The Germany-Japan Agreed Trustworthiness Communication Rule for Securing Supply Chains of Industrial IoT

27th May 2021

Robot Revolution & Industrial IoT Initiative (RRI)
Junya Fujita (R&D Group, Hitachi, ltd.)

Agenda

1. Introduction

2. The Germany-Japan Agreed Trustworthiness Communication Rule

3. Conclusion and Next Step

Agenda

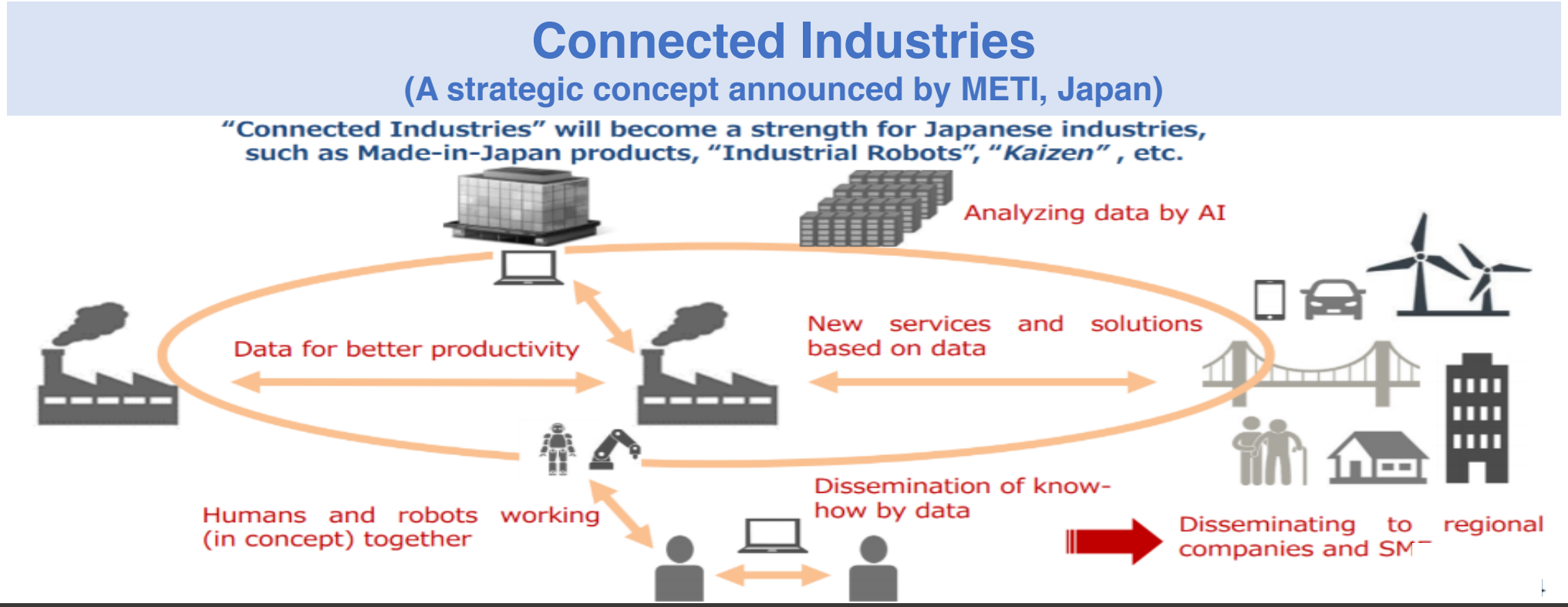
1. Introduction

2. The Germany-Japan Agreed Trustworthiness Communication Rule

3. Conclusion and Next Step

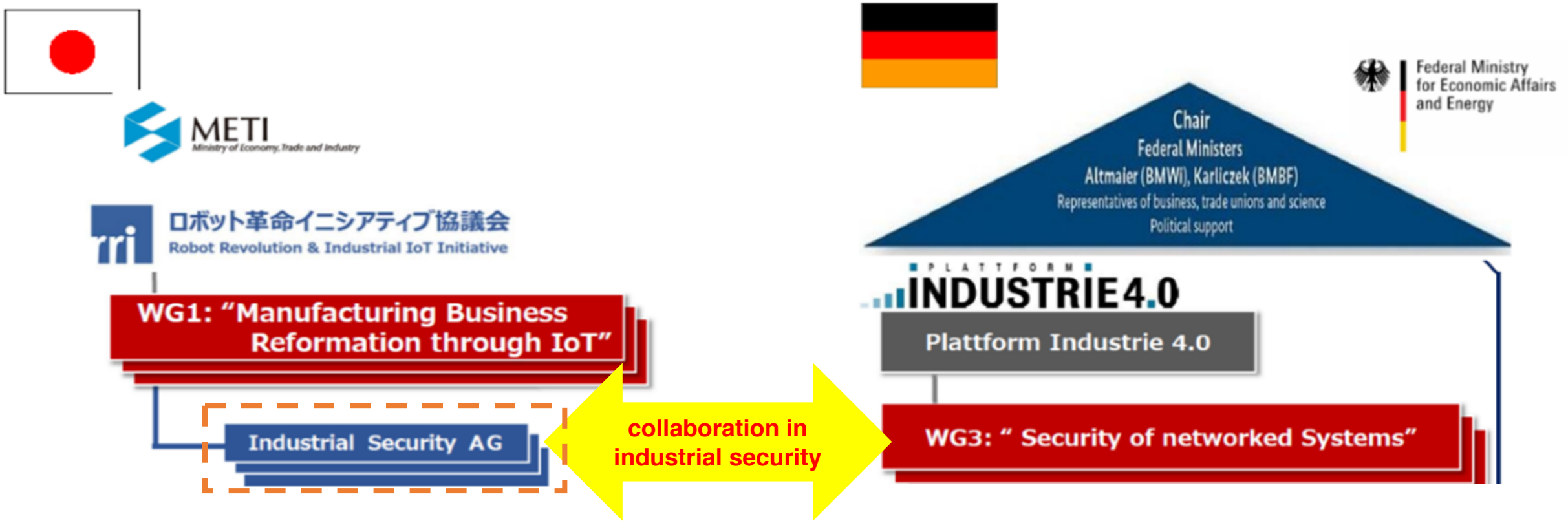
About RRI & Connected Industries

- The Robot Revolution and Industrial IoT Initiative (RRI) is a private-led organization platform to promote "Robot Revolution" based on Japanese government's strategy.
- Around 500 organizations in Japan are members of RRI.
- RRI promotes "Connected-Industries" in industrial fields such as manufacturing, logistics, facilities, constructions and so on



Germany-Japan Collaboration in Industrial Security

- Japan(RRI) and Germany (PI4.0: Plattform Industrie 4.0) concluded an agreement on enhancement of collaboration （In April 2016）
