and up-to-date as possible. If, for example, a module is implemented to encrypt data, the developer should make use of popular cryptographic libraries which are still actively updated in particular.

The implementation is followed by security tests, firstly in the form of static and dynamic code analysis. Reference can be made in particular to fuzzing (the testing of software with randomised input data) and the testing for weak points in storage management (e. g. using address sanitizers and similar tools). Many programming errors can frequently be recognised in this way. Ideally, a manual code review using source code should also be conducted.

Before the actual release, it must be ensured that all security requirements which have been identified in the first step have been satisfied. Executable programs and all following updates should be digitally signed by the integrator.

For further information on the development and assessment of software components, reference is finally made to the standard ISO/IEC 25000 ("Software Engineering – Software Product Quality Requirements and Evaluation (SQuaRE) – Guide to SQuaRE") and to the corresponding standard series ISO/IEC 250xx. The Security Development Lifecycle (SDL)[33] defined by Microsoft also offers more detailed descriptions of the aspects mentioned.

7.2 Software update and maintenance

The update and maintenance of software following its delivery is at least just as important as its secure development to the extent permitted by the operation and maintenance windows. In order to meet the highly dynamic threat situation, the risks should ideally be reassessed on a regular basis: new security requirements will then result which are incorporated into the development process accordingly as change requests. This adjustment (change) should be made by the software developer who reacts to new threats with corresponding protective measures. When selecting the components, it is essential that the operator clarifies the extent to which this form of maintenance and adjustment (i. e. the possibility to apply for and input changes) to current threats is supported by the supplier. In particular, the software developer should be able to react quickly to any security loopholes becoming known and supply corresponding updates which can be incorporated just as quickly during maintenance work. The supply of the updates should be incorporated in a clearly defined release management process which also incorporates comprehensive software update tests – the operator cannot afford to jeopardise the availability or integrity of his system by a software update which secures against a weak point which will probably not be attacked. Furthermore, the update process is also to be secured against attacks: remote updates must be conducted via secure channels, all new software must be digitally signed by the developer and this signature must be verified by the serviced component. Particularly in the field area, the compatibility of the update with other dependant components must also be ensured.

7.3 Software governance

In addition to development and service, an important role is also played by software governance, i. e. the organisation and management of the entire software infrastructure. The complexity of modern systems requires a large number of coordinated software solutions. Rules on the incorporation and management of programs must be set up to manage this in part very heterogeneous software landscape within a system. First of all, all the software components in a system must be pinpointed and documented. This general overview must be updated constantly irrespective of the rules defined to incorporate new components.

The implementation of secure software management firstly requires a regulation as to the conditions under which new software components and programs may be integrated into the system. The defined criteria for secure software must be at least considered here. The rules on incorporating software must be defined individually for every zone. For example, which software classes or even special programs may be installed can be stipulated for every zone. The use of application whitelisting (see the next section) and blacklisting is to be recommended here, also combined with specific rules for the relevant players and roles. If a player requires a program or a special program version for which he has no installation authorisation, the system can nevertheless continue to be adjusted flexibly and securely by establishing a software request process. Such a process will then contain

33 See Microsoft (publisher) (2016)

the checking of the aforementioned requisite minimum standards using which the software security of the entire system can be kept at an appropriate level. It is also a good idea to use software management systems with which the operator can centrally incorporate, manage, update or remove distributed programs simultaneously.

This identification and documentation of all software components of the system furthermore provides a foundation on which to observe the current threat situation: if weak points or security loopholes are recognised, the operator can determine whether his system is directly affected by them. The identification of all software components currently presents great challenges to system operators. However, this practice will be essential for Industrie 4.0 systems and should at least be aspired to.

7.4 Whitelisting and system hardening

It has been common place in office IT in recent years to supply or operate server systems only with those functions which are absolutely necessary. In the late 90ies and at the beginning of the millennium it was still usual to have all services available in the operating system active in the delivered state even if they were not used. Later on, so-called "system hardening" was then performed subsequently during which the services and functions which were not used were deactivated. This still tends to be unusual in IT components of production and leads to very large areas of vulnerability due to non-updated systems. These areas of vulnerability are no longer acceptable in the context of Industrie 4.0 so that protective measures are urgently needed for obsolete systems which are no longer being maintained. In addition to the mathematically predictive systems emerging at the time these guidelines were written[34], whitelisting solutions have proved to be effective and helpful. In the simplest case, whitelisting means the creation of a list of permitted programs: exclusively programs on this list can be started. Lists which automatically learn from the normal system behaviour are considerably more advanced. This method of protecting existing systems is the most important from today's point of view and is installed as a small software component in an old system classified as "clean" and observes the behaviour of the system processes, services, the network communication and the interaction of the programs over a period of time. Following this learning phase, the system is switched to monitoring mode and reports any previously unprotocolled behaviour as out of the ordinary. The system is activated following a manual decision as to which of the new patterns are normal or abnormal. Any unusual activity (as triggered by a virus infection or the start of programs from a USB stick) is now actively suppressed.

34 Such as the mechanisms presented by the US company Cylance

8 Considering IT security in the purchase of machinery and systems

New dangers are associated with the increasing networking of machinery and systems within the context of Industrie 4.0 which have so far being given very little consideration in the procurement process. Up to now, the focus has been placed on functional scope, availability and output rates when selecting machinery and systems. This has meant that new production machines are supplied with system software even today with a maintenance commitment from the integrator which has already expired.

The fact that security requirements are not considered is particularly critical in connection with the long life cycles (frequently greater than 20 years) of machinery and systems. It is frequently not possible to subsequently adjust to the new threat situation because such changes to machinery and systems would usually entail far reaching consequences, such as the loss of support by the provider or a complete new examination of the system in accordance with the Industrial Safety Ordinance (BetrSichV). The ongoing operation of the above-mentioned obsolete operating and control systems is one of the greatest challenges for current production IT. It must be considered here whether “freezing” the systems by special software is a good idea and compatible with the integrator.

To make matters worse, there is the fatal and always existent idea that machines which are practically not connected to the internet are unassailable. Attacks such as Stuxnet have proven the opposite here and similarly show the subsequent need for adjustment to an altered threat situation.

The altered security situation with much malware and targeted attacks on industrial systems clearly show that when selecting machinery and systems a minimum level of sustainable IT security must be demanded so that secure connection and secure operation is facilitated. Not only the time of acquisition but also the entire life cycle of machinery and systems must be taken into consideration. When introducing a security concept for IT in production, the purchase process must first be considered and revised in order to correctly set the path for the future. Preparing or extending procurement guidelines can introduce requirements on IT security of machinery and systems and requested from the supplier.

