# 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

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	
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

# Contents

# 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	15
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)
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 Results
(Attack Entry Point Basis)89
Table 5-1: Improvement Measures to Reduce Risk
Table 5-2: Distribution of Risk Values in the Tree Before
and After Countermeasures are Implemented
Table 5-3: List of Attack Routes and Changes in Risk Values before
and after Countermeasures (Extract)

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

#### Notes on the Revised Second Edition

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

We hope that this separate volume helps provide a clear picture of the total number of 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 impactbased 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  $\clubsuit$  in the figure depicts outputs created by the person in charge of risk analysis, and  $\bigcirc$  is used for outputs obtained by customizing examples outlined in the Guide.

2. Preparing for Risk Assessment						
Title in this Volume		Output	Output Use	Guide		
2.1	1	List of Assets	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	Ī	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	4.4.5. Table 4-20 to Table 4-24			
		3. Asset-based F	Risk Analysis			
Title in this Volume Output O						
3.1	10	Summary Chart of Threat Levels	-			
3.2	1	Asset-based Risk Assessment Shee	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	1		
Title in this Volume		Output		Guide		
4.1	14	List of Attack Scenarios		6.2.2. Table 6-6		
4.2	15-1	List of Attack Routes		6.5.1. Table 6-11 to Table 6-12		
4.2	(15)-2	Attack Route Diagram		6.5.1. Figure 6-9		
4.3	(16)	Business Impact-based Risk Assess	ment Sheet	6.6.4. ~ 6.11.		
4.4	1	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	I System	Chapter 7		

#### Table 1-1. List of Outputs

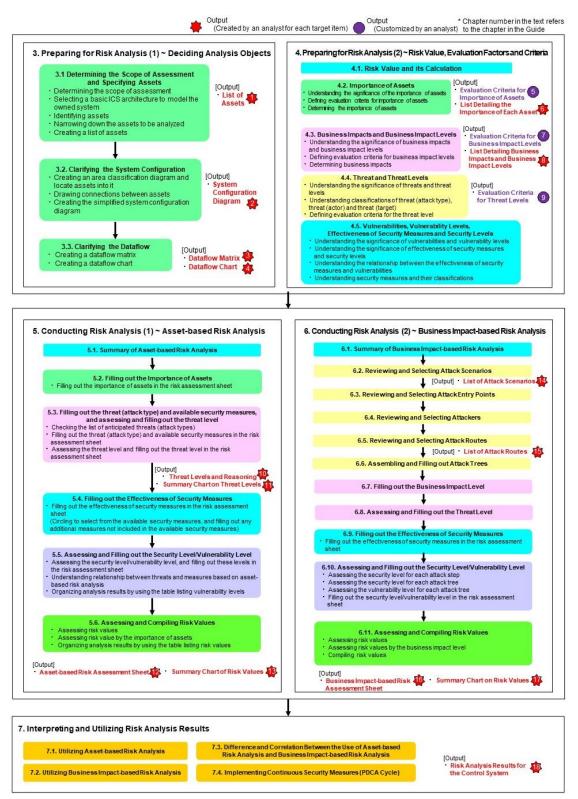


Figure 1-1: Risk Analysis Flow and Outputs

• 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		
Network 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

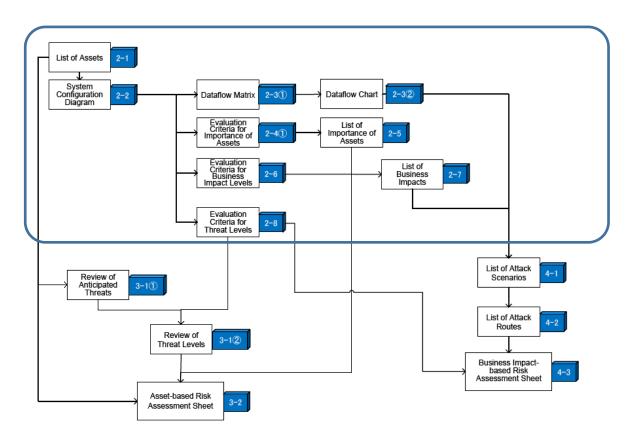


Figure 2-1: Preparation Work Flow

# 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 Assets	Network Asset (with Communication Control Functions)		0	0			0							
	Network Asset (without Communication Control Functions)										0	0		
	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	×	×	×	×	×	×	×	×	×	×	×
Pi	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	ar 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		sets (Including Role/Function, Sc		Continuity, Occurity Weasures)	5
Asset Name	Monitoring Terminal	Firewall	Switch, DMZ	4 Data Historian (Relay)	Data Historian
Role/Function	<ul> <li>A terminal used to monitor processes and on- site status.</li> <li>There is no operating procedure for accessing devices on the control network from the monitoring terminal.</li> </ul>	A device that functions to prevent attacks and	A device that converges and relays multiple networks	<ul> <li>A server that is used to reference the data historian in the control network (information side) from the asset in the information network.</li> </ul>	<ul> <li>A server where process values and control parameters are stored and analyzed over an extended period of time.</li> </ul>
Scope of Impact/Impact on Business Continuity	<ul> <li>Unauthorized modification of data held by the asset or a failure in this asset does not directly impact business continuity.</li> </ul>	<ul> <li>Unauthorized modification of the asset's configured settings can lead to an attack or intrusion.</li> <li>Even in the case of a failure in this asset, field devices can be operated directly to ensure business continuity.</li> </ul>	<ul> <li>Even in the case of a failure in this asset, field devices can be operated directly to ensure business continuity.</li> </ul>	<ul> <li>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.</li> </ul>	<ul> <li>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.</li> </ul>
Effectiveness of Security Measures (Physical/Operational)	<ul> <li>Physical security measures (placement of security guards, lock and key management, entrance and exit management, etc.) are implemented on business premises and buildings.</li> <li>Only internal business personnel are able to physically access office devices.</li> </ul>	<ul> <li>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.</li> <li>Control system device operators are limited, both physically and logically, to the absolute minimum number of internal personnel required.</li> </ul>	<ul> <li>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.</li> <li>Control system device operators are limited, both physically and logically, to the absolute minimum number of internal personnel required.</li> </ul>	<ul> <li>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.</li> <li>Control system device operators are limited, both physically and logically, to the absolute minimum number of internal personnel required.</li> <li>While operating rules prohibit connections to external storage media and smartphone devices, technical measures are not taken.</li> </ul>	<ul> <li>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.</li> <li>Control system device operators are limited, both physically and logically, to the absolute minimum number of internal personnel required.</li> <li>While operating rules prohibit connections to external storage media and smartphone devices, technical measures are not taken.</li> </ul>
Effectiveness of Security Measures (Technical)	<ul> <li>The OS used is Windows 7, and updates are applied as they are made available.</li> <li>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.</li> <li>Users are authenticated when logging in remotely or directly.</li> </ul>	<ul> <li>Users are authenticated when logging in remotely or directly.</li> <li>Only administrator accounts are used, and there are no operator accounts.</li> <li>Remote management functions are only available on administrator accounts.</li> <li>A packet filter firewall is used, and firewall rules only permit communications with the following two connections (IP protocol).</li> <li>Monitoring Terminal &lt;-&gt; Data Historian (Relay) Data Historian (Relay) &lt;-&gt; Data Historian</li> <li>The firewall firmware updates are applied as they are made available.</li> <li>The timing of updates is determined by the maintenance vendor.</li> </ul>	<ul> <li>Users are authenticated when logging in remotely or directly.</li> <li>Only administrator accounts are used, and there are no operator accounts.</li> <li>Remote management functions are only available on administrator accounts.</li> <li>The switch firmware updates are applied as they are made available.</li> <li>The timing of updates is determined by the maintenance vendor.</li> </ul>	<ul> <li>The OS used is Windows Server 2008, and updates are not applied.</li> <li>Users are authenticated when logging in remotely or directly.</li> <li>There are two types of accounts: operator accounts and administrator accounts. Remote management functions are only available on administrator accounts.</li> <li>Data backups are performed on a weekly basis, and three generations of data are stored.</li> <li>Emergency patches are applied within one week of their release.</li> <li>While anti-virus software is installed, signature patterns are only updated once every six months, rather than on a daily basis.</li> </ul>	<ul> <li>The OS used is Windows Server 2008, and updates are not applied.</li> <li>Users are authenticated when logging in remotely or directly.</li> <li>There are two types of accounts: operator accounts and administrator accounts. Remote management functions are only available on administrator accounts.</li> <li>Data backups are performed on a weekly basis, and three generations of data are stored.</li> </ul>

