PLATTFORM INDUSTRIE 4.0

DISCUSSION PAPER

Integrity of Data, Systems and Processes as the Core Element of Networking and Digitalization

In Cooperation with

ZVEI: Die Elektroindustrie

Imprint

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

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

Design and production
PRpetuum GmbH, Munich

Status
April 2018

Print
MKL Druck GmbH & Co. KG, Ostbevern

Illustrations
monsitj – Fotolia (Title), peshkov – Fotolia (p. 4),
sdecoret – Fotolia (p. 15), kiri – Fotolia (p. 19)

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.

FSC
www.fsc.org
MIX
Paper from
responsible sources
FSC® C108626

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

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

Contents

1. Objective and scope

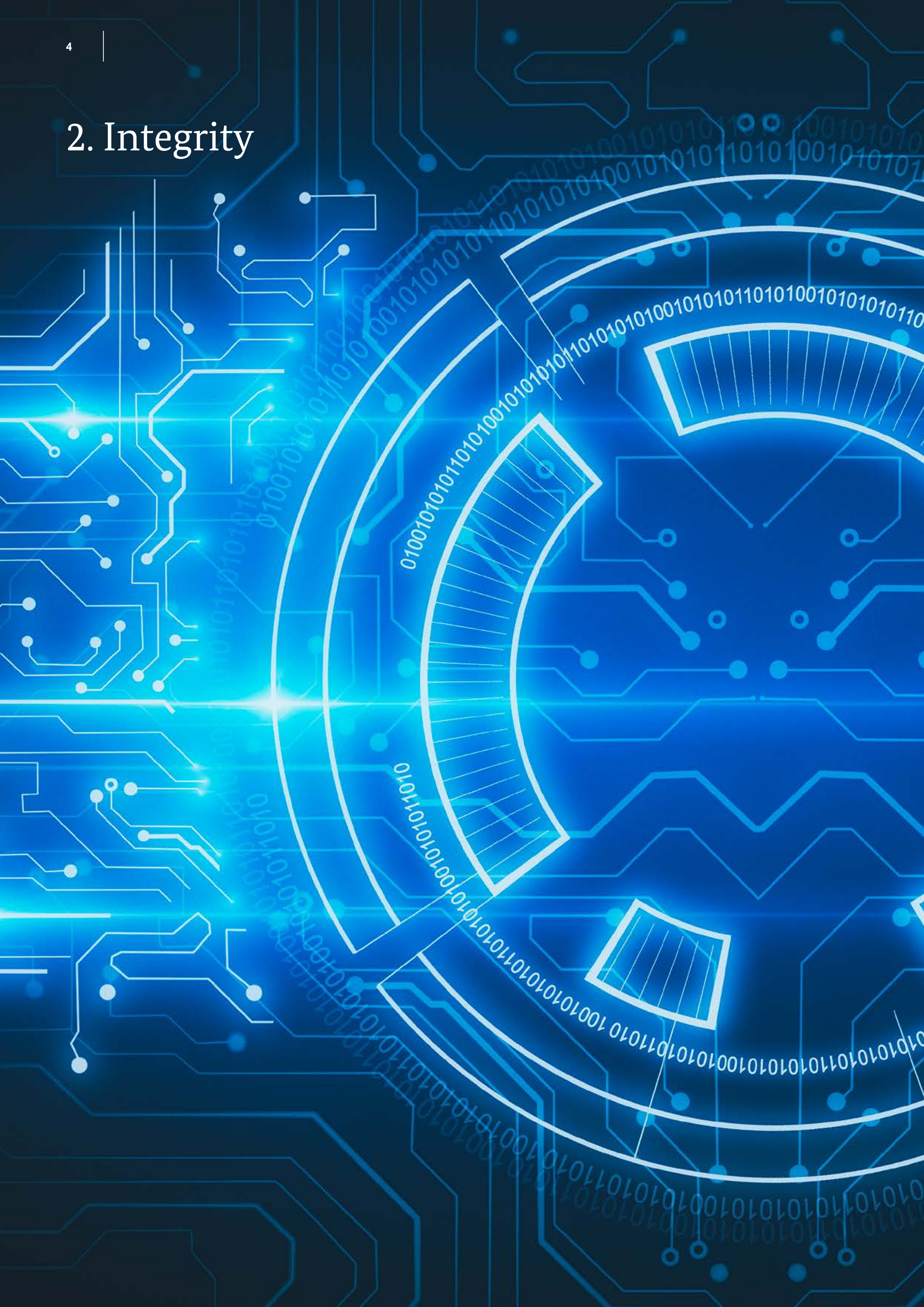
This white paper summarizes the ongoing technical discussions of SG security group of ZVEI regarding requirements, validation, and implementation of data, system, and process integrity.

The objective of this document is to develop a common understanding of the subject of integrity in context of international cross-company cooperation and increasing digitalization of industrial products and systems (i.e. Industrie 4.0, Industrial IoT). The paper serves as a basis for discussion, consolidation of knowledge and guidance for other working groups in the field of industrial security and Industrie 4.0.

The document addresses the question as to what extent the correctness, completeness and integrity of data, systems, and processes can be assured. The focus is put on technical data. This means that the personal data and the aspects of user privacy are not covered.

The paper is particularly relevant for component manufacturers, integrators, service providers and operators. Issues in the context of international supplier relationships and cross-company cooperation are relevant both within and beyond the security community. This white paper is also intended for personnel responsible for product management and procurement.

2. Integrity



2.1 Background: digitalization and networking

With the growing trends for digitalization and networking, dependence on the correctness of internal and external data, systems, and processes is also increasing. This is essential for all business process within and outside a company. Integrity is often viewed as a technical aspect, but it has a direct impact on aspects like profitability, reputation and regulatory responsibility.