When procuring new machinery or systems, it must be ensured in advance that a coordinated and long-term solution for the secure operation of the system over the entire life cycle is prepared and agreed with the supplier. Industrial associations such as ZVEI and VDMA point out this requirement to their members in their own publications and draw up requirements for more IT security criteria in the procurement of modules or components.

8.1 Overall consideration of the procurement process

The approach of considering IT security of machinery and systems at the procurement stage shows once again that IT security is a complex project which has an impact on all corporate areas. The uniform adjustment of the procurement

process to the new requirements of IT security and Industrie 4.0 is a complex matter. The digitalisation and automation of processes is a sensible idea in the long-term and associated with much work and high investments from the point of view of SMEs. Of course, not all measures need to be launched simultaneously and frequently simple changes or the introduction of new tools will help to improve the level of IT security in the procurement process.

IT security must be a main component of the procurement process for machinery and systems. For this purpose, a uniform procurement process with adequate scope must firstly be defined and it must also be "lived" accordingly. If good processes, guidelines and tools are already established, they need to be extended to give consideration to IT security. In some places, it will be a good idea to define additional processes rather than adjust tried and tested ones. Such decisions must be made individually for every company and every procurement process and must be based on an adequate analysis.

Therefore, the first step towards IT security in the procurement process must be a corresponding **process analysis** that focusses on the consideration of IT security. It is frequently shown in practice here that the procurement process itself and its corresponding processes (e.g. supplier management processes) are not adequately defined and that IT security is not considered at all. Adjacent processes which would serve as an important input for IT security (e.g. asset management) are also usually non-existent. Frequently, the skills necessary for IT security in Industrie 4.0 also do not yet exist and often also fail to figure in corporate strategy. Some of the questions addressed in the analysis phase are as follows:

- Does a procurement guideline for machinery and systems exist and does it take IT security into consideration?
- Are suppliers assessed in terms of the IT security of their processes, products and services offered?
- How are the IT components, new machinery and systems incorporated into existing systems (asset management)?
- Do sufficient IT security skills exist in production and are they incorporated in the procurement process?
- Is there an overview of "communication partners" in production and the data exchanged?
- Is this overview checked for IT security risks as part of the "incorporation concept"?

Ideally, the analysis will show as many of the relevant weak points in the company as possible and must be given attention at the highest managerial level to facilitate the planning of new processes by the requisite resources. The main activities of the process planning phase are listed in the following:

Process planning steps

- Preparation of new concepts
- Preparation of new guidelines
- Revision of existing processes
- New design of absent processes
- Development of requisite skills
- Draft of new guidelines

The **implementation** of the defined measures must be actively requested and promoted by management. Once analysis, planning and implementation have been completed, a continuous **evaluation** of the implemented measures must be conducted in the operating phase as a final step. Based on the results of the evaluation the implemented measures and processes are continuously improved and revised.

8.2 Objectives of a procurement guideline

When the operator procures production facilities in the form of machinery and systems, he usually also purchases the corresponding IT components. He must, therefore, become acquainted with the IT of the product and with IT security. An updated procurement guideline is a good and less complex tool for IT security in the procurement process. Even if it may not contain all requirements in a first step, it Is important to include IT security of machinery and systems here at all. The instructions in a procurement guideline of this type make it necessary to address the topic of IT security and help to assert basic requirements for the supplier and to actively pose questions on IT security . It is necessary here to prepare the content of the procurement guideline in close cooperation with those responsible for IT security.

All foundations of IT security so far considered here can and must apply also and in particular to production machinery and their components and the software used. The knowledge gained from the upstream sections therefore directly leads to requirements which are to be actively requested from the supplier using a procurement guideline. For example, in order to facilitate complete asset management, it must be possible for the operator to see which IT components are built into a system (see chapter). The security requirements which may be derived directly or indirectly from the previous sections are now transferred in the following to the content of a procurement guideline in the form of a requirements and features catalogue. There is no claim here to completeness and it is intended to provide initial inspiration. It must furthermore be pointed out that new laws

and standards will first have to be created for some requirements and features in the context of Industrie 4.0 so that currently not all requirements can be met.

8.3 Exemplary catalogue for the procurement guideline

The following requirements and features catalogue lists the requirements to be placed on the integrator of machinery and systems or rather how the products are to be assessed in terms of which security-relevant features. Every company must evaluate individually whether these are hard (direct influence of the purchase decision) or desirable aspects (e.g. requirements which will be associated with Industrie 4.0 but are not yet necessary today). The market must be examined here in terms of the maximum possible satisfaction of requirements.

A. Access protection by user management

Requirements placed on the integrator of machinery and systems	Details i.a. in sections
Strict functional separation between administrative and productive authorisations by internal user management of the system and its IT components.	6.7
User accounts of the system can be provisioned using centralised authorisation management (identity and authorisation management).	6.1
Simplified login to IT components and web applications using interfaces to central login procedures.[35]	6.1
Methods of strong authentication can be used.[36]	6.1

B. Physical access protection

Requirements placed on the integrator of machinery and systems	Details i.a. in sections
Unauthorised persons making modifications to system parts or control components is prevented, e.g. by physical separation between operator and administrator functions, by lockable operating panel or by function enabling using radio chips (RFID).	6.4
Possibilities to monitor the lines of the control system. The new Intrusion Detection Systems (IDS) already provide recognition function.	5.9

C. Cryptographic capabilities of the system and components

Requirements placed on the integrator of machinery and systems	Details i.a. in sections
The algorithms and key lengths used as well as the crypto libraries used by the software manufacturer are disclosed.	5.7
Risk analysis of the software used has been conducted. The results are transparently shown to the operator.	7
Weak protocols or endangered data transfers are appropriately secured by cryptography.	See also 5.7 and 5.9
Changes to encryption algorithms, key lengths or libraries used must be communicated or disclosed to the operator.	7.3
Open and known, tested cryptographic standards such as TLS 1.2 or higher are used and the recommendations of the BSI are followed when selecting the approved algorithms.	5.5 and 6.5

35 Incorporation in an Enterprise Single Sign-On (SSO) or Web-SSO which facilitates the single login and simple use of several applications and systems.

36 Such as the use of ID cards/chipcards (so-called smartcards) or the use of electronic keycards or keyholders with radio technology (RFID).

