# Industrie 4.0 Security Guidelines

## Recommendations for actions

in cooperation with

accessec Fraunhofer AISEC protect-ing.de VDMA

This document was originally published in German. Since translation might be misleading, consideration of the original German Edition is recommended:

**"Leitfaden Industrie 4.0 Security"**
ISBN 978-3-8163-0689-4

www.i40-security.de

# Editorial

Wolfgang Bokämper

Dear Members and Readers

Our world is becoming more connected and digitalized all the time – and production is no exception. Apart from the technical implementation itself, this challenge – Industrie 4.0 – requires secure embedding.

Industrie 4.0 means that data, and thus information, is available anytime, anywhere. This kind of availability brings numerous opportunities, making information and its connection a significant factor in production. In the course of processes like this, dividing boundaries between companies may disappear – or will have to – since product development chains also cross company borders.

If one thinks about this, it becomes clear that the task of “security” is leaving the office behind and is making new demands. The term “availability” gains another dimension. If an email program were to break down for half a day, it would be inconvenient but not life-threatening. But a shutdown like this in production would be a disaster for all supply chains. As such, security is an important basis or “safety net” for Industrie 4.0.

I can already see a clear trend towards more IT on the shop floor today. Even the term “artificial intelligence” has made its way into production halls. Logistics, mobility... everything is connected and needs information accordingly. Viewing processes in a comprehensive way is indispensable. It is obvious that this task can be neither addressed nor solved in isolation. Everything is a part of the chain: from component manufacturing to integration to operating the plants.

Often regarded primarily from a technical standpoint, this chain of course also includes the people – developers, automation engineers, operators, users and so on. Management has the important task of integrating security awareness as part of employees' everyday routines.

Let’s take on Industrie 4.0 in a “secure” way, and success will prove us right.

W. Bokämper

**Wolfgang Bokämper**
Speaker of VDMA Task Forceon Industrial Security,
Division Manager Procurement, Organization & Quality Assurance,
Kolbus GmbH & Co. KG, Rahden, Germany

# Inhaltsverzeichnis

# Management summary

Machine manufacturers worldwide face great challenges in digitizing their industrial products and services. In particular, challenges regarding safe and secure implementations of Industrial IoT (IIoT) and Industrie 4.0 solutions are of utmost importance. Reliable and constantly secure operation of machines and systems connected worldwide is a fundamental challenge that must be addressed if IIoT/ Industrie 4.0 is to be implemented successfully. For this purpose, VDMA provides its members with guidelines on “Industrie 4.0 Security”.

Security itself is about safeguarding IT systems. In order to differentiate from IT security, we refer to safeguarding information technology in industrial plants, machines and systems as “Industrial Security”. If these systems are now connected via integration of Industrie 4.0, both the manufacturer and operator need to consider how to ensure the security of this connectivity across companies at all times. That is the issue at the heart of Industrie 4.0 security. This industry transformation will only be possible if the latest production and process systems are secured reliably.

The goal of Industrie 4.0 Security is to ensure the security of future machines and plants throughout their lifecycles, rather than the current situation in which security functions have to be bolted on later. In the future, security must be an integral aspect for mechanical and plant engineering companies right from the beginning of the entire production development process (“security by design”). The integration of security means that it must ultimately be seen as a functional component of future plants and systems, establishing “security as a function”.

These guidelines serve as an introduction for mechanical and plant engineering companies and offer guidance as to which topics, technologies and processes they need to consider in order to enhance the security of complex systems. The focus is on the perspective of manufacturers and integrators. The document also includes requirements for properties or functions that suppliers will have to provide in the future. The sector-specific focus on the viewpoint of mechanical and plant engineering enables the range of requirements to be covered appropriately and offers the necessary depth to demonstrate specific courses of action.

In order to meet the goals for the provision of sustainably and permanently secure systems for Industrie 4.0, the guidelines describe security considerations as a goal of equal rank right from the development and design process. In addition, the requirements of Industrie 4.0 security include examining hazards and risks prior to commissioning, managing cyber-risks during operation and maintaining the security function throughout the entire product lifecycle of connected machines and systems. The risk assessment prepares manufacturers and integrators for threats to be anticipated both now and in the future and allows them to guarantee the operator a minimum level of security upon commissioning. A process for accepting, assessing and reacting to relevant security threats must be established during the product's lifecycle.

The guidelines provide help with this in the form of VDMA's Industrie 4.0 toolbox, supported by an online self-assessment.

# Using the guidelines

These guidelines provide the opportunity to single out specific aspects and to review them on your own. However, it is a good idea to start off with the organizational and analytical topics, such as the lifecycle of a plant, before addressing the more technical topics, such as user accounts, passwords and network segmentation. Each section provides information on helpful courses of action; these should be assessed as part of continuous security management in order to set the right priorities.  This is the best way to effect sustained changes to the product development process and minimize recurring costs for the provision of security functions. Integrating all parties involved and committing to both development and design in equal measure are absolutely essential here. For simplification's sake, these terms shall be used interchangeably in the following: “component” will be used as a synonym for “system part” and thus comprises all components and combinations thereof used to construct a plant.

The fold-out page at the end shows the functional classes of the “VDMA Industrie 4.0 Toolbox – Products”. A scale of Industrie 4.0 functionality from one to five is used within the classes (A to F in this case). The entries in the left-hand column refer to a classic production machine, while the right-hand column corresponds to the full vision of Industrie 4.0.

### Recommendations for action and minimum requirements

Fundamental recommendations for action and minimum requirements for protective measures that allow a certain basic level of protection for the machine are listed in this document. Each recommendation is also assigned a corresponding product function so that relevant protection measures only need to be identified for the respective machine during development. This compromise represents a large increase in security for companies heading towards Industrie 4.0.

Product functions are also assigned to the recommendations for action, in order to indicate the point at which a recommendation for action becomes a minimum requirement on the Industrie 4.0 scale from one to five – in other words, from which functionality a protective measure has to be put in place. The “VDMA Industrie 4.0 Toolbox – Products” is used as a scale for this. For example, the following graphic shows that the measure is a minimum requirement as soon as a product has at least a fieldbus interface or data storage for information exchange (Figure 1).

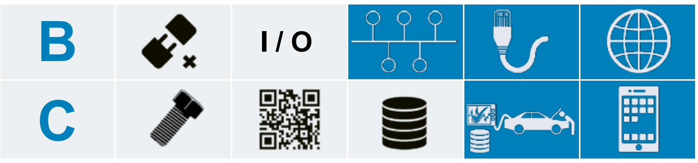


Figure 1: Example of a recommendation for action

Where there are multiple labels, they are to be regarded as “or” requirements.

An online questionnaire at

**www.i40-security.de**

makes it easier for readers to begin determining where they stand. Answering the questionnaire (anonymously) enables quick self-assessment and refers to specific sections of the guidelines that offer fitting recommendations for action to improve the situation even without a risk analysis.

Some recommendations for action are a minimum requirement, and are labeled as such with the following graphic (Figure 2).

**! MINIMUM REQUIREMENT !**

Figure 2: Indication of a minimum requirement

Furthermore, we label the section of the product lifecycle in which the recommendation for action (or respective minimum requirement) should be implemented. We differentiate between the development phase, the integration phase, the operating time with manufacturer guarantee and the operating time without guarantee.

The classification with regard to the product lifecycle is shown by the following symbols (Figure 3).

The development phase and the operating times with and without warranty are relevant in this example.

### Table: Overview of the recommendations for action

The table on pages 38 to 41 gives a compact overview of the recommendations for action. Additionally, the recommendations for action are assigned to the following areas:

**The four phases of the product lifecycle:**

- Development
- Integration
- Operation within warranty
- Remaining lifetime operation

**The levels of application derived from the Industrie 4.0 Toolbox:**

- A: Integration of sensors/actuators
- B: Communication
- C: Functionalities for data storage and information exchange
- D: Monitoring

**The groups responsible for implementation:**

- Manufacturer
- Integrator
- Operator

A dot in the product lifecycle or responsibility for implementation field indicates that the recommendation for action applies for this phase or person responsible.

The numbers 1 to 5 as shown in the application levels specify the development level from which a recommendation for action becomes a minimum requirement.

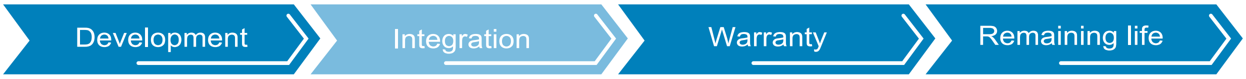


Figure 3: Example of classification in the product lifecycle

# 1. Risk analysis

## Gain an overview

**The security evaluation starts with a risk analysis, which should be established as an integral part of the development process. This means that security aspects can be incorporated into the concept and the design of the machine right from the initial requirements analysis at the start of development.**

Although integrating a risk analysis into the design and development process often involves unaccustomed extra effort to begin with, this can be reduced to a manageable level through a structured and repeatable process. Adapting methods already established at the plant (such as FMEA – Failure Mode and Effects Analysis) for risk observation has proven useful. Above all, the early additional effort pays for itself over the course of development, since security functions can be considered integral parts of the machine and do not need to be added later at great expense.

All subsequent steps in the risk analysis should be taken into account during the entire development process and carried out regularly during operation with and without manufacturer guarantee.

An efficient process can be reduced to the following points (see also the VDI/VDE 2182 directive[1]).

### 1.1. Identifying assets

At first, a consensus must be reached as to which components within the machine are valuable and in need of protection. This might include hardware and software components, for example, but also data and programs of high value as intellectual property. The recommended first step is to become aware of the material and intangible values, which is then reflected in the identification and listing of the respective components.

! MINIMUM REQUIREMENT !

Development › Integration › Warranty › Remaining life

### 1.2. Determining protection goals

Now protection goals can be created for the assets. If a specific component within the machine was assigned a high value (during the first step), a protection goal should be created for this component. For a dataset within the machine that has been rated as critical and on which the functions of other connected machines depend, the protection goal could be as follows: “Ensure availability of the data during remote access to machine”.

! MINIMUM REQUIREMENT !

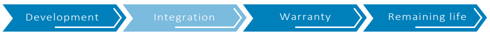
Development › Integration › Warranty › Remaining life

[1] VDI/VDE 2182, IT security for industrial automation – General model, Part 1. (2007).

### 1.3. Identifying threats

Once the machine components in need of protection have been identified, the next step is to consider the associated threats. A threat analysis provides insights on the practical threats to be expected during machine operation and what to prepare for in terms of the respective damage. The usual summaries and lists of current threats, such as the compilation from the German Federal Office for Information Security (BSI)[2], can help with this.

! MINIMUM REQUIREMENT !

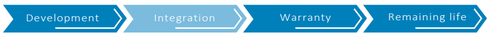


### 1.4. Risk assessment

Based on the threat analysis, the risks assigned to threats can be evaluated. The risk of a listed threat is total damage weighted by the probability of occurrence.

The assessment is carried out based on an attack model to be created in advance, which specifies the assumed capabilities of a potential attacker.

! MINIMUM REQUIREMENT !



Completely determining all risks and their prioritization directly leads to the selection of suitable protective measures and thus forms the basis for optimal safeguarding of the machine or plant. On the other hand, a comprehensive risk analysis can be very extensive and thus may not be feasible for a medium-sized company.

This is why integrating a risk analysis approach into the development process is recommended, at least to the extent that assets are recognized, the associated protection goals formulated and the responsible parties in each case are aware of the common threats during planning and development of the machine.

In this regard, these guidelines are a compromise between the status quo in which security considerations are often non-existent and the ideal situation in which all protective measures are determined based on a detailed risk analysis.

[2] BSI: Industrial Control System Security – Top 10 Threats and Countermeasures

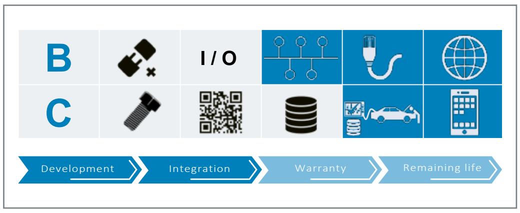
# 2. Network segmentation

## Divide and conquer!

**The plant should be divided into zones based on the individual system parts' security requirements. The connected machines and components within a zone are characterized by similar security requirements. Technical measures should be used to separate the individual segments.**

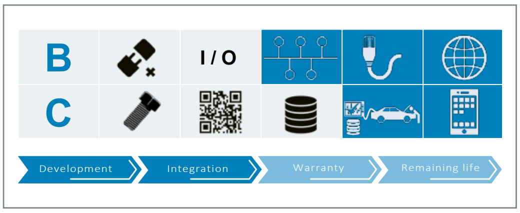
### 2.1. Definition of risk-based security requirements assigned to plants and components

Security requirements should be determined based on common methods of risk assessment. As described in Section 1, the assets should first be identified. Once the protection goals have been determined, a threat analysis is carried out. A risk analysis then provides information on the security requirements of the plants and components. Assigning the security requirements determined in this manner allows the definition of zones, i.e. network segments with components with comparable requirements.



