IPA Better Life with IT

Security Risk Assessment Guide for Industrial Control Systems

Quick Guide

Information-technology Promotion Agency, Japan
Technology Headquarters
IT Security Center (ISEC)

April 2018

Security Risk Assessment Guide for ICS
Main Guide Book and Supplement

[Contents from Main Guide Book]

Chapter 1. Risk Assessment as Security Measures

Chapter 2. Overview and Work Flow of Risk Assessment

Chapter 3. Getting Ready for Risk Assessment

Chapter 4. Working on Risk Assessment

- 4.1. Asset-based Risk Assessment
- 4.2. Business Risk-based Risk Assessment

Chapter 5. Interpreting and Making Use of Risk Assessment

Chapter 6. Security Test

Chapter 7. Additional Standards to Specific Measures

Reference and Appendix

Published in October, 2017

Main Guide Book

350 pp.

Supplement

70 pp.

Download available at: https://www.ipa.go.jp/security/controlsystem/riskassessment.html

Tactics of Fighting against Cyberattacks
- Importance of Security Risk Assessment -

Sun Wu, a military strategist in the Spring and Autumn Period of China, was the author of "Sun Tzu," in which he said the maxim: "Know thyself, Know thy enemies, Fear not one-hundred battles."
In our cyberattack age, we could interpret "enemies" as "threats" (including attackers) and "thyself" as "our organization." Then, the maxim shows us what we should do to be effective for security.
Security risk assessment is the art of warfare of the cyberattack age that implements
Know thyself, Know thy enemies, Fear not one-hundred battles.

"Risk assessment" = The process to make clear the business risks with the assessment indices ①, ②, and ③

① The value (importance) of the objects (assets and business) of the assessment, the dimensions of and influence over possible risk
② The possible threats to the objects of the assessment and the probability of the occurrence
③ The acceptability (the vulnerability of the objects of the assessment and the unreadiness to provide measures) at the occurrence of any of the possible threats

The importance and the effectiveness of risk assessment

- To realize effective risk mitigation
- To realize effective security investment (to add measures, to select efficient test points)
- To provide a base for establishing a PDCA cycle and for continuing the maintenance and enhancement of security

Methods of and Challenges in Risk Assessment
– Various Methods of Security Risk Assessment and their Features and Challenges –

IPA

Methods of risk assessment and their features

Assessment method			Labor	Effectiveness
Baseline approach			Small	△
Informal approach			Small	× ?
Detailed risk assessment	Asset-based		Medium	○
	Scenario-based	Attack tree assessment (ATA)	Large	○
		Fault tree assessment (FTA)	Large	○
Combination approach			Large	◎

Challenges in detailed risk assessment

[Challenge A] Specific procedures and steps of the risk assessment are not clear.

[Challenge B] You want to avoid it because (it is said that) you need a huge amount of labor for risk assessment.

➡ The Guide shows you the answers to these challenges.

Two Types of Detailed Risk Assessment Presented
Asset-based Risk Assessment and Business Risk-based Risk Assessment

★ Asset-based risk assessment <Know thyself>

To conduct the risk assessment with the three assessment indices—the importance (value), the possible threats, and the vulnerability—on each of the assets (servers, terminals, communication devices, etc.) among the assets constituting the system you should protect. ⇒ Enable to assess the threats and the state of security comprehensively with respect to assets

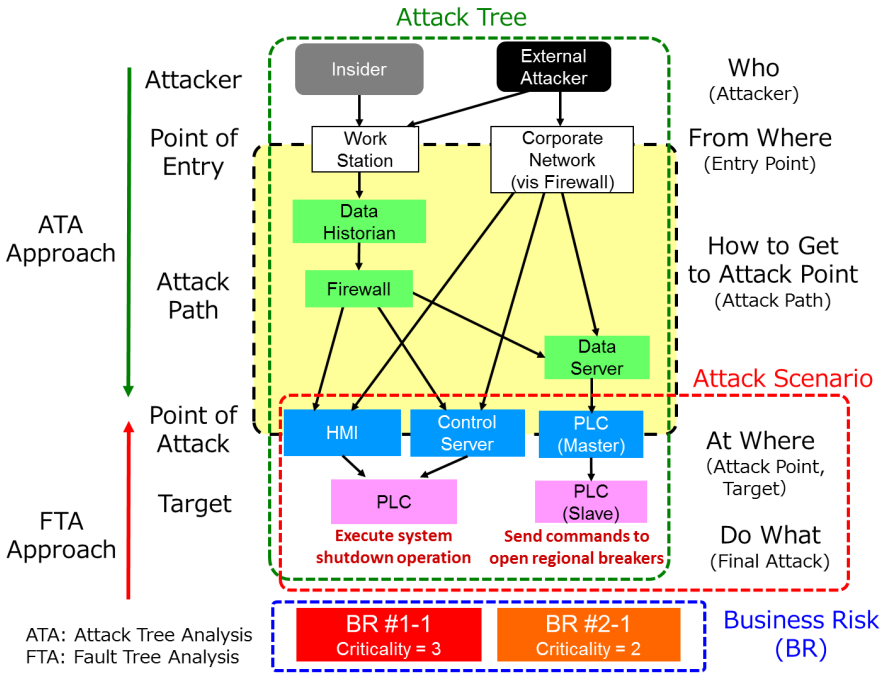
★ Business Risk-based risk assessment <Know thy enemies>

To define the business risk you want to avoid with respect to the business and service having been realized by the system you should protect, and to conduct a risk assessment with the three assessment indices: the level of the business risk at an occurrence, the probability the attack scenario may actually occur, and the vulnerability to the scenario (the acceptability of the scenario)

⇒ Enable to assess the attacks that lead to business

(The strongpoints of ATA and FTA are combined)