D. Definition of the secure delivery status (security by default)

Requirements placed on the integrator of machinery and systems	Details i.a. in sections
The machine or system is to be delivered by the integrator such that all functions not directly required for minimum operation are deactivated as standard in the basic installation.	7.1
Information on the activation and deactivation of features must be present in the documentation supplied.	4.1
The security settings for the features of the minimum operation must be validated.	
During commissioning, the software may not use any standard passwords or user accounts.	6.1 and 6.7
When awarding new individual passwords for the administrative accounts, password rules for the awarding of secure passwords must be used	6.7
It must be possible to alter the passwords of the administrative accesses from the software (if no directory service is used for the management of rights).	6.1

E. Proof of secure software development

Requirements placed on the integrator of machinery and systems	Details i.a. in sections
Uniform quality and test management in the development of software and corresponding documentation.	7
Disclosure of test cases, test reports and update of release notes for every update.	7.2 und 7.3
Proof of the development of software in accordance with the requirements of Secure Software Development Lifecycle (SDL): the machine or system manufacturer must prove that this has been taken into consideration in the selection of the software suppliers.	7.1
Warranty that software has been exclusively used in the products which has been designed for security and that third party software, in particular open source software, has been correctly examined for weak points.	7.3
It must be possible to operate the software in a failproof manner (if necessary). The integrator must be able to prove how this fail safe feature can be achieved.	

F. Segregation of duties – SoD

Requirements placed on the integrator of machinery and systems	Details i.a. in sections
The software may under no circumstances be operated in the context of a higher privileged user (admin, system root etc.).[37]	6.7
The software must be designed for the use of minimum privileges and must also be executable in the context of a user account managed via an active directory (AD) without special privileges.	6.6

G. Application integration via a DMZ/service zone

Requirements placed on the integrator of machinery and systems	Details i.a. in sections
The incorporation of the system network in production via the known “gateways” is of particular interest and for the operator. The provider should specify which protocols and ports are required for secure operation.	5.2 and 5.3

H. Integration of the software into the existing security management

Requirements placed on the integrator of machinery and systems	Details i.a. in sections
The integration of the software into existing security management systems is facilitated by the protocols and interfaces used, for example. Examples of systems which are to be incorporated under certain circumstances: • IAM identity management/authorisation management • Log management and SIEM Security Information Event Management • AD active directory	6 5.9.1 6.8

37 In particular, through the introduction of the User Account Control (UAC) in Windows Vista, 7 and 8, a large part of the applications developed for Windows XP no longer work because this “SYSTEM” or “ADMINISTRATOR” requires a context.

I. Internet access

Requirements placed on the integrator of machinery and systems	Details i. a. in sections
Software used in the machine or systems may not automatically create a connection to the outside (to the internet).	etwa 5 ff.
A “stand-alone” operation of software (without connection to the internet) must be possible. If the Internet access is elementary and necessary, it must be possible to operate the machine or system from a DMZ.	5.1
A detailed presentation of which protocols and ports are used and which data are exchanged for which and purpose is provided by the supplier.	5.2 and 5.3
The operator must be in a position at all times to suppress connections unilaterally without permanently impairing production.	5.5

J. Openness of the (remote) maintenance functions of the system

Requirements placed on the integrator of machinery and systems	Details i. a. in sections
If remote maintenance is viewed to be necessary, this access must be provided where possible using an established standard procedure[38] and must be restricted in time.	Abschnitt 5.5
The connection can only be initiated from the inside out in order to make non-authorised third party access more difficult.	5.5
A connection may be set up exclusively with an explicit consent of the operator as part of the connection setup process by an administrator (four-eye’s principle).	5.5
It must be possible to monitor the activities conducted during remote maintenance.	5.9
It must be possible to restrict the incoming connection where possible to the system part concerned. (It is advisable here to design the segregation of the logical parts or segments of the system during the planning of the system by the integrator such that the operator can set the access points accordingly).	5.9 and in particular 5.9.2

K. Weak points and update management

Requirements placed on the integrator of machinery and systems	Details i. a. in sections
The integrator of the machine or systems undertakes to immediately pass on information on newly found weak points in his system to the system operator.[38]	7.1 as well as 7.2
The machine or system manufacturer should provide contractual proof of the agreed weak point management with his software suppliers.	7 ff.
The machine and system manufacturer should independently monitor the known channels for publication of security weak points.	7.3
The integrator should supply suitable security updates and patches as soon as security loopholes become For this purpose, it is necessary that the software can be updated by means of updates, upgrades, patches, fixes and hotfixes.	7, in particular 7.2

L. Patch management by the operator

Requirements placed on the integrator of machinery and systems	Details i. a. in sections
Any weak points in system components and the software used which become apparent during the course of the product life cycle must be eliminated by patches.	as above Section 7 ff.
Only in strictly defined and appropriate cases (safety-critical applications and systems) should patches mean that the provider needs to fear disadvantages in support or the loss of support due to a change in the delivered product.	7.2

M. Restriction to the inalterability of the delivered product

Requirements placed on the integrator of machinery and systems	Details i. a. in sections
The extent to which the machine and system manufacturer can satisfy the demand for the facility to update and even replace IT-relevant system components must be shown.	7.2
It must be shown which modifications to the product can be made without this having negative consequences (such as any necessary renewed review in accordance with the Industrial Safety Ordinance (BetrSichV).	7.2

38 see VDMA publisher (without year)

N. Documentation

Requirements placed on the integrator of machinery and systems	Details i. a. in sections
Detailed software documentation is provided and includes the following: • Presentation of the internal software architecture • Description of the core functions • Structure of the interfaces • Information on the framework conditions under which software can be operated (system requirements) • Known problems and restrictions in interoperability[39]	in particular Section 7 ff.
Documentation of internal system features and overarching dataflows[40]	5 and 6.5
The documentation must regularly be adjusted if software is modified and provided to the operator.	

O. Requirements placed on later administration (security in deployment)

Requirements placed on the integrator of machinery and systems	Details i. a. in sections
Documentation and tools of the software integrator are to be provided in order to put the administrators in a position and support them in setting up the software in a best possible manner.	7.2, 7.3
A list of all files and configurations of the basic installation and of all features, upgrades, updates, patches, fixes und hotfixes which can be subsequently installed is supplied.	in particular 4.1.4 and 4.1.5
The software is to have a rollback functionality using which updates made at a given time can be reverted (de-installed/removed).	4.4
The software should contain an integrated version check with the assistance of which the administrator can determine the current version or the current patch level of the software at any time, for example.	

8.4 Requirements placed on suppliers/ integrators of machinery and systems

A number of requirements to be placed on IT security may be derived from the aforementioned procurement conditions, particularly for the suppliers. On the basis of the current level of knowledge of suppliers and their restricted resources, they cannot have immediately binding character or be defined as exclusion criteria because this will be something that the suppliers will not be able to satisfy across the board. Nevertheless, the need of operators for more security for the systems and for more adaptability of the IT components must be taken into consideration for the medium-term migration to Industrie 4.0 processes. Only through clear communication of the need for such functions and properties will be the integrators and the suppliers experience the necessary market pressure to have corresponding functions developed. A few of the requirements are as follows:

- Guarantee the IT security of systems and sub-systems through proven security processes, concepts and responsibilities
- Securely develop systems and software under consideration of the security requirements which are derived from the threat and risk analyses
- Conduct detailed risk analysis for every machine type or every individual system
- Preventatively and actively close any security loopholes found
- Use secure software, also open-source validation and code reviews
- Contractually secure weak points management with suppliers
- Document hardware and software used and pass documentation on to the operator
- Adjust business models in order to guarantee support over the product lifecycle
- Facilitate connection of security systems

8.5 Requirements placed on standardisation

Clear regulations and binding standards must be defined to ensure that the integrator of machinery and systems can meet the requirements derived from the procurement guideline. Work is being conducted on such laws, standards and tools in various organisations and associations.