### 2.2. Zoning of services

The various network areas of production (e.g. ERP, MES or SCADA networks) are particularly characterized by the services provided. These services within the production network should also be considered in particular during zoning. The idea behind this is to ensure that network segments directly connected to the machine only contain services with comparable security requirements. Services might include software modules for processing or providing machine data, for example, as well as configuration modules that compile machine functions according to a configuration file. In zoning, it is important to ensure that the failure of one zone affects as few other zones as possible.



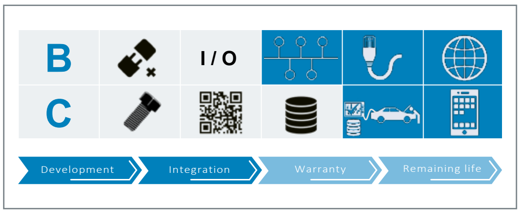
### 2.3. Using isolation measures

If security zones are assigned to the machine's hardware and software components, they should be sufficiently separated from one another through technical measures. This is intended to make it more difficult for the compromising of one section of the machine to spread to the entire system. Potential technical measures to separate the identified segments include firewalls or data diodes. The key result of this for the machine is that, depending on the need for protection, it has to provide filter functions not only for incoming and outgoing communication but also for communication within the machine itself.

Detection of malware or protocol anomalies based on network communication between the defined network segments is recommended. These kinds of protective technologies are often used directly in firewalls.

For network segments in particular danger, data diodes should ensure that information only flows in the pre-defined direction. Preference should be given to solutions in which isolation is achieved through hardware separation. In order to implement and adjust data diodes in the best way possible, all data that flows into and out of a machine should be identified.

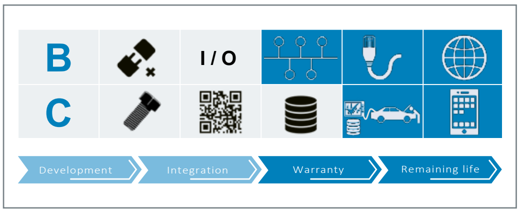
Furthermore, VPN solutions allow networks in separate locations to be compiled into one segment, so that similar or identical plants can be managed together despite the distance between them.



### 2.4. Periodic checking of isolation measures for effectiveness and patchability of filter components

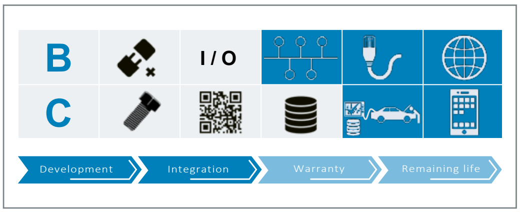
It should be possible to check the effectiveness of the technical isolation measures regularly. In the case of a firewall or other filter technologies, it may also be necessary to check the filtering rules regularly. The plant construction engineers should ensure the update capability so that this task can be carried out by the operator himself or be offered as a service to the operator. The time between the checks largely depends on the respective machine. While machines with low connectivity can be securely configured even with relatively static filtering rules, the filtering rules for machines with high function variability and corresponding communication should be checked and adapted more frequently. Product changeovers and conversion/relocation can also change a plant's need for protection, necessitating further adjustments to the network and IP configuration.

Where weak points have been recognized in the filter components, it should be ensured that the manufacturer is able to patch the affected modules quickly (see Section 9).



### 2.5. DNS and other services per zone

Due to the sharp rise expected in components capable of communication within the plant, it can be assumed that the central DNS server will be increasingly overloaded by all the requests from the plant. This is why network segmentation should be mapped to the DNS infrastructure as far as possible. The often very complex networks and large number of network segments make it a good idea to assign multiple segments with similar protection needs to one DNS server. Since the DNS configuration is to be carried out by both the integrator and the operator, the machines and plants should ensure the corresponding functionality for flexible configuration.



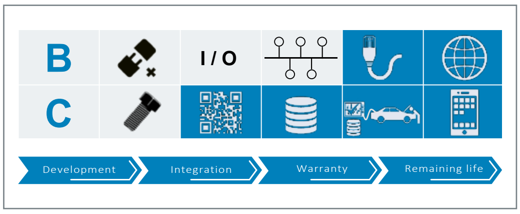
# 3. User accounts, credentials, authentication and authorization

## Not everyone is allowed to do everything …

**The production system should ensure the secure management of user accounts and assigned access data (credentials, e.g. passwords, tokens, SSH keys and biometric authentication data).**

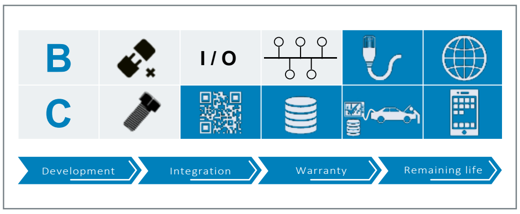
### 3.1. Individual user accounts

It should be possible to set up individual user accounts for each entity. “Entities” refers both to the people interacting with the machine and to other machines and systems that access the services provided, both remotely and locally. This is the only way to ensure that all access to the machine can be matched to a player (see Section 7), which helps in recognizing attacks and investigating IT security incidents. It is important to remember that the operator should be given the option of documenting all user accounts for machines and assigning them to a responsible human party who knows the origin and mode of action of the technical account. Individual user accounts also provide a basis for distributing rights to individuals and roles. Particular attention must be paid here to the fact that there should be no accounts for groups of players: User accounts should be created individually for every plant user and not based on assigned roles.



### 3.2. Account management

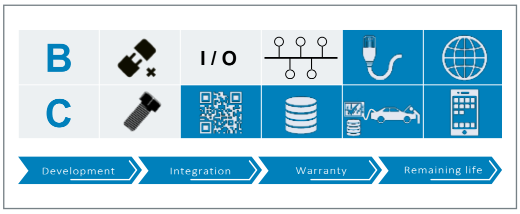
The number of players can fluctuate widely depending on the environment in which the machine is used. The best case is where the machine is operated for long periods of time by the same group of players. The worst case is where the players change very frequently, or even operate the machine for just a few shifts. The machine should ensure efficient handling in managing the individual user accounts, especially with regard to adding, activating, modifying, deactivating and removing accounts. This can often be done by managing the user accounts centrally. As such, it is recommended that a machine supports integration into existing identity management systems or inclusion of the user accounts in directory services



### 3.3. Distribution and management of credentials

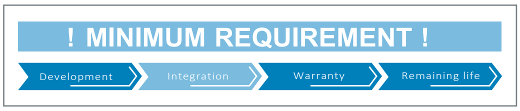
Each individual user account is linked to access data; the respective player should be familiar with this data for authentication and authorization. The management of these credentials should be designed to allow secure and efficient distribution. In practical terms, this means that, although the process for resetting the credentials in case of loss corresponds to the respective security requirement, it needs to be designed flexibly so that machine operation is always ensured. This is intended to prevent downtimes due to complex resetting arrangements. When passwords are used, it is important to ensure that default passwords can also be changed during a reset. The credentials should be created in line with the latest standards and recommendations (see Section 14).

Security modules protected from physical attacks (such as TPMs or SmartCards) are recommended for storing and saving credentials. If these are not available, it must at the very least be ensured that credentials are never saved as plain text, only their salted hashes (see also BSI ICS Compendium for manufacturers and integrators[3]).



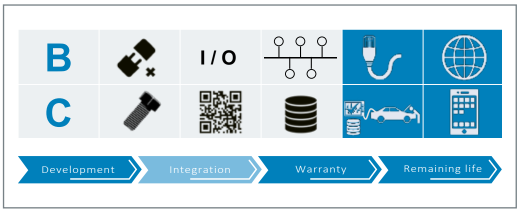
### 3.4. Authenticating human users, software processes and components

All human users and software processes and components should undergo authentication based on the defined authentication data every time they access the machine. Once the machine has successfully authenticated the player, access should be limited to that session.



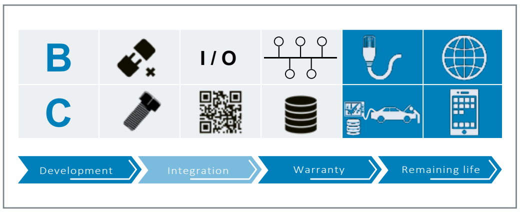
### 3.5. Public-Key authentication

Authentication should involve as few public key encryption processes as possible. Secure and efficient key management and a secure choice of cryptographic material based on the options of the embedded systems (see Section 14) are important here, and integrating the machine into existing public key infrastructures is especially recommended in this case[4]. It is important to remember that a PKI (Public Key Infrastructure) usually has no functions for certificate lifecycle management, which should be provided by the operator in order to avoid system downtimes due to expired certificates.



### 3.6. Creating zones and access concepts with corresponding authentication

Players should be subject to authentication not only on individual components, but also when crossing zone boundaries as defined in Section 2. If a player wants to undergo authentication on a component that is not within his or her zone, authentication should take place at each zone transition on the way to the target component. Additionally, authentication should be conducted for every access via every interface of the machine. In terms of usability, using established processes for automation (single sign-on by transmitting tokens, such as SAML, Kerberos or OAuth 2.0) is both useful and efficient.

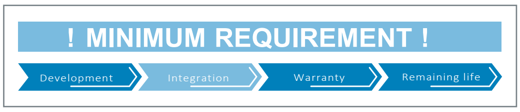


[3] https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS/empfehlungen_node.html

[4] Both the Microsoft Certificate Services of a Windows server and Enterprise Java Bean CA (EJBC) offer cost-effective options for issuing certificates

### 3.7. The machine should ensure an authorization check of the players/services after every authentication

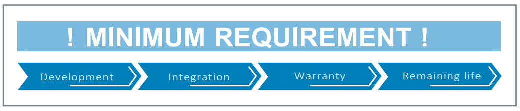
Once a player has been successfully authenticated by the machine, the rights assigned to his or her individual account should be checked immediately. If the rights assigned to the player do not correspond to those required for access, access should be denied and an appropriate entry generated for the event log. While rights are distributed for the player by account management, the access rights assigned to the components and services should be pre-defined and documented by the integrator. It should be possible to adjust the access rights to components and services even after the machine has been commissioned, as the environmental requirements change all the time. In order to simplify rights management for the operators and to relieve the components, it can be useful to make these centrally managed (e.g. using XACML).



### 3.8. Strong authentication to external interfaces

All access to the plant's external interfaces should be safeguarded through strong authentication. Where cryptographic authentication mechanisms are used, the parameters (e.g. key lengths) should be selected according to the latest standards. For instance, various VPN solutions, IPSec and TLS for remote access already offer strong authentication, given a secure configuration.

It should be noted here that factory-state machine components are often supplied with initial default accounts (e.g. administrator with a default password). Strong authentication also and particularly means that this kind of default account should be adjusted to the actual accounts and the intended identities when the machine is commissioned. Hard-coded and thus unchangeable credentials are not only insecure but also require an expensive hardware replacement if the access data is compromised.



