PLATTFORM INDUSTRIE4.0

WORKING PAPER

Technical Overview:
Secure cross-company communication

Imprint

Published by
Federal Ministry for Economic Affairs and Energy (BMWi)
Public Relations
10119 Berlin
www.bmwi.de

Text and editing
Plattform Industrie 4.0
Bertolt-Brecht-Platz 3
10117 Berlin

Design and production
PRpetuum GmbH, Munich

Status
April 2016

Illustrations
MaximP – Shutterstock (title); BillionPhotos.com – Fotolia (p. 6, p. 8); GKSD – Fotolia (p. 11); sdecoret – Fotolia (p. 16); Artur Marciniec – Fotolia (p. 19); Syda Productions – Fotolia (p. 20)

Zertifikat seit 2002
audit berufundfamilie

The Federal Ministry for Economic Affairs and Energy was awarded the audit berufundfamilie® for its family-friendly staff policy. The certificate is granted by berufundfamilie gGmbH, an initiative of the Hertie Foundation.

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

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

Contents

1. Introduction

The aim of this paper is to formulate a common position about the basic requirements, security challenges and different approaches for secure communication in Industrie 4.0 environments, which specifically addresses the needs of cross-company value networks.

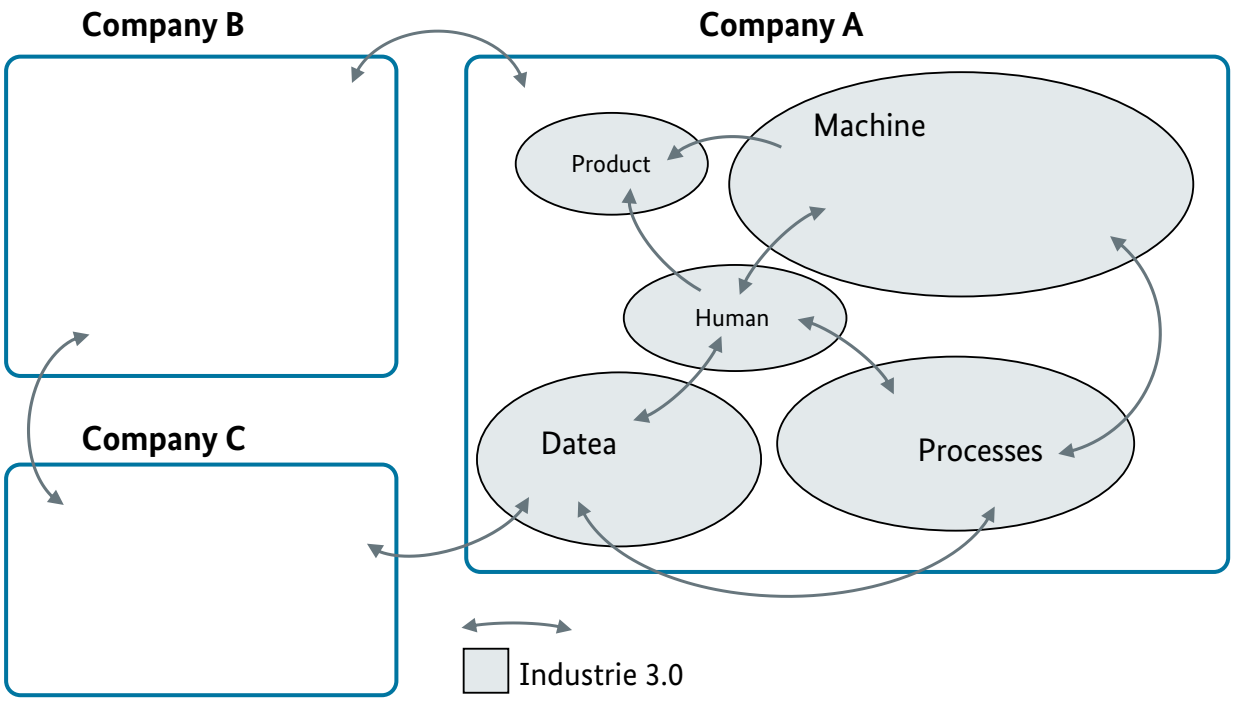
The contents are deliberately outlined in general terms to ensure transferability. Any detailed security consideration must necessarily focus on the individual case in order to take account of the relevant circumstances. For this reason, the paper does not describe specific projects or implementation details.

The document is aimed at decision-makers and users in the Industrie 4.0 context. It illustrates the essential framework conditions, guiding principles and lessons learned that are relevant to security in this area.

1.1 Current situation in the Industrie 3.0 model

Many aspects of Industrie 4.0, the "fourth industrial revolution", are already reflected in the latest technological developments or will emerge as the next advance in existing technologies. In automation technology, proprietary bus systems have already been largely replaced by Ethernet and Internet protocols. Automated communication between companies usually takes place at a small number of interfaces: While communication as far as the automation level has become standard in some areas, for example, for remote maintenance, it has not yet been accepted in many other areas due to security concerns, among other reasons. Communication links that are established without trust in the relevant communication partner therefore fail to harness the full technical potential; see Figure1.

