How can we guarantee a secure communication?

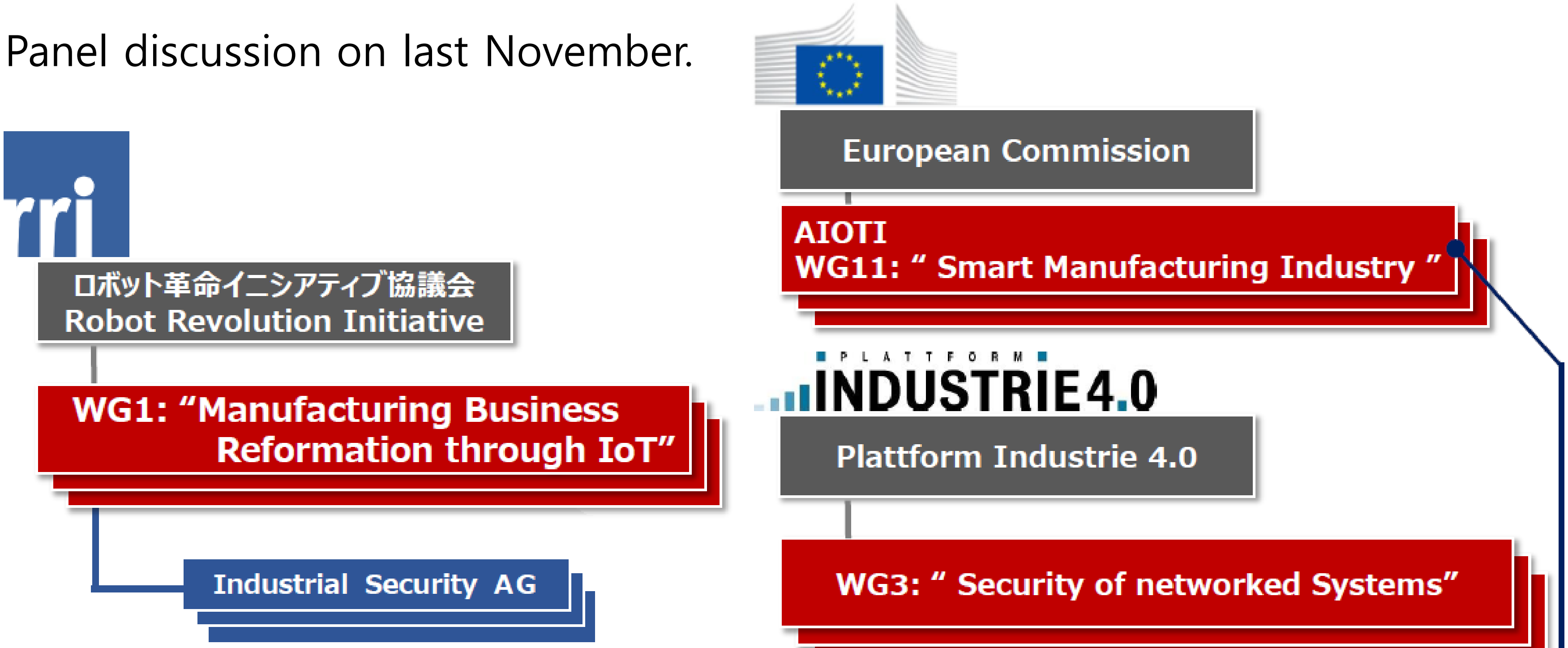
Dr. Takeshi Yoneda

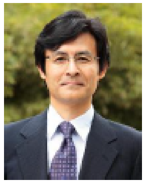
Industrial security AG, RRI

Information Security Dept.
Information Technology R&D Center.
Mitsubishi Electric Corp.

Introduction of RRI Industrial Security AG

Panel discussion on last November.


ロボット革命イニシアティブ協議会
Robot Revolution Initiative
WG1: “Manufacturing Business Reformation through IoT”
Industrial Security AG
European Commission
AIOTI
WG11: “ Smart Manufacturing Industry ”
PLATTFORM INDUSTRIE 4.0
Plattform Industrie 4.0
WG3: “ Security of networked Systems”



