IPA Better Life with IT

Risk Assessment for Industrial Control Systems in Japan

April 26 , 2021

Information-technology Promotion Agency, Japan

IPA Activities focused on Security

IPA drives various national IT initiatives under the Ministry of Economy, Trade and Industry (METI) as an independent administrative agency.

■ICSCoE (Industrial Cyber Security Center of Excellence）

- Training Top Gun specialists to protect ICS systems

■ISEC (IT Security Center）

- **ICS security**, IoT security, Vulnerability information handling/disclosure
- Threat information sharing (J-CSIP), Cyber rescue/Consultation Team (J-CRAT)
- Common criteria certification , Cryptography research and evaluation
- SME support ,Security literacy promotion
- Public sector support (Security audit, Monitoring public important systems)

■National Examination

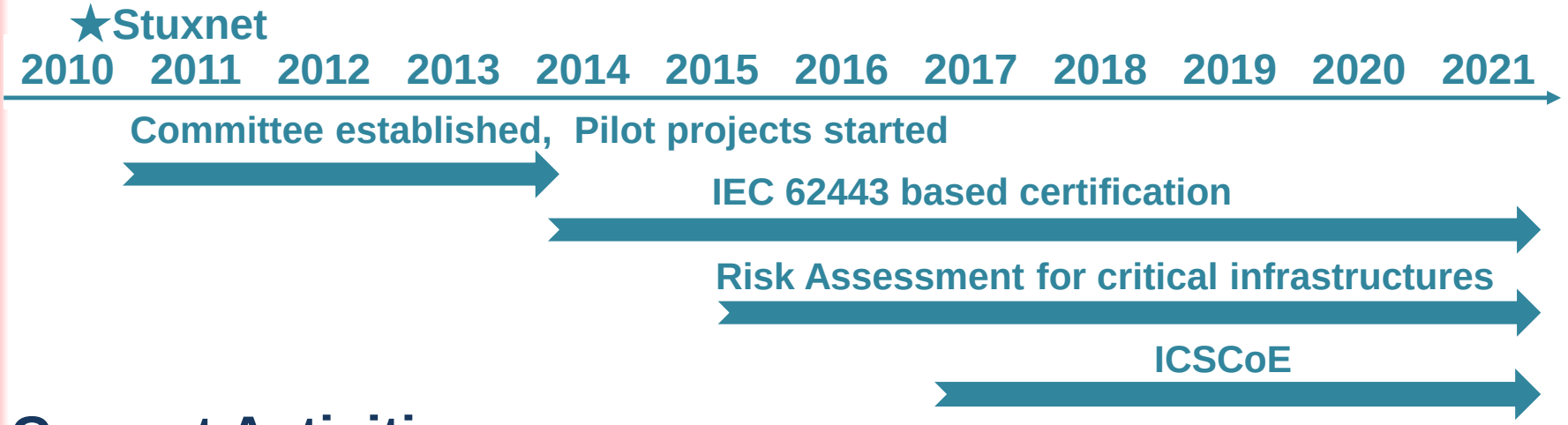
- National examinations for IT engineers. including information security area.

■Publication of technical report & statistics

- Various reports monitoring IT society & technology trend including information security

Activities for ICS Security

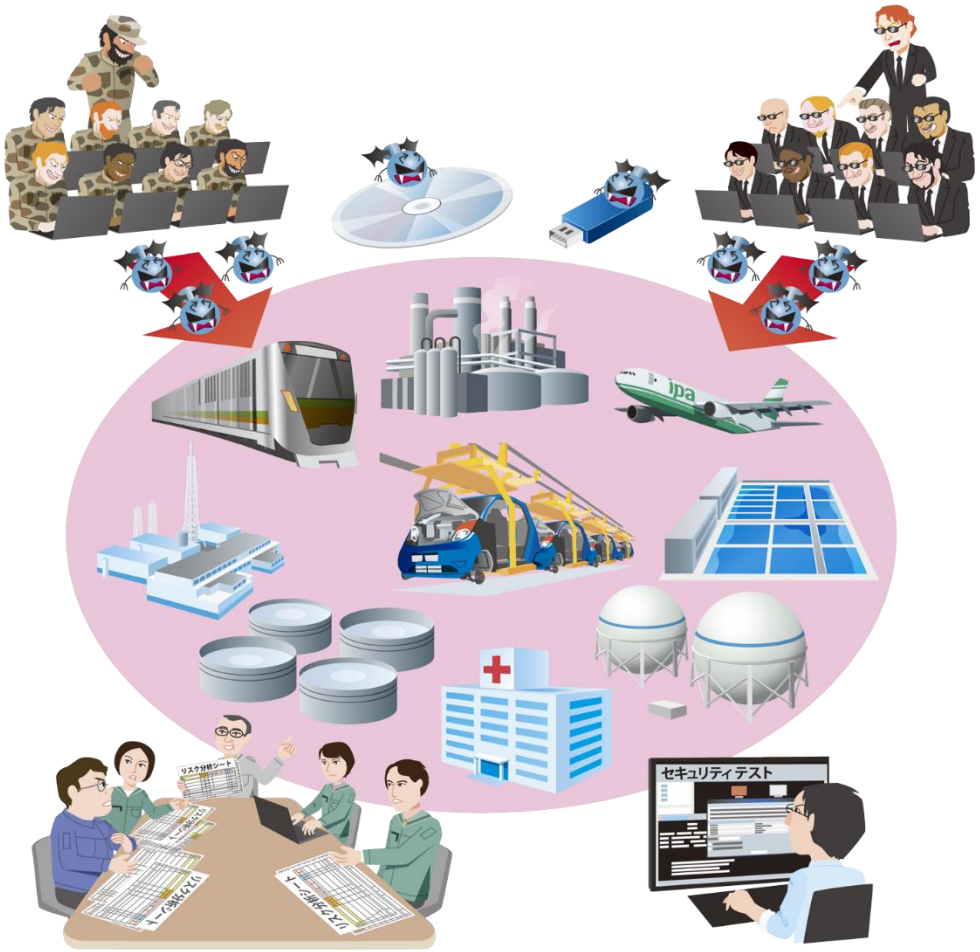
History (RE: ICS security)