Digitalization

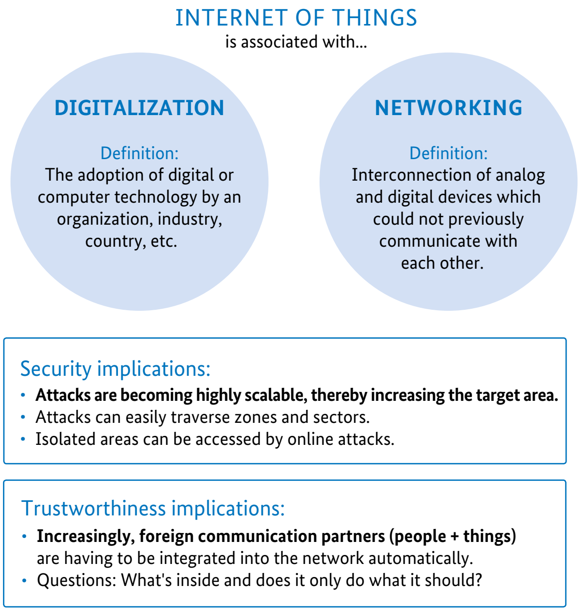
The interconnection of physical things is progressing in many areas of our daily life. Essential pre-requisites for the Internet of Things (IoT) and the Internet of Everything (IoE) are ‘digitalization’ and ‘networking’. These lay the foundations for an economy of things and services. For instance, interconnection of components in the area of energy networks, cities, households, and manufacturing environments are leading to the advent of smart grids, smart cities, smart homes, and smart industries (= Industrie 4.0). Current estimates predict that by 2020, about 50 billion things will be linked via the Internet of Things (IoT). In the future, connectivity between people, processes, data, and things, generally referred to as the Internet of Everything (IoE), will increase considerably.

The concept of digitalization implies that digital or computer technology is increasingly adopted by an organization, industry, country, etc. Although the terms “digitization” and “digitalization” are not always distinguished clearly, the term “digitization” refers to the digital representation of analogue data. In the context of this paper, however, the implications on integrity coming from an increasing adoption of digital, computer-based technology in industrial systems is discussed.

In the past, procedures were performed mechanically or electronically by fixed circuits. During recent decades, a transition to more flexible products comprising more software components has taken place. Although software has been used in production environments for decades, a much broader range of devices is now available with the ability to execute any type of code. Particularly in the context of the Internet of Things (IoT) and its industrial counterpart, the Industrial Internet of Things (IIoT), devices are not only equipped with arithmetic and logic units, but are also equipped with computer-based systems, various software, and communication interfaces. In contrast to mechanical and fixed electronic solutions, devices comprising software are more flexible as their software can be updated or reconfigured to modify their features. On the other hand, an operator cannot always be sure about modifications in functionalities of the device after a software update. This situation becomes particularly critical when one considers the possibility of software modification or reconfiguration by an attacker. Through vulnerabilities, e.g. buffer overflows, or unsafe software uploads, an attacker can manipulate the software of a device, so that its functions are altered, restricted, or new (unwanted) functions are added.

Networking

Networking is achieved through communication at all levels, including across corporate and sectoral boundaries. For instance, this includes communication within operational technology (OT), and communication between OT and information technology (IT). It also includes communication between manufacturers, suppliers, customers, and other partners.



INTERNET OF THINGS
is associated with...

DIGITALIZATION

Definition:
The adoption of digital or computer technology by an organization, industry, country, etc.

NETWORKING

Definition:
Interconnection of analog and digital devices which could not previously communicate with each other.

Security implications:

- **Attacks are becoming highly scalable, thereby increasing the target area.**
- Attacks can easily traverse zones and sectors.
- Isolated areas can be accessed by online attacks.

Trustworthiness implications:

- **Increasingly, foreign communication partners (people + things)** are having to be integrated into the network automatically.
- Questions: What's inside and does it only do what it should?

Source: ZVEI

In general, IT and OT have common basic security objectives of confidentiality, availability, and integrity. However, they are differently prioritized in typical IT and OT environments. So far, availability and confidentiality have been ensured by the operator's knowledge of all the equipment involved. With the increasing use of networked digital technologies, dependency on external communication partners and their behaviors is growing.

Consequence: Changes in the established industrial environment due to digitalization and networking

- Security concepts must be extended from within company to cross-company protection.
- The boundary between production OT and office IT disappears over time.

2.2 Importance of integrity protection

With the growing trends for digitalization and interconnected devices, reliance on correctness of internal/external data and accurate operations of systems/processes is also increasing. This is essential for all business processes within and outside a company. Although integrity is often viewed as a technical aspect, it has a direct impact on profitability, reputation, and regulatory responsibilities.

In industrial environments, integrity has a direct impact on the operations of a manufacturing plant and the quality of manufactured products. The influence of integrity on the quality of products becomes obvious when one considers the consequences of a lack of integrity in the manufacturing process. Provision of incorrect data by sensors and control systems can lead to the production of faulty or insufficiently precise products. As a result of incorrect sensor readings, these faulty products may even go unnoticed during quality assurance processes. This can extend as far as the delivery of malfunctioning, unreliable products to the customer, leading to damage to the manufacturer's reputation and liability issues.

In addition to the product-quality related consequences discussed above, a non-integrity protected manufacturing plant can have reduced availability. Even if the sensor and control information has been transferred correctly, the control system may not be able to evaluate this sensor data correctly or perform consequent actions if its integrity is not ensured.

Similarly, a lack of integrity can have a drastic impact on safety-critical systems and processes. If incorrect data is processed by safety-critical applications, the application may result in fatal errors. This is particularly relevant for regulatory requirements and responsibilities.

