Industrial security Requirements
-extracted from discussion on a cross organization use case-

Industrial security AG, RRI
Our Goal: To identify new security requirements in future manufacturing systems of Industrie4.0
Challenges

To identify new security requirements, we have to first identify and share future business use cases and their system architecture.

First target

- Future business use cases (business needs)
- Future System Architecture

Difficult!
Futuristic but realistic from the view point of mega trend.

Difficult!
Realistic from the view point of current technology and to-be technology.

Easy if the system architecture is clear
Tech. concepts of I4.0 (“Admin shell”, “Industrial Data space” etc.) are here!

Security Function

Not discussed yet
Security Implementation

2017 Copyright Robot Revolution Initiative, All Rights Reserved.
A system architecture of the Use Case

Operation states of each controller in factories are monitored through the Data Access Platform by External Advisors for early fault detection and recovery.

- Operation logs of Robot Controllers in each factory (e.g., in German) are gathered to the platform in the 3rd country.
- External Adversary in Japan for Robot Cont. gets the data of them from the platform.
- If a EA predicts faults, it sends the alarm to the corresponding ERP.
- The ERP contacts with Production scheduler and determines the production schedule and maintenance schedule.
Security requirements for the architecture

“Global”, “dynamic” and “horizontal integration” could be the key to identify I4.0 specific security requirements.

System/network
- Unique IDs should be assigned to users to authenticate them
- Need to access policy” should be applied to system and network
- In order to adapt dynamic change of entities which need access to the system and network, automatic access control change mechanism should be introduced.
- Communications for inter-organization and inter-component should be protected.

Components
- Unique IDs are assigned for unified global access and identification.
- Access right for components should be “need to access” basis (ex. in a role based manner).
- “Who access to what components when” should be kept for audit and tracability.

Etc.(data)
- Personal information should be protected for complying with privacy regulation.
Future work

We are going to identify new security requirements though the process of ①②③④, and also to deeply understand Industie4.0 Sec.Func. with the need of proper implementation.
Appendix
Both German and Japan side have shared the whole picture which shows where values exist in product/production lifecycle and its maintenance. We have chosen VBS as the start discussion item.

IPD: Innovative Product Development
SPD: Seamless and Dynamic Plant Engineering
AF: Adaptable Factory
SP2: Smart Product Development for Smart Production
OCP: Order-Controlled Production
HTI: Human-Technology-Interaction in the Production
SAL: Self Organization and Adaptive Logistics
TAP: Transparency and Adaptability of Delivered Products
VBS: Value Based Service

VBS: Value Based Service
This objective is for manufacturers to attain higher availability (smaller down time) by means of early fault detection and rapid fault isolation and/or recovery.

The present scenario introduces Platform, which collects the operating information of machines used all over the world and gain benefits by offering the information to External Advisory.

By doing so, External Advisory does not have to pay effort on collecting information, and he/she can enhance its diagnosis expertise.

Alternatively, External Advisory can gain benefits by offering a model of machines regarding their faulty behavior and necessary measurement to Platform.

By doing so, Platform can gain benefits by providing diagnosis service to Manufacturer using their information infrastructure, which is used for monitoring machines.
This figure shows how new kinds of interactions and trust are needed in industrie4.0 So that management can intuitively understand the security challenges in industrie4.0.
Admin shells applied for the system structure

Each component and server with “admin shell” could be join to I4.0 systems and interact with each other as a standardized I4.0 object.

**Diagram Description:**
- **Manufacture A:**
  - Admin. Shell (AS)
  - Production Scheduler (PS)
  - ERP
  - OA Terminal

- **Factory 1:**
  - Robot Cont. 1
  - PLC 1
  - MES 1

- **Factory 2:**
  - Robot Cont. 2
  - PLC 2
  - MES 2

- **External Advisor B:**
  - Data Analyzing Server (DAS)
  - OA Terminal

**Legend:**
- **DF:** Digital Factory
- **AS:** Admin Shell
- **Internet:**
- **Firewall:**

**Identification and Compo. Manager:**
- **Identification Item:**
  - Identification of the cntrl. panel
- **DF Header:**
- **DF Body:**
  - Partial model 1
  - Partial model 2
  - Partial model 3
  - Compo. Manager