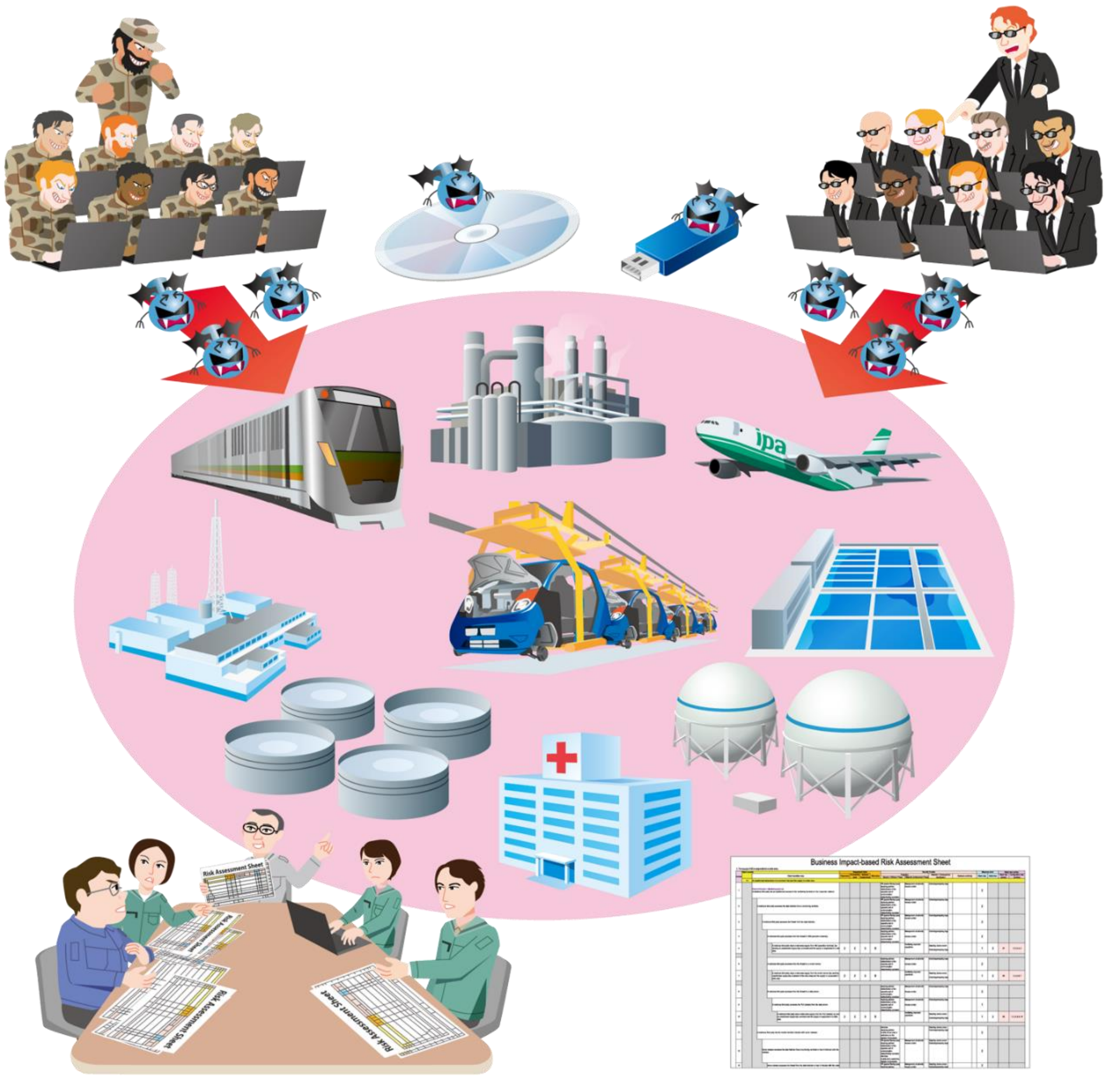
Practical Examples of Security Risk Assessment for Industrial Control Systems

~ Separate Volume of Security Risk Assessment Guide for Industrial Control Systems (ICS) ~



March 2020

IPA
Information-technology Promotion Agency, Japan
IT Security Center

Contents

Figure Contents

Table Contents

Introduction

"Security Risk Assessment Guide for Industrial Control Systems (ICS)" (hereinafter, the "Guide") focuses primarily on developing a correct understanding of security risk analysis, and explaining methodologies, including specific procedures used to prepare risk assessment sheets. Therefore, due to limitations in the paper space available, we have kept the focus of explanatory notes provided on examples of asset-based risk assessment sheets for certain system assets, and business impact-based risk assessment sheets covering attack scenarios and attack trees for certain business impacts.

In this separate volume, we provide descriptions on the implementation of asset-based risk analysis and business impact-based risk analysis for typical model systems. The three main objectives of this are as follows.

(1) Present an overall picture of risk analysis and analysis results

Concerns of increase in the man-hours and the number of outputs required from risk analysis in detailed risk assessment are key factors in why it is often shied away from. Here, we present an overall picture of the amount of man-hours required, and the extent to which analysis outputs are prepared when actually conducting risk analysis on a model system. In this, we hope to present risk analysis as something that is "not as bad as it looks", providing a practical look at implementing risk analysis by understanding the specific procedures involved, using assessment materials (threats, measures, the correspondence charts for such, assessment sheet formats, etc.), and methods for refining analysis targets.

(2) Provide overall materials by presenting the results of a risk assessment sheet

We hope to reduce the man-hours required for risk analysis by providing the results of a risk assessment sheet for a typical model control system for re-use and customizing materials, where possible, when conducting system analysis in your own organization.

(3) Introduction to variations in compiling risk assessment sheets

In business impact-based risk analysis, the risk assessment sheet could potentially be compiled in various ways based on the complexity of the analysis target model, and the intended purpose for using the risk analysis results. We hope the specific examples of such variations provided can serve as a reference for choosing the optimal method for compiling the risk assessment sheet when performing risk analysis on target systems in your own organization.

We hope that this separate volume helps provide a clear picture of the total number of man-hours required for, and outputs (interim and final deliverables of works) produced from risk analysis in detailed risk assessment, and aids a large number of businesses with control systems in taking the first step toward conducting risk analysis in detailed risk assessment.

October 2, 2017

Megumi Kinoshita,	Information-technology Promotion Agency, Japan
Shigehito Kosukegawa,	Information-technology Promotion Agency, Japan
Hirosato Tsuji,	Information-technology Promotion Agency, Japan
Hiroko Okashita,	Information-technology Promotion Agency, Japan (At the time of publication)
Seiya Kudo,	Information-technology Promotion Agency, Japan (At the time of publication)
Eiji Shiota,	Information-technology Promotion Agency, Japan
Satoshi Fukuhara,	Information-technology Promotion Agency, Japan
Kazuyuki Yoshida,	Information-technology Promotion Agency, Japan (At the time of publication)
Toshiyuki Kuwana,	Information-technology Promotion Agency, Japan
Chisato Konno,	Information-technology Promotion Agency, Japan

Notes on the Revised Second Edition

Added and amended output examples presented in the separate volume according to additions and amendments made to the Revised Second Edition of the Guide. Added new interim output examples recommended during risk analysis.

We hope that this separate volume helps provide a clear picture of the total number of man-hours required for, and outputs (interim and final deliverables of works) produced from risk analysis in detailed risk assessment, and aids a large number of businesses with control systems in taking the first step toward conducting risk analysis in detailed risk assessment.

Shigehito Kosukegawa, Information-technology Promotion Agency, Japan
Gen Kinoshita, Information-technology Promotion Agency, Japan
Megumi Kinoshita, Information-technology Promotion Agency, Japan
Hirosato Tsuji, Information-technology Promotion Agency, Japan
Hiroko Okashita, Information-technology Promotion Agency, Japan
(At the time of publication)
Eiji Shiota, Information-technology Promotion Agency, Japan
Satoshi Fukuhara, Information-technology Promotion Agency, Japan
Kazuyuki Yoshida, Information-technology Promotion Agency, Japan
(At the time of publication)
Toshiyuki Kuwana, Information-technology Promotion Agency, Japan

This page has intentionally been left blank.

1. Structure of This Volume

This volume introduces examples of risk analysis being implemented based on the risk analysis methods described in the Guide.

- Presumptions

  This volume assumes that the reader has read and understood the risk analysis methods, and ways of utilizing risk analysis results, described in the Guide. In addition, details of risk analysis flows in this volume reference descriptions provided in the Guide. Chapter, section and item numbers (*x.y.z*), and figure and table numbers (*Figure x-y*, *Table x-y*) written in blue italics refer to parts of the Guide text.

- Target system for risk analysis introduced in this volume

  The control system introduced in the "Configuration Diagram of a Typical Control System" in *Section 3.2.3. Figure 3-8* of the Guide is used as the target system for risk analysis (hereinafter, the "model system"). As indicated in the Guide, devices (used) in non-regular operation are excluded from risk analysis. Risk analysis implements focuses solely on devices (used) in regular operation.

- Structure and features of this volume

  Although the Guide introduces some examples of asset-based and business impact-based risk analysis (assessment sheets) implemented on the model system, this volume presents the full range of risk analysis implementation examples. In addition, it should be noted that the examples provided in the Guide and this volume sometimes use different threat levels, vulnerability levels, risk values, and other assessment values.

  - Implementation examples of asset-based risk analysis

    The examples presented show asset-based risk analysis being performed on all assets of the model system in regular operation.

  - Implementation examples of business impact-based risk analysis

    The examples presented show business impact-based risk analysis being performed considering attack scenarios for five types of business impacts on the model system. Further, a total of three assessment sheet formats are presented as assessment sheet formats used for business impact-based risk analysis results - the standard assessment sheet format, and two other formats that are put together in different ways from the standard sheet. We hope this serves as a reference when considering the assessment sheet format best suited to the target model and objective of the risk analysis you are performing.

  - Use examples of risk analysis results

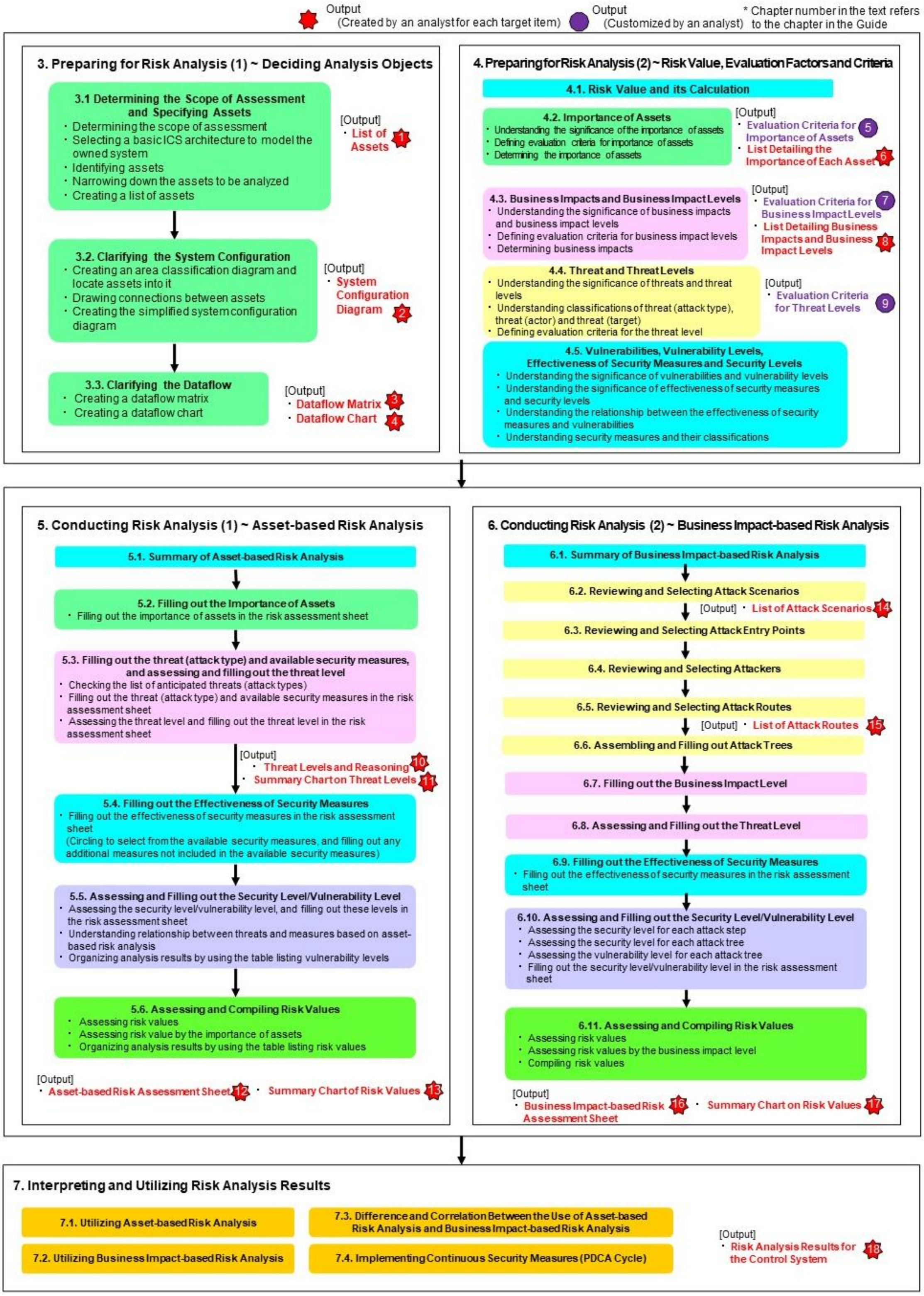
    Here we present improvement measures for reducing the risk of business impact to the model system on the basis of business impact-based risk analysis implementation examples.

- Risk analysis flow and outputs

  The risk analysis flow and outputs for the implementation examples described in Chapters 2 to 5 are outlined in Figure 1-1. (Figure 1-1. indicates the outputs depicted in *Figure 2-2* of the Guide as numbers (1 to 17) in the separate volume) The ★ in the figure depicts outputs created by the person in charge of risk analysis, and ⬣ is used for outputs obtained by customizing examples outlined in the Guide.

Table 1-1. List of Outputs

2. Preparing for Risk Assessment				
Title in this Volume	Output		Output Use	Guide
2.1	①	List of Assets	Asset/Business Impact-based	*3.1.5. Table 3-9*
2.2	②	System Configuration Diagram	Asset/Business Impact-based	*3.2.3. Figure 3-8*
2.3.①	③	Dataflow Matrix	Asset/Business Impact-based	*3.3.1. Table 3-10*
2.3.②	④	Dataflow Chart	Asset/Business Impact-based	*3.3.2. Figure 3-14*
2.4	⑤	Evaluation Criteria for Importance of Assets	Asset-based	*4.2.2. Table 4-5*
2.5	⑥	List Detailing the Importance of Each Asset	Asset-based	*4.2.3. Table 4-9*
2.6	⑦	Evaluation Criteria for Business Impact Levels	Business Impact-based	*4.3.2. Table 4-11*
2.7	⑧	List Detailing Business Impacts and Business Impact Levels	Business Impact-based	*4.3.3. Table 4-12*
2.8	⑨	Evaluation Criteria for Threat Levels	Asset/Business Impact-based	*4.4.5. Table 4-20 to Table 4-24*
3. Asset-based Risk Analysis				
Title in this Volume	Output			Guide
3.1	⑩	Summary Chart of Threat Levels		-
3.2	⑪	Asset-based Risk Assessment Sheet		*Chapter 5*
3.3.①	⑫	Summary Chart of Vulnerability Levels		-
3.3.②	⑬	Summary Chart on Risk Values		-
4. Asset-based Risk Analysis				
Title in this Volume	Output			Guide
4.1	⑭	List of Attack Scenarios		*6.2.2. Table 6-6*
4.2	⑮-1	List of Attack Routes		*6.5.1. Table 6-11 to Table 6-12*
4.2	⑮-2	Attack Route Diagram		*6.5.1. Figure 6-9*
4.3	⑯	Business Impact-based Risk Assessment Sheet		*6.6.4. ~ 6.11.*
4.4	⑰	Summary Chart on Risk Values		*6.11.3.*
5. Use of Risk Assessment				
Title in this Volume	Output			Guide
5	⑱	Risk Analysis Results for the Control System		*Chapter 7*


Output (Created by an analyst for each target item)

Output (Customized by an analyst)

* Chapter number in the text refers to the chapter in the Guide

3. Preparing for Risk Analysis (1) ~ Deciding Analysis Objects

3.1 Determining the Scope of Assessment and Specifying Assets
- Determining the scope of assessment
- Selecting a basic ICS architecture to model the owned system
- Identifying assets
- Narrowing down the assets to be analyzed
- Creating a list of assets

[Output]
- List of Assets 1

3.2. Clarifying the System Configuration
- Creating an area classification diagram and locate assets into it
- Drawing connections between assets
- Creating the simplified system configuration diagram

[Output]
- System Configuration Diagram 2

3.3. Clarifying the Dataflow
- Creating a dataflow matrix
- Creating a dataflow chart

[Output]
- Dataflow Matrix 3
- Dataflow Chart 4

4. Preparing for Risk Analysis (2) ~ Risk Value, Evaluation Factors and Criteria

4.1. Risk Value and its Calculation

4.2. Importance of Assets
- Understanding the significance of the importance of assets
- Defining evaluation criteria for importance of assets
- Determining the importance of assets

[Output]
- Evaluation Criteria for Importance of Assets 5
- List Detailing the Importance of Each Asset 6

4.3. Business Impacts and Business Impact Levels
- Understanding the significance of business impacts and business impact levels
- Defining evaluation criteria for business impact levels
- Determining business impacts

[Output]
- Evaluation Criteria for Business Impact Levels 7
- List Detailing Business Impacts and Business Impact Levels 8

4.4. Threat and Threat Levels
- Understanding the significance of threats and threat levels
- Understanding classifications of threat (attack type), threat (actor) and threat (target)
- Defining evaluation criteria for the threat level

[Output]
- Evaluation Criteria for Threat Levels 9

4.5. Vulnerabilities, Vulnerability Levels, Effectiveness of Security Measures and Security Levels
- Understanding the significance of vulnerabilities and vulnerability levels
- Understanding the significance of effectiveness of security measures and security levels
- Understanding the relationship between the effectiveness of security measures and vulnerabilities
- Understanding security measures and their classifications

5. Conducting Risk Analysis (1) ~ Asset-based Risk Analysis

5.1. Summary of Asset-based Risk Analysis

5.2. Filling out the Importance of Assets
- Filling out the importance of assets in the risk assessment sheet

5.3. Filling out the threat (attack type) and available security measures, and assessing and filling out the threat level
- Checking the list of anticipated threats (attack types)
- Filling out the threat (attack type) and available security measures in the risk assessment sheet
- Assessing the threat level and filling out the threat level in the risk assessment sheet

[Output]
- Threat Levels and Reasoning 10
- Summary Chart on Threat Levels 11

5.4. Filling out the Effectiveness of Security Measures
- Filling out the effectiveness of security measures in the risk assessment sheet (Circling to select from the available security measures, and filling out any additional measures not included in the available security measures)

5.5. Assessing and Filling out the Security Level/Vulnerability Level
- Assessing the security level/vulnerability level, and filling out these levels in the risk assessment sheet
- Understanding relationship between threats and measures based on asset-based risk analysis
- Organizing analysis results by using the table listing vulnerability levels

5.6. Assessing and Compiling Risk Values
- Assessing risk values
- Assessing risk value by the importance of assets
- Organizing analysis results by using the table listing risk values

[Output]
- Asset-based Risk Assessment Sheet 12
- Summary Chart of Risk Values 13

6. Conducting Risk Analysis (2) ~ Business Impact-based Risk Analysis

6.1. Summary of Business Impact-based Risk Analysis

6.2. Reviewing and Selecting Attack Scenarios

[Output]
- List of Attack Scenarios 14

6.3. Reviewing and Selecting Attack Entry Points

6.4. Reviewing and Selecting Attackers

6.5. Reviewing and Selecting Attack Routes

[Output]
- List of Attack Routes 15

6.6. Assembling and Filling out Attack Trees

6.7. Filling out the Business Impact Level

6.8. Assessing and Filling out the Threat Level

6.9. Filling out the Effectiveness of Security Measures
- Filling out the effectiveness of security measures in the risk assessment sheet

6.10. Assessing and Filling out the Security Level/Vulnerability Level
- Assessing the security level for each attack step
- Assessing the security level for each attack tree
- Assessing the vulnerability level for each attack tree
- Filling out the security level/vulnerability level in the risk assessment sheet

6.11. Assessing and Compiling Risk Values
- Assessing risk values
- Assessing risk values by the business impact level
- Compiling risk values

[Output]
- Business Impact-based Risk Assessment Sheet 16
- Summary Chart on Risk Values 17

7. Interpreting and Utilizing Risk Analysis Results

7.1. Utilizing Asset-based Risk Analysis

7.2. Utilizing Business Impact-based Risk Analysis

7.3. Difference and Correlation Between the Use of Asset-based Risk Analysis and Business Impact-based Risk Analysis

7.4. Implementing Continuous Security Measures (PDCA Cycle)

[Output]
- Risk Analysis Results for the Control System 18

Figure 1-1: Risk Analysis Flow and Outputs

- Example and explanation of outputs

  The risk analysis presented in this volume is implemented in accordance with the “risk analysis flow”. Interim materials (outputs) are prepared at each step to complete the risk analysis. Examples of these outputs are presented according to the risk analysis flow. The main points to be aware of when preparing outputs are described below.

(Example)

[Task 2.1.①] Preparing a list of assets for the system being analyzed.

- Refer to *Table 3-9* in the Guide when specifying the asset category (device or route of data), functions, installation location, connected network, presence of a maintenance port, type of data handled, vendor, OS, and protocols.

[Output 2.1.①]

No		1	2
Asset Name		Monitoring Terminal	Firewall
Type of Assets	IT Asset	○	
	OT Asset		
	Network Asset (with Communication Control Functions)		○
	Network Asset (without Communication Control Functions)		
Asset Functions	Input/Output	○	
	Storing Data		
	Issuing Commands		
	Gateway Function		○
Type of Communication Line		▨	▨
Installation Location		Office	Server Room
Connected Network	Information Network	○	○
	DMZ		○
	Control Network (Information Side)		○
	Control Network (Field Side)		
	Field Network		
	Other		
Network Connected to Maintenance Port		×	Information Network
Presence of Operation Interface		○	×

[Explanation 2.1.(1)]

- Organizing information needed to perform risk analysis in detailed risk assessment in a format that is easy to use for analysis

  How precise the outputs are greatly affects the man-hours required for subsequent processes, and analysis accuracy.

  Filling out the entire list of assets is not necessary. Simply filling out items that reference existing documents is one approach.

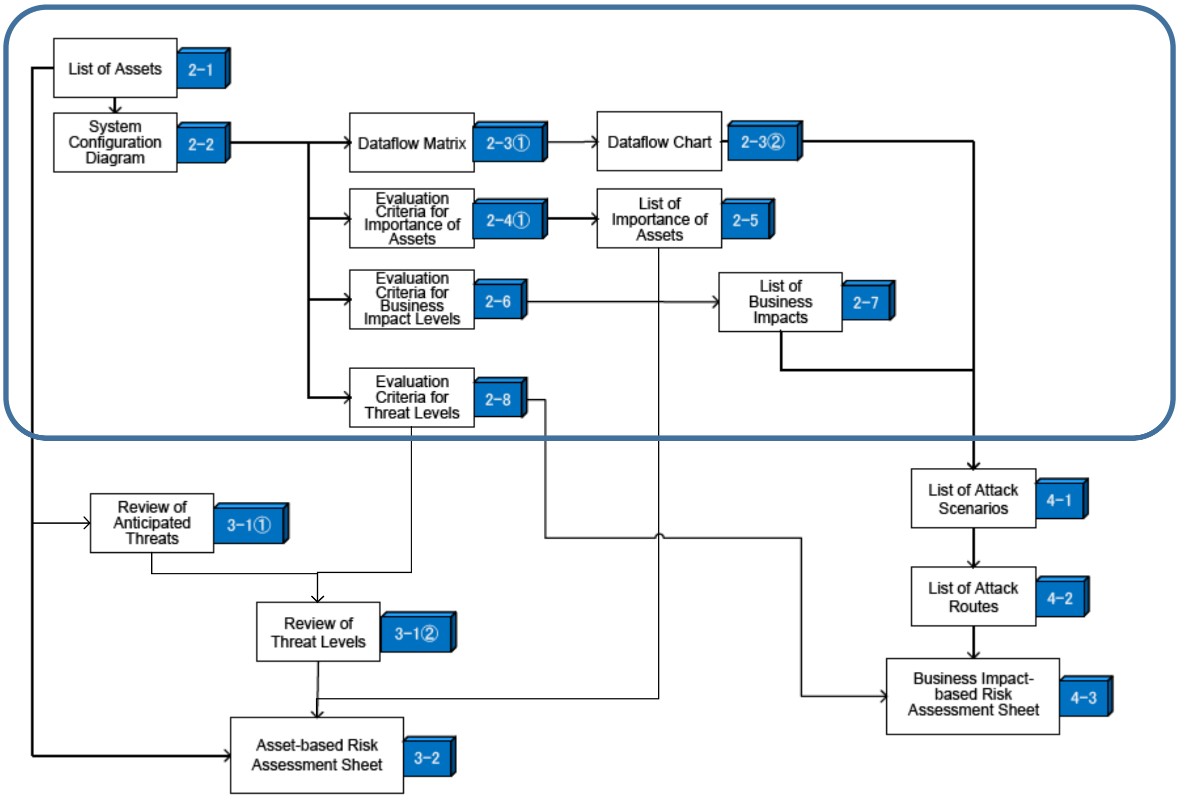
  Another approach is to provide additional detail to certain items as necessary while analysis is ongoing.

2. Preparing for Risk Analysis

Outputs created as part of risk analysis preparations are described below.

Table 2-1: List of Outputs for the Preparation Work

Section In this Volume	Output	Output Use	Guide
2.1	List of Assets	Asset/Business Impact-based	3.1.5. Table 3-9
2.2	System Configuration Diagram	Asset/Business Impact-based	3.2.3. Figure 3-8
2.3.①	Dataflow Matrix	Asset/Business Impact-based	3.3.1. Table 3-10
2.3.②	Dataflow Chart	Asset/Business Impact-based	3.3.2. Figure 3-14
2.4	Evaluation Criteria for Importance of Assets	Asset-based	4.2.2. Table 4-5
2.5	List Detailing the Importance of Each Asset	Asset-based	4.2.3. Table 4-9
2.6	Evaluation Criteria for Business Impact Levels	Business Impact-based	4.3.2. Table 4-11
2.7	List Detailing Business Impacts and Business Impact Levels	Business Impact-based	4.3.3. Table 4-12
2.8	Evaluation Criteria for Threat Levels	Asset/Business Impact-based	4.4.5. Table 4-20 to Table 4-24



List of Assets
2-1
System Configuration Diagram
2-2
Dataflow Matrix
2-3①
Dataflow Chart
2-3②
Evaluation Criteria for Importance of Assets
2-4①
List of Importance of Assets
2-5
Evaluation Criteria for Business Impact Levels
2-6
List of Business Impacts
2-7
Evaluation Criteria for Threat Levels
2-8
List of Attack Scenarios
4-1
Review of Anticipated Threats
3-1①
List of Attack Routes
4-2
Review of Threat Levels
3-1②
Business Impact-based Risk Assessment Sheet
4-3
Asset-based Risk Assessment Sheet
3-2

Figure 2-1: Preparation Work Flow

2.1. List of Assets

[Task2.1①] Preparing a list of assets for the system being analyzed.

- Specifying the asset category, functions, installation location, connected network, presence of a maintenance port, vendor, OS, and protocols while referring to *Table 3-9* in the Guide.

[Output2.1①]

A list of assets is shown in the next section (Table 2-2Table 2-2).

[Explanation2.1①]

- Organizing information needed to perform risk analysis in detailed risk assessment in a format that is easy to use for analysis

It is recommended to organize information needed to perform risk analysis in detailed risk assessment in a list of assets. How precise the outputs are greatly affects the man-hours required for subsequent processes, and analysis accuracy. However, filling out the entire list of assets is not necessary. Simply filling out items that reference existing documents is one approach. Another approach is to add or provide additional detail to certain items in the list of assets as necessary while analysis is ongoing.

- Clarifying connected networks (NW)

Assets may be connected to different management networks and monitoring networks outside of the regular network route. These networks may not be included in network diagrams prepared by the company, and need to be clarified.

- Considerations for the number of man-hours required for inspection when preparing a list of assets

Business operators that do not maintain a detailed list of assets may need to obtain this information from their control system operator, system builder or vendor. This requires a certain amount of man-hours, and due consideration must be given to providing sufficient leeway in the preparation period to account for this.

Table 2-2: List of Assets *1

No		1	2	3	4	5	6	7	8	9	10	11	12	13
Asset Name		Monitoring Terminal	Firewall	Switch, DMZ	Data Historian (Relay)	Data Historian	Switch, Control Network (Information Side)	EWS	Control Server	HMI (Operator Terminal)	Switch, Control Network (Field Side)	Field Network	Controller, Controller (Master)	Controller (Slave)
Type of Assets	IT Asset	○												
	OT Asset				○	○		○	○	○			○	○
	Network Asset (with Communication Control Functions)		○	○			○							
	Network Asset (without Communication Control Functions)										○	○		
Asset Functions	Input/Output	○			○	○		○	○	○			○	○
	Storing Data				○	○		○	○	○				
	Issuing Commands								○	○			○	○
	Gateway Function		○	○			○				○	○		
Type of Communication Line				LAN			LAN				LAN	Field Network		
Installation Location		Office	Server Room	Server Room	Server Room	Server Room	Server Room	Server Room	Server Room	Control Room	Server Room, Control Room, Field (on the Premises)	Field (on the Premises), Field (off the Premises)	Field (on the Premises)	Field (off the Premises)
Connected Network	Information Network	○	○											
	DMZ		○	○	○									
	Control Network (Information Side)		○			○	○	○	○	○				
	Control Network (Field Side)							○	○	○	○		○	
	Field Network											○	○	○
	Other													
Network Connected to Maintenance Port		×	Information Network	×	×	×	×	×	×	×	×	×	×	×
Presence of Operation Interface		○	×	×	○	○	×	○	○	○	×	×	×	×
Use of USB Port/Communications I/F		○	○	○	○	○	○	○	○	○	○	×	×	×
Regular Use of Media/Device Connections		×	×	×	×	×	×	○	×	×	×	×	×	×
Wireless Communication Capabilities		○	×	×	×	×	×	×	×	×	×	×	×	×
Regular Operation, Non-regular Operation		Regular Operation	Regular Operation	Regular Operation	Regular Operation	Regular Operation	Regular Operation	Regular Operation	Regular Operation	Regular Operation	Regular Operation	Regular Operation	Regular Operation	Regular Operation
Data Type and Dataflow		Written in Dataflow Matrix												
System Construction Vendor/Device Manufacturer		AB/XX	AB/YY	AB/ZZ	AB/XX	AB/XX	AB/ZZ	AB/XX	AB/XX	AB/XX	AB/ZZ	AB/XX	AB/XX	AB/XX
OS Type/Version		Windows 7	Proprietary OS	Proprietary OS	Windows Server 2008	Windows Server 2008	Proprietary OS	Windows XP	Windows Server 2008	Windows XP	Proprietary OS	Proprietary OS	Proprietary OS	Proprietary OS
Protocols		TCP, UDP	TCP, UDP	TCP, UDP	TCP, UDP	TCP, UDP	TCP, UDP, Proprietary	TCP, UDP, Proprietary	TCP, UDP, Proprietary	TCP, UDP, Proprietary	TCP, UDP, Proprietary	Proprietary	Proprietary	Proprietary

*1 Abbreviations of assets used in this table and the following text
FW: Firewall, SW: Switch, NW: Network

*2 The EWS installation location is the server room (there are also a large number of control systems where the EWS is located in the control room).

[Task 2.1②] Adding details of the countermeasures taken on the external environment of the asset—namely physical measures and operational measures—and technical measures on the asset itself to the list of assets.

[Output 2.1②]

Roles/functions, the scope of impact, and security measures added to the list of assets are shown from Page 17 onwards. (Table 2-3).

[Explanation 2.1②]

- Clarification of roles and scope of impact

  To facilitate judgment pertaining to the importance of assets and business impact level, it is recommended to clarify the impact from the potential outage or failure of an asset, and the unauthorized operation of the system on the asset.

- Clarification of external public services (in particular, remote connection functions)

  Whether or not an asset provides functions that explicitly allows for remote connectivity is vital information to consider when reviewing attack trees as part of business impact-based risk analysis.

- Filling out the security measures

  It is recommended to separate details on security status for physical security measures, operational security measures, and technical security measures added to assets.

  Physical security measures are used to review the security level for physical intrusion into buildings and rooms where assets are located, and the theft of said assets.

- Clarification of details concerning operational measures and technical measures

  It is recommended to describe countermeasures in greater detail when reviewing the security level. For example, it is recommended to outline whether smartphone or USB device connections are restricted on a technical level, whether they are prohibited from being brought into company premises, or whether connecting these devices is prohibited in operational rules.

