IIoT Value Chain Security
- Chain of Trust for Organizations and Products -

Ayaji Furukawa
Robot Revolution Initiative, Japan
Toshiba Corporation

Aliza Maftun
German Platform Industry 4.0, Germany
Siemens AG

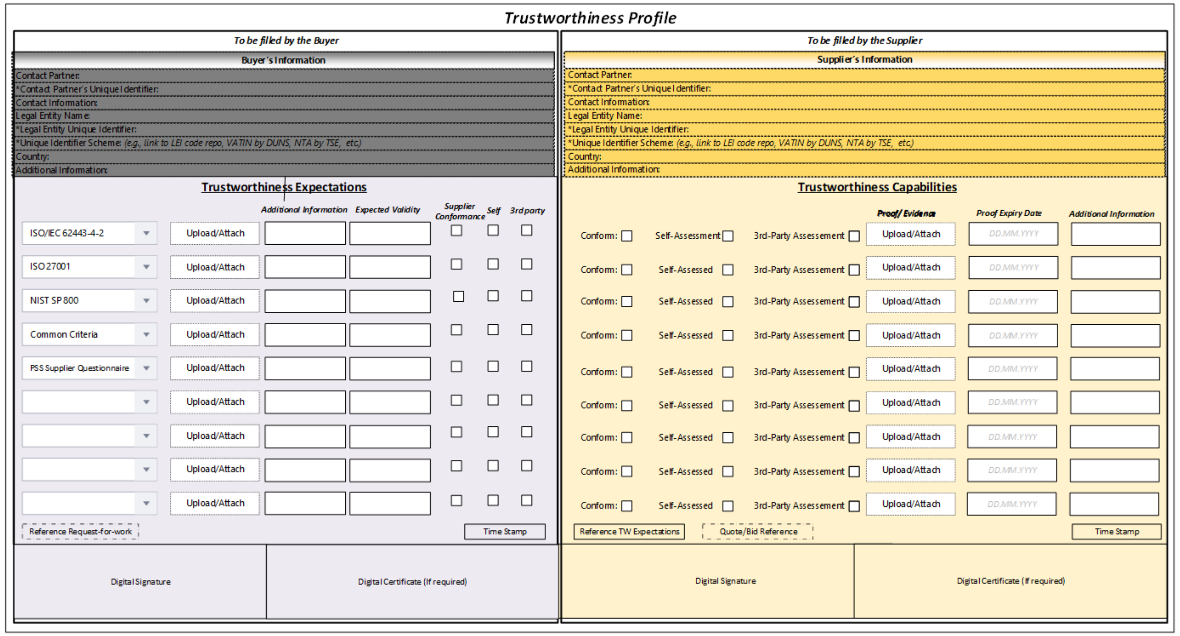
Agenda

- Introduction
- Motivation for Chain of Trust Along the Supply Chain
- Trustworthiness Definition, Structure and Concept
- Means to Support Trusted Interactions
- Trust Transitivity to Chain of Trust
- …

Introduction

Plattform Industrie 4.0, Germany and Robot Revolution Initiative, Japan had been collaborating since 2017 on topics concerning security of Industrial IoT (IIoT) and Industry 4.0 use cases.

The white paper introduced a **Trustworthiness Expectations and Capabilities Exchange Protocol" (TECEP).**



Source: *https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/IIoT_Value_Chain_Security.html*

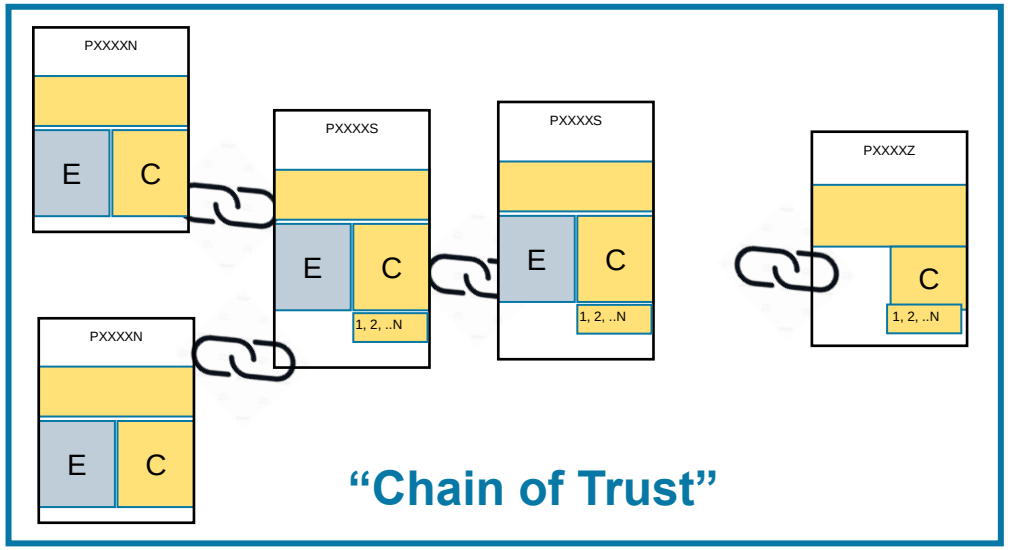
Why “Chain of Trust” Along the Supply Chain?

