PLATTFORM INDUSTRIE 4.0

DISCUSSION PAPER

Secure Retrieval of CAE Data

Imprint

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

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

Design
PRpetuum GmbH, Munich

Status
November 2018

Image credits
Monty Rakusen – Getty Images (title)
Gorodenkoff – istock (p. 4)
BlackJack3D – istock (p. 8)
Juice Images – Getty Images (p. 9)
Luis Alvarez – Getty Images (p. 11)
Monkeybusinessimages – istock (p. 13)
10’000 Hours – Getty Images (p. 14)

You can obtain this and other brochures from:
Federal Ministry for Economic Affairs
and Energy (BMWi)
Public Relations
Email: publikationen@bundesregierung.de
www.bmwi.de

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

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.

Contents

Introduction

Communication between Industrie 4.0 components is a cornerstone for the further development in the direction of networked, autonomously acting systems. Only the standardised, interoperable exchange of information at all stages of the product and system life cycle creates the preconditions for action to enhance efficiency, and exploit the new technical opportunities and new business models.

Place in the life cycle/RAMI4.0

Figure 1 shows the three fields of engineering, production and enterprise in RAMI4.0, each of which has clearly differing communication requirements. As a consequence, it is to be foreseen that correspondingly different technical solutions and protocols will come to be deployed.

- Individual devices and systems ('instances') communicate with one another in the production environment. The systems in the production environment are usually mission critical for the operator, and exchange process-related data. The Plattform Industrie 4.0 expects and supports the deployment of OPC UA as the communication architecture here, along with the associated communication protocols.

- In the field of enterprise communication and general value-creation networks, different requirements are in turn to be fulfilled with regard to the various information technology security objectives.

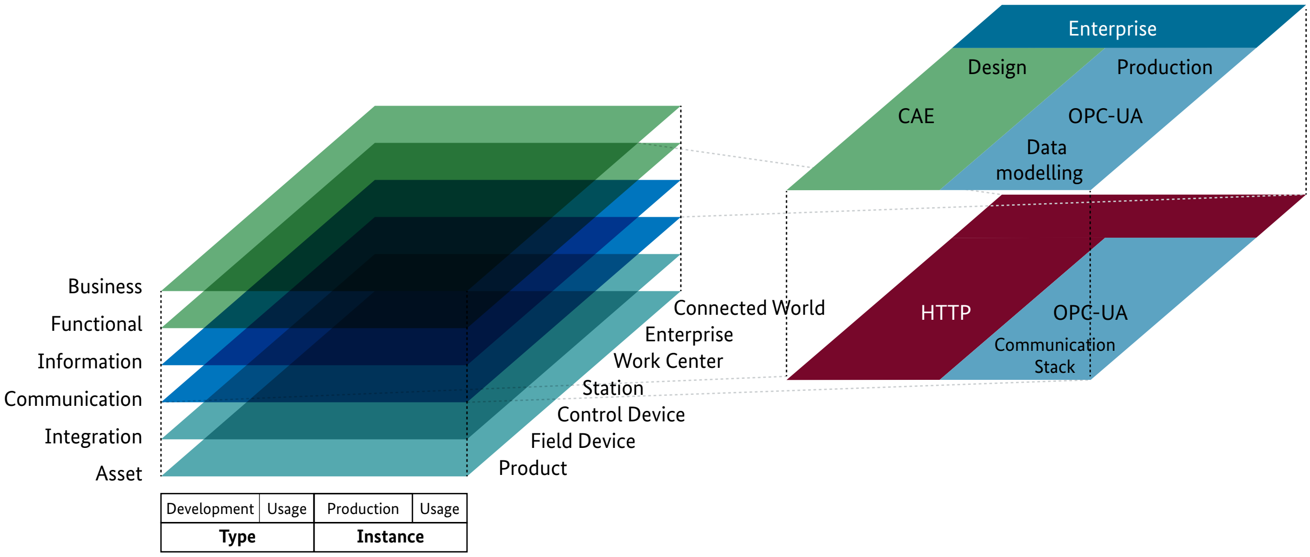
- Yet other requirements are to be fulfilled in engineering, which is concerned with the handling of types. Data sets can be very detailed and large in this field. Depending on the situation, design and development processes are also organised with a view to the longer term.

Content and aim of this discussion paper

The requirements for secure communication in the engineering process (green) are explored in this discussion paper using an application scenario. The participating stakeholders are identified, and their security requirements formulated. Industrie 4.0 concepts that are currently available and in development are analysed on the basis of these security requirements, in order to develop a proposed solution at a higher level of description.

The aim of the discussion and the proposed solution is to give interested parties and those who contribute to the shaping of Industrie 4.0 guidance for its further configuration. The document does not claim to present a complete, detailed solution. It is addressed to the technically interested reader.

Figure 1: Exemplary representation of communication relationships on the Communication and Information layers in RAMI4.0



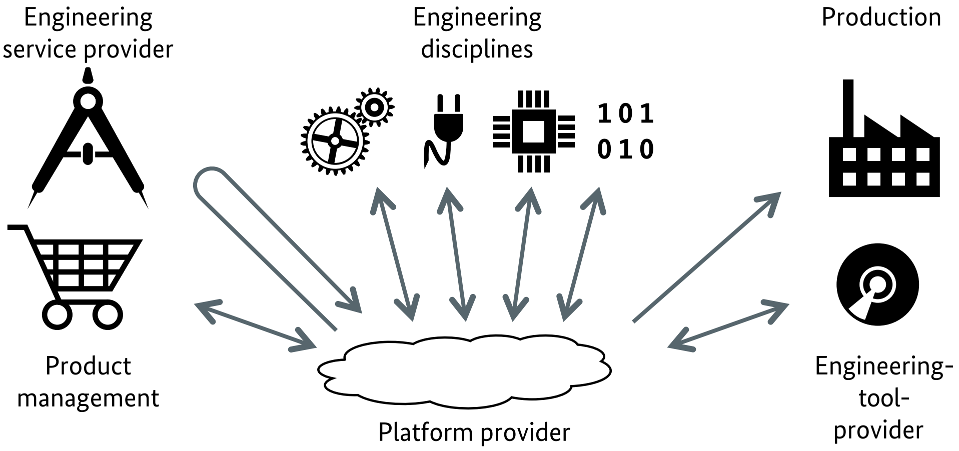
Source: Plattform Industrie 4.0

Application scenario: Smart Product Development

The Smart Product Development for Smart Production (SP2) scenario serves to illustrate the application of an appropriate mechanism (1). The scenario envisages that, for example, information about materials, components, the production process or the use of a product will be provided on a higher-level platform. The platform makes new forms of cooperation in product development and the automation of engineering activities possible.

One possible example of this kind of information retrieval being put into practice is the design of an electric drive. This scenario forms the foundation for the discussion of secure information retrieval undertaken in the present document, and will be described in greater detail below. The platform for the application example will not be analysed as part of this, while the focus is placed on information retrieval.

Figure 2: Smart Product Development for Smart Production value-creation network (1)



Source: Plattform Industrie 4.0

Overview

Figure 3 shows the model of cooperation under the classic division of labour between a manufacturer, an integrator and an operator. The example chosen is a drive that is assembled out of a converter and a motor, which are fitted together and fine-tuned to one another at the integrator's facility.

The manufacturer supplies information about the product types to the integrator, which uses the products to fabricate the higher-value end product. In turn, a type description is drawn up for this end product and made available by the integrator to its customer, the operator. Type information may be presented in the form of classic data sheets, contain 3D models, include data or software for the simulation or operation of the product (CAE data) or set out further offers.

Additionally, data that are specific to the instance in question, such as calibration or quality data, can now be generated for the physical products that are supplied. Electronic information could also be included, for authentication or batch tracking for example.

