The Role of Trustworthiness in secure supply chain for connected industries

27th Jan. 2021

Robot Revolution & Industrial IoT Initiative(RRI)
AYAJI Furukawa (Toshiba Corporation)

Agenda

1. Introduction
- RRI and Connected Industries
- RRI and PI4.0's collaboration for Industrial Security
- Past activities

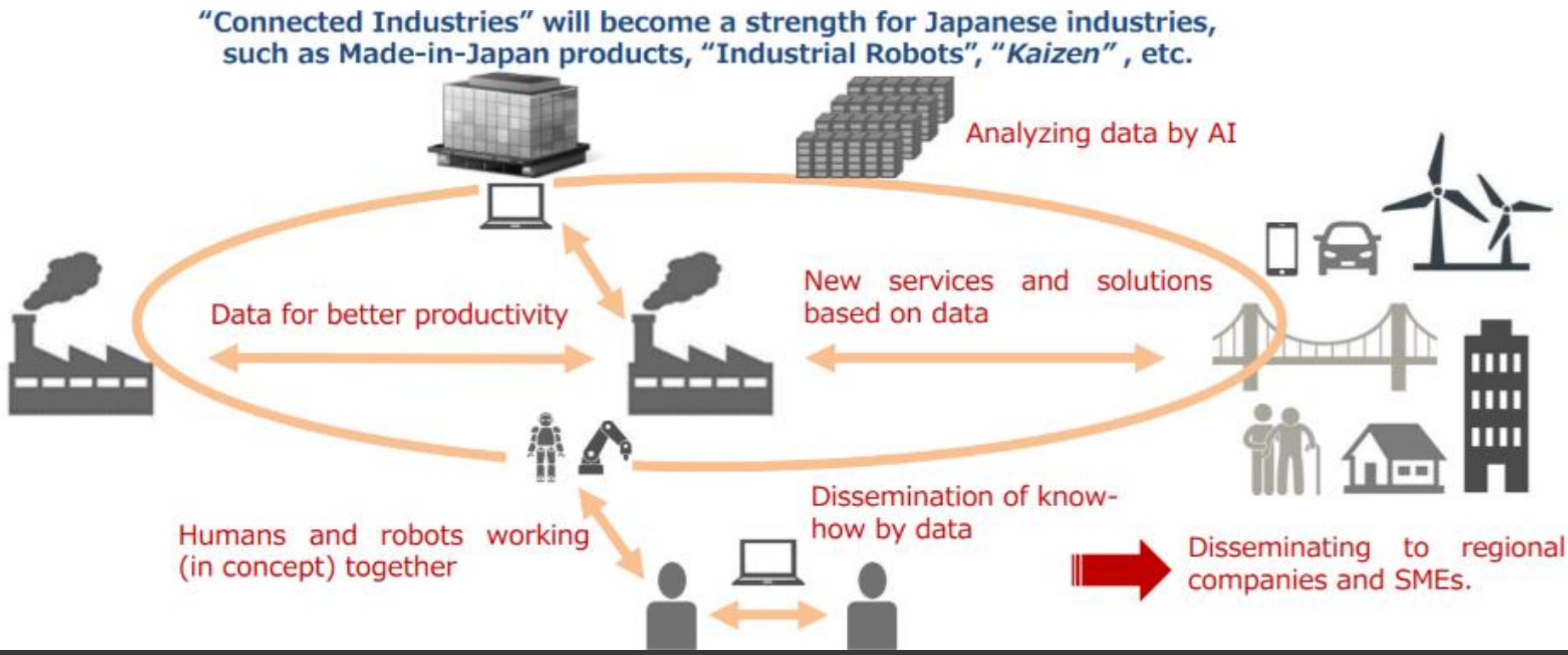
2. Security questionnaires for suppliers
- Background
- Scope & use case
- Maturity level
- Selected requirements
- Questionnaire in-practice- Example

3. Next Step

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 companies (mainly manufacturing industry) are members of RRI.
- RRI promotes "Connected-Industries" in the field of manufacturing.

Connected Industries



RRI and PI4.0's collaboration for Industrial Security

- the RRI of Japan and the PI4.0, Germany, concluded an agreement on enhancement of collaboration（2016.4）
- Industrial cyber security is one of the areas for our collaboration to create synergy.