- Utilizing the list of assets

  As the list of assets facilitates understanding of the effectiveness of security measures in the control system, it is recommended that, once prepared, the list of assets is regularly maintained (updated).

Table 2-3: List of Assets (Including Role/Function, Scope of Impact/Impact on Business Continuity, Security Measures)

No	1	2	3	4	5
Asset Name	Monitoring Terminal	Firewall	Switch, DMZ	Data Historian (Relay)	Data Historian
Role/Function	・ A terminal used to monitor processes and on-site status. ・ There is no operating procedure for accessing devices on the control network from the monitoring terminal.	・ A device that functions to prevent attacks and intrusions from external networks.	・ A device that converges and relays multiple networks.	・ A server that is used to reference the data historian in the control network (information side) from the asset in the information network.	・ A server where process values and control parameters are stored and analyzed over an extended period of time.
Scope of Impact/Impact on Business Continuity	・ Unauthorized modification of data held by the asset or a failure in this asset does not directly impact business continuity.	・ Unauthorized modification of the asset's configured settings can lead to an attack or intrusion. ・ Even in the case of a failure in this asset, field devices can be operated directly to ensure business continuity.	・ Even in the case of a failure in this asset, field devices can be operated directly to ensure business continuity.	・ While the asse's failures do not directly impact business continuity, data analysis of control processes will no longer be available, reducing the operating efficiency of the control system.	・ While unauthorized modification of data held by the asset or a failure in this asset does not directly impact business continuity, data analysis of control processes will no longer be available, reducing the operating efficiency of the control system.
Effectiveness of Security Measures (Physical/Operational)	・ Physical security measures (placement of security guards, lock and key management, entrance and exit management, etc.) are implemented on business premises and buildings. ・ Only internal business personnel are able to physically access office devices.	・ For business premises, buildings, rooms (server rooms and control rooms), racks, etc. that have control system devices installed, physical security measures (placement of security guards, lock and key management, entrance and exit management, surveillance cameras, intrusion detection sensors, etc.) are implemented. ・ Control system device operators are limited, both physically and logically, to the absolute minimum number of internal personnel required.	・ For business premises, buildings, rooms (server rooms and control rooms), racks, etc. that have control system devices installed, physical security measures (placement of security guards, lock and key management, entrance and exit management, surveillance cameras, intrusion detection sensors, etc.) are implemented. ・ Control system device operators are limited, both physically and logically, to the absolute minimum number of internal personnel required.	・ For business premises, buildings, rooms (server rooms and control rooms), racks, etc. that have control system devices installed, physical security measures (placement of security guards, lock and key management, entrance and exit management, surveillance cameras, intrusion detection sensors, etc.) are implemented. ・ Control system device operators are limited, both physically and logically, to the absolute minimum number of internal personnel required. ・ While operating rules prohibit connections to external storage media and smartphone devices, technical measures are not taken.	・ For business premises, buildings, rooms (server rooms and control rooms), racks, etc. that have control system devices installed, physical security measures (placement of security guards, lock and key management, entrance and exit management, surveillance cameras, intrusion detection sensors, etc.) are implemented. ・ Control system device operators are limited, both physically and logically, to the absolute minimum number of internal personnel required. ・ While operating rules prohibit connections to external storage media and smartphone devices, technical measures are not taken.
Effectiveness of Security Measures (Technical)	・ The OS used is Windows 7, and updates are applied as they are made available. ・ Security measures equivalent to those implemented for information systems are conducted, and various security products are available, including anti-virus software, email filters, and web filters. ・ Users are authenticated when logging in remotely or directly.	・ Users are authenticated when logging in remotely or directly. ・ Only administrator accounts are used, and there are no operator accounts. Remote management functions are only available on administrator accounts. ・ A packet filter firewall is used, and firewall rules only permit communications with the following two connections (IP protocol). Monitoring Terminal <-> Data Historian (Relay) Data Historian (Relay) <-> Data Historian ・ The firewall firmware updates are applied as they are made available. The timing of updates is determined by the maintenance vendor.	・ Users are authenticated when logging in remotely or directly. ・ Only administrator accounts are used, and there are no operator accounts. Remote management functions are only available on administrator accounts. ・ The switch firmware updates are applied as they are made available. The timing of updates is determined by the maintenance vendor.	・ The OS used is Windows Server 2008, and updates are not applied. ・ Users are authenticated when logging in remotely or directly. ・ There are two types of accounts: operator accounts and administrator accounts. Remote management functions are only available on administrator accounts. ・ Data backups are performed on a weekly basis, and three generations of data are stored. ・ Emergency patches are applied within one week of their release. ・ While anti-virus software is installed, signature patterns are only updated once every six months, rather than on a daily basis.	・ The OS used is Windows Server 2008, and updates are not applied. ・ Users are authenticated when logging in remotely or directly. ・ There are two types of accounts: operator accounts and administrator accounts. Remote management functions are only available on administrator accounts. ・ Data backups are performed on a weekly basis, and three generations of data are stored.

Table 2-3: List of Assets (Including Role/Function, Scope of Impact/Impact on Business Continuity, Security Measures)

No	6	7	8	9	10
Asset Name	Switch, Control Network (Information Side)	EWS	Control Server	HMI (Operator Terminal)	Switch, Control Network (Field Side)
Role/Function	・ A network used to transfer status (contact state) information and data with devices on an information network or devices in a DMZ (servers, etc.) for control purposes.	・ A device used to alter controller programs and modify control server programs. ・ The EWS is also used to bring in external data by connecting it with an external storage media (typically a USB memory stick).	・ A server that sends settings and commands to control devices and field equipment.	・ A terminal used to enter in instructions for control devices and field equipment. ・ Wide-area supply outage commands (commands used to suspend supply to predetermined areas) can be issued.	・ A network used to immediately transfer status information and data, used for control purposes, between the local network and devices (controllers) on a field network. It possesses high responsiveness, optimized for control functions. ・ Uses proprietary IP-based protocols.
Scope of Impact/Impact on Business Continuity	・ Even in the case of a failure in this asset, field devices can be operated directly to ensure business continuity.	・ Unauthorized modification of controller or control server programs or configured settings could prevent normal monitoring control. ・ It stores programs and data containing business secrets, so a data breach could lead to similar products emerging from competitors, and a reduction in the competitive strength of the company.	・ Contains important data that, if tampered with and altered, could cause a system malfunction to occur, resulting in a wide-area supply outage. ・ A failure in this asset would impact business continuity.	・ Even in the case of a failure in this asset, equipment and devices can be operated directly to ensure business continuity.	・ Even in the case of a failure in this asset, field devices can be operated directly to ensure business continuity.
Effectiveness of Security Measures (Physical/Operational)	・ For business premises, buildings, rooms (server rooms and control rooms), racks, etc. that have control system devices installed, physical security measures (placement of security guards, lock and key management, entrance and exit management, surveillance cameras, intrusion detection sensors, etc.) are implemented. ・ Control system device operators are limited, both physically and logically, to the absolute minimum number of internal personnel required. ・ Wires are physically protected by conduits.	・ For business premises, buildings, rooms (server rooms and control rooms), racks, etc. that have control system devices installed, physical security measures (placement of security guards, lock and key management, entrance and exit management, surveillance cameras, intrusion detection sensors, etc.) are implemented. ・ Control system device operators are limited, both physically and logically, to the absolute minimum number of internal personnel required. ・ While operating rules prohibit connections to external storage media and smartphone devices, technical measures are not taken.	・ For business premises, buildings, rooms (server rooms and control rooms), racks, etc. that have control system devices installed, physical security measures (placement of security guards, lock and key management, entrance and exit management, surveillance cameras, intrusion detection sensors, etc.) are implemented. ・ Control system device operators are limited, both physically and logically, to the absolute minimum number of internal personnel required. ・ While operating rules prohibit connections to smartphone devices, technical measures are not taken.	・ For business premises, buildings, rooms (server rooms and control rooms), racks, etc. that have control system devices installed, physical security measures (placement of security guards, lock and key management, entrance and exit management, surveillance cameras, intrusion detection sensors, etc.) are implemented. ・ Persons with access to control system devices are limited, both physically and logically, to the absolute minimum number of internal personnel required.	・ For business premises, buildings, rooms (server rooms and control rooms), racks, etc. that have control system devices installed, physical security measures (placement of security guards, lock and key management, entrance and exit management, surveillance cameras, intrusion detection sensors, etc.) are implemented. ・ Control system device operators are limited, both physically and logically, to the absolute minimum number of internal personnel required.
Effectiveness of Security Measures (Technical)	・ Users are authenticated when logging into the switch remotely or directly. ・ (On the switch) only administrator accounts are used, and there are no operator accounts. ・ Connection to remote management functions (on the switch) is restricted to the connection source IP address.	・ The OS used is Windows XP, and updates are not applied. ・ Anti-virus software is not installed. ・ There are two types of accounts: operator accounts and administrator accounts. Remote management functions are only available on administrator accounts. ・ Users are authenticated when logging in remotely or directly.	・ The OS used is Windows Server 2008, and updates are not applied. ・ Users are authenticated when logging in remotely or directly. ・ There are two types of accounts: operator accounts and administrator accounts. Remote management functions are only available on administrator accounts. ・ While anti-virus software is not installed, certain security measures, such as an application whitelisting, are taken.	・ The OS used is Windows XP, and updates are not applied. ・ Anti-virus software is not installed. ・ There are two types of accounts: operator accounts and administrator accounts. Remote management functions are only available on administrator accounts. ・ Users are authenticated when logging in remotely. ・ It is in an always-logged-in state and its screen lock is not set.	・ Wires are physically protected by conduits. ・ The control network (field side) uses IP protocols.

Table 2-3: List of Assets (Including Role/Function, Scope of Impact/Impact on Business Continuity, Security Measures)

No	11	12	13
Asset Name	Field Network	Controller, Controller (Master)	Controller (Slave)
Role/Function	・ A network between the controller (master) and controller (slave).	・ A device that accepts input/output signals, such as signals for controlling contacts and operation devices sent from the sensor. ・ Some controllers relay communications between the control server or data server, and the controller. The relaying side is referred to as the controller (master), and the relayed side is referred to as the controller (slave). ・ The controller (master) relays supply outage commands from the host system to the low-end controller (master) to be issued. ・ Connected to controlled devices via a serial port, or an alternative method.	・ A device that accepts input/output signals, such as signals for controlling contacts and operation devices sent from the sensor. ・ It is a low-end system of the controller (master) and receives supply outage commands from the controller (master). ・ Connected to controlled devices via a serial port, or an alternative method.
Scope of Impact/Impact on Business Continuity	・ Even in the case of a failure in this asset, field devices can be operated directly to ensure business continuity.	・ Contains programs that, if tampered with and altered, could cause a system malfunction to occur, resulting in a supply outage. ・ A failure in this asset would trigger the safety mechanism, resulting in a supply outage. ・ Under the controller (master) are such a number of controllers (slave) that could cause a wide-area supply outage.	・ Contains programs that, if tampered with and altered, could cause a system malfunction to occur, resulting in a supply outage. ・ A failure in this asset would trigger the safety mechanism, resulting in a supply outage.
Effectiveness of Security Measures (Physical/Operational)	・ Field networks outside business premises are installed in locked containers and installation boxes.	・ For business premises, buildings, rooms (server rooms and control rooms), racks, etc. that have control system devices installed, physical security measures (placement of security guards, lock and key management, entrance and exit management, surveillance cameras, intrusion detection sensors, etc.) are implemented. ・ Control system device operators are limited, both physically and logically, to the absolute minimum number of internal personnel required.	・ Field devices outside business premises are installed in locked containers and installation boxes.
Effectiveness of Security Measures (Technical)		・ A proprietary OS is used, and there is no anti-virus software available for the controller. ・ Controller firmware updates are not applied. ・ Users are authenticated when logging in remotely or directly. ・ Only administrator accounts are available, with remote management functions.	・ The OS is a proprietary OS, and there is no anti-virus software available for the controller. ・ Controller firmware updates are not applied. ・ Users are authenticated when logging in remotely or directly. ・ Only administrator accounts are available, with remote management functions.

This page has intentionally been left blank.

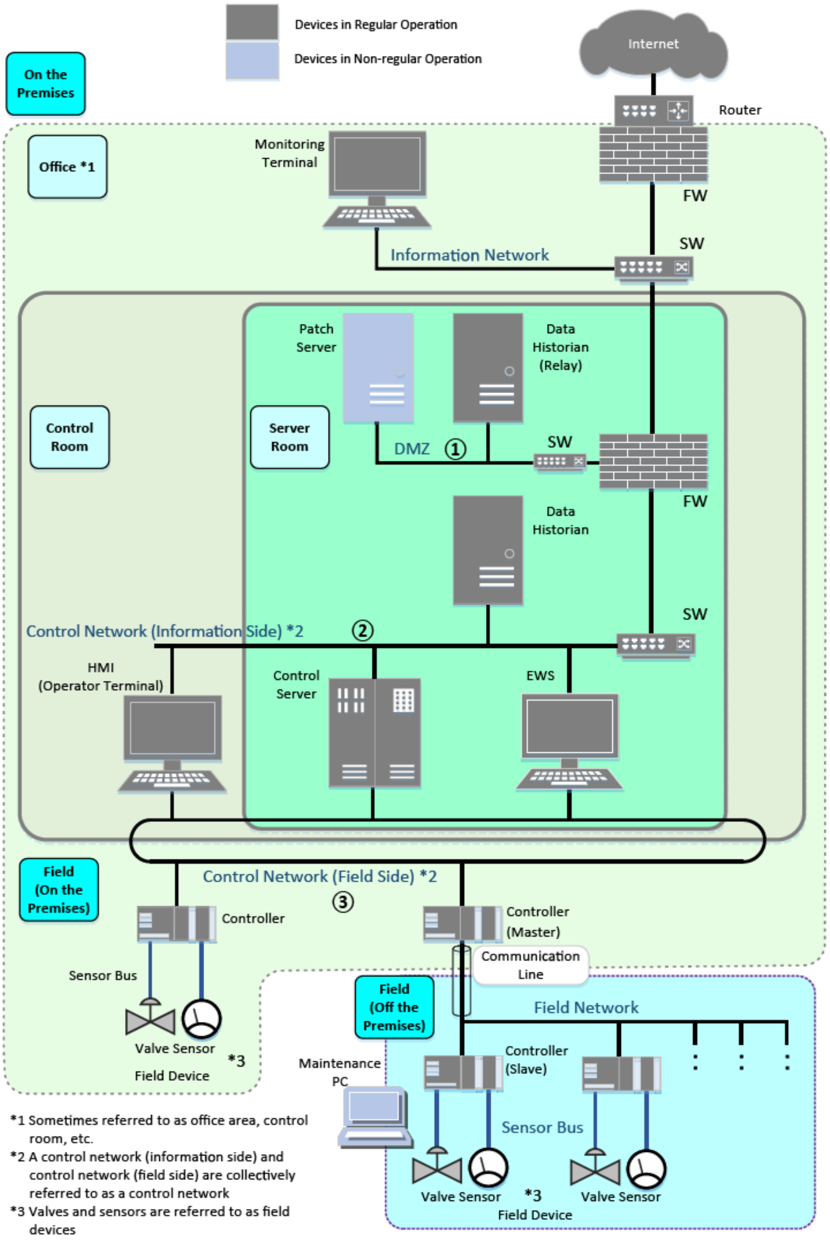
2.2. System Configuration Diagram

[Task 2.2] Preparing a system configuration diagram of the system being analyzed.

- Referring to *Figure 3-8* in the Guide to do so.
- Ensuring that the network connection status and physical installation location of assets are clearly outlined in the system configuration diagram.

[Output 2.2]

This volume uses the same diagram as that shown in *Figure 3-8* of the Guide as the system configuration diagram (Figure 2-2).



*1 Sometimes referred to as office area, control room, etc.

*2 A control network (information side) and control network (field side) are collectively referred to as a control network

*3 Valves and sensors are referred to as field devices

Figure 2-2: System Configuration Diagram

[Explanation 2.2]

- Preparing a system configuration diagram for risk analysis

  Listing the assets required to perform risk analysis while referring to existing network configuration diagrams (information system configuration diagrams, control system configuration diagrams, etc.).
  Some assets and network routes may not be included in a network diagram. These may be found during security testing, or at other points during risk analysis, and should be taken into consideration.

- Describing the network connections and physical location of the asset

  It is a good practice to arrange the system configuration diagram so that both the logical network connection status, and the physical location of an asset are identified at the same time. This is useful when investigating whether a third party, or an insider unrelated to the control system, can mount an intrusion attack when considering threats involving a physical intrusion in business impact-based risk analysis.

- Assets with redundant configurations can be omitted from the system configuration diagram

  It is not necessary to include all devices written in a network configuration diagram in a system configuration diagram.
  Example: Multiple network switches in the same network are shown as one switch.
  Example: Multiple HMIs and controllers can be expressed as a single HMI or controller.

  However, any assets omitted from the system configuration diagram should otherwise be recorded in a list of assets.

2.3. Dataflow Matrix

[Task 2.3①] Summarizing network data transmitted between assets on the system being analyzed in a dataflow matrix chart.

- Referring to *Table 3-10* in the Guide for details on the format used.

[Output 2.3①]

The dataflow matrix is shown below (Table 2-4).

Table 2-4: Dataflow Matrix

Receiver Sender	Route of Data	Monitoring Terminal	Data Historian (Relay)	Data Historian	Control Server	EWS	HMI (Operator Terminal)	Controller	Controller (Master)	Controller (Slave)
Monitoring Terminal	Information Network	■								
Data Historian (Relay)	DMZ	Process Value (Historian Data)	■							
Data Historian	Control NW (Info)		Process Value (Historian Data)	■						
Control Server	Control NW (Info)			Process Value	■					
	Control NW (Field)				■			Control Command	Control Command	
EWS	Control NW (Info)					■				
	Control NW (Field)					■		Engineering Settings	Engineering Settings	
HMI (Operator Terminal)	Control NW (Info)						■			
	Control NW (Field)						■	Control Command	Control Command	
Controller	Control NW (Field)				Process Value		Process Value	■		
Controller (Master)	Control NW (Field)				Process Value		Process Value		■	
	Field Network								■	Control Command
Controller (Slave)	Field Network								Process Value	■

[Explanation 2.3①]

- Understanding dataflow

  Clarifying types of communications between assets, and the purpose of such communications in order to review attack trees in risk analysis.

  Distinguishing program changes, settings changes, and other dataflows that lead to the final attack on the control system from other dataflows.

- Simple method to describing dataflows

  In order to simplify the dataflow matrix, in a dataflow where a data reference request is sent from asset A to asset B, with asset A then receiving a response, data is described as being sent from asset B to asset A, omitting the data reference requests from asset A to asset B.

- Clarification of the dataflow network

  If an asset is connected to multiple networks, it should be clearly defined which network is used to send and receive data. In this volume, this corresponds to dataflow where data is sent and received by the HMI, EWS, control server, and controller (master).

  In addition, describing dataflow that straddles multiple networks to the degree possible.

- Dataflow outside network routes

  Data that is input/output also exists outside network routes, such as data brought in using USB devices and other external storage media and maintenance PCs. In this volume, the use of external storage media is described in the list of assets, and is not included in the dataflow.

[Task 2.3②] Summarizing data transmitted between assets on the system being analyzed in a dataflow chart.

- ➢ Referring to *Figure 3-14* in the Guide to do so.
- ➢ Adding dataflows to the system configuration diagram.

[Output 2.3②]
A dataflow chart of the system being analyzed is shown below.

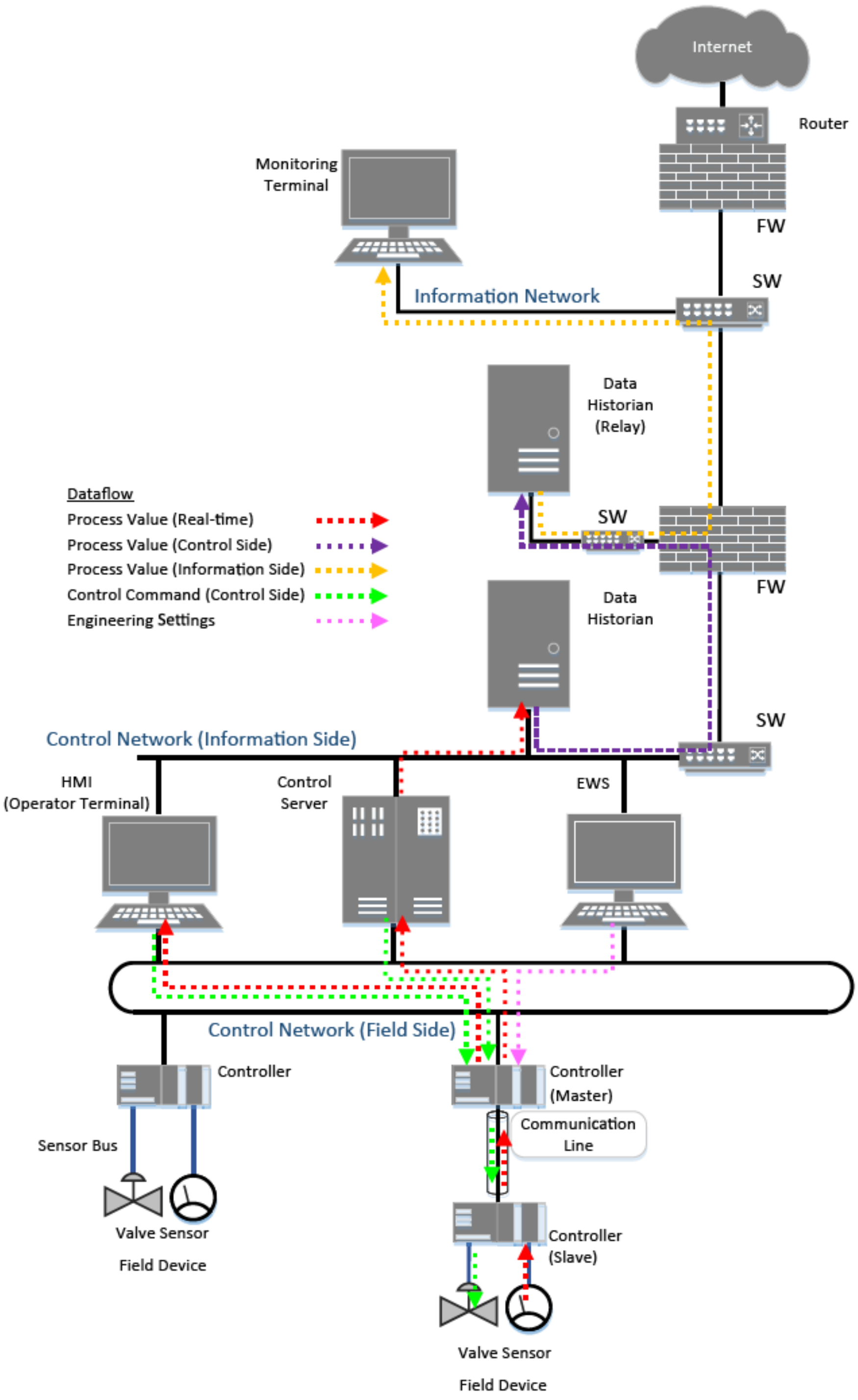


Figure 2-3: Dataflow Chart

2.4. Evaluation Criteria for Importance of Assets

[Task 2.4] Preparing evaluation criteria for evaluating the importance of assets in three phases (High impact: 3 > Medium impact: 2 > Low impact: 1).

- Referring to *Table 4-5* in the Guide to provide clear numerical values based on the characteristics of the business as boundary values for evaluation. In addition, providing reasoning behind such boundary values.

[Output 2.4]

An example of evaluation criteria for importance of assets is provided below (Table 2-5).

Table 2-5: Example Definitions of Evaluation Criteria for Importance of Assets

Evaluation Value	Evaluation Criteria
3	・ Assets which, if lost, or subject to unauthorized operation, would have a major impact on the business. - Potential for an extended system outage (for two weeks or more). - Potential for the system becoming inoperable, causing damage or pollution in the surrounding environment.
2	・ Assets which, if lost, or subject to unauthorized operation, would have a medium-level impact on the business. - Potential for a system outage over a period (of three days to two weeks). - Potential for the system becoming inoperable, causing damage to company premises.
1	・ Assets which, if lost, or subject to unauthorized operation, would have a low-level impact on the business. - Potential for a system outage over a period (of less than three days). - If the system becomes inoperable, there is no risk of damage to the control system.

Criteria behind the control system outage period: If there are two weeks' worth of stored inventory and the asset's failure could lead to a control system outage of under two weeks, the asset has an importance (business impact) of 2. Those that could lead to a longer outage have an importance (business impact) of 3.

- If evaluation criteria with evaluation values of differing importance apply, the evaluation value with the higher level of importance is used.

[Explanation 2.4]

- Evaluation Criteria for Importance of Assets

  The evaluation criteria for importance of assets in a control system is most easily understood when set from the perspective of asset availability. However, note that evaluation criteria for importance of assets that only takes availability into account will reduce the importance of boundary firewalls between information networks and control networks, and assets containing confidential information (in this case, EWS).

- Criteria for control system (plant) outage periods

  Ideally, it is advisable to refer to the company's business continuity plan (BCP) and other internal rules when determining the criteria for control system outage periods. For example, if the target period for restoring the control system is two weeks (target period for resuming product manufacturing and supply), and there is two weeks' worth of inventory in stock, any control system outage that exceeds two weeks could be considered to have a major impact on operations.

2.5. List Detailing the Importance of Each Asset

[Task 2.5] Determining the importance of assets.

- Determining the importance of assets in accordance with “Evaluation Criteria for Importance of Assets”.
- Including reasoning used as the basis for determining the importance.

[Output 2.5]

The importance of assets, and the reasoning for such are described below (Table 2-6).

Table 2-6: Importance of Assets

#	Asset	Importance	Reasoning
1	Monitoring Terminal	1	The asset becoming inoperable would not affect the safe operation of the control system.
2	Firewall	3	Maliciously modifying firewall filter settings could lead to direct unauthorized access of a control network with a low level of security measures via the information network.
3	Switch (within DMZ), DMZ	2	A failure of the DMZ network would not immediately impact the control system.
4	Data Historian (Relay)	2	While a shutdown of the historian would not affect the safe operation of the control system, this would prevent data analysis and could potentially reduce the operating efficiency of the control system.
5	Data Historian	2	While a shutdown of the historian would not affect the safe operation of the control system, this would prevent data analysis and could potentially reduce the operating efficiency of the control system.
6	Switch (Control Network (Information Side)), Control Network (Information Side)	2	A shutdown of the control network (information side) would not immediately impact the control system.
7	EWS	3	If the EWS is taken over, the program logic used by the controller could be tampered with and altered.
8	Control Server	3	If this asset becomes inoperable, or is subject to unauthorized operation, there is an extremely high likelihood that this would affect the safe operation of the control system.
9	HMI (Operator Terminal)	3	If monitoring is disabled for all HMIs, monitoring operations will no longer be possible. The control system may shutdown temporarily.
10	Control Network (Field Side)	3	While the system will not shutdown if this network is shutdown, monitoring and other operations will no longer be possible.
11	Field Network	3	If this network becomes congested, or is shutdown, regular monitoring control will no longer be possible, and there is a high likelihood that this would prevent the safe operation of the control system.
12	Controller, Controller (Master)	3	If this asset becomes inoperable, or is subject to unauthorized operation, there is an extremely high likelihood that this would affect the safe operation of the control system.
13	Controller (Slave)	3	If this asset becomes inoperable, or is subject to unauthorized operation, there is an extremely high likelihood that this would affect the safe operation of the control system.

[Explanation 2.5]

- Evaluation on the importance of redundant assets (from an availability perspective)

  When evaluating the importance of assets from the perspective of availability, set the evaluation value on availability based on the impact felt if all assets are lost, rather than reducing the evaluation value because the loss of one asset would not impact availability if multiple assets are available. Redundancy is counted and organized as measures implemented.

  Whether redundancy as a measure preventing a threat of asset failure (loss) has been implemented or not is determined as part of risk analysis in detailed risk assessment (asset-based risk analysis and business impact-based risk analysis).

- Evaluation of importance from the perspective of integrity and confidentiality

  Certain assets should be evaluated from the perspective of integrity and confidentiality. In this example, this evaluation applies to the firewall and EWS.

  While the failure of the firewall itself has a limited impact on the stable operation of the control system, the unauthorized access and unauthorized modification of firewall settings can have a major impact on the stable operation of the control system by allowing for direct cyber attacks on the control network from the information network. As such, the firewall is set to a high level of importance in terms of integrity and confidentiality.

  An EWS failure would adversely impact the control system by preventing controller setting changes, but would not have an immediate impact on the stable operation of the control system. If the information stored on the EWS is leaked to competitors, it could result in the loss of operating profits over the long-term. As such, the EWS is set to a high level of importance in terms of integrity and confidentiality.

2.6. Evaluation Criteria for Business Impact Level

[Task 2.6] Determining evaluation criteria for evaluating the business impact in three phases (High impact: 3 > Medium impact: 1 > Low impact: 1).

- Ideally, it is desirable to adapt the evaluation criteria presented in *Table 4-11* of the Guide to reflect the specific circumstances of the business.

[Output 2.6]

Examples of evaluation criteria for business impact levels are provided below (Table 2-7).

Table 2-7: Example Evaluation Criteria for Business Impact Levels

Evaluation Value		Evaluation Criteria
3	High Business Impact	・ The following may result from a failure occurring. - Potential for an extended system outage (for two weeks or more). - Potential losses amounting to 500 million yen or more. - Potential to cause damage or pollution in the surrounding environment.
2	Medium Business Impact	・ The following may result from a failure occurring. - Potential for a system outage over a period (for three days to two weeks). - Potential losses of between 100 million yen up to 500 million yen. - Potential to cause damage to company premises.
1	Low Business Impact	・ The following may result from a failure occurring. - While there is the potential for a system outage over a period (of less than three days), this will not greatly affect operations. - While there is the potential for losses under 100 million yen, this will not greatly affect operations. - No potential to cause damage to company premises.

Criteria behind the control system outage period: If there are two weeks' worth of stored inventory and the asset's failure could lead to a control system outage of under two weeks, the asset has an importance (business impact) of 2. Those that could lead to a longer outage have an importance (business impact) of 3.

- If evaluation criteria with evaluation values of differing business impact apply, the evaluation value with the higher business impact level is used.

[Explanation 2.6]

- Examples of evaluation criteria

  It is recommended to tailor the evaluation criteria for business impact level according to the circumstances facing the business while referring to the provisions of laws and regulations and guidelines (for example, *Table 4-8* in the Guide), and the internal rules that apply to the business (for example, the business continuity plan).

  As a specific example of the evaluation criteria for business impact level being applied, “Example of a Typical Consequence Scale According to IEC 62443-2-1” introduced in *Table 4-6* in the Guide can be used. Three evaluation criteria were selected in the evaluation criteria for business impact level (Table 2-7).

  - Manufacturing/production disrupt/suspend for a set period of time
  - Cost of losses (anticipated losses from the shipment of products meeting quality standards, or information leaks)
  - Impact on the environment both on the premises, at the place of business, and off the premises

2.7. Review of Business Impacts and Business Impact Levels

[Task 2.7①] Determining the business impacts, and providing a summary of such, for the system being analyzed.

- Briefly describing the cause of the business impact, and the affect it has, in the summary of business impacts.
- "*4.3.1* Meanings of Business Impacts and Business Impact Levels" and *Table 4-12* "Examples of Business Impact Definitions (1)" in the Guide can be used as references.

[Output 2.7①]

Business impacts on the system being analyzed are described below (Table 2-8).

Table 2-8: List of Business Impacts

#	Business Impact	Business Impact Summary
1	Wide Area Product Supply Outage	Improper use of legitimate supply outage functions caused by a cyber attack on supply facilities, which produces a wide area product supply outage, resulting in significant social impacts and a dramatic loss of trust in the company.
2	Occurrence of Fires and Explosion Incidents	Outbreak of fires and explosions due to control abnormalities and a loss of monitoring facilities for handling hazardous materials caused by a cyber attack on manufacturing facilities. Such attacks impact local residents and the environment, cause significant losses in compensation claims, and lead to a dramatic loss of trust in the company.
3	Supply of Defective Product	Manufacturing and supply of a product that does not meet quality standards/criteria caused by a cyber attack on manufacturing facilities, causing significant inconvenience to customers, significant losses in compensation claims, and a dramatic loss of trust in the company.
4	Manufacturing/Production Disrupt/Suspend	Manufacturing/production disrupt/suspend due to forcibly terminated processes due to process control abnormalities and operation monitoring failures caused by a cyber attack on manufacturing facilities.
5	Leak of Confidential Information	A cyber attack on the control system, resulting in an external leak of company production secrets, impacting the company's competitive edge against other companies, and leading to a deterioration in competitive strength.

[Task 2.7②] Determining the business impact level in accordance with the evaluation criteria for importance.

- In addition, providing reasoning for the business impact level set according to the "Evaluation Criteria for Business Impact Level".

[Output 2.7②]
The business impact level for business impacts, and the reasoning for such are described below (Table 2-9).