39 Any combinations of software , operating systems, databases to be connected etc.

40 Essential in particular if this communication is to be securely monitored using Intrusion Prevention Systems (IPS), for example.

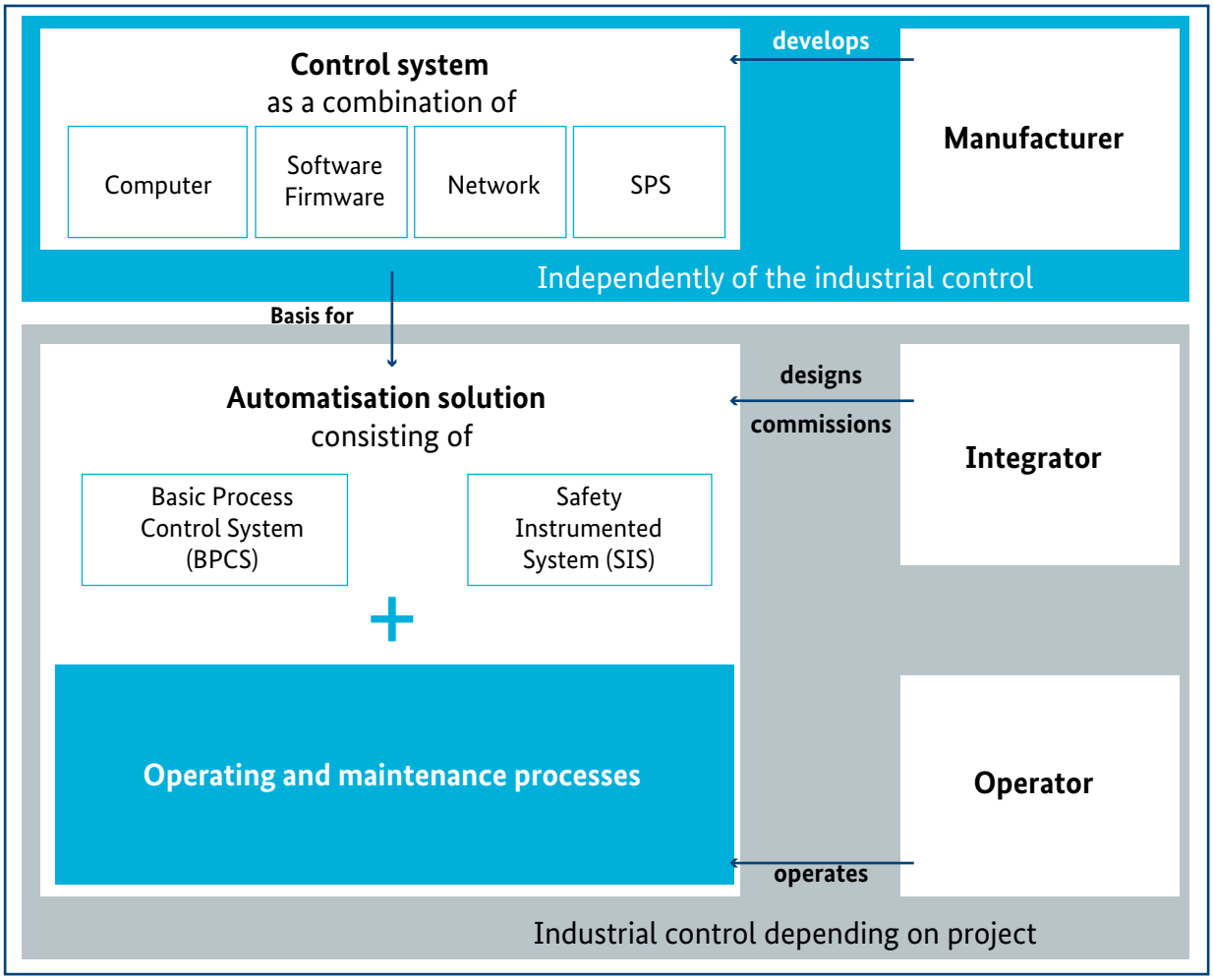
Regulations of this kind must above all else be overarching because the integrator of machinery and systems cannot be solely responsible for the security and the secure operation of machinery and systems. The main participating roles (e.g. manufacturer, integrator, operator) and their different areas of work and responsibilities are currently defined by IEC 62443 and by VDI/VDE 2182 amongst others. Further concretisation is required in this area.

8.6 Relevant roles according to IEC 62443

IIt becomes clear, particularly in the procurement process for machinery and systems, that IT security can only be ensured by the collaboration of the complete supply chain and that all relevant roles must make their contribution here. In accordance with IEC 62443, the roles are manufacturers, integrators and operators of machinery and systems. Figure 10 provides a first overview.[41, 42]

In addition to the view taken by the IEC 62443, these topics are also considered in VDI/VDE 2182 from a slightly different perspective. Here, the interdependence between manufacturer, integrator and operator is considered alongside the internal cycles, as shown in Figure 13. However, the roles themselves cannot always be clearly separated and the assignment of the corresponding responsibilities in the context of Industrie 4.0. is being discussed at different levels. Manufacturers in this connection are understood to be the manufacturers and suppliers of (control) components. The role of the machinery and systems manufacturer is described by the integrator here, whereby there may well be two different roles because the design and commissioning can also be considered separately from each other. The role of the integrator in terms of commissioning and the associated responsibilities are also frequently outsourced to external service providers.

Figure 10: Roles of the IEC 62443



Source: Kobes, P. (2015)

41 See Kobes, P. (2015)

42 See VDE Verlag (2016)

9 Standards, documents and organisations

The reliable implementation of concepts such as Industrie 4.0 and the Internet of Things (IoT) requires rules and structures which must overcome the existing sectoral borders between electrical technology, mechanical engineering and IT. Uniform standards and guidelines – ideally at a global level – facilitate the interoperability of companies in the first place and create a basis of trust through corresponding proof that they are being observed.

Standards, guidelines and manuals are similarly an essential component in the implementation of the recommended procedure, sometimes required by law, to create a suitable IT security level. As an introduction to the subject, the following provides an overview of the large number of standards and guidelines after which relevant documents are selected in line with the target groups.