⇒ Desktop penetration testing

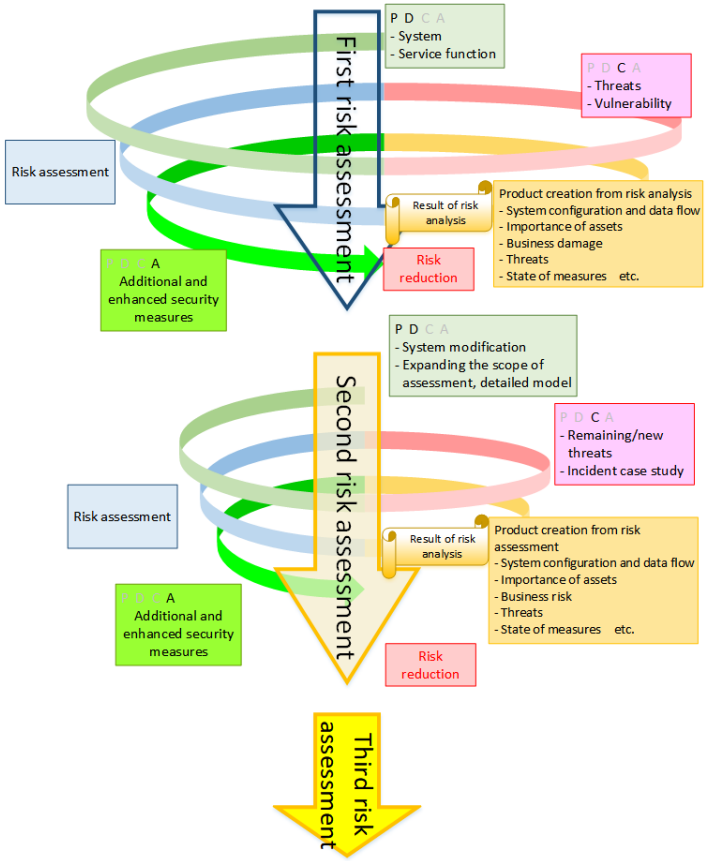


1. Risk Assessment as Security Measures

Main Guide Book pp.12-17

The importance and necessity of a risk assessment of control systema are presented.

- The necessity of the security measures on a control system
  - Changes in systems and components
  - Connection with external networks, storage media brought in from the outside
  - Characteristics of control systems
  - Increasing reports on vulnerabilities, targeted attacks, malware infections, and so forth
- The importance of risk assessment
  - The process to make clear the systems you should protect and the levels of the threats and the risk to the business realized by the systems
  - Essential as a security measure

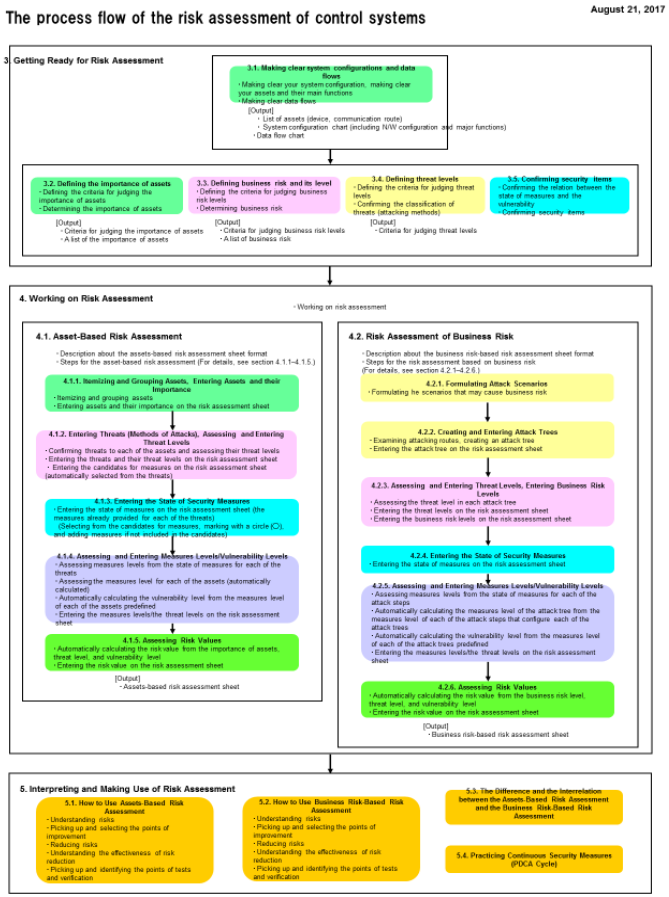


2. Overview and Work Flow of Risk Assessment

Main Guide Book pp.18-34

The comparison of the methods for risk assessment, the steps of the work, and how to use this guide are presented.

- The overview of risk assessment
  - Baseline approach
  - Informal approach
  - Detailed risk assessment
  - Combination approach
- The work flow of risk assessment
  - Asset-based risk assessment
  - Business risk-based risk assessment
- The composition of this guide and how to use it
  - The composition of this guide
  - A suggestion for conducting security assessment



3. Getting Ready for Risk Assessment

Main Guide Book pp. 35-36

Analyze your organization and understanding it. = "The most important step to know thyself"

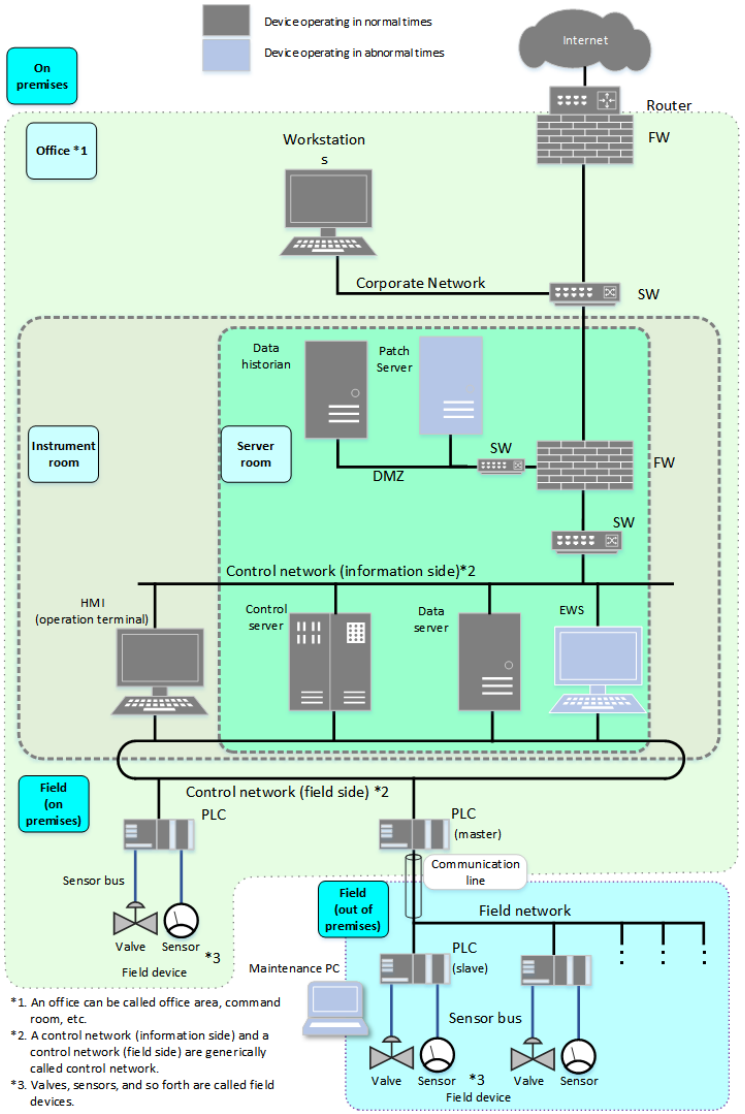
[Preparatory steps and their outputs]