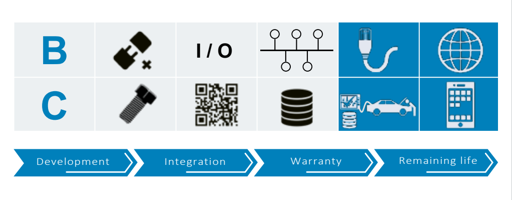
# 4. Using secure protocols

## Eavesdropping and altering forbidden

**For attackers without direct access to the machine, the initial point of attack is often the communication with external components. State-of-the-art secure protocols should always be used to ensure the confidentiality, integrity and authenticity of the data sent. Protocols that have already been standardized should be used wherever possible.**

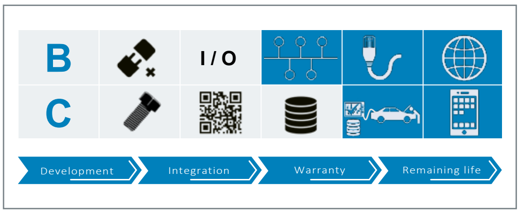
### 4.1. Confidentiality of communication with IP-based protocols

Established safeguarding measures can ensure the confidentiality and integrity of transmitted data for IP-based protocols for communication between machines in different locations. The use of TLS 1.3 and protocols based on it (e.g. HTTPS) is particularly recommended for this. If the need for downward compatibility with old systems makes encryption impossible, communication should be tunneled through a secure protocol. This recommendation is given under the assumption that time-sensitive applications do not communicate via IP-based protocols and that the latency added by encrypting the application data is negligible.



### 4.2. Integrity of communication

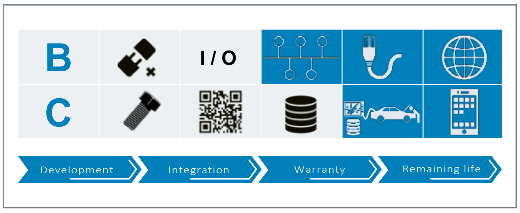
The integrity of the communication data should be ensured both within and outside the machine. The application data transmitted needs to be accurate for the machine to function correctly. As a result, undetected manipulation of application data during transmission can have serious consequences for the machine as a whole. Open standards and common implementations based on state-of-the-art technology, such as TLS 1.3, are also useful here for practical implementation.



### 4.3. Type, strength and quality of encryption algorithms

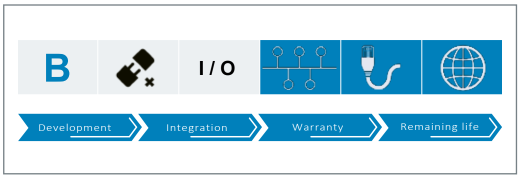
Given the large number of cryptographic algorithms and the even greater selection of possible implementations, the use of standardized encryption processes approved by public bodies is highly recommended. The processes recommended by public bodies (see Section 14) include specifications for selecting suitable parameters (e.g. key lengths). Due to the ever-changing threat situation, these recommendations from public bodies are subject to regular revision.

When developing the machine, it is important to ensure that appropriate adjustments can be made to existing machines and plants. In-house developments not subject to cryptanalysis by experts are not advised under any circumstances.



### 4.4. Special consideration of fieldbus

At the fieldbus level, the authenticity and integrity of communication should be ensured as a minimum. Given the real-time requirements, a decision regarding whether it is necessary or even possible to encrypt the data at fieldbus level should be taken based on what the plant is used for.



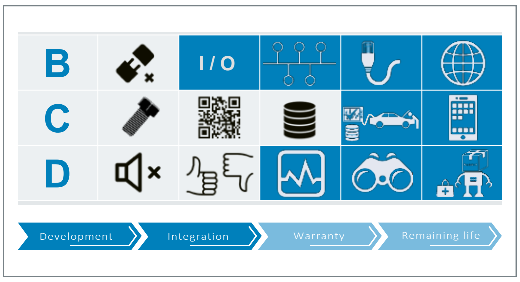
# 5. Safeguarding wireless technologies

## On bridging and air gaps …

**All wireless technologies supported by the machine should be safeguarded in line with the latest standards.**

### 5.1. Secure configuration

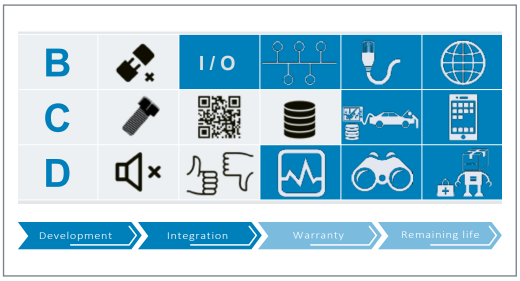
In addition to functional (safety) requirements, the security requirements of the wireless technology being used must be fulfilled. The first step is the secure configuration of the wireless technologies used – setting the smallest possible range (by adjusting the signal strength or shielding) and the highest possible interference resistance. Where the downward compatibility needs mean that the components cannot be securely configured, the insecure communication channels should be tunneled and safeguarded through secure protocols.



### 5.2. Wireless access management

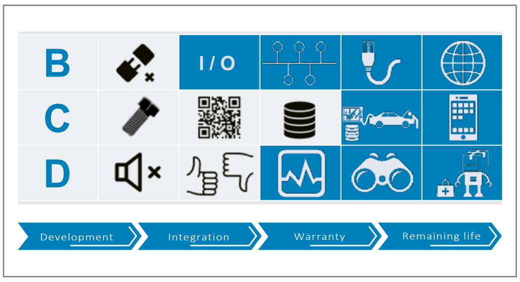
When accessed via wireless technologies, the plant should conduct strong authentication (see Sections 3 and 6) and log all interactions in the session. Activating access restriction after the initial setup is recommended, as long as this does not significantly limit the effective operation of the machine. The access restriction can be configured based on need; technical implementation is possible by MAC filtering.

The same applies to relay stations, which can significantly expand the physical signal range. In environments with a particular need for protection, the use of 802.1x should be considered and made possible.



### 5.3. Time-dependency of security of cryptographic functions

Since wireless networks are very exposed and the machine is used for long periods, security configurations should be checked regularly. This especially includes the cryptographic functions of the wireless network. If the cipher suites, parameters or implementations used are affected by current attacks, they should be replaced with secure versions immediately. An overview of currently secure protocols and cryptographic functions can be found in the relevant standards and recommendations from the BSI and NIST (see Section 14). If the components used are not compatible with stronger algorithms due to their limited computing capability, rotating the key material quickly is an alternative.



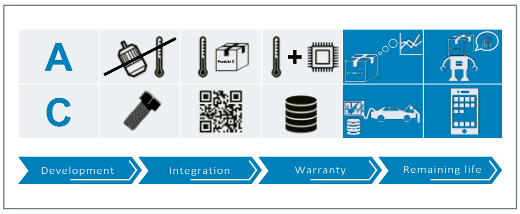
# 6. Secure remote service

## The right path through uncertain terrain

**The plant manufacturer should ensure that the systems for secure remote service and maintenance conform to the identified need for protection.**

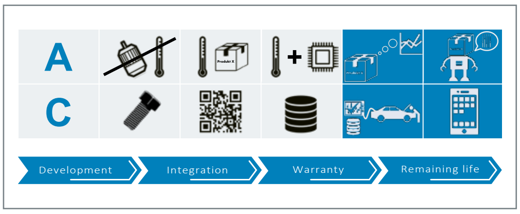
### 6.1. Controls on setting up and ending a remote access session

Regulations on opening and ending a remote access session form the basis for establishing a secure remote service process, and should define when and under what conditions a session may start. Before every remote service session, it is important to check whether the player has the necessary rights and whether the machine's current workload allows for a maintenance interval. The session should automatically be blocked after a specified period if the user has not performed any actions in this period. A blocked session can only be resumed following repeated identification, authentication and authorization. Both the machine and the remote service user should be able to initiate the end of the remote session. The machine may need to end the session if the user calls up unauthorized functions or attempts to adjust settings. All data on a session (including the time, duration and executed actions) should be logged. In addition to the measures named, remote access can be limited through further filtering measures, e.g. limiting the accessible IP address range.



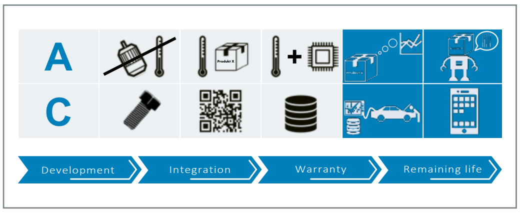
### 6.2. Safeguarding through technical and organizational measures

When and under what conditions remote service can take place should be specified at an organizational level. For example, remote service can be ruled out while the machine is carrying out critical functions for other, dependent machines. Compliance with these specifications should be technically safeguarded, such as by automatically checking a specified policy prior to every remote service access.



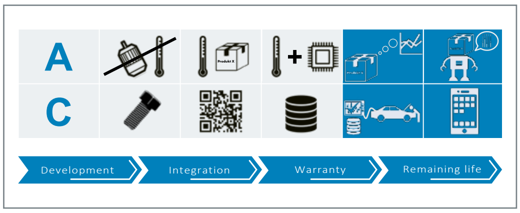
### 6.3. Encrypting the connections

Remote service should be carried out via a cryptographically secured connection. This is the only way to ensure the authenticity of the player and the confidentiality of the transmitted data (see in particular Section 4).



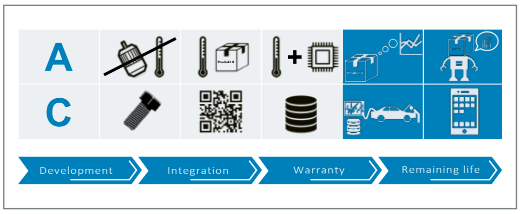
### 6.4. Establishing access processes

The actions a player is permitted to take should be clearly defined for every access. Any deviation from these access processes should cause the session to end. If the connection is ended repeatedly within a pre-defined time period (e.g. due to incorrect login data), further access should be forbidden and only be permitted again when the administrator with corresponding rights has reactivated it.



### 6.5. Securing connections to other networks

If a player wants to connect to further components from an existing connection to a machine component, all the processes mentioned for setting up and ending a remote access session and establishing access processes should be conducted for every further connection of this type. In particular, re-authorization should be carried out if the target component is in a different network segment or zone; for more on this, see Section 3.6. It can be a good idea to give the operator the additional option of a remote service platform based on standard services, since operating several technologies at the same time usually involves a great deal of effort for the operator.



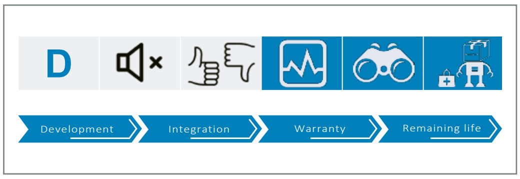
# 7. Monitoring and recognizing attacks

## Trust is good…

**It is unrealistic to assume that a machine is completely secure against attacks, even when the latest security technology is used, so functions for recognizing attacks and other security-related incidents should be available. All logged data should be saved centrally whenever possible in order to make subsequent evaluation easier.**

### 7.1. Monitoring all access to machine components

First, all access to machine components should be logged and saved for further processing. All access from untrustworthy networks should be logged in particular. This should even include access by components to services within the machine. At least the identity of the players/components involved and the time, duration and type of access should be kept for subsequent evaluation. The monitoring system should be separate from the productive system. If the operator is already using an SIEM (security information and event monitoring) system, the possibility of connecting to the plant should be examined.

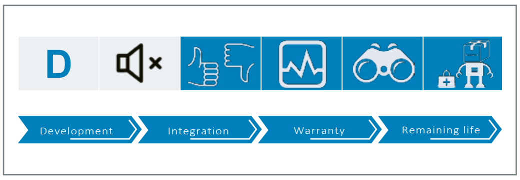


### 7.2. Integrating monitoring functions in the control desk

The functions for monitoring access and other security-related incidents should be directly integrated into the machine's control station. This means that control stations and other systems directly superordinate to the machine should support the option of recording, just as the machine itself does. This allows direct analysis when a malfunction is detected. Security-related incidents include incorrect password entry, exhaustion of resources, attempts at unauthorized access and changes to security-related configuration files (cf. the IT-Grundschutz (baseline security) catalogs from the BSI[5]) .

The control station thus becomes a central component for logging and processing security-related data, which is why the additional communication load on such a component should be taken into consideration during the design and development of the machine, since complex machines spread across a wide area can produce a considerable data throughput.

Furthermore, it is important to ensure that none of the incidents recorded contain sensitive data, e.g. key material (see also the BSI ICS Compendium for manufacturers and integrators[6]).



### 7.3. Virus scanners

The computers directly connected to the machine are often the gateway for malware, so using a virus scanner on these components is recommended. Standard virus scanners recognize attacks using a pre-defined malware signature. These types of rule-based methods for detecting attacks have the advantage of identifying familiar attack patterns with relative reliability.