Figure 1: Communication links and trust relationships in Industrie 3.0



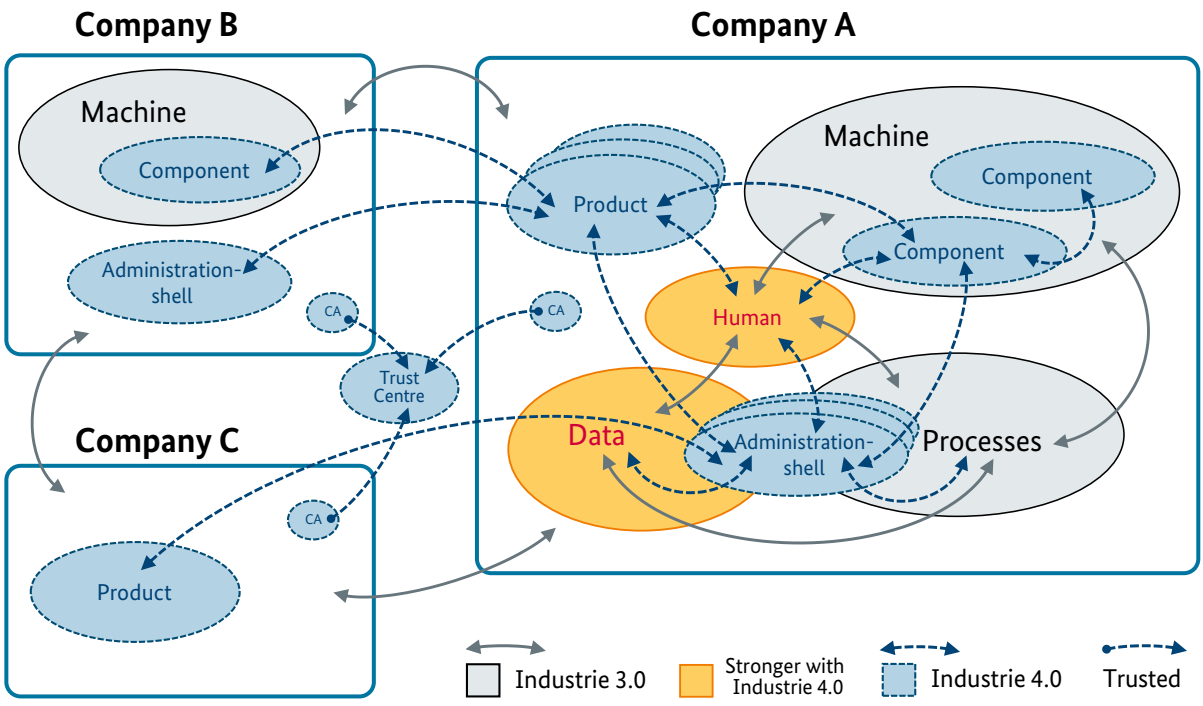
Source: Plattform Industrie 4.0

1.2 What's new in Industrie 4.0?

For Industrie 4.0 to become a reality, agile communication links that bridge company boundaries are required. To achieve order-controlled production in lot size 1, essential data is provided "just-in-time" from a decentralised source, rather than being stored in centralised systems for long periods in advance. Readiness for electronic interaction at all times is essential for participation in marketplace concepts and dynamic value networks. This imposes additional requirements on the security of communication links in terms of confidentiality, integrity and availability.

For successful information exchange, there must be trust in the security of the communication link, and in the secure processing of information by the relevant communication partner. Aside from the technical aspects, this depends on the relevant partners having a firmly embedded, reliable and measurable approach to operational security – based on an Information Security Management System ISMS, for example; see (1).

Figure 2: Communication links and trust relationships in Industrie 4.0



Source: Plattform Industrie 4.0

2. Communication

Communication *(from the Latin commūnicāre, meaning "to share") can be understood as the exchange or transfer of information.*

A single, uniform definition of communication does not exist. Communication studies is an academic discipline within the social sciences and arts that deals with processes of human communication. This document considers communication as a technical process.

2.1 Secure communication as core issue

2.1.1 Growing importance of communication

'Industrie 4.0' is a collective term embracing the wave of opportunities created as a result of advances in hardware and software. A key driver of this new wave is that data and information must be made available for processing. In Industrie 3.0, this process usually occurs at a local level, for example, by means of communication links to sensors and actuators within a plant. At the company level, Manufacturing Execution Systems (MES) or an overlying Enterprise Resource Planning Systems (ERP) are used for communication. Operating and quality data are recorded in the appropriate systems.

In future scenarios, the direct exchange of data and information across company boundaries will open up new opportunities. Both humans and machines are to be considered as communication partners in these scenarios. In addition, communication across company boundaries will no longer only occur at the management level (MES/ERP), but also at subordinate levels: for example, from a particular machine or component directly to its supplier. End-to-end connectivity will become scalable as a result of the switch to IPv6 and must also be taken into account.

2.1.2 Secure communication is essential

From a security perspective, requirements from many areas such as the protection of expertise, data and trade secrets will apply. These are always represented by the traditional security objectives (see Section 4.1) of

- Confidentiality
- Integrity and
- Availability.

Cross-company communication that bridges organisational boundaries and occur via WAN connections (Wide Area Network) places higher demands on communication confidentiality. In the context of the Industrie 4.0 business pro-

cess, ensuring the availability of data and the communication connections also plays an increasingly crucial role.

Industrie 4.0 will also map legally relevant communication, for example, as part of ordering and logistics processes. Our consideration of the subject must therefore also include secondary subordinate security objectives such as:

- Authenticity
- Non-repudiation
- Binding force and
- Accountability

(See Section 4.1).

2.2 Perspective and definitions

Secure communication links can be achieved by various technical means. This paper aims to formulate implementation requirements and strategies that will remain valid no matter how individual technologies develop. For this reason, our considerations take a higher level perspective: the Presentation layer (layer 6) and the Application layer (layer 7) in the OSI 7-layer model (see Section 11.1).

2.2.1 Communication at the Presentation layer and higher layers

Secure file transfer is an example of a confidential communication process. This system allows a file to be encrypted for a particular recipient and transferred without further ado. A file can also be transferred, even if unencrypted, via an encrypted connection between two computers. Furthermore, an unencrypted transfer between two computers is possible if the remote connection between two locations is encrypted as a Virtual Private Network (VPN). Either company-specific VPN gateways or the services of a telecommunications company can be used in this case. Each of these options has advantages and disadvantages in relation to archivability, monitoring options, scalability and other properties that need to be considered.

2.2.2 Relationship with lower layers in the communication model

The precise details of technical implementation, for example, which algorithms, key lengths or transfer technology (wireless, wired) are to be used are not considered here. These topics are being studied by other bodies working to advance the required basic technologies through specialisation and continuous updates. The Technical Guidelines of the Federal Office for Information Security (BSI) is one such example. The European Union Agency for Network and Information Security (ENISA) is another body involved in this area at European level. The American National Institute for Standards and Technology (NIST) provides guidance on many of the technologies used internationally in the area of cryptography. The Internet Engineering Task Force (IETF) defines Internet protocol standards, while the European Telecommunications Standards Institute (ETSI) and the International Telegraph Union (ITU) develop technical standards in the field of telecommunications.

Industrie 4.0 applications are likely to impose particular requirements on these basic technologies, for example in the area of quality of service. These requirements are the subject of discussions surrounding the Reference Architecture Model for Industrie 4.0; see (2).

2.3 Effects on organisations

Businesses wishing to participate in cross-company value networks will have to further adapt their organisational processes in line with the business model. Simply implementing technical solutions in IT security is not enough: the solutions must be accompanied by appropriate organisational measures. In order to build trust, security standards must be evaluated according to the maturity level of IT security based on, for example, the Capability Maturity Model Integration (CMMI).

Small and medium-sized business must be supported by appropriate standards to achieve this goal. Larger business will also need to develop their Information Security Management Systems (ISMS) accordingly.

3. Objectives and benefits of secure communication

The diverse array of value networks linking companies in the Industrie 4.0 environment facilitates the emergence of new business fields and production processes. Data exchange between different companies generally occurs via the Internet, which makes Industrie 4.0 processes more vulnerable to attack. For this reason, there needs to be a particular focus on secure communication that crosses company boundaries. The aim of secure communication is to develop a high level of trust in the security of new Industrie 4.0 processes and thus eliminate any concerns and obstacles in this area that might hinder their progress. Protecting vital company assets is the chief priority here.

The benefit of secure communication is that it provides the basis for enabling secure operation of Industrie 4.0 scenarios. Secure communication in Germany and Europe can increase acceptance of these scenarios and generate or maintain momentum for Industrie 4.0, thus allowing innovations emerging in this new era of smart manufacturing to thrive in the long term. Since communication security will in future be an immediate and integral part of scenarios, it will be easier for manufacturing companies to take part in and shape new production processes, because the communication participants (machines, for example) will already meet minimum security standards. Furthermore, integrated communication security within Industrie 4.0 will be a selling point for machinery manufacturers: initially as an important 'future-proofing' feature of the machine but also ultimately as a general, essential characteristic of all production machines. In future, it will be difficult or impossible to sell any machines lacking this characteristic.