There exist many security approaches, which can be used for supply chains, e.g.:

ISO/IEC 28000, ISO 2700x, IEC 62443, ISO 15408, ISO 20243, ….

However, there does not exist a standard suite yet:

- which establishes & measures trustworthiness of security properties **along** the supply chain,
- which provides **assurance for several nodes** of the supply chain,
- which supports **interoperability**, and
- which enables **automated processing**.



Motivation

Growing supply chain attacks

Several different entities and stakeholders

Leverage many different processes, technologies and tools

Aim of our collaboration is to provide support to manufacturers so that they can **find trustworthy components** easily and can **establish ad-hoc trustworthy relationships** with other supply chain participants.

Ensure integrity and genuinity of recieved product

Provide assurance about own product to the customer

Prove compliance to applicable standards and regulations

Trustworthiness Definition and Structure

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

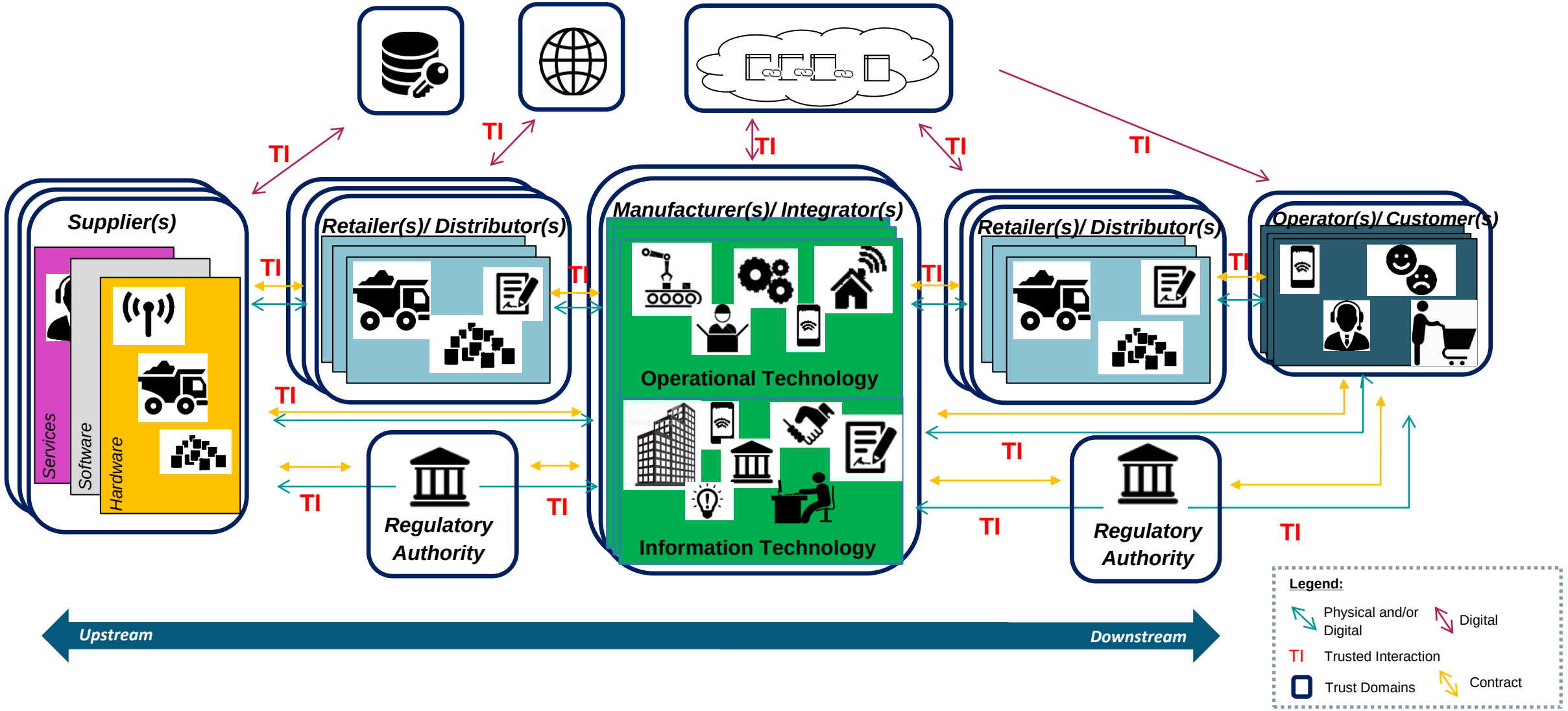
Organizational Trustworthiness

"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. "

Trustworthiness Concept for Organizational Trustworthiness



Means to Support Trusted Interactions

Secure Identities for Entities

- X.509 PKI Certificates
- DIDs/SSIs
- …

Persistent link between digital infromation and the corresponding physical entity

