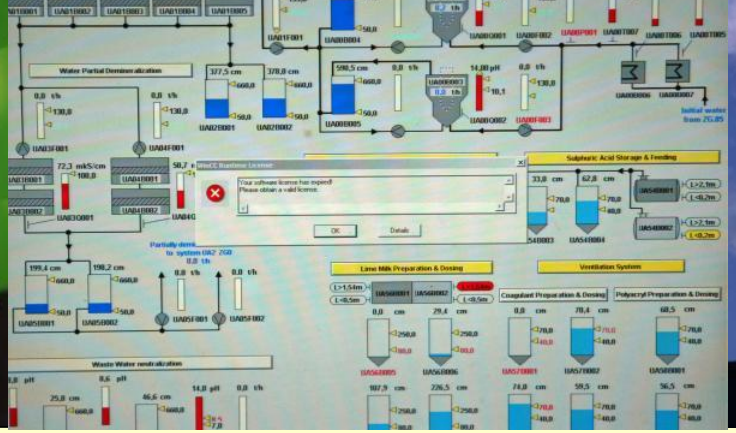
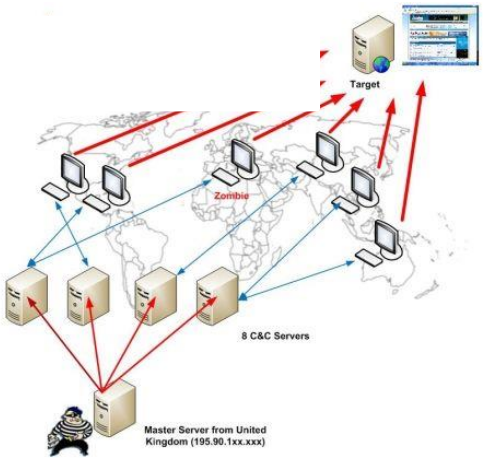


Cyber-Security Measures for ICS focusing on Safety

Yoshihiro Hashimoto and Ichiro Koshijima

Nagoya Institute of Technology, Japan



http://www.manage.nitech.ac.jp/Security/

Every Industrial Plant has Cyber Threats

Stuxnet (Epoch making Malware discovered in 2010)

The first **cyber weapon** for **physical destruction**
developed by USA and Israel governments
Target: **PLC** for centrifuges in **Iran's uranium enrichment plant**
Although its infection is spread via internet, P2P or USB, onset is limited to the target.

PLC was attacked even if **it was isolated from internet**.
Multiple zero-day (unpatched vulnerability) exploits are utilized, so, anti-virus software was useless.

Subspecies of Stuxnet (Variation Increasing)

Target: **Any type of Control System** (not Limited for **PLC**)
Energy , Water supply, Chemical Plant, Transportation, Building, etc.
Many incidents have already been reported.
Even heat control system of a swimming pool was attacked in E.U.

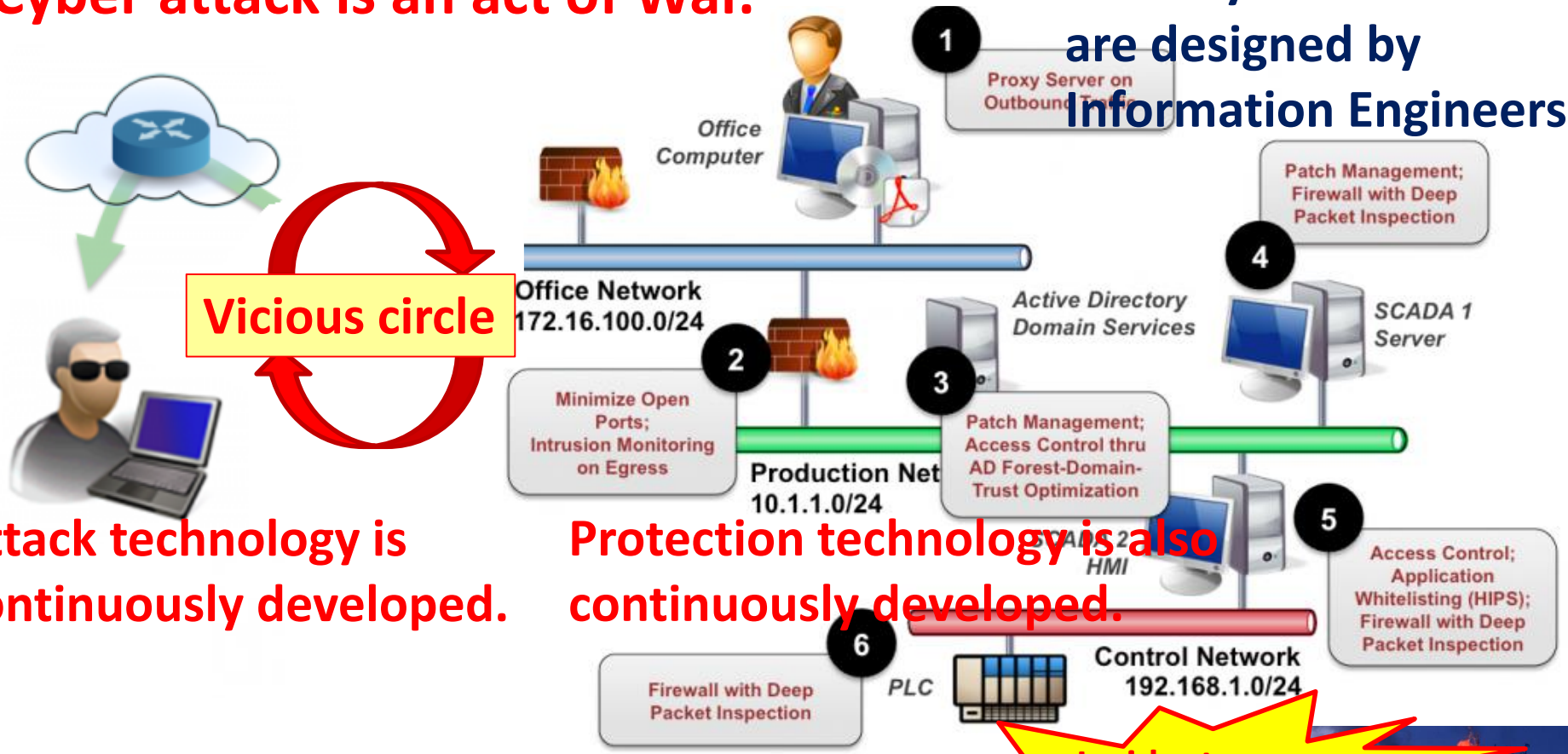
Characteristics: Subspecies of Stuxnet can be developed by **Pranksters, too**.
Plant Location is irrelevant for cyber attacks.

Havex (Malware to steal information from OPC server discovered in 2014)

Development of Cyber security technology becomes Vicious circle.

Cyber attack is an act of War.

Security measures are designed by Information Engineers



Attack technology is continuously developed.

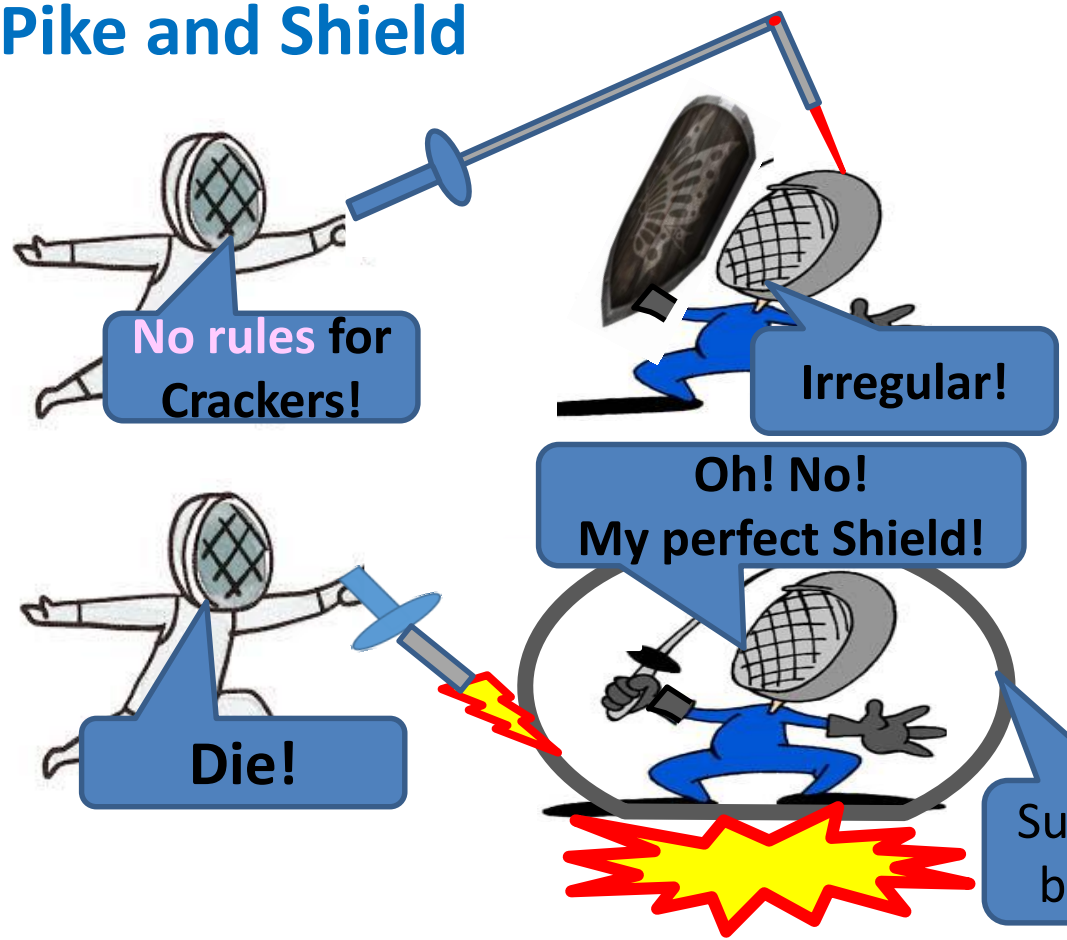
Protection technology is also continuously developed.

http://www.automationworld.com/security/solutions-emerge-prevent-control-system-cyber-attacks(2012/07/14)

If Serious Accidents occurred by attacks using Unknown Vulnerability, do you say "There were No Ways to avoid it." ?

Battle between Hackers and Protectors

Pike and Shield



Who are the protectors?

Cyber-Security is discussed by Information Engineers.

However, Safety was the matter of Plant Engineers.

How can Plant Engineers and Information Engineers collaborate to maintain Safety against cyber-attacks?

Security Measures Focusing on Safety

Maintain **Safety** even if the attacker used **unknown vulnerability**!
What kinds of measures can be applied to this field?

Firewall

Terminal

Business Server

Gateway

SCADA

Data Server

OPC Server

PLC S-7-300

Sensor

Valve

Controller

Information Engineers' Field

Plant Engineers' Field

Office Network

Production Network

Control Network

Cyber-Attacks can be regarded as "**Malicious** Controller Failures and **Malicious** Miss-Operation"

- Cyber-attackers can directly manipulate physical items only via controllers.
- If the information on the HMI of SCADA was tampered, Operators might cause Miss-Judge or Miss-Operation.

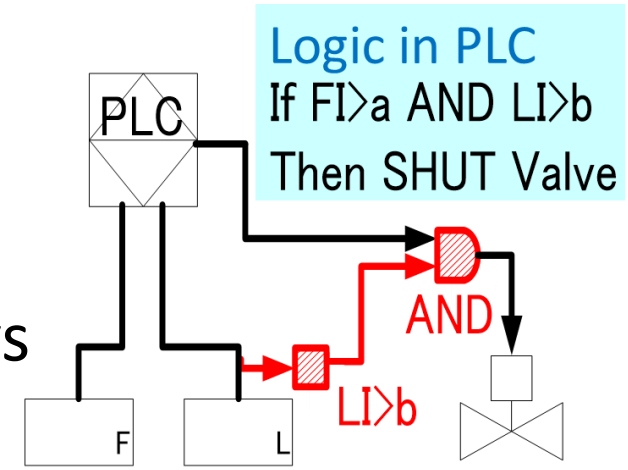
Measures against

Unknown types of Cyber-attacks

1) To adopt **Unintelligent** systems.

Analog communication and Relays

2) To design **Fail-Safe and Fool-Proof** thoroughly



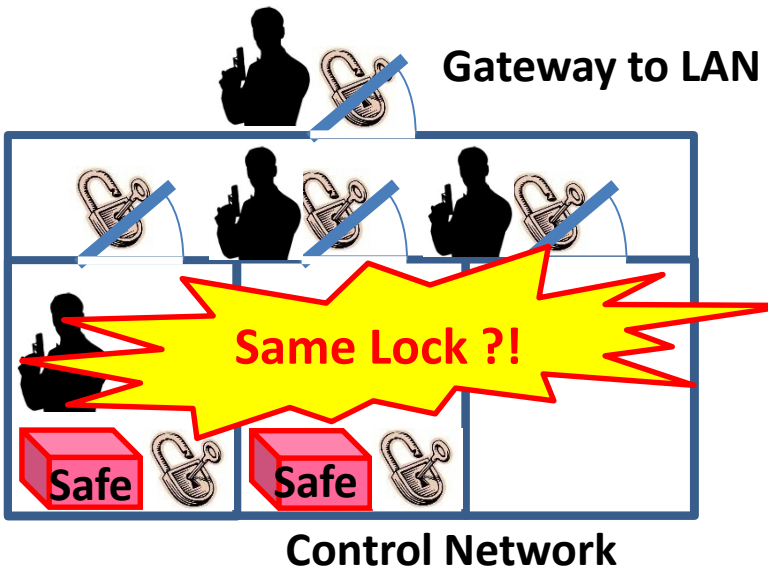
Analog Signal & Relays
don't suffer Cyber attacks.

Heterogeneous Multiplex Multilayer Measures

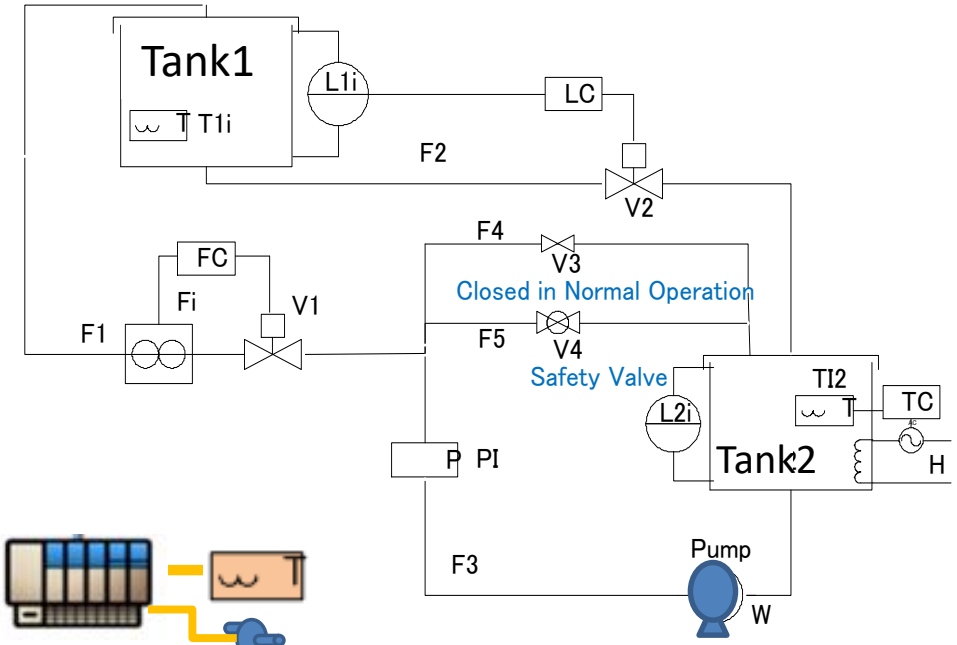
- **In Safety Analysis, Single failure** is usually assumed.
- Even if the same parts are utilized, the failure rate can be reduced to the 2nd power.
- **In Cyber-attacks**, **Multiple Multi-types attacks might occur at Multi-places Simultaneously**.
- Vulnerability might appear in application, protocol, operation system and so on **in future**.
- **Variation** is necessary in the Cyber-Security Measures.

