Security for Industrial IoT
- The Role of Trustworthiness -

14th Oct. 2020

Robot Revolution & Industrial IoT Initiative(RRI)

AYAJI furukawa (Toshiba Corporation)

Agenda

- **RRI(Japan) & PI4(Germany) collaboration, The goal of our activity**

- **White Paper (IIOT Value Chain Security –The Role of Trustworthiness) 2020**

- **Security questionnaires for suppliers**

- **Next Step**

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

- PI4.0(Germany) & RRI(Japan) announced three common position papers
"Facilitating International Co-operation for Secure Industrial Internet of Things/ Industrie4.0"
    (16th March 2017, 16th May 2018, 3rd April, 2019)

PI4.0: Plattform Industrie4.0, RRI: Robot Revolution & Industrial IoT Initiative

– PI4.0 and RRI had discussed the role of trustworthiness intensively during FY19 and have provided the whitepaper **"IIOT Value Chain Security –The role of Trustworthiness" 2020**

– *In the future, collaboration activities between RRI and PI4.0 plan to realize the TWP(Trustworthiness Profile) in a demonstrator, which would provide a standardized basis for establishing digitalized trustworthy relationships between buyers and suppliers.*
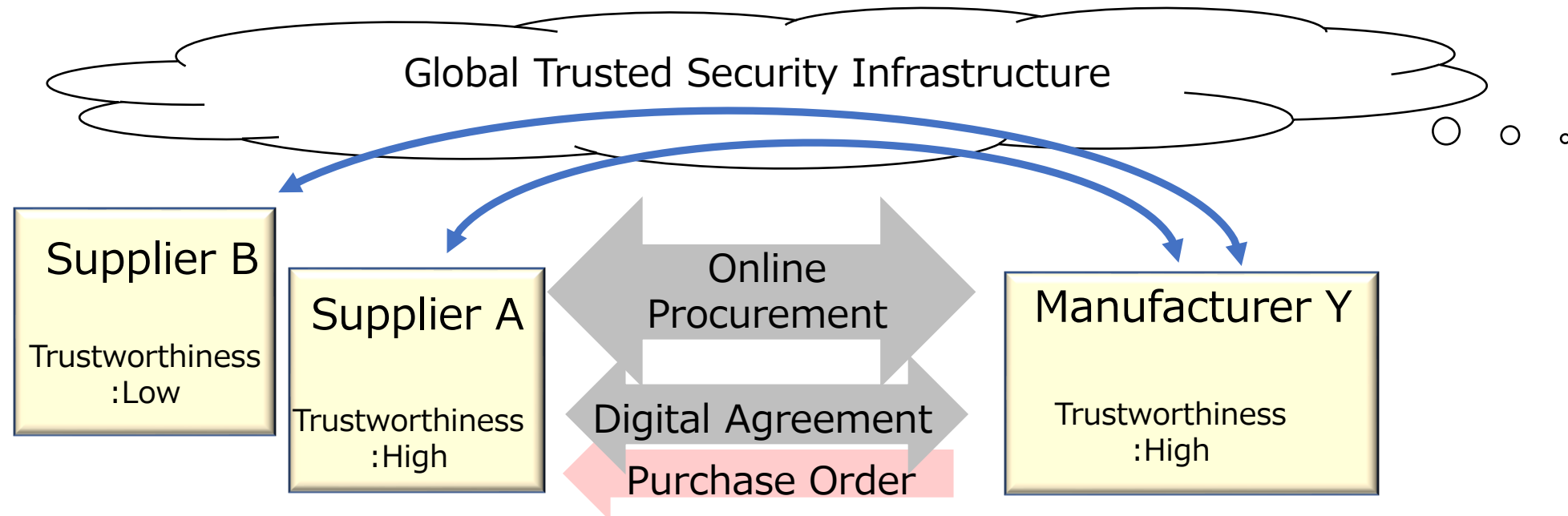
– On the Japanese side, establish a "Security questionnaires for suppliers"

- Global value networks require comprehensive trustworthiness architectures covering all entities, regardless of their geographical location.

