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

PLATTFORM INDUSTRIE4.0

WHITE PAPER

IIoT Value Chain Security

Chain of Trust for Organizations and Products

Imprint

Publisher
Federal Ministry for Economic Affairs and Climate Action (BMWK)
Public Relations
10119 Berlin
www.bmwk.de

Editorial responsibility
Plattform Industrie 4.0
Bülowstraße 78
10783 Berlin

Status
April 2022

This publication is available for download only.

Design
PRpetuum GmbH, 80801 Munich

Picture credit
Adobe Stock / Sashkin / Title

Central procurement service:
Email: publikationen@bundesregierung.de
Tel.: +49 30 182722721
Fax: +49 30 18102722721

This publication is issued by the Federal Ministry of Economic Affairs and Climate Action as part of its public relations work. The publication is available free of charge. It is not for sale and may not be used by political parties or groups for electoral campaigning.

Contents

Figures

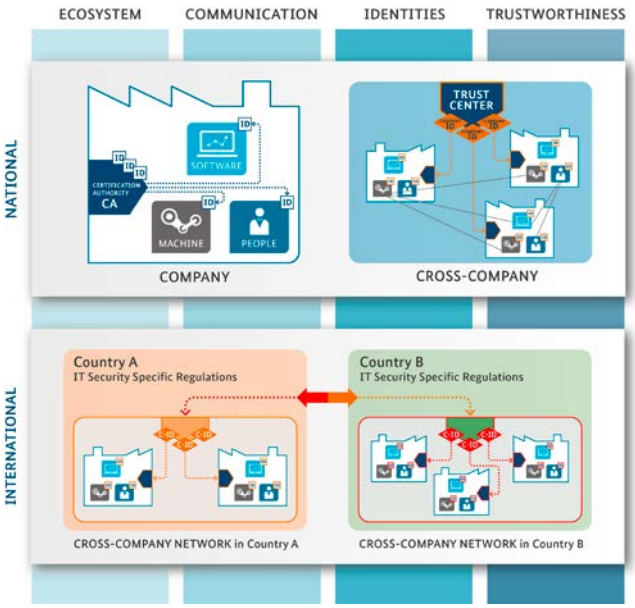
1. Background

In the past, Plattform Industrie 4.0, Germany and Robot Revolution & Industrial IoT Initiative (RRI), Japan announced four publications, “Facilitating International Cooperation for Secure Industrial Internet of Things/ Industry 4.0” (16th March 2017, 16th May 2018, 3rd April 2019, 23rd September 2020).

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 their geographical locations. Therefore, our previously published whitepaper elaborated the role of trustworthiness in global value chains and introduced mechanisms to assure trustworthiness between existing or potential business partners (see Figure1 and Figure2).

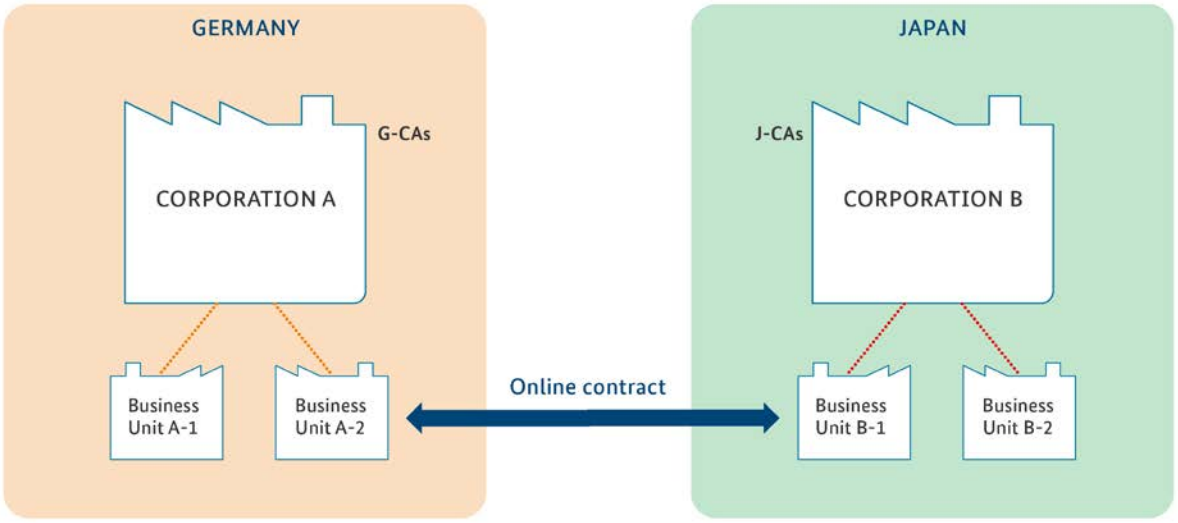
In line with these publications, Plattform Industrie 4.0 and RRI decided to proceed with the topic ‘chain of trust for organizations and production’ and worked on describing the role of trustworthiness of product to foster trustworthiness in increasingly digital and interconnected economies.

