Practical Examples of Security Risk Assessment for Industrial Control Systems

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



March 2020



Information-technology Promotion Agency, Japan IT Security Center

Contents

Introduction	5
Notes on the Revised Second Edition	7
1. Structure of This Volume	9
2. Preparing for Risk Analysis	13
2.1. List of Assets	14
2.2. System Configuration Diagram	21
2.3. Dataflow Matrix	23
2.4. Evaluation Criteria for Importance of Assets	26
2.5. List Detailing the Importance of Each Asset	28
2.6. Evaluation Criteria for Business Impact Level	30
2.7. Review of Business Impacts and Business Impact Levels	32
2.8. Evaluation Criteria for Threat Level	35
3. Asset-based Risk Analysis	37
3.1. Review of Threat Level	38
3.2. Filling Out the Asset-based Risk Assessment Sheet	41
3.3. Summary of Risk Values	57
4. Business Impact-based Risk Analysis	59
4.1. Preparing a List of Attack Scenarios	60
4.2. Preparing a List of Attack Routes	63
4.3. Preparing a Risk Assessment Sheet	68
4.4. Summary of Risk Values	89
5. Utilizing Risk Analysis	90
5.1. Risk Analysis Results for the Control System	
(Improvement Measures to Reduce Risk)	90

Figure Contents

Figure 1-1: Risk Analysis Flow and Outputs	11
Figure 2-1: Preparation Work Flow	13
Figure 2-2: System Configuration Diagram	21
Figure 2-3: Dataflow Chart	25
Figure 3-1: Asset-based Risk Analysis Work Flow	37
Figure 4-1: Business Impact-based Risk Analysis Work Flow	59
Figure 4-2: Attack Route Diagram	67
Table Contents	
Table 2-1: List of Outputs for the Preparation Work	13
Table 2-2: List of Assets	
Table 2-3: List of Assets (Including Role/Function,	
Scope of Impact/Impact on Business Continuity, Security Measures)	17
Table 2-4: Dataflow Matrix	23
Table 2-5: Example Definitions of Evaluation Criteria for Importance of Assets	26
Table 2-6: Importance of Assets	28
Table 2-7: Example Evaluation Criteria for Business Impact Levels	30
Table 2-8: List of Business Impacts	32
Table 2-9: List of Business Impacts and Business Impact Levels	33
Table 2-10: Evaluation Criteria for Threat Levels	35
Table 3-1: Outputs for Preparations Used	37
Table 3-2: Outputs Prepared in Asset-based Risk Analysis Work	37
Table 3-3: List of Anticipated Threats to the Asset Being Analyzed	38
Table 3-4: HMI (Operator Terminal) Threat Levels and Reasoning	39
Table 3-5: Summary Chart of Asset Threat Levels	40
Table 3-6: Asset-based Risk Assessment Sheet	43
Table 3-7: Summary Chart of Vulnerability Levels for Asset-based Risk Analysis	57
Table 3-8: Summary Chart of Risk Values for Asset-based Risk Analysis	58
Table 4-1: Outputs for Preparations Used	59
Table 4-2: Outputs Prepared in Business Impact-based Risk Analysis Work	59
Table 4-3: Format of Attack Scenarios	60
Table 4-4: List of Attack Scenarios	61
Table 4-5: Format for a List of Attack Routes	63
Table 4-6: List of Attack Routes (Sorted by Scenario)	65

Table 4-7: List of Attack Routes (Sorted by Attack Entry Point)	. 66
Table 4-8: Business Impact-based Risk Assessment Sheet (Sorted by Scenario)	. 71
Table 4-9: Business Impact-based Risk Assessment Sheet (Sorted by Attack Entry Point)	. 79
Table 4-10: Business Impact-based Risk Assessment Sheet (Hybrid Version)	. 82
Table 4-11: Summary Chart of Risk Values for Business Impact-based Risk Analysis Results	. 89
Table 4-12: Summary Chart of Risk Values for Business Impact-based Risk Analysis Res	ults
(Attack Entry Point Basis)	. 89
Table 5-1: Improvement Measures to Reduce Risk	. 91
Table 5-2: Distribution of Risk Values in the Tree Before	
and After Countermeasures are Implemented	. 92
Table 5-3: List of Attack Routes and Changes in Risk Values before	
and after Countermeasures (Extract)	. 93

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 manhours 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.

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 Information-technology Promotion Agency, Japan Satoshi Fukuhara, Kazuyuki Yoshida, Information-technology Promotion Agency, Japan (At the time of publication) Toshiyuki Kuwana, Information-technology Promotion Agency, Japan

Information-technology Promotion Agency, Japan

Chisato Konno,

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 manhours 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	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 F	Risk Analysis					
Title in this Volume		Output		Guide				
3.1	10	Summary Chart of Threat Levels		-				
3.2	11)	Asset-based Risk Assessment Shee	t	Chapter 5				
3.3.①	12	Summary Chart of Vulnerability Leve	els	-				
3.3.②	13	Summary Chart on Risk Values		-				
		4. Asset-based F	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				
4.2	(13)-1	List of Attack Routes		to Table 6-12				
4.2	15-2	Attack Route Diagram		6.5.1. Figure 6-9				
4.3	16	Business Impact-based Risk Assess	6.6.4. ~ 6.11.					
4.4	11)	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 Contro	l System	Chapter 7				

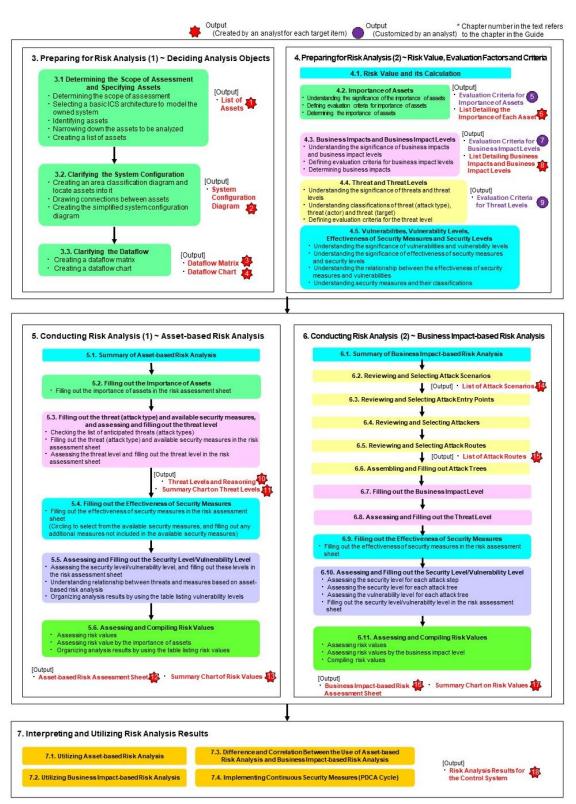


Figure 1-1: Risk Analysis Flow and Outputs

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
	IT Asset	0	
Type of	OT Asset		
Assets	Network Asset (with Communication Control Functions) Network Asset (without Communication Control Functions)		0
	Input/Output	0	
Asset	Storing Data		
Functions	Issuing Commands		
	Gateway Function		0
	Type of Communication Line		
	Installation Location	Office	Server Room
	Information Network	0	0
	DMZ		0
Connected	Control Network (Information Side)		0
Network	Control Network (Field Side)		
	Field Network		
-	Other		
Net	work Connected to Maintenance Port	×	Information Network
	Presence of Operation Interface	0	×

[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

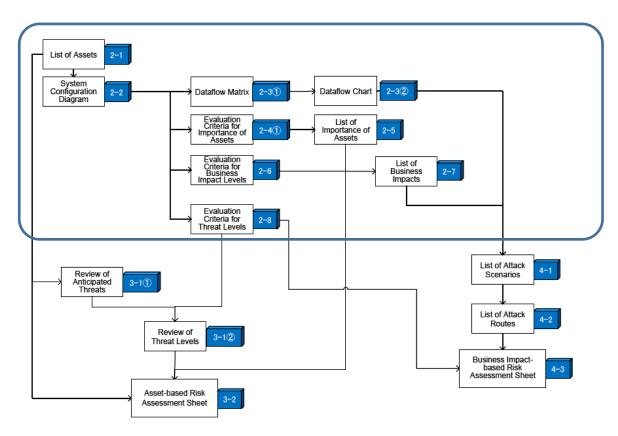


Figure 2-1: Preparation Work Flow

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)
	IT Asset	0												
	OT Asset				0	0		0	0	0			0	0
Type of	Network Asset		0	0			0							
Assets	(with Communication Control Functions)		U	U			U							
	Network Asset (without Communication										0	0		
	Control Functions)	_				_		_					_	
1	Input/Output	0			0	0		0	0	0			0	0
Asset	Storing Data				0	0		0	0	0			_	
Functions	Issuing Commands								0	0			0	0
	Gateway Function		0	0			0				0	0		
	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)
	Information Network	0	0											
	DMZ		0	0	0									
Connected	Control Network (Information Side)		0			0	0	0	0	0				
Network	Control Network (Field Side)							0	0	0	0		0	
	Field Network											0	0	0
	Other													
Netwo	ork Connected to Maintenance Port	×	Information Network	×	×	×	×	×	×	×	×	×	×	×
Pr	resence of Operation Interface	0	×	×	0	0	×	0	0	0	×	×	×	×
Use	of USB Port/Communications I/F	0	0	0	0	0	0	0	0	0	0	×	×	×
Regular	r Use of Media/Device Connections	×	×	×	×	×	×	0	×	×	×	×	×	×
Wire	less Communication Capabilities	0	×	×	×	×	×	×	×	×	×	×	×	×
Regula	r 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		Writ	tten in Dataflow M	atrix										
System C	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	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 onsite 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.
	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 antivirus 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).

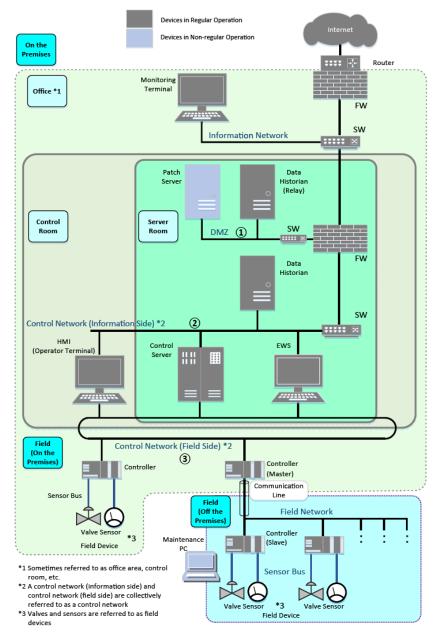


Figure 2-2: System Configuration Diagram

[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	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) Control NW (Field)			Process Value				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) Field Network				Process Value		Process Value			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.

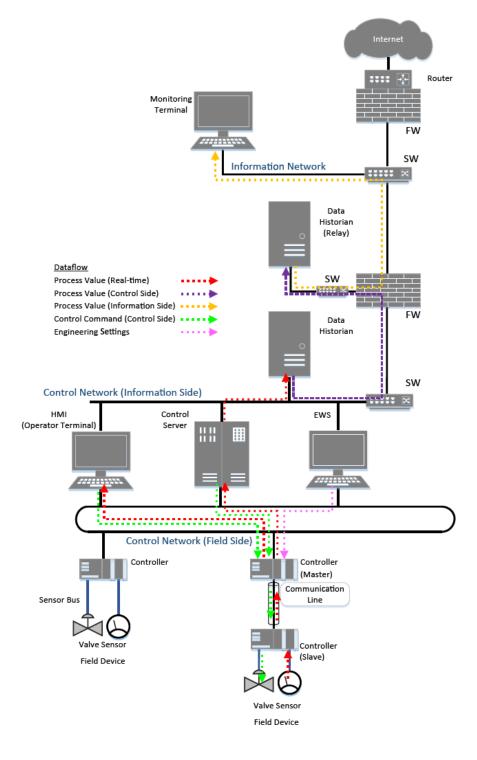


Figure 2-3: Dataflow Chart

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		
	Assets which, if lost, or subject to unauthorized operation, would have a major		
	impact on the business.		
3	- 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.		
	Assets which, if lost, or subject to unauthorized operation, would have a medium-		
	level impact on the business.		
2	- 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.		
	Assets which, if lost, or subject to unauthorized operation, would have a low-level		
4	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 <u>two weeks' worth</u> of stored inventory and the asset's failure could lead to a control system outage of <u>under two weeks</u>, 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).

#	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 efficienc 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		Evaluation Criteria
		The following may result from a failure occurring.
3	High Business	- Potential for an extended system outage (for two weeks or more).
3	Impact	- Potential losses amounting to 500 million yen or more.
		- Potential to cause damage or pollution in the surrounding environment.
	Madium	The following may result from a failure occurring.
2	Medium	- Potential for a system outage over a period (for three days to two weeks).
2 Business Impact		- Potential losses of between 100 million yen up to 500 million yen.
	impact	- Potential to cause damage to company premises.
		The following may result from a failure occurring.
		- While there is the potential for a system outage over a period (of less than
1	Low Business	three days), this will not greatly affect operations.
l	Impact	- 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 <u>two weeks' worth</u> of stored inventory and the asset's failure could lead to a control system outage of <u>under two weeks</u>, 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		
		Improper use of legitimate supply outage functions caused by a		
1	Wide Area Product Supply	cyber attack on supply facilities, which produces a wide area		
'	Outage	product supply outage, resulting in significant social impacts and		
		a dramatic loss of trust in the company.		
		Outbreak of fires and explosions due to control abnormalities		
		and a loss of monitoring facilities for handling hazardous		
2	Occurrence of Fires and	materials caused by a cyber attack on manufacturing facilities.		
	Explosion Incidents	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.		
		Manufacturing and supply of a product that does not meet		
		quality standards/criteria caused by a cyber attack on		
3	Supply of Defective Product	manufacturing facilities, causing significant inconvenience to		
		customers, significant losses in compensation claims, and a		
		dramatic loss of trust in the company.		
		Manufacturing/production disrupt/suspend due to forcibly		
4	Manufacturing/Production	terminated processes due to process control abnormalities and		
4	Disrupt/Suspend	operation monitoring failures caused by a cyber attack on		
		manufacturing facilities.		
		A cyber attack on the control system, resulting in an external		
5	Leak of Confidential	leak of company production secrets, impacting the company's		
٥	Information	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	
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

Table 2-10. Evaluation Officia for Tiffed Ecvels			
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

_		- J
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	_

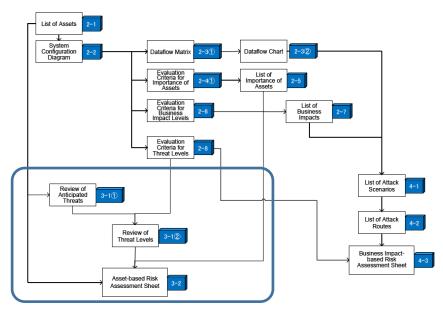


Figure 3-1: Asset-based Risk Analysis Work Flow

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	0	0											
OT Asset			0	0	0		0	0	0			0	0
Network Asset (with Communication Control Functions)			0			0							
Network Asset (without Communication Control Functions)										0	0		
Unauthorized Access	~	~	~	~	~	~	~	~	~		_	V	~
Physical Intrusion	~	~	~	~	~	~	~	~	~			~	~
Unauthorized Operation	~	~	~	~	~	~	~	~	<i>v</i>			<i>v</i>	~
Human Error in Operation	~	~	<i>V</i>	~		~	~		<i>v</i>			<i>v</i>	~
Connecting Unauthorized Media or Device	~	~	~	~	\(\sigma \)	~	~	<i>\</i>	~			<i>v</i>	~
Execution of Unauthorized Processes	~	~	~	~	~	~	~	~	<i>v</i>			<i>v</i>	~
Malware Infection	~	_	<i>v</i>	~	~	~	~		<i>v</i>			-	~
Information Theft		<i>'</i>						<i>'</i>				V	~
	٧ ٧	<i>y</i>	<i>'</i>	٧ ٧	V	ν ν	<i>y</i>	<i>\</i>	<i>'</i>			<i>V</i>	~
Unauthorized Modification of Information Information Destruction					V							<i>v</i>	
	<i>'</i>	<i>V</i>	<i>V</i>	~	<i>V</i>	<i>V</i>	<i>V</i>	<i>'</i>	<i>V</i>				<i>'</i>
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 <u>"malicious third party"</u> (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

	Table 3-4: HIVII (U		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	0			0	0		0	0	0			0	0
Network Asset (with Communication Control Functions)		0	0			0							
Network Asset (without Communication Control Functions)										0	0		
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.

The state Property												Counterm	easur	res			Security Level
Part	Item Number	Type of Assets	Target Device					Threat (Attack Type)	Description		ection				ae	Business Continuity	By Threat
Part		Information System Asset	Maniforing Terminal	Threat Level	Vulnerability Level	Importance of Assets	Risk Value	Linauthorizad Access	Intrusion of the devices via the naturals to execute an attack			Objective Achievement Pha			J		\vdash
Part		mormation System Asset	Monitoring Terminal					Unaumonzed Access	intrusion of the device via the network to execute an attack.						+		
2 2 2 2 3 4 5 5 6 6 6 6 6 6 6 6																	
Part															\perp		, ,
Property of the property of th	1			3	2		D				_				+		2
Part											Ť				+		
Part											0						
Service of the control of the contro										Avoidance of Vulnerability					\perp		
Service of the control of the contro						4		Dt	Unauthorbed arross of sertines/areas (device installation invations, etc.) with arross	5	_			0 3	_		
Part Assert Control Control Part Assert Control Control Part Assert Co	2			2	2		Ь В	Physical intrusion	restrictions.		0				+		2
A Secretary of the process of the control of the co	-			_	-		-		installed in racks, cabinets, etc.).	Econ dia noy management	Ė			and dolon Detection Condo			ı - I
Part	3			2	2	1 1	D	Unauthorized Operation		Operator Authentication	0						2
The second process of the control of					_	1 1									_		\vdash
Part								Human Error in Operation			0				+		
Part	4			3	2		D		device).	mail I itering	-				\neg		2
Control of inchronous Control of Control o																	
Both Market Principal Control Age Contro						1 1						(0 1 1 6)			_		\vdash
The control of the co										Restriction on Connecting Device and its Usage	0	(Same as on the Left)		(-		
Secretary of June State Company of the Company of t	5			3	2		D	INICUIA OF DEVICE							_		2
Processing Continues		l		L]	<u></u>								士		
2 2 3 6															Ţ		, — —
Security States (Continued Continued	۾ ا						_	Processes			_				+		, I
Alloware anticipate in recompany of common productions production of production of common productions and common productions and common productions and common productions and common productions are common p	J				"				GOVICO.		\vdash	,			+		
Service of the control of the contro	_			L	L		L					, and an and any					
Part Product Part Product Part Part Product Part	\neg]		Malware Infection			0				コ		$\neg \neg$
Advanced Tributed Companies on American Information (Information Companies on American Information Companies On Informati									the attack target device.						Ţ		, 1
Advantage limit of the control of th	7			3	2		D				0				+		2
Harmation Thail Part of Financial Control Con		l									_				+		1
Uniform to the property of the control and property of the				L_	<u>L_</u>]	L								_		
B B C Unadmiced Modification of Information (Information Confidence of Information Confidence of	\neg							Information Theft							I		, ——
Description Model state of Journal Model state of Journal Model state of Model st	ا ۾						_				_			Integrated Log Management System	+		, , ,
Particular biological of public design o	۰			3	3		"		irriormation) stored on the device.		\vdash				+		, '
Advancable production of the control												(Guille ab oil alle Edit)			_		
A great of the confidence of the confidence of the foliage of the						1 1		Unauthorized Modification of	Unauthorized modification of information (software,	Permission Management		(Same as on the Left)		Device Error Detection	D	ata Backup	
Internation Desiration Part	9			2	3		D	Information							_		1
Description of settings of set									keys and other confidential information) stored on the device.	Data Signature	_	(Same as on the Left)		Integrated Log Management System	+		ı J
Description of settings of set	-					1 1		Information Destruction	Destroying of information (software, authentication		_	Permission Management		Device Error Detection	D	ata Backup	\Box
Local foreign framework of the device. 2 3 1 1 D. Understood framework in the second program device of one of the second program device of one of the second program device of one of the second program device of the sec	10			١,			<u>_</u>										
Description of important Configuration (Contraction) Description of Important Configuration (Contraction) Description of Important Contraction (Contraction) Description of Contraction (Contraction) Description of Contraction (Contraction) Description of Contraction (Contraction) Description of Contraction (Contraction) De	10			1	"		"		confidential information) stored on the device.					Integrated Log Management System			, ' I
Description of important Configuration (Contraction) Description of Important Configuration (Contraction) Description of Important Contraction (Contraction) Description of Contraction (Contraction) Description of Contraction (Contraction) Description of Contraction (Contraction) Description of Contraction (Contraction) De						+ +		Lineutherized Transmission	Sanding upouthorized control commands (softings changes	Seemontation/Zening	⊢	(Comp on on the Left)		Log Collection/Log Applysis	-		\vdash
Accepted of Important Operations Appropriate Communication Services and Services Accepted to Communication Services Accepted Acc						1	_	Unautionzed Transmission			\vdash				+		
Decided Adaca Security of regular device operations by sending processing requests find exceed the processing copycity of the devices are send of a DOOS stack, etc. Disch Adaca Security of regular device operations by sending processing requests find exceed the processing copycity of the devices are send of a DOOS stack, etc. Disch Adaca Security of the devices of the processing copycity of the processing copycity of the processing copycity of the processing copycity of the processing	11			2	3	'	D								_		1
Decided Adaca Security of regular device operations by sending processing requests find exceed the processing copycity of the devices are send of a DOOS stack, etc. Disch Adaca Security of regular device operations by sending processing requests find exceed the processing copycity of the devices are send of a DOOS stack, etc. Disch Adaca Security of the devices of the processing copycity of the processing copycity of the processing copycity of the processing copycity of the processing						1											
Do Adapt.								Outage	Stopping device functions.		_						ı l
Dod Atlack E Dod Atlack Participate division operation by parallely processing capacity of the division as a result of a Diod state, etc. Dod The Device here in Division of the processing capacity of the division as a result of a Diod state, etc. Dod The Device here in Division of the Diod state, etc. Dod The Device here in Division of the Diod state, etc. Dod The Device here in Division of the Diod state, etc. Dod The Device here in Division of the Diod state, etc. Dod The Device here in Division of the Divisio	12			2	3		D				\vdash				- F	alisale Design	1 1
E processing opposite by the device as a result of a DOS state, etc. Device a Not Annotation (a) the device as a result of a DOS state, etc. Device a Not New Management (a) the device as a result of a DOS state, etc. Device Revi. Device Revi. Devic				_	-		-				\vdash				_		
E processing opposite by the device as a result of a DOS state, etc. Device a Not Annotation (a) the device as a result of a DOS state, etc. Device a Not New Management (a) the device as a result of a DOS state, etc. Device Revi. Device Revi. Devic						1 1									_		
The device as a result of a DDoS attack, etc. Commence of the Commence of t								DoS Attack		DDoS Countermeasures	⊢						ı J
D Tradit Device that	13			1	3		E								- P	alisale Design	1 1
Packet Striffing Their of information (subtware, authentication information information (subtware, authentication information (subtware, authentication information (subtware, authentication information information (subtware, authentication information informatio									,								
Packet Striffing Their of information (subtware, authentication information information (subtware, authentication information (subtware, authentication information (subtware, authentication information information (subtware, authentication information informatio]											\Box
Transpers (Device at Time of Information (Information) Transpersing (Device at Time of Information) Transpersion (Device at Time of Information (Device at Time of Information) Transpersion (Device at Time of Information (Device at Time of Information) Transpersion (Device at Time of Information) Transpersion (Device at Time of Information (Device at Time of Information) Transpersion (Device at Time of Information (Device at Time of Information) Transpersion (Device at Time of Information (Device at Time of Information) Transpersion (Device at Time of Information (Device at Time	14	l		,	,		n	Theft	Device theft.	Lock and Key Management	0	(Same as on the Left)		(Same as on the Left)			, ,
Temporing Device at Time ordination of States and other confidence in Childracian (Childracian in The for Disposal of The Childracian of The Childraci	1**			'	1		"				\vdash				+		-
Tampering Device at Time Configuration Service and Children Service and						1 1		Information Theft by	Theft of information (software, authentication information,	Tamper Resistance		(Same as on the Left)			⇉		
Roofe Disposing	15			2	2		l p			Obfuscation					コ		, ,
Route Blocking Communication are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communications are blocked by pulling out the communication are blocked by pulling out the communicat	1			-	-		-			Zeroization	٥	(Same as on the Left)			+		
Communication called by pulling out the Alternatively communications are blocked by pulling out the Alternatively communication cable from the device. Device Alternatively pulling out the Integrated Communication cable from the device. Device Alternatively pulling out the Integrated Communication cable from the device. Device Alternative Communications traffic PW (Packet Filtering Type) Device Alternative Communications traffic PW (Packet Filtering Type) Device Alternative Communications traffic PW (Packet Filtering Type) Device Alternative Communications		l				† †				Entrance and Exit Management (IC Card)				Device Error Detection	R	Redundancy	
Ommunication cable from the device. Causing congestion by generating the communications traffic W. (Packet Filtering Type) Device Error Detection Period Aller Monitoring Period Communications Period									communication cable.						_f`		
Network Congestion Causing congestion by generating the communications traffic PW (Packet Filtering Type) PSIOS PSIOS Docce Alive Monitoring Log Collection Log Analysis Heyericable (no functions) Jamming Interference with radio communications. Packet Soffing Theft of information flowing on the network. Unsubhorized Modification of Maliciously modifying information flowing on the network. Unsubhorized Modification of Maliciously modifying information flowing on the network. Connecting Unsubhorized Device and Maliciously modifying information flowing on the network. Encryption of Communications Channels Data Encryption Encryption of Communications Channels Data Signature Encryption of Communications Encryption of Communications Encryption of Communica															\Box		
Network Congestion by generating the communications traffic PW (Packet Filtering Type) Device Error Detection Sensor Network Congestion by generating the communications traffic PW (Application Gateway Type) Device Error Detection Redundancy WAF Device Error Detection Redundancy WAF Device Error Detection PSIDS Device Error Detection Dos Countermeasures Dos Countermeasures Dos Countermeasures Device Error Detection Redundancy Device Error Detection Device Error Detection Redundancy Device Error Detection Device Error Device Error Device Device Error Device Error Device Device Error Device Error Device Device Error Device Error Device	16	l							communication cable from the device.						\perp		
Network Congestion Causing congestion by generating the communications staffic that exceeds the capacity of the device. We (Packet Filtering Type) Device Alive Monitoring that exceeds the capacity of the device. We (Packet Filtering Type) Device Alive Monitoring that exceeds the capacity of the device. We (Packet Filtering Type) Device Alive Monitoring that exceeds the capacity of the device. We (Packet Filtering Type) Device Alive Monitoring that exceeds the capacity of the device. We (Packet Filtering Type) Device Alive Monitoring that exceeds the capacity of the device. We (Packet Filtering Type) Device Alive Monitoring that exceeds the capacity of the device. We (Packet Filtering Type) Device Alive Monitoring that exceeds the capacity of the device. Not applicable (no functions) Jamming Interference with radio communications. Device Error Detection Redundancy Device Error Detection Device Error Detection Redundancy Device Alive Monitoring that exceeds the capacity of the device. Redundancy Device Alive Monitoring that exceeds the capacity of the device. Redundancy Device Alive Monitoring to packet Staffing that exceeds the capacity of the device. Redundancy Device Alive Monitoring to packet Staffing that exceeds the capacity of the device. Redundancy Device Error Detection Device Error Detectio															+		
That exceeds the capacity of the device. PM (Application Gateway Type) Device Alive Monitoring Make Make														GSIGH Detection Sensor	+		
That exceeds the capacity of the device. PM (Application Gateway Type) Device Alive Monitoring Device Alive Monitor		l				1		Network Congestion							R	Redundancy	
PSIDS DOS Countermeasures Not applicable (no functions) Jamming Interference with radio communications. Device Error Detection Redundancy Device Afree Monitoring Log Collection/Log Analysis Integrated Log Management System Encryption of Communications Channels Data Encryption Exclusive Line Unauthorized Modification of Maliciously modifying information flowing on the network. Encryption of Communications Channels Data Encryption Exclusive Line Unauthorized Modification of Maliciously modifying information flowing on the network. Encryption of Communications Channels Data Signature Exclusive Line Connecting unauthorized device on the network Restriction on Connecting Device and its Usage Log Collection/Log Analysis										FW (Application Gateway Type)					I		
Dos Countermeasures Dos Countermeasures Device Error Detection Redundancy	17														+		
Not applicable (no functions) Jamming Interference with radio communications. Device Airw Monitoring Device Airw Moni															+		
Device Alew Monitoring																	
Packet Sniffing Theft of information flowing on the network. Packet Sniffing Theft of information flowing on the network. Encryption of Communications Channels Data Encryption Exclusive Line Unauthorized Modification of Maliciously modifying information flowing on the network. Encryption of Communications Channels Log Collection/Log Analysis Data Signature Exclusive Line Connecting Unauthorized Connecting unauthorized device on the network Device Restriction on Connecting Device and its Usage Log Collection/Log Analysis		Not applicable (or for	unctions)					Jamming	Interference with radio communications.						R	Redundancy	
Packet Sniffing Theft of information flowing on the network. Encryption of Communications Channels Data Encryption Exclusive Line Unauthorized Modification of Maliciously modifying information flowing on the network. Encryption of Communications Channels Data Encryption Exclusive Line Unauthorized Modification of Maliciously modifying information flowing on the network. Communication Data Encryption of Communications Channels Data Signature Exclusive Line Connecting Unauthorized Connecting unauthorized device on the network Device Restriction on Connecting Device and its Usage Log Collection/Log Analysis	40	потаррисаріе (поти	21100113)												4		
Packet Sniffing Theft of information flowing on the network. Encryption of Communications Channels Data Encryption Exclusive Line Unauthorized Modification of Maliciously modifying information flowing on the network. Communication Data Encryption of Communications Channels Data Signature Exclusive Line Connecting Unauthorized Connecting unauthorized device on the network Device Restriction on Connecting Device and its Usage Log Collection/Log Analysis Log Collection/Log Analysis Log Collection/Log Analysis	18														+		
Data Encryption Exclusive Line Unauthorized Modification of Maliciously modifying information flowing on the network. Communication Data Connecting Unauthorized Connecting unauthorized device on the network Device Data Encryption Exclusive Line Encryption Encryption Encryption Exclusive Line Log Collection/Log Analysis Device Device Analysis Log Collection/Log Analysis														y me and me agent of stem	+		
Data Encryption Exclusive Line Unauthorized Modification of Maliciously modifying information flowing on the network. Communication Data Connecting Unauthorized Connecting unauthorized device on the network Device Data Encryption Exclusive Line Encryption Encr						1 1		Packet Sniffing	Theft of information flowing on the network.								
Exclusive Line Unauthorized Modification of Maliciously modifying information flowing on the network. Communication Data Connecting Unauthorized Connecting Unauthorized device on the network Device Exclusive Line Connecting Unauthorized device on the network Device Exclusive Line Connecting Unauthorized device on the network Log Collection/Log Analysis	19									Data Encryption					\Box		
Communication Data Data Signature Exclusive Line Connecting Unauthorized Connecting unauthorized device on the network Device Device Data Signature Exclusive Line Restriction on Connecting Device and its Usage Log Collection/Log Analysis										Exclusive Line					-		
Communication Data Data Signature Exclusive Line Connecting Unauthorized Connecting unauthorized device on the network Device Device Data Signature Exclusive Line Restriction on Connecting Device and its Usage Log Collection/Log Analysis						1 1		Unauthorized Modification of	Maliciously modifying information flowing on the network	Encryption of Communications Channels				Log Collection/Log Analysis	+		
Exclusive Line Connecting Unauthorized Connecting unauthorized device on the network Device Exclusive Line Restriction on Connecting Device and its Usage Log Collection/Log Analysis	20														1		
Device Log Collection/Log Analysis	20																
Device Log Collection/Log Analysis		l				ļ ļ		C	Constitution of the contract o	Destriction on Committee Desire				Destriction on Committee C	4		
									Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage					+		
	21														1		