Our past activities

- 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

White paper
(IIoT Value Chain Security -The Role of Trustworthiness)

- 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**

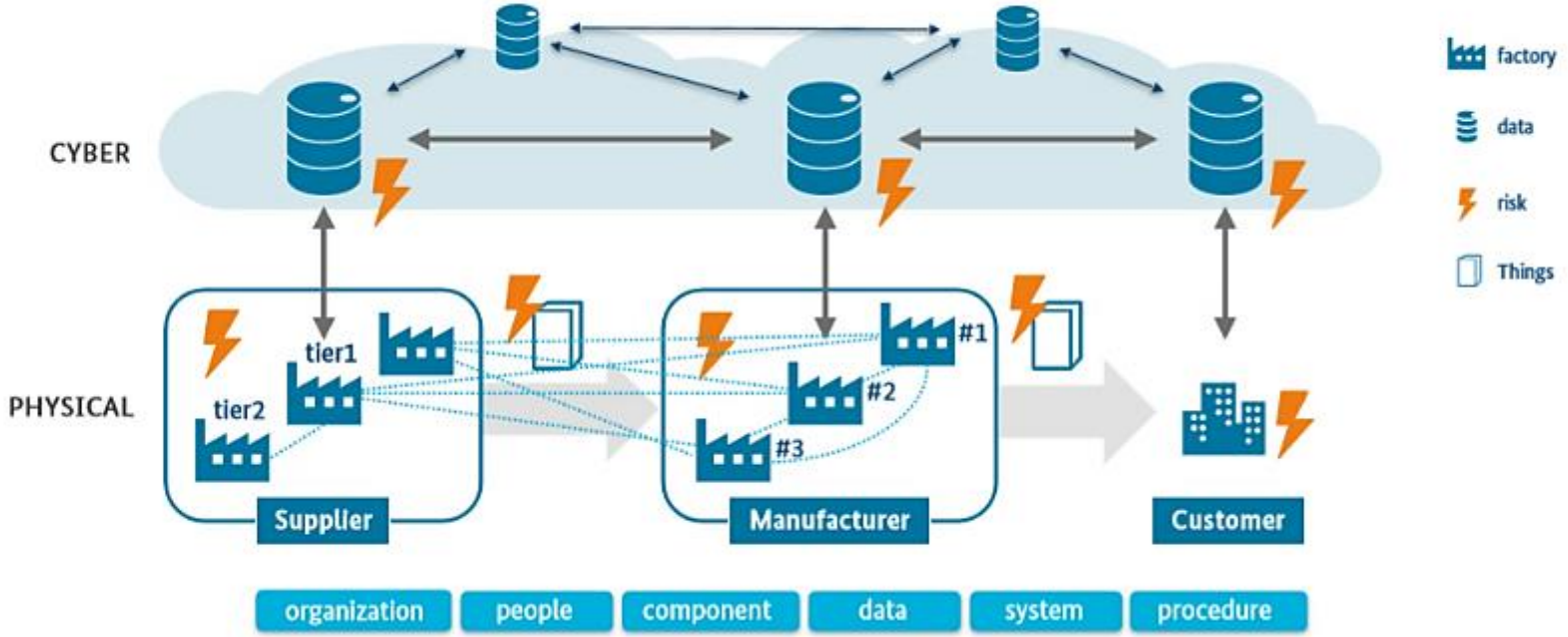
- *In the future, collaboration activities between RRI and PI4.0 plan to realize the TWP(Trustworthiness Profile) in a demonstrator, which would provide a standardized basis for establishing digitalized trustworthy relationships between buyers and suppliers.*

- On the Japanese side,
  establish a "Security questionnaires for suppliers"

Background
~Risks in Connected Industries~

- 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

Trustworthiness

- 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".

- Depending on the ues-case and on the specific product, different characteristics would apply to fulfill stakeholder's expectations.