[5] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/kataloge.html

[6] https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS/empfehlungen_node.html

But the rate is unsatisfactory when it comes to detecting new types of malware that do not yet generate a signature. To ensure a rudimentary level of security against standard malware, the signatures should be regularly updated. To stop an excessive scan load affecting the performance of the computers, almost all manufacturers offer the option of defining adaptive scans, which exclude libraries known to be free of malware from the scan based on their signature.

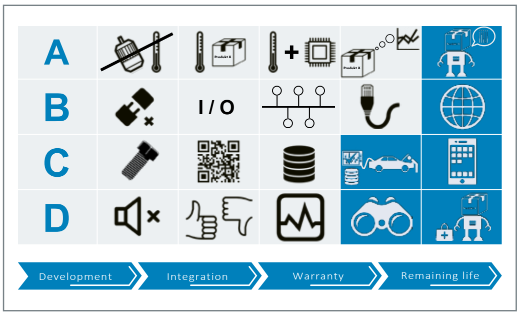
**! MINIMUM REQUIREMENT !**

Development › Integration › Warranty › Remaining life

### 7.4. Network IDS and anomaly detection in complex machines

In order to detect new attack patterns that have not been seen before, additional measures for detecting anomalies should be integrated. This approach assumes that the machine is behaving normally and recognizes any deviation as an anomaly. While this kind of method often generates false positives in complex networks (e.g. in the office network), it is well suited to machine networks, whose basic behavior is often significantly more uniform and allows for easier characterization. Normal machine behavior can be defined based on diverse properties, such as patterns in the network communication, user behavior, the activity of the machine modules, sensor data and system log files.

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) should be implemented for network monitoring of complex machines, or their use enabled by the operator. Exposed components in particular should be equipped with the corresponding functionality so that undesired behavior can be detected based on heuristics. It should be further noted that the IDS/IPS solutions currently available do not allow the protocols used in the plant network to be detected and processed adequately, if at all. There is an urgent need for cooperation here, so that malicious packages can be identified automatically at the protocol level.



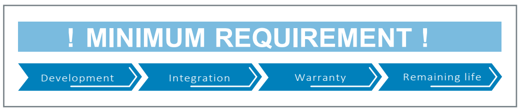
# 8. Recovery plan

## Plan B

**Both the plant manufacturer and the integrator should define a recovery plan that resets the plant to a trustworthy state in case of a malfunction or an attack.**

### 8.1. Creating backup systems

Backup systems are storage systems that allow all data on the machine to be secured. Backup systems should be fully integrated into the machine's development process, and multiple backups are recommended to ensure a suitable level of data availability and reliability. If central backup servers are used, the machine should have functions for secure data exchange with these servers.

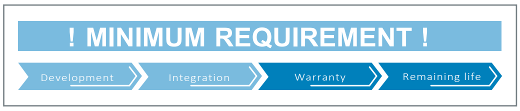


! MINIMUM REQUIREMENT !

Development | Integration | Warranty | Remaining life

### 8.2. Creating regular backups

All data required for operating the machine should be saved to backup systems at regular intervals. The time intervals and encryption requirements for this should be specified by the integrator or the operator based on the threat situation and the need for protection.

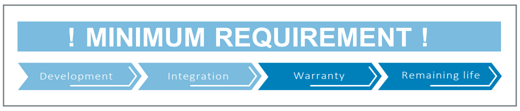


! MINIMUM REQUIREMENT !

Development | Integration | Warranty | Remaining life

### 8.3. Checking backups for recoverability

All backups should be checked for recoverability regularly. Redundancy in the backup systems should guarantee that, if recovery with one backup fails, another backup can be used.

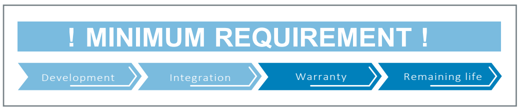


! MINIMUM REQUIREMENT !

Development | Integration | Warranty | Remaining life

### 8.4. Restoring a trustworthy state after a malfunction/attack

After an attack, the machine needs to be restored to a trustworthy state. Created regularly, backups allow the machine to be restored to its status prior to malfunctioning. Checking the components directly dependent on the machine is also recommended so that they can also be restored to a trustworthy state if necessary.

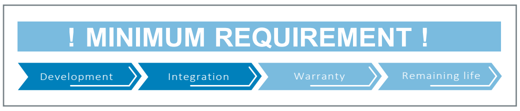


! MINIMUM REQUIREMENT !

Development | Integration | Warranty | Remaining life

### 8.5. Recovering encrypted data

When the machine is restored to a trustworthy state, some data will only be available in encrypted form. The backup systems need to allow recovery of the encrypted data.



! MINIMUM REQUIREMENT !

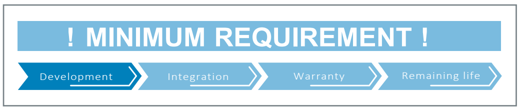
Development | Integration | Warranty | Remaining life

# 9. Secure product lifecycle

## From design to phase-out

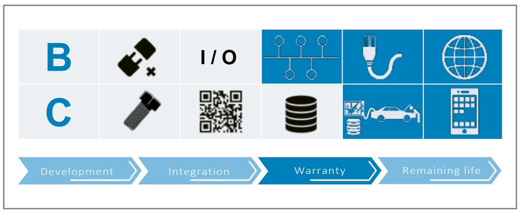
**The plant manufacturer should define and ensure a secure machine lifecycle. As described in Section 1, the product should ideally be subject to regular risk analysis. This is often a challenge for small and medium-sized enterprises due to a lack of resources. To ensure a secure product lifecycle of the machine despite this, the following practical measures should be taken.**

Based on documented threat models, the plant manufacturer should ensure that the plant's security functions meet the need for protection appropriately (see also Section 16).


! MINIMUM REQUIREMENT !

### 9.1. Monitoring vulnerabilities

Machine manufacturers, integrators and operators should be in a position to classify newly-detected attack vectors by their risk potential. Quickly assessing whether a newly discovered vulnerability is relevant for machine configuration is especially important. Machine configurations are often very complex with versatile component classes, so a machine inventory should be created to do this. Note that the inventory undertaken by the manufacturer can often only record the state at commissioning. The responsibility for conducting such an inventory can thus fall to the plant operator, especially when the operator changes the configuration.

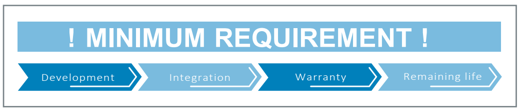


### 9.2. Manufacturer monitoring of the threat situation

As well as monitoring current vulnerabilities, the manufacturer should be aware of the current threat situation and incorporate this into the development of new machines. If, for example, there is an increase in concrete attacks on a particular component class built into the machine without the machine being directly affected, the manufacturer should still know about appropriate protective measures.

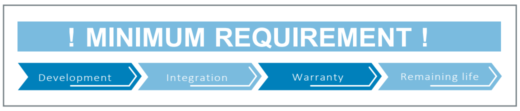
### 9.3. Responsiveness to vulnerabilities

Monitoring specific vulnerabilities and the general threat situation should enable the manufacturer/integrator to react quickly to any vulnerability detected and to protect the machines and plants against new threats. A pre-defined procedure to follow when a vulnerability is detected is a minimum requirement for reacting appropriately. In-house processes that can be initiated at any time when needed should therefore be defined.


! MINIMUM REQUIREMENT !

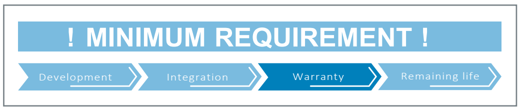
### 9.4. Determining the channels of communication within the plant

One of the more important in-house processes is defining communication channels. The person to contact when vulnerabilities are detected externally should be clearly defined, as should the procedure for passing on this information within the company (how and to whom). In terms of communication outside the company, it is recommended that the manufacturer/integrator inform the operator early of any vulnerabilities identified for the affected machine series.


! MINIMUM REQUIREMENT !

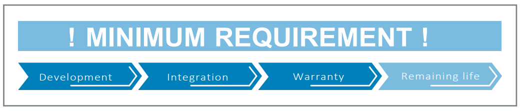
### 9.5. Patch management

In order to ensure that the plant is adjusted to new threat situations and newly-detected vulnerabilities, the manufacturer should define a secure process for handling and integrating patches. This also includes planning all the necessary resources in advance, as well as defining distribution mechanisms for the patch to allow fast integration. An infrastructure for distributing the patches to the operators should be available; the operators should maintain processes and infrastructures for accepting, testing and installing patches.



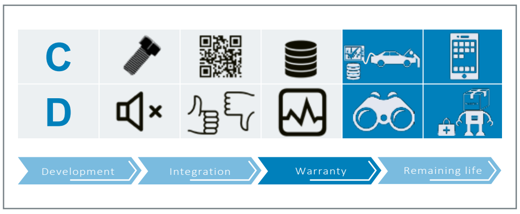
### 9.6. Nomination of internal and external responsible parties

For the required processes to run efficiently, internal and external responsible parties need to be designated. Persons responsible for assessing an incoming report of a weak point and for the development and rollout of patches should be identified. The responsible parties should be granted authority to act and be provided with the necessary means to coordinate patch management efficiently.



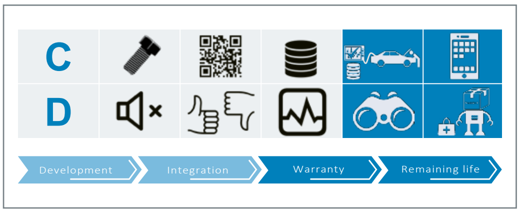
### 9.7. Handling end of support (EoS)

When support for a machine comes to an end, clearly defined processes should be specified. If possible, the integrator should inform the operator early on that support, especially in the form of patches, is about to expire. Depending on where they are used, many machines have long service lives over several years, so the time of EoS should ideally be known right from the start of plant planning.



### 9.8. Phase-out management

When a machine is to be phased out, a secure phase-out process should be defined. This should particularly ensure that unauthorized third parties cannot access sensitive data. The most important point here is the destruction of all the machine's mass storage. Destruction of especially critical components can also lower the risk of reverse engineering.



# 10. Adapting and testing components

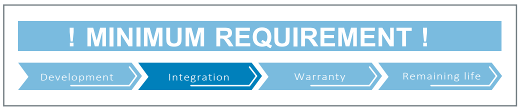
## Survival of the fittest

**The plant's defined security functionality should be checked regularly to make sure that it is robust even in a very dynamic environment.**

### 10.1. Adjust standard settings

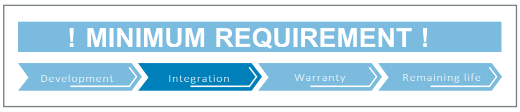
Attention must be paid to ensure that the default settings are adjusted both during the initial setup and after every recovery of a trustworthy state. Default passwords for administrator accounts (see Section 3) and deactivated security functions are common gateways for attacks. The security functions of the machine and its secure configuration are listed in the documentation in full (see Section 16).
All adjustments and settings should be logged for subsequent tests.

Adjusting the default settings should ensure that the new configuration is appropriate for the threat situation.



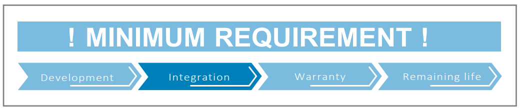
### 10.2. Adapting the hardware configuration

If the machine is available with various hardware configurations, it is important to check whether the intended configuration offers appropriate security functionality for the threat situation before integration.



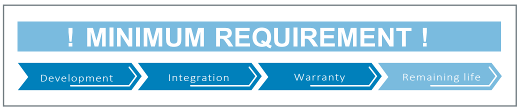
### 10.3. Internet access within the ICS network

It is important to check whether Internet access is possible within the plant network. If so, it is also important to check that this Internet access does not contradict the defined security functionality of the plant and that the accessing components are sufficiently isolated from critical parts of the machine.



### 10.4. Tests for verification and validation

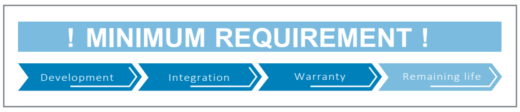
The security functions of the plant should be both verified (comparison with specifications) and validated (i.e. checking the suitability of the security functions). Although this kind of check cannot usually eliminate the occurrence of weak points, it can greatly reduce them. Conducting a thorough test initially requires the creation of a test plan. This then forms the basis for preparing the test and includes planning test cases and scenarios (see also the BSI's ICS Compendium for manufacturers and integrators[7]). Conducting the test can be a great deal of work and should be initiated by the respective responsible party. The results of the check should be documented.