Table 2-9: List of Business Impacts and Business Impact Levels

Business Impact	Business Impact Summary	Business Impact Level	Reasoning
Wide Area Product Supply Outage	Improper use of legitimate supply outage functions caused by a cyber attack on supply facilities, which produces a wide area product supply outage, resulting in significant social impacts and a dramatic loss of trust in the company.	3	Evaluation is set to level "3" due to the potential for losses amounting to 500 million yen or more.
Occurrence of Fires and Explosion Incidents	Outbreak of fires and explosions due to control abnormalities and a loss of monitoring facilities for handling hazardous materials caused by a cyber attack on manufacturing facilities. Such attacks impact local residents and the environment, cause significant losses in compensation claims, and lead to a dramatic loss of trust in the company.	3	Evaluation is set to level "3" due to the significant impact on the surrounding environment.
Supply of Defective Product	Manufacturing and supply of a product that does not meet quality standards/criteria caused by a cyber attack on manufacturing facilities, causing significant inconvenience to customers, significant losses in compensation claims, and a dramatic loss of trust in the company.	2	Evaluation is set to level "2" due to anticipated losses of between 100 million yen up to 500 million yen.
Manufacturing/Production Disrupt/Suspend	Manufacturing/production disrupt/suspend due to forcibly terminated processes due to process control abnormalities and operation monitoring failures caused by a cyber attack on manufacturing facilities.	1	Evaluation is set to level "1" due to an anticipated outage period of under 3 days.
Leak of Confidential Information	A cyber attack on the control system, resulting in an external leak of company production secrets, impacting the company's competitive edge against other companies, and leading to a deterioration in competitive strength.	3	Evaluation is set to level "3" due to the potential for significant losses in the order of 500 million yen or more should confidential information concerning competitive advantages unique to the company be leaked outside the company.

[Explanation 2.7①②]

- Definition of Business Impact

  In “*4.3.1* Meanings of Business Impacts and Business Impact Levels” in the Guide, examples of business impacts are introduced from a broad range of perspectives, encompassing CIA perspectives (C: Confidentiality, I: Integrity, A: Availability) and HSE perspectives (H: Health, S: Safety, E: Impact on the environment). These can be used as a guide to defining business impacts according to the characteristics of the control system used by the business.

- Degree of information in the business impact summary

  Ideally, when defining the cause of a business impact, it is desirable to describe which assets are subject to cyber attack, and what kind of abnormalities occur. When writing the degree of business impact, it is desirable to align descriptions with the “Evaluation Criteria for Business Impact Level”. (Some room for interpretation can be left when writing the degree of business impact, while the degree of impact from high, medium, or low is clearly defined and used as the basis for determining the business impact level.)

Business Impact	Business Impact Summary	Item	Remarks
Occurrence of Fires and Explosion Incidents	Outbreak of fires and explosions due to control abnormalities and a loss of monitoring facilities for handling hazardous materials caused by a cyber attack on manufacturing facilities.	Causes of Business Impacts	Used when formulating attack scenarios
		Business Impact (Accident)	
	Such attacks impact local residents and the environment, cause significant losses in compensation claims, and lead to a dramatic loss of trust in the company.	Affect of Business Impact	Used when formulating the business impact level

2.8. Evaluation Criteria for Threat Level

[Task 2.8] Determining the evaluation criteria for threat level (Likelihood of occurrence 3: High > 2: Medium > 1: Low).

- The evaluation criteria described in *Tables 4-20 to 4-24* in the Guide can be used as a reference.

[Output 2.8]

The evaluation criteria for threat level are outlined below (Table 2-10).

Table 2-10: Evaluation Criteria for Threat Levels

Threat Level	Evaluation Criteria Based on an Attack by a Malicious Third Party	Evaluation Criteria Based on the Logical Placement of Assets	Evaluation Criteria based on the Physical Placement of Assets
3	・ When attacked by an individual attacker (regardless of skill), it has a high likelihood of success.	・ Assets on a network (information network) that can be connected to the Internet.	・ Assets in a location that can be accessed by anyone, without any access restrictions for the premises or room.
2	・ When attacked by an individual attacker with a certain degree of skill, it could potentially succeed.	・ Assets on a network (control network) that is indirectly connected to an information network.	・ Assets in a location with access restrictions for the premises or room.
1	・ When attacked by a state level cyber attacker (military or equivalent group), it could potentially succeed.	・ Assets on an isolated network.	・ Assets in a room with strict manned surveillance system, and access restrictions to enter the premises or room that involve stringent authentication procedures.

* If varying threat levels apply to a threat, the threat level is determined based on a general evaluation.

[Explanation 2.8]

- Skill of the attacker in threat evaluation criteria

  While there are various skill factors to consider, it is recommended to give a comprehensive evaluation of skill level for the following three points in the threat evaluation criteria.
  - Knowledge and skills in information security required for an intrusion via a network
  - Knowledge and skills in social engineering required for a physical intrusion
  - Knowledge and skills of control systems to cause the control system to malfunction

- Reviewing the threat evaluation criteria in the risk analysis phase

  The evaluation criteria for threat level can vary between asset-based risk analysis and business impact-based risk analysis.

  In asset-based risk analysis, a risk analysis of security measures other than those for assets being analyzed may evaluate “factors reducing the threat level”, rather than evaluating the “security level (vulnerability level)”.

  Conversely, in business impact-based risk analysis, security measures contained in the system being analyzed must be evaluated in terms of the security level, and cannot not be evaluated as factors reducing the threat level.

3. Asset-based Risk Analysis

Asset-based risk analysis involves using the following outputs prepared previously to conduct a risk analysis.

Table 3-1: Outputs for Preparations Used

Section In this Volume	Outputs for Preparations Used	Guide
2.1	List of Assets	3.1.5. Table 3-9
2.2	System Configuration Diagram	3.2.3. Figure 3-8
2.3.①	Dataflow Matrix	3.3.1. Table 3-10
2.3.②	Dataflow Chart	3.3.2. Figure 3-14
2.4	Evaluation Criteria for Importance of Assets	4.2.2. Table 4-5
2.5	List Detailing the Importance of Each Asset	4.2.3. Table 4-9
2.8	Evaluation Criteria for Threat Levels	4.4.5. Table 4-20 to Table 4-24

A list of outputs that is newly prepared as part of asset-based risk analysis is shown below.

Table 3-2: Outputs Prepared in Asset-based Risk Analysis Work

Section In this Volume	Asset-based Output	Guide
3.1	Summary Chart of Threat Levels	-
3.2	Asset-based Risk Assessment Sheet	Chapter 5
3.3.①	Summary Chart of Vulnerability Levels	-
3.3.②	Summary Chart on Risk Values	-

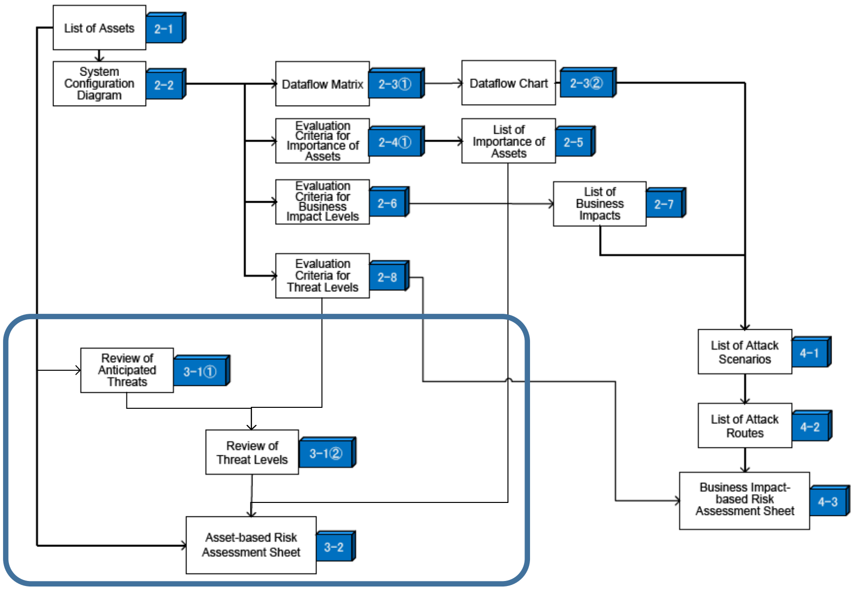

List of Assets
2-1
System Configuration Diagram
2-2
Dataflow Matrix
2-3①
Dataflow Chart
2-3②
Evaluation Criteria for Importance of Assets
2-4①
List of Importance of Assets
2-5
Evaluation Criteria for Business Impact Levels
2-6
List of Business Impacts
2-7
Evaluation Criteria for Threat Levels
2-8
Review of Anticipated Threats
3-1①
Review of Threat Levels
3-1②
Asset-based Risk Assessment Sheet
3-2
List of Attack Scenarios
4-1
List of Attack Routes
4-2
Business Impact-based Risk Assessment Sheet
4-3

Figure 3-1: Asset-based Risk Analysis Work Flow

3.1. Review of Threat Level

[Task 3.1①] Reviewing and determining threats (attack types) for assets being analyzed.

- “*Table 5-4*: List of Anticipated Threats (Attack Types) and Corresponding Type of Assets” in the Guide is used as a reference.
- “Section 2.1., Table 2-2: List of Assets” is used as a reference for details on the type of assets subject to analysis.

[Output 3.1②]

A summary chart of threats (attack types) for assets being analyzed is provided below (Table 3-3).

Table 3-3: List of Anticipated Threats to the Asset Being Analyzed

Threat / Asset	Monitoring Terminal	Firewall	DMZ	Data Historian (Relay)	Data Historian	Control Network (Information Side)	EWS	Control Server	HMI (Operator Terminal)	Control Network (Field Side)	Field Network	Controller (Master)	Controller (Slave)
IT Asset	○	○											
OT Asset			○	○	○		○	○	○			○	○
Network Asset (with Communication Control Functions)			○			○							
Network Asset (without Communication Control Functions)										○	○		
Unauthorized Access	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
Physical Intrusion	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
Unauthorized Operation	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
Human Error in Operation	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
Connecting Unauthorized Media or Device	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
Execution of Unauthorized Processes	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
Malware Infection	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
Information Theft	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
Unauthorized Modification of Information	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
Information Destruction	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
Unauthorized Transmission	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
Outage	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
DoS/DDoS Attack	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
Theft	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
When Stolen or Discarded	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
Route Blocking			✔			✔				✔	✔		
Network Congestion			✔			✔				✔	✔		
Jamming													
Packet Sniffing			✔			✔				✔	✔		
Unauthorized Modification of Communication Data			✔			✔				✔	✔		
Connecting Unauthorized Device			✔			✔				✔	✔		

✓: Threat (attack type) that applies to the asset

Grayed out: Threat (attack type) that does not apply to the asset

For information system assets (IT assets) or control system assets (OT assets), threats #1 through to #15 could potentially occur. For network assets (NW assets), threats #16 through to #21 could potentially occur. As the network assets in this example do not use wireless functions, it is assumed that no threat of jamming (#18) would occur.

[Task 3.1②] Determining the threat level of the threat (attack type) for each asset.

- It is assumed that the attacker is a "malicious third party" (human error by a third party, human error by an insider, and malicious insiders are excluded in asset-based risk analysis).
- Determining the threat level of the threat (attack type) for specific assets by using the evaluation criteria in "2.8 Evaluation Criteria for Threat Levels".
- Setting forth the reasoning used as the basis for determining the threat level.

[Output 3.1②]

A table showing the threat level set and the reasoning for such for the HMI (operator terminal) is provided below. Threat levels of all assets are shown in [Output 3.1③].

Table 3-4: HMI (Operator Terminal) Threat Levels and Reasoning

#	Threat (Attack Type)	Threat Level	Reasoning
1	Unauthorized Access	2	Due to the existence of free and paid hacking tools, this can be performed by attackers with a certain degree of skill.
2	Physical Intrusion	2	This can be performed by attackers with a certain degree of social engineering skills (trespassing, etc.).
3	Unauthorized Operation	2	While console operations can be performed by any attacker, regardless of skill levels, as consoles are located within buildings on the premises, this poses a low threat.
4	Human Error in Operation	2	While this can only be performed by attackers familiar with the control system and control processes, this could leave the controller susceptible to a direct attack.
5	Connecting Unauthorized Media or Device	3	Connecting unauthorized media or devices can be performed by any attacker, regardless of skill levels.
6	Execution of Unauthorized Processes	3	While this can only be performed by attackers with a certain degree of skill, the threat level this poses is high as this could leave the controller susceptible to a direct attack.
7	Malware Infection	3	The frequency of malware infection of general-purpose OS assets is high.
8	Information Theft	3	The threat level this poses is high, as this can easily be achieved if the system is infected with malware (#7).
9	Unauthorized Modification of Information	3	The threat level this poses is high, as this can easily be achieved if the system is infected with malware (#7).
10	Information Destruction	3	The threat level this poses is high, as this can easily be achieved if the system is infected with malware (#7).
11	Unauthorized Transmission	3	The threat level this poses is high, as this can easily be achieved if the system is infected with malware (#7).
12	Outage	3	The threat level this poses is high, as this can easily be achieved if the system is infected with malware (#7).
13	DoS Attack	1	As operations can continue on a substitute device, even when experiencing heavy loads, the threat level this poses is low.
14	Theft	2	This can be performed by attackers with a certain degree of social engineering skills (trespassing, etc.).
15	Information Theft by Tampering Device at Time of Theft or Disposal	2	This can be achieved following a theft (#14).
16	Route Blocking	-	Not applicable as this is not a network asset.
17	Network Congestion	-	Not applicable as this is not a network asset.
18	Jamming	-	Not applicable as this is not a network asset, and wireless functions are not used.
19	Packet Sniffing	-	Not applicable as this is not a network asset.
20	Unauthorized Modification of Communication Data	-	Not applicable as this is not a network asset.
21	Connecting Unauthorized Device	-	Not applicable as this is not a network asset.

[Task 3.1③] Reviewing the threat level for all assets subject to analysis, and summarizing these in table form.

- This allows better understanding and reviewing of the distribution of threat levels in combinations of asset and threat types.

[Output 3.1③]

A summary chart of asset threat levels is provided below.

Table 3-5: Summary Chart of Asset Threat Levels

Threat \ Asset	Monitoring Terminal	Firewall	DMZ	Data Historian (Relay)	Data Historian	Control Network (Information Side)	EWS	Control Server	HMI (Operator Terminal)	Control Network (Field Side)	Field Network	Controller (Master)	Controller (Slave)
IT Asset or OT Asset	○			○	○		○	○	○			○	○
Network Asset (with Communication Control Functions)		○	○			○							
Network Asset (without Communication Control Functions)										○	○		
Unauthorized Access	3	3	3	3	2	2	2	2	2			2	2
Physical Intrusion	2	1	1	1	1	1	1	1	2			2	3
Unauthorized Operation	2	2	2	2	2	2	2	2	2			2	3
Human Error in Operation	3	2	2	2	2	2	2	2	2			2	2
Connecting Unauthorized Media or Device	3	2	2	2	2	2	3	2	3			2	2
Execution of Unauthorized Processes	3	2	2	2	2	1	3	3	3			2	2
Malware Infection	3	1	1	3	3	1	3	3	3			1	1
Information Theft	3	1	1	3	3	1	3	3	3			3	3
Unauthorized Modification of Information	2	3	3	3	3	2	3	3	3			3	3
Information Destruction	2	2	2	3	3	2	3	3	3			3	3
Unauthorized Transmission	2	1	1	3	3	1	3	3	3			3	3
Outage	2	2	2	3	3	2	3	3	3			2	3
DoS/DDoS Attack	1	3	3	1	1	3	1	1	1			3	3
Theft	2	1	1	1	1	1	2	1	2			2	3
When Stolen or Discarded	2	1	1	1	1	1	2	1	2			2	3
Route Blocking			2			2				3	3		
Network Congestion			2			2				2	2		
Jamming													
Packet Sniffing			2			2				2	2		
Unauthorized Modification of Communication Data			2			2				2	2		
Connecting Unauthorized Device			3			3				2	2		

3.2. Filling Out the Asset-based Risk Assessment Sheet

Following the procedure described in "*Chapter 5* Asset-based Risk Analysis" in the Guide to conduct an asset-based risk analysis of the system to be analyzed. Detailed instructions are shown in the Guide. This section only provides a general overview of the procedure.

[Task 3.2①] Filling out the importance of the asset in the asset-based risk assessment sheet.

- ➢ Filling out the value defined in "Table 2-6: Importance of Assets" in the assessment sheet.

[Task 3.2②] Filling out the threat level in the asset-based risk assessment sheet. Graying out any threats that are not anticipated.

- ➢ Filling out threat level of anticipated threats for the asset, using "Table 3-3: List of Anticipated Threats to the Asset Being Analyzed" as a reference. Graying out any threats that are not anticipated.

[Task 3.2③] Confirming the effectiveness of security measures to threats, and circling countermeasures that have been implemented. Adding any supplementary notes on countermeasures implemented, if applicable. Adding additional countermeasures as necessary.

- ➢ Comparing the effectiveness of security measures in the asset-based risk assessment sheet with the security measures in "Table 2-3: List of Assets (Including Role/Function, Scope of Impact/Impact on Business Continuity, Security Measures)", and circling the effectiveness of security measures that applies.

[Task 3.2④] Assessing the security level from the details of countermeasures provided, and filling out the security level and vulnerability level in the assessment sheet.

- ➢ Filling out the security level and vulnerability level, by using the criteria described in "*Item 5.5.1 Table 5-7*" of the Guide.

[Task 3.2⑤] Determining the risk value based on the importance level, threat level and vulnerability level, and filling it out in the assessment sheet.

[Output 3.2]

An example of a filled-out asset-based risk assessment sheet is provided from page 43 (Table 3-6).

This page has intentionally been left blank.

Table 3-6: Asset-based Risk Assessment Sheet

Legend: ○ Measures implemented   Grayed out lines: Threats not taken into account for the corresponding asset   Green text in measures: Supplementary information on measures

Item Number	Type of Assets	Target Device	Assessment Metrics				Threat (Attack Type)	Description	Countermeasures								Security Level
									Protection				Detection/Understanding Damage		Business Continuity		By Threat
			Threat Level	Vulnerability Level	Importance of Assets	Risk Value			Intrusion/Spreading Phase		Objective Achievement Phase						
1	Information System Asset	**Monitoring Terminal**	3	2	1	D	Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type)				IPS/IDS				2
									FW (Application Gateway Type)				Log Collection/Log Analysis				
									One-way Gateway				Integrated Log Management System				
									Proxy Server								
									WAF								
									Peer-to-Peer Authentication	○							
									IPS/IDS								
									Applying Patches	○							
									Avoidance of Vulnerability								
2			2	2		D	Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with access restrictions. It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).	Entrance and Exit Management (IC Card)	○			Surveillance Camera				2
									Lock and Key Management	○			Intrusion Detection Sensor				
3			2	2		D	Unauthorized Operation	Intrusion through direct operation of the device's console or other component to execute an attack.	Operator Authentication	○							2
4			3	2		D	Human Error in Operation	An attack triggered by a human error in operation by internal personnel (an employee or partner with access privileges to the device). An act equivalent to an attack is performed on the device as a result of a proper media or device connection.	URL Filtering/Web Reputation	○							2
									Mail Filtering	○							
5			3	2		D	Connecting Unauthorized Media or Device	Connection of unauthorized media or device (CD/DVD, USB device, etc.) brought in from outside the organization with the device to execute an attack.	Restriction on Connecting Device and its Usage	○	(Same as on the Left)		(Same as on the Left)				2
													Log Collection/Log Analysis				
													Integrated Log Management System				
6			3	3		C	Execution of Unauthorized Processes	Unauthorized execution of legitimate programs, commands, services, and other processes found on the attack target device.	Permission Management		(Same as on the Left)		Device Error Detection				1
									Access Control		(Same as on the Left)		Device Alive Monitoring				
									Application Whitelisting		(Same as on the Left)		Log Collection/Log Analysis				
									Approval of Important Operations		(Same as on the Left)		Integrated Log Management System				
7			3	2		D	Malware Infection	Infection or running of malware (unauthorized programs) on the attack target device.	Anti-virus	○			Device Error Detection				2
									Application Whitelisting				Device Alive Monitoring				
									Applying Patches	○			Log Collection/Log Analysis				
									Avoidance of Vulnerability				Integrated Log Management System				
									Data Signature								
8			3	3		C	Information Theft	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management		(Same as on the Left)		Log Collection/Log Analysis				1
									Access Control		(Same as on the Left)		Integrated Log Management System				
									Data Encryption		(Same as on the Left)						
									DLP		(Same as on the Left)						
9			2	3		D	Unauthorized Modification of Information	Unauthorized modification of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management		(Same as on the Left)		Device Error Detection		Data Backup		1
									Access Control		(Same as on the Left)		Log Collection/Log Analysis				
									Data Signature		(Same as on the Left)		Integrated Log Management System				
10			2	3		D	Information Destruction	Destroying of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.			Permission Management		Device Error Detection		Data Backup		1
											Access Control		Log Collection/Log Analysis				
													Integrated Log Management System				
11			2	3		D	Unauthorized Transmission	Sending unauthorized control commands (settings changes, power shutdowns, etc.) and unauthorized data to other devices.	Segmentation/Zoning		(Same as on the Left)		Log Collection/Log Analysis				1
									Data Signature		(Same as on the Left)		Integrated Log Management System				
									Approval of Important Operations		(Same as on the Left)						
12			2	3		D	Outage	Stopping device functions.					Device Error Detection		Redundancy		1
													Device Alive Monitoring		Failsafe Design		
													Log Collection/Log Analysis				
													Integrated Log Management System				
13			1	3		E	DoS Attack	Interruption of regular device operations by sending processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.	DDoS Countermeasures				Device Error Detection		Redundancy		1
													Device Alive Monitoring		Failsafe Design		
													Log Collection/Log Analysis				
													Integrated Log Management System				
14			2	2		D	Theft	Device theft.	Lock and Key Management	○	(Same as on the Left)		(Same as on the Left)				2
15			2	2		D	Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Tamper Resistance		(Same as on the Left)						2
									Obfuscation		(Same as on the Left)						
									Zeroization	○	(Same as on the Left)						
16							Route Blocking	Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Entrance and Exit Management (IC Card)				Device Error Detection		Redundancy		
									Lock and Key management				Device Alive Monitoring				
													Log Collection/Log Analysis				
													Integrated Log Management System				
													Surveillance Camera				
													Intrusion Detection Sensor				
17							Network Congestion	Causing congestion by generating the communications traffic that exceeds the capacity of the device.	FW (Packet Filtering Type)				Device Error Detection		Redundancy		
									FW (Application Gateway Type)				Device Alive Monitoring				
									WAF				Log Collection/Log Analysis				
									IPS/IDS				Integrated Log Management System				
									DDoS Countermeasures								
18							Jamming	Interference with radio communications.					Device Error Detection		Redundancy		
													Device Alive Monitoring				
													Log Collection/Log Analysis				
													Integrated Log Management System				
19							Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels								
									Data Encryption								
									Exclusive Line								
20							Unauthorized Modification of Communication Data	Maliciously modifying information flowing on the network.	Encryption of Communications Channels				Log Collection/Log Analysis				
									Data Signature				Integrated Log Management System				
									Exclusive Line								
21							Connecting Unauthorized Device	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage				Restriction on Connecting Device and its Usage				
													Log Collection/Log Analysis				
													Integrated Log Management System				

Not applicable (no functions)

Table 3-6: Asset-based Risk Assessment Sheet

Legend: ○ Measures implemented Grayed out lines: Threats not taken into account for the corresponding asset Green text in measures: Supplementary information on measures

Item Number	Type of Assets	Target Device	Assessment Metrics				Threat (Attack Type)	Description	Countermeasures				Security Level
									Protection		Detection/Understanding Damage	Business Continuity	By Threat
			Threat Level	Vulnerability Level	Importance of Assets	Risk Value			Intrusion/Spreading Phase	Objective Achievement Phase			
1	Network Asset	**Firewall**	3	2	3	A	Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type) ○ FW (Application Gateway Type) One-way Gateway Proxy Server WAF Peer-to-Peer Authentication ○ IPS/IDS Applying Patches ○ Avoidance of Vulnerability		IPS/IDS Log Collection/Log Analysis Integrated Log Management System		2
2			1	1		C	Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with access restrictions. It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).	Entrance and Exit Management (IC Card, Biometric Authentication) ○ Lock and Key Management ○		Surveillance Camera ○ Intrusion Detection Sensor ○		3
3			2	2		B	Unauthorized Operation	Intrusion through direct operation of the device's console or other component to execute an attack.	Operator Authentication (ID/Pass) ○				2
4			2	3		A	Human Error in Operation	An attack triggered by a human error in operation by internal personnel (an employee or partner with access privileges to the device). An act equivalent to an attack is performed on the device as a result of a proper media or device connection.	URL Filtering/Web Reputation Mail Filtering				1
5			2	3		A	Connecting Unauthorized Media or Device	Connection of unauthorized media or device (CD/DVD, USB device, etc.) brought in from outside the organization with the device to execute an attack.	Restriction on Connecting Device and its Usage	(Same as on the Left)	(Same as on the Left) Log Collection/Log Analysis Integrated Log Management System		1
6			2	2		B	Execution of Unauthorized Processes	Unauthorized execution of legitimate programs, commands, services, and other processes found on the attack target device.	Permission Management ○ Access Control Application Whitelisting Approval of Important Operations	(Same as on the Left) (Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		2
7			1	3		B	Malware Infection	Infection or running of malware (unauthorized programs) on the attack target device.	Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		1
8			1	2		C	Information Theft	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management ○ Access Control Data Encryption DLP	(Same as on the Left) (Same as on the Left) (Same as on the Left) (Same as on the Left)	Log Collection/Log Analysis Integrated Log Management System		2
9			3	2		A	Unauthorized Modification of Information	Unauthorized modification of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management ○ Access Control Data Signature	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	2
10			2	2		B	Information Destruction	Destroying of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.		Permission Management Access Control ○	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	2
11			1	3		B	Unauthorized Transmission	Sending unauthorized control commands (settings changes, power shutdowns, etc.) and unauthorized data to other devices.	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Log Collection/Log Analysis Integrated Log Management System		1
12			2	3		A	Outage	Stopping device functions.			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Redundancy Failsafe Design	1
13			3	3		A	DoS Attack	Interruption of regular device operations by sending processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.	DDoS Countermeasures		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Redundancy Failsafe Design	1
14			1	2		C	Theft	Device theft.	Lock and Key Management ○	(Same as on the Left)	(Same as on the Left)		2
15			1	2		C	Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Tamper Resistance Obfuscation Zeroization ○	(Same as on the Left) (Same as on the Left) (Same as on the Left)			2
16							Route Blocking	Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Entrance and Exit Management (IC Card, Biometric Authentication) ○ Lock and Key management ○		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera ○ Intrusion Detection Sensor ○	Redundancy	
17							Network Congestion	Causing congestion by generating the communications traffic that exceeds the capacity of the device.	FW (Packet Filtering Type) ○ FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Redundancy	
18							Jamming	Interference with radio communications.			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Redundancy	
19							Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels Data Encryption Exclusive Line				
20							Unauthorized Modification of Communication Data	Maliciously modifying information flowing on the network.	Encryption of Communications Channels Data Signature Exclusive Line		Log Collection/Log Analysis Integrated Log Management System		
21							Connecting Unauthorized Device	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage		Restriction on Connecting Device and its Usage Log Collection/Log Analysis Integrated Log Management System		

Not applicable (no functions)

Table 3-6: Asset-based Risk Assessment Sheet

Legend: ○ Measures implemented   Grayed out lines: Threats not taken into account for the corresponding asset   Green text in measures: Supplementary information on measures

Item Number	Type of Assets	Target Device	Assessment Metrics				Threat (Attack Type)	Description	Countermeasures								Security Level
			Threat Level	Vulnerability Level	Importance of Assets	Risk Value			Protection				Detection/Understanding Damage		Business Continuity		By Threat
									Intrusion/Spreading Phase		Objective Achievement Phase						
1	Network Asset	Switch (within DMZ), DMZ	3	2	2	B	Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type)				IPS/IDS				2
									FW (Application Gateway Type)				Log Collection/Log Analysis				
									One-way Gateway				Integrated Log Management System				
									Proxy Server								
									WAF								
									Peer-to-Peer Authentication	○							
									IPS/IDS								
									Applying Patches	○							
									Avoidance of Vulnerability								
2			1	1		D	Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with access restrictions. It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).	Entrance and Exit Management (IC Card, Biometric Authentication)	○			Surveillance Camera	○			3
									Lock and Key management	○			Intrusion Detection Sensor	○			
3			2	2		C	Unauthorized Operation	Intrusion through direct operation of the device's console or other component to execute an attack.	Operator Authentication (ID/Pass)	○							2
4			2	3		B	Human Error in Operation	An attack triggered by a human error in operation by internal personnel (an employee or partner with access privileges to the device). An act equivalent to an attack is performed on the device as a result of a proper media or device connection.	URL Filtering/Web Reputation								1
									Mail Filtering								
5			2	3		B	Connecting Unauthorized Media or Device	Connection of unauthorized media or device (CD/DVD, USB device, etc.) brought in from outside the organization with the device to execute an attack.	Restriction on Connecting Device and its Usage		(Same as on the Left)		(Same as on the Left)				1
													Log Collection/Log Analysis				
													Integrated Log Management System				
6			2	2		C	Execution of Unauthorized Processes	Unauthorized execution of legitimate programs, commands, services, and other processes found on the attack target device.	Permission Management	○	(Same as on the Left)		Device Error Detection				2
									Access Control		(Same as on the Left)		Device Alive Monitoring				
									Application Whitelisting		(Same as on the Left)		Log Collection/Log Analysis				
									Approval of Important Operations		(Same as on the Left)		Integrated Log Management System				
7			1	3		C	Malware Infection	Infection or running of malware (unauthorized programs) on the attack target device.	Anti-virus				Device Error Detection				1
									Application Whitelisting				Device Alive Monitoring				
									Applying Patches				Log Collection/Log Analysis				
									Avoidance of Vulnerability				Integrated Log Management System				
									Data Signature								
8			1	2		D	Information Theft	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management	○	(Same as on the Left)		Log Collection/Log Analysis				2
									Access Control		(Same as on the Left)		Integrated Log Management System				
									Data Encryption		(Same as on the Left)						
									DLP		(Same as on the Left)						
9			3	2		B	Unauthorized Modification of Information	Unauthorized modification of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management	○	(Same as on the Left)		Device Error Detection		Data Backup		2
									Access Control		(Same as on the Left)		Log Collection/Log Analysis				
									Data Signature		(Same as on the Left)		Integrated Log Management System				
10			2	2		C	Information Destruction	Destroying of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.			Permission Management		Device Error Detection		Data Backup		2
											Access Control	○	Log Collection/Log Analysis				
													Integrated Log Management System				
11			1	3		C	Unauthorized Transmission	Sending unauthorized control commands (settings changes, power shutdowns, etc.) and unauthorized data to other devices.	Segmentation/Zoning		(Same as on the Left)		Log Collection/Log Analysis				1
									Data Signature		(Same as on the Left)		Integrated Log Management System				
									Approval of Important Operations		(Same as on the Left)						
12			2	3		B	Outage	Stopping device functions.					Device Error Detection		Redundancy		1
													Device Alive Monitoring		Failsafe Design		
													Log Collection/Log Analysis				
													Integrated Log Management System				
13			3	3		B	DoS Attack	Interruption of regular device operations by sending processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.	DDoS Countermeasures				Device Error Detection		Redundancy		1
													Device Alive Monitoring		Failsafe Design		
													Log Collection/Log Analysis				
													Integrated Log Management System				
14			1	2		D	Theft	Device theft.	Lock and Key Management	○	(Same as on the Left)		(Same as on the Left)				2
15			1	2		D	Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Tamper Resistance		(Same as on the Left)						2
									Obfuscation		(Same as on the Left)						
									Zeroization	○	(Same as on the Left)						
16			2	1		D	Route Blocking	Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Entrance and Exit Management (IC Card, Biometric Authentication)	○			Device Error Detection		Redundancy		3
									Lock and Key management	○			Device Alive Monitoring				
													Log Collection/Log Analysis				
													Integrated Log Management System				
													Surveillance Camera	○			
													Intrusion Detection Sensor	○			
17			2	3		B	Network Congestion	Causing congestion by generating the communications traffic that exceeds the capacity of the device.	FW (Packet Filtering Type)				Device Error Detection		Redundancy		1
									FW (Application Gateway Type)				Device Alive Monitoring				
									WAF				Log Collection/Log Analysis				
									IPS/IDS				Integrated Log Management System				
									DDoS Countermeasures								
18	Not applicable (no functions)						Jamming	Interference with radio communications.					Device Error Detection		Redundancy		
													Device Alive Monitoring				
													Log Collection/Log Analysis				
													Integrated Log Management System				
19			2	3		B	Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels								1
									Data Encryption								
									Exclusive Line								
20			2	3		B	Unauthorized Modification of Communication Data	Maliciously modifying information flowing on the network.	Encryption of Communications Channels				Log Collection/Log Analysis				1
									Data Signature				Integrated Log Management System				
									Exclusive Line								
21			3	3		B	Connecting Unauthorized Device	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage				Restriction on Connecting Device and its Usage				1
													Log Collection/Log Analysis				
													Integrated Log Management System				