- "Industrial Security" is one of the areas to be focused



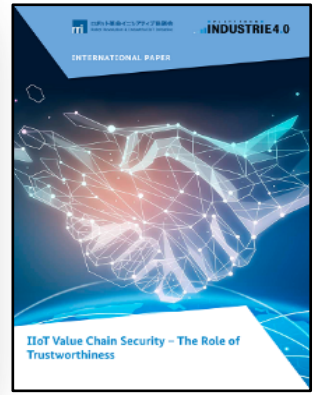
Our Past Activities

- The goal of our activities are:
  - ➢ To identify new security requirements for Industrie 4.0& Connected Industries and
  - ➢ To incorporate trustworthiness in upcoming interconnected economies

- PI4.0(Germany) & RRI(Japan) published a common position paper:
  "Facilitating International Cooperation for Secure Industrial Internet of Things/ Industrie 4.0"
  (The latest update is released in April 2019)
  https://www.jmfrri.gr.jp/english/document/library/1107.html

- PI4.0 and RRI had discussed the role of trustworthiness intensively in 2019 and released a whitepaper "IIoT Value Chain Security –The role of Trustworthiness" in September 2020

Today, some topics that PI4.0/RRI had discussed are introduced



(DE/EN) https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/IIoT_Value_Chain_Security.html
(JP) https://www.jmfrri.gr.jp/document/library/1652.html

