



Industrial Trustworthiness and Security

Dr. Wolfgang Klasen

Siemens AG

German Platform Industry 4.0 ,Germany



Hirozumi Eki

ARGO GRAPHICS INC.

Robot Revolution
& Industrial IoT Initiative, Japan

Contents

- **Background**
- **Recent discussions from our group**
- **The world to aim for**
- **How can trustworthiness in value chains be defined?**
- **Trustworthiness concept for supply and value chains**
- **Next steps for collaboration**

Plattform Industrie 4.0, Germany, and Robot Revolution Initiative & Industrial IoT Initiative (RRI), Japan, are successfully collaborating since 2017 on topics concerning security of Industrial IoT (IIoT) and establishing trustworthy relationships between value chain stakeholders, regardless of their business verticals or geographical locations.

The group develops a structured approach to trustworthiness for organizations, products, and data across supply and value chains. Having published seven white papers, it now focuses on product-data trustworthiness to shape policy through global standardization.



(May 2018)



(April 2019)



(Sept. 2020)



(April 2022)



(April 2023)



(April 2024)



(April 2025)

Robot Revolution and Industrial IoT Initiative (RRI) includes approximately 400 participants from manufacturing companies, research institutions, and local governments.

The Industrial Security Action Group, chaired by Professor Matsumoto, includes members from ARGO GRAPHICS, Sony Semiconductor Solutions, Toshiba, Hitachi, Mitsubishi Heavy Industries, Mitsubishi Electric, and Fujitsu.

In collaboration with Plattform Industrie 4.0, the group identifies common challenges and shares insights to ensure the trustworthiness of Products and data across supply and value chains.



(May 2018)



(April 2019)



(Sept. 2020)



(April 2022)



(April 2023)



(April 2024)



(April 2025)

What is the “Trustworthiness of Product Related Data(PRD)” that is distributed across companies and countries in the supply chain and value chain

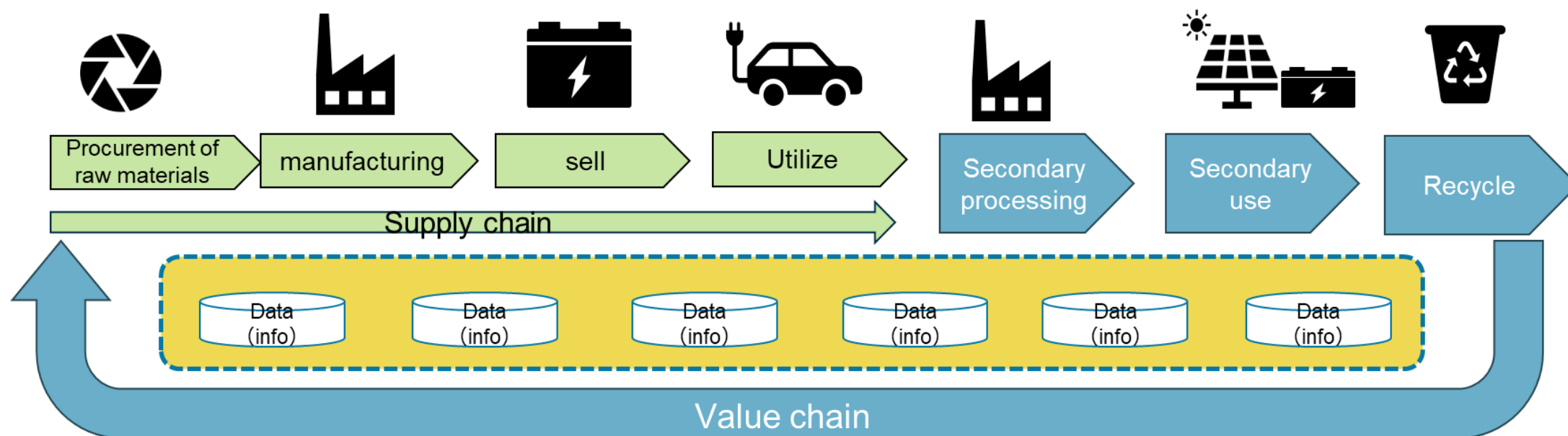
Collaboration topics:

Establishing trustworthiness in IIoT supply & value chains

A key feature of our activities is that they are not limited to Japan — through collaboration with Germany, we actively address industrial security while quickly capturing trends and developments in Europe.