3.1 Protecting vital company assets

Industrie 4.0 increases the need for electronic communication that goes beyond existing company boundaries. To achieve targeted investment in security, company assets requiring protection must be identified (for example, formulae, procedural parameters, process-related quality assurance methods). All valuable information has a so-called 'protection requirement', which must be met by appropriate measures in each case. This protection requirement must be reliably safeguarded throughout the entire Industrie 4.0 process, depending on the way task sharing is planned, to ensure that each company can rely on confidential treatment and protection of its own assets in the communication process with other companies. The more accurately that companies can identify risks to their own assets, the more efficiently that security objectives can be planned and implemented. Based on these objectives, it is possible to draw up minimum requirements for internal and cross-company security measures as early as the investment planning stage.

4. Secure communication channels

4.1 Introduction

The communication channels normally used in the Industrie 4.0 environment vary, depending on the communication partner. In **Human-to-Human communication**, no other electronic data processing takes place, apart from the transfer of messages (for example by telephone or e-mail).

In **Human-to-Machine communication**, a person controls the operation of a machine. In this case, electronic data processing occurs at the interface between the human and machine. In **Machine-to-Machine (M2M) communication**, one machine controls the operation of other machines, in order to implement automation across a number of machines for example. In this case, data processing occurs on both ends of the communication. There is no human intervention, or at most only in a monitoring role. The machines communicate independently with each other.

In the case of the machine-to-machine communication used intensively in the Industrie 4.0 context, steps must be taken to ensure that the communication partners are trustworthy (see Figure 2: Communication links and trust relationships in Industrie 4.0). The identity of the communication partners and the originality of the exchanged data in the communication channel must be protected. Both of these elements are exposed to risk through cyber-attacks. Trust must be negotiated between the various partners involved, taking into account the communication locations and partners.

In **local communication**, data are exchanged within one particular company location. The communication infrastructure is usually managed by an IT organisation. This organisation can technically negotiate and secure trust with the local communication partners. In **cross-location communication**, data are exchanged between different locations of a particular company. The communication infrastructure may be managed by different IT organisations within the company, if necessary. The information exchange between the locations takes place via WAN connections (Wide Area Network) supplied by telecommunication providers. In this case, the company temporarily has no control over the data traffic. It is more difficult to negotiate and secure trust in this scenario due to the various partners involved: the company lacks controls over all of the essential communication components (DNS server, for example). In **cross-company communication**, data are exchanged between different companies. In this case, the same conditions apply as for cross-location communication. In addition, the communication partner is located outside the control of the company, both in technical and organisational terms. Negotiating and securing trust is further complicated as the number of partners involved is increased.

As a rule, the following security considerations must be observed when introducing secure communication channels:

1. **Availability:** The infrastructure must be protected against an outage. For example, an attacker could try to disrupt control of a chemical plant by sabotaging the communication infrastructure and thus causing significant damage to products and facilities.

2. **Integrity:** The data must be protected against unauthorised changes. A potential attacker could try, for example, to obtain the control commands for a machine, replace these with other commands and thus trigger critical malfunctions. According to the BSI Security Report 2014, hackers used this approach to damage a blast furnace in a German steel works (3).

3. **Confidentiality:** The data must be protected against unauthorised access. Authenticating communication partners is a key challenge. How does the machine recognise that it is dealing with another particular machine and not a faked identity created by an attacker, for example, to seize sensitive data? Man-In-The-Middle scenarios, in which an attacker diverts the flow of data via an intermediate station in order to eavesdrop or manipulate data (data integrity is also concerned), are considered to be critical attacks. Authorisation is another issue closely linked to authentication. The purpose of authorisation is to grant the communication partner access to certain functions. Advanced attacks illegally open up existing access to include authorisations for critical functions.

Authentication mechanisms are used to ensure the authenticity of the communication partner or the originality of a data source. Authenticity checks are vital for ensuring confidentiality and integrity.

To allow processes to be retraced in the event of an error or attack, it is essential that messages exchanged between communication partners cannot be repudiated (non-repudiation). Protocol functions are frequently used for this purpose: they allow additional tracking and evaluation of data traffic if required. Non-repudiation is also a relevant security objective in relation to legal considerations.

The security objectives of authenticity and non-repudiation together define the term ‘binding force’. A machine verifies its authenticity to another machine by means of

authentication mechanisms and the information exchange between the two machines is recorded for the purposes of evaluation.

To allow retrospective analysis of the entire process in the event of an error or attack, proof of accountability must be ensured. If, for example, a machine produces the wrong materials, it must be possible to identify or account for the basic causes of the malfunction (use of incorrect parameters originating from a particular source, sent at a particular time by the authenticated communication partner).

Typically, the classic proactive security measures for ensuring confidentiality and integrity are as follows:

- User and identity management (authentication, authorisation). For more details, see the Technical Overview on Secure Identities (4).
- Data encryption and signatures

These two measures are used to ensure authenticity.

Availability is a core security element of IT-supported processes. In the industrial world, the availability of systems, components, network connections and data has a high priority. Standard proactive security measures for ensuring availability require additional infrastructure components (such as special hardware and software solutions and redundant configurations of the communication system).

The standard reactive security measures typically consist of security monitors/detectors, if necessary supported by automatic reactive methods that, for example, automatically block a suspicious communication partner. The events recorded by these measures allow security-related occurrences to be investigated retrospectively and thus provide valuable information on further security measures to be taken.

The security measures of binding force and non-repudiation are essential prerequisites for reactive measures.

4.2 Communication design

Maintaining cross-company connections between humans and machines in the networked world of Industrie 4.0 while observing the principles of confidentiality, integrity and availability requires a holistic approach in the form of a communication design.

In this regard, a communication design helps to identify and document the various connections required for information exchange and to meet the criticality requirements for the business process through through protective measures. It can be useful in this case to differentiate between various network statuses such as regular operation, emergency operation, maintenance mode or analysis mode. The primary goal is to maintain the communication function. This function is especially vulnerable, particularly in dynamic, cross-company networks. Differentiating between different network statuses – such as maintenance and emergency operation – makes sense because it allows early proactive detection of any strange or irregular communication behaviour. There are also advantages even in the case of a retrospective response to security incidents, since it is much easier to carry out a targeted analysis of a security incident if a communication design is available. This expedites the response procedure, especially in the case of advanced and targeted attacks. In responding to random attacks, it can be useful to minimise communication behaviour to the bare essentials in order to reduce vulnerability.

A communication design identifies the components requiring protection (asset identification, for example) and communication channels; comprises a risk assessment; classifies the components and the data exchanged; defines suitable measures for ensuring system stability (such as redundant configurations).