Table 3-6: Asset-based Risk Assessment Sheet

Legend: ○ Measures implemented   Grayed out lines: Threats not taken into account for the corresponding asset   Green text in measures: Supplementary information on measures

Item Number	Type of Assets	Target Device	Assessment Metrics				Threat (Attack Type)	Description	Countermeasures								Security Level
									Protection				Detection/Understanding Damage		Business Continuity		By Threat
			Threat Level	Vulnerability Level	Importance of Assets	Risk Value			Intrusion/Spreading Phase		Objective Achievement Phase						
1	Control System Asset	Data Historian (Relay)	3	2	2	B	Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type)				IPS/IDS				2
									FW (Application Gateway Type)				Log Collection/Log Analysis				
									One-way Gateway				Integrated Log Management System				
									Proxy Server								
									WAF								
									Peer-to-Peer Authentication	○							
									IPS/IDS								
									Applying Patches (Web Server Only)	○							
									Avoidance of Vulnerability								
2			1	1		D	Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with access restrictions. It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).	Entrance and Exit Management (IC Card, Biometric Authentication)	○			Surveillance Camera	○			3
									Lock and Key management	○			Intrusion Detection Sensor	○			
3			2	2		C	Unauthorized Operation	Intrusion through direct operation of the device's console or other component to execute an attack.	Operator Authentication (ID/Pass)	○							2
4			2	3		B	Human Error in Operation	An attack triggered by a human error in operation by internal personnel (an employee or partner with access privileges to the device). An act equivalent to an attack is performed on the device as a result of a proper media or device connection.	URL Filtering/Web Reputation								1
									Mail Filtering								
5			2	3		B	Connecting Unauthorized Media or Device	Connection of unauthorized media or device (CD/DVD, USB device, etc.) brought in from outside the organization with the device to execute an attack.	Restriction on Connecting Device and its Usage		(Same as on the Left)		Restriction on Connecting Device and its Usage				1
													Log Collection/Log Analysis				
													Integrated Log Management System				
6			2	2		C	Execution of Unauthorized Processes	Unauthorized execution of legitimate programs, commands, services, and other processes found on the attack target device.	Permission Management	○	(Same as on the Left)		Device Error Detection				2
									Access Control		(Same as on the Left)		Device Alive Monitoring				
									Application Whitelisting		(Same as on the Left)		Log Collection/Log Analysis				
									Approval of Important Operations		(Same as on the Left)		Integrated Log Management System				
7			3	2		B	Malware Infection	Infection or running of malware (unauthorized programs) on the attack target device.	Anti-virus	○			Device Error Detection				2
									Application Whitelisting				Device Alive Monitoring				
									Applying Patches				Log Collection/Log Analysis				
									Avoidance of Vulnerability				Integrated Log Management System				
									Data Signature								
8			3	2		B	Information Theft	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management	○	(Same as on the Left)		Log Collection/Log Analysis				2
									Access Control		(Same as on the Left)		Integrated Log Management System				
									Data Encryption		(Same as on the Left)						
									DLP		(Same as on the Left)						
9			3	2		B	Unauthorized Modification of Information	Unauthorized modification of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management	○	(Same as on the Left)		Device Error Detection		Data Backup	○	2
									Access Control		(Same as on the Left)		Log Collection/Log Analysis				
									Data Signature		(Same as on the Left)		Integrated Log Management System				
10			3	2		B	Information Destruction	Destroying of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.			Permission Management	○	Device Error Detection		Data Backup	○	2
											Access Control	○	Log Collection/Log Analysis				
													Integrated Log Management System				
11			3	3		B	Unauthorized Transmission	Sending unauthorized control commands (settings changes, power shutdowns, etc.) and unauthorized data to other devices.	Segmentation/Zoning		(Same as on the Left)		Log Collection/Log Analysis				1
									Data Signature		(Same as on the Left)		Integrated Log Management System				
									Approval of Important Operations		(Same as on the Left)						
12			3	3		B	Outage	Stopping device functions.					Device Error Detection		Redundancy		1
													Device Alive Monitoring		Failsafe Design		
													Log Collection/Log Analysis				
													Integrated Log Management System				
13			1	3		C	DoS Attack	Interruption of regular device operations by sending processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.	DDoS Countermeasures				Device Error Detection		Redundancy		1
													Device Alive Monitoring		Failsafe Design		
													Log Collection/Log Analysis				
													Integrated Log Management System				
14			1	2		D	Theft	Device theft.	Lock and Key Management	○	(Same as on the Left)		(Same as on the Left)				2
15			1	2		D	Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Tamper Resistance		(Same as on the Left)						2
									Obfuscation		(Same as on the Left)						
									Zeroization	○	(Same as on the Left)						
16							Route Blocking	Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Entrance and Exit Management				Device Error Detection		Redundancy		
									Lock and Key management				Device Alive Monitoring				
													Log Collection/Log Analysis				
													Integrated Log Management System				
													Surveillance Camera				
													Intrusion Detection Sensor				
17							Network Congestion	Causing congestion by generating the communications traffic that exceeds the capacity of the device.	FW (Packet Filtering Type)				Device Error Detection		Redundancy		
									FW (Application Gateway Type)				Device Alive Monitoring				
									WAF				Log Collection/Log Analysis				
									IPS/IDS				Integrated Log Management System				
									DDoS Countermeasures								
18							Jamming	Interference with radio communications.					Device Error Detection		Redundancy		
													Device Alive Monitoring				
													Log Collection/Log Analysis				
													Integrated Log Management System				
19	Not applicable (no functions)						Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels								
									Data Encryption								
									Exclusive Line								
20							Unauthorized Modification of Communication Data	Maliciously modifying information flowing on the network.	Encryption of Communications Channels				Log Collection/Log Analysis				
									Data Signature				Integrated Log Management System				
									Exclusive Line								
21							Connecting Unauthorized Device	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage				Restriction on Connecting Device and its Usage				
													Log Collection/Log Analysis				
													Integrated Log Management System				

Table 3-6: Asset-based Risk Assessment Sheet

Legend: ○ Measures implemented   Grayed out lines: Threats not taken into account for the corresponding asset   Green text in measures: Supplementary information on measures

Item Number	Type of Assets	Target Device	Assessment Metrics				Threat (Attack Type)	Description	Countermeasures				Security Level
			Threat Level	Vulnerability Level	Importance of Assets	Risk Value			Protection		Detection/Understanding Damage	Business Continuity	By Threat
									Intrusion/Spreading Phase	Objective Achievement Phase			
1	Control System Asset	Data Historian	2	2	2	C	Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type) FW (Application Gateway Type) One-way Gateway Proxy Server WAF Peer-to-Peer Authentication ○ IPS/IDS Applying Patches Avoidance of Vulnerability		IPS/IDS Log Collection/Log Analysis Integrated Log Management System		2
2			1	1		D	Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with access restrictions. It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).	Entrance and Exit Management (IC Card, Biometric Authentication) ○ Lock and Key management ○		Surveillance Camera ○ Intrusion Detection Sensor ○		3
3			2	2		C	Unauthorized Operation	Intrusion through direct operation of the device's console or other component to execute an attack.	Operator Authentication (ID/Pass) ○				2
4			2	3		B	Human Error in Operation	An attack triggered by a human error in operation by internal personnel (an employee or partner with access privileges to the device). An act equivalent to an attack is performed on the device as a result of a proper media or device connection.	URL Filtering/Web Reputation Mail Filtering				1
5			2	3		B	Connecting Unauthorized Media or Device	Connection of unauthorized media or device (CD/DVD, USB device, etc.) brought in from outside the organization with the device to execute an attack.	Restriction on Connecting Device and its Usage	(Same as on the Left)	(Same as on the Left) Log Collection/Log Analysis Integrated Log Management System		1
6			2	2		C	Execution of Unauthorized Processes	Unauthorized execution of legitimate programs, commands, services, and other processes found on the attack target device.	Permission Management ○ Access Control Application Whitelisting ○ Approval of Important Operations	(Same as on the Left) (Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		2
7			3	2		B	Malware Infection	Infection or running of malware (unauthorized programs) on the attack target device.	Anti-virus Application Whitelisting ○ Applying Patches Avoidance of Vulnerability Data Signature		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		2
8			3	2		B	Information Theft	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management ○ Access Control Data Encryption DLP	(Same as on the Left) (Same as on the Left) (Same as on the Left) (Same as on the Left)	Log Collection/Log Analysis Integrated Log Management System		2
9			3	2		B	Unauthorized Modification of Information	Unauthorized modification of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management ○ Access Control Data Signature	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup ○	2
10			3	2		B	Information Destruction	Destroying of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.		Permission Management ○ Access Control	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup ○	2
11			3	3		B	Unauthorized Transmission	Sending unauthorized control commands (settings changes, power shutdowns, etc.) and unauthorized data to other devices.	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Log Collection/Log Analysis Integrated Log Management System		1
12			3	3		B	Outage	Stopping device functions.			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Redundancy Failsafe Design	1
13			1	3		C	DoS Attack	Interruption of regular device operations by sending processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.	DDoS Countermeasures		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Redundancy Failsafe Design	1
14			1	2		D	Theft	Device theft.	Lock and Key Management ○	(Same as on the Left)	(Same as on the Left)		2
15			1	2		D	Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Tamper Resistance Obfuscation Zeroization ○	(Same as on the Left) (Same as on the Left) (Same as on the Left)			2
16							Route Blocking	Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Entrance and Exit Management Lock and Key management		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor	Redundancy	
17							Network Congestion	Causing congestion by generating the communications traffic that exceeds the capacity of the device.	FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Redundancy	
18							Jamming	Interference with radio communications.			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Redundancy	
19							Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels Data Encryption Exclusive Line				
20							Unauthorized Modification of Communication Data	Maliciously modifying information flowing on the network.	Encryption of Communications Channels Data Signature Exclusive Line		Log Collection/Log Analysis Integrated Log Management System		
21							Connecting Unauthorized Device	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage		Restriction on Connecting Device and its Usage Log Collection/Log Analysis Integrated Log Management System		

Not applicable (no functions)

Table 3-6: Asset-based Risk Assessment Sheet

Legend: ○ Measures implemented Grayed out lines: Threats not taken into account for the corresponding asset Green text in measures: Supplementary information on measures

Item Number	Type of Assets	Target Device	Assessment Metrics				Threat (Attack Type)	Description	Countermeasures								Security Level
									Protection				Detection/Understanding Damage		Business Continuity		By Threat
			Threat Level	Vulnerability Level	Importance of Assets	Risk Value			Intrusion/Spreading Phase		Objective Achievement Phase						
1	Network Asset	**Switch (in Control Network (Information Side)), Control Network (Information Side)**	**2**	**2**	**2**	**C**	Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type) FW (Application Gateway Type) One-way Gateway Proxy Server WAF Peer-to-Peer Authentication IPS/IDS Applying Patches Avoidance of Vulnerability	 ○			IPS/IDS Log Collection/Log Analysis Integrated Log Management System				2
2			**1**	**2**		**D**	Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with access restrictions. It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).	Entrance and Exit Management (IC Card) Lock and Key Management	○ ○			Surveillance Camera Intrusion Detection Sensor	○ ○			2
3			**2**	**2**		**C**	Unauthorized Operation	Intrusion through direct operation of the device's console or other component to execute an attack.	Operator Authentication (ID/Pass)	○							2
4			**2**	**3**		**B**	Human Error in Operation	An attack triggered by a human error in operation by internal personnel (an employee or partner with access privileges to the device). An act equivalent to an attack is performed on the device as a result of a proper media or device connection.	URL Filtering/Web Reputation Mail Filtering								1
5			**2**	**3**		**B**	Connecting Unauthorized Media or Device	Connection of unauthorized media or device (CD/DVD, USB device, etc.) brought in from outside the organization with the device to execute an attack.	Restriction on Connecting Device and its Usage		(Same as on the Left)		(Same as on the Left) Log Collection/Log Analysis Integrated Log Management System				1
6			**1**	**2**		**D**	Execution of Unauthorized Processes	Unauthorized execution of legitimate programs, commands, services, and other processes found on the attack target device.	Permission Management Access Control Application Whitelisting Approval of Important Operations	○	(Same as on the Left) (Same as on the Left) (Same as on the Left) (Same as on the Left)		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System				2
7			**1**	**3**		**C**	Malware Infection	Infection or running of malware (unauthorized programs) on the attack target device.	Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System				1
8			**1**	**2**		**D**	Information Theft	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management Access Control Data Encryption DLP	○	(Same as on the Left) (Same as on the Left) (Same as on the Left) (Same as on the Left)		Log Collection/Log Analysis Integrated Log Management System				2
9			**2**	**2**		**C**	Unauthorized Modification of Information	Unauthorized modification of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management Access Control Data Signature	○	(Same as on the Left) (Same as on the Left) (Same as on the Left)		Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		2
10			**2**	**2**		**C**	Information Destruction	Destroying of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.			Permission Management Access Control	 ○	Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		2
11			**1**	**3**		**C**	Unauthorized Transmission	Sending unauthorized control commands (settings changes, power shutdowns, etc.) and unauthorized data to other devices.	Segmentation/Zoning Data Signature Approval of Important Operations		(Same as on the Left) (Same as on the Left) (Same as on the Left)		Log Collection/Log Analysis Integrated Log Management System				1
12			**2**	**3**		**B**	Outage	Stopping device functions.					Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy Failsafe Design		1
13			**3**	**3**		**B**	DoS Attack	Interruption of regular device operations by sending processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.	DDoS Countermeasures				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy Failsafe Design		1
14			**1**	**2**		**D**	Theft	Device theft.	Lock and Key Management	○	(Same as on the Left)		Lock and Key Management	○			2
15			**1**	**2**		**D**	Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Tamper Resistance Obfuscation Zeroization	 ○	(Same as on the Left) (Same as on the Left) (Same as on the Left)						2
16			**2**	**2**		**C**	Route Blocking	Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Entrance and Exit Management (IC Card) Lock and Key management	○ ○			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor	 ○ ○	Redundancy		2
17			**2**	**3**		**B**	Network Congestion	Causing congestion by generating the communications traffic that exceeds the capacity of the device.	FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy		1
18	Not applicable (no functions)						Jamming	Interference with radio communications.					Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy		
19			**2**	**3**		**B**	Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels Data Encryption Exclusive Line								1
20			**2**	**3**		**B**	Unauthorized Modification of Communication Data	Maliciously modifying information flowing on the network.	Encryption of Communications Channels Data Signature Exclusive Line				Log Collection/Log Analysis Integrated Log Management System				1
21			**3**	**3**		**B**	Connecting Unauthorized Device	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage				Restriction on Connecting Device and its Usage Log Collection/Log Analysis Integrated Log Management System				1

Table 3-6: Asset-based Risk Assessment Sheet

Legend: ○ Measures implemented Grayed out lines: Threats not taken into account for the corresponding asset Green text in measures: Supplementary information on measures

Item Number	Type of Assets	Target Device	Assessment Metrics				Threat (Attack Type)	Description	Countermeasures								Security Level
									Protection				Detection/Understanding Damage		Business Continuity		By Threat
			Threat Level	Vulnerability Level	Importance of Assets	Risk Value			Intrusion/Spreading Phase		Objective Achievement Phase						
1	Control System Asset	EWS	2	2	3	B	Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type)				IPS/IDS				2
									FW (Application Gateway Type)				Log Collection/Log Analysis				
									One-way Gateway				Integrated Log Management System				
									Proxy Server								
									WAF								
									Peer-to-Peer Authentication	○							
									IPS/IDS								
									Applying Patches								
									Avoidance of Vulnerability								
2			1	1		C	Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with access restrictions. It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).	Entrance and Exit Management (IC Card, Biometric Authentication)	○			Surveillance Camera	○			3
									Lock and Key Management	○			Intrusion Detection Sensor	○			
3			2	2		B	Unauthorized Operation	Intrusion through direct operation of the device's console or other component to execute an attack.	Operator Authentication (ID/Pass)	○							2
4			2	3		A	Human Error in Operation	An attack triggered by a human error in operation by internal personnel (an employee or partner with access privileges to the device). An act equivalent to an attack is performed on the device as a result of a proper media or device connection.	URL Filtering/Web Reputation								1
									Mail Filtering								
5			3	3		A	Connecting Unauthorized Media or Device	Connection of unauthorized media or device (CD/DVD, USB device, etc.) brought in from outside the organization with the device to execute an attack.	Restriction on Connecting Device and its Usage		(Same as on the Left)		(Same as on the Left)				1
													Log Collection/Log Analysis				
													Integrated Log Management System				
6			3	3		A	Execution of Unauthorized Processes	Unauthorized execution of legitimate programs, commands, services, and other processes found on the attack target device.	Permission Management		(Same as on the Left)		Device Error Detection				1
									Access Control		(Same as on the Left)		Device Alive Monitoring				
									Application Whitelisting		(Same as on the Left)		Log Collection/Log Analysis				
									Approval of Important Operations		(Same as on the Left)		Integrated Log Management System				
7			3	3		A	Malware Infection	Infection or running of malware (unauthorized programs) on the attack target device.	Anti-virus				Device Error Detection				1
									Application Whitelisting				Device Alive Monitoring				
									Applying Patches				Log Collection/Log Analysis				
									Avoidance of Vulnerability				Integrated Log Management System				
									Data Signature								
8			3	3		A	Information Theft	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management		(Same as on the Left)		Log Collection/Log Analysis				1
									Access Control		(Same as on the Left)		Integrated Log Management System				
									Data Encryption		(Same as on the Left)						
									DLP		(Same as on the Left)						
9			3	3		A	Unauthorized Modification of Information	Unauthorized modification of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management		(Same as on the Left)		Device Error Detection		Data Backup		1
									Access Control		(Same as on the Left)		Log Collection/Log Analysis				
									Data Signature		(Same as on the Left)		Integrated Log Management System				
10			3	3		A	Information Destruction	Destroying of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.			Permission Management		Device Error Detection		Data Backup		1
											Access Control		Log Collection/Log Analysis				
													Integrated Log Management System				
11			3	3		A	Unauthorized Transmission	Sending unauthorized control commands (settings changes, power shutdowns, etc.) and unauthorized data to other devices.	Segmentation/Zoning		(Same as on the Left)		Log Collection/Log Analysis				1
									Data Signature		(Same as on the Left)		Integrated Log Management System				
									Approval of Important Operations		(Same as on the Left)						
12			3	3		A	Outage	Stopping device functions.					Device Error Detection		Redundancy		1
													Device Alive Monitoring		Failsafe Design		
													Log Collection/Log Analysis				
													Integrated Log Management System				
13			1	3		B	DoS Attack	Interruption of regular device operations by sending processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.	DDoS Countermeasures				Device Error Detection		Redundancy		1
													Device Alive Monitoring		Failsafe Design		
													Log Collection/Log Analysis				
													Integrated Log Management System				
14			2	2		B	Theft	Device theft.	Lock and Key Management	○	(Same as on the Left)		(Same as on the Left)				2
15			2	2		B	Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Tamper Resistance		(Same as on the Left)						2
									Obfuscation		(Same as on the Left)						
									Zeroization	○	(Same as on the Left)						
16							Route Blocking	Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Entrance and Exit Management				Device Error Detection		Redundancy		
									Lock and Key management				Device Alive Monitoring				
													Log Collection/Log Analysis				
													Integrated Log Management System				
													Surveillance Camera				
													Intrusion Detection Sensor				
17							Network Congestion	Causing congestion by generating the communications traffic that exceeds the capacity of the device.	FW (Packet Filtering Type)				Device Error Detection		Redundancy		
									FW (Application Gateway Type)				Device Alive Monitoring				
									WAF				Log Collection/Log Analysis				
									IPS/IDS				Integrated Log Management System				
									DDoS Countermeasures								
18	Not applicable (no functions)						Jamming	Interference with radio communications.					Device Error Detection		Redundancy		
													Device Alive Monitoring				
													Log Collection/Log Analysis				
													Integrated Log Management System				
19							Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels								
									Data Encryption								
									Exclusive Line								
20							Unauthorized Modification of Communication Data	Maliciously modifying information flowing on the network.	Encryption of Communications Channels				Log Collection/Log Analysis				
									Data Signature				Integrated Log Management System				
									Exclusive Line								
21							Connecting Unauthorized Device	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage				Restriction on Connecting Device and its Usage				
													Log Collection/Log Analysis				
													Integrated Log Management System				

Table 3-6: Asset-based Risk Assessment Sheet

Legend: ○ Measures implemented   Grayed out lines: Threats not taken into account for the corresponding asset   Green text in measures: Supplementary information on measures

Item Number	Type of Assets	Target Device	Assessment Metrics				Threat (Attack Type)	Description	Countermeasures								Security Level
									Protection				Detection/Understanding Damage		Business Continuity		By Threat
			Threat Level	Vulnerability Level	Importance of Assets	Risk Value			Intrusion/Spreading Phase		Objective Achievement Phase						
1	Control System Asset	**Control Server**	2	2	3	B	Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type)				IPS/IDS				2
									FW (Application Gateway Type)				Log Collection/Log Analysis				
									One-way Gateway				Integrated Log Management System				
									Proxy Server								
									WAF								
									Peer-to-Peer Authentication	○							
									IPS/IDS								
									Applying Patches								
									Avoidance of Vulnerability								
2			1	1		C	Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with access restrictions. It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).	Entrance and Exit Management (IC Card, Biometric Authentication)	○			Surveillance Camera	○			3
									Lock and Key management	○			Intrusion Detection Sensor	○			
3			2	2		B	Unauthorized Operation	Intrusion through direct operation of the device's console or other component to execute an attack.	Operator Authentication (ID/Pass)	○							2
4			2	3		A	Human Error in Operation	An attack triggered by a human error in operation by internal personnel (an employee or partner with access privileges to the device). An act equivalent to an attack is performed on the device as a result of a proper media or device connection.	URL Filtering/Web Reputation								1
									Mail Filtering								
5			2	3		A	Connecting Unauthorized Media or Device	Connection of unauthorized media or device (CD/DVD, USB device, etc.) brought in from outside the organization with the device to execute an attack.	Restriction on Connecting Device and its Usage		(Same as on the Left)		(Same as on the Left)				1
													Log Collection/Log Analysis				
													Integrated Log Management System				
6			3	2		A	Execution of Unauthorized Processes	Unauthorized execution of legitimate programs, commands, services, and other processes found on the attack target device.	Permission Management	○	(Same as on the Left)		Device Error Detection				2
									Access Control		(Same as on the Left)		Device Alive Monitoring				
									Application Whitelisting	○	(Same as on the Left)		Log Collection/Log Analysis				
									Approval of Important Operations		(Same as on the Left)		Integrated Log Management System				
7			3	2		A	Malware Infection	Infection or running of malware (unauthorized programs) on the attack target device.	Anti-virus				Device Error Detection				2
									Application Whitelisting	○			Device Alive Monitoring				
									Applying Patches				Log Collection/Log Analysis				
									Avoidance of Vulnerability				Integrated Log Management System				
									Data Signature								
8			3	2		A	Information Theft	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management	○	(Same as on the Left)		Log Collection/Log Analysis				2
									Access Control		(Same as on the Left)		Integrated Log Management System				
									Data Encryption		(Same as on the Left)						
									DLP		(Same as on the Left)						
9			3	2		A	Unauthorized Modification of Information	Unauthorized modification of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management	○	(Same as on the Left)		Device Error Detection		Data Backup	○	2
									Access Control		(Same as on the Left)		Log Collection/Log Analysis				
									Data Signature		(Same as on the Left)		Integrated Log Management System				
10			3	2		A	Information Destruction	Destroying of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.			Permission Management	○	Device Error Detection		Data Backup	○	2
											Access Control		Log Collection/Log Analysis				
													Integrated Log Management System				
11			3	3		A	Unauthorized Transmission	Sending unauthorized control commands (settings changes, power shutdowns, etc.) and unauthorized data to other devices.	Segmentation/Zoning		(Same as on the Left)		Log Collection/Log Analysis				1
									Data Signature		(Same as on the Left)		Integrated Log Management System				
									Approval of Important Operations		(Same as on the Left)						
12			3	3		A	Outage	Stopping device functions.					Device Error Detection		Redundancy		1
													Device Alive Monitoring		Failsafe Design		
													Log Collection/Log Analysis				
													Integrated Log Management System				
13			1	3		B	DoS Attack	Interruption of regular device operations by sending processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.	DDoS Countermeasures				Device Error Detection		Redundancy		1
													Device Alive Monitoring		Failsafe Design		
													Log Collection/Log Analysis				
													Integrated Log Management System				
14			1	2		C	Theft	Device theft.	Lock and Key Management	○	(Same as on the Left)		(Same as on the Left)				2
15			1	2		C	Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Tamper Resistance		(Same as on the Left)						2
									Obfuscation		(Same as on the Left)						
									Zeroization	○	(Same as on the Left)						
16							Route Blocking	Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Entrance and Exit Management				Device Error Detection		Redundancy		
									Lock and Key management				Device Alive Monitoring				
													Log Collection/Log Analysis				
													Integrated Log Management System				
													Surveillance Camera				
													Intrusion Detection Sensor				
17							Network Congestion	Causing congestion by generating the communications traffic that exceeds the capacity of the device.	FW (Packet Filtering Type)				Device Error Detection		Redundancy		
									FW (Application Gateway Type)				Device Alive Monitoring				
									WAF				Log Collection/Log Analysis				
									IPS/IDS				Integrated Log Management System				
									DDoS Countermeasures								
18	Not applicable (no functions)						Jamming	Interference with radio communications.					Device Error Detection		Redundancy		
													Device Alive Monitoring				
													Log Collection/Log Analysis				
													Integrated Log Management System				
19							Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels								
									Data Encryption								
									Exclusive Line								
20							Unauthorized Modification of Communication Data	Maliciously modifying information flowing on the network.	Encryption of Communications Channels				Log Collection/Log Analysis				
									Data Signature				Integrated Log Management System				
									Exclusive Line								
21							Connecting Unauthorized Device	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage				Restriction on Connecting Device and its Usage				
													Log Collection/Log Analysis				
													Integrated Log Management System				

Table 3-6: Asset-based Risk Assessment Sheet

Legend: ○ Measures implemented   Grayed out lines: Threats not taken into account for the corresponding asset   Green text in measures: Supplementary information on measures

Item Number	Type of Assets	Target Device	Assessment Metrics				Threat (Attack Type)	Description	Countermeasures								Security Level
									Protection				Detection/Understanding Damage		Business Continuity		By Threat
			Threat Level	Vulnerability Level	Importance of Assets	Risk Value			Intrusion/Spreading Phase		Objective Achievement Phase						
1	Control System Asset	HMI (Operator Terminal)	2	2	3	B	Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type) FW (Application Gateway Type) One-way Gateway Proxy Server WAF Peer-to-Peer Authentication IPS/IDS Applying Patches Avoidance of Vulnerability	 ○			IPS/IDS Log Collection/Log Analysis Integrated Log Management System				2
2			2	2		B	Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with access restrictions. It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).	Entrance and Exit Management (IC Card) Lock and Key Management	○ ○			Surveillance Camera Intrusion Detection Sensor	○ ○			2
3			2	3		A	Unauthorized Operation	Intrusion through direct operation of the device's console or other component to execute an attack.	Operator Authentication								1
4			2	3		A	Human Error in Operation	An attack triggered by a human error in operation by internal personnel (an employee or partner with access privileges to the device). An act equivalent to an attack is performed on the device as a result of a proper media or device connection.	URL Filtering/Web Reputation Mail Filtering								1
5			3	3		A	Connecting Unauthorized Media or Device	Connection of unauthorized media or device (CD/DVD, USB device, etc.) brought in from outside the organization with the device to execute an attack.	Restriction on Connecting Device and its Usage		(Same as on the Left)		(Same as on the Left) Log Collection/Log Analysis Integrated Log Management System				1
6			3	3		A	Execution of Unauthorized Processes	Unauthorized execution of legitimate programs, commands, services, and other processes found on the attack target device.	Permission Management Access Control Application Whitelisting Approval of Important Operations		(Same as on the Left) (Same as on the Left) (Same as on the Left) (Same as on the Left)		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System				1
7			3	3		A	Malware Infection	Infection or running of malware (unauthorized programs) on the attack target device.	Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System				1
8			3	3		A	Information Theft	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management Access Control Data Encryption DLP		(Same as on the Left) (Same as on the Left) (Same as on the Left) (Same as on the Left)		Log Collection/Log Analysis Integrated Log Management System				1
9			3	3		A	Unauthorized Modification of Information	Unauthorized modification of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management Access Control Data Signature		(Same as on the Left) (Same as on the Left) (Same as on the Left)		Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		1
10			3	3		A	Information Destruction	Destroying of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.			Permission Management Access Control		Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		1
11			3	3		A	Unauthorized Transmission	Sending unauthorized control commands (settings changes, power shutdowns, etc.) and unauthorized data to other devices.	Segmentation/Zoning Data Signature Approval of Important Operations		(Same as on the Left) (Same as on the Left) (Same as on the Left)		Log Collection/Log Analysis Integrated Log Management System				1
12			3	3		A	Outage	Stopping device functions.					Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy Failsafe Design		1
13			1	3		B	DoS Attack	Interruption of regular device operations by sending processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.	DDoS Countermeasures				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy Failsafe Design		1
14			2	2		B	Theft	Device theft.	Lock and Key Management	○	(Same as on the Left)		(Same as on the Left)				2
15			2	2		B	Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Tamper Resistance Obfuscation Zeroization	 ○	(Same as on the Left) (Same as on the Left) (Same as on the Left)						2
16							Route Blocking	Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Entrance and Exit Management Lock and Key management				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor		Redundancy		
17							Network Congestion	Causing congestion by generating the communications traffic that exceeds the capacity of the device.	FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy		
18	Not applicable (no functions)						Jamming	Interference with radio communications.					Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy		
19							Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels Data Encryption Exclusive Line								
20							Unauthorized Modification of Communication Data	Maliciously modifying information flowing on the network.	Encryption of Communications Channels Data Signature Exclusive Line				Log Collection/Log Analysis Integrated Log Management System				
21							Connecting Unauthorized Device	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage				Restriction on Connecting Device and its Usage Log Collection/Log Analysis Integrated Log Management System				

Table 3-6: Asset-based Risk Assessment Sheet

Legend: ○ Measures implemented Grayed out lines: Threats not taken into account for the corresponding asset Green text in measures: Supplementary information on measures

Item Number	Type of Assets	Target Device	Assessment Metrics				Threat (Attack Type)	Description	Countermeasures								Security Level
									Protection				Detection/Understanding Damage		Business Continuity		By Threat
			Threat Level	Vulnerability Level	Importance of Assets	Risk Value			Intrusion/Spreading Phase		Objective Achievement Phase						
1	Network Asset	Control Network (Field Side)			3		Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type) FW (Application Gateway Type) One-way Gateway Proxy Server WAF Peer-to-Peer Authentication IPS/IDS Applying Patches Avoidance of Vulnerability				IPS/IDS Log Collection/Log Analysis Integrated Log Management System				
2							Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with access restrictions. It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).	Entrance and Exit Management Lock and Key Management				Surveillance Camera Intrusion Detection Sensor				
3							Unauthorized Operation	Intrusion through direct operation of the device's console or other component to execute an attack.	Operator Authentication								
4							Human Error in Operation	An attack triggered by a human error in operation by internal personnel (an employee or partner with access privileges to the device). An act equivalent to an attack is performed on the device as a result of a proper media or device connection.	URL Filtering/Web Reputation Mail Filtering								
5							Connecting Unauthorized Media or Device	Connection of unauthorized media or device (CD/DVD, USB device, etc.) brought in from outside the organization with the device to execute an attack.	Restriction on Connecting Device and its Usage		(Same as on the Left)		Restriction on Connecting Device and its Usage Log Collection/Log Analysis Integrated Log Management System				
6							Execution of Unauthorized Processes	Unauthorized execution of legitimate programs, commands, services, and other processes found on the attack target device.	Permission Management Access Control Application Whitelisting Approval of Important Operations		(Same as on the Left) (Same as on the Left) (Same as on the Left) (Same as on the Left)		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System				
7							Malware Infection	Infection or running of malware (unauthorized programs) on the attack target device.	Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System				
8							Information Theft	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management Access Control Data Encryption DLP		(Same as on the Left) (Same as on the Left) (Same as on the Left) (Same as on the Left)		Log Collection/Log Analysis Integrated Log Management System				
9							Unauthorized Modification of Information	Unauthorized modification of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management Access Control Data Signature		(Same as on the Left) (Same as on the Left) (Same as on the Left)		Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		
10							Information Destruction	Destroying of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.			Permission Management Access Control		Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		
11							Unauthorized Transmission	Sending unauthorized control commands (settings changes, power shutdowns, etc.) and unauthorized data to other devices.	Segmentation/Zoning Data Signature Approval of Important Operations		(Same as on the Left) (Same as on the Left) (Same as on the Left)		Log Collection/Log Analysis Integrated Log Management System				
12							Outage	Stopping device functions.					Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy Failsafe Design		
13							DoS Attack	Interruption of regular device operations by sending processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.	DDoS Countermeasures				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy Failsafe Design		
14							Theft	Device theft.	Lock and Key Management	○	(Same as on the Left)		(Same as on the Left)				
15							Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Tamper Resistance Obfuscation Zeroization		(Same as on the Left) (Same as on the Left) (Same as on the Left)						
16			3	2		A	Route Blocking	Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Entrance and Exit Management (IC Card, Biometric Authentication) Lock and Key management	○ ○			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor		Redundancy		2
17			2	3		A	Network Congestion	Causing congestion by generating the communications traffic that exceeds the capacity of the device.	FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy		1
18	Not applicable (no functions)						Jamming	Interference with radio communications.					Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy		
19			2	3		A	Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels Data Encryption Exclusive Line								1
20			2	3		A	Unauthorized Modification of Communication Data	Maliciously modifying information flowing on the network.	Encryption of Communications Channels Data Signature Exclusive Line				Log Collection/Log Analysis Integrated Log Management System				1
21			2	3		A	Connecting Unauthorized Device	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage				Restriction on Connecting Device and its Usage Log Collection/Log Analysis Integrated Log Management System				1