Current Activities

- **Risk Assessment for Critical infrastructure Industries**
  - Select Industry, representative ICS system and asset owner , IPA and the asset owner jointly assess the ICS Systems in an industry, and IPA provides the feedback to each industry.
  - Target Industry: Critical Infrastructures (Electric Power, Gas, Water, Oil etc.)
- **Publication of Risk Assessment Guide**
- **Seminar/Training for Asset owners and the related ICS suppliers.**

IPA Risk Assessment Method



Risk Assessment

Risk Assessment

- Risk Assessment = Risk identification+ Risk Analysis+ Risk Evaluation
- Fundamental of security measures (See NIST Cyber Security Framework, METI Cyber Physical Security framework)

Goal

- Achieve effective risk reduction
- Enable effective investment
- Provide a foundation for PDCA cycle and continuous security improvement

Methods

- Baseline approach (check sheet etc.)
- Detailed analysis approach (Asset-based approach, Attack-based approach)
- Informal Approach (Review by Expert)
- Combined Approach

Security Risk Assessment Guide for Industrial Control Systems (ICS)

Focused on Risk Assessment for ICS System, excludes management related items.

【Guide：Table of Contents】

1. Role and Importance of Risk Assessment in Security
2. Overview and Procedure of Risk Assessment
3. Preparing for Risk Assessment (1)
   - Deciding Assessment Objects
4. Preparing for Risk Assessment (2)
   - Risk Value, Evaluation Factors and Criteria
5. Conducting Risk Assessment (1)
   - Asset-based Risk Assessment
6. Conducting Risk Assessment (2)
   - Business Impact-based Risk Assessment
7. Interpreting and Utilizing Risk Assessment Results
8. Security Test
9. Additional Criteria for Specific Security Controls

Reference, Appendixes

Guide

380 pages

Risk Assessment Example

Famous ICS Cyber Incidents

Download available at : https://www.ipa.go.jp/security/controlsystem/riskanalysis.html (Japanese only)

Step of Risk Assessment

1.Determine the scope of ICS for assessment

2.Identify all assets consisting of ICS, and
identify the current security measures for each asset.

3.Execute Asset-based assessment

4.List Business impacts

5.Execute Business Impact-based assessment
～ Create attack trees to find insufficiency of security measures ～

6. Execute Security Test for ICS (Penetration test, Capture test)

7.Decide plan to mitigate risk
～ how and when to remediate the system or change operations ～

1.Determine scope

2+3. Identify assets and the current measures, Asset-based Approach

4+5. Business Impacts List , Business impact-based Approach

6. Security Test (Penetration test etc.)

7. Decide plan to mitigate risk

PDCA

Preparation for Risk Assessment

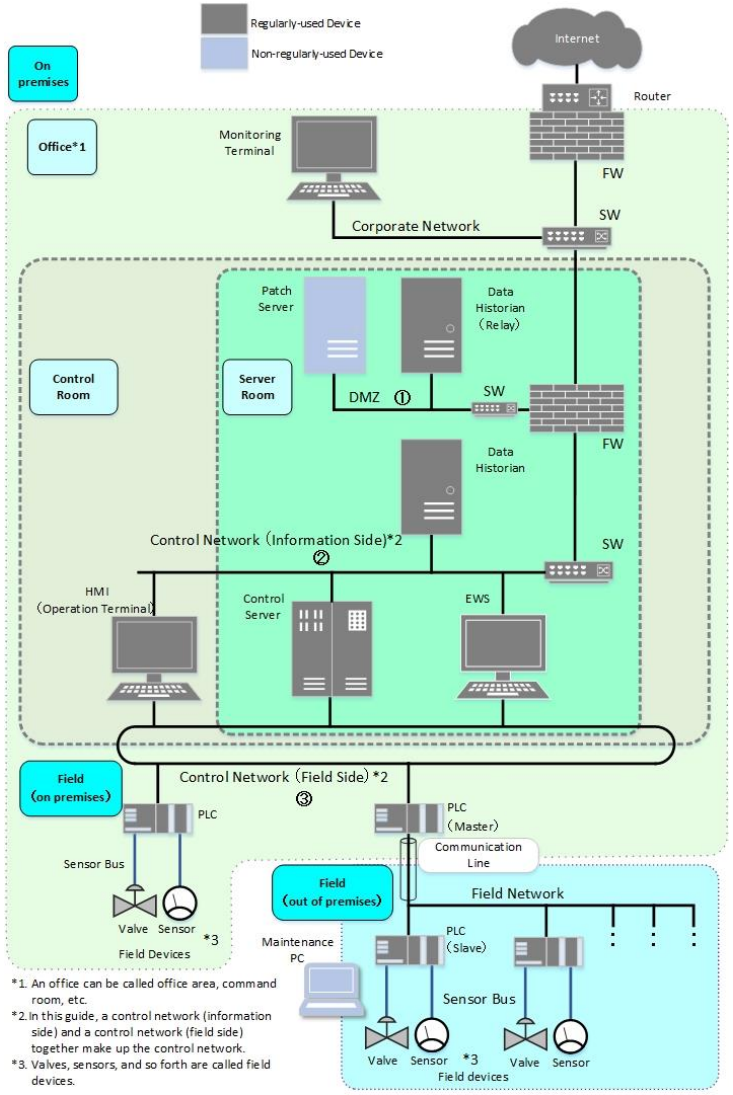
Grasp your current ICS status before analysis

【Preparation Works】

1. Determine the scope of ICS for assessment
2. Identify all ICS consisting assets
3. Create simple system configuration figures
   which everyone joining assessment can understand
4. Investigate the current security measures for each asset

Preparation for Risk Assessment

【Simple system configuration】



*1. An office can be called office area, command room, etc.
*2. In this guide, a control network (information side) and a control network (field side) together make up the control network.
*3. Valves, sensors, and so forth are called field devices.