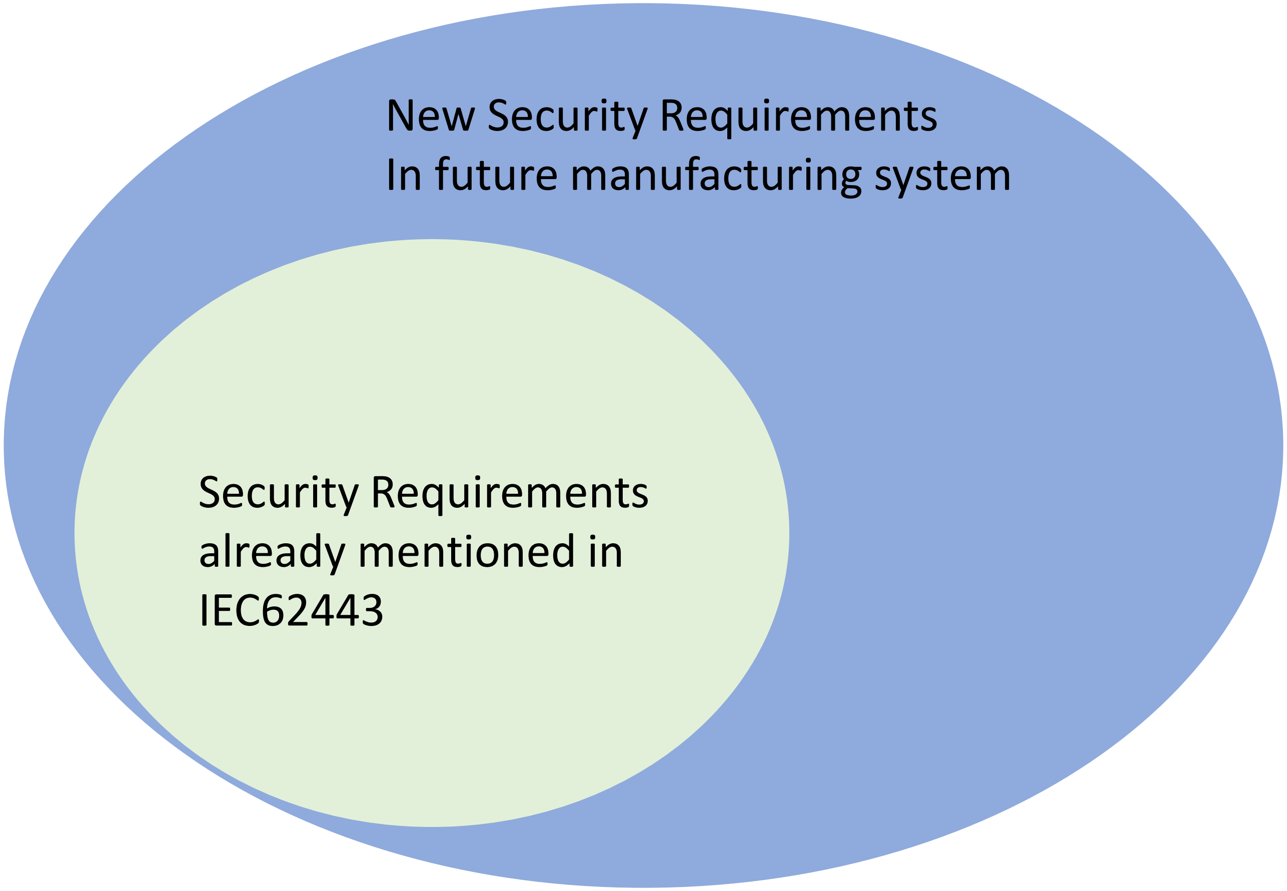
Dr. Tsutomu Matsumoto Dr. Takeshi Yoneda

Masue Shiba, Tutomu Yamada
Yutaka Manchu, Atsushi Kitamura

Dr. Wolfgang Klasen
Mr. Steffen Zimmermann
Mr. Lukas Linke
Mr. Thomas Walloschke

VDMA ZVEI: Die Elektroindustrie

Our Goal: To identify new security requirements in future manufacturing systems of Industrie4.0