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

No	6	7	8	9	
Asset Name	Switch, Control Network (Information Side)	EWS	Control Server	HMI (Operator Terminal)	
Role/Function	<ul> <li>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.</li> </ul>	<ul> <li>A device used to alter controller programs and modify control server programs.</li> <li>The EWS is also used to bring in external data by connecting it with an external storage media (typically a USB memory stick).</li> </ul>	<ul> <li>A server that sends settings and commands to control devices and field equipment.</li> </ul>	<ul> <li>A terminal used to enter in instructions for control devices and field equipment.</li> <li>Wide-area supply outage commands (commands used to suspend supply to predetermined areas) can be issued.</li> </ul>	<ul> <li>A n</li> <li>inform</li> <li>betwee</li> <li>(contribution</li> <li>high r</li> <li>function</li> <li>Use</li> </ul>
Scope of Impact/Impact on Business Continuity	<ul> <li>Even in the case of a failure in this asset, field devices can be operated directly to ensure business continuity.</li> </ul>	<ul> <li>Unauthorized modification of controller or control server programs or configured settings could prevent normal monitoring control.</li> <li>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.</li> </ul>	<ul> <li>Contains important data that, if tampered with and altered, could cause a system malfunction to occur, resulting in a wide-area supply outage.</li> <li>A failure in this asset would impact business continuity.</li> </ul>	• Even in the case of a failure in this asset, equipment and devices can be operated directly to ensure business continuity.	• Eve device busine
Effectiveness of Security	<ul> <li>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.</li> <li>Control system device operators are limited, both physically and logically, to the absolute minimum number of internal personnel required.</li> <li>Wires are physically protected by conduits.</li> </ul>	<ul> <li>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.</li> <li>Control system device operators are limited, both physically and logically, to the absolute minimum number of internal personnel required.</li> <li>While operating rules prohibit connections to external storage media and smartphone devices, technical measures are not taken.</li> </ul>	<ul> <li>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.</li> <li>Control system device operators are limited, both physically and logically, to the absolute minimum number of internal personnel required.</li> <li>While operating rules prohibit connections to smartphone devices, technical measures are not taken.</li> </ul>	<ul> <li>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.</li> <li>Persons with access to control system devices are limited, both physically and logically, to the absolute minimum number of internal personnel required.</li> </ul>	<ul> <li>For (serve that he physic securi entrar camel impler</li> <li>Cor both p minim</li> </ul>
Effectiveness of Security Measures (Technical)	<ul> <li>Users are authenticated when logging into the switch remotely or directly.</li> <li>(On the switch) only administrator accounts are used, and there are no operator accounts.</li> <li>Connection to remote management functions (on the switch) is restricted to the connection source IP address.</li> </ul>	<ul> <li>The OS used is Windows XP, and updates are not applied.</li> <li>Anti-virus software is not installed.</li> <li>There are two types of accounts: operator accounts and administrator accounts. Remote management functions are only available on administrator accounts.</li> <li>Users are authenticated when logging in remotely or directly.</li> </ul>	<ul> <li>The OS used is Windows Server 2008, and updates are not applied.</li> <li>Users are authenticated when logging in remotely or directly.</li> <li>There are two types of accounts: operator accounts and administrator accounts. Remote management functions are only available on administrator accounts.</li> <li>While anti-virus software is not installed, certain security measures, such as an application whitelisting, are taken.</li> </ul>	<ul> <li>The OS used is Windows XP, and updates are not applied.</li> <li>Anti-virus software is not installed.</li> <li>There are two types of accounts: operator accounts and administrator accounts. Remote management functions are only available on administrator accounts.</li> <li>Users are authenticated when logging in remotely.</li> <li>It is in an always-logged-in state and its screen lock is not set.</li> </ul>	• Wir • The protoc

	10	
Switch.	Control Network (Field Side)	

A network used to immediately transfer status prmation and data, used for control purposes, tween the local network and devices portrollers) on a field network. It possesses

h responsiveness, optimized for control actions.

Uses proprietary IP-based protocols.

Even in the case of a failure in this asset, field vices can be operated directly to ensure siness continuity.

For business premises, buildings, rooms erver rooms and control rooms), racks, etc. at have control system devices installed, ysical security measures (placement of curity guards, lock and key management, trance and exit management, surveillance meras, intrusion detection sensors, etc.) are plemented.

Control system device operators are limited, th physically and logically, to the absolute nimum number of internal personnel required.

Wires are physically protected by conduits. The control network (field side) uses IP btocols.

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

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

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).

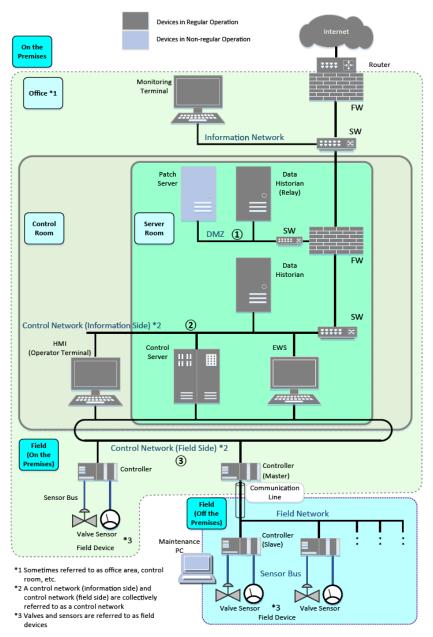


Figure 2-2: System Configuration Diagram

[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).

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

Table 2-4: Dataflow Matrix

#### [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.

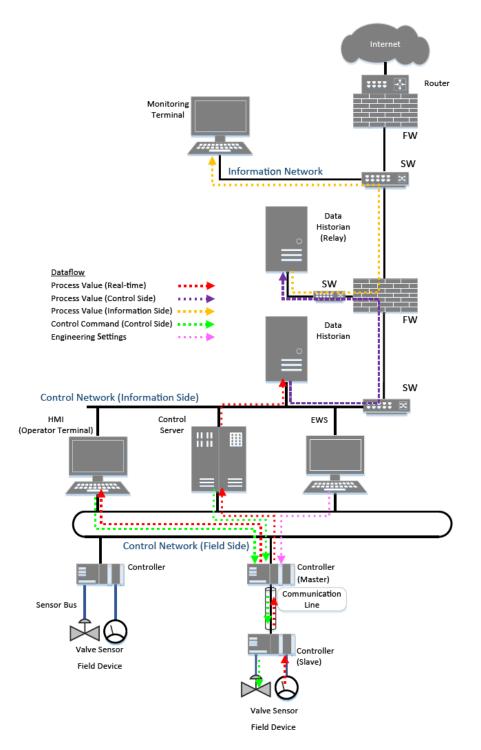


Figure 2-3: Dataflow Chart

# 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).

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
1	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.

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

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, <u>any control system outage that exceeds two weeks could be considered to have a major impact</u> 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 efficiency of the control system.		
5	Data Historian	2	While a shutdown of the historian would not affect the safe operation of the control system, this would prevent data analysis and could potentially reduce the operating efficiency of the control system.		
6	Switch (Control Network (Information Side)), Control Network (Information Side)	2	A shutdown of the control network (information side) would not immediately impact the control system.		
7	EWS	3	If the EWS is taken over, the program logic used by the controller could be tampered with and altered.		
8	Control Server	3	If this asset becomes inoperable, or is subject to unauthorized operation, there is an extremely high likelihood that this would affect the safe operation of the control system.		
9	HMI (Operator Terminal)	3	If monitoring is disabled for all HMIs, monitoring operations will no longer be possible. The control system may shutdown temporarily.		
10	Control Network (Field Side)	3	While the system will not shutdown if this network is shutdown, monitoring and other operations will no longer be possible.		
11	Field Network	3	If this network becomes congested, or is shutdown, regular monitoring control will no longer be possible, and there is a high likelihood that this would prevent the safe operation of the control system.		
12	Controller, Controller (Master)	3	If this asset becomes inoperable, or is subject to unauthorized operation, there is an extremely high likelihood that this would affect the safe operation of the control system.		
13	Controller (Slave)	3	If this asset becomes inoperable, or is subject to unauthorized operation, there is an extremely high likelihood that this would affect the safe operation of the control system.		

#### [Explanation 2.5]

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

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

#### • Evaluation of importance from the perspective of integrity and confidentiality

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

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

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

# 2.6. Evaluation Criteria for Business Impact Level

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

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

#### [Output 2.6]

Examples of evaluation criteria for business impact levels are provided below (Table 2-7). Table 2-7: Example Evaluation Criteria for Business Impact Levels

	Table 2-7. Example Evaluation Uniteria for Business Impact Levels				
Evaluation Value		Evaluation Criteria			
		<ul> <li>The following may result from a failure occurring.</li> </ul>			
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	<ul> <li>The following may result from a failure occurring.</li> </ul>			
2	Medium	- Potential for a system outage over a period (for three days to two weeks).			
2	Business	- Potential losses of between 100 million yen up to 500 million yen.			
	Impact	- Potential to cause damage to company premises.			
		<ul> <li>The following may result from a failure occurring.</li> </ul>			
		- 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.			
	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

		C 2-0. List of Dusiness 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.
2	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
5	Information	competitive edge against other companies, and leading to a
		deterioration in competitive strength.

[Task 2.7<sup>(2)</sup>] 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).

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.

Table 2 0. List of Dusiness Im	waata and Duckaaa Im	
Table 2-9: List of Business Im	ipacts and Business in	inpact Levels

[Explanation 2.7(1)2]

• 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	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
of Fires and Explosion Incidents		Business Impact (Accident)	
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.	Affect of Business Impact	Used when formulating the business impact level

# 2.8. Evaluation Criteria for Threat Level

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

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

#### [Output 2.8]

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

	Table 2-10: Evaluation Criteria for Threat Levels				
Threat	Evaluation Criteria Based on	Evaluation Criteria Based on	Evaluation Criteria based		
Level	an Attack by a Malicious Third	the Logical Placement of	on the Physical Placement		
Level	Party	Assets	of Assets		
3	<ul> <li>When attacked by an individual attacker (regardless of skill), it has a high likelihood of success.</li> </ul>	<ul> <li>Assets on a network (information network) that can be connected to the Internet.</li> </ul>	<ul> <li>Assets in a location that can be accessed by anyone, without any access restrictions for the premises or room.</li> </ul>		
2	<ul> <li>When attacked by an individual attacker with a certain degree of skill, it could potentially succeed.</li> </ul>	<ul> <li>Assets on a network (control network) that is indirectly connected to an information network.</li> </ul>	<ul> <li>Assets in a location with access restrictions for the premises or room.</li> </ul>		
1	<ul> <li>When attacked by a state level cyber attacker (military or equivalent group), it could potentially succeed.</li> </ul>	<ul> <li>Assets on an isolated network.</li> </ul>	Assets in a room with strict manned surveillance system, and access restrictions to enter the premises or room that involve stringent authentication procedures.		