Section	Preparation	Output
3.1	• Making clear your system configuration • Making clear your assets and their main functions • Making clear data flows	• A list of assets • System configuration chart • Data flow chart
3.2	• Defining the criteria for judging the importance of assets • Determining the importance of assets	• Criteria for judging the importance of assets • A list of the importance of assets
3.3	• Defining the criteria for judging business risk levels • Determining business risk	• Criteria for judging business risk levels • A list of business risk
3.4	• Defining the criteria for judging threat levels • Reviewing the classification of threats (attacking methods)	• Criteria for judging threat levels
3.5	• Reviewing the relation between the state of security and the vulnerability • Reviewing security items	

3. Getting Ready for Risk Assessment
3.1. Making Clear System Configurations and Data Flows

Main Guide Book pp. 37-71

- Finding assets
- Making clear and modeling your system configuration
  - Determining the scope of assessment
  - Model your system for assessment
  - Organizing assets and their auxiliary information
  - Narrowing down the assets you should analyze (Grouping and excluding)
  - Location
  - Describing the information on the connections among assets
- Making clear data flows
  - Mapping data flows on a system configuration chart



3. Getting Ready for Risk Assessment
3.2. Determining Importance of Assets

Main Guide Book pp. 72-82

- Importance of assets
  - One of the assessment indices in asset-based risk assessment
  - The assessment score (from 1 (lowest) to 3 (highest)) in consideration to the value of system assets, possible business risk caused by attacks, and the influence of the business continuity

[An example of defining the criteria for judging the importance of assets]

Assessment score	Judgment criterion
3	・If there is an attack on assets, the system may not be running for a long period. ・If assets leak information, a huge amount of loss may occur. ・If there is an attack on assets, a large-scale human suffering and/or environmental damage may occur.
2	・If there is an attack on assets, the system may not be running for a certain period. ・If assets leak information, a certain amount of loss may occur. ・If there is an attack on assets, a middle-scale human suffering and/or environmental damage may occur.
1	・If there is an attack on assets, the system may not be running for a short period. ・If assets leak information, a small amount of loss may occur. ・If there is an attack on assets, a small-scale human suffering and/or environmental damage may occur.

3. Getting Ready for Risk Assessment
3.3. Defining Business Risk and its Level

Main Guide Book pp. 83-87

- Business risk level
  - One of the assessment indices in business risk-based risk assessment
  - The assessment score (from 1 (lowest) to 3 (highest)) in consideration to the business risk caused by threats

[An example of defining the criteria for judging business risk levels]

Assessment score	Judgment criterion
3	Business damage is large. [Example] ・The damage, if it happens, influences the whole system. ・Some crucial or permanent damage may occur to the business operation of the company.
2	Business damage is medium. [Example] ・The damage, if it happens, influences only a part of the system. ・Some considerable or long-term damage may occur to the business operation of the company.
1	Business damage is small. [Example] ・The damage, if it happens, influences only a minor part of the system. ・Some medium or smaller temporary damage may occur to the business operation of the company.

3. Getting Ready for Risk Assessment
3.3. Defining Business Risk and its Level

Main Guide Book pp. 83-87

- Business risk
  - Events and situations that hinder the organization in its stable business operation and business continuity
  - Each business operator defines these based on the scope of risk and the impact on the business operation of the company at an occurrence.

Number	Business risk	Overview of Business risk	Business risk level
1	The supply of XX is suspended in a wide area.	An attack on a XX production facility, XX supply facility, etc. stops the supply in a wide area, influencing the community very much, causing a large amount of loss including the cost for compensation, and degrading the trust in the company very much.	3
2	The supply of XX is suspended in a limited area.	An attack on a XX production facility, XX supply facility, etc. stops the supply in a limited area, influencing the community, causing loss including the cost for compensation, and degrading the trust in the company.	2
3	The supply of off-spec XX	An attack on a XX production facility, XX supply facility, etc. alters the system to produce and deliver off-spec XX to the customer, influencing the community, causing loss including the cost for compensation, and degrading the trust in the company.	2
4	Destruction of facility	An attack on a XX production facility, XX supply facility, etc. destroys the facility and stops the supply, causing causalities (employees and neighbors), influencing the community very much, causing a large amount of loss including the cost for compensation, and degrading the trust in the company very much.	3
5	Causing a large-scale cost for measures	A cyberattack does not cause any such risk that stops the supply of XX, but it makes clear the vulnerability of the current measures, causing a huge amount of cost for the measures for solution.	1

3. Getting Ready for Risk Assessment
3.4. Defining Threat Levels

Main Guide Book pp. 88-91

- Threat levels
  - One of the assessment indices in two types of risk assessment
  - The assessment score (from 1 (lowest) to 3 (highest)) in consideration to the probability of the occurrences

[An example of defining the criteria for judging threat levels]

Assessment score	Judgment criterion
3	The probability of occurrence is high. [Example] ・If an attacker with whatever skills attempts an attack, the probability of its success is high. ・An occurrence is assumed in the near future.
2	The probability of occurrence is medium. [Example] ・If an attacker or group of attackers with a certain level of skills attempts an attack, there is probability of its success. ・An occurrence is assumed in the life cycle of the object of an assessment system.
1	The probability of occurrence is low. [Example] ・If nation-state attackers (military forces, intelligence agencies or similar bodies) attempts an attack, there is probability of its success. ・An occurrence is hardly assumable in the life cycle of the object of an assessment system.

3. Getting Ready for Risk Assessment
3.4. Defining Threat Levels

Main Guide Book pp. 88-91

[Excerpts from the threats (the methods of attacks) against assets (equipment)]