Transfer of type information

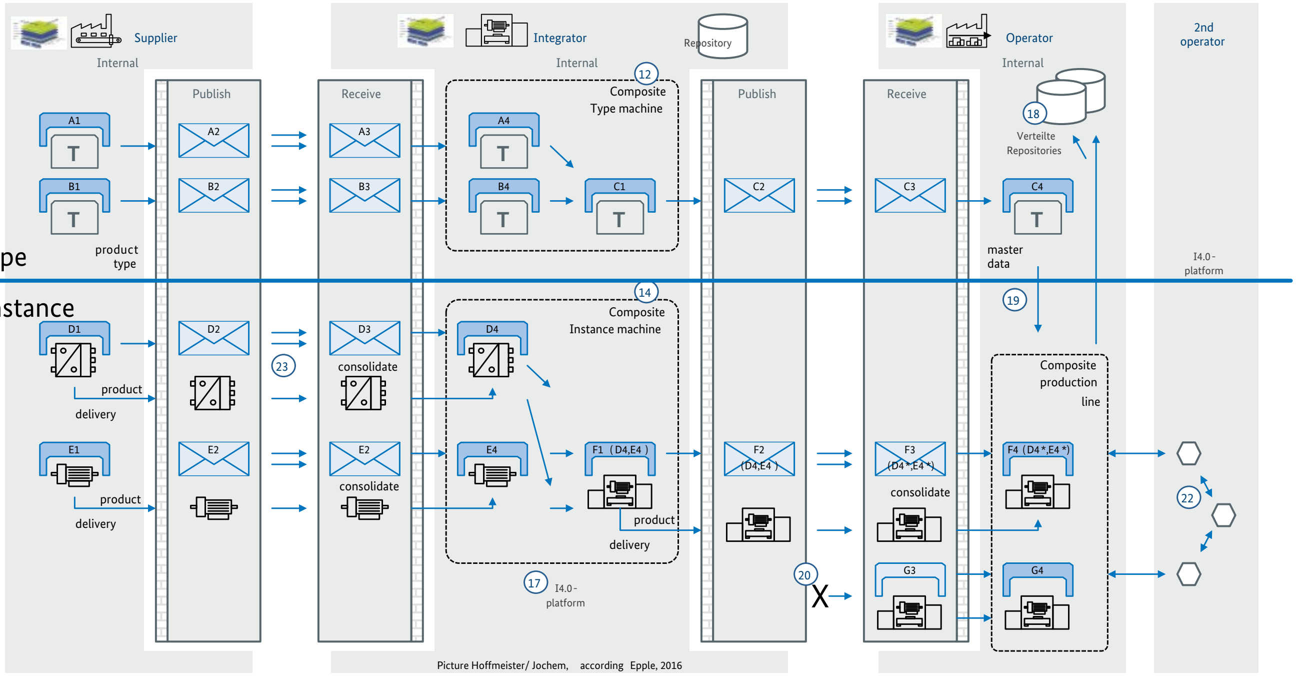
The present discussion paper focuses on the transfer of type information that is required for the engineering of an end product, here a drive ('CAE data') (see Figure 4). Type information is exchanged in the context of the RAMI4.0 life cycle model (3) and IEC 62890 (see Figure 1). From the point of view of the component manufacturer, use is being made of the available type information, whereas the integrator sees it flowing into their development process.

As a matter of principle, data can be transferred either offline or online, although the second of these two options will be of the greatest significance in Industrie 4.0.

The following case is analysed for the scenario:

- One of the integrator's employees is to design a drive.
- The manufacturer of drive components supplies the necessary CAE data about its products.
- This is dependent on an online connection.

Figure 3: Overall scenario taken from (2). Above: type information; below: instance data



Picture Hoffmeister/ Jochem, according Epple, 2016

Source: ZVEI

- To carry out their task, the employee is able to access the product data about the drive components, in which respect the support provided when components are selected (by characteristics, order numbers or similar criteria) will not be considered any further here.

- The CAE data can be compiled specifically for the customer as long as their account is valid. Not every customer receives all or the same data. For example, particular information might only be supplied if a confidentiality agreement has been concluded.

The interaction between the systems at the manufacturer and integrator's facilities will be analysed. To simplify the account that is given here, just one manufacturer will be assumed, but the analysis is also perfectly valid for the approach taken when several manufacturers are involved.

Figure 5 shows the technical systems that will play a role in the analysis:

- The type information is stored in an appropriate system at the manufacturer's facility, which supplies them in the necessary format when a query is made. In order to be able to decide whether and which data are supplied on request, a customer relationship management (CRM) database could be incorporated into the system.

- At the integrator's facility, an employee works on an engineering station to perform their task.

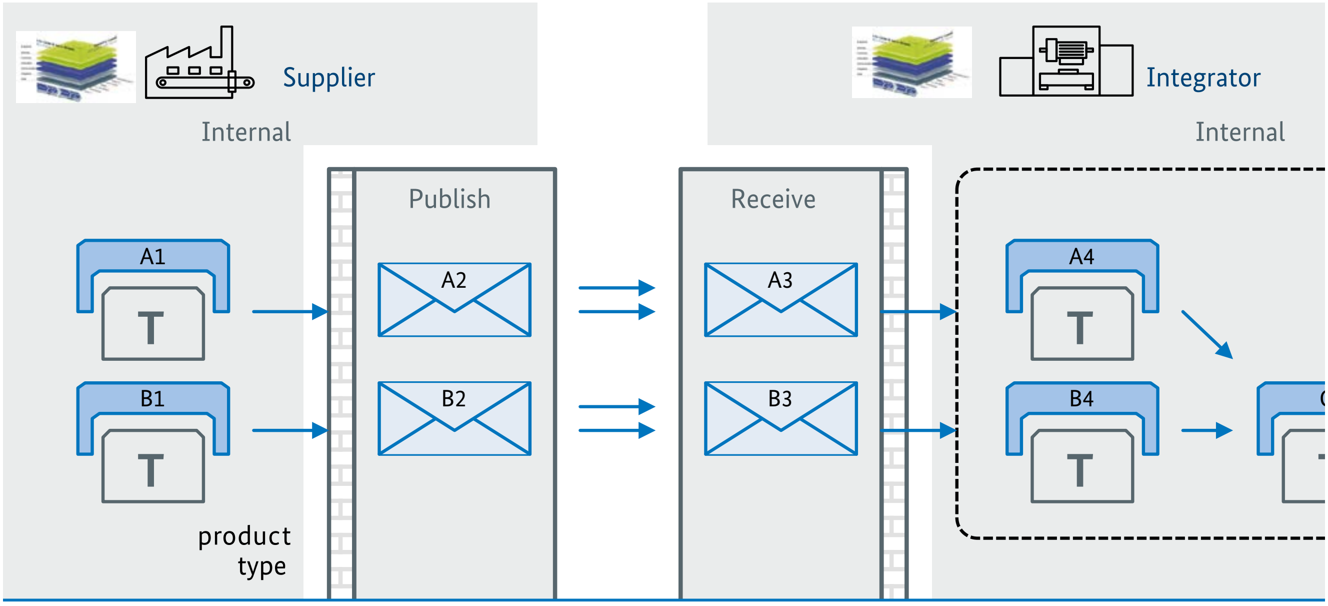
- The interaction takes place between the two companies, each of which constitutes a security domain in its own right and has implemented appropriate security measures – here represented by the security gateways.

Assumptions and definitions

As far as the transfer of the type information is concerned, it is assumed that this consists of data that, unlike process data, are not constantly changing. The transfer will therefore take place at a particular point in time and encompass a large data set. A model for the distribution of data updates is not looked at here. The transfer of process data imposes different requirements on communication systems.

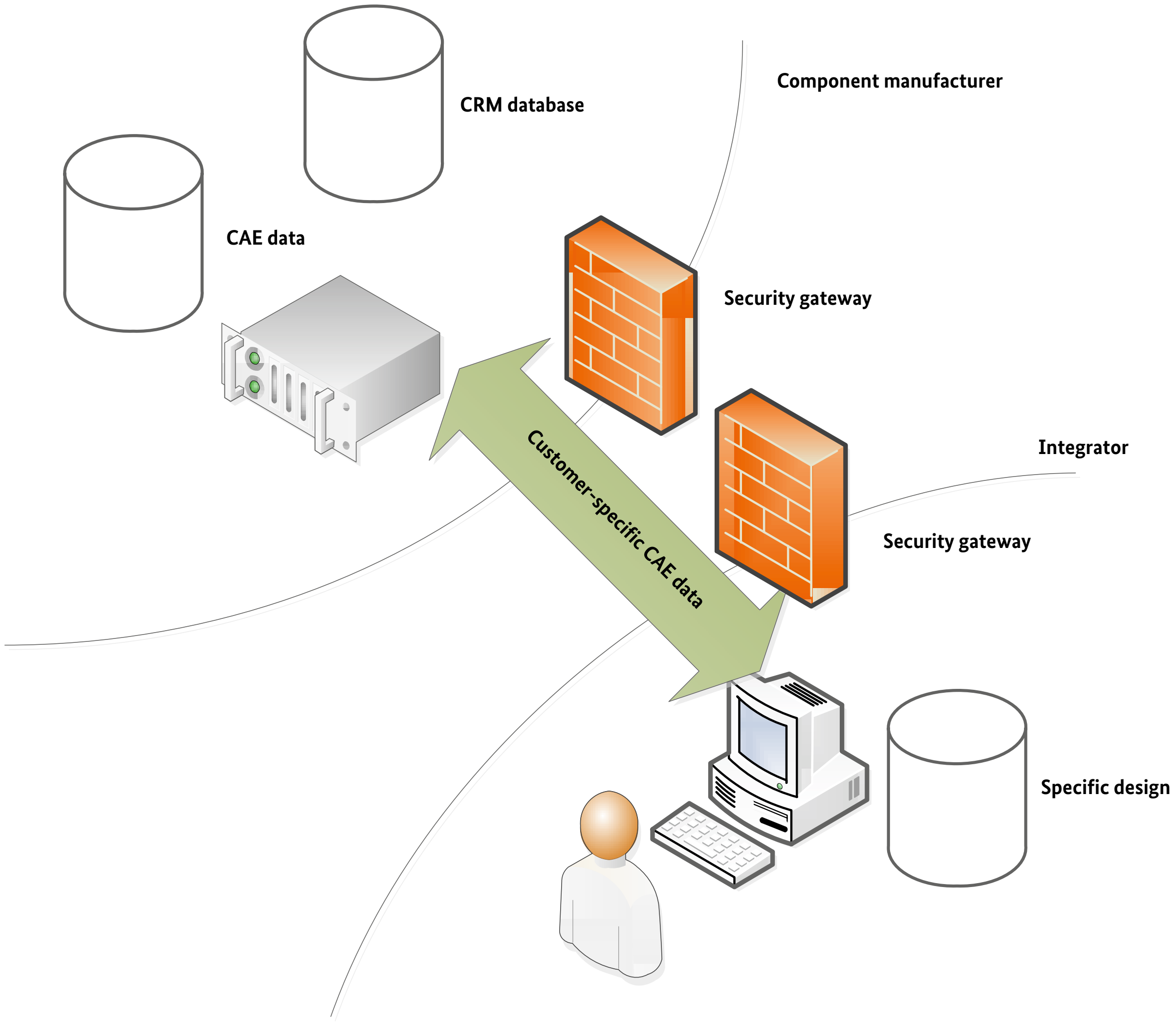
It is assumed there will be one or several files that, where applicable, can be brought together in an archive. The paper *Details of the Asset Administration Shell* (2) puts forward a format based on the Open Packaging Conventions (4). No limitations on the type information are presupposed so that, for example, executable programs may also be

Figure 4: Transfer of type information



Source: ZVEI

Figure 5: Systems involved



Source: Plattform Industrie 4.0

included and have to be taken into consideration in the security analysis.

