PLATTFORM INDUSTRIE 4.0

DISCUSSION PAPER

Secure Communication for Industrie 4.0

Imprint

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

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

Design and production
PRpetuum GmbH, Munich

Last updated
November 2016

Picture credits
Mimi Potter – Fotolia (Title)

This brochure is published as part of the public relations work of the Federal Ministry for Economic Affairs and Energy. It is distributed free of charge and is not intended for sale. The distribution of this brochure at campaign events or at information stands run by political parties is prohibited, and political party-related information or advertising shall not be inserted in, printed on, or affixed to this publication.

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

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

Content

List of figures

Introduction

With innovative ideas and approaches, Industrie 4.0 finds brand new ways of cooperation – especially also at technical level. Plant, machinery and products interact, exchange data and keep in constant communication with each other. It makes no difference whether a machine is communicating with another on the same shopfloor or with an installation in a factory on the other side of the world. This can only work, though, if technical communication mechanisms ensure that Industrie 4.0 components can come into secure and interoperable contact with each other.

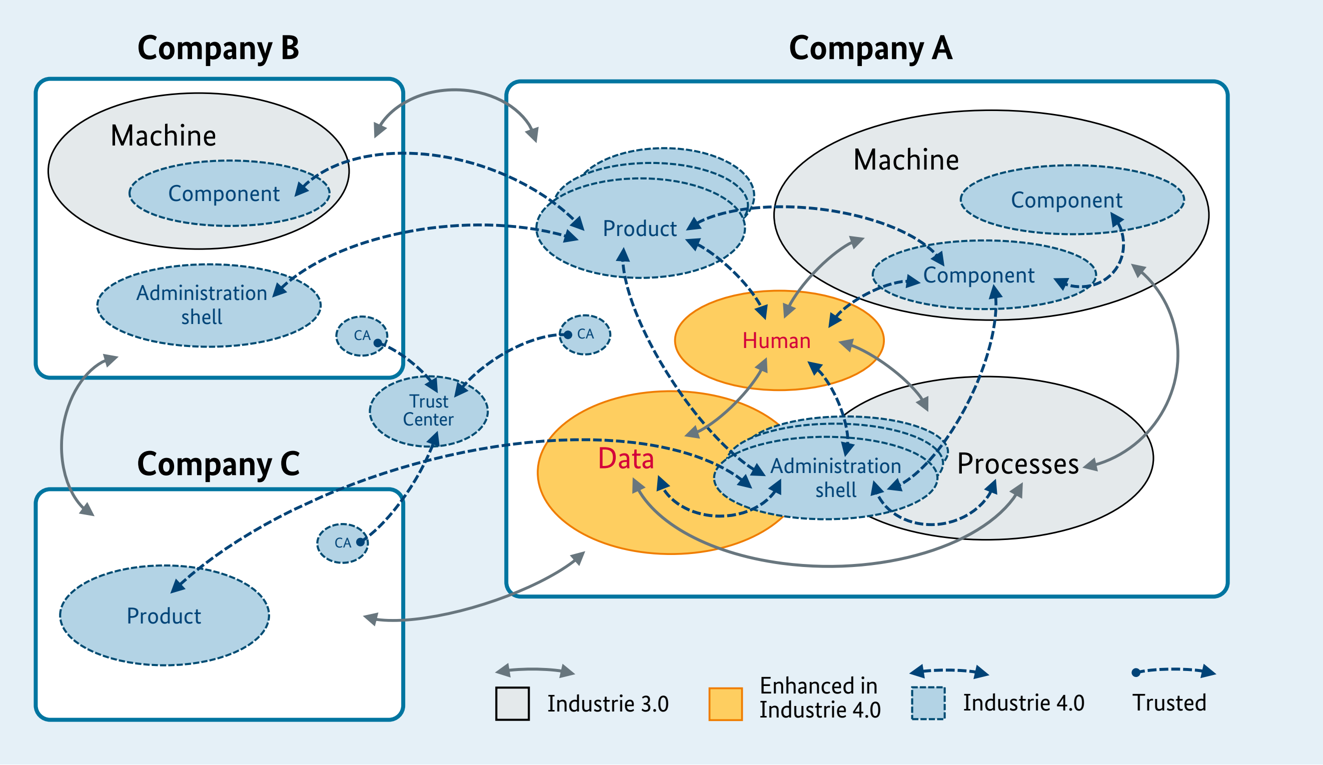
The present paper will discuss this kind of Industrie 4.0-compliant communication, with a clear focus on the technical aspects of secure communication, mostly ignoring organisational requirements. It is aimed at Industrie 4.0 decision-makers and operators and besides the general framework and guiding principles will provide them with information on some examples of practical findings gained in Industrie 4.0 communication that meet requirements for secure IT infrastructure.

What’s new about Industrie 4.0?

While in Industry 3.0 automation components, such as sensors, mostly communicate in-company, i.e. within the in-house security domain, in Industrie 4.0 they interact beyond corporate boundaries (1) (Figure 1). Here, communication relationships must enable all participants to exchange information or provide services. Services are, for example, actions such as: ‘Please measure the temperature’ or ‘Move the carriage ten centimetres forward.’ An end-to-end network connection is not, however, essential for this.

Communication has to meet two essential requirements: functionality and security. This is exactly what the present document will look at: How must communication be designed to function and to be secure? We shall consider the officefloor (information technology – IT) and the shopfloor (operations technology – OT). Officefloor security ensures the performance of corporate tasks and its primary concern has so far been with data protection. The shopfloor in contrast encompasses automation tasks where the prime focus is on real-time capability and availability in commu-

Figure 1: Communication relationships in Industrie 4.0



nication; because: no communication = no production. In Industrie 4.0, there is an increasingly close interaction and convergence between these two floors. Apart from the current security requirements for both, Industrie 4.0 makes other specific demands, because communication is increasingly taking place in automated mode and at intercompany level (Figure 2).

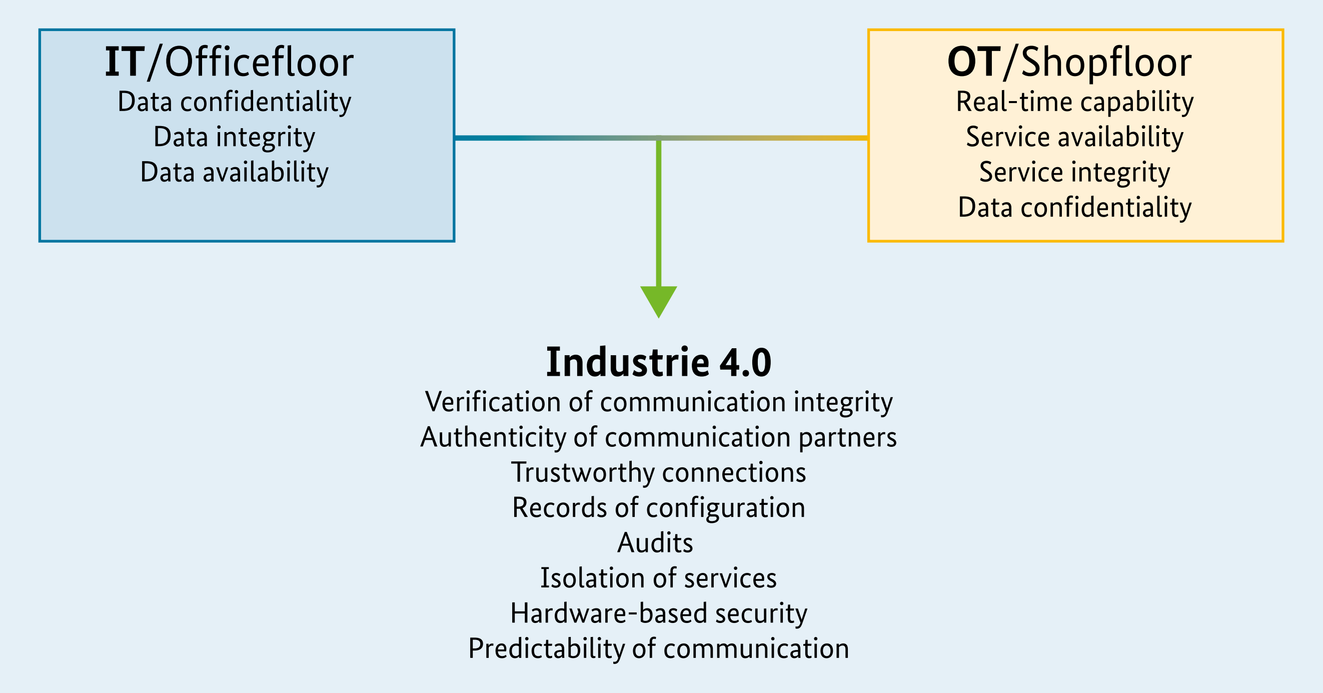
Challenges

How communication is designed among various firms, nations and continents is therefore coming to be a critical success factor: Secure, trustworthy technical processes and protocol structures in connected services enabled by networks (e.g. preventive maintenance) play a key role. Important in this connection are new national influences exerted by individual trade partners on technical security and trust rules: Some countries prohibit encryption, for example. To implement global end-to-end security solutions, trust relationships need to be redefined and participants must be able to identify and handle these in a transparent way. Existing communication technologies are being upgraded into a global industrial trust model. All sides must be taken into account here: the security needs of industrial partners and national requirements.