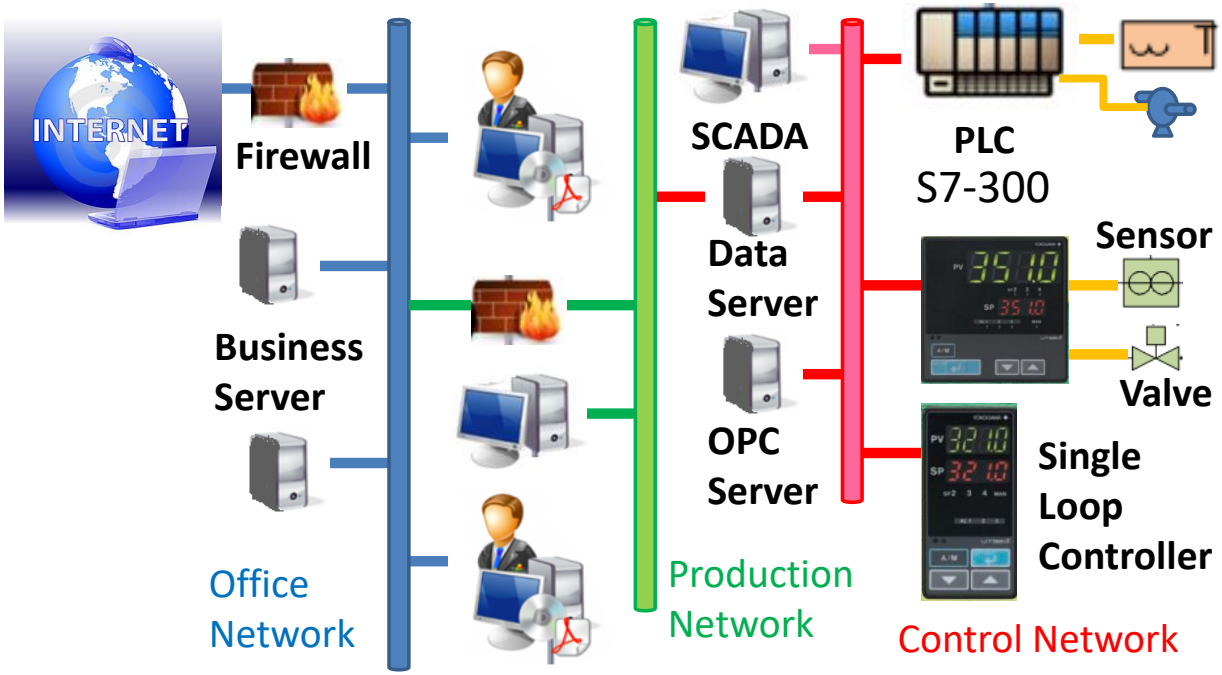
Before whole system loses control,
Detect attack and Maintain Safety!

- **What must be protected in the saves in Control Networks?**



Test bed in Nagoya Inst. of Tech.

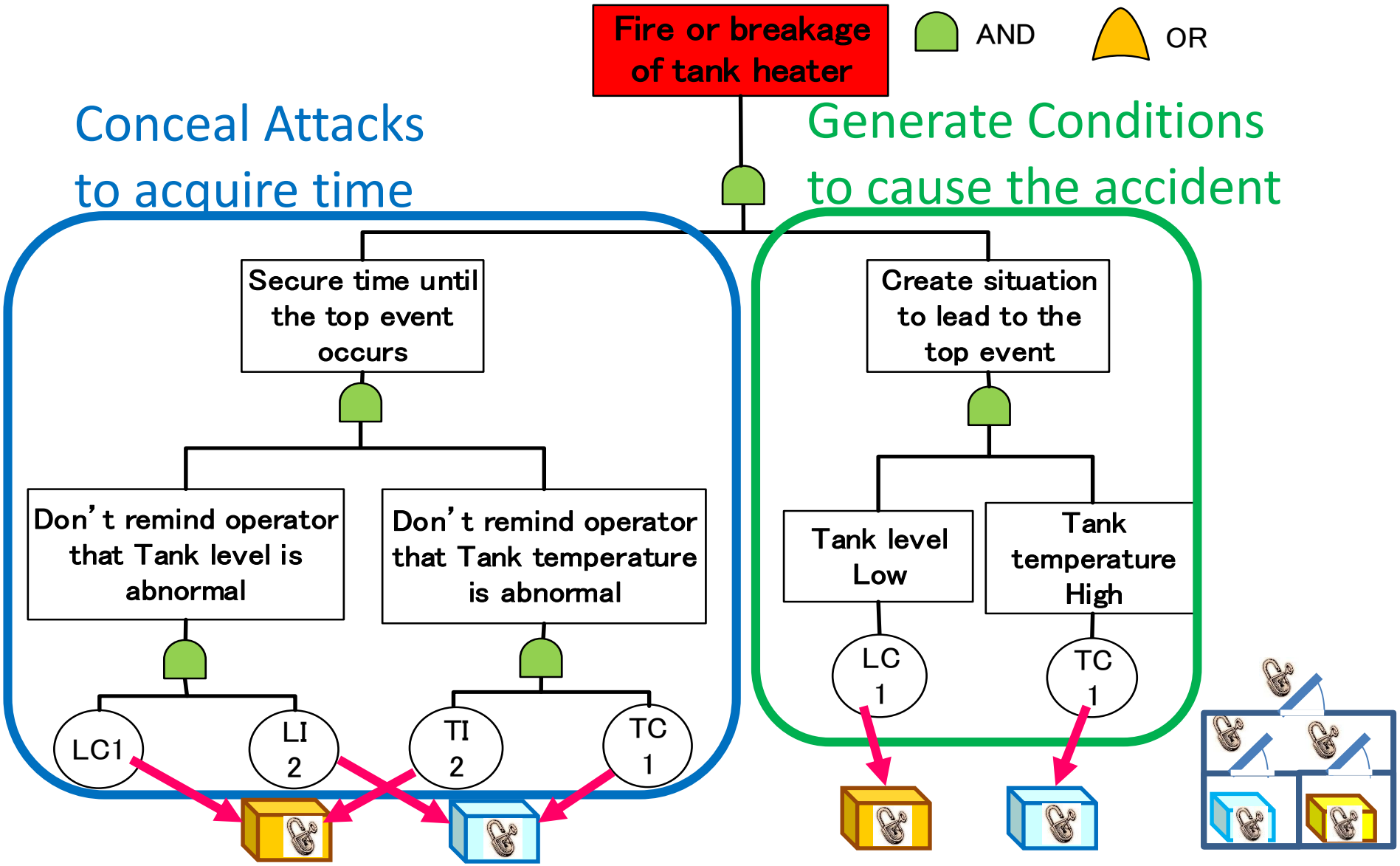




Yokogawa and Siemens Controllers are available.

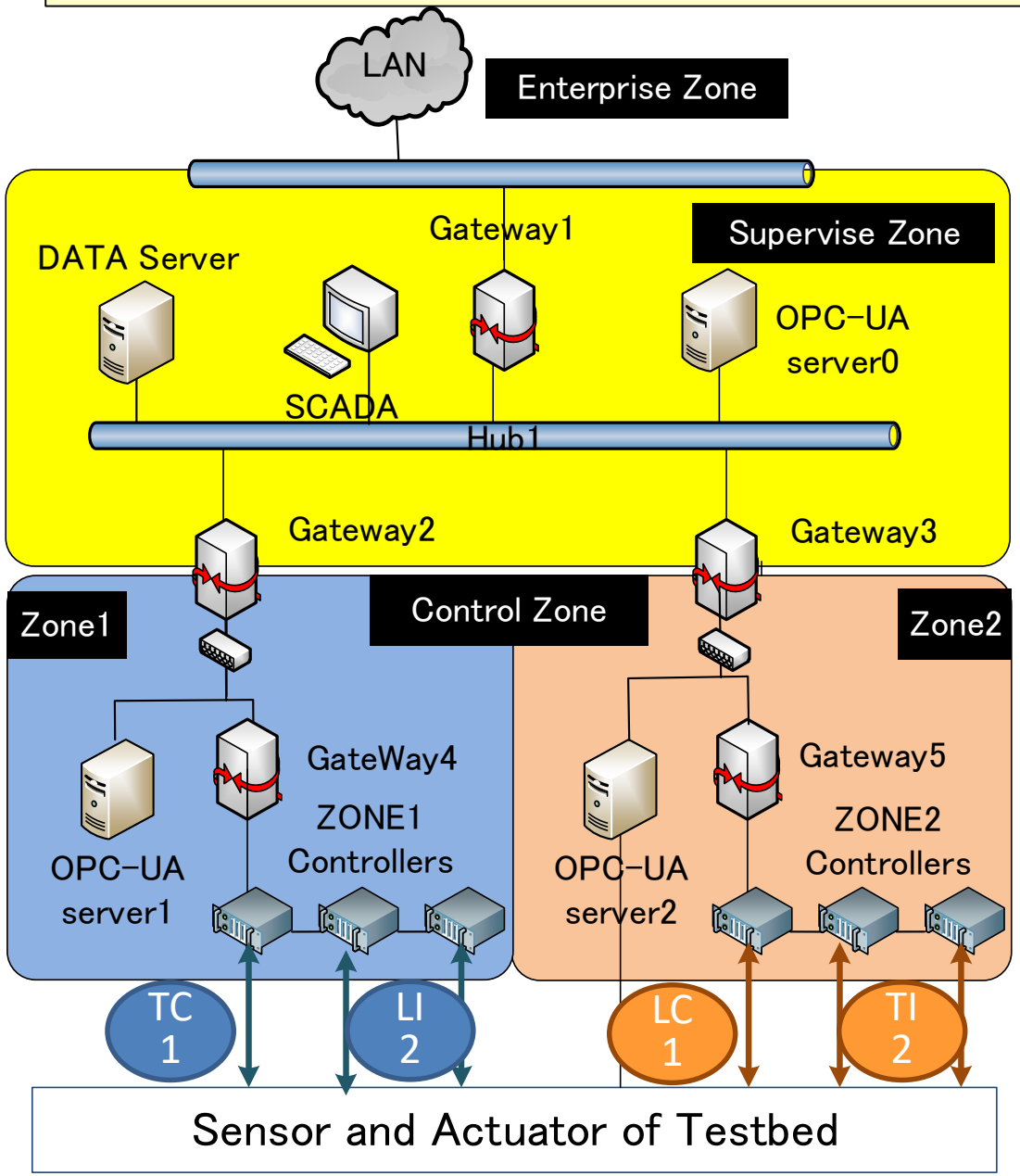
Network structures can be modified.

Fault Tree Analysis for Cyber-Security



Before whole system loses control, Detect attack and Maintain Safety!

Zone Division of Control Network



Controller Data are collected by **OPC-UA server** 1 and 2 in each zone.

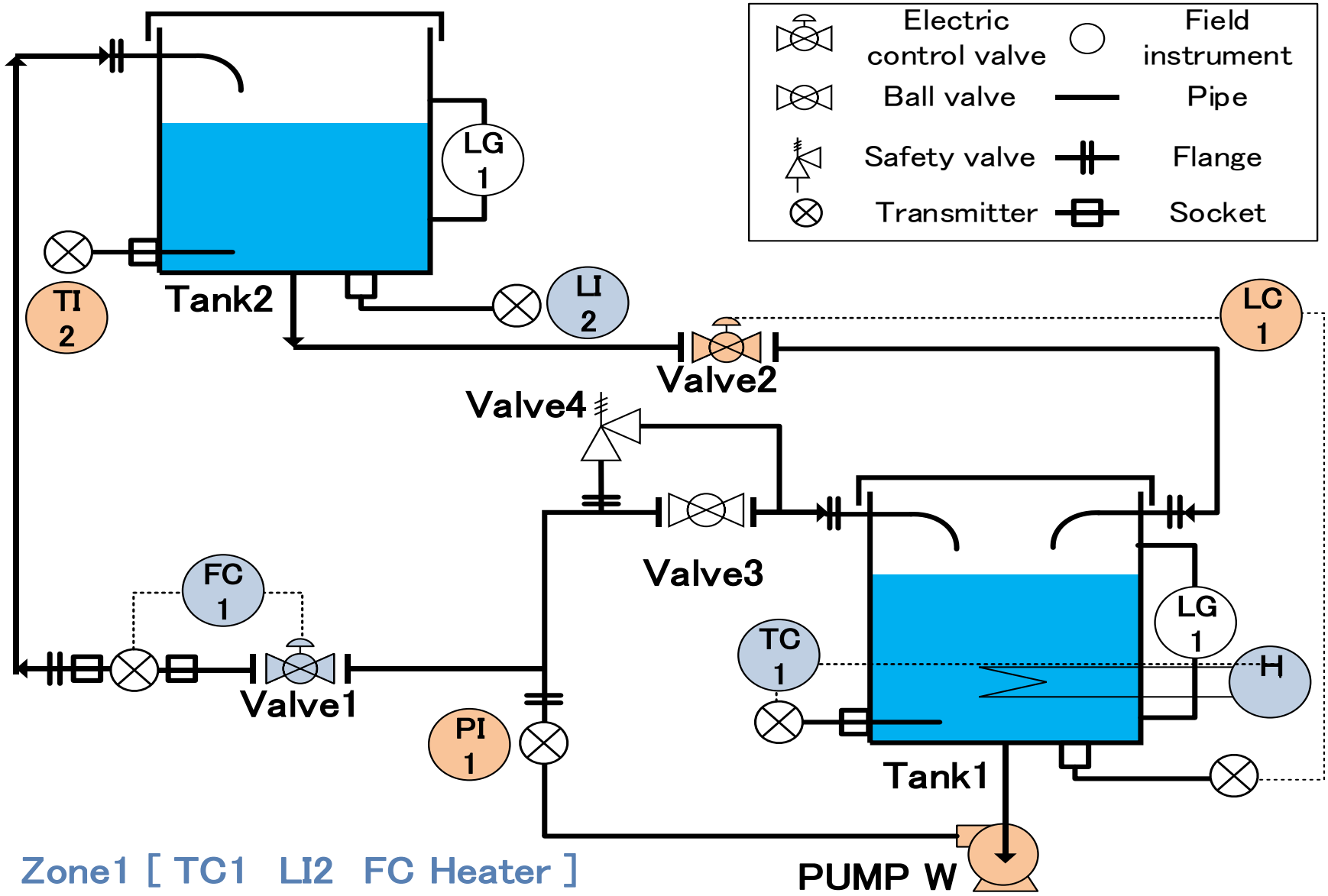
OPC-UA server0 gathers the data.

SCADA communicate with OPC-UA server0.

All of three OPC-UA servers Contains all tags and Communicate all data.

Zone division might be able to be executed in the instrument room.