【Asset Inventory】

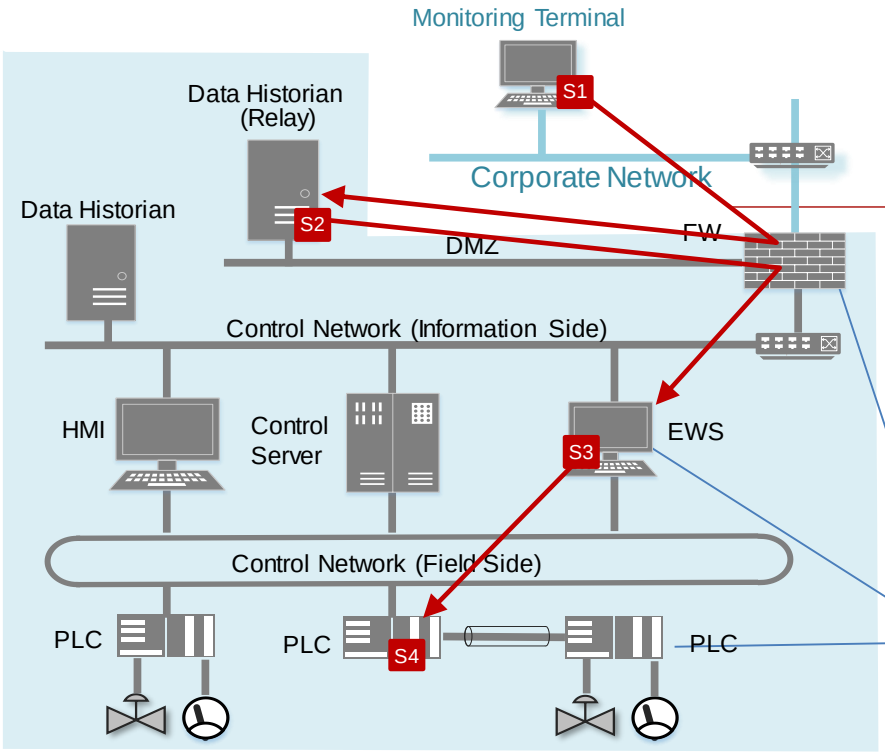
No.		1	2	3	4	5	6	7	8
Asset		Monitoring Terminal	Firewall	DMZ	Data Historian (Relay)	Controll Server	EWS	Controller (Master)	Field NW
Asset Type	Informatin System Asset	○	○		○	○	○		
	Control System Asset							○	
	Network Asset			○					○
Function	Data Input / Output	○					○		
	Data Storage				○				
	Command Issuance	○				○	○	○*1	
	Gate		○						
Type of Network				LAN					Leased Line
Location		Control Room	Server Room	Server Room	Server Room	Server Room	Server Room	Field	Filed
Connected NW	Corporate NW	○	○						
	DMZ		○		○				
	Control NW(Information Side)		○			○	○		
	Control NW(Field Side)					○	○	○	
	Others								
Connected NW of Management Port		×	Corporate NW	×	×	×	×	×	×
Operation I/F		○	×		○	○	○	×	
USB Port ／Communicatin I/F		○(USB)	○(LAN)		○(USB)	○(USB)	○(USB)	○(USB)	
Regularly-used external media		×	×		×	×	○	×	
Wireless Function		×	×	×	×	×	×	×	×
Regularly-used／Non-regularly used		Regularly	Regularly	Regularly	Regularly	Regularly	Regularly	Regularly	Regularly
Data Type / Data Path		Described in Data Flow Matrix							
System Vendor／Device Manufacturer		ABY/HH	ABY/HH	ABY/HH	ABY/HH	ABY/HH	ABY/HH	ABY/HH	ABY/CCJ
OS／Version		Windows	Proprietary		Windows	Windows	Windows	Proprietary	
Protocol		TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP,Proprietary	TCP,UDP	Proprietary	Proprietary
Security Controls		Described in Asset-based Analysis Sheet							

【Dataflow between assets】

to→ P:Process Value C:Control Command S:Engineering Settings ↓from	Monitoring Terminal	FW	Data Historian (Relay)	Data Historian	EWS	Control Server	HMI	Controller (Master)	Controller (Slave)
Monitoring Termial									
FW	P								
Data Historian (Relay)		P							
Data Historian		P							
EWS								C	
Control Server				P				C	
HMI								C	
Controller (M)						P	P		C
Controller (S)								P	

Two Approach of Risk Assessment

- Asset-based approach:
  Confirm status of security measures for each asset.
- Business Impact-based approach:
  - Define business impact list
  - Create attack trees which cause business impact from the attacker's view
  - Verify the sufficiency of security measures.



Top-down Approach

Business impact-based Approach

- Define business impact list
- Create attack trees which cause business impact from the attacker's view
- Verify the sufficiency of security measures.
- Judge whether the attack could be stopped or not

(note)This example shows the attack tree (Cooperation network →FW → Data Historian →EWS →PLC)

Asset-based Approach

-Confirm security measures for each asset (FW, EWS, HMI, PLC etc.)