The challenge facing secure Industrie 4.0 communication is to find solutions on the one hand that are based on trustworthy standards and conform in the long term with statutory norms and on the other are sufficiently flexible to support industry with its new business models. That is why it is important to regularly monitor and deal with new avenues of attack.

In addition to this, the development of machine-to-machine communication (M2M) will in future be based on globally recognised and consistent security concepts. For this, components rated as trustworthy are assigned defined identifiers, so that other plant or machinery in the production and value chains can identify them as suitable and secure. These identifiers verify that components meet behavioural requirements and communication can and should then take place. In secure and highly-available communications infrastructures, they will therefore lay a major foundation for future business continuity for companies, because they will ensure their economic sustainability. Separate initiatives by individual nations are risky: They could lead to isolation and prevent participation in global, highly automated value chains and value-added services.

Figure 2: Closer cooperation between office and shop floors



How can we meet this challenge?

Ideally, platform services make up a direct component of secure communication and can in future themselves effectively protect production data from unauthorised access or modification or establish know-how and IP protection based on trustworthy digital rights management (DRM) technologies. Embedding trust requirements in electronic contracts between machines will play a decisive future role in M2M communication.[1]

Moreover, it is becoming increasingly important during and also after a communication to technically determine whether the behaviour of participant entities is trustworthy, not just prior to or during the communication setup. Especially for the protection of communication partners, attention is focusing more on the consistent, automated monitoring of semantics. This describes the purpose of the respective communication. The global trust and platform services must ensure that producers, systems and components are technically assessed (scoring) to automatically detect threats before, during but also after a communication, such as virus infections.

[1] OpenFog Consortium (https://www.openfogconsortium.org/) – [Draft work on machine contracting]

Communication relationships

The Common automation device – Profile guideline IEC TR 62390:2005 (3) defines profiles for device classification (e.g. temperature sensor) with a common set of functionalities in a given industrial domain. Modelled on this, the sub-working group, Secure Communication for Industrie 4.0, has come to an understanding for a Security Policy for Industrie 4.0 (Figure 3).

The Security Policy addresses all levels of relationships among Industrie 4.0 components. It aims at ensuring the interoperability of all levels addressed by IEC TR 62390. Examples of this interoperability would be:

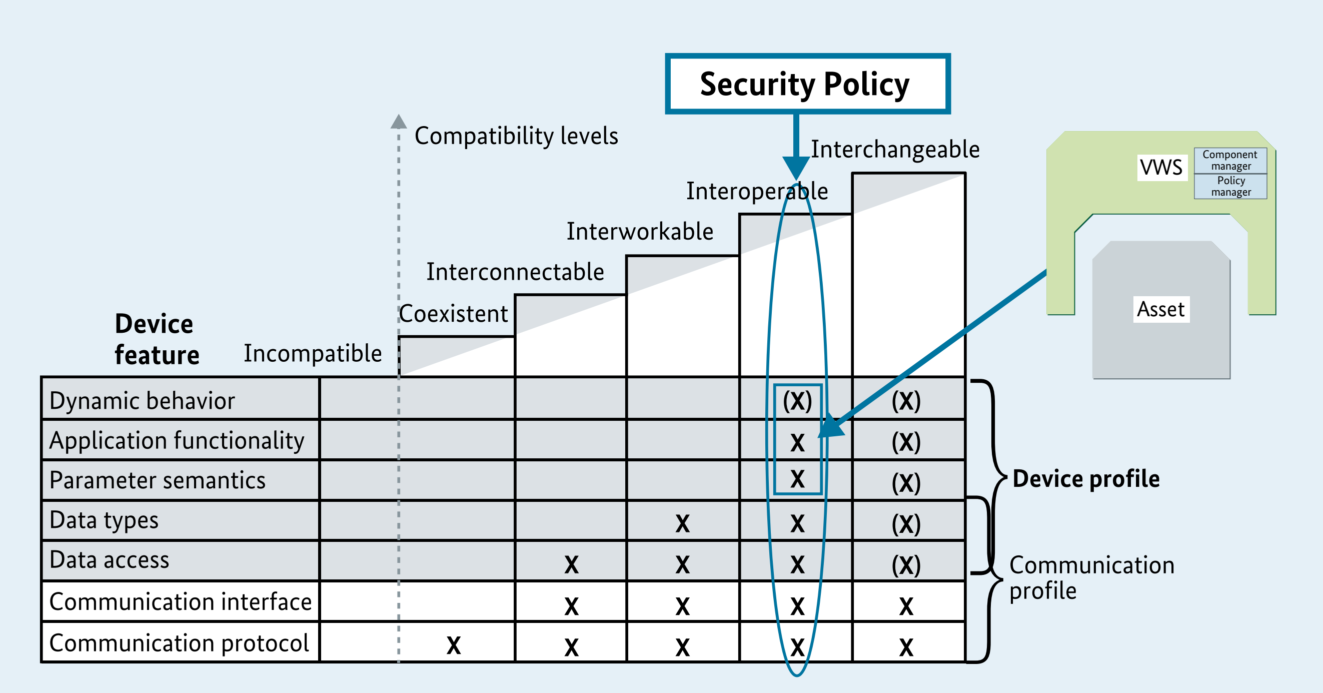
- Dynamic behaviour: trust in the same neutral trust anchors, security profiles
- Application functionality: permissions of a tenant/client
- Parameter semantics: user and role models
- Data types: certificates, security tokens
- Data access: role-based access (read, read/write, write)
- Communication interface (Layers 5-7): OPC UA
- Communication protocol (Layers 1-4): TLS

For Industrie 4.0 components wrapped by their administration shells, it is no longer sufficient to match communication at protocol level (Figure 3). There is also a need for agreements on permissions (Who is allowed to do what?), trust anchors (electronic keys, for example) and security profiles.

To be able to start a cooperation, the administration shell must supply information on the security capabilities of Industrie 4.0 components. This is the only way for the mutual verification of possible cooperation (for example in connection with the level of trustworthiness to be defined, as discussed in the document Security of the Asset Administration Shell, Industrie 4.0 Platform/ZVEI 2017, (4)).

To describe an Industrie 4.0-compliant communication, we must consider in future an Industrie 4.0 communication stack (Figure 11) that is not solely confined to the lower layers of the OSI layered model. Instead, more attention has to be paid to all the interactions and contents exchanged (Figure 4).

Figure 3: Security Policy for Industrie 4.0



Device feature	Incompatible	Coexistent	Interconnectable	Interworkable	Interoperable	Interchangeable
Dynamic behavior					(X)	(X)
Application functionality					X	(X)
Parameter semantics					X	(X)
Data types				X	X	(X)
Data access			X	X	X	(X)
Communication interface			X	X	X	X
Communication protocol		X	X	X	X	X

For example: A measured value must be transmitted from Machine A to Machine B. Many different protocols are available for the reliable and secure transmission of the value on the network layer. It could, for example, be authenticated by a secure transmission and a certified receipt. It could also already be certified at the source, so that the transmitted message includes not only the measured value but also the certification confirming its authenticity. This would enable a reduction in secure transmission requirements. Selecting an appropriate combination of information and transport security depends on the specific application. In this case, it could be information on or conditions for time response, the available processing power or the scope for subsequent verification.

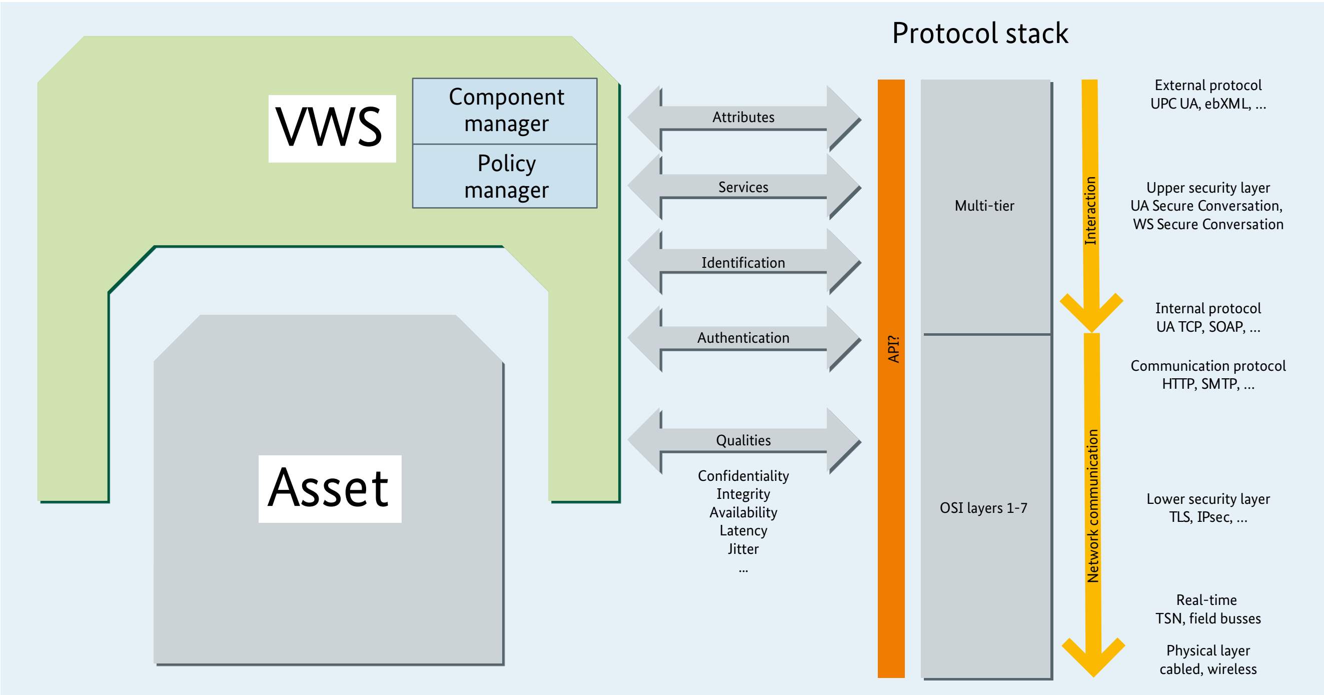
General requirements of communication and architecture