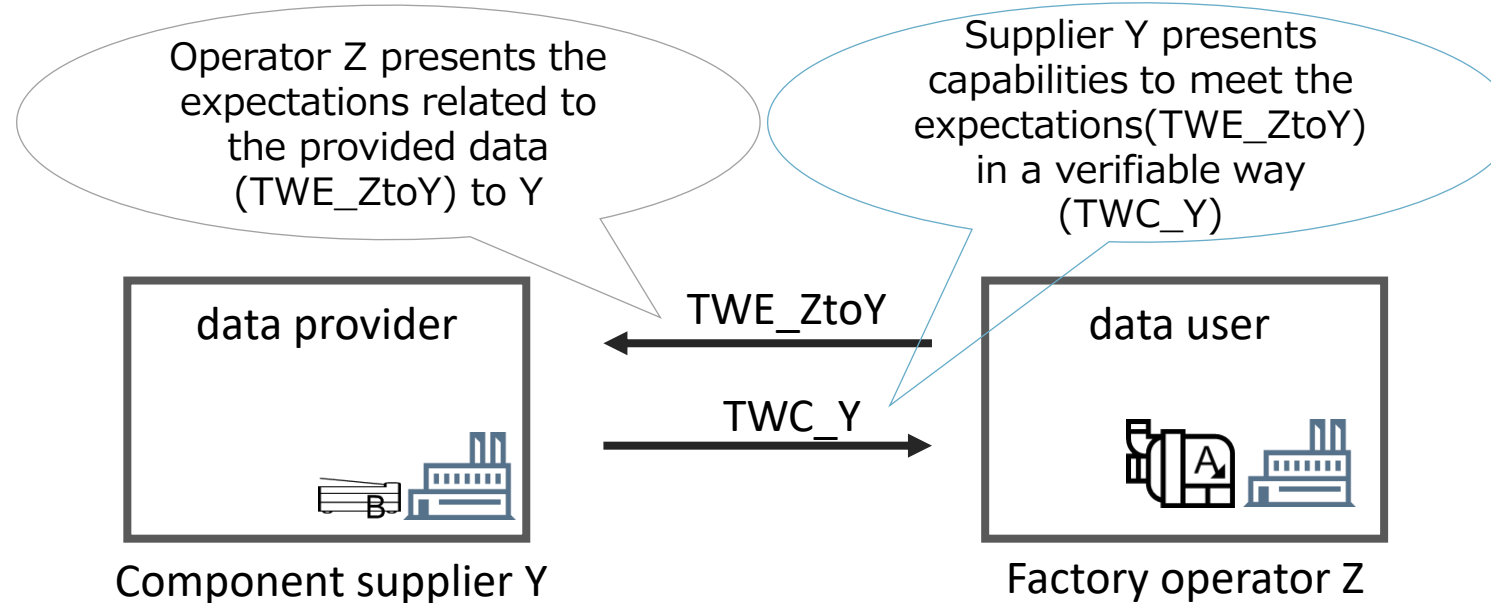
April 2025



Trustworthiness is defined as ability to meet stakeholders' expectations, and it is a means of establishing trustworthy relationships.

To elaborate on the Trustworthiness discussion, RRI/PI 4.0 defines it as follows:

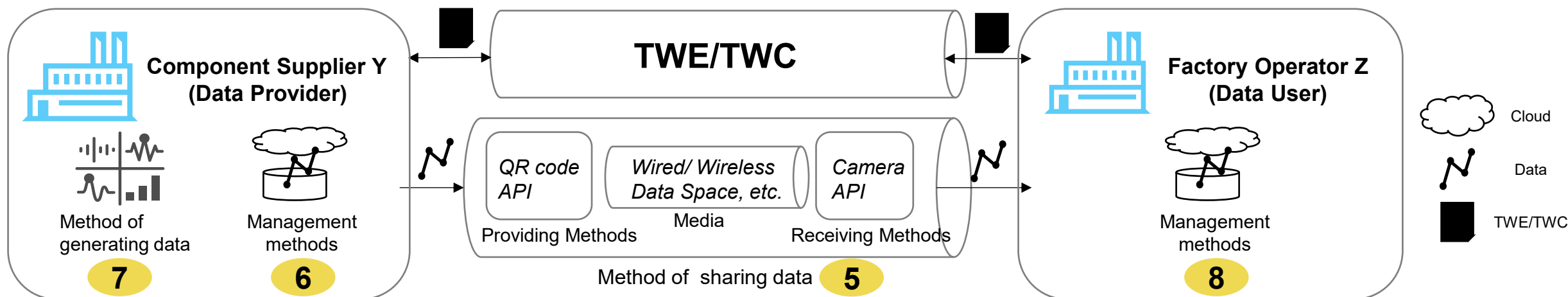
- Trustworthiness Expectation (TWE): Expectation to stakeholders
- Trustworthiness Capability (TWC): Capability to meet the above expectations in a verifiable way



According to the above, if Z accepts the capability in a verifiable way(TWC_Y), and it meets the expectations, Z will trust Y

Trustworthy relationships of PRD are established
by starting to consider to 8 items based on a use case

Items to consider
1: Identify the use case, ユースケースの特定
2: Define the problem statement , 課題定義
3: Identify the object, 対象の特定
4: Identify the actors/ TD, アクターの特定
5: Identify sharing method, 流通・共有方法の特定
6: Identify data provider's management method, 提供者側データ管理方法の特定
7: Identify data generation process and method, 提供者側データ生成プロセス・方法の特定
8: Identify data user's data management method, 利用者側のデータ管理方法の特定