Figure 1: Overall Industry 4.0 Production Scenario



Source: Plattform Industrie 4.0

Figure 2: Targeted Use Case – Cross-Border Business Relationships



Source: Plattform Industrie 4.0

2. Introduction

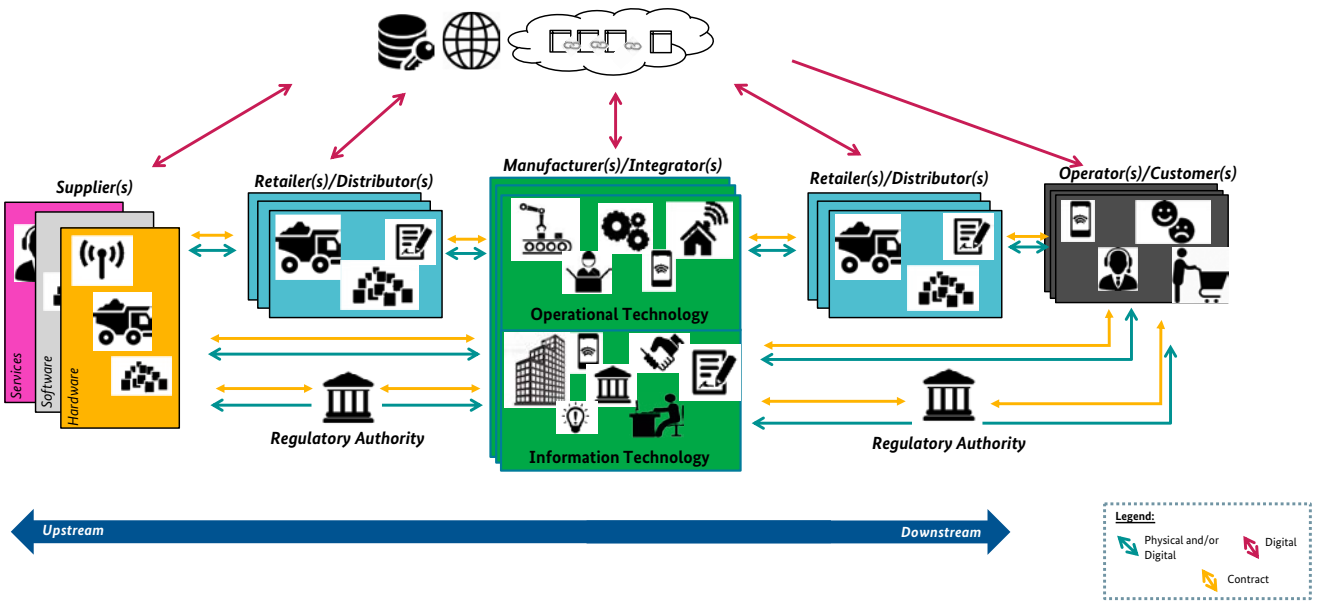
Highly automated international and global collaboration of industrial production environments is a key feature of Industry 4.0 (I4.0) and Society 5.0/Connected Industries. In various countries, production facilities will be able to collaborate with each other in nearly real time regardless of their geographical location. Therefore, availability of a comprehensive trustworthy ecosystem is an indispensable prerequisite.

Generally, supply chains are complex with many stages and stakeholders. Figure 1 shows a simplified supply chain of connected industries. In order to create digital business relationships across continents, all security related entities (organizations, people, components, data, procedures, systems) and communication processes need to be trustworthy.

Typically supply chains entities comprise of following actors:

- Suppliers that provide products and/or services. Products may comprise of hardware, software, and/or both. Suppliers typically act as a business partner to manufacturers/integrators.
- Manufacturers develop products leveraging products of their suppliers. Manufacturers provide their products to integrators, end users or customers. In some cases, manufacturers may also leverage open-source software components.
- Integrators design, install, and commission systems for end users or customers by combining equipment, controls, and software products from multiple manufacturers.
- Operators ensure the intended operation of the system for the end users or customers.
- Regulatory authorities or Security Certification Certificate Providers (SCCPs) checks compliance of products and/or processes to applicable regulations and standards correspondingly.
- Retailers, Distributors and Logistics are responsible for flow of goods along the supply chain. It may typically have suppliers, integrators, manufacturers, regulatory authorities, certification bodies, end users, and customers as its business partners.

Figure 3: Generic Supply Chain



Source: Plattform Industrie 4.0

- End users or customers acquire or procure products from manufacturers or integrators and receive services from operators.
- Supply chain attackers are entities with the intention of disrupting the supply chain or harming supply chain participants and products.

For ensuring trustworthiness in Industry 4.0/Society 5.0 ecosystem, trustworthy collaboration mechanisms and infrastructure must be developed. Therefore, this whitepaper introduces a systematic approach to establish trustworthiness along multiple nodes in a supply chain, focusing on organizations and products.

To achieve the overall target of establishing trustworthy supply chain, this white paper also focuses on relevant aspects of trustworthiness of organizations and products. This whitepaper presents an extension of the Trustworthiness Expectations and Capabilities Exchange Profile to support the realization of chain of trust along global supply chains.

3. Motivation

A supply chain typically consists of many entities contributing with their components and services to make a product available for the end user. A product goes through several processes, including integration of components, testing, certification, etc., before it reaches the end user. Supply chain actors have their own processes and may record information about their contribution in a similar or a very different manner. It is also quite cumbersome for the end user to find out the exact information about the product inhand and to confirm if the product meets its expectations.

Additionally, with increasing supply chain attacks, it is also essential to track the product's development life cycle to ensure that it comes from a trusted source, leverages components from trusted sources, is backdoor/malware free, is designed and allowed for the particular market, follows applicable standards and regulations, etc.

For instance, consider a manufacturer who manufactures his product using some off-the-shelf components and some components procured from suppliers located continents apart. Now, the manufacturer wants to verify the trustworthiness of the components before using them to manufacture its own products. Additionally, it also wants to provide confidence to its customers that its products are trustworthy as verified trustworthy components has been leveraged. The manufacturer also wants to ensure its customers that its products are genuine, and leverage only genuine components procured from suppliers that do not support child labor, do not exploit minerals, fulfil social regulations, and compensate their carbon footprint.