Communication relationships among Industrie 4.0 components must facilitate interaction that permits them to exchange data and provide services for enabling automation with the necessary properties. The present studies on this pertain to the interaction model (5), network communication (6) and service architectures (7). The starting point is the representation of every Industrie 4.0 component by the administration shell (8) that describes it and supplies resources, such as data, information and services. To be able to make use of these resources, communication must meet certain requirements:

- We may assume in general that most communication will take place via a **TCP/IP network**. In future, the IPv6 protocol will be deployed on the network layer (IPv4 protocol largely in use today). This protocol forms the **basis for connecting Industrie 4.0 networks**, because it enables any officefloor and shopfloor system to communicate at local and global level. Various protocols of the TCP/IP protocol suite rely on the IP protocol. Data transfer via TCP or UDP can be reliable or unreliable. Additional protocols also enable the representation of initial interaction models. Architectures such as OPC UA on the shopfloor or technologies such as web services and SOAP ensure that formatted data is transmitted and actions initiated.

- As the basic network structure of TCP/IP networks will be adopted for Industrie 4.0 communication, account also needs to be taken of related requirements and security considerations. Decades-long established officefloor models are already in place to administer and secure these networks (see section on applicability

Figure 4: Industrie 4.0 components



of various protocols). Consideration needs to be given to network planning aspects such as restrictive network segmentation through firewalls, access control lists, VLANs and network access control as well as effective operational event monitoring for systematic network surveillance to be able to respond to anomalies. In addition, the security of the lower layers in the ISO/OSI model also plays a role (e.g. encryption of wireless networks and connections via public networks, such as VPN).

Industrie 4.0 components interact

As soon as an end-to-end connection has been made on the network and transport layer, where TCP/IP and OPC UA, for example, has been used, the logical interfaces of Industrie 4.0 communication - the administration shells - can enter into contact with each other. Security and efficiency are also considerations here. Whoever is permitted to access the resources (data, information and services) of the administration shell is regulated by a rights permission model (4) that is included in administration shell design. For this, the communication partner must be identified and authenticated. It is therefore important that the communication protocol and communication stack provide appropriate security mechanisms.

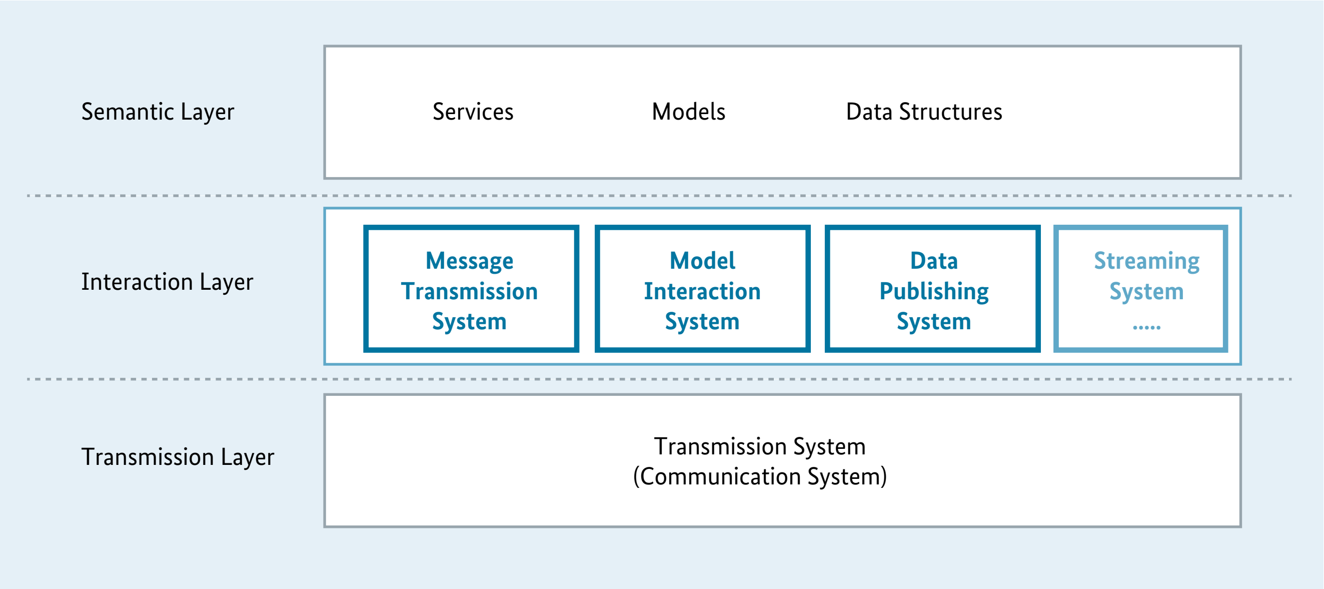
What exact shape the communication relationships take is determined by requirements on time response or security criteria for confidentiality or integrity, for example. Where necessary, these requirements, such as, 'I need an answer in below one millisecond and it must have a digital signature', must be able to be stipulated in the communication stack and must be verifiable during the entire communication process: when setting up, using (status request) and after terminating the connection (logging). The communication stack must also support the negotiation/evaluation of higher-quality properties such as that of a security protocol of the communication partner's trustworthiness (1) and connect them with the rights management of the administration shell.

This kind of structure (Figure 5) has been defined in the document on communication models by the OpenAAS Project, Com4.0-Basic (9). The next step is to look at the interaction and transmission layers it cites in future discussion with the architecture depicted in Figure 4 and develop this further into a coherent overall picture.

Communication structures

In practice, this gives rise to very disparate structures for supporting communication, depending on requirements and applications used.

Figure 5: Communication aspects as depicted in Com4.0-Basic



End-to-end communication

In the simplest case, two Industrie 4.0 components communicate directly with each other (Figure 6). The requisite infrastructure of network and support services must be available for this, e.g. for name resolution in the IP addresses or identity management.

Communication via gateways

In many organisations, communication is conducted via gateways that enable the control of data and the separation of domains (Figure 7).

Components or subsystems that do not communicate in compliance with Industrie 4.0 themselves can be connected through appropriate Industrie 4.0 gateways (Figure 8). This kind of connection is necessary to assimilate existing installations into the future Industrie 4.0 world.

Another case: There are components that lack sufficient computing power and storage capacity to engage in extensive communication on their own. It can be expedient here to make use of other protocols, especially in the local environment. These components in the networks in front of an appropriate Industrie 4.0 gateway have no or only limited properties of an Industrie 4.0 component so that an Industrie 4.0 gateway must support communication. Industrie 4.0 gateways are also an option where, for example, small and medium-sized enterprises lack the in-house resources for introducing and operating Industrie 4.0 components, but nevertheless wish to participate. In this case, an Industrie 4.0 gateway can be operated for secure data exchange by a service provider.

Industrie 4.0 gateways must be generally able to protect the systems behind them. That does not preclude an Industrie 4.0 gateway itself from being located behind another gateway in the network.

Publish-subscribe model

Publish-subscribe models can distribute information to several partners. The receivers (subscribers) register with the sender (publisher) or a distribution service to participate in the flow of information. The subscribers select the type of message they wish to receive (Figure 9).