#	Threats (methods of attacks)	Description	Example
1	Unauthorized access	To hack into a device via network	● To exploit authentication information having been obtained maliciously (unauthorized login) ● To hack into a device that does not have any authentication mechanism ● To exploit vulnerability of a device ● To exploit defective settings (unnecessary processes are running, unnecessary ports are open, etc.)
2	Physical intrusion	To make an unauthorized intrusion into a restricted zone or area (any location where a device is placed etc.), or To unlock a device the access to which is physically limited (a device placed on a rack, in a box, etc.)	● Unauthorized intrusion into premises, an instrument room, or a server room ● Unauthorized access to a rack or housing box
3	Unauthorized manipulation	To directly manipulate the console of equipment etc. for intrusion and for attacking	● To exploit authentication information having been obtained maliciously (unauthorized login) ● To hack into a device that does not have any authentication mechanism ● To exploit vulnerability of a device
4	Erroneous operation	To induce incorrect operation by an internal user (an employee or a business partner with privilege to access the device) for attacking To do an act equivalent to an attack as a result of connecting some authorized media or device to a device	● To open an attachment to mail ● To bring in some authorized media that is infected with malware
5	Connecting unauthorized media or device	To bring in some unauthorized media or device (CD/DVD, USV device, etc.) and connect it to a device to attack	● Connecting unauthorized media ● To import data from media or to export data into media
6	Executing unauthorized processes	To make an unauthorized execution of an authorized program, command, service, etc. on the device to attack	● Executing unauthorized programs or commands ● Unauthorized execution of services
7	Malware infection	To have a device infected with malware (unauthorized program) and to execute the malware to attack the device	
8	Information theft	To steal information stored on a device (software, authentication information, information on configuration settings, encrypted keys, and/or other secret information)	● Stealing control parameters
9	Falsifying information	To falsify information stored on a device (software, authentication information, information on configuration settings, encrypted keys, and/or other secret information)	● To falsify control programs ● To falsify control parameters
10	Destroying information	To destroy information saved on a device (software, authentication information, information on configuration settings, encrypted key, and/or other secret information)	● To delete control data ● To forcefully encrypt control data
11	Unauthorized transmission	To send unauthorized commands (to change settings, to cut off power, etc.) or unauthorized data to another device	● To execute an unauthorized control command or data transmission command ● To falsify transmission data
12	Shutdown	To shutdown a device	● To execute an unauthorized shutdown command

3. Getting Ready for Risk Assessment
3.5. Reviewing Security Items

Main Guide Book pp. 94-104

- Vulnerability level
  - One of the assessment indices in two types of risk assessment
  - The assessment score (from 1 (lowest) to 3 (highest)) in consideration to the probability of accepting an occurring threat

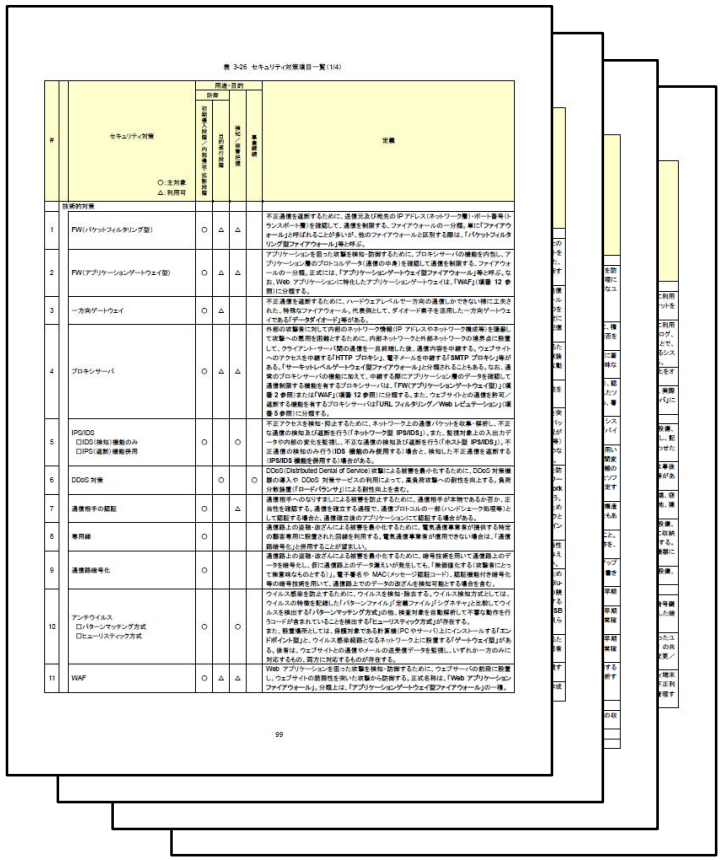
Assessment score		Judgment criterion
Vulnerability level	Measures level	
3	1	The probability of easily accepting a threat is high at its occurrence. No measures are taken for threats. The probability of successful attacks is high. [Example] ・In past examples, it was confirmed that attacks making use of vulnerability occurred and was successful to cause damage.
2	2	The probability of accepting a threat is medium at its occurrence. Some measures are taken for threats but are not sufficient. The probability of successful attacks is medium. [Example] ・General measures are taken. Whether an attack succeeds depends on the level of the attacker. ・In past examples, it was confirmed that attacks making use of vulnerability occurred and that no major damage was caused.
1	3	The probability of easily accepting a threat is low at its occurrence. Sufficient measures are provided for threats. [Example] ・Effective measures and multi-layered measures are provided. The probability of successful attacks is low. ・In past examples, no attacks occurred that made use of vulnerability.

3. Getting Ready for Risk Assessment
3.5. Reviewing Security Items

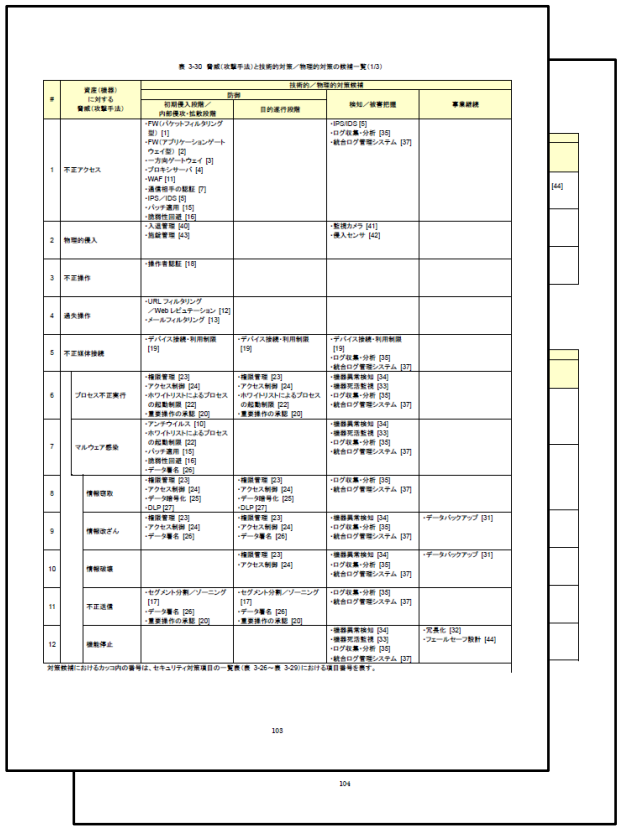
Main Guide Book pp. 94-104

Measures for threats and security as well as the list of measures are provided.