The configuration of the data that are transferred, their structure and presentation are not considered in the present document. The customer-specific generation of the data set and its import into the engineering system also lie outside the scope of this document, as does the further use of the data. Business models could include a limited licence that sets how long users are able to access the data for. The enforcement of restrictions of this kind is typically termed digital rights management (DRM), and is in turn a technical topic in its own right that has little to do with the communication process as such.

The present analysis is focussed on the technical measures taken, and the organisational measures that accompany them. More wide-ranging legal analyses, concerning confidentiality agreements for example, are not undertaken.

Security

Information security measures serve to protect corporate assets and ensure compliance with statutory standards. The main security objectives are:

- confidentiality
- integrity
- availability

Further security objectives are drawn on to supplement or support these objectives:

- authenticity
- binding force
- non-repudiation

Additionally, the term reliability is used in the production field. Availability is usually expressed as a statistical value that reflects downtime or the speed with which operations are restored, one hour per year for example. Reliability means freedom from faults. In a physical process, even a single fault that lasts just ten seconds may have relevant impacts that could not be assessed by calculating a statistical mean.

Risk-based approach

To determine the security objectives to be met and/or the measures to be derived from them, a company's assets have to be identified and the threats that affect them described. A risk assessment can be undertaken on the basis of this threat analysis. When this is done, it is a particular challenge that the level of risk is calculated from the maximum harm an event would cause and the probability of its occurrence. However, events' probability of occurrence is hard to capture because threats are constantly evolving. Attackers' motivation and the publicisation of security flaws are contributory factors here that cannot be accounted for in the classic concepts of risk management.

- ISO 27001 (5), which is customarily applied in the corporate environment, therefore uses a classification of the levels of protection required for different kinds of information (e.g. public, internal, restricted, confidential) to support risk assessment and the drafting of packages of measures.
- The IEC 62443 standard (6), which was drawn up for the automation sector, additionally posits an attacker model as a basis for the definition of security levels for automation systems and components.

Communication security

In the present case of the exchange of CAE data, it is assumed that communication takes place between IT systems and, to this extent, the systematic approach set out in ISO 27001 finds application.

In many fields, the security approach is concerned with preventing security incidents by taking suitable measures. However, 100% protection is not possible, so detection (the identification of attacks) and response (countermeasures) are always addressed as well in the relevant standards (ISO 27001, IEC 62443 etc.).

In order to detect and avert attacks, it is necessary to monitor internal systems and the exchange of data with external business partners (ISO 27001: A.12.4, *Logging and monitoring*, A.12.2, *Protection from malware*, A.13.2, *Information transfer*). Alongside the logging of processes and the evaluation of these logs, the restriction and monitoring of communications are important instruments. The use of firewalls and proxy functions in the security gateway is consistent with the state of the art. In many companies, the direct communication of internal systems with the outside world is restricted to the http protocol. Encrypted communication is a particular challenge for monitoring. On the one hand, encryption ensures information is exchanged confidentially but, on the other, it allows the uncontrolled transfer of internal data from the company or the penetration of malware into its systems. As far as this is concerned, it is common practice today for encrypted communication to be 'split' at the security gateway so it can then be analysed appropriately in accordance with the relevant protocol. Content that does not comply with the protocol or cannot be analysed for other reasons is usually rejected in order to stop undesirable or dangerous data transfers. Exceptions can be set up, in which case the benefits of such an exception, making possible communication that would be blocked through other channels for example, have to be weighed up against the additional risks that will be faced. This is usually accompanied by an assessment of the communication partner's trustworthiness: for example, communication monitoring could be deactivated for banking transactions between employees in the accounts department and known financial institutions, because the protection of access data might enjoy higher priority than the threat posed by the interaction with the financial institution.

Interested groups

Information security always looks at a stakeholder and their corporate assets, which are dealt with in accordance with their relevant security objectives and risk assessment. Should the interests of various stakeholders be affected, different assessments of the same risk may therefore be reached. In order to compensate for this, agreements are necessary between stakeholders (confidentiality agreements, service level agreements, supplier management), because otherwise risks cannot be assessed and taken into consideration in a balanced manner. The negotiation of such contracts is an essential component of the pertinent standards, and is described, for example, in ISO 27036, *Information security for supplier relationships*.

Security domains can also be established within a company. A security domain is a technologically, organisationally or spatially coherent domain with uniform security requirements and/or a single security administration. In many companies, the office services/IT and production departments at least are security domains in their own right today.

Stakeholders

The application scenarios that have been set out can be used to identify various stakeholders with a view to the life cycle pursuant to the Reference Architecture Model Industrie 4.0 (RAMI4.0). The interplay of these stakeholders is shown in Figure 6, although only the stakeholders featured against a green background are considered in this discussion paper. In this respect, each of the stakeholders looked at has different requirements concerning the security of their information. These interests are described in detail in the present section.

To complement this, possible threats are described for each stakeholder. The implementation strategies for the handling of risk are discussed in an exemplary outline solution.

Component manufacturer

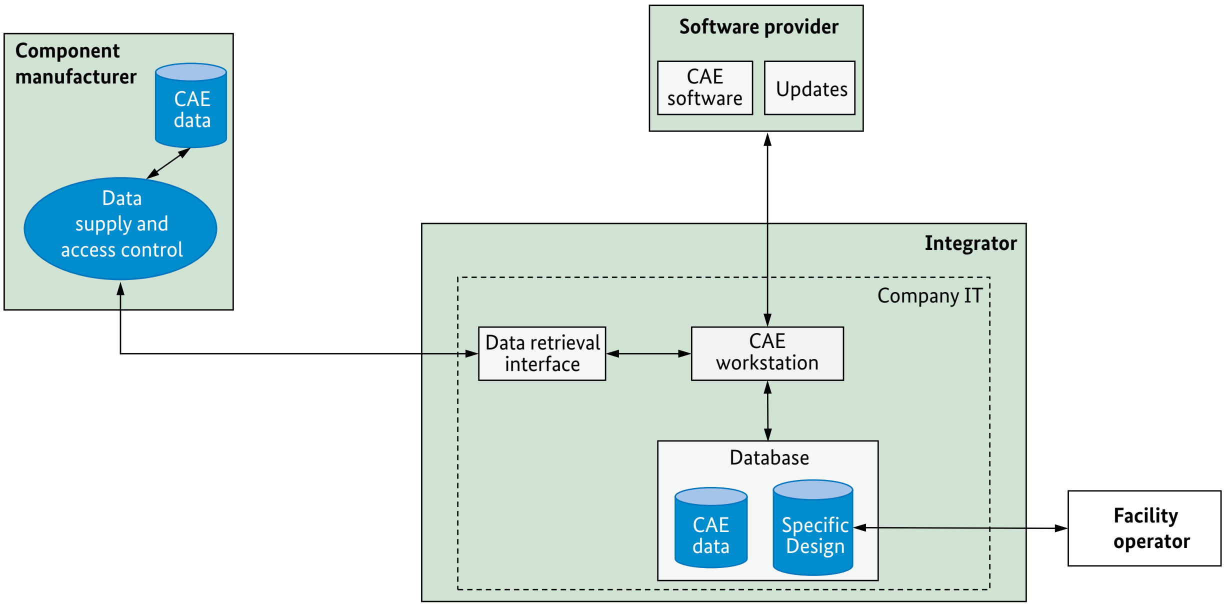
Roles and functions

The component manufacturer supplies its know-how for the integration and use of its own products. For example, it might supply a motor's speed regulation characteristic. The component manufacturer has to take suitable measures in order to protect its data from unauthorised use. In this respect, the confidentiality of the data is to be ascribed a high level of significance, and it is to be ensured that the data are sent to the correct recipient. DRM measures that are more wide ranging than this are not looked at here.

The component manufacturer and the integrator conclude an initial data usage contract in which, apart from the method used to retrieve the type information, the privileges of the employees who take part in the integrator's business process are also regulated. Today user accounts are usually set up by the manufacturer for this purpose, and the manufacturer's authenticity is verified by means of certificates. When this is done, the use of the accounts is to be limited by a validity period in order to prevent data continuing to be accessed when an employee leaves the integrator.