Table 3-6: Asset-based Risk Assessment Sheet

Legend: ○ Measures implemented   Grayed out lines: Threats not taken into account for the corresponding asset   Green text in measures: Supplementary information on measures

Item Number	Type of Assets	Target Device	Assessment Metrics				Threat (Attack Type)	Description	Countermeasures								Security Level
									Protection				Detection/Understanding Damage		Business Continuity		By Threat
			Threat Level	Vulnerability Level	Importance of Assets	Risk Value			Intrusion/Spreading Phase		Objective Achievement Phase						
1	Network Asset	**Field Network**			3		Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type) FW (Application Gateway Type) One-way Gateway Proxy Server WAF Peer-to-Peer Authentication IPS/IDS Applying Patches Avoidance of Vulnerability				IPS/IDS Log Collection/Log Analysis Integrated Log Management System				
2							Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with access restrictions. It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).	Entrance and Exit Management Lock and Key Management				Surveillance Camera Intrusion Detection Sensor				
3							Unauthorized Operation	Intrusion through direct operation of the device's console or other component to execute an attack.	Operator Authentication								
4							Human Error in Operation	An attack triggered by a human error in operation by internal personnel (an employee or partner with access privileges to the device). An act equivalent to an attack is performed on the device as a result of a proper media or device connection.	URL Filtering/Web Reputation Mail Filtering								
5							Connecting Unauthorized Media or Device	Connection of unauthorized media or device (CD/DVD, USB device, etc.) brought in from outside the organization with the device to execute an attack.	Restriction on Connecting Device and its Usage		(Same as on the Left)		Restriction on Connecting Device and its Usage Log Collection/Log Analysis Integrated Log Management System				
6							Execution of Unauthorized Processes	Unauthorized execution of legitimate programs, commands, services, and other processes found on the attack target device.	Permission Management Access Control Application Whitelisting Approval of Important Operations		(Same as on the Left) (Same as on the Left) (Same as on the Left) (Same as on the Left)		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System				
7							Malware Infection	Infection or running of malware (unauthorized programs) on the attack target device.	Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System				
8							Information Theft	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management Access Control Data Encryption DLP		(Same as on the Left) (Same as on the Left) (Same as on the Left) (Same as on the Left)		Log Collection/Log Analysis Integrated Log Management System				
9							Unauthorized Modification of Information	Unauthorized modification of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management Access Control Data Signature		(Same as on the Left) (Same as on the Left) (Same as on the Left)		Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		
10							Information Destruction	Destroying of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.			Permission Management Access Control		Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		
11							Unauthorized Transmission	Sending unauthorized control commands (settings changes, power shutdowns, etc.) and unauthorized data to other devices.	Segmentation/Zoning Data Signature Approval of Important Operations		(Same as on the Left) (Same as on the Left) (Same as on the Left)		Log Collection/Log Analysis Integrated Log Management System				
12							Outage	Stopping device functions.					Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy Failsafe Design		
13							DoS Attack	Interruption of regular device operations by sending processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.	DDoS Countermeasures				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy Failsafe Design		
14							Theft	Device theft.	Lock and Key Management		(Same as on the Left)		(Same as on the Left)				
15							Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Tamper Resistance Obfuscation Zeroization		(Same as on the Left) (Same as on the Left) (Same as on the Left)						
16			3	2		A	Route Blocking	Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Entrance and Exit Management (on the Premises Only) Lock and Key management	○ ○			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor		Redundancy		2
17			2	3		A	Network Congestion	Causing congestion by generating the communications traffic that exceeds the capacity of the device.	FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy		1
18	Not applicable (no functions)						Jamming	Interference with radio communications.					Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy		
19			2	3		A	Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels Data Encryption Exclusive Line								1
20			2	3		A	Unauthorized Modification of Communication Data	Maliciously modifying information flowing on the network.	Encryption of Communications Channels Data Signature Exclusive Line				Log Collection/Log Analysis Integrated Log Management System				1
21			2	3		A	Connecting Unauthorized Device	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage				Restriction on Connecting Device and its Usage Log Collection/Log Analysis Integrated Log Management System				1

Table 3-6: Asset-based Risk Assessment Sheet

Legend: ○ Measures implemented Grayed out lines: Threats not taken into account for the corresponding asset Green text in measures: Supplementary information on measures

Item Number	Type of Assets	Target Device	Assessment Metrics				Threat (Attack Type)	Description	Countermeasures								Security Level
									Protection				Detection/Understanding Damage		Business Continuity		By Threat
			Threat Level	Vulnerability Level	Importance of Assets	Risk Value			Intrusion/Spreading Phase		Objective Achievement Phase						
1	Control System Asset	Controller, Controller (Master)	2	3	3	A	Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type)				IPS/IDS				1
									FW (Application Gateway Type)				Log Collection/Log Analysis				
									One-way Gateway				Integrated Log Management System				
									Proxy Server								
									WAF								
									Peer-to-Peer Authentication								
									IPS/IDS								
									Applying Patches								
									Avoidance of Vulnerability								
2			2	2		B	Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with access restrictions. It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).	Entrance and Exit Management (IC Card)	○			Surveillance Camera	○			2
									Lock and Key Management	○			Intrusion Detection Sensor	○			
3			2	2		B	Unauthorized Operation	Intrusion through direct operation of the device's console or other component to execute an attack.	Operator Authentication (ID/Pass)	○							2
4			2	3		A	Human Error in Operation	An attack triggered by a human error in operation by internal personnel (an employee or partner with access privileges to the device). An act equivalent to an attack is performed on the device as a result of a proper media or device connection.	URL Filtering/Web Reputation								1
									Mail Filtering								
5			2	3		A	Connecting Unauthorized Media or Device	Connection of unauthorized media or device (CD/DVD, USB device, etc.) brought in from outside the organization with the device to execute an attack.	Restriction on Connecting Device and its Usage		(Same as on the Left)		(Same as on the Left)				1
													Log Collection/Log Analysis				
													Integrated Log Management System				
6			2	3		A	Execution of Unauthorized Processes	Unauthorized execution of legitimate programs, commands, services, and other processes found on the attack target device.	Permission Management		(Same as on the Left)		Device Error Detection				1
									Access Control		(Same as on the Left)		Device Alive Monitoring				
									Application Whitelisting		(Same as on the Left)		Log Collection/Log Analysis				
									Approval of Important Operations		(Same as on the Left)		Integrated Log Management System				
7			1	3		B	Malware Infection	Infection or running of malware (unauthorized programs) on the attack target device.	Anti-virus				Device Error Detection				1
									Application Whitelisting				Device Alive Monitoring				
									Applying Patches				Log Collection/Log Analysis				
									Avoidance of Vulnerability				Integrated Log Management System				
									Data Signature								
8			3	3		A	Information Theft	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management		(Same as on the Left)		Log Collection/Log Analysis				1
									Access Control		(Same as on the Left)		Integrated Log Management System				
									Data Encryption		(Same as on the Left)						
									DLP		(Same as on the Left)						
9			3	3		A	Unauthorized Modification of Information	Unauthorized modification of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management		(Same as on the Left)		Device Error Detection		Data Backup		1
									Access Control		(Same as on the Left)		Log Collection/Log Analysis				
									Data Signature		(Same as on the Left)		Integrated Log Management System				
10			3	3		A	Information Destruction	Destroying of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.			Permission Management		Device Error Detection		Data Backup		1
											Access Control		Log Collection/Log Analysis				
													Integrated Log Management System				
11			3	3		A	Unauthorized Transmission	Sending unauthorized control commands (settings changes, power shutdowns, etc.) and unauthorized data to other devices.	Segmentation/Zoning		(Same as on the Left)		Log Collection/Log Analysis				1
									Data Signature		(Same as on the Left)		Integrated Log Management System				
									Approval of Important Operations		(Same as on the Left)						
12			2	3		A	Outage	Stopping device functions.					Device Error Detection		Redundancy		1
													Device Alive Monitoring		Failsafe Design		
													Log Collection/Log Analysis				
													Integrated Log Management System				
13			3	3		A	DoS Attack	Interruption of regular device operations by sending processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.	DDoS Countermeasures				Device Error Detection		Redundancy		1
													Device Alive Monitoring		Failsafe Design		
													Log Collection/Log Analysis				
													Integrated Log Management System				
14			2	2		B	Theft	Device theft.	Lock and Key Management	○	(Same as on the Left)		(Same as on the Left)				2
15			2	2		B	Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Tamper Resistance		(Same as on the Left)						2
									Obfuscation		(Same as on the Left)						
									Zeroization	○	(Same as on the Left)						
16							Route Blocking	Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Entrance and Exit Management				Device Error Detection		Redundancy		
									Lock and Key management				Device Alive Monitoring				
													Log Collection/Log Analysis				
													Integrated Log Management System				
													Surveillance Camera				
													Intrusion Detection Sensor				
17							Network Congestion	Causing congestion by generating the communications traffic that exceeds the capacity of the device.	FW (Packet Filtering Type)				Device Error Detection		Redundancy		
									FW (Application Gateway Type)				Device Alive Monitoring				
									WAF				Log Collection/Log Analysis				
									IPS/IDS				Integrated Log Management System				
									DDoS Countermeasures								
18							Jamming	Interference with radio communications.					Device Error Detection		Redundancy		
													Device Alive Monitoring				
													Log Collection/Log Analysis				
													Integrated Log Management System				
19							Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels								
									Data Encryption								
									Exclusive Line								
20							Unauthorized Modification of Communication Data	Maliciously modifying information flowing on the network.	Encryption of Communications Channels				Log Collection/Log Analysis				
									Data Signature				Integrated Log Management System				
									Exclusive Line								
21							Connecting Unauthorized Device	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage				Restriction on Connecting Device and its Usage				
													Log Collection/Log Analysis				
													Integrated Log Management System				

Not applicable (no functions)

Table 3-6: Asset-based Risk Assessment Sheet

Legend: ○ Measures implemented   Grayed out lines: Threats not taken into account for the corresponding asset   Green text in measures: Supplementary information on measures

Item Number	Type of Assets	Target Device	Assessment Metrics				Threat (Attack Type)	Description	Countermeasures								Security Level
									Protection				Detection/Understanding Damage		Business Continuity		By Threat
			Threat Level	Vulnerability Level	Importance of Assets	Risk Value			Intrusion/Spreading Phase		Objective Achievement Phase						
1	Control System Asset	Controller (Slave)	2	3	3	A	Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type) FW (Application Gateway Type) One-way Gateway Proxy Server WAF Peer-to-Peer Authentication IPS/IDS Applying Patches Avoidance of Vulnerability				IPS/IDS Log Collection/Log Analysis Integrated Log Management System				1
2			3	2		A	Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with access restrictions. It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).	Entrance and Exit Management Lock and Key Management	 ○			Surveillance Camera Intrusion Detection Sensor				2
3			3	2		A	Unauthorized Operation	Intrusion through direct operation of the device's console or other component to execute an attack.	Operator Authentication (ID/Pass)	○							2
4			2	3		A	Human Error in Operation	An attack triggered by a human error in operation by internal personnel (an employee or partner with access privileges to the device). An act equivalent to an attack is performed on the device as a result of a proper media or device connection.	URL Filtering/Web Reputation Mail Filtering								1
5			2	3		A	Connecting Unauthorized Media or Device	Connection of unauthorized media or device (CD/DVD, USB device, etc.) brought in from outside the organization with the device to execute an attack.	Restriction on Connecting Device and its Usage		(Same as on the Left)		(Same as on the Left) Log Collection/Log Analysis Integrated Log Management System				1
6			2	3		A	Execution of Unauthorized Processes	Unauthorized execution of legitimate programs, commands, services, and other processes found on the attack target device.	Permission Management Access Control Application Whitelisting Approval of Important Operations		(Same as on the Left) (Same as on the Left) (Same as on the Left) (Same as on the Left)		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System				1
7			1	3		B	Malware Infection	Infection or running of malware (unauthorized programs) on the attack target device.	Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System				1
8			3	3		A	Information Theft	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management Access Control Data Encryption DLP		(Same as on the Left) (Same as on the Left) (Same as on the Left) (Same as on the Left)		Log Collection/Log Analysis Integrated Log Management System				1
9			3	3		A	Unauthorized Modification of Information	Unauthorized modification of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management Access Control Data Signature		(Same as on the Left) (Same as on the Left) (Same as on the Left)		Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		1
10			3	3		A	Information Destruction	Destroying of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.			Permission Management Access Control		Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		1
11			3	3		A	Unauthorized Transmission	Sending unauthorized control commands (settings changes, power shutdowns, etc.) and unauthorized data to other devices.	Segmentation/Zoning Data Signature Approval of Important Operations		(Same as on the Left) (Same as on the Left) (Same as on the Left)		Log Collection/Log Analysis Integrated Log Management System				1
12			3	3		A	Outage	Stopping device functions.					Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy Failsafe Design	○ ○	1
13			3	3		A	DoS Attack	Interruption of regular device operations by sending processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.	DDoS Countermeasures				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy Failsafe Design	○ ○	1
14			3	2		A	Theft	Device theft.	Lock and Key Management	○	(Same as on the Left)		(Same as on the Left)				2
15			3	2		A	Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Tamper Resistance Obfuscation Zeroization	 ○	(Same as on the Left) (Same as on the Left) (Same as on the Left)						2
16							Route Blocking	Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Entrance and Exit Management Lock and Key management				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor		Redundancy		
17							Network Congestion	Causing congestion by generating the communications traffic that exceeds the capacity of the device.	FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy		
18	Not applicable (no functions)						Jamming	Interference with radio communications.					Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy		
19							Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels Data Encryption Exclusive Line								
20							Unauthorized Modification of Communication Data	Maliciously modifying information flowing on the network.	Encryption of Communications Channels Data Signature Exclusive Line				Log Collection/Log Analysis Integrated Log Management System				
21							Connecting Unauthorized Device	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage				Restriction on Connecting Device and its Usage Log Collection/Log Analysis Integrated Log Management System				

This page has intentionally been left blank.

3.3. Summary of Risk Values

[Task 3.3①] Preparing a summary chart of vulnerability levels.

- This allows better understanding and reviewing of the distribution of vulnerability levels in combinations of asset and threat types.

[Output 3.3①]

A summary chart of asset vulnerability levels is provided below (Table 3-7).

Table 3-7: Summary Chart of Vulnerability Levels for Asset-based Risk Analysis

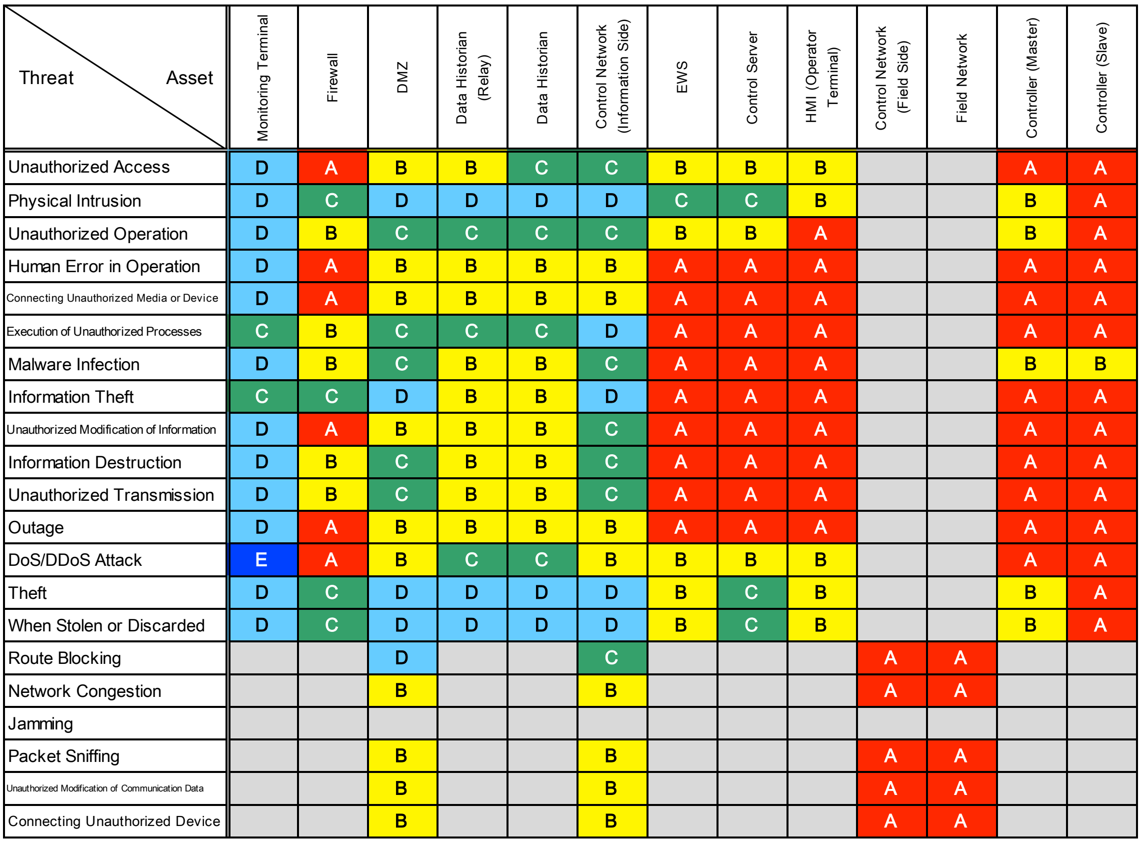
Threat Asset	Monitoring Terminal	Firewall	DMZ	Data Historian (Relay)	Data Historian	Control Network (Information Side)	EWS	Control Server	HMI (Operator Terminal)	Control Network (Field Side)	Field Network	Controller (Master)	Controller (Slave)
Unauthorized Access	2	2	2	2	2	2	2	2	2			3	3
Physical Intrusion	2	1	1	1	1	2	1	1	2			2	2
Unauthorized Operation	2	2	2	2	2	2	2	2	3			2	2
Human Error in Operation	2	3	3	3	3	3	3	3	3			3	3
Connecting Unauthorized Media or Device	2	3	3	3	3	3	3	3	3			3	3
Execution of Unauthorized Processes	3	2	2	2	2	2	3	2	3			3	3
Malware Infection	2	3	3	2	2	3	3	2	3			3	3
Information Theft	3	2	2	2	2	2	3	2	3			3	3
Unauthorized Modification of Information	3	2	2	2	2	2	3	2	3			3	3
Information Destruction	3	2	2	2	2	2	3	2	3			3	3
Unauthorized Transmission	3	3	3	3	3	3	3	3	3			3	3
Outage	3	3	3	3	3	3	3	3	3			3	3
DoS/DDoS Attack	3	3	3	3	3	3	3	3	3			3	3
Theft	2	2	2	2	2	2	2	2	2			2	2
When Stolen or Discarded	2	2	2	2	2	2	2	2	2			2	2
Route Blocking			1			2				2	2		
Network Congestion			3			3				3	3		
Jamming													
Packet Sniffing			3			3				3	3		
Unauthorized Modification of Communication Data			3			3				3	3		
Connecting Unauthorized Device			3			3				3	3		

[Task 3.3②] Preparing a summary chart of risk values.

[Output 3.3②]

A summary chart of risk values is provided below (Table 3-8).

Table 3-8: Summary Chart of Risk Values for Asset-based Risk Analysis



Threat Asset	Monitoring Terminal	Firewall	DMZ	Data Historian (Relay)	Data Historian	Control Network (Information Side)	EWS	Control Server	HMI (Operator Terminal)	Control Network (Field Side)	Field Network	Controller (Master)	Controller (Slave)
Unauthorized Access	D	A	B	B	C	C	B	B	B			A	A
Physical Intrusion	D	C	D	D	D	D	C	C	B			B	A
Unauthorized Operation	D	B	C	C	C	C	B	B	A			B	A
Human Error in Operation	D	A	B	B	B	B	A	A	A			A	A
Connecting Unauthorized Media or Device	D	A	B	B	B	B	A	A	A			A	A
Execution of Unauthorized Processes	C	B	C	C	C	D	A	A	A			A	A
Malware Infection	D	B	C	B	B	C	A	A	A			B	B
Information Theft	C	C	D	B	B	D	A	A	A			A	A
Unauthorized Modification of Information	D	A	B	B	B	C	A	A	A			A	A
Information Destruction	D	B	C	B	B	C	A	A	A			A	A
Unauthorized Transmission	D	B	C	B	B	C	A	A	A			A	A
Outage	D	A	B	B	B	B	A	A	A			A	A
DoS/DDoS Attack	E	A	B	C	C	B	B	B	B			A	A
Theft	D	C	D	D	D	D	B	C	B			B	A
When Stolen or Discarded	D	C	D	D	D	D	B	C	B			B	A
Route Blocking			D			C				A	A		
Network Congestion			B			B				A	A		
Jamming													
Packet Sniffing			B			B				A	A		
Unauthorized Modification of Communication Data			B			B				A	A		
Connecting Unauthorized Device			B			B				A	A		

4. Business Impact-based Risk Analysis

Business impact-based risk analysis involves using the following outputs prepared previously to conduct a risk analysis.

Table 4-1: Outputs for Preparations Used

Section In this Volume	Outputs for Preparations Used	Guide
2.1	List of Assets	*3.1.5. Table 3-9*
2.2	System Configuration Diagram	*3.2.3. Figure 3-8*
2.3.①	Dataflow Matrix	*3.3.1. Table 3-10*
2.3.②	Dataflow Chart	*3.3.2. Figure 3-14*
2.6	Evaluation Criteria for Business Impact Levels	*4.3.2. Table 4-11*
2.7	List Detailing Business Impacts and Business Impact Levels	*4.3.3. Table 4-12*
2.8	Evaluation Criteria for Threat Levels	*4.4.5. Table 4-20 to Table 4-24*

A list of outputs that is newly prepared as part of business impact-based risk analysis is shown below.

Table 4-2: Outputs Prepared in Business Impact-based Risk Analysis Work

Section In this Volume	Asset-based Output	Guide
4.1	List of Attack Scenarios	*6.2.2. Table 6-6*
4.2	List of Attack Routes	*6.5.1. Table 6-11 to Table 6-12*
4.3	Attack Route Diagram	*6.5.1. Figure 6-9*
4.4	Business Impact-based Risk Assessment Sheet	*6.6.4. to 6.11.*
4.5	Summary of Risk Values	*6.11.3.*

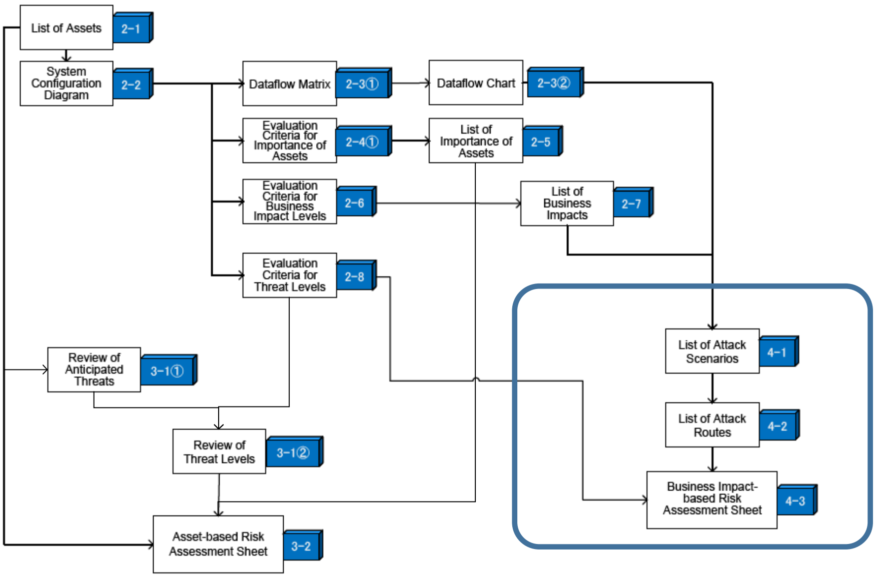

List of Assets
2-1
System Configuration Diagram
2-2
Dataflow Matrix
2-3①
Dataflow Chart
2-3②
Evaluation Criteria for Importance of Assets
2-4①
List of Importance of Assets
2-5
Evaluation Criteria for Business Impact Levels
2-6
List of Business Impacts
2-7
Evaluation Criteria for Threat Levels
2-8
Review of Anticipated Threats
3-1①
Review of Threat Levels
3-1②
Asset-based Risk Assessment Sheet
3-2
List of Attack Scenarios
4-1
List of Attack Routes
4-2
Business Impact-based Risk Assessment Sheet
4-3

Figure 4-1: Business Impact-based Risk Analysis Work Flow

4.1. Preparing a List of Attack Scenarios

In this section, specific attack scenarios are prepared, based on the "Table 2-8: List of Business Impacts" prepared in Section 2.7.

[Task 4.1①] Reviewing the cyber attack (attack scenario summary) acting as the cause of the business impact.
[Task 4.1②] Listing the attack targets for the attack scenario.
[Task 4.1③] Listing the attack execution assets for the attack scenario.

- It is necessary to include attack execution assets where data is flowing to attack targets, referring to the dataflow matrix provided in Section 2.3.

[Task 4.1④] Listing specific attack types for the attack scenario.

Table 4-3: Format of Attack Scenarios

<table>
<tr><th>#</th><th>Business Impact</th><th colspan="4">Summary of Business Impacts and Attack Scenarios</th><th>Business Impact Level</th></tr>
<tr><td rowspan="6">1</td><td rowspan="6">Wide Area Energy Supply Outage</td><td colspan="4">Improper use of legitimate supply outage functions caused by a cyber attack on supply facilities, which produces a wide area energy supply outage, resulting in significant social impacts and a dramatic loss of trust in the company.</td><td rowspan="6">3</td></tr>
<tr><td rowspan="5">1-1</td><td colspan="3">① A wide area supply outage caused by the use of wide area supply outage functions.</td></tr>
<tr><td>Attack Execution Asset</td><td>Attack Target</td><td>Final Attack</td></tr>
<tr><td>③ HMI</td><td>② Controller</td><td>④ Causes wide-area supply outage.</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

[Output 4.1]

A list of attack scenarios is provided below (Table 4-4). For information on notes *1 to *5 in the table, see over the page.

Table 4-4: List of Attack Scenarios

Item Number	Business Impact	Summary of Business Impacts and Attack Scenarios (*1)					Business Impact Level
1	Wide Area Fuel Supply Outage	Improper use of legitimate supply outage functions caused by a cyber attack on supply facilities, which produces a wide area fuel supply outage, resulting in significant social impacts and a dramatic loss of trust in the company.					3 (*2)
		Scenario #	Attack Scenario	Attack Execution Asset	Attack Target	Final Attack	
		1-1	A wide area supply outage caused by the use of wide area supply outage functions.	HMI	Controller	Causes wide-area supply outage.	
		1-2	A wide area supply outage caused by supply outage commands being sent to multiple controllers.	Controller (Master)	Controller (Slave)	Sends malicious control command to cause supply outage.	
2	Occurrence of fires and explosion incidents	Outbreak of fires and explosions due to control abnormalities and a loss of monitoring facilities for handling hazardous materials caused by a cyber attack on manufacturing facilities. Such attacks impact local residents and the environment, cause significant losses in compensation claims, and lead to a dramatic loss of trust in the company. (*3)					3
		Item Number	Attack Scenario	Attack Execution Asset	Attack Target	Final Attack	
		2-1	Outbreak of fires and explosions due to control abnormalities in facilities for handling hazardous materials caused by the setting of improper target values.	HMI	Controller	Sets incorrect target value for controller.	
				Control Server	Controller	Sets incorrect target value for controller.	
		2-2	Outbreak of fires and explosions due to control abnormalities in facilities for handling hazardous materials caused by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs.	EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.	
		2-3	Outbreak of fires and explosions due to erratic behavior in facilities for handling hazardous materials where the unauthorized modification of data and programs prevents a proper response, even when operations are performed correctly.	HMI	HMI	Tampers with and alters data/software in HMI.	
				Control Server	Control Server	Tampers with and alters data/software in control server.	
		2-4	Outbreak of fires and explosions caused by a loss of monitoring and monitoring control at facilities for handling hazardous materials due to congestion in the control network (field side).	Control Network (Field Side) Connected Device	Control Network (Field Side)	Maliciously modifies network settings and disables communications.	
						Infects with malware causing unauthorized communications, and disables communications.	
3	Supply of Defective Fuel	Manufacturing and supply of fuel that does not meet quality standards caused by a cyber attack on manufacturing facilities, causing significant inconvenience to customers, significant losses in compensation claims, and a dramatic loss of trust in the company.					2 (*4)
		Item Number	Attack Scenario	Attack Execution Asset	Attack Target	Final Attack	
		3-1	Production of fuel that does not meet quality standards due to control abnormalities in production facilities caused by the setting of improper target values.	HMI	Controller	Sets incorrect target value for controller.	
				Control Server	Controller	Sets incorrect target value for controller.	
		3-2	Production of fuel that does not meet quality standards due to control abnormalities in production facilities caused by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs.	EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.	
		3-3	Production of fuel that does not meet quality standards due to control abnormalities in production facilities caused by tampering with and altering data/software.	HMI	HMI	Tampers with and alters data/software in HMI.	
				Control Server	Control Server	Tampers with and alters data/software in control server.	
4	Manufacturing/ Production Disrupt/ Suspend	Manufacturing/production disrupt/suspend and damages due to forcibly terminated processes due to process control abnormalities and operation monitoring failures caused by a cyber attack on manufacturing facilities.					1 (*5)
		Item Number	Attack Scenario	Attack Execution Asset	Attack Target	Final Attack	
		4-1	Control abnormalities in production facilities caused by the setting of improper target values. This leads to processes being terminated for safety reasons.	HMI	Controller	Sets incorrect target value for controller.	
				Control Server	Controller	Sets incorrect target value for controller.	
		4-2	Control abnormalities in production facilities caused by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs. This leads to processes being terminated for safety reasons.	EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.	
		4-3	Operational abnormalities in production facilities caused by tampering with and altering data/software. This leads to processes being terminated for safety reasons.	HMI	HMI	Tampers with and alters data/software in HMI.	
				Control Server	Control Server	Tampers with and alters data/software in control server.	
		4-4	A destructive malware or ransomware infection that disables monitoring of production facilities and prevent monitoring control. This leads to processes being terminated for safety reasons.	HMI	HMI	Infects the system with destructive malware and ransomware, disabling monitoring operations.	
5	Leak of confidential information	A cyber attack on the control system, resulting in an external leak of company production secrets, impacting the company's competitive edge against other companies, and leading to a deterioration in competitive strength.					3
		Item Number	Attack Scenario	Attack Execution Asset	Attack Target	Final Attack	
		5-1	Theft of company production secrets stored on the control system, resulting in an external information leak.	EWS	EWS	Theft of confidential information stored on the EWS.	
				Control Server	Control Server	Theft of confidential information stored on the control server.	

*1: The facilities and operating functions described in these examples are used for demonstrative purposes only.

*2: While the business impact level is listed as “3” in these examples, this could be changed to “2”, or even “1” provided that the supply structure in place is such that the supply outage only persists for a set period of time before supply is restored, and that the supply outage can be resolved (supply can be resumed) before the customer is impacted.

*3: In the case of an actual explosion or fire, other factors besides the cyber attack may be involved.

*4: In these examples, even if products that do not meet quality standards/criteria are produced due to a cyber attack on the manufacturing process, the business impact level shall be set to “2” provided that widespread losses are averted by limiting damages to those sustained within the company by discarding affected lots, finding affected products during inspection processes, or issuing a recall/retrieving affected products that have been supplied.

*5: When processes are terminated for safety reasons due to a loss of monitoring (disabled monitoring control), in these examples the business impact level is set to “1”.

4.2. Preparing a List of Attack Routes

In this section, a list of attack routes is prepared, based on the list of attack scenarios prepared in 4.1.

[Task 4.2①] Listing the attack entry points for the attack execution asset “HMI” in attack scenario 1-1.

[Task 4.2②] Listing assets between the attack entry point and the attack execution asset. Providing details on the attack route from the attack entry point to the attack execution asset in the system configuration diagram.

- It is necessary to include assets along the attack path where data is flowing to the attack execution asset and the attack target, referring to the dataflow matrix provided in Section 2.3.

[Task 4.2③] Determining the attacker.