Thanks to the loose coupling of publisher and subscriber, where the number of subscribers that register poses no technical problem, it is easy to scale information distribu-

Figure 6: Industrie 4.0 components communicate end-to-end

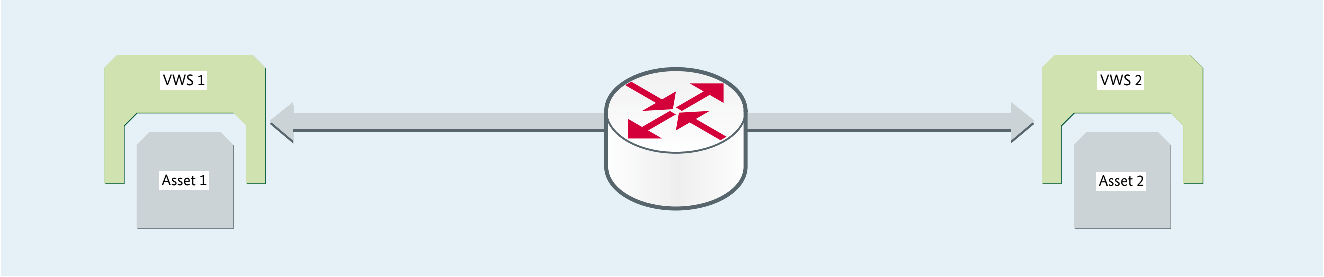


Figure 7: Industrie 4.0 components communicate via firewalls, proxies or gateways

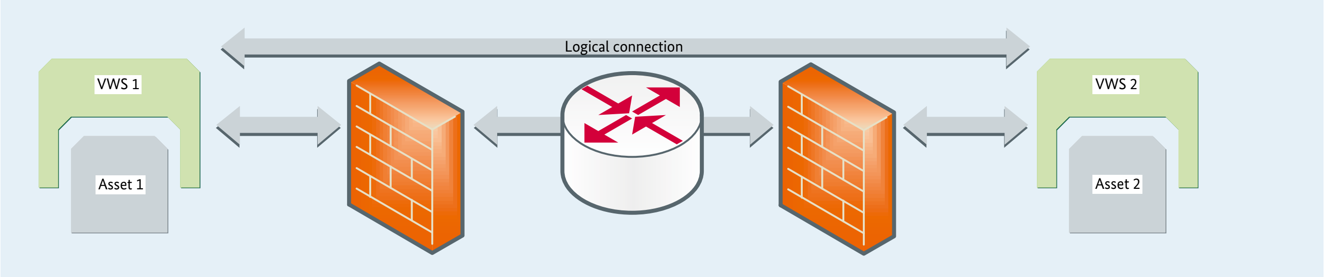
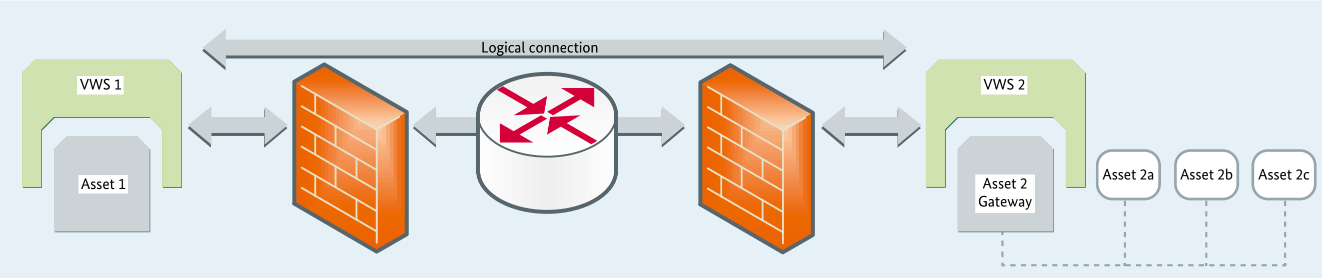


Figure 8: Connection of additional components via Industrie 4.0 gateways



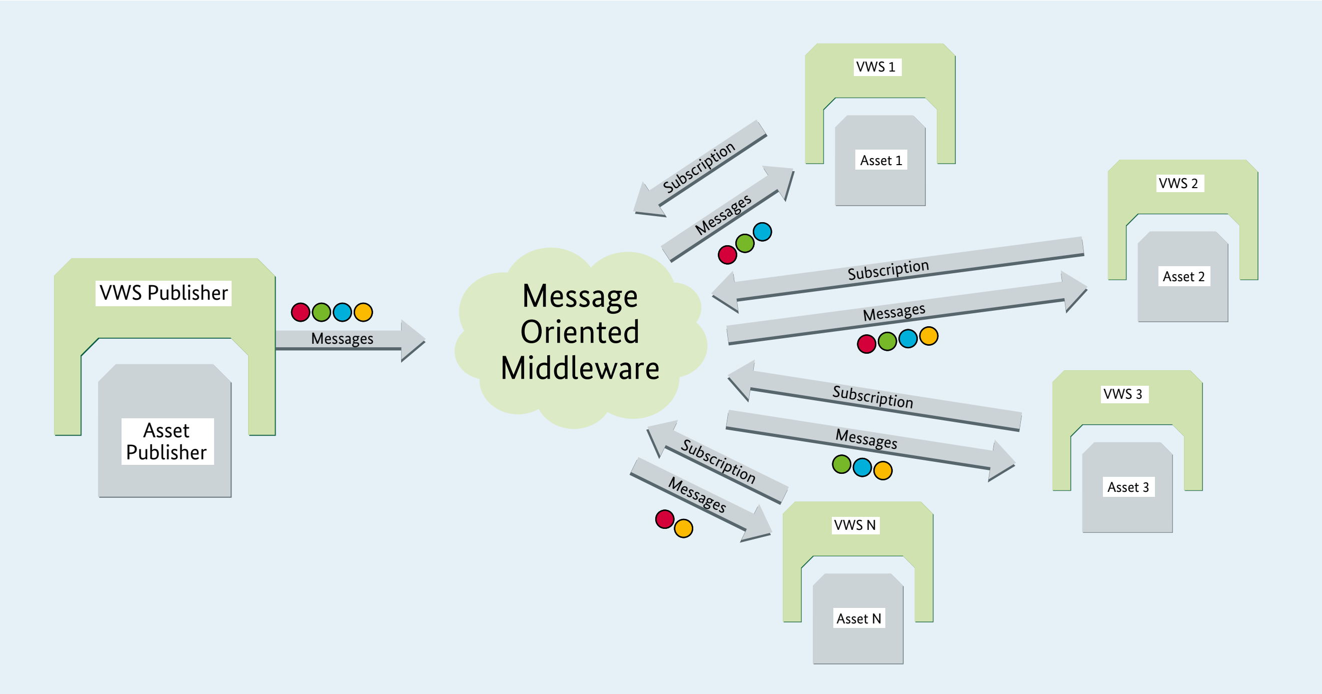
tion. These kinds of models make frequent use of data telegrams without acknowledgement (UDP) and are either designed to tolerate lost telegrams, as with audio or video applications, or they presuppose a very reliable network infrastructure, as is often assured in automation through large bandwidth reserves. In addition, there is a reliable mode where the subscriber can consistently receive all previously undelivered telegrams. This communication method is, however, more time-consuming and is normally used in real-time-uncritical applications where data consistency is the sole concern (business processes, contracts, production orders, alarm messages).

Communication with the network as partner

Time-critical automation applications that must, for example, operate in synchronous mode to be able to cooperate often call for special network properties, such as latency (delay) or jitter (deterministic time response). Today, they are specified in engineering, that is, in planning and implementing automation, and are inserted in all components, including the relevant network components.

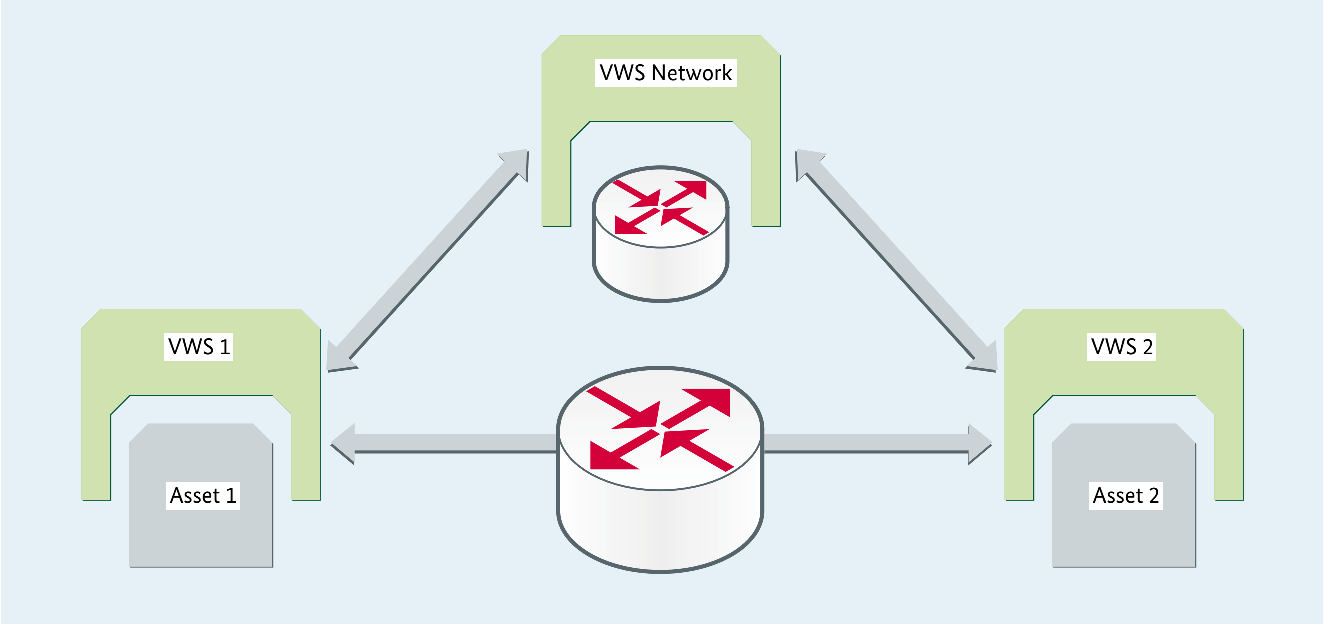
As Industrie 4.0 concepts are highly flexible, Industrie 4.0 components must be able to demand the special properties from the network. That is why it is useful for the network

Figure 9: Publish-subscribe model



infrastructure to provide its own Industrie 4.0-compliant interface as an administration shell (10) (Figure 10). This way, the infrastructure can be fully integrated into the Industrie 4.0 world. Depending on the specific application, individual network elements, such as routers or switches, can be represented by their administration shell. Examples of this can be found in TSN.