	Lege	end: O Measures	implem	nentea	Gray	ed out I	ines: Threats no	t taken into account for the corres	ponding asset Green	tex				mati	ion on measures		
Item Number	Type of Assets	Target Device		sessment Me			Threat (Attack Type)	Description	Prote	ection			Detection/Understanding Dar	mane	Business Continuity		Security Level By Threat
			Threat Level	Vulnerability Level	Importance of Assets	Risk Value			Intrusion/Spreading Phase		Objective Achievement Phas	_	,	illaye	Business Continuity		
	Network Asset	Firewall					Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type)	0			IPS/IDS				
									FW (Application Gateway Type)	₩			Log Collection/Log Analysis			\rightarrow	
			l	1					One-way Gateway	-	+	_	Integrated Log Management System	\vdash			
									Proxy Server	_							
1			3	2		A			WAF Peer-to-Peer Authentication	-	+	_					2
										0	+	_					
									IPS/IDS	-		_				_	
									Applying Patches	0		_					
									Avoidance of Vulnerability	-	-	_				_	
					-		Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with	Entrance and Exit Management (IC Card, Biometric Authentication)	0	+	_	Surveillance Camera	0		_	
			١.	١.		l _	r ilysicai ilitrusiori	access restrictions.	Lock and Key Management	0			Intrusion Detection Sensor	0			
2			1	1		C		It also refers to removing restrictions on devices with physical access restrictions									3
								(devices installed in racks, cabinets, etc.).		_							
3			2	2		В	Unauthorized Operation	Intrusion through direct operation of the device's console or other component to execute an attack.	Operator Authentication (ID/Pass)	0	+	-				-	2
				1	1		Human Error in Operation	An attack triggered by a human error in operation by internal	URL Filtering/Web Reputation	_	+	_				-	
							Tiulilan Enor in Operation		Mail Filtering								
4			2	3		A		device).									1
			_	-				An act equivalent to an attack is performed on the device as a result									
								of a proper media or device connection.									
					1		Connecting Unauthorized	Connection of unauthorized media or device (CD/DVD, USB	Restriction on Connecting Device and its Usage		(Same as on the Left)		(Same as on the Left)				
5			2	3		A	Media or Device	device, etc.) brought in from outside the organization with the					Log Collection/Log Analysis				1
-			1	"		^		device to execute an attack.		_	+ -	_	Integrated Log Management System	_			.
				1	1				Deminsion Manager	<u> </u>	(Company on the Late)		Davies France Data Africa				
			l					Unauthorized execution of legitimate programs, commands,	Permission Management Access Control	F°	(Same as on the Left) (Same as on the Left)		Device Error Detection Device Alive Monitoring			\dashv	
6			,			В	Processes	services, and other processes found on the attack target	Application Whitelisting	1	(Same as on the Left)		Log Collection/Log Analysis			-	2
υ			2	2		•		device.	Approval of Important Operations	<u> </u>	(Same as on the Left)		Integrated Log Management System			-	4
			l								1 - Danie do di ale Leit)					\dashv	
				1	1		Malware Infection	Infection or running of malware (unauthorized programs) on	Anti-virus	_	+	-	Device Error Detection			\dashv	+
			l				maware micellon	the attack target device.	Application Whitelisting				Device Alive Monitoring				
_			Ι.	1 .		_		and any across.	Applying Patches				Log Collection/Log Analysis				. 1
7			1	3		В			Avoidance of Vulnerability				Integrated Log Management System			\neg	1
			l						Data Signature							\neg	
					1		Information Theft	Theft of information (software, authentication information,	Permission Management	0	(Same as on the Left)		Log Collection/Log Analysis				
								configuration settings, encryption keys and other confidential	Access Control	_	(Same as on the Left)		Integrated Log Management System				
8			1	2		C		information) stored on the device.	Data Encryption	_	(Same as on the Left)						2
									DLP	_	(Same as on the Left)						
									D	L.	(0		Davis - Farm Datasi's		Data Basilian		
								Unauthorized modification of information (software,	Permission Management Access Control	0	(Same as on the Left) (Same as on the Left)		Device Error Detection Log Collection/Log Analysis		Data Backup		
9			3	2		A	Information	authentication information, configuration settings, encryption		-	(Same as on the Left)	-				-	2
			l	1				keys and other confidential information) stored on the device.	Data Signature	1	(Jame as On the Left)		Integrated Log Management System			-	1
			\vdash	+	1	<u> </u>	Information Destruction	Destroying of information (software, authentication		-	Permission Management	-	Device Error Detection	\vdash	Data Backup	\dashv	
				1 .		_					Access Control		Log Collection/Log Analysis			\dashv	1
10			2	2		В		information, configuration settings, encryption keys and other confidential information) stored on the device.					Integrated Log Management System				2
								Confidential illionnation) stored on the device.									
					1		Unauthorized Transmission	Sending unauthorized control commands (settings changes,	Segmentation/Zoning		(Same as on the Left)		Log Collection/Log Analysis				
				١ .	3	_		power shutdowns, etc.) and unauthorized data to other	Data Signature		(Same as on the Left)		Integrated Log Management System				
11			1	3	"	В		devices.	Approval of Important Operations		(Same as on the Left)						1
							Outage	Stopping device functions.		_			Device Error Detection		Redundancy		
										├		_	Device Alive Monitoring		Failsafe Design		
12			2	3		A				_			Log Collection/Log Analysis				1
										-			Integrated Log Management System			-	
				1	1		DeC Attests	latere eties of secular device executions by seculing	DDoS Countermeasures	-	+	-	Device Error Detection		Redundancy	-	
							DoS Attack	Interruption of regular device operations by sending processing requests that exceed the processing capacity of	DDGG GGGRIGHTGGGGG	-			Device Alive Monitoring		Failsafe Design	\neg	
13			3	3		A		the device as a result of a DDoS attack, etc.					Log Collection/Log Analysis			\neg	1
			•	"		^		the device as a result of a DDo3 attack, etc.					Integrated Log Management System				
					1		Theft	Device theft.	Lock and Key Management	0	(Same as on the Left)		(Same as on the Left)				
14			1	2		С											2
			l													\neg	
					1		Information Theft by	Theft of information (software, authentication information,	Tamper Resistance		(Same as on the Left)						
15			1	2		С	Tampering Device at Time		Obfuscation	_	(Same as on the Left)						2
.5			١.	-			of Theft or Disposal	information) stored on devices which were stolen or disposed of and	Zeroization	0	(Same as on the Left)						-
				_	1		D. 1. Di. 11	then disassembled.					Douise Error Date (*		Podundancii		
					1			Communications are blocked by disconnecting the	Entrance and Exit Management (IC Card, Biometric Authentication) Lock and Key management	0			Device Error Detection Device Alive Monitoring		Redundancy		
					1			Communication Cable.					Log Collection/Log Analysis				
16					1			Alternatively, communications are blocked by pulling out the communication cable from the device.					Integrated Log Management System				
10								communication cause if Offi the device:					Surveillance Camera	0			
												_	Intrusion Detection Sensor	0			
					1												
					1		Network Congestion	Causing congestion by generating the communications traffic	FW (Packet Filtering Type)	0			Device Error Detection		Redundancy		
					1				FW (Application Gateway Type)				Device Alive Monitoring				
									WAF				Log Collection/Log Analysis				
17					1				IPS/IDS				Integrated Log Management System				
					1				DDoS Countermeasures								
	Notare li			•	-		Jamming	Interference with radio communications.					Device Error Detection		Redundancy		
	Not applicable (no fu	unctions)											Device Alive Monitoring				
18													Log Collection/Log Analysis				
													Integrated Log Management System				
					1		Packet Sniffing		Encryption of Communications Channels								
40									Data Encryption								
19					1				Exclusive Line								
					1												
					1		Unauthorized Modification of	Maliciously modifying information flowing on the network.	Encryption of Communications Channels				Log Collection/Log Analysis				
					1		Communication Data		Data Signature				Integrated Log Management System				
20					1				Exclusive Line								
					1		Connecting Unauthorized	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage				Restriction on Connecting Device and its Usage				
					1		Device						Log Collection/Log Analysis				
21					1								Integrated Log Management System				
					1												
_												_		_		-	

										Counterme	sures				Security Leve
Bem Number	Type of Assets	Target Device		Vulnerability Level	trics Importance of Assets	Risk Value	Threat (Attack Type)	Description	Prote Intrusion/Spreading Phase		Detection/Understanding Da	mage	Business Continuity		By Threat
1	Network Asset	Switch (within DMZ), DMZ					Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type)		IPS/IDS				
									FW (Application Gateway Type)		Log Collection/Log Analysis				
									One-way Gateway		Integrated Log Management System				
									Proxy Server WAF					$\overline{}$	
1			3	2		В			Peer-to-Peer Authentication					_	2
									IPS/IDS					\dashv	
									Applying Patches	0					
									Avoidance of Vulnerability					$\overline{}$	
									,					\neg	
					1		Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with access	Entrance and Exit Management (IC Card, Biometric Authentication)	0	Surveillance Camera	0			
2			1	1		D		It also refers to removing restrictions on devices with physical access restrictions (devices	Lock and Key management	0	Intrusion Detection Sensor	0			3
					1			Installed in racks, cabinets, etc.).	O A - th ti ti (ID ID)	_		_		_	
3			2	2		С	Unauthorized Operation	Intrusion through direct operation of the device's console or other component to execute an attack.	Operator Authentication (ID/Pass)	0				-	2
_					1		Human Error in Operation	An attack triggered by a human error in operation by internal	URL Filtering/Web Reputation						
								personnel (an employee or partner with access privileges to the	Mail Filtering						
4			2	3		В		device).							1
								An act equivalent to an attack is performed on the device as a result							
								of a proper media or device connection.							
							Connecting Unauthorized	Connection of unauthorized media or device (CD/DVD, USB	Restriction on Connecting Device and its Usage	(Same as on the Left)	(Same as on the Left)			_	
5			2	3		В		device, etc.) brought in from outside the organization with the			Log Collection/Log Analysis Integrated Log Management System			-	1
								device to execute an attack.			integrated Log Management System				
_			-		1		Cusa dias of Has dhadad	l landeninad avandina of lanitim de avances a comunado	Permission Management	(Same as on the Left)	Device Error Detection			-+	
								Unauthorized execution of legitimate programs, commands,	Access Control	(Same as on the Left)	Device Alive Monitoring			$\overline{}$	
6	- 1		2	2		С	Processes	services, and other processes found on the attack target device.	Application Whitelisting	(Same as on the Left)	Log Collection/Log Analysis			\neg	2
-	- 1		1 -	-		•			Approval of Important Operations	(Same as on the Left)	Integrated Log Management System				-
			1							1				\dashv	
\neg					1		Malware Infection	Infection or running of malware (unauthorized programs) on	Anti-virus		Device Error Detection				
	- 1							the attack target device.	Application Whitelisting		Device Alive Monitoring				
,			١.,			_			Applying Patches		Log Collection/Log Analysis				
′			1	3		C			Avoidance of Vulnerability		Integrated Log Management System	匚			1
	- 1								Data Signature						
							Information Theft	Theft of information (software, authentication information,	Permission Management	(Same as on the Left)	Log Collection/Log Analysis			-	
								configuration settings, encryption keys and other confidential	Access Control	(Same as on the Left)	Integrated Log Management System				
8			1	2		D		information) stored on the device.	Data Encryption	(Same as on the Left)					2
									DLP	(Same as on the Left)		_		-	
_					4				Demississ Massausst	(Company the Left)	Davies Free Datestics		Data Backup	_	
								Unauthorized modification of information (software,	Permission Management Access Control	(Same as on the Left) (Same as on the Left)	Device Error Detection Log Collection/Log Analysis		Бага Баскир	\dashv	
9			3	2		В		authentication information, configuration settings, encryption	Data Signature	(Same as on the Left)	Integrated Log Management System			\dashv	2
								keys and other confidential information) stored on the device.	Data Signature	(Same as on the Left)	integrated bog management by stem			_	
			_		1		Information Destruction	Destroying of information (software, authentication		Permission Management	Device Error Detection		Data Backup		
			١.			_	IIIIOIIIIaboii Desti uctioii	information, configuration settings, encryption keys and other		Access Control	Log Collection/Log Analysis				
10			2	2		С		confidential information) stored on the device.			Integrated Log Management System				2
								confidential illumation) stored on the device.							
					1		Unauthorized Transmission	Sending unauthorized control commands (settings changes,	Segmentation/Zoning	(Same as on the Left)	Log Collection/Log Analysis				
11			1	3		С		power shutdowns, etc.) and unauthorized data to other	Data Signature	(Same as on the Left)	Integrated Log Management System				4
"			l '	"	2	"		devices.	Approval of Important Operations	(Same as on the Left)					'
					1						Decision Francisco		Dedender		
							Outage	Stopping device functions.			Device Error Detection Device Alive Monitoring		Redundancy Failsafe Design	\dashv	
12				3		В					Log Collection/Log Analysis		r alisale Design	$\overline{}$	1
12			2	*		°					Integrated Log Management System			-	'
											integrated Edg management dystem			\dashv	
$\overline{}$			_		1		DoS Attack	Interruption of regular device operations by sending	DDoS Countermeasures		Device Error Detection		Redundancy		
								processing requests that exceed the processing capacity of			Device Alive Monitoring		Failsafe Design		
13			3	3		В		the device as a result of a DDoS attack, etc.			Log Collection/Log Analysis				1
								,			Integrated Log Management System				
							Theft	Device theft.	Lock and Key Management	 (Same as on the Left) 	(Same as on the Left)				
14	[1	2		D					I	1			2
	[1	I		1	ı				i I		
						_		W 6 414 11 1 6 1 1 1 1 1 1 1 1 1 1 1 1 1	Tomass Decistores	(Sama as as the Left)					
							Information Theft by	Theft of information (software, authentication information,	Tamper Resistance	(Same as on the Left)				-	
15	[1	2		D	Tampering Device at Time	configuration settings, encryption keys and other confidential	Obfuscation	(Same as on the Left)				=	2
15			1	2					Obfuscation						2
15			1	2	_		Tampering Device at Time of Theft or Disposal	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Obfuscation Zeroization	(Same as on the Left)	Device Error Detection		Redundancy		2
15			1	2	_		Tampering Device at Time of Theft or Disposal Route Blocking	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the	Obfuscation	(Same as on the Left)	Device Error Detection Device Alive Monitoring		Redundancy		2
15			1	2			Tampering Device at Time of Theft or Disposal Route Blocking	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable.	Obfuscation Zeroization Entrance and Exit Management (IC Card, Biometric Authentication)	(Same as on the Left) (Same as on the Left)			Redundancy		2
15			2	2	-		Tampering Device at Time of Theft or Disposal Route Blocking	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the	Obfuscation Zeroization Entrance and Exit Management (IC Card, Biometric Authentication)	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy		3
15					_	_	Tampering Device at Time of Theft or Disposal Route Blocking	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the	Obfuscation Zeroization Entrance and Exit Management (IC Card, Biometric Authentication)	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera	0	Redundancy		3
15						_	Tampering Device at Time of Theft or Disposal Route Blocking	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the	Obfuscation Zeroization Entrance and Exit Management (IC Card, Biometric Authentication)	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	0	Redundancy		3
15						_	Tampering Device at Time of Theft or Disposal Route Blocking	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Obfuscation Zeroization Strates and Est Management IC Cost. Sometic Advantagement Lock and Key management	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor	0			3
16						_	Tampering Device at Time of Theft or Disposal Route Blocking	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic	Obfuscation Zeroization Entering and Est Management IC Cost. Remote Atherisative Lock and Key management FW (Packet Filtering Type)	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection	0	Redundancy		3
15					_	_	Tampering Device at Time of Theft or Disposal Route Blocking	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Obfuscation Zeroization Setroization Extrace and Est Management (C Cart. Biometric Authoritisation) Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type)	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Managemer System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring	0 0			3
16			2	1		D	Tampering Device at Time of Theft or Disposal Route Blocking	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Obfuscation Zeroization demand and list Meagament (C Cast. Biometic Authoritoston). Lock and Key management FW (Packet Filtering Type) FW (Packet Filtering Type) FW (Application Gateway Type) WAF	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	0			3
						_	Tampering Device at Time of Theft or Disposal Route Blocking	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Obfuscation Zeroization Sensure and Est Management IC Cost. Biometic Authoritostock. Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/IDS	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Managemer System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring	0			3
			2	1		D	Tampering Device at Time of Theft or Disposal Route Blocking	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Obfuscation Zeroization demand and list Meagament (C Cast. Biometic Authoritoston). Lock and Key management FW (Packet Filtering Type) FW (Packet Filtering Type) FW (Application Gateway Type) WAF	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	0 0			3
			2	1		D B	Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Obfuscation Zeroization Sensure and Est Management IC Cost. Biometic Authoritostock. Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/IDS	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	0	Redundancy		3
17	iotapplicable (no furn	nctions)	2	1		D B	Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Obfuscation Zeroization Sensure and Est Management IC Cost. Biometic Authoritostock. Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/IDS	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection	0			3
17 N	iot applicable (no fun	nctions)	2	1		D B	Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Obfuscation Zeroization Sensure and Est Management IC Cost. Biometic Authoritostock. Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/IDS	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring	0	Redundancy		3
17	lot applicable (no fur	nctions)	2	1		D B	Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Obfuscation Zeroization Sensure and Est Management IC Cost. Biometic Authoritostock. Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/IDS	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Sensor Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	0	Redundancy		3
17 N	iot applicable (no furi	nctions)	2	1		D B	Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Obfuscation Zeroization Sensure and Est Management IC Cost. Biometic Authoritostock. Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/IDS	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring	0	Redundancy		3
17 N	iot applicable (no furi	nctions)	2	1		D B	Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Obfuscation Zeroization General and Est Management (C.Cast. Research Annurrouter) Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Sensor Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	0	Redundancy		3
17 N	lot applicable (no fur	nctions)	2	1		D B	Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Obfuscation Zeroization Enterest and Est Management (C Cast. Remarks Authorite study). Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/IDS DDoS Countermeasures Encryption of Communications Channels	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Sensor Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	0	Redundancy		3
17 N	iotapplicable (no fur	nctions)	2	1	-	D B	Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Obfuscation Zeroization Intranse and Est Management (**Cost. Biometic Authoritosteck Lock and Key management** FW (Packet Filtering Type) FW (Application Gateway Type) WAF PPS/IDS DDoS Countermeasures Encryption of Communications Channels Data Encryption	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Sensor Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	0	Redundancy		3 1 1
17 N	iot applicable (no fur	nctions)	2 2	3		D B	Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Obfuscation Zeroization Enterest and Est Management (C Cast. Remarks Authorite study). Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/IDS DDoS Countermeasures Encryption of Communications Channels	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Sensor Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	0	Redundancy		1
17 N	lot applicable (no fun	nctions)	2 2	3		D B	Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications.	Obfuscation Zeroization Generate and list Management IC Cost. Binaries Authoriteation Lock and Key management EW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/IDS DDoS Countermeasures Encryption of Communications Channels Data Encryption Exclusive Line	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Sensor Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	0	Redundancy		1
17 N	iot applicable (no fur	nctions)	2 2	3	-	D B	Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications.	Obfuscation Zeroization Zeroization Continues and Est Management Coast, Biometic Authoritostees Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PPS/IDS DOS Countermeasures Encryption of Communications Channels Data Encryption Exclusive Line Encryption of Communications Channels	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Log Collection/Log Analysis Integrated Log Management System	0	Redundancy		1
17 N 18 19	lot applicable (no fur	nctions)	2 2	3		D B	Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications.	Obfuscation Zeroization Zeroization Generate and fet Management (C Cast. Remarks Authorization) Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures Encryption of Communications Channels Data Encryption Exclusive Line Encryption of Communications Channels Data Signature	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Sensor Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	0	Redundancy		1
17 N	lot applicable (no fun	nctions)	2 2	3	-	D B	Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications.	Obfuscation Zeroization Zeroization Continues and Est Management Coast, Biometic Authoritostees Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PPS/IDS DOS Countermeasures Encryption of Communications Channels Data Encryption Exclusive Line Encryption of Communications Channels	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Log Collection/Log Analysis Integrated Log Management System	0	Redundancy		1
17 N 18 N 19	iot applicable (no furi	nctions)	2 2	3		D B	Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of Communication Data	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications. Theft of information flowing on the network. Maliciously modifying information flowing on the network.	Obfuscation Zeroization Zeroization Lock and Key management Enter a set list Management (C.Cast. Remarks Authorization) Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures Encryption of Communications Channels Data Encryption Exclusive Line Encryption of Communications Channels Data Signature Exclusive Line	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	0	Redundancy		1
17 N 18 N 19	lot applicable (no fur	nctions)	2 2	3		D B	Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of Communication Data Connecting Unauthorized	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications.	Obfuscation Zeroization Zeroization Generate and fet Management (C Cast. Remarks Authorization) Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures Encryption of Communications Channels Data Encryption Exclusive Line Encryption of Communications Channels Data Signature	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Log Collection/Log Analysis Integrated Log Management System Integrated Log Management System Integrated Log Management System	0 0	Redundancy		1
17 N 18 20	tot applicable (no fun	nctions)	2 2 2	3		D B	Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of Communication Data	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications. Theft of information flowing on the network. Maliciously modifying information flowing on the network.	Obfuscation Zeroization Zeroization Lock and Key management Enter a set list Management (C.Cast. Remarks Authorization) Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures Encryption of Communications Channels Data Encryption Exclusive Line Encryption of Communications Channels Data Signature Exclusive Line	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Log Collection/Log Analysis Integrated Log Management System Log Collection/Log Analysis Integrated Log Management System Authorized Log Management System Authorized Log Management System Authorized Log Management System Log Collection/Log Analysis	0	Redundancy		1
17 N 18 N 19	iotapplicable (no fur	nctions)	2 2	3		D B	Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of Communication Data Connecting Unauthorized	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications. Theft of information flowing on the network. Maliciously modifying information flowing on the network.	Obfuscation Zeroization Zeroization Lock and Key management Enter a set list Management (C.Cast. Remarks Authorization) Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures Encryption of Communications Channels Data Encryption Exclusive Line Encryption of Communications Channels Data Signature Exclusive Line	(Same as on the Left) (Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Log Collection/Log Analysis Integrated Log Management System Integrated Log Management System Integrated Log Management System	0 0	Redundancy		1