[Task 4.2④] Carrying out tasks ① to ③ for all attack scenarios.

Table 4-5: Format for a List of Attack Routes

Attack Scenario	Who	From Where	How			Attack Execution Asset	Attack Target	Final Attack
	Attacker	Attack Entry Point	Attack Path 1	Attack Path 2	Attack Path 3			
1-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	Controller	Causes wide-area supply outage.
1-1	Malicious Third Party	Information Network	FW			HMI	Controller	Causes wide-area supply outage.
1-1	Insider (Human Error)	HMI (Physical Intrusion)				HMI	Controller	Causes wide-area supply outage.
1-2	3	1			2	Controller (M)	Controller (S)	Sends malicious control command to cause supply outage.
1-2						Controller (M)	Controller (S)	Sends malicious control command to cause supply outage.
1-2						Controller (M)	Controller (S)	Sends malicious control command to cause supply outage.

This page has intentionally been left blank.

[Output 4.2]

The following shows both a list of attack routes compiled by scenario number (Table 4-6), and a list of attack routes compiled by attack entry point (Table 4-7).

Table 4-6: List of Attack Routes (Sorted by Scenario)

Attack Tree Number	Scenario Number	Who	From Where	How					
		Attacker	Attack Entry Point	Attack Path 1	Attack Path 2	Attack Path 3	Attack Execution Asset	Attack Target	Final Attack
1-1	1-1	Malicious Third Party	Information Network	FW			HMI	Controller	Causes wide-area supply outage.
1-2	1-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	Controller	Causes wide-area supply outage.
1-3	1-1	Insider (Human Error)	HMI (Physical Intrusion)				HMI	Controller	Causes wide-area supply outage.
1-4	1-2	Malicious Third Party	Information Network	FW	EWS		Controller (M)	Controller (S)	Sends malicious control command to cause supply outage.
1-5	1-2	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian	EWS	Controller (M)	Controller (S)	Sends malicious control command to cause supply outage.
1-6	1-2	Insider (Human Error)	EWS (Physical Intrusion)				Controller (M)	Controller (S)	Sends malicious control command to cause supply outage.
Tree #	Scenario #	Attacker	Attack Entry Point	Attack Path 1	Attack Path 2	Attack Path 3	Attack Execution Asset	Attack Target	Final Attack
2-1	2-1	Malicious Third Party	Information Network	FW			HMI	Controller	Sets incorrect target value for controller.
2-2	2-1	Malicious Third Party	Information Network	FW			Control Server	Controller	Sets incorrect target value for controller.
2-3	2-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	Controller	Sets incorrect target value for controller.
2-4	2-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		Control Server	Controller	Sets incorrect target value for controller.
2-5	2-1	Insider (Human Error)	HMI (Physical Intrusion)				HMI	Controller	Sets incorrect target value for controller.
2-6	2-1	Insider (Human Error)	Control Server (Physical Intrusion)				Control Server	Controller	Sets incorrect target value for controller.
2-7	2-2	Malicious Third Party	Information Network	FW			EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
2-8	2-2	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
2-9	2-2	Insider (Human Error)	EWS (Physical Intrusion)				EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
2-10	2-3	Malicious Third Party	Information Network	FW			HMI	HMI	Tampers with and alters data/software in HMI.
2-11	2-3	Malicious Third Party	Information Network	FW			Control Server	Control Server	Tampers with and alters data/software in control server.
2-12	2-3	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	HMI	Tampers with and alters data/software in HMI.
2-13	2-3	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		Control Server	Control Server	Tampers with and alters data/software in control server.
2-14	2-3	Insider (Human Error)	HMI (Physical Intrusion)				HMI	HMI	Tampers with and alters data/software in HMI.
2-15	2-3	Insider (Human Error)	Control Server (Physical Intrusion)				Control Server	Control Server	Tampers with and alters data/software in control server.
2-16	2-4	Malicious Third Party	Information Network	FW			HMI	Control Network (Field Side)	Maliciously modifies network settings and disables communications.
2-17	2-4	Malicious Third Party	Information Network	FW			HMI	Control Network (Field Side)	Infects with malware causing unauthorized communications, and disables communications.
2-18	2-4	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	Control Network (Field Side)	Maliciously modifies network settings and disables communications.
2-19	2-4	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	Control Network (Field Side)	Infects with malware causing unauthorized communications, and disables communications.
2-20	2-4	Insider (Human Error)	HMI (Physical Intrusion)				HMI	Control Network (Field Side)	Maliciously modifies network settings and disables communications.
2-21	2-4	Insider (Human Error)	HMI (Physical Intrusion)				HMI	Control Network (Field Side)	Infects with malware causing unauthorized communications, and disables communications.
2-22	2-4	Insider (Human Error)	EWS (Physical Intrusion)				EWS	Control Network (Field Side)	Maliciously modifies network settings and disables communications.
2-23	2-4	Insider (Human Error)	EWS (Physical Intrusion)				EWS	Control Network (Field Side)	Infects with malware causing unauthorized communications, and disables communications.
Tree #	Scenario #	Attacker	Attack Entry Point	Attack Path 1	Attack Path 2	Attack Path 3	Attack Execution Asset	Attack Target	Final Attack
3-1	3-1	Malicious Third Party	Information Network	FW			HMI	Controller	Sets incorrect target value for controller.
3-2	3-1	Malicious Third Party	Information Network	FW			Control Server	Controller	Sets incorrect target value for controller.
3-3	3-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	Controller	Sets incorrect target value for controller.
3-4	3-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		Control Server	Controller	Sets incorrect target value for controller.
3-5	3-1	Insider (Human Error)	HMI (Physical Intrusion)				HMI	Controller	Sets incorrect target value for controller.
3-6	3-1	Insider (Human Error)	Control Server (Physical Intrusion)				Control Server	Controller	Sets incorrect target value for controller.
3-7	3-2	Malicious Third Party	Information Network	FW			EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
3-8	3-2	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
3-9	3-2	Insider (Human Error)	EWS (Physical Intrusion)				EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
3-10	3-3	Malicious Third Party	Information Network	FW			HMI	HMI	Tampers with and alters data/software in HMI.
3-11	3-3	Malicious Third Party	Information Network	FW			Control Server	Control Server	Tampers with and alters data/software in control server.
3-12	3-3	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	HMI	Tampers with and alters data/software in HMI.
3-13	3-3	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		Control Server	Control Server	Tampers with and alters data/software in control server.
3-14	3-3	Insider (Human Error)	HMI (Physical Intrusion)				HMI	HMI	Tampers with and alters data/software in HMI.
3-15	3-3	Insider (Human Error)	Control Server (Physical Intrusion)				Control Server	Control Server	Tampers with and alters data/software in control server.
Tree #	Scenario #	Attacker	Attack Entry Point	Attack Path 1	Attack Path 2	Attack Path 3	Attack Execution Asset	Attack Target	Final Attack
4-1	4-1	Malicious Third Party	Information Network	FW			HMI	Controller	Sets incorrect target value for controller.
4-2	4-1	Malicious Third Party	Information Network	FW			Control Server	Controller	Sets incorrect target value for controller.
4-3	4-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	Controller	Sets incorrect target value for controller.
4-4	4-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		Control Server	Controller	Sets incorrect target value for controller.
4-5	4-1	Insider (Human Error)	HMI (Physical Intrusion)				HMI	Controller	Sets incorrect target value for controller.
4-6	4-1	Insider (Human Error)	Control Server (Physical Intrusion)				Control Server	Controller	Sets incorrect target value for controller.
4-7	4-2	Malicious Third Party	Information Network	FW			EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
4-8	4-2	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
4-9	4-2	Insider (Human Error)	EWS (Physical Intrusion)				EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
4-10	4-3	Malicious Third Party	Information Network	FW			HMI	HMI	Tampers with and alters data/software in HMI.
4-11	4-3	Malicious Third Party	Information Network	FW			Control Server	Control Server	Tampers with and alters data/software in control server.
4-12	4-3	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	HMI	Tampers with and alters data/software in HMI.
4-13	4-3	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		Control Server	Control Server	Tampers with and alters data/software in control server.
4-14	4-3	Insider (Human Error)	HMI (Physical Intrusion)				HMI	HMI	Tampers with and alters data/software in HMI.
4-15	4-3	Insider (Human Error)	Control Server (Physical Intrusion)				Control Server	Control Server	Tampers with and alters data/software in control server.
4-16	4-4	Malicious Third Party	Information Network	FW			HMI	HMI	Infects the system with destructive malware and ransomware, disabling monitoring operations.
4-17	4-4	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	HMI	Infects the system with destructive malware and ransomware, disabling monitoring operations.
4-18	4-4	Insider (Human Error)	HMI (Physical Intrusion)				HMI	HMI	Infects the system with destructive malware and ransomware, disabling monitoring operations.
4-19	4-4	Insider (Human Error)	EWS (Physical Intrusion)				HMI	HMI	Infects the system with destructive malware and ransomware, disabling monitoring operations.
Tree #	Scenario #	Attacker	Attack Entry Point	Attack Path 1	Attack Path 2	Attack Path 3	Attack Execution Asset	Attack Target	Final Attack
5-1	5-1	Malicious Third Party	Information Network	FW			Control Server	Control Server	Theft of confidential information stored on the control server.
5-2	5-1	Malicious Third Party	Information Network	FW			EWS	EWS	Theft of confidential information stored on the EWS.
5-3	5-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		Control Server	Control Server	Theft of confidential information stored on the control server.
5-4	5-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		EWS	EWS	Theft of confidential information stored on the EWS.

Table 4-7: List of Attack Routes (Sorted by Attack Entry Point)

Attack Tree Number	Scenario Number	Who	From Where	How					
		Attacker	Attack Entry Point	Attack Path 1	Attack Path 2	Attack Path 3	Attack Execution Asset	Attack Target	Final Attack
1-1	2-3	Malicious Third Party	Information Network	FW			HMI	HMI	Tampers with and alters data/software in HMI.
1-2	3-3	Malicious Third Party	Information Network	FW			HMI	HMI	Tampers with and alters data/software in HMI.
1-3	4-3	Malicious Third Party	Information Network	FW			HMI	HMI	Tampers with and alters data/software in HMI.
1-4	4-4	Malicious Third Party	Information Network	FW			HMI	HMI	Infects the system with destructive malware and ransomware, disabling monitoring operations.
1-5	1-1	Malicious Third Party	Information Network	FW			HMI	Controller	Causes wide-area supply outage.
1-6	2-1	Malicious Third Party	Information Network	FW			HMI	Controller	Sets incorrect target value for controller.
1-7	3-1	Malicious Third Party	Information Network	FW			HMI	Controller	Sets incorrect target value for controller.
1-8	4-1	Malicious Third Party	Information Network	FW			HMI	Controller	Sets incorrect target value for controller.
1-9	2-4	Malicious Third Party	Information Network	FW			HMI	Control Network (Field Side)	Maliciously modifies network settings and disables communications.
1-10	2-4	Malicious Third Party	Information Network	FW			HMI	Control Network (Field Side)	Infects with malware causing unauthorized communications, and disables communications.
1-11	2-3	Malicious Third Party	Information Network	FW			Control Server	Control Server	Tampers with and alters data/software in control server.
1-12	3-3	Malicious Third Party	Information Network	FW			Control Server	Control Server	Tampers with and alters data/software in control server.
1-13	4-3	Malicious Third Party	Information Network	FW			Control Server	Control Server	Tampers with and alters data/software in control server.
1-14	5-1	Malicious Third Party	Information Network	FW			Control Server	Control Server	Theft of confidential information stored on the control server.
1-15	2-1	Malicious Third Party	Information Network	FW			Control Server	Controller	Sets incorrect target value for controller.
1-16	3-1	Malicious Third Party	Information Network	FW			Control Server	Controller	Sets incorrect target value for controller.
1-17	4-1	Malicious Third Party	Information Network	FW			Control Server	Controller	Sets incorrect target value for controller.
1-18	5-1	Malicious Third Party	Information Network	FW			EWS	EWS	Theft of confidential information stored on the EWS.
1-19	2-2	Malicious Third Party	Information Network	FW			EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
1-20	3-2	Malicious Third Party	Information Network	FW			EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
1-21	4-2	Malicious Third Party	Information Network	FW			EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
1-22	1-2	Malicious Third Party	Information Network	FW	EWS		Controller (M)	Controller (S)	Sends malicious control command to cause supply outage.
Tree #	Scenario #	Attacker	Attack Entry Point	Attack Path 1	Attack Path 2	Attack Path 3	Attack Execution Asset	Attack Target	Final Attack
2-1	2-3	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	HMI	Tampers with and alters data/software in HMI.
2-2	3-3	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	HMI	Tampers with and alters data/software in HMI.
2-3	4-3	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	HMI	Tampers with and alters data/software in HMI.
2-4	4-4	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	HMI	Infects the system with destructive malware and ransomware, disabling monitoring operations.
2-5	1-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	Controller	Causes wide-area supply outage.
2-6	2-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	Controller	Sets incorrect target value for controller.
2-7	3-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	Controller	Sets incorrect target value for controller.
2-8	4-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	Controller	Sets incorrect target value for controller.
2-9	2-4	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	Control Network (Field Side)	Maliciously modifies network settings and disables communications.
2-10	2-4	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	Control Network (Field Side)	Infects with malware causing unauthorized communications, and disables communications.
2-11	2-3	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		Control Server	Control Server	Tampers with and alters data/software in control server.
2-12	3-3	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		Control Server	Control Server	Tampers with and alters data/software in control server.
2-13	4-3	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		Control Server	Control Server	Tampers with and alters data/software in control server.
2-14	5-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		Control Server	Control Server	Theft of confidential information stored on the control server.
2-15	2-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		Control Server	Controller	Sets incorrect target value for controller.
2-16	3-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		Control Server	Controller	Sets incorrect target value for controller.
2-17	4-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		Control Server	Controller	Sets incorrect target value for controller.
2-18	5-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		EWS	EWS	Theft of confidential information stored on the EWS.
2-19	2-2	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
2-20	3-2	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
2-21	4-2	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
2-22	1-2	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian	EWS	Controller (M)	Controller (S)	Sends malicious control command to cause supply outage.
Tree #	Scenario #	Attacker	Attack Entry Point	Attack Path 1	Attack Path 2	Attack Path 3	Attack Execution Asset	Attack Target	Final Attack
3-1	2-3	Insider (Human Error)	HMI (Physical Intrusion)				HMI	HMI	Tampers with and alters data/software in HMI.
3-2	3-3	Insider (Human Error)	HMI (Physical Intrusion)				HMI	HMI	Tampers with and alters data/software in HMI.
3-3	4-3	Insider (Human Error)	HMI (Physical Intrusion)				HMI	HMI	Tampers with and alters data/software in HMI.
3-4	4-4	Insider (Human Error)	HMI (Physical Intrusion)				HMI	HMI	Infects the system with destructive malware and ransomware, disabling monitoring operations.
3-5	1-1	Insider (Human Error)	HMI (Physical Intrusion)				HMI	Controller	Causes wide-area supply outage.
3-6	2-1	Insider (Human Error)	HMI (Physical Intrusion)				HMI	Controller	Sets incorrect target value for controller.
3-7	3-1	Insider (Human Error)	HMI (Physical Intrusion)				HMI	Controller	Sets incorrect target value for controller.
3-8	4-1	Insider (Human Error)	HMI (Physical Intrusion)				HMI	Controller	Sets incorrect target value for controller.
3-9	2-4	Insider (Human Error)	HMI (Physical Intrusion)				HMI	Control Network (Field Side)	Maliciously modifies network settings and disables communications.
3-10	2-4	Insider (Human Error)	HMI (Physical Intrusion)				HMI	Control Network (Field Side)	Infects with malware causing unauthorized communications, and disables communications.
3-11	2-3	Insider (Human Error)	Control Server (Physical Intrusion)				Control Server	Control Server	Tampers with and alters data/software in control server.
3-12	3-3	Insider (Human Error)	Control Server (Physical Intrusion)				Control Server	Control Server	Tampers with and alters data/software in control server.
3-13	4-3	Insider (Human Error)	Control Server (Physical Intrusion)				Control Server	Control Server	Tampers with and alters data/software in control server.
3-15	2-1	Insider (Human Error)	Control Server (Physical Intrusion)				Control Server	Controller	Sets incorrect target value for controller.
3-16	3-1	Insider (Human Error)	Control Server (Physical Intrusion)				Control Server	Controller	Sets incorrect target value for controller.
3-17	4-1	Insider (Human Error)	Control Server (Physical Intrusion)				Control Server	Controller	Sets incorrect target value for controller.
3-18	4-4	Insider (Human Error)	EWS (Physical Intrusion)				HMI	HMI	Infects the system with destructive malware and ransomware, disabling monitoring operations.
3-20	2-2	Insider (Human Error)	EWS (Physical Intrusion)				EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
3-21	3-2	Insider (Human Error)	EWS (Physical Intrusion)				EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
3-22	4-2	Insider (Human Error)	EWS (Physical Intrusion)				EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
3-23	2-4	Insider (Human Error)	EWS (Physical Intrusion)				EWS	Control Network (Field Side)	Maliciously modifies network settings and disables communications.
3-24	2-4	Insider (Human Error)	EWS (Physical Intrusion)				EWS	Control Network (Field Side)	Infects with malware causing unauthorized communications, and disables communications.
3-25	1-2	Insider (Human Error)	EWS (Physical Intrusion)				Controller (M)	Controller (S)	Sends malicious control command to cause supply outage.

An attack route diagram detailing the attack route from the attack entry point to the attack execution asset in the system configuration diagram is provided below.

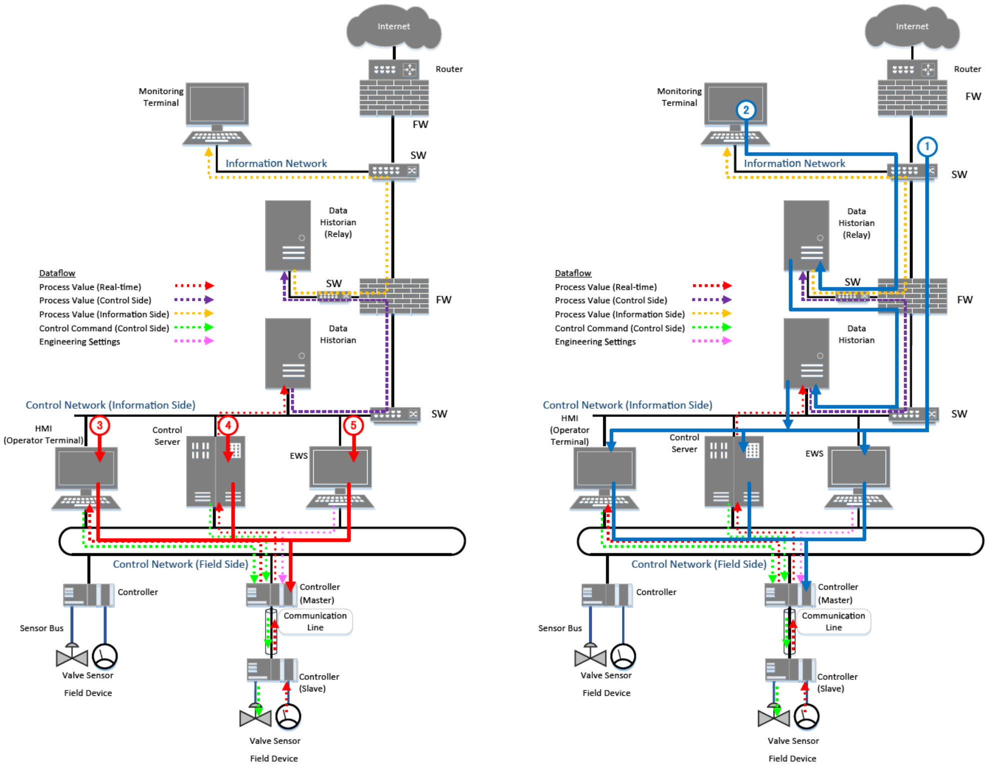


Figure 4-2: Attack Route Diagram

4.3. Preparing a Risk Assessment Sheet

The procedure described in "*Chapter 6* Business Impact-based Risk Analysis" in the Guide is performed to conduct a business impact-based risk analysis of the system to be analyzed. Detailed instructions are shown in the Guide. This section only provides a general overview of the procedure.

[Task 4.3①] Preparing an attack tree, and filling out in the assessment sheet based on "Section 4.2 Table 4-6: List of Attack Routes".

- ➢ An attack tree is prepared, referring to "*Clause 6.6.2* Filling out the Attack Tree" in the Guide.

[Task 4.3②] Reviewing the threat level of the attack tree, and filling out in the assessment sheet.

- ➢ The method used to evaluate the threat level in the attack tree is determined, referring to "*Section 6.8* Evaluating the Threat Level" in the Guide.
- ➢ Determining the threat level for each individual attack tree, referring to "Table 2-10: Evaluation Criteria for Threat Levels".

[Task 4.3③] Filling out the business impact level for the attack tree in the assessment sheet.

- ➢ Filling out the business impact level of attack scenarios in the assessment sheet, referring to the definition in "Table 4-4: List of Attack Scenarios".

[Task 4.3④] Investigating the effectiveness of security measures implemented for attacks anticipated in each step of the attack tree, and filling out the effectiveness of security measures in the assessment sheet.

- ➢ The effectiveness of security measures is filled out in the assessment sheet, referring to "*Section 6.9* Filling out the Effectiveness of Security Measures" in the Guide.

[Task 4.3⑤] Evaluating the security level/vulnerability level in the attack tree, and then filling out in the assessment sheet.

- ➢ The security level and vulnerability level in the attack tree is assessed, and then filled out in the assessment sheet, referring to "*Section 6.10* Evaluating and Filling out the Security Level/Vulnerability Level" in the Guide.

[Task 4.3⑥] Evaluating the risk values in the attack tree, and then filling out in the assessment sheet.

- ➢ Risk values are evaluated, referring to "*Section 6.11* Evaluating the Risk Values" in the Guide.

[Output 4.3]

The business impact risk assessment sheet is shown as "Table 4-8: Business Impact-based Risk Assessment Sheet (Sorted by Scenario)" from page 71 onwards. The two different ways to summarize an assessment sheet (three types of assessment sheets in total) are shown in Table 4-9 and Table 4-10 as references.

[Explanation 4.3]

- Characteristics of the three assessment sheet formats (entry examples)

  The Table 4-8: Business Impact-based Risk Assessment Sheet (Sorted by Scenario) sorts and organizes attack trees based on the Table 4-6: List of Attack Routes.This sheet summarizes attack trees corresponding to attack scenarios for each business impact item, with attack trees sorted by attack entry point. This sorting method facilitates comparisons with attack scenarios, and presents attack trees in an easy-to-understand manner in the early stages of analysis. However, one drawback with this method is that it increases the number of attack steps to be included in the sheet (increasing redundancy).

  Alternatively, the Table 4-9: Business Impact-based Risk Assessment Sheet (Sorted by Attack Entry Point) arranges attack trees starting from the attack entry point, and is the sorting method used with the ATA (Attack Tree Analysis) approach.Due to the difficulties in organizing attack trees without an overall view of the circumstances at hand, this method of organization is unsuitable for the early stages of analysis. However, one advantage of this method is the ease at which you can verify common attack steps that require strengthening when evaluating analysis results. In addition, this method minimizes the number of attack steps that need to be included in the sheet.

  Further, the Table 4-10: Business Impact-based Risk Assessment Sheet (Hybrid Version) offers a compromise approach to the two methods described above.This sheet compiles several business impact items and organizes attack trees for each, with attack trees sorted by attack entry point. Another approach is to categorize attack trees by business impact/business impact item, using this method to organize them, starting analysis with high priority business impacts/business impact items.

- Control system safety features and alarms (*)

  Assessment sheet entry examples do not account for control system safety features and alarms in the Countermeasures column. For example, for scenarios #1-1 and #1-2 in Table 4-8, even if a cyber attack attempts to cause a supply outage, alarms and other control system features may immediately recognize the attack and allow supply to be restored before a business impact occurs.When performing a risk analysis on the control system used by the business, it is recommended to alter the vulnerability level ratings in line with control system safety features, alarms, and operational recovery, etc.

  * Alarm: Refers to control system alarms, system alerts, events. This does not refer to information security warning events.

This page has intentionally been left blank.

Table 4-8: Business Impact-based Risk Assessment Sheet (Sorted by Scenario)

1. Wide Area Product Supply Outage

Item Number	Attack Scenario		Assessment Metrics				Countermeasures				Security Level		Attack Tree Number	
		Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Protection		Detection/ Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
							Intrusion/ Spreading Phase	Objective Achievement Phase						
	1-1	A wide area supply outage caused by the use of wide area supply outage functions.												
1		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes “execution of unauthorized processes” (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the “execution of unauthorized processes”.					FW ○ Peer-to-Peer Authentication ○ Applying Patches ○ Avoidance of Vulnerability *Permission Management* ○	(Same as on the left)	IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*		2 *1			
2		Unauthorized access of the HMI via the FW by a malicious third party. * Unauthorized access includes “execution of unauthorized processes”.					Peer-to-Peer Authentication ○ Applying Patches Avoidance of Vulnerability *Permission Management*		IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*		2			
3	1-1	Supply outage encompassing a wide area caused by a malicious third party using wide area supply outage functions on the controller from the HMI.	2	2	3	B	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#1-1	1,2,3
4		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes “execution of unauthorized processes” (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the “execution of unauthorized processes”.					Peer-to-Peer Authentication ○ Applying Patches ○ Avoidance of Vulnerability *Permission Management* ○	(Same as on the left)	IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*		2 *1			
5		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes “execution of unauthorized processes”.					Peer-to-Peer Authentication ○ Applying Patches Avoidance of Vulnerability *Permission Management* ○		IPS/IDS Log Collection/Log Analysi Integrated Log Management System *Device Alive Monitoring*		2			
6		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes “execution of unauthorized processes”.					Peer-to-Peer Authentication ○ Applying Patches Avoidance of Vulnerability *Permission Management*		IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*		2			
7	1-1	Supply outage encompassing a wide area caused by a malicious third party using wide area supply outage functions on the controller from the HMI.	2	2	3	B	Same as item number 3				1	2	#1-2	4,5,6,7
8		Attack Entry Point = HMI Due to human error by an insider, the HMI is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at “connecting to unauthorized media”.					Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		1 *2			
9	1-1	Supply outage encompassing a wide area caused by malware triggering wide area supply outage functions from the HMI.	2	3	3	A	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	1	#1-3	8,9
	1-2	A wide area supply outage caused by supply outage commands being sent to multiple controllers.												
10		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes “execution of unauthorized processes” (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the “execution of unauthorized processes”.					Same as item number 1				2 *1			
11		Unauthorized access of the EWS via the FW by a malicious third party. * Unauthorized access includes “execution of unauthorized processes” (privilege escalation).					Peer-to-Peer Authentication ○ Applying Patches *Permission Management* *Application Whitelisting*	(Same as on the left) (Same as on the left)	IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*		1			
12		Tampering with and altering data/software in controller (M) from the EWS by a malicious third party.					Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1			
13	1-2	Issuing of commands to stop the controller (S) via the controller (M) by a malicious third party. Supply outage encompassing a wide area.	2	2	3	B	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#1-4	10,11,12,13
14		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes “execution of unauthorized processes” (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the “execution of unauthorized processes”.					Same as item number 4				2 *1			
15		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes “execution of unauthorized processes”.					Same as item number 5				2			
16		Unauthorized access of the EWS from the data historian by a malicious third party. * Unauthorized access includes “execution of unauthorized processes”.					Peer-to-Peer Authentication ○ Applying Patches *Permission Management* *Application Whitelisting*	(Same as on the left) (Same as on the left)	IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*		2			
17		Tampering with and altering data/software in controller (M) from the EWS by a malicious third party.					Same as item number 12				1			
18	1-2	Issuing of commands to stop the controller (S) via the controller (M) by a malicious third party. Supply outage encompassing a wide area.	2	2	3	B	Same as item number 13				1	2	#1-5	14,15,16,17,18
19		Attack Entry Point = EWS Due to human error by an insider, the EWS is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at “connecting to unauthorized media”.					Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		1 *2			
20		Tampering with and altering data/software in controller (M) from the EWS by malware infection.					Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1			
21	1-2	Issuing of commands to stop the controller (S) via the controller (M) by malware infection. Supply outage encompassing a wide area.	2	3	3	A	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	1	#1-6	19,20,21
X														

[Note]

*1 It is recommended to refer to “Section 9.4 Firewall Settings” in the Guide for evaluating countermeasures.

*2 It is recommended to refer to “Section 9.5 Security Measures for External Storage Media” in the Guide for evaluating countermeasures.

Table 4-8: Business Impact-based Risk Assessment Sheet (Sorted by Scenario)

2. Occurrence of Fires and Explosion Incidents

Item Number	Attack Scenario		Assessment Metrics				Countermeasures				Security Level		Attack Tree Number	
							Protection							
		Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Intrusion/ Spreading Phase	Objective Achievement Phase	Detection/ Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
	2-1	Outbreak of fires and explosions due to control abnormalities in facilities for handling hazardous materials caused by the setting of improper target values.												
22		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 1				2 *1			
23		Unauthorized access of the HMI via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 2				2			
24	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the HMI by a malicious third party.	2	2	3	B	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#2-1	22,23,24
25		Unauthorized access of the control server via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Peer-to-Peer Authentication ○ Applying Patches *Permission Management* ○ *Application Whitelisting* ○	 (Same as on the left) (Same as on the left)	IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*		2			
26	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the control server by a malicious third party.	2	2	3	B	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#2-2	22,25,26
27		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 4				2 *1			
28		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 5				2			
29		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 6				2			
30	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the HMI by a malicious third party.	2	2	3	B	Same as item number 24				1	2	#2-3	27,28,29,30
31		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Peer-to-Peer Authentication ○ Applying Patches Avoidance of Vulnerability *Permission Management* ○		IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*		2			
32	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the control server by a malicious third party.	2	2	3	B	Same as item number 26				1	2	#2-4	27,28,31,32
33		Attack Entry Point = HMI Due to human error by an insider, the HMI is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 8				1 *2			
34	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the HMI by a malware infection.	2	3	3	A	Same as item number 24				1	1	#2-5	33,34
35		Attack Entry Point = Control Server Due to human error by an insider, the control server is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Anti-virus Application Whitelisting ○ Applying Patches Avoidance of Vulnerability Data Signature		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		2 *2			
36	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the control server by a malware infection.	2	2	3	B	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#2-6	35,36
	2-2	Outbreak of fires and explosions due to control abnormalities in facilities for handling hazardous materials caused by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs.												
37		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 1				2 *1			
38		Unauthorized access of the EWS via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Same as item number 11				1			
39	2-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	3	B	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	2	#2-7	37,38,39
40		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 4				2 *1			
41		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 5				2			
42		Unauthorized access of the EWS from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 16				2			
43	2-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	3	B	Same as item number 39				1	2	#2-8	40,41,42,43
44		Attack Entry Point = EWS Due to human error by an insider, the EWS is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 19				1 *2			
45	2-2	A malware infection maliciously modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	3	3	A	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	1	#2-9	44,45

Table 4-8: Business Impact-based Risk Assessment Sheet (Sorted by Scenario)

2. Occurrence of Fires and Explosion Incidents

Item Number	Attack Scenario		Assessment Metrics				Countermeasures				Security Level		Attack Tree Number	
		Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Protection: Intrusion/ Spreading Phase	Protection: Objective Achievement Phase	Detection/ Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
	2-1	Outbreak of fires and explosions due to control abnormalities in facilities for handling hazardous materials caused by the setting of improper target values.												
	2-3	Outbreak of fires and explosions due to erratic behavior in facilities for handling hazardous materials where the unauthorized modification of data and programs prevents a proper response, even when operations are performed correctly.												
46		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 1				2 *1			
47		Unauthorized access of the HMI via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 2				2			
48	2-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	3	B	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	2	#2-10	46,47,48
49		Unauthorized access of the control server via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Same as item number 25				2			
50	2-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	3	B	Permission Management ○ Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	2	2	#2-11	46,49,50
51		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 4				2 *1			
52		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 28				2			
53		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 6				2			
54	2-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	3	B	Same as item number 48				1	2	#2-12	51,52,53,54
55		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 31				2			
56	2-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	3	B	Same as item number 50				1	2	#2-13	51,52,55,56
57		Attack Entry Point = HMI Due to human error by an insider, the HMI is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 8				1 *2			
58	2-3	Tampering with and altering data/software in the HMI by malware infection.	2	3	3	A	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	1	#2-14	57,58
59		Attack Entry Point = Control Server Due to human error by an insider, the control server is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 35				2 *2			
60	2-3	Tampering with and altering data/software in the control server by malware infection.	2	2	3	B	Permission Management ○ Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	2	2	#2-15	59,60
	2-4	Outbreak of fires and explosions caused by a loss of monitoring and monitoring control at facilities for handling hazardous materials due to congestion in the control network (field side).												
61		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 1				2 *1			
62		Unauthorized access of the HMI via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 2				2			
63	2-4	Tampering with and altering the control network (field side) settings from the HMI to cause network congestion in the control network by a malicious third party. This prevents the monitoring of the control system.	2	2	3	B	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	2	#2-16	61,62,63
64	2-4	Infection of the HMI with malware by a malicious third party to cause unauthorized communication with the control network (field side) and prevent control network communications. This prevents the monitoring of the control system.	2	2	3	B	Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		1	2	#2-17	61,62,64
65		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 4				2 *1			
66		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 5				2			
67		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 6				2			
68	2-4	Tampering with and altering the control network (field side) settings from the HMI to cause network congestion in the control network by a malicious third party. This prevents the monitoring of the control system.	2	2	3	B	Same as item number 63				1	2	#2-18	65,66,67,68
69	2-4	Infection of the HMI with malware by a malicious third party to cause unauthorized communication with the control network (field side) and prevent control network communications. This prevents the monitoring of the control system.	2	2	3	B	Same as item number 64				1	2	#2-19	65,66,67,69
70		Attack Entry Point = HMI Due to human error by an insider, the HMI is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 8				1 *2			
71	2-4	Tampering with and altering the control network (field side) settings from the HMI to cause network congestion in the control network by malware infection. This prevents the monitoring of the control system.	2	3	3	A	Same as item number 63				1	1	#2-20	70,71
72	2-4	Malware infection causing unauthorized communication with the control network (field side), and preventing control network communications. This prevents the monitoring of the control system.	2	3	3	A	Same as item number 64				1	1	#2-21	70,72
73		Attack Entry Point = EWS Due to human error by an insider, the EWS is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 19				1 *2			
74	2-4	Tampering with and altering the control network (field side) settings from the EWS to cause network congestion in the control network by malware infection. This prevents the monitoring of the control system.	2	3	3	A	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	1	#2-22	73,74
75	2-4	Malware infection causing unauthorized communication with the control network (field side), and preventing control network communications. This prevents the monitoring of the control system.	2	3	3	A	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	1	#2-23	73,75
X														

[Note]
*1 It is recommended to refer to "Section 9.4 Firewall Settings" in the Guide for evaluating countermeasures.
*2 It is recommended to refer to "Section 9.5 Security Measures for External Storage Media" in the Guide for evaluating countermeasures.