A complete overview of relevant documents cannot be provided here. However, a few of the most relevant organisations, standards and guidelines and similar documents are to be presented clearly in the following.

9.1 Relevant organisations

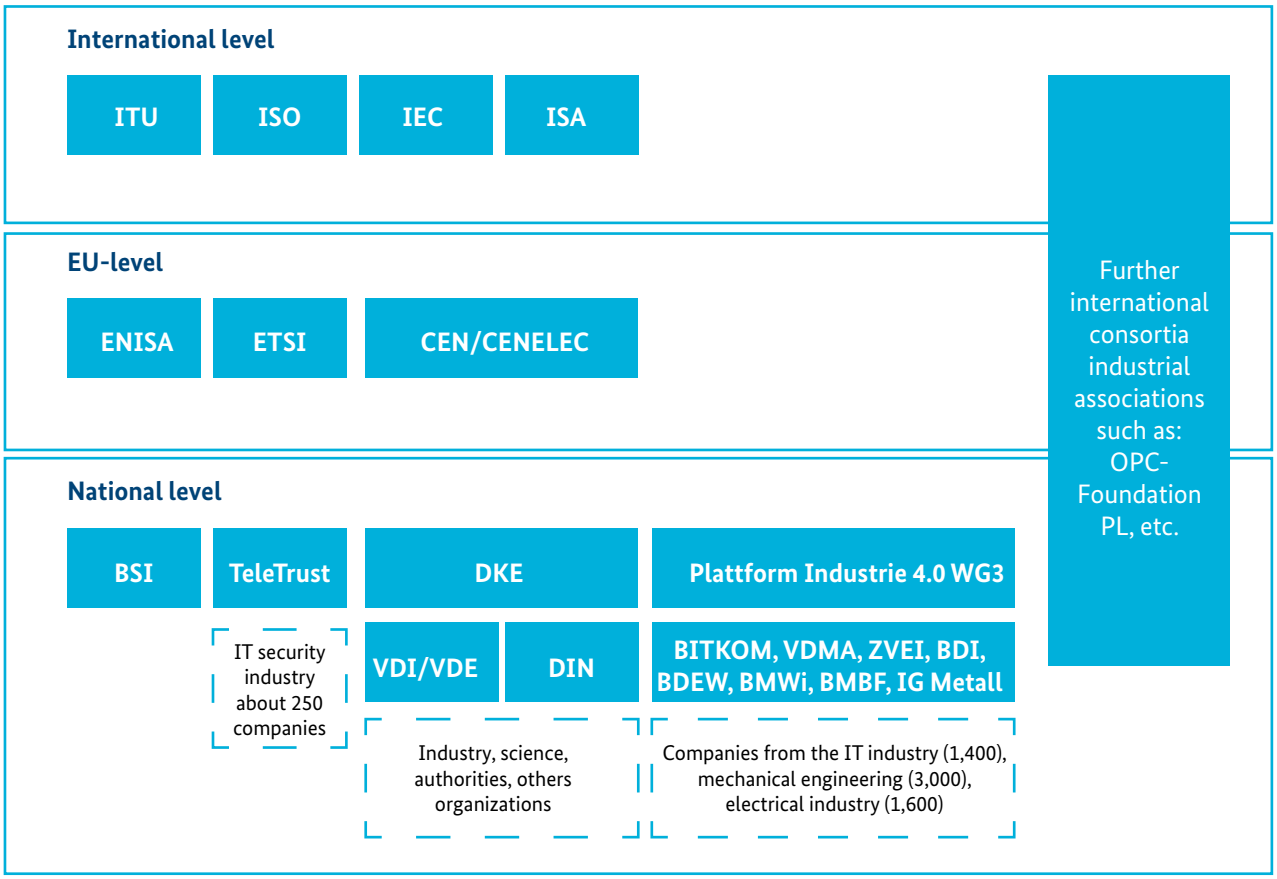
The issuing organisation is a main feature of standards, guidelines and similar documents. The issuing organisation indicates how relevant the document is in terms of its cross-industry reach and geographical spread. Knowing the issuing organisation therefore permits an initial classification of the document. Numerous documents therefore exist for an extensive overview; they are recommended here as further reading and include the following:

- Study of the Federal Ministry for Economic Affairs and Energy “IT Security for Industrie 4.0” [43]
- Graphic overview of the DKE on “Working groups and committees in the area of Industrie 4.0” [44]
- Compass of IT security standards of Bitkom[45]
- “Manual on the state of the art” of the TeleTrusT, in context of the IT Security Act with recommendations on the state of the art[46]

The long version of the final report on the BMWi study named above includes an overview prepared by the Fraunhofer Institute for Embedded Systems and Communication Technology (ESK) on the organisations of relevance in the context of IT security and Industrie 4.0 (see Figure 11).

43 See BMWi (publisher) (2016c)
44 See VDE (publisher) (2016)
45 See bitkom (publisher) (2014)
46 See TeleTrust (publisher) (2014)

Figure 11: Overview of the organisations relevant to IT security and I4.0



ITU – International Telecommunication Union
ISO – International Organization for Standardization
IEC – International Electrotechnical Commission
ISA – International Society of Automation
ENISA – European Union Agency for Network and Information Security
ETSI – European Telecommunications Standards Institute
CEN/CENELEC – European Committee for Standardization / European Committee for Electrotechnical Standardization
BSI – Bundesamt für Sicherheit in der Informationstechnik
TeleTrust – Bundesverband IT-Sicherheit e.V.
Bitkom – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
DKE – Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE
VDI – Verein Deutscher Ingenieure e.V.
VDE – Verband der Elektrotechnik und Elektronik
DIN – Deutsches Institut für Normung
VDMA – Verband Deutscher Maschinen- und Anlagenbau e.V.

Source: according to BMWi (publisher) (2016 c), p.30

9.2 Standards and guidelines

A general distinction can be made between ISO/IEC-, DIN EN and other standards. According to the International Organization for Standardization (ISO), a standard is a document which provides the requirements, specifications, guidelines or features for systematic use. Internationally valid standards are created by international organisations such as the ISO which facilitate progress and support solutions for global challenges.

In addition to the standards, there is also a number of regulations and acts which are to be considered in the context of IT security, such as the Federal Data Protection Act (BDSG) or the new IT Security Act.

9.2.1 ISO/IEC 2700x

The ISO/IEC 27001 standard describes the basic requirements placed on the management system of information security (ISMS) of an organisation. Other standards from the ISO/IEC 2700x series are supplements to the ISO/ IEC 27001. For example, requirements on bodies which audit or certify an ISMS are described in ISO/IEC 27006. A certification of this type of companies or organisations is suitable at a global level to provide evidence of compliance with IT security. The target group of the family of standards is corporate IT. The series of standards is continuously updated and extended.