Zone Division of Instruments



Zone1 [TC1 LI2 FC Heater]

Zone2 [LC1 TI2 PI Pump]

Design of Zone division

- Zone division for Cyber-Security must be discussed based on the properties of the Plant.

  (1) Fault Trees of all serious accidents must be generated.

  (2) Propagation of every malicious operation under concealment must be considered,

- For selection of Security tools (corresponding to Lock, Security camera, gate keeper, patrol and etc.) knowledge of information technology is necessary.

  (a) It must be avoided that
  all measures have the same vulnerability,
  even if it is unknown one.

- Corporation of Plant Engineers and Information ones are essential.

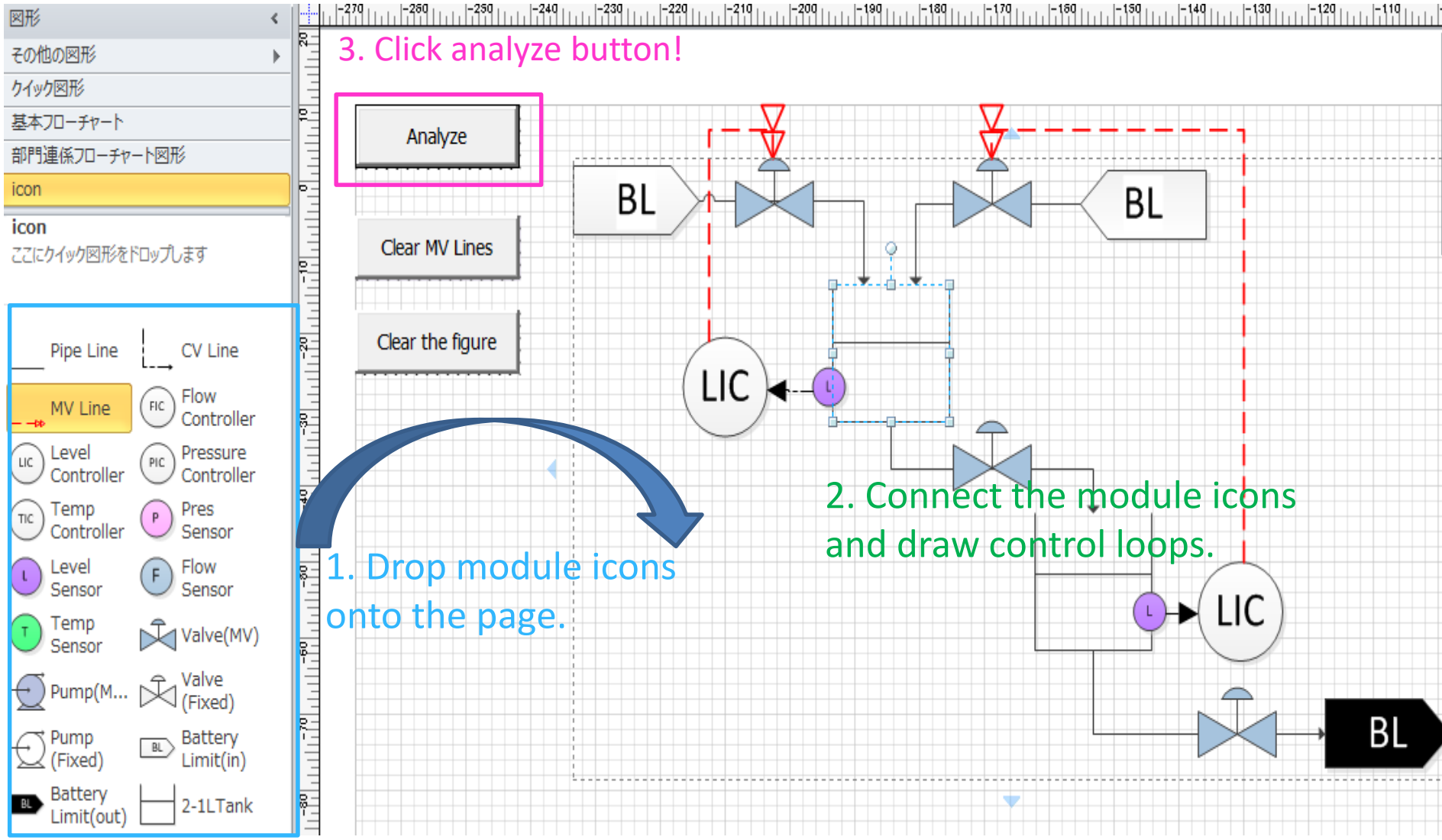
CAD for Zone dividing

- In some industrial plants, more than 1000 variables such as PV and MV of controllers are managed by one operator.
- There are huge number of options of zone dividing of controllers and sensors.
- The relationships among controllers and sensors can be expressed as DAE (Differential and Algebraic Equations).
- The equations are registered in CAD for Process Design

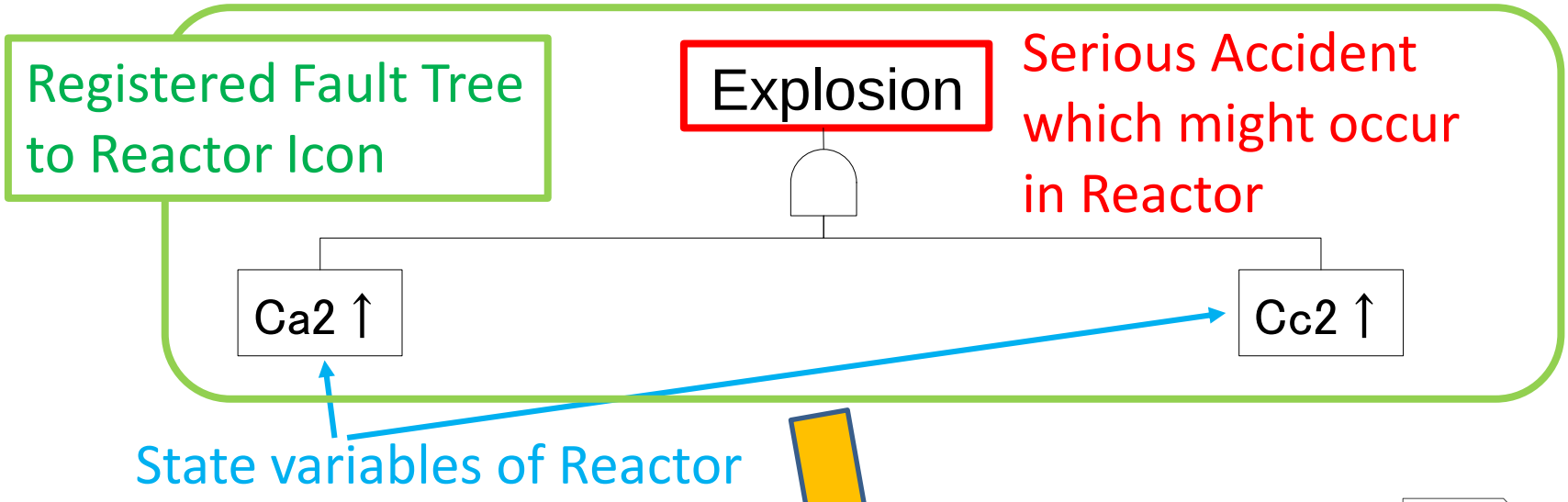
Development of CAD for Zone dividing

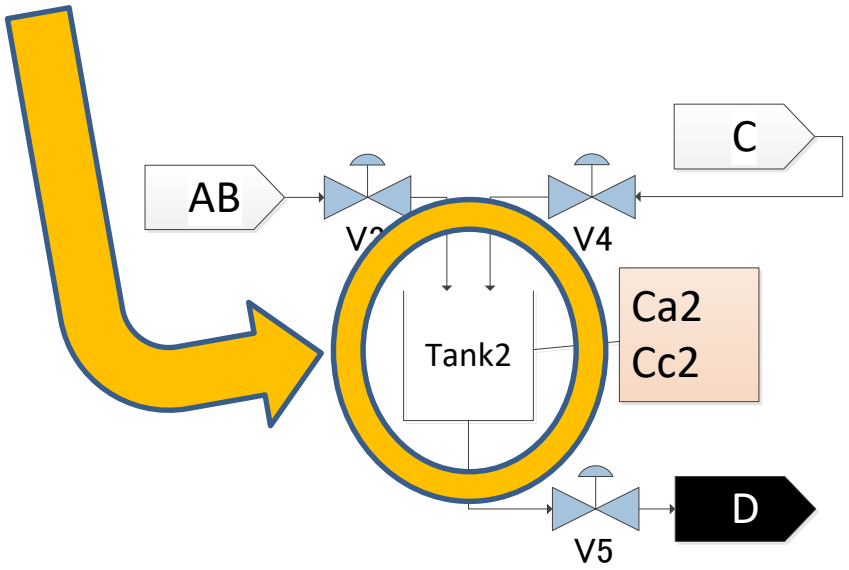
- CAD to generate Fault Tree for Zone Diving
- CAD for Zone Diving to detect operation under concealment

CAD to generate Fault Tree



Registration of Top part of Fault Trees for Equipment Modules

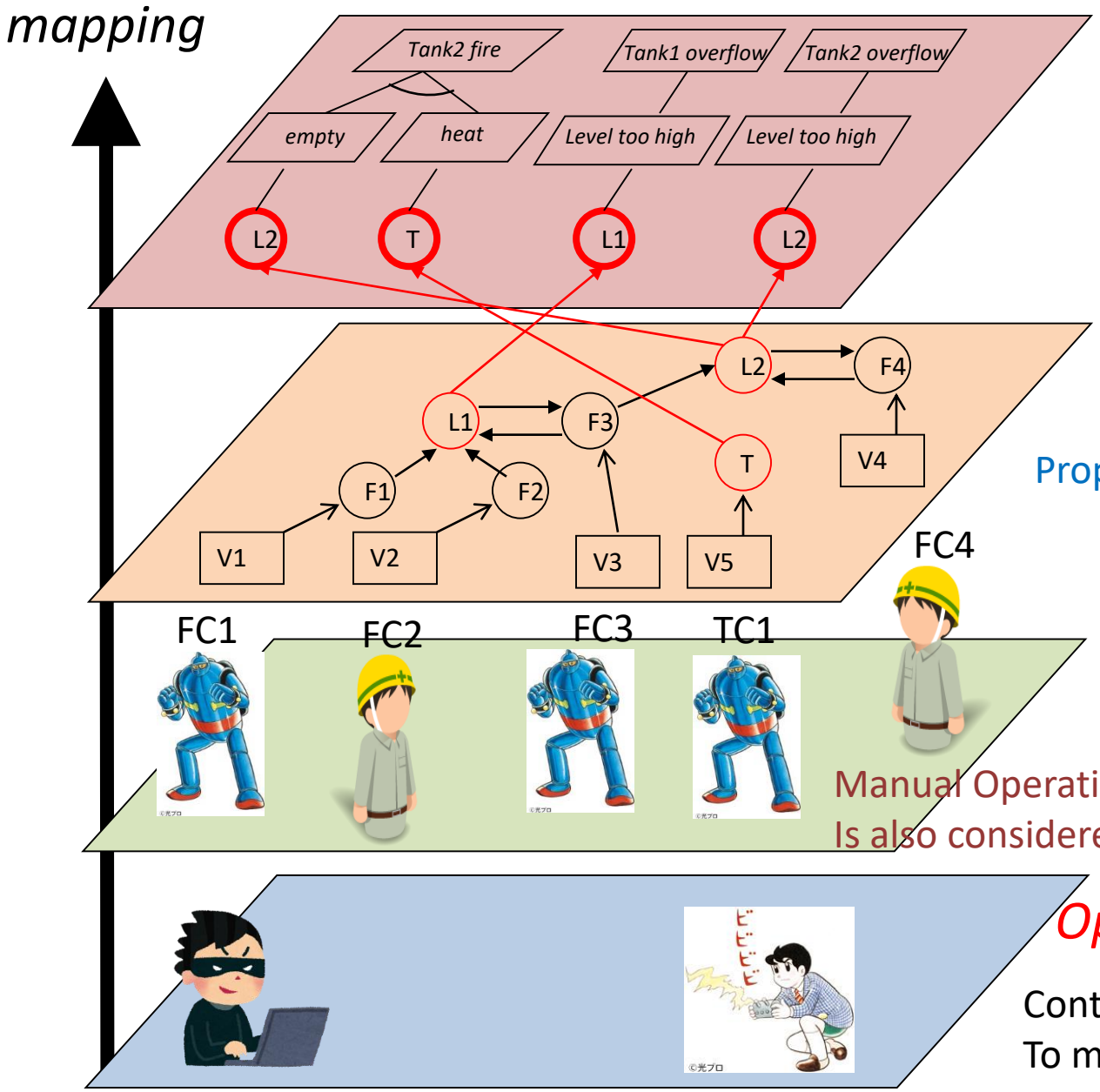




Causes of the **accident** might occur in the **other equipment**.

Propagation of the changes from Causes can be calculated by CAD.

Structure of Accidents caused by Cyber-Attacks



fault tree of safety

State to cause Accidents

cause-effect model

Propagation of State transition

Attacked controllers

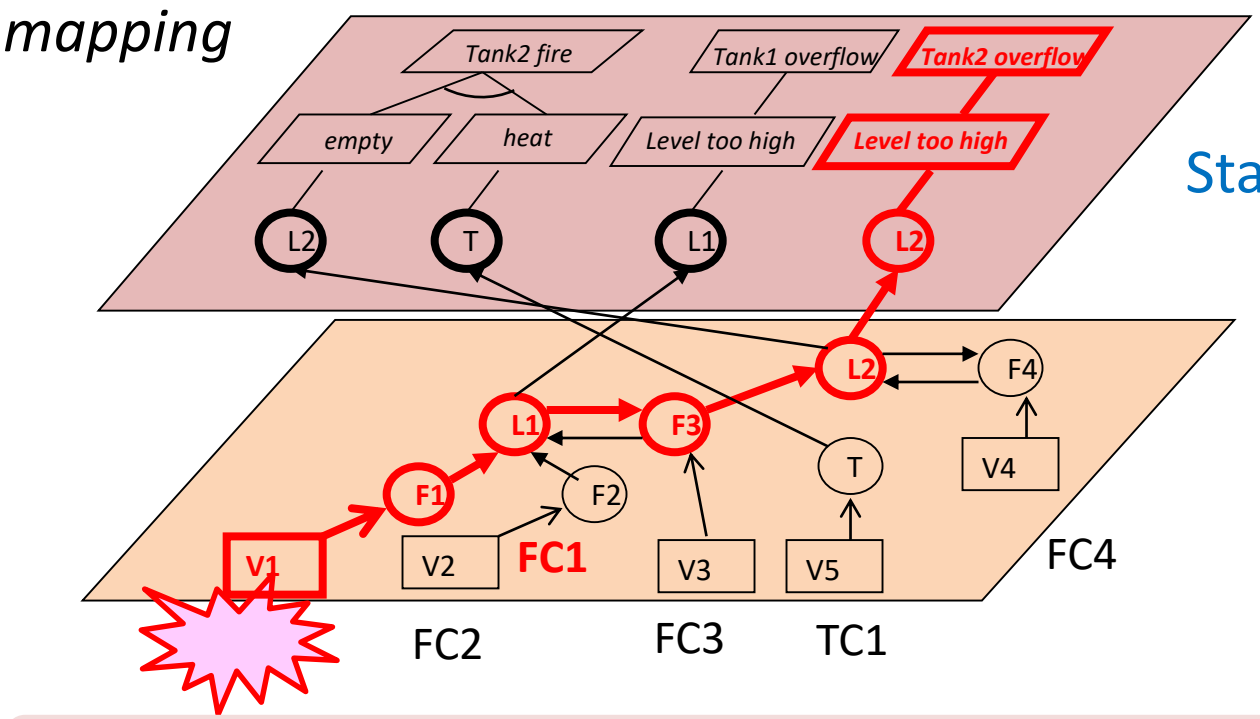
Malicious Manipulation
And Concealment

Manual Operation
Is also considered as Controller Acton.

