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

PLATTFORM INDUSTRIE 4.0 | ROBOT REVOLUTION INITIATIVE

PLATTFORM INDUSTRIE 4.0

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

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

In recent years, Industrial Internet of Things (IIoT)/Industrie 4.0 has progressed in various countries. However, previously unconnected devices and those that were not assumed to be connected can now be connected, security/safety risks are expected to increase. Many devices and systems are used for 10 or more years, and therefore security/safety measures for those must be implemented immediately. The development of secure as well as safe devices and systems is also expected to contribute to the expansion of international competitiveness.

Overall, the superior goal should be to foster cyber resilience, as well as security and trustworthiness in increasingly digital and interconnected economies. As a result, cyber security cannot only be seen as a technical issue, but rather a multilateral cooperation is required between all stakeholders (politics, economy, academia, society). This paper outlines starting points which provide a mutual understanding of the process.

I. Security Guiding Principles for IIoT Device/System Development and Operations

In a connected society, malfunctions and unauthorized operations occurring in devices and systems can cause unreasonable damage such as injury, death and loss of property, etc. The impact of those damages can spread extensively through networks. Countermeasures for such risks include ensuring the integrity, availability, and confidentiality of IoT devices. System development and operations for such security/safety measures should be considered on the basis of fundamental principles. Safety is an essential protection goal for many use cases.

Five Guiding Principles of IIoT/Industrie 4.0 Security Countermeasures

[Plan] Establish a basic policy in consideration of IoT characteristics.

[Analyze] Identify IoT risks.

[Design] Consider a consistent, effective and resilient design to protect security/safety-critical assets.

[Implement/Connect] Consider processes, technical and network-based countermeasures.

[Operate/Maintain] Maintain a safe and secure state, dispatch and share information and consider business continuity.

II. Security for IIoT / Industrie 4.0

One of the main advantages of IIoT/Industrie 4.0 is expected to be derived from the cooperation among companies enabled by increasing automated exchange of data and information. For example, efficiency can be increased when each stakeholder exchanges data and information and explores optimal distribution of resources under the consensus of each other.

Data and information exchange across company borders requires trust in the partners that are part of the production network. Security measures, both technical and organizational, have to be established by all participating companies along the value chain.

Some key elements of trust are strong authentication, access control and

authorization of all communicating entities (e.g. IIoT devices/systems, humans and organizations). Any cooperation should be organized in a secure and reliable manner. In addition, the unique identification of process stakeholders should be checked and any expertise regarding components, processes, machines and plants is to be protected.

Trustworthiness of products, solutions, and communication is a key issue for industries and their customers. The integrity of the value chain is necessary, such that end users can have confidence in its security.

Worldwide harmonization

International trade regulations need to be transparent and harmonized. There should not be excessive examination and censorship by governments and secure international industrial cooperation facilitated. It is not feasible for single countries to work in isolation regarding security in global IIoT/Industrie 4.0. Supply structures are spread across a variety of countries. Machines and plants are sold all over the world. Neither the business sphere of global companies, nor the cyber-attacks themselves stop at international borders. A harmonized approach based on international standards at international level is the only way to achieve consistent and trustful security levels, including small and medium-sized companies.

This will strengthen the global protection of users and customers.

III. Future Work

Both sides recommend the development of standards related to the points outlined in Sections Ⅰ& Ⅱ above. The development is to be conducted in internationally agreed standardization processes as found in ISO or IEC committees, and will discuss details under this common security position paper. This requires the identification of challenges and the initiation of necessary basic guidelines for reliable and secure international IIoT/Industrie 4.0.

PLATTFORM INDUSTRIE 4.0

www.plattform-i40.de
For more information on the Plattform Industrie 4.0, please contact:
Henning Banthien
Secretary General
h.banthien@plattform-i40.de

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

www.jmfrri.gr.jp
For more information on the Robot Revolution Initiative, please contact:
Tomoaki Kubo
Secretary General
tomoaki.kubo@jmfrri.gr.jp