#### Table 2-10: Evaluation Criteria for Threat Levels

\* 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.

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

Table 3-1:	Outputs	for	Preparations	Used
------------	---------	-----	--------------	------

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

-		
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	-

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

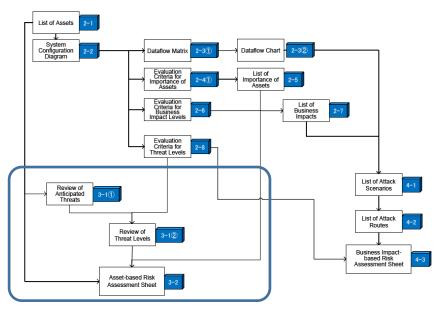


Figure 3-1: Asset-based Risk Analysis Work Flow

## 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).

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) Network Asset			0			0							
Network Asset (without Communication Control Functions)										0	0		
Unauthorized Access	~	~	~	~	~	~	~	~	~			~	~
Physical Intrusion	~	~	~	~	~	~	~	~	~			~	~
Unauthorized Operation	~	~	~	~	~	~	~	~	~			~	~
Human Error in Operation	~	~	~	~	~	~	~	~	~			~	~
Connecting Unauthorized Media or Device	~	~	~	~	~	~	~	~	~			~	~
Execution of Unauthorized Processes	~	~	~	<	~	~	~	~	~			~	~
Malware Infection	~	~	~	~	~	~	~	~	<			~	~
Information Theft	~	~	~	<	~	~	~	~	~			~	~
Unauthorized Modification of Information	~	~	~	~	~	~	~	~	~			~	~
Information Destruction	~	~	~	~	~	~	~	~	~			~	~
Unauthorized Transmission	~	~	~	~	~	~	~	~	<			~	~
Outage	~	~	~	~	~	~	~	~	~			~	~
DoS/DDoS Attack	~	~	~	~	~	~	~	~	~			~	~
Theft	~	~	~	~	~	~	~	~	~			~	~
When Stolen or Discarded	~	~	~	~	~	~	~	~	<			~	~
Route Blocking			~			~				~	~		
Network Congestion			~			~				~	~		
Jamming													
Packet Sniffing			~			~				~	~		
Unauthorized Modification of Communication Data			~			~				~	~		
Connecting Unauthorized Device	-		~			~				~	~		

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

 $\checkmark$ : 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]

Г

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].

#	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.

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

[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.

Threat Asset	Monitoring Terminal	Firewall	ZMQ	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		

Table 3-5: Summary Chart of Asset Threat Levels

## 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.

Sumber	Type of Assets	Target Device	Ass	sessment Me	etrics		Threat (Attack Type)	Description	Prote	tection		Detection() lad	Participa di Carta di		Seci By
			Threat Level	Vulnerability Level	i Importance of Assets	Risk Value			Intrusion/Spreading Phase		Objective Achievement Phase	Detection/Understanding Dama	ge Business Continuity		-,
	Information System Asset	Monitoring Terminal					Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type)			IPS/IDS			-
									FW (Application Gateway Type) One-way Gateway	+ +		Log Collection/Log Analysis Integrated Log Management System			-
									Proxy Server			Integrated cog Management Oystern			1
									WAF						1
			3	2		D			Peer-to-Peer Authentication	0					1
									IPS/IDS						1
									Applying Patches	0					
									Avoidance of Vulnerability	+					4
4					4		Dia chattara cha	Unauthorized access of sections/areas (device installation locations, etc.) with access	5 · · · · · · · · · · · · · · · · · · ·			0			+
			2	2		р	Physical Intrusion	restrictions. It also refers to removing restrictions on devices with physical access restrictions (devices	Entrance and Exit Management (IC Card) Lock and Key Management	0		Surveillance Camera Intrusion Detection Sensor			-
			-	-		-		installed in racks, cabinets, etc.).	Lock and resy management	-		Indusion Detection Censor			1
					1	-	Unauthorized Operation	Intrusion through direct operation of the device's console or other	Operator Authentication	0					+
			2	2		D		component to execute an attack.							1
					1		Human Error in Operation	An attack triggered by a human error in operation by internal	URL Filtering/Web Reputation	0					
									Mail Filtering	0					4
			3	2		D		device). 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	Partriction on Connecting Davice and its Lisage	B 0 (5	Same as on the Left)	(Same as on the Left)			+
							Media or Device	device, etc.) brought in from outside the organization with the	restriction on connecting bevice and its usage	- v (c	Same as on the Leit)	Log Collection/Log Analysis			-
			3	2		D		device to execute an attack.		+ +		Integrated Log Management System			1
															1
					1		Execution of Unauthorized	Unauthorized execution of legitimate programs, commands,	Permission Management	(5	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
			3	3	1	c		device.	Application Whitelisting	(\$	Same as on the Left)	Log Collection/Log Analysis			
									Approval of Important Operations	(5	Same as on the Left)	Integrated Log Management System			1
					4	L				1					1
							Malware Infection		Anti-virus	•		Device Error Detection		<b>—</b>	4
			1		1	1		the attack target device.	Application Whitelisting			Device Alive Monitoring		-	-
			3	2	1	D			Applying Patches	- °		Log Collection/Log Analysis		-	-
			1		1	1			Avoidance of Vulnerability	+		Integrated Log Management System	+		+
									Data Signature	+ +		+ +			-
┥					1		Information Theft	Theft of information (software, authentication information,	Permission Management	19	Same as on the Left)	Log Collection/Log Analysis	1		+
								configuration settings, encryption keys and other confidential			Same as on the Left)	Integrated Log Management System			1
			3	3		c		information) stored on the device.	Data Encryption		Same as on the Left)				1
								,	DLP		Same as on the Left)				1
															1
							Unauthorized Modification o	f Unauthorized modification of information (software,	Permission Management		Same as on the Left)	Device Error Detection	Data Backup		
			2	3		D	Information	authentication information, configuration settings, encryption	Access Control		Same as on the Left)	Log Collection/Log Analysis			4
			I -	1		-		keys and other confidential information) stored on the device.	Data Signature	(\$	Same as on the Left)	Integrated Log Management System			4
-					4										+
							Information Destruction	Destroying of information (software, authentication			Permission Management	Device Error Detection	Data Backup		-
			2	3		D		information, configuration settings, encryption keys and other		A	Access Control	Log Collection/Log Analysis			+
								confidential information) stored on the device.		+ $+$		Integrated Log Management System			+
-					1		Unauthorized Transmission	Sending unauthorized control commands (settings changes,	Segmentation/Zoning	(5	Same as on the Left)	Log Collection/Log Analysis			+
					1			power shutdowns, etc.) and unauthorized data to other	Data Signature		Same as on the Left)	Integrated Log Management System			1
			2	3		D		devices.	Approval of Important Operations		Same as on the Left)				1
															1
							Outage	Stopping device functions.				Device Error Detection	Redundancy		
												Device Alive Monitoring	Failsafe Design		4
			2	3		D				+		Log Collection/Log Analysis			4
										+ +		Integrated Log Management System			+
			-		+	L	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
			1	3		E		the device as a result of a DDoS attack, etc.				Log Collection/Log Analysis	-		1
												Integrated Log Management System			1
															1
Τ					1		Theft	Device theft.	Lock and Key Management	· (5	Same as on the Left)	(Same as on the Left)			Г
			2	2	1	D									4
			L		4	L				+		L			+
							Information Theft by	Theft of information (software, authentication information,	Tamper Resistance		Same as on the Left)	L			+
			2	2		D	Tampering Device at Time	configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed	0010000001	10	Same as on the Left) Same as on the Left)	++			+
							of Theft or Disposal	of and then disassembled.			oamo as on the Left)	++			+
ſ					1		Route Blocking	Communications are blocked by disconnecting the	Entrance and Exit Management (IC Card)			Device Error Detection	Redundancy		t
l					I			communication cable.	Lock and Key management			Device Alive Monitoring			1
1					I			Alternatively, communications are blocked by pulling out the				Log Collection/Log Analysis			1
1					I			communication cable from the device.				Integrated Log Management System			1
1					I							Surveillance Camera			4
1					I							Intrusion Detection Sensor			4
ł					4								0.1.1		4
1							Network Congestion	Causing congestion by generating the communications traffic that exceeds the capacity of the device.				Device Error Detection	Redundancy		4
I.								unar exceeds the capacity of the device.	FW (Application Gateway Type) WAF	+ +		Device Alive Monitoring Log Collection/Log Analysis			4
1									IPS/IDS			Integrated Log Management System			1
l									DDoS Countermeasures						1
l					I										1
1	(		-		-		Jamming	Interference with radio communications.				Device Error Detection	Redundancy		Г
l	Not applicable (no fu	inctions)										Device Alive Monitoring			1
L												Log Collection/Log Analysis			4
ſ												Integrated Log Management System			4
Į.			-		+										4
l					I		Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels						4
					I				Data Encryption	+					4
1									Exclusive Line						4
1					+										4
l					I			f Maliciously modifying information flowing on the network.	Encryption of Communications Channels			Log Collection/Log Analysis			4
					I		Communication Data		Data Signature			Integrated Log Management System			4
I.									Exclusive Line				_		4
					+		Connection Uses II	Connection unsytherized device on the	Participa on Connection Device and in the			Restriction on Connecting Device and its Usage			+
							Connecting Unauthorized	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage	- 1		and a second sec			4
							Device					Log Collection/Log Analysis			
							Device					Log Collection/Log Analysis Integrated Log Management System			-