Operating or Attacking

Controller can be manipulated
To make plant unsafe.

Cause controller search according to the transition path



fault tree of safety

State to cause Accidents

cause-effect model

Propagation of State transition

The cause might occur in other plant far from the Accident

Approach to CAD

Register DAE（Differential Algebraic Equation) to each Equipment module.

From the Combined Equations for the whole plant, qualitative model to calculate state transition is generated.

Application Example

e.g. Tank with Heater system

Differential Equation

$$\frac{dL_1}{dt} = \frac{F_a - F_b}{A_1}$$

$$\frac{dT_1}{dt} = \frac{F_a * (T_a - T_1) + H}{A_1 * L_1}$$

Algebraic Equation

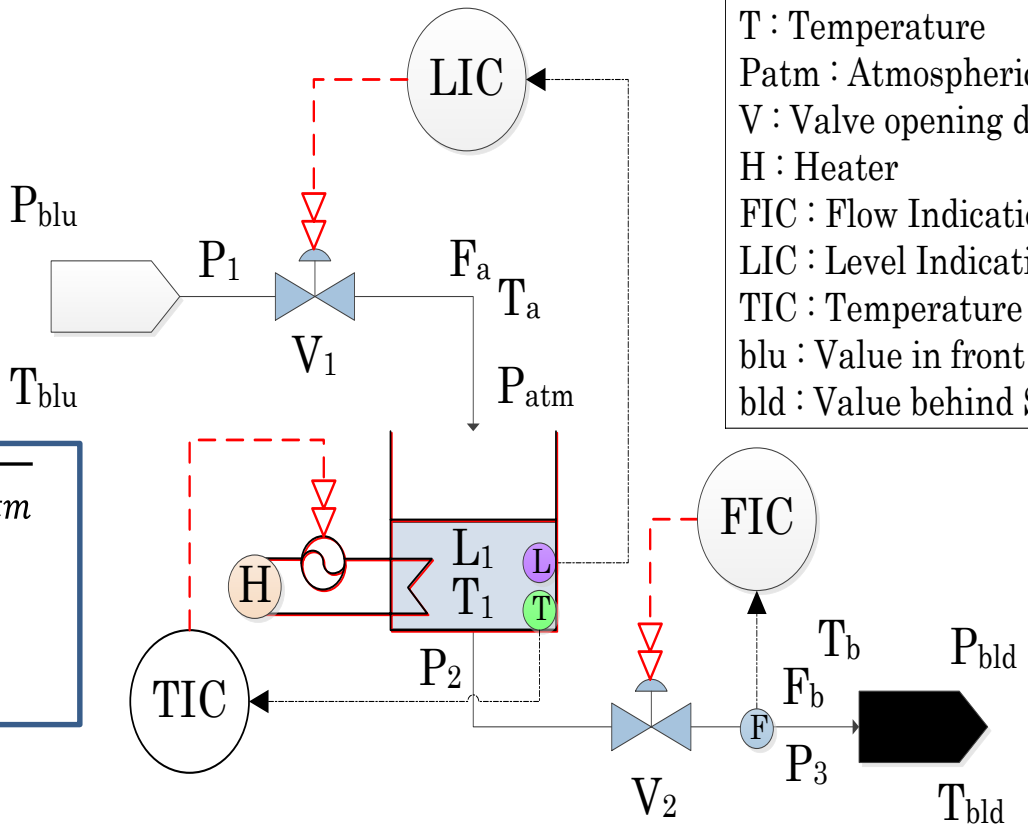
$$0 = F_a - k_1 * V_1 * \sqrt{P_1 - P_{atm}}$$

$$0 = F_b - k_2 * V_2 * \sqrt{P_2 - P_3}$$

$$0 = P_2 - (P_{atm} + \alpha * L_1)$$

$$0 = T_1 - T_b$$

F : Flow rate
P : Pressure
L : Tank's level
T : Temperature
Patm : Atmospheric pressure
V : Valve opening degree
H : Heater
FIC : Flow Indication Controller
LIC : Level Indication Controller
TIC : Temperature Indication Controller
blu : Value in front of System
bld : Value behind System

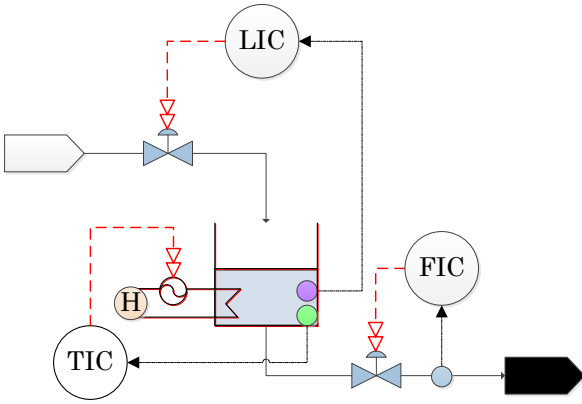


Example of Fault Tree generated with proposed CAD

Top Event :

Over Heat of Tank

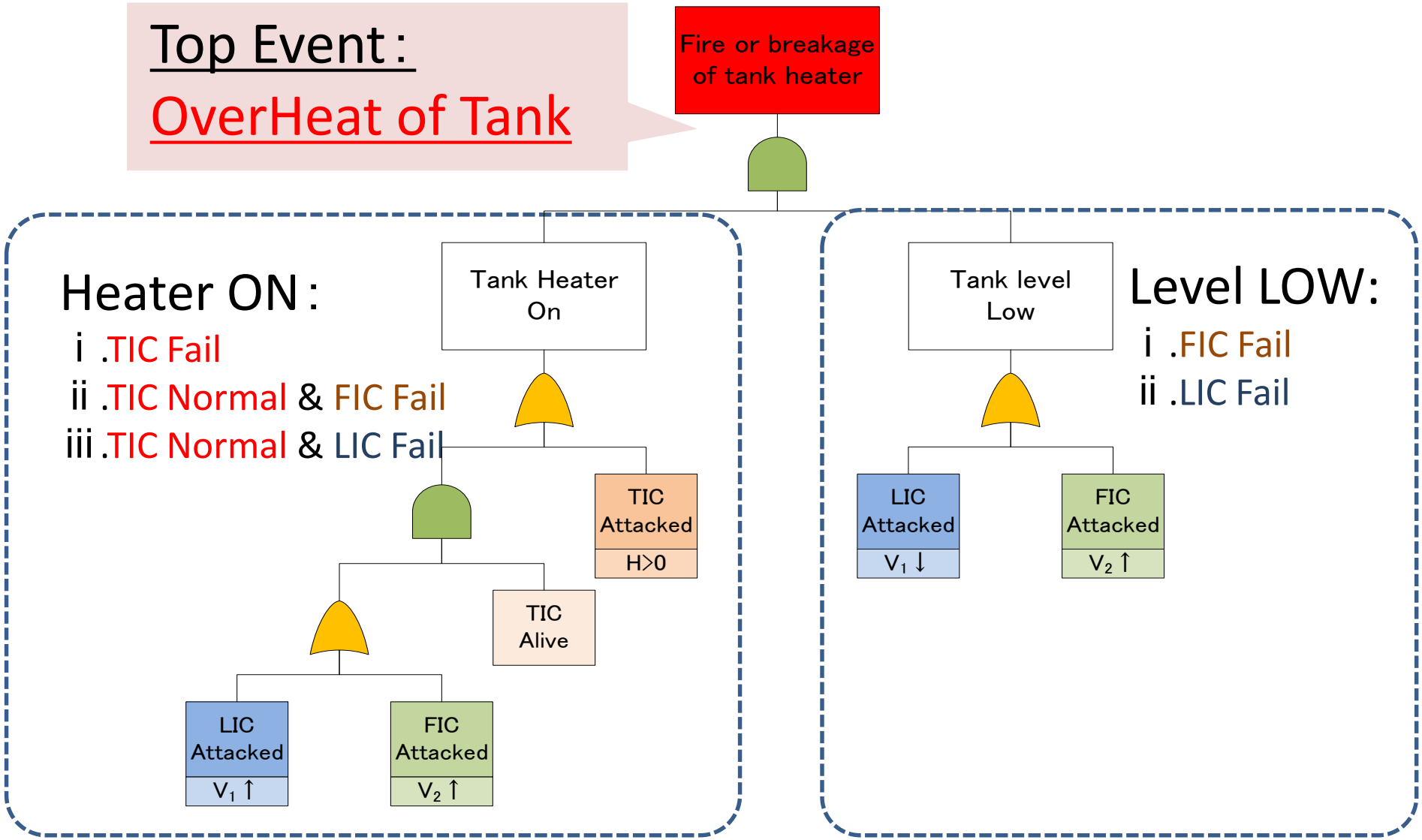
【Heater ON】
&【Level LOW】



Scenario of Accident caused by Attacks to Controllers

Top Event :

OverHeat of Tank



Expansion of Fault Tree in searching Controller Failures

Cyber-Security Measures based on Fault Tree

Find the Pair of Controllers of AND conditions in Fault Tree.

To maintain Safety against Cyber-Attacks

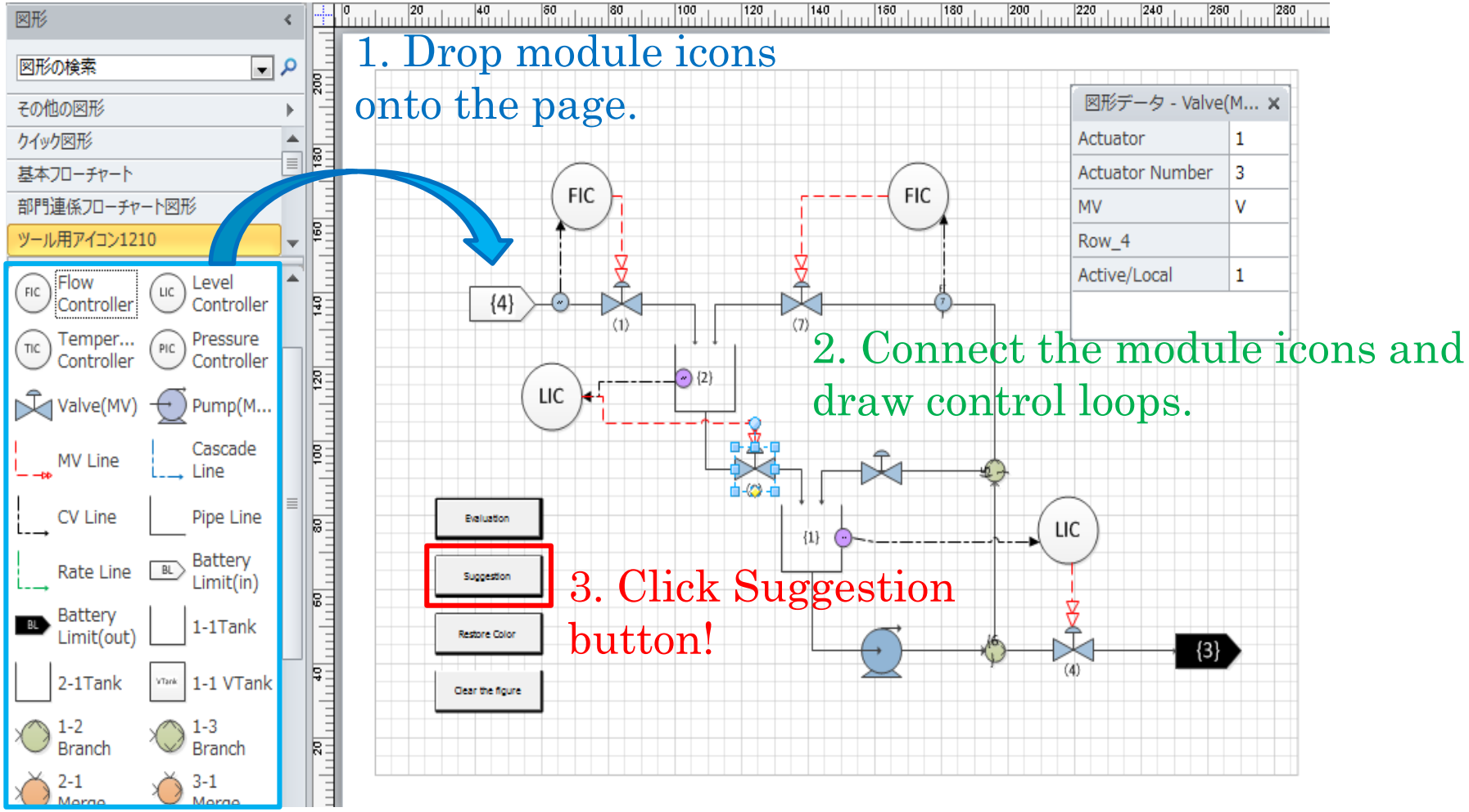
- Protect the Controllers in AND conditions using Cyber-Security Measures Not to be defeated Simultaneously.

(Approach 1)
The Controllers should be contained in different network zones
And the zones should be protected with different security tools.

(Approach 2)
Controllers should be improved to deny Unsafe commands from Cyber-Attackers.

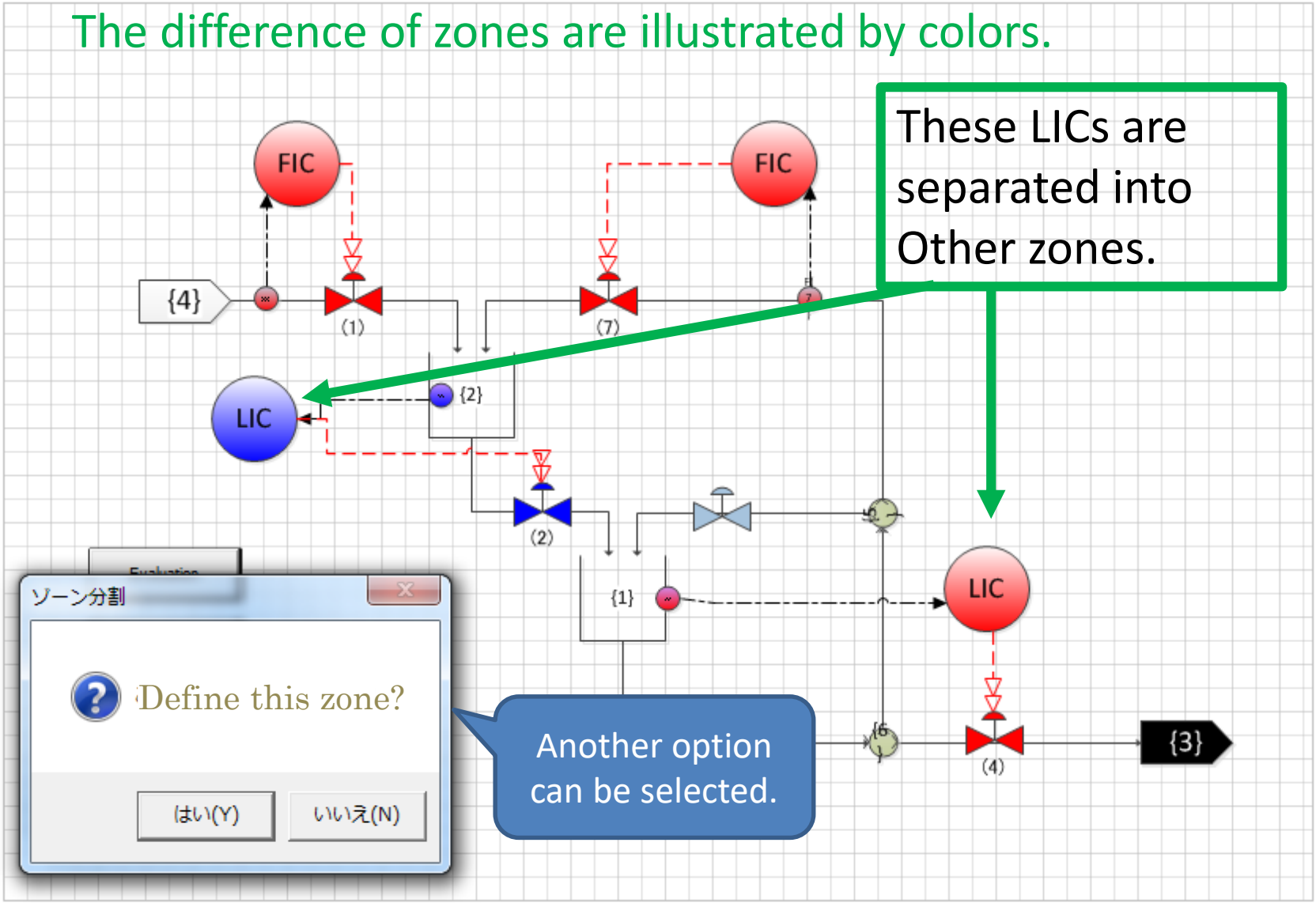
CAD for Zone Dividing to Detect Operation under Concealment

- By crucifixion the module, and to set up a connection, it is possible to design Zone Division



Zone Division obtained by CAD

The difference of zones are illustrated by colors.



