ロボット革命・産業 IoT イニシアティブ協議会
Robot Revolution & Industrial IoT Initiative

PLATTFORM INDUSTRIE 4.0

INTERNATIONAL PAPER

IIoT Value Chain Security

Realizing Trustworthiness Attributes for Supply Chain Elements

German-Japan cooperation

Imprint

Publisher
Federal Ministry for Economic Affairs and Climate Action (BMWK)
Public Relations
11019 Berlin
www.bmwk.de

Editorial responsibility
Plattform Industrie 4.0
Bülowstraße 78
10783 Berlin

Status
April 2023

This publication is available for download only.

Design
PRpetuum GmbH, 80801 Munich

Picture credit
ZinetroN / Adobe Stock / title

Central ordering service for publications of the Federal Government:
Email: publikationen@bundesregierung.de
Tel.: +49 30 182722721
Fax: +49 30 18102722721

Table of contents

List of figures

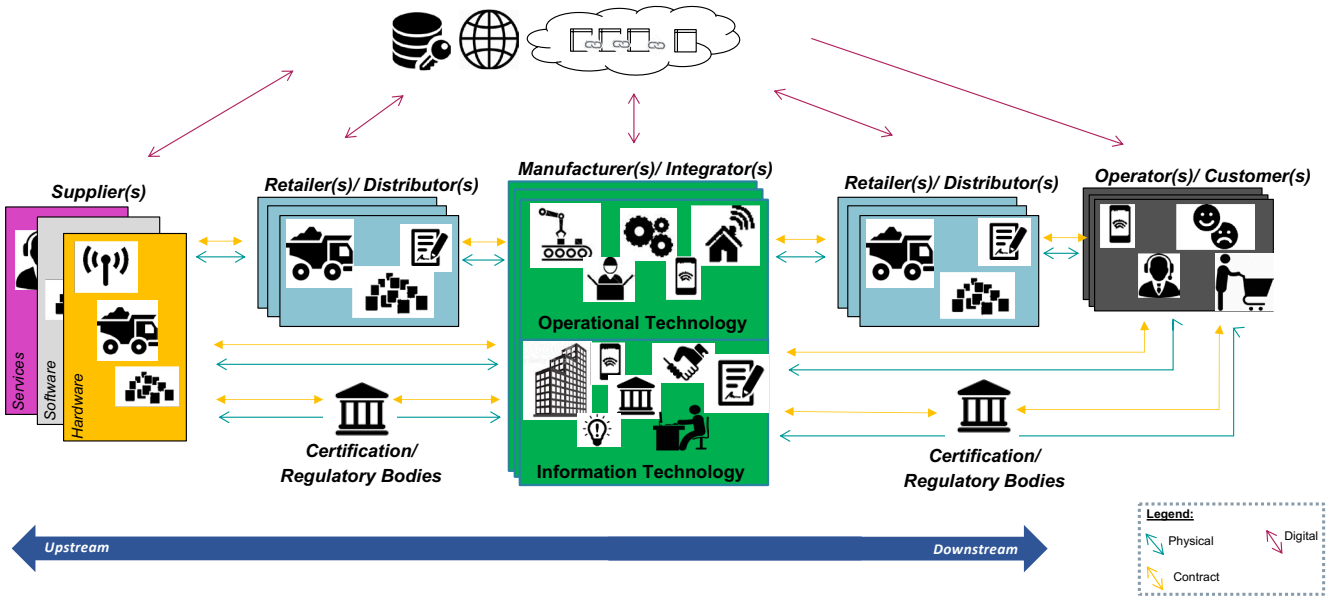
1. Background

In the past, Plattform Industrie4.0, Germany, and Robot Revolution & Industrial IoT Initiative (RRI), Japan announced five publications, “facilitating international cooperation for secure Industrial Internet of Things/ Industry 4.0”.

RRI, Japan and Plattform Industrie 4.0, Germany, concentrated their activities to the possibility of creating trustworthy relationships between companies, regardless of their business histories or geographical locations. Therefore, our previously published whitepaper elaborated the role of trustworthiness in global value chains and introduced the concept of chain of trust along global supply chains. In order to create digital business relationships across continents, all security related entities and communication processes need to be trustworthy, as it can be seen in Figure1 that shows a simplified supply chain of connected industries. The last common white [2], structure of trustworthiness across a supply chain of analyzed which consists of organizations’ and products’ Trustworthiness and introduced their relationship.

In line with these publications, Plattform Industrie 4.0 and RRI decided to proceed with the topic ‘realizing supply chain trustworthiness’ and worked on describing different chain of trustworthiness topologies and identifying trustworthiness supporting infrastructure.

Figure 1: Generic supply chain



Source: Plattform Industrie 4.0

2. Introduction

Highly automated international and global collaboration of industrial production environments is a key feature of Industry 4.0 and Society 5.0/Connected Industries. In various countries, production facilities will be able to collaborate with each other in nearly real time regardless of their geographical location. Therefore, availability of a comprehensive trustworthy ecosystem is an indispensable prerequisite.

For ensuring trustworthiness in an industry 4.0/ Society 5.0 ecosystem, trustworthy collaboration mechanisms and infrastructure must be developed. Therefore, this white-paper presents possibilities of propagation of trustworthiness along global supply chains that can be leveraged in any industrial context.

To achieve the overall target of establishing trustworthy global supply chains, the white paper lists requirements for a trustworthy infrastructure and provides examples of their realization, for example, a trustworthiness repository.