Access control by means of user accounts is known as Role Based Access Control (RBAC), and is established as the state of the art (see the section on 'Technologies used'). Use privileges are stored in a database, which has to be covered by the security concept. Not only that, this database offers the opportunity to establish new business models as posited in the Platform Industrie 4.0 application scenarios. It would therefore be imaginable for the component manufacturer to collate CAE data for the customer individually, depending on the payment model.

Figure 6: Interaction of stakeholders



Source: Plattform Industrie 4.0

Furthermore, measures to safeguard the integrity of information should be integrated into the component manufacturer's security analysis (7). The integrity of information has a direct influence on the quality of a product. The smallest alterations in a set of parameters for the drive control unit to be deployed by the integrator can result in deviations from the intended functionality as planned at the design stage. This can go so far that the quality of the products fabricated using the drive the manufacturer has designed is no longer consistent with their specifications, so triggering product liability claims.

The component manufacturer provides the integrator with an interface for the retrieval of the desired data. The interface is operated by the manufacturer's central IT department, and functions fully automatically. Under the Industrie 4.0 ethos, this means the requested CAE data are released without any intervention on the part of the manufacturer's employees, its back office sales department for example.

Risks

The component manufacturer maintains a CRM database for the administration of customer information. Apart from contact data, this database contains the contractually stipulated rules for the retrieval of CAE data. In order to make the requested data available to the user, they must be authorised to access those data. When the user is authorised, there is a danger of a potential attacker eavesdropping on the communication during the registration process and, where the commonly applied method of authentication with a user name and password is implemented, then obtaining the access data. With the aid of the access data, the component manufacturer's know-how could then be retrieved without permission by someone simulating a false identity. Attempts to forcibly obtain access to the data retrieval interface using brute force attacks, in which all possible permutations of the access data are tested out fully automatically, would also be imaginable.

Under certain circumstances, depending on the kind of attack and its scale, an attacker can take over the component manufacturer's whole IT infrastructure. If this happened in the application case, they could exploit the situation to manipulate CAE data. It would then be imaginable for them to falsify information that was going to be retrieved or attach malware to it: in other words, the integrity of the requested information could no longer be guaranteed.

Such interference is facilitated by the ability to open CAE data with write access rights. In order to prevent this, it should merely be possible for CAE data and other sensitive information to be opened from the CAE database in a read-only form. Furthermore, an attacker could exploit the access rights they had obtained to hoover up information. This means, for example, that the manufacturer's entire CAE data could be siphoned off in one go if the data on all components were retrieved.

Furthermore, the customer-specific information (data sheet for the physical product, CAE data, calibration data etc.) are supplied via a dedicated interface, a web service for example. The robustness of this interface against what are known as denial of service (DoS) attacks is to be ensured in order to guarantee the availability of the service that is offered.

Integrator

Roles and functions

In the application case that is analysed, the integrator is the instance in the value-creation chain that develops a technical solution to meet the customer's wishes, and supplies this solution to the customer for use in the customer's own products and facilities. The integrator retrieves the requisite information from the component manufacturer for this purpose.

The integrity and authenticity of the information are to be regarded as the most valuable goods to be protected if a faultless service is to be delivered. As a matter of principle, technical and organisational measures are to be taken in order, for example, to protect internal systems/infrastructure from infection with malware and log security incidents that have taken place. It is obvious to establish an information security management system (ISMS) for this purpose that describes suitable IT security measures on the basis of a previous risk analysis (see the section on the 'Risk-based approach'). The monitoring of outgoing communication continues to be an important function for the company's IT department (firewalls, gateways etc.), and makes it possible for undesirable communication to be detected.

Particular attention should to be paid to CAE workstations. These are normal employee PCs with dedicated engineering software installed on them, and are exposed to at least the same dangers as other systems involved in internal communication. These dangers include malware, in particular. Additionally, such engineering stations are also frequently deployed in special networks, like those for prototype construction, which entail additional hazards on account of what is usually their lower level of security.

Risks

The IT infrastructure forms the backbone for the administration of business processes, and is to be secured against potential attackers. In this respect, attention is mainly paid to protection against the infiltration of malware and the theft of business secrets. As far as this is concerned, it also has to be considered that employees can copy the component manufacturer's data, at their CAE workstations for example. Furthermore, it would be possible for product data to be manipulated so as to cause a malfunction in the facility operator's systems.

CAE software provider

Roles and functions

The CAE software provider supplies the integrator with a software tool for the development of its products. This software has two interfaces: a data retrieval interface for the component manufacturer's data, and a data retrieval interface for reading and writing in the integrator's in-house CAE database. This means there are two potential entry routes that are available to attackers.

In order to guarantee trustworthiness for the end user, it is therefore incumbent upon the software producer to issue regular security updates in response to vulnerabilities. In view of the extensive networking in Industrie 4.0, updates are also to be installed as soon as a participant wishes to get involved in Industrie 4.0 communication, so they do not represent a threat to other participants.

Risks

One risk posed to the integrator by the CAE software lies in the exploitation of vulnerabilities. Under certain circumstances, such vulnerabilities could be exploited to infect the CAE workstation with malware, which may in turn make it possible to gain access to the integrator's company IT system. The software producer consequently has a duty to implement its software to the best of its knowledge and in accordance with the state of the art, and to provide necessary security updates.

Access to CAE data (see Figure 2) could, for example, be gained by means of a plugin within the CAE software. Under certain circumstances, depending on the component manufacturer, a separate plugin has to be installed. Should this be done, there is a danger of the user installing untrustworthy software that, for example, opens up a second communication channel to an unauthorised party when it is used. This places a duty on the software provider only to permit the installation of trustworthy, tested extensions.

In this respect, external data sources (USB storage media, CD/DVD) and all types of data (3D models, executable files etc.) are also to be taken into consideration. The authenticity of the data should be checked using digital signatures. In order to reduce the risks from downloaded CAE data that are infected with malware, the data should be checked with a virus scanner before they are used. This could be supported technically by the CAE software.

Employee at CAE workstation

Roles and functions

The design of electric drives is undertaken by the employee at the CAE workstation. This work-station may be a specific development PC or the employee's own workstation with other programs, such as office applications, installed on it.

The main security objective here is the confidentiality of the information. Technical and organisational measures must be taken that prevent customer-specific project data leaving the company on pathways that are not foreseen for this, for example if they are copied onto USB storage media.

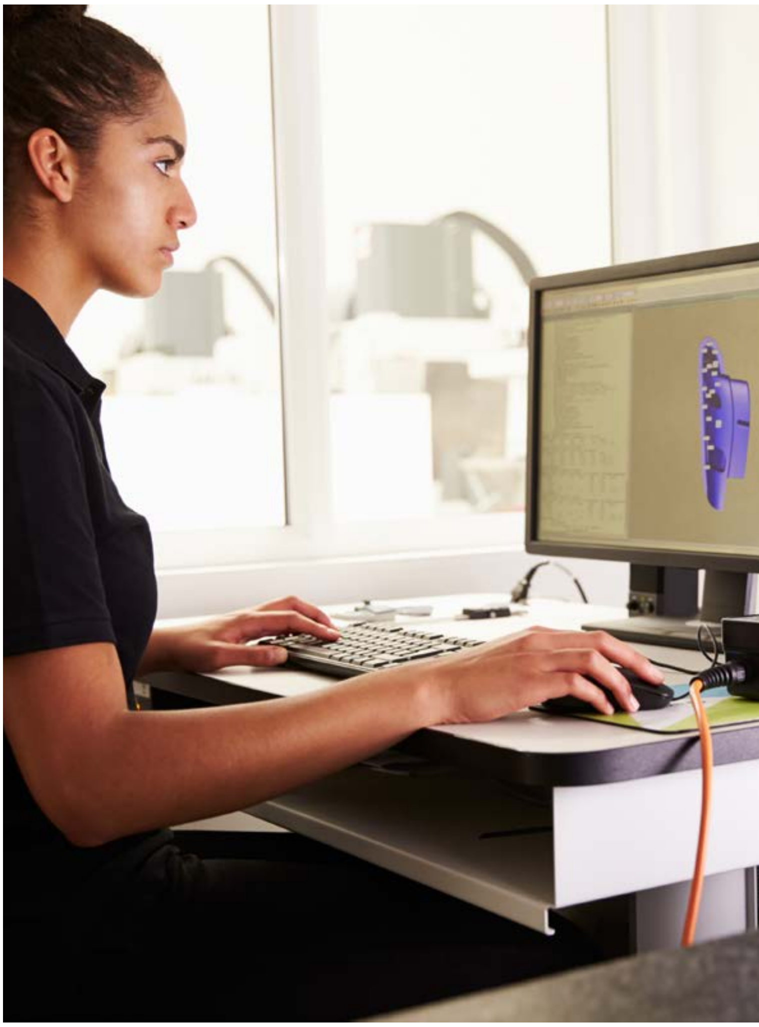
Another aspect is the safeguarding of the employee's personal rights, to which a special role has been ascribed with the introduction of the General Data Protection Regulation (GDPR). Under the application scenario, the user should be informed that a log file will be set up for each business process. If possible product liability claims are made, these log files can be used to clarify beyond all doubt whether the CAE data were defective when they were delivered or incorrectly used at the integrator's facility.

Risks from the employee

The threat scenarios for an employee at a CAE workstation have to be differentiated: the damage the employee can cause as a potential inside perpetrator has to be distinguished from the impacts due to unintentional errors.