											Counterm	neasures		Security L
m Number	Type of Assets	Target Device		sessment Me			Threat (Attack Type)	Description	Prote	ection		Detection/Understanding Damage	e Business Continuity	By Thre
	Control System Asset	Data Historian (Balay)	Threat Level	Vulnerability Level	Importance of Assets	Risk Value	Heartherinad Assess	hateraine of the devices in the natural, to account an attack	Intrusion/Spreading Phase		Objective Achievement Pha	ase		
١	Control System Asset	Data Historian (Relay)					Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type) FW (Application Gateway Type)			IPS/IDS Log Collection/Log Analysis		-
									One-way Gateway			Integrated Log Management System	+	\dashv
									Proxy Server			incgrace Eng management by Stein		-
.				١.		_			WAF					٠,
1			3	2		В			Peer-to-Peer Authentication	0				2
									IPS/IDS					
									Applying Patches (Web Server Only)	0				
									Avoidance of Vulnerability					
_				١.,		D	Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with access restrictions.	Entrance and Exit Management (IC Card, Biometric Authentication) Lock and Key management	0		Surveillance Camera Intrusion Detection Sensor O	+ +	- ,
2			1	1		٠,		It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).	Lock and Key management	Ť		Intrusion Detection Sensor	+	3
				 	1		Unauthorized Operation	Intrusion through direct operation of the device's console or other	Operator Authentication (ID/Pass)	0				
3			2	2		С		component to execute an attack.						2
							Human Error in Operation	An attack triggered by a human error in operation by internal	URL Filtering/Web Reputation	_				_
.								personnel (an employee or partner with access privileges to the device).	Mail Filtering	_				
4			2	3		В		An act equivalent to an attack is performed on the device as a result		_			+	⊣ '
								of a proper media or device connection.		_				_
-			-	<u> </u>	1		Connecting Unauthorized	Connection of unauthorized media or device (CD/DVD, USB	Restriction on Connecting Device and its Usage		(Same as on the Left)	Restriction on Connecting Device and its Usage		
_						_		device, etc.) brought in from outside the organization with the				Log Collection/Log Analysis		
٥			2	3		В		device to execute an attack.				Integrated Log Management System		1
							Execution of Unauthorized	Unauthorized execution of legitimate programs, commands,	Permission Management	0	(Same as on the Left)	Device Error Detection	+	_
			_	_		_		services, and other processes found on the attack target	Access Control	 	(Same as on the Left)	Device Alive Monitoring	+	- _
,			2	2		С		device.	Application Whitelisting Approval of Important Operations	-	(Same as on the Left) (Same as on the Left)	Log Collection/Log Analysis Integrated Log Management System	+	2
				1					Approval of important Operations	<u> </u>	(Codine as On the Left)	inegrated Log management System	+	\dashv
\dashv				 	1		Malware Infection	Infection or running of malware (unauthorized programs) on	Anti-virus	0		Device Error Detection	+	_
				1				Intection or running of maiware (unauthorized programs) on the attack target device.	Application Whitelisting			Device Alive Monitoring		\neg
,			_	_		_		and the second s	Applying Patches			Log Collection/Log Analysis		
′			3	2		В			Avoidance of Vulnerability			Integrated Log Management System		2
									Data Signature					
			<u></u>	<u></u>										
٦							Information Theft	Theft of information (software, authentication information,	Permission Management	0	(Same as on the Left)	Log Collection/Log Analysis		
_				١.		_		configuration settings, encryption keys and other confidential	Access Control	<u> </u>	(Same as on the Left)	Integrated Log Management System		-
8			3	2		В		information) stored on the device.	Data Encryption DLP	_	(Same as on the Left)		+	_ 2
									DLP	\vdash	(Same as on the Left)		+ +	-
-				_	1		I Inauthorized Modification of	Unauthorized modification of information (software,	Permission Management	0	(Same as on the Left)	Device Error Detection	Data Backup	0
.				١.		_		authentication information, configuration settings, encryption	Access Control		(Same as on the Left)	Log Collection/Log Analysis	1	T .
9			3	2		В		keys and other confidential information) stored on the device.	Data Signature		(Same as on the Left)	Integrated Log Management System		2
								,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,						
							Information Destruction	Destroying of information (software, authentication		_	Permission Management	Device Error Detection	Data Backup	0
10			3	2		В		information, configuration settings, encryption keys and other		<u> </u>	Access Control	Log Collection/Log Analysis	+	
								confidential information) stored on the device.		_		Integrated Log Management System		_
-			-		-		I Inquithorized Transmission	Sonding upputhorized control commands (sottings changes	Segmentation/Zoning	_	(Same as on the Left)	Log Collection/Log Analysis	+	_
								Sending unauthorized control commands (settings changes, power shutdowns, etc.) and unauthorized data to other	Data Signature		(Same as on the Left)	Integrated Log Management System		
11			3	3	2	В		devices.	Approval of Important Operations		(Same as on the Left)			1
								uevices.	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		, , , , , , , , , , , , , , , , , , , ,			
					1		Outage	Stopping device functions.				Device Error Detection	Redundancy	
										_		Device Alive Monitoring	Failsafe Design	
12			3	3		В				<u> </u>		Log Collection/Log Analysis		1
										_		Integrated Log Management System		
					-		D.O.Allest	haloman distriction of the state of the stat	DDoS Countermoscures	_		Davisa Error Datastica	Podundonov	_
								Interruption of regular device operations by sending	DDoS Countermeasures			Device Error Detection Device Alive Monitoring	Redundancy Failsafe Design	-
13			1	3		С		processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.				Log Collection/Log Analysis	T amount a congre	1
.				•		•		the device as a result of a DDo3 attack, etc.				Integrated Log Management System		
					1		Theft	Device theft.	Lock and Key Management	0	(Same as on the Left)	(Same as on the Left)		
14			1	2		D								2
				_	1	_		Theft of information (software, authentication information,						
15									Tamper Resistance		(Same as on the Left)			_
1			1	2		D		configuration settings, encryption keys and other confidential	Obfuscation Zeroization		(Same as on the Left) (Same as on the Left)			2
- 1			1	2		D	of Theft or Disposal	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed	Obfuscation Zeroization	0	(Same as on the Left)			2
			1	2			of Theft or Disposal	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Obfuscation Zeroization	0	(Same as on the Left)	Daving Free Dates:	Reduction	2
			1	2			of Theft or Disposal Route Blocking	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the	Obfuscation Zeroization Entrance and Exit Management	0	(Same as on the Left)	Device Error Detection	Redundancy	2
			1	2	_		of Theft or Disposal Route Blocking	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable.	Obfuscation Zeroization	0	(Same as on the Left)	Device Alive Monitoring	Redundancy	2
16			1	2			of Theft or Disposal Route Blocking	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the	Obfuscation Zeroization Entrance and Exit Management	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis	Redundancy	2
16			1	2			of Theft or Disposal Route Blocking	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable.	Obfuscation Zeroization Entrance and Exit Management	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Redundancy	2
16			1	2			of Theft or Disposal Route Blocking	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the	Obfuscation Zeroization Entrance and Exit Management	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis	Redundancy	2
16			1	2			of Theft or Disposal Route Blocking	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the	Obfuscation Zeroization Entrance and Exit Management	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera	Redundancy	2
16			1	2			of Theft or Disposal Route Blocking	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the	Obfuscation Zeroization Entrance and Exit Management Lock and Key management	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera	Redundancy Redundancy	2
16			1	2			of Theft or Disposal Route Blocking Network Congestion	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Othuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type)	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor		2
			1	2			of Theft or Disposal Route Blocking Network Congestion	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Othuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis		2
			1	2			of Theft or Disposal Route Blocking Network Congestion	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Carmera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring		2
			1	2			of Theft or Disposal Route Blocking Network Congestion	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Othuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis		2
			1	2			of Theft or Disposal Route Blocking Network Congestion	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Carmera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Redundancy	2
			1	2			of Theft or Disposal Route Blocking Network Congestion	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Carmera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection		2
7			1	2	-		of Theft or Disposal Route Blocking Network Congestion	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated tog Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring	Redundancy	2
7			1	2			of Theft or Disposal Route Blocking Network Congestion	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis University of the Collection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	Redundancy	2
17			1	2			of Theft or Disposal Route Blocking Network Congestion	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated tog Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring	Redundancy	2
17	Not applicable in of the Not applicable in order	nortions	1	2	-		of Theft or Disposal Route Blocking Network Congestion Jamming	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device.	Othuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis University of the Collection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	Redundancy	2
17	Not applicable (no fu	inctions)	1	2	-		of Theft or Disposal Route Blocking Network Congestion	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications.	Obfuscation Zeroization Entrance and Exit Management Lock and Key management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/IDS DDoS Countermeasures Encryption of Communications Channels	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis University of the Collection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	Redundancy	2
17	Not applicable (no fu	unctions)	1	2	-		of Theft or Disposal Route Blocking Network Congestion Jamming	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications.	Othuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis University of the Collection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	Redundancy	2
17	Not applicable (no fu	inctions)	1	2	-		of Theft or Disposal Route Blocking Network Congestion Jamming	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications.	Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS Dos Countermeasures Encryption of Communications Channels Data Encryption	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis University of the Collection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	Redundancy	2
17	Not applicable (no fu	inctions)	1	2	-		of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications.	Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS Dos Countermeasures Encryption of Communications Channels Data Encryption	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis University of the Collection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	Redundancy	2
117	Not applicable (no fu	inctions)	1	2			of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications.	Obfuscation Zeroization Entrance and Exit Management Lock and Key management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures Encryption of Communications Channels Data Encryption of Communications Channels Data Signature	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis strepated Log Management System Surveillance Camera intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis stregated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis stregated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis stregated Log Management System	Redundancy	2
17 18 19 20	Not applicable (no fu	inctions)	1	2			of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications.	Othuscation Zeroization Entrance and Exit Management Lock and Key management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures Encryption of Communications Channels Data Encryption Exclusive Line Encryption of Communications Channels	0	(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated tog Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Use Collection/Log Analysis Integrated Log Management System Log Collection/Log Analysis Integrated Log Management System Log Collection/Log Analysis	Redundancy	2
117	Not applicable (no fu	unctions)	1	2			of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of Communication Data	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communications are blocked by pulling out the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications. Theft of information flowing on the network.	Othuscation Zeroization Entrance and Exit Management Lock and Key management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures Encryption of Communications Channels Data Encryption Exclusive Line Encryption of Communications Channels Data Signature Exclusive Line		(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Uniformatical System Log Collection/Log Analysis Integrated Log Management System Log Collection/Log Analysis Integrated Log Management System	Redundancy	2
117	Not applicable (no fu	inctions)	1	2	-		of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of Communication Data Connecting Unauthorized	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications.	Obfuscation Zeroization Entrance and Exit Management Lock and Key management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures Encryption of Communications Channels Data Encryption of Communications Channels Data Signature		(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Log Collection/Log Analysis Integrated Log Management System Log Collection/Log Analysis Integrated Log Management System Matricton or Circuiting Device and to Liveye Matricton or Circuiting Device and to Liveye Matricton or Circuiting Device and to Liveye Matricton or Circuiting Device and to Liveye	Redundancy	2
117	Not applicable (no fu	inctions)	1	2			of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of Communication Data	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communications are blocked by pulling out the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications. Theft of information flowing on the network.	Othuscation Zeroization Entrance and Exit Management Lock and Key management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures Encryption of Communications Channels Data Encryption Exclusive Line Encryption of Communications Channels Data Signature Exclusive Line		(Same as on the Left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Uniformatical System Log Collection/Log Analysis Integrated Log Management System Log Collection/Log Analysis Integrated Log Management System	Redundancy	2

_	==90.							iken into account for the correspon			Countern						Security Level
item Numbe	Type of Assets	Target Device		sessment Met			Threat (Attack Type)	Description		ection			Detection/Understanding Da	mage	Business Continuity		By Threat
	Control System Asset	Data Historian	Threat Level	Vulnerability Level	Importance of Assets		Unauthorized Access	Intrusion of the device via the network to execute an	Intrusion/Spreading Phase FW (Packet Filtering Type)		Objective Achievement Ph		IPS/IDS	1			
	Control System Asset	Data Historian					Unauthorized Access	attack.	FW (Application Gateway Type)				Log Collection/Log Analysis				
								audor.	One-way Gateway				Integrated Log Management System				
									Proxy Server								
1			2	2		С			WAF								2
'			_	-		-			Peer-to-Peer Authentication IPS/IDS	0							-
									Applying Patches					_			
									Avoidance of Vulnerability								
	1				[Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.)		0			Surveillance Camera	0			
2			1	1		D		with access restrictions. It also refers to removing restrictions on devices with physical access	Lock and Key management	٥			Intrusion Detection Sensor	0		-	3
]							restrictions (devices installed in racks, cabinets, etc.).									
3			2	2		С	Unauthorized Operation	Intrusion through direct operation of the device's console or other component to execute an attack.	Operator Authentication (ID/Pass)	0				_		-	2
	·						Human Error in Operation	An attack triggered by a human error in operation by internal personnel	URL Filtering/Web Reputation			_		\vdash		-	
							Transaction in operation	(an employee or partner with access privileges to the device).	Mail Filtering								
4			2	3		В		An act equivalent to an attack is performed on the device as a result of a proper media or device connection.									1
								proper media or device definedation.									
-	-						Connecting Unauthorized Media or Device	Connection of unauthorized media or device (CD/DVD, USB device, etc.)	Restriction on Connecting Device and its Usage		(Same as on the Left)		(Same as on the Left)		-		
						_		brought in from outside the organization with the device to execute an	restriction on connecting Bevice and its esage		(Carrie do Ori dio Eori)		Log Collection/Log Analysis				
5			2	3		В		attack.					Integrated Log Management System				1
	ļ				ı L												
1				1	[Execution of Unauthorized Processes	Unauthorized execution of legitimate programs, commands, services, and other processes found on the attack target device.	Permission Management Access Control	0	(Same as on the Left) (Same as on the Left)		Device Error Detection Device Alive Monitoring	-	 	\dashv	1
6			2	2		С		and a processor work on the disask target DEVICE.	Application Whitelisting	0	(Same as on the Left) (Same as on the Left)		Log Collection/Log Analysis	_		\dashv	2
ľ			*	1		-			Approval of Important Operations		(Same as on the Left)		Integrated Log Management System				-
L]																
]				ı İ	_	Malware Infection	Infection or running of malware (unauthorized programs) on the attack	Anti-virus				Device Error Detection				
								target device.	Application Whitelisting	0			Device Alive Monitoring	-		\dashv	
7			3	2		В			Applying Patches Avoidance of Vulnerability	_			Log Collection/Log Analysis Integrated Log Management System	_		-	2
									Data Signature				===ograteu Log management System	\vdash		-	
									Sub Signature							\dashv	
	1						Information Theft	Theft of information (software, authentication information, configuration	Permission Management	0	(Same as on the Left)		Log Collection/Log Analysis				
				.		_		settings, encryption keys and other confidential information) stored on the device.			(Same as on the Left)		Integrated Log Management System	<u> </u>			
8			3	2		В			Data Encryption DLP		(Same as on the Left) (Same as on the Left)						2
									DLP		(Same as on the Lett)						
	1						Unauthorized Modification of Information	Unauthorized modification of information (software, authentication	Permission Management	0	(Same as on the Left)		Device Error Detection		Data Backup	0	
١,								information, configuration settings, encryption keys and other confidential	Access Control		(Same as on the Left)		Log Collection/Log Analysis				2
9			3	2		В		information) stored on the device.	Data Signature		(Same as on the Left)		Integrated Log Management System				2
											Darminaina Managamant		Device Franches		Data Bashus	_	
							Information Destruction	Destroying of information (software, authentication information, configuration settings, encryption keys and other confidential information)			Permission Management Access Control	0	Device Error Detection Log Collection/Log Analysis	\vdash	Data Backup	_	
10			3	2		В		stored on the device.			7 LOCOS CONTO		Integrated Log Management System				2
	1						Unauthorized Transmission	Sending unauthorized control commands (settings changes, power	Segmentation/Zoning		(Same as on the Left)		Log Collection/Log Analysis				
11			3	3	2	В		shutdowns, etc.) and unauthorized data to other devices.	Data Signature		(Same as on the Left)		Integrated Log Management System				1
									Approval of Important Operations		(Same as on the Left)			-			
	-						Outage	Stopping device functions.					Device Error Detection		Redundancy		
							Cuago						Device Alive Monitoring		Failsafe Design		
12			3	3		В							Log Collection/Log Analysis				1
													Integrated Log Management System				
	-						DoS Attack	Interruption of regular device operations by sending processing requests	DDoS Countermeasures				Device Error Detection		Redundancy		
								that exceed the processing capacity of the device as a result of a DDoS					Device Alive Monitoring		Failsafe Design		
13			1	3		С		attack, etc.					Log Collection/Log Analysis				1
													Integrated Log Management System	_			
	.						Theft	Device theft.	Last and Kar Management		(Company on the Left)		(Come on an the Left)				
14			1	2		D	Theft		Lock and Key Management	-	(Same as on the Left)		(Same as on the Left)			-	2
1				-		-										\dashv	
	1						Information Theft by Tangering Device at Time of Theft or Deposit	Theft of information (software, authentication information, configuration	Tamper Resistance		(Same as on the Left)						
15			1	2		D		settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Obfuscation	<u> </u>	(Same as on the Left)			_		-	2
				-				and the state of t	Zeroization	°	(Same as on the Left)						
							Route Blocking	Communications are blocked by disconnecting the communication cable.	Entrance and Exit Management				Device Error Detection		Redundancy		
								Alternatively, communications are blocked by pulling out the	Lock and Key management				Device Alive Monitoring				
								communication cable from the device.					Log Collection/Log Analysis				
16													Integrated Log Management System Surveillance Camera				
													Intrusion Detection Sensor				
	1						Network Congestion	Causing congestion by generating the communications traffic that	FW (Packet Filtering Type)				Device Error Detection		Redundancy		
								exceeds the capacity of the device.	FW (Application Gateway Type)				Device Alive Monitoring				
17									WAF				Log Collection/Log Analysis				
									IPS/IDS DDoS Countermeasures				Integrated Log Management System				
									DDGS Countermeasures								
	1		H	-			Jamming	Interference with radio communications.					Device Error Detection		Redundancy		
	Not applicable (no fu	nctions)					, i						Device Alive Monitoring				
18													Log Collection/Log Analysis				
													Integrated Log Management System				
				_	-												
							Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels								
19									Data Encryption Exclusive Line								
									LAGIOSIVE LINE								
							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				
20									Exclusive Line								
	ļ				l L												
					[Connecting Unauthorized Device	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage				Restriction on Connecting Device and its Usage				
21													Log Collection/Log Analysis				
													Integrated Log Management System				

					,-			taken into account for the corresp								-	
llem Number	Type of Assets	Target Device		sessment Me			Threat (Attack Type)	Description		ection	Countern		es Detection/Understanding Da	mane	Business Continuity		y Threat
	Make and A	Quiltab (In Quarter)	Threat Level	Vulnerability Level	Importance of Assets	Risk Value		lateration of the decises of the section of	Intrusion/Spreading Phase		Objective Achievement Ph	se		aye	Duamos Continuity		
	Network Asset	Switch (in Control Network					Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type)	_			IPS/IDS			_	
		(Information Side)), Control Network (Information Side)							FW (Application Gateway Type) One-way Gateway	\vdash			Log Collection/Log Analysis Integrated Log Management System			-	
		THE WORK (IIIIOTIII audit Olde)							Proxy Server								
1			2	2		С			WAF								2
'			1	-		"			Peer-to-Peer Authentication	0							2
									IPS/IDS								
									Applying Patches	_							
									Avoidance of Vulnerability	⊢		_				\dashv	
					1		Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with access	Entrance and Exit Management (IC Card)	0			Surveillance Camera	0			
2			1	2		D	,	restrictions. It also refers to removing restrictions on devices with physical access restrictions (devices	Lock and Key Management	0			Intrusion Detection Sensor	0			2
								Installed in racks, cabinets, etc.).									
3			2	2		С	Unauthorized Operation	Intrusion through direct operation of the device's console or other	Operator Authentication (ID/Pass)	0		_				_	2
					1		Human Error in Operation	component to execute an attack. An attack triggered by a human error in operation by internal	URL Filtering/Web Reputation	-		_				_	
							Truman Error in Operation	personnel (an employee or partner with access privileges to the	Mail Filtering								
4			2	3		В		device).									1
								An act equivalent to an attack is performed on the device as a result									
					1			of a proper media or device connection.	Destruition of Committee Desire and its University		(0		(0				
							Connecting Unauthorized	Connection of unauthorized media or device (CD/DVD, USB	Restriction on Connecting Device and its Usage		(Same as on the Left)		(Same as on the Left) Log Collection/Log Analysis			_	
5			2	3		В	Media or Device	device, etc.) brought in from outside the organization with the					Integrated Log Management System			_	1
								device to execute an attack.									
					1		Execution of Unauthorized	Unauthorized execution of legitimate programs, commands,	Permission Management	0	(Same as on the Left)		Device Error Detection				
							Processes	services, and other processes found on the attack target	Access Control		(Same as on the Left)		Device Alive Monitoring			_	
6			1	2		D		device.	Application Whitelisting	-	(Same as on the Left)		Log Collection/Log Analysis			\dashv	2
1									Approval of Important Operations	\vdash	(Same as on the Left)		Integrated Log Management System			\dashv	- 1
\vdash			—		1		Malware Infection	Infection or running of malware (unauthorized programs) on	Anti-virus	\vdash		-	Device Error Detection			+	
								the attack target device.	Application Whitelisting				Device Alive Monitoring				- 1
7			.			_			Applying Patches				Log Collection/Log Analysis				, I
/			'	3		С			Avoidance of Vulnerability				Integrated Log Management System				1
									Data Signature	$\overline{}$]					1
<u> </u>					1		lefe	The first construction (see from the construction)	Permission Managers	_	(Como ao ao tha Laft)		Log Collection/Log Application	\vdash		\perp	
							Information Theft	Theft of information (software, authentication information,	Permission Management Access Control	l °	(Same as on the Left) (Same as on the Left)		Log Collection/Log Analysis Integrated Log Management System			\dashv	- 1
8			1	2		D		configuration settings, encryption keys and other confidential information) stored on the device.	Data Encryption	_	(Same as on the Left)					-	2
"			l .	-		-		illiornation) stored on the device.	DLP		(Same as on the Left)						-
]		Unauthorized Modification of	Unauthorized modification of information (software,	Permission Management	0	(Same as on the Left)		Device Error Detection		Data Backup		
9			2	2		С	Information	authentication information, configuration settings, encryption	Access Control		(Same as on the Left)	_	Log Collection/Log Analysis			_	2
								keys and other confidential information) stored on the device.	Data Signature	-	(Same as on the Left)		Integrated Log Management System			-	
					1		Information Destruction	Destroying of information (software, authentication		\vdash	Permission Management	_	Device Error Detection		Data Backup		
10			١,	2		С		information, configuration settings, encryption keys and other			Access Control	0	Log Collection/Log Analysis				2
10			2	4		١ ٠		confidential information) stored on the device.					Integrated Log Management System				2
									0		(0		Landa Barbarda and Arabara				
							Unauthorized Transmission	Sending unauthorized control commands (settings changes,	Segmentation/Zoning Data Signature	-	(Same as on the Left) (Same as on the Left)	-	Log Collection/Log Analysis Integrated Log Management System			-	
11			1	3	2	С		power shutdowns, etc.) and unauthorized data to other devices.	Approval of Important Operations	\vdash	(Same as on the Left)		micgrated Log management dystem			_	1
								devices.			(
					1		Outage	Stopping device functions.					Device Error Detection		Redundancy		
										_			Device Alive Monitoring		Failsafe Design	_	
12			2	3		В				_			Log Collection/Log Analysis			_	1
										\vdash		_	Integrated Log Management System			\dashv	
					1		DoS Attack	Interruption of regular device operations by sending	DDoS Countermeasures				Device Error Detection		Redundancy		
								processing requests that exceed the processing capacity of					Device Alive Monitoring		Failsafe Design		
13			3	3		В		the device as a result of a DDoS attack, etc.					Log Collection/Log Analysis				1
										_			Integrated Log Management System			_	
\vdash					-		TheA	Device that	Last and Kar Massaures	_	(Same as on the Left)	_	Last and Var. Management				
14			1	2		D	Theft	Device theft.	Lock and Key Management	۲	(Gaine as on the Left)		Lock and Key Management	<u> </u>		\dashv	2
"			Ι .	-		-										\dashv	-
					1		Information Theft by	Theft of information (software, authentication information,	Tamper Resistance		(Same as on the Left)						\neg
15			1	2		D		configuration settings, encryption keys and other confidential	Obfuscation	_	(Same as on the Left)					_	2
			Ι .	-			of Theft or Disposal	information) stored on devices which were stolen or disposed of and then disassembled.	Zeroization	· ·	(Same as on the Left)					_	-
\vdash			—	 	1	<u> </u>	Route Blocking		Entrance and Exit Management (IC Card)	0		-	Device Error Detection		Redundancy	+	
							. tode blocking	communication cable.	Lock and Key management	0			Device Alive Monitoring				1
								Alternatively, communications are blocked by pulling out the					Log Collection/Log Analysis				1
16			2	2		С		communication cable from the device.		\vdash			Integrated Log Management System				2
1										<u> </u>			Surveillance Camera	0			- 1
													Intrusion Detection Sensor	0		\dashv	1
\vdash			—		1	—	Network Congestion	Causing congestion by generating the communications traffic	FW (Packet Filtering Type)	\vdash		-	Device Error Detection		Redundancy	+	
								that exceeds the capacity of the device.	FW (Application Gateway Type)				Device Error Detection Device Alive Monitoring		, countainoj	\dashv	- 1
4-			_	_		_			WAF				Log Collection/Log Analysis			\dashv	, 1
17			2	3		В			IPS/IDS				Integrated Log Management System			\dashv	1
									DDoS Countermeasures								1
	Not applicable (no fu	unctions)					Jamming	Interference with radio communications.					Device Error Detection		Redundancy		
													Device Alive Monitoring				
18													Log Collection/Log Analysis Integrated Log Management System				
													gruico cog managenerii System				
					1		Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels								-
			١ .	1 _		_			Data Encryption							\dashv	_ [
19			2	3		В			Exclusive Line								1
			<u></u>]												
								Maliciously modifying information flowing on the network.	Encryption of Communications Channels				Log Collection/Log Analysis				
20			2	3		В	Communication Data		Data Signature				Integrated Log Management System				₁
			-	•		-			Exclusive Line]		$oxed{\Box}$			·]
<u> </u>					1		0	2	Doubleton or Consult. 2	_				_		\perp	
								Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage	\vdash			Restriction on Connecting Device and its Usage	<u> </u>		\dashv	- 1
21			3	3		В	Device			\vdash		-	Log Collection/Log Analysis Integrated Log Management System			\dashv	1
1										\vdash		-	against oyaldii			\dashv	1
			1	1	1		I .	1	i .		1						