The aim of this activity is to provide support to such manufacturers so that they can find trustworthy components easily and can establish adhoc trustworthy relationships with operator(s)/customer(s)/end user(s).

4. Trustworthiness Structure

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

Generally, abilities of supply chain actors, that depict their trustworthiness, can be classified into two broad types. First type is organization related abilities like governance and risk management. Second type is product related abilities like providing products with competent quality, cost, and delivery.

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.

For instance, stakeholders across a supply chain negotiate and verify trustworthiness to select potential business partner as shown in Figure 4. At first, supplier and manufacturer negotiate and exchange their organizations' trustworthiness expectations and capabilities for establishment of a contractual agreement. The manufacturer selects a supplier that meets its organizational trustworthiness expectations, such as proved by compliance to IEC 62443 4-1, and makes a contract with the supplier. After that, the manufacturer makes a purchase order specifying product's trustworthiness expectations, such as compliance to IEC 62443 4-2. Once the product is delivered by the supplier, the manufacturer verifies the product trustworthiness based on its expectations and the product trustworthiness capabilities claimed by the supplier.

As shown in Figure 4, entities in the upper half declare attributes regarding organizations and products and lower half entities verify those attributes. Therefore, organizations' and products' trustworthiness can be understood as follows:

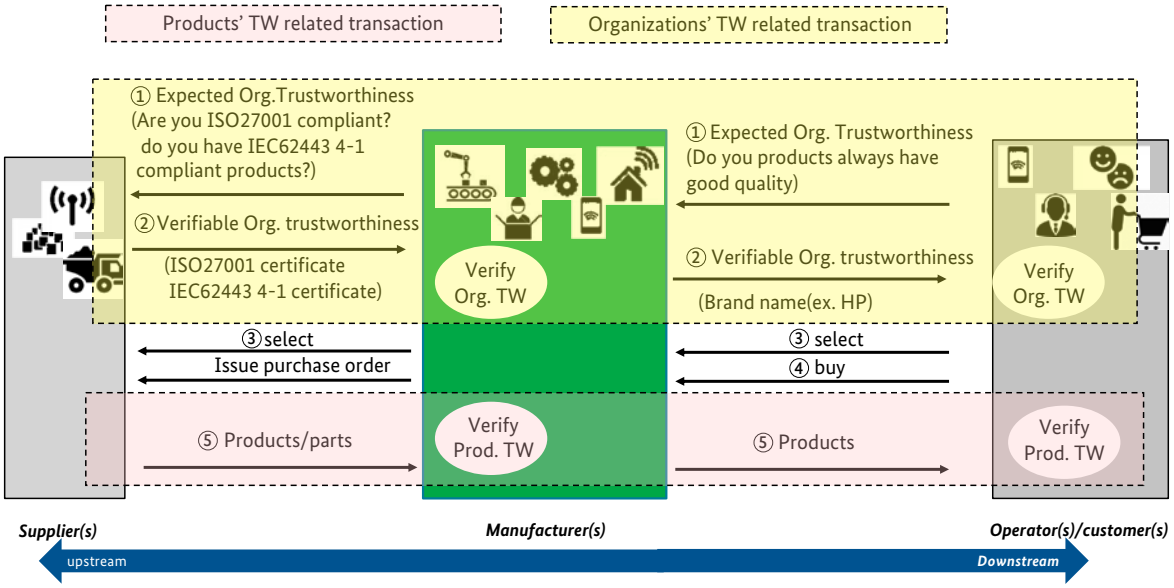
Organization's Trustworthiness

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.

Figure 4: Transactions Related to Organizations' and Products' Trustworthiness Along a Supply Chain



Source: Plattform Industrie 4.0

5. Structured Approach to Achieve Trustworthiness

5.1 Introduction to Trust Domains and Trust Interaction

A stakeholder has its resources and business activities in a physical or logical domain that can be termed as a Trust Domain. A Trust Domain (TD) can be defined as a domain with a specified authority that determines its present and targeted trustworthiness attributes. The specified authority or the responsible owner of the TD determines the trustworthiness attributes for all the entities that are part of this trust domain. A TD can be represented by an organization or a part of it. Based on the business context or applicable laws, a hierarchy of main and subtrust domains or overlapping TDs can also exist.

A supply chain comprises of several TDs that may negotiate and establish contracts to conduct business with each other. Each TD has a defined responsible entity for managing and establishing contracts with entities external to its TD.

The Trusted Interaction (TI) is an interaction interface between distinct trust domains. At each TI, communicating TDs must exchange, negotiate, and verify their current and expected trustworthiness attributes. In this way, the interaction between two TDs will have its defined trustworthiness attributes and the future interactions must be established accordingly.

Therefore, different TDs will interact with each other via TI to agree on the organizations' trustworthiness including expected capabilities of manufactured. The agreement is made during contract or procurement process. Likewise, products' trustworthiness often relates to expected attributes, especially security, that is defined in processes and product identity at the supplier and checked at the TI with the reliable product's identity by the manufacturer.

5.2 Introduction to the Trustworthiness Concept

The trustworthiness concept is an approach to establish trustworthiness along a supply chain in a structured manner. The approach can be applied to new businesses and can be leveraged to update the existing business relationships to make them more trustworthy.