en Number			_								â :				_	
iem Number			Ass	sessment Me	trics			<b>A</b> 14	Deste		Countermea	sures		1		Security Level
	Type of Assets	Target Device	Thursday			D'sh Mahar	Threat (Attack Type)	Description	Prote	ection		Detection/Understanding [	Damage	Business Continuity		By Threat
			I hreat Level	Vulnerability Level	Importance of Assets	Risk Value			Intrusion/Spreading Phase	-	Objective Achievement Phase		-	-		
	Network Asset	Firewali					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				
									One-way Gateway			Integrated Log Management System				
									Proxy Server							
.									WAF							
1			3	2		A			Peer-to-Peer Authentication	0						2
									IPS/IDS				-		_	
										0						
									Applying Patches				-			
									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			
2			1	1		c		access restrictions. It also refers to computer matricipes on devices with obvicing access restrictions.	Lock and Key Management	0		Intrusion Detection Sensor	0			3
								It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).								-
_										0			_			
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
_									UDI Etherine Mak Desudation							
							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.								
							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
2			2	3		<b>^</b>		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				
							Processes	services, and other processes found on the attack target	Access Control		(Same as on the Left)	Device Alive Monitoring				
6			2	2		в			Application Whitelisting		(Same as on the Left)	Log Collection/Log Analysis				2
-			-	-		-		device.	Approval of Important Operations		(Same as on the Left)	Integrated Log Management System	-			-
											(		-			
_							Mahuara Infantian	Infection or a maine of molecure (case discipled programs) on	Anti-virus			Device Error Detection	-			
							Malware Infection	Infection or running of malware (unauthorized programs) on	Application Whitelisting			Device Alive Monitoring	-		_	
								the attack target device.					-		_	
7			1	3		в			Applying Patches			Log Collection/Log Analysis	-			1
				-		-			Avoidance of Vulnerability			Integrated Log Management System	_			-
									Data Signature							
					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
				_		-		information) stored on the device.	DLP		(Same as on the Left)					
											(		-			
_					1		Lingutherized Medification of	Unauthorized modification of information (software,	Permission Management	0	(Same as on the Left)	Device Error Detection	-	Data Backup		
									Access Control		(Same as on the Left)	Log Collection/Log Analysis				
9			3	2		A	Information	authentication information, configuration settings, encryption	Data Signature		(Same as on the Left)	Integrated Log Management System			_	2
								keys and other confidential information) stored on the device.	Data Oignature		(Game as on the Left)	incgrates tog intragement dystern	-		_	
					-		Life and the Device of the				Permission Management	Dovice Error Detection	-	Data Backup		
							Information Destruction	Destroying of information (software, authentication			A seese Cankel	Device Error Detection		Data Backup		
10			2	2		в		information, configuration settings, encryption keys and other			Access Control	Log Collection/Log Analysis	-			2
								confidential information) stored on the device.				Integrated Log Management System	-			
													_			
							Unauthorized Transmission	Sending unauthorized control commands (settings changes,	Segmentation/Zoning		(Same as on the Left)	Log Collection/Log Analysis	-			
11			1	3	3	в		power shutdowns, etc.) and unauthorized data to other	Data Signature		(Same as on the Left)	Integrated Log Management System	_			1
				-		-		devices.	Approval of Important Operations		(Same as on the Left)					-
							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		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		A		the device as a result of a DDoS attack, etc.				Log Collection/Log Analysis				1
												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		c	- Hole	borios dist.	Econ and roy management		(ounto up on the cold)	(came as on the Eory	_		_	2
' <b>-</b>			· ·	-		Ŭ					l		-			2
					4		lafe and the The Art	Theft of information (adjuster adjusting information	Tamper Resistance		(Same as on the Left)		-			
1							Information Theft by	Theft of information (software, authentication information,	Obfuscation		(Same as on the Left)		+			
15			1	2				configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and	<b>B</b> 1 1	0	10 1 1 10		+	1	-+	2
- 1							of Theft or Disposal	information) stored on devices which were stolen or disposed of and then disassembled.		5	(Same as on the Left)		-			
				L	4				-	-		Device Free Datastic	-	Deducdency		
							Route Blocking	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	_	
								communication cable.	Look and Noy management				-		_	
								Alternatively, communications are blocked by pulling out the				Log Collection/Log Analysis				
								communication cable from the device.				Integrated Log Management System				
16												Surveillance Camera	0			
16												Intrusion Detection Sensor	0			
16																
16					1		Network Congestion	Causing congestion by generating the communications traffic	FW (Packet Filtering Type)	0		Device Error Detection		Redundancy		
16								that exceeds the capacity of the device.	FW (Application Gateway Type)			Device Alive Monitoring	+		_	
16								that exceeds the capacity of the device.					-			
16									WAF			Log Collection/Log Analysis				
16									IDC/IDC							
									IPS/IDS			Integrated Log Management System	_			
									IPS/IDS DDoS Countermeasures			Integrated Log Management System				
												Integrated Log Management System				
							Jamming	Interference with radio communications.				Integrated Log Management System Device Error Detection		Redundancy		
	Not applicable (no fut	unctions)					Jamming					Device Error Detection		Redundancy		
17	Not applicable (no fu	unctions)					Jamming					Device Error Detection Device Alive Monitoring		Redundancy		
	Not applicable (no fut	unctions)					Jamming					Device Error Detection Device Alive Monitoring Log Collection/Log Analysis		Redundancy		
17	Not applicable (no fu	inctions)					Jamming					Device Error Detection Device Alive Monitoring		Redundancy		
17	Not applicable (no fur	unctions)						Interference with radio communications.	DDoS Countermeasures			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis		Redundancy		
17	Not applicable (no fu	unctions)					Jamming Packet Sniffing	Interference with radio communications.	DDoS Countermeasures			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis		Redundancy		
17	Not applicable (no fu	unctions)						Interference with radio communications.	DDoS Countermeasures			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis		Redundancy		
17	Not applicable (no fu	inctions)						Interference with radio communications.	DDoS Countermeasures			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis		Redundancy		
17	Not applicable (no fu	unctions)						Interference with radio communications.	DDoS Countermeasures			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis		Redundancy		
17	Not applicable (no fu	unctions)					Packet Sniffing	Interference with radio communications. Theft of information flowing on the network.	DDoS Countermeasures			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis inegrated Log Management System		Redundancy		
17	Not applicable (no fu	inctions)					Packet Sniffing Unauthorized Modification of	Interference with radio communications.	DDoS Countermeasures Encryption of Communications Channels Data Encryption Exclusive Line Encryption of Communications Channels			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy		
17 18 19	Not applicable (no fu	inctions)					Packet Sniffing	Interference with radio communications. Theft of information flowing on the network. Maliciously modifying information flowing on the network.	DDoS Countermeasures Encryption of Communications Channels Data Encryption Exclusive Line Encryption of Communications Channels Data Signature			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis inegrated Log Management System		Redundancy		
17	Not applicable (no fut	inctions)					Packet Sniffing Unauthorized Modification of	Interference with radio communications. Theft of information flowing on the network. Maliciously modifying information flowing on the network.	DDoS Countermeasures Encryption of Communications Channels Data Encryption Exclusive Line Encryption of Communications Channels			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy		
17 18 19	Not applicable (no fu	unctions)			-		Packet Sniffing Unauthorized Modification of	Interference with radio communications. Theft of information flowing on the network. Maliciously modifying information flowing on the network.	DDoS Countermeasures Encryption of Communications Channels Data Encryption Exclusive Line Encryption of Communications Channels Data Signature			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy		
17 18 19	Not applicable (no fu	unctions)			-		Packet Sniffing Unauthorized Modification of Communication Data	Interference with radio communications. Theft of information flowing on the network. Maliciously modifying information flowing on the network.	DDoS Countermeasures			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Redundancy		
17 18 19 20	Not applicable (no fu	unctions)			-		Packet Sniffing Unauthorized Modification of Communication Data Connecting Unauthorized	Interference with radio communications. Theft of information flowing on the network. Maliciously modifying information flowing on the network.	DDoS Countermeasures Encryption of Communications Channels Data Encryption Exclusive Line Encryption of Communications Channels Data Signature			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Log Collection/Log Analysis Integrated Log Management System Restricts an Concerting Desice and to Loge Restricts an Concerting Desice and the Loge Restricts and Restricts		Redundancy		
17 18 19	Not applicable (no fu	unctions)			-		Packet Sniffing Unauthorized Modification of Communication Data	Interference with radio communications. Theft of information flowing on the network. Maliciously modifying information flowing on the network.	DDoS Countermeasures			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 Integrated Log Collection/Log Analysis Integrated Log Management System Integrated Log Collection/Log Analysis Integrated Log Management System Integrated Log Collection/Log Analysis Integrated Log Management System Integrated Log Collection/Log Analysis Integrated Log Management System Integ		Redundancy		
17 18 19 20	Not applicable (no fu	unctions)			-		Packet Sniffing Unauthorized Modification of Communication Data Connecting Unauthorized	Interference with radio communications. Theft of information flowing on the network. Maliciously modifying information flowing on the network.	DDoS Countermeasures		Image: Section (1998)         Image: Section (1998)           Image: Section (1998)         Image: Section (1998) <tr< td=""><td>Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Log Collection/Log Analysis Integrated Log Management System Restricts an Concerting Desice and to Loge Restricts an Concerting Desice and the Loge Restricts and Restricts</td><td></td><td>Redundancy</td><td></td><td></td></tr<>	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Log Collection/Log Analysis Integrated Log Management System Restricts an Concerting Desice and to Loge Restricts an Concerting Desice and the Loge Restricts and Restricts		Redundancy		