P-matrix(CE matrix to express Process behavior)

Cyber-Attacks

might be Manipulated and Concealed

might be Modified or Concealed

P	Process Variables				Manipulated Variables					Disturbance variable		Observed Variables									
	L1{1}	L1{2}	F(1)	F(7)	V(1)	V(2)	W(3)	V(4)	V(7)	Patm	Pbl	L1{2} i	L1{1} i	F(1) i	F(7) i	V(1) i	V(2) i	W(3) i	V(4) i	V(7) i
L1{1}	1	1	0	1						1	1	0	0	0	0					
L1{2}	0	1	1	1							0	0	0	0	0					
F(1)	0	0	1	0	1						1	0	0	0	0					
F(7)	1	0	0	1							1	0	0	0	0					
V(1)	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V(2)	0	0	0	0			0	0	0	0	0	0	0	0	0	0	0	0	0	0
W(								0	0	0	0	0	0	0	0	0	0	0	0	0
V(									0	0	0	0	0	0	0	0	0	0	0	0
V(									1	0	0	0	0	0	0	0	0	0	0	0
Pa									0	1	0	0	0	0	0	0	0	0	0	0
Pbl	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
L1{2} i	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
L1{1} i	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
F(1) i	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
F(7) i	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
V(1) i	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
V(2) i	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
W(3) i	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
V(4) i	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
V(7) i	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Real Values

Can be Faked

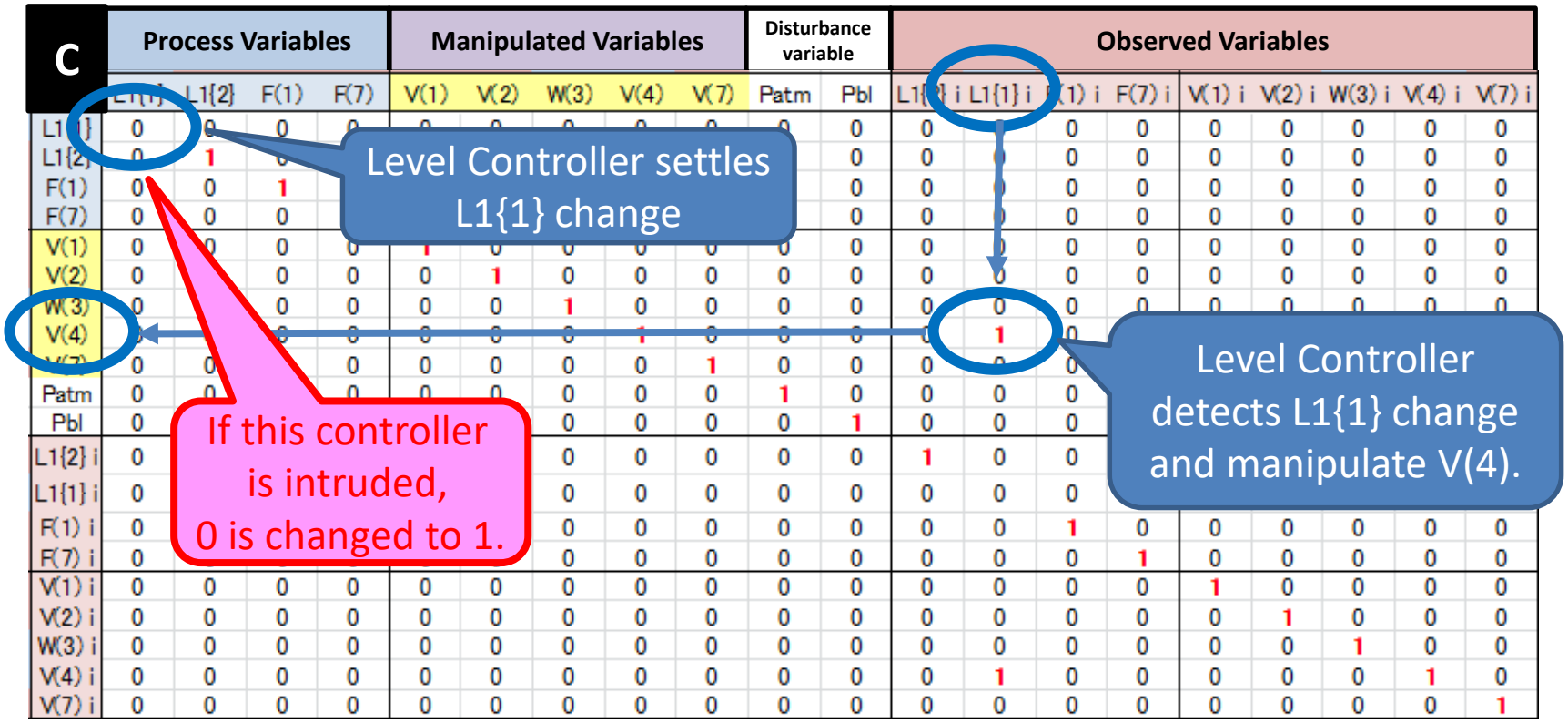
Valve V(1) affects Flow F(1)

Columns:Causes Rows:Effects

C-matrix (Controller's behavior)

Example: Level Controller detects L1{1} change and manipulate V(4).
By the controller L1{1} is settled.

If the controller was intruded, C-matrix was changed.
L1{1} change could not be settled.



Zone division affects the layout of '1's in C-matrix.

O-matrix (Observation might be faked by cyber-attacks)
Expression of Concealment by Cyber-Attackers

Real Values

O	Process Variables				Manipulated Variables					Disturbance variable		Observed Variables								
	L1{1}	L1{2}	F(1)	F(7)	V(1)	V(2)	W(3)	V(4)	V(7)	Patm	Pbl	L1{2} i	L1{1} i	F(1) i	F(7) i	V(1) i	V(2) i	W(3) i	V(4) i	V(7) i
L1{1}	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
L1{2}	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
F(1)	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
F(7)	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V(1)	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V(2)	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
W(3)	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
V(4)	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
V(7)	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
Patm	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
Pbl	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
L1{2} i	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
L1{1} i	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
F(1) i	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
F(7) i	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
V(1) i	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
V(2) i	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
W(3) i	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0
V(4) i	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0
V(7) i	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

The changes in intruded zones are concealed by cyber-attackers.

Observed Values

Expression of Cyber-Attacks to Zones

M-matrix(Remote-Manipulation to the Intruded Zones)

MVs in intruded zones

Mb		2	2
		W(3)	V(4)
2	L1{1}	0	0
1	L1{2}	0	0
1	F(1)	0	0
1	F(7)	0	0
1	V(1)	0	0
1	V(2)	0	0
2	W(3)	1	0
2	V(4)	0	1
1	V(7)	0	0
0	Patm	0	0
0	Pbl	0	0
1	L1{2} i	0	0
2	L1{1} i	0	0
1	F(1) i	0	0
1	F(7) i	0	0
1	V(1) i	0	0
1	V(2) i	0	0
2	W(3) i	0	0
2	V(4) i	0	0
1	V(7) i	0	0

S-matrix(Observation in Survival Zones)

Sb		2	1	1	1	1	1	2	2	1	0	0	1	2	1	1	1	1	2	2	1
		L1{1}	L1{2}	F(1)	F(7)	V(1)	V(2)	W(3)	V(4)	V(7)	Patm	Pbl	L1{2} i	L1{1} i	F(1) i	F(7) i	V(1) i	V(2) i	W(3) i	V(4) i	V(7) i
1	L1{2} i	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
1	F(1) i	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
1	F(7) i	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
1	V(1) i	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
1	V(2) i	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
1	V(7) i	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

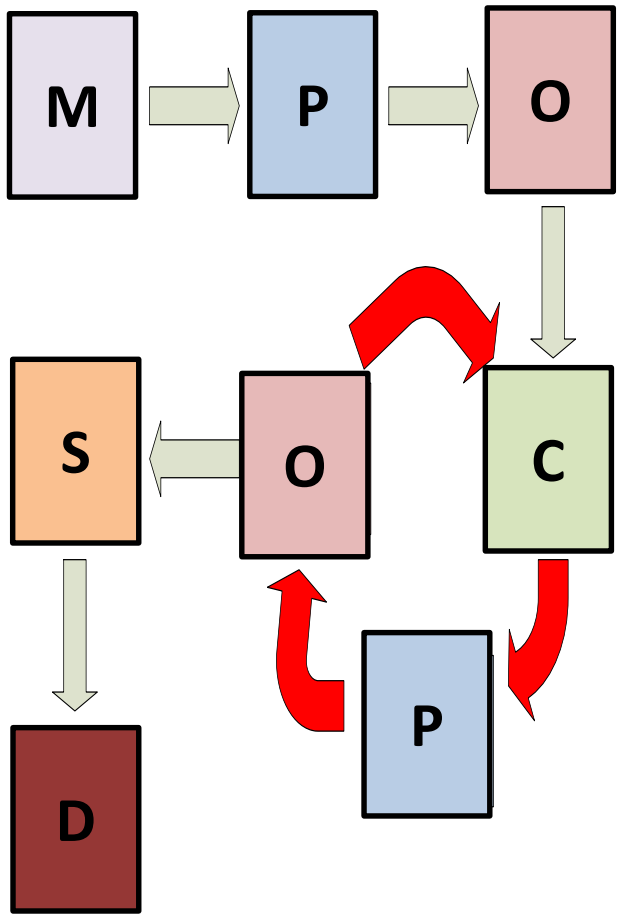
PVs in survival zones

Detectability of Cyber-Attacks

When Zone division is assumed,

C, O, M and S matrices can be generated.

The detectability of remote-operation under concealment by cyber-attackers can be calculated as follows.



- Detectability Matrix

$$D(m)=\sum_{k=1}^{m} S * (O * P * C)^{k-1} * O * P * M$$

The columns are remote-manipulation in intruded zones and
the rows are observation in survival zones.

Detectability changes according to Zone Division

- The elements show the Detectability of Cyber-attacks in the zones.

- If L1{1} and L1{2} is the same zone, it can not be detected.

Dam		1	1	1
		V(2)	V(4)	V(7)
2	F1(1) i	0	0	0
2	V(1) i	0	0	0
2	W(3) i	0	0	0

Undetectable

Dbm		2	2
		V(1)	W(3)
1	L1{2} i	2	0
1	L1{1} i	0	2
1	F(7) i	0	2
1	V(2) i	0	0
1	V(4) i	0	2
1	V(7) i	0	2

- If L1{1} and L1{2} is a separate zone, it can be detected.

Dam		1	1	1
		V(1)	V(2)	V(7)
2	L1{1} i	3	2	2
2	W(3) i	0	0	0
2	V(4) i	0	2	3

Dbm		2	2
		W(3)	V(4)
1	L1{2} i	0	0
1	F(1) i	0	0
1	F(7) i	1	1
1	V(1) i	0	0
1	V(2) i	0	0
1	V(7) i	0	0

CAD generates many options of zone diving and checks detectability automatically. Zone dividing to detect cyber-attack is selected from the options.

How should Security Measures be proposed?

It is not necessary to explain the necessity.
Please propose adequate cyber-security measures for our plants.

If the measures would be expensive, my boss would complain "There are many risks besides cyber-security!"

Wonderful! Let's do it!

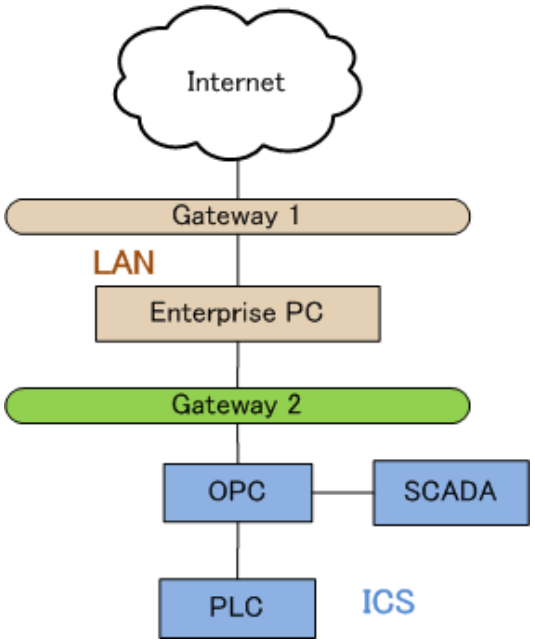
I want to say it. But, what information should I get to say so?

I want to hear it. But, what information should I give to hear it?

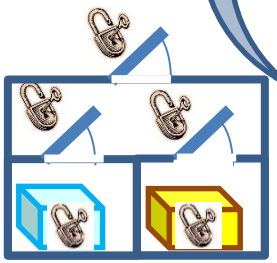
Design Approach of Cyber-Security Systems

1. **Fault Tree** Analysis for Zone Diving
2. **Attack Route** Analysis to Essential Controllers
3. Select Security tools to satisfy the required SAL using **SAL Assessment Table** for each attack route
4. Make **Scenarios** of Incidents or Accidents based on the Alarm of detection systems
5. Plan the **Operators' actions** to maintain safety at the hypothetical incidents
6. Return to Stage 3 until Cost and Effects of measures are **compromised**.