Agenda

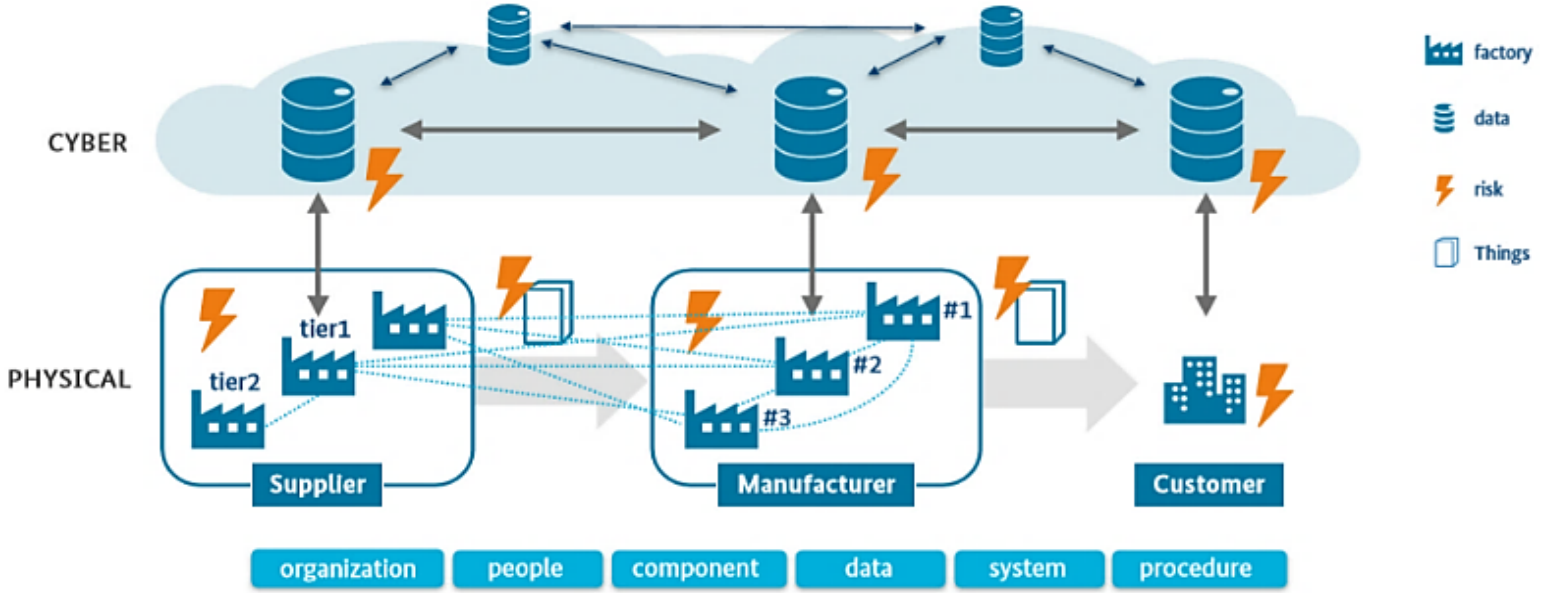
1. Introduction

2. The Germany-Japan Agreed Trustworthiness Communication Rule

3. Conclusion and Next Step

Background - Global Value Chain and Security Risks

- Global value chains accelerated by information and communication technologies require comprehensive "***trustworthiness* architectures**" covering all entities, regardless of their geographical location
- Product manufacturers need to:
  1) develop products that satisfy rapidly changing customer needs
  2) collaborate with other suppliers to develop their products securely
  3) find appropriate suppliers timely through the Internet



Reference: Whitepaper "IIOT Value Chain Security –The Role of Trustworthiness

The definition of "Trustworthiness" in the discussion

– In the context of our project, the definition of the term **"trustworthiness"** proposed by the ISO/IEC JTC1/WG13 has been adapted as:

> ***For supply value chain security and risk management, the term "Trustworthiness" corresponds to the supplier's ability to meet the expectations of the potential contract partner in a verifiable way***

– "Trustworthiness" is depended on use-cases in supply chains and products, different characteristics would be considered to fulfill stakeholder's expectations.