Thus, ensuring integrity within an industrial plant is of the utmost importance for manufactured products, the safety of manufacturing processes and compliance with regulatory requirements. If several industrial plants are interconnected, integrity protection is vital for all of them as they can be considered as a single production cell.

2.2.1 Importance of integrity for other objectives

The protection of the integrity of data and systems is a prerequisite for achieving the other objectives, such as availability and confidentiality.

Processes based on non-integrity protected data and systems are most likely to be erroneous. Furthermore, if there is no integrity-violation detection mechanism, the result will be inaccurate products and incorrect data. These consequential errors are no longer recognizable as integrity errors, since any protective measures will be re-applied and output data will not be rechecked. In this respect, integrity monitoring measures based on appropriate application-dependent assessment of the effects are useful, as recommended in Section 2.6.

Correspondingly, detection of integrity violation can lead to reduced availability or even emergency shutdowns. For instance, typically incorrect data is directly discarded if the data is originally protected by (cryptographic) checksums. Depending on the application, availability can be enhanced if the data is re-supplied by means of redundancy or retransmission despite a possible delay. Availability is affected where a process is interrupted due to discarded, erroneous data, but the impact of this is less than the results of usage of faulty data.

In particular, system integrity is important for confidentiality. If a system is compromised, an attacker may be able to read confidential data or the encrypted communications at the endpoints. Therefore, various standards and recommendations require that the integrity of the cryptographic systems is checked during start-up and/or operation. Most protocols for storing or transmitting data combine encryption with cryptographic integrity-protection mechanisms.

Key Point:

- Integrity protection of data, systems and processes is important and forms the foundation for other objectives, such as availability and confidentiality.

2.3 Aim: data and system integrity

The integrity of a component or a system describes the integrity of its functionality, i.e. the integrity of a device or system exists if its behavior/functionality is as desired and described.

Integrity can be defined for each component and implementation level of a device: hardware, operating system, drivers, applications, and configuration parameters. An integrity-protected device includes tamper protection as well. The overall integrity of a device includes assessment of the integrity of all of its subcomponents.

The term "integrity protection" is used to describe mechanisms/functions that prevent unauthorized modifications and thereby prevent unauthorized manipulation. For example, one of the well-known integrity protection mechanisms for data exchange is Message Authentication Code (MAC). A classic Cyclic Redundancy Checksum (CRC) is itself vulnerable to manipulation, and is therefore not an integrity protection mechanism. Note that this paper uses the term integrity within a security context, considering intentional manipulations.

However, while considering integrity, dynamic aspects must be taken into consideration as well. These include unauthorized changes during system operation. For example, if data from sensors of a production line is transmitted to a human-machine interface (HMI) and the data is processed accordingly before being displayed, this is a desired change in the data. Likewise, authorized changes to system functions can be made due to necessary hardware replacement or by planned software upgrades. These legitimate dynamic changes must not lead to any loss of integrity, so functions for "integrity protection" must be appropriately designed and flexibly adapted.

When considering integrity, the following questions shall be addressed:

Integrity protection of the data:
When looking at the requirements, it is necessary to distinguish between data in transit and data at rest, i.e. the stored data.

For the data in transit:

- **Integrity protection of data during transmission:** How can it be reliably detected whether the data has not been corrupted while it was being exchanged between different components? Or how can it be ensured that transmitted data has arrived correctly? Or how can it be ensured that the data was not modified, neither via random variations nor by deliberate changes, during transmission?

- **Authenticity of data during transmission:** How can it be reliably detected that transmitted data was sent by a particular component? How can the authenticity of the transmitted data be checked? It should be possible to check whether data was sent from a particular component and not created by an attacker or imported or modified during the transfer.

For the data stored on a component:

- **Integrity of data at rest/stored data:** How to ensure that the data has not been tampered with since the last check? For example, this can be relevant for system configuration data. Integrity of data at rest includes recognition of targeted and random variations.

- **Authenticity of data at rest/stored data:** How can you reliably recognize who has stored the data, who the data is from, or who made the last change?

For desired operations of system/components, it is essential that the data (such as control commands, configuration parameters, etc.) is stored and exchanged without any alteration. Without integrity protection of such data, secure and correct operations of a system/component cannot be ensured. The commands that are sent to or from a system controller such as required engine speed, signal for emergency shutdown, etc., must be protected against manipulation by an attacker.

Integrity of the system:

- How can one ensure that the components involved in data communication only serve their intended functionality?

  For example, it is also possible for another part of the control software to have vulnerabilities that can be exploited by an attacker to influence behavior of the control system in such a way that an emergency shutdown is no longer executed.

2.4 Considering integrity of the entire system

Usually, an industrial system consists of multiple subsystems that communicate with each other. Each subsystem should be protected against unauthorized manipulation, as the integrity of the overall system is dependent on the integrity of its subsystems. Additionally, integrity of the data exchanged between these subsystems must also be taken into consideration while looking at the overall integrity of the system. The entire system can be considered as integrity-protected if all of its subsystems and communications between its subsystems are tamper-resistant. Conversely, lack of integrity of one subsystem or communication path can have significant effects on the integrity of the entire system.

The impact of lack of integrity of a subsystem depends on its role in the overall system. For instance, a manipulated central controller can result in far more severe effects compared to a component that does not have a significant influence on the manufacturing line or the final product. In order to assess the consequences of a violation of integrity of an individual component, a detailed examination of its impact on the entire system is necessary. Integrity violation consequences can range from negligible impact to threats to life and the environment. Therefore, the assessment of the entire system entails an assessment of subsystem failure.

2.4.1 Parameters and interDependents

While a quantitative assessment of integrity (e.g. “the system is 78 % integrity-protected”) is not feasible, qualitative consideration of integrity enables the design of compensatory measures. Multi-dimensional reasons resulting in loss of a system’s integrity should be taken into account.