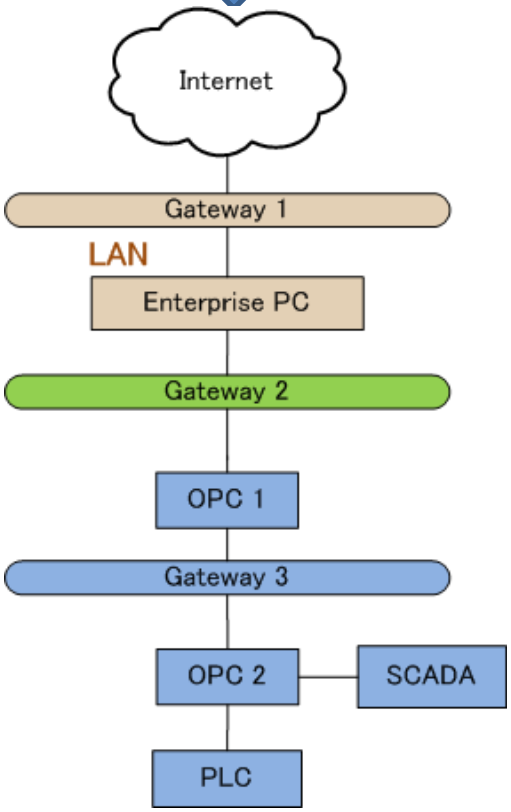
Protection I: Configuration Design for Safety Improvement



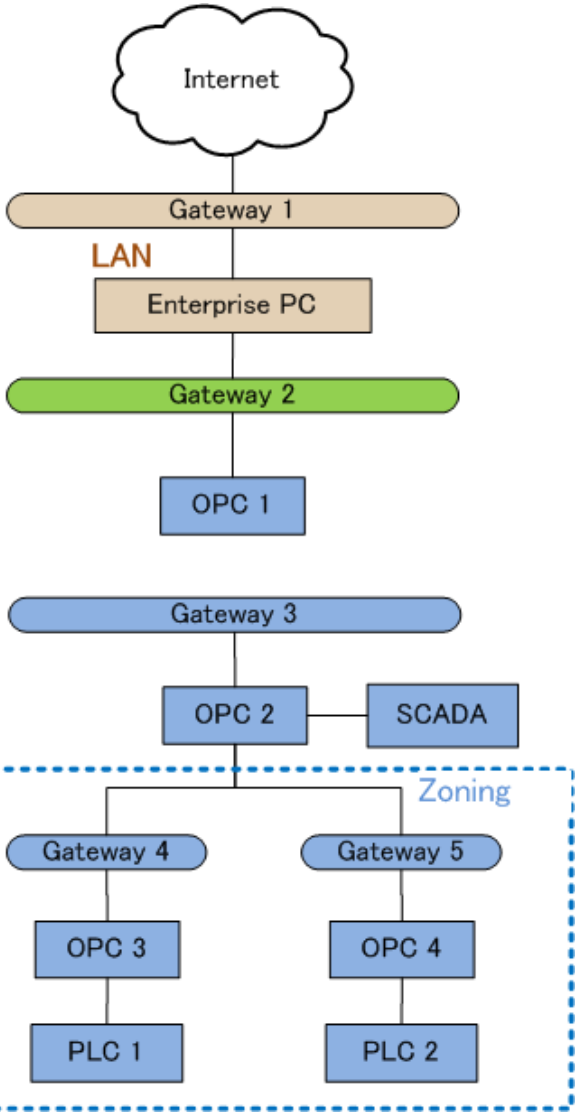
(a) Original ICS



Hazard Analysis



(b) Multi-layer protection in ICS



(c) Zone divided in ICS

Analysis Based on Intrusion Pathways

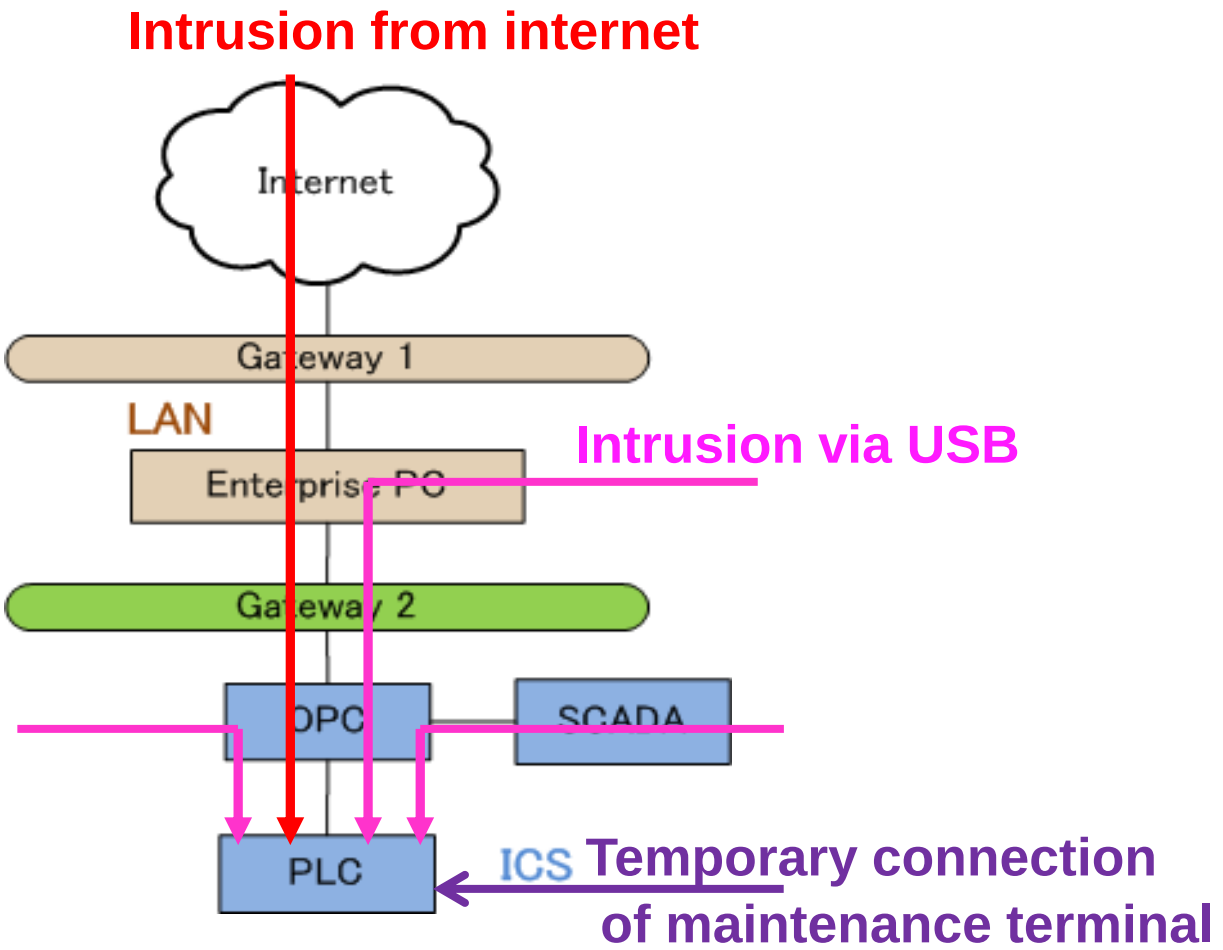


Fig. 3 Intrusion pathways in Original ICS

All pathways must be secure for SCI security

Protection II: Selecting Measures Against Cyber-attacks in ICS

In this research, the 7 foundational requirements has been utilized [6]. They are defined in ISA 99. 01. 01, which is the standard to evaluate the cyber-security of ICS.

FR (Foundational Requirements)

- Access control (AC)
- Use control (UC)
- Data Integrity (DI)
- Data confidentiality (DC)
- Restrict data flow (RDF)
- Timely response to an event (TRE)
- Resource availability (RA)

Requrements for SAL(Security Assurance Level)

SAL1: Protection against casual or coincidental violation
SAL2: Protection against intentional violation using simple means
SAL3: Protection against intentional violation using sophisticated means
SAL4: Protection against intentional violation using sophisticated means with extended resources

(AC) Access control
(UC) Use control
(DI) Data integrity
(DC) Data confidentiality
(RDF) Restrict data flow
(TRF) Timely response to an event
(RA) , Resource availability(RA)

SAL	AC-SAL
1	Identify and authenticate IACS users by mechanisms which protect against casual or coincidental access by unauthorized entities.
2	Identify and authenticate IACS users by mechanisms which protect against intentional unauthorized access by entities using simple means.
3	Identify and authenticate IACS users by mechanisms which protect against intentional unauthorized access by entities using sophisticated means.
4	Identify and authenticate IACS users by mechanisms which protect against intentional unauthorized access by entities using sophisticated means with extended resources.

SAL	UC-SAL
1	Restrict use of the system or assets according to specified privileges to protect against casual or coincidental misuse.
2	Restrict use of the system or assets according to specified privileges to protect against circumvention by entities using simple means.
3	Restrict use of the system or assets according to specified privileges to protect against circumvention by entities using sophisticated means.
4	Restrict use of the system or assets according to specified privileges to protect against circumvention by entities using sophisticated means with extended resources.

SAL	DI-SAL
1	Protect the integrity of information in the system against casual or coincidental manipulation.
2	Protect the integrity of information in the system against manipulation by someone using simple means.
3	Protect the integrity of information in the system against manipulation by someone using sophisticated means.
4	Protect the integrity of information in the system against manipulation by someone using sophisticated means with extended resources.

SAL	DC-SAL
1	Prevent the dissemination of information via eavesdropping or casual exposure.
2	Prevent the dissemination of information to an entity actively searching for it using simple means.
3	Prevent the dissemination of information to an entity actively searching for it using sophisticated means.
4	Prevent the dissemination of information to an entity actively searching for it using sophisticated means with extended resources.

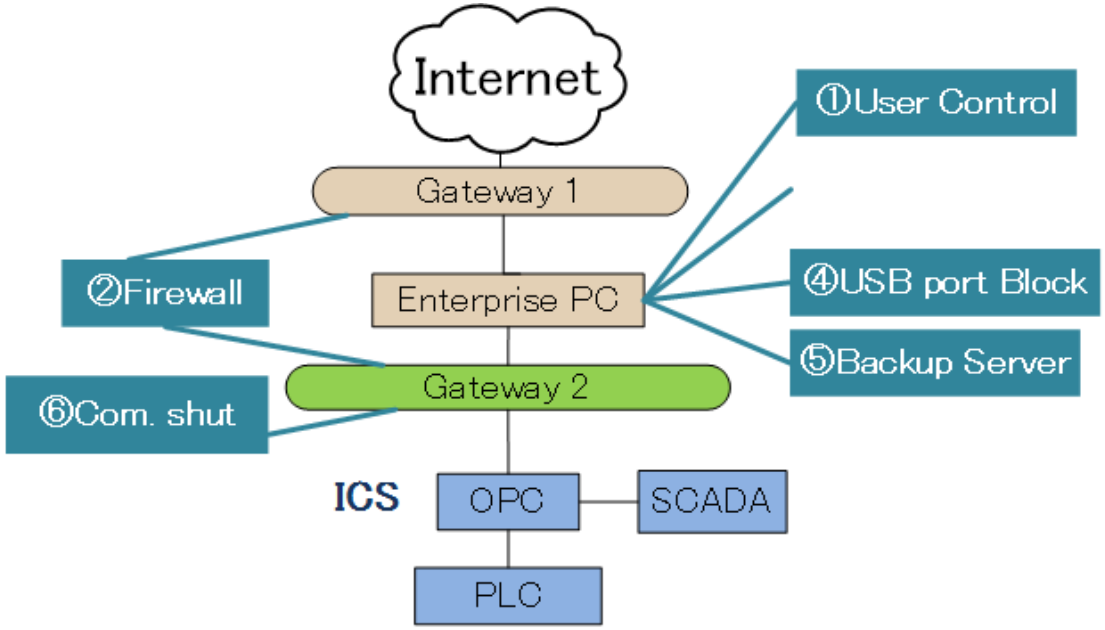
SAL	RDF-SAL
1	Prevent the casual or coincidental circumvention of zone and conduit segmentation systems.
2	Prevent the intended circumvention of zone and conduit segmentation systems by entities using simple means.
3	Prevent the intended circumvention of zone and conduit segmentation systems by entities using sophisticated means.
4	Prevent the intended circumvention of zone and conduit segmentation systems by entities using sophisticated means with extended resources.

SAL	TRE-SAL
1	Monitor the operation of the system and respond to incidents when they are discovered by providing the forensic evidence when queried.
2	Monitor the operation of the system and respond to incidents when they are discovered by actively collecting forensic evidence from the system.
3	Monitor the operation of the system and respond to incidents when they are discovered by actively pushing forensic evidence to the proper authority.
4	Monitor the operation of the system and respond to incidents when they are discovered by actively pushing forensic evidence to the proper authority in near real-time.

SAL	RA-SAL
1	Ensure that the system operates reliably under normal production conditions and prevents denial-of-service situations caused by the casual or coincidental actions of an entity.
2	Ensure that the system operates reliably under normal and abnormal production conditions and prevents denial-of-service situations by entities using simple means.
3	Ensure that the system operates reliably under normal, abnormal, and extreme production conditions and prevents denial-of-service situations by entities using sophisticated means.
4	Ensure that the system operates reliably under normal, abnormal, and extreme production conditions and prevents denial-of-service situations by entities using sophisticated means with extended resources.

Protection II: Selecting Measures Against Cyber-attacks in ICS

Because any tools are not almighty, combination of measures is necessary.



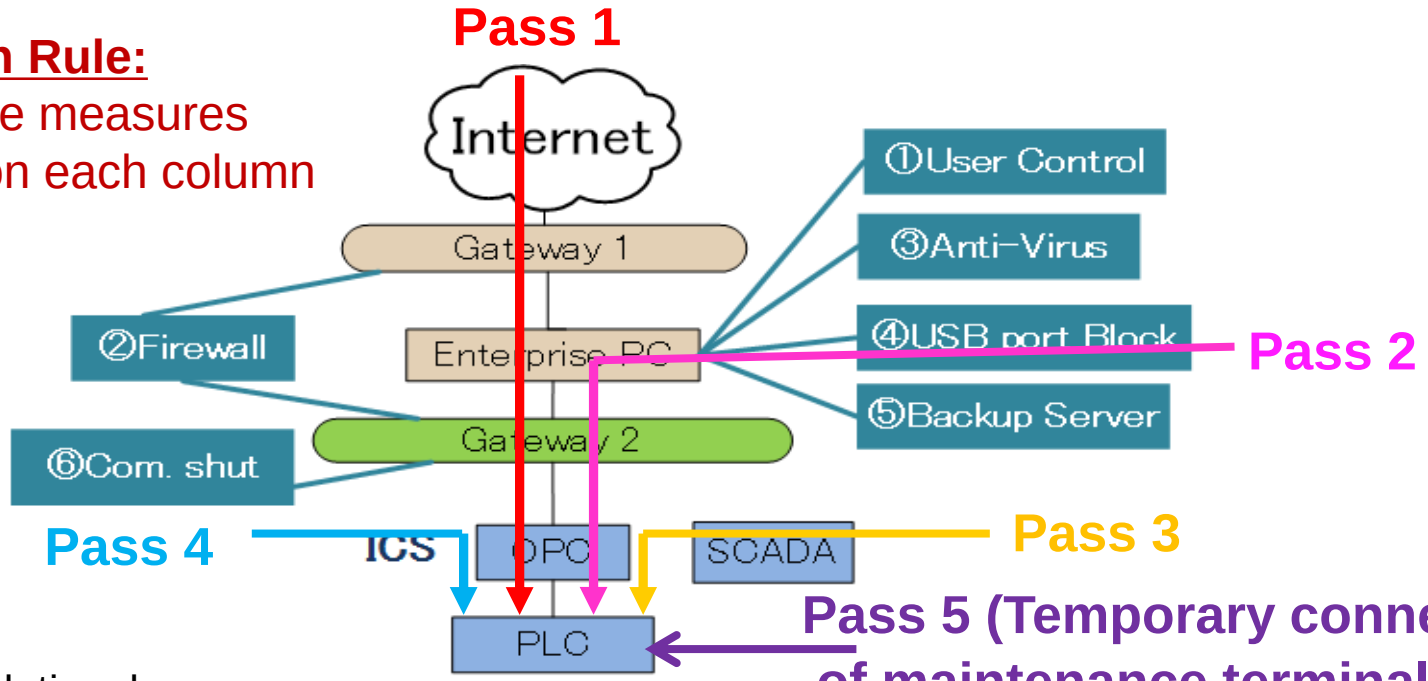
Type of Tools and Location must be selected.