Bottom-Up Approach

Asset-based Approach

- List threats (attack techniques) and available security controls for each asset
- Check which security controls are implemented for each asset

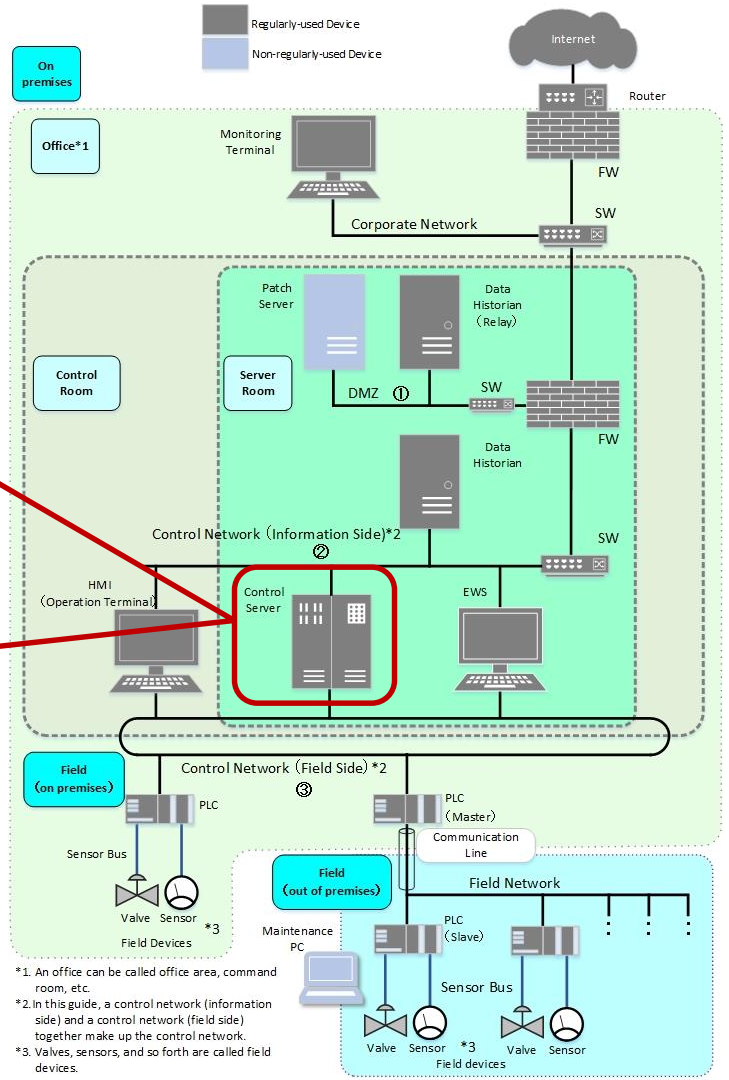
Threats (attack techniques)

Unauthorized Access
Malware Infection
Data Modification
Shutdown etc.

Implemented Security Controls (Vulnerability level)

Whitelist
Sender/Receiver Authentication
User Authentication
Privilege Management etc.

Asset Importance



Asset-based Approach

- Example of the completed sheet of Asset-based Risk Assessment

Asset-based Risk Assessment Sheet

[Legend] ○: Implemented / ×: Not Implemented / Greyout : Threats not considered in the asset / Green characters: additional information of the security measure

No.	Asset Type	Assessment Object	Evaluation Factor: Threat Level	Vulnerability Level	Importance of Asset	Risk Value	Threat (Attack Technique)	Description	Security Controls: Protection: Intrusion / Diffusion Phase		Protection: Objective Achievement Phase		Detection / Consequence Identification		Business Continuity		Security Level Per Threat
1	Information System Asset	**Control Server**	2	2	3	B	Unauthorized Access	Hack into a devices via network and execute an attack.	FW (Packet Filtering type) FW (Application Gateway type) Unidirectional Gateway Proxy Server WAF Authentication of Connecting Equip. IPS／IDS Patch Application Vulnerability Avoidance	○			IPS／IDS Logging／Analysis Integrated Log Management System			2
2			2	1		C	Physical Intrusion	Intrude a restricted area (where equipment is installed, etc.) , or unlock a device the access to which is physically limited (a device installed in a server room, etc.)	Physical Access Control (IC card, Biometric Authentication) Lock-up／Key Management	○			Surveillance Camera Intrusion Sensor	○ ○			3
3			2	2		B	Fraudulent Manipulation	Intrude by direct operation of the console of the device etc. and execute an attack.	Operator Authentication (ID/Pass)	○							2
4			2	3		A	Incorrect Operation	Induce an incorrect operation of the insider (a person with privilege to access the device among employees and business partners) and execute an attack. Connect an authorized medium or device to the device and an action equivalent to an attack is executed as a consequence.	URL Filtering／Web Reputation Mail Filtering								1
5			2	3		A	Connecting Unauthorized Media/Device	Connect illegally brought malicious medium (CD/DVD, USB device etc.) to the device and execute an attack.	Device Connection and Usage Restriction		(same as left)		(same as left) Logging／Analysis Integrated Log Management System				1
6			3	2		A	Unauthorized Execution of Process	Fraudulently execute a process existing in the attack target device, such as legitimate programs, commands, services etc.	Privilege Management Access Control Process Run Limitation by Whitelist Approval of Critical Operations	○	(same as left) (same as left) (same as left) (same as left)		Device Anomaly Detection Device Alive Monitoring Logging／Analysis Integrated Log Management System				2
7			3	1		B	Malware Infection	Infect and execute malware on the target device	Anti Virus Process Run Limitation by Whitelist Patch Application Vulnerability Avoidance Digital Signature	○			Device Anomaly Detection Device Alive Monitoring Logging／Analysis Integrated Log Management System				3
8			3	2		A	Data Theft	Steal data (software, credential, configuration settings, confidential information such as an encryption key) stored in the device.	Permission Management Access Control Data Encryption DLP	○	(same as left) (same as left) (same as left) (same as left)		Logging／Analysis Integrated Log Management System				2
9			3	2		A	Data Modification	Modify data (software, credential, configuration settings, confidential information such as an encryption key) stored in the device.	Permission Management Access Control Digital Signature	○	(same as left) (same as left) (same as left)		Device Anomaly Detection Logging／Analysis Integrated Log Management System		Data Backup	○	2
10			2	2		B	Data Destruction	Make information (software, credential configuration settings, confidential information such as an encryption key) stored in the device unusable.			Privilege Management Access Control	○	Device Anomaly Detection Logging／Analysis Integrated Log Management System		Data Backup	○	2
11			3	3		A	Malicious Command	Send malicious control commands (set point change, power off, etc.) or malicious data to other devices.	Segmentation／Zoning Digital Signature Approval of Critical Operations		(same as left) (same as left) (same as left)		Logging／Analysis Integrated Log Management System				1
12			3	3		A	Shutdown	Halt the function of device.					Device Anomaly Detection Device Alive Monitoring Logging／Analysis Integrated Log Management System		Redundancy Fail-safe Design		1
13			1	3		B	Denial-of-service Attack	Requests processing that exceeds the processing capability of the device by DDoS attacks, etc., and interferes with the normal operation of the device.	Anti DDoS Solution				Device Anomaly Detection Device Alive Monitoring Logging／Analysis Integrated Log Management System		Redundancy Fail-safe Design		1
14			1	2		C	Theft	Steal device or equipment	Lock-up／Key Management	○	(same as left)		(同左)				2
15			3	3		A	Information theft by disassembling stolen and discarded equipment	A stolen device or a discarded device is disassembled, and information (software, authentication information, configuration setting information, confidential information such as an encryption key) stored in the device is stolen.	Tamper Resistant Obfuscation Secure Deletion		(same as left) (same as left) (same as left)						1