	Leger	nd: OMeasures imp	lement	ted C	Grayed	out line	s: Threats not ta	aken into account for the correspo	nding asset Green tex	t in measures: Suppl	ementary informa	tion on measures	
Rem Number	Type of Assets	Target Device		essment Me	etrics Importance of Assets	Dist. Materia	Threat (Attack Type)	Description	Prote		Detection/Understanding Dar	mage Business Continuity	Security Level By Threat
1	Network Asset	Switch (within DMZ), DMZ	3	2	Importance d'Assets	B	Unauthorized Access	Intrusion of the device via the network to execute an attack.	Intrusion/Spreading Phase FW (Packet Filtering Type) FW (Application Gateway Type) One-way Gateway Proxy Gateway Proxy Server WAF Peer-to-Peer Authentication	Objective Achievement Phase	IPS/IDS Log Collection/Log Analysis Integrated Log Management System		2
					-		Physical Intrusion	Unachitized access of sections/areas (device installation locations, etc.) with access	IPS/IDS Applying Patches Avoidance of Vulnerability Entrace and Exit Management (C. Carl, Biometric Authentication)	•         •           •         •           •         •	Surveillance Camera		
2			1	1		D		restrictions. It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).	Lock and Key management	0	Intrusion Detection Sensor	0	3
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
4			2	3		в	Human Error in Operation	An attack triggered by a human error in operation by internal personnel (an employee or partner with access privileges to the device). An act equivalent to an attack is performed on the device as a result of a proper media or device connection.					
5			2	3		В	Connecting Unauthorized Media or Device	Connection of unauthorized media or device (CD/DVD, USB device, etc.) brought in from outside the organization with the device to execute an attack.		(Same as on the Left)	(Same as on the Left) Log Collection/Log Analysis Integrated Log Management System		- - 1
6			2	2		с	Execution of Unauthorized Processes	Unauthorized execution of legitimate programs, commands, services, and other processes found on the attack target device.	Permission Management Access Control Application Whitelisting Approval of Important Operations	(Same as on the Left)     (Same as on the Left)     (Same as on the Left)     (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		2
7			1	3		с	Malware Infection	Infection or running of malware (unauthorized programs) on the attack target device.	Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		1
8			1	2		D	Information Theft	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management Access Control Data Encryption DLP	(Same as on the Left)     (Same as on the Left)     (Same as on the Left)     (Same as on the Left)	Log Collection/Log Analysis Integrated Log Management System		2
9			3	2		в	Unauthorized Modification of Information	Unauthorized modification of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Permission Management Access Control Data Signature	(Same as on the Left)     (Same as on the Left)     (Same as on the Left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	2
10			2	2		c	Information Destruction	Destroying of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on the device.		Permission Management Access Control •	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	2
11			1	3	2	c		Sending unauthorized control commands (settings changes, power shutdowns, etc.) and unauthorized data to other devices.	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Log Collection/Log Analysis Integrated Log Management System		1
12			2	3		в	Outage	Stopping device functions.			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Redundancy Failsafe Design	1
13			3	3		в	DoS Attack	Interruption of regular device operations by sending processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.	DDoS Countermeasures		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Redundancy Failsafe Design	1
14			1	2		D	Theft	Device theft.	Lock and Key Management	(Same as on the Left)	(Same as on the Left)		2
15			1	2		D	Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Tamper Resistance Obfuscation Zeroization	(Same as on the Left) (Same as on the Left) o (Same as on the Left)			2
16			2	1		D	Route Blocking	Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Enterce and Ent Management (C. Carl Bioretic Americator) Lock and Key management	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor	Redundancy	3
17			2	3		В	Network Congestion	Causing congestion by generating the communications traffic that exceeds the capacity of the device.	FW (Packet Filtering Type) FW (Application Gateway Type) WAF IPS/IDS DDoS Countermeasures		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Redundancy	1
18	Not applicable (no fu	nctions)			· · · · ·		Jamming	Interference with radio communications.			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Redundancy	
19			2	3		в	Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels Data Encryption Exclusive Line				1
20			2	3		в	Unauthorized Modification of Communication Data	Maliciously modifying information flowing on the network.	Encryption of Communications Channels Data Signature Exclusive Line		Log Collection/Log Analysis Integrated Log Management System		1
21			3	3		В	Connecting Unauthorized Device	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage		Restriction on Connecting Device and its Usage Log Collection/Log Analysis Integrated Log Management System		1

	Type of Assets Target Device		at Level Vulnerabi	nent Met		Risk Value	Threat (Attack Type)	Description	Prote Intrusion/Spreading Phase	Counter	Detection/Understanding Da	image	Business Continuity	
C	Control System Asset Data Historian (Relay)			-			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					
		3	3 5	2		в			WAF					
		-		-		-			Peer-to-Peer Authentication	0				
									IPS/IDS					
									Applying Patches (Web Server Only)	0				
									Avoidance of Vulnerability					
_					1									
							Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with access restrictions.	Entrance and Exit Management (IC Card, Biometric Authentication)	0	Surveillance Camera Intrusion Detection Sensor	0		
		1	'   '	1		D		It also refers to removing restrictions on devices with physical access restrictions (devices installed in ranks, cabinets, etc.)	Lock and Key management		Initiasion Detection Sensor	Ŭ		
-					1		Unauthorized Operation	Intrusion through direct operation of the device's console or other	Operator Authentication (ID/Pass)	0		+ +		
		2	2 2	2		C	onautionzeu Operation	component to execute an attack.						
1			-		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					
		2	2 7	3		В		device).						
								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)	Restriction on Connecting Device and its Usage			
		2	2 7	3		в	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					-				Demission Management		Device Free Detection			
								Unauthorized execution of legitimate programs, commands,	Permission Management Access Control	<ul> <li>(Same as on the Left)</li> <li>(Same as on the Left)</li> </ul>	Device Error Detection Device Alive Monitoring			
		2	<b>,</b> .	2		c	Processes	services, and other processes found on the attack target	Application Whitelisting	(Same as on the Left)	Log Collection/Log Analysis			
		2	-   -	2		Ŭ		device.	Approval of Important Operations	(Same as on the Left)	Integrated Log Management System			
1									Preserver of an portant Operations	(ound do on the Leity	management oystelli			
1			-+		1		Malware Infection	Infection or running of malware (unauthorized programs) on	Anti-virus	0	Device Error Detection			
								the attack target device.	Application Whitelisting		Device Alive Monitoring			
1				.		-			Applying Patches		Log Collection/Log Analysis			
		3	3 2	2		В			Avoidance of Vulnerability		Integrated Log Management System			
									Data Signature					
1														
					1		Information Theft	Theft of information (software, authentication information,	Permission Management	<ul> <li>(Same as on the Left)</li> </ul>	Log Collection/Log Analysis			
								configuration settings, encryption keys and other confidential	Access Control	(Same as on the Left)	Integrated Log Management System	$ \downarrow \downarrow$		
		3	3   7	2		В		information) stored on the device.	Data Encryption	(Same as on the Left)		+		
1									DLP	(Same as on the Left)		+		
					4	L	11	Handhadaa Marka Marka Ara	Permission Management	(Somo oo c= the l = #)	Dovino Erres Detection		ata Backup	
1								Unauthorized modification of information (software,	Permission Management	<ul> <li>(Same as on the Left)</li> <li>(Same as on the Left)</li> </ul>	Device Error Detection	<u> </u> −_  <sup>□</sup>	)ata Backup	U
		3	3   ;	2		в	Information	authentication information, configuration settings, encryption	Access Control	(Same as on the Left)	Log Collection/Log Analysis Integrated Log Management System	+		
								keys and other confidential information) stored on the device.	Data Signature	(Same as on the Lett)	megrated cog management system	+		
			-+-		1	L	Information Destruction	Destroying of information (software, authentication		Permission Management	Device Error Detection		ata Backup	0
							anormation Destruction	information, configuration (software, authentication information, configuration settings, encryption keys and other		Access Control	Log Collection/Log Analysis		and address	
[		3	3   2	2		В					Integrated Log Management System			
								confidential information) stored on the device.						
1					1		Unauthorized Transmission	Sending unauthorized control commands (settings changes,	Segmentation/Zoning	(Same as on the Left)	Log Collection/Log Analysis			
				,				power shutdowns, etc.) and unauthorized data to other	Data Signature	(Same as on the Left)	Integrated Log Management System			
		3	2   3	3	2	В		devices.	Approval of Important Operations	(Same as on the Left)				
						L								
				1			Outage	Stopping device functions.			Device Error Detection		Redundancy	
				.		_					Device Alive Monitoring	F	ailsafe Design	
		3	3 3	3		В					Log Collection/Log Analysis	+		
											Integrated Log Management System			
+					-		DoS Attack	laters ation of reaction device exerctions by another	DDoS Countermeasures		Device Error Detection		Redundancy	
							DOS Allack	Interruption of regular device operations by sending	bboo countermeasures		Device Alive Monitoring		ailsafe Design	
		1	1 .	3		c		processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.			Log Collection/Log Analysis			
		· ·		•		ľ		the device as a result of a DDOS attack, etc.			Integrated Log Management System			
1					1		Theft	Device theft.	Lock and Key Management	<ul> <li>(Same as on the Left)</li> </ul>	(Same as on the Left)			
		1	1 7	2		D				(	(			
											1			
1					1		Information Theft by	Theft of information (software, authentication information,	Tamper Resistance	(Same as on the Left)				
1			.			_		configuration settings, encryption keys and other confidential	Obfuscation	(Same as on the Left)				
		1	1   2	2		D	of Theft or Disposal	information) stored on devices which were stolen or disposed	Zeroization	<ul> <li>(Same as on the Left)</li> </ul>				
1								of and then disassembled.				Ιſ		1
					1		Route Blocking	Communications are blocked by disconnecting the	Entrance and Exit Management		Device Error Detection	R	Redundancy	
							9	communication cable.	Lock and Key management		Device Alive Monitoring			
								Alternatively, communications are blocked by pulling out the			Log Collection/Log Analysis			
								communication cable from the device.			Integrated Log Management System			
											Surveillance Camera			
											Intrusion Detection Sensor			
					1		Network Congestion	Causing congestion by generating the communications traffic	FW (Packet Filtering Type)		Device Error Detection	R	Redundancy	
								that exceeds the capacity of the device.	FW (Application Gateway Type)		Device Alive Monitoring			
									WAF		Log Collection/Log Analysis			
									IPS/IDS		Integrated Log Management System			
									DDoS Countermeasures					
					1									
							Jamming	Interference with radio communications.			Device Error Detection	R	Redundancy	
											Device Alive Monitoring			
											Log Collection/Log Analysis			
											Integrated Log Management System			
												1		
	Not applicable (no functions)						Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels					
	Not applicable (no functions)						Packet Sniffing	Theft of information flowing on the network.						
	Not applicable (no functions)						Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels Data Encryption Exclusive Line					
	Not applicable (no functions)						Packet Sniffing	Theft of information flowing on the network.	Data Encryption					
	Not applicable (no functions)								Data Encryption Exclusive Line		Log Collection/I no Analysis			
	Not applicable (no functions)						Unauthorized Modification of	Theft of information flowing on the network. Maliciously modifying information flowing on the network.	Data Encryption Exclusive Line Encryption of Communications Channels		Log Collection/Log Analysis Integrated Log Management System			
	Notapplicable (no functions)								Data Encryption Exclusive Line Encryption of Communications Channels Data Signature		Log Collection/Log Analysis Integrated Log Management System			
	Not applicable (no functions)						Unauthorized Modification of		Data Encryption Exclusive Line Encryption of Communications Channels					
	Not applicable (no functions)						Unauthorized Modification of Communication Data	Maliciously modifying information flowing on the network.	Data Encryption Exclusive Line Encryption of Communications Channels Data Signature Exclusive Line					
	Not applicable (no functions)						Unauthorized Modification of Communication Data Connecting Unauthorized		Data Encryption Exclusive Line Encryption of Communications Channels Data Signature		Integrated Log Management System			
	Not applicable (no functions)						Unauthorized Modification of Communication Data	Maliciously modifying information flowing on the network.	Data Encryption Exclusive Line Encryption of Communications Channels Data Signature Exclusive Line		Integrated Log Management System			