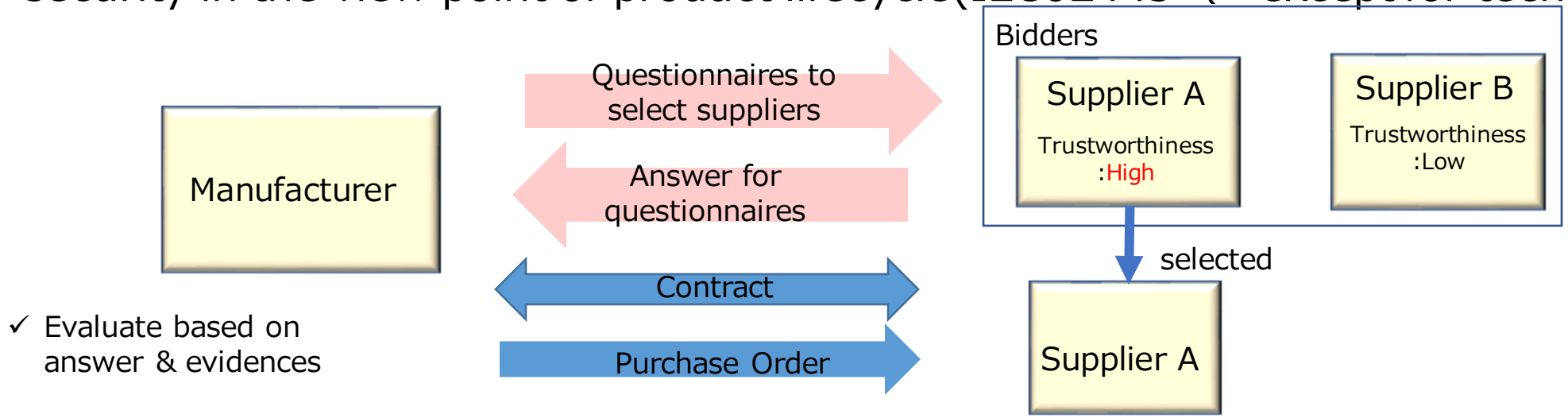
Ref: the whitepaper "IIOT Value Chain Security –The role of Trustworthiness" 2020

Scope & Use case ~Security questionnaires for suppliers~

- A template for security requirements in the supply chain as baseline to select supplier before contract, being applied across sectors of manufacturing industry.

(Any specific regulation (Electricity, automobile, defense etc.) follows these rules)

- Questioner: Procurement department for manufacturer
- Answerer: Bidder for development department
- The answer for the questionnaires 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"
- Focus on Organization security（METI/CPSF, NIST/CSF,ISMS）and industrial control system security in the view point of product lifecycle(IEC62443（＊except for technical requirements)



✓ Evaluate based on answer & evidences

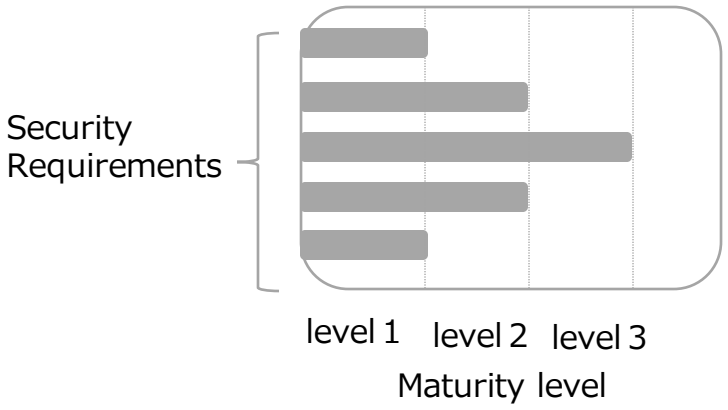
Use case of profile (Answer of questionnaire)

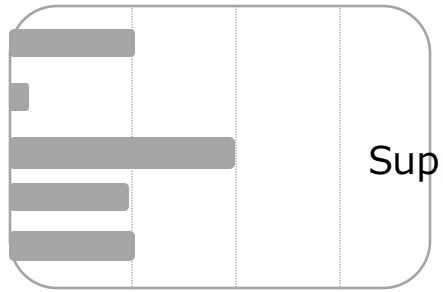
Supplier

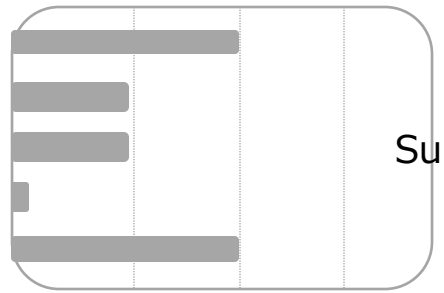
Answer from supplier=Supplier's capability