3. Motivation

Global supply chains are complex comprising various stakeholders. Traditionally, trustworthiness amongst supply chain stakeholders is established based on an extensive history of working together under various legal contracts. As economies are moving towards adaption of more digitalization, ad-hoc and flexible trustworthy relationships along supply chains are essential. Therefore, in addition to legal contracts, technical means are required to establish trustworthiness along supply chain in an efficient manner. In this whitepaper, we focus on exploring ways of formalizing and realizing chain of trustworthiness along supply chains, especially from technical perspective leveraging different technologies including central and distributed technologies.

4. Supply Chain Trustworthiness

Global supply chains are long and complex, comprising of stakeholders that are sometimes continents apart. Additionally, the participants in a supply chain have different capabilities based on their business context. Therefore, it is not trivial to define trustworthiness attributes that signify the trustworthiness of the entire supply chain.

ISO/IEC JTC 1 WG13 [1] is working on the definition and reference architecture for the word trustworthiness. In this whitepaper, we adapted the definition of trustworthiness that is being developed at [1] in the context of supply chains. Therefore, trustworthiness in supply chains can be understood as follows:

“Trustworthiness corresponds to the ability of a stakeholder to make its claims verifiable, between immediate or along multiple entities in a supply chain”.

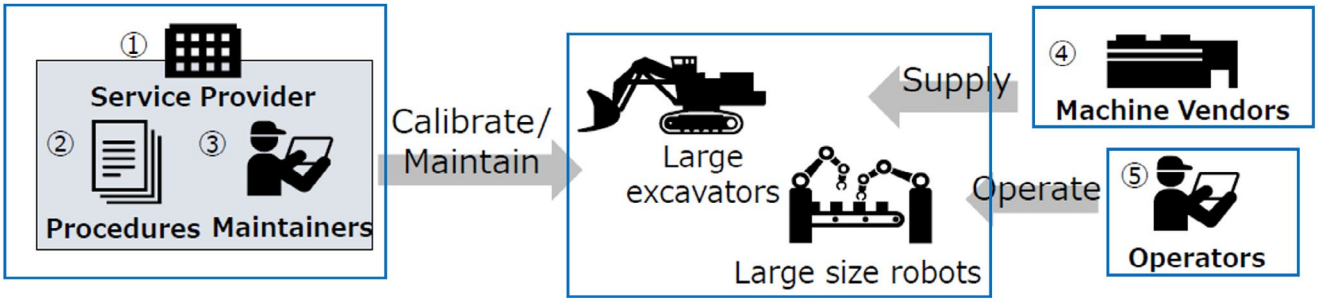
Note: Depending on the use case or business context, different attributes would define trustworthiness. These attributes may include authenticity, resilience, accountability, traceability, sustainability, compliance to social regulations, etc. for organizations. In terms of products’, trustworthiness attributes may include authenticity, integrity, resilience, availability, reliability, confidentiality, privacy, safety, usability, etc.

5. The Trustworthiness Concept in Practice

A Trustworthiness (TW) concept introduced in our last common white paper [2], presented a structured way to handle supply chain trustworthiness leveraging the concept of Trust Domains (TDs) and Trusted Interactions (TIs). Entities within a TD are suggested to identify their TW at-tributes related to that particular supply chain, business context or use case.

An example of service and maintenance of large machines in-field is shown below, in Figure 2. It is often cumbersome to track the entity responsible for down-time after maintenance or updates of machines in fields. So having this target in mind, the trustworthiness concept can be used to identify measures that must be met at TIs to ensure that the entity responsible for each mainte-nance of machine is immutably logged.

Figure 2: An example of service and maintenance of large machines in-field



Source: Plattform Industrie 4.0

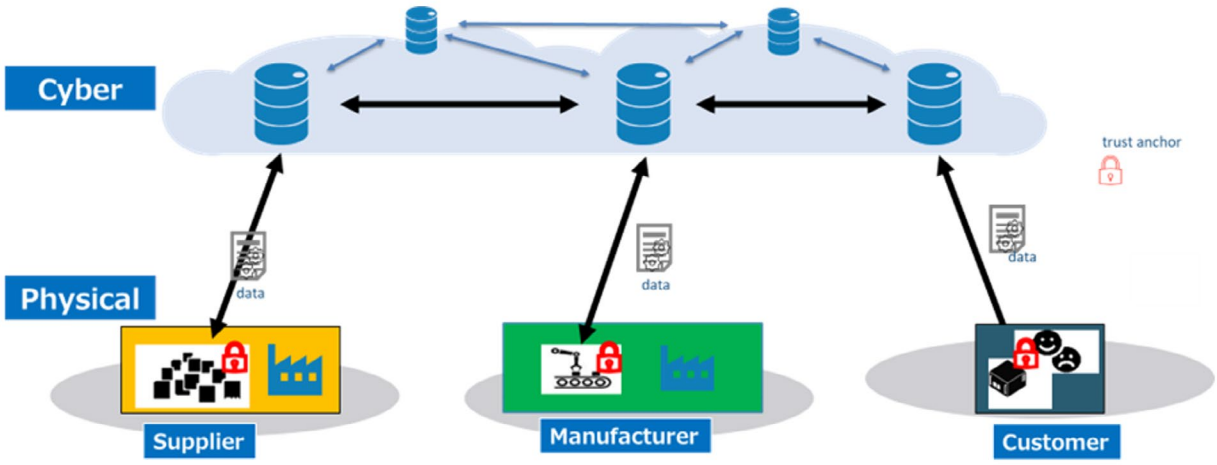
In figure 2, different trust domains are shown (blue rectangles) that should identify their trustworthiness attributes, as listed in the table below. Now when the TDs interact amongst themselves, they must negotiate and exchange proof of measures to achieve the targeted and negotiated trustworthiness attributes. The following TWP example, shows the "Type" entry consists of "organization", "people", "procedure", "component", "data", and "system" as in [4].