The evaluation of security tools based on foundational requirements

	AC-SAL	UC-SAL	DI-SAL	DC-SAL	RDF-SAL	TRE-SAL	RA-SAL
①User Control	○	○		○			
②Firewall			○	○	○		
③Anti-Virus			○	○		○	
④USB port Block			○	○			
⑤Backup Server						○	○
⑥Com. shut			○	○	○		

Protection II: Selecting Measures Against Cyber-attacks in ICS

Evaluation Rule:
At least one measures must exit on each column (ISA99).



Foundational requirements

Intrusion Pathways

Table 2 Measures setting by intrusion pathways analysis the case of Fig. 3

	AC-SAL	UC-SAL	DI-SAL	DC-SAL	RDF-SAL	TRE-SAL	RA-SAL
Gatway 1			②	②	②		
Enterprise PC	① (④)	①	③, ④	①, ③, ④		③, ⑤	⑤
Gatway 2			②, ⑥	②, ⑥	②, ⑥		
OPC							
SCADA							
PLC							

In this case, all FRs are met, however, because there are no cyber-security measures in ICS, the plant is danger if cyber-attacks from OPC.

Protection II: Selecting Measures Against Cyber-attacks in ICS

The Case of Measures Selection for ICS (i): PLC Safety with Lowest Cost

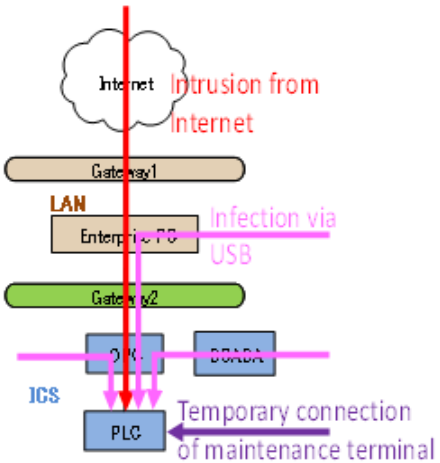


Fig. 3 Intrusion pathways

Table 2 No cyber-security measures in ICS

	AC	UC	DI	DC	RDF	TRE	RA
SCADA							
OPC							
PLC							

Considering the commonality of intrusion pathways, measures are selected from PLC.

	AC	UC	DI	DC	RDF	TRE	RA
SCADA							
OPC							
PLC	①	①		①			⑤

Because the measure applying to PLC is limited, to meet all of the FR, the tools 3 and 6 are set on OPC

	AC	UC	DI	DC	RDF	TRE	RA
SCADA							
OPC			③ ⑥	③ ⑥	⑥	③	
PLC	①	①		①			⑤

Protection II: Measures Against Cyber-attacks in ICS

The Case of Measures Selection for ICS (ii): Suppressing the Damage of Cyber-attacks by Early Detection

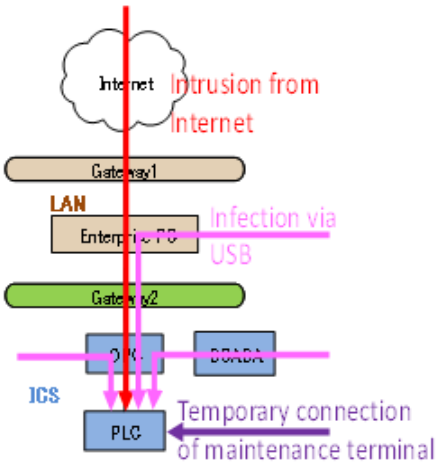


Fig. 3 Intrusion pathways

Table 2 No cyber-security measures in ICS

	AC	UC	DI	DC	RDF	TRE	RA
SCADA							
OPC							
PLC							

For early detection, measures are set from entrance (SCADA).

	AC	UC	DI	DC	RDF	TRE	RA
SCADA	①	①	④	① ④			
OPC							
PLC							

Because the measure applying to SCADA is limited, to meet all of the FR, the tools 3, 6 and 5 are set on OPC

	AC	UC	DI	DC	RDF	TRE	RA
SCADA	①	①	④	① ④			
OPC			③ ⑥	③ ⑥	⑥	③	⑤
PLC							

Protection III: Heterogeneity of Security Tools for Unknown Vulnerability

Even though plural tools were applied, they might be unavailable at once if they are homogenous.

Table 2 Measures setting by intrusion pathways analysis the case of Fig. 3

	AC	UC	DI	DC	RDF	TRE	RA
Gatway 1			②	②	②		
Enterprise PC	①	①	③, ④	①, ③, ④		③, ⑤	⑤
Gatway 2			②, ⑥	②, ⑥	②, ⑥		
OPC							
SCADA							
PLC							

Heterogeneity is important for multi-layer security protection.

Table 5. Heterogeneity check of tools on Pathways of Table 2

	Firewall	DataExProtocol	OS	NetDevice	FileExchange
Gatway 1	CISCO	OSI-PI	CISCO	CISCO	SMB
Enterprise PC	McAfee	OSI-PI, OPC-2.0	Windows 7	Aried	SMB
Gatway 2	Linux	OPC-2.0	CENT-OS	Catalyst	
OPC	Windows	Profi-net, OPC-2.0	Windows XP	Intel	
SCADA	TrendMicro	OPC-2.0	Server 2008	Intel	
PLC		Profi-net		Siemens	

Toward Spread of Security Measures

- A systematic approach to design robust protection systems against cyber-attacks for ICS is neccessary.

- Measure selection table for cyber-security can visualize the performance of measures.
  The types of tools and the location to apply them to can be discussed easily.

The cyber-security measures should be discussed considering possible hazards and budgets.

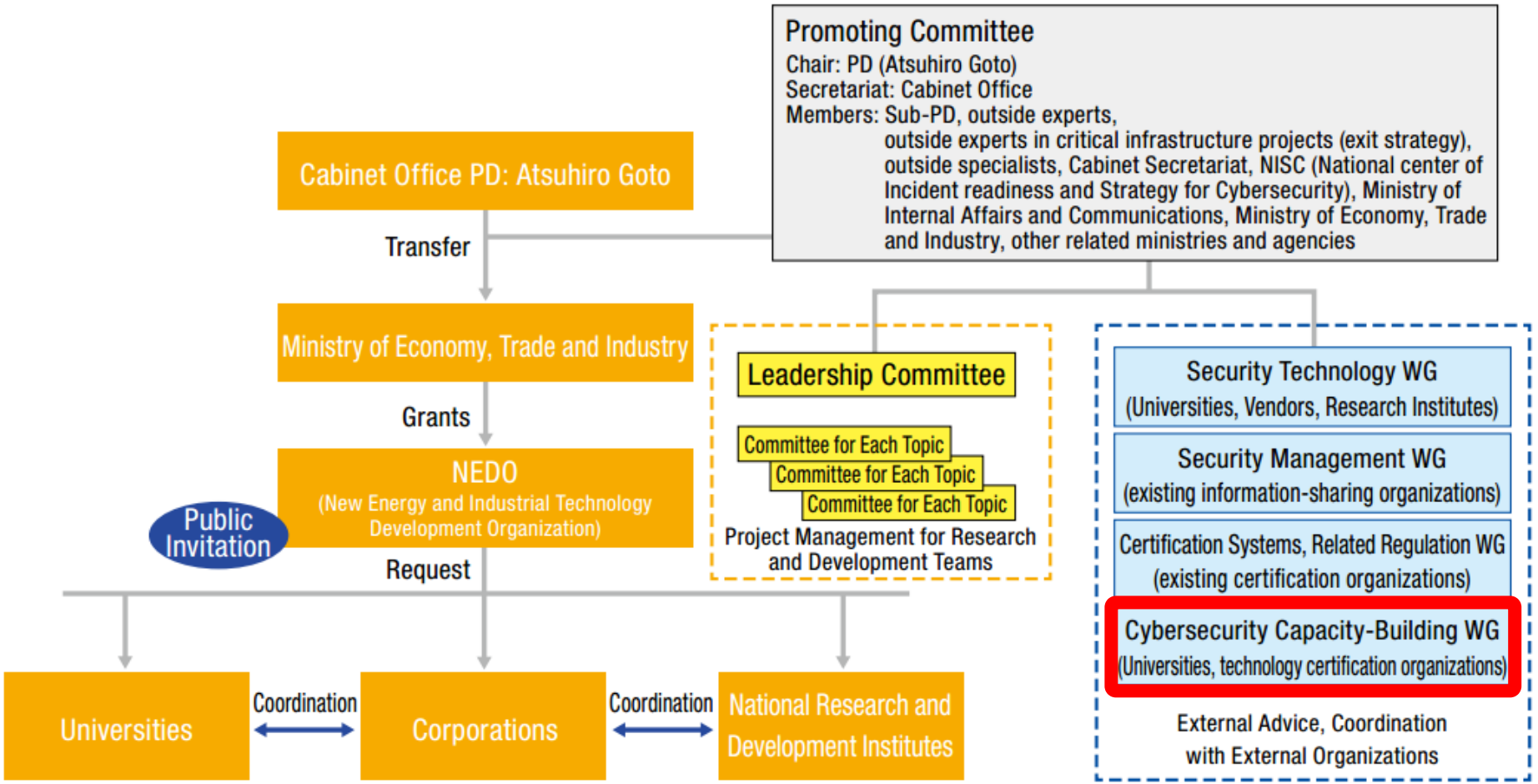
The measures selection tables are very helpful to the discussion between planners and managers.

戦略的イノベーション創造プログラム
Cross-ministerial Strategic Innovation Promotion Program

Pioneering the Future: Japanese Science, Technology and Innovation

One of 11 projects in SIP is "Cyber-Security for Critical Infrastructure"

2015～2019　Budget for 2016：2.5billion Yen



•Implementation Structure

Incident Response

- Make Scenarios based on the Alarm of Measures
  (Intrusion Detection System, Anti-Virus, Honeypot,…)
- Plant Operators' Action to maintain Safety.

(Scenario 1) Accident occurred without Alarms.

(Scenario 1') IDS alarm was detected.

(Scenario 1") Mal-Operation was executed after IDS alarm.

(Scenario 2) Mal-Operation was executed by Malware without Alarms.

(Scenario 2') Malware was detected by Anti-Virus.

How can you estimate the Risk of Serious Accidents?

How can you manage the urgent situation?

How can you maintain safety under the attacked situation?

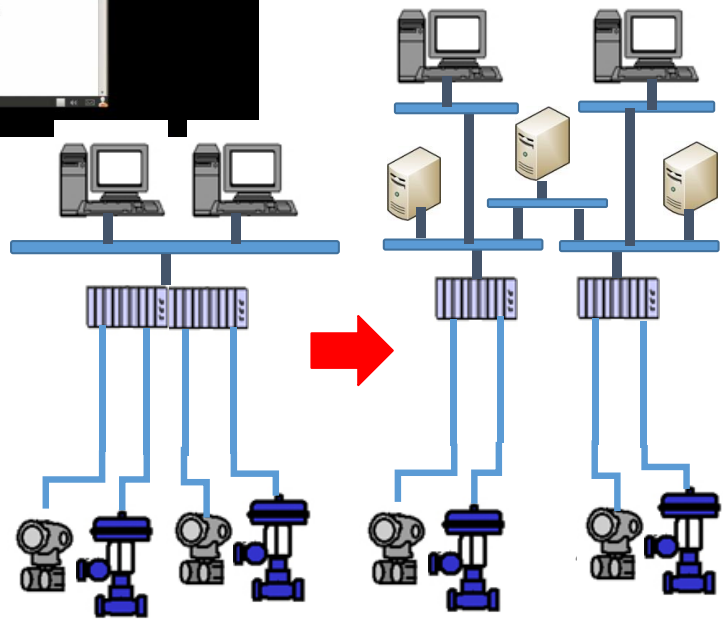
Necessity of Security tools to manage the urgent situation must be imaged.

ICS Security Workshop in Nagoya Inst. Tech. (1)

（1st）March 19,20 in 2015　18 participants from 13 companies
(2nd) August 26,27 in 2015　74 participants from 30 companies
(3rd) March 26,27 in 2016　47 participants from 26 companies
(4th) September 27 in 2016 54 participants from 32 companies

Number of visitors was more than 400 in April 2016

Dividing Control Network into Zones



ICS Security Workshop in Nagoya Inst. Tech. (2)

Security-II (Cyber Security corresponding to Safety-II)

Focusing not only Safety but also BCP/BCM,

training for collaboration in the whole organization (divisions for plant operation, asset, information, sales, management and so on) and outers to measure the cyber-attacks is proposed.

The scenarios are cyber attacks to an energy service company.

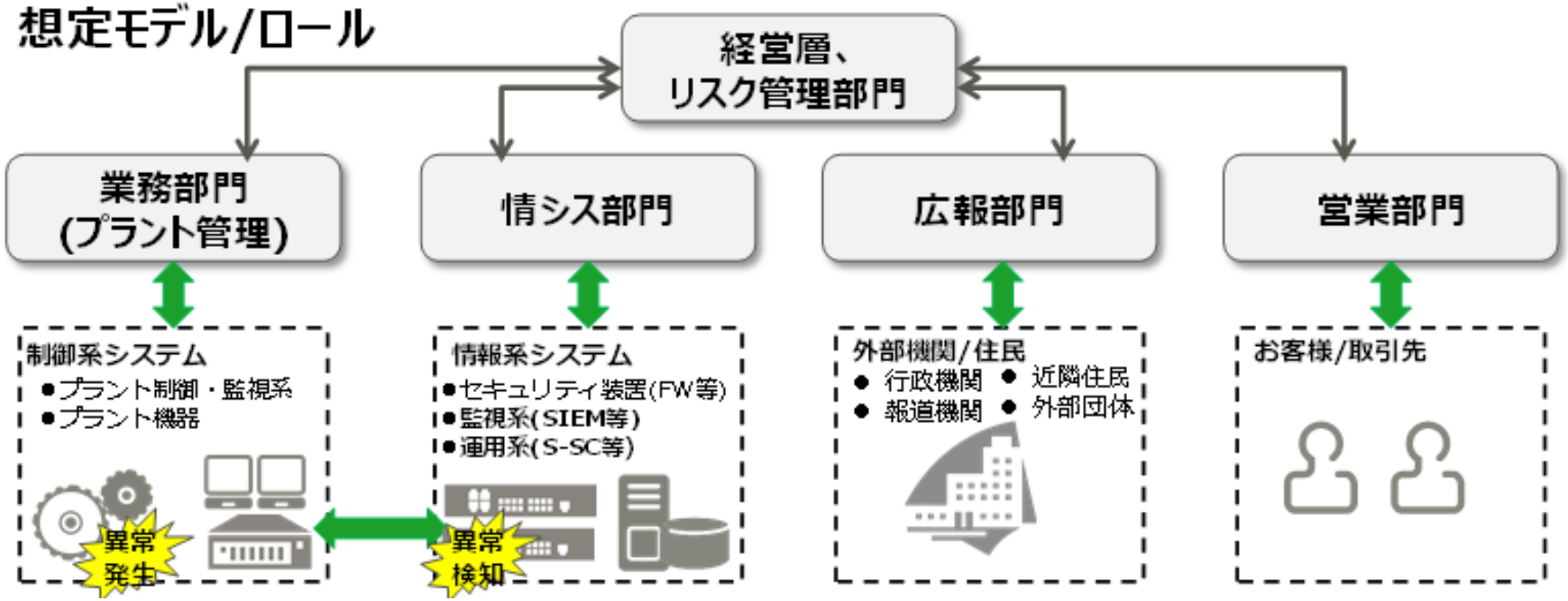
to prevent the diffusion of the damage
and for prompt recovery.