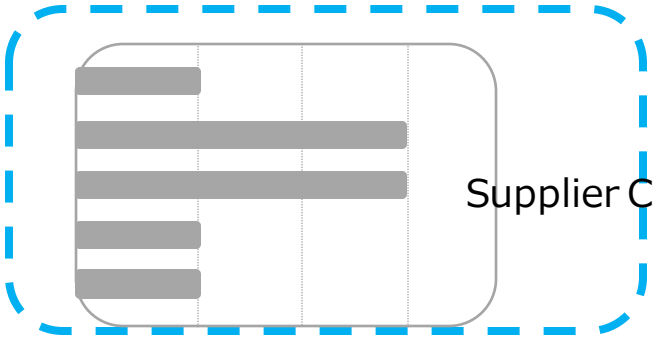
Manufacturer

Expected level for trustworthiness profile
= requirement

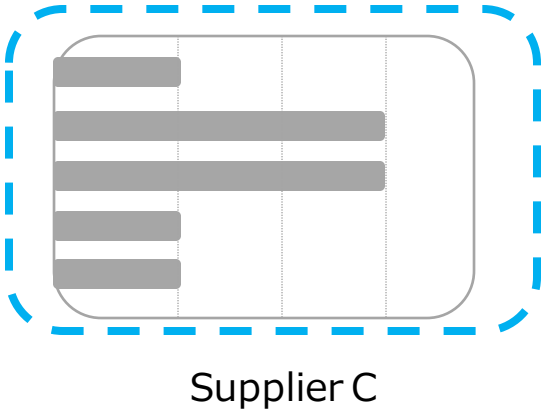








Selected supplier



Supplier C

Maturity level for Trustworthiness

◆ Check maturity level by two axes
①Management – layer process
Processes achieved by high-level management side
(Policies and procedures referred by senior managers)
②Operation-layer process
Security processes achieved by manufacturing and production side
(Policies and procedures referred by personnel in fields)

Partial

Level1

①Management
・Partially implemented by organization level

②Operation
・Documented

Risk Informed

Level2

①Management
・Implemented by organization and got approval by a chief security officer

②Operation
・Documented and developed

Repeatable

Level3

①Management
・Implemented, reviewed and adapted by organization
・Got approval by a chief security officer

②Operation
・Documented, developed
・Reviewed, updated

The contents and the amount of evidences are developed

Risk management process is developed

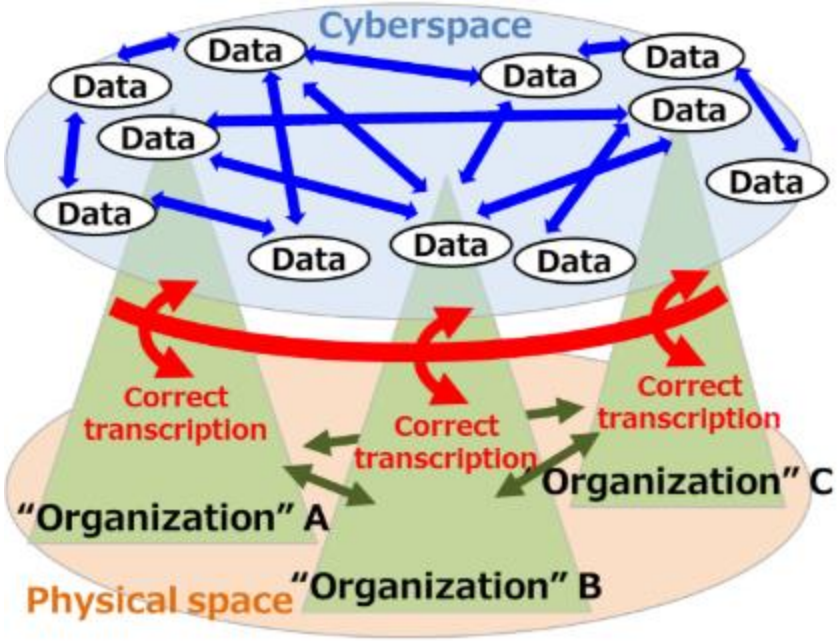
Selected requirements in RRI questionnaire from CPSF

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)

The Cyber/Physical Security Framework (CPSF)
https://www.meti.go.jp/english/press/2019/pdf/0418_001a.pdf

Selected requirements in RRI questionnaire from CPSF

II. How we had prioritized requirements and selected 17 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, management processes and organization.