Figure 10: Industrie 4.0 components communicate with the network on requisite features



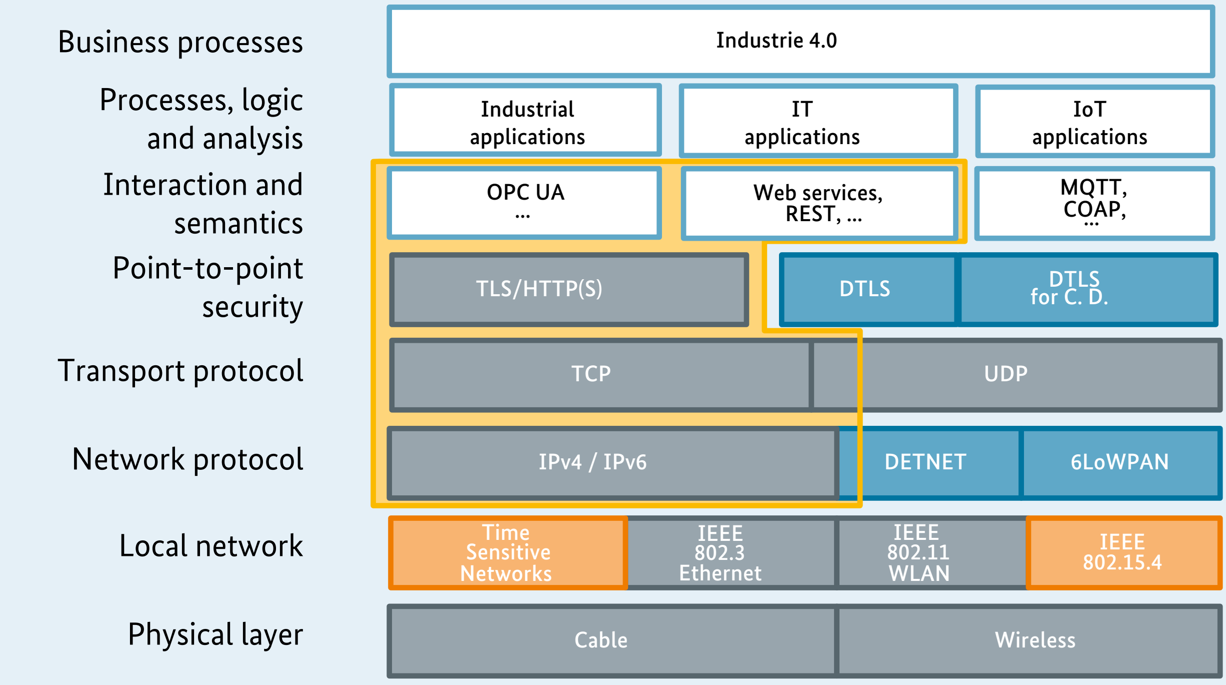
Applicability of various protocols

For decades, network communication has been successfully divided into protocol layers and protocols. Protocol layers describe the services that the protocols implemented on them deliver. Depending on the purpose or environment, the protocols provide suitable services, including name resolution, for example. As a rule, the interfaces between the individual protocol layers are generic, so that several possible combinations of different protocols can be deployed. It is, for example, possible to set up a TCP/IP communication both via cable-linked types of network such as IEEE 802.3 Ethernet and via wireless networks such as IEEE 802.11 WLAN – without having to alter the overlaying protocols and application logic. This plurality of protocols will also form part of Industrie 4.0, because it will be necessary to have uniform communication among administration shells via all types of network – as evident from applications used in industry:

- For rapid communication in **closed loop systems**, for example, it can be important to communicate via real-time capable TSN Ethernet networks.
- Powerful Ethernet networks without TSN or flexible wireless networks with WLAN can be used for **data traffic with lower deterministic communication requirements**, where it is not so important whether a data packet arrives at a predefined point in time.
- Applications that primarily need l**ong runtimes for battery-powered devices** (sensors or smart device tags) will in all probability require 802.15.4 low-power networks in combination with low-power network protocols such as 6LoWPAN and COAP.

A clear layered model can already even plan for technologies (such as deterministic radio communication) that are not yet available today and can then be easily introduced at a later date. Various protocols and architectures will exist in tandem on the application layer, as either principally officefloor technologies (web services, for example) or automation technology (e.g. OPC UA) will be deployed in specific domains.

Figure 11: Plurality of network protocols in Industrie 4.0 applications



🟨 Some protocols and standards extend over several layers of the communication stack. In the chart, examples of layers and protocols used by OPC UA are highlighted in yellow.

Different technologies have established themselves in automation and IT that are not easy to alter for technical and organizational reasons. Here too, we can therefore expect the parallel use of different protocols and architectures (pluralism).

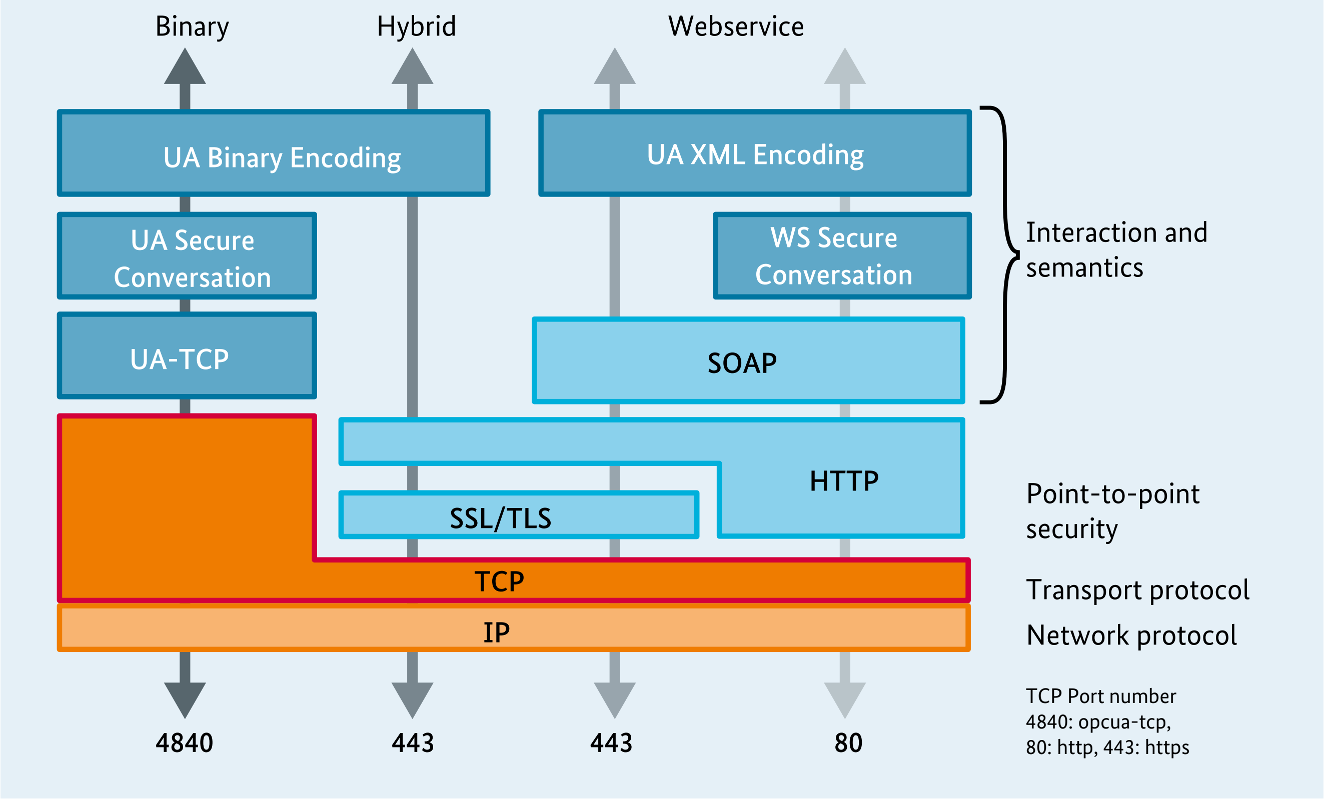
It might appear that protocol pluralism as described above is chaotic and unnecessarily complex, but thanks to clear transfer points at the protocol layers, protocols can be effectively operated in combination with each other. In practice, there are also already communication capabilities among domains: OPC UA, for example, already provides for officefloor interactions and implements these - such as the application of web services and the TLS security protocol.