ICS Security Workshop in Nagoya Inst. Tech. (3)

Group discussion is executed by the participants of the workshop from detection and recovery.



■ 想定モデル/ロール



Paper list (1)

2016

① **A method for proposal of ICS cyber security measures (in Japanese), Sun Jing, H. Takagi, I. Koshijima, Y. Hashimoto, J. of Society of Plant Engineers Japan, 28,3 (2016-10)**

② **An approach for ICS cyber security measures (in Japanese), Sun Jing, H. Takagi, I. Koshijima, Y. Hashimoto, J. of Transdisplinary Federation of Science and Technology (Oukan) , Vol.10, No.2, pp.107-115 (2016-10)**

③ **A Hot-Backup System for Backup and Restore of ICS to Recover from Cyber-Attack, S.Yamamoto, T.Hamaguchi, S.Jing, I.Koshijima, Y.Hashimoto: Advances in Human Factors, Software, and Systems Engineering, Advances in Intelligent Systems and Computing 492, 45-53 (2016-07)**

④ **Zoning Management of Secured Industrial Control System, W.Machii, A.Tuchiya, T.Aoyama, T.Hamaguchi, Y.Hashimoto, I.Koshijima: Proceedings of the 7th International Symposium on Design, Operation and Control of Chemical Processes, B131 (2016-07)**

⑤ **Developing ICS Security Training for Resilient Cyber Incident Management, Tomomi Aoyama, Kenji Watanabe, Ichiro Koshijima, Yoshihiro Hashimoto, Proceedings of the 7th International Symposium on Design, Operation and Control of Chemical Processes, P101 (2016-07)**

⑥ **Generation of Fault Trees for ICS Safety and Security, H.Moritani, T.Yamamoto, S.Yamamoto, K.Ito, J.Sun, T.Hamaguchi, I.Koshijima, Y.Hashimoto: Proceedings of the 7th International Symposium on Design, Operation and Control of Chemical Processes, P102 (2016-07)**

⑦ **Design Approach of ICS Security Systems, J.Sun, H.Takagi, K.Ito, H.Moritani, T.Hamaguchi, I.Koshijima, Y.Hashimoto: Proceedings of the 7th International Symposium on Design, Operation and Control of Chemical Processes, P103 (2016-07)**

⑧ **A Method for Generating Alarm Configurations using DAEs for Plant Alarm System Design, T.Hamaguchi, H.Sakashita, H.Moritani, K.Takeda, N.Kimura, M.Noda; Proceedings of the 7th International Symposium on Design, Operation and Control of Chemical Processes, D212 (2016-07)**

⑨ **A Metric for Quantitative Estimation of Production Process Resilience based on the Production Support System in the Chemical Industry, Hajime Eguchi, Tomomi Aoyama, Kohei Seki, Ichiro Koshijima, Journal of Chemical Engineering of Japan, Vol.49, No.7, pp.673-679 (2016-07)**

⑩ **A Metric for Quantitative Estimation of Production Process Resilience based on the Skills and Knowledge of Production Plant Personnel in the Chemical Industry, Hajime Eguchi, Tomomi Aoyama, Kohei Seki, Donal O'Donovan, Ichiro Koshijima, Journal of Chemical Engineering of Japan, Vol.49, No.1, pp.35-41 (2016-01)**

2015

① **Srategic Security Protection for Industrial Control System, P H.Takagi, T.Morita, M.Matta, H.Moritani, T.Hamaguchi, S.Jing, I.Koshijima, Y.Hashimoto, Proc. SICE Annual Conference, pp.1215-1221 (2015-08)**

② **Industrial Control System Monitoring Based on Communication Profile, Masafumi Matta, Masato Koike, Wataru Machii, Tomomi Aoyama, Hidemasa Naruoka, Ichiro Koshijima, Yoshihiro Hashimoto, Journal of Chemical Engineering of Japan, Vol.48, No. 8, pp.609-618 (2015-08)**

Paper list (2)

2015

③ ICS Honeypot System (CamouflageNet) Based on Attacker's Human Factors, Hidemasa Naruoka, , Masafumi Matsuta, Wataru Machii, Tomomi Aoyama, Masahito Koike, Ichiro Koshijima, Yoshihiro Hashimoto, Procedia Manufacturing, Vol.3, pp,1074–1081 (2015-07) doi:10.1016/j.promfg.2015.07.175

④ How Management Goes Wrong? – The Human Factor Lessons Learned from a Cyber Incident Handling Exercise, Tomomi Aoyama, , Hidemasa Naruoka, Ichiro Koshijima, Kenji Watanabe, Procedia Manufacturing, Vol.3, pp.1082–1087 (2015-07) doi:10.1016/j.promfg.2015.07.178

⑤ Optimal Personnel Reallocation based on the Skills and Knowledge in the Chemical Industry, Hajime Eguchi, Tomomi Aoyama, Kohei Seki, Donal O'Donovan, Ichiro Koshijima, Journal of the Institute of Industrial Applications Engineers, Vol.3, No.3, pp.126–133 (2015-07)

⑥ Organizational Structure on the Resilience of Production Processes based on Artificial Factors in the Chemical Industry, Hajime Eguchi, Tomomi Aoyama, Kohei Seki, Donal O'Donovan, Ichiro Koshijima, Journal of the Institute of Industrial Applications Engineers, Vol.3, No.3, pp.141–147 (2015-07)

⑦ Dynamic Zoning Based on Situational Activitie for ICS Security, Wataru Machii, Isao Kato, Masahito Koike, Masafumi Matta, Tomomi Aoyama, Hidemasa Naruoka, Ichiro Koshijima, Yoshihiro Hashimoto, the 10th Asian Control Conference 2015 (ASCC 2015), pp.1242-1246 (2015-05)

⑧ Studying Resilient Cyber Incident Management from Large-scale Cyber Security Training, Tomomi Aoyama, Hidemasa Naruoka, Ichiro Koshijima, Wataru Machii and Kohei Seki, the 10th Asian Control Conference 2015 (ASCC 2015), pp.2890-2893 (2015-05)

⑨ Impact of an Organizational Structure on the Resilience of Production Processes Based on Artificial Factors in the Chemical Industry, Hajime Eguchi, Tomomi Aoyama, Kohei Seki, Donal O'Donovan, Ichiro Koshijima, The 3rd International Conference on Industrial Application Engineering 2015 (ICIAE2015), GS3-4 (2015-03)

⑩ 状況マネジメントのための動的対応シナリオ生成手法に関する基礎的研究, 濱田佑希, 青山智春, 越島一郎, 渡辺研司, 永里賢治, 国際プロジェクト・プログラムマネジメント学会誌, Vol.9, No.2, pp.237-254 (2015-03)

⑪ Business Process Model Approach for Management of Plant Alarm System, K.Takeda, T.Hamaguchi, N.Kimura, M.Noda: J. of Chemical Engineering of Japan, 48(8), 641-645 (2015)

⑫ A Method for Generation and Check of Alarm Configurations Using Cause-Effect Matrices for Plant Alarm System Design, T.Hamaguchi, B.Mondori, K.Takeda, N.Kimura, M.Noda: Proc. 17th International Conference on Human-Computer Interaction, 549-556 (2015)

⑬ Modelling of a Business Process for Alarm Management Lifecycle in Chemical Industries, K.Takeda, T.Hamaguchi, N.Kimura, M.Noda: Proc. 17th International Conference on Human-Computer Interaction, 579-587 (2015)

⑭ Strategic Security Protection for Industrial Control System, H.Takagi, T.Morita, M.Matta, H.Moritani, T.Hamaguchi, S.Jing, I.Koshijima, Y.Hashimoto, Proc. SICE Annual Confernce, 1215-1221 (2015)

⑮ Organizational Structure on the Resilience of Production Processes based on Human Factors in the Chemical Industry, Hajime Eguchi, Tomomi Aoyama, Kohei Seki, Donal O'Donovan, Ichiro Koshijima, Journal of Engineering Science and Technology Special Issue on SOMCHE 2014 & RSCE 2014 Conference, pp.30-40 (2015-01)

Paper list (3)

2014

1) Development of CAD for Zone Dividing of Process Control Networks to Improve Cyber Security, H. Moritani, S. Yogo, T. Morita, M. Kojima, K. Watanabe, J. Sung, I. Koshijima, Y. Hashimoto, ICCAS 2014, Oct. 22-25, Korea (2014-10)
2) プロセス制御系のサイバーセキュリティ対策の立案と評価，橋本芳宏，越島一郎，ヒューマンファクターズ，Vol.19(1)，pp.18-25 (2014-08)
3) Industrial Control System Monitoring based on Communication Profile, Masafumi Matta, Masato Koike, Wataru Machii, Tomomi Aoyama, Hidemasa Naruoka, Ichiro Koshijima, Yoshihiro Hashimoto, The 5th World Conference of Safety of Oil and Gas Industry, Okayama, Japan, Paper No. 1092435, (2014-06)
4) Dynamic Zoning of the Industrial Control System for Security Improvement, Wataru Machii, Tomomi Aoyama, Ichiro Koshijima, Yoshihiro Hashimoto, The 5th World Conference of Safety of Oil and Gas Industry, Okayama, Japan, Paper No. 1065756 (2014-06)
5) BPM Approach for Describing Plant Alarm System Design Process, K.Takeda, T.Hamaguchi, N.Kimura, M.Noda, Proc. WCOGI 2014, PS-3,(2014-06)
6) Framework for Life Cycle Security and Safety for Critical Infrastructures, Tomomi Aoyama, Ichiro Koshijima, Yoshihiro Hashimoto, The 5th World Conference of Safety of Oil and Gas Industry, Paper No. 1092680 (2014-06)
7) プラントライフサイクルエンジニアリングの業務プロセスモデルに基づくプラントアラームシステムの変更管理, 武田和宏, 濵口孝司, 木村直樹, 野田賢: 化学工学論文集, 40(3), pp. 224-229 (2014)
8) A Design Method of a Plant Alarm System for First Alarm Alternative Signals using a Modularized CE Model, K.Takeda, T.Hamaguchi, N.Kimura, M.Noda, Process Safety and Environmental Protection, 92, pp. 406-411 (2014)

2013

1) Impact Analysis of Political Decisions, S. Eryuruk, I. Koshijima, T. Kato, 2013 Asian Conference of Management Science & Applications, pp.411-419 (2013)
2) A Process Alarm Design of Quantitative Value with Zone Dividing for Control System Security, J. Sun, Y. Hashimoto, S. Yogo, T. Morita, H. Moritani, I. Koshijima, 2013 Asian Conference of Management Science & Applications, pp.372-377 (2013)
3) Detection of Cyber-Attacks with Zone Dividing and PCA, T. Morita, S. Yogo, M. Koike, T. Hamaguchi, S. Jing, I. Koshijima, Y. Hashimoto, 17th International Conference in Knowledge Based and Intelligent Information and Engineering Systems, Vol.22, pp.727-736 (2013)
4) A Unified Framework for Safety and Security Assessment in Critical Infrastructures, T. Aoyama, M. Koike, I. Koshijima, Y. Hashimoto, Proc. of Safety and Security Engineering V, pp.67-77 (2013)
5) Safety Securing Approach against Cyber-Attacks for Process Control System, Y. Hashimoto, T. Toyoshima, S. Yogo, M. Koike, T. Hamaguchi, S. Jing, I. Koshijima, Computers & Chemical Engineering, Vol.57, pp.181-186 (2013)
6) Generating Alternative Modules for a Plant Alarm System Based on First-Out Alarm Alternative Signals, T.Hamaguchi, B.Mondori, K.Takeda, N.Kimura, M.Noda, Procedia Computer Science, 22, pp. 937-944 (2013)
7) Method of Designing Plant Alarm System based on First Alarm Alternative Signals for Each Assumed Plant Malfunction, K.Takeda, T.Hamaguchi, N.Kimura, M.Noda, Proc. PSE Asia 2013, pp. 245-250 (2013)
8) Determination of Alarm Setpoint for Alarm System Rationalization using Performance Evaluation, N.Kimura, T.Hamaguchi, K.Takeda, M.Noda, LNCS 8017, pp. 507-514 (2013)

Paper list (4)

2012

1) Conceptual Framework for Security Hazard Management in Critical Infrastructures, Y. Hashimoto, T. Toyoshima, S. Yogo, M. Koike, S. Jing, I. Koshijima, The 11th International Symposium on Process Systems Engineering, CDROM (2012)
2) A Method of Designing Plant Alarm Systems with Hierarchical Cause-Effect Model, T.Hamaguchi, K.Takeda, M.Noda, N.Kimura, Proc. PSE 2012, pp. 265-269 (2012)
3) サステナブルP2Mへの展開 ープラント-プロダクトLCMとしてのプログラムマネジメントー,西田絢子, 越島一郎, 梅田富雄, 国際プロジェクト・プログラムマネジメント学会誌, Vol.6, No.2, pp.165-175 (2012)

~2011

1) サイバーテロを想定した場合のリスク解析と対策の構築, 豊嶌剛史, 孫晶, 越島一郎, 橋本芳宏, J. of Human Factors in Japan, Vol.15, No.2, pp.4-9 (2011)
2) ミッションマネジメントのためのコンセプト設計と管理に関する基本的考察, 濱田和弥, 村田裕樹, 越島一郎, 国際プロジェクト・プログラム学会誌, Vol.5, No.2, pp.137-149 (2011)
3) Design Method of Plant Alarm Systems on the Basis of Two-Layer Cause-Effect Model, K.Takeda, A.H.B.M.Aimi, T.Hamaguchi, M.Noda, LNAI 6883, pp. 415-422 (2011)
4) An Evaluation Method for Plant Alarm System Based on a Two-Layer Cause-Effect Model, N.Kimura, K.Takeda, M.Noda, T.Hamaguchi, Proc. ESCAPE-21, pp. 1065-1069 (2011)
5) Consistency Checking Method of Inventory Control for Countermeasures Planning System, T. Hamaguchi, K. Takeda, H. Matsumoto, Y. Hashimoto, LNAI 6277, pp.417-426 (2010)
6) Integration of Multi-agent Controller and Scheduler for Multi-purpose and Multi-batch Plant, T. Hamaguchi, M. Inoue, T. Yoshida, K. Kawano, H. A. Gabbar, K. Takeda, Y. Shimada, T. Kitazima, Y. Hashimoto, KES 2007 Part II, pp.736-743(2007)
7) Agent-Based Batch Process Control Systems, M. Sakamoto, H. Eguchi, T. Hamaguchi, Y. Ota, Y. Hashimoto, T. Itoh, KES2004 Part II, (2004)
8) Abnormal situation correction based on controller reconfiguration, T. Hamaguchi, Y. Hashimoto, T. Itoh, A. Yoneya, Y. Togari, Journal of Process Control, Vol.13, No.2, pp.169-175 (2003)
9) An Approach to Potential Risk Analysis of Networked Chemical Plants, A.Shindo, H. Yamazaki, A. Toki, I. Koshijima, T. Umeda, PSE 2000, (2000)