Table 1: Example TWP for service and maintenance use case

TWP Context	Type	Trustworthiness Attributes	(Digital) Verifiable Proof
Calibration and maintenance service provider which has certification.	Organization	Reliability	ISO/IEC 17025 Certificate
Calibration equipment which has certification.	Component	Reliability, Accountability, Accuracy	Calibration certificate for equipment
Methods of calibration and/or maintenance which follow law or standards.	Procedure	Reliability, Accountability, Accuracy	ISO 9001 Certificate
Maintainers who have certification or specific skills.	People	Reliability, Accountability	License for maintenance

The digital information derived from products by different entities through the supply chain are also an important element for supply chain trustworthiness. The digital information corresponding to the product (for e.g., digital twin) must have a consistent and robust link to the corresponding physical world entity. Otherwise, it is difficult to ensure that the shared information is multilaterally trustworthy. Each product that securely bind the product's attributes to the product's identity must present accurate and up-to-date information about the product. In order to support this persistent link, the corresponding entity must have a trust anchor that binds subject's identity to the corresponding information. In this way, subject(s) essential for establishing trustworthiness can be identified. Trust anchors can be realized, for instance, in form of Secure Elements (Security ICs) or various types of Physical Unclonable Functions (PUFs), which cannot be copied or forged easily. In this way, persistent binding of the product information to the corresponding product can be maintained throughout the product life cycle and can be used to verify its authenticity and reliability.

Figure 3: Persistent binding of digital and physical world



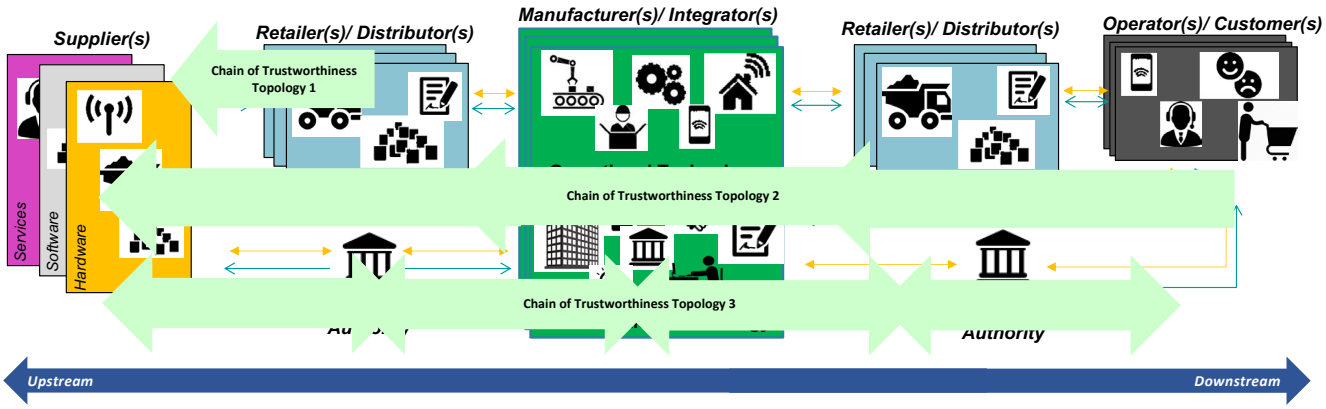
Source: Plattform Industrie 4.0

6. Chain of Trustworthiness Topologies

The last common whitepaper [2] introduced a technology-agnostic structure to exchange Trustworthiness Expectations (TWEs) and Trustworthiness Capabilities (TWCs) along the supply chain, called the Trustworthiness Profile (TWP). Extending on the utilization of the TWP, the following section describes different constellations of trustworthy relations that can lead to a chain of trustworthiness.

The last whitepaper also introduced the trust transitivity leading to the concept of chain of trust. In the following sections, we elaborate the derivation of chain of trustworthiness and depict different constellations of trustworthy in a supply chain.

Figure 4: Chain of trustworthiness topologies



Source: Plattform Industrie 4.0

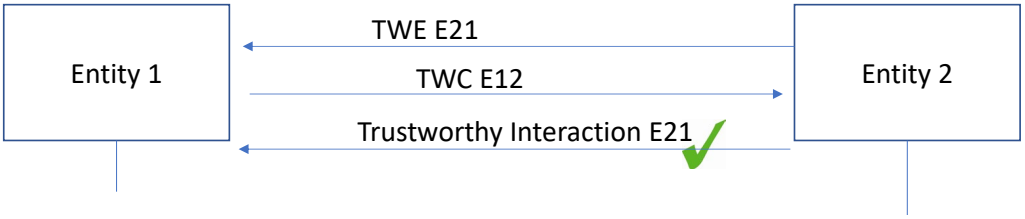
6.1 Chain of Trustworthiness Topology 1, i.e., Unilateral Trustworthiness

In the following text, TWEs are trustworthiness expectations, TWCs are trustworthiness capabilities, and the following alphanumeric shows the order of entities, for example, E21 implies from entity 2 to entity 1.