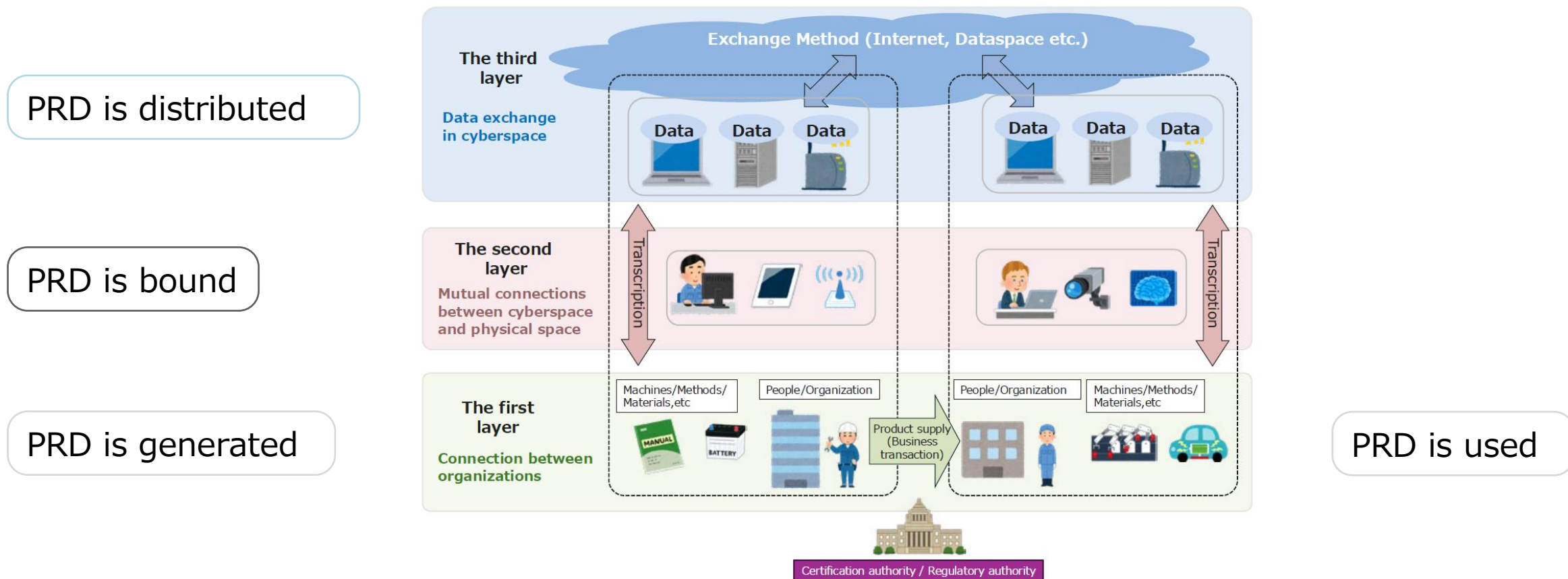


Figure 1: PRD as per the Cyber Physical Security Framework

CPSF (Cyber-Physical Security Framework)

The Ministry of Economy, Trade and Industry (METI) has presented an overall framework for security measures in industrial society in Society 5.0, where value is created through a new supply chain that highly integrates cyberspace and physical space.

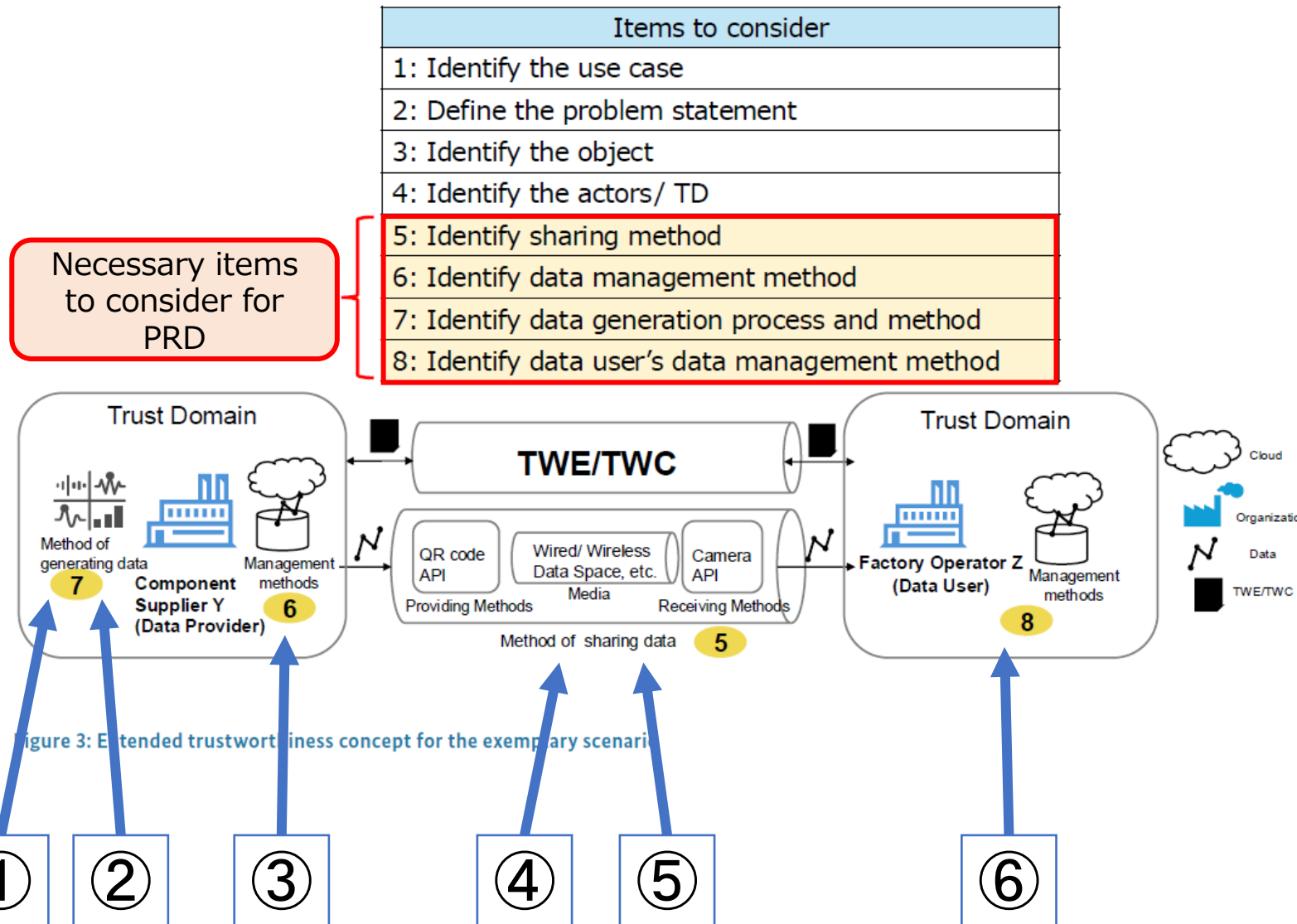
The process of generating this value is organized into three layers of industrial structure:

Layer 1: Inter-company connections

Layer 2: Connections between physical space and cyberspace

Layer 3: Connections within cyberspace

<https://www.meti.go.jp/policy/netsecurity/wg1/wg1.html>

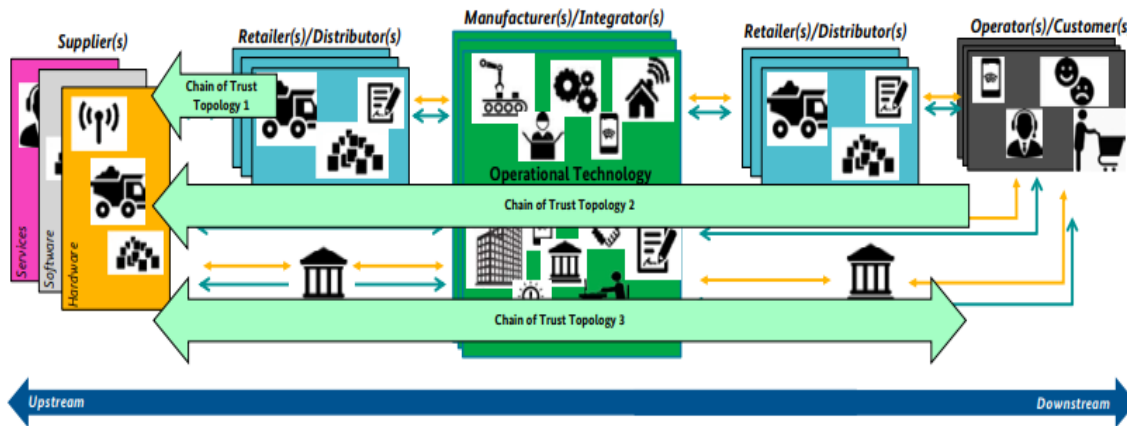


- ① The method of measuring and obtaining the amount of CO2 generated during product manufacturing must be reasonable.
- ② The product must be linked to the data on the amount of CO2 generated
- ③ That the data is managed correctly
- ④ Ability to transmit data correctly over the network
- ⑤ Data users can receive data correctly from the network
- ⑥ The data user's use of the data does not deviate from the data provider's terms of use.

Developing rules to understand the entire supply and value chain like DPP
Suppliers also have to exchange Trustworthiness with people other than those who directly sell products.

From around 2021, Japan and Germany began discussing the need for a chain of trust between upstream ~ downstream of the supply chain, and in recent years, it has been materialized.