As seen in previous chapter, trustworthiness in a supply chain can be divided into two types (shown in Figure 5):

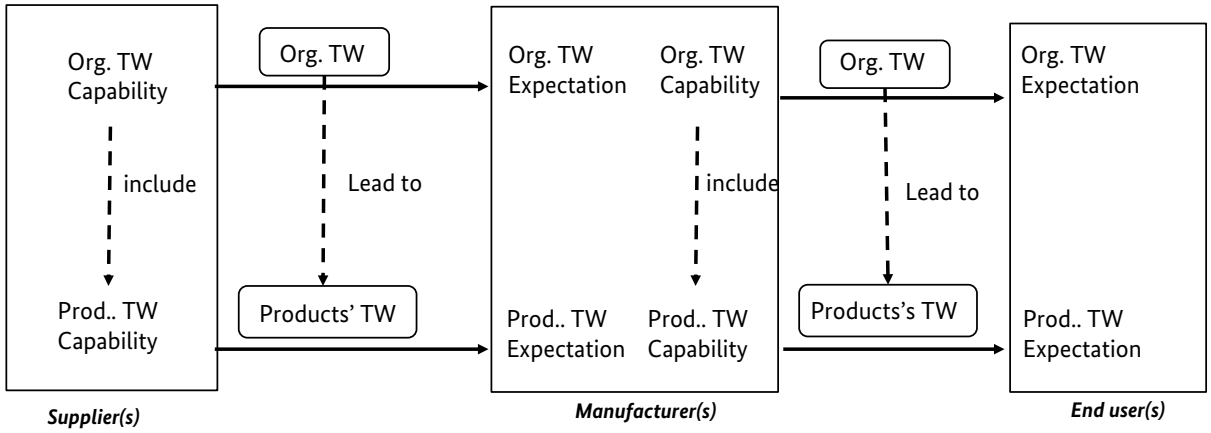
- First type is the Trustworthiness propagation across TDs along the supply chain.
- Second type is transformation and interpretation of organizations' trustworthiness to products' trustworthiness within a TD.

Figure 5 shows the relationship between the two types of trustworthiness:

- Trustworthiness propagation across TDs:
  - Upstream entities in a supply chain provide organizations' trustworthiness corresponding to the expectations from downstream supply chain entities.
  - After organizations' trustworthiness, upstream supply chain entities provide details about their products' trustworthiness.
- Transformation and interpretation of organizations' trustworthiness to products' trustworthiness within a TD:
  - Organizations' trustworthiness leads to Products' trustworthiness. If any entity provides a proof of its organization's trustworthiness, it means that its business processes for manufacturing respective products are trustworthy. So, in this way, organizations' trustworthiness leads to products' trustworthiness. For example, if a supply chain entity complies with RRI's Industrial Security Supply Chain Questionnaire including IEC 62443 4-1, its products are expected to have security as products' trustworthiness to a certain extent.

It is noted that sometimes products themselves can and should prove their trustworthiness without referencing to the organizations' trustworthiness, especially in secondhand market. Products' trustworthiness, such as quality including performance, usually degrades with time or while they are used. So, buyers of secondhand products have to verify the products' trustworthiness at the time of buying regardless of its manufacturer's trustworthiness.

Figure 5: Relationships between Organizations' and Products' Trustworthiness



Source: Plattform Industrie 4.0

5.3 Realization of the Trustworthiness Concept for Organizational Trustworthiness

The topic of achieving trustworthiness along the supply chain must be handled systematically so that the all the aspects are covered, and trustworthiness is achieved in a structured and overarching manner. To do so, organizations that want to expand their business by participating in existing supply chains or by developing new supply chains are recommended to follow the following steps:

- Identify distinct Trust Domains (TD) in its supply chain.
- Determine its own TD and establish targeted trustworthiness attributes for itself.
- Identify the requirements that entities part of its TD must fulfil to achieve the targeted trustworthiness attributes.
- Determine and realize measures to fulfil identified requirements.
- Find out other TDs that it needs to interact with for its business.
- Initiate a trustworthiness negotiation process with the identified TDs by defining its own trustworthiness attributes and expected trustworthiness attributes. The communicating TDs can do likewise, and they both establish a TI with negotiated trustworthiness attributes.
- Both communicating TDs should now identify the requirements and supporting measures to achieve the decided trustworthiness targets, such as integrity, availability, etc.

5.4 Realization of the Trustworthiness Concept for Trustworthiness of Products

Now moving towards the trustworthiness of products, the operator, end user or the customer must request the manufacturers to ensure that:

1) Parts/materials used to manufacture the product are authentic and genuine.