- Security ICs
- PUFs
- …

Proof of compliance to standards and regulations

- QCCs
- SCCs
- …

Standardized means to exchange TW capabilties

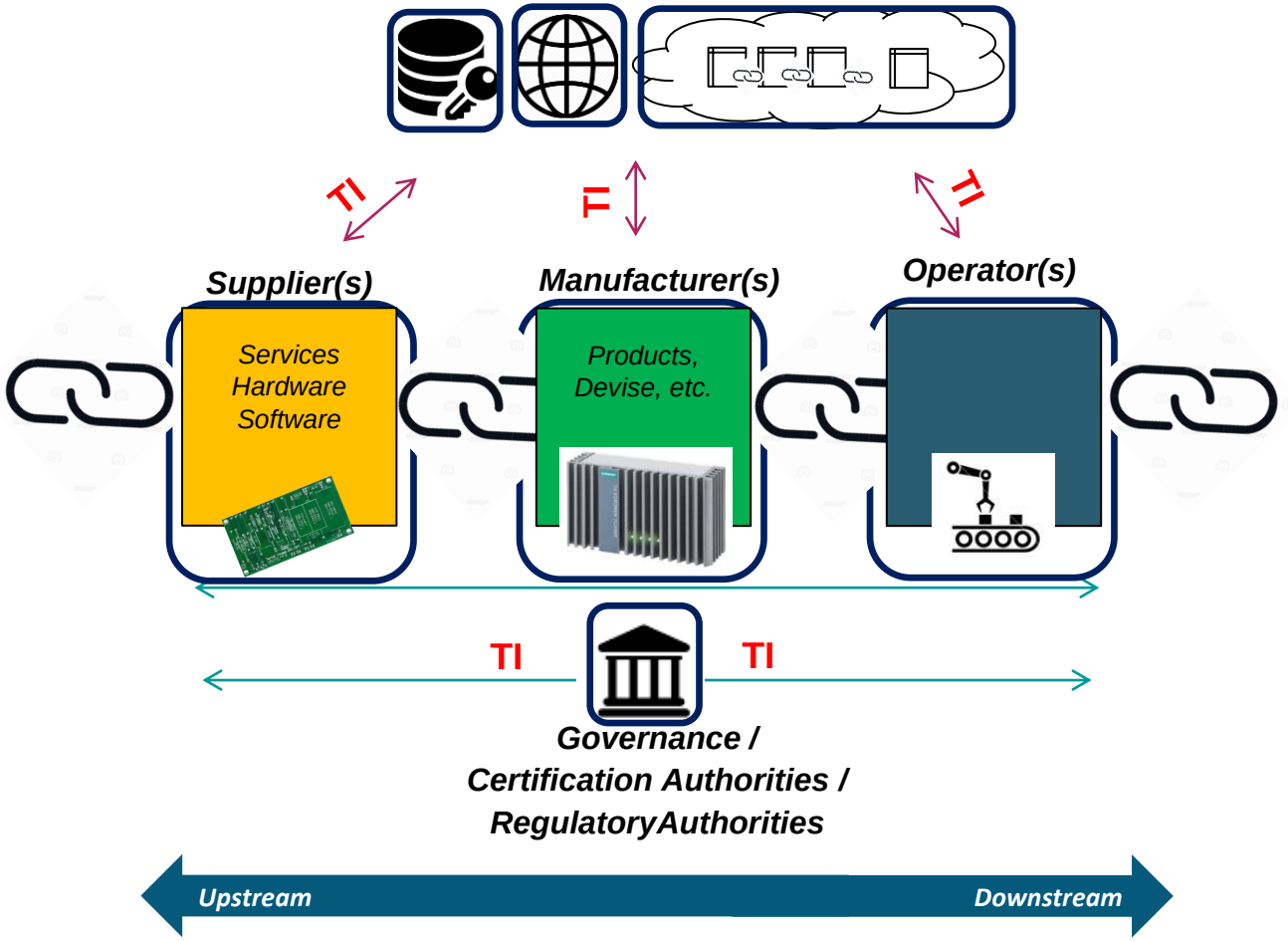
- TWP
- Extended TWP
- …

DID: Decentralized Identifier; SSI: Self Sovereign Identity; QCC: Quality Certifying Certificate; SCC: Security Certifying Certificate; TWP: Trustworthiness Profile

