PLATTFORM INDUSTRIE 4.0

Federal Ministry
for Economic Affairs
and Energy

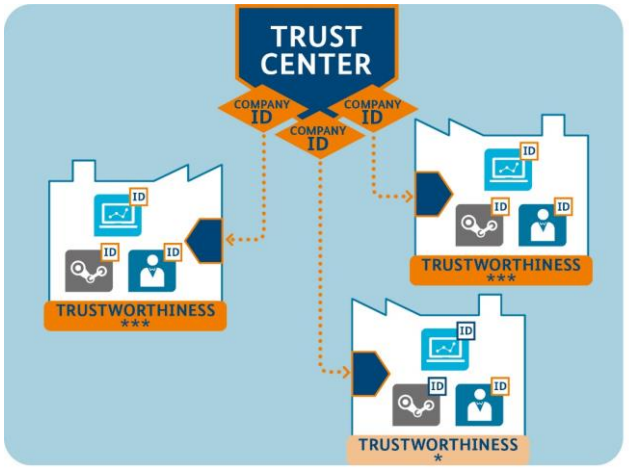
Trustworthiness and Integrity

Integrity a fundamental Protection Goal for Trustworthiness

Michael Jochem, Robert Bosch GmbH
Berlin, 2018/05/15

Key Questions for this session

- How to determine the trustworthiness within a Global Industrial Value Networks?
- How to provide assurance regarding trustworthiness?
- What kind of role play integrity and integrity protection in this context?
- What should actors do to be able to recognize and control integrity with it's dynamics along the lifecycle of products and solutions across their roles



Integrity - A brief definition

- Integrity = Correctness, unalteredness and completeness
- Integrity of **own data** and increasingly **external data** and integrity of (trust in the proper functioning) **systems** and **processes** is absolutely necessary.
  - Digitalization and networking require the integrity of the communication partners (people + things) in the value chain network
  - partners have to be integrated into the network automatically
- **Integrity is essential** for all business processes within and outside a company.

Importance for other protection objectives

Processes based on non-integrity protected data and systems are most likely to be erroneous.

- Consequential errors that manifest themselves in the form of product defects or incorrect data, up to loss of reputation or triggering product liability

Integrity protection is becoming more important and an essential foundation for availability and confidentiality.

- Integrity can be defined for each component and implementation level of a device

The term "**integrity protection**" is used to describe mechanisms/functions that prevent unauthorized modifications and thereby, prevent unauthorized manipulation

Determination: Data and System Integrity

Data Integrity - Data in transit

- Integrity: How can it be reliably detected whether the data has not been manipulated while it was being exchanged between different components?
- Authenticity: How can it be reliably detected that transmitted data was sent by the intended component?

Data Integrity - Data at rest

- Integrity: How to ensure that the data has not been tampered since the last check?
- Authenticity: How can you reliably recognize who has stored the data, who is the data from, or who made the last change?

System Integrity

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

Integrity protection ensures secure and correct operations of systems/components

Possible challenges of Integrity

- Changes in the system over time
- Ageing of crypto-algorithms with new scientific advancements and higher computing power
- Technical progress in offensive security
- Human errors and faulty operations
- Technical failure and environmental influences

Handling of disturbance of integrity
Case study “Condition Monitoring”

Consider a machine which is equipped with sensors for “Condition Monitoring”.

In the chain extending from the sensors on the machine to the service provider, following integrity problems can occur:

Possible disturbance of integrity:

- 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

Financial damage:

- 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.

PLATTFORM INDUSTRIE 4.0

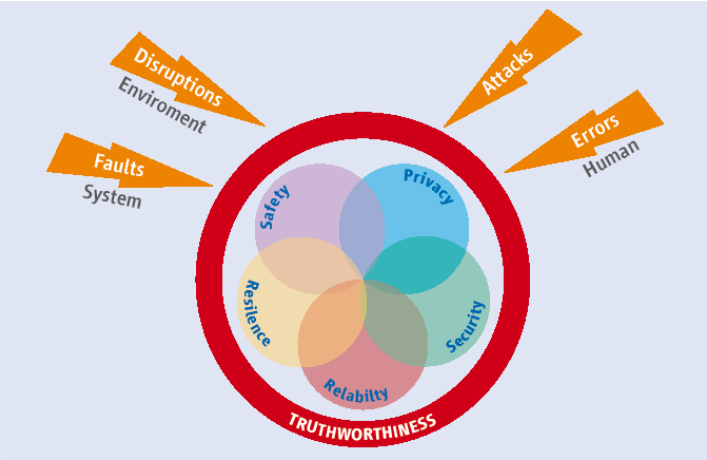
Federal Ministry for Economic Affairs and Energy

Technical measures for ensuring integrity protection (excerpt) *1)

Hazard	Manufacturer	Integrator	Operator
Random 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 Logging	Use of protocols with signatures 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 Logging	Use of protocols with signatures Roll-out identities of components Logging	Monitoring the logs Management of identities on system components

*1) © PI4.0/ZVEI Whitepaper – Integrity of Data, Systems and Processes

Integrity and Trustworthiness – A close relationship?