9.2.2 IEC 62443/ISA 99

The IEC 62443 "Industrial Communication Networks – Network and System Security" is the international series of standards on IT security in industrial automation systems. These standards will have a fundamental character both for the specialised area of automation technology and for that of network control technology and control technology for further critical infrastructures. They address the target groups of manufacturers, integrators and operators. From the point of view of the operator target group, requirements on suppliers are described and the requirements placed on a security management system for Industrial Automation and Control Systems (IACS) defined which is to be seen as a profile from ISO/IEC 2700x. The close connection with ISO/IEC 2700x becomes clear here.

9.2.3 VDI/VDE Richtlinie 2182

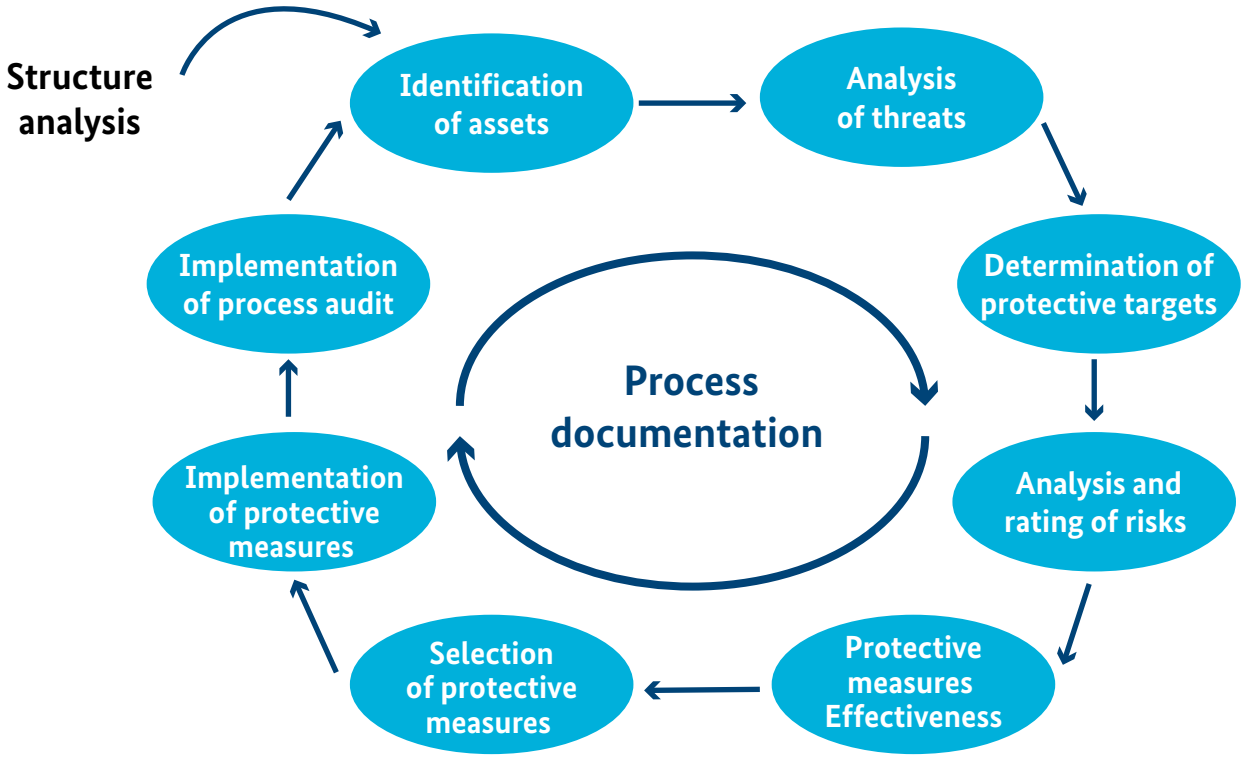
The guideline describes interdependences between manufacturers of automation solutions, mechanical engineers and system integrators as well as the operators of production and process systems. Within the Industrie 4.0 context, these stakeholders are part of a value-added network which is to be assessed from the point of view of IT security.

The guideline follows a risk-based approach which firstly describes the automation solution as the object of consideration. This object of consideration is the focal point in the application of the VDI/ VDE 2182 model. It passes through different life cycle phases (manufacture, integration, operation). It must be considered here that a life cycle phase is not necessarily restricted to an individual organisation. It is generally known, for example, that the manufacturer of the automation solution does not only develop but also manufactures the product. The manufacturer, therefore, also frequently assumes the role of an operator. Within the context of Industrie 4.0 these life cycle phases can be represented by a large number of organisations interconnected in value-added networks.

The method defined on sheet 1 of the Guideline can be applied to existing and developing automation solutions. The approach described therein is based on a process-oriented and cyclical procedure. The model consists of several process steps.

The entire process itself must be worked through at certain times (time- and/or event-controlled) in order to ensure the information security of the object of consideration over its entire product or system lifecycle.

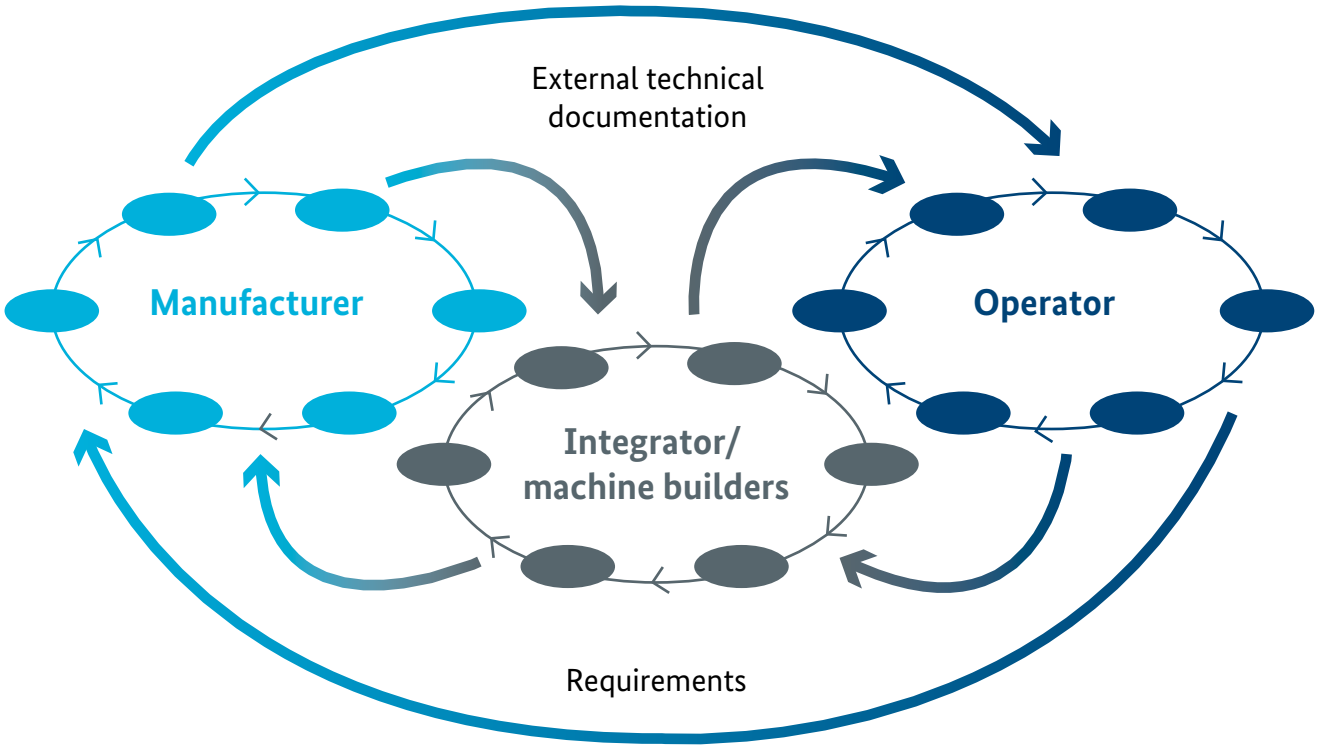
Figure 12: Rating of protective measures effectiveness[47]