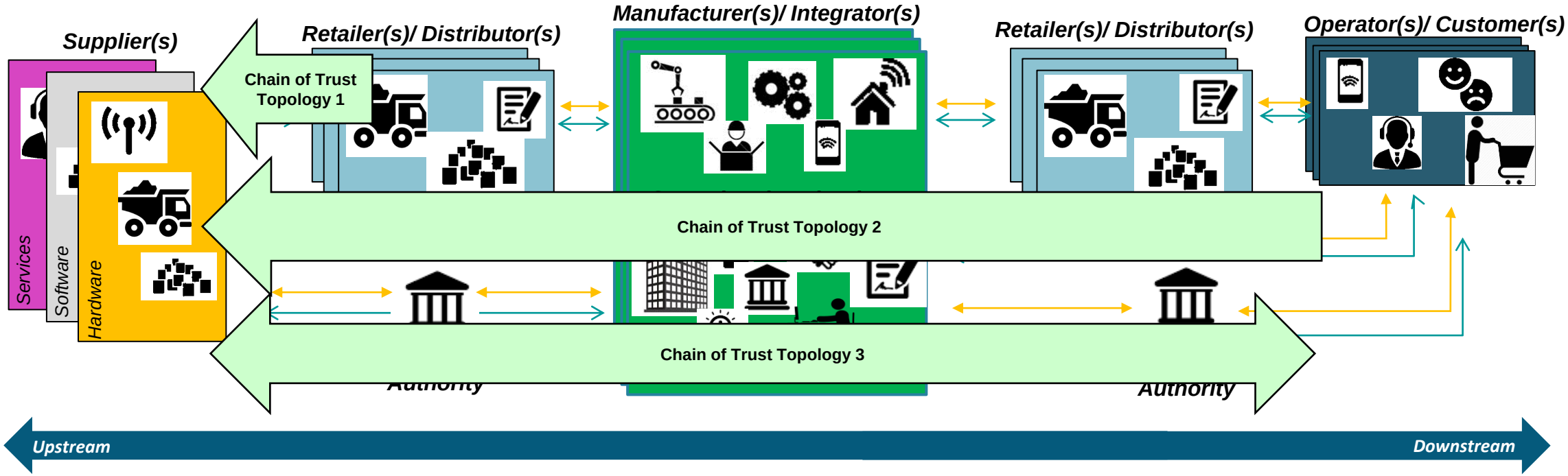
Trust Transitivity to Chain of Trust

Trust transitivity is when trust can be extended outside the two trust domains.

This leads to the concept of **“chain of trust"**, i,e., concatenate the trustworthiness of interactions between trust domains in a supply chain.