The first chain of trustworthiness topology, i.e., unilateral trustworthy relationship is where the downstream entity (entity 2) first sends its trustworthiness expectations (TWE E21) to the immediate upstream entity (entity 1). Likewise, then the upstream entity sends its corresponding trustworthiness capabilities (TWC E12) to the downstream entity. In this way, the downstream entity can evaluate upstream entity's TWCs based on its own company policy and can determine the aspects or extent of trustworthiness in its relation to the immediate upstream entity, as depicted by the green tick mark in the figure below. Therefore, it is only unidirectional trustworthiness. The trustworthiness profile, introduced in [3] can be used in such scenarios.

This is one of the most common scenarios. Often the buyer (e.g., Entity 2) requires proof of certain properties and the seller (e.g., Entity 1) provides assurances.

Figure 5: Chain of trustworthiness topology 1, i.e., unilateral trustworthiness



Source: Plattform Industrie 4.0

6.2 Chain of Trustworthiness Topology 2, i.e., Unilateral Trustworthiness Propagation

This is extension of the previous approach. Here the trustworthiness expectations (TWE E32) from the downstream entitites are communicated to the upstream entities in a hop-to-hop manner.

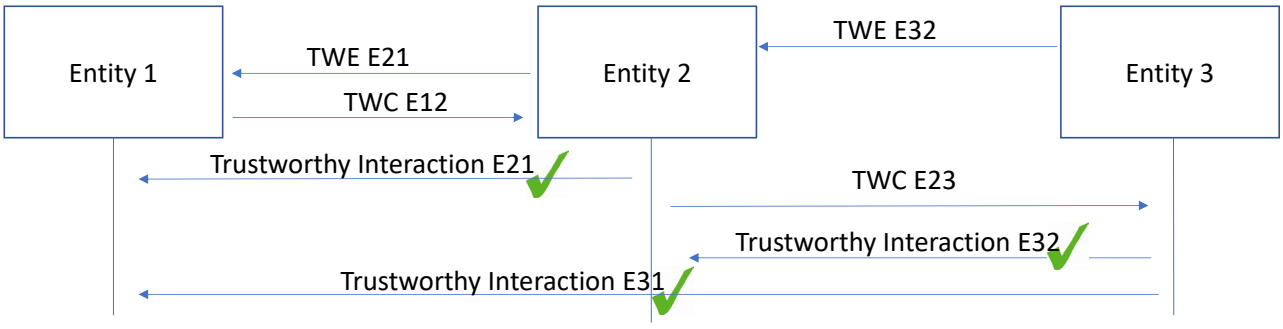
The downstream entity, i.e., Entity 3 asks its immediate upstream node, i.e., Entity 2 for his TWEs (TWE E32) which aslo includes its trustworthiness expectations from the entity before Entity 2, i.e., the Entity 1, for e.g., a sub-supplier. Entity 2 includes Entity 3's TWEs to his TWEs that it sends to Entity 1, i.e., TWE E21. Therefore, TWE E21 also includes TWE E31. Entity 1 then prepares and sends its corresponding trustworthiness capabilities, i.e., TWC E12 that also includes TWC E13. Entity 2 can evaluate them and determine the aspects or extent of trustworthiness in its relationship with Entity 1, i.e., trustworthy interaction E21.

Now the Entity 2 can extract entity 1's trustworthiness capabilities that were requested by Entity 3 and combine its own TWCs to generate combined trustworthiness capabilities, i.e., TWC E23, that actually includes parts of TWC E12.

Next, the Entity 3 can evaluate the received TWCs based on its own company policy and determine the aspects or extent of trustworthiness in its relationship with Entity 2 (Trustworthy interaction E32) and Entity 1 (Trustworthy interaction E31). In this way, for a specific business context Entity 3 will Trust Entity 1 without having any direct relation with it. So, Entity 3 trusts Entity 1 only via Entity 2. Therefore, it is essential for Entity 3 have trustworthy relation with Entity 2 to trust Entity 1.

The extended trustworthiness profile introduced in our last whitepaper [2] can be leveraged in such scenarios. This constellation depicts scenarios where buyers' requests assurance from not only suppliers but also their sub-suppliers.

Figure 6: Chain of trustworthiness topology 2, i.e., unilateral trustworthiness propagation



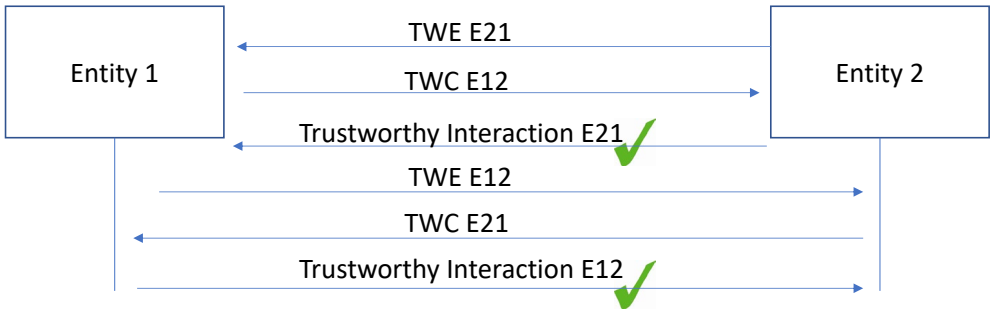
Source: Plattform Industrie 4.0

6.3 Chain of Trustworthiness Topology 3, i.e., Bilateral Trustworthiness

This approach is similar to the first approach with the addition that the Entity 1 also send its TWEs (TWE E12) to Entity 2 and likewise, Entity 2 will also send its TWCs (i.e., TWC E21) to Entity 1. Now, both the entities can evaluate other entity's TWCs based on their company policy and determine the aspects or extent of trustworthiness in its relationship with the other, i.e., Trustworthy interaction E21 and Trustworthy interaction E12.