Figure 11 shows the possible design of communication stacks. (Additional protocols are conceivable and are not unlikely in these communication stacks.)

For protocol plurality, it is important to make effective use of the security mechanisms available on the individual layers. In general, many of these protocols support authentication, encryption and integrity protection functions. In addition, various mechanisms can be installed on the layers to control access.

Figure 12 shows the layered construction of OPC UA. Here too, OPC UA clearly avails itself of functions on different layers. Even within this standard, there are equally capable, interchangeable protocols (SOAP and UA TCP, for instance). On the lower layers, OPC UA also makes use of the functions of TCP/IP networks. As OPC UA is specified independently of specific types of network (Ethernet or WLAN), it can be deployed in many environments. The minimum requirement for operation is merely the availability of an IP network, which is feasible in most industrial applications.

Figure 12: OPC UA elevates security to the application level

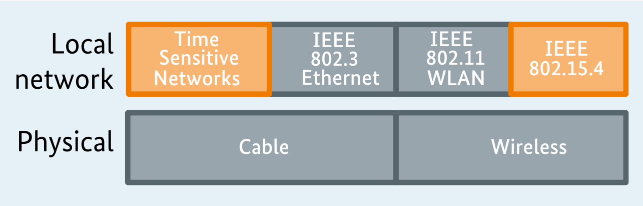


Security requirements and mechanisms on communication stack layers

The security of an entire system cannot be assured on one layer or at one single point. Instead, all points on the communication stack must be designed to be secure. This means taking account of the functions and management mechanisms of the protocols and the confidentiality and integrity of the data transported via them. We shall outline the security requirements and mechanisms of the individual layers in the following:

Data link and physical layers

The data link and physical layers (OSI Layers 1+2) encompass the physical transmission of a signal and the transfer of data in a local network. The predominant technologies in OSI Layers 1+2 are IEEE 802.3 (Ethernet), IEEE 802.11 (Wireless LAN) and IEEE 802.15.4.



A key security issue is determining **which devices may participate in the network**. The security system must ensure that only authorised participants can send data or network packets to the network or receive data from it. This can be done by encrypting data communication (such as with WLAN) and authenticating participants (via IEEE 802.1X/RADIUS, for example). A new network participant, for example, identifies himself to the network with his own username and password or certificate. If the network access control mechanisms take effect, the unauthorised participants (a hacker with his own laptop, for example) cannot participate in the network or cannot decrypt its data traffic.

Physical security (e.g. access to routers, switches and end systems by unauthorised persons) is very important on the data link and physical layers. Suitable protective measures range from locable cabinets for network devices to switching off unused Ethernet ports in the software.

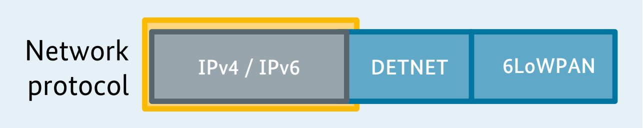
The data link and physical layers also perform another major task: They must meet **quality-of-service requirements**. Technologies such as TSN, can, for example, supply deterministic data packets in real-time critical applications. Security mechanisms must, however, be installed to safeguard real-time critical traffic from overload due to other types of traffic. A classical problem in the automation world is a defective component that causes network overload due to excess data traffic and brings production to a standstill.

Other possible hacking targets are protocols that manage processes on the data link and physical layers. If a hacker manipulates these protocols, this can seriously disrupt the functioning of a network. That is why suitable measures (e.g. port security and DHCP snooping) must be taken to protect against changes and disruptions in the **functions of management protocols**, such as the Address Resolution Protocol (ARP), the Dynamic Host Configuration Protocol (DHCP), multicast protocols and QoS protocols.

As with all other layers, **operating data** of the data link and physical layers can be collected that provide important indicators for identifying attacks. They record, for example, when and where a device was connected to the network or which other network participants receive (have received) packets from a device.

Network layer

The network layer with its principal communication protocol, the Internet Protocol (IP), connects individual IP-capable devices, also across network boundaries: It enables devices to be addressed or reached company-wide or worldwide. It is therefore all the more essential to separate intended and necessary from unintended and possibly harmful communication connections.



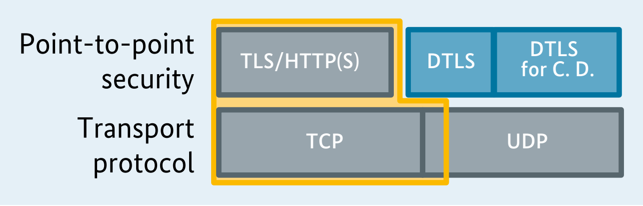
To place restrictions on these connections, **access control lists, firewalls and gateways** are, for example, deployed. Protection strategies can be implementedwith the help of these technologies and devices as described in ISO/IEC 62443 (e.g. zones & conduits). Devices are aggregated into suitable functional groups (e.g. all devices in a special plant component) where communication among devices is permitted on a selective basis. At the same time, this can prevent communication with other devices, such as with a hacker's notebook, even if it is located in the same company. This segmentation places a narrow constraint on the scope of the hacker in the network and protects vulnerable systems from being influenced by compromised components and makes intrusion into the system far more difficult.

Moreover, various **secure networks can be linked via insecure networks** on the network layer with the help of virtual private network (VPN) technologies. This way, sites outside a plant can be connected with a central facility in the company - mostly the central IT. Here too, the individual communication relationships need to be segmented (via firewalls and gateways, for instance).

Data can also be collected at the network layer **that are relevant for secure operation**. They can be used to detect attacks. Where, for example, unusual communication takes place between devices without functional relevance or exceptional communication patterns occur, caution is needed – they can indicate an attack.

Transport layer and end-to-end security

The transport layer connects individual applications on various devices. To ensure their security, the identity of devices and services is an essential issue.



Two protocols have found widespread use for secure transport layer connections: **Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)**. Industrial protocols (such as OPC UA) are also able to apply these protocols.

These protocols apply X.509 certificates for the **reliable cryptographic confirmation of the identity of an end system and membership of a specific organisation**. An end-to-end encryption or integrity protection is established between the communication endpoints authenticated in this way. This prevents hacking attempts: The appropriate selection of cryptographic mechanisms can prevent a hacker from intercepting connections and modifying data.

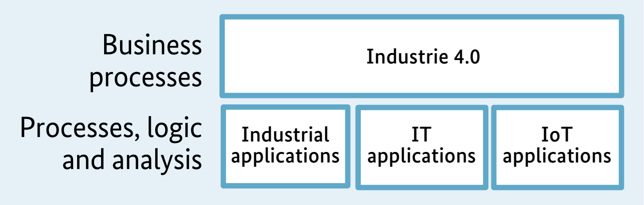
End-to-end encryption does not, however, just afford benefits for security: Due to encryption, devices, such as firewalls, that check incoming traffic for anomalies cannot inspect it and can no longer detect hacking patterns, so that attacks remain concealed. There is a middle way to assure end-to-end security while permitting the inspection of traffic: It can be decrypted in a trustworthy gateway. To do this, the gateway breaks up the secure connection and inspects the data. This approach, however, has its shortcomings, especially when it comes to determining which gateway is trustworthy. Moreover, it is not available for all protocols.

Data concerning the transport layer can be used for monitoring and detecting an attack. These are in particular the identities of communication endpoints and their communication patterns.

Process and business logic

Parts of Industrie 4.0 communication are situated above the described layers. These pertain to specific applications, including process logic or modelled business processes.

Visualisation formats have already been in place for years for the normative description and exchange of process and business logics, for example, the **Unified Modelling Language (UML), Business Process Model and Notation (BPMN) and Business Process Execution Language (BPEL)**. Moreover, related models have established themselves in industry, on the office and shop floors, such as **Service-oriented Architecture (SOA)** and largely digitised execution systems, such as the **Manufacturing Execution System (MES)** and **Enterprise Resource Planning (ERP)**.



A streamlined form of handling operations and data on these layers in Industrie 4.0 is the **administration shell**. It combines data and interaction models and provides essential security functions (e.g. authentication, integrity and access protection and event logging). The **identities of the participants involved in an Industrie 4.0 communication**, their roles and permissions are also key on these three layers. As industrial processes and business logic are modelled and implemented on the upper layers, appropriate measures are essential to assure reliability and legal certainty. In particular, processes must be auditable and the system or a party must be verifiable as trustworthy.

As many corporate systems are already in place that manage and model business processes and information, there may be a need to **connect many current legacy systems with each other with adapters and gateways**. With this sort of connection, it is important to maintain the security properties and traceability of actions, that is, to determine who communicated with whom, when and what about.