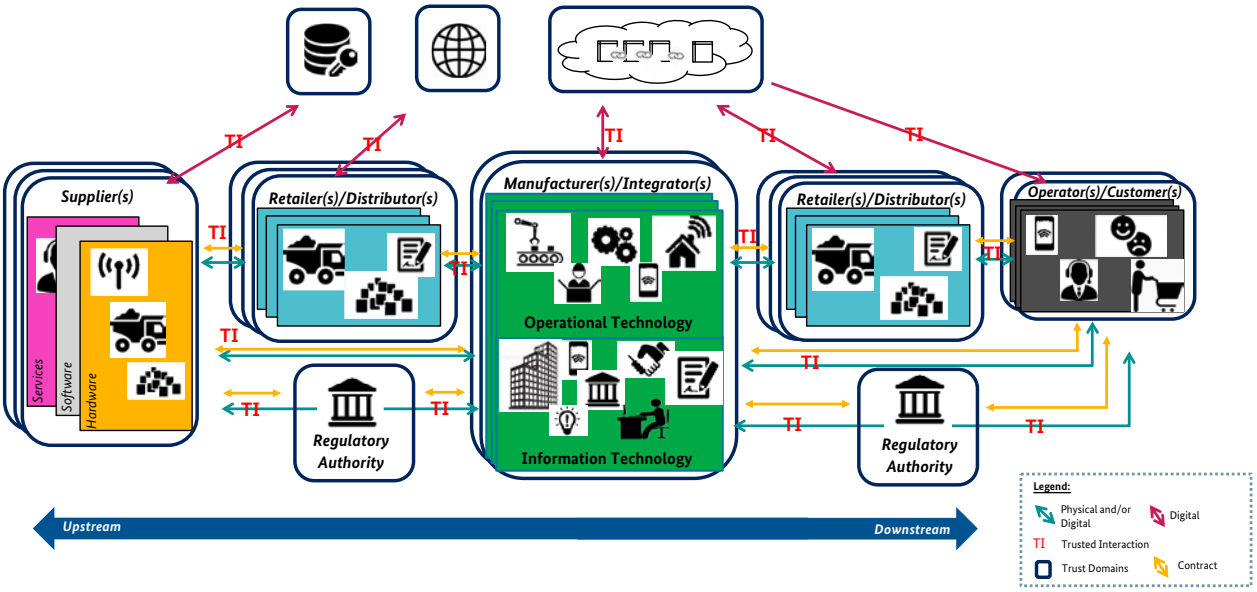
2) Only parts/materials that meet the contracted requirements are leveraged:

   - No illegal sub-parts and substances,
   - No illegal procurement process,
   - No violation of contract

3) Parts/materials don't have unspecified functions, such as malware and hardware Trojan horse.

4) Products can be demonstrated that no malware and contamination is included during design and manufacturing processes.

Figure 6: Trust Domains and Trust Interactions in a Supply Chain



Source: Plattform Industrie 4.0

5) Authenticity of products and their components can be verified.

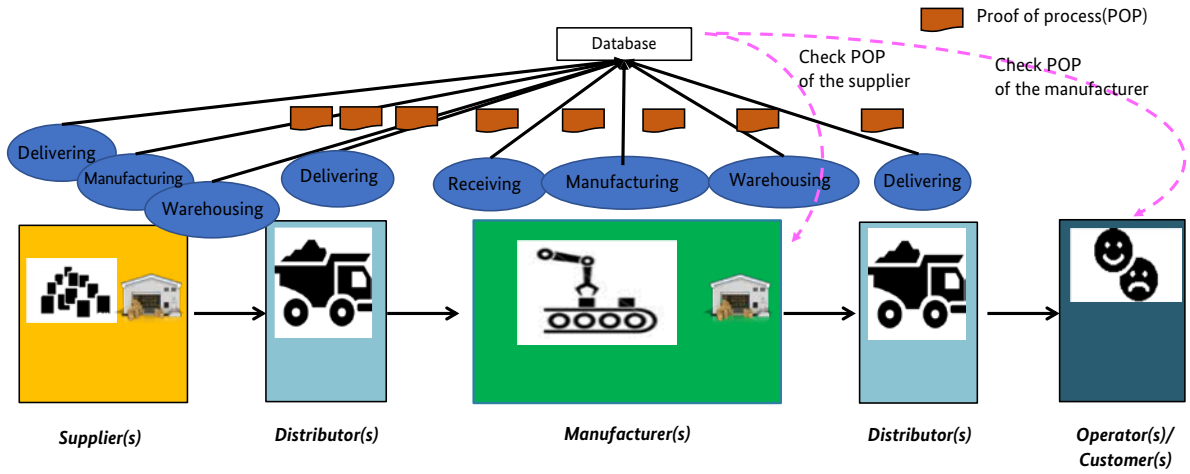
6) Products are not compromised and didn't undergo quality degradation during the delivery processes.

7) Products are designed and manufactured by following appropriate processes following applicable standards and regulations.

For example, consider Figure 7. In order to establish product trustworthiness, following must be performed:

- Verify (1), (2), (3) on receiving or while manufacturing.
- Verify (4) during design and manufacturing phase.
- Ensure (5) while manufacturing.
- Verify (5) on storing and delivering the products.

Figure 7: Establishing Products' Trustworthiness Along its Supply Chain



Source: Plattform Industrie 4.0

Some solutions to achieve the above-mentioned guidelines are listed in the following table:

Table 1: Solution examples Products' Trustworthiness

Technical Requirements	Solution examples
(1) Parts/material are authentic (real). • Providing proofs of proper delivering • Checking the identicality of parts/material produced and those received -IDs should be assigned to identify parts /material -Binding between IDs and parts /material should never been altered. -A process should be exist to check the IDs from the sub-supplier are identical to the IDs at the supplier.	• Physical Protection: temper proof • Proof of process using database • Barcode/RFID/ • Secure chip • Artifact-metrics
(2) Parts/material don't have illegal issues • Requesting that in the procurement requirements • Providing proofs that proper procurement had done. • Providing proofs of keeping the contract with the Manufacturer	• Making contract and clarify responsibility of the sub-supplier • Certification certificate (obtained before contract) • Proof of process using database
(3) Parts/material don't have harmful functions including malware • Providing proofs of checking no harmful functions in the parts and material	
(4) Products have no malware and contamination during design and manufacturing • Providing proofs of proper design and manufacturing processes	• Making contract and clarify responsibility of the supplier • Certification certificate (obtained before contract) • Proof of process using database
(6) Products are delivered without compromise and quality degradation. • Providing proofs of proper delivering processes	
(5) Products have IDs Manufacturer to verify authenticity. -Making and assigning proper IDs to products	• Barcode/RFID/ • Secure chip • Artifact-metrics

6. Means to Support Trusted Interaction

When a TD wants to establish a link with another TD, it first establishes a TI. For the establishment of a TI, it is essential that both the communicating entities can identify each other and also prove their authenticity to one another. For this purpose, technological solutions such as X.509 PKI certificates or W3C decentralized identifiers[1] can come into play. Usually, entities prove their authenticity be proving possession of a private key and the corresponding public is vetted and confirmed by a trusted third party, also called as a certificate authority in PKI.