Ref: the whitepaper "IIOT Value Chain Security –The role of Trustworthiness" 2020

Online Procurement and Digital Agreement

- To achieve global value chains, online procurement & digital agreement are important
- Matters related to trustworthiness:

Online procurement

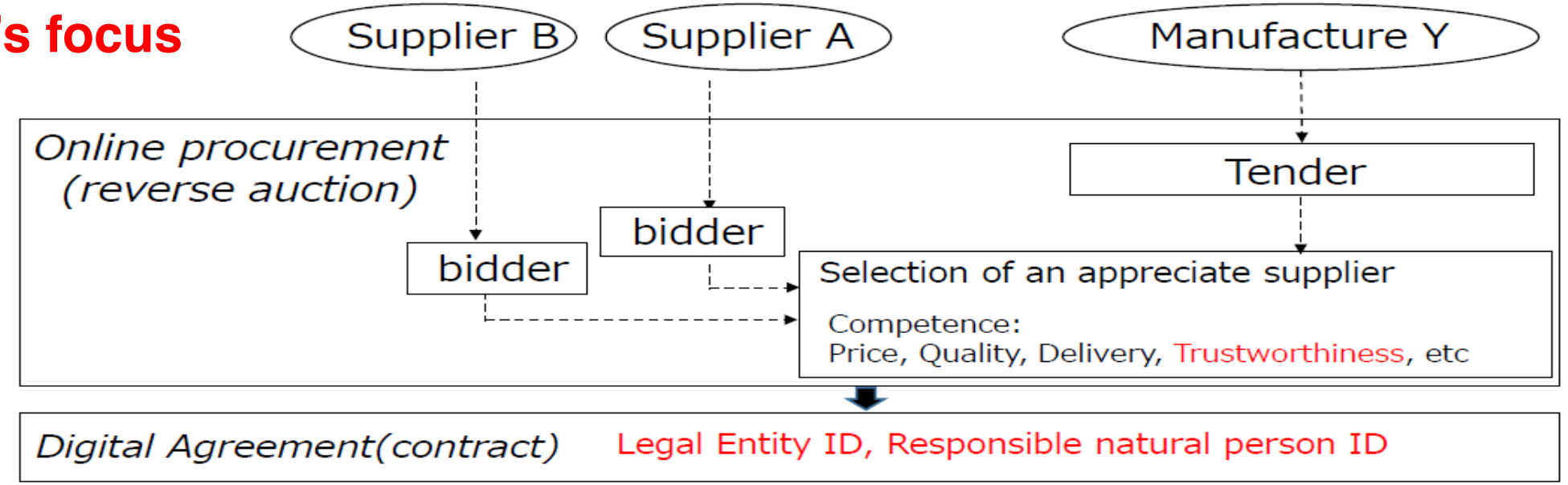
- Authenticity of parties
- Security level of their products
- Security level of their security activities