Parts of the process and business logic can also be implemented at **intercompany** level. It is conceivable that IT systems of other companies (e.g. suppliers or clients) or systems of external providers (e.g. cloud systems) are intertwined at this level with the enterprise's own applications. Especially in intercompany communication, a firm must ensure that suitable protective mechanisms are in place, that communication operations and transactions can be traced and that it is operating within the law.

Practical example: order-controlled production

On the previous pages, we examined communication stacks and possible protocols, but to account for all the central aspects of secure communication, we also need to take a closer look at relevant Industrie 4.0 applications

Among other things, the practical example shows communication relationships in the order-controlled production of a customised bicycle handlebar as depicted by the Industrie 4.0 Platform (11) (Figure 13).[2] The flowchart for the communication steps is shown in Figure 14:

Step 1: Bicycle manufacturer assigns the call to tender to a broker.

Step 2: Broker distributes the call to tender to prospective suppliers.

Step 3: Interested suppliers submit bids to broker.

Step 4: Broker conveys pre-filtered bids to the bicycle manufacturer.

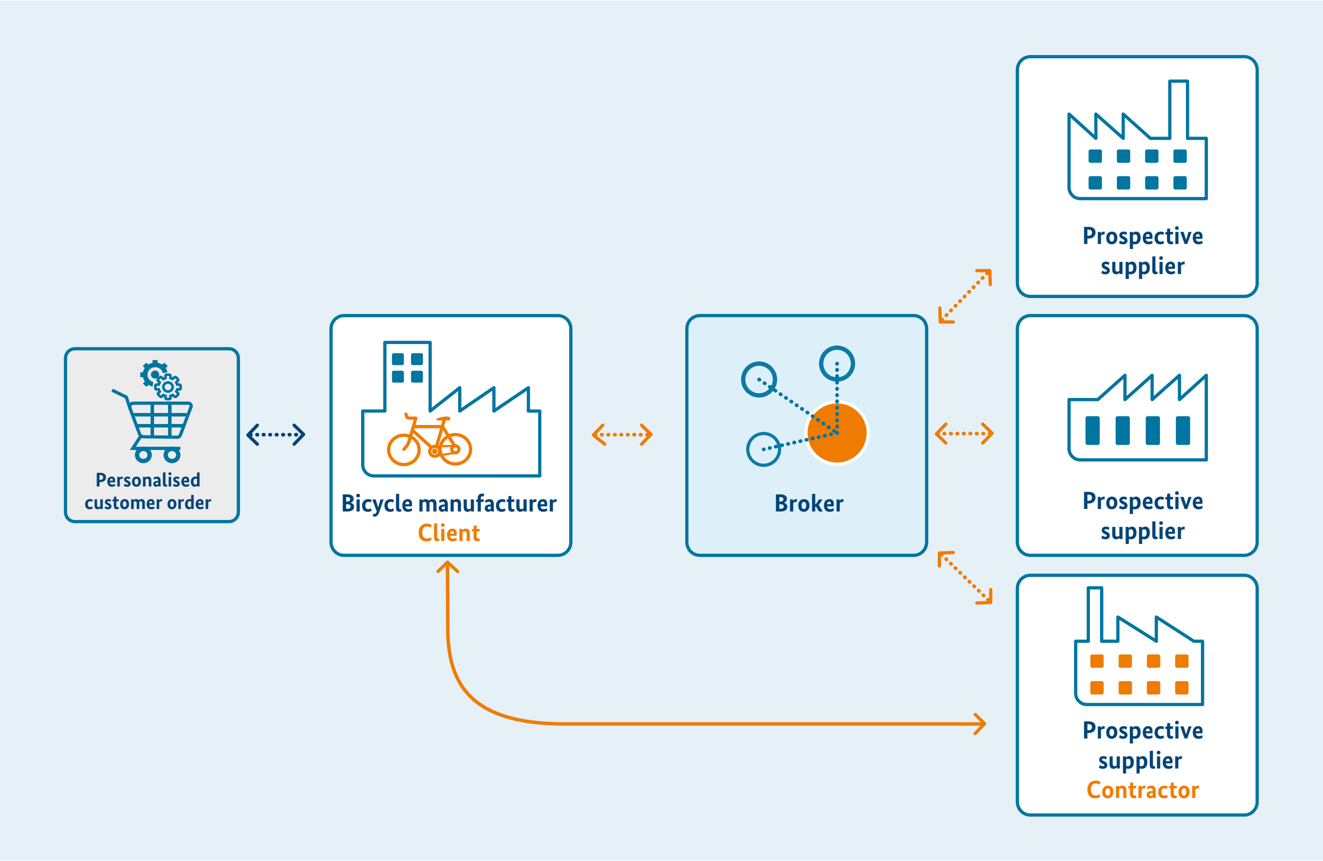
Step 5: Bicycle manufacturer (client) places the order directly with the selected supplier (contractor).

Step 6: Contractor sends client the agreed data on the customised product as part of product memory.

Step 7: *Physical product is delivered.*

For each of these steps, communication requirements can now be specified to determine which protocols are suitable. Based on these steps, appropriate upgrades of existing protocols can also be undertaken.

Figure 13: Order-controlled production of a customised bicycle handlebar



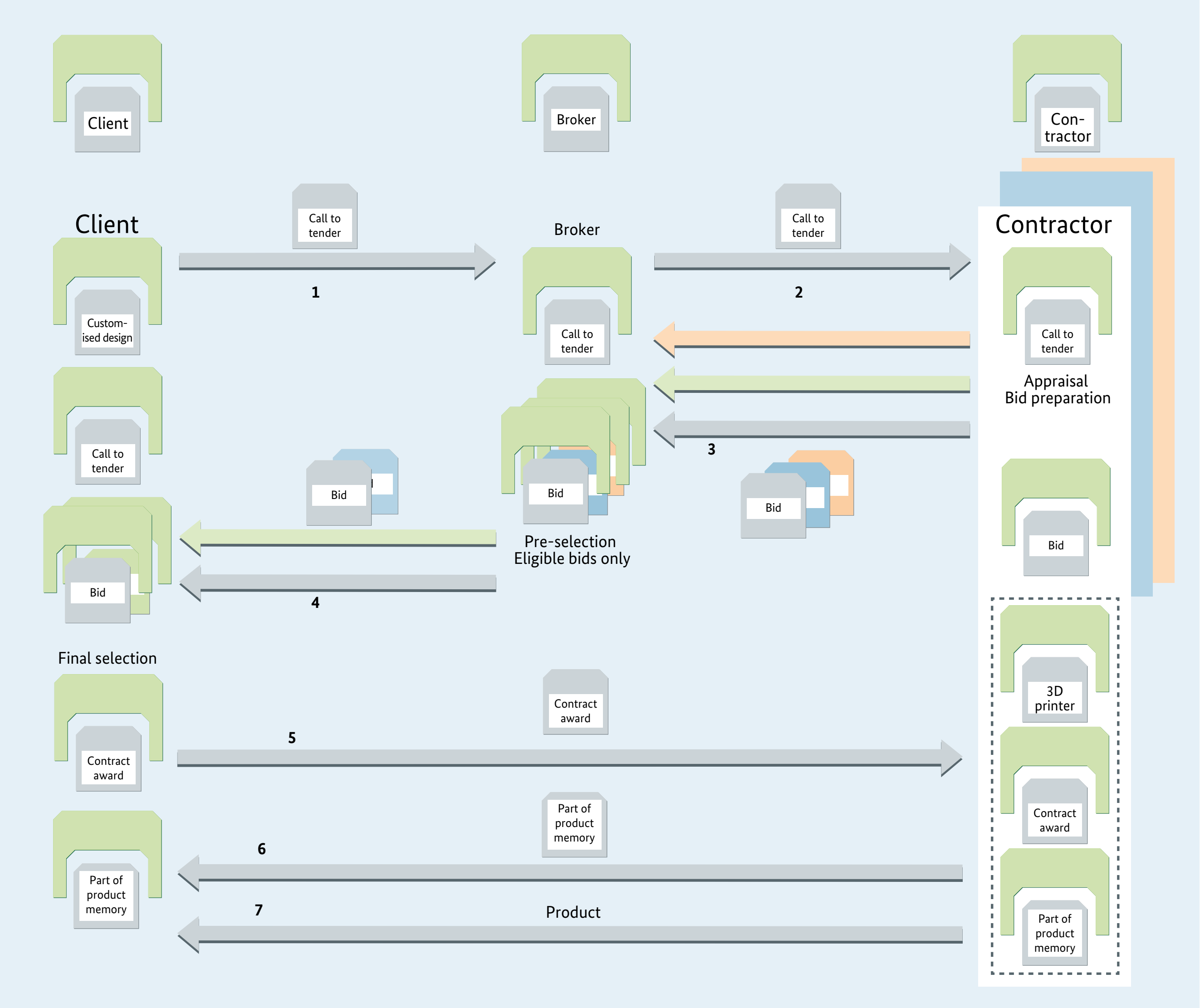
[2] The practical example concerns a call to tender that includes both the technical specifications for the product and all commercial and legal parameters. This call to tender is then distributed by a broker to prospective suppliers that it appraises beforehand, including their IT security trustworthiness, as much of the exchanged data, including 3D printer data on the customised bicycle handlebar, is sensitive information.

