Facilitating International Cooperation for Secure Industrial Internet of Things / Industrie 4.0 2018

- PLATTFORM INDUSTRIE 4.0 (PI4) Germany and Robot Revolution Initiative (RRI) Japan announced their common position paper about Industrial Internet of Things (IIoT)/Industrie 4.0 on 16th March 2017 at the conference “Digitising Manufacturing in the G20 – Initiatives, Best Practice and Policy Approaches “.[1)]
- Our main goal is to foster cyber resilience, as well as security and trustworthiness in increasingly digital and interconnected economies.
- This paper describes the next PI4 & RRI activities and outlines the common basic understanding of trustworthiness in the context of cooperation in "Secure Industrial Internet of Things / Industrie 4.0".

NEXT STEP:
Challenge for Secure Supply Chain of Connected Industries

- Ensuring security is challenging, especially in cross-company and cross-border communication scenarios. Secure (company-wide/ cross-company) operations require trust between all parties involved.
- Trustworthiness is an important qualitative decision-making criterion for the entire secure value chain. Each manufacturer wants to give his customer clear, comprehensive and reliable information about the properties of the system, product and data delivered.

In order to achieve security and trustworthiness all parties involved aim to:

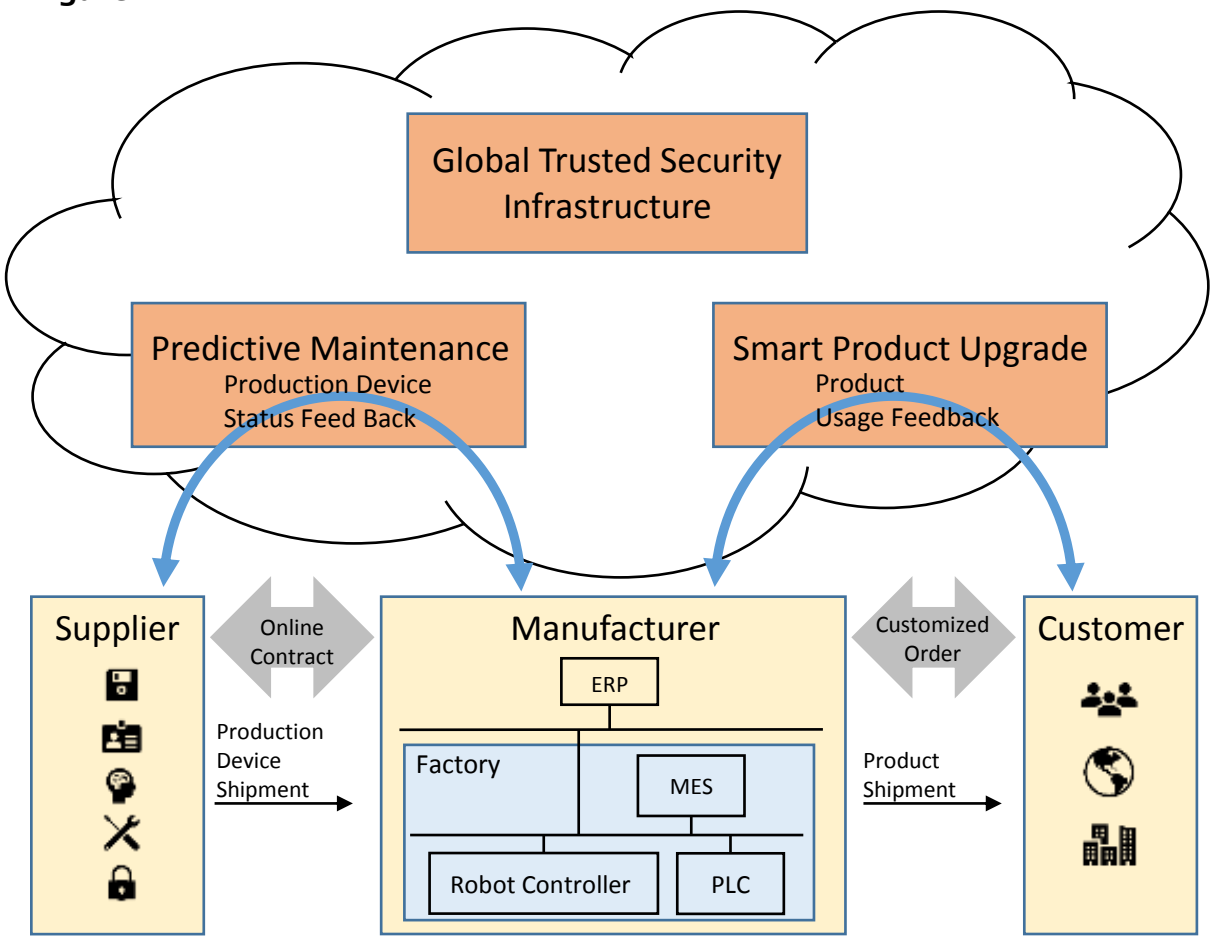
- Incorporate trustworthiness in the lifecycle of services, products, production systems and IT/OT systems - on a risk-based approach
- Implement secure communications (company-wide/ cross-company)
- Establish open, clear and transparent indicators and profiles for trustworthiness on company-, system-,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

[1] https://www.plattform-i40.de/I40/Redaktion/EN/Downloads/Publikation/Secure-Industrial-Internet-of-Things.pdf;jsessionid=4556384F8BD04E4842016B133893BF5F?__blob=publicationFile&v=3

- We are going to identify security requirements through use-cases where we can share future customer needs and system architectures. (see figure 1)

    - Manufacturing system operators choose a production device vendor online and order production devices from this vendor.
    - The production device supplier provides a unique digital identity to enable traceability of devices throughout the supply chain
    - When the production devices are provided, integrity and authenticity are checked out at operator sites to ensure the trustworthiness of the production devices.
    - In addition to the digital identity assigned by the production device supplier, the manufacturing system operators assign digital identities for the operation from their own security domains. Depending on the use case, different IDs can be used to manage the production process or to monitor the predictive maintenance.
    - Information collected during production processes must be protected against manipulation or disclosure and must be available, such that necessary decisions can be made.

<Figure 1>



Key elements for a secure supply chain are:

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

・ It is essential to ensure the security of key elements factors of a supply chain based the principle of security by design.

・ Manufactures 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.

・ Methods for assessing the trustworthiness of the cooperation partners are variable, such as manufacturer's self-declarations, certificates, and audits.

Need for Action

Both sides, Platform Industrie 4.0 and Robot Revolution Initiative,

・ Recommend a further discussion on methods for assessing the trustworthiness of supply chain key elements, and strive for the development and standardization of common, accepted policies for a global secure supply chain;

・ Identify the targets of trustworthiness among organizations, people, systems, procedures, components (e.g. parts, products, devices) and data;

・ Identify the trustworthiness assurance and levels for the targets, which may be requested automatically from each participant of the supply chain;

・ Develop a common roadmap with joint next steps and priorities and provide input for the ongoing international standardization work.