					sessment Met				incoming account for the correspon			Countermeasu					Security Level
Item Numbe	Type of Assets	Т	Farget Device			Importance of Assets Risk V	Threat (Atta	ck Type)	Description	Prote Intrusion/Spreading Phase	ection	Objective Achievement Phase	Detection/Understanding Da	mage	Business Continuity		By Threat
	Control System Asset	EWS			,	Tubic I	Unauthorized A	ccess	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type)		Objective / to illeve iller i illeve	IPS/IDS				
										FW (Application Gateway Type)	_		Log Collection/Log Analysis				
										One-way Gateway Proxy Server			Integrated Log Management System	Н		-	
1				2	2	В				WAF							2
					-					Peer-to-Peer Authentication IPS/IDS	0			H			
										Applying Patches							
										Avoidance of Vulnerability						\blacksquare	
	1		-				Physical Intrusion	on	Unauthorized access of sections/areas (device installation locations,	Entrance and Exit Management (IC Card, Biometric Authentication)	0		Surveillance Camera	0			
					.		1,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		etc.) with access restrictions.	Lock and Key Management	0		Intrusion Detection Sensor	0			
2				1	1	c			It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).								3
	<u> </u>																
3				2	2	В	Unauthorized O	peration	Intrusion through direct operation of the device's console or other component to execute an attack.	Operator Authentication (ID/Pass)	0			Н		$\overline{}$	2
	†		}				Human Error in	Operation	An attack triggered by a human error in operation by internal	URL Filtering/Web Reputation							
4					.	.			personnel (an employee or partner with access privileges to the device).	Mail Filtering	-			Н			
4				2	3	_ A			An act equivalent to an attack is performed on the device as a result								1
			_						of a proper media or device connection.			(0	(0				
				_	_		Connecting Una Media or Device		Connection of unauthorized media or device (CD/DVD, USB device, etc.) brought in from outside the organization with the	Restriction on Connecting Device and its Usage		(Same as on the Left)	(Same as on the Left) Log Collection/Log Analysis			\equiv	
5				3	3	A			device to execute an attack.				Integrated Log Management System				1
\vdash	 		-		\vdash		Execution of Un	authorized	Unauthorized execution of legitimate programs, commands,	Permission Management		(Same as on the Left)	Device Error Detection	\vdash		_	
							Processes		services, and other processes found on the attack target	Access Control		(Same as on the Left)	Device Alive Monitoring				
6				3	3	_ A			device.	Application Whitelisting Approval of Important Operations		(Same as on the Left) (Same as on the Left)	Log Collection/Log Analysis Integrated Log Management System	\vdash			1
L]											Canada Sir and Edity					
							Malware Infection	on		Anti-virus Application Whitelisting			Device Error Detection Device Alive Monitoring	H			
_				_					the attack target device.	Applying Patches	L		Log Collection/Log Analysis				
7				3	3	_ A				Avoidance of Vulnerability			Integrated Log Management System				1
										Data Signature				\vdash		\dashv	
	†		-				Information The	ft	Theft of information (software, authentication information,	Permission Management		(Same as on the Left)	Log Collection/Log Analysis				
8				3	3					Access Control Data Encryption	-	(Same as on the Left) (Same as on the Left)	Integrated Log Management System				1
°				•		^			information) stored on the device.	DLP		(Same as on the Left)					'
			-							Damining Manager		(Company of the Left)	Device Free Detection		Data Paulus		
١.				_		l .	Information	odification o	f Unauthorized modification of information (software, authentication information, configuration settings, encryption	Permission Management Access Control		(Same as on the Left) (Same as on the Left)	Device Error Detection Log Collection/Log Analysis		Data Backup		
9				3	3	_ A			keys and other confidential information) stored on the device.	Data Signature		(Same as on the Left)	Integrated Log Management System				1
	-		-			_	Information Des	truction	Destroying of information (software, authentication		-	Permission Management	Device Error Detection		Data Backup		
10				3	3			0 000011	information, configuration settings, encryption keys and other			Access Control	Log Collection/Log Analysis				1
1.0				•		^			confidential information) stored on the device.		├		Integrated Log Management System	Н			
	†		}			3	Unauthorized Tr	ransmission	Sending unauthorized control commands (settings changes,	Segmentation/Zoning		(Same as on the Left)	Log Collection/Log Analysis				
11				3	3	ĭ A	I .		power shutdowns, etc.) and unauthorized data to other	Data Signature Approval of Important Operations	-	(Same as on the Left) (Same as on the Left)	Integrated Log Management System				1
									devices.	Approval of important Operations		(Carrie as on the Left)				$\overline{}$	
	1						Outage		Stopping device functions.				Device Error Detection Device Alive Monitoring		Redundancy Failsafe Design		
12				3	3								Log Collection/Log Analysis		i alisale Design		1
													Integrated Log Management System			\blacksquare	
	1		-				DoS Attack		Interruption of regular device operations by sending	DDoS Countermeasures	\vdash		Device Error Detection	Н	Redundancy		
									processing requests that exceed the processing capacity of				Device Alive Monitoring		Failsafe Design		
13				1	3	В			the device as a result of a DDoS attack, etc.		-		Log Collection/Log Analysis Integrated Log Management System				1
]																
14				2	2	В	Theft		Device theft.	Lock and Key Management	0	(Same as on the Left)	(Same as on the Left)				2
]]				1	•											-
							Information The		Theft of information (software, authentication information, configuration settings, encryption keys and other confidential	Tamper Resistance Obfuscation		(Same as on the Left) (Same as on the Left)		H			
15				2	2	В	Tampering Devi of Theft or Dispo		information) stored on devices which were stolen or disposed of and		0	(Same as on the Left)					2
	. I								then disassembled.	Entrance and Exit Management			Device Error Detection		Redundancy		
							Route Blocking		Communications are blocked by disconnecting the communication cable.	Lock and Key management			Device Alive Monitoring		y		
									Alternatively, communications are blocked by pulling out the				Log Collection/Log Analysis				
16									communication cable from the device.				Integrated Log Management System Surveillance Camera				
													Intrusion Detection Sensor				
							Network Conse	stine	Causing congestion by generating the communications traffic	FW (Packet Filtering Type)			Device Error Detection		Redundancy		
							Network Conge	outon f	that exceeds the capacity of the device.	FW (Application Gateway Type)			Device Alive Monitoring		. todulidanoy		
17										WAF			Log Collection/Log Analysis				
										IPS/IDS DDoS Countermeasures			Integrated Log Management System				
	<u> </u>																
	Not applicable (no fun	ctions)					Jamming		Interference with radio communications.				Device Error Detection		Redundancy		
18													Device Alive Monitoring Log Collection/Log Analysis				
							Л						Integrated Log Management System				
	-		ŀ				Danket Calif		That of information flowing on the natural	Encounting of Communications Change							
							Packet Sniffing			Encryption of Communications Channels Data Encryption							
19										Exclusive Line							
	ļ ļ						I Inquithorized M	odification	f Maliciously modifying information flowing on the network.	Encryption of Communications Channels			Log Collection/Log Analysis				
20							Communication			Data Signature			Integrated Log Management System				
20										Exclusive Line							
	 						Connecting Una	uthorized	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage			Restriction on Connecting Device and its Usage				
21							Device Device	E0u	2 - Standard Control of the Helwork	Donice and its Usage			Log Collection/Log Analysis				
21													Integrated Log Management System				

								taken into account for the corres			Counterme						Security Level
Item Number	Type of Assets	Target Device		sessment Me			Threat (Attack Type)	Description	Prote	ection			Detection/Understanding Da	mane	Business Continuity		By Threat
ш			Threat Level	Vulnerability Level	importance of Assets	Risk Value			Intrusion/Spreading Phase		Objective Achievement Phas	se	-	aye	Duamess Continuity		
	Control System Asset	Control Server			1		Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type)				IPS/IDS	—		Щ	
									FW (Application Gateway Type)				Log Collection/Log Analysis	<u> </u>			
									One-way Gateway				Integrated Log Management System	┡			
									Proxy Server					_			
1			2	2		В			WAF					├		-	2
									Peer-to-Peer Authentication	0	 			-		\blacksquare	
									IPS/IDS		 			-			
									Applying Patches			_		-		\blacksquare	
									Avoidance of Vulnerability		-	-		├		-	
\vdash				-	4		Di contra di con	No. 10 and 10 an	-	0	+		C	-		-	
							Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with access restrictions.	Entrance and Exit Management (IC Card, Biometric Authentication) Lock and Key management	0			Surveillance Camera Intrusion Detection Sensor	0			
2			1	1		С		It also refers to removing restrictions on devices with physical	Lock and Ney management	-			Intrasion Detection densor	Ť			3
^				1 '		ľ		access restrictions (devices installed in racks, cabinets, etc.).									3
			_	1 .	1		Unauthorized Operation	Intrusion through direct operation of the device's console or other	Operator Authentication (ID/Pass)	0	 						
3			2	2		В		component to execute an attack.									2
					1		Human Error in Operation	An attack triggered by a human error in operation by internal	URL Filtering/Web Reputation								
								personnel (an employee or partner with access privileges to the	Mail Filtering					_			
4			2	3		A		device).						_			1
								An act equivalent to an attack is performed on the device as a result of a proper media or device connection.									
								or a proper media or device connection.									
Н					1		Connecting Unauthorized	Connection of unauthorized media or device (CD/DVD, USB	Restriction on Connecting Device and its Usage		(Same as on the Left)		(Same as on the Left)				
ا ۽ ا			_				Media or Device	device, etc.) brought in from outside the organization with the					Log Collection/Log Analysis				
5			2	3		A		device to execute an attack.					Integrated Log Management System				1
╚					_												
П					1		Execution of Unauthorized	Unauthorized execution of legitimate programs, commands,	Permission Management	0	(Same as on the Left)		Device Error Detection				
					1		Processes	services, and other processes found on the attack target	Access Control		(Same as on the Left)		Device Alive Monitoring	_		\Box	
6			3	2	1	A		device.	Application Whitelisting	0	(Same as on the Left)		Log Collection/Log Analysis			\square	2
					1				Approval of Important Operations		(Same as on the Left)		Integrated Log Management System	_		ш	
ш					4				A-Ei				Device For D	_			
					1		Malware Infection	Infection or running of malware (unauthorized programs) on	Anti-virus Application Whitelisting	_	+	-	Device Error Detection Device Alive Monitoring	_		\vdash	
					1			the attack target device.	Application Whitelisting Applying Patches	J	+		Log Collection/Log Analysis	-		\vdash	
7			3	2		A					+	-	Integrated Log Management System	-		-	2
					1				Avoidance of Vulnerability Data Signature	-	+	-		\vdash		\vdash	
					1				Sold Signature			-		-		\vdash	
\vdash					1		Information Theft	Theft of information (software, authentication information,	Permission Management	0	(Same as on the Left)		Log Collection/Log Analysis			\vdash	
							anomaton more	configuration settings, encryption keys and other confidential			(Same as on the Left)		Integrated Log Management System				
8			3	2		A		information) stored on the device.	Data Encryption		(Same as on the Left)						2
									DLP		(Same as on the Left)						
					7		Unauthorized Modification of	Unauthorized modification of information (software,	Permission Management	0	(Same as on the Left)		Device Error Detection		Data Backup	0	
9			3	2			Information	authentication information, configuration settings, encryption	Access Control		(Same as on the Left)		Log Collection/Log Analysis				2
				1	1	A .		keys and other confidential information) stored on the device.	Data Signature		(Same as on the Left)		Integrated Log Management System	_		\Box	-
ш					4						L				2 . 2 .		
							Information Destruction	Destroying of information (software, authentication			Permission Management		Device Error Detection	-	Data Backup	0	
10			3	2		A		information, configuration settings, encryption keys and other			Access Control		Log Collection/Log Analysis Integrated Log Management System	_		-	2
								confidential information) stored on the device.			 	-	integrated Edg management System	├		-	
\vdash				1	┥ .		Handbariand Tanasarianian	Continuo de circular control construit de la control de la	Segmentation/Zoning		(Same as on the Left)		Log Collection/Log Analysis	-			
					3		Oliautionzeu Transmission	Sending unauthorized control commands (settings changes, power shutdowns, etc.) and unauthorized data to other	Data Signature		(Same as on the Left)		Integrated Log Management System				
11			3	3		A		devices.	Approval of Important Operations		(Same as on the Left)					-	1
								devices.	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,								
\Box					1		Outage	Stopping device functions.					Device Error Detection		Redundancy		
								3.1					Device Alive Monitoring		Failsafe Design		
12			3	3		A							Log Collection/Log Analysis				1
													Integrated Log Management System				
ш					_												
							DoS Attack	Interruption of regular device operations by sending	DDoS Countermeasures				Device Error Detection	_	Redundancy		
l . l				l .		_		processing requests that exceed the processing capacity of					Device Alive Monitoring	_	Failsafe Design		
13			1	3		В		the device as a result of a DDoS attack, etc.					Log Collection/Log Analysis	_			1
													Integrated Log Management System	-		\Box	
\vdash				_	4		71.0	5 :- 4 6		-	(0 11 1 1 11		(0				
14			1	2	1	С	Theft	Device theft.	Lock and Key Management	Ü	(Same as on the Left)		(Same as on the Left)			\vdash	2
14			'	*	1	"					+	-		_		\vdash	2
\vdash				+	1		Information Theft by	Theft of information (software, authentication information,	Tamper Resistance		(Same as on the Left)			_		\vdash	
				_	1			configuration settings, encryption keys and other confidential	Obfuscation		(Same as on the Left)					\vdash	
15			1	2	1	С	of Theft or Disposal	information) stored on devices which were stolen or disposed of and		0	(Same as on the Left)					\Box	2
LI				\perp		L		then disassembled.									
					1		Route Blocking	Communications are blocked by disconnecting the	Entrance and Exit Management				Device Error Detection		Redundancy		
								communication cable.	Lock and Key management				Device Alive Monitoring				
					1			Alternatively, communications are blocked by pulling out the					Log Collection/Log Analysis				
16								communication cable from the device.					Integrated Log Management System				
					1								Surveillance Camera				
					1								Intrusion Detection Sensor				
					4				DW/D 1 15% : 7								
							Network Congestion	Causing congestion by generating the communications traffic					Device Error Detection		Redundancy		
								that exceeds the capacity of the device.	FW (Application Gateway Type) WAF				Device Alive Monitoring				
17									IPS/IDS				Log Collection/Log Analysis Integrated Log Management System				
									DDoS Countermeasures								
									DDGG Countermeasures								
					4	$\overline{}$	Jamming	Interference with radio communications.					Device Error Detection		Redundancy		
	Not applicable (no fu	nctions))	ou.aimig	The same with radio continual lications.					Device Alive Monitoring		, toduluanty		
18													Log Collection/Log Analysis				
													Integrated Log Management System				
					1		Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels								
					1		. Lond Coming		Data Encryption								
19									Exclusive Line			Ħ					
					1												
					1		Unauthorized Modification of	Maliciously modifying information flowing on the network.	Encryption of Communications Channels				Log Collection/Log Analysis				
					1		Communication Data		Data Signature				Integrated Log Management System				
20							2 2 Data		Exclusive Line				January agencin cystell				
					1												
					1		Connecting Unauthorized	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage				Restriction on Connecting Device and its Usage				
							Device	g and	and a second				Log Collection/Log Analysis				
21													Integrated Log Management System				

	Logo	T					oo: Triioato fiot	taken into account for the corresp	I		Counterme					_	Security Level
Item Number	Type of Assets	Target Device		sessment Me			Threat (Attack Type)	Description	Prote	ction			Detection/Understanding Da	mage	Business Continuity		By Threat
	Ocatal Co. 1	UMU (0t	Threat Level	Vulnerability Level	Importance of Assets	Risk Value	11	had a second the second term of	Intrusion/Spreading Phase		Objective Achievement Phase	_		-			
	Control System Asset	HMI (Operator Terminal)					Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type)		+		PS/IDS			\vdash	
	1								FW (Application Gateway Type)				Log Collection/Log Analysis ntegrated Log Management System			_	
	1								One-way Gateway		 		ntegrated Log management System			\vdash	
									Proxy Server WAF		+	\dashv		\vdash		\vdash	l
1	1		2	2		В			Peer-to-Peer Authentication	0		\dashv				-	2
	1								IPS/IDS			\dashv					
	1								Applying Patches			\dashv					
	1								Avoidance of Vulnerability			\neg					
	1								A troidance of Tanierability			\dashv					
	1				1		Physical Intrusion	Unauthorized access of sections/areas (device installation locations,	Entrance and Exit Management (IC Card)	0			Surveillance Camera	0			
	1						,	etc.) with access restrictions.	Lock and Key Management	0		ŀ	ntrusion Detection Sensor	0			
2			2	2		В		It also refers to removing restrictions on devices with physical				П					2
								access restrictions (devices installed in racks, cabinets, etc.).			1 1				i .		
					1												
3	1		2	3		A	Unauthorized Operation	Intrusion through direct operation of the device's console or other	Operator Authentication		-	\dashv				\vdash	1
	1				-			component to execute an attack. An attack triggered by a human error in operation by internal	URL Filtering/Web Reputation		-	\dashv				\vdash	
							Human Error in Operation		Mail Filtering			\dashv					
4	1		2	3		A		device).				\neg					1
	1		-	•		_ ^		An act equivalent to an attack is performed on the device as a result				\neg					
								of a proper media or device connection.				\neg					
	1				1		Connecting Unauthorized	Connection of unauthorized media or device (CD/DVD, USB	Restriction on Connecting Device and its Usage		(Same as on the Left)	(Same as on the Left)				
	1		١.,				Media or Device	device, etc.) brought in from outside the organization with the				L	og Collection/Log Analysis				4
э	i '		3	3		A		device to execute an attack.				li	ntegrated Log Management System	ш		ш	1
	,				1							\bot		ш		ш	
]	i '							Unauthorized execution of legitimate programs, commands,	Permission Management		(Same as on the Left)		Device Error Detection	\sqcup		\vdash	7
	i '		١	1 -		l .	Processes	services, and other processes found on the attack target	Access Control		(Same as on the Left)		Device Alive Monitoring	\vdash		\vdash	
6	i '		3	3		Α .		device.	Application Whitelisting		(Same as on the Left) (Same as on the Left)		Log Collection/Log Analysis	$\vdash\vdash$		\vdash	1
	i '								Approval of Important Operations		(Same as on the Left)		ntegrated Log Management System	$\vdash\vdash$		\vdash	
	i '		—		1		Malwara Infaction	Infaction or nunning of molyage (unoutbested accesses)	Anti-virus		+		Device Error Detection	\vdash		\vdash	
	i '						Malware Infection		Application Whitelisting				Device Alive Monitoring	H		\vdash	
	i '							the attack target device.	Applying Patches				og Collection/Log Analysis	М		П	l
7	i '		3	3		Α .			Avoidance of Vulnerability				ntegrated Log Management System	Н			1
	i '								Data Signature			一		Н			
									-			\dashv		М		П	I
	1				1		Information Theft	Theft of information (software, authentication information,	Permission Management		(Same as on the Left)		og Collection/Log Analysis				
	1								Access Control		(Same as on the Left)	i i	ntegrated Log Management System				
8	1		3	3		A		information) stored on the device.	Data Encryption		(Same as on the Left)						1
	1							, in the second	DLP		(Same as on the Left)						
	1				1							_					
	1						Unauthorized Modification of	Unauthorized modification of information (software,	Permission Management		(Same as on the Left)		Device Error Detection		Data Backup		
9	1		3	3		Α	Information	authentication information, configuration settings, encryption	Access Control		(Same as on the Left)		og Collection/Log Analysis				1
								keys and other confidential information) stored on the device.	Data Signature		(Same as on the Left)		ntegrated Log Management System			-	
	i				-						Permission Management		Device Error Detection		Data Backup		
							Information Destruction	Destroying of information (software, authentication			Permission Management Access Control		og Collection/Log Analysis		Баца Баскир		
10			3	3		A		information, configuration settings, encryption keys and other			Access Control		ntegrated Log Management System				1
								confidential information) stored on the device.			 	-					
			_		1		I Inquithorized Transmission	Sending unauthorized control commands (settings changes,	Segmentation/Zoning		(Same as on the Left)	_	og Collection/Log Analysis				
					3		Ondution260 Transmission		Data Signature		(Same as on the Left)		ntegrated Log Management System				
11	1		3	3		Α .		devices.	Approval of Important Operations		(Same as on the Left)						1
	1							devices.				\neg					
	1				1		Outage	Stopping device functions.					Device Error Detection		Redundancy		
	1												Device Alive Monitoring		Failsafe Design		
12	1		3	3		A							og Collection/Log Analysis				1
	1											- 1	ntegrated Log Management System				
					1												
							DoS Attack	Interruption of regular device operations by sending	DDoS Countermeasures				Device Error Detection		Redundancy		
40						_		processing requests that exceed the processing capacity of					Device Alive Monitoring Log Collection/Log Analysis		Failsafe Design		
13			1	3		В		the device as a result of a DDoS attack, etc.			+		ntegrated Log Management System				1
												-F	negrates cog management oystem				
	1				1		Theft	Device theft.	Lock and Key Management	0	(Same as on the Left)	-	Same as on the Left)				
14	i '		2	2		В			uno reoy management	-	(Lamo do Sil tiro Lolt)	-	OU ON UND LOTE			\vdash	2
	i '		-	-		-					 	\dashv		\vdash		\vdash	-
	i '				1		Information Theft by	Theft of information (software, authentication information,	Tamper Resistance		(Same as on the Left)			╚		L	
45	i '		١ .	_		-		configuration settings, encryption keys and other confidential	Obfuscation	_	(Same as on the Left)						
15	i '		2	2		"	of Theft or Disposal	information) stored on devices which were stolen or disposed of and	Zeroization	0	(Same as on the Left)			Ш			۷.
	i '				1			then disassembled.						ш	D. J. J.		
	<i>i</i>						Route Blocking	Communications are blocked by disconnecting the	Entrance and Exit Management				Device Error Detection Device Alive Monitoring		Redundancy		
	<i>i</i>							communication cable.	Lock and Key management								
16	<i>i</i>							Alternatively, communications are blocked by pulling out the					Log Collection/Log Analysis Integrated Log Management System				
ıυ	<i>i</i>							communication cable from the device.					Surveillance Camera				
	<i>i</i>												ntrusion Detection Sensor				
	<i>i</i>												caron detection delisor				
	<i>i</i>				1		Network Congestion	Causing congestion by generating the communications traffic	FW (Packet Filtering Tyne)			r	Device Error Detection		Redundancy		
	i '				1				FW (Application Gateway Type)				Device Alive Monitoring				
	<i>i</i>								WAF				og Collection/Log Analysis				
17	<i>i</i>								IPS/IDS				ntegrated Log Management System				
	<i>i</i>								DDoS Countermeasures			-					
	<i>i</i>											-					
					_		Jamming	Interference with radio communications.				r	Device Error Detection		Redundancy		
	Not applicable (no fur	nctions)											Device Alive Monitoring		,		
18												-	og Collection/Log Analysis				
													ntegrated Log Management System				
					_							1					
	<i>i</i>				1		Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels								
	<i>i</i>						,		Data Encryption								
19	i '				1				Exclusive Line			-					
	i '				1				EXCUSOR CHIC			-					
	<i>i</i>				1		Unauthorized Modification of	Maliciously modifying information flowing on the network.	Encryption of Communications Channels				og Collection/Log Analysis				
	<i>i</i>						Communication Data		Data Signature				ntegrated Log Management System				
20	<i>i</i>						Data		Exclusive Line			-					
	<i>i</i>																
	<i>i</i>				1		Connecting Unauthorized	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage			9	testriction on Connecting Device and its Usage				
	<i>i</i>				1		Device Or Mathorized						og Collection/Log Analysis				
21	<i>i</i>												ntegrated Log Management System				
	i '				1												

_								terrino account for the correspo	<u> </u>		Countermeas					Security Lev
n Number	Type of Assets	Target Device	Ass	ssessment Me	etrics		Threat (Attack Type)	Description	Prote	ection	Countermeas			2 2 2		By Threa
			Threat Level	BI Vulnerability Leve	el Importance of Assets	Risk Value			Intrusion/Spreading Phase		Objective Achievement Phase	Detection/Understanding Dar	mage	Business Continuity		
	Network Asset	Control Network (Field Side)					Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type)			IPS/IDS				
		,							FW (Application Gateway Type)			Log Collection/Log Analysis				
	ļ								One-way Gateway			Integrated Log Management System				
	ļ								Proxy Server						=	
									WAF						-	
1									Peer-to-Peer Authentication						-	
															=	
									IPS/IDS						_	1
									Applying Patches						_	4
									Avoidance of Vulnerability						_	4
							Physical Intrusion	Unauthorized access of sections/areas (device installation locations,				Surveillance Camera				4
								etc.) with access restrictions.	Lock and Key Management			Intrusion Detection Sensor				1
2								It also refers to removing restrictions on devices with physical								
								access restrictions (devices installed in racks, cabinets, etc.).								
3					1		Unauthorized Operation	Intrusion through direct operation of the device's console or other	Operator Authentication							
5								component to execute an attack.								
							Human Error in Operation	An attack triggered by a human error in operation by internal	URL Filtering/Web Reputation							4
								personnel (an employee or partner with access privileges to the	Mail Filtering							1
4								device).								
								An act equivalent to an attack is performed on the device as a result								1
								of a proper media or device connection.								1
					1 1		Connecting Unauthorized	Connection of unauthorized media or device (CD/DVD, USB	Restriction on Connecting Device and its Usage		(Same as on the Left)	Restriction on Connecting Device and its Usage				
							Media or Device	device, etc.) brought in from outside the organization with the				Log Collection/Log Analysis				1
5	,							device to execute an attack.				Integrated Log Management System				
	,							and the control of all deck.								
					1		Execution of Unauthorized	Unauthorized execution of legitimate programs, commands,	Permission Management		(Same as on the Left)	Device Error Detection				
							Processes		Access Control		(Same as on the Left)	Device Alive Monitoring				
6					1		10000000	services, and other processes found on the attack target device.	Application Whitelisting		(Same as on the Left)	Log Collection/Log Analysis				
								device.	Approval of Important Operations		(Same as on the Left)	Integrated Log Management System				
									Approval of important Operations		(Gaine as On the Left)					
					4 !				Anti.virue			Davice Error Detection				\vdash
							Malware Infection	Infection or running of malware (unauthorized programs) on	Annii-virus			Device Error Detection			=	
								the attack target device.	Application Whitelisting			Device Alive Monitoring			=	
									Applying Patches			Log Collection/Log Analysis				
									Avoidance of Vulnerability			Integrated Log Management System				
									Data Signature							
					.											
	,						Information Theft	Theft of information (software, authentication information,	Permission Management		(Same as on the Left)	Log Collection/Log Analysis				4
								configuration settings, encryption keys and other confidential	Access Control		(Same as on the Left)	Integrated Log Management System				1
3								information) stored on the device.	Data Encryption		(Same as on the Left)					1
								, ,	DLP		(Same as on the Left)					1
																1
					1 1		Unauthorized Modification of	Unauthorized modification of information (software,	Permission Management		(Same as on the Left)	Device Error Detection		Data Backup		
							Information	authentication information, configuration settings, encryption	Access Control		(Same as on the Left)	Log Collection/Log Analysis				1
							IIIOIIIIauoii	keys and other confidential information) stored on the device.			(Same as on the Left)	Integrated Log Management System				1
									,							
					1		Information Destruction	Destroying of information (software, authentication			Permission Management	Device Error Detection		Data Backup		
							Information Destruction				Access Control	Log Collection/Log Analysis		Data Backup	=	í.
0								information, configuration settings, encryption keys and other			Access Control		_		-	1
								confidential information) stored on the device.				Integrated Log Management System				
					4											
					3		Unauthorized Transmission	Sending unauthorized control commands (settings changes,	Segmentation/Zoning		(Same as on the Left)	Log Collection/Log Analysis			_	4
1								power shutdowns, etc.) and unauthorized data to other	Data Signature		(Same as on the Left)	Integrated Log Management System			_	4
								devices.	Approval of Important Operations		(Same as on the Left)					4
							Outage	Stopping device functions.				Device Error Detection		Redundancy		4
												Device Alive Monitoring		Failsafe Design		1
2												Log Collection/Log Analysis				1
												Integrated Log Management System				1
																1
					1 1		DoS Attack	Interruption of regular device operations by sending	DDoS Countermeasures			Device Error Detection		Redundancy		
								processing requests that exceed the processing capacity of				Device Alive Monitoring		Failsafe Design		1
3								the device as a result of a DDoS attack, etc.				Log Collection/Log Analysis				1
								and device as a result of a DDOC attack, etc.				Integrated Log Management System				1
															=	1
	,				-		Theft	Device theft.	Lock and Key Management	0	(Same as on the Left)	(Same as on the Left)				
1	,											(22 on the coll)				
				_	-		Information Tt. 6:	Theft of information (software, authentication information,	Tamper Resistance		(Same as on the Left)					
	,						Information Theft by	and a vertice and income and other and other and deated	Obfuscation		(Same as on the Left)					
5	,						Tampering Device at Time	information) stored on devices which were stolen or disposed of and	Zeroization		(Same as on the Left)					
							of Theft or Disposal	then disassembled.	LOIGEAUGI		(Gaine as On the Left)					
	,				4		D 1 D 1:			0		Daviso Error Datastica		Podundonov		
	,			1			Route Blocking	Communications are blocked by disconnecting the	Entrance and Exit Management (IC Card, Biometric Authentication)	0	 	Device Error Detection	—	Redundancy	-	í
				1				communication cable.	Lock and Key management	0	+	Device Alive Monitoring	<u> </u>		-	ı
	,			1 .				Alternatively, communications are blocked by pulling out the		_		Log Collection/Log Analysis	<u> </u>			1 .
1	,		3	2		A		communication cable from the device.	L	_	1	Integrated Log Management System	_			2
				1								Surveillance Camera				4
				1						ш		Intrusion Detection Sensor]	4
_ [,									L			L			L
╛				1	7		Network Congestion	Causing congestion by generating the communications traffic	FW (Packet Filtering Type)			Device Error Detection		Redundancy		
1	,			1				that exceeds the capacity of the device.	FW (Application Gateway Type)		1	Device Alive Monitoring		-,	\neg	1
	,			1				and a suppose of the device.	WAF		 	Log Collection/Log Analysis		 	-	1
1	,		2	3		A				-	 		—		-	1
-				1					PS/IDS	_		Integrated Log Management System	_			ł
	,			1					DDoS Countermeasures	_	1					4
⅃					_					oxdot			\perp			
1	(,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,						Jamming	Interference with radio communications.				Device Error Detection		Redundancy		
	Not applicable (no fu	inctions)										Device Alive Monitoring				
												Log Collection/Log Analysis				
												Integrated Log Management System				
1												-gg managantan aysiani				
4				_			Dealest Caiffe	The first country flow in a section of								
J				1			Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels							4
1			2	3		A			Data Encryption				_			1
				"		^			Exclusive Line						7	
1	,			1												1
7				1	7 1		Unauthorized Modification of	Maliciously modifying information flowing on the network.	Encryption of Communications Channels			Log Collection/Log Analysis				$\overline{}$
1	,			1							 	Integrated Log Management System		 	\dashv	1
1			2	3		A	Communication Data		Data Signature	_	 	macyrateu Log martagement System		 	-	1
1	,			1					Exclusive Line	-	1	_	<u> </u>			4
┙				1						<u> </u>						
1	,						Connecting Unauthorized	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage	L		Restriction on Connecting Device and its Usage	L			
- [_	_			Device					Log Collection/Log Analysis			\neg	Ι.
1	,		2	3		A						Integrated Log Management System			\neg	1
				1											-	ı
_							1	i	i .		<u>ı</u>	1				4