These may include:

- **Changes in the system over time:** Complex industrial systems are often used over long periods of time. This means that these industrial systems have been modified to adapt various requirements. With time, these adjustments could have adverse effects on the ability to resist attacks. For instance, a system that has become more insecure over time can be modified by an attacker, so that either the system or data integrity is no longer guaranteed. Proactive measures can compensate for increasing vulnerability through additional audits or by isolation of the system.

  Example scenario: A firewall is configured for an application. Later, this application is replaced by another application, but the firewall rules are not adapted. Therefore, these changes in the software or configuration parameters of the applications can lead to undesired interactions, as in this particular scenario, the firewall is not adjusted/updated in line with the application.

- **Ageing of crypto-algorithms with new scientific advancements and higher computing capacity:** Rapid technical progress and new scientific findings result in the ageing of existing cryptographic algorithms. In the past, cryptographic mechanisms had to be replaced after a few years, since they lacked adequate protection. Two known central elements to ensure data integrity are cryptographic hashes and macs and digital signatures. These mechanisms have also suffered from ageing. Therefore, while designing systems, it is important to consider the interchangeability of cryptographic algorithms. During system operation, it is necessary to regularly check the credibility of the employed cryptographic algorithms. Otherwise, an inadvertent change of data and systems is highly likely.

- **Technical progress in offensive security:** Security researchers and attackers are constantly developing new methods of attack against existing systems. The discovery of a new attack often leads to an abrupt loss of assumed integrity of a system. In this case, either insecure software components must be updated or additional compensatory measures (e.g. detection and isolation measures) must be employed to maintain integrity.

- **Human errors and faulty operations:** During system operation or configuration, incorrect entries or undesired modifications to the wrong component may occur.

Therefore, automatic detection of error must be possible in such scenarios.

- **Technical failure and environmental influences:** In case of faults in the system hardware or disturbing environmental influences (such as electromagnetic radiation, etc.), random changes in data (in transit or stored) may occur. Such errors must be recognized and handled accordingly. In such scenarios, redundant storage, error correcting, and re-transmission mechanisms can be employed to restore correct data.

Even when considering a single system, it is possible to identify sub-components which have an influence on the system. Important subcomponents of a system are:

a. Hardware of the system not only includes typical IT components such as memory, CPU and peripherals, but also sensors and controlling components.

b. System's software, including libraries and interfaces.

c. Communication protocols via which a system exchanges data.

d. The overall system architecture and resulting configurations of the individual subsystems.

Impact of all individual subcomponents must be considered in the qualitative examination of the overall integrity of a system.

2.4.2 Considering the integrity of an example PLC scenario

For further consideration and conceptualization of integrity, an industry-relevant example of a programmable logic controller (PLC) is illustrated here. PLCs provide central monitoring, control, and automation tasks between SCADA, the manufacturing execution system (MES) and enterprise resource and field level. From a security perspective, it takes on an interesting "interface and gateway element" within production and other automation applications (e.g. smart home, smart building, etc.).

The following generic process and action chain is used in Figure 1:

From sensors, measured data (such as temperature, pressure, fill state, etc.) is detected and transmitted to the PLC. PLC receives the transmitted data, processes it, and sends commands to the actors. The actor (such as a motor or a pump) executes the command.

During transmission of data from sensors to the PLC and eventually to the actuator, the following (selected) risks to data integrity exist:

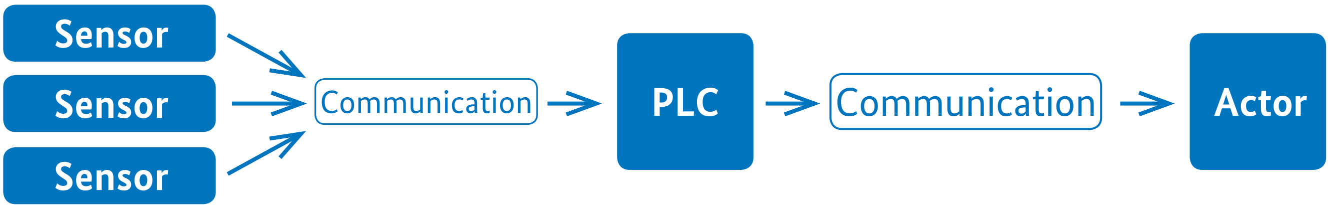
- Inclusion of random transmission errors such as by electromagnetic radiation, etc.
- Manipulation of transmitted measurements.
- Importing of false data/incorrect measurements.

The occurrence of these risks results in inaccurate operations of the PLC. For instance, based on falsified data, the PLC might make incorrect decisions that are subsequently executed by the actuator.

Lack of integrity can lead to incorrect operations of a PLC, which can result in the following problems:

- Modification of the system's OS, control program or configuration parameters by random errors.
- Targeted manipulation of the system's OS, software, control program or configurations by an attacker.
- Accidental/incorrect modification of the system's control program or configuration parameters by an operator.

Figure 1: Example of a Generic Industrial Process



Such situations have an adverse influence on the desired and accurate operations of a PLC. In such a scenario, data from sensors and control commands to the actuator become incorrect as well.

The example scenario discussed above shows that, while evaluating the integrity of the overall system, both individual components and the entire system must be considered. Therefore, transmission of data between various components must be examined and ensured, since incorrect data is the basis for the incorrect decisions leading to incorrect/undesired actions. On the other hand, the overall system and the control program must be accurate as well. Otherwise, even legitimate data, i.e. data that has not been modified during transmission, leads to undesired results.

To ensure integrity protection of the overall system, preventive and reactive measures must be taken. These measures allow detection of changes in data and systems and, on the other hand, they prevent changes, restore desired behavior, or inform the responsible personnel about how to respond to such violations.