Chain of Trust Topologies



Chain of Trust Topology 2 - Extended Trustworthiness Profile

Trustworthiness Profile

To be filled by the Buyer

Buyer's Information

Contact Partner:
*Contact Partner's Unique Identifier:
Contact Information:
Legal Entity Name:
*Legal Entity Unique Identifier:
*Unique Identifier Scheme: *(e.g., link to LEI code repo, VATIN by DUNS, NTA by TSE, etc.)*
Country:
Additional Information:

Trustworthiness Expectations

		Additional Information	*Expected Validity*	*Supplier Conformance*	*Self*	*3rd party*
ISO/IEC 62443-4-2	Upload/Attach			☐	☐	☐
Please confirm if your supplier(s) complies to the above listed expectation ☐ Yes ☐ No						
NIST SP 800	Upload/Attach			☐	☐	☐
Please confirm if your supplier(s) complies to the above listed expectation ☐ Yes ☐ No						
PSS Supplier Questionnaire	Upload/Attach			☐	☐	☐
Please confirm if your supplier(s) complies to the above listed expectation ☐ Yes ☐ No						
Common Criteria	Upload/Attach			☐	☐	☐
Please confirm if your supplier(s) complies to the above listed expectation ☐ Yes ☐ No						

Reference Request-for-work | Time Stamp

Digital Signature | Digital Certificate (If required)

To be filled by the Supplier

Supplier's Information

Contact Partner:
*Contact Partner's Unique Identifier:
Contact Information:
Legal Entity Name:
*Legal Entity Unique Identifier:
*Unique Identifier Scheme: *(e.g., link to LEI code repo, VATIN by DUNS, NTA by TSE, etc.)*
Country:
Additional Information:

Trustworthiness Capabilities

			Proof/ Evidence	*Proof Expiry Date*	*Additional Information*
Conform: ☐	Self-Assessment ☐	3rd-Party Assessement ☐	Upload/Attach	DD.MM.YYYY	
	Supplier(s) Conform: ☐ Yes ☐ No		Upload/Attach	DD.MM.YYYY	
Conform: ☐	Self-Assessed ☐	3rd-Party Assessement ☐	Upload/Attach	DD.MM.YYYY	
	Supplier(s) Conform: ☐ Yes ☐ No		Upload/Attach	DD.MM.YYYY	
Conform: ☐	Self-Assessed ☐	3rd-Party Assessement ☐	Upload/Attach	DD.MM.YYYY	
	Supplier(s) Conform: ☐ Yes ☐ No		Upload/Attach	DD.MM.YYYY	
Conform: ☐	Self-Assessed ☐	3rd-Party Assessement ☐	Upload/Attach	DD.MM.YYYY	
	Supplier(s) Conform: ☐ Yes ☐ No		Upload/Attach	DD.MM.YYYY	

Reference TW Expectations | Quote/Bid Reference | Time Stamp

Digital Signature | Digital Certificate (If required)