					*					Countermo	easure	es			Se	curity Level
Item Number	Type of Assets	Target Device		sessment Met		Threat (Attack Type)	Description		ection	L au	\Box	Detection/Understanding Da	mage	Business Continuity	В	y Threat
	Natural Asset	Field Network	Threat Level	Vulnerability Level	Importance of Assets Risk Valu		hate raises of the administrative the most ready to account a second	Intrusion/Spreading Phase		Objective Achievement Phase			Ť	,	+	
	Network Asset	FIEID NETWORK				Unauthorized Access		FW (Packet Filtering Type) FW (Application Gateway Type)	_			IPS/IDS Log Collection/Log Analysis	_		-	
								One-way Gateway			-	Integrated Log Management System			\dashv	
								Proxy Server	_		-	micgrated Edg management dystem			\dashv	
								WAF			$\overline{}$				\dashv	
1								Peer-to-Peer Authentication							\dashv	
								IPS/IDS							\neg	
								Applying Patches							\neg	
								Avoidance of Vulnerability							7	
						Physical Intrusion	Unauthorized access of sections/areas (device installation locations,					Surveillance Camera			_	
2							etc.) with access restrictions.	Lock and Key Management			_	Intrusion Detection Sensor			_	
_							It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).									
							decess restrictions (decrees instance in racity, educate, etc.).									
3						Unauthorized Operation	Intrusion through direct operation of the device's console or other	Operator Authentication							\exists	
3							component to execute an attack.	UDI ETI COMPLETE	_		_					
						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	URL Filtering/Web Reputation Mail Filtering			-				\dashv	
4							device).	Ividii I illoiliig							\dashv	
7							An act equivalent to an attack is performed on the device as a result								\dashv	
							of a proper media or device connection.								\neg	
						Connecting Unauthorized	Connection of unauthorized media or device (CD/DVD, USB	Restriction on Connecting Device and its Usage		(Same as on the Left)		Restriction on Connecting Device and its Usage				
5						Media or Device	device, etc.) brought in from outside the organization with the					Log Collection/Log Analysis				
,							device to execute an attack.					Integrated Log Management System			4	
						E F (1)	Hard day of the Control	Dermination Management		(Comp on on the Left)		Davino Error Detection				
								Permission Management Access Control		(Same as on the Left) (Same as on the Left)		Device Error Detection Device Alive Monitoring			+	
6						Processes	services, and other processes found on the attack target device.	Application Whitelisting		(Same as on the Left)		Log Collection/Log Analysis			+	
							device.	Approval of Important Operations		(Same as on the Left)		Integrated Log Management System				
										,						
						Malware Infection	Infection or running of malware (unauthorized programs) on	Anti-virus				Device Error Detection				
							the attack target device.	Application Whitelisting			-	Device Alive Monitoring			_	
7								Applying Patches				Log Collection/Log Analysis				
								Avoidance of Vulnerability				Integrated Log Management System			-	
								Data Signature			-				\dashv	
						Information Theft	Theft of information (software, authentication information,	Permission Management		(Same as on the Left)		Log Collection/Log Analysis			+	
						IIIIOIIIIauoii IIIeit	configuration settings, encryption keys and other confidential	Access Control		(Same as on the Left)		Integrated Log Management System			_	
8							information) stored on the device.	Data Encryption		(Same as on the Left)	T				\neg	
							and maken) stored on the device.	DLP		(Same as on the Left)						
							f Unauthorized modification of information (software,	Permission Management		(Same as on the Left)		Device Error Detection		Data Backup	\dashv	
9						Information	authentication information, configuration settings, encryption	Access Control	_	(Same as on the Left)	-	Log Collection/Log Analysis			_	
							keys and other confidential information) stored on the device.	Data Signature	-	(Same as on the Left)	-	Integrated Log Management System			-	
						Information Destruction	Destroying of information (software, authentication			Permission Management		Device Error Detection		Data Backup	+	
						IIIIOITTIAUOTI Desti uctioti	information, configuration settings, encryption keys and other			Access Control		Log Collection/Log Analysis			┪	
10							confidential information) stored on the device.					Integrated Log Management System				
							ormacinal morniasor) stored or the device.									
					3	Unauthorized Transmission	Sending unauthorized control commands (settings changes,	Segmentation/Zoning		(Same as on the Left)		Log Collection/Log Analysis				
11					, , , , , , , , , , , , , , , , , , ,		power shutdowns, etc.) and unauthorized data to other	Data Signature		(Same as on the Left)	-	Integrated Log Management System			_	
							devices.	Approval of Important Operations		(Same as on the Left)	\dashv				\dashv	
						Outage	Stopping device functions.		-		\dashv	Device Error Detection		Redundancy	+	
						Outage	Stopping device functions.					Device Alive Monitoring		Failsafe Design	\dashv	
12												Log Collection/Log Analysis			7	
												Integrated Log Management System				
						DoS Attack	Interruption of regular device operations by sending	DDoS Countermeasures			-	Device Error Detection		Redundancy Epiloafo Decian	-	
13							processing requests that exceed the processing capacity of			 		Device Alive Monitoring Log Collection/Log Analysis		Failsafe Design	\dashv	
13							the device as a result of a DDoS attack, etc.				\dashv	Integrated Log Management System			\dashv	
															\dashv	
						Theft	Device theft.	Lock and Key Management		(Same as on the Left)		(Same as on the Left)				
14																
															\Box	
						Information Theft by	Theft of information (software, authentication information,	Tamper Resistance		(Same as on the Left)					+	
15							configuration settings, encryption keys and other confidential	Obfuscation Zeroization		(Same as on the Left)					-	
						of Theft or Disposal	information) stored on devices which were stolen or disposed of and then disassembled.	Lo. o. Eduori		(Coline as on the Left)					+	
						Route Blocking	Communications are blocked by disconnecting the	Entrance and Exit Management (on the Premises Only)	0			Device Error Detection		Redundancy		
							communication cable.	Lock and Key management	0			Device Alive Monitoring				
							Alternatively, communications are blocked by pulling out the					Log Collection/Log Analysis			_	
16			3	2	A		communication cable from the device.		<u> </u>			Integrated Log Management System	-		_	2
1									_			Surveillance Camera			\dashv	
							1			+	\dashv	Intrusion Detection Sensor	<u> </u>		\dashv	
\vdash			—	\vdash	 	Network Congestion	Causing congestion by generating the communications treffic	FW (Packet Filtering Type)	 	+	\dashv	Device Error Detection	-	Redundancy	+	
						IVELWOIK CONGESTION	Causing congestion by generating the communications traffic that exceeds the capacity of the device.	FW (Packet Filtering Type) FW (Application Gateway Type)	\vdash	 		Device Error Detection Device Alive Monitoring		recountaincy	\dashv	l
1			l .					WAF			-	Log Collection/Log Analysis		-	\dashv	_
17			2	3	A			IPS/IDS				Integrated Log Management System			\dashv	1
								DDoS Countermeasures			\neg				\neg	
L			L	<u>∟</u> ∣			<u> </u>								_	
	Not applicable (no fun	netions				Jamming	Interference with radio communications.					Device Error Detection		Redundancy		
	ivot applicable (no fun	rictionS)										Device Alive Monitoring				
18												Log Collection/Log Analysis			_	
						Л						Integrated Log Management System			\perp	
						D I I O W	7.0.00									
						Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels	\vdash	—	-		<u> </u>		\dashv	
19			2	3	A			Data Encryption	_	 	\dashv				\dashv	1
							1	Exclusive Line	\vdash	+	\dashv		<u> </u>		\dashv	
				\vdash	<u> </u>	Unauthorized Modification of	f Maliciously modifying information flowing on the network.	Encryption of Communications Channels	\vdash	 	\dashv	Log Collection/Log Analysis			+	
			l .	_		Communication Data		Data Signature			\dashv	Integrated Log Management System			\dashv	
20			2	3	A	James Data	1	Exclusive Line			\dashv				\dashv	1
							1				\dashv				\dashv	
				\vdash		Connecting Unauthorized	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage			_	Restriction on Connecting Device and its Usage				
21			2	3	A	Device						Log Collection/Log Analysis				1
21			'	"	^							Integrated Log Management System				.
			_				•		_				_			

March Marc	_								Kerr into account for the correspon			Counterm					Security Level
Company Comp	Item Numb	Type of Assets	Target Device	Ass	sessment Me	etrics		Threat (Attack Type)	Description	Prote	ection				Punings Continuity	_	
Part	\perp			Threat Level	Vulnerability Level	Importance of Assets	Risk Value					Objective Achievement Pha	se	arnage	business Continuity		
Part								Unauthorized Access	Intrusion of the device via the network to execute an attack.								
1			(Master)											_		_	
1													Integrated Log Management System	₩		-	
														+-		-	
	1			2	3		A							+-		-	1
Part														\vdash		-	
Part														\vdash		$\overline{}$	
Part																	
1																	
1		1				1		Physical Intrusion	Unauthorized access of sections/areas (device installation locations,	Entrance and Exit Management (IC Card)	0		Surveillance Camera	0			
Second Continues of the Continues of t										Lock and Key Management	0		Intrusion Detection Sensor	0			
Part	2			2	2		B										2
Part									access restrictions (devices installed in racks, cabinets, etc.).								
Part	-	1		—		1		Unauthorized Operation	Intrusion through direct operation of the device's console or other	Operator Authentication (ID/Pass)	0			+		-	
Part	3			2	2		B	Oridation200 Operation									2
No.]				1		Human Error in Operation								=	
Processor Proc	1									Mail Filtering				_			
Part	4			2	3		A							-			1
E Command principal princi	1													-		_	
1	-	-		-		1		Connecting Unauthorized	* *	Restriction on Connecting Device and its Usage		(Same as on the Left)	(Same as on the Left)	-		-	
2 3 A Province of Company	1											(como do on the con)					
Part	5			2	3		A										1
Part	L]		L			_		and the state of t								
Part]				1		Execution of Unauthorized	Unauthorized execution of legitimate programs, commands,								
Package Pack	1													_			
Name	6			2	3		A							_			1
Part	1	[1					Approval of Important Operations		(Same as on the Left)	Integrated Log Management System	-		-	
Part	\vdash	1		—	-	-	\vdash	M-1 1-6	Market and the state of the sta	Anti-virue			Davice Error Dotostion	-		\rightarrow	
Part														+		-	
No.	1				1				tne attack target device.					+	 	\dashv	
Part	7			1	3		В							+		-	1
Part	1												gonem oystem			-	
Part	1																
2 2 3 4		1				1		Information Theft	Theft of information (software, authentication information,	Permission Management		(Same as on the Left)	Log Collection/Log Analysis				
2 2 3 4										Access Control		(Same as on the Left)					
1	8			3	3		A										1
2 3 3 A Microsian submitted configuration configur									,	DLP		(Same as on the Left)					
2 3 3 A Microsian submitted configuration configur]															
1								Unauthorized Modification of						+	Data Backup	_	
A Principal potentials of A Principal potent	9			3	3		l a l							+		_	1
Barriage									keys and other confidential information) stored on the device.	Data Signature		(Same as on the Lett)	Integrated Log Management System	\vdash		_	
Barriage	-	-		-		1		Information Death estima	Dealer in a finfermation (a of the sea of the stination			Permission Management	Device Error Detection	+	Data Backun	-+	
A Superficiency of project of the devices of the de								Information Destruction							Data Datikap		
3 3 3 4 A Design foundational control of communicity participal participation of control of communicity participation of control of communicity participation of control of cont	10			3	3		A							\vdash		$\overline{}$	1
1 Post Symmetry Post Sym									confidential information) stored on the device.								
Part		1				1		Unauthorized Transmission	Sending unauthorized control commands (settings changes,	Segmentation/Zoning		(Same as on the Left)	Log Collection/Log Analysis				
A Surgery device functions Segrety device functions Segrety device fun				١.	١.	3											
2 3 A A Substitute of register devices operations by sending processing expect of the control of Fortificial Contr	111			"	•		^			Approval of Important Operations		(Same as on the Left)					'
2 3 A A Substitute of register devices operations by sending processing expect of the control of Fortificial Contr		1				1								ـــــــــــــــــــــــــــــــــــــ		_	
Doc Afface services or requirement from the processing requests that exceeds the processing requests of the device as a result of a DOod statut, etc. 10								Outage	Stopping device functions.					+		_	
Dock Rises. A Set active of the processory requested with or even file processory appeals for the control file processor and the control file processor appeals for the control file processor and the control file for	40			١.	١.									+	railsale Design	-	
Dod About Represent processing injuries that the processing capacity of processing capacity of the processing capacity of the processing capacity of the processing capacity of the device of the device of the processing capacity of the device of the processing capacity of the device of the device of the processing capacity of the device of the processing capacity of the device of the devic	12			2	*		^							+		-	1
A processary regregates the accrease the processary regregates the processary regre													integrated Edg management dystem	+		-	
A processary regregates the accrease the processary regregates the processary regre		†				1		DoS Attack	Interruption of regular device operations by sending	DDoS Countermeasures			Device Error Detection		Redundancy	_	
13 3 3 6 The file of the device as a result of a DOod stack, etc. 14 2 2 8 8 Well manufacture of the comment of the comm																	
B Their Device that, Lock and Key Management D Same as on the Left) 2 2 B Tampering Device at Time of information tretting, ecopyring legs and other confidence of the Left D Sportal Tampering Device at Time of Intelligence of Time of Intelligenc	13			3	3		A						Log Collection/Log Analysis				1
15 2 2 8 Information (orbitally supported by water after confidence or disposal or fundamental or support of the formation (orbitally supported by water after confidence or disposal or fundamental or fundamental or fundamental or fundamental or disposal or fundamental or fundamental or fundamental or fundamental or disposal or fundamental or fundamental or fundamental or disposal or fundamental or													Integrated Log Management System				
15 2 2 8 Information (orbitally supported by water after confidence or disposal or fundamental or support of the formation (orbitally supported by water after confidence or disposal or fundamental or fundamental or fundamental or fundamental or disposal or fundamental or fundamental or fundamental or fundamental or disposal or fundamental or fundamental or fundamental or disposal or fundamental or]															
That of information Theft by B Tampering Device at Time B Tampering Device After Device Device And Notice Time B Tampering Device After Device And Notice B Tampering Device After Device Devic	1.			l	l		_ 7	Theft	Device theft.	Lock and Key Management	0	(Same as on the Left)	(Same as on the Left)				_]
2 2 B Tampering Device at Time of Their of Deposal of Their of Tamper Openion and Time of Their of Poliposal of Their of The	14			2	2		B							_			2
2 2 B Tampering Device at Time of Their of Deposal of Their of Tamper Openion and Time of Their of Poliposal of Their of The	\vdash	4 !				1	\vdash			Tamana Basista		(Cama as a 11 - 1 - 5)		1			
The for Disposal Informational stored on devices which were store or disposed of and Ziroczation Communications are blocked by manufactures and Exist Management Communications are blocked by disconnecting the communication cable Commu	1								and the second of the second o	Obfuscation		(Cama as as the Laft)		+		-	
Roude Blocking Communications are blocked by disconnecting the communication cable. Alternative American Communications are blocked by pulling out the communication cable from the device. Network Congestion Network Congestion Observed American Communications are blocked by pulling out the communication cable from the device. Observed American Communications are blocked by pulling out the communication cable from the device. Observed American Communications are blocked by pulling out the communications brain and pulling out the communications are blocked by pulling out the communications by pulling out the communications are blocked by pulling out the communications by pulling out the communications are blocked by pulling out the communications by pulling out t	15			2	2		B		information) stored on devices which were stolen or discosed of and	Zeroization	0			1	 	-	2
Rode Blocking Communications are blocked by gloconecting the communication cable. Alternatively, communication cable. Alternatively, communication cable from the device. Network Congestion Causing congestion by generating the communications traffic. Network Congestion Causing congestion by generating the communications traffic. Network Congestion Causing congestion by generating the communications traffic. Network Congestion Causing congestion by generating the communications traffic. Network Congestion Network Congestion Causing congestion by generating the communications traffic. Network Congestion Network Congestion Causing congestion by generating the communications traffic. Not applicable (not functions) Not applicable (not functions) Not applicable (not functions) Jamming Interference with radio communications. Not applicable (not functions) Not applicab	1				1			ui ineπ or Disposal			Ĺ	La constant contraction of the c				-	
December		1 !				1		Route Blockina		Entrance and Exit Management			Device Error Detection		Redundancy		
Alternatively, communications are blocked by pulling out the communications are blocked by pulling out the communications cable from the device. Network Congestion Surrelliance Camera Surrell													Device Alive Monitoring				
Communication cable from the device. Surveillance Carears																	
Network Congestion by generating the communications traffic FW (Packet Filtning Type) Device Error Detection Redundancy that exceeds the capacity of the device. Not applicable (no functions)	16																
Network Congestion Network Congestion by generating the communications straffic that exceeds the capacity of the device. Not applicable (no functions) N																	
that exceeds the capacity of the device. FW (Application Gateway Type) Device Alive Monitoring Log Collection Log Analysis FS/IDS													Intrusion Detection Sensor				
that exceeds the capacity of the device. FW (Application Gateway Type) Device Alive Monitoring Log Collection Log Analysis FS/IDS		4				1											
WAF Lig Collection Log Analysis Management System Manageme															redundancy		
PS/IDS Door Countermeasures Door Counte									ural exceeds the capacity of the device.	rvv (Application Gateway Type)							
DDoS Countermeasures Device Error Detection Redundancy	17																
Not applicable (no functions) Packet Sniffing Packet Sniffing													integrated Log Management System				
Not applicable (no functions) Device Alive Monitoring Log CollectionLog Analysis										DD03 Countermeasures							
Not applicable (no functions) Device Alive Monitoring Log CollectionLog Analysis				$\overline{}$		1	$\overline{}$	Iommina	Interference with radio communications				Doving Error Detection		Padundanau		
Packet Sniffing Theft of information flowing on the network. Encryption of Communications Channels Data Encryption Exclusive Line Unauthorized Modification of Maliciously modifying information flowing on the network. Encryption of Communications Channels Data Encryption Exclusive Line Unauthorized Modification of Maliciously modifying information flowing on the network. Communication Data Connecting Unauthorized Connecting unauthorized device on the network Device Connecting Unauthorized device on the network Device Log Collection/Log Analysis Log Collection/Log Analysis Log Collection/Log Analysis		Not applicable (no fund	ctions)					varining	and for ence with Faulo Communications.						reduituancy		
Packet Sniffing Theft of information flowing on the network. Encryption of Communications Channels Data Encryption Exclusive Line Unauthorized Modification of Maliciously modifying information flowing on the network. Encryption of Communications Channels Data Encryption Exclusive Line Unauthorized Modification of Maliciously modifying information flowing on the network. Encryption of Communications Channels Data Signature Exclusive Line Connecting Unauthorized Connecting unauthorized device on the network Device Connecting Unauthorized device on the network Device Inconnecting Device and its Usage Ungesting Inconnecting Device and its Usage Ungesting Inconnecting Unauthorized Unauthorized Device on the network Device Inconnecting Device and its Usage Ungesting Inconnecting Ungesting Ungesting Inconnecting Ungesting Inconnecting Ungesting	18															-	
Packet Sniffing Theft of information flowing on the network. Data Encryption Exclusive Line	70																
Data Encryption Exclusive Line Unauthorized Modification of Maliciously modifying information flowing on the network. Communication Data Connecting Unauthorized Connecting unauthorized device on the network Device Device Data Encryption Exclusive Line Encryption of Communications Channels Log Collection/Log Analysis Integrated Lag Management System Exclusive Line Connecting Unauthorized device on the network Device Restriction on Connecting Device and its Usage Log Collection/Log Analysis													3				
Data Encryption Exclusive Line Unauthorized Modification of Maliciously modifying information flowing on the network. Communication Data Connecting Unauthorized Connecting unauthorized device on the network Device Device Data Encryption Exclusive Line Encryption of Communications Channels Log Collection/Log Analysis Integrated Lag Management System Exclusive Line Connecting Unauthorized device on the network Device Restriction on Connecting Device and its Usage Log Collection/Log Analysis		1 !				1		Packet Sniffing	Theft of information flowing on the network	Encryption of Communications Channels							
Unauthorized Modification of Maliciously modifying information flowing on the network. Unauthorized Modification of Maliciously modifying information flowing on the network. Encryption of Communications Channels Data Signature Exclusive Line Connecting Unauthorized Connecting unauthorized device on the network Device Restriction on Connecting Device and its Usage Log Collection/Log Analysis								y	2.00.000								
Unauthorized Modification of Maliciously modifying information flowing on the network. Communication Data Unauthorized Modification of Maliciously modifying information flowing on the network. Data Signature Exclusive Line Connecting Unauthorized device on the network Device Connecting unauthorized device on the network Device Log Collection/Log Analysis Log Collection/Log Analysis	19																
Communication Data Data Signature Integrated Log Management System Exclusive Line Connecting Unauthorized Connecting unauthorized device on the network Device Log Collection/Log Analysis																	
Communication Data Data Signature Exclusive Line Connecting Unauthorized Connecting unauthorized device on the network Device Data Signature Exclusive Line Log Collection/Log Analysis		1				1		Unauthorized Modification of	Maliciously modifying information flowing on the network	Encryption of Communications Channels			Log Collection/Log Analysis				
Exclusive Line Connecting Unauthorized Connecting unauthorized device on the network Device Exclusive Line Log Collection/Log Analysis																	
Connecting Unauthorized Connecting unauthorized device on the network Device Connecting Unauthorized device on the network Device Connecting Unauthorized device on the network Device Unauthorized Device and its Usage Device Unauthorized Unauthorized Device on the network Device Unauthorized Device On the network Device Unauthorized Device On the network Unauthorized	20																
Device Log Collection/Log Analysis																	
Device Log Collection/Log Analysis		1				1		Connecting Unauthorized	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage			Restriction on Connecting Device and its Usage				
Integrated Log Management System	24												Log Collection/Log Analysis				
	21																

	Type of Assets ontrol System Asset	Target Device Controller (Slave)	Threat Level	Vulnerability Level	Importance of Assets		Threat (Attack Type) Unauthorized Access	Description Intrusion of the device via the network to execute an attack.	Intrusion/Spreading Phase	ection	Objective Achievement Phase	Detection/Understanding Damage IPS/IDS	Business Continuity		By Threat
1	ontrol System Asset	Controller (Slave)					I Inauthorized Access	lateration of the planta with the materials to account an establish			,	ipe/ipe			
1		, ,	1					Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type)	, ,		IF 3/ID3		'	
1							01100110112007100000		FW (Application Gateway Type)			Log Collection/Log Analysis			
2	I								One-way Gateway			Integrated Log Management System			
2									Proxy Server						
2			١.						WAF						
2			2	3		A			Peer-to-Peer Authentication						1
2									IPS/IDS						
2									Applying Patches						
2									Avoidance of Vulnerability						
2															
2							Physical Intrusion	Unauthorized access of sections/areas (device installation locations,	Entrance and Exit Management			Surveillance Camera			
2								etc.) with access restrictions.	Lock and Key Management	0		Intrusion Detection Sensor			
- 1			3	2		A		It also refers to removing restrictions on devices with physical							2
- 1								access restrictions (devices installed in racks, cabinets, etc.).							
3			3	2		A	Unauthorized Operation		Operator Authentication (ID/Pass)	0		l		\vdash	2
-								component to execute an attack. An attack triggered by a human error in operation by internal	URL Filtering/Web Reputation	\vdash					
							Human Error in Operation	personnel (an employee or partner with access privileges to the	Mail Filtering						
4			2	3		A .		device).		\vdash					1
·			-	•				An act equivalent to an attack is performed on the device as a result							
								of a proper media or device connection.							
\neg							Connecting Unauthorized	Connection of unauthorized media or device (CD/DVD, USB	Restriction on Connecting Device and its Usage	((Same as on the Left)	(Same as on the Left)			
_			١ .				Media or Device	device, etc.) brought in from outside the organization with the				Log Collection/Log Analysis			
5			2	3		A		device to execute an attack.				Integrated Log Management System			1
							Execution of Unauthorized	Unauthorized execution of legitimate programs, commands,	Permission Management		(Same as on the Left)	Device Error Detection			
				.		.	Processes	services, and other processes found on the attack target	Access Control		(Same as on the Left)	Device Alive Monitoring	1	\vdash	
6			2	3		A		device.	Application Whitelisting		(Same as on the Left)	Log Collection/Log Analysis	1	\vdash	1
									Approval of Important Operations	((Same as on the Left)	Integrated Log Management System	-	\vdash	
_									Aug. de	\vdash		D. C. F. D. L. C.			
									Anti-virus Application Whitelisting	\vdash		Device Error Detection Device Alive Monitoring	1	\vdash	
										\vdash					
7			1	3		В			Applying Patches Avoidance of Vulnerability	\vdash		Log Collection/Log Analysis Integrated Log Management System	1	\vdash	1
										\vdash		megrated edg management dystem			
									Data Signature	\vdash		 			
\dashv							Information Theft	Theft of information (software, authentication information,	Permission Management	- ((Same as on the Left)	Log Collection/Log Analysis			
								configuration settings, encryption keys and other confidential	Access Control		(Same as on the Left)	Integrated Log Management System			
8			3	3		A .		information) stored on the device.	Data Encryption		(Same as on the Left)				1
·				•		_ ^		illiornation) stored on the device.	DLP		(Same as on the Left)				
\neg							Unauthorized Modification of	Unauthorized modification of information (software,	Permission Management	((Same as on the Left)	Device Error Detection	Data Backup		
9			١.	3				authentication information, configuration settings, encryption	Access Control	((Same as on the Left)	Log Collection/Log Analysis			
,			3	•		A			Data Signature	((Same as on the Left)	Integrated Log Management System			'
							Information Destruction	Destroying of information (software, authentication			Permission Management	Device Error Detection	Data Backup		
10			3	3		A		information, configuration settings, encryption keys and other		<i></i>	Access Control	Log Collection/Log Analysis			1
								confidential information) stored on the device.		\vdash		Integrated Log Management System			
_						\vdash			Compatation/Zening		(Same as on the Left)	Log Collection/Log Analysis			
					3			Sending unauthorized control commands (settings changes,	Segmentation/Zoning Data Signature		(Same as on the Left)	Integrated Log Management System			
11			3	3		A		power shutdowns, etc.) and unauthorized data to other	Approval of Important Operations		(Same as on the Left)				1
								devices.	у фротаго ппротага орогалого	N	(came as on the con)				
\dashv							Outage	Stopping device functions.				Device Error Detection	Redundancy	0	
												Device Alive Monitoring	Failsafe Design	0	
12			3	3		A						Log Collection/Log Analysis			1
												Integrated Log Management System			
							DoS Attack	Interruption of regular device operations by sending	DDoS Countermeasures	\vdash		Device Error Detection	Redundancy	0	
			l .	_				processing requests that exceed the processing capacity of		\vdash		Device Alive Monitoring	Failsafe Design	0	
13			3	3		A		the device as a result of a DDoS attack, etc.		\vdash		Log Collection/Log Analysis			1
										\vdash		Integrated Log Management System			
-							Th-0	Device theft.	Last and Kar Manager		(Same as on the Left)	(Same as on the Left)			
14			3	2			Theft	Device trieit.	Lock and Key Management	- ((Same as on the Left)	(Same as on the Left)			2
1			"	•		A				\vdash			+	\vdash	-
\dashv							Information Theft by	Theft of information (software, authentication information,	Tamper Resistance	1	(Same as on the Left)				
			١.	_			Tampering Device at Time		Obfuscation	((Same as on the Left)				_
٥			3	2			of Theft or Disposal	information) stored on devices which were stolen or disposed of and	Zeroization	0 ((Same as on the Left)				2
								then disassembled.							
								Communications are blocked by disconnecting the	Entrance and Exit Management			Device Error Detection	Redundancy		
								communication cable.	Lock and Key management			Device Alive Monitoring			
								Alternatively, communications are blocked by pulling out the				Log Collection/Log Analysis			
16								communication cable from the device.				Integrated Log Management System			
												Surveillance Camera Intrusion Detection Sensor			
												III III USIUTI Detection Sensor			
							Notwork Congreties	Causing congestion by generating the communications traffic	EW (Docket Filtering Trans)			Device Error Detection	Redundancy		
									FW (Application Gateway Type)			Device Error Detection Device Alive Monitoring	redulidancy		
									WAF			Log Collection/Log Analysis			
17									IPS/IDS			Integrated Log Management System			
									DDoS Countermeasures			Janes and management dystem			
									DD03 Counternleasures						
-1							Jamming	Interference with radio communications.				Device Error Detection	Redundancy		
	Not applicable (no fu	unctions)					vandilly	mitoriorice with radio communications.				Device Error Detection Device Alive Monitoring	reduliuality		
18												Log Collection/Log Analysis			
												Integrated Log Management System			
	<u> </u>											, and an agent of state			
					1		Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels						
							. who ording	or information nowing on the network.	Data Encryption						
19									Exclusive Line						
									EXCUSIVE LINE						
					1		Linouthorized Marks	Moliciously modifying information flows	Engagetion of Communication Communication			Log Collection 1 A- 1			
								Maliciously modifying information flowing on the network.	Encryption of Communications Channels			Log Collection/Log Analysis Integrated Log Management System			
							Communication Data		Data Signature			inegrated Log Management System			
20									Exclusive Line						
10					I										
20					i		0	0	Destruires on Occasion Destruire			0-std0			
								Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage			Restriction on Connecting Device and its Usage			
20							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 3.3@] 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	Α	В	В	С	С	В	В	В			Α	Α
Physical Intrusion	D	С	D	D	D	D	С	С	В			В	Α
Unauthorized Operation	D	В	С	С	С	С	В	В	Α			В	Α
Human Error in Operation	D	Α	В	В	В	В	Α	Α	Α			Α	Α
Connecting Unauthorized Media or Device	D	Α	В	В	В	В	Α	Α	Α			Α	Α
Execution of Unauthorized Processes	С	В	С	С	С	D	Α	Α	Α			Α	Α
Malware Infection	D	В	С	В	В	С	Α	Α	Α			В	В
Information Theft	С	С	D	В	В	D	Α	Α	Α			Α	Α
Unauthorized Modification of Information	D	Α	В	В	В	С	Α	Α	Α			Α	Α
Information Destruction	D	В	С	В	В	С	Α	Α	Α			Α	Α
Unauthorized Transmission	D	В	С	В	В	С	Α	Α	Α			Α	Α
Outage	D	Α	В	В	в	В	Α	Α	Α			Α	Α
DoS/DDoS Attack	Е	Α	В	С	O	В	В	В	В			Α	Α
Theft	D	С	D	D	D	D	В	С	В			В	Α
When Stolen or Discarded	D	С	D	D	D	D	В	С	В			В	Α
Route Blocking			D			С				Α	Α		
Network Congestion			В			В				Α	Α		
Jamming													
Packet Sniffing			В			В				Α	Α		
Unauthorized Modification of Communication Data			В			В				Α	Α		
Connecting Unauthorized Device			В			В				Α	Α		

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
2.0	Evaluation Criteria for	4.2.2. Table 4.44
2.6	Business Impact Levels	4.3.2. Table 4-11
0.7	List Detailing Business Impacts	4.2.2. Table 4.42
2.7	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.