2.5 Technical measures for detecting intregrity violations and ensuring integrity protection

Based on the example described in the previous section (Section 2.4), possible measures for detection of loss of integrity are described in this section. A distinction is made on the basis of responsible person for implementing these measures. The following table presents an overview of various measures.

2.5.1 Use of protocols with checksums

Nowadays, transmission protocols commonly employ checksums for the detection of random errors that may arise due to electromagnetic radiation. A known variant is CRC. The CRC checksum allows detection of modifications and, to a limited extent, even correction of errors.

Appropriate protocols must be implemented and supported by the component manufacturer.

2.5.2 Use of protocols with signatures

Simple checksums do not provide protection against intentional changes by an attacker, as the attacker can carefully adapt the change to the checksum, or modify the checksum. Signatures or key-based cryptographic hash functions provide resistance against such unauthorized changes. Examples include MAC or asymmetric-cryptography based digital signatures using RSA, DSA, or elliptic curve based EC-DSA. Such functions are found in OPC UA or TLS.

These protocols must be implemented and supported by the manufacturer in components.

Note that the transmitter and receiver must be able to check the authenticity of the messages. This requires that both sides have an identity that can be verified by the other.

2.5.3 Using checksums to detect errors/modifications

Similar to detection of errors during transmission, mechanisms should be implemented to detect randomly occurring errors within components of a system. For instance, an error may arise due to electromagnetic radiation or hardware defects.

2.5.4 Use of signed firmware updates/Software

Generally, delivery and installation of firmware/software is a critical process. It is necessary to prevent installation of manipulated variants. For example, an attacker could integrate a malicious function that allows him to attack at a later time or can create a backdoor to access unauthorized data without being noticed.

Therefore, firmware/software installation packages must be able to prove their integrity and authenticity. Manufacturers must provide appropriate information, such as checksums, on an independent channel. Alternatively, a signature attached to the firmware can be checked before an update. Software/firmware update/installation must take place only after successful verification of the attached signature.

Table 1: Overview of measures for integrity protection

Hazard	Manufacturer	Integrator	Operator
Random transmission errors, such as by electromagnetic radiation, etc.	Use of protocols with checksums	Use of logs with checksums	Monitoring the logs
Manipulation of measured data by an attacker	Use of protocols with signatures (symmetric or asymmetric signature) Logging	Use of protocols with signatures (symmetric or asymmetric signature) Roll-out identities of components Logging	Monitoring the logs Management of identities on system components
An attacker causes the system to import incorrect data	Use of protocols with signatures (symmetric or asymmetric signature) Logging	Use of protocols with signatures (symmetric or asymmetric signature) Roll-out identities of components Logging	Monitoring the logs Management of identities on system components
Modification of the operating system, control program or configuration parameters by random errors	Using checksums to detect errors/ modifications	Use of checksums and confirmations	Use of checksums and confirmations
Targeted manipulation of the operating system/firmware/ key memory by an attacker	Use of signed firmware updates Secure boot Secure storage area	Authenticate origin of firmware updates	Authenticate origin of firmware updates
Targeted manipulation of the control program by an attacker	Possibilities for signing control program Possibilities for verifying authenticity of the control program before importing it into the system Logging	Possibilities for signing control program Roll-out identities of components Logging	Monitoring the logs Management of identities on system components
Targeted manipulation of system configurations by an attacker	Possibilities for signature configuration parameters Logging	Possibilities for signing configuration parameters Roll-out identities of components Logging	Monitoring the logs Management of identities on system components
Accidental/incorrect modification of the control program or system configurations by an operator	Possibilities for secure identification and authentication of users and components Possibilities for validating configuration parameters Logging	User authentication and authorization before modification Define default configuration parameters and validate them Logging	Monitoring the logs Management of identities on system components

2.5.5 Ways to monitor system integrity

Manufacturers must provide measures to verify and monitor the integrity of its produced components. One possible way to accomplish this is by employing secure boot. Utilizing secure boot, the booting-up process is restricted so that only firmware having a valid signature is executed.

2.5.6 Possibilities for signing control programs and configuration parameters

Modifying a system’s control program or configuration parameters can have a significant influence on the system. For instance, a manipulated control program can lead to incorrect actions resulting in production of defective products or damage to the manufacturing machinery. A similar example applies for configuration parameters as well.

Therefore, it should be possible to detect and verify the modifications in the control program and configuration parameters before applying them to the controller.

2.5.7 Possibilities of user authentication and authorization before control program or configuration parameters modification

Before modifying a component, the user should authenticate himself to the component, i.e. provide evidence that he has the relevant authorizations. This can be done via passwords, digital certificates, etc. It is closely related to the roll-out of identities on components, discussed in Section 2.5.9. Additionally, the component must be capable to decide whether the user is entitled to make the changes or not. This process is called authorization.

Along with the modifications, the responsible user details should also be logged. These logging measures increase traceability which can help solve problems during an identified security breach.

2.5.8 Possibilities for validating configuration parameters

In order to be able to detect and avoid incorrect user entries, it must be possible to specify a range of values for input parameters. This can be a range of numbers or a fixed length of characters. Prior to the value processing, deviation of input compared to defined range is checked. This check must be carried out at all interfaces. As an alternative, the dependencies between parameters can be checked. For example: Parameter A must be false if Parameter B was previously set to "2" The relationships can be checked using feature tree models or during code examination.

2.5.9 Roll-out of component identities

In order to use some of the previously mentioned measures, there must be simple and secure methods for setting up identities of each component. These are required for authentication. Although setting up identities does not directly serve the purpose of integrity protection, its absence is problematic as it will impede establishment of the other integrity-protection measures. Further information about secure identities can be found in the "Technical Overview: Secure Identities" for Industrie 4.0 Platform (https://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/sichere-identitaeten.html).