This constellation can be imagined as when the seller also requests some assurances from its buyer, for e.g., use of its products in the allowed markets.

Figure 7: Chain of trustworthiness topology 3, i.e., bilateral trustworthiness



Source: Plattform Industrie 4.0

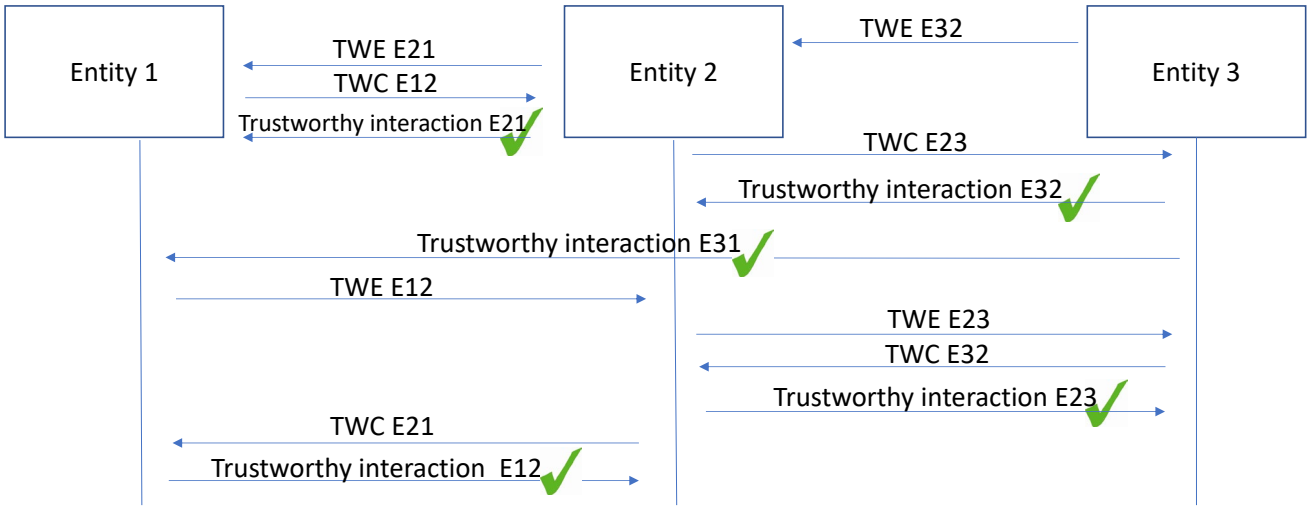
6.4 Chain of Trustworthiness Topology 3, i.e., Bilateral Hop-to-Hop Trustworthiness Propagation

This approach is extension of approach introduced in Section 6.2. Here, not only the downstream entities send their trustworthiness expectations to the upstream entities but also the upstream entities will send their trustworthiness expectations (TWE E12 and TWE E23) to downstream entities and downstream entities send their trustworthiness capabilities to the upstream entities (TWC E21 and TWC E32). Now, all entities evaluate the received TWCs corresponding to their TWEs based on their company policy and determine the aspects or extent of trustworthiness in its relationship with that entity.

The significant aspect is that the Entity 3 trusts Entity 1 via Entity 2, i.e., Trustworthy interaction E31 but the other way round is not so, that is Entity 1 doesn't have a trustworthy relation with Entity 3 via Entity 2, i.e., Trustworthy interaction 13 doesn't exist. But in case TWC E21 would also include the trustworthiness capabilities sent by Entity 3 to Entity 2, i.e., TWC E32, then the Entity 1 would also have an indirect trustworthy relation with Entity 3 via Entity 2.

Such a constellation can be imagined in scenarios where upstream entities require assurance only from their immediate downstream entity, for e.g., allowance of sale of a product in a particular region or market. And the downstream entities require assurances from not only the immediate upstream entity but also from the entity before, for e.g., sub-suppliers.

Figure 8: Chain of trustworthiness topology 3, i.e., hop-to-hop bilateral trustworthiness propagation



Source: Plattform Industrie 4.0

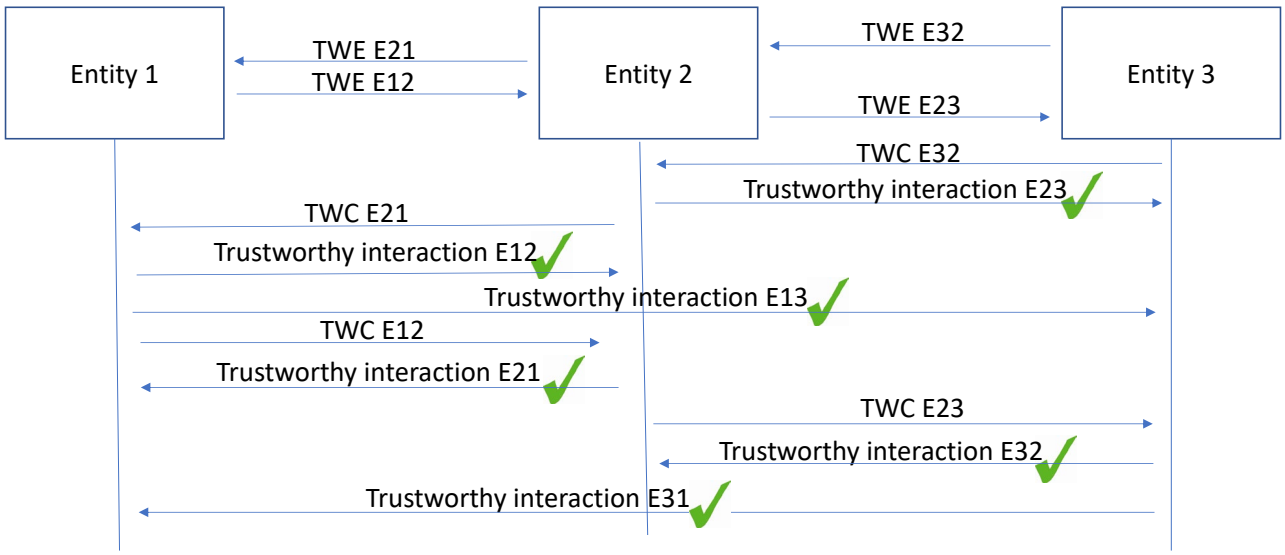
6.5 Chain of Trustworthiness Topology 3, i.e., Continuous Bilateral Trustworthiness Propagation