4.3 Availability/reliability

In the Industrie 4.0 context, Internet functions and options can be applied to real objects. The objects are linked and can communicate with each other (machine-to-machine communication). The Industrie 4.0 'order-controlled production' application scenario (see Section 11.2) presents a flexible production configuration, which deploys cross-company and cross-plant networking of production capabilities and capacities to rapidly adapt to changing market and order conditions. Secure communication is essential to make optimum use of the capabilities and capacities of the existing production facilities.

A key factor in secure communication is ensuring the **communication availability** required for this purpose. To achieve the optimum application scenario, whereby 'company-specific' production capabilities and capacities are expanded on the fly to meet the order situation, on a largely automated basis, all technical systems involved

must respond operationally with the appropriate response time and in the agreed time delay and offer availability ('Just-in-Time', 'Just-in-Sequence'). This response time is often referred to as real time in an industrial context. In the following section, the term 'application and process-compliant response time' is used as an explanatory synonym for 'real-time' to clarify the response time relationship and dependencies. Application and process-compliant response time in communication processes defines the specified period in which information must be available or transported. This can occur synchronously or asynchronously and thus 'on-demand'. However, it is imperative to ensure end-to-end synchronisation of all technical systems involved in the process for this purpose. It is therefore vital to specify important design factors for ensuring availability and reliability of a communication process from the outset, that is, as early as the design stage, and to check their effectiveness on an ongoing basis. Depending on the criticality and process chain dependency of the participants in the communication process, the technical and organisational aspects for ensuring the availability and **resilience** of the communication infrastructure must also be taken into account. Technical factors to be considered include: quality of service, bandwidth of the communication infrastructure used and requirement-specific communication properties of the participating systems, in addition to guaranteed synchronisation. To address organisational design aspects relating to the availability and reliability of secure communication, the risk of possible fault, manipulation or outage scenarios in communication processes must be evaluated and appropriate countermeasures planned. The measures drafted as a result, such as redundancy and resilience strategies, and self-recovering processes that restore function, must also be implemented in line with the assessed criticality of the process chains involved.

4.4 Safeguards

Determining when a cross-company communication process can be considered to be secure depends on the protection specifications and the information to be exchanged.

4.4.1 Classification: a continuous process

The rules on retrospective use of information, that is classification in general, generally come directly from internal company catalogues or also indirectly from existing contracts. They are defined by external regulations such as national legal frameworks or international standards and agreements. Classification is also a **regular** task – on the basis of individual evaluations carried out by information creators themselves in order to safeguard intellectual property, for example (implications under patent law and competition law). Applying consistent classification metrics

within the company will ultimately result in consistent documentation within companies. This procedure should therefore also be provided for automated processes (production data, formulae).

4.4.2 Determining the protection requirement

A risk assessment must be carried out as a first basic step to evaluate the level of protection required. It must ask: how much damage would be incurred by a company if, for example, certain types of data were stolen or manipulated or if production processes were changed in the event of a security incident?

Classifying critical company assets (systems, data sheets, plans, formulae, marketing data) is useful, or indeed indispensable, in order to weigh up the risks. This classification should specify to what extent these assets can be exchanged with others (for example, with partner companies) or are for internal access only.

A cross-company, consistent system of classification is necessary to prevent misunderstandings and ensure categorisation can be applied across different companies. A simple and consistent classification system is proposed below:

- No protective measures: **Public**
- Medium level of protection: **Confidential, for business partners (new in Industrie 4.0 scenarios)**
- High level of protection: **Confidential, for internal use**

For a detailed review of protection requirements and classifications, see Section 4.5.

4.4.3 Scope of protective measures

While established standards exist in the traditional field of IT (ISO 2700x, “BSI IT-Grundschutz” Baseline Security for IT-Systems), these only have limited applicability for production infrastructures (cf. ISO 27002 with 27019). The following overview gives an initial idea of the protection areas expected under Industrie 4.0.

Security properties of components and network entities involved: Documented security properties must be available. This is primarily the manufacturer’s responsibility. These properties must now be exchanged securely between machines and possibly also between companies, and mutually consolidated. In this context, each company must be capable of defining their minimum requirements for information exchange. The accepted security level is then agreed on the basis of these minimum requirements. The exchange and, if automated, also the negotiation must be verifiable and available for plausibility testing at all times.

Information about the security level that is desired on one hand and supported on the other between the supply and demand sides may need to be negotiated confidentially. This consideration affects companies with horizontal and vertical links, such as, for example, a machine supplier, customer, component supplier and operator. In the case of automated negotiation, confidential handling must also be clearly evident and remain verifiable for documentation purposes (see Section 4.4.4).

Resilience plays a key role in Industrie 4.0. The components involved must show resilience against human errors (indiscriminate) and sabotage (targeted). Incorrect parameter configuration of a machine should not be possible, for example. Before processing critical control commands, such as actively setting a speed parameter for a motor control unit, the components could carry out a plausibility check. The difficulty here lies in identifying the range of plausible parameters. Typically, the resilience of network components is ensured by redundant network technology, whereby a switch takes place if a route is down. The question of whether or not and in what format a redundant configuration makes economic sense must depend on the risk assessment.

If it is true that unknown, advanced and frequent targeted attacks are only identified after they have been successful (for example, Stuxnet or BlackEnergy or the cyber-attacks on Ukraine’s power grid), companies must consider continuous monitoring. At a higher security maturity level, this monitoring may be accompanied by automated correlation of security messages across system and company boundaries. The market for expert systems that identify attacks within the industrial environment is currently limited to just a few companies. Another security feature of modern network monitoring and alarm systems (SIEM) is that they can also carry out forensic analyses after an event, for example, incorrect control commands. This prevents a situation where a security breach is identified, but the process used to infiltrate the systems cannot be retraced. If it is not possible to retrace the process and thus identify the weaknesses and the attack path, we cannot assume that the attacker has been successfully eliminated. In this case, it

may be necessary to replace all components. This could result in very high costs, particularly in machine networks, far in excess of the known costs incurred in the SONY-PSN and Bundestag hacking cases.

Keeping up to date on current weaknesses and attack processes is generally recommended. This requires a register of components used, or asset database.

4.4.4 Retraceability/verifiability

The ability of a company to establish appropriate security measures is one thing. Making sure these can actually be verified is another. As a rule: Established security measures should be commensurate with risk and within the generally applied scope (see, for example, Catalogue of IT security requirements (IT-Sicherheitskatalog) (5), IT Security Law (Sicherheitsgesetz) (6)). Implementation of the security measures must be documented. This raises several challenges for companies, since the appropriate and generally applicable scope of measures depends on different factors: The particular sector occupied by the company, any existing regulatory requirements and, not least, the organisational maturity (in other words, the options available to) the company or partner company. For companies to be able to react to current threats, knowledge of publicly available, documented recent security breaches is essential.

As cross-company value creation increases, so too will the need for verifiability, for example, in the form of audits. This mainly concerns sensible preventive measures: Regular documentation can be used to establish a company's organisational capabilities. This documentation can also be useful after a security breach. Based on this documentation, proof can be provided to show that all essential risks have been adequately considered and also that the relevant processes are being observed. In addition, this accountability (depending on the maturity level) can also play an important role, for example for internal auditing: It enables a review of compliance with security measures.