em Number			Acc	essment Me	etrics						Countern	ieasu	es				Security Leve
	Type of Assets	Target Device				Risk Value	Threat (Attack Type)	Description	Prote Intrusion/Spreading Phase	ection	Objective Achievement Pha	ISP.	Detection/Understanding Da	mage	Business Continuity		By Threat
	Control System Asset	Data Historian	Thick Level	Turking Care	into a ce o cana	TUSK Value	Unauthorized Access	Intrusion of the device via the network to execute an	FW (Packet Filtering Type)		Objective Achievement I h	130	IPS/IDS	1			
	-							attack.	FW (Application Gateway Type)				Log Collection/Log Analysis				
									One-way Gateway				Integrated Log Management System				
									Proxy Server					-			
1			2	2		c			WAF Peer-to-Peer Authentication	0				-			2
									IPS/IDS	-							
									Applying Patches								
									Avoidance of Vulnerability								
_					-		Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.)	Entrance and Exit Management (IC Card, Biometric Authentication)	0			Surveillance Camera	0			
2			1	1		р	i nyaidai inirdalori	with access restrictions.	Lock and Key management	0			Intrusion Detection Sensor	0			3
~			· ·			-		It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).									0
3			2	2	1	с	Unauthorized Operation	Intrusion through direct operation of the device's console or other	Operator Authentication (ID/Pass)	0							2
3				2	4	<u> </u>		component to execute an attack.	U.D. Filtering Mich Desutation								2
							Human Error in Operation	An attack triggered by a human error in operation by internal personnel (an employee or partner with access privileges to the device).	URL Filtering/Web Reputation 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 connection.									
					4		Connection Unauthorized Media or Device	Connection of unauthorized media or device (CD/DVD, USB device, etc.)	Pertiction on Connecting Davice and its Licage	<u> </u>	(Same as on the Left)		(Same as on the Left)				
_								brought in from outside the organization with the device to execute an	recenced on connecting before and its eading		(ound do on the Long		Log Collection/Log Analysis				
5			2	3		В		attack.					Integrated Log Management System				1
					4				Denvision Management		(O		De las Este Data d'as				
							Execution of Unauthorized Processes	Inauthorized 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	-			
6			2	2		c		_	Application Whitelisting	0	(Same as on the Left)		Log Collection/Log Analysis				2
									Approval of Important Operations		(Same as on the Left)		Integrated Log Management System				
			<u> </u>		-	<u> </u>	Mahuara Infontion	Infection or number of maleure (second second	Anti-virue				Device Error Detection				
			1				Malware Infection	Infection or running of malware (unauthorized programs) on the attack target device.	Anti-virus Application Whitelisting	0			Device Error Detection Device Alive Monitoring	1			
,				_					Applying Patches				Log Collection/Log Analysis				2
1			3	2		В			Avoidance of Vulnerability				Integrated Log Management System				2
									Data Signature	<u> </u>				<u> </u>			
_					-		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	Access Control		(Same as on the Left)		Integrated Log Management System				
8			3	2		В		device.	Data Encryption		(Same as on the Left)						2
									DLP		(Same as on the Left)			-			
					-	<u> </u>	Unauthorized Modification of Information	Unauthorized modification of information (software, authentication	Permission Management	0	(Same as on the Left)		Device Error Detection	-	Data Backup	0	
9						в		information, configuration settings, encryption keys and other confidential	Access Control		(Same as on the Left)		Log Collection/Log Analysis				2
9			3	2		P		information) stored on the device.	Data Signature		(Same as on the Left)		Integrated Log Management System				2
					-		Information Destruction	Destroying of information (software, authentication information,			Permission Management	0	Device Error Detection	<u> </u>	Data Backup	0	
							mormation Destruction	configuration settings, encryption keys and other confidential information)			Access Control	-	Log Collection/Log Analysis				
10			3	2		В		stored on the device.					Integrated Log Management System				2
					4		Description of Theorem Sector	Sending unauthorized control commands (settings changes, power	Segmentation/Zoning		(Same as on the Left)		Log Collection/Log Analysis				
							Unauthorized Transmission	shutdowns, etc.) and unauthorized data to other devices.	Data Signature		(Same as on the Left)		Integrated Log Management System				
11			3	3	2	В			Approval of Important Operations		(Same as on the Left)						1
					1												
							Outage	Stopping device functions.					Device Error Detection Device Alive Monitoring	-	Redundancy Failsafe Design		
12			3	3		в							Log Collection/Log Analysis				1
						_							Integrated Log Management System				
					-				DDaS Caustamana				Device Free Detection		Deducdency		
							DoS Attack	Interruption of regular device operations by sending processing requests that exceed the processing capacity of the device as a result of a DDoS	DD0S Countermeasures				Device Error Detection Device Alive Monitoring		Redundancy Failsafe Design		
13			1	3		c		attack, etc.					Log Collection/Log Analysis				1
													Integrated Log Management System				
					4		71.0	Device theft.	Lash and Kan Managara		(O		(0				
14			1	2		р	Theft	Device meit.	Lock and Key Management	0	(Same as on the Left)		(Same as on the Left)				2
			· ·	-		-											-
					1		Information Theft by Tampering Device at Time of Theft or Disposal	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		(Same as on the Left)						2
			1						Zeroization		(Same as on the Left)			-			
					1		Route Blocking	Communications are blocked by disconnecting the communication cable.					Device Error Detection		Redundancy		
								Alternatively, communications are blocked by pulling out the communication cable from the device.	Lock and Key management				Device Alive Monitoring Log Collection/Log Analysis				
16													Log Collection/Log Analysis Integrated Log Management System				
10												_	Surveillance Camera				
													Intrusion Detection Sensor				
					-												
							Network Congestion		FW (Packet Filtering Type)			_	Device Error Detection Device Alive Monitoring		Redundancy		
									FW (Application Gateway Type) WAF				Log Collection/Log Analysis				
									IPS/IDS				Integrated Log Management System				
17									DDoS Countermeasures								
17							I						During Francisco		Deductor		
17							Jamming	Interference with radio communications.					Device Error Detection Device Alive Monitoring		Redundancy		
17	Not applicable (no fu	inctions)			1									-			
17	Not applicable (no fu	inctions)			1								Log Collection/Log Analysis				
	Not applicable (no fu	inctions)			1								Log Collection/Log Analysis Integrated Log Management System				
	Not applicable (no fu	nctions)															
	Not applicable (no fu	nctions)			1		Packet Sniffing	Thet of information flowing on the network.	Encryption of Communications Channels								
	Not applicable (no fu	nctions)			1		Packet Sniffing		Data Encryption								
18	Not applicable (no fu	nctions)			-		Packet Sniffing										
18	Not applicable (no fu	nctions)							Data Encryption Exclusive Line				Integrated Log Management System				
18	Not applicable (no fu	nctions)			-			Maliciously modifying information flowing on the network.	Data Encryption Exclusive Line Encryption of Communications Channels Data Signature								
18	Not applicable (no fu	nctions)			-			Maliciously modifying information flowing on the network.	Data Encryption Exclusive Line Encryption of Communications Channels				Integrated Log Management System				
18	Not applicable (no fu	nctions)			-		Unatherized Welffeelon of Communication Data	Maliciously modifying information flowing on the network.	Data Encryption Exclusive Line Encryption of Communications Channels Data Signature Exclusive Line				Integrated Log Management System				
18 19 20	Not applicable (no fu	nctions)			-		Unatherized Welffeelon of Communication Data	Maliciously modifying information flowing on the network.	Data Encryption Exclusive Line Encryption of Communications Channels Data Signature				Integrated Log Management System				
18	Not applicable (no fu	inctions)			-		Unatherized Welffeelon of Communication Data	Maliciously modifying information flowing on the network.	Data Encryption Exclusive Line Encryption of Communications Channels Data Signature Exclusive Line				Integrated Log Management System				