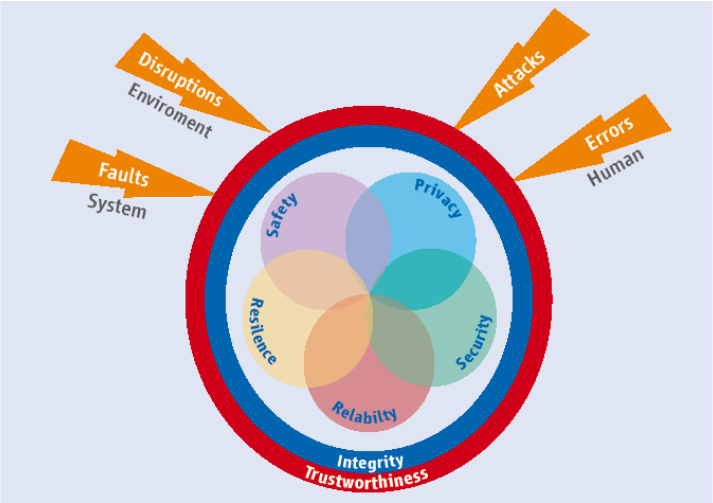
Source: Industrial Internet Consortium and ZVEI

- Trustworthiness 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.
  - Key characteristics:

    Security, Safety, Privacy, Reliability and Resilience

- The term ‘trustworthiness’ is used to describe the quality of existing and future relationships between companies, people, systems, and components

Integrity and Trustworthiness – A close relationship?



Source: Industrial Internet Consortium and ZVEI

- Manufacturers, integrators, operators and service providers face similar challenges during digitalization and networking
  - They are becoming increasingly dependent on the **integrity** (correctness, completeness and unalteredness) of data, systems and processes
  - Integrity (**blue ring**) becomes a major protection target for all five key characteristic of trustworthiness.
- Protecting integrity is becoming more important than availability

Integrity and Trustworthiness – A close relationship?

Trustworthiness - Examples of the importance of integrity

- **Security**: Integrity is an important protection target
- **Safety:** Failure to transmit values (light beam interruption/non-interruption) can mislead safety related emergency-stop mechanisms and can cause life endangering consequences
- **Privacy**: Integrity is also vital for data during processing, i.e. personal data must remain intact, complete and up to date during processing
- **Reliability**: Incorrect transmission of PLC data can have adverse implications on reliability of production
- **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, i.e. request to re-transmit corrupt data

PLATTFORM INDUSTRIE 4.0

Federal Ministry for Economic Affairs and Energy

Key Questions and Requirements

What kind of role play integrity and integrity protection in this context?

- Integrity measures must be **communicated transparently and unequivocally** by all actors (**manufacturers, integrators, operators and service providers**) to their customers and **demanded from their suppliers**
- Integrity protection mechanisms support that the customer gets excactly what the supplier released and the custumer orders
- Integrity protection is the basis for trustworthy cooperation across company and national borders
- Integrity protection is becoming increasingly important for the elementary parameters of quality, cost and time of production

Key Questions and Requirements

What should actors do to be able to recognize and control integrity with their dynamics along the lifecycle of products and solutions across their roles?

- **Manufacturers, integrators, operators and service providers** need to be able to recognize and control **integrity** along the lifecycle of products and solutions across their roles
  - For the overall protection of integrity, each actor is responsible individually
  - From the manufacturer's point of view, trustworthy information about the components of its suppliers is required
- For **standardization**, the internationally uniform documentation and declaration of integrity and trustworthiness information is a challenge
  - Therefore, the goal is to query and display the measures along the supply chain across national boundaries
- **Politics** can help build trusted infrastructures together with the industry
  - No actor can master the challenges alone

PLATTFORM INDUSTRIE 4.0

Federal Ministry
for Economic Affairs
and Energy

Plattform Industrie 4.0
Working Group „Security of Networked Systems“

Thank you for your attention!

Contact:

Michael Jochem, Robert Bosch GmbH

michael.jochem@de.bosch.com