(Technical security controls are out of scope because they depend on products)

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

Select requirements in RRI questionnaire from CPSF

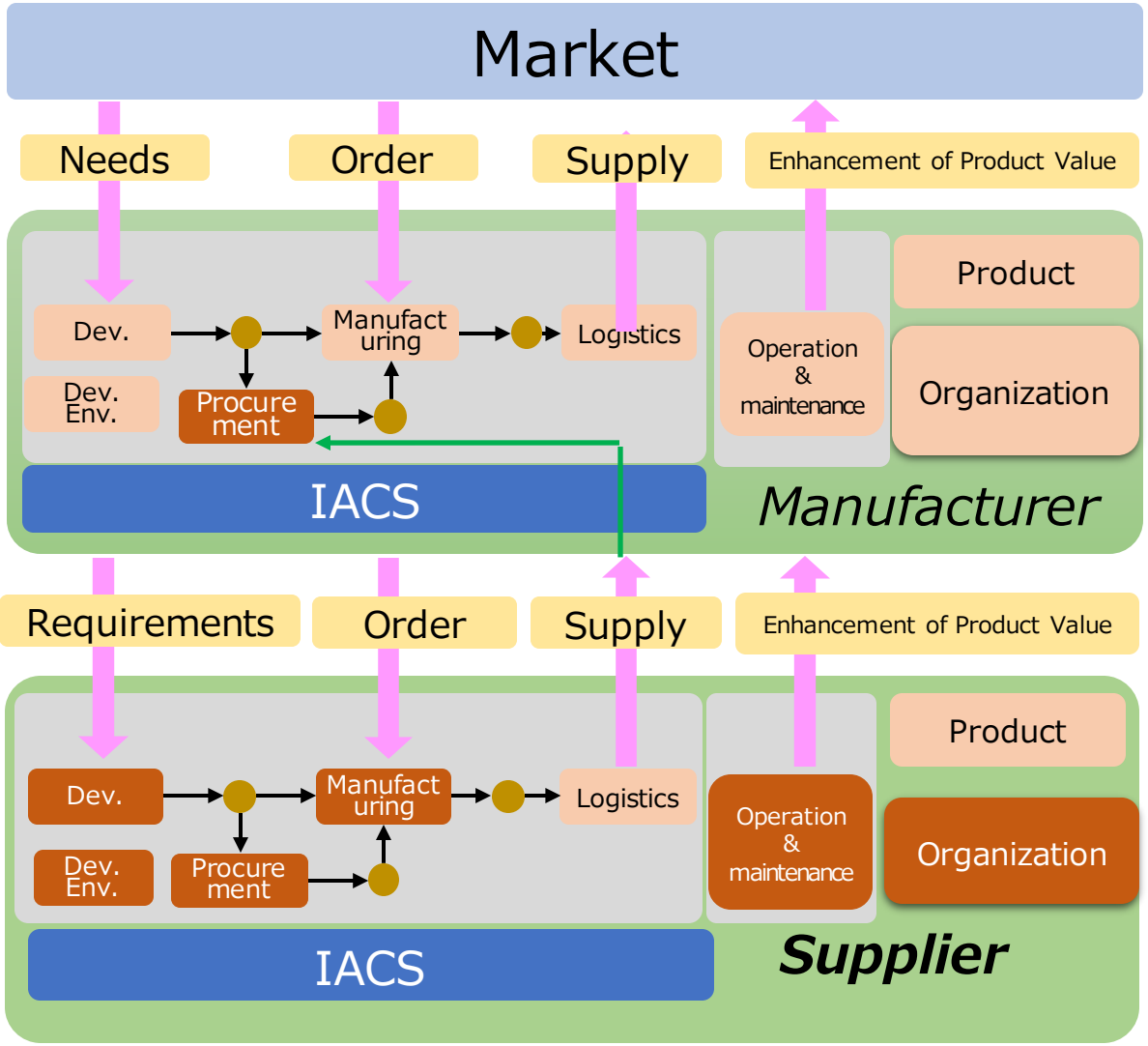
The total number of requirements in CPSF are 104

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

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)

4 domains
17 items

Additional requirements



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

Selected category for questionnaire

I . We added additional requirements

-development,
-development environment,
-procurement,
-Operation & maintenance(O&M)
-Production equipment

from the view point of product life cycle.
e.g.) IEC 62443 2-1,2-4,4-1

Additional requirements

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

Additional requirements

ECM development process	IEC 62443-4-1 SM	Include security management requirements in the product development process.
Development environment	IEC 62443-4-1 SM	Manage product development environment according to security requirements.
	IEC 62443-4-1 SM	Confirm that the source code and data contents of the product are maintained correctly.
Procurement	IEC 62443-2-4 SP.02	Present documentation that ensure the security level of the products and services provided.
O&M	IEC 62443-4-1 SG	Provide manuals to securely set up and make the equipment robust.
	IEC 62443-4-1 SG	Provide manuals for secure use and disposal of equipment.
Production equipment	IEC 62443-2-4 SP.01.01, SP.01.02	Manage construction of production equipment according to security requirements.
	IEC 62443-2-1	Manage operation of production equipment according to security requirements.