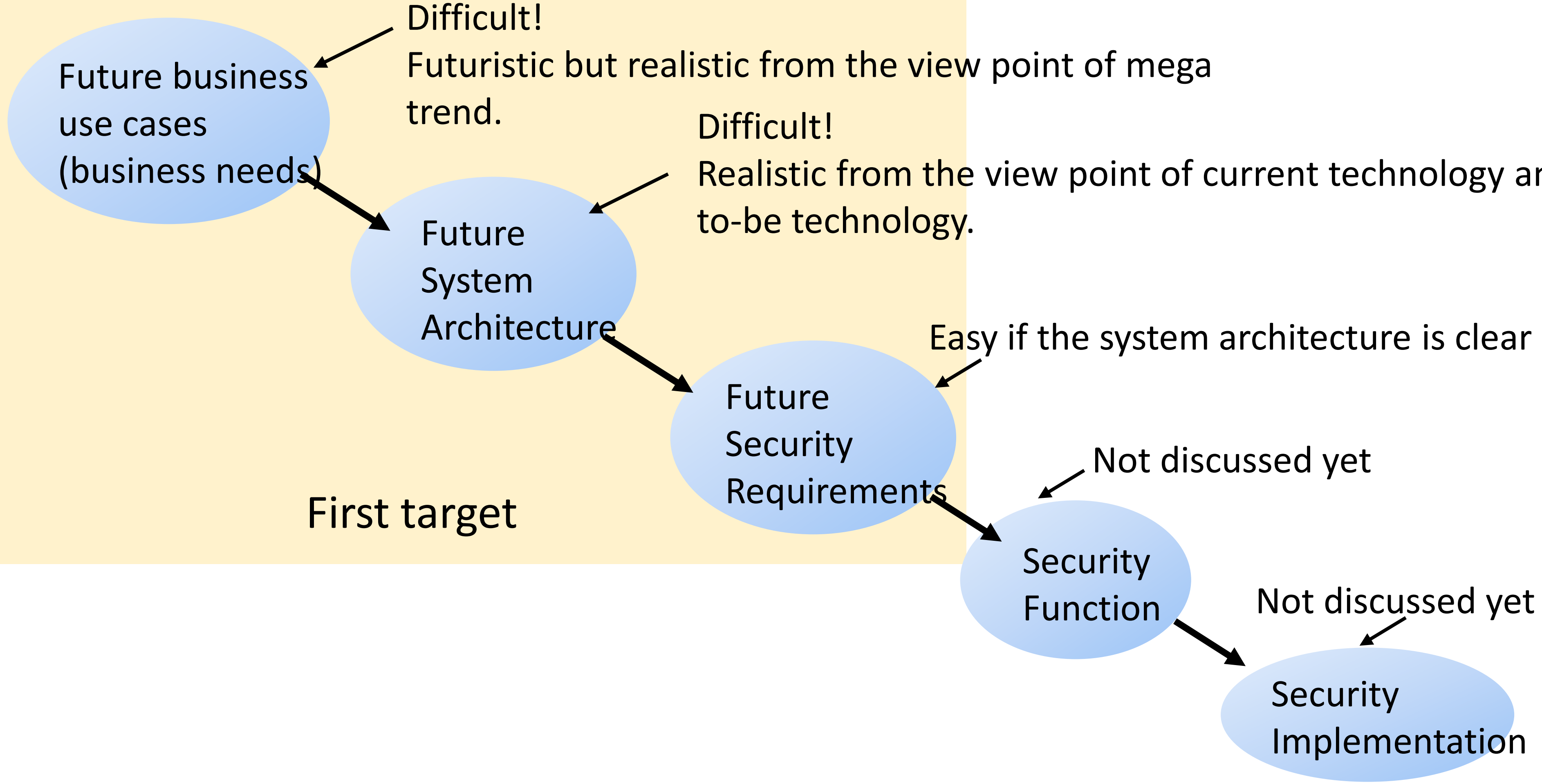


New Security Requirements
In future manufacturing system

Security Requirements
already mentioned in
IEC62443

Challenges

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



Future business use cases (business needs)