Figure 9: Chain of Trust Topologies



Source: Plattform Industrie 4.0

IIoT Value Chain Security

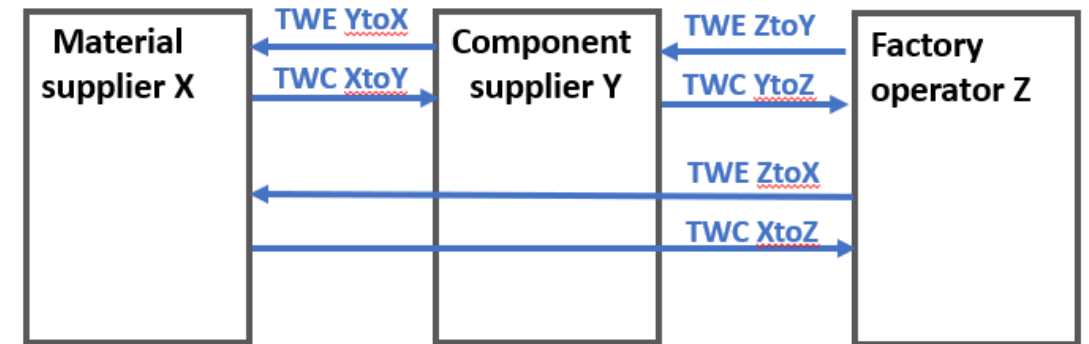
IIoT Value Chain Security Chain of Trust for Organizations and Products

7.1 Trust Transitivity to Chain of Trust m7.2 Chain of Trust Topologies

Suppliers receive various TWEs along the value chain.

Suppliers need to present TWCs and supporting data to value chain stakeholders.

TWE: Trustworthiness Expectation TWC: Trustworthiness Capability



IIoT Value Chain Security

Realizing Trustworthiness Attributes for Supply Chain Elements

- The data user can also verify that the product related data (PRD) provided by the data provider is free of falsification and errors
- Data users will not use PRD that deviates from the terms of use of data providers.
→ Data users who have not obtained PRD directly from data providers will not deviate from the terms of use of data providers.



We will make the trading environment of the global supply chain safer and more secure,
and we contribute to the creation of value for data distributed in the supply chain.
= Ensuring trust among stakeholders

- In order to ensure the trustworthiness of PRD in the supply chain, it is important to create a system that collaborates between the public and private sectors
- It is necessary to discuss use cases to ensure the trustworthiness of PRD in the supply chain throughout the manufacturing industry and agree on how to realize it
- RRI has a place where many companies can participate and discuss, so we would like to discuss the creation of an ecosystem with everyone



Industrial Trustworthiness and Security



Dr. Wolfgang Klasen

Siemens AG

German Platform Industry 4.0 ,Germany

Hirozumi Eki

ARGO GRAPHICS INC.

Robot Revolution
& Industrial IoT Initiative, Japan

How can trustworthiness in value chains be defined?

*Trustworthiness corresponds to the
“ability to meet stakeholders’ expectations in a
verifiable way”,
along multiple entities in a supply or value
chain.”*

- Note: Depending on the use case or business context, trustworthiness may be defined by attributes like authenticity, resilience, accountability, traceability, compliance to social regulations, integrity, availability, reliability, confidentiality, privacy, safety, maintainability, usability, etc.
- See: ISO/IEC TS 5723:2022

Organizational Trustworthiness

“Extent to which the declared attributes of an organization can be verified by the relying party and satisfies its expectations”