The greatest threat is posed by the employee as an inside perpetrator. With their knowledge of the IT infrastructure, they can deliberately circumvent security measures in order to install malware and/or steal intellectual property.

The employee can also unintentionally become an inside perpetrator if malicious code is installed on the CAE workstation, from an apparently trustworthy email message for example.



Outline solution/discussion

An exemplary solution for the requirements described above will be proposed in the following section. This proposed solution combines available, well-known technical solutions with up-to-date results from other Platform Industrie 4.0 working groups. It is intended to serve as a basis for discussion in the further work that is carried out.

Ideas from the previous publications *Secure cross-company communication* (8) and *Secure Communication for Industrie 4.0* (9) are taken up in the proposed solution. At the same time, use is made, in particular, of the discussions in (9) about the realisation of security measures either with the instruments offered by the transport channel or with the aid of the message that is transmitted.

Technologies used

Before the actual approach taken to the secure retrieval of type information is discussed, common methods for web-based communication and the authorisation of business relationships will first of all be explained.

Web-based communication

Stable communication that functions reliably for all parties as far as possible entails various requirements concerning communication.

Existing IT infrastructure such as firewalls or proxies may block communication links on account of their source, their target or the communications port through which they are routed. A protocol analysis can also assess compliance with protocols, as well as the content that is transmitted. Preference is consequently to be given to well-known, well-established procedures and protocols that are consistent with the recognised state of the art, and are widely supported. The aim is to use as uniform as possible a concept in order to ensure that both communication partners find a common basis for communication.

HTTP and FTP are possible examples of protocols in the application-oriented layers (layers 5-7) of the ISO/OSI model that are well-established in a cross-company context. Both basic protocols allow the use of what are usually explicitly configured proxies, through which the flow of information can be channelled and, depending on the implementation, controlled as well. Information is also frequently exchanged by email, that is to say using the SMTP protocol. However, this option is not discussed any further in the present example of online data retrieval.

HTTPS, the variant of HTTP secured with TLS, is recommended, and the use of up-to-date versions of TLS (≥ v1.2) assumed as a prerequisite. As a matter of principle, it is left up to the communication participants whether they have the TLS connection established between the end devices in question or via infrastructure in the communication channel, for example through a proxy (end-to-end vs transport encryption). When devices are connected directly with TLS, it is possible to use certificates at the customer and server ends to ensure the identification and authentication of both systems involved in the communication with the instruments provided by TLS, so that certificates are mutually recognised. The information from the certificates can then be accessed on the Application Layer. Should this not be possible because no direct connection is established or the information on the parties' identities in the Protocol Stack is not forwarded, authentication has to be implemented on the Application Layer.

On the Presentation Layer and/or Application Layer, web services are used that work with protocols such as REST or SOAP; see the example in Figure 7 taken from the discussion paper *Secure Communication for Industrie 4.0* (9). One essential consequence of the possible use of proxies, in particular, is the shifting of authentication mechanisms to the higher protocol levels in the Application Layer.

Authentication and authorisation

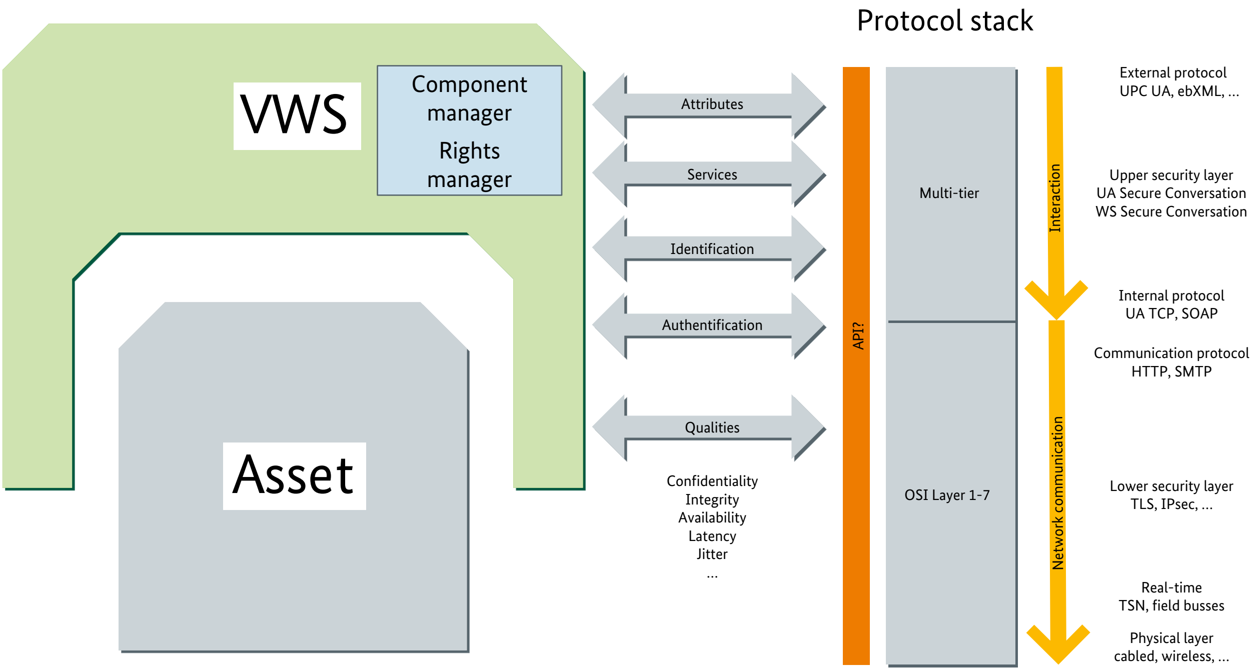
Once the user has been authenticated, the application can carry out authorisation, that is to say decide whether and/or which operations are permitted. In the present case of the retrieval of CAE data, this is a decision about whether and, where applicable, which data are supplied to the requestor. Many documents in the IEC 62443 series (6), such as parts 3-3, *System security requirements and security levels*, and 4-2, *Technical security requirements for IACS components*, make reference to Role Based Access Control (RBAC) in the context of authorisation. The concept is therefore to be explained here before the more powerful Attribute Based Access Control (ABAC) is discussed as part of the proposed solution.

Role Based Access Control (RBAC)

The RBAC mechanism is the classic approach to authorisation. Its realisation for the application scenario is shown in Figure 8.

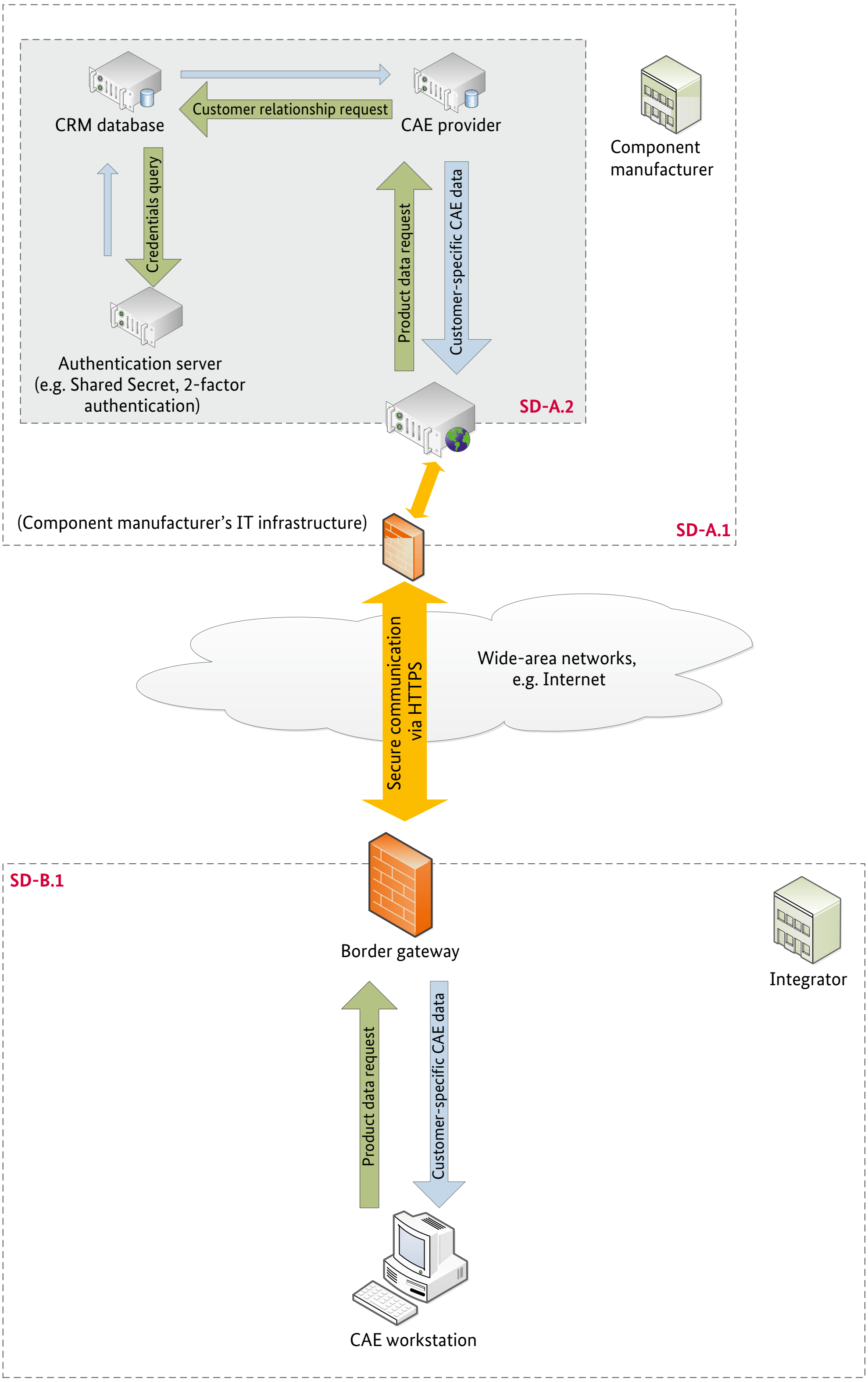
The employee at the CAE workstation generates a request to retrieve CAE data for the development of the electric drive. A request contains the performance characteristics of the components to be deployed, the motor's rated speed for example. The request itself is encrypted and transmitted to the component manufacturer via a secure communication channel. The transmission protocol deployed is HTTPS, which makes it possible to review the authenticity of the CAE data server and allows data to be transferred confidentially without being compromised.