Truck	Transform	Ass	sessment Me	trics		Three (Annual T	Development			measures	_			Security Le
Number Type of Assets	Target Device	Threat Level	Vulnerability Level	Importance of Assets	Risk Value	Threat (Attack Type)	Description	Protect Intrusion/Spreading Phase	Objective Achievement P	Detection/Understanding D	amage	Business Continuity	E	By Threa
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							FW (Application Gateway Type)		Log Collection/Log Analysis				
	Network (Information Side)							One-way Gateway		Integrated Log Management System				
								Proxy Server						
		2	2		c			WAF		<u>   </u>	+ $+$			2
								Peer-to-Peer Authentication	0		+		<u> </u>	
								IPS/IDS			+ +			
								Applying Patches Avoidance of Vulnerability			+			
								Avoidance of vulnerability			++		<u> </u>	
				1		Physical Intrusion	Unauthorized access of sections/areas (device installation locations, etc.) with access	Entrance and Exit Management (IC Card)	0	Surveillance Camera	0			
		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.).							
		2	2		с	Unauthorized Operation	Intrusion through direct operation of the device's console or other	Operator Authentication (ID/Pass)	0		$\square$		$\square$	2
		<u> </u>	-	-	<u> </u>		component to execute an attack. An attack triggered by a human error in operation by internal	LIPL Eithering/Mab Reputation			+		+	
						Human Error in Operation		URL Filtering/Web Reputation Mail Filtering			+ +			
		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)			<u> </u>	
		2	3		в	Media or Device	device, etc.) brought in from outside the organization with the			Log Collection/Log Analysis Integrated Log Management System	+			1
							device to execute an attack.			inegrated Eog Manageneric System	+ +		H	
						Execution of Unauthorized	Unauthorized execution of legitimate programs, commands,	Permission Management	<ul> <li>(Same as on the Left)</li> </ul>	Device Error Detection	+ +			
						Processes	services, and other processes found on the attack target	Access Control	(Same as on the Left)	Device Alive Monitoring				
		1	2		D		device.	Application Whitelisting	(Same as on the Left)	Log Collection/Log Analysis	$+ \top$			2
								Approval of Important Operations	(Same as on the Left)	Integrated Log Management System	+ $+$	7	$\square$	
		L		4	L	Maharan I. C. M		Antivirus		Dovine Free Datastica	+		$\vdash$	
						Malware Infection		Anti-virus Application Whitelisting		Device Error Detection Device Alive Monitoring	+			
							the attack target device.	Applying Patches		Log Collection/Log Analysis	+-+-			
		1	3		c			Avoidance of Vulnerability		Integrated Log Management System	++-		$\square$	1
								Data Signature	1				$\square$	
						Information Theft	Theft of information (software, authentication information,	Permission Management	<ul> <li>(Same as on the Left)</li> </ul>	Log Collection/Log Analysis	+		$\vdash$	
							configuration settings, encryption keys and other confidential	Access Control	(Same as on the Left)	Integrated Log Management System	+ +			
		1	2		D		information) stored on the device.	Data Encryption DLP	(Same as on the Left) (Same as on the Left)		++			2
									(Same as on the Leit)		+ +			
		<u> </u>		1		Unauthorized Modification of	Unauthorized modification of information (software,	Permission Management	<ul> <li>(Same as on the Left)</li> </ul>	Device Error Detection	Dat	ta Backup		
					c	Information	authentication information, configuration settings, encryption	Access Control	(Same as on the Left)	Log Collection/Log Analysis				2
		2	2				keys and other confidential information) stored on the device.	Data Signature	(Same as on the Left)	Integrated Log Management System				2
													$\vdash$	
						Information Destruction	Destroying of information (software, authentication		Permission Management Access Control	Oevice Error Detection     Log Collection/Log Analysis		ta Backup		
		2	2		c		information, configuration settings, encryption keys and other		Access Control	Integrated Log Management System	++-			2
							confidential information) stored on the device.				+ +			
						Unauthorized Transmission	Sending unauthorized control commands (settings changes,	Segmentation/Zoning	(Same as on the Left)	Log Collection/Log Analysis				
		1	3	2	c		power shutdowns, etc.) and unauthorized data to other	Data Signature	(Same as on the Left)	Integrated Log Management System				1
		l .	ľ	-	ľ		devices.	Approval of Important Operations	(Same as on the Left)		+ $+$			
		L		-		0.1	Otension de las Castinas			Device Error Detection	- Rer	dundancy	┢━┿	
						Outage	Stopping device functions.			Device Alive Monitoring		Isafe Design		
		2	3		в					Log Collection/Log Analysis				1
		-	-		-					Integrated Log Management System				
						DoS Attack	Interruption of regular device operations by sending	DDoS Countermeasures		Device Error Detection		dundancy	<u> </u>	
					в		processing requests that exceed the processing capacity of			Device Alive Monitoring Log Collection/Log Analysis		Isafe Design		
		3	3		в		the device as a result of a DDoS attack, etc.			Integrated Log Management System	+			1
											+			
				1		Theft	Device theft.	Lock and Key Management	<ul> <li>(Same as on the Left)</li> </ul>	Lock and Key Management	0			
		1	2		D									2
						Information Theft by	Theft of information (software, authentication information,	Tamper Resistance	(Same as on the Left)		+ +		<u> </u>	
		1	2		D	Tampering Device at Time		Obfuscation	(Same as on the Left)		+		$\vdash$	2
						of Theft or Disposal	information) stored on devices which were stolen or disposed of and then disassembled.	2012/20101	<ul> <li>(Same as on the Left)</li> </ul>		+ $+$		<u> </u>	
				1		Route Blocking	Communications are blocked by disconnecting the	Entrance and Exit Management (IC Card)	0	Device Error Detection	Rec	dundancy		
						, i i i i i i i i i i i i i i i i i i i	communication cable.	Lock and Key management	0	Device Alive Monitoring	$+ \top$			
							Alternatively, communications are blocked by pulling out the			Log Collection/Log Analysis				
		2	2		c		communication cable from the device.	ļ l		Integrated Log Management System	+ $+$		$\vdash$	2
										Surveillance Camera	•		$\vdash$	
										Intrusion Detection Sensor	+		$\vdash$	
		<u> </u>	-	1	<u>├</u> ──	Network Conception	Causing congestion by generating the communications traffic	EW (Packet Filtering Turce)		Device Error Detection		dundancy	<b>⊢</b> +	
						Network Congestion	that exceeds the capacity of the device.	FW (Packet Filtering Type) FW (Application Gateway Type)		Device Error Detection Device Alive Monitoring		dundancy	<u> </u>	
							and another are capacity of are device.	WAF		Log Collection/Log Analysis	+			
		2	3		В			IPS/IDS	1	Integrated Log Management System	+-+-			1
								DDoS Countermeasures			++		$\square$	
Not applicable (no f	unctions)			-		Jamming	Interference with radio communications.			Device Error Detection	Red	dundancy		
.vocappiicable (not	anceonaj									Device Alive Monitoring				
										Log Collection/Log Analysis	+		$\square$	
										Integrated Log Management System	+			
		-		-	F	Packet Spiffer	That of information flowing on the activity	Enonution of Communications Character			+-+		$\vdash$	
						Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels			+ +-		<u> </u>	
		2	3		в			Data Encryption Exclusive Line			+ +		<u> </u>	1
											++-			
				1	<u> </u>	Unauthorized Modification of	Maliciously modifying information flowing on the network.	Encryption of Communications Channels		Log Collection/Log Analysis	++		$\vdash$	
					-	Communication Data		Data Signature		Integrated Log Management System	++			
					В			Exclusive Line			+			1
		2	3							· · · ·				
		2	3								++		$\square$	
		2	3	-		Connecting Unauthorized	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage		Restriction on Connecting Device and its Usage	++		$\square$	
		<u> </u>		-		Connecting Unauthorized Device	Connecting unauthorized device on the network			Log Collection/Log Analysis				
		2	3	-	в	-	Connecting unauthorized device on the network							1