[7] https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS/empfehlungen_node.html

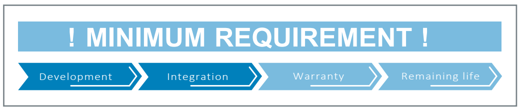
### 10.5. Tests for software and information integrity

The integrity of all the machine's software components and configuration data should be ensured. One option here is digital signatures, which are checked each time the configuration data is imported and every time a program is run. The signature procedure used should be state of the art with regard to parameters and cryptographic material (see Section 14).


! MINIMUM REQUIREMENT !

### 10.6. Selecting secure components

Suppliers often integrate external components into the machine. In such cases, the integrator should check whether the external components satisfy the identified security requirements (see also Section 15). This can be evaluated based on certification of the supplied components or by trained developers (see Section 17).
If certification is used for checking, attention should be paid to ensure that the certificate is valid at least until commissioning and that the scope of the check is adequate for the intended purpose in the plant.


! MINIMUM REQUIREMENT !

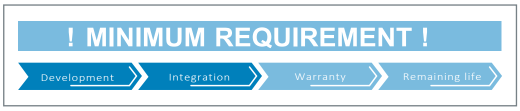
# 11. Foregoing unnecessary component functions

## As little as possible, as much as necessary

**A machine as a whole or individual components within the plant often have access to a variety of functions that are not used for operation in certain application environments. These kinds of superfluous product functions can significantly increase the potential attack area and are often gateways for attackers. Functions that are irrelevant for the machine's field of application should not be included.**

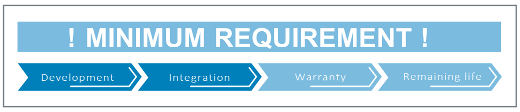
### 11.1. Removing unnecessary software and services

The first step is to remove all services and software components that are not immediately necessary for operating the machine. If they cannot be removed, deactivating the unnecessary software components is an option, although this can be very complex in some products (especially software from suppliers). The selection of the software that is actually active should be flexible and its implementation easy to access for the integrator and operator. Function dependencies in particular should be automatically dismantled. Ideally, the integrator selects the functions necessary for operation and only these and the functions/software parts dependent on them are incorporated into the machine.



### 11.2. Removing/deactivating all hardware components not in use

Similarly, unused hardware components should also be eliminated as much as possible. Specific adjustment of the hardware configuration can be very complex in some machines, so it should at least be possible to deactivate all the machines' hardware components (e.g. unneeded interfaces). In the same way as the removal of unnecessary software and services, the machine should ideally automatically deactivate all hardware components not currently in use.



# 12. Component hardening

## A chain is only as strong as its weakest link

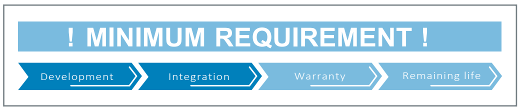
**Increasing connectivity and more intelligent functions mean that security can no longer be implemented through compartmentalization alone. Secure, hardened components will play an increasingly important role.**

### 12.1. Components may only execute hardened code

Only programs whose development process takes a minimal level of quality criteria into consideration should be run on the machine. This is intended to ensure that the software components comply with a suitable quality standard. More generally, it is recommended that the programs are developed and maintained in line with state-of-the-art software engineering technology.

VDMA has published “Software quality assurance” guidelines to help with this[8].

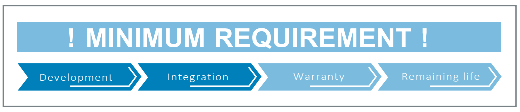
Guidelines for quality criteria and the evaluation of software products, such as the standard ISO/IEC 25000 (”Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Guide to SQuaRE”) and the associated standards series ISO/IEC 250xx, can also be used.



### 12.2. Security tests as an integral part of development and system integration

Secuity tests should be an integral part of development and system integration. Fuzzing tools should be used to test all application program interfaces (APIs) and network interfaces classified as critical.

Random testing with structured but invalid input is often enough to discover significant vulnerabilities, which the developer can then resolve. Furthermore, tools for static code analysis should be used to help resolve common programming errors. In addition to these automated approaches, manual code analyses should be conducted. This can take the form of trained developers (see Section 17) within the development department cross-checking the source code.



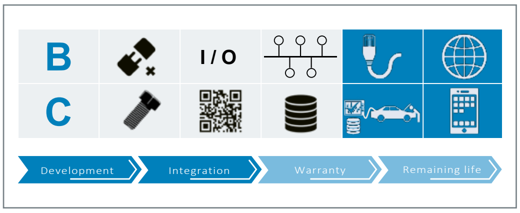
### 12.3. DoS protection

One specific danger for the plant is the “denial of service” (DoS) attack, which blocks the service offered by the plant. In addition to special attack methods, by far the most common cause of a DoS is an overloaded infrastructure, e.g. when massive numbers of requests are sent to the service.

When the start of a DoS attack is detected, blocking lists of the senders' IP addresses should be entered into the firewall automatically (see Section 2).

If possible, the services should be spread across multiple virtual entities through server load distribution, so that the load can be spread effectively to intact entities if the physical computer fails.

The developers should receive training (see Section 17) on further measures (such as recognizing IP spoofing according to RFC 2267 or SYN cookies).

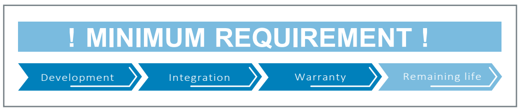


[8] http://www.vdma-verlag.com/home/p123.html

### 12.4. Application whitelisting and blacklisting

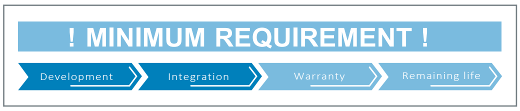
Application whitelisting further reduces the potential attack area of the plant. One way to do this is by only allowing programs that have been signed (by the machine's manufacturer) to be run on the machine. Each time a program is opened, it checks whether the program signature can be correctly verified and whether the issuer is on the whitelist. Application whitelisting allows the implementation of both very flexible and restrictive policies for program execution.

Blacklisting can also be used in the same way as whitelisting; it excludes programs that are known to be malicious and those that are simply not allowed (such as Internet Explorer, Java, Flash). Blacklisting requires regular updates to the list and thus an appropriate updating process in the plant.



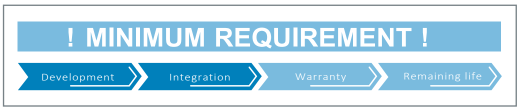
### 12.5. Reducing system complexity

When the machine is developed, the complexity of the components and the system as a whole should be kept as low as possible. Function reduction is the key point here, and is addressed separately in Section 11. Additionally, similar groups of functions should be compiled in modules and components, which often enables the abstraction levels of the machine's functions to be mapped to components. This makes it easier to maintain, further develop and modify the machines and ultimately reduces the potential attack area.



### 12.6. Safeguarding field devices located outside the plant from physical attacks

If the machine is implemented as a distributed system, it is important to ensure that remote field devices outside the plant are protected. Safeguarding against physical attacks is especially important here. Where components with a particularly high need for protection are located far away, the use of hardware security modules (HSM) may be necessary to ensure that sensitive key material is stored securely.

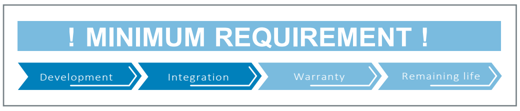


### 12.7. Safeguarding electronic external interfaces

All of the machine's digital external interfaces should be safeguarded against access not intended by the manufacturer.

This kind of safeguarding is initially carried out based on complete identification and documentation of all implemented interfaces. In order to log all interfaces called up by other systems, all communication paths to external software modules should be defined in particular, and clearly documented in a context diagram.

In a class of their own are debugging interfaces, which attackers often exploit to gain direct access to a machine. As such, all debugging interfaces (e.g. IEEE 1149.1 JTAG, background debug mode (BDM) or USB interfaces) should first be identified and documented. The way debugging interfaces like this are treated depends on the anticipated attack model.



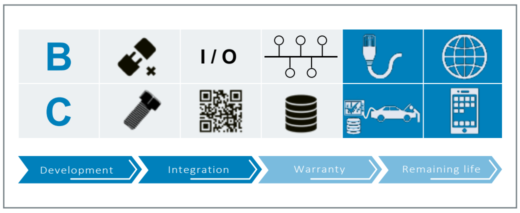
# 13. Isolation techniques within the machine/virtualization

## Neatly separated

**In order to reduce the effects of a malfunction within a machine as much as possible, the individual software components should be separated from one another using suitable isolation techniques. This can be done using virtualization solutions and trusted execution environments (TEE). Implementing these techniques can be demanding in certain machine configurations.**

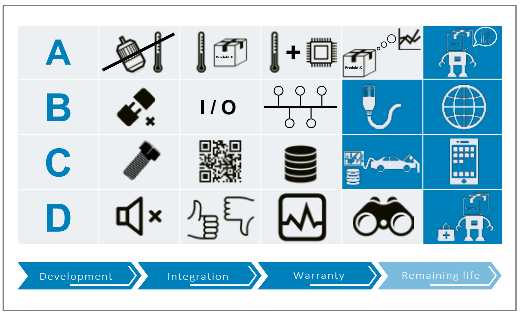
### 13.1. Protection against malicious code by sandboxing and virtualization

Damage from malicious code can often be limited by running machine programs in a sandbox or a virtual environment. First, this allows the rights and functions available to the program to be specifically restricted, which often leads to a significantly reduced potential attack area. Secondly, the effects of a successful attack are usually limited to the local virtual environment. There are plenty of attacks known to target virtualization solutions (e.g. attacks on hypervisors), but having to break out of the isolated environment is still effective at stopping much of the common malware.



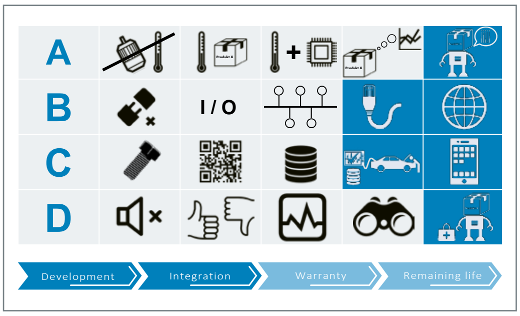
### 13.2. The machine should implement restrictions for "mobile code"

"Mobile code" refers to programs and scripts that are frequently exchanged (e.g. Java(script), ActiveX or VBScript), which can cause considerable damage within the machine. As described in Section 12.4, only programs from trustworthy sources should be run. As a weaker alternative, programs of unknown origin can be run with greatly reduced rights. Sandboxing and virtualizing allow programs to be run in environments with pre-defined and restricted functionality.



### 13.3. Delimiting the operational and configuration data of application programs

Virtualization techniques enable the isolation of operational and configuration data from application programs in particular. Since such data is often accessed by multiple machine components, this can effectively minimize the risk of large parts of the machine being compromised by malicious manipulation of the configuration data.



# 14. Cryptography

## The book with standardized seals

**The use of secure cryptographic processes forms the foundation for using secure protocols, for authentication measures and for safeguarding wireless technologies. All cryptographic algorithms and parameters must be state of the art. This section will go into more detail on selecting suitable algorithms and parameters.**

### 14.1. Implementing standardized algorithms

Developing secure cryptographic algorithms is a complex process that includes cryptanalysis by experts, so in-house development is highly discouraged. Public bodies provide compilations and recommendations of fully-developed processes and parameters that are currently secure. For example, recommendations for cryptographic processes and key lengths are presented in documents from the BSI [9, 10], NIST[11] and the Bundesnetzagentur[12] (German Federal Network Agency).When processes are selected, the product lifecycle of the plant should be consulted so that the development of computing power can be taken into account for plants that are used for long periods over many years. The key length should be selected according to the planned period of use. Processes for replacing or updating the cipher suites should be provided when possible.