◆ ***This requirement is added because it will become important when production facilities are connected to IT networks within the company in the Connected Industry in the near future.***

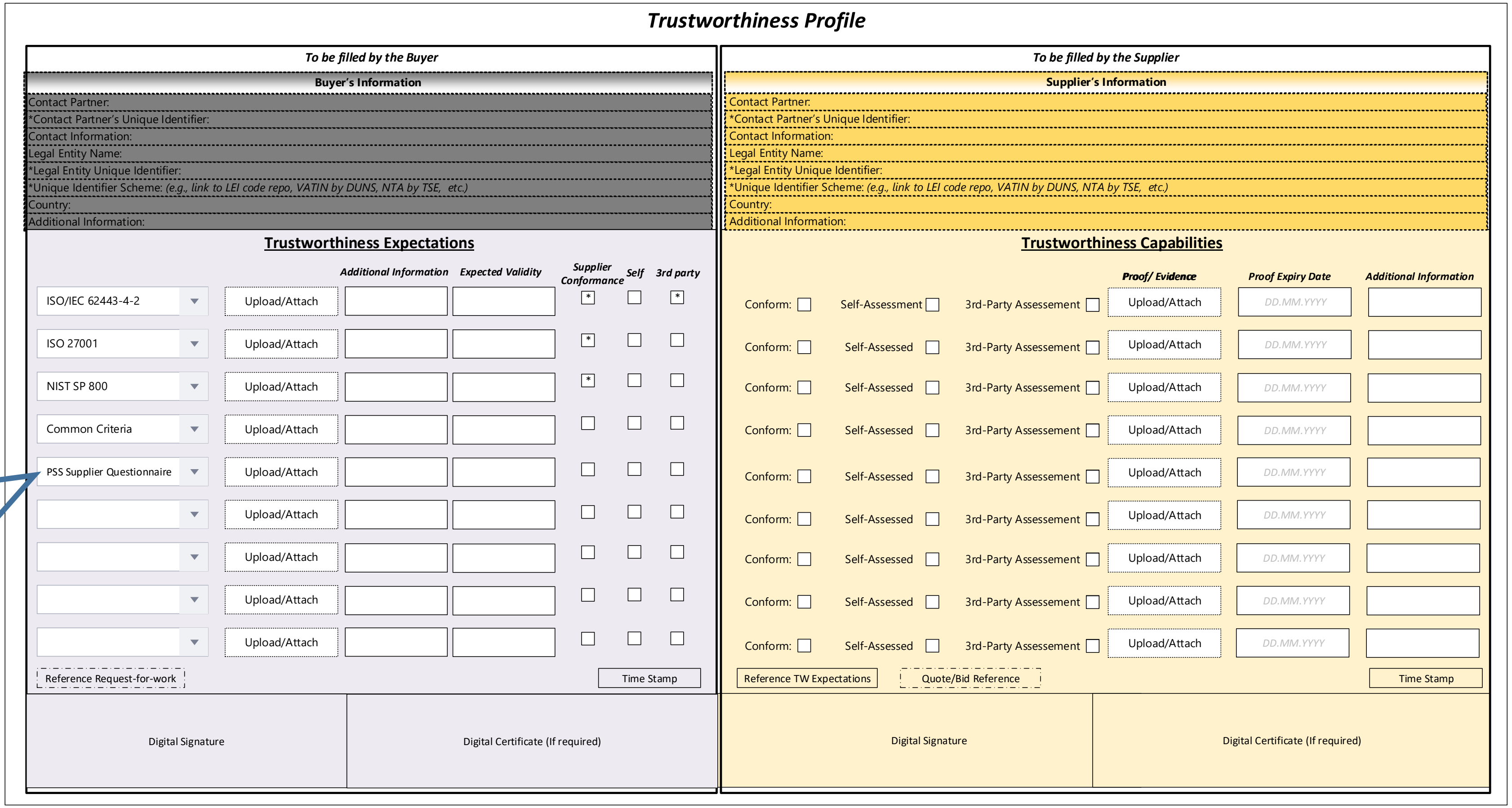
Questionnaire in-practice- Example

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 officers and Chief information security officer regularly review, update, and maintain security policies.
			☐Implemented ☐Planned to be implemented ☐Not applicable