2.5.10 Logging

Changes to data, systems and processes should be logged in order to detect integrity violation. If integrity of a system or data is affected, this should be documented. All the process must be monitored from the very beginning and their deviations/abnormal behaviors must be logged.

2.5.11 Monitoring the logs

Logs must be monitored to determine new and unusual events. It is necessary to pre-define and document the log monitoring procedure for the detection of integrity violation.

2.5.12 Management of identities of the components

In addition to the roll-out of component identities, it is necessary to manage them permanently. Apart from exchange of regular authentication data, unique identities of currently valid users must also be maintained. Such functionalities must be provided on the components, and processes must be established that initiate these necessary activities.

2.5.13 Signing and verification of the origin of firmware updates

Updates play an important role, especially for elimination of safety-relevant weak points from components. In order to prevent misuse, it is necessary to verify integrity and authenticity of updates before importing them. This ensures that the update has not been modified (i.e. does not include a feature added by an attacker) and originates from the legitimate vendor (i.e. not from a third party/attacker).

2.6 Handling problems of integrity

The disruption of integrity can lead to a variety of hazards in a system. Depending on the component, lack of integrity can have a wide range of effects, rendering a wide range of reactions appropriate. On detection of an integrity breach, a range of appropriate behaviors extends from controlled execution to an immediate shutdown or emergency treatment. Following examples illustrates this concept:

An example scenario where a serious problem does not occur despite the loss of integrity of a component is a machine whose sensors misrepresent the lubricant level for automatic lubrication. The system can continue its operation despite a low lubricant level. However, in such a scenario, an emergency shutdown of the machine is not required as loss of integrity does not have a direct serious effect.

An example which warrants immediate shutdown is disturbance of integrity of a safety-critical unit. For instance, incorrect indications of temperature sensors corresponding to a machine's power supply. This can lead to the destruction of the power source or can cause a danger to workers' lives. In such a scenario, action must be taken immediately on detection of loss of integrity.

The above mentioned examples show that a lack of integrity can have very different implications, and the responses to the detection of integrity violation can be very different. Therefore, an individual assessment of each component and impact of integrity violation on it is necessary. Key questions could be: which components are critical for the desired operations and which data forms the basis of subsequent decisions?

For further explanation, two case studies are discussed below:

Case Study 1 – "Condition Monitoring":

Consider a machine which is equipped with sensors.
In order to allow maintenance of the machine, the collected sensor data of the machine is made available to the service provider via a cloud-based platform.
In the chain extending from the sensors on the machine to the service provider, the following integrity problems can occur:

- Incorrect measurements recorded by the sensors.
- Measured sensor data is corrupted during transmission from the sensors to the cloud-based platform.
- Measured sensor data is corrupted during transmission from cloud-based platform to the service provider.

Regardless of the way in which the integrity of the measured data has been disturbed, the results can be financial damage to the machine operator:

- Low impact: Financial damage due to frequent maintenance of faulty sensors (early detection).
- High impact: Financial loss due to reduced production caused as a result of faulty sensor data (late detection). In this case, loss of integrity results in loss of availability as well.

Case Study 2 – “Raw Material Ordering”

A machine (3D printer) orders necessary raw material for the production process from the (internal/external) supplier. In this scenario, loss of integrity can lead to the following problems:

- Raw material is ordered too early.
- Raw material is ordered incorrectly.
- Raw material is ordered too late.

Regardless of where and in which way the integrity of the measured data was disturbed, the results can be in terms of financial damage to the machine operator:

- Low impact: Financial impact due to early delivery (higher storage costs).
- High impact: Financial damage due to late or wrong order (in addition to the disturbance of the integrity, this causes an availability problem as well).

2.7 Outlook: integrity protection as basis of trustworthiness

Ensuring security is challenging, especially in cross-company and cross-border communication scenarios. In order to achieve secure (company-wide/cross-company) communication, trust must be established between the participating communication partners. It may be that the communication partners have known each other for a long time, or they may be getting in touch with each other for the first time. For an economic operator, the question arises as to what extent these known and new communication partners can be trusted and how to securely network with them to exchange information.

In the context of industrial facilities, integrity also affects the physical world and the safety of people and the environment. In order to promote the digitalization of industrial plants, communication partners must be as trustworthy as possible. This in turn implies that the operator and the user can rely on the accurate operations of the system: integrity of the communication channels and integrity of the state of the system (according to the current state-of-the-art) are ensured.

3. Trustworthiness

3.1 What is trustworthiness?

Trustworthiness (Figure 2) describes the degree of confidence that the product provides in relation to all important system features in the context of environmental problems, human errors, system failures and attacks. The term 'trustworthiness' is used to describe the quality of existing and future relationships between companies, people, systems, and components. A trustworthy system ensures that all of its components behave in an expected manner. The integrity assurance of each unit forms the basis of trustworthiness. Trustworthiness, however, goes even further than integrity: for example, a malicious system that is integrity protected (unchanged and correctly operating) cannot be trusted by its communicating partners. This example shows that although integrity is an essential component of trustworthiness, it alone is not sufficient to assure trustworthiness as the intention of the owner or operator of the system, component, or company has significant influence on the overall trustworthiness. From this observation it can be concluded that trustworthiness is a property between different systems, firms, and individuals, while integrity is a feature within a system, component, or company. The concept applies equally to information technology (IT) and operational technology (OT), albeit in a context-dependent manner, with a different weighting given to each category.