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

Future System Architecture

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

Future Security Requirements

Easy if the system architecture is clear

Security Function

Not discussed yet

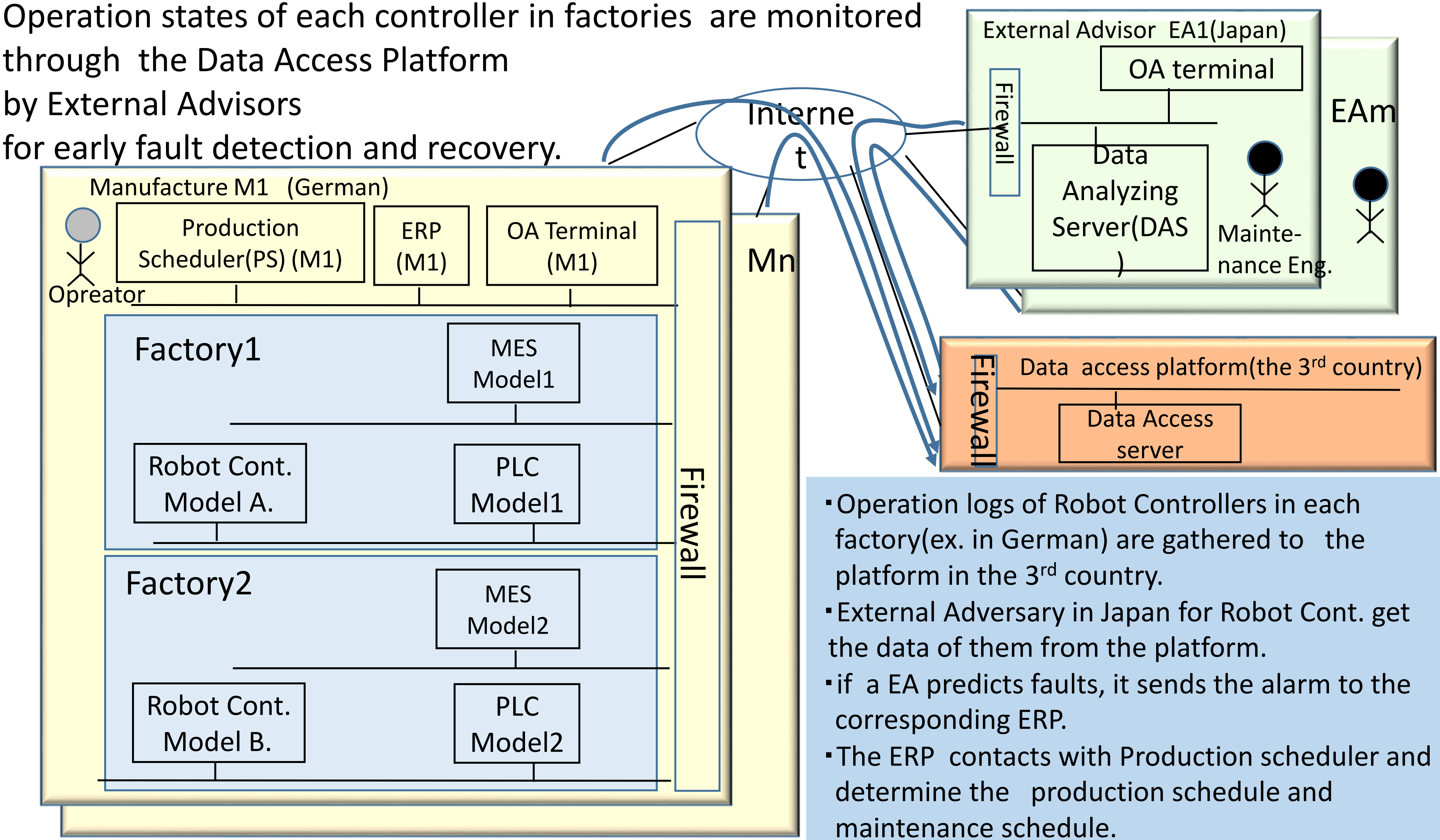
Security Implementation

Not discussed yet

First target

One business 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(ex. in German) are gathered to the platform in the 3rd country.
- External Adversary in Japan for Robot Cont. get 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 determine 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

-In order to adapt dynamic change of entities which need access to the system and network, automatic access control change mechanism should be introduced.

Components

- Unique IDs are assigned for unified global access and identification.

Etc.(data)

- Personal information should be protected for complying with privacy regulation.

Takeaways though collaboration and answers for the session questions

Q1. How can we ensure consistent and secure handling of data and information in a multi-peer value creation network?

A1. We should share security guidelines and standards with global harmonization. Especially, we should share

- -security frameworks.
- -business use cases to identify domain specific security requirements/countermeasures.

Security framework

We should link our security frame of security requirements/measure to widely used framework to globally harmonize.

Security requirements

Threats		1	2	3	4
	a	●		●	●
	b		●		
	c			●	

For Example →

-NIST Cyber security framework
-ISO 27001

		1	2	3	4
Loss of C	A	●		●	●
Loss of I	B		●		
Loss of A	C			●	

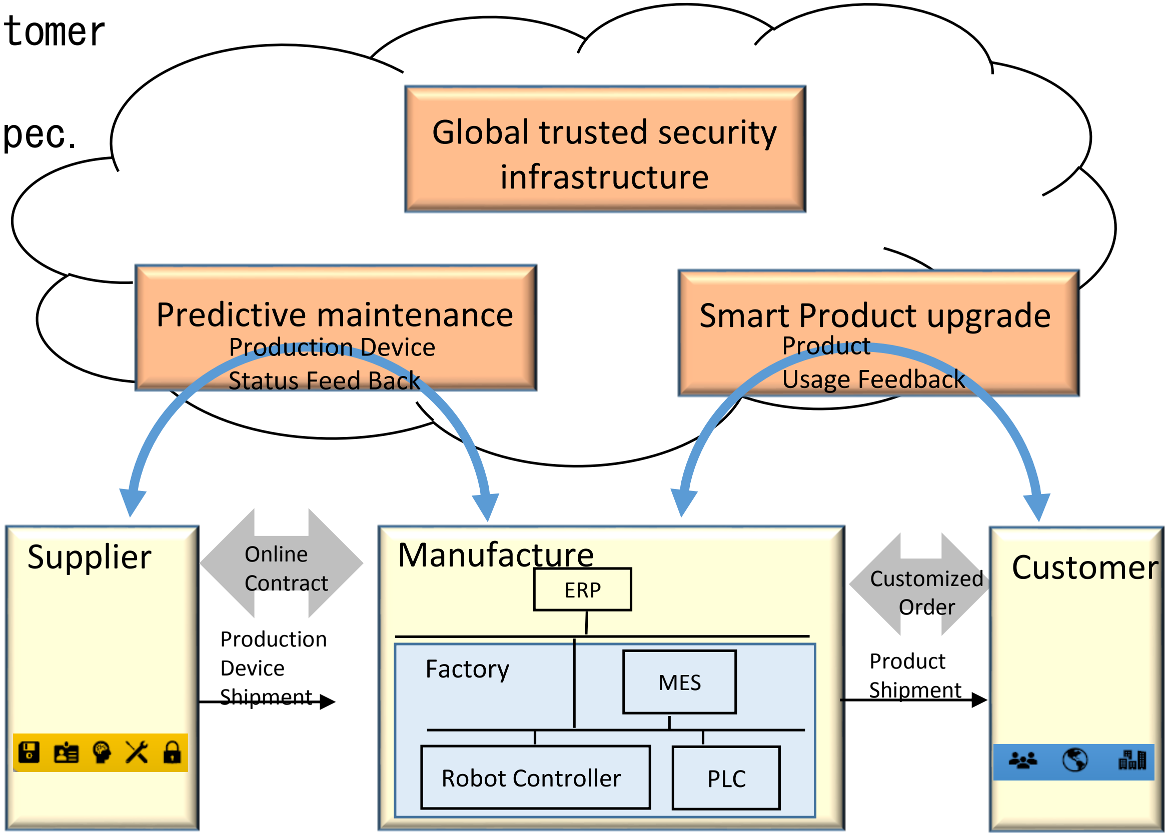
C:Confidentiality, I:Integrity, A:Avalabiity