IIoT Value Chain Security
- Chain of Trust for Organizations and Products -

Ayaji Furukawa

Robot Revolution & Industrial IoT Initiative, Japan

Toshiba Corporation

Aliza Maftun

German Platform Industry 4.0

Siemens AG

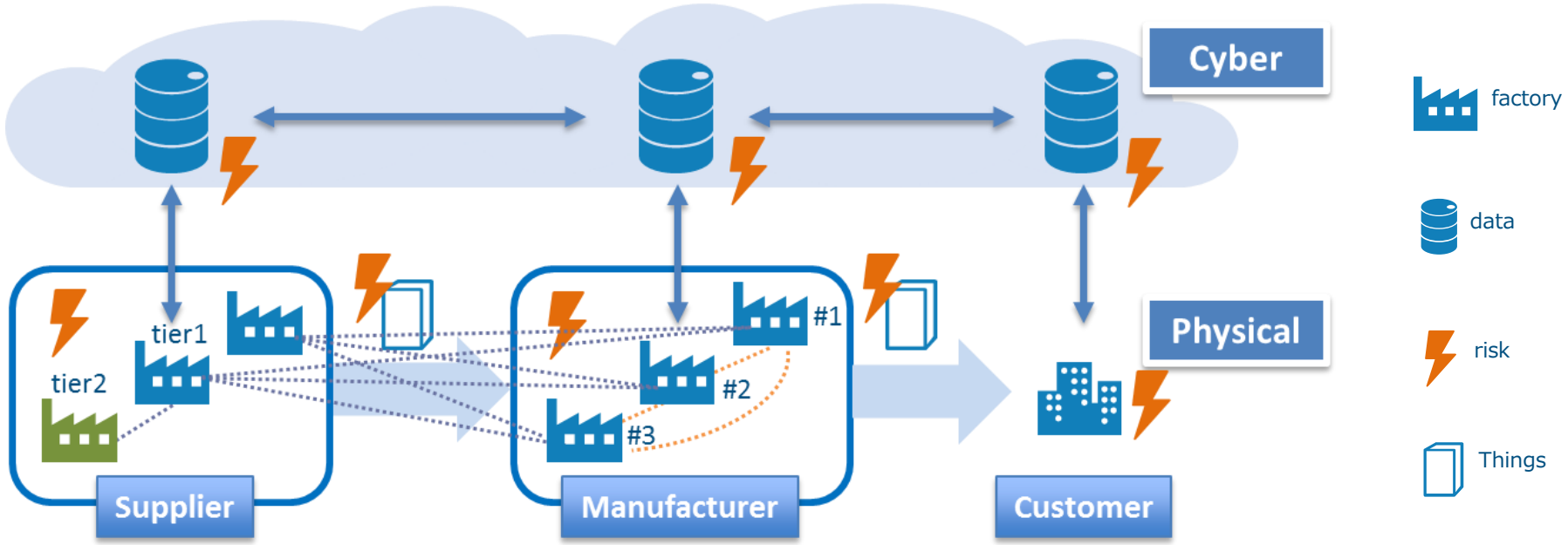
Agenda

- Trustworthiness Definition and structure
- Product Trustworthiness
- Trustworthiness Structure
- Relationships Between Organizations' and Products' Trustworthiness
- Moving Towards the Trustworthiness of Products
- Chain of Trust Topologies
- Future Work

Global Value Chain

Information security has become an essential aspect of **trustworthiness** because manufacturers and suppliers are becoming interdependent as parties in the global value chain accelerated through the Internet.

1) Need to develop products that satisfy rapidly changing customer needs.
2) Need to collaborate with suppliers whose products are required to develop the products.
3) Need to find appropriate suppliers from all over the world timely though the Internet.



Trustworthiness Definition and Structure

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

Organizational Trustworthiness

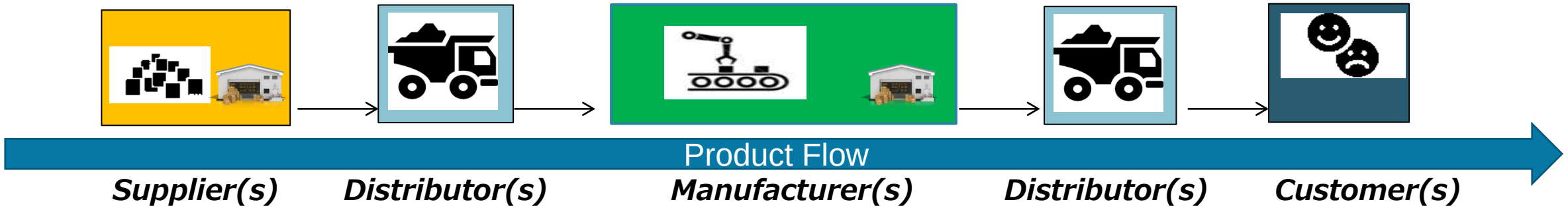
"Extent to which the declared attributes of an organization can be verified by the relying party and satisfies its expectations."