Collaboration activities between RRI and PI4.0

◆ 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



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			*		*
ISO 27001	Upload/Attach			*		
NIST SP 800	Upload/Attach			*		
Common Criteria	Upload/Attach					
PSS Supplier Questionnaire	Upload/Attach					
	Upload/Attach					
	Upload/Attach					
	Upload/Attach					
	Upload/Attach					

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	
Conform:	Self-Assessed	3rd-Party Assessement	Upload/Attach	DD.MM.YYYY	
Conform:	Self-Assessed	3rd-Party Assessement	Upload/Attach	DD.MM.YYYY	
Conform:	Self-Assessed	3rd-Party Assessement	Upload/Attach	DD.MM.YYYY	
Conform:	Self-Assessed	3rd-Party Assessement	Upload/Attach	DD.MM.YYYY	
Conform:	Self-Assessed	3rd-Party Assessement	Upload/Attach	DD.MM.YYYY	
Conform:	Self-Assessed	3rd-Party Assessement	Upload/Attach	DD.MM.YYYY	
Conform:	Self-Assessed	3rd-Party Assessement	Upload/Attach	DD.MM.YYYY	
Conform:	Self-Assessed	3rd-Party Assessement	Upload/Attach	DD.MM.YYYY	

Reference TW Expectations | Quote/Bid Reference | Time Stamp

Digital Signature | Digital Certificate (If required)

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 and the answer for the questionnaire would be standardized, would be used digitally for online contracts.

ANNEX: Selected 17 security requirements for suppliers from CPSF

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 in the organization.
	CPS.GV-1 **(Governance)**	Develop and announce security policies, define roles and responsibilities for security across the organization and other relevant parties (Suppliers) .
	CPS.RA-1 **(Risk Assessment)**	Analyze the vulnerability of the organization's assets and document the result.
	CPS.RM-1 **(Risk Management Strategy)**	Establish and manage the cyber security risk management process by appropriate relevant parties within the organization.
	CPS.SC-1 **(Supply Chan Risk Management)**	Establish and manage the supply chain risk management process by appropriate relevant parties within the organization.

https://www.meti.go.jp/english/press/2019/pdf/0418_001b.pdf

ANNEX: Selected 17 security requirements for suppliers from CPSF

Protect	CPS.AC-1 **(Identify Management & Access Control)**	Issue, manage, validate, revoke, and audit Identification (ID) and authentication information (credential) for authorized devices, people, and processes executed.
	CPS.AT-1 **(Awareness &Training)**	Provide appropriate training and education to all individuals in the organization so that they can understand assigned roles and responsibilities to prevent from or respond to security incidents.
	CPS.DS-1 **(Data Security)**	Agree in advance on security requirements for protection of information, if the organization exchanges protected information with other organizations.
	CPS.IP-1 **(Information Protection Process & Procedures)**	Initial configuration of assets and configuration changes to assets are managed based on security principles.
	CPS.IP-9 **(Information Protection Process & Procedures)**	Include items concerning security in personnel processes such as recruitment and transfer of personnel. Manage the access rights of personnel.
	CPS.MA-1 **(Maintenance)**	Maintain system components with approved tools and record the history.
	CPS.MA- 2 **(Maintenance)**	Maintain system components of the delivered system with approved tools and record the history.

ANNEX: Selected 17 security requirements for suppliers from CPSF

Detect	CPS.AE-1 **(Anomalies & Events)**	Identify the routine network operation and the flow of information between people and systems during the operation.
	CPS.AE-2 **(Anomalies & Events)**	Establish a organization to detect, analyze, and respond to security events.
	CPS.CM-1 **(Security Continuous Monitoring)**	Monitor internal network and external network connection point.
	CPS.DP-1 **(Detection Process)**	Define the roles and responsibilities of security event detection.
Respond / Recover	CPS.RP-1 **(Response Planning)** **(Recovery Planning)**	Implement the response to detected incidents according to the established response procedure.

Thank you very much!

ayaji2.furukawa@toshiba.co.jp