Business Use case

Business use cases are important to draw knowledge from specialist belonging to different business domains and to focus on common topic.

Sample Use case: Manufactures determine suppliers which could provide parts assembled to products which satisfy customer need

Discussion on trustworthiness:
Online contract triggered by customer orders would occur.
In the contract not only parts spec. volume, price and due-date,
but also trustworthiness of the organizations of suppliers should be agreed.



Takeaways though collaboration and answers for the session questions

Q2． How can we determine the authenticity and trustworthiness of peers in ad hoc relationships?

A2． From the technical view point， Using PKI with attribute Certificates where the mutually agreed trustworthiness levels are included.

Challenges are we should agree on

- what is trustworthiness.
- to which trustworthiness is assigned.
- how many levels trustworthiness should have.
- what level of trustworthiness is enough

PKI： Public Key Infrastructure

What is trustworthiness?

Security is obviously included in trustworthiness. It seems that trustworthiness is used to judge whether they can make contract or begin transaction with a peer.

If Company A has gotten ISMS certification. he has a level of trustworthiness.
The fact would be used just after authentication and before authorization
in order to judge whether what kind of access privilege could be assigned to the peer.

	Requirements/countermeasures				
Threats	(Risk)Identify	Protect Authentication Authorization	Detect	Respond	Recover
Loss of Confidentiality	●	●			
Loss of Integrity	●	●	●		
Loss of Availability	●	●		●	●

What is trustworthiness?

After sharing how to use trustworthiness, we should expand the definition of trustworthiness including safety, privacy, resilience, reliability.

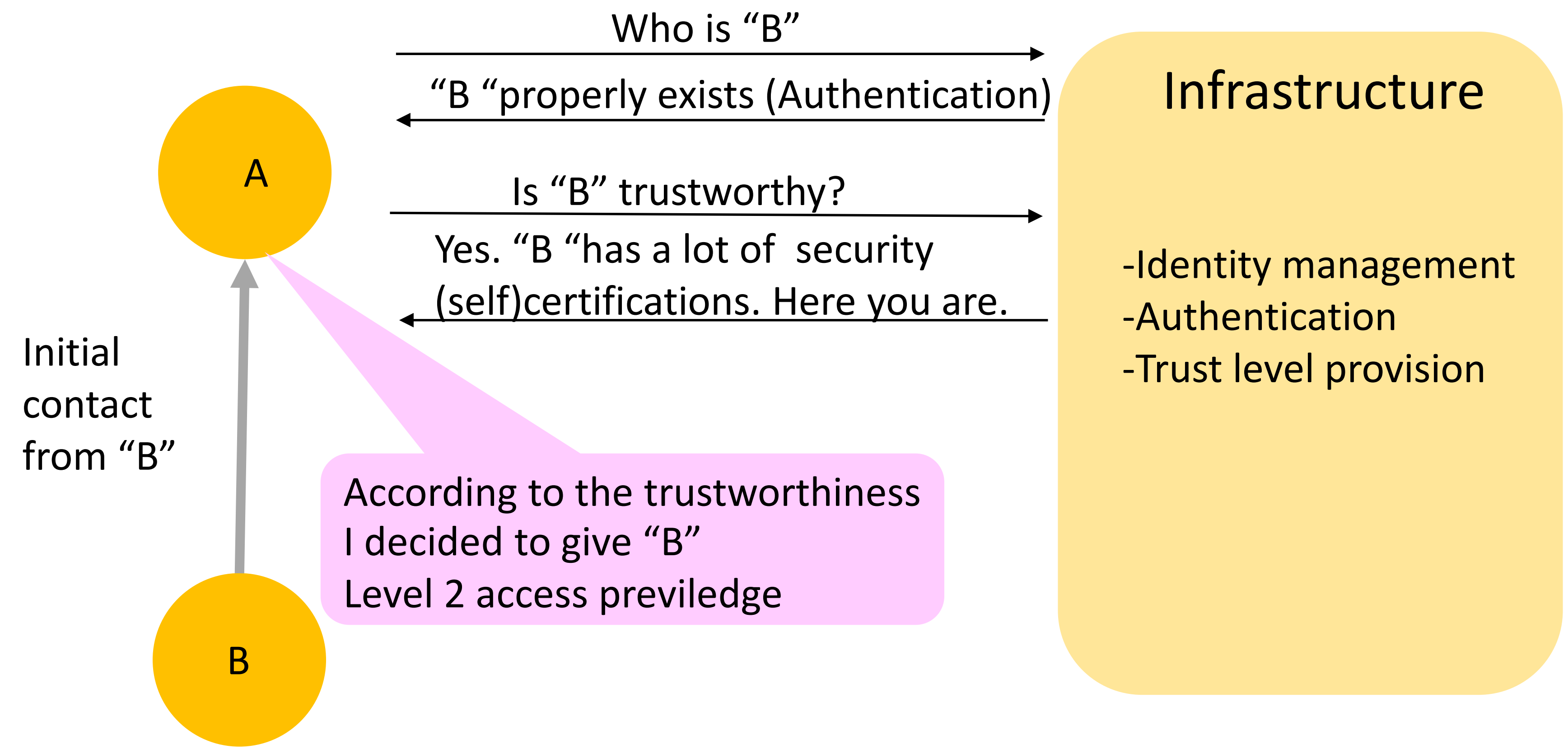
Threats		Requirements/Counter measures				
Loss of trustworthiness	Loss of security	(Risk)Identify	Protect Authentication Authorization	Detect	Respond	Recover
security *privacy*	Confidentiality	●	●			
	Integrity	●	●	●		
Resilience *reliability*	Availability	●	●		●	●
safety		○			○	○