This is similar to approach 3a with a different sequence of exchange of TWCs and TWEs so that Entity1 is also able to establish a trustworthy relation with Entity 3 via Entity 2, i.e., Trustworthy interaction E13.

With the help of these chain of trustworthiness topologies, entities in a supply chain can formalize their relationship with other communicating entities and identify their trustworthiness relationships with them.

Bilateral trustworthiness propagation topologies can be leveraged for customized or catalog products. For e.g., the manufacturer of a product wants to ensure that the material used for the development of its products is allowed in its targeted market, or that their products are sold in the intended and allowed market, etc.

Figure 9: Chain of trustworthiness topology 3, i.e., continuous bilateral trustworthiness propagation



Source: Plattform Industrie 4.0

7. Supply Chain Trustworthiness Supporting Infrastructure

From supply chain perspective, depending on the business context or use case, a trustworthiness supporting infrastructure must meet different requirements, and have subsequent measures in place. The following non-exhaustive list presents some of such requirements:

- **Robustness, availability, and resilience, e.g.: no single point of failure**
  - Robustness against known attacks and environmental accidents is an important requirement for a trustworthiness infrastructure.
  - Single point of failure must be avoided.
  - Appropriate incidence response must be implemented to support resilience.
  - Availability of information needs to be secured (by backups) and needs to be communicated transparently without discrimination to relevant (applicable, authorized) entities.
  - Chain of trustworthiness must be adaptable and resilient to any (single) point of failure.
  - Long term availability must be supported for assets with long life cycles.

- **Scalability**
  - Trustworthiness infrastructure must be applicable to global IoT market and user community.
  - Interoperability relevant for trustworthiness must be considered from the design phase of systems and solutions.
  - Solutions must be interoperable and must be able to cooperate with other solutions (as long as possible without compromising security).
  - From suppliers' perspective, material and parts must be easily integrated in various markets (horizontally scalable).
  - From buyer's perspective, common interfaces for sharing part or material related information with the other potential buyers in various markets must be available.
- **Privacy/confidentiality preserving**
  - Only the necessary business IPs must be shared with the authorized entities.
  - Business cases must be protected against known attacks.
  - Applicable privacy laws must be obeyed.
  - The system must allow to specify and control access to any data.
- **Integrity, Authenticity, Accountability**
  - Integrity and authenticity of information along the whole supply chain must be verifiable for every relevant supply chain stakeholder.
  - Accountability of actions taken must be supported (logging, etc.).
  - Entity can verify the authenticity of the products and data along the whole supply chain.

- **Support of different trust levels**
  - Depending on the business context appropriate trust levels need to be supported.
  - Trust levels are not for free and must be financed by the business case using it. Thus, different verticals may want to support different trust levels.
  - Interoperation and mapping of trust levels of solutions in different verticals (with different trust levels) should be possible.

- **Easy usage, easy join, and easy leave**
  - Participants should be able to use/join the chain of trustworthiness environment easily (by low effort and cost).
  - If someone leaves the chain of trustworthiness, this must not impose a failure/revocation of already made statements and claims.
  - From infrastructure administrator's perspective, the cost to build and operate the infrastructure is also important from the standpoint of easy provision.

- **Clear governance**
  - Non discriminative and unbiased.
  - Provable compliance to regulations and standards.

8. Trustworthiness Repository

In order to realize chain of trustworthiness topologies described in the section 6, a mechanism is needed to indicate or share TWEs and TWCs with other supply chain entities. Trustworthiness repository can be leveraged for sharing TWPs between supply chain entities and it can be understood as:

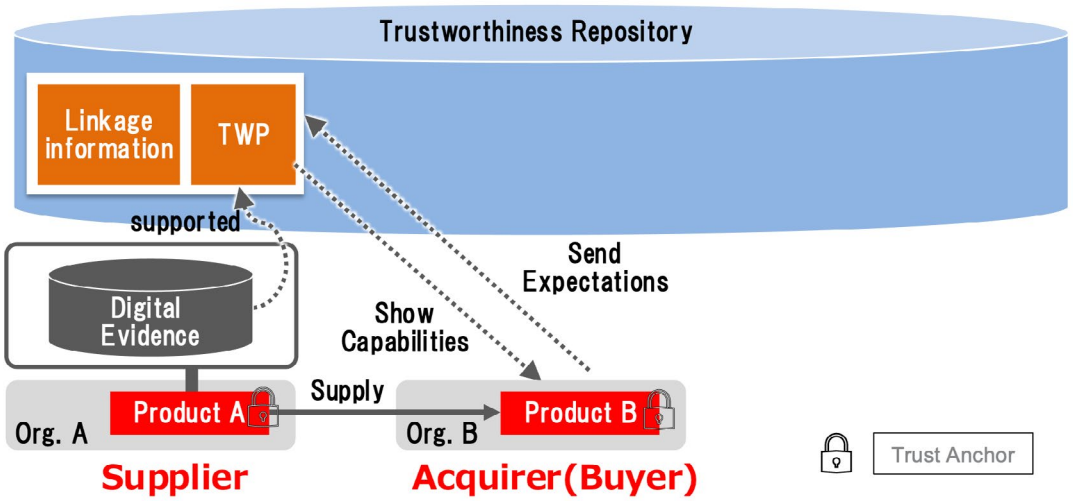
A trustworthiness repository contains TWP (Trustworthiness Profile) that consolidates conformity and trustworthiness relevant information. Based on the contained information, the trustworthiness repository provides functions to search for chains of trustworthiness.

TWP is information used for both trustworthiness "expectations" and "capabilities" and is supported by digital evidence. Linkage information is used to enable TWPs to be associated, and to build a chain of trustworthiness. Linkage information consists of, for example, information on which product combinations a certain product is composed of and where a certain product is used.

For digital evidence, trust anchors can be used to ensure a higher degree of reliability. Trust anchors provide a consistent and robust link to the physical product and support presentation of an accurate and up-to-date evidence information about the product. For example, digital data measured by reliable sensors is more reliable compared to the data collected visually by humans, as it is free of human errors. Furthermore, reliability can be enhanced by guaranteeing that the "activity amount" (data) measured by the sensor itself has not been tampered with. In that sense, digital evidence leveraging trust anchors provide robust trustworthiness in supply chains.

The following figure (Figure 10) illustrates the sharing of TWC as described in Section 6.1, i.e., Unilateral Trustworthiness. In this case, organization A is equal to Entity 1, and organization B is equal to Entity 2. Organization A supplies product A to organization B, and organization B uses this product A to make a product B. Figure 10 shows the mechanism for sharing A's TWC with organization B. At first, organization B its TWE for organization A or product A to the trustworthiness repository. Then, the trustworthiness repository replies with TWP corresponding to the TWEs sent by organization B. Then, organization B can obtain the TWCs of A, i.e., TWC E12 in Figure5, from the trustworthiness repository.

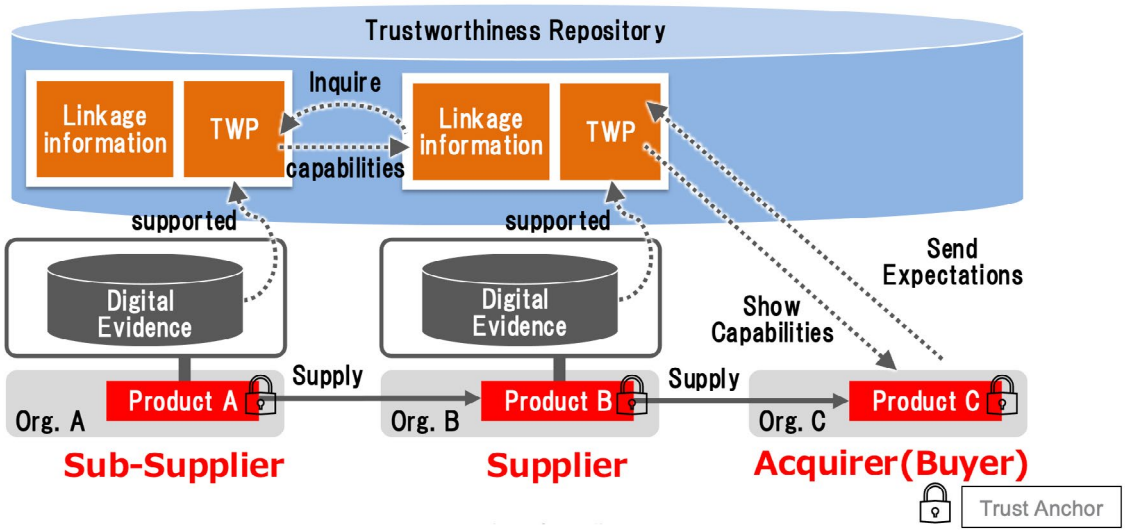
Figure 10: Trustworthiness repository for unilateral trustworthiness



Source: Plattform Industrie 4.0

As another example, the sharing of TWC in Section 6.2, i.e., Unilateral Trustworthiness Propagation, is shown in the Figure 11. In this case, organization A is equal to Entity 1, organization B is equal to Entity 2, and organization C is equal to Entity 3. Organization A supplies product A to organization B, and organization B uses the product A to make a product B. Organization B supplies product B to organization C, and organization C uses the product B to make a product C. This figure shows the mechanism sharing A's and B's TWC to organization C. At first, organization C sends its TWEs for organization A's or product A's and for organization B's or product B's to the trustworthiness repository. Then, Trustworthiness repository replies and show the TWP of A and B that are corresponding to the TWEs coming from organization C. Organization C can obtain A's TWP, i.e., TWC E12 in Figure 6, by querying A's TWP by using B's linkage information depicting that product B is composed of product A. Then, organization C can then obtain the TWPs of A and B, i.e., TWC E23 and TWC E12, from the trustworthiness repository.