Table 4-8: Business Impact-based Risk Assessment Sheet (Sorted by Scenario)

3. Supply of Defective Product

Item Number	Attack Scenario	Attack Tree/Attack Steps	Assessment Metrics: Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Countermeasures: Protection: Intrusion/ Spreading Phase	Protection: Objective Achievement Phase	Detection/ Understanding Damage	Business Continuity	Security Level: Attack Steps	Attack Tree	Attack Tree Number: Attack Tree Number	Configuration Steps (Item Number)
	3-1	Production of a product that does not meet quality standards/criteria due to control abnormalities in production facilities caused by the setting of improper target values.												
76		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 1				2 *1			
77		Unauthorized access of the HMI via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 2				2			
78	3-1	Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the HMI by a malicious third party.	2	2	2	C	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#3-1	76,77,78
79		Unauthorized access of the control server via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Same as item number 25				2			
80	3-1	Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the control server by a malicious third party.	2	2	2	C	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#3-2	76,79,80
81		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 4				2 *1			
82		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 5				2			
83		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 6				2			
84	3-1	Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the HMI by a malicious third party.	2	2	2	C	Same as item number 78				1	2	#3-3	81,82,83,84
85		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 31				2			
86	3-1	Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the control server by a malicious third party.	2	2	2	C	Same as item number 80				1	2	#3-4	81,82,85,86
87		Attack Entry Point = HMI Due to human error by an insider, the HMI is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 8				1 *2			
88	3-1	Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the HMI by a malware infection.	2	3	2	B	Same as item number 78				1	1	#3-5	87,88
89		Attack Entry Point = Control Server Due to human error by an insider, the control server is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 35				2 *2			
90	3-1	Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the control server by a malware infection.	2	2	2	C	Same as item number 80				1	2	#3-6	89,90
	3-2	Production of a product that does not meet quality standards/criteria due to control abnormalities in production facilities caused by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs.												
91		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 1				2 *1			
92		Unauthorized access of the EWS via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Same as item number 11				1			
93	3-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	2	C	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	2	#3-7	91,92,93
94		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 4				2 *1			
95		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 5				2			
96		Unauthorized access of the EWS from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 16				2			
97	3-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	2	C	Same as item number 93				1	2	#3-8	94,95,96,97
98		Attack Entry Point = EWS Due to human error by an insider, the EWS is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 19				1 *2			
99	3-2	A malware infection maliciously modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	3	2	B	Same as item number 93				1	1	#3-9	98,99

Table 4-8: Business Impact-based Risk Assessment Sheet (Sorted by Scenario)

3. Supply of Defective Product

Item Number	Attack Scenario		Assessment Metrics				Countermeasures				Security Level		Attack Tree Number	
		Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Protection		Detection/ Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
							Intrusion/ Spreading Phase	Objective Achievement Phase						
	3-1	Production of a product that does not meet quality standards/criteria due to control abnormalities in production facilities caused by the setting of improper target values.												
	3-3	Production of a product that does not meet quality standards/criteria due to control abnormalities in production facilities caused by tampering with and altering data/software.												
100		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 1				2 *1			
101		Unauthorized access of the HMI via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 2				2			
102	3-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	2	C	Same as item number 48				1	2	#3-10	100,101,102
103		Unauthorized access of the control server via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Same as item number 25				2			
104	3-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	2	C	Same as item number 50				2	2	#3-11	100,103,104
105		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 4				2 *1			
106		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 5				2			
107		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 6				2			
108	3-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	2	C	Same as item number 48				1	2	#3-12	105,106,107,108
109		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 31				2			
110	3-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	2	C	Same as item number 50				1	2	#3-13	105,106,109,110
111		Attack Entry Point = HMI Due to human error by an insider, the HMI is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 8				1 *2			
112	3-3	Tampering with and altering data/software in the HMI by malware infection.	2	3	2	B	Same as item number 58				1	1	#3-14	111,112
113		Attack Entry Point = Control Server Due to human error by an insider, the control server is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 35				3 *2			
114	3-3	Tampering with and altering data/software in the control server by malware infection.	2	2	2	C	Same as item number 60				2	2	#3-15	113,114
X														

[Note]

*1 It is recommended to refer to "Section 9.4 Firewall Settings" in the Guide for evaluating countermeasures.

*2 It is recommended to refer to "Section 9.5 Security Measures for External Storage Media" in the Guide for evaluating countermeasures.

Table 4-8: Business Impact-based Risk Assessment Sheet (Sorted by Scenario)

4. Manufacturing/Production Disrupt/Suspend

Item Number	Attack Scenario		Assessment Metrics				Countermeasures				Security Level		Attack Tree Number	
							Protection		Detection/ Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
		Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Intrusion/ Spreading Phase	Objective Achievement Phase						
	4-1	Control abnormalities in production facilities caused by the setting of improper target values. This leads to processes being terminated for safety reasons.												
117		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 1				2 *1			
118		Unauthorized access of the HMI via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 2				2			
119	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the HMI by a malicious third party.	2	2	1	D	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#4-1	117,118,119
120	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the control server by a malicious third party.	2	2	1	D	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#4-2	117,118,120
121		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 4				2 *1			
122		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 5				2			
123		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 6				2			
124	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the HMI by a malicious third party.	2	2	1	D	Same as item number 119				1	2	#4-3	121,122,123,124
125		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 31				2			
126	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the control server by a malicious third party.	2	2	1	D	Same as item number 120				1	2	#4-4	121,122,125,126
127		Attack Entry Point = HMI Due to human error by an insider, the HMI is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 8				1 *2			
128	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the HMI by a malware infection.	2	3	1	D	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	1	#4-5	127,128
129		Attack Entry Point = Control Server Due to human error by an insider, the control server is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 35				2 *2			
130	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the control server by a malware infection.	2	2	1	D	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#4-6	129,130
	4-2	Control abnormalities in production facilities caused by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs. This leads to processes being terminated for safety reasons.												
131		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 1				2 *1			
132		Unauthorized access of the EWS via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Same as item number 11				1			
133	4-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	1	D	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	2	#4-7	131,132,133
134		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 4				2 *1			
135		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 5				2			
136		Unauthorized access of the EWS from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 16				2			
137	4-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	1	D	Same as item number 133				1	2	#4-8	134,135,136,137
138		Attack Entry Point = EWS Due to human error by an insider, the EWS is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 19				1 *2			
139	4-2	A malware infection maliciously modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	3	1	D	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	1	#4-9	138,139

Table 4-8: Business Impact-based Risk Assessment Sheet (Sorted by Scenario)

4. Manufacturing/Production Disrupt/Suspend

Item Number	Attack Scenario		Assessment Metrics				Countermeasures				Security Level		Attack Tree Number	
		Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Protection		Detection/ Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
							Intrusion/ Spreading Phase	Objective Achievement Phase						
	4-1	Control abnormalities in production facilities caused by the setting of improper target values. This leads to processes being terminated for safety reasons.												
	4-3	Operational abnormalities in production facilities caused by tampering with and altering data/software. This leads to processes being terminated for safety reasons.												
140		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 1				2 *1			
141		Unauthorized access of the HMI via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 2				2			
142	4-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	1	D	Same as item number 48				1	2	#4-10	140,141,142
143		Unauthorized access of the control server via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Same as item number 25				2			
144	4-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	1	D	Same as item number 50				2	2	#4-11	140,143,144
145		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 4				2 *1			
146		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 5				2			
147		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 6				2			
148	4-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	1	D	Same as item number 48				1	2	#4-12	145,146,147,148
149		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 31				2			
150	4-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	1	D	Same as item number 50				1	2	#4-13	145,146,149,150
151		Attack Entry Point = HMI Due to human error by an insider, the HMI is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 8				1 *2			
152	4-3	Tampering with and altering data/software in the HMI by malware infection.	2	3	1	D	Same as item number 58				1	1	#4-14	151,152
153		Attack Entry Point = Control Server Due to human error by an insider, the control server is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 35				3 *2			
154	4-3	Tampering with and altering data/software in the control server by malware infection.	2	2	1	D	Same as item number 60				1	2	#4-15	152,154
	4-4	A destructive malware or ransomware infection that disables monitoring of production facilities and prevent monitoring control. This leads to processes being terminated for safety reasons.												
155		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 1				2 *1			
156		Unauthorized access of the HMI via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 2				2			
157	4-4	Infection of the HMI with destructive malware (ransomware, etc.) by a malicious third party. This prevents the monitoring of the control system.	2	2	1	D	Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature	*Permission Management* *Access Control*	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	*Data Backup*	1	2	#4-16	155,156,157
158		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 4				2 *1			
159		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 5				2			
160		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 6				2			
161	4-4	Infection of the HMI with destructive malware (ransomware, etc.) by a malicious third party. This prevents the monitoring of the control system.	2	2	1	D	Same as item number 157				1	2	#4-17	158,159,160,161
162		Attack Entry Point = HMI Due to human error by an insider, the HMI is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 8				1 *2			
163	4-4	Data destroyed by destructive malware (ransomware, etc.). This prevents the monitoring of the control system.	2	3	1	D	Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature	*Permission Management* *Access Control*	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	*Data Backup*	1	1	#4-18	162,163
164		Attack Entry Point = EWS Due to human error by an insider, the EWS is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 19				1 *2			
165	4-4	Malware infection of the HMI. Data destroyed by destructive malware (ransomware, etc.). This prevents the monitoring of the control system.	2	3	1	D	Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature	*Permission Management* *Access Control*	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	*Data Backup*	1	1	#4-19	164,165
X														

[Note]

***1** It is recommended to refer to "Section 9.4 Firewall Settings" in the Guide for evaluating countermeasures.

***2** It is recommended to refer to "Section 9.5 Security Measures for External Storage Media" in the Guide for evaluating countermeasures.

Table 4-8: Business Impact-based Risk Assessment Sheet (Sorted by Scenario)

5. Leak of Confidential Information

Item Number	Attack Scenario		Assessment Metrics				Countermeasures				Security Level		Attack Tree Number	
							Protection		Detection/ Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
		Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Intrusion/ Spreading Phase	Objective Achievement Phase						
	5-1	Theft of company production secrets stored on the control system, resulting in an external information leak.												
166		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes “execution of unauthorized processes” (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the “execution of unauthorized processes”.					Same as item number 1				2 *1			
167		Unauthorized access of the control server via the FW by a malicious third party. * Unauthorized access includes “execution of unauthorized processes” (privilege escalation).					Same as item number 25				2			
168	5-1	Theft of data on the control server by a malicious third party. (Data then retrieved by following the reverse route.)	2	2	3	B	Permission Management ○ Access Control Data Encryption DLP	(Same as on the left) (Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		2	2	#5-1	166,167,168
169		Unauthorized access of the EWS via the FW by a malicious third party. * Unauthorized access includes “execution of unauthorized processes” (privilege escalation).					Same as item number 11				1			
170	5-1	Theft of data on the EWS by a malicious third party. (Data then retrieved by following the reverse route.)	2	2	3	B	Permission Management Access Control Data Encryption DLP	(Same as on the left) (Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#5-2	166,169,170
171		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes “execution of unauthorized processes” (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the “execution of unauthorized processes”.					Same as item number 4				2 *1			
172		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes “execution of unauthorized processes”.					Same as item number 5				2			
173		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes “execution of unauthorized processes”.					Same as item number 31				2			
174	5-1	Theft of data on the control server by a malicious third party. (Data then retrieved by following the reverse route.)	2	2	3	B	Same as item number 168				1	2	#5-3	171,172,173,174
175		Unauthorized access of the EWS from the data historian by a malicious third party. * Unauthorized access includes “execution of unauthorized processes”.					Same as item number 16				1			
176	5-1	Theft of data on the EWS by a malicious third party. (Data then retrieved by following the reverse route.)	2	2	3	B	Same as item number 170				1	2	#5-4	171,172,175,176
X														

[Note]

*1 It is recommended to refer to “Section 9.4 Firewall Settings” in the Guide for evaluating countermeasures.

*2 It is recommended to refer to “Section 9.5 Security Measures for External Storage Media” in the Guide for evaluating countermeasures.

Table 4-9: Business Impact-based Risk Assessment Sheet (Sorted by Attack Entry Point)

1. Wide Area Product Supply Outage, 2. Occurrence of Fires and Explosion Incidents, 3. Supply of Defective Products, 4. Manufacturing/Production Disrupt/Suspend, 5. Leak of Confidential Information

Item Number	Attack Scenario		Assessment Metrics				Countermeasures								Security Level		Attack Tree Number	
		Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Protection				Detection/ Understanding Damage		Business Continuity		Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
							Intrusion/ Spreading Phase		Objective Achievement Phase									
	1-1	1-1: A wide area supply outage caused by the use of wide area supply outage functions.																
	1-2	1-2: A wide area supply outage caused by supply outage commands being sent to multiple controllers.																
	2-1	2-1: Outbreak of fires and explosions due to control abnormalities in facilities for handling hazardous materials caused by the setting of improper target values.																
	2-2	2-2: Outbreak of fires and explosions due to control abnormalities in facilities for handling hazardous materials caused by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs.																
	2-3	2-3: Outbreak of fires and explosions due to erratic behavior in facilities for handling hazardous materials where the unauthorized modification of data and programs prevents a proper response, even when operations are performed correctly.																
	2-4	2-4: Outbreak of fires and explosions caused by a loss of monitoring and monitoring control at facilities for handling hazardous materials due to congestion in the control network (field side).																
	3-1	3-1: Production of a product that does not meet quality standards/criteria due to control abnormalities in production facilities caused by the setting of improper target values.																
	3-2	3-2: Production of a product that does not meet quality standards/criteria due to control abnormalities in production facilities caused by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs.																
	3-3	3-3: Production of a product that does not meet quality standards/criteria due to control abnormalities in production facilities caused by tampering with and altering data/software.																
	4-1	4-1: Control abnormalities in production facilities caused by the setting of improper target values. This leads to processes being terminated for safety reasons.																
	4-2	4-2: Control abnormalities in production facilities caused by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs. This leads to processes being terminated for safety reasons.																
	4-3	4-3: Operational abnormalities in production facilities caused by tampering with and altering data/software. This leads to processes being terminated for safety reasons.																
	4-4	4-4: A destructive malware or ransomware infection that disables monitoring of production facilities and prevent monitoring control. This leads to processes being terminated for safety reasons.																
	5-1	5-1: Theft of company production secrets stored on the control system, resulting in an external information leak.																
1		**Attack Entry Point = Information Network** Unauthorized firewall access by a malicious third party. * Unauthorized access includes “execution of unauthorized processes” (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the “execution of unauthorized processes”.					FW Peer-to-Peer Authentication Applying Patches Avoidance of Vulnerability *Permission Management*	○ ○ ○ ○	 (Same as on the left)		IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*				2 *1			
2		Unauthorized access of the HMI via the FW by a malicious third party. * Unauthorized access includes “execution of unauthorized processes”.					Peer-to-Peer Authentication Applying Patches Avoidance of Vulnerability *Permission Management*	○			IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*				2			
3	2-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	3	B	Permission Management Access Control Data Signature		(Same as on the left) (Same as on the left) (Same as on the left)		Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		1	2	#1-1	1,2,3
4	3-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	2	C	Same as item number 3								1	2	#1-2	1,2,4
5	4-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	1	D	Same as item number 3								1	2	#1-3	1,2,5
6	4-4	Infection of the HMI with destructive malware (ransomware, etc.) by a malicious third party. This prevents the monitoring of the control system.	2	2	1	D	Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature		*Permission Management* *Access Control*		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		*Data Backup*		1	2	#1-4	1,2,6
7	1-1	Supply outage encompassing a wide area caused by a malicious third party using wide area supply outage functions on the controller from the HMI.	2	2	3	B	Segmentation/Zoning Data Signature Approval of Important Operations		(Same as on the left) (Same as on the left) (Same as on the left)		Log Collection/Log Analysis Integrated Log Management System				1	2	#1-5	1,2,7
8	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the HMI by a malicious third party.	2	2	3	B	Segmentation/Zoning Data Signature Approval of Important Operations		(Same as on the left) (Same as on the left) (Same as on the left)		Log Collection/Log Analysis Integrated Log Management System				1	2	#1-6	1,2,8
9	3-1	Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the HMI by a malicious third party.	2	2	2	C	Same as item number 8								1	2	#1-7	1,2,9
10	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the HMI by a malicious third party.	2	2	1	D	Same as item number 8								1	2	#1-8	1,2,10
11	2-4	Tampering with and altering the control network (field side) settings from the HMI to cause network congestion in the control network by a malicious third party. This prevents the monitoring of the control system.	2	2	3	B	Permission Management Access Control Data Signature		(Same as on the left) (Same as on the left) (Same as on the left)		Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		1	2	#1-9	1,2,11
12	2-4	Infection of the HMI with malware by a malicious third party to cause unauthorized communication with the control network (field side) and prevent control network communications. This prevents the monitoring of the control system.	2	2	3	B	Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System				1	2	#1-10	1,2,12
13		Unauthorized access of the control server via the FW by a malicious third party. * Unauthorized access includes “execution of unauthorized processes” (privilege escalation).					Peer-to-Peer Authentication Applying Patches *Permission Management* *Application Whitelisting*	○ ○	 (Same as on the left) (Same as on the left)		IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*				2			
14	2-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	3	B	Permission Management Access Control Data Signature	○	(Same as on the left) (Same as on the left) (Same as on the left)		Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		2	2	#1-11	1,13,14
15	3-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	2	C	Same as item number 14								2	2	#1-12	1,13,15
16	4-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	1	D	Same as item number 14								2	2	#1-13	1,13,16
17	5-1	Theft of data on the control server by a malicious third party. (Data then retrieved by following the reverse route.)	2	2	3	B	Permission Management Access Control Data Encryption DLP		(Same as on the left) (Same as on the left) (Same as on the left) (Same as on the left)		Log Collection/Log Analysis Integrated Log Management System				1	2	#1-14	1,13,17
18	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the control server by a malicious third party.	2	2	3	B	Segmentation/Zoning Data Signature Approval of Important Operations		(Same as on the left) (Same as on the left) (Same as on the left)		Log Collection/Log Analysis Integrated Log Management System				1	2	#1-15	1,13,18
19	3-1	Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the control server by a malicious third party.	2	2	2	C	Same as item number 18								1	2	#1-16	1,13,19
20	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the control server by a malicious third party.	2	2	1	D	Same as item number 18								1	2	#1-17	1,13,20
21		Unauthorized access of the EWS via the FW by a malicious third party. * Unauthorized access includes “execution of unauthorized processes” (privilege escalation).					Peer-to-Peer Authentication Applying Patches *Permission Management* *Application Whitelisting*	○	 (Same as on the left) (Same as on the left)		IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*				1			
22	5-1	Theft of data on the EWS by a malicious third party. (Data then retrieved by following the reverse route.)	2	2	3	B	Permission Management Access Control Data Encryption DLP		(Same as on the left) (Same as on the left) (Same as on the left) (Same as on the left)		Log Collection/Log Analysis Integrated Log Management System				1	2	#1-18	1,21,22
23	2-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	3	B	Permission Management Access Control Data Signature		(Same as on the left) (Same as on the left) (Same as on the left)		Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		1	2	#1-19	1,21,23
24	3-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	2	C	Same as item number 23								1	2	#1-20	1,21,24
25	4-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	1	D	Same as item number 23								1	2	#1-21	1,21,25
26		Tampering with and altering data/software in controller (M) from the EWS by a malicious third party.					Permission Management Access Control Data Signature		(Same as on the left) (Same as on the left) (Same as on the left)		Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		1			
27	1-2	Issuing of commands to stop the controller (S) via the controller (M) by a malicious third party. Supply outage encompassing a wide area.	2	2	3	B	Segmentation/Zoning Data Signature Approval of Important Operations		(Same as on the left) (Same as on the left) (Same as on the left)		Log Collection/Log Analysis Integrated Log Management System				1	2	#1-22	1,21,26,27
X																		

[Note]
*1 It is recommended to refer to “Section 9.4 Firewall Settings” in the Guide for evaluating countermeasures.

Table 4-9: Business Impact-based Risk Assessment Sheet (Sorted by Attack Entry Point)

1. Wide Area Product Supply Outage, 2. Occurrence of Fires and Explosion Incidents, 3. Supply of Defective Products, 4. Manufacturing/Production Disrupt/Suspend, 5. Leak of Confidential Information

Item Number	Attack Scenario		Assessment Metrics				Countermeasures								Security Level		Attack Tree Number	
							Protection				Detection/ Understanding Damage		Business Continuity					
		Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Intrusion/ Spreading Phase		Objective Achievement Phase						Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
	1-1	1-1: A wide area supply outage caused by the use of wide area supply outage functions.																
	1-2	1-2: A wide area supply outage caused by supply outage commands being sent to multiple controllers.																
	2-1	2-1: Outbreak of fires and explosions due to control abnormalities in facilities for handling hazardous materials caused by the setting of improper target values.																
	2-2	2-2: Outbreak of fires and explosions due to control abnormalities in facilities for handling hazardous materials caused by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs.																
	2-3	2-3: Outbreak of fires and explosions due to erratic behavior in facilities for handling hazardous materials where the unauthorized modification of data and programs prevents a proper response, even when operations are performed correctly.																
	2-4	2-4: Outbreak of fires and explosions caused by a loss of monitoring and monitoring control at facilities for handling hazardous materials due to congestion in the control network (field side).																
	3-1	3-1: Production of a product that does not meet quality standards/criteria due to control abnormalities in production facilities caused by the setting of improper target values.																
	3-2	3-2: Production of a product that does not meet quality standards/criteria due to control abnormalities in production facilities caused by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs.																
	3-3	3-3: Production of a product that does not meet quality standards/criteria due to control abnormalities in production facilities caused by tampering with and altering data/software.																
	4-1	4-1: Control abnormalities in production facilities caused by the setting of improper target values. This leads to processes being terminated for safety reasons.																
	4-2	4-2: Control abnormalities in production facilities caused by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs. This leads to processes being terminated for safety reasons.																
	4-3	4-3: Operational abnormalities in production facilities caused by tampering with and altering data/software. This leads to processes being terminated for safety reasons.																
	4-4	4-4: A destructive malware or ransomware infection that disables monitoring of production facilities and prevent monitoring control. This leads to processes being terminated for safety reasons.																
	5-1	5-1: Theft of company production secrets stored on the control system, resulting in an external information leak.																
28		**Attack Entry Point = Monitoring Terminal** Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Peer-to-Peer Authentication Applying Patches Avoidance of Vulnerability *Permission Management*	○ ○ ○	 (Same as on the left)		IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*				2 *1			
29		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Peer-to-Peer Authentication Applying Patches Avoidance of Vulnerability *Permission Management*	○ ○			IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*				2			
30		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Peer-to-Peer Authentication Applying Patches Avoidance of Vulnerability *Permission Management*	○			IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*				2			
31	2-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	3	B	Same as item number 3								1	2	#2-1	28,29,30,31
32	3-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	2	C	Same as item number 3								1	2	#2-2	28,29,30,32
33	4-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	1	D	Same as item number 3								1	2	#2-3	28,29,30,33
34	4-4	Infection of the HMI with destructive malware (ransomware, etc.) by a malicious third party. This prevents the monitoring of the control system.	2	2	1	D	Same as item number 6								1	2	#2-4	28,29,30,34
35	1-1	Supply outage encompassing a wide area caused by a malicious third party using wide area supply outage functions on the controller from the HMI.	2	2	3	B	Same as item number 7								1	2	#2-5	28,29,30,35
36	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the HMI by a malicious third party.	2	2	3	B	Same as item number 8								1	2	#2-6	28,29,30,36
37	3-1	Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the HMI by a malicious third party.	2	2	2	C	Same as item number 8								1	2	#2-7	28,29,30,37
38	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the HMI by a malicious third party.	2	2	1	D	Same as item number 8								1	2	#2-8	28,29,30,38
39	2-4	Tampering with and altering the control network (field side) settings from the HMI to cause network congestion in the control network by a malicious third party. This prevents the monitoring of the control system.	2	2	3	B	Same as item number 11								1	2	#2-9	28,29,30,39
40	2-4	Infection of the HMI with malware by a malicious third party to cause unauthorized communication with the control network (field side) and prevent control network communications. This prevents the monitoring of the control system.	2	2	3	B	Same as item number 12								1	2	#2-10	28,29,30,40
41		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Peer-to-Peer Authentication Applying Patches Avoidance of Vulnerability *Permission Management*	○			IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*				1			
42	2-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	3	B	Same as item number 14								1	2	#2-11	28,29,41,42
43	3-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	2	C	Same as item number 14								1	2	#2-12	28,29,41,43
44	4-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	1	D	Same as item number 14								1	2	#2-13	28,29,41,44
45	5-1	Theft of data on the control server by a malicious third party. (Data then retrieved by following the reverse route.)	2	2	3	B	Same as item number 17								1	2	#2-14	28,29,41,45
46	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the control server by a malicious third party.	2	2	3	B	Same as item number 18								1	2	#2-15	28,29,41,46
47	3-1	Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the control server by a malicious third party.	2	2	2	C	Same as item number 18								1	2	#2-16	28,29,41,47
48	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the control server by a malicious third party.	2	2	1	D	Same as item number 18								1	2	#2-17	28,29,41,48
49		Unauthorized access of the EWS from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 21								2			
50	5-1	Theft of data on the EWS by a malicious third party. (Data then retrieved by following the reverse route.)	2	2	3	B	Same as item number 22								1	2	#2-18	28,29,49,50
51	2-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	3	B	Same as item number 23								1	2	#2-19	28,29,49,51
52	3-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	2	C	Same as item number 23								1	2	#2-20	28,29,49,52
53	4-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	1	D	Same as item number 23								1	2	#2-21	28,29,49,53
54		Tampering with and altering data/software in controller (M) from the EWS by a malicious third party.					Same as item number 26								1			
55	1-2	Issuing of commands to stop the controller (S) via the controller (M) by a malicious third party. Supply outage encompassing a wide area.	2	2	3	B	Same as item number 27								1	2	#2-22	28,29,49,54,55
X																		

[Note]
*1 It is recommended to refer to "Section 9.4 Firewall Settings" in the Guide for evaluating countermeasures.

Table 4-9: Business Impact-based Risk Assessment Sheet (Sorted by Attack Entry Point)

1. Wide Area Product Supply Outage, 2. Occurrence of Fires and Explosion Incidents, 3. Supply of Defective Products, 4. Manufacturing/Production Disrupt/Suspend, 5. Leak of Confidential Information

Item Number	Attack Scenario		Assessment Metrics				Countermeasures								Security Level		Attack Tree Number	
		Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Protection				Detection/ Understanding Damage		Business Continuity		Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
							Intrusion/ Spreading Phase		Objective Achievement Phase									
	1-1	1-1: A wide area supply outage caused by the use of wide area supply outage functions.																
	1-2	1-2: A wide area supply outage caused by supply outage commands being sent to multiple controllers.																
	2-1	2-1: Outbreak of fires and explosions due to control abnormalities in facilities for handling hazardous materials caused by the setting of improper target values.																
	2-2	2-2: Outbreak of fires and explosions due to control abnormalities in facilities for handling hazardous materials caused by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs.																
	2-3	2-3: Outbreak of fires and explosions due to erratic behavior in facilities for handling hazardous materials where the unauthorized modification of data and programs prevents a proper response, even when operations are performed correctly.																
	2-4	2-4: Outbreak of fires and explosions caused by a loss of monitoring and monitoring control at facilities for handling hazardous materials due to congestion in the control network (field side).																
	3-1	3-1: Production of a product that does not meet quality standards/criteria due to control abnormalities in production facilities caused by the setting of improper target values.																
	3-2	3-2: Production of a product that does not meet quality standards/criteria due to control abnormalities in production facilities caused by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs.																
	3-3	3-3: Production of a product that does not meet quality standards/criteria due to control abnormalities in production facilities caused by tampering with and altering data/software.																
	4-1	4-1: Control abnormalities in production facilities caused by the setting of improper target values. This leads to processes being terminated for safety reasons.																
	4-2	4-2: Control abnormalities in production facilities caused by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs. This leads to processes being terminated for safety reasons.																
	4-3	4-3: Operational abnormalities in production facilities caused by tampering with and altering data/software. This leads to processes being terminated for safety reasons.																
	4-4	4-4: A destructive malware or ransomware infection that disables monitoring of production facilities and prevent monitoring control. This leads to processes being terminated for safety reasons.																
	5-1	5-1: Theft of company production secrets stored on the control system, resulting in an external information leak.																
56		Attack Entry Point = HMI Due to human error by an insider, the HMI is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at “connecting to unauthorized media”.					Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System				1 *2			
57	2-3	Tampering with and altering data/software in the HMI by malware infection.	2	3	3	A	Same as item number 3								1	1	#3-1	56,57
58	3-3	Tampering with and altering data/software in the HMI by malware infection.	2	3	2	B	Same as item number 3								1	1	#3-2	56,58
59	4-3	Tampering with and altering data/software in the HMI by malware infection.	2	3	1	D	Same as item number 3								1	1	#3-3	56,59
60	4-4	Data destroyed by destructive malware (ransomware, etc.). This prevents the monitoring of the control system.	2	3	1	D	Same as item number 6								1	1	#3-4	56,60
61	1-1	Supply outage encompassing a wide area caused by malware triggering wide area supply outage functions from the HMI.	2	3	3	A	Same as item number 7								1	1	#3-5	56,61
62	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the HMI by a malware infection.	2	3	3	A	Same as item number 7								1	1	#3-6	56,62
63	3-1	Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the HMI by a malware infection.	2	3	2	B	Same as item number 7								1	1	#3-7	56,63
64	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the HMI by a malware infection.	2	3	1	D	Same as item number 7								1	1	#3-8	56,64
65	2-4	Tampering with and altering the control network (field side) settings from the HMI to cause network congestion in the control network by malware infection. This prevents the monitoring of the control system.	2	3	3	A	Same as item number 11								1	1	#3-9	56,65
66	2-4	Malware infection causing unauthorized communication with the control network (field side), and preventing control network communications. This prevents the monitoring of the control system.	2	3	3	A	Same as item number 12								1	1	#3-10	56,66
67		Attack Entry Point = Control Server Due to human error by an insider, the control server is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at “connecting to unauthorized media”.					Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature	 ○ 			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System				2 *2			
68	2-3	Tampering with and altering data/software in the control server by malware infection.	2	2	3	B	Same as item number 14								1	2	#3-11	67,68
69	3-3	Tampering with and altering data/software in the control server by malware infection.	2	2	2	C	Same as item number 14								1	2	#3-12	67,69
70	4-3	Tampering with and altering data/software in the control server by malware infection.	2	2	1	D	Same as item number 14								1	2	#3-13	67,70
71	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the control server by a malware infection.	2	2	3	B	Same as item number 18								1	2	#3-14	67,71
72	3-1	Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the control server by a malware infection.	2	2	2	C	Same as item number 18								1	2	#3-15	67,72
73	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the control server by a malware infection.	2	2	1	D	Same as item number 18								1	2	#3-16	67,73
74		Attack Entry Point=EWS Due to human error by an insider, the EWS is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it assumes that there is no threat of a deliberate attempt to “connect to unauthorized media”.					Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature				Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System				1 *2			
75	4-4	Malware infection of the HMI. Data destroyed by destructive malware (ransomware, etc.). This prevents the monitoring of the control system.	2	3	1	D	Same as item number 6								1	1	#3-17	74,75
76	2-2	A malware infection maliciously modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	3	3	A	Same as item number 23								1	1	#3-18	74,76
77	3-2	A malware infection maliciously modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	3	2	B	Same as item number 23								1	1	#3-19	74,77
78	4-2	A malware infection maliciously modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	3	1	D	Same as item number 23								1	1	#3-20	74,78
79	2-4	Tampering with and altering the control network (field side) settings from the EWS to cause network congestion in the control network by malware infection. This prevents the monitoring of the control system.	2	3	3	A	Permission Management Access Control Data Signature		(Same as on the left) (Same as on the left) (Same as on the left)		Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		1	1	#3-21	74,79
80	2-4	Malware infection causing unauthorized communication with the control network (field side), and preventing control network communications. This prevents the monitoring of the control system.	2	3	3	A	Permission Management Access Control Data Signature		(Same as on the left) (Same as on the left) (Same as on the left)		Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		1	1	#3-22	74,80
81		Tampering with and altering data/software in controller (M) from the EWS by malware infection.					Same as item number 26								1			
82	1-2	Issuing of commands to stop the controller (S) via the controller (M) by malware infection. Supply outage encompassing a wide area.	2	3	3	A	Same as item number 27								1	1	#3-23	74,81,82
X																		