Can we put the countermeasures of safety hazards, under the same security framework? Or we should change the framework?

Takeaways though collaboration and answers for the session questions

Q3. Which infrastructure support is needed to assure secure and reliable communication in the distributed value chain?

A3. As shown in the previous slides, an infrastructure which provides trustworthiness of peers should be provided.


Who is “B”
“B “properly exists (Authentication)
A
Is “B” trustworthy?
Yes. “B “has a lot of security (self)certifications. Here you are.
Initial contact from “B”
B
Infrastructure

-Identity management
-Authentication
-Trust level provision

According to the trustworthiness I decided to give “B” Level 2 access previledge

Future work

・Development and standardization of common, accepted policies for the global secure supply chain.

・Identification of the targets of trustworthiness among organization, people, system, procedure, components (e.g. parts, product, device) and data.

・Identification of the trustworthiness assurance and levels for the targets

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

One more thing: If time allows

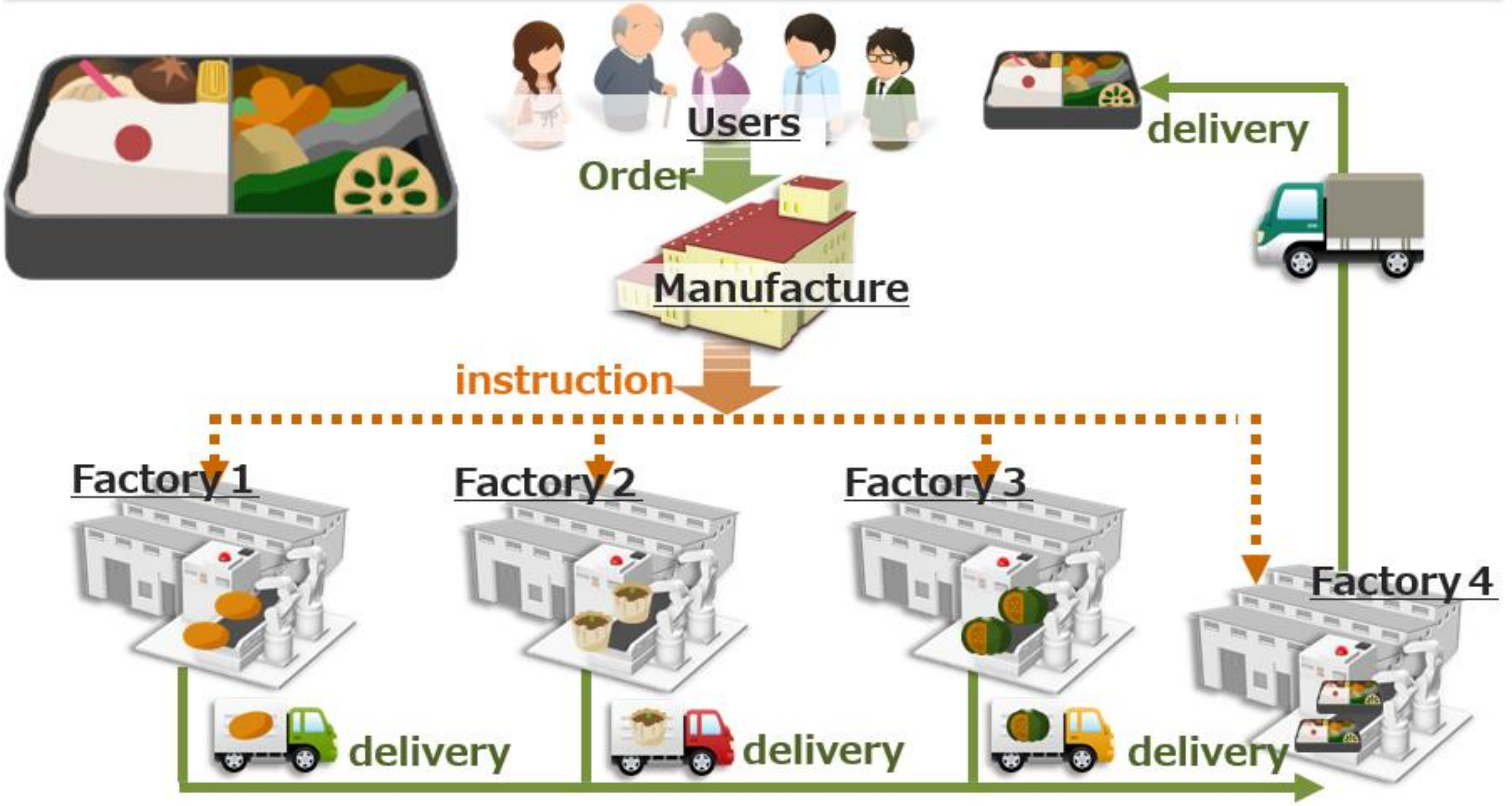
Mass custom production of Japanese Lunch Box