[Lists of security items (47 items in total]



[Lists of threats (methods of attacks) and the available technological or physical measures]

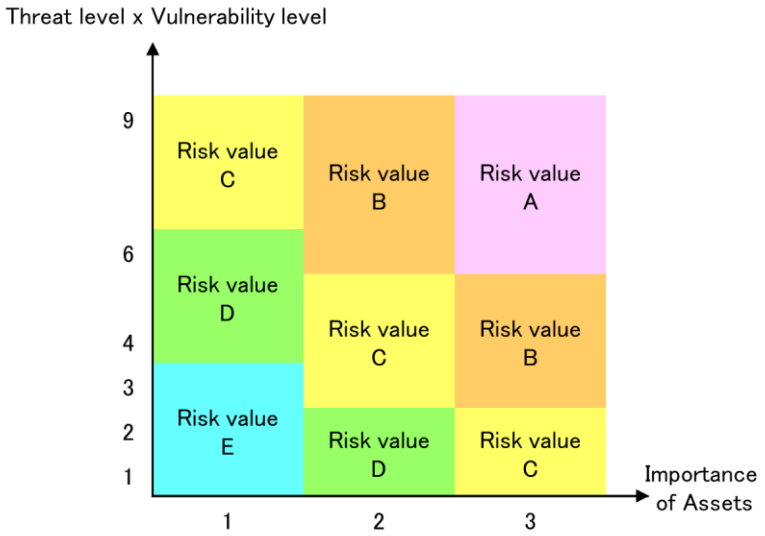


4. Working on Risk Assessment
4.1. Asset-based Risk Assessment

Main Guide Book pp.106-147

The methods of assessment in terms of the assets that compose a control system are described.
—The possible direct threats to the assets and the adequacy of the secutiry measures are assessed.—

- With respect to the assets groups that compose the control system you should protect,
- the levels of the risk (risk value) of each of the assets are calculated from
  - Importance of assets
  - Threat level
    (The probability of threat occurrences)
  - Vulnerability level
    (The probability of accepting
    a threat at its occurrence)



Definitions of the risk value areas by each of assets

4. Working on Risk Assessment
4.1. Asset-based Risk Assessment

Main Guide Book pp.106-147

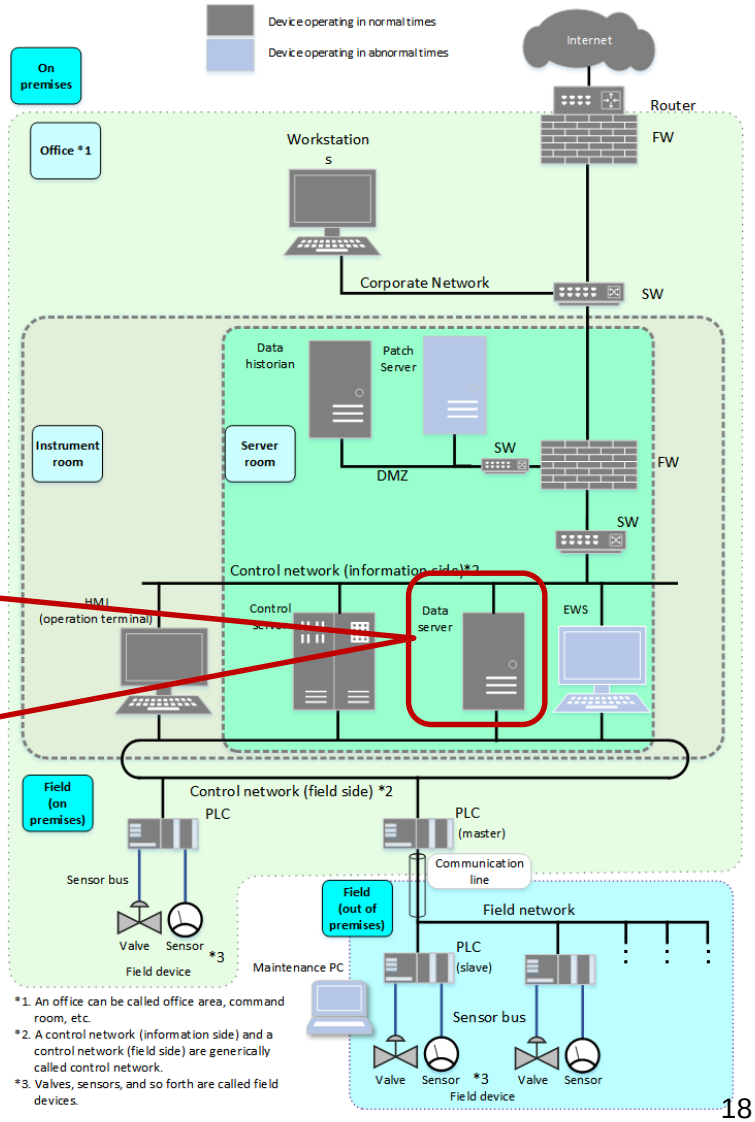
- The assets that compose the control system you should protect are grouped depending on functions, types, etc.
- With respect to the assets groups
  - ★ Threats (methods of attacks)
  - ★ State of security

  are entered. → Vulnerability level is determined

Threats (methods of attacks)
Unauthorized access
Malware infection
Falsifying information
Suspension of functions, etc.

State of security
Authentication of the opposite end of communication
White list
Authenticating operators
Management of authority, etc.

Vulnerability level of each threat



4. Working on Risk Assessment
4.1. Asset-based Risk Assessment

Main Guide Book pp.106-147

Asset-based risk assessment sheet

Signs: ○ Measures provided × Measures not provided Grayed out column: The threats not considered for the assets

