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

PLATTFORM INDUSTRIE 4.0

# FACILITATING INTERNATIONAL COOPERATION FOR SECURE INDUSTRIAL INTERNET OF THINGS / INDUSTRIE 4.0

## 1. Overview and background

Plattform Industrie 4.0 (PI4.0) of Germany and Robot Revolution & Industrial IoT Initiative (RRI) of Japan announced their common position paper "Facilitating International Cooperation for Secure Industrial Internet of Things/Industrie 4.0" on 16th March 2017 at the conference "Digitizing Manufacturing in the G20 – Initiatives, Best Practice and Policy Approaches". Based on this common position paper we, German experts of the Plattform Industrie 4.0's Working Group "Security of Networked Systems and Japanese experts from RRI's Action Group "Industrial Security", have been exchanging opinions and issued the second position paper on 16th May 2018 at the conference "Securing Global Industrial Value Networks - Synchronizing International Approaches". In line with these two common position papers, we are issuing this 3rd common position paper at the conference "HANNOVER MESSE 2019". The goal of this activity is to foster trustworthiness in increasingly digital and interconnected economies.

Highly automated international and global collaboration of industrial production environments is a key feature of Industrie 4.0 (I4.0). In various countries, production facilities will be able to collaborate with each other in an ad-hoc and automated manner across continents. Therefore, availability of a secure comprehensive I4.0 ecosystem is an indispensable prerequisite. Secure operations require trust between all parties involved. Trustworthiness is an important qualitative decision-making criterion for the entire secure value chain. In a connected society, malfunctions and unauthorized operations occurring in devices and systems can cause high-impact damages such as injury, death and loss of property. The impact of those damages can spread extensively through networks. Hence, countermeasures that ensure trustworthiness have high priority.

In order to achieve trustworthiness, all involved parties aim to:

- Implement secure communications (company-wide/ cross-company).
- Incorporate trustworthiness in the lifecycle of services, products, production systems and IT/OT systems - on a risk-based approach.
- Establish open and transparent profiles for trustworthiness on a company-, system-, and product-level.
- Provide assurances regarding the trustworthiness of their products to the customer.
- Accomplish that each partner's trustworthiness can be identified along the entire supply chain.

In line with the previous activities, the goal of this common position paper is to foster trustworthiness in increasingly digital and interconnected economies.

Figure 1 illustrates a high-level architecture of supply chain in connected industries

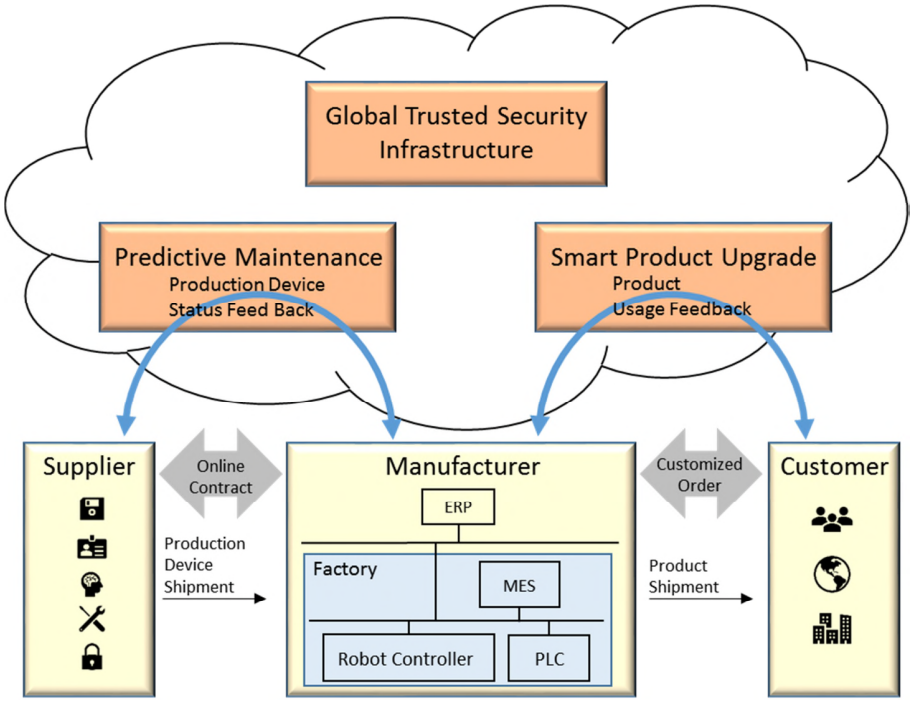


Figure 1: High-level Architecture of Supply Chain in Connected Industries

A global trusted security infrastructure provides the framework for secure communication. Secure digital identities and the consistent adoption of relevant standards are necessary prerequisites for the described use-cases, the online contract and the online exchange of data within a global supply chain.

In order to ensure trustworthiness in a connected supply chain, further key elements have been identified and they are:

- Organization
- People
- Component (e.g. parts, product, device)
- Data
- Procedure
- System

Therefore, in order to realize secure supply chains in connected industries:

- It is essential to ensure the security of key elements of a supply chain based on the principle of security-by-design.
- Manufacturers should be able to identify the trustworthiness of each key element and act depending on the level of confidence.
- Standardized rules and agreed policies are necessary for the access to each key element in the supply chain.
- Variable methods for assessing trustworthiness of cooperation partners need to be established, such as manufacturer's self-declarations, certificates, and audits.