[Note]
*1 It is recommended to refer to “Section 9.4 Firewall Settings” in the Guide for evaluating countermeasures.
*2 It is recommended to refer to “Section 9.5 Security Measures for External Storage Media” in the Guide for evaluating

Table 4-10: Business Impact-based Risk Assessment Sheet (Hybrid Version)

1. Wide Area Product Supply Outage

Item Number	Attack Scenario		Assessment Metrics				Countermeasures				Security Level		Attack Tree Number	
		Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Protection: Intrusion/ Spreading Phase	Protection: Objective Achievement Phase	Detection/ Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
	1-1 1-2	1-1: A wide area supply outage caused by the use of wide area supply outage functions. 1-2: A wide area supply outage caused by supply outage commands being sent to multiple controllers.												
1		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes “execution of unauthorized processes” (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the “execution of unauthorized processes”.					FW ○ Peer-to-Peer Authentication ○ Applying Patches ○ Avoidance of Vulnerability *Permission Management* ○	 (Same as on the left)	IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*		2 *1			
2		Unauthorized access of the HMI via the FW by a malicious third party. * Unauthorized access includes “execution of unauthorized processes”.					Peer-to-Peer Authentication ○ Applying Patches Avoidance of Vulnerability *Permission Management*		IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*		2			
3	1-1	Supply outage encompassing a wide area caused by a malicious third party using wide area supply outage functions on the controller from the HMI.	2	2	3	B	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#1-1	1,2,3
4		Unauthorized access of the EWS via the FW by a malicious third party. * Unauthorized access includes “execution of unauthorized processes” (privilege escalation).					Peer-to-Peer Authentication ○ Applying Patches *Permission Management* *Application Whitelisting*	 (Same as on the left) (Same as on the left)	IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*		2			
5		Tampering with and altering data/software in controller (M) from the EWS by a malicious third party.					Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1			
6	1-2	Issuing of commands to stop the controller (S) via the controller (M) by a malicious third party. Supply outage encompassing a wide area.	2	2	3	B	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#1-2	1,4,5,6
7		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes “execution of unauthorized processes” (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the “execution of unauthorized processes”.					Peer-to-Peer Authentication ○ Applying Patches ○ Avoidance of Vulnerability *Permission Management* ○	 (Same as on the left)	IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*		2 *1			
8		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes “execution of unauthorized processes”.					Peer-to-Peer Authentication ○ Applying Patches Avoidance of Vulnerability *Permission Management* ○		IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*		2			
9		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes “execution of unauthorized processes”.					Peer-to-Peer Authentication ○ Applying Patches Avoidance of Vulnerability *Permission Management*		IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*		2			
10	1-1	Supply outage encompassing a wide area caused by a malicious third party using wide area supply outage functions on the controller from the HMI.	2	2	3	B	Same as item number 3				1	2	#1-3	7,8,9,10
11		Unauthorized access of the EWS from the data historian by a malicious third party. * Unauthorized access includes “execution of unauthorized processes”.					Peer-to-Peer Authentication ○ Applying Patches *Permission Management* *Application Whitelisting*	 (Same as on the left) (Same as on the left)	IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*		2			
12		Tampering with and altering data/software in controller (M) from the EWS by a malicious third party.					Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1			
13	1-2	Issuing of commands to stop the controller (S) via the controller (M) by a malicious third party. Supply outage encompassing a wide area.	2	2	3	B	Same as item number 6				1	2	#1-4	7,8,11,12,13
14		Attack Entry Point = HMI Due to human error by an insider, the HMI is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at “connecting to unauthorized media”.					Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		1 *2			
15	1-1	Supply outage encompassing a wide area caused by malware triggering wide area supply outage functions from the HMI.	2	3	3	A	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	1	#1-5	14,15
16		Attack Entry Point = EWS Due to human error by an insider, the EWS is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at “connecting to unauthorized media”.					Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		1 *2			
17		Tampering with and altering data/software in controller (M) from the EWS by malware infection.					Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1			
18	1-2	Issuing of commands to stop the controller (S) via the controller (M) by malware infection. Supply outage encompassing a wide area.	2	3	3	A	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	1	#1-6	16,17,18
X														

[Note]

*1 It is recommended to refer to “Section 9.4 Firewall Settings” in the Guide for evaluating countermeasures.

*2 It is recommended to refer to “Section 9 Security Measures for External Storage Media” in the Guide for evaluating countermeasures.

Table 4-10: Business Impact-based Risk Assessment Sheet (Hybrid Version)

2. Occurrence of Fires and Explosion Incidents

Item Number	Attack Scenario		Assessment Metrics				Countermeasures				Security Level		Attack Tree Number	
		Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Protection		Detection/ Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
							Intrusion/ Spreading Phase	Objective Achievement Phase						
	2-1 2-2 2-3 2-4	2-1: Outbreak of fires and explosions due to control abnormalities in facilities for handling hazardous materials caused by the setting of improper target values. 2-2: Outbreak of fires and explosions due to control abnormalities in facilities for handling hazardous materials caused by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs. 2-3: Outbreak of fires and explosions due to erratic behavior in facilities for handling hazardous materials where the unauthorized modification of data and programs prevents a proper response, even when operations are performed correctly. 2-4: Outbreak of fires and explosions caused by a loss of monitoring and monitoring control at facilities for handling hazardous materials due to congestion in the control network (field side).												
19		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 1				2 *1			
20		Unauthorized access of the HMI via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 2				2			
21	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the HMI by a malicious third party.	2	2	3	B	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#2-1	19,20,21
22	2-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	3	B	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	2	#2-2	19,20,22
23	2-4	Tampering with and altering the control network (field side) settings from the HMI to cause network congestion in the control network by a malicious third party. This prevents the monitoring of the control system.	2	2	3	B	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	2	#2-3	19,20,23
24	2-4	Infection of the HMI with malware by a malicious third party to cause unauthorized communication with the control network (field side) and prevent control network communications. This prevents the monitoring of the control system.	2	2	3	B	Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		1	2	#2-4	19,20,24
25		Unauthorized access of the control server via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Peer-to-Peer Authentication ○ Applying Patches *Permission Management* ○ *Application Whitelisting* ○	(Same as on the left) (Same as on the left)	IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*		2			
26	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the control server by a malicious third party.	2	2	3	B	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#2-5	19,25,26
27	2-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	3	B	Permission Management ○ Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	2	2	#2-6	19,25,27
28		Unauthorized access of the EWS via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Same as item number 4				2			
29	2-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	3	B	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	2	#2-7	19,28,29
30		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 7				2 *1			
31		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 8				2			
32		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 9				2			
33	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the HMI by a malicious third party.	2	2	3	B	Same as item number 21				1	2	#2-8	30,31,32,33
34	2-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	3	B	Same as item number 22				1	2	#2-9	30,31,32,34
35	2-4	Tampering with and altering the control network (field side) settings from the HMI to cause network congestion in the control network by a malicious third party. This prevents the monitoring of the control system.	2	2	3	B	Same as item number 23				1	2	#2-10	30,31,32,35
36	2-4	Infection of the HMI with malware by a malicious third party to cause unauthorized communication with the control network (field side) and prevent control network communications. This prevents the monitoring of the control system.	2	2	3	B	Same as item number 24				1	2	#2-11	30,31,32,36
37		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Peer-to-Peer Authentication ○ Applying Patches Avoidance of Vulnerability *Permission Management* ○		IPS/IDS Log Collection/Log Analysis Integrated Log Management System *Device Alive Monitoring*		2			
38	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the control server by a malicious third party.	2	2	3	B	Same as item number 26				1	2	#2-12	30,31,37,38
39	2-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	3	B	Same as item number 27				1	2	#2-13	30,31,37,39
40		Unauthorized access of the EWS from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 11				2			
41	2-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	3	B	Same as item number 29				1	2	#2-14	30,31,40,41

Table 4-10: Business Impact-based Risk Assessment Sheet (Hybrid Version)

2. Occurrence of Fires and Explosion Incidents

Item Number	Attack Scenario		Assessment Metrics				Countermeasures				Security Level		Attack Tree Number	
		Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Protection		Detection/ Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
							Intrusion/ Spreading Phase	Objective Achievement Phase						
	2-1 2-2 2-3 2-4	2-1: Outbreak of fires and explosions due to control abnormalities in facilities for handling hazardous materials caused by the setting of improper target values. 2-2: Outbreak of fires and explosions due to control abnormalities in facilities for handling hazardous materials caused by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs. 2-3: Outbreak of fires and explosions due to erratic behavior in facilities for handling hazardous materials where the unauthorized modification of data and programs prevents a proper response, even when operations are performed correctly. 2-4: Outbreak of fires and explosions caused by a loss of monitoring and monitoring control at facilities for handling hazardous materials due to congestion in the control network (field side).												
42		Attack Entry Point=HMI Due to human error by an insider, the HMI is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at “connecting to unauthorized media”.					Same as item number 14				1 *2			
43	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the HMI by a malware infection.	2	3	3	A	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	1	#2-15	42,43
44	2-3	Tampering with and altering data/software in the HMI by malware infection.	2	3	3	A	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	1	#2-16	42,44
45	2-4	Tampering with and altering the control network (field side) settings from the HMI to cause network congestion in the control network by malware infection. This prevents the monitoring of the control system.	2	3	3	A	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	1	#2-17	42,45
46	2-4	Malware infection causing unauthorized communication with the control network (field side), and preventing control network communications. This prevents the monitoring of the control system.	2	3	3	A	Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		1	1	#2-18	42,46
47		Attack Entry Point = Control Server Due to human error by an insider, the control server is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at “connecting to unauthorized media”.					Anti-virus Application Whitelisting ○ Applying Patches Avoidance of Vulnerability Data Signature		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		2 *2			
48	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the control server by a malware infection.	2	2	3	B	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#2-19	47,48
49	2-3	Tampering with and altering data/software in the control server by malware infection.	2	2	3	B	Permission Management ○ Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	2	2	#2-20	47,49
50		Attack Entry Point = EWS Due to human error by an insider, the EWS is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at “connecting to unauthorized media”.					Same as item number 16				1 *2			
51	2-2	A malware infection maliciously modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	3	3	A	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	1	#2-21	50,51
52	2-4	Tampering with and altering the control network (field side) settings from the EWS to cause network congestion in the control network by malware infection. This prevents the monitoring of the control system.	2	3	3	A	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	1	#2-22	50,52
53	2-4	Malware infection causing unauthorized communication with the control network (field side), and preventing control network communications. This prevents the monitoring of the control system.	2	3	3	A	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	1	#2-23	50,53
X														

[Note]
*1 It is recommended to refer to “Section 9.4 Firewall Settings” in the Guide for evaluating countermeasures.
*2 It is recommended to refer to “Section 9 Security Measures for External Storage Media” in the Guide for evaluating countermeasures.

Table 4-10: Business Impact-based Risk Assessment Sheet (Hybrid Version)

3. Supply of Defective Product

Item Number	Attack Scenario		Assessment Metrics				Countermeasures								Security Level		Attack Tree Number	
		Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Protection				Detection/ Understanding Damage		Business Continuity		Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
							Intrusion/ Spreading Phase		Objective Achievement Phase									
	3-1 3-2 3-3	3-1: Production of a product that does not meet quality standards/criteria due to control abnormalities in production facilities caused by the setting of improper target values. 3-2: Production of a product that does not meet quality standards/criteria due to control abnormalities in production facilities caused by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs. 3-3: Production of a product that does not meet quality standards/criteria due to control abnormalities in production facilities caused by tampering with and altering data/software.																
54		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 1								2 *1			
55		Unauthorized access of the HMI via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 2								2			
56	3-1	Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the HMI by a malicious third party.	2	2	2	C	Segmentation/Zoning Data Signature Approval of Important Operations		(Same as on the left) (Same as on the left) (Same as on the left)		Log Collection/Log Analysis Integrated Log Management System				1	2	#3-1	54,55,56
57	3-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	2	C	Permission Management Access Control Data Signature		(Same as on the left) (Same as on the left) (Same as on the left)		Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		1	2	#3-2	54,55,57
58		Unauthorized access of the control server via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Same as item number 25								2			
59	3-1	Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the control server by a malicious third party.	2	2	2	C	Segmentation/Zoning Data Signature Approval of Important Operations		(Same as on the left) (Same as on the left) (Same as on the left)		Log Collection/Log Analysis Integrated Log Management System				1	2	#3-3	54,58,59
60	3-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	2	C	Permission Management Access Control Data Signature	○	(Same as on the left) (Same as on the left) (Same as on the left)		Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		2	2	#3-4	54,58,60
61		Unauthorized access of the EWS via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Same as item number 4								2			
62	3-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	2	C	Permission Management Access Control Data Signature		(Same as on the left) (Same as on the left) (Same as on the left)		Device Error Detection Log Collection/Log Analysis Integrated Log Management System		Data Backup		1	2	#3-5	54,61,62
63		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 7								2 *1			
64		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 8								2			
65		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 9								2			
66	3-1	Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the HMI by a malicious third party.	2	2	2	C	Same as item number 56								1	2	#3-6	63,64,65,66
67	3-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	2	C	Same as item number 57								1	2	#3-7	63,64,65,67
68		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 37								2			
69	3-1	Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the control server by a malicious third party.	2	2	2	C	Same as item number 59								1	2	#3-8	63,64,68,69
70	3-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	2	C	Same as item number 60								1	2	#3-9	63,64,68,70
71		Unauthorized access of the EWS from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 11								2			
72	3-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	2	C	Same as item number 62								1	2	#3-10	63,64,71,72
73		Attack Entry Point = HMI Due to human error by an insider, the HMI is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 14								1 *2			
74	3-1	Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the HMI by a malware infection.	2	3	2	B	Same as item number 56								1	1	#3-11	73,74
75	3-3	Tampering with and altering data/software in the HMI by malware infection.	2	3	2	B	Same as item number 57								1	1	#3-12	73,75
76		Attack Entry Point = Control Server Due to human error by an insider, the control server is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 47								2 *2			
77	3-1	Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the control server by a malware infection.	2	2	2	C	Same as item number 59								1	2	#3-13	76,77
78	3-3	Tampering with and altering data/software in the control server by malware infection.	2	2	2	C	Same as item number 60								1	2	#3-14	76,78
79		Attack Entry Point = EWS Due to human error by an insider, the EWS is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 16								1 *2			
80	3-2	A malware infection maliciously modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	3	2	B	Same as item number 62								1	1	#3-15	79,80
X																		

[Note]

*1 It is recommended to refer to "Section 9.4 Firewall Settings" in the Guide for evaluating countermeasures.

*2 It is recommended to refer to "Section 9 Security Measures for External Storage Media" in the Guide for evaluating countermeasures.

Table 4-10: Business Impact-based Risk Assessment Sheet (Hybrid Version)

4. Manufacturing/Production Disrupt/Suspend

Item Number	Attack Scenario		Assessment Metrics				Countermeasures				Security Level		Attack Tree Number	
		Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Protection		Detection/ Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
							Intrusion/ Spreading Phase	Objective Achievement Phase						
	4-1 4-2 4-3 4-4	4-1: Control abnormalities in production facilities caused by the setting of improper target values. This leads to processes being terminated for safety reasons. 4-2: Control abnormalities in production facilities caused by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs. This leads to processes being terminated for safety reasons. 4-3: Operational abnormalities in production facilities caused by tampering with and altering data/software. This leads to processes being terminated for safety reasons. 4-4: A destructive malware or ransomware infection that disables monitoring of production facilities and prevent monitoring control. This leads to processes being terminated for safety reasons.												
81		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 1				2 *1			
82		Unauthorized access of the HMI via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 2				2			
83	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the HMI by a malicious third party.	2	2	1	D	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#4-1	81,82,83
84	4-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	1	D	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	2	#4-2	81,82,84
85	4-4	Infection of the HMI with destructive malware (ransomware, etc.) by a malicious third party. This prevents the monitoring of the control system.	2	2	1	D	Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature	*Permission Management* *Access Control*	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	*Data Backup*	1	2	#4-3	81,82,85
86		Unauthorized access of the control server via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Same as item number 25				2			
87	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the control server by a malicious third party.	2	2	1	D	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#4-4	81,86,87
88	4-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	1	D	Permission Management ○ Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	2	2	#4-5	81,86,88
89		Unauthorized access of the EWS via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Same as item number 4				1			
90	4-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	1	D	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	2	#4-6	81,89,90
91		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item number 7				2 *1			
92		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 8				2			
93		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 9				2			
94	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the HMI by a malicious third party.	2	2	1	D	Same as item number 83				1	2	#4-7	91,92,93,94
95	4-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	1	D	Same as item number 84				1	2	#4-8	91,92,93,95
96	4-4	Infection of the HMI with destructive malware (ransomware, etc.) by a malicious third party. This prevents the monitoring of the control system.	2	2	1	D	Same as item number 85				1	2	#4-9	91,92,93,96
97		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 37				2			
98	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the control server by a malicious third party.	2	2	1	D	Same as item number 87				1	2	#4-10	91,92,97,98
99	4-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	1	D	Same as item number 88				1	2	#4-11	91,92,97,99
100		Unauthorized access of the EWS from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 11				2			
101	4-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	1	D	Same as item number 90				1	2	#4-12	91,92,100,101
102		Attack Entry Point = HMI Due to human error by an insider, the HMI is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 14				1 *2			
103	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the HMI by a malware infection.	2	3	1	D	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	1	#4-13	102,103
104	4-3	Tampering with and altering data/software in the HMI by malware infection.	2	3	1	D	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	1	#4-14	102,104
105	4-4	Data destroyed by destructive malware (ransomware, etc.). This prevents the monitoring of the control system.	2	3	1	D	Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature	*Permission Management* *Access Control*	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	*Data Backup*	1	1	#4-15	102,105
106		Attack Entry Point = Control Server Due to human error by an insider, the control server is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 47				2 *2			
107	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the control server by a malware infection.	2	2	1	D	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#4-16	106,107
108	4-3	Tampering with and altering data/software in the control server by malware infection.	2	2	1	D	Permission Management ○ Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	2	#4-17	106,108
109		Attack Entry Point = EWS Due to human error by an insider, the EWS is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item number 16				1 *2			
110	4-2	A malware infection maliciously modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	3	1	D	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	1	#4-18	109,110
111	4-4	Malware infection of the HMI. Data destroyed by destructive malware (ransomware, etc.). This prevents the monitoring of the control system.	2	3	1	D	Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature	*Permission Management* *Access Control*	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	*Data Backup*	1	1	#4-19	109,111
X														

[Note]

*1 It is recommended to refer to "Section 9.4 Firewall Settings" in the Guide for evaluating countermeasures.

*2 It is recommended to refer to "Section 9 Security Measures for External Storage Media" in the Guide for evaluating countermeasures.

Table 4-10: Business Impact-based Risk Assessment Sheet (Hybrid Version)

5. Leak of Confidential Information

Item Number	Attack Scenario		Assessment Metrics				Countermeasures								Security Level		Attack Tree Number	
		Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Protection				Detection/ Understanding Damage		Business Continuity		Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
							Intrusion/ Spreading Phase		Objective Achievement Phase									
	5-1	5-1: Theft of company production secrets stored on the control system, resulting in an external information leak.																
112		**Attack Entry Point = Information Network** Unauthorized firewall access by a malicious third party. * Unauthorized access includes “execution of unauthorized processes” (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the “execution of unauthorized processes”.					Same as item number 1								2 *1			
113		Unauthorized access of the control server via the FW by a malicious third party. * Unauthorized access includes “execution of unauthorized processes” (privilege escalation).					Same as item number 25								2			
114	5-1	Theft of data on the control server by a malicious third party. (Data then retrieved by following the reverse route.)	2	2	3	B	Permission Management Access Control Data Encryption DLP	○	(Same as on the left) (Same as on the left) (Same as on the left) (Same as on the left)		Log Collection/Log Analysis Integrated Log Management System				2	2	#5-1	112,113,114
115		Unauthorized access of the EWS via the FW by a malicious third party. * Unauthorized access includes “execution of unauthorized processes” (privilege escalation).					Same as item number 4								1			
116	5-1	Theft of data on the EWS by a malicious third party. (Data then retrieved by following the reverse route.)	2	2	3	B	Permission Management Access Control Data Encryption DLP		(Same as on the left) (Same as on the left) (Same as on the left) (Same as on the left)		Log Collection/Log Analysis Integrated Log Management System				1	2	#5-2	112,115,116
117		**Attack Entry Point = Monitoring Terminal** Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes “execution of unauthorized processes” (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the “execution of unauthorized processes”.					Same as item number 7								2 *1			
118		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes “execution of unauthorized processes”.					Same as item number 8								2			
119		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes “execution of unauthorized processes”.					Same as item number 37								2			
120	5-1	Theft of data on the control server by a malicious third party. (Data then retrieved by following the reverse route.)	2	2	3	B	Same as item number 114								1	2	#5-3	117,118,119,120
121		Unauthorized access of the EWS from the data historian by a malicious third party. * Unauthorized access includes “execution of unauthorized processes”.					Same as item number 11								2			
122	5-1	Theft of data on the EWS by a malicious third party. (Data then retrieved by following the reverse route.)	2	2	3	B	Same as item number 116								1	2	#5-4	117,118,121,122
X																		

[Note]
***1** It is recommended to refer to “Section 9.4 Firewall Settings” in the Guide for evaluating countermeasures.
***2** It is recommended to refer to “Section 9 Security Measures for External Storage Media” in the Guide for evaluating countermeasures.

This page has intentionally been left blank.

4.4. Summary of Risk Values

[Task 4.4] Summarizing risk values for attack trees analyzed with business impact-based risk analysis.

[Output 4.4]

Examples of compiled business impact-based risk analysis results are provided below (Table 4-11).

Table 4-11: Summary Chart of Risk Values for Business Impact-based Risk Analysis Results

Risk Value	Total Number of Attack Trees	Business Impact Scenario		Number of Attack Trees (By Business Scenario)
A	10	1	Wide Area Product Supply Outage	2
		2	Occurrence of Fires and Explosion Incidents	7
B	29	1	Wide Area Product Supply Outage	4
		2	Occurrence of Fires and Explosion Incidents	16
		3	Supply of Defective Product	3
		5	Leak of Confidential Information	4
C	12	3	Supply of Defective Product	12
D	19	4	Manufacturing/Production Disrupt/Suspend	19
E	0	-		0

Examples of risk values (A, B) compiled by attack entry point are provided below (Table 4-12).

Table 4-12: Summary Chart of Risk Values for Business Impact-based Risk Analysis Results (Attack Entry Point Basis)

#	Risk Value	Attack Entry Point	Number of Attack Trees	Total Number of Attack Trees
1	A	HMI (Physical Intrusion)	4	9
2		EWS (Physical Intrusion)	5	
3	B	Information Network [-> FW]	11	29
4		Monitoring Terminal -> [Data Historian (Relay)]	11	
5		HMI (Physical Intrusion)	1	
6		EWS (Physical Intrusion)	2	
7		Control Server (Physical Intrusion)	2	
8	C	(Omitted)	12	12
9	D	(Omitted)	19	19
10	E	(Omitted)	0	0

5. Utilizing Risk Analysis

5.1. Risk Analysis Results for the Control System (Improvement Measures to Reduce Risk)

[Task 5.1①] Reviewing security measures for reducing risk in the attack trees with a risk value of A or B on the basis of the results of a business impact-based risk analysis.

- Effective methods for reducing risk in the control system are explained in detail in "*Chapter 7* Interpreting and Utilizing Risk Assessment Results" in the Guide.

[Output 5.1①]

A summary of improvement measures for reducing risk can be found over the page (Table 5-1).

Table 5-1: Improvement Measures to Reduce Risk

#	Asset	Attack Steps	Current Attack Tree Risk Value (Corresponds with Table 4-1)	Current Countermeasures (Countermeasures Currently Addressing the Threat in Question)	Additional Countermeasures (Proposed Improvements to Countermeasures, Strengthened Countermeasures)	Attack Tree Risk Value after Additional Countermeasures
1	HMI	Due to human error by an insider, the HMI is infected with malware after being connected to a malware-infected USB storage device.	A Applicable Trees = 4 (Table 4-12#1)	None	・ Applying whitelist (Vulnerability Level 3 -> 2)	B Applicable Trees = 4
2			B Applicable Tree = 1 (Table 4-12#6)			C Applicable Tree = 1
3	EWS	Due to human error by an insider, the EWS is infected with malware after being connected to a malware-infected USB storage device.	A Applicable Trees = 5 (Table 4-12#2)	None	・ Applying whitelist (Vulnerability Level 3 -> 2)	B Applicable Trees = 5
4			B Applicable Trees = 2 (Table 4-12#5)			C Applicable Trees = 2
5	Firewall (FW)	Unauthorized firewall access by a malicious third party.	B Applicable Trees = 11 (Table 4-12#3)	・ Applying security patches ・ User authentication (password)	(Proposal 1) ・ Strengthening firewall administrator authentication. Applying additional countermeasures, such as restricting screen access to access attempts that pass through a secure jump server, and using two-factor authentication. (Vulnerability Level 2 -> 1) (Proposal 2) ・ Shifting the administrator interface from the information network to the control network, and blocking firewall access from the information network. (Vulnerability Level 2 -> 1) * This assumes that firewall patch updates can be applied offline.	C Applicable Trees = 11
6		Unauthorized access of assets on the control network via the data historian (relay) in the DMZ by a malicious third party.	B Applicable Trees = 11 (Table 4-12#4)	・ Keeping communication connections to an absolute minimum (IP packet level restrictions)	Strengthened measures are considered, referring to "Section 9.4 Firewall Settings" in the Guide. Specifically, risk values for all applicable trees can be reduced from B to C by introducing a one-way gateway. (Vulnerability Level 2 -> 1)	C Applicable Trees = 11
7	Control Server	Due to human error by an insider, the control server is infected with malware after being connected to a malware-infected USB storage device.	B Applicable Trees = 2 (Table 4-12#7)	・ Application whitelisting to restrict the execution of unauthorized processes.	(No additional countermeasures)	B Applicable Trees = 2

[Task 5.1②] Compiling a summary of how risk values change before and after countermeasures.

[Output 5.1②]

The distribution of risk values by tree before and after countermeasures is outlined below (Table 5-2). In addition, a sheet summarizing a list of attack routes and changes in risk values is provided over the page (Table 5-3).

Table 5-2: Distribution of Risk Values in the Tree Before and After Countermeasures are Implemented

Risk Value	Current Number of Attack Trees	Number of Attack Trees after Improvements
A	9	0
B	27	11
C	12	27
D	19	17
E	0	12

Table 5-3: List of Attack Routes and Changes in Risk Values before and after Countermeasures (Extract)

		Who	From Where	How						Before Countermeasures				After Countermeasures			
Attack Tree Number	Scenario Number	Attacker	Attack Entry Point	Attack Path 1	Attack Path 2	Attack Path 3	Attack Execution Asset	Attack Target	Final Attack	Threat	Vulnerability	Business Impact	Risk Value	Threat	Vulnerability	Business Impact	Risk Value
1-1	1-1	Malicious Third Party	Information Network	FW			HMI	Controller	Causes wide-area supply outage.	2	2	3	B	2	1	3	C
1-2	1-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	Controller	Causes wide-area supply outage.	2	2	3	B	2	1	3	C
1-3	1-1	Insider (Human Error)	HMI (Physical Intrusion)				HMI	Controller	Causes wide-area supply outage.	2	3	3	A	2	2	3	B
1-4	1-2	Malicious Third Party	Information Network	FW	EWS		Controller (M)	Controller (S)	Sends malicious control command to cause supply outage.	2	2	3	B	2	1	3	C
1-5	1-2	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian	EWS	Controller (M)	Controller (S)	Sends malicious control command to cause supply outage.	2	2	3	B	2	1	3	C
1-6	1-2	Insider (Human Error)	EWS (Physical Intrusion)				Controller (M)	Controller (S)	Sends malicious control command to cause supply outage.	2	3	3	A	2	2	3	B
2-1	2-1	Malicious Third Party	Information Network	FW			HMI	Controller	Sets incorrect target value for controller.	2	2	3	B	2	1	3	C
2-2	2-1	Malicious Third Party	Information Network	FW			Control Server	Controller	Sets incorrect target value for controller.	2	2	3	B	2	1	3	C
2-3	2-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	Controller	Sets incorrect target value for controller.	2	2	3	B	2	1	3	C
2-4	2-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		Control Server	Controller	Sets incorrect target value for controller.	2	2	3	B	2	1	3	C
2-5	2-1	Insider (Human Error)	HMI (Physical Intrusion)				HMI	Controller	Sets incorrect target value for controller.	2	3	3	A	2	2	3	B
2-6	2-1	Insider (Human Error)	Control Server (Physical Intrusion)				Control Server	Controller	Sets incorrect target value for controller.	2	2	3	B	2	2	3	B
2-7	2-2	Malicious Third Party	Information Network	FW			EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.	2	2	3	B	2	1	3	C
2-8	2-2	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.	2	2	3	B	2	1	3	C
2-9	2-2	Insider (Human Error)	EWS (Physical Intrusion)				EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.	2	3	3	A	2	2	3	B
2-10	2-3	Malicious Third Party	Information Network	FW			HMI	HMI	Tampers with and alters data/software in HMI.	2	2	3	B	2	1	3	C
2-11	2-3	Malicious Third Party	Information Network	FW			Control Server	Control Server	Tampers with and alters data/software in control server.	2	2	3	B	2	1	3	C
2-12	2-3	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	HMI	Tampers with and alters data/software in HMI.	2	2	3	B	2	1	3	C
2-13	2-3	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		Control Server	Control Server	Tampers with and alters data/software in control server.	2	2	3	B	2	1	3	C
2-14	2-3	Insider (Human Error)	HMI (Physical Intrusion)				HMI	HMI	Tampers with and alters data/software in HMI.	2	3	3	A	2	2	3	B
2-15	2-3	Insider (Human Error)	Control Server (Physical Intrusion)				Control Server	Control Server	Tampers with and alters data/software in control server.	2	2	3	B	2	2	3	B
2-16	2-4	Malicious Third Party	Information Network	FW			HMI	Control Network (Field Side)	Maliciously modifies network settings and disables communications.	2	2	3	B	2	1	3	C
2-17	2-4	Malicious Third Party	Information Network	FW			HMI	Control Network (Field Side)	Infects with malware causing unauthorized communications, and disables communications.	2	2	3	B	2	1	3	C
2-18	2-4	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	Control Network (Field Side)	Maliciously modifies network settings and disables communications.	2	2	3	B	2	1	3	C
2-19	2-4	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	Control Network (Field Side)	Infects with malware causing unauthorized communications, and disables communications.	2	2	3	B	2	1	3	C
2-20	2-4	Insider (Human Error)	HMI (Physical Intrusion)				HMI	Control Network (Field Side)	Maliciously modifies network settings and disables communications.	2	3	3	A	2	2	3	B
2-21	2-4	Insider (Human Error)	HMI (Physical Intrusion)				HMI	Control Network (Field Side)	Infects with malware causing unauthorized communications, and disables communications.	2	3	3	A	2	2	3	B
2-22	2-4	Insider (Human Error)	EWS (Physical Intrusion)				EWS	Control Network (Field Side)	Maliciously modifies network settings and disables communications.	2	3	3	A	2	2	3	B
2-23	2-4	Insider (Human Error)	EWS (Physical Intrusion)				EWS	Control Network (Field Side)	Infects with malware causing unauthorized communications, and disables communications.	2	3	3	A	2	2	3	B

This page has intentionally been left blank.

Update History

October 2, 2017	1st Edition
October 15, 2018	2nd Edition
October 31, 2018	Corrected errors
March 31, 2020	2nd Edition (March 2020 Edition) Added Table 1-1 (page 10) and Table 5-3 (page 93).

This document can be downloaded from the following URL.
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

Information-technology Promotion Agency, Japan
IT Security Center

Bunkyo Green Court, Center Office
2-28-8 Honkomagome, Bunkyo-ku, Tokyo 113-6591

Tel: +81 3-5978-7527   Fax: +81 3-5978-7552
https://www.ipa.go.jp/security/