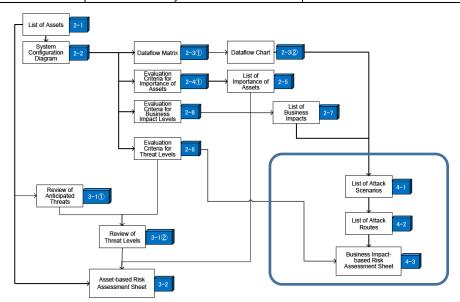


Figure 4-1: Business Impact-based Risk Analysis Work Flow

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.

Business **Business** Summary of Business Impacts and Attack Scenarios Impact Impact Level 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. Wide Area A wide area supply outage caused by the use of wide area supply outage Energy functions. Supply Attack Execution 3 Attack Target Final Attack Outage Asset 1-1 2 НМІ Controller Causes wide-area supply outage.

Table 4-3: Format of Attack Scenarios

[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

Business						Busines
Impact		Summary of Busin	ess Impacts and Attack S	cenarios (*1)		Impact Le
			attack on supply facilities,	which produces a wi	de area fuel supply outage, resulting in	
	Scenario#	Attack Scenario	Attack Execution Asset	Attack Target	Final Attack	3 (*2)
Supply Outage	1-1		нмі	Controller	Causes wide-area supply outage.	(2)
	1-2	A wide area supply outage caused by supply outage	Controller (Master)	Controller (Slave)	Sends malicious control command to cause	•
	manufacturing fa	s and explosions due to control abnormalities and a los cilities. Such attacks impact local residents and the en		r handling hazardous	materials caused by a cyber attack on	
	Item Number	Attack Scenario	Attack Execution Asset	Attack Target	Final Attack	
	2-1	abnormalities in facilities for handling hazardous	нмі	Controller	Sets incorrect target value for controller.	
		materials caused by the setting of improper target values.	Control Server	Controller	Sets incorrect target value for controller.	
Occurrence of fires and explosion	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.	3
incidents		Outbreak of fires and explosions due to erratic	нмі	НМІ	Tampers with and alters data/software in	
	2-3	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.	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.	
				_	cilities, causing significant inconvenience to	
	,				Final Attack	
	Remindinger					
	3-1	standards due to control abnormalities in production facilities caused by the setting of improper target	Control Server	Controller	Sets incorrect target value for controller.	
Supply of Defective Fuel	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.	2 (*4)
		Production of fuel that does not meet quality	НМІ	НМІ	Tampers with and alters data/software in	
	3-3	facilities caused by tampering with and altering data/software.	Control Server	Control Server	Tampers with and alters data/software in control server.	
	• .		y terminated processes du	ue to process control	abnormalities and operation monitoring	
	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	нмі	Controller	Sets incorrect target value for controller.	
		to processes being terminated for safety reasons.	Control Server	Controller	Sets incorrect target value for controller.	
					<u> </u>	
Manufacturing/ Production Disrupt/ Suspend	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.	1 (*5)
Production Disrupt/		by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs. This leads to processes being terminated for safety reasons. Operational abnormalities in production facilities caused by tampering with and altering data/software.	EWS	Controller	(such as threshold values). Tampers with	
Production Disrupt/	4-2 4-3	by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs. This leads to processes being terminated for safety reasons. Operational abnormalities in production facilities			(such as threshold values). Tampers with and alters data/software in controller. Tampers with and alters data/software in	
Production Disrupt/		by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs. This leads to processes being terminated for safety reasons. Operational abnormalities in production facilities caused by tampering with and altering data/software. This leads to processes being terminated for safety	нмі	нмі	(such as threshold values). Tampers with and alters data/software in controller. Tampers with and alters data/software in HMI. Tampers with and alters data/software in	
Production Disrupt/ Suspend	4-3 4-4 A cyber attack o	by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs. This leads to processes being terminated for safety reasons. Operational abnormalities in production facilities caused by tampering with and altering data/software. This leads to processes being terminated for safety reasons. A destructive malware or ransomware infection that disables monitoring of production facilities and prevent monitoring control. This leads to processes	HMI Control Server	HMI Control Server	(such as threshold values). Tampers with and alters data/software in controller. Tampers with and alters data/software in HMI. Tampers with and alters data/software in control server. Infects the system with destructive malware and ransomware, disabling monitoring operations.	
Production Disrupt/ Suspend Leak of	4-3 4-4 A cyber attack o	by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs. This leads to processes being terminated for safety reasons. Operational abnormalities in production facilities caused by tampering with and altering data/software. This leads to processes being terminated for safety reasons. 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. In the control system, resulting in an external leak of colleading to a deterioration in competitive strength.	HMI Control Server	HMI Control Server	(such as threshold values). Tampers with and alters data/software in controller. Tampers with and alters data/software in HMI. Tampers with and alters data/software in control server. Infects the system with destructive malware and ransomware, disabling monitoring operations.	(*5)
Production Disrupt/ Suspend	4-3 4-4 A cyber attack o	by the malicious modification of settings (thresholds, etc.) or tampering with and altering programs. This leads to processes being terminated for safety reasons. Operational abnormalities in production facilities caused by tampering with and altering data/software. This leads to processes being terminated for safety reasons. 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 Control Server HMI company production secret	HMI Control Server HMI s, impacting the comp	(such as threshold values). Tampers with and alters data/software in controller. Tampers with and alters data/software in HMI. Tampers with and alters data/software in control server. Infects the system with destructive malware and ransomware, disabling monitoring operations.	
	Occurrence of fires and explosion incidents Supply of Defective Fuel	Wide Area Fuel Supply Outage 1-1 1-2 Outbreak of fires manufacturing fatrust in the complement lem Number 2-1 Occurrence of fires and explosion incidents 2-3 Manufacturing a customers, signitem Number 3-1 Supply of Defective Fuel 3-2 Manufacturing a customers and customers are customers are customers and customers are customers are customers are customers are customers and customers are custome	significant social impacts and a dramatic loss of trust in the company. Wide Area Fuel Supply Outage 1-1	Supply Outage Scenario # Attack Scenario Attack Execution Asset	significant social impacts and a dramatic loss of trust in the company. Scenario #	Supply Outage Supply Outage Attack Scenario Attack Scenari

- *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

	Who	From Where	0.10	How		Attack		
Attack						Execution	Attack	Final Attack
Scenario	Attacker	Attack Entry Point	Attack Path 1	Attack Path 2	Attack Path 3	Asset	Target	
1-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		НМІ	Controller	Causes wide- area supply outage.
1-1	Malicious Third Party	Information Network	FW			НМІ	Controller	Causes wide- area supply outage.
1-1	Insider (Human Error)	HMI (Physical Intrusion)				НМІ	Controller	Causes wide- area supply outage.
1-2	3					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)

				Table 4	-6: List of Atta	ick Roules (Sorted by S	cenano)	
Attack Tree	Scenario	Who	From Where					How	
Number	Number	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			НМІ	Controller	Causes wide-area supply outage.
1-2	1-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		НМІ	Controller	Causes wide-area supply outage.
1-3	1-1	Insider (Human Error)	HMI (Physical Intrusion)				НМІ	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)	- cas contain (crossy)			Controller (M)	Controller (S)	Sends malicious control command to cause supply outage.
	Scenario #			Attack Path 1	Attack Path 2	Attack Path 3	Attack Execution Asset	Attack Target	Final Attack
Tree #		Attacker	Attack Entry Point	FW	Attack Fatil 2	Allack Fall 3			
2-1	2-1	Malicious Third Party	Information Network				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)				НМІ	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			НМІ	НМІ	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		нмі	нмі	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)				нмі	нмі	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			НМІ	Control Network (Field Side)	Maliciously modifies network settings and disables communications.
2-17	2-4	Malicious Third Party	Information Network	FW			нмі	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		НМІ	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		НМІ	Control Network (Field Side) Control Network (Field Side)	Infects with malware causing unauthorized communications, and disables communications. Malicipus by modifies network settings and disables communications.
		Insider (Human Error)	HMI (Physical Intrusion)						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			НМІ	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		НМІ	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)				НМІ	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			НМІ	НМІ	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		НМІ	НМІ	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)				НМІ	НМІ	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			нмі	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.
4-4	4-1	Insider (Human Error)	HMI (Physical Intrusion)	Saturnatorian (Nelay)	- Sta i notorian		HMI	Controller	Sets incorrect target value for controller.
			Control Server (Physical Intrusion)						-
4-6	4-1	Insider (Human Error)		EW			Control Server	Controller	Sets incorrect target value for controller. Malicipus wordings actions of controller (such as threshold values). Tempers with and alters databathurse is controller.
4-7	4-2	Malicious Third Party	Information Network	FW	Deta Historia		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		НМІ	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)				нмі	НМІ	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			НМІ	НМІ	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		нмі	нмі	Infects the system with destructive malware and ransomware, disabling monitoring operations.
4-18	4-4	Insider (Human Error)	HMI (Physical Intrusion)				нмі	НМІ	Infects the system with destructive malware and ransomware, disabling monitoring operations.
4-19	4-4	Insider (Human Error)	EWS (Physical Intrusion)				нмі	НМІ	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.
	-						l .	l	*** *** * *

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

Attack	0	Who	From Where				-	łow	
Tree	Scenario Number			Attack Dath 4	Attack Dath 2	Attack Dath 2			Final Attack
Number		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			НМІ	HMI	Tampers with and alters data/software in HMI.
1-2	3-3	Malicious Third Party	Information Network	FW			НМІ	НМІ	Tampers with and alters data/software in HMI.
1-3	4-3	Malicious Third Party	Information Network	FW			HMI	НМІ	Tampers with and alters data/software in HMI.
1-4	4-4	Malicious Third Party	Information Network	FW			HMI	НМІ	Infects the system with destructive malware and ransomware, disabling monitoring operations.
1-5	1-1	Malicious Third Party	Information Network	FW			НМІ	Controller	Causes wide-area supply outage.
1-6	2-1	Malicious Third Party	Information Network	FW			НМІ	Controller	Sets incorrect target value for controller.
1-7	3-1	Malicious Third Party	Information Network	FW			НМІ	Controller	Sets incorrect target value for controller.
1-8	4-1	Malicious Third Party	Information Network	FW			НМІ	Controller	Sets incorrect target value for controller.
1-9	2-4	Malicious Third Party	Information Network	FW			НМІ	Control Network (Field Side)	Maliciously modifies network settings and disables communications.
1-10	2-4	Malicious Third Party	Information Network	FW			НМІ	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		Malicious Third Party	Information Network	FW			Control Server	Control Server	Tampers with and alters data/software in control server.
1-14		Malicious Third Party	Information Network	FW			Control Server	Control Server	Theft of confidential information stored on the control server.
1-15		-	Information Network	FW			Control Server	Controller	
		Malicious Third Party							Sets incorrect target value for controller.
1-16		Malicious Third Party	Information Network	FW			Control Server	Controller	Sets incorrect target value for controller.
1-17		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		нмі	нмі	Tampers with and alters data/software in HMI.
2-2		Malicious Third Party	Monitoring Terminal	,	Data Historian		НМІ	НМІ	Tampers with and alters data/software in HMI.
2-3		Malicious Third Party	Monitoring Terminal		Data Historian		НМІ	НМІ	Tampers with and alters data/software in HMI.
2-4	-	Malicious Third Party	Monitoring Terminal		Data Historian		нмі	нмі	Infects the system with destructive malware and ransomware, disabling monitoring operations.
	-		_						
2-5	-	Malicious Third Party	Monitoring Terminal		Data Historian		HMI	Controller	Causes wide-area supply outage.
2-6		Malicious Third Party	Monitoring Terminal		Data Historian		НМІ	Controller	Sets incorrect target value for controller.
2-7	3-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		НМІ	Controller	Sets incorrect target value for controller.
2-8	4-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		НМІ	Controller	Sets incorrect target value for controller.
2-9	2-4	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		НМІ	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		НМІ	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	-	Malicious Third Party	Monitoring Terminal		Data Historian		Control Server	Controller	Sets incorrect target value for controller.
2-16		Malicious Third Party	Monitoring Terminal		Data Historian		Control Server	Controller	Sets incorrect target value for controller.
2-17	-	-	_		Data Historian		Control Server	Controller	Sets incorrect target value for controller.
	-	Malicious Third Party	Monitoring Terminal	, ,,,					•
2-18	5-1	Malicious Third Party	Monitoring Terminal	, ,,,	Data Historian		EWS	EWS	Theft of confidential information stored on the EWS.
2-19	2-2	Malicious Third Party	Monitoring Terminal	. ,,,	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)				НМІ	НМІ	Tampers with and alters data/software in HMI.
3-2	3-3	Insider (Human Error)	HMI (Physical Intrusion)				нмі	НМІ	Tampers with and alters data/software in HMI.
3-3	4-3	Insider (Human Error)	HMI (Physical Intrusion)				нмі	НМІ	Tampers with and alters data/software in HMI.
3-4	4-4	Insider (Human Error)	HMI (Physical Intrusion)				НМІ	НМІ	Infects the system with destructive malware and ransomware, disabling monitoring operations.
3-5		Insider (Human Error)	HMI (Physical Intrusion)				нмі	Controller	Causes wide-area supply outage.
3-6	2-1	Insider (Human Error)	HMI (Physical Intrusion)				нмі	Controller	Sets incorrect target value for controller.
									-
3-7		Insider (Human Error)	HMI (Physical Intrusion)				HMI	Controller	Sets incorrect target value for controller.
3-8		Insider (Human Error)	HMI (Physical Intrusion)				HMI	Controller	Sets incorrect target value for controller.
3-9	2-4	Insider (Human Error)	HMI (Physical Intrusion)				НМІ	Control Network (Field Side)	Maliciously modifies network settings and disables communications.
3-10	2-4	Insider (Human Error)	HMI (Physical Intrusion)				НМІ	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)				НМІ	НМІ	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.
3-20	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		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.

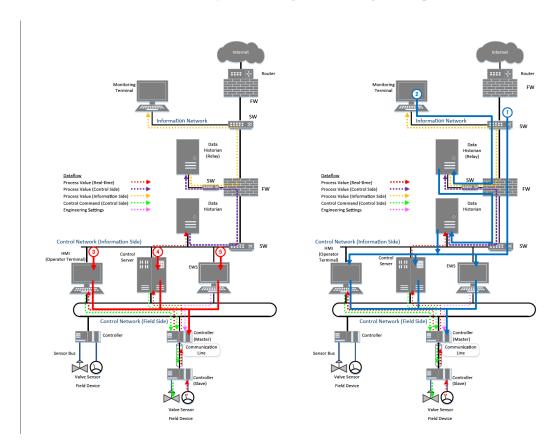


Figure 4-2: Attack Route Diagram

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

	Attack Scenario		Assessment Metrics					Securit	ty Level	Attack T	ree Number		
Item Number		Attack Tree/Attack Steps	Threat Level Vulnerability Level	Business Impact Level	Risk Value	Pro Intrusion/ Spreading Phase	Objective Achievement Phase	Detection/ Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
1	1-1	A wide area supply outage caused by the use of wide area supply of 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".	utage functions.			FW OPer-to-Peer Authentication Applying Patches Avoidance of Vulnerability Permission Management OPER OPER OPER OPER OPER OPER OPER OPER	(Same as on the left)	IPS/IDS Log CollectionLog Analysis stagulate 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	В	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 O	(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	В		Same as ite	em 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	Α	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 be Attack Entry Point = Information Network	ing sent to multiple contro	llers.									
10		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 Hegyated 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	В	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 Hegysted Log Management System		1	2	#1-4	10,11,12,1
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 it	em number 4		2 *1			
15		Unauthorized access of the data historian from the data historian (relay) by a mallcious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as ite	em 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 ite	m 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	В		Same as ite	m number 13		1	2	#1-5	14,15,16,1 7,18
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 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	Α	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
х													

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

2. Occurrence of Fires and Explosion Incidents

E At			e of Fires and Explosion Incidents Countermeasures Countermeasures									Attack T	ree Number
Number	2-1	Attack Tree/Attack Steps Outbreak of fires and explosions due to control abnormalities in fac	Threat Level	Vulnerability Level	Business Impact Level Risk Value	Intrusion/ Spreading Phase	Objective Achievement Phase	Detection/ Understanding Damage	Business Continuity	Attack Steps	y Level Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
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".		ilig Hazaruut	is materials Caused by the	setting of improper te	Same as ite	em 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 ite	em number 2		2			
24	2-1	Abnormal control of facilities for handling hazardous materials du to the setting of inappropriate target values for the controller from the HMI by a malicious third party.		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 В	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 ite	em number 4		2 *1			
28		Unauthorized access of the data historian from the data historian (relay by a mallicious third party. * Unauthorized access includes "execution of unauthorized processes"					Same as ite	em 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 ite	em number 6		2			
30	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values fo the controller from the HMI by a malicious third party.	2	2	3 B		Same as iter	m number 24		1	2	#2-3	27,28,29,3
31		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes". [Abnormal control of facilities for handling hazardous				Peer-to-Peer Authentication Applying Patches Avoidance of Vulnerability Permission Management O		IPS/IDS Log Collection/Log Analysis Integrated Log Management Bystem Device Alive Monitoring		2			
32	2-1	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 iter	m number 26		1	2	#2-4	27,28,31,3
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 bein 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".	9			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
37		Outbreak of fires and explosions due to control abnormalities in factor 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".		ing hazardou	s materials caused by the	e malicious modificatio	,	s, etc.) or tampering wit	h and altering program	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).	1010101010101010101010101010101010				Same as iter	m 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 В	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 ite	em 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 ite	em 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 iter	m 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 iter	m number 39		1	2	#2-8	40,41,42,4
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 iter	m 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)

	nce of Fires and Explosion Incidents		A	ent Metrics			Counto			Coourit	v I evel	Attack 7	Trop Numbe
Attack	Scenario Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Pi Intrusion/ Spreading Phase	rotection Objective Achievemen	Detection/ nt Understanding Damage	Business Continuity	Security Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
2-1	Outbreak of fires and explosions due to control abnormalities in facil							vents a proper response	e, even when operations	are perfor	med corre	ctly.	
6	Attack Entry Point = Information Network Unauthorized frewall 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							item number 1		2 *1			
7	of unauthorized processes". 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			
8 2-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	3	В	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	46,47,4
9	Unauthorized access of the control server via the FW by a malicious third party. * Unauthorized access includes *execution of unauthorized processes* (privilege escalation).					Data Signature		tem number 25		2			
0 2-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	3	В	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,
1	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). Countempasures used tor the two threats are merged. Tallet lost is used to dender the "execution of unauthorized processes".						Same as	item number 4		2 *1			
2	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 i	item number 28		2			
3	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			
4 2-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	3	В		Same as i	item number 48		1	2	#2-12	51,52,5 4
5	Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".						Same as i	item number 31		2			
6 2-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	3	В		Same as i	tem number 50		1	2	#2-13	51,52,5 6
7	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			
8 2-3	Tampering with and altering data/software in the HMI by malware infection.	2	3	3	Α	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	57,5
9	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 i	tem number 35		2 *2			
0 2-3	Tampering with and altering data/software in the control server by malware infection.	2	2	3	В	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	59,6
1	Outbreak of fires and explosions caused by a loss of monitoring and Attack Entry Point = Information Network Unauthorized frewall 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*.	d monitoring c	ontrol at faci	ilities for hand	dling hazardou	us materials due to d	-	network (field side). item number 1		2 *1			
2	Unauthorized access of the HMI via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Permission Management	Same as	item number 2	Data Backup	2			
3 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 mallicious third party. This prevents the monitoring of the control system.	2	2	3	В	Access Control Data Signature Anti-virus	(Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System Device Error Detection	Data Dackup	1	2	#2-16	61,62
4 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	В	Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature		Device Alive Monitoring Log Collection/Log Analysis resprated Log Management Bystem		1	2	#2-17	61,62
5	Attack Entry Point = Monitoring Terminal Unauthorized access of the dath silstorian (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, fallic text is used to denote the "execution of unauthorized processes".						Same as	item number 4		2 *1			
6	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			
7	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			
8 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	В		Same as i	tem number 63		1	2	#2-18	65,66, 8
9 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	В		Same as i	item number 64		1	2	#2-19	65,66, 9
0	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			
1 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	А		Same as i	tem number 63		1	1	#2-20	70,
2 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	А		Same as i	item number 64		1	1	#2-21	70,
3	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 i	tem number 19		1 *2			
4 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	А	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 **rteg sted Log Management System	Data Backup	1	1	#2-22	73,
5 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	А	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 tricg alid Log Management System	Data Backup	1	1	#2-23	73,7

73

[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

3. Sı	apply of	of Defective Product												
Item Number		Attack Tree/Attack Steps Production of a product that does not meet quality standards/criteria	Threat Level	ilnerability Level	Business Impact Level		Intrusion/ Spreading Phase	Countern tection Objective Achievement Phase	Detection/ Understanding Damage	Business Continuity	Securit Attack Steps	Attack Tree	Attack 1 Attack Tree Number	Configuration Steps (Item Number)
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".	ude to control an	on On Taille	es in product		auseu by the setting t	Same as ite			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 ite			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	С	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		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 iter	n 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	С	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 ite	m 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 ite	m 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". Production of a product that does not meet quality						Same as ite	m number 6		2			
84	3-1	standards/criteria due to the setting of imporporiate target values for the controller from the HMI by a malicious third party.	2	2	2	С	ı	Same as iter	n number 78		1	2	#3-3	81,82,83,8
85		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes". Production of a product that does not meet quality						Same as iter	n number 31		2			
86	3-1	standards/criteria due to the setting of impropropriate target values for the controller from the control server by a malicious third party.	2	2	2	С		Same as iter	n number 80		1	2	#3-4	81,82,85,8
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 ite	m 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	В		Same as iter	m 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 iter	n 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	С		Same as iter	n number 80		1	2	#3-6	89,90
91		Production of a product that does not meet quality standards/criteria 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".	due to control ab	bnormalitie	es in product	ion facilities o	aused by the maliciou	us modification of setting Same as ite		ampering with and alter	ing progra 2 *1	ams.		
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 iter	n 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	С	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 httg://decl.og/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 ite	m 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 ite	m 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 iter	n 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	С		Same as iter	n number 93		1	2	#3-8	94,95,96,9
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 iter	n 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	В		Same as iter	n 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

		Scenario			Assessme	nt Metrics			Counterm	neasures		Securit	y Level	Attack T	ree Number
tem	, maok	Coonario			. 1003001116			Drof	ection			Count	, 20701	,uon I	
Item Number			Attack Tree/Attack Steps	Threat Level	Vuinerability 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)
Ψ.	3-1	Production of a p	product that does not meet quality standards/criteria	due to contro	l abnormaliti	L es in product	ion facilities o	caused by the setting o	of improper target values	S					
	3-3	Production of a p	product that does not meet quality standards/criteria	due to contro	l abnormaliti	es in product	ion facilities o	caused by tampering w	vith and altering data/sof	ftware.					
100		Unauthorized firewall * Unauthorized acces escalation). Countern	Information Network access by a malicious third party. s includes "execution of unauthorized processes" (privilege leasures used for the two threats are merged. Italic text is used to of unauthorized processes".						Same as ite	m number 1		2 *1			
101			ized access of the HMI via the FW by a malicious third party. rized access includes "execution of unauthorized processes".						Same as ite	m number 2		2			
102	3-3		Tampering with and altering data/software in the HMI by a malicious third party.	2	2	2	С		Same as iten	n number 48		1	2	#3-10	100,101,10 2
103		third party * Unautho	ized access of the control server via the FW by a malicious						Same as iten	n number 25		2			
104	3-3		Tampering with and altering data/software in the control server by a malicious third party.	2	2	2	С		Same as iten	n number 50		2	2	#3-11	100,103,10 4
105		* Unauthorized access inc	onitoring Terminal e data historian (relay) from a monitoring terminal by a malicious third party. dudes "execution of unauthorized processes" (privilege escalation). If the two threats are merged. Italic text is used to denote the "execution of						Same as ite	m number 4		2 *1			
106		by a malic	ized access of the data historian from the data historian (relay) icious third party. prized access includes "execution of unauthorized processes".						Same as ite	m 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 ite	m number 6		2			
108	3-3		Tampering with and altering data/software in the HMI by a malicious third party.	2	2	2	С		Same as iten	n number 48		1	2	#3-12	105,106,10 7,108
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 iten	n number 31		2			
110	3-3		Tampering with and altering data/software in the control server by a malicious third party.	2	2	2	С		Same as iten	n number 50		1	2	#3-13	105,106,10 9,110
111		connected to a male	t = HMI by an insider, the HMI is infected with malware after being vare-infected USB storage device. of actions by an insider, it is assumed that there is no threat ppt at "connecting to unauthorized media".						Same as iter	m number 8		1 *2			
112	3-3	Tamperin infection.	g with and altering data/software in the HMI by malware	2	3	2	В		Same as iten	n number 58		1	1	#3-14	111,112
113		connected to a malwa	= Control Server y an insider, the control server is infected with malware after being tre-infected USB storage device. of actions by an insider, it is assumed that there is no threat of a connecting to unauthorized media*.						Same as iten	n number 35		3 *2			
114	3-3	Tamperin malware i	g with and altering data/software in the control server by nfection.	2	2	2	С		Same as iten	n number 60		2	2	#3-15	113,114
х															
ш	[No	1-3													