**In-house cryptographic development is highly discouraged.**

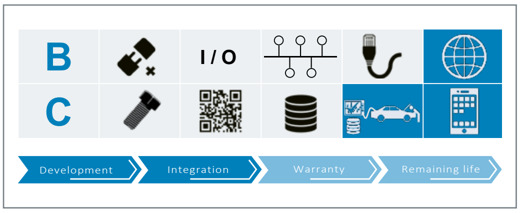
**! MINIMUM REQUIREMENT !**

Development Integration Warranty Remaining life

### 14.2. Integrating into existing Public Key Infrastructures

The plant manufacturer should ensure that the plants can be integrated into existing PKIs. In particular, it should be possible to use current certificates of existing PKIs. A secure process for generating, integrating and handling the corresponding cryptographic material should be defined for this. To allow certificates to be updated during operation, certificate lifecycle management (CLM) or the option of using it should be provided to the operator.
Components based on Microsoft Windows can use the Simple Certificate Enrollment Protocol (SCEP) and Network Device Enrollment Service (NDES) as protocols if a Microsoft CA is used.

When certificates are verified, the owner, issuer and validity status must be checked.
Furthermore, the certificate chains should be fully checked and as few root certificates as possible should be included in the list of trustworthy certificates. Since the functioning of a certificate revocation list (CRL) in a machine-to-machine (M2M) communication environment has not proved useful due to the sometimes frequent changes and the resulting fast-growing list lengths, the use of an OCSP (online certificate status protocol) should be considered.



[9] BSI TR-03111 „Elliptic Curve Cryptography“
[10] SI TR-02102-1 ”Cryptographic procedure: recommendations and key lengths ”
[11] http://csrc.nist.gov/groups/ST/toolkit/
[12] Announcement on electronic signature according to the German Signatures Act and the Signatures Ordinance (overview of suitable algorithms)

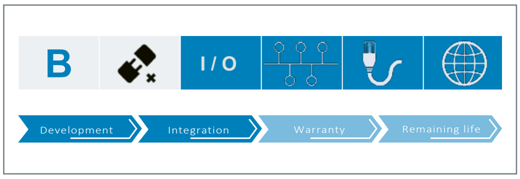
# 15. Determining security requirements for vendors and suppliers

## Declare and demand what you want

**If supplied components are integrated into plants and do not meet the identified security requirements, this can undermine the machine's security concept. As the weakest link in the chain, these components are often the gateway for attackers. Suitable regulations for secure third party components and a secure integration process for supplied components need to be defined.**

### 15.1. Checking security requirements of supplied components

The security requirements identified by the manufacturer/integrator of the plant should be met for every supplied component within its functional range. The security requirements can be checked by the integrator or supplier, or by both together. In highly confidential projects, the integrator should carry out the check based on the documentation provided by the supplier. If this is not necessary, the suppler can provide an initial estimate of conformity in the form of a quote. The supplied components' ability to satisfy the identified need for protection should be ensured. Conformity checks or the results of audits by third parties can also be used for this.



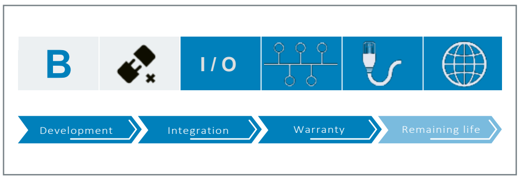
### 15.2. Identifying one's own role as a supplier

If the machine is integrated into another product as a sub-component, the manufacturer should provide the customer with documentation of all security measures. The documentation should enable him to check whether the components to be supplied meet the protection needs of the target system. The manufacturer should be aware of his own role as a supplier and define organizational processes accordingly.
This can take the form of checking the security requirements for the machine to be supplied with the corresponding delivery quote, or documenting and disclosing the protection concept.

! MINIMUM REQUIREMENT !
Development
Integration
Warranty
Remaining life

### 15.3. Outsourced software development

Where software or parts thereof are provided by third parties, it should be included in the secure development process. This applies in particular to libraries and code from open repositories.
Control mechanisms should be established both to ensure that company security measures are implemented within the third party product and to minimize the potential for weak points or known malicious code. Even external system parts should be included in the risk assessment, so the necessary information on these parts must be obtained.



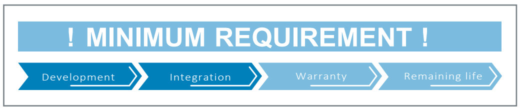
# 16. Documentation

## Make a note of it

**Security measures can only be implemented smoothly if they are fully documented.**

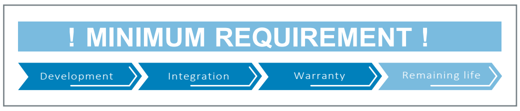
### 16.1. Interfaces

All security-related interfaces should be identified and documented. This especially includes debugging interfaces in hardware and software.



### 16.2. Established processes

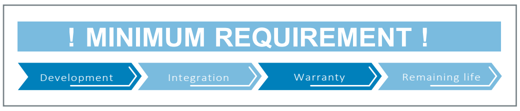
All the organizational and technical processes addressed in this document should be identified and documented. The organizational procedure and the responsible roles should be derived from the documentation.
Even someone who is unfamiliar with the process should be able to recognize the steps to be taken in a given situation. The established processes should be documented internally.



### 16.3. Documentation of risk analysis

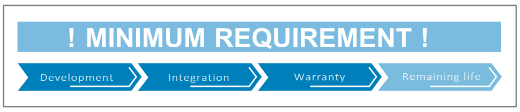
The results of the risk analyses (see Section 1) should be documented and archived for subsequent use. This applies particularly to documented threat models. The documentation should show the methods on which the risk analysis was based and information used to assess the effect and probability of the attacks.

The risk analysis should be documented internally only, as attackers can use a public risk analysis to identify the threats with the greatest potential for damage. Only the resulting requirements for protective measures and need for protection should be included in the external documentation.



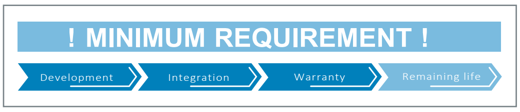
### 16.4. Distributed rights

The distribution of rights to the players defined in Section 3 should be documented. It is especially important to log changes to the rights distribution, so that they can be used for security analyses at a later date.



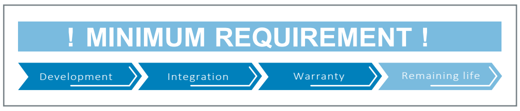
### 16.5. Machine inventory

The manufacturer should create a machine inventory that takes all relevant device, communication and management aspects (including hardware and software) into consideration. Ideally, the machine should be able to generate a report on the components that are currently installed including their properties. A diagram of the components should illustrate the functional connection between them.



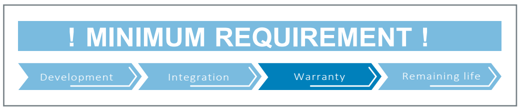
### 16.6. Document management

Organizational processes for creating, distributing and releasing documents should be defined. The relevant documents must be checked at regular intervals to ensure that they are up to date.


! MINIMUM REQUIREMENT !

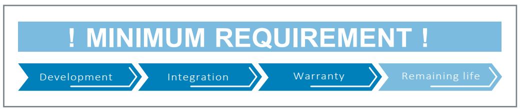
### 16.7. Security incidents

All security incidents should be documented and archived. This includes incidents within the organization and, if possible, security incidents that have been observed in machines already in use. The documentation of security incidents should initially be internal. If third parties are also affected by a security incident or the cause of the incident poses a threat to the environment, a report to this effect should be created and communicated to the pertinent parties (see Section 9.4).


! MINIMUM REQUIREMENT !

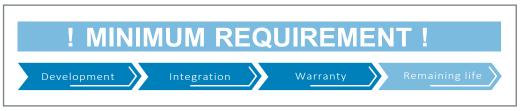
### 16.8. Strategy and security controls

The machine's security concept and all security measures should be documented, as well as the function of the security measures. This includes their implementation and configuration, as well as information on maintenance. This is the basis for the checks on security requirements listed in Section 15.2. Ideally, the manufacturer should provide a manual on the security functions of the machine.


! MINIMUM REQUIREMENT !

### 16.9. Organizational processes and roles

All security-related organizational processes and the responsible parties and contacts in each case should be documented. The external contact should be documented and made clear for external players at all times (see also Section 9.6).


! MINIMUM REQUIREMENT !

# 17. Developer training on security

## The only substitute for knowledge is knowledge

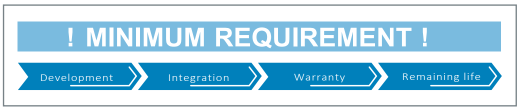
**Increasing employee expertise when it comes to information technology in general, and IT security, network security and the features of IT in production plants in particular, is an urgent and essential measure for sustainably developing and improving the security environment. It demands that new requirements be added to established job profiles (for example through advanced training).**

Since safety approvals prevent plants from being modified at will during operation (such as by installing software updates after approval), improving IT security, such as by increasing the code quality in all components installed in the plants, is extremely important. Advanced training should therefore focus on enhancing expertise in secure software development; increased knowledge of network technology, system architecture, protocols and IT standards is also essential in order to raise the security level for the plants themselves and their future operation. The following sections list the information that is important to convey and indicate seminars that are already on offer.

### 17.1. Awareness

Any security measure is only as strong as its weakest link; inattention, ignorance and negligence can all result in critical gaps. Every employee must understand that they are part of something bigger when it comes to safety and security, and their contribution can have a decisive influence on the quality of the plant's security. All line managers, management, employees and temporary staff should have the importance of their actions emphasized, and taught about compliant conduct.

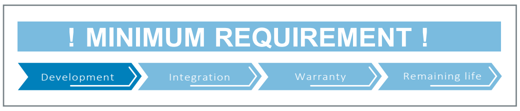
General instruction on basic IT security topics not only protects the plants themselves – the product – but also the entire company. Only those who know the risks can take appropriate care!



### 17.2. (Software) developers and designers

Designers, development engineers and trained software developers (such as IT specialists in application development) should receive regular training on the relevance of code security. Covering general concepts such as secure development lifecycle (SDL) and refreshing the basics of authentication, authorization and session management are essential in order to prevent common errors and improve the quality of the development process. Core requirements for developers include the following:

- Introduction to SDL
- Conducting code reviews manually
- Using static tools for code review
- Conducting security tests
- Methods of secure software development
- Classifying data (permission, access)
- Difference between office IT and ICS
- Potential attack targets in industrial IT systems and components (ICS/SCADA)
- Special features in bus topologies
- Security controls for ICS/SCADA devices
- Network segmentation and firewall concepts
- Integration into security management



### 17.3. Plant planners and project designers

In addition to the development engineers, the planners and product managers play an important role. If they do not understand what the customer (operator) needs when it comes to the increasingly complex integration of a new plant into the existing production landscape, it is difficult for the product managers to give the developers concrete specifications for important functions and properties of the plants. These include requirements of the operating systems being used, network technologies, protocols and interfaces. Consequently, the aforementioned training content should be mandatory for anyone tasked with planning and product management and should be supplemented with the following content:

- (IT) components in production networks
- Basics of directory services/databases
- Basics of TCP/IP and bus networks
- Security-related specifications for plant documentation (context diagrams)
- Important security protocols and how they work (cryptographic basics)
- Risk analysis and risk management
- The latest operating systems and their (security) management
- Basics of asset, patch and vulnerability management
- Hardening of IT systems against attacks
- Basics of virtualization
- Computer emergency response and incident management in plant networks
- Statutory framework conditions
- Attack vectors and typical weak points

The content shown above focuses primarily on technical issues, but organizational and sociological aspects are just as important, if not more so. Even with good training, no progress can be made at the operative level without the strong support of the decision makers and company management to reinforce the IT security of their products and solutions.

Training on secure development lifecycle approaches alone is not useful unless the company establishes the necessary technical and organizational conditions for adapting the development processes and design to SDL. This includes making security a fixed design goal and giving employees the time and means to implement this security right from the beginning. Decision makers should be aware that sustainable improvements to security can only be achieved with a sustainable realignment of the company.