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

Reference: Whitepaper "IIOT Value Chain Security –The Role of Trustworthiness
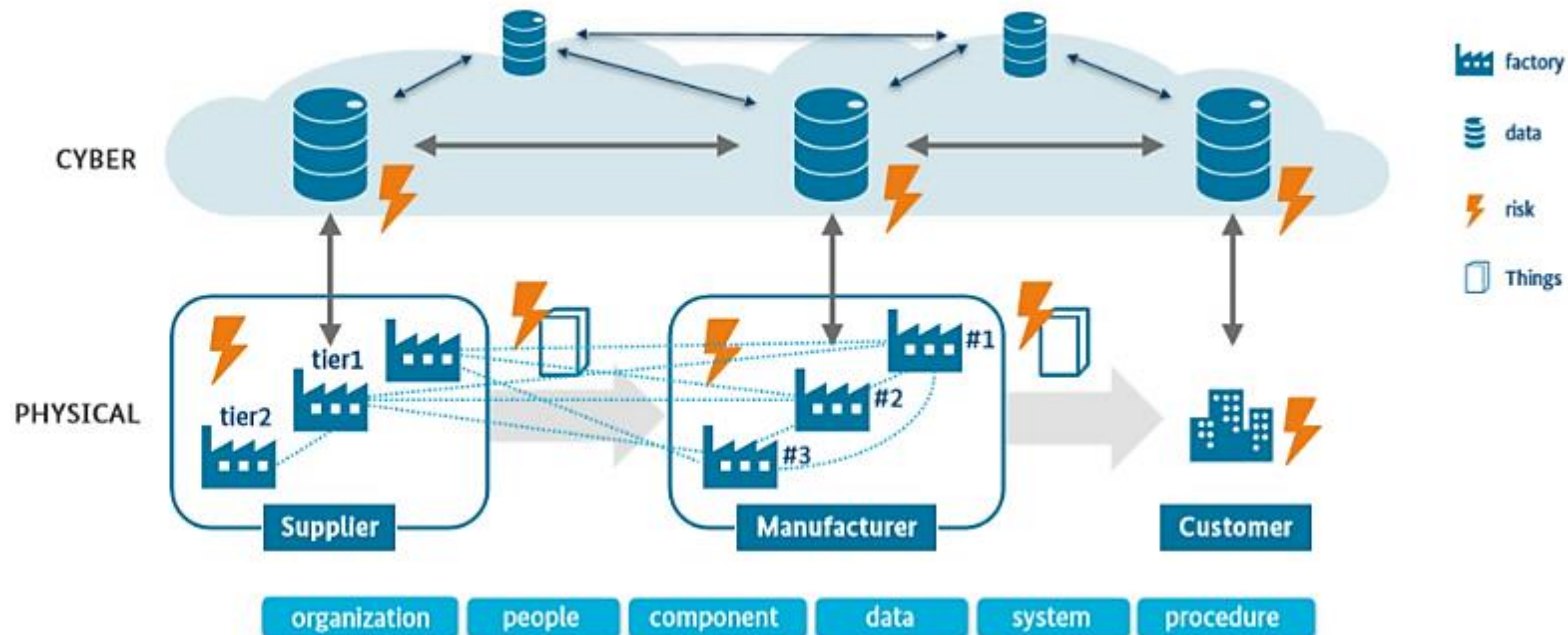
- A template for security in the supply chain as baseline
- "Requirement" in the supply chain between the manufacturer and the supplier
- The answer for the questionnaire would be useful for the Manufacturer to determine "the supplier's trustworthiness" and "how supplier's in the value chain have the same trustworthiness level"