The documentation comprises two areas: First, it outlines measures that describe evidence of an existing guideline/instruction. Second, it demonstrates that the steps described actually occur at regular intervals. The documentation can include both organisational and technical measures.

Balancing the conflicting goals of supporting verification and analysation on the one hand and possible encryption on the other is a particular challenge. The need to encrypt confidential communication can compromise analysis transparency. Generally speaking, encrypted data cannot be evaluated. Before using encryption technologies, companies are therefore well advised to consider the consequences, particularly for a retrospective security analysis that may be carried out under limited circumstances. It is also important to remember: Deciding on the correct balance between encryption and traceability should be made as part of an overall risk evaluation.

4.5 Protection requirement and classification of critical company assets

4.5.1 Determining the level of protection

Determining the level of protection is a basic measure. It can be done by carrying out a risk assessment. The key question here is to establish which security incidents are possible and likely, whether security requirements are specified and applicable, and if so, which ones. The responsible department and the data and service owners must be involved in assessing the scope of protection. In this process, the classification of data and services should have an impact on the type and scope of protective measures.

4.5.2 Classification of the critical company assets

The classification of documents and production data is based on an assessment of the specific protection requirement for each type of information based on the previously mentioned regulations (see Section 4.4.2). A basic distinction at least between the categories 'Confidential' and 'Public' should be possible. 'Public' in this context means data that is open to unlimited public access (for example, product data sheet, manual, marketing information). It could and should be possible, by definition, to make this data open to all (open data). In this case, the category 'Confidential' should be further subdivided (for example, into 'normal', 'high', 'very high' according to BSI Baseline Security for IT Systems). Further tree method classification into **Protection requirement categories** should be possible (for example, role-based access rights for development departments, production teams A, B, C, senior management).

This type of classification is primarily designed to achieve verifiable and consistent implementation of the protection requirement level **within** a company, and thus provide a basis for the next step: **cross**-company communication that complies with protection requirements.

4.5.3 Cross-company classifications

From the listed classification requirements for **internal company** information, it is immediately obvious that the catalogue system, on the basis of a secure, identified, **cross**-company communication process, must be known to all participants within the communication network. These catalogues must therefore be negotiated in advance by the parties involved. If the classifications are rigorously adhered to, there should be no room left for interpretation. They must therefore be semantically unambiguous. The rules against transferring between different categories that have already been set appropriately must be complied with in order to prevent any unintentional or subversive switching of information to another protection requirement category. A popular measure for maintaining this type of compliance with security objectives is based on using 'Digital Rights Management Technologies' (DRM). The rules against saving data outside relevant business processes must be strictly observed. Completing consistent and appropriate classifications and complying with requirements within the processes is considered to be a regular task.

4.5.4 Coexistence of protection requirement categories 'Public' and 'Confidential' and new opportunities

Information that is already classified as 'Public', for example by Creative Commons licences, and is publicly accessible has already had an impact on the market and acquired increasing importance. It has assumed its fixed position **beside information** that has been classified as 'Confidential' and can appear in shared production processes. Implementing a **universal** strategy for information classification therefore provides a sound basis for future automated production.

4.5.5 Protection requirement based on example of point-to-point connection between two machines

The aim of achieving 'autonomous and automated networking of production capabilities beyond individual factory boundaries in order to optimise the portfolio with regard to customer and market requirements' will place a particular focus on increasing forms of communication that can ensure robust, professional processes and protect intellectual property during information classification (IP). In the future, a new protection requirement will be assigned to the point-to-point communication of autonomous machine-to-machine communication.

With 'I4.0 degree of automation' and 'I4.0 Readiness' already available to protect a point-to-point communication, we now need practical and sustainable business processes that can also be implemented in a simple format as 'on-demand production processes' without any particular protection requirement. This must be possible, rather than having to master the entire complex model at the very outset. Market practices are based on extended trust models, which also take account of an increased protection requirement. For example, methods for communicating publicly identifiable rankings are a possible option, based on experiences with the manufacturers involved.

4.5.6 Extended forms of communication

In theory, there are no limits to communication within the Industrie 4.0 environment. This means that today's companies may evolve into other enterprise types equipped with new forms of communication. Autonomous machine-to-machine communication is not necessarily restricted to an autonomous point-to-point connection between two machines in different companies. This communication can form any part of future wallet-driven solutions, which search for, negotiate, execute and complete job orders entirely autonomously, based on the same principle used by existing solutions on the financial market. This approach makes another Industrie 4.0 objective feasible: automatic production capacity control for customised standard products.

Many of the consequences of fully autonomous, algorithmic business processes are already known from the relevant trading platforms on financial markets. Future extended forms of communication for Industrie 4.0 must therefore be accompanied by appropriate security measures that address all levels of the new communication processes and allow secure execution, especially at the technical, business and legal levels. If Industrie 4.0 is also to meet **security-related** requirements against cyber-attacks, it makes sense to introduce the model gradually while taking account of relevant security guidelines.

4.5.7 New protection requirement

Security measures require a risk-focused treatment of information to work effectively. The scope of protective measures should be based on whether or not certain data or a service requires protection. Simply assuming that 'everything requires protection' is not advised. This kind

of approach is likely to diminish competitiveness because of the costs involved. It is important not to define too many different categories, particularly at the introductory stage, to keep measures manageable. Access to information should always be on a 'need-to-know' basis: A good reason, which is plausible and verifiable in the business context, must be provided before data and services are released. The following section describes three categories that could suffice in an initial review of an organisation: two from the 'Confidential' category and the 'Public' category:

4.5.7.1 Confidential, for internal use

Highest protection category: Data or services may only be shared within the company itself and must not go outside the company. Examples include confidential formulae or unpublished patents.

4.5.7.2 Confidential, for business partners

Medium protection category: The exchange of information across companies is a fundamental part of Industrie 4.0. Proper handling of business information and documentation of the correct processes involved is essential. This applies, for example, to the automatic exchange of production information and alloys.

In the field of machine manufacturing, it is usual practice to reduce the risk of losing sensitive data through distribution across several service providers.

For this category, relevant data for the application scenario comprises, for example, confidential production steps and production capacities, and in particular, the security properties of components and entities involved (for example, the factory where the components are physically located).

4.5.7.3 Public

Confidentiality is not a requirement in this case. Either the information and services do not require protection or they have deliberately been made publicly available. Examples include machine movement data or sensor data, if publication of this data is not critical.

5. Communication partners

5.1 Agile communication between security domains

Agile communication means that clear security specifications are available before communication is established and these are accepted and understood by the communication partners. Flexible exchange of control and plant data without red tape is only possible under these circumstances. Agile communication thus does not mean communicating without connection security. A procedure without connection security would not last long in any network: it would openly invite the abuse of sensitive control and plant data.