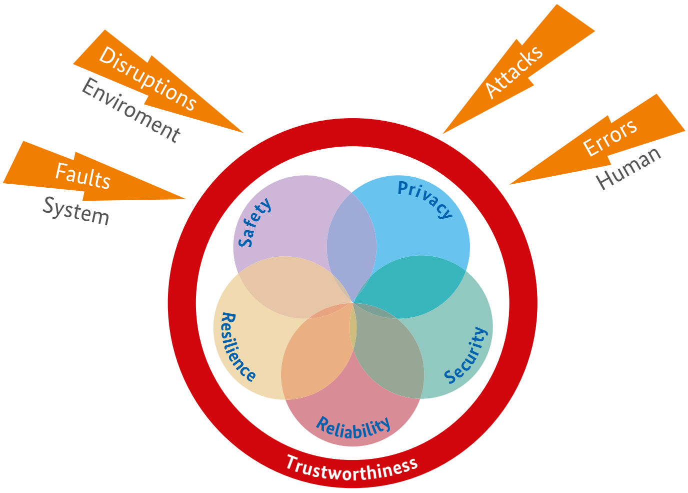
Therefore, characteristic categories for trustworthiness are:

- Security
- Safety
- Privacy
- Reliability
- Resilience

The possible absence of one or more categories (e.g. safety in IT or privacy in OT) does not alter the basic concept of trustworthiness.

Manufacturers, integrators and operators face similar challenges during digitalization and networking. They are becoming increasingly dependent on the correctness, completeness, and originality of data, systems, communications and processes. Trustworthiness requirements are increasing with the advancements in the direction of automated and autonomous systems. This leads to a reconsideration of the basic design. Traditionally, availability was the highest priority for industry. However, in automated and autonomous processes, the potential for human reactive influence

Figure 2: Categories of Trustworthiness



Source: Industrial Internet Consortium

is small. Data, system, communications, and processes must be correct from the start of the value chain as a defective/faulty product will result in more financial loss compared to periodic process disruptions/stoppages (see product recalls, warranty obligations and claims for damages after sale). The missing integrity means that an error in the transmission or an error in the implementation of the processes can lead to a faulty behavior and thus potentially a faulty product.

Trustworthiness considers the accuracy of the implemented functions and exploitability of (known) vulnerabilities that an attacker can exploit to adversely affect a component. In particular, trustworthiness means that there are not any unwanted or undocumented additional, altered, or removed functionalities.

3.2 Integrity as an essential component of trustworthiness

Among the above-mentioned viewpoints, integrity becomes a major protection target for all five characteristic categories of trustworthiness.

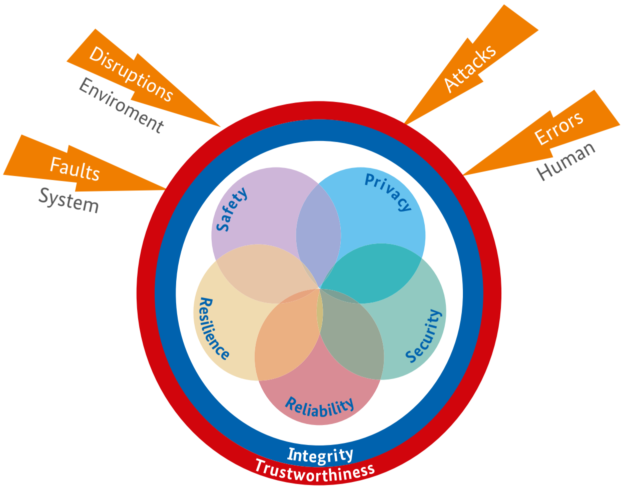
Technical measures and processes must be adequately defined and interlinked in order to ensure integrity, i.e. the core protection target.

Here are a few examples to stress the importance of integrity protection in each of the categories mentioned in Figure 3:

- **Security:** In information security, integrity is an important protection target. For instance, incorrect production parameters can lead to faulty products in a very short amount of time. Integrity is further closely linked to the authentication of users or roles in a production environment. In case of transmission of incorrect data, authentication of legitimate users will not be possible. Finally, integrity can also affect other protection objectives, such as confidentiality, since confidentiality of data cannot be guaranteed on compromised systems.

- **Safety:** In a production environment, photoelectric barriers are frequently used for safety tasks. For instance, if a person enters a hazardous area in the vicinity of an industrial robot, this is often detected by light barriers and the robot is instructed to halt immediately. Failure to transmit values (light beam interruption/non-interruption) can mislead safety related emergency-stop mechanisms and can cause life endangering consequences.

Figure 3: Integrity (Blue Ring) as an Overarching Protection Target for all Five Categories



Source: Industrial Internet Consortium

- **Privacy:** Integrity and privacy are not directly related but indirect references between them exist. For example, it is difficult to ensure confidentiality of personal data on a compromised system, thus resulting in loss of privacy. At the same time, integrity is also vital for data during processing, i.e. personal data must remain intact, complete and up to date during processing.

- **Reliability:** For instance, incorrect transmission of PLC data can have adverse implications on reliability of production. This can lead to serious consequences as the plant can be driven in critical areas without the system operator being aware of this malfunction.

- **Resilience:** In context of this document, resilience is understood as the ability of a technical system to not to fail completely in case of faults and partial failures, but rather to maintain essential system functions and services, and to return to the original state as soon as possible. Thus, in addition to availability and confidentiality, integrity is also used to increase the resilience of a system. For instance, the erroneous transmission of required data to production control is detected, and measures for maintaining the correct functioning of a system, such as a request to re-transmit the required data for production control, are triggered.

3.3 Trustworthiness for supply and value chain

Within the framework of cyber-security in the industrial environment, trustworthiness is an important qualitative decision-making criterion for the company along the entire value chain.

The manufacturer wants to give his customers clear, comprehensive, and reliable information about the properties (in particular, security, and thus also integrity) of the system/product/component delivered. For this, he needs reliable information about the components from other suppliers that have been included in his product. Overall trustworthiness of this information chain also depends on the development, production, and logistics processes involved.