Global Trusted Security Infrastructure

Supplier B

Trustworthiness :Low

Supplier A

Trustworthiness :High

Online Procurement

Digital Agreement

Purchase Order

Manufacturer Y

Trustworthiness :High

The total number of requirements in CPSF are 104

NIST/CSF	METI/CPSF	
Identity	CPS.AM	ID.AM (Asset Management)
	CPS.BE	ID.BE (Business Environment)
	CPS.GV	ID.GV (Governance)
	CPS.RA	ID.RA (Risk Assessment)
	CPS.RM	ID.RM (Risk Management Strategy)
	CPS.SC	ID.SC (Supply Chain Risk Management)
Protect	CPS.AC	PR.AC (Identity Management and Access Control)
	CPS.AT	PR.AT (Awareness and Training)
	CPS.DS	PR.DS (Data Security)
	CPS.IP	PR.IP (Information Protection Processes and Procedures)
	CPS.MA	PR.MA (Maintenance)
	CPS.PT	PR.PT (Protective Technology)
Detect	CPS.AE	DE.AE (Anomalies and Events)
	CPS.CM	DE.CM (Security Continuous Monitoring)
	CPS.DP	DE.DP (Detection Processes)
Respond/ Recovery	CPS.RP	RS.RP (Response Planning) RC.RP (Recovery Planning)
	CPS.CO	RS.CO (Communications) RC.CO (Communications)
	CPS.AN	RS.AN (Analysis)
	CPS.MI	RS.MI (Mitigation)
	CPS.IM	RS.IM (Improvements) RC.IM (Improvements)
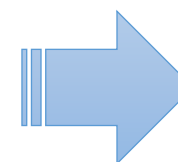
15 items

*CPSF:Cyber/Physical Security Framework (CPSF)
https://www.meti.go.jp/english/press/2019/0418_001.html 6

Ⅰ．Why we had chosen METI CPSF (Cyber Physical Security Framework) as baseline:

- CPSF provides cybersecurity requirements focused on communications between companies and/or organizations categorized as 3 levels,
- The 1st layer ,The 2nd layer, The 3rd layer and six elements (organization, people, component, data, procedure and system).

- CPSF provides informative references of other standards (e.g. NIST CSF and IEC 62443) on each requirement and this information supports our tasks.

- CPSF is enterprise-wide security framework and security requirements are described for each entity in a company.
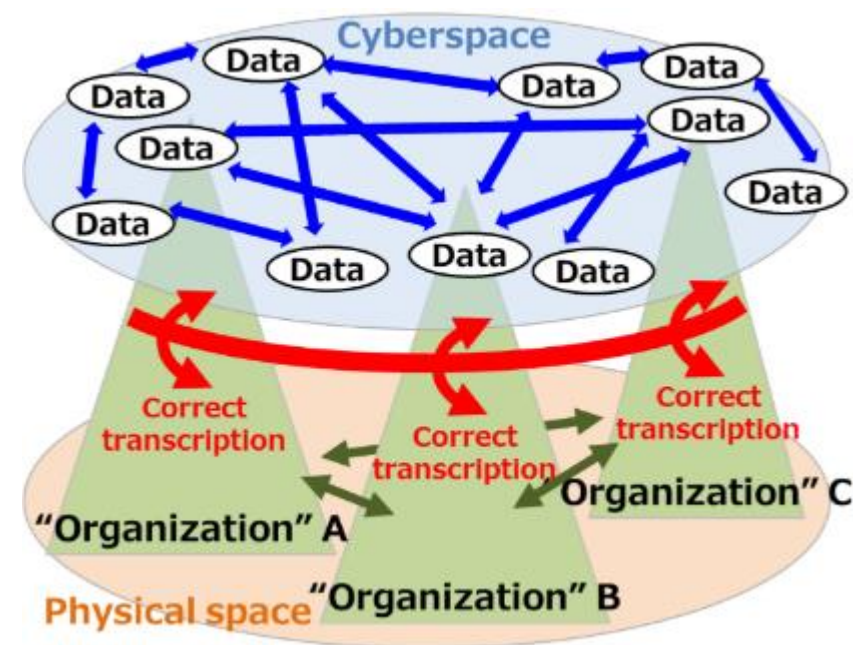
The 1st layer (Connections between organizations in physical space)
The 2nd layer (Mutual connections between cyberspace and physical space)
The 3rd layer (Connections in cyberspace)

II. How we had prioritized requirements and selected 15 requirements is:

- Security requirements that we have already achieved in our companies.

- Security requirements that we require for product/system suppliers at least.

- Security controls in operation and management processes or procedures.
(Technical security controls are out of scope because they depend on products)

- High(Policy)-level security requirements in the security risk management process.