The identification and authentication of communication partners (production plants) is therefore a fundamental requirement of security domains. Communication should only be established with identified users/plants/components, in order to generate the trust required for exchanging control and plant data. Logical groupings of communication channels (conduits) are used for the communication. These conduits connect two or more zones or domains with shared IT security requirements.

5.2 Identification

The parties involved must identify themselves at the start of a communication process. In existing Industrie 3.0 systems, this identification only occurs via address information, for example, via the IP address of a component. In some cases, users are not identified at all because no system of access control has been implemented or because access data is publicly available.

For Industrie 4.0, secure identification of the parties involved is essential. This process must be designed to meet the security requirements; see Section 3.1. Further discussion of secure identities is provided in the relevant Technical Overview (4).

5.2.1 Addressability of communication partners

Addressability is one of the major challenges in identification of communication partners. Each entity can have several identities, which may be added or changed over the lifecycle. In relation to addressability and cross-company communication, the particular role currently assumed by an entity is often relevant. For addressing purposes, mapping of the currently relevant identity must be supported.

For example: For a mechanical engineer addressing a machine, the identity from a manufacturer's view (e.g. the series number) is most likely to be important. The operator is more likely to identify the machine by its current installation site or purpose.

In the Industrie 4.0 environment, appropriate addressing could occur by means of the administrative shells (1), which can comprise this information over various lifecycles. Aside from the pure administration of information, secure integration of identity checks must also be provided in the connection negotiation. This can be achieved in different ways:

- The addressing process takes place by means of the administrative shell, whereby the desired identity is mapped onto the secure identity that is stored to the entity. In this case, it is vital that the mapping function using the administrative shell is at least as secure as the identity on the entity.

- The addressing process takes place using the administrative shell, whereby the desired identity is also securely

stored to the entity. While negotiating the connection, the communication partners each carry out 'End-to-End' checks to verify if their counterparts meet the reciprocal security profile and identity requirements (see Section 5.2.3).

These requirements should be taken into account from the ground up, that is, from the design stage of the communication mechanisms ('Security-by-Design'). Retrospectively ensuring compliance is practically impossible, as briefly outlined in the Annex11.3 (example of e-mail communication).

It is therefore necessary to ensure that the protocol for negotiating the communication link between the parties involved also transfers details about which identity is to be addressed. The Transportation Layer Security (TLS) protocol currently in widespread use provides these details with the 'Server Name Indication' extension up to one particular point. More complex identity requirements must be incorporated into the semantics during negotiation of communication links (see Section 5.2.3). All relevant properties and necessary data, such as a digital certificate to confirm identity, are features of an Industrie 4.0 component and thus represented in the administrative shell.

5.2.2 Different rights and roles

The rights and roles model reflects expectations of the communication partner's identity. Even when technical connections are established between individuals or machines, the roles and associated rights are crucial.

Role-Based Access Control (RBAC) is of particular interest here. Under this approach, users identify themselves with their credentials (usually a user name and password) and are then authenticated. A permission management system authorises users to carry out further actions in accordance with their particular roles. In the case of cross-company access, there is now the added complication that both the authentication mentioned and the rights management must be agreed between the companies and implemented in line with necessary security measures.

The cross-company, dynamic value networks that are part of Industrie 4.0 require a greater understanding of rights and roles. If Industrie 4.0 components are to carry out business transactions autonomously across company boundaries, standardised specifications must also be agreed for these components. Within companies, value limit guidelines are usually used to determine the permissible options for components. In a cross-company context, it will need to be clarified whether the legally binding force that can apply for people, for example, through full commercial authority, is transferable to machines.

5.2.3 Security profile

During negotiation of the communication link, the properties of an entity include not only the relevant identity but also the partner's security profile. This security profile, which is a requirement for all Industrie 4.0 components, describes the security features (certified if necessary) and covers properties such as a company's own protection requirement, for example, in the case of an item of information, or the available protection mechanisms and evaluation of these mechanisms. During the negotiation process in Industrie 4.0 communication, the relevant requirements profile and the available security properties are compared and the information exchange is either terminated, or continued at a reduced or full level, depending on the security level reached. Besides the individual Industrie 4.0 components, the operating environment must also be taken into account in this process.

The following examples are provided to illustrate this concept:

- Within a variant of order-controlled production that is still supplier-dependent, you want to transfer data to just one machine, provided this was supplied by machine builder X and is being operated by asset owner Y.

- In a more flexible variant of order-controlled production, you want to transfer data to one machine only. This machine guarantees information confidentiality according to protection level Z in compliance with a standard ABCDE type examination and is installed at the site of an asset owner with highly mature IT security.

The technical execution of this task is extremely challenging. The integrity of the communication partner must be ensured in line with security guidelines and classification. It is not enough, for example, to evaluate the security profile. It must also be implemented to ensure that it corresponds to the actual system status, that is, that a device has not been compromised. This implementation could ultimately comprise the physical protection of the device,

which must be provided either by installing it in a trusted environment (organisation), or through regular checks on integrity (process) or technical measures (for example, automatic deletion if the device is opened).

The security features of Industrie 4.0 components are currently being drafted, but were not available before the publication of this document.

5.2.4 Security domains

A security domain refers to an area where uniform security administration or security guidelines are applicable. In the context of cross-company communication, information exchange occurs between different security domains: the addressing process and rights management therefore takes place using security profiles that have been agreed between the communication partners (see Sections 5.2.2 and 5.2.3). In the context of business connections that have been negotiated on an agile basis, this process will not be possible without standardisation, even if contractual freedom allows certain options in individual cases.