Product Trustworthiness

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

Product Trustworthiness - Motivation

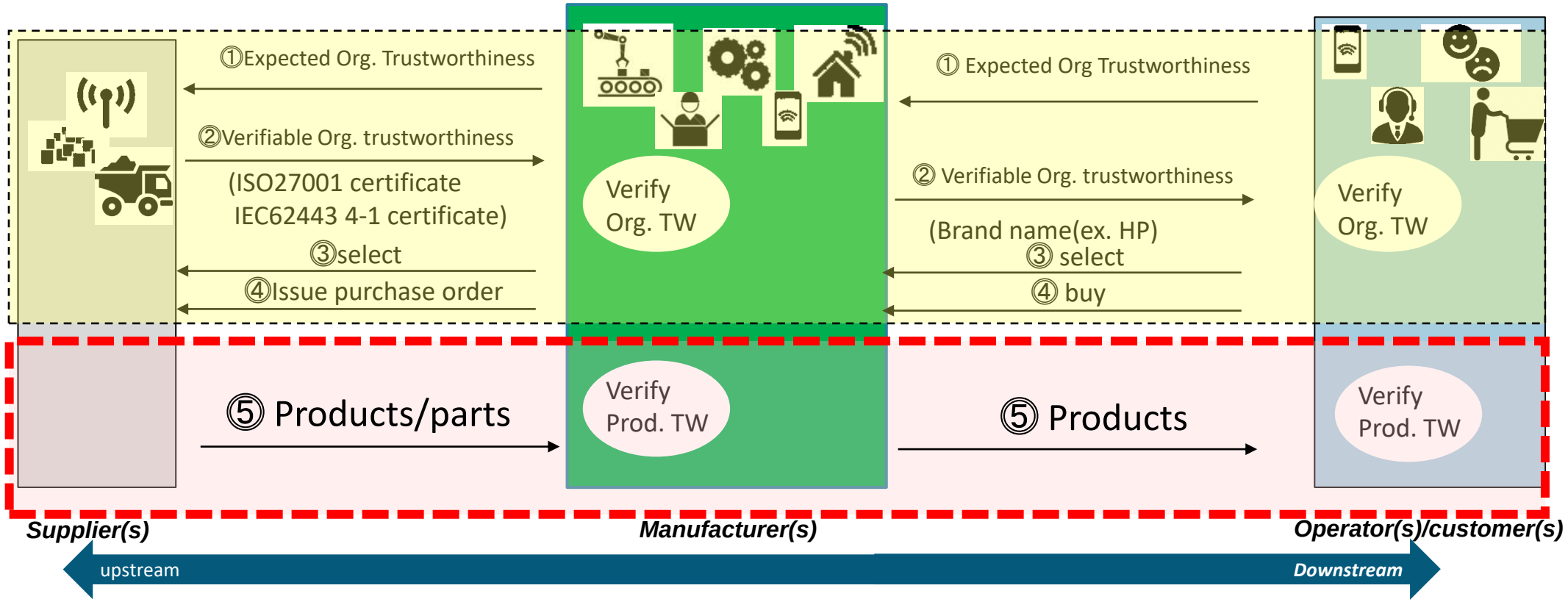
- Manufacturers would like to make sure that the Product is composed of genuine parts and/or malware free parts.
- Manufacturers want to verify the trustworthiness of the components before using them to manufacture its own products.
- Manufacturers want to provide confidence to its customer that its product are trustworthy, such as to fulfil social regulations, and compensate carbon footprint.



Trustworthiness Structure

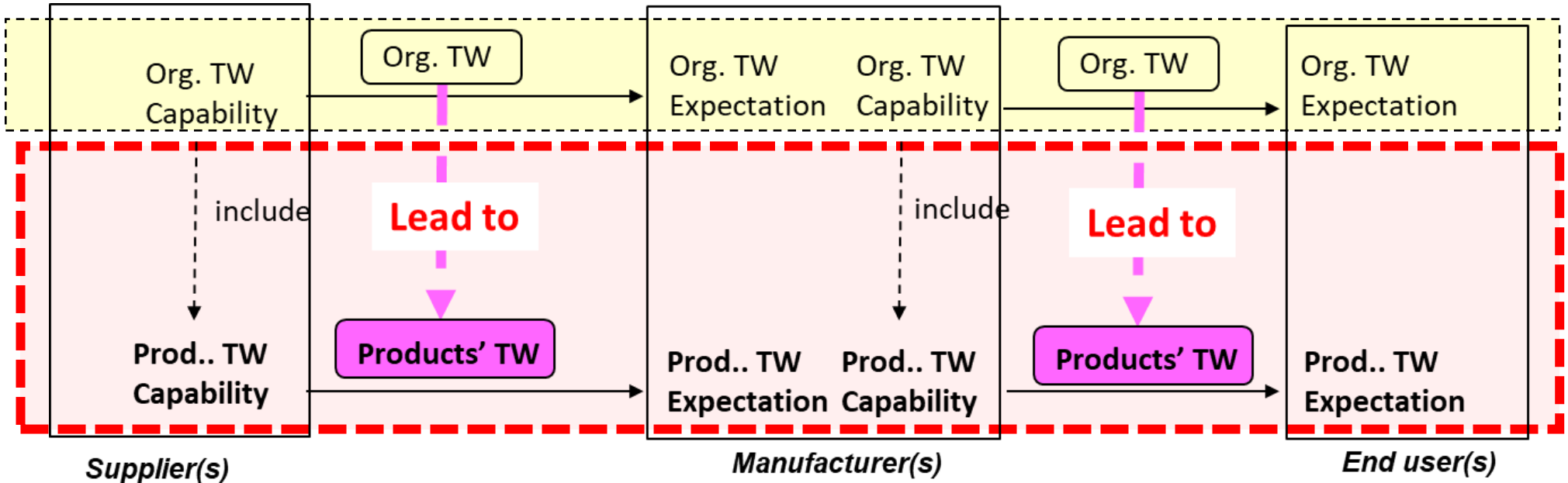
Abilities of supply chain actors describe Trustworthiness