Identify	CPS.AM-1 (Asset Management)	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.
	CPS.GV-1 (Governance)	Develop security policies, define roles and responsibilities for security across the organization and other relevant parties, and clarify the information-sharing method among stakeholders.
	CPS.RA-1 (Risk Assessment)	Identify the vulnerability of the organization's assets and document the list of identified vulnerability with the corresponding asset.
	CPS.RM-1 (Risk Management Strategy)	Confirm the implementation status of the organization's' cyber security risk management and communicate the results to appropriate parties within the organization (e.g. senior management). Define the scope of responsibilities of the organization and the relevant parties (e.g. subcontractor), and establish and implement the process to confirm the implementation status of security risk management of relevant parties.
	CPS.SC-1 (Supply Chan Risk Management)	Formulate the standard of security measures relevant to the supply chain in consideration of the business life cycle, and agree on contents with the business partners after clarifying the scope of the responsibilities.

*CPSF description(need to revise as questionnaire description)   https://www.meti.go.jp/english/press/2019/pdf/0418_001b.pdf

Protect	CPS.AC-1 **(Identify Management & Access Control)**	Establish and implement procedures to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.
	CPS.AT-1 **(Awareness &Training)**	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.
	CPS.DS-1 **(Data Security)**	If the organization exchanges protected information with other organizations, agree in advance on security requirements for protection of such information.
	CPS.IP-1 **(Information Protection Process & Procedures)**	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.
	CPS.IP-9 **(Information Protection Process & Procedures)**	Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.
	CPS.MA-1 **(Maintenance)**	Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updates with managed tools properly and in a timely manner while recording the history. Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands, where applicable.

Detect	CPS.AE-1 **(Anomalies & Events)**	Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.
	CPS.CM-1 **(Security Continuous Monitoring)**	Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.
	CPS.DP-1 **(Detection Process)**	Clarify the role and responsibility of the organization as well as service providers in detecting security events so that they can fulfill their accountabilities.
Respond / Recover	CPS.RP-1 **(Response Planning)** **(Recovery Planning)**	Develop and implement previously the procedure of response after detecting incidents (security operation process) that includes the response of Organization, People, Components, System to identify the content of response, priority, and scope of response taken after an incident occurs.
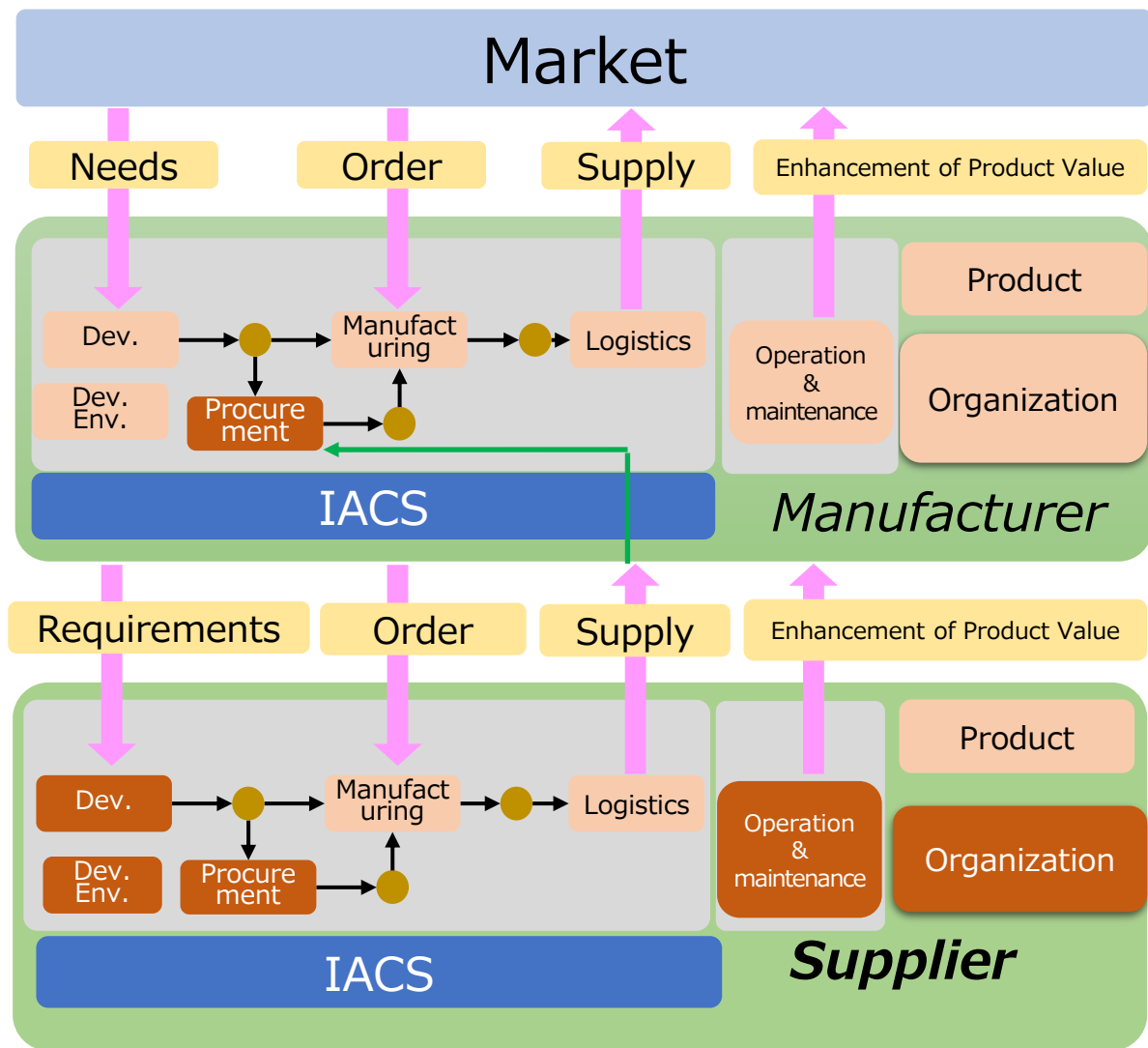
I. **We added additional requirements**
-development,
-development environment,
-procurement,
-Operation & maintenance(O&M)
from the view point of product life cycle.
e.g.) IEC 62443 2-1,2-4,4-1