**! MINIMUM REQUIREMENT !**

Development
Integration
Warranty
Remaining life

### 17.4. Responsible party for product security

Although the majority of companies do not yet have a Product Security Officer, the need for this function is indisputable. In order to be able to perform their tasks, the PSO should have good basic knowledge of IT infrastructure and of ICS/SCADA technology. In addition, it is essential that the PSO addresses the topic of security management, so that they can define and communicate the security strategy for the company's own products together with the Chief (Information) Security Officer and the product managers. To do this, the PSO needs deeper insights into:

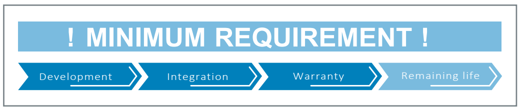
- Security analysis and risk management
- Risk analysis and assessment
- Regulations and policies
- Weak point and incident management
- Product lifecycle IT/plant
- Reporting and reporting channel for incidents

**! MINIMUM REQUIREMENT !**

Development
Integration
Warranty
Remaining life

### 17.5 Training methods

Since the content to be taught is sometimes very complex and specific, and the participants in the group have vastly different levels of knowledge, it is difficult for standardized training sessions to teach everything required. Various well-known providers offer German-language introductory courses on IT security in production and industrial security, which can be used as a foundation. In addition to that, more internationally oriented courses from SANS (especially parts of ICS410 and SEC401) have proven a useful introduction to the topic. The US-CERT also teaches specialist knowledge free of charge; the training is available both web-based and in the ICS lab[13]. In the authors' experience, slightly adapted introductory training for a small internal team is the most effective option. This can then be used as the basis for a tailored training plan that better caters to the company's needs.



[13] https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

| Overview of the recommendations for action | | | Development | Integration | Operation within Warranty |
|---|---|---|---|---|---|
| **Risk analysis** | 1.1. | Identifying assets | ● | | ● |
| | 1.2. | Determining protection goals | ● | | ● |
| | 1.3. | Identifying threats | ● | | ● |
| | 1.4. | Risk assessment | ● | | ● |
| **Network segmentation** | 2.1. | Definition of risk-based security requirements assigned to plants and components | ● | ● | |
| | 2.2. | Zoning of services | ● | | |
| | 2.3. | Using isolation measures | ● | ● | |
| | 2.4. | Periodic checking of isolation measures for effectiveness and patchability of filter components | | | ● |
| | 2.5. | DNS and other services per zone | ● | ● | |
| **User accounts, credentials, authentication and authorization** | 3.1. | Individual user accounts | ● | ● | ● |
| | 3.2. | Account management | ● | ● | ● |
| | 3.3. | Distribution and management of credentials | ● | ● | ● |
| | 3.4. | Authenticating human users, software processes and components | ● | | ● |
| | 3.5. | Public-Key authentication | ● | | ● |
| | 3.6. | Creating zones and access concepts with corresponding authentication | ● | | ● |
| | 3.7. | The machine should ensure an authorization check of the players / services after every authentication | ● | | ● |
| | 3.8. | Strong authentication to external interfaces | ● | ● | ● |
| **Using secure protocols** | 4.1. | Confidentiality of communication with IP-based protocols | ● | ● | ● |
| | 4.2. | Integrity of communication | ● | ● | ● |
| | 4.3. | Type, strength and quality of encryption algorithms | ● | ● | ● |
| | 4.4. | Special consideration of fieldbus | ● | ● | ● |
| **Safeguarding wireless technologies** | 5.1. | Secure configuration | ● | ● | |
| | 5.2. | Wireless access management | ● | ● | |
| | 5.3. | Time-dependency of security of cryptographic functions | ● | ● | ● |
| **Secure remote service** | 6.1. | Controls on setting up and ending a remote access session | ● | ● | ● |
| | 6.2. | Safeguarding through technical and organizational measures | ● | ● | ● |
| | 6.3. | Encrypting the connections | ● | ● | ● |
| | 6.4. | Establishing access processes | ● | ● | ● |
| | 6.5. | Securing connections to other networks | ● | ● | ● |
| **Monitoring and recognizing attacks** | 7.1. | Monitoring all access to machine components | ● | ● | ● |
| | 7.2. | Integrating monitoring functions in the control desk | ● | ● | ● |
| | 7.3. | Virus scanners | ● | ● | ● |
| | 7.4. | Network IDS and anomaly detection in complex machines | ● | ● | ● |
| **Recovery plan** | 8.1. | Creating backup systems | ● | ● | ● |
| | 8.2. | Creating regular backups | | | ● |
| | 8.3. | Checking backups for recoverability | | | ● |
| | 8.4. | Restoring a trustworthy state after a malfunction/attack | | | ● |
| | 8.5. | Recovering encrypted data | ● | ● | |
| **Secure product lifecycle** | 9.1. | Monitoring vulnerabilities | | | ● |
| | 9.2. | Manufacturer monitoring of the threat situation | ● | | |
| | 9.3. | Responsiveness to vulnerabilities | ● | | ● |
| | 9.4. | Determining channels of communication | ● | | ● |

| Remaining lifetime operation | Integration of sensors/ actuators | Communication / Connectivity | Functionalities for data storage and information exchange | Monitoring | Manufacturer | Integrator | Operator |
|---|---|---|---|---|---|---|---|
| ● | 1 | 1 | 1 | 1 | ● | ● | ● |
| ● | 1 | 1 | 1 | 1 | ● | ● | ● |
| ● | 1 | 1 | 1 | 1 | ● | ● | ● |
| ● | 1 | 1 | 1 | 1 | ● | ● | ● |
|  |  | 3 | 4 |  | ● | ● |  |
|  |  | 3 | 4 |  | ● | ● |  |
|  |  | 3 | 4 |  | ● | ● |  |
| ● |  | 3 | 4 |  |  | ● | ● |
|  |  | 3 | 4 |  | ● | ● |  |
| ● |  | 4 | 2 |  | ● | ● | ● |
| ● |  | 4 | 2 |  | ● | ● | ● |
| ● |  | 4 | 2 |  | ● | ● | ● |
| ● | 1 | 1 | 1 | 1 | ● | ● | ● |
| ● |  | 4 | 4 |  | ● | ● | ● |
| ● |  | 4 | 4 |  | ● | ● | ● |
| ● | 1 | 1 | 1 | 1 | ● | ● | ● |
| ● | 1 | 1 | 1 | 1 | ● | ● | ● |
| ● |  | 4 | 4 |  | ● | ● | ● |
| ● |  | 3 | 4 |  | ● | ● | ● |
| ● |  | 3 | 4 |  | ● | ● | ● |
| ● |  | 3 |  |  | ● | ● | ● |
|  |  | 2 | 4 | 3 |  | ● | ● |
|  |  | 2 | 4 | 3 | ● | ● | ● |
| ● |  | 2 | 4 | 3 | ● | ● | ● |
| ● | 4 |  | 4 |  | ● | ● | ● |
| ● | 4 |  | 4 |  | ● | ● | ● |
| ● | 4 |  | 4 |  | ● | ● | ● |
| ● | 4 |  | 4 |  | ● | ● | ● |
| ● | 4 |  | 4 |  |  | ● | ● |
| ● |  |  |  | 3 | ● | ● | ● |
| ● |  |  |  | 2 |  | ● |  |
| ● | 1 | 1 | 1 | 1 | ● | ● | ● |
| ● | 5 | 5 | 4 | 4 | ● | ● | ● |
| ● | 1 | 1 | 1 | 1 | ● | ● | ● |
| ● | 1 | 1 | 1 | 1 |  |  | ● |
| ● | 1 | 1 | 1 | 1 |  |  | ● |
| ● | 1 | 1 | 1 | 1 | ● | ● | ● |
|  | 1 | 1 | 1 | 1 | ● | ● | ● |
|  |  | 3 | 4 |  | ● | ● | ● |
|  | 1 | 1 | 1 | 1 | ● |  |  |
|  | 1 | 1 | 1 | 1 | ● | ● | ● |
|  | 1 | 1 | 1 | 1 | ● | ● | ● |

| Overview of the recommendations for action | | | Development | Integration | Operation within Warranty |
|---|---|---|---|---|---|
| **Secure product lifecycle** | 9.5. | Patch management | | | ● |
| | 9.6. | Nomination of internal and external responsible parties | ● | ● | ● |
| | 9.7. | Handling end of support (EoS) | | | ● |
| | 9.8. | Phase-out management | | | ● |
| **Adapting and testing components** | 10.1. | Adjust standard settings | | ● | |
| | 10.2. | Adapting the hardware configuration | | ● | |
| | 10.3. | Internet access within the ICS network | | ● | |
| | 10.4. | Tests for verification and validation | ● | ● | ● |
| | 10.5. | Tests for software and information integrity | ● | ● | ● |
| | 10.6. | Selecting secure components | ● | ● | |
| **Foregoing unnecessary component functions** | 11.1. | Removing unnecessary software and services | ● | ● | |
| | 11.2. | Removing/deactivating all hardware components not in use | ● | ● | |
| **Component hardening** | 12.1. | Components may only execute hardened code | ● | ● | |
| | 12.2. | Security tests as an integral part of development and system integration | ● | ● | |
| | 12.3. | DoS protection | ● | ● | |
| | 12.4. | Application whitelisting and blacklisting | ● | ● | ● |
| | 12.5. | Reducing system complexity | ● | ● | |
| | 12.6. | Safeguarding field devices located outside the plant from physical attacks | ● | ● | |
| | 12.7. | Safeguarding electronic external interfaces | ● | ● | |
| **Insulation techniques within the machine/virtualization** | 13.1. | Protection against malicious code by sandboxing and virtualization | ● | ● | |
| | 13.2. | The machine should implement restrictions for “mobile code” | ● | ● | ● |
| | 13.3. | Delimiting the operational and configuration data of application programs | ● | ● | |
| **Cryptography** | 14.1. | Implementing standardized algorithms | ● | ● | |
| | 14.2. | Integrating into existing Public Key Infrastructures | ● | ● | |
| **Determining security requirements for vendors and suppliers** | 15.1. | Checking security requirements of supplied components | ● | ● | |
| | 15.2. | Identifying one's own role as a supplier | ● | ● | |
| | 15.3. | Outsourced software development | ● | ● | ● |
| **Documentation** | 16.1. | Interfaces | ● | ● | |
| | 16.2. | Established processes | ● | ● | ● |
| | 16.3. | Documentation of risk analysis | ● | | ● |
| | 16.4. | Distributed rights | ● | ● | ● |
| | 16.5. | Machine inventory | ● | ● | ● |
| | 16.6. | Document management | ● | ● | ● |
| | 16.7. | Security incidents | | | ● |
| | 16.8. | Strategy and security controls | ● | ● | ● |
| | 16.9. | Organizational processes and roles | ● | ● | ● |
| **Developer training on security** | 17.1. | Awareness | ● | ● | ● |
| | 17.2. | (Software) developers and designers | ● | | |
| | 17.3. | Plant planners and project designers | ● | ● | ● |
| | 17.4. | Responsible party for product security | ● | ● | ● |
| | 17.5. | Training methods | ● | ● | ● |

| Remaining lifetime operation | Integration of sensors/ actuators | Communication / Connectivity | Functionalities for data storage and information exchange | Monitoring | Manufacturer | Integrator | Operator |
|---|---|---|---|---|---|---|---|
|  | 1 | 1 | 1 | 1 | ● | ● | ● |
|  | 1 | 1 | 1 | 1 | ● | ● | ● |
|  |  |  | 3 | 3 |  | ● | ● |
| ● |  |  | 3 | 3 |  | ● | ● |
|  | 1 | 1 | 1 | 1 |  | ● | ● |
|  | 1 | 1 | 1 | 1 | ● | ● |  |
|  | 1 | 1 | 1 | 1 |  | ● | ● |
|  | 1 | 1 | 1 | 1 | ● | ● |  |
|  | 1 | 1 | 1 | 1 | ● | ● |  |
|  | 1 | 1 | 1 | 1 | ● | ● | ● |
|  | 1 | 1 | 1 | 1 | ● | ● |  |
|  | 1 | 1 | 1 | 1 | ● | ● |  |
|  | 1 | 1 | 1 | 1 | ● | ● |  |
|  | 1 | 1 | 1 | 1 | ● | ● |  |
|  |  | 4 | 4 |  | ● | ● |  |
|  | 1 | 1 | 1 | 1 | ● | ● | ● |
|  | 1 | 1 | 1 | 1 | ● | ● |  |
|  | 1 | 1 | 1 | 1 | ● | ● | ● |
|  | 1 | 1 | 1 | 1 | ● | ● |  |
|  |  | 4 | 4 |  | ● | ● |  |
|  | 5 | 4 | 4 | 5 | ● | ● |  |
|  | 5 | 4 | 4 | 5 | ● | ● |  |
|  | 1 | 1 | 1 | 1 | ● | ● |  |
|  |  | 5 | 4 |  | ● | ● | ● |
|  |  | 2 |  |  | ● | ● | ● |
|  | 1 | 1 | 1 | 1 | ● | ● |  |
|  |  | 2 |  |  | ● | ● |  |
|  | 1 | 1 | 1 | 1 | ● | ● |  |
|  | 1 | 1 | 1 | 1 | ● | ● | ● |
|  | 1 | 1 | 1 | 1 | ● | ● | ● |
|  | 1 | 1 | 1 | 1 | ● | ● | ● |
|  | 1 | 1 | 1 | 1 | ● | ● |  |
|  | 1 | 1 | 1 | 1 | ● | ● | ● |
|  | 1 | 1 | 1 | 1 | ● | ● | ● |
|  | 1 | 1 | 1 | 1 | ● | ● | ● |
|  | 1 | 1 | 1 | 1 | ● | ● | ● |
| ● | 1 | 1 | 1 | 1 | ● | ● | ● |
|  | 1 | 1 | 1 | 1 | ● | ● |  |
| ● | 1 | 1 | 1 | 1 |  | ● |  |
| ● | 1 | 1 | 1 | 1 |  | ● | ● |
|  | 1 | 1 | 1 | 1 | ● | ● | ● |

# Additional Information

The listed recommendations for action are intended to present basic protection for a small to medium enterprise on its way to Industrie 4.0. If the first steps have already been taken and the machine is to be designed for the future with complete Industrie 4.0 functionality, it is worth reading the additional literature.