Source: according to VDI/VDE 218248

47 See VDI/VDE Guideline 2182-1

Figure 13: Model for interaction between manufacturers, operators, integrators[48]



Source: according to VDI/VDE 218248

In the risk analysis, focus is placed on the object of consideration, the specific or typical use environment of which must initially be defined as part of a structure analysis. Accordingly, the structure analysis provides the foundation for working through the individual process steps. A further foundation is provided by the definition of the events or time at which the process is to be started. It becomes clear here that the process is based on a cyclical, iterative model. A further essential foundation is provided by the definition of the roles, i. e. those persons who are actively involved in the respective process steps and must assume a certain task (responsibility inter alia).

The results and the decision-making path of every process step must be documented. Process documentation is produced at the end to guarantee traceability and ultimately provide the basis for auditing.

The process described supports the user of the method in determining and validating an appropriate and economical security solution for a specific object of consideration.

The guideline is looked after by the VDI/VDE-GMA technical committee 5.22.

9.2.4 BSI IT-Grundschutz (IT basic protection)

The Federal Agency for Digital Security (BSI) provides an extensive library of standards on information security and supplementary practical documents for IT-Grundschutz (IT basic protection). Up to 2005 the BSI publication was entitled “IT-Grundschutz Manual” and was then updated and restructured and thereby “renamed” into BSI standards on information security and IT-Grundschutz catalogues.

IT-Grundschutz catalogues are subdivided into modules, risk catalogues and measure catalogues. The modules comprise components, approaches and IT systems in a layer model and are the link between risk and measure catalogues.

IT-Grundschutz interprets the very general requirements of the ISO standards of the 2700x series and provides users with practical assistance in implementation with many tips, background information and examples. IT-Grundschutz is also compatible with the ISO 2700x series so that certification according to ISO2700x is possible on the basis of IT-Grundschutz. A further advantage of BSI IT-Grundsschutz is the free availability of the information on the Internet. All documents are available in German. Work is currently

48 See VDI/VDE Guideline 2182-1

in progress on extending the requirements in production but these drafts were not available to the authors at the time these guidelines were written.

An overview of the BSI standards on information security is provided in the following:

100-1: Management systems for Information Security (ISMS)

This BSI standard describes the basic requirements placed on an ISMS. Its components and tasks are also described under consideration of the requirements of the ISO 27001 standard inter alia.

100-2: Procedure for IT-Grundschutz

The BSI standard 100-2 describes how the BSI standard 100-1 can be implemented practically (see BSI (publisher) (2008b)).

100-3: Risk analysis on the basis of IT-Grundschutz

This BSI standard describes a simplified procedure for risk analysis. A greater need for protection is to be suitably considered. According to the standard, the risk analysis will always be expedient if components cannot be adequately secured by IT-Grundschutz measures alone (see BSI (publisher) (2008c)).

100-4: Emergency management

The emergency management standard defines a systematic path for the development, examination and further development of emergency management. The underlying concepts are intended to increase the resilience of the own institution and secure the continuity of the core business processes and specialist tasks in the case of crises and emergencies (see BSI (publisher) (2008d)).

9.3 Further guidelines and publications of Plattform Industrie 4.0

As has already been mentioned as part of the role model according to IEC 62443/ ISA 99, the roles and responsibilities of the relevant stakeholders are blurring. The original distinction between lobby associations and standardisation organisations is also becoming increasingly fuzzy. The publications of organisations typically name the relevant target groups so that the document can be addressed to them accordingly. Nevertheless, it is a good idea to read documents which go beyond the own target group. A few guidelines are listed in the following as a simplified overview which have a similar character as this document and which are addressed to different groups.

Guidelines on Industrie 4 .0 Security – Recommended action for SMEs

Target group: Manufacturers or machinery and systems
Author: VDMA, accessec GmbH & Fraunhofer AISEC
Publisher: VDMA
Status: Published[49]

ZVEI Security orientation guideline for manufacturers (provisional working title)

Target group: Manufacturers from the electrical industry
Author: ZVEI and Koramis GmbH
Publisher: ZVEI
Status: In progress

Guidelines on security for mechanical and system engineering. The path through the IEC 62443

Target group: Manufacturers of machinery and systems
Author: Industrial Security working group at VDMA and HiSolutions AG
Publisher: VDMA
Status: Publication planned in November 2016

It should also be pointed out here that in addition to these guidelines, Plattform Industrie 4.0 provides other publications and partner publications on the subject of Industrie 4.0 and IT security. The publications may be accessed in the online library[50] and are available in German and in English in some cases.