Asset

Threat

Security Controls

Control Server

Unauthorized Access

Physical Intrusion

Unauthorized Media

Malware Infection

Dos

Implemented security controls

Implemented security controls

Implemented security controls

Implemented security controls

Business Impact-based Approach

Keyword: Attacker's View, Business Impact-based

(Step1) List business impacts caused by cyber attack, prioritize them with business impact level.

(Step2) Identify "asset and situation" (targets) which cause a business impact by FTA Approach.

(Step3) List attack trees to reach a target

(Step4) Confirm the current security measures, for each attack tree.

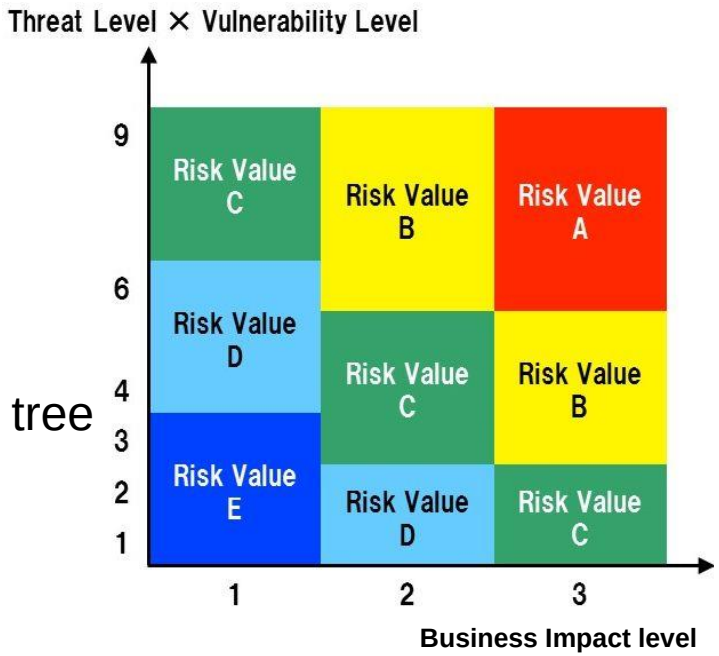
(Step5) Calculate Risk Value for each attack tree

- Threat level ,Vulnerability level, Business impact level
- Calculate Risk Value from the above 3 values.

(Step6) Evaluate how to mitigate the Risk of each tree (Additional security measure, operation change, etc.)

(Step7) Decide mitigation plan considering cost.

(Step8) PDCA (Periodically return to 1)



Business Impact-based Approach

(Step1) List business impacts

- List business impacts(damages) caused by Cyber attack and prioritize them with business Impact level.

C(Confidentiality) + **I**(Integrity) + **A**(Availability) + **H**(Health) + **S**(Safety) + **E**(Environment)

case: city gas supply

#	Business Damage	Description	Business Impact Level
1	Wide Area Gas Supply Outage	Cyber attack on Gas supply facility. could result in supply outage over a wide area, largely affecting society, and causing huge financial loss such as compensation costs, and loss of credibility.	3
2	Limited Area Gas Supply Outage	Cyber attack on Gas supply facility could result in supply outage in a limited area, affecting society, and causing financial loss such as compensation costs, and loss of credibility.	2
3	Supply of Off-spec Gas	Cyber attack on Gas supply facility, etc. could result in supply of city gas which doesn't meet defined specifications/standards, affecting society, and causing financial loss such as compensation costs, and loss of credibility.	2
4	Destruction of Equipment/Facility	Cyber attack on Gas supply facility. could result in destruction of the equipment/facility, affecting society, causing casualties (employees and/or neighbors) and financial loss such as compensation costs, and loss of credibility.	3
5	Steal confidential information	Steal BOM of city gas and manufacturing method , could result in warrying about competency.	1