Figure 15 depicts an example of how the call to tender is transmitted from the bicycle manufacturer to the broker (first communication step). Clearly, security issues are most relevant for the legal certainty of the transaction. Technical requirements of the communication process, such as typically time response in semi-automated processes, are, however, less relevant in the present case. The transaction can last several seconds without jeopardising the operation.

To transfer the call to tender, the integrity of the data contained in it must be protected in all respects and if necessary authenticated with an electronic signature. This ensures that the call to tender cannot be falsified – either during the transmission to the broker or during the ensuing distribution to prospective suppliers. It may also make sense to use confidential transmission for the path to the broker and the subsequent distribution. The requirements and implementations should, however, be viewed separately and assessed for the protocols deployed: on the one hand for confidentiality along the communication route and on the other for protecting the integrity of the information itself.

Figure 15 shows how this could be technically implemented (Note: It cites examples of protocols that are applied in electronic business, without considering in more depth

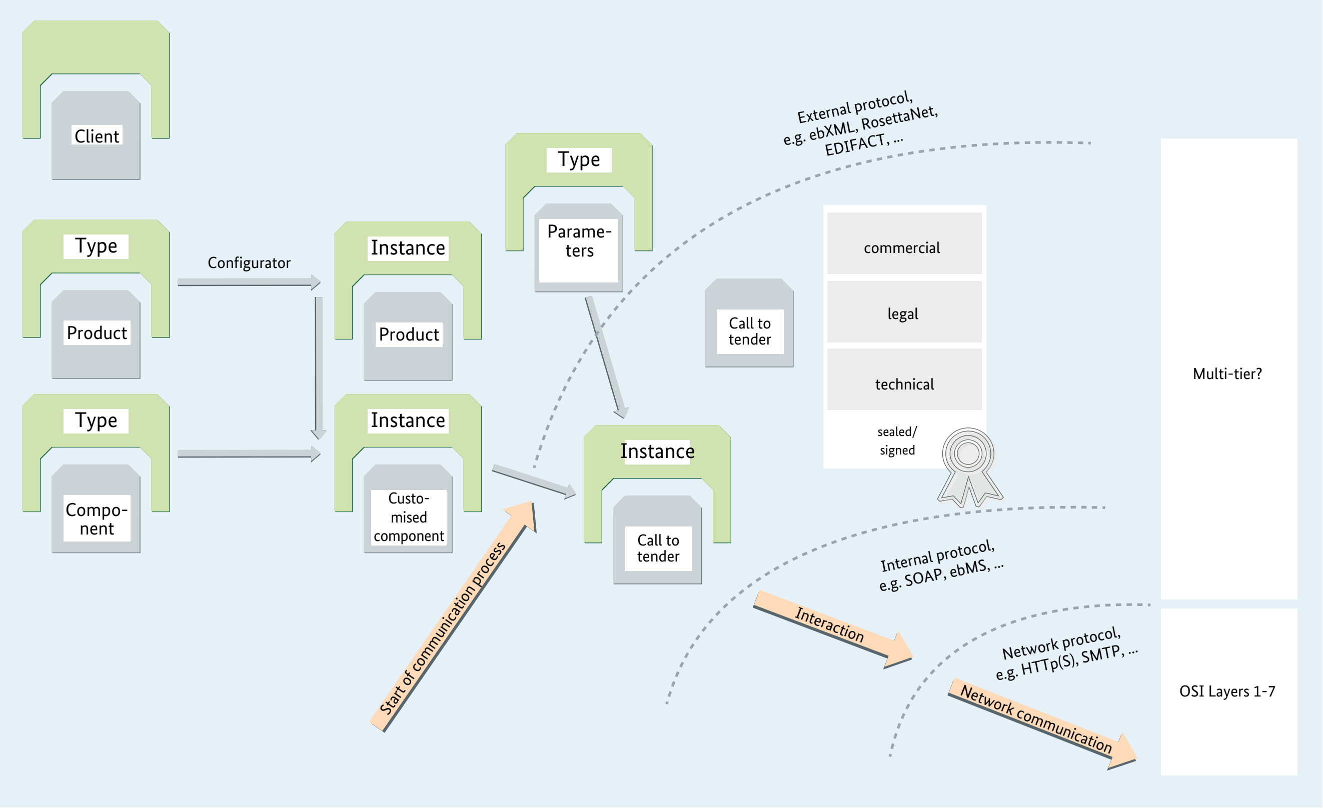
Figure 14: Communication flowchart



whether they are actually suitable.): In the first step, the call to tender is generated as a message and provided with a digital signature. On the way to the broker, it is encrypted.

As the digital signature of the call to tender is available throughout, integrity and authenticity are always retained both at the broker and during a subsequent transmission.

Figure 15: Communication step 1 – possible transmission of a call to tender



Summary and outlook

The discussion paper shows the need to consider different layers of communication protocols for ensuring secure communication. For this, it is important to analyse many different practical applications as the only way to compare and assess possible protocols and arrive at criteria for Industrie 4.0-compliant communication.

The example outlined above from an application scenario for order-controlled production deals with a business transaction. If technical processes are also involved, other aspects will play a major role that have a particular influence on the security and runtime performance design of communication (e.g. latency). The future work of the Sub-Group must therefore include a description and investigation of a scenario on the automation layer with relevance to real-time communication and interaction among systems of various producers. Another major component will be to shed more light on intercompany communication and the integration of Cloud services, because the industrial world faces the challenge of planning communication for flexibility and for minimising organisational, that is, manual operational tasks. We therefore recommend including the findings of other groups of experts on this issue in future studies, such as the IIC Connectivity Framework (12), the IIC Security Framework (13) or the Reference Architecture Model for Industrial Data Space (14).

References

1. *Technischer Überblick „Sichere unternehmensübergreifende Kommunikation“.* Berlin: Plattform Industrie 4.0, 2016.

2. *Facilitating International Cooperation for Secure Industrial Internet of Things/Industrie 4.0.* Berlin: Plattform Industrie 4.0, 2017.

3. Common automation device – Profile guideline. IEC TR 62390:2005.

4. *Security der Verwaltungsschale.* Berlin/Frankfurt: Plattform Industrie 4.0/ZVEI, 2017.

5. *Interaktionsmodell für Industrie 4.0-Komponenten.* Berlin: Plattform Industrie 4.0, 2016.

6. *Netzkommunikation für Industrie 4.0.* Berlin: Plattform Industrie 4.0, 2016.

7. Reference Model for Industrie 4.0 Service architectures – Basic concepts of an interaction-based architecture. DIN SPEC 16593, 2017.

8. *Technischer Überblick „Struktur der Verwaltungsschale“.* s.l.: Plattform Industrie 4.0, 2016.

9. *Com4.0-Basic: Basic Models of Communication.* Aachen: RWTH Aachen, 2016.

10. *Network-based Communication for Industrie 4.0: Proposal for an Administration Shell.* Berlin: Plattform Industrie 4.0, 2016.

11. *Anwendungsszenario trifft Praxis: Auftragsgesteuerte Produktion eines individuellen Fahrradlenkers.* Berlin: Plattform Industrie 4.0, 2017.

12. *The Industrial Internet of Things/Volume G5: Connectivity Framework*. Needham, MA, USA: Industrial Internet Consortium, 2017.

13. *Industrial Internet of Things/Volume G4: Security Framework.* Needham, MA, USA: Industrial Internet Consortium, 2016.

14. *Reference Architecture Model for the Industrial Data Space.* München/Berlin: Fraunhofer Gesellschaft/Industrial Data Space e.V., 2017.

AUTHORS:
Prof. Dr. Tobias Heer, Hirschmann Automation & Control GmbH; Markus Heintel, Siemens AG; Stefan Hiensch, Bundesnetzagentur; Dr. Lutz Jänicke (Leitung), Phoenix Contact GmbH & Co KG; Michael Jochem, Robert Bosch GmbH; Bernd Kärcher, Festo AG & Co. KG; Marcel Kisch, IBM Deutschland GmbH; Jens Mehrfeld, Bundesamt für Sicherheit in der Informationstechnik; Gerhard Oeynhausen, Telekom AG; Tobias Pfeiffer, Festo AG & Co. KG; Frank Schewe, Phoenix Contact Electronics GmbH; Dr. Michael Schmitt, SAP SE; Dr. Dirk Schulz, ABB AG; Detlef Tenhagen, HARTING AG & Co KG; Klaus Theuerkauf, IFAK Institut für Automation und Kommunikation e.V.; Andreas Teuscher, SICK AG; Thomas Walloschke, Fujitsu Technology Solutions GmbH

This publication is the joint outcome of Working Group 1, Reference Architectures, Norms and Standardisation and Working Group 3, Security of networked Systems (Industrie 4.0 Platform).

www.plattform-i40.de