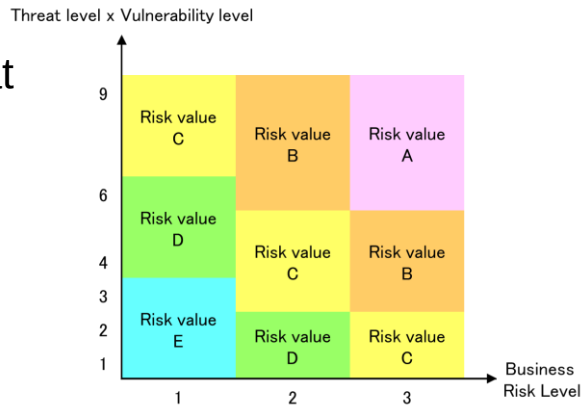
Number	Classification of Assets	Target Device	Assessment index				Threats (methods of attacks)	Measures						Measures Level
								Protection				Detection/Understanding Risk	Business Continuity	
			Threat Level	Vulnerability Level	Importance of Assets	Risk Value		Intrusion/Diffusion Phase		Objective-Execution Phase				Each Threat
1	Information assets	**Data server**	2	2		B	Unauthorized access	FW (packet filtering type) FW (application gateway type) One-way gateway Proxy server WAF Authentication of the opposite end of communicatio ○ IPS/IDS Applying patches Avoiding vulnerability				IPS/IDS Collecting/analyzing logs Unified log management system		2
2			2	1		C	Physical intrusion	Entrance/exit management (IC card, biometric ide ○ Lock management ○				Monitoring camera ○ Intrusion sensor ○		3
3			2	2		B	Unauthorized manipulation	Operator authentication (ID/Pass) ○						2
4			2	3		A	Misperception-induced operation	URL filtering/Web reputation Mail filtering						1
5			2	3		A	Connecting unauthorized media or device	Restriction on device connection and use		(Ditto)		Restriction on device connection and use Collecting/analyzing logs Unified log management system		1
6			2	2		B	Executing unauthorized processes	Management of authority ○ Access control A white list to restrict the startups of processes ○ Confirming important operations		(Ditto) (Ditto) (Ditto) (Ditto)		Detecting device errors Device alive monitoring Collecting/analyzing logs Unified log management system		2
7			1	2		C	Malware infection	Anti-virus A white list to restrict the startups of processes ○ Applying patches Avoiding vulnerability Data signature				Detecting device errors Device alive monitoring Collecting/analyzing logs Unified log management system		2
8			3	2	3	A	Information theft	Management of authority ○ Access control Data encryption DLP		(Ditto) (Ditto) (Ditto) (Ditto)		Collecting/analyzing logs Unified log management system		2
9			3	3		A	Falsifying information	Management of authority Access control Data signature		(Ditto) (Ditto) (Ditto)		Detecting device errors Collecting/analyzing logs Unified log management system	Data backup ○	1
10			3	3		A	Destroying information			Management of authority ○ Access control		Detecting device errors Collecting/analyzing logs Unified log management system	Data backup ○	1
11			3	3		A	Unauthorized transmission	Segment dividing/zoning Data signature Confirming important operations		(Ditto) (Ditto) (Ditto)		Collecting/analyzing logs Unified log management system		1
12			2	3		A	Stopping a function					Detecting device errors Device alive monitoring Collecting/analyzing logs Unified log management system	Applying redundancy Failsafe design	1
13			3	3		A	Heavy load attack	DDoS measures				Detecting device errors Device alive monitoring Collecting/analyzing logs Unified log management system	Applying redundancy Failsafe design	1
14			2	2		B	Theft	Lock management ○		(Ditto)		Lock management ○		2
15			3	3		A	Information theft from disassembly in the case of a theft or disposal	Tamper resistance Obfuscation Secure erase		(Ditto) (Ditto) (Ditto)				1
16			3	2		A	Path blocking	Entrance/exit management (IC card, biometric ide ○ Lock management ○				Detecting device errors Device alive monitoring Collecting/analyzing logs Unified log management system Monitoring camera ○ Intrusion sensor ○	Applying redundancy	2

4. Working on Risk Assessment
4.2. Business Risk-based Risk Assessment

Main Guide Book pp.148-231

The means for scenario-based detailed risk assessment are described by using an attack tree.

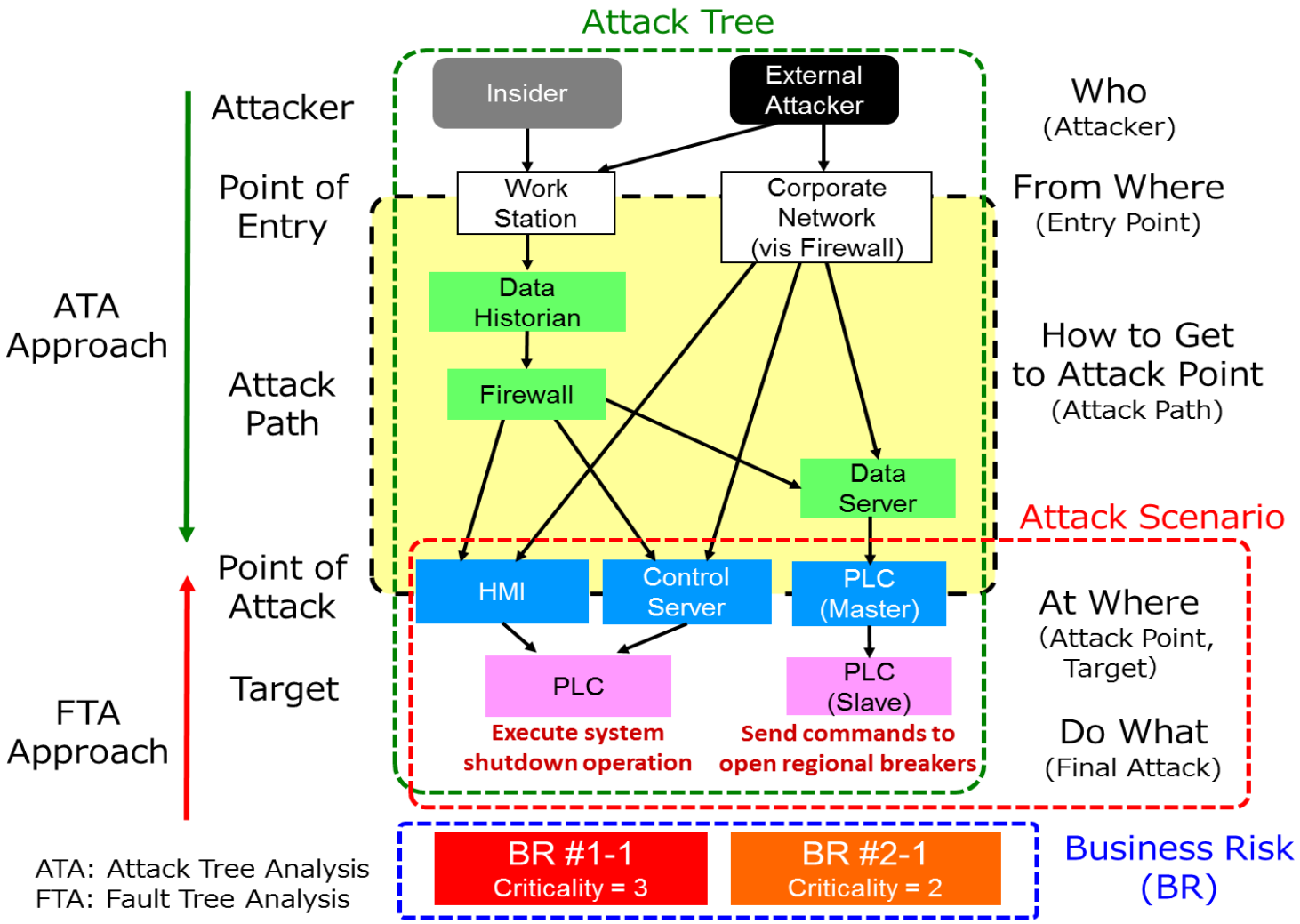
- Attack scenario
  - The scenarios that embody a point of attack, target and final attack that may cause a business risk an organization wants to avoid
- Attack tree
  - The steps of a series of attacks that embody an attacker, an entry point and attack path to realize an attack scenario in addition to a point of attack, target and final attack included in the attack scenario
- The levels of the risk (risk value) of each attack tree are calculated from
  - Threat level (The probability of threat occurrences)
  - Vulnerability level (The probability of accepting a threat at its occurrence)
  - Business risk level (The severity of business risk)