From a manufacturer's perspective, trustworthiness is a promise of desired operation, expressed through a manufacturer's declaration. An audit/certification by an independent body can increase the level of confidence in the manufacturer's declaration.

From an integrator's perspective, trustworthiness is the promise to integrate trustworthy components using secure processes, so that the operator can be given an installation with clearly described security features. When components are being selected, it is important to ensure the trustworthiness of the component manufacturer.

The trustworthiness of an installation can only be reliably assessed over the lifetime of a plant if the integrity of the plant is protected and changes in its state are recorded as part of security management.

In our everyday life, while evaluating trustworthiness amongst people, experience and intuition (e.g. history, general opinion, personal knowledge, and the "gut feeling") play a significant role. In the corporate environment, this relationship of trust must be substantiated, for example through certifications or audits. These assessments can never be 100% objective. In such cases, analysis of technical systems allows for a certain resilience. The economic situation of the company and its organizational environment must also be taken into consideration. Possibilities of deliberate deception by staff or entire organizations make an "objective" consideration even more difficult. In this respect, the long-term relationship between two companies, their personal experiences and history will remain an important criterion.

The autonomous assessment of trustworthiness between I4.0 components must be based on facts, evidence, rules, and the context. This requires digitalization and modeling of experiences and evaluations.

4. Requirements for the actors

Manufacturers, integrators, operators, and service providers must first recognize the importance of integrity and adopt necessary measures to ensure integrity protection. For the overall protection of integrity, each actor is individually responsible:

Manufacturer

Manufacturers focus on two main tasks, i.e. the supply of integrity-protected products/systems and communication of transparency of their processes. Accordingly, measures to protect integrity in the development and production process must be taken into account. Concrete indications are provided in parts 4-1 and 4-2 of the IEC 62443 for networked industrial plants and ISO 27034 for safe software development.

The implementation of the measures can be achieved through the established mechanisms defined in the manufacturer's declaration, or a declaration prepared according to the above standards is made transparent to the customer.

Integrator

Integrators rely on the documentation and declaration provided by the manufacturers for determining integrity and trustworthiness. It is the responsibility of the integrators to recognize, assess and correct any disturbances of integrity in the system. They should detect integrity breaches and employ appropriate ways of identifying, authenticating, signing, and, where applicable, use certificates for their respective applications (see Section 2.5).

Operator

Similar to the integrator, the operator bears the responsibility for the entire system for detecting, evaluating, correcting, or compensating disruption to integrity and trustworthiness. Due to the influence of integrity on security, safety, and privacy, it is essential for the operator to employ protective measures to achieve his goals and legal requirements.

Service provider

Industrie 4.0 will enhance the significance of service providers on the market. An example of a service provider is the marketplace for process data. This process data is offered by a broker on the market and bought by an operator. The data purchase saves the operator production downtimes and development efforts and risks, for example. For integrity and trustworthiness assurance, the service providers are dependent on the documentation and declaration provided by the manufacturers and integrators.

All the above mentioned actors have a common task of ensuring integrity throughout the entire life-cycle of components and systems. The procedure and duration of the measures must be communicated transparently and unequivocally by all actors to their customers. For example, this can be done by providing an explanation or guidelines conforming to the above mentioned standards.

Policy-makers

Implementation of Industrie 4.0 requires integrity-protected and trustworthy infrastructures. Policy-makers can work with industry to facilitate their establishment. No one can master the challenges of mobile, digital identities, communication, and data processing alone.

Standardization

International standards series such as IEC 62443 and ISO 2700x provide the basis for integrity and trustworthiness. Further, preparing an internationally uniform documentation and declaration of integrity and trustworthiness is a challenge. Therefore, the goal is to query and display the measures along the supply chain across national boundaries.

5. Summary

With the growing complexity of products and systems due to digitalization and networking, the importance of integrity protection is growing. Users must be able to rely on the correctness, completeness and unalteredness of their data, systems and processes. Failure to do so will not only result in creation of defective products and solutions but also compromise their overall quality, leading to customer claims, warranties, recalls, and hence loss of reputation. Integrity protection has become more important with the advent of Industrie 4.0 as integrity has a direct impact on its elementary parameters such as quality, cost, and duration of production. In addition, integrity protection will continue to provide the basis for compliance with statutory requirements for functional safety.

There are numerous ways to deal with integrity disruptions (as mentioned in Section 2.5 and 2.6). It will be crucial for industry to be able to ensure integrity with its dynamics (technology and risk development) throughout the lifespan of the products and solutions spread across different domains. Ultimately, the integrity of data, systems and processes is one of the main foundations for the realization of trustworthy systems. This, in turn, is the basis for trustworthy co-operation across corporate and country boundaries.

AUTHORS

Nicole Dönicke, Kjellberg Finsterwalde | Wolfgang Fritsche, IABG mbH | Dr. Thomas Gamer, ABB AG | Prof. Dr. Tobias Heer, Hirschmann Automation and Control GmbH | Dr. Lutz Jänicke, PHOENIX CONTACT GmbH & Co. KG | Michael Jochem, Robert Bosch GmbH | Dr. Wolfgang Klasen, Siemens AG | Thomas Lantermann, Mitsubishi Electric Europe B.V. | Lukas Linke, Zentralverband Elektrotechnik- und Elektronikindustrie e.V. | Jens Mehrfeld, Bundesamt für Sicherheit in der Informationstechnik | Tobias Pfeiffer, Festo AG & Co. KG | Andreas Teuscher, SICK AG

The document has been prepared by members of SG Security.
This is part of the Leadership Circle of Industrie 4.0 (ZVEI). It handles all aspects of security for Industrie 4.0
and supports work of WG 3 “security of networked systems” of Plattform Industrie 4.0.

www.plattform-i40.de