49 See VDMA Verlag (no year)

50 www.plattform-i40.de/I40/Navigation/DE/In-der-Praxis/Online-Bibliothek/online-bibliothek.html

10 List of figures

11 Literature and sources

bitkom (Publisher) (2014): „Leitfaden: Kompass der IT-Sicherheitsstandards“
URL: https://www.bitkom.org/Bitkom/Publikationen/Kompass-der-IT-Sicherheitsstandards.html, last access: 19.10.2016

BMWi (Publisher) (2016a): „Technischer Überblick: Sichere unternehmensübergreifende Kommunikation“, Ergebnispapier der Plattform Industrie 4.0, URL: https://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/sichere-unternehmensuebergreifende-kommunikation.pdf?__blob=publicationFile&v=8, last access: 19.10.2016

BMWi (Publisher) (2016b): „Technischer Überblick: Sichere Identitäten“, URL: https://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/sichere-identitaeten.pdf?__blob=publicationFile&v=8, last access: 19.10.2016

BMWi (Publisher) (2016c): „Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie: IT-Sicherheit für die Industrie 4.0“, URL: http://www.bmwi.de/DE/Mediathek/publikationen,did=764200.html, last access: 19.10.2016

BMWi (Publisher) (2016d): „Plattform Industrie 4.0 – Online-Bibliothek“, URL: http://www.plattform-i40.de/I40/Navigation/DE/In-der-Praxis/Online-Bibliothek/online-bibliothek.html, last access: 19.10.2016

BSI (Publisher) (2008a): „BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)“,
URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1001.pdf?__blob=publicationFile, last access: 19.10.2016

BSI (Publisher) (2008b): „BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise“, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.pdf?__blob=publicationFile, last access: 19.10.2016

BSI (Publisher) (2008c): „BSI-Standard 100-3: Risikoanalyse auf Basis von IT-Grundschutz“, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1003.pdf?__blob=publicationFile, last access: 19.10.2016

BSI (Publisher) (2008d): „BSI-Standard 100-4: Notfallmanagement“, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004_pdf.pdf?__blob=publicationFile, last access: 19.10.2016

BSI (Publisher) (2012): „Technical Guideline TR-03111: Elliptic Curve Cryptography“, URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_pdf.pdf;jsessionid=3D1A9885F1F664C54D120C3633467099.2_cid368?__blob=publicationFile&v=1, last access: 19.10.2016

BSI (Publisher) (2015): „BSI – Technische Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen“,
URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=2, last access: 19.10.2016

Bundesnetzagentur (2015): „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)“, Entwurf, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/Algorithmenkatalog_Entwurf.pdf?__blob=publicationFile, last access: 19.10.2016

Kobes, P. (2015): „Defense-in-Depth: Grundlage für eine erfolgreiche Verteidigungsstrategie gegen Cyberangriffe“,
URL: http://www.elektrotechnik.vogel.de/defense-in-depth-grundlage-fuer-eine-erfolgreiche-verteidigungsstrategie-gegen-cyberangriffe-a-473371/, last access: 19.10.2016

Kobes, P. (2016): „Leitfaden Industrial Security, IEC 62443 einfach erklärt“, URL: https://www.vde-verlag.de/buecher/484165/leitfaden-industrial-security.html, last access: 21.09.2016

Microsoft (Publisher) (2016): „Security Development Lifecycle“, URL: https://www.microsoft.com/en-us/SDL, last access: 19.10.2016

NIST (Publisher) (2014): „Cryptographic Toolkit“, URL: http://csrc.nist.gov/groups/ST/toolkit/, last access: 19.10.2016

Siemens AG (Publisher) (2010): „Device Manager für SIMATIC LOGON“, URL: http://www.industry.siemens.com/datapool/industry/industrysolutions/services/de/Device-Manager-SIMATIC-LOGON-de.pdf, last access: 19.10.2016

TeleTrust (Publisher) (2014): „TeleTrusT-Handreichung: Stand der Technik“, URL: https://www.teletrust.de/publikationen/broschueren/stand-der-technik/, last access: 19.10.2016

VDE (Publisher) (2016): „Arbeitsgruppen und Gremien im Bereich Industrie 4.0“, URL: https://www.dke.de/de/themen/industrie-4-0/arbeitsgruppen-und-gremien-im-bereich-industrie-4-0, last access: 19.10.2016

VDI/VDE Richtlinie 2182-1: „Informationssicherheit in der industriellen Automatisierung – Allgemeines Vorgehensmodell“, Weißdruck 2011

VDMA Verlag (o. J.): „Leitfaden Industrie 4.0 Security“, URL: http://leitfaden-i40-security.vdma-verlag.de/, last access: 19.10.2016

ZVEI (Publisher) (2015): „Industrie 4.0: Die Industrie 4.0-Komponente“, URL: https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2015/april/Die_Industrie_4.0-Komponente/Faktenblatt-Die-Industrie-4_0-Komponente.PDF, last access: 19.10.2016

12 List of abbreviations

ABAC – Attribute Based Access Control

API – Application Programming Interface

ASE – Automation Security Engineer

ASLR – Address Space Layout Randomization

ASO – Automation Security Officer

BYOD – Bring Your Own Device

CBAC – Context Based Access Control

CI – Configuration Item

CLM – Certificate Lifecycle Management

CMDB – Configuration Management Database

CSMS – Cyber Security Management System

DAC – Discretionary Access Control

DDoS – Distributed Denial of Service

DEP – Data Execution Prevention

ERP – Enterprise-Resource-Planning

I4.0 – Industrie 4.0

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

ISMS – Managementsystem für Informationssicherheit

ITIL – IT Infrastructure Library

MAC - Mandatory Access Control

M2M – Machine to Machine

MES – Manufacturing Execution System

OCSP – Online Certificate Status Protocol

PKI – Public Key Infrastructure

PSO – Production Security Officer

RBAC – Role-based Access Control

SDL – Security Development Lifecycle

SIEM – Security Information and Event Management

SPS – Speicherprogrammierbare Steuerung

SSO – Single Sign-On

UAC – User Account Control

VPN – Virtuelles Privates Netzwerk

AUTHORS:

Heiko Adamczyk, KORAMIS GmbH | Carsten Angeli, KUKA Roboter GmbH | Konstantin Böttinger, Fraunhofer AISEC | Bartol Filipovic, Fraunhofer AISEC | Wolfgang Fritsche, IABG | Dr. Detlef Houdeau, Infineon Technologies AG | Dr. Martin Hutle, Fraunhofer AISEC | Dr. Lutz Jänicke, Phoenix Contact GmbH & Co. KG | Michael Jochem, Robert Bosch GmbH | Marcel Kisch, IBM Deutschland GmbH | Dr. Wolfgang Klasen, Siemens AG | Dr. Bernd Kosch, Fujitsu Technology Solutions GmbH | Michael Krammel, KORAMIS GmbH | Lukas Linke, ZVEI e.V. | Torsten Nitschke, Phoenix Contact Software GmbH | Sebastian Rohr, accessec GmbH | Michael Sandner, Volkswagen AG | Dr. Michael Schmitt, SAP SE | Martin Schwibach, BASF SE | Nadine Sinner, accessec GmbH | Andreas Teuscher, Sick AG | Thomas Walloschke, Fujitsu Technology Solutions GmbH | Jürgen Zorenc, accessec GmbH

This publication is the result of the working group “Security of networked systems” of Plattform Industrie 4.0.

www.plattform-i40.de