Definitions of the risk value areas by each attack tree

4. Working on Risk Assessment
4.2. Business Risk-based Risk Assessment

Main Guide Book pp.148-231



4. Working on Risk Assessment
4.2. Business Risk-based Risk Assessment

Main Guide Book pp.148-231

Business Risk-Based Risk Assessment Sheet

1. The supply of XX is suspended in a wide area.

Number	Attack scenario	Attack tree/attack step	Assessment index: Threat level	Assessment index: Vulnerability level	Assessment index: Business risk level	Assessment index: Risk value	Measures: Protection: Intrusion/diffusion phase	Measures: Protection: Objective-Execution Phase	Measures: Detection/understanding risk	Measures: Business Continuity	Measures level: Attack step	Measures level: Attack tree	Attack tree number: Attack tree number	Attack tree number: Configuration step (number)
	1-1	An unauthorized transmission of a command interrupts the supply in a wide area.												
1		Point of intrusion = Monitoring terminal A malicious third party has an unauthorized access to the monitoring terminal on the information network.					FW (packet filtering type) Applying patches Authentication of the opposite end of communications Authenticating operators ○	Management of authority ○ Access control ○	Collecting/analyzing logs ○		2			
2		A malicious third party accesses the data historian from a monitoring terminal.					FW (packet filtering type) ○ Applying patches Authentication of the opposite end of communications Authenticating operators ○	Management of authority ○ Access control ○	Collecting/analyzing logs ○		2			
3		A malicious third party accesses the firewall from the data historian.					FW (packet filtering type) ○ Applying patches Authentication of the opposite end of communications Authenticating operators ○	Management of authority ○ Access control ○	Collecting/analyzing logs ○		2			
4		A malicious third party accesses from the firewall to HMI (operation terminal).					Applying patches Authentication of the opposite end of communications Authenticating operators ○	Management of authority ○ Access control ○	Collecting/analyzing logs ○		2			
5		A malicious third party stops a wide-area supply from HMI (operation terminal) (by sending an unauthorized supply-stop command) and the supply is suspended in a wide area.	2	2	3			Confirming important operations	Detecting device errors ○ Collecting/analyzing logs ○		1	2	#1	1, 2, 3, 4, 5
6		A malicious third party accesses from the firewall to a control server.					Applying patches Authentication of the opposite end of communications Authenticating operators ○	Management of authority ○ Access control ○	Collecting/analyzing logs ○		2			
7		A malicious third party stops a wide-area supply from the control server (by sending an unauthorized supply-stop command in the wide area) and the supply is suspended in a wide area.	2	2	3			Confirming important operations	Detecting device errors ○ Collecting/analyzing logs ○		1	2	#2	1, 2, 3, 6, 7
8		A malicious third party accesses from the firewall to a data server.					Applying patches Authentication of the opposite end of communications Authenticating operators ○	Management of authority ○ Access control ○	Collecting/analyzing logs ○		2			
9		A malicious third party accesses the PLC (master) from the data server.					Applying patches Authentication of the opposite end of communications Authenticating operators	Management of authority Access control	Collecting/analyzing logs ○		1			
10		A malicious third party stops a wide-area supply from the PLC (master) by sending an unauthorized supply-stop command and the supply is suspended in a wide area.	2	2	3			Confirming important operations	Detecting device errors ○ Collecting/analyzing logs ○		1	2	#3	1, 2, 3, 8, 9, 10
11		A malicious third party has the monitor terminal infected with some malware.					Anti-virus ○ Applying patches ○ A white list as a list of restrictions on the startups of processes		Detecting device errors Collecting/analyzing logs ○		2			

5. Interpreting and Making Use of Risk Assessment

Main Guide Book pp. 232-255

There are new steps for enhancing the security of control systems.

- Interpreting and utilizing the result of a risk assessment
  - To find the security weak points and mitigate the risk of cyberattacks, lower the risk values obtained as the result of the assessment as much as possible
- Making use of risk values
  - Understanding risk values
  - Picking up and selecting the points of improvement
  - Mitigating risks
  - Confirming the effectiveness of risk mitigation
  - Picking up and identifying test points (where to test the current measures in a security test)
- The difference in the usage and the relation between the two types of risk assessment
- Practicing continuous security measures (PDCA cycle)

6. Security Test

Main Guide Book pp. 256-275

The secureness and the effectiveness of the state of security and the robustness against threats are verified.

- Objectives and effectiveness of security tests
  - Using actual machines to confirm the result of a risk assessment of a control system
  - Investigating the current situation of a control system
- The types, objectives, and targets of a security test

Objectives	Target of test		
	Network	OS/middleware	Application
Detecting known vulnerability	・Vulnerability inspection (System security inspection)		・Vulnerability inspection (Web application diagnosis)
Detecting zero-day vulnerability	・Fuzzing		・Source code security review
Verifying the possibility of intrusion	・Penetration testing		
Inspecting suspicious communications	・Packet capture test		
Investigating unauthorized network devices	・Network discovery ・Wireless scanning		

7. Additional Requirements from Security Standards

Main Guide Book pp. 276-281

The state of the implementation of specific security measure items is confirmed and assessed further in detail.