II. **How we had selected additional requirements is**
-already implemented by us
-appropriate to request the requirements to suppliers
-not technical but managing/operational
-not too specific but moderately general

*IACS(Industrial Automation and Control System)
*Dev.(Development)
*Env.(Environment)

Selected category for questionnaire

Category	(5) Manufacturing site security - 1	
Security requirement	Have you created a list of the hardware and software that make up the system and its management information? And is it properly managed?	
evidence	1)Including, but not limited to, an electronic or written list of assets, 2)including asset names, versions, network addresses, administrative responsibility, licensing information, and locations; operational policies, 3)including transportable media; asset bail line configuration and audit rules; automatic asset discovery and removal mechanisms; and more.	
Example : Answer **Maturity level**	1	Assets are identified, listed and prioritized according to their priority. ☐Implemented ☐Planned to be implemented ☐Not applicable
	2	Maintain the asset list by regularly reviewing and updating it. Control and limit the use of portable media. Prohibit the removal of highly sensitive data. ☐Implemented ☐Planned to be implemented ☐Not applicable
	3	The asset list is updated in real time. Regular audits for compliance with the organization's defined baseline structure. A mechanism is in place and operational to automatically detect and remove unauthorized assets. ☐Implemented ☐Planned to be implemented ☐Not applicable

13

◆ In the future, collaboration activities between RRI and PI4.0 plan to realize the TWP in a demonstrator, which would provide a standardized basis for establishing digitalized trustworthy relationships between buyers and suppliers.

RRI Security questionnaires for suppliers would be incorporated

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

Next Step

- RRI is developing security questionnaires for suppliers in FY2020 based on Cyber/Physical Security Framework issued by METI, Japan.

- RRI expects the questionnaire would be standardized and the answer for the questionnaire would be evaluated and digitally signed by 3rd party security certification bodies.

Thank you very much!

ayaji2.furukawa@toshiba.co.jp