Figure 7: Industrie 4.0 components and Protocol Stack (9)



Source: Plattform Industrie 4.0

Figure 8: RBAC mechanism for the chosen application scenario


CRM database
Customer relationship request
CAE provider
Component manufacturer
Credentials query
Product data request
Customer-specific CAE data
Authentication server (e.g. Shared Secret, 2-factor authentication)
SD-A.2
(Component manufacturer's IT infrastructure)
SD-A.1
Secure communication via HTTPS
Wide-area networks, e.g. Internet
SD-B.1
Border gateway
Integrator
Product data request
Customer-specific CAE data
CAE workstation

Source: Plattform Industrie 4.0

Before it is fed into the RBAC mechanism (see Figure 8), the request must initially pass the security gateway located on the boundary to the component manufacturer's Security Domain A.1 (SD-A.1), where it is validated in accordance with the manufacturer's security guidelines. The checked request is subsequently communicated to the component manufacturer's web server, which is located in Security Domain A.2 (SD-A.2).

Initially each of the integrator's employees has to register to retrieve CAE data with the component manufacturer, in whose system user accounts are set up. Data retrieval is subsequently initiated by the employee logging in to the manufacturer's system. For this purpose, the access data are transferred to the manufacturer via the secure HTTPS connection and compared with the access data stored in the authentication server. In the classic case, the access data consist of a user name and password or 2-factor authentication.

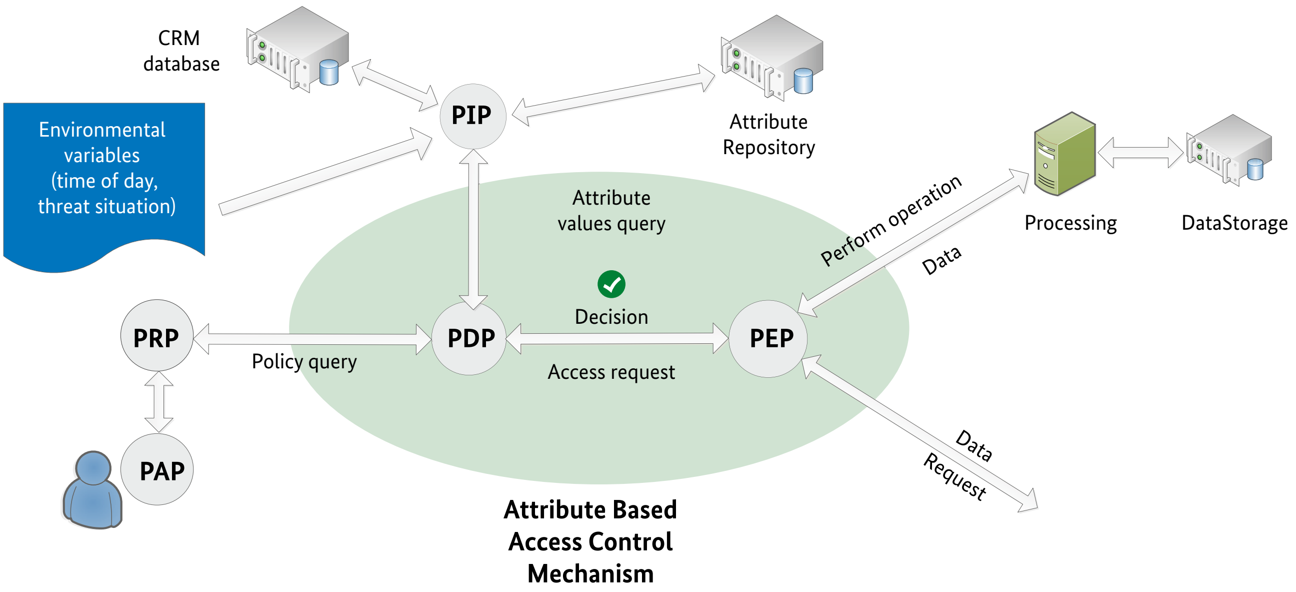
If authentication is successful, the CRM database reviews the user's privileges relating to the CAE data that have been requested. Once this has been done, it is possible that, depending on the business model, different CAE data may be supplied for each integrator. Finally, the employee has to authorise the launch of the business process using a password/2-factor authentication. The CAE data are subsequently transferred to the workstation via the same secure communication channel.

Attribute Based Access Control (ABAC)

A more flexible further development of the role-based approach provides for the use of attributes instead of roles: Attribute Based Access Control (ABAC). ABAC is a comparatively recent development and still not widespread in industry, but the concept's power is required for Industrie 4.0 (10). A technically sound implementation strategy is to be found, for example, in NIST Special Publication 800-162, *Guide to Attribute Based Access Control* (11), which forms the foundation for the outline solution.

The most important terms will initially be explained to ensure they are understood consistently.

Figure 9: The ABAC approach



Source: Plattform Industrie 4.0

- **Subject:** A subject is an entity that submits requests to perform operations upon an object. It may be a human user or an autonomously acting application. In this document, the subject is to be equated with the employee/ user.

- **Object:** An object is the resource upon which the subject wishes to perform an operation: a device, a file or a process for example.

- **Attribute:** An attribute is a characteristic of a subject, object or environmental variable. Attributes always consist of a name-value pair.

- **Policy:** A policy sets out the rules for, and relationships between, a subject and an object. For the ABAC mechanism, the policy consists of the subject's rights to access the object.

Compared to Role Based Access Control, which is relatively simple to realise, a large number of components are involved in the decision-making process under ABAC. Their interplay is shown in Figure 9. The eXtensible Access Control Markup Language (XACML) format (12) could be deployed for the internal processing and administration of policy information.

The Policy Enforcement Point (PEP) is foreseen as the element that enforces the ABAC mechanism. The first step is for the PEP to receive the request and convert it into an operational requirement, employee X (subject) is allowed to access (operation) document YZ (object) for example.

The Policy Decision Point (PDP) has the function of deciding whether access is granted to the requested data. It uses two sources for this purpose: the Policy Retrieval Point (PRP) and the Policy Information Point (PIP).

The Policy Retrieval Point (PRP) can be realised in the form of a database, and contains the company's current valid policies. The policies are administered by the Policy Administration Point (PAP), with the help of which adjustments can be made to the PRP. The PDP downloads policies from this database during the ABAC process.

The Policy Information Point (PIP) supports the PDP in the evaluation of policies. The Attribute Repository, current environmental variables (time of day, current threat situation etc.) and the CRM database serve as sources for the PIP.

More extensive subject attributes can be stored in the CRM database that, for example, may relate to contractual agreements between the component manufacturer and the integrator. By contrast, the Attribute Repository contains the approved object characteristics for the requesting subject. One simple example that can be mentioned here is that of documents classified as having the attribute 'restricted'.

Once the PDP has received all the necessary information, the request is evaluated against the policy. The decision is subsequently communicated to the PEP which, if a positive decision has been reached, approves the performance of the operation with the relevant information for its processing. The correct data can be compiled in line with this information, and records generated for tracking or billing purposes while the operation is being processed.

AASX file format

The document *Details of the Asset Administration Shell* (2) proposes a file format for the transfer of information between Industrie 4.0 components that is based on the Open Packaging Conventions (4). This file format, known as 'AASX', is able to use the fundamental characteristics of the Open Packaging Conventions. It offers a container within which information of all kinds can be transported.

The concept of the Open Packaging Conventions and their use in the AASX format support the verification of content using digital signatures so that the authenticity of the transmitted information can be tested at any time, irrespective of the transport route via which the data travel. When the AASX file format is used, it therefore ceases to be necessary to rely on communication protocols to ensure authenticity.

The encryption of data is not stipulated in the Open Packaging Conventions. Options for the protection of confidentiality are discussed for the AASX format in *Details of the Asset Administration Shell* (2). It is assumed in the present document that the protection of confidentiality is ensured by the transport method that is used, here the HTTPS protocol.