- Selecting encryption techniques and their usage standards
- Measures for targeting type attacks
- Measures against internal threats
- Various settings on the firewall
- Security measures for external storage media

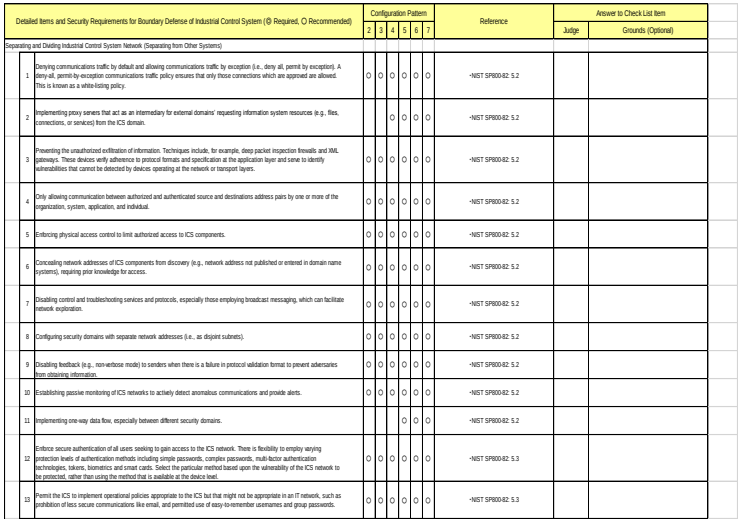
- Providing assessment items in various additional standards as a check list
  - Assessment items and security requirements
    - Setting "required" or "recommended"
  - Reference
    - Related international standards, industry standards and other referential points
  - Assumed respondent/business division (Check list for "measures for internal threat check list" only)
  - Answer column

Not limited to control systems, applicable to information systems.

Appendix

Main Guide Book pp.284-347

- How to use firewalls for security zone segmentation
  - Definition of firewalls
  - Classification of firewalls
  - Architecture to implement firewalls
- Check list for specific security measures
  - Check list to use encryption techniques
  - Check list for measures for targeted attacks
  - Check list for measures for internal misconducts
  - Check list for firewall configuration
  - Check list for measures for external storage media
- Control system incidents (case studies)
- Glossary



	Detailed Items and Security Requirements for Boundary Defense of Industrial Control System (◎ Required, ○ Recommended)	Configuration Pattern 2	3	4	5	6	7	Reference	Answer to Check List Item: Judge	Grounds (Optional)
Separating and Dividing Industrial Control System Network (Separating from Other Systems)										
1	Denying communications traffic by default and allowing communications traffic by exception (i.e., deny all, permit by exception). A deny-all, permit-by-exception communications traffic policy ensures that only those connections which are approved are allowed. This is known as a white-listing policy.	○	○	○	○	○	○	-NIST SP800-82 5.2		
2	Implementing proxy severs that act as an intermediary for external domains' requesting information system resources (e.g., files, connections, or services) from the ICS domain.				○	○	○	-NIST SP800-82 5.2		
3	Preventing the unauthorized exfiltration of information. Techniques include, for example, deep packet inspection firewalls and XML gateways. These devices verify adherence to protocol formats and specification at the application layer and serve to identify vulnerabilities that cannot be detected by devices operating at the network or transport layers.	○	○	○	○	○	○	-NIST SP800-82 5.2		
4	Only allowing communication between authorized and authenticated source and destinations address pairs by one or more of the organization, system, application, and individual.	○	○	○	○	○	○	-NIST SP800-82 5.2		
5	Enforcing physical access control to limit authorized access to ICS components.	○	○	○	○	○	○	-NIST SP800-82 5.2		
6	Concealing network addresses of ICS components from discovery (e.g., network address not published or entered in domain name systems), requiring prior knowledge for access.	○	○	○	○	○	○	-NIST SP800-82 5.2		
7	Disabling control and troubleshooting services and protocols, especially those employing broadcast messaging, which can facilitate network exploration.	○	○	○	○	○	○	-NIST SP800-82 5.2		
8	Configuring security domains with separate network addresses (i.e., as disjoint subnets).	○	○	○	○	○	○	-NIST SP800-82 5.2		
9	Disabling feedback (e.g., non-verbose mode) to senders when there is a failure in protocol validation format to prevent adversaries from obtaining information.	○	○	○	○	○	○	-NIST SP800-82 5.2		
10	Establishing passive monitoring of ICS networks to actively detect anomalous communications and provide alerts.	○	○	○	○	○	○	-NIST SP800-82 5.2		
11	Implementing one-way data flow, especially between different security domains.				○	○	○	-NIST SP800-82 5.2		
12	Enforce secure authentication of all users seeking to gain access to the ICS network. There is flexibility to employ varying protection levels of authentication methods including simple passwords, complex passwords, multi-factor authentication technologies, tokens, biometrics and smart cards. Select the particular method based upon the vulnerability of the ICS network to be protected, rather than using the method that is available at the device level.	○	○	○	○	○	○	-NIST SP800-82 5.3		
13	Permit the ICS to implement operational policies appropriate to the ICS but that might not be appropriate in an IT network, such as prohibition of less secure communications like email, and permitted use of easy-to-remember usernames and group passwords.	○	○	○	○	○	○	-NIST SP800-82 5.3		

Examples of Conducting Risk Assessment on ICS

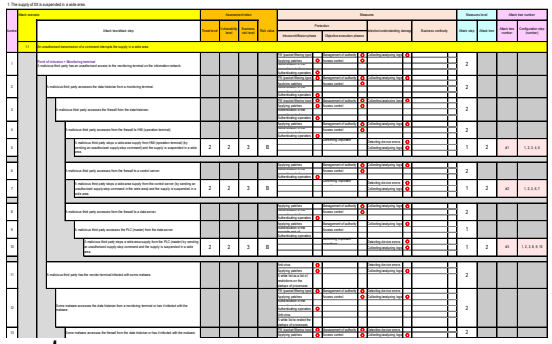
Security Risk Assessment Guide for ICS – Supplement

Supplement pp. 1-70

Here are examples of conducting perfect risk assessment on exemplary model systems.

① System configuration
② A list of assets
③ Data flow chart
④ Criteria for judging the importance of assets
⑤ A list of the importance of assets
⑥ Criteria for judging business risk levels
⑦ A list of business risk
⑧ Criteria for judging assets levels
⑨ Asset-based risk assessment sheet
⑩ Attack scenarios
⑪ Business risk-based risk assessment sheet
⑫ Results of the risk assessment of control systems (Measures for improvement to mitigate risk)

Business Risk-Based Risk Assessment Sheet



Download all risk assessment sheets (Excel files) at:
https://www.ipa.go.jp/security/controlsystem/riskassessment.html

Conclusion
"Security Risk Assessment Guide for ICS"

This is a risk assessment guide for enabling the overall enhancement of control system security.

  - Enhancing the understanding of risk assessment and promoting it
  - Presenting specific procedures and guidance for conducting security assessment
- Explaining two types of detailed risk assessment methods
  - Asset-based, business risk-based
- Providing materials for risk assessment
  - Risk assessment sheet (formats, examples of actual cases)
  - Lists of threats (methods of attacks) and measures
  - Detailed check lists for specific security measures
- Presenting the examples of how to utilize the results of risk assessment
  - How to improve measures to mitigate risk
  - Guidance to consider security tests