Once the identity profile of the communicating entities is established, trustworthiness targets of the TI are determined. Both communicating TDs, must decide on measures to achieve those trustworthiness targets. As stated above, measure could be to ensure organizational trustworthiness at first followed by product trustworthiness in some cases. For both trustworthiness related transactions in Figure 4, it is essential to identify the subject(s), i. e., processes and products that must be kept into consideration to establish the required trust at the TI. For e. g., a device used in critical infrastructures must undergo extensive security testing and certification. Therefore, the device and likewise tests and processes that it has gone through must be uniquely and reliable identifiable. Additionally, the information corresponding to the subject (product or process) must have a consistent and robust link to the corresponding physical world entity. For e. g., digital twin of a device must have a persistent link to the device and must present accurate and up-to-date information about the device. In order to support this persistent link, the corresponding entity must have a trust anchor that binds the subject's identity to the corresponding information. In this way, subject(s) essential for establishing trust at TI can be identified. Trust anchors can be provided by so called Secure Elements (Security ICs) or various types of Physical Unclonable Functions (PUFs), which cannot be copied or forked easily[2].

Further, to achieve trustworthiness targets at the TIs, the entities must develop certain qualities that can be proven to the communicating TD. For e. g., while communicating to an entity in Europe, an entity from other TD must confirm its compliance to GDPR. Generally, such proofs are provided by compliance to certain standards or regulations, whereby the compliance is audited, verified and attested by a trusted third party. In Industry 4.0 context, such trusted third parties are termed as 'Quality Certifying Certificate Provider (QCCP), these entities, for e. g., TÜV Süd, SGS, JQA, etc., audit organizations, their processes, and/or products based on some predetermined criteria (standard) and issue a detailed report along with a compliance certificate, also called 'Quality Certifying Certificate (QCC)'. QCCs can be exchanged by entities of the communicating TDs to prove their capabilities to one another.

In order to negotiate and exchange trustworthiness expectations and capabilities, a standardized structure must be employed to ensure interoperability and scalability. Therefore, the Trustworthiness Profile, introduced in "IIoT Value Chain Security – The Role of Trustworthiness"3, can be leveraged to negotiate and exchange the trustworthiness expectations and capabilities at the TIs.

In "IIoT Value Chain Security – The Role of Trustworthiness"[3], the trustworthiness profile is used bilaterally between two communicating TDs in the supply chain ("supplier" and "buyer"). The supplier uses his QCCs to proof the capabilities of his own valued add to the delivered component. If the buyer wants to get assurance of capabilities of the suppliers' value add the concept for "Chain of Trust" needs to be introduced: In some business cases, if a proof of trustworthiness of various/all value adds along the supply chain is desired, this white paper introduces the extended trustworthiness profile, shown in Figure 8. The extended trustworthiness profile provides the buyer and the supplier the option to specify expectations and prove capabilities of other entities upstream the supply chain. The supplier has the option to attach capabilities of its suppliers to fulfil the expectations of its potential buyer.

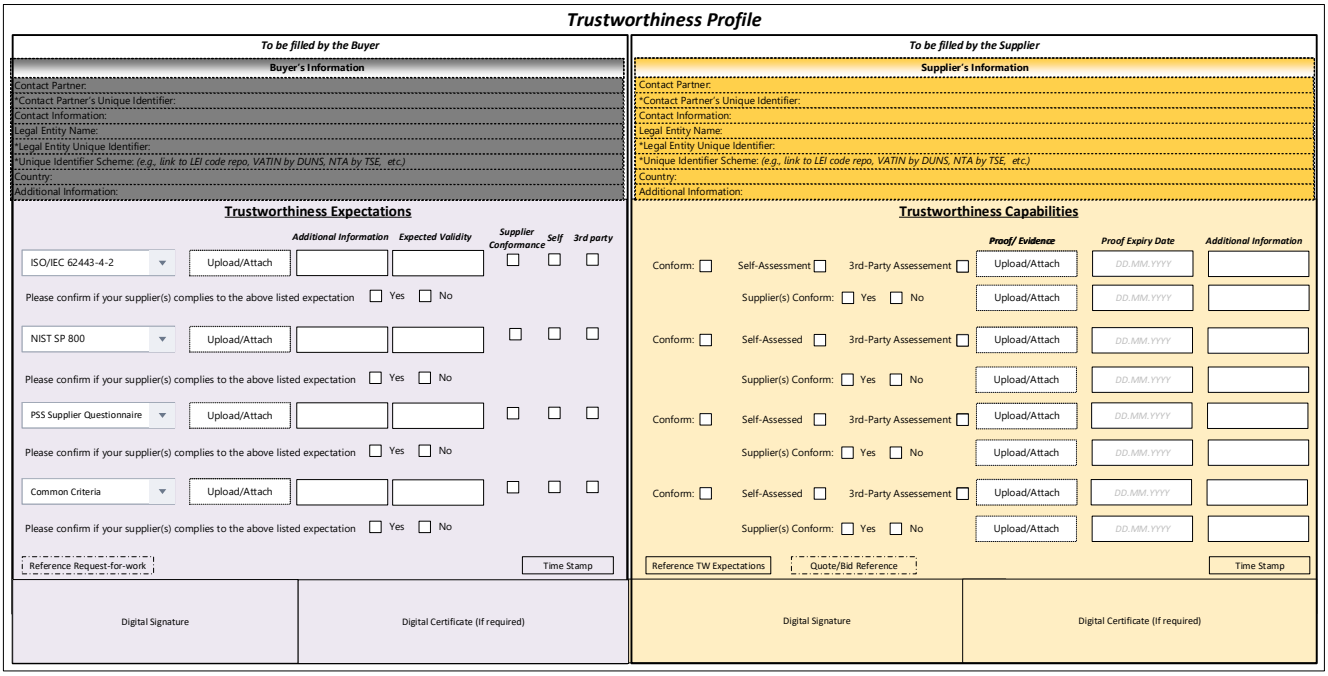
This covers scenarios where a proof of any other communicating TD's trustworthiness prior in the supply chain must be provided to the buyer. A TWP, which covers proofs for the supplier's suppliers is shown in Figure 8.