Business Impact-based Approach

(Step2) List Targets , Create Attack Tree

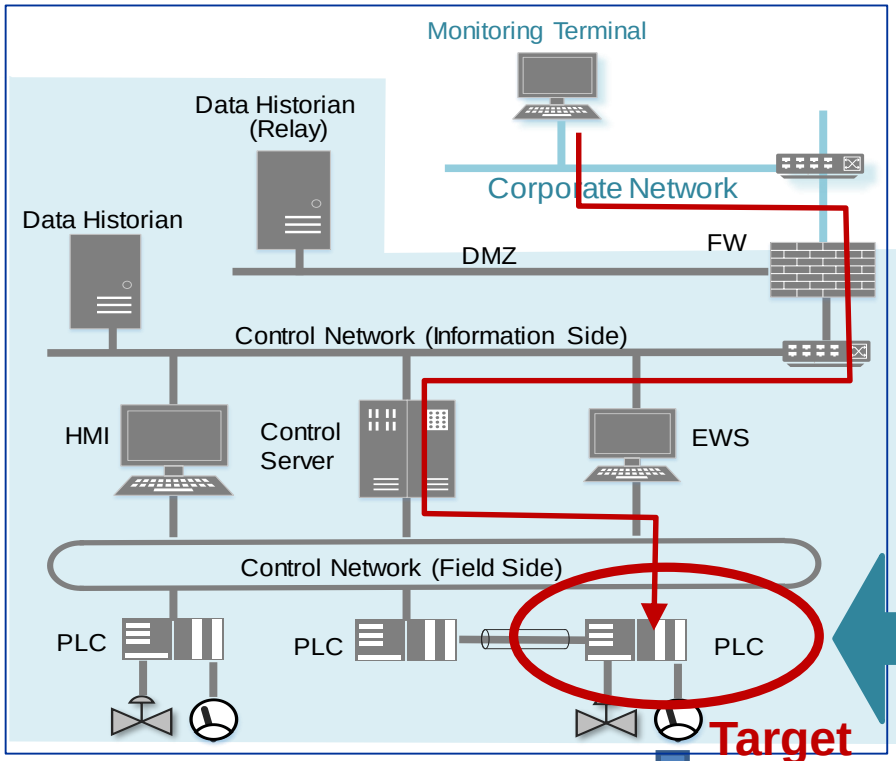
- ✓ **List targets which cause a business impacts with FTA approach.**
- ✓ **Select a target**
- ✓ **Create an attack tree to reach the target by ATA approach.**

Who × From Where × Which route × to reach Target

ATA
(Attack tree analysis)

Target

FTA
(Fault tree analysis)



Who
(= External Attacker on Corporate NW)

From where
(= from FW)

Which route to reach the target
(See red arrow)

Final Attack

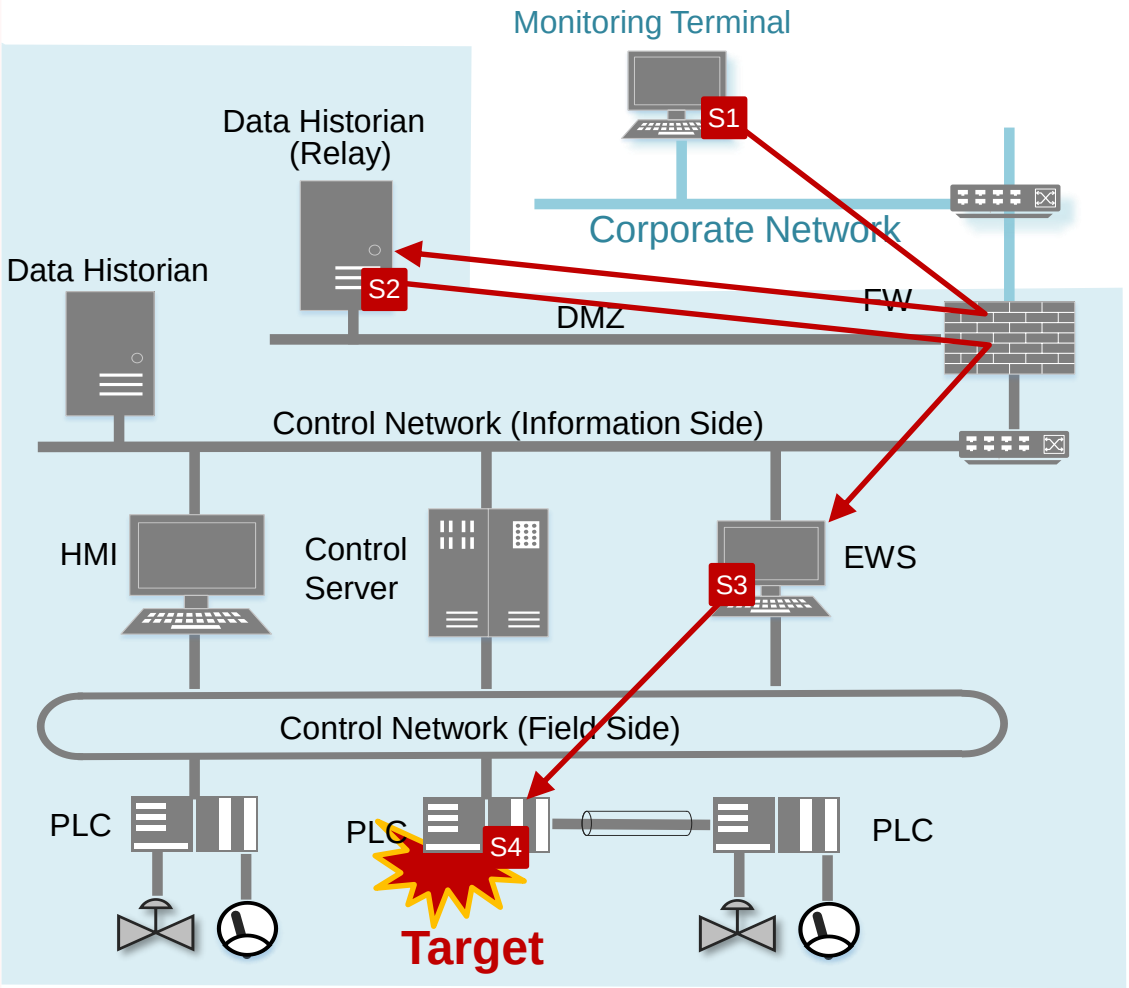
Cause business Impact

Business Impact : supply outage in wide area
(Business Impact level =3 (High))

Business Impact-based Approach

(Step3) Create Attack Tree

Example of Attack Tree



Step	Attack method
S1	From the cooperate NW, an attacker breaks into Data Historian using web vulnerability.
S2	From Data Historian, the attacker breaks into EWS.
S3	The attacker modifies PLC firmware and install it to PLCs.
S4	After hours, PLCs go to shutdown process and ICS system is forced to be shutdown.