## 2. Trustworthiness

Global value networks require comprehensive trustworthiness architectures covering all participants, regardless of their physical position and location. Trustworthiness describes the level of trust that an entity meets. The term is used to describe the quality of existing and future relationships between companies, people, systems and components.

The characteristic categories for trustworthiness are: security, safety, privacy, reliability and resilience. The crucial components of security are integrity, availability, and confidentiality. This concept applies equally to information technology (IT) and operational technology (OT).

Integrity of products, processes and machines must be assured across these value networks and during the whole lifecycle of a product or a machine. This is an important property of trustworthiness. Without the integrity of organizations and systems, the respective outputs, e.g. documents or products cannot be trusted.

## 3. Possible use-case scenario: Establishing the infrastructure for secure I 4.0-communication between Germany and Japan

The future I4.0 security ecosystem must establish trustworthiness among all participating partners. The partners must be identified, and their respective trust-relevant characteristics must be determined. Using the example of establishing a new business relationship between two companies located in separate countries (for instance Japan and Germany) that do not have previous history of working together, it is intended to demonstrate the possibility of creating an ad-hoc contact between the two companies via an online process using their secure digital identities.

The following business case in the I4.0 context illustrated in Figure 2 occurs: A potential supplier based in Japan wants to establish a new business relationship with a customer in Germany. They did not collaborate or work on any joint projects in the past. They need support to establish a secure communication and collaboration. At this stage, existing and new international standards are to be applied.

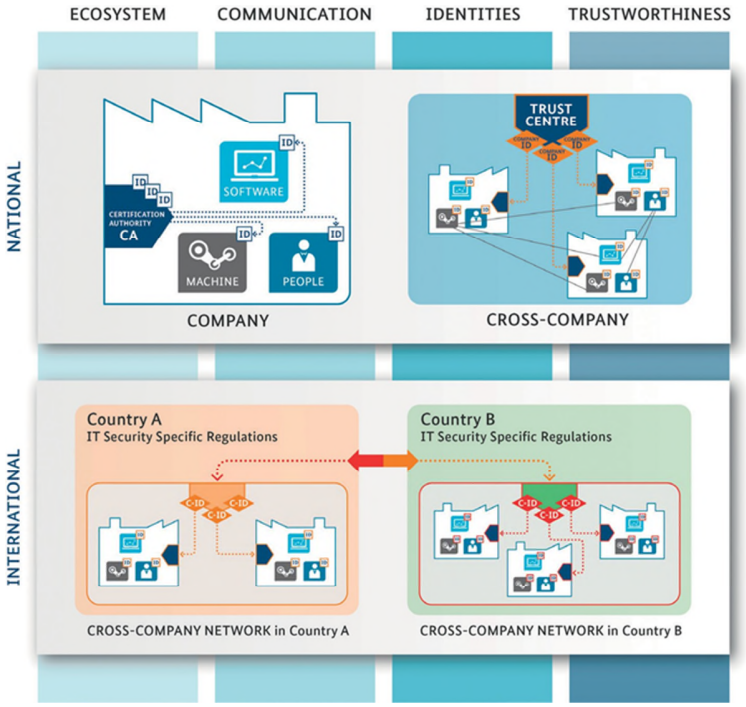


Figure 2: Overall I4.0-Production Scenario

## 4. Problem outline

The Working Group “Security of Networked Systems” from PI4.0 in Germany and the Action Group “Industrial Security” of RRI in Japan jointly postulate key issues that need to be taken into consideration for a lasting business relationship between customers and suppliers across the two countries:

- How to design a trusted global security infrastructure?
- Which criteria and metrics can be used to determine the trustworthiness of a company and its products?
- How is a (partially-) automated verification of trustworthiness of the business partner possible without prior discussions, confidentiality agreements and business contracts?
- How can the creation, provisioning and management of secure digital identities across countries be realized in this infrastructure?
    - How can secure digital identities for companies, people, machines and software processes be issued, distributed and used?
    - How can we ensure that secure digital identities in both countries have the same or comparable security level?
    - How can it be ensured that digital identities are valid and are used exclusively by authorized users (persons, machines, SW processes) and within the scope of a defined release process?
    - How can such an infrastructure be operated realistically? How can a gradual introduction be made?
- Is a single overarching global certificate-based process for delivering secure digital identities globally applicable, feasible, and economical?
    - How can existing national procedures be linked internationally?
    - Is it enough to link individual national procedures bi-nationally via "bridge" constructions? Are group constructions required?
- How can a worldwide recognition of trust service providers be organized?

## 5. Need for further Action

- Conduct bilateral project for international interoperability of solutions, including:
    - Definition and detailed description of the use case focusing on organization security.
    - Jointly formulated requirements to solve the defined problems; i) for prerequisite measures, ii) for possible implementations.
    - Expand the definition and detailed description of the use case focusing on system and component security.
    - Joint demonstrators to validate interoperability.
    - Evaluation and recommendation.
- Evaluate solutions for robustness and scalability
    - Evaluation can be successful if the accepted solution can be transferred to viable business models.

Contact: jimukyoku@jmfrri.gr.jp; geschaeftsstelle@plattform-i40.de

---