5.2.5 Life cycle

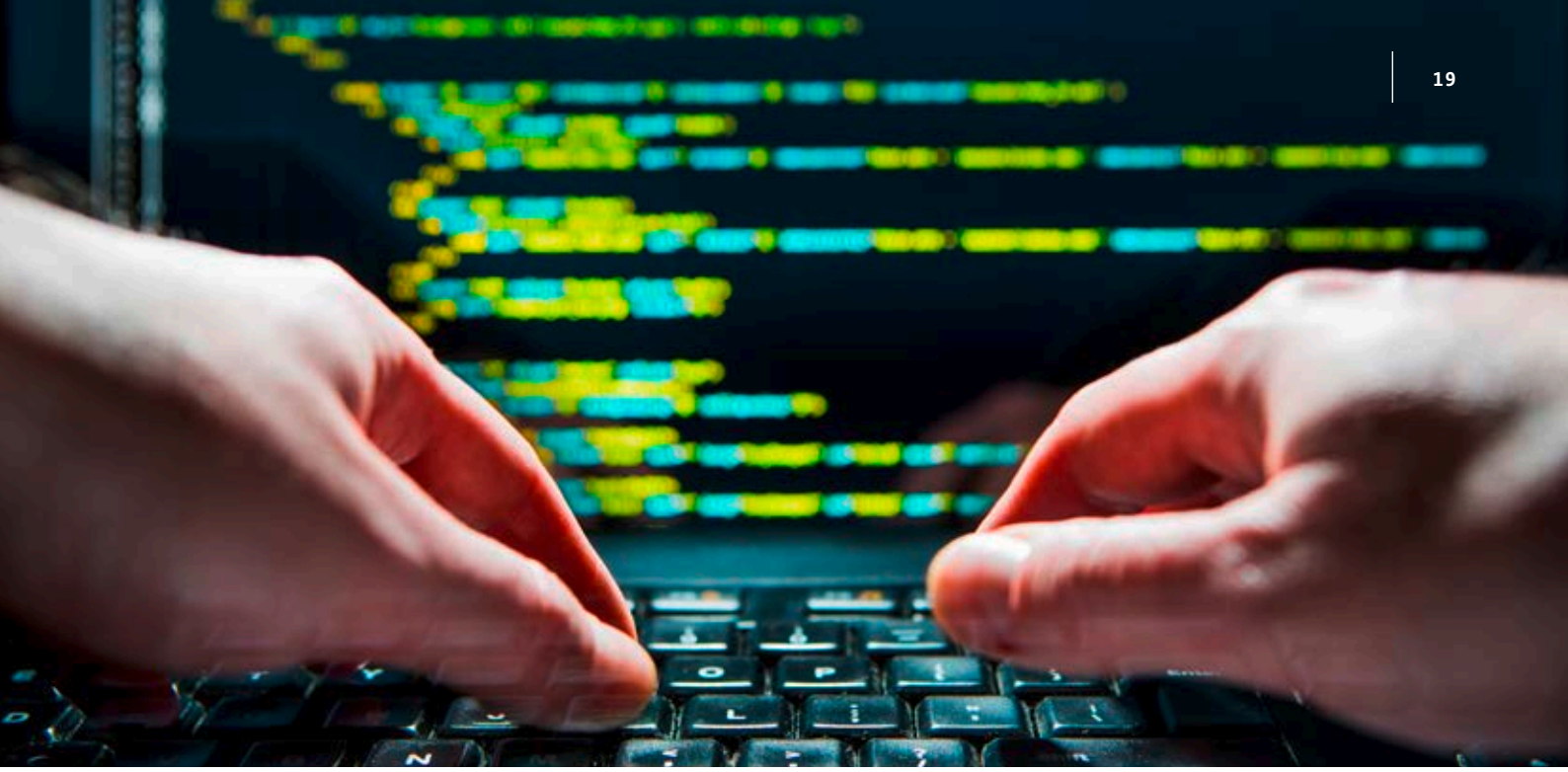
Industrie 4.0 components have features that change over their lifecycle. This results in changing identities or security profiles, for example. In addition to commissioning with an initial configuration and set of parameters, normal operation must also be supported, along with exchange and decommissioning.

In the agile production facilities of Industrie 4.0, the tasks of an Industrie 4.0 component can change rapidly. The addressing process plays an essential role in this regard; see Section 5.2.1. The life cycle of identities is described in the Technical Overview Secure Identities (4) in the section on Identity Management.

5.2.6 Semantic entities

Productive Industrie 4.0 scenarios are subject to continuous change. For example, new production steps can be introduced with the help of additional machines, production machines need to be switched or temporarily replaced because they are faulty or written off. Maintaining a resilient production process presents a challenge. It must continue to run or only be subject to short interruptions, despite or indeed in view of the necessary security considerations. A quick exchange of production machines therefore entails fully automated establishment of security attributes and the integration of these attributes in the relevant scenario.

Semantic entities are a useful means of simplifying the life-cycle management of the production process. A semantic entity essentially comprises a semantically interpretable name for the machine or production step (e.g. shoe sole gluing machine) and its assigned technical parameters (e.g. IP address, MAC address, machine number, plant, position, row, etc.). The semantically interpretable name is used for complete addressing of the machine at the time of setup and also during the production process. If a machine is replaced and a replacement machine added, the existing semantic name is adopted and new, currently active technical parameters assigned. In this way, the production process and the relevant semantic entities remain stable, highly flexible and easy to manage, even in the event of major modifications.



6. Selected legal considerations

The selected general comments here are intended to highlight that existing legal requirements will still need to be considered in the future. Further considerations and discussions on liability or binding force (see Section 5.2.2) in the area of machine-to-machine communication are dealt with in the Plattform Industrie 4.0 working group on the legal framework.

- **Data protection**
  The German Data Protection Law, which is valid until 2018, can apply in the area of Industrie 4.0, even if 'only' machine-to-machine communication is executed. The relevant protection requirement, such as confidentiality, must continue to be observed during the autonomous exchange of personal data between machines. As of 2018, the European General Data Protection Regulation will apply the new stipulations, incorporating national amendments – in connection with the applicable national law of the member states in each and all cases. However, in the main, the regulation will reflect the current legislative situation. For Industrie 4.0 production processes that bridge country borders, the relevant national amendments will apply, in addition to the European General Data Protection Regulation.

- **Competition law**
  Implementing security technologies for secure communication and secure identities for Industrie 4.0 opens up a wide range of options for competitive restrictions through technological and organisational means. For example, it is possible for **sector-specific trust services** that provide certain manufacturers or suppliers with the required 'clearance certificates' in the form of electronic certificates for trusted communication to intervene directly in the market, by revoking or denying certificates. The current sector-specific best-practice solutions focus on mature trust models, which should be implemented in future Industrie 4.0 trust models in a non-discriminatory manner.

- **Sabotage protection**
  In general, subversive technologies are used to effect deliberate competition restrictions. It is important to recognise and prevent these technologies. For this reason, technical procedures are normally used to protect communication with the minimum economic impact. However, these procedures must also be subject to legal considerations. The extent to which security agencies should be involved in relation to the technologies and communication solutions used must therefore be decided on a case-by-case basis. Furthermore, Industrie 4.0 is also an area that can be relevant for security from a national perspective. It certainly concerns the providers of the critical infrastructure integrated in Industrie 4.0 processes.

7. Recommended actions

Based on the above points, certain recommendations can be made on integrating secure communication processes in the Industrie 4.0 vision, as it is introduced.

7.1 Reliable communication channels

The agile construction of value networks and implementation of services using private and public cloud infrastructures are essential elements of Industrie 4.0. Companies must have access to reliable Internet connections if they are to participate. The necessary bandwidth must be available not only on paper but guaranteed in practice. Availability commitments must be feasible; see Section 4.3.

7.2 Secure identities

The basis of all secure communication processes is the secure identification of communication partners and the secure negotiation of security profiles; see Section 5.2. The Technical Overview Secure Identities (4) discusses requirements and technical concepts.

7.3 Negotiation of security profiles

Ensuring information security is a key factor in information exchange. Communication partners must be able to exchange their security profiles for this purpose while the communication link is established. This factor must be taken into account in the communication protocols; see Section 5.2.3. The security profile will be an essential feature of an Industrie 4.0 component.

7.4 Technical support for information classification

Information that is exchanged between communication partners must be categorised according to a classification system; see Section 4.5. In automated information exchange within the Industrie 4.0 environment, the classification system must be technically supported: it must not only be represented in the information itself (a document, for example), but also in the related administrative shell. Digital rights management (DRM) plays a role in the technical implementation of the protection; see Section 4.5.3.