Proposed solution

The approach set out in this discussion paper envisages the implementation of Attribute Based Access Control (ABAC) so that its greater flexibility can be used in future concepts for cooperation between companies. Since ABAC places requirements on communication, details of the use of ABAC are explored in this proposed solution.

Security domains

The system conceived for the realisation of the application case is shown in Figure 10. Three security domains can initially be identified within the system: Security Domain SD-A is located at the component manufacturer's facility and divided into a domain for IT infrastructure (SD-A.1) and the domain SD-A.2, which accommodates the web service-based ABAC mechanism. The integrator owns the third security domain, SD-B, which contains the CAE workstation for the retrieval of type information.

Description of the approach

The solution that is outlined describes the logical steps for the retrieval of CAE data, in which ABAC is deployed by the component manufacturer (see Figure 10). A proposal for its technical realisation can be found in the discussion paper drawn up by the Platform Industrie 4.0 Sub-Working Group Roles and Legal Models (10). Figure 11 shows the steps in a swim lane diagram. In particular, the following steps are to be carried out:

Request to the component manufacturer

The employee at the integrator's facility has the task of designing an electric drive [1], for which they work on the CAE workstation. Since the information they require is not yet stored in the system, they use the CAE software to submit a request to the component manufacturer [2]. This request includes the object and subject attributes necessary for the ABAC process, as well as the operation that is to be performed. The harmonisation of the attributes and their significance with the data in the manufacturer's system is a necessary precondition in a cross-company context. The following are envisaged in the present example as relevant attributes, the transmission of which must be supported in the protocol that is used for the web services:

- Requestor (subject):
  - Employee with further attributes, such as role
  - Requesting company with further attributes
  - CAE software with further attributes, such as software version or licence key
- Information requested (object):
  - Kind/part number/selection parameter
- Desired operation:
  - Read/copy

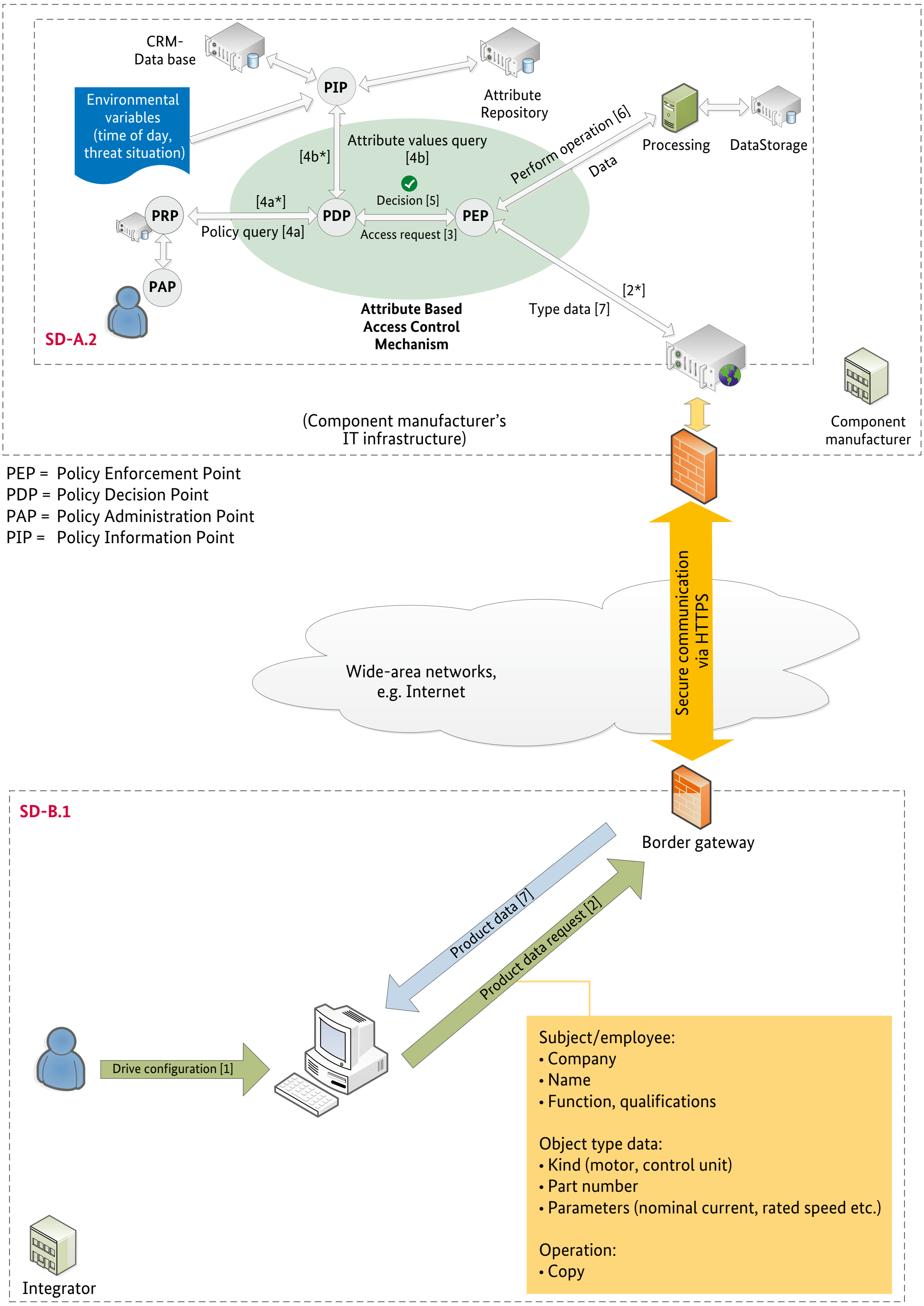
Transmission of request

The request now has to be transmitted to the component manufacturer via a secure communication channel. HTTPS is envisaged as the transmission protocol for this, which makes it possible to review the authenticity of the component manufacturer's download service, and allows the data to be transferred confidentially without being compromised.

As a first step, the request must pass the security gate located on the boundary of Security Domain SD-B.1. Several kinds of security gateway are common here, each of which has a direct influence on communications:

- If the security gateway is just a simple firewall, the request can pass it directly.
- If it is a simple proxy, the proxy will forward the stream of data in the request unchanged.
- If it is a proxy with authentication, the subject at the integrator's facility will have to prove their credentials to the integrator's proxy. This is frequently done with the subject's user name and a profile in a local Active Directory. Only if the user (or a system) has permission to communicate with the Internet will the connection be allowed through.

Figure 10: Realisation of the ABAC mechanism for the secure download of type information



Source: Plattform Industrie 4.0

- If it is a filtering web gateway, the content of the http data stream is analysed as well, and content that is either not permitted or dangerous, viruses for example, will be blocked. HTTPS connections combine this with the 'splitting' of the encrypted connection so that the content can be filtered. Splitting the connection in this way interrupts the integrity and confidentiality chain between the workstation and the component manufacturer, at the same time as making it impossible to use client certificates for authentication. Concepts intended to resolve this difficulty are found in proposals such as Multi-Context TLS for middleboxes (13), but have not been incorporated into standards, at least to date.

  A new encrypted communication connection to the component manufacturer is established at the web gateway's output port.

In a professional, corporate environment, it is to be assumed that filtering web gateways are deployed, and communication is to be organised accordingly. The proposed use of web services could be implemented in this fashion with Web Services Security (WS-Security) in SOAP. The access data would be included in the request in the form of security tokens, and the request would be digitally signed.

At the component manufacturer's end, the request first of all has to pass the security gateway located on the boundary to Security Domain SD-A.1, where it is validated in accordance with the manufacturer's security guidelines. The checked request is subsequently communicated to the Security Domain SD-A.2 web server. To begin with, an initial check on the consistency of the request is carried out in the web server, then the subject's access privileges are determined using ABAC (see Figure 10, process 2*).

Authentication and authorisation

The access control mechanism shown in Figure 10 validates the request in accordance with the approach described in the section on 'Attribute Based Access Control'. The authenticity of the request has to be checked at this point. This could be done by attaching a digital signature to the request, and confirming the requestor's identity and attributes with an X.509 certificate.

What is important is that messages are exchanged between the systems involved in the component manufacturer's ABAC structure at process steps [3], [4] and [5] in Figure 10 via a secure communication channel. It would also be imaginable and, under certain circumstances, appropriate to relocate the Policy Decision Point (PDP) and the Policy Enforcement Point (PEP) to a different security domain. This would offer the advantage that an attacker would have to overcome another barrier before they were able to manipulate the decision.