Business Impact-based Approach

(Step4,5) Confirm current security measures, calculate Risk Value

Step	Attack method	Vulnerability Level	Security Control
S1	From the corporate NW, an attacker break into Data Historian using web vulnerability.	2	△ Update Web vulnerability ○ Sender/receiver authentication .
S2	From Data Historian, the attacker break into EWS.	2	○ Sender/receiver authentication ○ Unnecessary ports is closed × Inappropriate direction
S3	The attacker modifies PLC firmware and installs it onto PLCs.	3	× Proper authentication and authorization × Physical intrusion prevention × Firmware update is inhibited in online status
S4	After hours, PLCs go to shutdown process and ICS system is forced to be shutdown.	3	× Firmware object is checked with certification

Vulnerability of the attack tree is level 2

1. Security control Is sufficient to stop attack
2. Security control is insufficient
3. Security control is poor

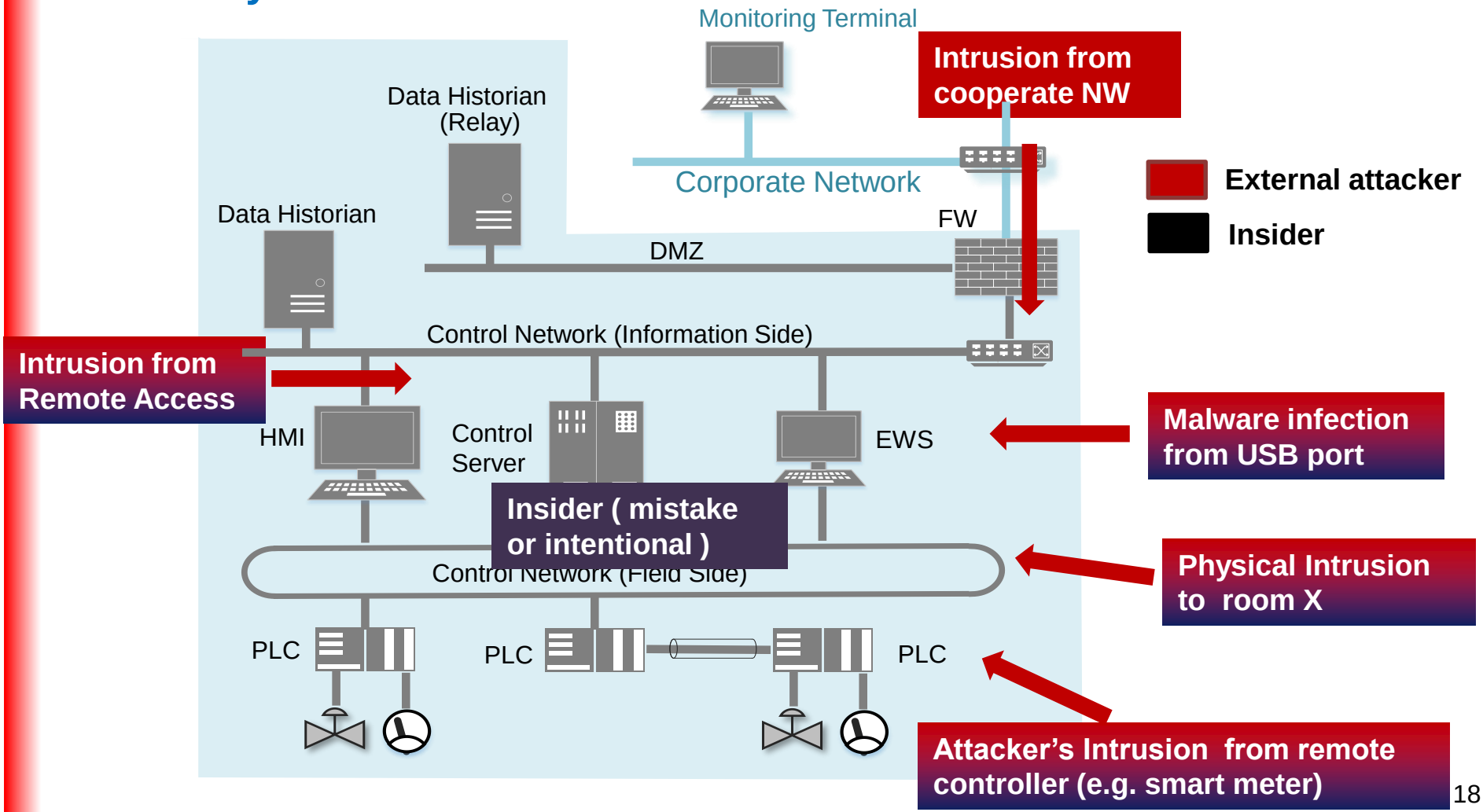
Risk Value = f (Business Impact level , Vulnerability level × Threat level)

B = f (3 , 2 × 2)

Business Impact-based Approach

(Step3) List Attack Trees

List attack trees for possible entry points, and verify sufficiency of security controls