1 https://www.w3.org/TR/did-core

2 https://ieeexplore.ieee.org/document/8645638

3 https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/IIoT_Value_Chain_Security.html

Figure 8: Extended Trustworthiness Profile



Source: Plattform Industrie 4.0

It is considered that in certain scenarios, the supplier might not want to disclose its suppliers to its buyer for business reasons. Therefore, different technological solutions, for e.g., leveraging verifying credentials, can be used to preserve privacy of other TDs and to only prove certain quality.

7. Trust Transitivity Along the Supply Chain – Chain of Trust

7.1 Trust Transitivity to Chain of Trust

Trust transitivity is when trust can be extended outside the two trust domains between whom it was established. In a supply chain, trust transitivity can be understood as communication of trustworthiness capabilities upstream and downstream a supply chain. This leads to the concept of "chain of trust", i. e., concatenate the trustworthiness of interactions between trust domains in a supply chain.

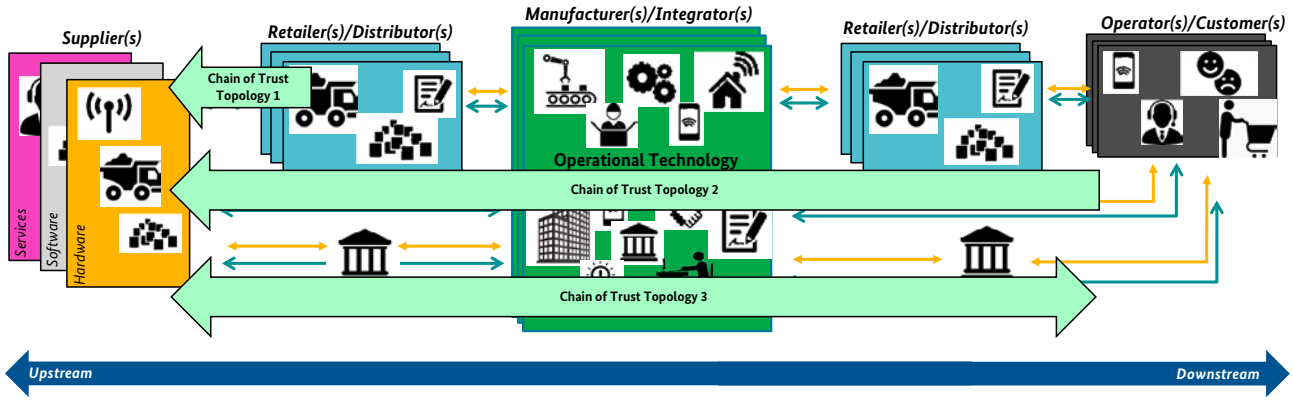
7.2 Chain of Trust Topologies

This paper introduces the concept of chain of trust that implies that all the relationships in a supply chain, from upstream to downstream, are trustworthy. There are three possible topologies to achieve chain of trust along the supply chain, as shown in Figure 9.

First chain of trust topology concerns the interaction between two immediate nodes in the supply chain. Each entity in a supply chain negotiates and determines trustworthiness before establishing a business contact with any other entity. As shown in Figure 9, downstream entity, such as a retailer, can present his trustworthiness expectations to the supplier. Likewise, the supplier must provide the retailer its corresponding trustworthiness expectations to create a trustworthy business relation. In this regard, the Trustworthiness Profile, introduced in "IIoT Value Chain Security – The Role of Trustworthiness"[4] can be helpful as it enables the negotiation and consolidation of trustworthiness expectations and capabilities between two immediate nodes in a supply chain. At present, digital signatures based on X.509 PKI and Quality Certifying Certificates issued by third parties also help in establishing trustworthiness regarding particular aspects between two entities in a supply chain. Moreover, contracts, questionnaires and agreements are an essential component of establishing trust. In terms of products, anticounterfeiting measures, such as protective seals, biomarkers, etc., also help in the establishment of trust between two entities in a supply chain.