➡ **Exchange "Trustworthiness profile"**

Digital agreement

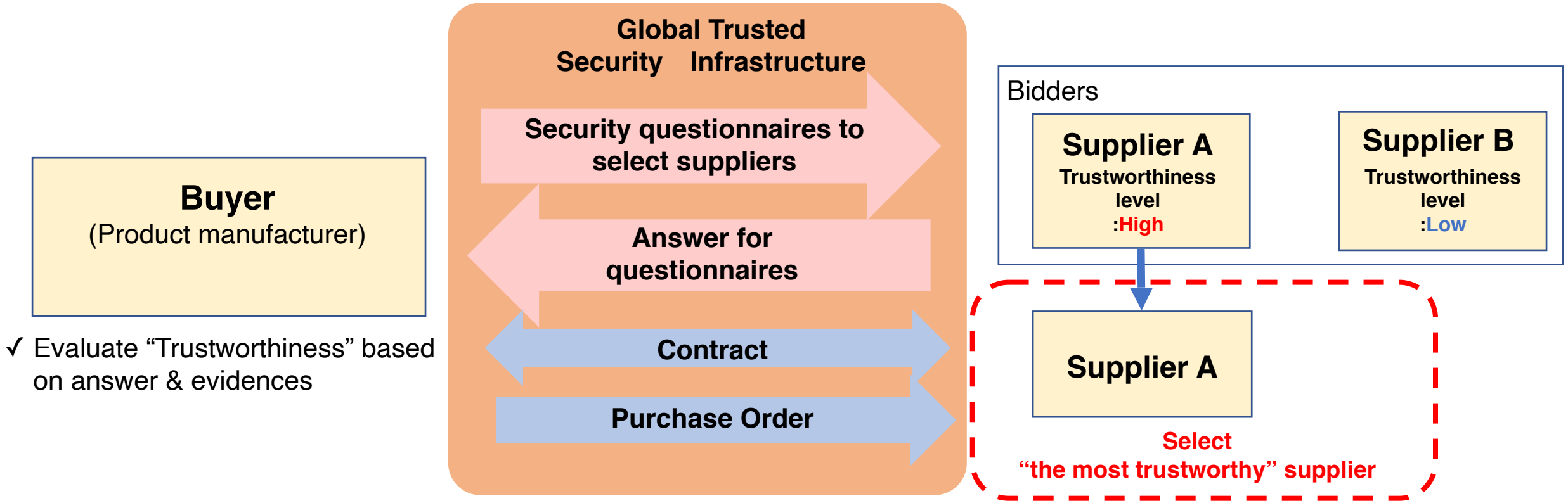
- Authenticity of the organization as a legal entity represented by a legal entity ID
- Authenticity of the signer as a responsible natural person represented by a natural person ID

Today's focus



Exchange Trustworthiness Information in online procurement

- In online procurement process, organizations exchange machine-readable "TWP(Trustworthiness Profile)" each other before contracting
- RRI and PI4.0 had discussed to plan the TWP in a demonstrator, which provides a digitalized trustworthy relationships between buyers and suppliers in global value chains



Our discussions topics for TWP

- To establish the security requirements(questionnaire) for TWP, referred major security standards

  (Examples security standard)

  ➢ ISO 27001 (Information Security Management System)
  ➢ IEC 62443 (Security Requirements for Industrial Automation Systems)
  ➢ VDA-ISA (Criteria for Supply Chain Security in automotive industry)
  ➢ NIST CSF and METI CPSF (Risk Management Processes for Organizations)

Acronyms
ISO: International Organization for Standardization
IEC: International Electrotechnical Commission
VDA: Verband der Automobilindustrie, Germany
ISA: Information Security Assessment
NIST: National Institute of Standards and Technology, USA
CPF: Cybersecurity Framework
METI Ministry of Economy, Trade and Industry, Japan
CPSF: Cyber-Physical Security Framework

- On the German (PI4.0) side, planned the design of an exchange protocol for TWP (TECEP: Trustworthiness Expectations and Capabilities Exchange Protocol)

- On the Japanese (RRI) side, planned a questionnaire for suppliers
  ➢ The questionnaire is based on security standards and requirements that have been achieved in Japanese industries
  ➢ The questionnaire consists of 25 items to evaluate security controls in operation, management processes and organization
  ➢ The questionnaire provides evidences and criteria of maturity levels on each requirement

JP https://www.jmfrri.gr.jp/document/library/1890.html
EN https://www.jmfrri.gr.jp/english/document/library/1892.html

An Example of Items in Questionnaire

Category			Governance
Security requirement			Develop and announce security policies, define roles and responsibilities for security across the organization and other relevant parties (Suppliers) .
Example: Answer	evidence		History of security policy development and approval, and approval of revisions to the security policy. Describe the security roles and responsibilities of the organization and other relevant organizations (e.g., contractors), and any arrangements for security with contractors in the security policy.
	Maturity level	1	The security officer of the organization has developed (documented) a security policy.
			▫Implemented ☐Planned to be implemented ☐Not applicable
		2	The organization's Chief information security officer has approved and implemented the security policy. The organization manages and implements the approved documents.
			▫Implemented ☐Planned to be implemented ☐Not applicable
		3	The organization's security officer and chief information security officer regularly review, update, and maintain security policies.
			▫Implemented ☐Planned to be implemented ☐Not applicable