Business Impact-based Approach

- Example of the completed sheet of Business Impact-based Risk Assessment

Business Impact-based Risk Assessment Sheet

1. XX Supply Outage Over a Wide Area

No.	Attack Scenario / Attack Tree／Attack Step	Evaluation Factor: Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Security Controls: Protection: Intrusion／Lateral Movement	Mission Execition Phase	Detection／Impact Identification	Business Continuity	Security Level: Attack Step	Attack Tree	Attack Tree Number	Component Steps (No.)
1-1	Wide area supply outage occurs by conducting unauthorized and malicious operations.												
1	**Network Attack Entry Point : Monitoring Terminal** A malicious outsider gains unauthorised access to the monitoring terminal.					Authentication of Connecting Party ○ Patch Application ○ Vulnerability Avoidance Privilege Management ○		Logging／Analysis Integrated Log Management System		2			
2	A malicious outsider gains an authorised access to the data hystorian (relay) from the monitoring terminal.					Authentication of Connecting Party ● Patch Application ● Vulnerability Avoidance Privilege Management ●		IPS/IDS Logging／Analysis Integrated Log Management System Device Alive Monitoring		1			
3	A malicious outsider gains an authorised access to the data hystorian from the data hystorian (relay).					Authentication of Connecting Party ● Patch Application Vulnerability Avoidance Privilege Management ●		IPS/IDS Logging／Analysis Integrated Log Management System Device Alive Monitoring		1			
4	A malicious outsider gains an authorised access to HMI from the data hystorian.					Authentication of Connecting Party ○ Patch Application Vulnerability Avoidance Privilege Management		IPS/IDS Logging／Analysis Integrated Log Management System Device Alive Monitoring		2			
5	A malicious outsider sends commands from HMI to the controller for causing wide area supply outage.	2	2	3	B	Segmentation／Zoning Digital Signature Approval of Critical Operations		Logging／Analysis Integrated Log Management System		1	2	#1	1,2,3,4,5
6	**Physical Attack Entry Point : HMI** An insider enters into the control room.					Physical Access Control (IC card) ● Lock up／key Management ●		Surveillance Camera ○ Intrusion Sensor ○ Logging／Analysis Integrated Log Management System		1			
7	An insider logs on to HMI.					Operator Authentication		Logging／Analysis Integrated Log Management System		1			
8	An insider accidentally connects a USB media infected with malware to the HMI, then the HMI is infected with malware.					Anti Virus (Media) Anti Virus (HMI) Poet Lock Process Run Limitation by Whitelist Patch Application Vulnerability Avoidance Digital Signature		Device Anomaly Detection Device Alive Monitoring Logging／Analysis Integrated Log Management System		1			
9	The malware executes operations for causing wide area supply outage.	2	3	3	A	Segmentation／Zoning Digital Signature Approval of Critical Operations		Logging／Analysis Integrated Log Management System		1	1	#2	6,7,8,9
1-2	Wide area supply outage occurs by sending legitimate commands to controllers.												
10	**Network Attack Entry Point : Corporate NW** A malicious outsider gains unauthorized access to FW via corporate NW.					FW ○ Authentication of Connecting Party ○ Patch Application ○ Vulnerability Avoidance Privilege Management ○		IPS/IDS Log Collection／Analysis Integrated Log Management System Device Alive Monitoring		2			
11	A malicious outsider gains access to EWS via FW.					Authentication of Connecting Party ○ Patch Application Vulnerability Avoidance Privilege Management		IPS/IDS Log Collection／Analysis Integrated Log Management System Device Alive Monitoring		1			
12	A malicious outsider gains access to the master controller via EWS.					Authentication of Connecting Party Patch Application Vulnerability Avoidance Privilege Management		Log Collection／Analysis Integrated Log Management System Device Anomaly Detection		1			
13	A malicious outsider sends supply outage commands from the master contoller to the slave controllers.	2	2	3	B	Segmentation／Zoning Digital Signature Approval of Critical Operations		Log Collection／Analysis Integrated Log Management System		1	2	#3	10,11,12,13

Risk Value

Attack Tree 1

Attack Tree 2

Attack Tree 3

Utilization of Risk Assessment

(Step6,7) Evaluate risk mitigations and decide mitigation plan

(Work1) Evaluate Risk Mitigation

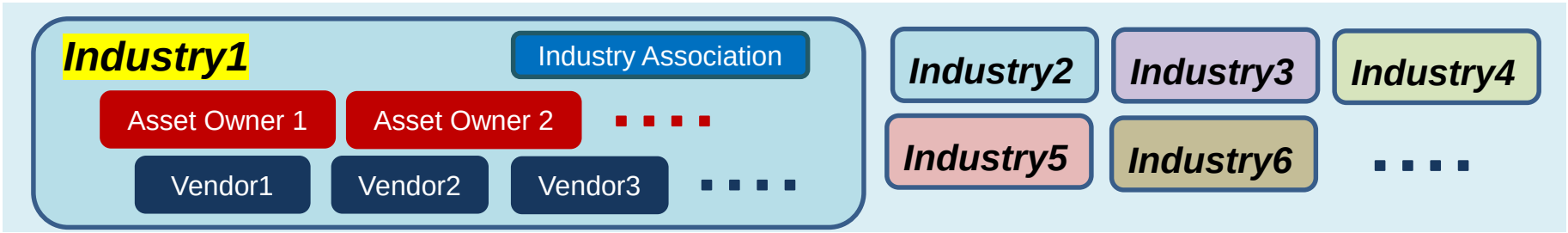
Attack Tree	Risk value (before)	Measure to mitigate risk	Risk value (After)
Attack Tree 1	A	Measure1, 3	B
Attack Tree 2	B	Measure 2	C
Attack Tree 3	A	Measure 4	B
…			
Attack Tree N		Measure N	

(Work2) Fix Risk Mitigation Plan

Measure	Explanation	Class	Severity & Effect	Cost	Select
Measure 1	PW hardening	Op	High	Low	●
Measure 2	Add Internal Gateway in ICS	Sys	Middle	Very High	
Measure 3	Add IPS between OT and IT	Sys	High	Middle	●
Measure 4	2 factors Authen. at remote access entry	Sys	Middle	High	●
…					

IPA continues to contribute

Critical Infrastructure Industries



Feedback to industry※

Assess a representative ICS system jointly

- ✓ Select Industry, asset owner, and ICS system
- ✓ IPA and the asset owner jointly assess the ICS System
- ✓ We execute security test on ICS System
- ✓ We provide the feedback to each industry

Experience:

Electric Power (Smart Meter Sys.), Gas, Water, Oil ,Chemical, Local government (Garbage Incinerator), Railroad, New electric power generation(Fire), Logistics, Smart Factory

IPA+ Asset Owner X ⟺ METI + Regulatory Agency

※Feedback includes typical system configuration which is familiar to the industry , risk analysis sheets, points to be improved (example), without proprietary information.

Thank you !

Contact: isec-ics@ipa.go.jp

Reference: Security Risk Assessment Guide for Industrial Control Systems(Quick Guide) https://www.ipa.go.jp/files/000065768.pdf