Second chain of trust topology is when the trustworthiness capabilities of a supply chain entity is communicated to (one or several) nodes downstream a supply chain. The extended Trustworthiness Profile, shown in Figure 8, can support in this regard. As shown in Figure 9, trustworthiness expectations of downstream supply chain entities are propagated to upstream entities and likewise, trustworthiness capabilities are communicated downstream along multiple nodes. The extended Trustworthiness Profile enables consolidation and communication of capabilities of supplier's suppliers in a systematic manner. This will help the buyer to not only determine the trustworthiness of its immediate supplier but also to determine the trustworthiness of the components leveraged in the product that has been provided by the supplier. At present, this kind of trust propagation is

Figure 9: Chain of Trust Topologies



Source: Plattform Industrie 4.0

4 https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/IIoT_Value_Chain_Security.html

usually supported in form of carefully formulated questionnaires and contracts between the suppliers and buyers. In future, we assume that technologies such as DIDs, verifiable credentials would support the realization of such trust propagation along multiple nodes in a supply chain.
Especially, in some business scenarios, the supplier would not want to disclose certain information of its suppliers to its buyer. So, zeroknowledge based solutions can be used to support such use cases. Additionally, to strict binding of trustworthiness capabilities to the corresponding entity can again be realized using anti-counterfeiting measures.

Third chain of trust topology is when trustworthiness capabilities of all nodes in a supply chain are tracked and are traceable upstream, at any supply chain stage (with appropriate permissions). This implies bidirectional trust along the supply chain. As shown in Figure 9, both trustworthiness expectations and capabilities are propagated downstream and upstream the supply chain. This chain of trust topology is especially useful in scenarios where the supplier (seller) wants to ensure that its products are sold only in the intended market and comply to applicable national/international regulations. Track and trace solutions that consider trustworthiness aspects can be helpful in this regard.

7.3 General Requirements for Chain of Trust

Since trust is established by exchanging information that depicts trustworthiness of the corresponding entity, it is important to ensure that the information is also trustworthy. In order to ensure trustworthiness of information, it is essential that the there's a persistent binding between the realworld entity and its digital information which is accurate and up to date. In all such scenarios, it is essential to ensure that they digital world depicts an accurate and authentic picture of the corresponding realworld entity.

Supply chain comprises of many actors, products, components, etc. which lead to continuous generation of data/information. This also leads to continuously increasing amount of data that is essential for establishing trustworthiness. Therefore, measures should be taken to ensure availability of the right data and also for secure storage and communication of trustworthiness related information.

In some business scenarios, business partners would not be comfortable sharing all the information with other supply chain entities. For instance, the supplier might not want to disclose its suppliers to its buyer. But from the buyer perspective, it would be essential to know the trustworthiness aspects of the components used by the supplier. Therefore, in such scenarios, measures should be put in place to ensure confidentiality and IPR protection. Moving on, a governance structure can be thought of to address supply chain trustworthiness in a regulated manner.

Supply chains are not very complex as they also include interactions between different industrial verticals. Usually, certain structures or formats are used in particular industry verticals but interoperability between different industry verticals is not ensured. In order to achieve chain of trust, special consideration must be given to interaction between different industry verticals or different stages of supply chain, so that they can interoperate. Preferably solutions scalable regardless of industry vertical must be leveraged.

Above mentioned requirements are not an exhaustive list. For example, depending on business case, specific requirements can be determined using a comprehensive threat and risk assessment.

8. Conclusion

Plattform Industrie 4.0 and Robot Revolution & Industrial IoT Initiative first analyzed the structure of trustworthiness across a supply chain which consists of organizations' and products' Trustworthiness. From procurement's perspective, organizations' trustworthiness is used to select appropriate suppliers before establishment of contractual agreement. Product's trustworthiness is specified using attributes such as security and quality and is usually verified by buyers after the contractual agreement is established.

By using appropriate technologies such as globally unique IDs, digital signatures, digital proof of process, trustworthiness of organizations' and products' can be determined. Leveraging interoperable formats like trustworthiness profile, etc., chain of trust can be realized that will support global supply chains to be more trustworthy.

9. Future Work

Our whitepaper has introduced the classification of supply chain trustworthiness into organizations' and products' trustworthiness. This research and extensive discussions helped us identify following aspects that we would like to work on in the future:

1. In certain scenarios, suppliers would like to keep identity and details of parts/ material used in its products anonymous. However, manufacturers would like to have this information in order to determine the trustworthiness of the supplier. How can this tradeoff be supported by technological solutions?

2. Interoperability of solutions that support the exchange of trustworthiness expectations and capabilities.

3. Reliable subject identities as they are essential identify and authenticate not only the products but also their corresponding capabilities, including QCCs.

4. Means of collaboration between systems that establish trustworthiness along the supply chain. We have to create a supply chain trustworthiness system which is not entirely dependent on the trustworthiness of each participating entity. Our goal is to implement, as much as possible, robustness and resilience by technical means, which cannot be disturbed by any single stakeholder in the supply chain. It is a very difficult goal but we are positive to achieve it through technical means.

LIST OF PARTICIPANTS

Vanessa Bellinghausen, BSI | Junya Fujita, Hitachi Ltd. | Ayaji Furukawa, Toshiba Corporation | Dr.-Ing. Lutz Jänicke, PHOENIX CONTACT GmbH & Co. KG | Michael Jochem, Robert Bosch GmbH | Atsushi Kitamura, Robot Revolution & Industrial IoT Initiative | Dr. Wolfgang Klasen, Siemens AG | Aliza Maftun, Siemens AG | Kumiko Mahara, Sony Semiconductor Solutions Corporation | Prof. Tsutomu Matsumoto, Yokohama National University | Prof. Dr. Kai Rannenberg, Goethe University Frankfurt | Masue Shiba, Toshiba Corporation | Nobuaki Suzuki, Toshiba Corporation | Dr. Takeshi Yoneda, Mitsubishi Electric Corporation

This publication has been developed by the Working Group on Security of Networked Systems of the Plattform Industrie 4.0 in cooperation with our Japanese Colleagues from the Robot Revolution & Industrial IoT Initiative.

www.plattform-i40.de