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

4. Manufacturing/Production Disrupt/Suspend

				_										
tem Number		Attack Tree/Attack Steps Control abnormalities in production facilities caused by the setting of	Threat Level	Vuinerability Level	Business Impact Level	Risk Value	Intrusion/ Spreading Phase	Counterment otection Objective Achievement Phase	Detection/ Understanding Damage	Business Continuity	Security Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
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".	прорега	get values.	ilis leads to p	lucesses De	ing terrimated for sa	Same as item	ı 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	 	og Collection/Log Analysis egrated Log Management System		1	2	#4-1	117,118,11 9
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		og Collection/Log Analysis egrated Log Management System		1	2	#4-2	117,118,12 0
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	ı 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	ı 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 r	number 119		1	2	#4-3	121,122,12 3,124
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	Abnormatises 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 partly.	2	2	1	D		Same as item r	number 120		1	2	#4-4	121,122,12 5,126
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	ı 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		og Collection/Log Analysis egrated 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	·····	og Collection/Log Analysis sgrated Log Management System		1	2	#4-6	129,130
131		Control abnormalities in production facilities caused by the malicious 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".	<u>modification</u>	of settings (thresholds, et	c.) or tampeı	ing with and altering	programs. This leads to programs.		inated for safety reasons	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) Lo	evice Error Detection og Collection/Log Analysis sgrated Log Management System	Data Backup	1	2	#4-7	131,132,13 3
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 mallicious 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 r	number 133		1	2	#4-8	134,135,13 6,137
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		evice Error Detection og Collection/Log Analysis egrated Log Management System	Data Backup	1	1	#4-9	138,139

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

		rring/Production Disrupt/Suspend	Assessme	nt Matrice	Countermeasures	Securit	u Lovel	Attack T	ree Number
tem	Allack	Scenario			Protection Detection/			Attack	Configuration
Number	4-1	Attack Tree/Attack Steps Control abnormalities in production facilities caused by the setting of		Business Impact Level Risk Value	Spreading Phase Phase Damage	Attack Steps	Attack Tree	Tree Number	Steps (Item Number)
		Operational abnormalities in production facilities caused by tamperin Attack Entry Point = Information Network							
140		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	140,141,14 2
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	140,143,14 4
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	145,146,14 7,148
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	145,146,14 9,150
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 monitor Attack Entry Point = Information Network	ring of production facilities	and prevent monitoring	control. This leads to processes being terminated for safety reasons.				
155		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". Unauthorized access of the HMI via the FW by a malicious third party.			Same as item number 1	2 *1			
156		* Unauthorized access includes "execution of unauthorized processes".			Same as item number 2 Anti-virus Permission Management Device Error Detection Data Backup	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	Application Whitelisting Access Control Device Alive Monitoring Applying Patches Log Collection Log Analysis Avoidance of Vulnerability Data Signature	1	2	#4-16	155,156,15 7
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.			Same as item number 5	2			
160		* Unauthorized access includes "execution of unauthorized processes". 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	158,159,16 0,161
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 Permission Management Device Error Detection Data Backup Application Whitelisting Access Control Device Alive Monitoring Applying Patches Log ColectionLog Analysis Avoidance of Vulnerability Integrate Log Management System Data Signature Device Error Detection Data Backup Data Signature Device Alive Monitoring Data Signature Device Error Detection Data Backup Data Backup Device Alive Monitoring Device Alive Monito	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			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 Permission Management Device Error Detection Data Backup Application Whitelisting Access Control Device Alive Monitoring Applying Patches Log Collection/Log Analysis Avoidance of Vulnerability Bata Signature	1	1	#4-19	164,165
х									

[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

=	Attack	Scenario		Assessme	ent Metrics			Counter	measures		Securi	ty Level	Attack T	ree Number
Item 7							Pro	tection	Detection/				Attack	Configuration
Number		Attack Tree/Attack Steps	Threat Level	Vuinerability Level	Business Impact Level	Risk Value	Intrusion/ Spreading Phase	Objective Achievement Phase	t Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Tree Number	Steps (Item Number)
	5-1	Theft of company production secrets stored on the control system, r	esulting in an	external info	rmation 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 it	em 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).							em 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	В	Permission Management O Access Control Data Encryption DLP	(Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		2	2	#5-1	166,167,16 8
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 ite	em 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	В	Permission Management Access Control Data Encryption DLP	(Same as on the left)	Log Collection/Log Analysis integrated Log Management System		1	2	#5-2	166,169,17 0
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 it	em 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 it	em 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 ite	em 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	В		Same as ite	m number 168		1	2	#5-3	171,172,17 3,174
175		Unauthorized access of the EWS from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".						Same as ite	em 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	В		Same as ite	m number 170		1	2	#5-4	171,172,17 5,176
х														

[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

Assessment Metrics

Countermeasures

Countermeasures

Countermeasures

Countermeasures

A	ttack	Scenario		Assessme	nt Metrics				measures		Securit	y Level	Attack 1	ree Number
		Attack Tree/Attack Steps	Threat Level	Vuinerability Level	Business Impact Level	Risk Value	P Intrusion/ Spreading Phase	Objective Achievemen	Detection/ t Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
	1-2	1-1: A wide area supply outage caused by the use of wide area sup 1-2: A wide area supply outage caused by supply outage command	ls being sent t	to multiple co										
Item Nu	2-2	 2-1: Outbreak of fires and explosions due to control abnormalities in 2-2: Outbreak of fires and explosions due to control abnormalities in 2-3: Outbreak of fires and explosions due to erratic behavior in facilities 	facilities for h	andling haza	rdous materi	als caused b	y the malicious modi	ification of settings (thresh				formed co	rrectly.	
Number	2-4	2-4: Outbreak of fires and explosions caused by a loss of monitoring 3-1: Production of a product that does not meet quality standards/cri	g and monitori	ing control at	facilities for h	nandling haza	rdous materials due	to congestion in the contr	ol network (field side).					
	3-3	 3-2: Production of a product that does not meet quality standards/cri 3-3: Production of a product that does not meet quality standards/cri 4-1: Control abnormalities in production facilities caused by the setting 	iteria due to c	ontrol abnorn	nalities in pro	duction facilit	ies caused by tampe	ering with and altering data) or tampering with and a	Itering pro	grams.		
	4-2	4-2: Control abnormalities in production facilities caused by the malid 4-3: Operational abnormalities in production facilities caused by tam	cious modifica	ation of setting	gs (threshold	s, etc.) or tan	npering with and alte	ering programs. This leads		erminated for safety reaso	ons.			
		4-4: A destructive malware or ransomware infection that disables mo 5-1: Theft of company production secrets stored on the control syste				eak.	ng control. This leads	s to processes being term		ons.		18888888888	8888888888	
1		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Peer-to-Peer Authentication Applying Patches	0	IPS/IDS Log Collection/Log Analysis Integrated Log Management System		2 *1			
Н		Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Avoidance of Vulnerability Permission Management Peer-to-Peer Authentication	O (Same as on the left) O	Device Alive Monitoring IPS/IDS		'			
2		Unauthorized access of the HMI via the FW by a malicious third party. *Unauthorized access includes *execution of unauthorized processes".					Applying Patches Avoidance of Vulnerability Permission Management		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	В	Permission Management Access Control	(Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis	Data Backup	1	2	#1-1	1,2,3
4	3-3	Tampering with and altering data/software in the HMI by a	2	2	2	С	Data Signature	(Same as on the left)	integrated Log Management System		1	2	#1-2	124
	3-3	malicious third party.	2	2				Same as ne	em number 3				#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			em number 3		1	2	#1-3	1,2,5
6		Infection of the HMI with destructive malware (ransomware, etc.) by a malicious third party. This prevents the monitoring	2	2	1	D	Anti-virus Application Whitelisting	Permission Management Access Control	Device Error Detection Device Alive Monitoring	Data Backup	1	2	#1-4	1,2,6
	4-4	of the control system.	2	2	'	D	Applying Patches Avoidance of Vulnerability Data Signature		Log Collection/Log Analysis Integrated Log Management System		•	2	#1-4	1,2,0
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	В	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		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	2	2	3	В	Approval of Important Operations Segmentation/Zoning Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis		1	2	#1-6	1,2,8
	0.4	malicious third party. Production of a product that does not meet quality standards/criteria due	0	2			Approval of Important Operations	(Same as on the left)					#4.7	100
9	3-1	to the setting of inappropriate target values for the controller from the HMI by a malicious third party. Abnormalities in the manufacturing facilities requiring an emergency stop of	2	2	2	C		Same as ite	em number 8		1	2	#1-7	1,2,9
10	4-1	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			em 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	В	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		Infection of the HMI with malware by a malicious third party to cause unauthorized communication with the control	2	2	3	В	Anti-virus Application Whitelisting		Device Error Detection Device Alive Monitoring		1	2	#1-10	1 2 12
	2-4	network (field side) and prevent control network communications. This prevents the monitoring of the control system.	2	2	3	Ь	Applying Patches Avoidance of Vulnerability Data Signature		Log Collection/Log Analysis Integrated Log Management System		•	2	#1-10	1,2,12
13		Unauthorized access of the control server via the FW by a malicious third party.					Peer-to-Peer Authentication Applying Patches		IPS/IDS Log Collection/Log Analysis		2			
		*Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Permission Management Application Whitelisting Permission Management	(Same as on the left) (Same as on the left) (Same as on the left)	Device Alive Monitoring Device Error Detection	Data Backup				
14	2-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	3	В	Access Control Data Signature	(Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		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	С		Same as ite	m 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 ite	m 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	В	Permission Management Access Control Data Encryption DLP	(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	В	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		1	2	#1-15	1,13,18
19	3-1	Production of a product that does not meet qualify 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	С			m 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 ite	m 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"					Peer-to-Peer Authentication Applying Patches	(Same as or the Left)	IPS/IDS Log Collection/Log Analysis		1			
		(privilege escalation).					Permission Management Application Whitelisting Permission Management	(Same as on the left) (Same as on the left) (Same as on the left)	Device Alive Monitoring Log Collection/Log Analysis		'			
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	В	Access Control Data Encryption DLP	(Same as on the left) (Same as on the left) (Same as on the left)	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	В	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	С		Same as ite	m 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			m 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 mallicious third party. Supply outage encompassing a wide area.	2	2	3	В	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								- South and total						
1	[Note]		rmeasures.											nununararararararararararararararararara

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

Attack Scenario

Assessment Metrics

Countermeasures

Security Level

Assessment Metrics

	Attack	Scenario			Assessme	nt Metrics			Counter	rmeasures		Securit	y Level	Attack T	ree Number
		Attack	Tree/Attack Steps	Threat Level	Vulnerability	Business	Risk Value	Pro Intrusion/	Objective Achievemen	Detection/ t Understanding	Business Continuity	Attack	Attack	Attack Tree	Configuration Steps (Item
			·		Level	Impact Level		Spreading Phase	Phase	Damage		Steps	Tree	Number	Number)
	1-1 1-2		outage caused by the use of wide area sup outage caused by supply outage command			ntrollers.									
Item	2-1 2-2		explosions due to control abnormalities in explosions due to control abnormalities in		-					sholds, etc.) or tamperin	ng with and altering prog	rame			
Z Z	2-3	2-3: Outbreak of fires and	explosions due to erratic behavior in facil	ities for handli	ng hazardou	s materials w	here the una	uthorized modification	of data and programs	prevents a proper resp	onse, even when opera		erformed o	correctly.	
Number	2-4 3-1		I explosions caused by a loss of monitorin uct that does not meet quality standards/cr	-	-		-		-	,					
7	3-2 3-3	The second secon	uct that does not meet quality standards/cruct that does not meet quality standards/cr							- 1	.) or tampering with and	altering pr	ograms.		
	4-1	4-1: Control abnormalities	s in production facilities caused by the sett	ing of imprope	er target value	es. This leads	to processe	s being terminated for	or safety reasons.						
	4-2 4-3		s in production facilities caused by the mal alities in production facilities caused by tan			0 ()	, , , , , , , , , , , , , , , , , , , ,	,			erminated for safety rea	sons.			
	4-4 5-1		re or ransomware infection that disables moduction secrets stored on the control syst					ng control. This leads	to processes being ter	minated for safety reas	ons.				
			an (relay) from a monitoring terminal by a malicious third party.					Peer-to-Peer Authentication Applying Patches		IPS/IDS Log Collection/Log Analysis		2			
28			tion of unauthorized processes" (privilege escalation). ats are merged. Italic text is used to denote the "execution of					Avoidance of Vulnerability Permission Management	(Same as on the left)	Integrated Log Management System Device Alive Monitoring		*1			
		Unauthorized access	s of the data historian from the data historian (relay))				Peer-to-Peer Authentication Applying Patches		IPS/IDS Log Collection/Log Analysis					
29		by a malicious third p	party. ess includes "execution of unauthorized processes".					Avoidance of Vulnerability		Integrated Log Management System		2			
			zed access of the HMI from the data historian by a					Permission Management Peer-to-Peer Authentication		Device Alive Monitoring IPS/IDS					
30			orized access includes "execution of unauthorized					Applying Patches Avoidance of Vulnerability		Log Collection/Log Analysis Integrated Log Management System		2			
		processes						Permission Management		Device Alive Monitoring					28,29,30,3
31	2-3		Tampering with and altering data/software in the HMI by a malicious third party.	2	2	3	В		Same as i	tem number 3		1	2	#2-1	1
	0.0		Tampering with and altering data/software in the	_					-				_	,,,,	28,29,30,3
32	3-3		HMI by a malicious third party.	2	2	2	С		Same as i	tem number 3		1	2	#2-2	2
33	4-3		Tampering with and altering data/software in the	2	2	1	D		Same as i	tem number 3		1	2	#2-3	28,29,30,3
			HMI by a malicious third party.	_		•			22.110 40 1			·	-	,,0	3
			Infection of the HMI with destructive malware												28,29,30,3
34	4-4		(ransomware, etc.) by a malicious third party. This prevents the monitoring of the control system.	2	2	1	D		Same as i	tem number 6		1	2	#2-4	4
35	1-1		Supply outage encompassing a wide area caused by a malicious third party using wide area supply outage functions	2	2	3	В		Same as i	tem number 7		1	2	#2-5	28,29,30,3
			on the controller from the HMI.												
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	В		Same as i	tem number 8		1	2	#2-6	28,29,30,3
			Production of a product that does not meet quality												28,29,30,3
37	3-1		standards/criteria due to the setting of inappropriate target values for the controller from the HMI by a malicious third party.	2	2	2	С		Same as i	tem number 8		1	2	#2-7	7
38	4-1		Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to	2	2	1	D		Same as i	tem number 8		1	2	#2-8	28,29,30,3
			the setting of inappropriate target values to the controller from the HMI by a malicious third party.			· 						·	_		8
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	2	2	3	В		Same as it	em number 11		1	2	#2-9	28,29,30,3
			of the control system.												
40			Infection of the HMI with malware by a malicious third party to cause unauthorized communication with the control network (field side) and prevent	2	2	3	В		Same as it	em number 12		1	2	#2-10	28,29,30,4
	2-4		control network communications. This prevents the monitoring of the control system.	_	-	, o	D		Carrio do la	ommunistr 12		ı '	_	#2 10	0
			zed access of the control server from the data					Peer-to-Peer Authentication		IPS/IDS					
41		historian b	by a malicious third party. brized access includes "execution of unauthorized					Applying Patches Avoidance of Vulnerability		Log Collection/Log Analysis Integrated Log Management System		1			
		processes						Permission Management		Device Alive Monitoring					00.00.44.4
42	2-3		Tampering with and altering data/software in the control server by a malicious third party.	2	2	3	В		Same as it	em number 14		1	2	#2-11	28,29,41,4
40			Tampering with and altering data/software in the	2					0			4	_	#0.40	28,29,41,4
43	3-3		control server by a malicious third party.	2	2	2	С		Same as its	em number 14		1	2	#2-12	3
44	4-3		Tampering with and altering data/software in the control server by a malicious third party.	2	2	1	D		Same as it	em number 14		1	2	#2-13	28,29,41,4
															4
45	5-1		Theft of data on the control server by a malicious third party. (Data then retrieved by following the reverse	2	2	3	В		Same as it	em number 17		1	2	#2-14	28,29,41,4
	0-1		route.)												5
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 majicious third party.	2	2	3	В		Same as it	em number 18		1	2	#2-15	28,29,41,4
\vdash			from the control server by a malicious third party. Production of a product that does not meet quality												-
47	3-1		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	С		Same as it	em number 18		1	2	#2-16	28,29,41,4
	4.4		Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate		2	4	2		0.00	om number 10		4	_	#0.47	28,29,41,4
48	4-1		target values to the controller from the control server by a malicious third party.	2	2	1	D		Same as it	em number 18		1	2	#2-17	8
			zed access of the EWS from the data historian by as third party.									_			
49			rized access includes "execution of unauthorized						Same as it	em number 21		2			
			Theft of data on the EWS by a malicious third												28,29,49,5
50	5-1		party. (Data then retrieved by following the reverse route.)	2	2	3	В		Same as it	em number 22		1	2	#2-18	0
			A malicious third party modifies settings (such as threshold												28,29,49,5
51	2-2		values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	3	В		Same as it	em number 23		1	2	#2-19	1
52	3-2		A malicious third party modifies settings (such as threshold values) of controller or tampers with and	2	2	2	С		Same as it	em number 23		1	2	#2-20	28,29,49,5
			alters data/software in controller from the EWS.		_	_			23.110 00 10	*		·	_		2
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 FWS	2	2	1	D		Same as it	em number 23		1	2	#2-21	28,29,49,5
			alters data/software in controller from the EWS. Tampering with and altering data/software in												
54			controller (M) from the EWS by a malicious third party.						Same as it	em number 26		1			
55	1-2		Issuing of commands to stop the controller (S) via the controller (M) by a malicious third party.	2	2	3	В		Same as its	em number 27		1	2	#2-22	28,29,49,5
	_	Netel	Supply outage encompassing a wide area.												4,55
Х		Note] 1 It is recommended to refer to "Se	ction 9.4 Firewall Settings" in the Guide for evaluating c	ountermeasures.											

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

		Scenario	-		ent Metrics	Bolootivo	Products, 4. Manufacturing/Production Disrupt/Suspend, 5. Leak of Confi		ty Level		Tree Number
	uok	Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Protection Detection/ Intrusion/ Objective Achievement Spreading Phase Phase Damage 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 1-2: A wide area supply outage caused by supply outage commands	s being sent to	o multiple co							
Item >	2-1 2-2 2-3		facilities for ha	andling haza	ardous materi	als caused b	y the setting of improper target values. y the malicious modification of settings (thresholds, etc.) or tampering with and altering pro uthorized modification of data and programs prevents a proper response, even when opera		perform a d	correctly	
Number	2-3 2-4 3-1	 2-3: Outbreak of fires and explosions due to erratic behavior in facilit 2-4: Outbreak of fires and explosions caused by a loss of monitoring 3-1: Production of a product that does not meet quality standards/crit 	and monitorir	ng control at	facilities for h	nandling haza	ardous materials due to congestion in the control network (field side).	nions are p	senomed	сопесцу.	
¥r	3-2 3-3		teria due to co	ontrol abnorr	malities in pro	duction facilit	ies caused by the malicious modification of settings (thresholds, etc.) or tampering with an	l altering p	rograms.		
	4-1 4-2	4-1: Control abnormalities in production facilities caused by the settin 4-2: Control abnormalities in production facilities caused by the malic	ng of improper cious modifica	target value tion of settin	es. This leads	s to processe s, etc.) or tar	s being terminated for safety reasons. npering with and altering programs. This leads to processes being terminated for safety rea	asons.			
	4-3 4-4 5-1		onitoring of pro	oduction faci	ilities and pre	vent monitori	processes being terminated for safety reasons. ng control. This leads to processes being terminated for safety reasons.				
	5-1	5-1: Theft of company production secrets stored on the control syste Attack Entry Point = HMI	, resulting in	i ali external	i illumation l		Anti-virus Device Error Detection Application Whitelisting Device Alive Monitoring				
56		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					Applying Patches Log Collection/Log Analysis Avoidance of Integrated Log	1 *2			
		of a deliberate attempt at "connecting to unauthorized media".					Vulnerability Management System Data Signature Management System	~			
57	2-3	Tampering with and altering data/software in the HMI by malware infection.	2	3	3	А	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	В	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. Abnormal control of facilities for handling hazardous materials due to	2	3	3	А	Same as item number 7	1	1	#3-5	56,61
62	2-1	the setting of inappropriate target values for the controller from the HMI by a malware infection.	2	3	3	А	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	В	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	А	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 Device Error Detection Application Whitelisting O Device Alive Monitoring Applying Patches Log Collection/Log Analysis Avoidance of Vulnerality Data Signature	2 *2			
68	2-3	Tampering with and altering data/software in the control server by malware infection.	2	2	3	В	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	С	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	В	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	С	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 Anti-virus Device Error Detection	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 Enror Detection Device Alive Monitoring Log Collection/Log Analysis Avoidance of Vulnerability Data Signature	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	Α	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	В	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	А	Permission Management (Same as on the left) Device Error Detection Data Backup Access Control (Same as on the left) Log CollectionLog Analysis Data Signature ((Same as on the left) magnetic to the approximation of the left)	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	Α	Permission Management (Same as on the left) Device Error Detection Data Backup Access Control (Same as on the left) Log Colection(Log Analysis Data Signature (Same as on the left) Imagedate Management System	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	Α	Same as item number 27	1	1	#3-23	74,81,82
х											
ı	Note]										

[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

		Scenario			Assassm	ent Metrics				Counter	measures		Securi	ty Level	Attack T	ree Number
Item	MILAUK	Scenario			Assessiii	ent Metrics	7		Prot	ection	Detection/				Attack	Configuration
		Attack Tr	ee/Attack Steps	Threat Level	Vulnerability Level	Business Impact Leve	Risk V	alue	Intrusion/	Objective Achievement	Understanding	Business Continuity	Attack Steps	Attack Tree	Tree	Steps (Item
Number						•			Spreading Phase	Phase	Damage				Number	Number)
ĕ	1-1 1-2		ge caused by the use of wide area sup ge caused by supply outage command			ontrollers.										
		,							FW o		IPS/IDS					
		Attack Entry Point = Information Unauthorized firewall access by a n							Peer-to-Peer Authentication		Log Collection/Log Analysis		2			
1		* Unauthorized access includes "ex	ecution of unauthorized processes" (privilege						Applying Patches Avoidance of Vulnerability		Integrated Log Management System Device Alive Monitoring		∠ *1			
		used to denote the "execution of un	for the two threats are merged. Italic text is authorized processes".						Permission Management •	(Same as on the left)		<u> </u>				
\dashv									Peer-to-Peer Authentication o		IPS/IDS					
2			he HMI via the FW by a malicious third party.						Applying Patches		Log Collection/Log Analysis		2			
		* Unauthorized access in	cludes "execution of unauthorized processes".						Avoidance of Vulnerability Permission Management		Integrated Log Management System Device Alive Monitoring		-			
\dashv		Supply outage	encompassing a wide area caused by a						Segmentation/Zoning	(Same as on the left)	Log Collection/Log Analysis					
3	1-1	malicious third on the controlle	party using wide area supply outage functions	2	2	3	В		Data Signature	(Same as on the left)	Integrated Log Management System		1	2	#1-1	1,2,3
=		on the controlle	a nom me rivii.						Approval of Important Operations Peer-to-Peer Authentication	(Same as on the left)	IPS/IDS					
			he EWS via the FW by a malicious third party.						Applying Patches	•	Log Collection/Log Analysis					
4		* Unauthorized access in (privilege escalation).	cludes "execution of unauthorized processes"						Permission Management	(Same as on the left)	Integrated Log Management System		2			
		G-77-12-5-12-12-17							Application Whitelisting	(Same as on the left)	Device Alive Monitoring					
5			and altering data/software in controller (M)						Permission Management Access Control	(Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis	Data Backup	1			
		from the EWS	by a malicious third party.						Data Signature	(Same as on the left)	Integrated Log Management System		'			
6	1-2		ng of commands to stop the controller (S) via the oller (M) by a malicious third party. Supply outage	2	2	3	В		Segmentation/Zoning	(Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management		1	2	#1-2	1,4,5,6
0	1-2		oller (M) by a mailclous third party. Supply outage mpassing a wide area.	2	2	3			Data Signature Approval of Important Operations	(Same as on the left)	Sustan		'	2	#1-2	1,4,5,6
=		Attack Entry Point = Monitoring Termina	al						Peer-to-Peer Authentication o		IPS/IDS					
7		* Unauthorized access includes "execution of	ay) from a monitoring terminal by a malicious third party. unauthorized processes" (privilege escalation).						Applying Patches o		Log Collection/Log Analysis		2			
		Countermeasures used for the two threats are unauthorized processes".	merged. Italic text is used to denote the "execution of						Avoidance of Vulnerability Permission Management O	(Same as on the left)	Integrated Log Management System Device Alive Monitoring		*1			
\neg		Linguithorized access of t	he data historian from the data historian (relay)						Peer-to-Peer Authentication o		IPS/IDS					
8		by a malicious third party.	ne data historian nom the data historian (relay)						Applying Patches Avoidance of Vulnerability		Log Collection/Log Analysis Integrated Log Management System		2			
		* Unauthorized access in	cludes "execution of unauthorized processes".						Permission Management O	·	Device Alive Monitoring					
		Unauthorized a	access of the HMI from the data historian by a						Peer-to-Peer Authentication o		IPS/IDS					
9		malicious third	party. access includes "execution of unauthorized						Applying Patches Avoidance of Vulnerability		Log Collection/Log Analysis Integrated Log Management System		2			
		processes".	access models execution of and allonized						Permission Management		Device Alive Monitoring					
40			y outage encompassing a wide area caused by a	0	0	2				C 1			4		44.0	7.0.40
10	1-1		ous third party using wide area supply outage functions controller from the HMI.	2	2	3	В			Salité às la	em number 3		'	2	#1-3	7,8,9,10
=		Unauthorized a	access of the EWS from the data historian by						Peer-to-Peer Authentication o		IPS/IDS					
11		a malicious thir	d party.						Applying Patches		Log Collection/Log Analysis		2			
``		* Unauthorized processes".	access includes "execution of unauthorized						Permission Management Application Whitelisting	(Same as on the left)	Integrated Log Management System Device Alive Monitoring		-			
\dashv			pering with and altering data/software in						Permission Management	(Same as on the left)	Device Error Detection	Data Backup				
12		cont	roller (M) from the EWS by a malicious third						Access Control	(Same as on the left)	Log Collection/Log Analysis		1			
\dashv		party							Data Signature	(Same as on the left)	Integrated Log Management System					
13	1-2		Issuing of commands to stop the controller (S) via the controller (M) by a malicious third party.	2	2	3	В			Same as it	em number 6		1	2	#1-4	7,8,11,12,1
_			Supply outage encompassing a wide area.				***************************************	*******							*************	3
		Attack Entry Point = HMI	a LIMI is infected with a service of the first						Anti-virus		Device Error Detection					
14		Due to human error by an insider, the connected to a malware-infected US	e HMI is infected with malware after being SB storage device.						Application Whitelisting Applying Patches		Device Alive Monitoring Log Collection/Log Analysis		1			
		* As this is the result of actions by a	n insider, it is assumed that there is no threat						Avoidance of Vulnerability		Log Collection/Log Analysis Integrated Log Management System		*2			
_		of a deliberate attempt at "connectin	g to unauthorized media".						Data Signature Segmentation/Zoning	(Same as on the left)	Log Collection/Log Analysis					
15	1-1		ssing a wide area caused by malware	2	3	3	Α		Segmentation/Zoning Data Signature	(Same as on the left)	Log Collection/Log Analysis Integrated Log Management System	•	1	1	#1-5	14,15
		unggening wide area supp	ly outage functions from the HMI.						Approval of Important Operations	(Same as on the left)						
		Attack Entry Point = EWS							Anti-virus		Device Error Detection					
16		Due to human error by an insider, the connected to a malware-infected US	e EWS is infected with malware after being						Application Whitelisting		Device Alive Monitoring		1			
10		* As this is the result of actions by a	n insider, it is assumed that there is no threat						Applying Patches Avoidance of Vulnerability		Log Collection/Log Analysis Megrated Log Management System		*2			
		of a deliberate attempt at "connecting	g to unauthorized media".						Data Signature	•		•				
17			ng data/software in controller (M) from the						Permission Management Access Control	(Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis	Data Backup	1			
		EWS by malware infectio	n.						Data Signature	(Same as on the left)	Integrated Log Management System					
10	1.2		mands to stop the controller (S) via the	2	3	3	^		Segmentation/Zoning	(Same as on the left)	Log Collection/Log Analysis		1	4	#1.6	16 17 19
18	1-2	encompassing	y malware infection. Supply outage a wide area.		3	3	A		Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left)	Integrated Log Management System		1	1	#1-6	16,17,18
х																
	[Note]															
	[. 10(0]		ttings" in the Guide for evaluating countermeasures													