Japanese bottom up approach for identifying security requirements and countermeasure.

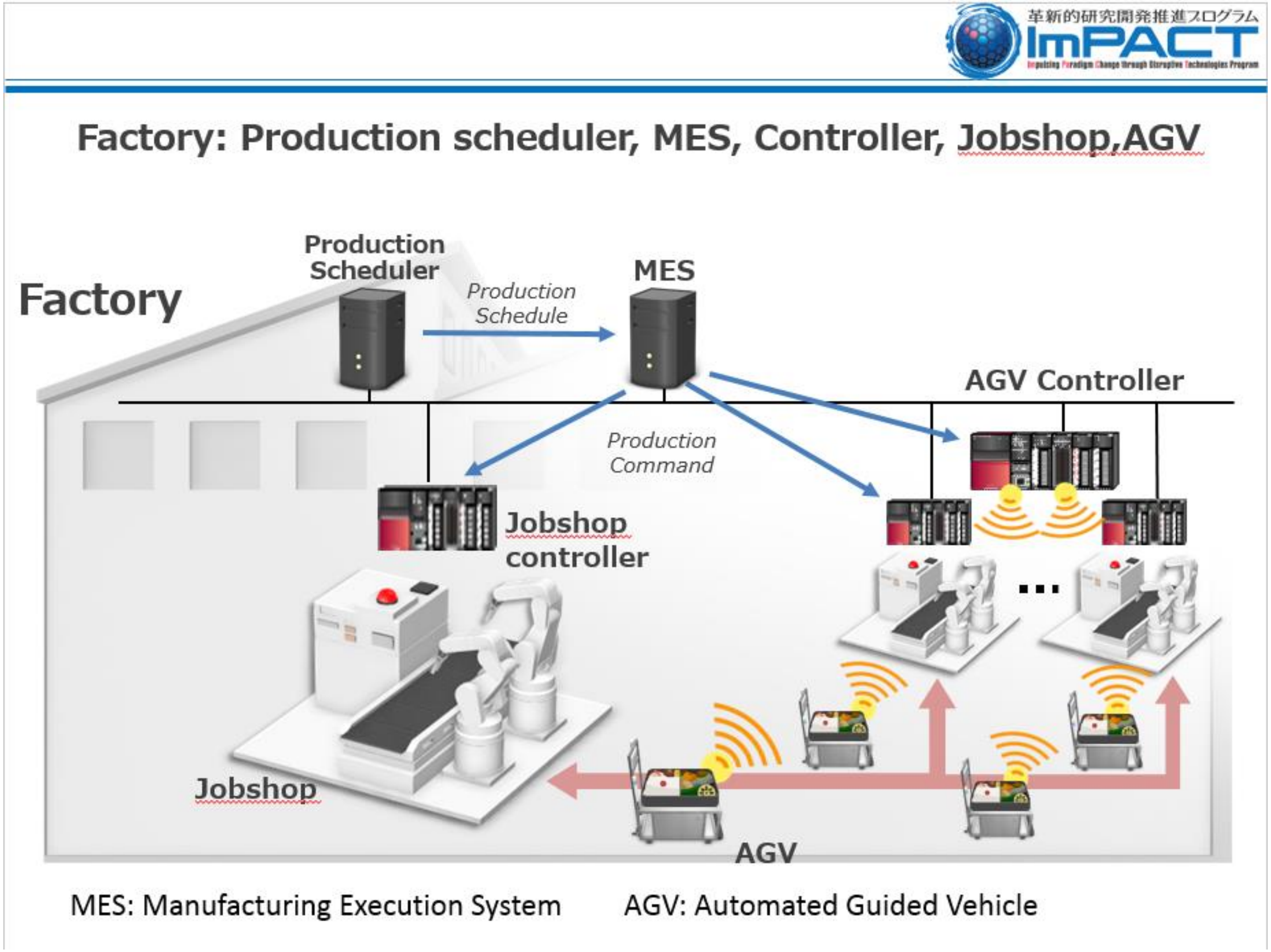
http://www.mitsubishielectric.co.jp/corporate/randd/laboratory/information_technology/english.html

Business Use case

- Users order what they want through internet.
- Manufacture receive a lot of orders of customized products (e.g. 10,000 pieces)
- Manufacture produce those products by collaboration with factories connected via internet. Then deliver to users on time.