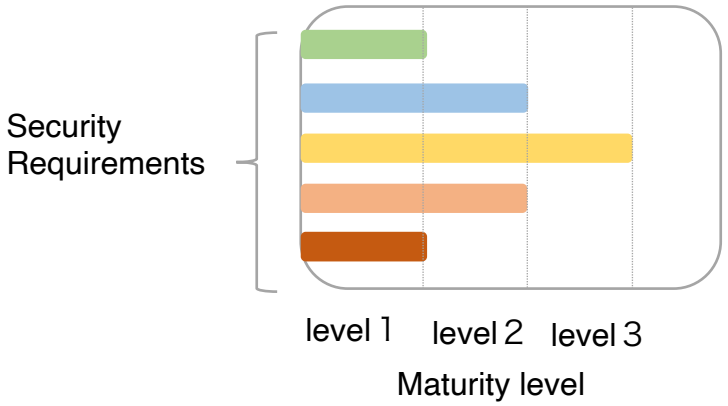
Use case of the questionnaire for TWP Evaluation

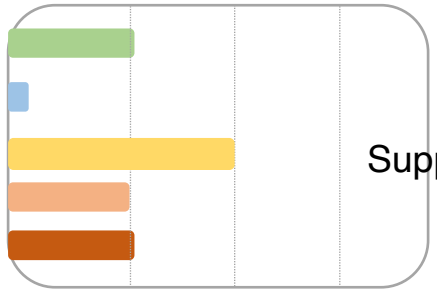
Supplier

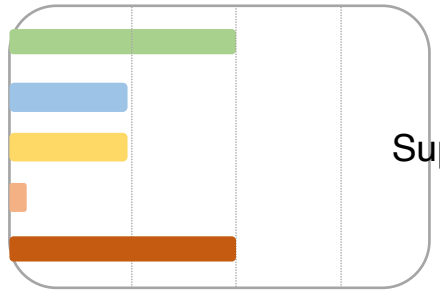
Answer from supplier=Supplier's capability of TWP