Figure 11: Trustworthiness repository for unilateral trustworthiness propagation



Source: Plattform Industrie 4.0

9. Conclusion

The whitepaper extends the trust transitivity concept, introduced in our last white paper, by introducing detailed chain of trustworthiness topologies. Chain of trustworthiness topologies depict possible scenarios of trustworthy relationships in global supply chains and can be leveraged to identify and realize the applicable topology to any business case.

Furthermore, by utilizing a mechanism for sharing TWPs and searching the relationship between them, such as a trustworthiness repository, chain of trustworthiness can be established throughout the supply chain.

10. Future Work

It is evident that data sharing amongst supply chain stakeholder will continue increasing. It is essential to ensure reliability of shared data. In the future, we intend to work on:

1. Trustworthy derivation of digital information from the products and organizations in a supply chain. The level of trustworthiness might be different depending on the use-case. We aim to examine different use cases as well.

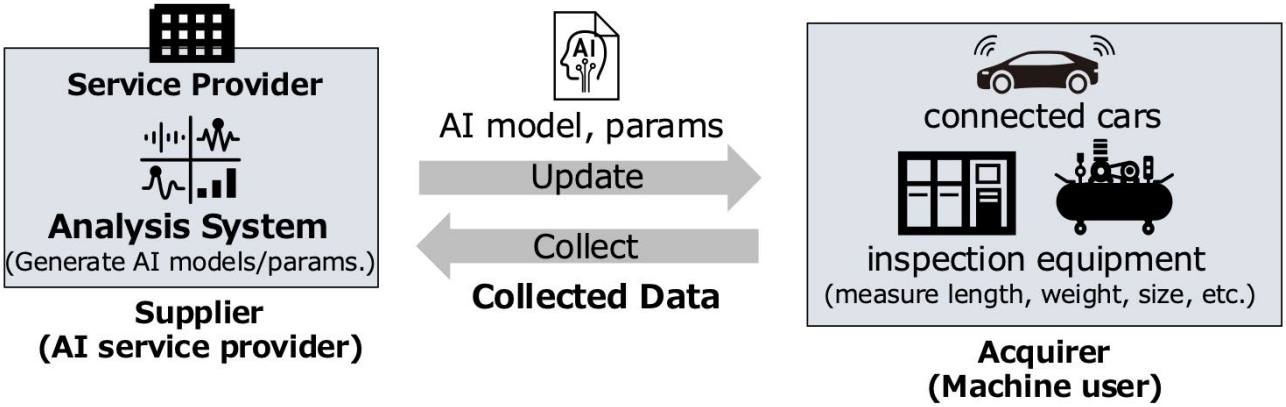
2. The supply chain is intricately branched. In the supply chain, trustworthiness is required for various objects. For that, we need means of collaboration between systems that establish trustworthiness along the supply chain. We need to build a supply chain trustworthiness system that is not entirely dependent on the trustworthiness of each participant.

3. Basic idea of trustworthiness repositories is introduced in this white paper. In the future, we intend to identify detailed functionalities of a trustworthiness repository. For example, each industrial vertical can have its own trustworthiness repositories which can be distributed. In the case of distributed, there is a need to discuss and examine the mechanism of cooperation that ensures interoperability between different trustworthiness repositories.

11. Annex

Another example use-case of AI model and parameters update service is shown in Figure 12 below. This service collects data from devices that utilize AI (e.g., connected cars and inspection equipment) to maintain or improve their performance, then generate and updates AI models and parameters based on the collected data.

Figure 12: An example of AI model and parameters update services



Source: Plattform Industrie 4.0

The following TWPs are required of service providers in this use-case.

Table 2: Example TWP for AI update service

TWP	Type	Trustworthiness Attributes [5]	(Digital) Evidence example
Data collected from current Machines at current timing.	Data	Integrity, Authenticity	Data of Metadata
Analysis system which works correctly and/or have security configuration followed by best practice.	System	Reliability, Accountability, Accuracy	Validation/Audit record

References

[1] https://jtc1info.org/sd-2-history/jtc1-working-groups/wg-13/

[2] https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/IIoT_Value_Chain_Security2.pdf?__blob=publicationFile&v=4

[3] https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/IIoT_Value_Chain_Security.pdf?__blob=publicationFile&v=9

[4] https://www.meti.go.jp/english/press/2019/0418_001.html. Letzter Abruf: 16.03.2023

[5] ISO/IEC TS5723:2022

LIST OF PARTICIPANTS

Aliza Maftun (Siemens AG) | Dr. Wolfgang Klasen (Siemens AG) | Dr. Lutz Jänicke (PHOENIX CONTACT GmbH & Co. KG) | Michael Jochem (Robert Bosch) | Prof. Kai Rannenberg (Goethe University Frankfurt) | Prof. Tsutomu Matsumoto (Yokohama National University) | Dr. Asahiko Yamada (National Institute of Advanced Industrial Science and Technology) | Atsushi Kitamura (Robot Revolution & Industrial IoT Initiative) | Ayaji Furukawa (Toshiba Corporation) | Junya Fujita (Hitachi Ltd.) | Kumiko Mahara (Sony Semiconductor Solutions Corporation) | Masue Shiba (Toshiba Corporation) | Nobuaki Suzuki (Toshiba Corporation) | Dr. Satoshi Kai (Hitachi Ltd.) | Dr. Takashi Ogura (Hitachi Ltd.)

A discussion paper by the Action Group “Industrial Security” of Robot Revolution & Industrial Initiative and the Working Group “Security of networked Systems” of the Plattform Industrie 4.0

www.plattform-i40.de