Important sources of information that may provide further help in establishing secure protection are listed below.

- BSI ICS Security Compendium[14]
- VDMA industrial security questionnaire[15]
- VDMA study on the status quo of industrial security[16]
- VDMA Guidelines Industrie 4.0[17]
- Light and Right Security ICS (LARS ICS)[18]
- VdS Quick Check Security[19]
- Industry 4.0 Readiness Online Self-Check for Businesses[20]
- ICS-CERT newsletter, reports and recommendations for action
- VDI 2182 – IT security for industrial automation
- ISO/IEC 27000 series on information security
- IEC 62443 on ICS security
- ISO/IEC 15408-1 Evaluation criteria for IT security
- NAMUR worksheet NE 153
- NAMUR worksheet NE 115

[14] https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS/empfehlungen_node.html
[15] http://pks.vdma.org/article/-/articleview/6262936
[16] https://www.vdma.org/article/-/articleview/2717338
[17] http://industrie40.vdma.org/article/-/articleview/8567185
[18] https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Tools/LarsICS/LarsICS_node.html
[19] http://vds.de/de/vds-cyber-security/cyber-security-fuer-kmu/
[20] https://www.industrie40-readiness.de/

# Glossary

**Authentication**
Proof of a user/device's authorized access (from the point of view of the device doing the checking) as well as logging in with access data (from the point of view of the one being checked).

**Authorization**
Approval for access.

**Operator (asset owner)**
Operator of a plant according to VDI/VDE 2182.

**Credentials**
Access data, such as passwords, keys or biometric data.

**DNS  (Domain Name System)**
Directory service for resolving addresses into IP addresses.

**DoS (Denial of Service).**
Breakdown of a network service due to (potentially deliberate) overloading.

**ERP (Enterprise Resource Planning)**
Planning of resources in a company.

**FMEA (Failure Mode and Effects Analysis)**
Method for determining and assessing errors.

**Manufacturer**
Vendor of a component or machine according to VDI/VDE 2182.

**HSM (Hardware Security Module)**
Dedicated security chip for executing cryptographic operations with secure storage.

**ICS (Industrial Control System)**
IT-based control system of the plant.

**IDS (Intrusion Detection System)**
System for automatic attack detection.

**Integrator**
The plant engineer or integrator of multiple components or machines according to VDI/VDE 2182.

**IPS (Intrusion Prevention System)**
IDS systems that also contain methods on defending again attackers.

**MAC filtering**
Filtering of data packages based on their MAC address.

**MES (Manufacturing Execution Systems)**
Production control system.

**PKI (Public Key Infrastructure)**
Distributed system for managing and checking certificates based on asymmetric cryptography.

**Sandboxing**
Executing code in a controlled and isolated execution environment.

**SCADA**
**(Supervisory Control and Data Acquisition)**
System for monitoring and controlling technical processes.

**TEE (Trusted Execution Environment)**
Secure and trustworthy runtime environment for programs, e.g. on an in-house processor core.

**Verifizierung**
Checking that software meets its specification

**Validierung**
Checking software with regard to its suitability in the application scenario.

**VPN (Virtual Private Network)**
Virtual, self-contained communication network that uses an existing communication network for transport and is secured by encryption.

# Security at VDMA

## The right protection is everything

**Industrie 4.0 is unthinkable without protecting the data and expertise involved in production and communication processes across companies. VDMA supports its members in all security-related fields.**

Industrial security protects machines and plants against failure, manipulation, expertise drain and sabotage. Put simply, the protection goals are availability, integrity, confidentiality and authenticity.

VDMA focuses on topics of security in its

- Information Security and
- Industrial Security

task forces and the working group on

- Product and Know-How Protection

### Information Security

The Information Security task force develops guidelines and practical aids for "traditional" IT and information security. Much of it's work is based on the ISO 27000 series of standards and the Grundschutz (basic protection) from the German Federal Office for Information Security (BSI). The participants are IT security officers (CISO) from mechanical and plant engineering companies.

### Industrial Security

The Industrial Security task force develops guidelines and practical aids for security in production and for mechanical and plant engineering products. The participants are mechanical and plant engineering companies, operators, automation companies, service providers, security experts and the BSI.

**Integrated security first: Machines and plants, products and expertise need effective protection.**

### Product and Know-How Protection

The Product and Know-How Protection working group (Protect-ing) combines the activities of technology and service providers in product security, know-how protection and prevention of product piracy. Mechanical engineers are not the only ones to profit from the exchange between manufacturers, authorities and users.

**Contact**
Steffen Zimmermann
Product and Know-How Protection
Phone +49 69 6603-1978
Email steffen.zimmermann@vdma.org

Internet http://pks.vdma.org/security
www.protect-ing.de
www.i40-security.de

# Industrie 4.0 at VDMA

## Building blocks prepare the way

**How companies can profit from Industrie 4.0, which aspects need to be considered during implementation and the form the path to connected production can take – the VDMA Forum Industrie 4.0 provides answers to these questions.**

Industrie 4.0 is transforming production: IT and Internet technologies are penetrating products and plants more than ever. People, machines and means of production communicate with each other throughout the entire value chain. But these changes have not happened overnight. The development towards Industrie 4.0 is more evolution than revolution. To make sure this gradual implementation is a success, VDMA accompanies and supports its members in a multitude of ways:

VDMA has brought together an association of expertise in the VDMA Forum Industrie 4.0. The forum consists of an interdisciplinary team of VDMA experts. As partners and service providers, they offer practical support to the member companies and the VDMA associations and departments in the following areas of activity, which are particularly relevant to Industrie 4.0:

**Politics & networks:** Important political conditions need to be agreed upon with stakeholders from politics and society..

**Production & business models:** Intelligent production systems make organizations and processes more efficient. Automation and batch size 1 production are no longer mutually exclusive. Innovative business fields are emerging.

**Research & innovation:** The results of research are a more decisive factor than ever in Germany's competitiveness as an industrial location. Funding instruments need to be reliable and the results of research need to be transferred into industrial practice quickly.

**Standards & standardization:** Consistent standards are the only way to ensure successful connection along the value chain. Participating in drawing up these standards and involving the relevant stakeholders in dialog is crucial.

**IT security & the law:** The automated exchange of data between connected production systems must be secure and reliable. In addition to protecting products, machines and plants, further development and reinterpretation of existing legislation are important factors.

**IT technologies & software:** Modern software architectures are the key to modular and flexible systems. Suitable methods and the knowledge of various experts are needed to ensure that these systems meet modern standards in terms of quality, availability and usability.

**People & work:** The activities in the factory of the future are becoming more challenging from both the technological and the organizational perspective. Interdisciplinary competencies are becoming increasingly important. The education system and companies will need to adapt to this.

### Support along the way

There are many small pieces of a jigsaw puzzle that come together to form a bigger picture. With the Forum Industrie 4.0, VDMA is committed to transforming the vision of Industrie 4.0 into practicable recommendations for action for the mechanical and plant engineering sector and to taking the perspective of users into account. The goal is to build a long-lasting, sustainable network that enables member companies to exchange experiences.

**Contact**
Dr. Beate Stahl
Forum Industrie 4.0
Phone +49 69 6603-1295
Email beate.stahl@vdma.org
Internet http://industrie40.vdma.org

# Project partners / Imprint

**VDMA**
**Product and Know-how Pro**
Steffen Zimmermann
Lyoner Str. 18
60528 Frankfurt am Main
Email protect-ing@vdma.org
Internet pks.vdma.org

**Fraunhofer Institute for Applied and Integrated Security (AISEC)**
Bartol Filipovic
Head of Product Protection and Industrial Security
Parkring 4
85748 Garching b. München
Email bartol.filipovic@aisec.fraunhofer.de
Internet www.aisec.fraunhofer.de

**accessec GmbH**
Sebastian Rohr
CTO + CSO
Marktstr. 47–49
64401 Groß-Bieberau

**Project management**
VDMA Product and Know-how Protection
Steffen Zimmermann

**Contribution of content**
Fraunhofer AISEC
Konstantin Böttinger
Bartol Filipovic
Dr. Martin Hutle

accessec GmbH
Sebastian Rohr

**Design and layout**
VDMA-Forum Industrie 4.0
Dr. Beate Metten
VDMA Verlag GmbH
Martina Becker

**Publisher**
VDMA Verlag GmbH
Lyoner Str. 18
60528 Frankfurt am Main

**Printing**
English: N.A.
German: Druck- und Verlagshaus Zarbock

**Year of publication**
2016

**Image credits**
Cover image: Olivier Le Moal – Fotolia.com
Page 3: Kolbus

**Graphics**
Fraunhofer AISEC
VDMA
Pictograms: https://thenounproject.com

# Toolbox Industrie 4.0

Industrie 4.0

| | | Products | | | | |
|---|---|---|---|---|---|---|
| A | Integration of sensors / actuators | *__No use__ of sensors/ actuators* | ***Sensors / actuators** are **integrated*** | ***Sensor readings are processed** by the product* | *Data is **evaluated for analyses** by the product* | *The product **independently responds** based on the gained data* |
| B | Communication / Connectivity | *The product has **no interfaces*** | *The product sends or receives **I/O signals*** | *The product has **field bus interfaces*** | *The product has **Industrial Ethernet interfaces*** | *The product has **access to the internet*** |
| C | Functionalities for data storage and information exchange | ***No functionalities*** | *Possibility of **individual identification*** | *Product has a passive **data store*** | *Product with **data storage** for autonomous **information exchange*** | *Data and information exchange as **integral part*** |
| D | Monitoring | *__No monitoring__ by the product* | ***Detection of failures*** | *Recording of **operating condition for diagnostic purposes*** | ***Prognosis** of its own **functional condition*** | ***Independently adopted** control **measures*** |
| E | Product-related IT services | ***No services*** | *Services via **online portals*** | ***Service execution directly via the product*** | ***Independently performed** services* | *Complete integration into an **infrastructure of IT services*** |
| F | Business models around the product | *Gaining profits from **selling standardized products*** | ***Sales and consulting** regarding the product* | ***Sales, consulting and adaption** of the product to meet customer specifications* | *Additional sale of **product-related services*** | *Sale of product functions* |

Toolbox Industrie 4.0 – Products (Source: VDMA / Guideline Industrie 4.0)

The four phases of the product lifecycle

Development → Integration → Warranty → Remaining life

**VDMA**
**Product and Know-how Protection**
Lyoner Str. 18
60528 Frankfurt am Main
Phone +49 69 6603-1978
Fax +49 69 6603-2978
Email protect-ing@vdma.org
Internet pks.vdma.org

**Fraunhofer Institute for Applied**
**and Integrated Security (AISEC)**
Parkring 4
85748 Garching b. München
Internet www.aisec.fraunhofer.de

**accessec GmbH**
Marktstr. 47–49
64401 Groß-Bieberau

**pks.vdma.org**
**www.i40-security.de**