[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

		Scenario	Acca	ssment Metric	0		Counter	measures		Securit	y Level	Attack T	ree Number
Item	Allack	Attack Tree/Attack Steps	Threat Level Vulner	ability Business rel Impact Leve	el Risk Value	Intrusion/ Spreading Phase	otection Objective Achievement Phase	Detection/	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
Number	2-1 2-2	2-1: Outbreak of fires and explosions due to control abnormalities in f 2-2: Outbreak of fires and explosions due to control abnormalities in f						holds, etc.) or tamperin	g with and altering prog	ırams.			
4	2-3	2-3: Outbreak of fires and explosions due to erratic behavior in facilities	es for handling haz	ardous materials	where the una	uthorized modificatio	n of data and programs p	prevents a proper resp	onse, even when opera		erformed	correctly.	
	2-4	2-4: Outbreak of fires and explosions caused by a loss of monitoring Attack Entry Point = Information Network	and monitoring co	itroi at iacilities io	r nandling naz	ardous materiais due	to congestion in the con	troi network (field side).	•				
19		Unauthorized firewall access by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege					Same as ite	em number 1		2			
		escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".								*1			
20		Unauthorized access of the HMI via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as ite	em number 2		2			
						Segmentation/Zoning	(Same as on the left)	Log Collection/Log Analysis					
21	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from	2	2 3	В	Data Signature	(Same as on the left)	Integrated Log Management System		1	2	#2-1	19,20,21
		the HMI by a malicious third party.				Approval of Important Operations Permission Management	(Same as on the left) (Same as on the left)	Device Error Detection	Data Backup				
22	2-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2 3	В	Access Control	(Same as on the left)	Log Collection/Log Analysis	Баш Баскар	1	2	#2-2	19,20,22
						Data Signature Permission Management	(Same as on the left)	Integrated Log Management System Device Error Detection	Data Backup				
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	В	Access Control	(Same as on the left)	Log Collection/Log Analysis		1	2	#2-3	19,20,23
						Data Signature Anti-virus	(Same as on the left)	Integrated Log Management System Device Error Detection					
		Infection of the HMI with malware by a malicious third party to cause unauthorized communication with the control				Application Whitelisting		Device Alive Monitoring					
24	2-4	network (field side) and prevent control network communications. This prevents the monitoring of the control	2	2 3	В	Applying Patches Avoidance of Vulnerability		Log Collection/Log Analysis Integrated Log Management System		1	2	#2-4	19,20,24
		system.				Data Signature				~			
		Unauthorized access of the control server via the FW by a malicious				Peer-to-Peer Authentication Applying Patches	0	IPS/IDS Log Collection/Log Analysis		~			
25		third party. * Unauthorized access includes "execution of unauthorized processes"				Permission Management	(Same as on the left)	Integrated Log Management System		2			
		(privilege escalation).				Application Whitelisting Segmentation/Zoning	(Same as on the left)	Device Alive Monitoring Log Collection/Log Analysis					
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	2	2 3	В	Data Signature	(Same as on the left)	Integrated Log Management System		1	2	#2-5	19,25,26
		server by a malicious third party.				Approval of Important Operations Permission Management	(Same as on the left) (Same as on the left)	Device Error Detection	Data Backup				
27	2-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2 3	В	Access Control	(Same as on the left)	Log Collection/Log Analysis	Data Dackup	2	2	#2-6	19,25,27
						Data Signature	(Same as on the left)	Integrated Log Management System					
28		Unauthorized access of the EWS via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes"					Same as ite	em number 4		2			
-0		(privilege escalation).					carrie do la	Sill Hamber 4					
20	2.2	A malicious third party modifies settings (such as threshold	2	2		Permission Management	(Same as on the left)	Device Error Detection	Data Backup	1	2	#0 7	10.29.20
29	2-2	values) of controller or tampers with and alters data/software in controller from the EWS.	2 4	2 3	В	Access Control Data Signature	(Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1		#2-7	19,28,29
		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party.								2			
30		* 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					Same as ite	em number 7		*1			
		unauthorized processes".											
31		Unauthorized access of the data historian from the data historian (relay) by a malicious third party.					Same as ite	em number 8		2			
		* Unauthorized access includes "execution of unauthorized processes".											
		Unauthorized access of the HMI from the data historian by a malicious third party.											
32		* Unauthorized access includes "execution of unauthorized					Same as ite	em number 9		2			
-	0.4	processes". Abnormal control of facilities for handling hazardous materials										"	30,31,32,3
33	2-1	due to the setting of inappropriate target values for the controller from the HMI by a malicious third party.	2 2	2 3	В		Same as ite	m number 21		1	2	#2-8	3
34	2-3	Tampering with and altering data/software in the HMI by a malicious third party.	2 2	2 3	В		Same as ite	m number 22		1	2	#2-9	30,31,32,3
35	2.4	Tampering with and altering the control network (field side) settings from the HMI to cause network congestion in the control	2 2	2 3	В		S	m number 22		1	2	#2-10	30,31,32,3
35	2-4	network by a malicious third party. This prevents the monitoring of the control system.	- '	. 3			Same as ite	m number 23				#2-10	5
	2.4	Infection of the HMI with malware by a malicious third party to cause unauthorized communication with the control network											30,31,32,3
36	2-4	(field side) and prevent control network communications. This prevents the monitoring of the control system.	2	2 3	В		Same as ite	m number 24		1	2	#2-11	6
		Unauthorized access of the control server from the data				Peer-to-Peer Authentication	0	IPS/IDS					
37		historian by a malicious third party. * Unauthorized access includes "execution of unauthorized				Applying Patches Avoidance of Vulnerability		Log Collection/Log Analysis Integrated Log Management System		2			
		processes".				Permission Management	0	Device Alive Monitoring		1			
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	3	В		Same as ite	m number 26		1	2	#2-12	30,31,37,3
20	2.2	Tampering with and altering data/software in the	2		- B		C "-	m number 27		1	_	#0.40	30,31,37,3
39	2-3	control server by a malicious third party.	2 2	2 3	В		Same as ite	m number 27		<u>'</u>	2	#2-13	9
40		Unauthorized access of the EWS from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as ite	m 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	2 2	2 3	В		Same as ite	m number 29		1	2	#2-14	30,31,40,4
		controller from the EWS.	- '				Jame as ite					,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	1

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

2. Occurrence of Fires and Explosion Incidents

Α	Attack	Scenario			Assessme	nt Metrics			Counter	measures		Securi	ty Level	Attack 1	ree Numb
		Attac	k Tree/Attack Steps	Threat Level	Vulnerability	Business	Risk Value		tection	Detection/ Understanding	Business Continuity	Attack	Attack	Attack Tree	Configura
		Allac	K 1166/Attack Oteps	Tillout Lovel	Level	Impact Level	Trisk Value	Intrusion/ Spreading Phase	Objective Achievement Phase	Damage	Dubinosa Continuity	Steps	Tree	Number	Numbe
			l explosions due to control abnormalities in												
			d explosions due to control abnormalities in		-									o o mo o the	
			dexplosions due to erratic behavior in facili dexplosions caused by a loss of monitoring		-							tions are	репогтеа	correctly.	
		Attack Entry Point=HMI	oxpresions educed by a rece of mentioning		ang control at		and graz	M	to congestion in the con	ao motivo in (noid oldo	, .				
			der, the HMI is infected with malware after being									1			
2		connected to a malware-infect	ed USB storage device. by an insider, it is assumed that there is no threat						Same as ite	m number 14		*2			
			necting to unauthorized media".												
		Abnormal control of	facilities for handling hazardous materials due to		*******************		*.*.*.*.*.*.*.*.*.*.*.	Segmentation/Zoning	(Same as on the left)	Log Collection/Log Analysis			1.1.1.1.1.1.1.1.1.1.1.1.1.		
3	2-1	the setting of inappr	opriate target values for the controller from the HMI	2	3	3	Α	Data Signature	(Same as on the left)	Integrated Log Management System		1	1	#2-15	42,
4		by a maiware infect	on.					Approval of Important Operations Permission Management	(Same as on the left) (Same as on the left)	Device Error Detection	Data Davidson				
	2-3		altering data/software in the HMI by malware	2	3	3	Α	Permission Management Access Control	(Same as on the left)	Log Collection/Log Analysis	Data Backup	1	1	#2-16	42,
		infection.		_			, ,	Data Signature	(Same as on the left)	Integrated Log Management System			,	<i>"</i> 2 .0	,
		Tampering with and alte	ring the control network (field side) settings from the HMI to					Permission Management	(Same as on the left)	Device Error Detection	Data Backup				
	2-4	cause network congesti the monitoring of the co	on in the control network by malware infection. This prevents	2	3	3	Α	Access Control	(Same as on the left)	Log Collection/Log Analysis		1	1	#2-17	42,
=								Data Signature Anti-virus	(Same as on the left)	Integrated Log Management System Device Error Detection					
		Mahusan infection o	in					Application Whitelisting		Device Alive Monitoring		1			
	2-4		ausing unauthorized communication with the control and preventing control network communications.	2	3	3	Α	Applying Patches		Log Collection/Log Analysis		1	1	#2-18	42.
	2-4	, ,,,	onitoring of the control system.					Avoidance of Vulnerability		Integrated Log Management System		{			
								Data Signature				<u> </u>			
		Attack Entry Point = Contr	ol Server					Anti-virus		Device Error Detection					
		Due to human error by an insi	der, the control server is infected with malware after					Application Whitelisting O		Device Alive Monitoring		2			
		being connected to a malware	-infected USB storage device. by an insider, it is assumed that there is no threat					Applying Patches		Log Collection/Log Analysis		*2			
		of a deliberate attempt at "con						Avoidance of Vulnerability Data Signature		Integrated Log Management System		ļ			
1		Abnormal control of	facilities for handling hazardous materials due to	3+0+0+0+0+0+0+0+0+0+0+0+0+0+0+0+	0+	**********************	8+8+8+8+8+8+8+8+8+8+8+8+8+8+8+	Segmentation/Zoning	(Same as on the left)	Log Collection/Log Analysis			0.0.0.0.0.0.0.0.0.0.0.0.0	3-2-2-2-2-2-2-2-2-2-2-	
3	2-1		opriate target values for the controller from the	2	2	3	В	Data Signature	(Same as on the left)	Integrated Log Management System		1	2	#2-19	47,
		control server by a	nalware infection.					Approval of Important Operations	(Same as on the left)						
,	2-3	Tampering with and	altering data/software in the control server by	2	2	3	В	Permission Management O Access Control	(Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis	Data Backup	2	2	#2-20	47,
	2-3	malware infection.				3	В	Data Signature	(Same as on the left)	Integrated Log Management System				#2-20	47,
=		Attack Entry Point = EWS													
			der, the EWS is infected with malware after being									1			
)		connected to a malware-infect	ed USB storage device. by an insider, it is assumed that there is no threat						Same as ite	m number 16		*2			
		of a deliberate attempt at "con	•									_			
1								Permission Management	(Same as on the left)	Device Error Detection	Data Backup				
ı	2-2		iciously modifies settings (such as threshold values) of h and alters data/software in controller from the EWS.	2	3	3	Α	Access Control	(Same as on the left)	Log Collection/Log Analysis		1	1	#2-21	50,
								Data Signature	(Same as on the left)	Integrated Log Management System					
			ring the control network (field side) settings from the EWS to					Permission Management	(Same as on the left)	Device Error Detection	Data Backup			""	
2	2-4	the monitoring of the co	on in the control network by malware infection. This prevents introl system.	2	3	3	Α	Access Control Data Signature	(Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	1	#2-22	50,
#			·					Permission Management	(Same as on the left)	Device Error Detection	Data Backup				
3	2-4		ng unauthorized communication with the control network (field introl network communications. This prevents the monitoring	2	3	3	Α	Access Control	(Same as on the left)	Log Collection/Log Analysis	Data Backup	1	1	#2-23	50,
		of the control system.						Data Signature	(Same as on the left)	Integrated Log Management System					,
		mu.													
		[Note]	ection 9.4 Firewall Settings" in the Guide for evaluating counter			1888						1			

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

3. Supply of Defective Product

	Attack	tack Scenario			Assessment Metrics			Countermeasures				Security Level			ree Number	
Item	· ····································	Coonano	Attack	k Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Intrusion/ Spreading Phas	Protection Objective Achiever	Detection/	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
Number	3-2	3-2: Production of	of a produ	uct that does not meet quality standards/cr uct that does not meet quality standards/cr	iteria due to c	ontrol abnorr	malities in prod	duction facilit	ies caused by the ies caused by the	setting of improper targ	of settings (thresholds, etc	.) or tampering with and	altering pr	ograms.		
54	3-3	Attack Entry Point = Unauthorized firewall acc * Unauthorized access in	Information cess by a mancludes "exector the two the		iteria due to c	ontrol abnorr	nalities in prod	duction facilit	ies caused by tam		g data/software. 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 processe						Same as item number 2							
56	3-1		to the setting	of a product that does not meet quality standards/criteria due og of inappropriate target values for the controller from the HMI ous third party.	2	2	2	С	Segmentation/Zoning (Same as on the left) Log Collection Log Analysis Data Signature (Same as on the left) Inspiration Signature (Same as on the left) Segmentation Department Operations (Same as on the left)			1	2	#3-1	54,55,56	
57	3-3			g with and altering data/software in the HMI by a third party.	2	2	2	С	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 resgrated Log Management System	Data Backup	1	2	#3-2	54,55,57
58		third party * Unautho	·.	ss of the control server via the FW by a malicious ess includes "execution of unauthorized processes").						Same a	as item number 25		2			
59	3-1		to the setting	of a product that does not meet quality standards/criteria due g of inappropriate target values for the controller from the er by a malicious third party.	2	2	2	С	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			g with and altering data/software in the control a malicious third party.	2	2	2	С	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		* Unautho		is of the EWS via the FW by a malicious third party. ess includes "execution of unauthorized processes").						Same	as item number 4		2			
62	3-2		values) of	us third party modifies settings (such as threshold controller or tampers with and alters data/software er from the EWS.	2	2	2	С	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		* Unauthorized access inc	e data historia ludes "execut	orminal an (relay) from a monitoring terminal by a malicious third party, tion of unauthorized processes" (privilege escalation), ats are merged. Italic text is used to denote the "execution of						Same	as item number 7		2 *1			
64		by a malic	ious third p	s of the data historian from the data historian (relay) party. ess includes "execution of unauthorized processes".					Same as item number 8							
65			malicious	ized access of the HMI from the data historian by a third party. prized access includes "execution of unauthorized s".					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	С	Same as item number 56				1	2	#3-6	63,64,65,6 6
67	3-3			Tampering with and altering data/software in the HMI by a malicious third party.	2	2	2	С		Same a	as item number 57		1	2	#3-7	63,64,65,6
68			historian b							Same a	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	С		Same a	as item number 59		1	2	#3-8	63,64,68,6
70	3-3			Tampering with and altering data/software in the control server by a malicious third party.	2	2	2	С		Same a	as item number 60		1	2	#3-9	63,64,68,7
71			a maliciou	ized access of the EWS from the data historian by is third party. orized access includes "execution of unauthorized s".						Same a	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	С	Same as item number 62				1	2	#3-10	63,64,71,7
73		connected to a malw * As this is the result	by an insid vare-infecte of actions	der, the HMI is infected with malware after being ed USB storage device. by an insider, it is assumed that there is no threat ecting to unauthorized media".						Same a	as item number 14		1 *2			
74	3-1	due to the	setting of	luct that does not meet quality standards/criteria inappropriate target values for the controller from re infection.	2	3	2	В		Same a	as item number 56		1	1	#3-11	73,74
75	3-3	Tamperini infection.	g with and	altering data/software in the HMI by malware	2	3	2	В		Same a	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 connecte 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 a	as item number 47		2 *2					
77	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	С		Same a	as item number 59		1	2	#3-13	76,77		
78	Tampering with and altering data/software in the control server by malware infection.			2	2	2	С		Same a	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	values) of		maliciously modifies settings (such as threshold or tampers with and alters data/software in WS.	2	3	2	В		Same a	as item number 62		1	1	#3-15	79,80
х																

[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

	Attack	Scenario	Assessment Metrics			Countermeasures	Securit	Security Level		ree Number
Item Nu		Attack Tree/Attack Steps	Threat Level Vulnerability	Business Impact Level	Risk Value	Protection Detection/ Intrusion/ Objective Achievement Spreading Phase Phase Damage Protection Detection/ Understanding Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
Number		4-1: Control abnormalities in production facilities caused by the setting of improper t 4-2: Control abnormalities in production facilities caused by the malicious modificatic 4-3: Operational abnormalities in production facilities caused by tampering with and	on of settings (thresholds, etc.) I altering data/software. This lea	or tampering with ar ads to processes be	ind altering pr eing terminate	ty reasons. ograms. This leads to processes being terminated for safety reasons. d for safety reasons.				
0.4	4-4	4-4: A destructive malware or ransomware infection that disables monitoring of proc Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party.	duction facilities and prevent mo	onitoring control. Thi	is leads to pr		2			
81		" 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". Unauthorized access of the HMI via the FW by a malicious third party.				Same as item number 1	*1			
82	4-1	Unauthorized access includes "execution of unauthorized processes". 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	2 2	1	D	Same as item number 2 Same as on the left Log Collection.Log Analysis	1	2	#4-1	81,82,83
84	4-3	third party. Tampering with and altering data/software in the HMI by a	2 2	1	D	Approval of Important Operations (Same as on the left) Permission Management (Same as on the left) Device Error Detection Data Backup Access Control (Same as on the left) Log Collection Log Analysis	1	2	#4-2	81,82,84
	4-3	malicious third party.			_	Data Signature (Same as on the left) Permission Management Device Error Detection Data Backup		_		
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	Access Control Device Alive Monitoring Access Control Log CollectionLog Analysis Acquiring Patiches Log CollectionLog Analysis Acquiring Authority Log Collection Log Analysis Acquiring Management System Data Signature	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	Came as on the left Log CollectionLog Analysis	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 O (Same as on the left) Device Error Detection Data Backup Access Control (Same as on the left) Log Collection.Log Analysis Data Signature (Same as on the left) Indication of the second control (Same as on the left)	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 (Same as on the left) Device Error Detection Data Backup Access Control (Same as on the left) Log Collection/Log Analysis Data Signature (Same as on the left) Integrated Log Management System	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	91,92,93,9 4
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	91,92,93,9
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. Linguithorized access of the control server from the data	2 2	1	D	Same as item number 85	1	2	#4-9	91,92,93,9 6
97		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes". Abnormalities in the manufacturing facilities requiring an				Same as item number 37	2			
98	4-1	Anonomalies in the manufacturing/production system due to memograpy 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	91,92,97,9
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	91,92,97,9
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	Abnomalities 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	Came as on the left Log Collection1.cg Analysis	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 (Same as on the left) Device Error Detection Data Backup Access Central (Same as on the left) Log Collection.log Analysis Data Signature (Same as on the left) Inspiration of the second sec	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	Access Control Device Error Detection Data Backup Access Control Device Alive Monitoring Access Control Device Alive Monitoring Log CollectionLog Analysis Avodance of Vulnerability Data Signature	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	Came as on the left Log CollectionLog Analysis	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	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 (Same as on the left) Device Error Detection Data Backup Access Control (Same as on the left) Log CollectionLog Analysis Data Signature (Same as on the left) Insgrand Log Management System	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	Activitus Permission Management Device Error Detection Data Backup Application Whitelisting Access Control Device Alive Monitoring Log Collection.Log Analysis Log Collection.Log Analysis Accessed Vulnerability Registrictly Response System	1	1	#4-19	109,111
x		[Note]				Dela Signature				
		*1 it is recommended to refer to "Section 9.4 Firewall Settings" in the Guide for evaluating coun *2 it is recommended to refer to "Section 9 Security Measures for External Storage Media" in the		ures.			•	essessessesses	10000	

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

5. Leak of Confidential Information

Item	Attack :	Scenario			Assessme	ent Metrics			Count	ermeasures		Security Leve		Attack 7	ree Number
n Number			Attack Tree/Attack Steps	Threat Level	Level	Business Impact Level		Prot Intrusion/ Spreading Phase	Objective Achievem Phase	Detection/ ent Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
4			npany production secrets stored on the control syst	em, resulting	in an externa	I information	leak.	1				1	100000000000000000000000000000000000000	100000000000000000000000000000000000000	
112		Unauthorized firewall * Unauthorized access escalation). Countern	Information Network access by a malicious third party. so includes "execution of unauthorized processes" (privilege neasures used for the two threats are merged. Italic text is used to not unauthorized processes".					Same as item number 1				2 *1			
113		third party * Unautho	rized access of the control server via the FW by a malicious y. orized access includes "execution of unauthorized processes" escalation).							s 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.) Permission Management (Same as on the left) Log Collection Log Analysis Access Control (Same as on the left) Insert Access					2	2	#5-1	112,113,11 4					
115		Unauthor * Unauthor (privilege					,	Same as item number 4							
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 (Same as on the left) Log Colection Log Analysis Access Control (Same as on the left) Party and Log Management System Data Encryption (Same as on the left) Purple (Same as on the left)					1	2	#5-2	112,115,11 6					
117		* Unauthorized access in	Ionitoring Terminal ne data historian (relay) from a monitoring terminal by a malicious third party. cludes "execution of unauthorized processes" (privilege escalation). or the two threats are merged. Italic text is used to denote the "execution of					Same as item number 7			2 *1				
118		by a mali	rized access of the data historian from the data historian (relay), cious third party. orized 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	s 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.) Theft of data on the control server by a malicious third party. Base Same as item number 114		1	2	#5-3	117,118,11 9,120								
121		Unauthorized access of the EWS from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".		me as item number 11											
122	5-1	Theft of data on the EWS by a malicious third party. ((Data then retrieved by following the reverse route.)				3	В	Same as item number 116				1	2	#5-4	117,118,12 1,122
х			to refer to "Section 9.4 Firewall Settings" in the Guide for evaluating count to refer to "Section 9 Security Measures for External Storage Media" in the					······							

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)	
		1	Wide Area Product Supply Outage	2	
Α	10	2	Occurrence of Fires and Explosion Incidents	7	
		1	Wide Area Product Supply Outage	4	
В	29	2	Occurrence of Fires and Explosion Incidents	16	
	23	3	Supply of Defective Product	3	
		5	Leak of Confidential Information	4	
С	12	3	Supply of Defective Product	12	
D	19	4	Manufacturing/Production Disrupt/Suspend		
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		HMI (Physical Intrusion)	4	
2	A	EWS (Physical Intrusion)	5	9
3		Information Network [-> FW]	11	
4		Monitoring Terminal -> [Data Historian (Relay)]	11	
5	В	HMI (Physical Intrusion)	1	29
6		EWS (Physical Intrusion)	2	
7		Control Server (Physical Intrusion)	2	
8	С	(Omitted)	12	12
9	D	(Omitted)	19	19
10	Е	(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

		Table 3-1. Improvement inteasures to Neduce Nisk										
;	#	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	⊔мі	Due to human error by an insider, the HMI is infected with malware	A Applicable Trees = 4 (Table 4-12#1)	None	Applying whitelist	B Applicable Trees = 4					
	2	TIIVII	after being connected to a malware-infected USB storage device.	B Applicable Tree = 1 (Table 4-12#6)	None	(Vulnerability Level 3 -> 2)	C Applicable Tree = 1					
	3	EWG	Due to human error by an insider, the EWS is infected with malware	A Applicable Trees = 5 (Table 4-12#2)	None	Applying whitelist	B Applicable Trees = 5					
	4	LVVO	after being connected to a malware-infected USB storage device.	B Applicable Trees = 2 (Table 4-12#5)	None	(Vulnerability Level 3 -> 2)	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		historian (relay) in the DMZ by a		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	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 5.1@] 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

nd Aiter Countermeasures are impleme										
Risk Value	Current Number of Attack Trees	Number of Attack Trees after Improvements								
Α	9	0								
В	27	11								
С	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		В	efore Coun	termeasur	es	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			нмі	Controller	Causes wide-area supply outage.	2	2	3	В	2	1	3	С
1-2	1-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		НМІ	Controller	Causes wide-area supply outage.	2	2	3	В	2	1	3	С
1-3	1-1	Insider (Human Error)	HMI (Physical Intrusion)				НМІ	Controller	Causes wide-area supply outage.	2	3	3	Α	2	2	3	В
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	В	2	1	3	С
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	В	2	1	3	С
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	Α	2	2	3	В
2-1	2-1	Malicious Third Party	Information Network	FW			нмі	Controller	Sets incorrect target value for controller.	2	2	3	В	2	1	3	С
2-2	2-1	Malicious Third Party	Information Network	FW			Control Server	Controller	Sets incorrect target value for controller.	2	2	3	В	2	1	3	С
2-3	2-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		НМІ	Controller	Sets incorrect target value for controller.	2	2	3	В	2	1	3	С
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	В	2	1	3	С
2-5	2-1	Insider (Human Error)	HMI (Physical Intrusion)				нмі	Controller	Sets incorrect target value for controller.	2	3	3	Α	2	2	3	В
2-6	2-1	Insider (Human Error)	Control Server (Physical Intrusion)				Control Server	Controller	Sets incorrect target value for controller.	2	2	3	В	2	2	3	В
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	В	2	1	3	С
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	В	2	1	3	С
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	Α	2	2	3	В
2-10	2-3	Malicious Third Party	Information Network	FW			НМІ	НМІ	Tampers with and alters data/software in HMI.	2	2	3	В	2	1	3	С
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	В	2	1	3	С
2-12	2-3	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		нмі	НМІ	Tampers with and alters data/software in HMI.	2	2	3	В	2	1	3	С
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	В	2	1	3	С
2-14	2-3	Insider (Human Error)	HMI (Physical Intrusion)				НМІ	НМІ	Tampers with and alters data/software in HMI.	2	3	3	Α	2	2	3	В
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	В	2	2	3	В
2-16	2-4	Malicious Third Party	Information Network	FW			НМІ	Control Network (Field Side)	Maliciously modifies network settings and disables communications.	2	2	3	В	2	1	3	С
2-17	2-4	Malicious Third Party	Information Network	FW			НМІ	Control Network (Field Side)	Infects with malware causing unauthorized communications, and disables communications.	2	2	3	В	2	1	3	С
2-18	2-4	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		НМІ	Control Network (Field Side)	Maliciously modifies network settings and disables communications.	2	2	3	В	2	1	3	С
2-19	2-4	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		НМІ	Control Network (Field Side)	Infects with malware causing unauthorized communications, and disables communications.	2	2	3	В	2	1	3	С
2-20	2-4	Insider (Human Error)	HMI (Physical Intrusion)				НМІ	Control Network (Field Side)	Maliciously modifies network settings and disables communications.	2	3	3	Α	2	2	3	В
2-21	2-4	Insider (Human Error)	HMI (Physical Intrusion)				НМІ	Control Network (Field Side)	Infects with malware causing unauthorized communications, and disables communications.	2	3	3	Α	2	2	3	В
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	Α	2	2	3	В
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	Α	2	2	3	В

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/