Product Trustworthiness

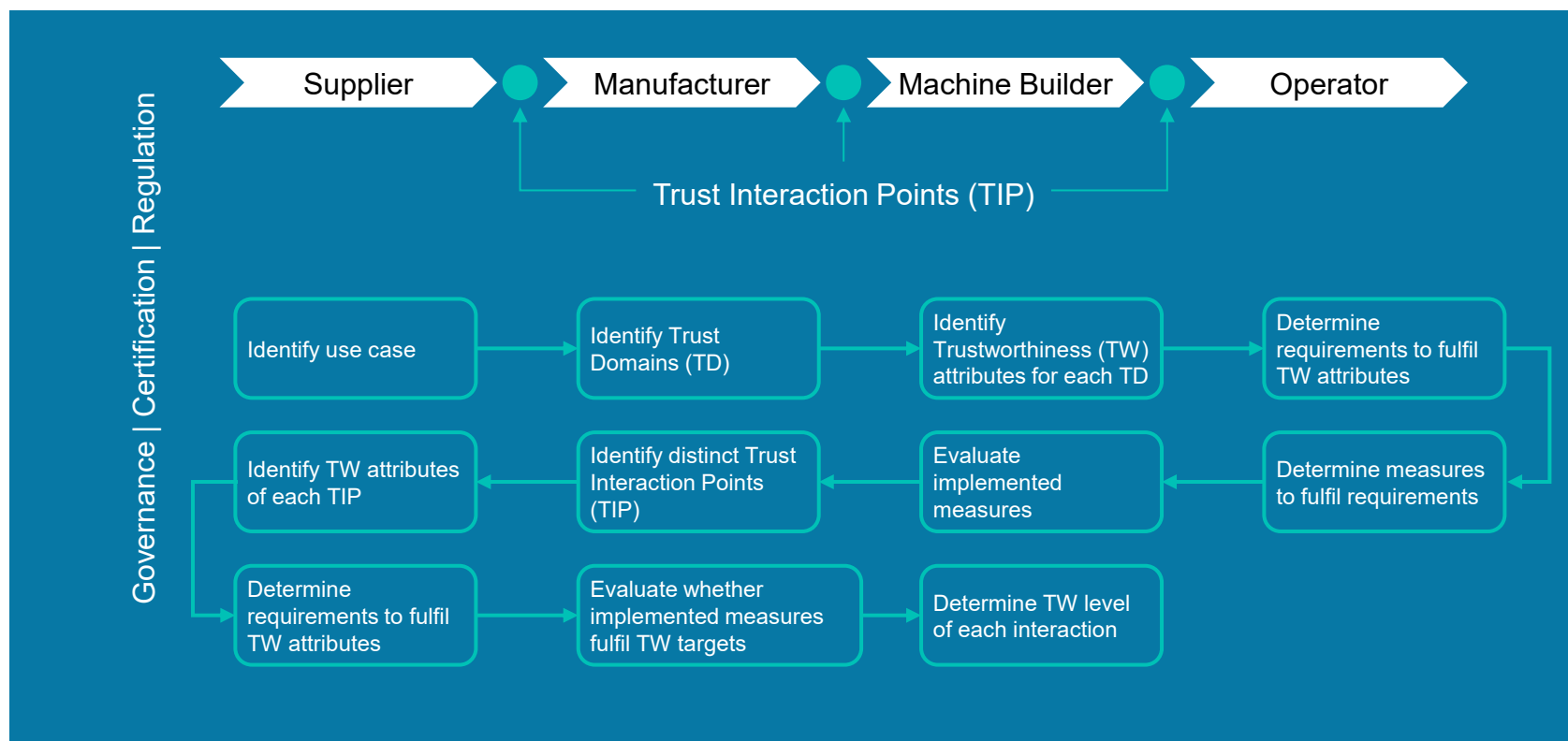
“Extent to which the declared attributes of a product can be verified by the receiving stakeholder and satisfies its expectations ”

Data Trustworthiness

“Extent to which a stakeholder can assure transparency regarding the implementation of data usage rights and/or obligation, and/or the traceability of the data including its generation, processing, and utilization”

Trustworthiness concept for supply and value chains

Trustworthiness concept presents a structured approach to address trustworthiness in any supply chain, value chain, or a value network, as specified within **ISO 22373:2025 – “Framework for establishing trustworthy supply and value chains”**.



Next steps for collaboration

Potential next steps for 2026 are:

- **Support for trustworthiness architecture for Data Space use case from other WG and Security Support for Manufacturing-X.**
- **Further establishment of Trustworthiness concept for data, examination of:**
 - **Means of ensuring persistence and reliable binding between a product and its data.**
 - **Analysis scenarios-based trustworthiness expectations (TWE) and capabilities (TWC) for data.**
 - **Analysis of AI opportunities, risks and threats regarding value chains.**
- **Additional candidates are “Role of trustworthiness for sustainability along value chains” and “Trustworthiness in standards related to EU DPP” .**
- **Work for overarching Security/Trustworthiness governance concept and “Wallet” for industrial cooperation.**



Thank you very much

Contact Information:

Dr. Wolfgang Klasen

Siemens AG

German Platform Industry 4.0 ,Germany

wolfgang.klasen.ext@siemens.com

Hirozumi Eki

ARGO GRAPHICS INC.

Robot Revolution& Industrial IoT Initiative, Japan

hirozumi_eki@argo-graph.co.jp