1) Organization related abilities like governance and risk management
2) Product related abilities like providing product with competent quality, cost and delivery



Relationships Between Organizations' and Products' Trustworthiness

- Organizations' trustworthiness leads to Products' trustworthiness
- The structure of trustworthiness across a supply chain which consists of organizations' and products' Trustworthiness.
- Organizations' trustworthiness is used to select appropriate suppliers before 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.



Moving Towards the Trustworthiness of Products

- 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.

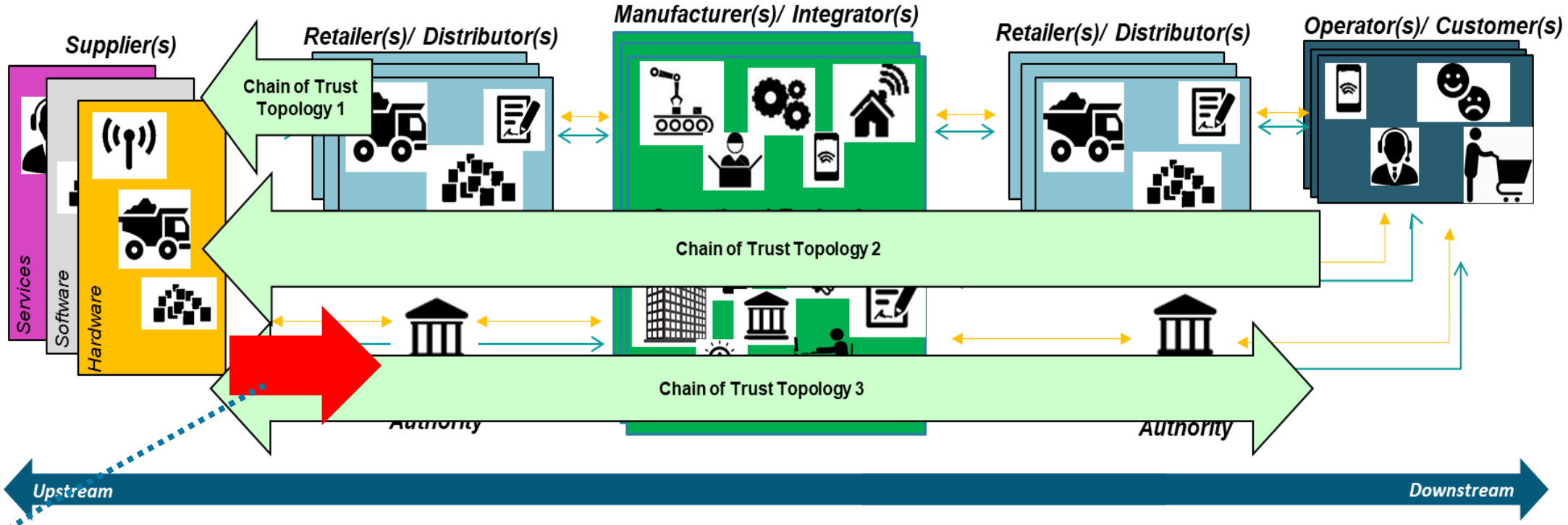
(4) Products can be demonstrated that no malware and contamination is included during de-sign and manufacturing processes.

(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.

Chain of Trust Topologies



- This implies bi-directional trust along 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

Future Work

- 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?

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

- Realization of Chain of Trust Topology 3_ We have to create a supply chain trustworthiness system which is not 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.

Thank you very much.

Ayaji Furukawa

ayaji2.furukawa@toshiba.co.jp

Aliza Maftun

aliza.maftun@siemens.com