8. Summary and outlook

This document reflects the interim results compiled by the Plattform Industrie 4.0 'Security of networked systems' working group for the Hanover Trade Fair 2016. Drawing on the company assets requiring protection, it presents secure cross-company communication links and proposes initial recommendations for action.

The task is ongoing, with the aim of further expanding and deepening the knowledge to hand. Work is also underway on additional topics such as monitoring of the information flow and subsequently developing urgent measures in response to security incidents.

9. Table of figures

10. Bibliography

1. *Umsetzungsstrategie Industrie 4.0*. Berlin/Frankfurt: Plattform Industrie 4.0, 2015.

2. *Reference Architecture Model for Industrie 4.0* (RAMI4.0). DIN SPEC 91345.

3. *The State of IT Security in Germany 2014*. Bonn: BSI, 2014.

4. *"Secure identities" Technical Overview.* Berlin: Plattform Industrie 4.0, 2016.

5. *Catalogue of IT security requirements (IT-Sicherheitskatalog) under Section 11 (1a) of the Energy Industry Act.* Bonn: Federal Network Agency, 2015.

6. *IT Security Law 2015.* (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme).

7. *REGULATION (EU) No. 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL* of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. eIDAS Regulation.

11. Annex

11.1 OSI 7-layer model

The OSI 7-layer model describes the different levels to which a successful communication process between applications is subject. Different technical implementations are available for each specific layer and relevant for that layer only. This enables an application to communicate over short or long distances, via either a wired or wireless connection, without the need for technical details.

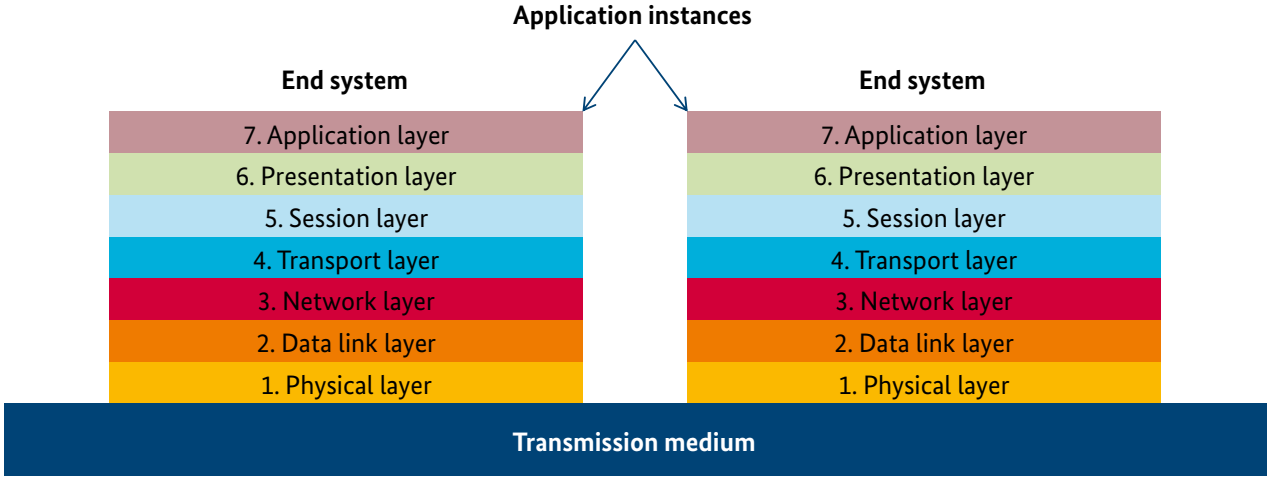
11.2 Application scenario S1 of Plattform Industrie 4.0: Order-controlled production

The Plattform Industrie 4.0 working group on research has formulated several application scenarios to assist the evaluation of requirements and solutions for Industrie 4.0. The 'Order-controlled production' application scenario was used in the work on 'Secure cross-company communication'.

Order-controlled production is essentially based on standardised process steps and the ability of the production facilities to describe their own capabilities. Through standardisation, it is possible to connect digital product development with automated order planning, placement and control in order to integrate all necessary production steps and production facilities. This type of networked control allows internal process modules to be combined in a much more flexible way. Secure (trusted) interfaces can also be used, in line with timing and quality requirements, to incorporate services (from partners) in the production. If production bottlenecks occur, the free production capacity of other companies can be used in order to boost production capacity temporarily. Suppliers are provided with the transport intelligence (direct control information from production and weather services) to enable them to decide which type of logistics (rail, road or air, for example, by drone) is required to meet delivery deadlines.

The aim is to facilitate targeted, more effective and independent integration of external production facilities and partners in the production sequence. The required order placement can largely be automated through standardised interfaces and trust relationships. Manufacturing companies thus focus purely on the value creation steps that allow them to set themselves apart from market competitors.

Figure 3: OSI 7-layer model



For the purposes of this document, only the top layers are relevant.

Source: Plattform Industrie 4.0

11.3 Secure communication between mail servers

The exchange of e-mails between mail servers is described, as an example of poorly designed agile communication. When e-mail exchange via the Internet was developed in the 1980s, secure communication was not yet a concern.

If you want to send an e-mail from one domain to another, the relevant mail server (Mail Exchange MX) is determined by the Domain Name Service (DNS) and the e-mail is sent to the named mail server, which either forwards the e-mail or delivers it directly.

A secure version of this process can encrypt the transfer between the mail servers, as described in RFC2487, which covers the use of Transportation Layer Security (TLS) for the Simple Mail Transfer Protocol (SMTP). However, this theory could never be implemented in practice, since the protocol did not include a method with a feature for checking whether the receiving mail server was authorised to receive the e-mail while the connection was being established. The support of multiple identities in the TLS protocol is also not optimal. In practice, the STARTTLS extension was only used for secure access from the client to the uniquely configured mail server. To solve this problem, DNS-Based Authentication of Named Entities (DANE) for SMTP with RFC7672 was published 15 years later, a protocol that additionally requires secure DNS (DNSSEC).

AUTHORS OF THE WORKING GROUP ON THE SECURITY OF NETWORKED SYSTEMS:

Ulf Feger, HUAWEI TECHNOLOGIES Deutschland GmbH | Dr. Lutz Jänicke (Management Board), PHOENIX CONTACT Cyber Security AG | Michael Jochem, Bosch Rexroth AG | Marcel Kisch, IBM Deutschland GmbH | Michael Krammel, Koramis GmbH | Jens Mehrfeld, Federal Office for Information Security (BSI) | Torsten Nitschke, PHOENIX CONTACT Software GmbH | Michael Sandner, Volkswagen AG | Dr. Michael Schmitt, SAP SE | Andreas Teuscher, SICK AG | Thomas Walloschke, Fujitsu Technology Solutions GmbH

This publication is a result of the work of the Working Group on the Security of Networked Systems (Plattform Industrie 4.0).

www.plattform-i40.de