System Architecture



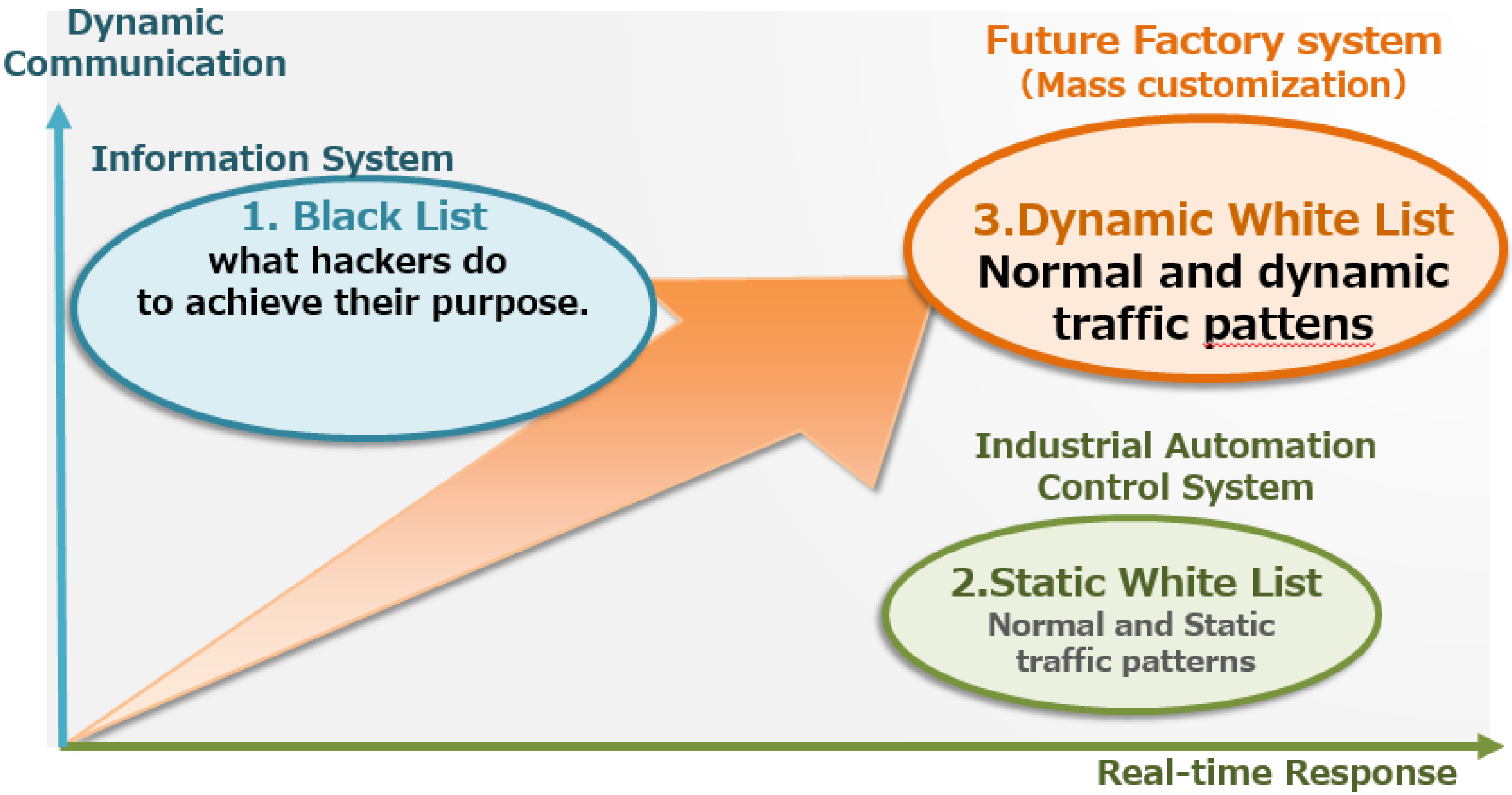
革新的研究開発推進プログラム ImPACT

Factory: Production scheduler, MES, Controller, Jobshop,AGV

MES: Manufacturing Execution System AGV: Automated Guided Vehicle

Security Analysis->Requirements>Functions

Information system: Black List
Industrial Control system: Static White List
Future Factory System: Dynamic White List



http://www.mitsubishielectric.co.jp/corporate/randd/laboratory/information_technology/english.html

Thank you!