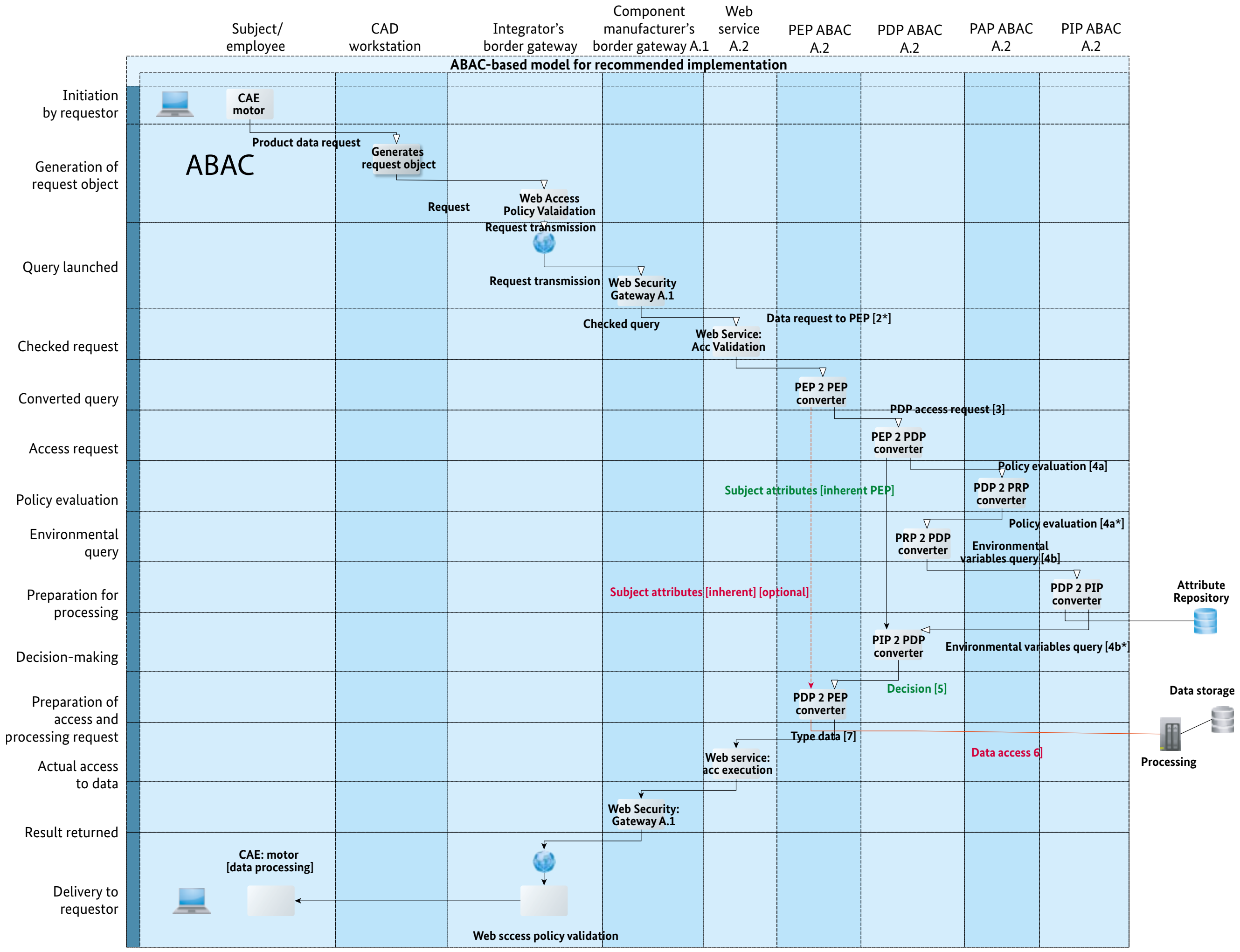
In order to validate the object and subject attributes in the request against the current policy, that policy should also have an attribute-based structure. The eXtensible Access Control Markup Language (XACML) format, which has been standardised by OASIS (12), is available for this purpose. Under this standard, a policy consists of rules that the requesting subject models in the form of a target.

Should it have been possible for the request to be successfully validated by the PDP, the PEP permits the performance of the operation [6]. In the application case, the computer labelled 'Processing' is accessed by means of web services. This computer generates an instance of the requested CAE data in line with the object attributes that have been transmitted.

Transfer of the data set to the requestor

In the final process step [7], the type data are sent to the CAE computer. The data are encrypted and transferred via the same secure connection for this purpose. When this is done, the data set remains reviewable during and after the transfer thanks to the use of the AASX format's signature mechanisms. This is dependent on support for the AASX format in the security gateway.

Figure 11: Swim lane diagram illustrating the proposed solution



Source: Plattform Industrie 4.0

Summary and outlook

This document describes the security requirements placed on the secure retrieval of CAE data, that is to say type information, from the perspectives of the participating stakeholders. On the basis of these requirements, a proposed solution is elaborated, which takes up other Platform Industrie 4.0 concepts, such as the file format for the exchange of information by administration shells and rights management in relation to Industrie 4.0 components.

Core statements

The use of web services via HTTPS is to be recommended for the cross-company retrieval of CAE data. On account of the frequent use of security gateways, authentication with X.509 certificates should not be stipulated as a precondition on the TLS Transport Layer. In the example, the data are exchanged with the AASX data format, which already provides mechanisms to protect their integrity and authenticity.

Links to other topics

The configuration of secure communication cannot be seen in isolation from other topics that are being discussed and elaborated in parallel. In particular, the implementation of rights management in the Industrie 4.0 context demands the secure supply of information on the identity of the communication partner. Communication systems have to support this technically, for example with secure authentication and the secure transfer of attribute information. It is also necessary to realise a structure for the mutual recognition of identities and digital certificates.

The International Data Spaces Association is working on its own concept for the secure exchange of data, including exchanges of data in the industrial environment. There are plans to draw up a comparative discussion paper.

Transfer of instance information

One related topic is the exchange of information about individual entities ('instances'), in which the same proposed solution or a further development of it may possibly be deployed. The analysis of its security will require an appropriate application scenario and identify different or additional requirements.

Information about an entity could, in principle, be retrieved by the entity itself. A technical product could, for example, retrieve licence rights, which would mean the product would know the services it was able to offer. The entity itself would then be in a position to prove its own credentials.

In other possible scenarios, a user or system might wish to retrieve instance-specific data, such as calibration data. Under this scenario, the additional difficulty has to be considered of how the user would be able to prove they actually had a right to confidential data, for example because they were the owner of the entity or the entity was in their possession. The significance and use of (secure) identities will have markedly greater prominence in the future.

Glossary

ABAC	Attribute Based Access Control
Brute force attack	Attack in which access data are decoded by automatically trying out all possible combinations
CAE	Computer-aided engineering
CRM	Customer relationship management
DRM	Digital rights management
HTTPS	HyperText Transport Protocol (S: secured via TLS)
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
PRP	Policy Retrieval Point
RBAC	Role Based Access Control
SD	Security domain
TLS	Transportation Layer Security
XACML	eXtensible Access Control Markup Language

List of figures

References

1. **Ergebnispapier „Fortschreibung der Anwendungsszenarien der Plattform Industrie 4.0“**.
Berlin: *Plattform Industrie 4.0*, 2016.

2. **Details of the Asset Administration Shell**, Part *1: The exchange of information between partners in the value chain.*
Frankfurt: ZVEI, 2018.

3. **DIN SPEC 91345:2016-04:** *Referenzarchitekturmodell Industrie 4.0 (RAMI4.0).* Berlin: Beuth Verlag, 2016.

4. **Information technology** – *Document description and processing languages – Office Open XML File Formats – Part 2:*
Open Packaging Conventions. ISO/IEC 29500-2:2012.

5. **Information technology** – *Security Techniques* – Information Security Management System. ISO/IEC 27000:2014.

6. **Industrial Communication Networks** – *Security for industrial automation and control systems.* IEC 62443.

7. **Discussion Paper “Integrität von Daten, Systemen und Prozessen als Kernelement der Digitalisierung“.**
Berlin: *Plattform Industrie 4.0,* 2018.

8. **Technical Overview: Secure cross-company communication.** Berlin: *Plattform Industrie 4.0,* 2016.

9. **Discussion Paper “Secure Communication for Industrie 4.0”.** Berlin: *Plattform Industrie 4.0,* 2017.

10. **Discussion Paper “Access control for Industrie 4.0 components for application by manufacturers, operators and integrators”.** Berlin: *Plattform Industrie 4.0,* 2018.

11. **Guide to Attribute Based Access Control (ABAC)** – *Definition and Considerations. s.l.:* NIST, 2014.

12. **OASIS. eXentsible Access Control Markup Language (XACML) Version 3.0.** [PDF] 2017.

13. **And Then There Were More: Secure Communication for More Than Two Parties.** Nayler, David, et al., et al.
Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies. 2017.

AUTHORS

Carsten Angeli, KUKA Roboter GmbH | André Braunmandl, Federal Office for Information Security | Prof. Tobias Heer, Hirschmann Automation & Control GmbH | Dr Christian Haas, Fraunhofer IOSB | Markus Heintel, Siemens AG | Dr James Hunt, Aicas GmbH | Dr Lutz Jänicke (chair), PHOENIX CONTACT GmbH & Co. KG | Fabian Mackenthun, NXP Semiconductors Germany GmbH | Jens Mehrfeld, Federal Office for Information Security | Till Oefler, Institute for Automation and Communication | Florian Patzer, Fraunhofer IOSB | Tobias Pfeiffer, Festo AG & Co. KG | Wolfgang Stadler, SICK AG | Detlef Tenhagen, HARTING Stiftung GmbH & Co. KG | Klaus Theuerkauf, Siemens Mobility GmbH | Dmitry Tikhonov, Assystem Germany GmbH | Thomas Walloschke, Fujitsu Technology Solutions GmbH

This publication is a joint outcome of the work by the Working Groups on Security of Networked Systems and Reference Architectures, Standards and Standardisation (Plattform Industrie 4.0).

www.plattform-i40.de