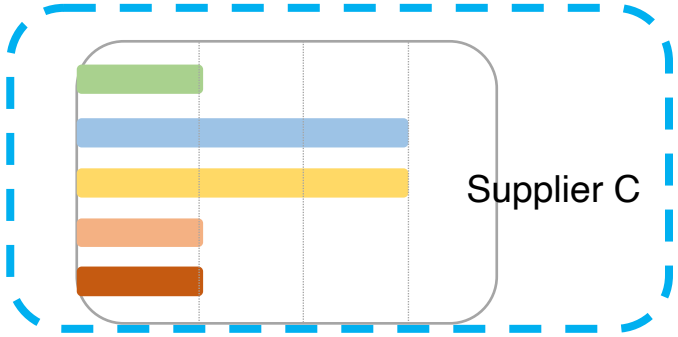
Buyer

Expected level for TWP = requirement

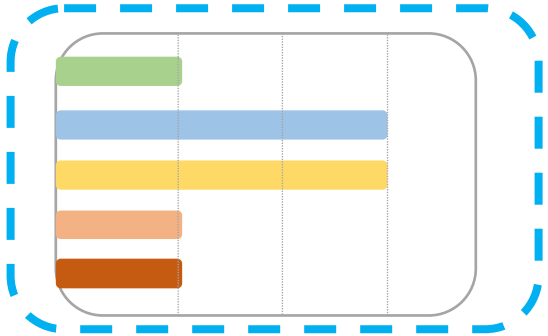








Selected supplier



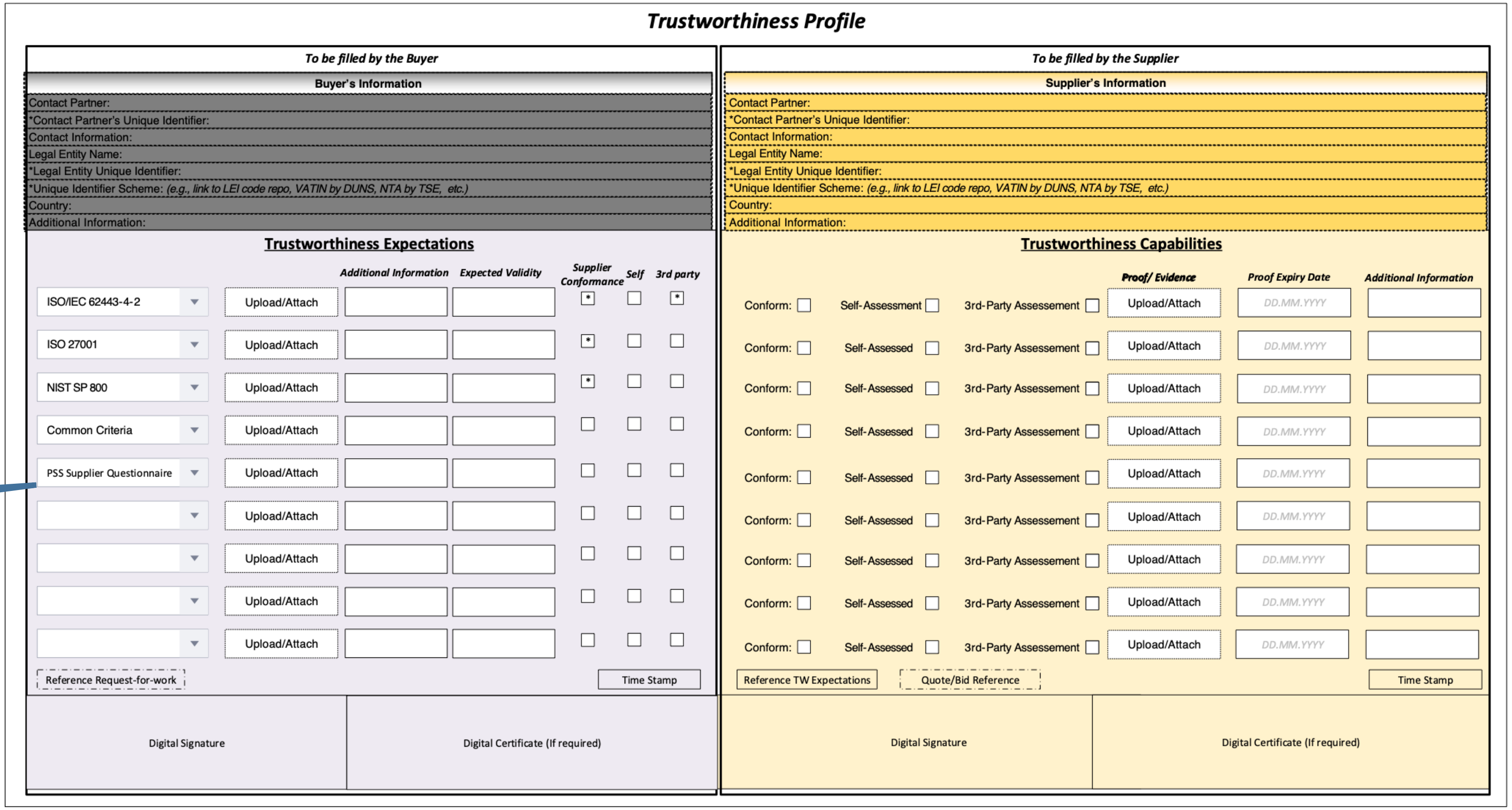
Supplier C

Collaboration activities between RRI and PI4.0

- On German side, a R&D project that develops TWP demonstrator has been running

(Ref.) https://legaltestbed.org/en/trust-demonstrator/

- The questionnaire would be incorporated into the demonstrator



RRI's questionnaires for suppliers would be incorporated

Reference: Whitepaper "IIoT Value Chain Security –The role of Trustworthiness.

Agenda

1. Introduction

2. The Germany-Japan Agreed Trustworthiness Communication Rule

3. **Conclusion and Next Step**

Conclusion and Next Step

- Japan(RRI) and Germany (PI4.0) are collaborating to establish a trustworthiness architecture for the next-generation industries

- RRI had planed a security questionnaires for suppliers to evaluate a trustworthiness profile (TWP) through the collaboration

- RRI expects the questionnaire and the answer for the questionnaire would be standardized, would be used digitally for online contracts

- **RRI and PI4.0 continue to discuss security issues in global value chains and continue to announce the result to the world continuously**

Thank you!

junya.fujita.so@hitachi.com