Type of Assets	s Target Device	As	Assessment Me	letrics		Threat (Attack Type)	Description	Prote	ection	ermeasures		
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		Threat Leve	Vel Vulnerability Level	vel Importance of Assets	Risk Value			Intrusion/Spreading Phase	Objective Achievement I	Phase Detection/Understanding Da	amage Business Continuity	
Control System As	sset EWS					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				
		2	2		в			WAF				
		-	-					Peer-to-Peer Authentication	0			
								IPS/IDS				
								Applying Patches			)	
								Avoidance of Vulnerability				
				-								
						Physical Intrusion	Unauthorized access of sections/areas (device installation locations,	Entrance and Exit Management (IC Card, Biometric Authentication) Lock and Key Management	0	Surveillance Camera Intrusion Detection Sensor	0	
		1	1		c		etc.) with access restrictions. It also refers to removing restrictions on devices with physical	LOCK and Key Management	5	Intrusion Detection Sensor		+
		· ·			Ŭ		access restrictions (devices installed in racks, cabinets, etc.).				/	
											/	
			-		_	Unauthorized Operation	Intrusion through direct operation of the device's console or	Operator Authentication (ID/Pass)	0			
		2	2		в		other component to execute an attack.				/	
						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				
		2	3		A		device).					
							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)	<b>₽−1</b>	
		3	3		A	Media or Device	device, etc.) brought in from outside the organization with the			Log Collection/Log Analysis Integrated Log Management System	<u>                                      </u>	
							device to execute an attack.			integrated Log Management System	<u>                                      </u>	
			+	-		Execution of Unauthorized	Unauthorized execution of legitimate programs, commands,	Permission Management	(Same as on the Left)	Device Error Detection	<u>+                                    </u>	+
						Processes	services, and other processes found on the attack target	Access Control	(Same as on the Left)	Device Alive Monitoring	· · · · · · · · · · · · · · · · · ·	$\square$
		3	3		A		device.	Application Whitelisting	(Same as on the Left)	Log Collection/Log Analysis	· · · · · · · · · · · · · · · · · ·	$\square$
		1	1					Approval of Important Operations	(Same as on the Left)	Integrated Log Management System	· · · · · · · · · · · · · · · · · ·	$\square$
				7		Malware Infection	Infection or running of malware (unauthorized programs) on	Anti-virus		Device Error Detection		
							the attack target device.	Application Whitelisting		Device Alive Monitoring	<u>    / / / / / / / / / / / / / / / / / /</u>	$\square$
		3	3		•			Applying Patches		Log Collection/Log Analysis	<u>                                     </u>	$\square$
		1	1		<b>^</b>			Avoidance of Vulnerability		Integrated Log Management System	<u>                                      </u>	$\square$
								Data Signature		+ +	<u>+ +</u>	$\vdash$
				4	L			Permission Management	(Como oo aa tha Laft)		+ + /	+
						Information Theft	Theft of information (software, authentication information,	Permission Management Access Control	(Same as on the Left) (Same as on the Left)	Log Collection/Log Analysis Integrated Log Management System	<u>+                                    </u>	+
		3	3				configuration settings, encryption keys and other confidential	Data Encryption	(Same as on the Left)	neg-noo cog mandyerrent oystem	<u>+                                    </u>	+
		3	3		A		information) stored on the device.	Dia Encryption	(Same as on the Left)		<u>+ +</u> →	+
									(Game as on the cert)		<u>+                                    </u>	
						I Inauthorized Modification of	f 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	, <u> </u>	
		3	3		A		keys and other confidential information) stored on the device.	Data Signature	(Same as on the Left)	Integrated Log Management System	<u>,                                     </u>	
						Information Destruction	Destroying of information (software, authentication		Permission Management	Device Error Detection	Data Backup	
		3	3		A		information, configuration settings, encryption keys and other		Access Control	Log Collection/Log Analysis	<u>                                       </u>	$\vdash$
		, i					confidential information) stored on the device.			Integrated Log Management System	<u>                                       </u>	
-			<u> </u>	-				Segmentation/Zening	(Some co on the Loff)	Log Collection/Log Applysic	<u>                                      </u>	
				3		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	<u>+                                    </u>	+
		3	3		A		power shutdowns, etc.) and unauthorized data to other devices.	Approval of Important Operations	(Same as on the Left)		<u>+ +</u> − − − − − − − − − − − − − − − − − −	+
							devices.	- + p	(		<u>                                     </u>	
1						Outage	Stopping device functions.			Device Error Detection	Redundancy	
										Device Alive Monitoring	Failsafe Design	
		3	3		A					Log Collection/Log Analysis		
										Integrated Log Management System		
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 Log Collection/Log Analysis	Failsafe Design	+
		1	3		В		the device as a result of a DDoS attack, etc.			Integrated Log Management System	<u>                                      </u>	+
										integrates bog management by sem	<u>↓ ↓                                  </u>	+
-			+	-		Theft	Device theft.	Lock and Key Management	<ul> <li>(Same as on the Left)</li> </ul>	(Same as on the Left)	<u>       </u>	
		2	2		в	Incit	Device their.	Lock and Key Management	(Same as on the Leit)	(Same as on the Leit)		
		-	· ·		<u> </u>					+ +	<u>+ +</u> →	+
			+			Information Theft by	Theft of information (software, authentication information,	Tamper Resistance	(Same as on the Left)		<u>                                      </u>	
		2	2		в	Tampering Device at Time	configuration settings, encryption keys and other confidential	Obfuscation	(Same as on the Left)			
		4	<b>4</b>		°	of Theft or Disposal	information) stored on devices which were stolen or disposed of and	Zeroization	<ul> <li>(Same as on the Left)</li> </ul>		<u> </u>	
				_			then disassembled.					
						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		
							Alternatively, communications are blocked by pulling out the			Log Collection/Log Analysis		$\left  \right $
							communication cable from the device.			Integrated Log Management System		+
										Surveillance Camera		+
										Intrusion Detection Sensor		
			_	-		Network Congestion	Causing congestion by generating the communications traffic	EW (Packet Filtering Turs)		Device Error Detection	Redundancy	
						Convert Congestion	that exceeds the capacity of the device.	FW (Packet Filtering Type) FW (Application Gateway Type)		Device Error Detection Device Alive Monitoring	recondency	+
							and an output of the up to the up to the	WAF		Log Collection/Log Analysis		
								IPS/IDS		Integrated Log Management System		
								DDoS Countermeasures		in the sign and general cystelli		$\square$
											<u> </u>	
			_	-		Jamming	Interference with radio communications.			Device Error Detection	Redundancy	
Not applicable (n	o functions)						Contraction of the second seco			Device Alive Monitoring		$\square$
										Log Collection/Log Analysis	<u> </u>	
										Integrated Log Management System		
		_									<u> </u>	
						Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels			<u> </u>	
								Data Encryption			<u> </u>	
								Exclusive Line				$\square$
												+
				-		Unauthorized Modification of	Maliciously modifying information flowing on the network.	Encryption of Communications Channels		Log Collection/Log Analysis		
						Communication Data	with the second se	Data Signature		Integrated Log Management System		
						South Data		Exclusive Line		mogratice cog management oystem		
												1
				-		Connecting Unauthorized	Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage		Restriction on Connecting Device and its Usage		
				-			Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage				
						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		

	Type of Assets	Target Device	As	sessment Me	etrics		Threat (Attack Type)	Description	Dest	tection	Counterine	asures	_				Sec B
	Type of Assets	Target Device	Threat Level	Vulnerahility Leve	el Importance of Assets	Risk Value	Threat (Attack Type)	Description	Intrusion/Spreading Phase		Objective Achievement Phas	Detection/Underst	anding Dam	nage	Business Continuity		
Co	Control System Asset	Control Server				THOIR FUIDO	Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type)			IPS/IDS		<u> </u>			+-
1~	ona or of otomin boot	Contact Corver			1 '		OnButhon260 Access	and dolor of the device via the network to execute an attack.	FW (Application Gateway Type)	+-+		Log Collection/Log	Analysis	-+	·	+	1
	1				1 '				One-way Gateway			Integrated Log Manageme				-	1
	1				1 '				Proxy Server				-			1	1
	1		2		1 '				WAF								1
	I		2	2	· ·	в			Peer-to-Peer Authentication	0							1
	1				1 '				IPS/IDS								1
	1				1 '				Applying Patches								]
	l				1 '				Avoidance of Vulnerability								1
	l				1 '												1
Τ	1				יך		Physical Intrusion	Unauthorized access of sections/areas (device installation locations,		0		Surveillance Came		0			_
	1				1 '			etc.) with access restrictions.	Lock and Key management	•		Intrusion Detection	Sensor	°			4
	1		1	1	1 '	c		It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).						.			
	1				1 '			access restrictions (devices installed in racks, cabinets, etc.).						.			
+	1			<u> </u>			Lineuthorized Operation	Intrusion through direct operation of the device's console or other	Operator Authentication (ID/Pass)	-						+	+
	1		2	2	1 '	В	Unauthorized Operation	component to execute an attack.	Operator Admentication (ID/F 833)							-	1
1	1				1 '		Human Error in Operation	An attack triggered by a human error in operation by internal	URL Filtering/Web Reputation								_
	1				1 '			personnel (an employee or partner with access privileges to the	Mail Filtering								
	l		2	3	1 '	A		device).									
	1				1 '			An act equivalent to an attack is performed on the device as a result of a proper media or device connection.		+				$ \rightarrow $			4
	l				1 '			or a proper media or device connection.						.			
t	1			-			Connecting Unauthorized	Connection of unauthorized media or device (CD/DVD, USB	Restriction on Connecting Device and its Usage	3)	Same as on the Left)	(Same as on the Le	ft)			-	+
	1				1 '		Media or Device	device, etc.) brought in from outside the organization with the				Log Collection/Log					1
	1		2	3	1 '	A		device to execute an attack.				Integrated Log Manageme	nt System				1
	l																
Τ	1				יך		Execution of Unauthorized	Unauthorized execution of legitimate programs, commands,	Permission Management		Same as on the Left)	Device Error Detec					-
	1				1 '		Processes	services, and other processes found on the attack target	Access Control		Same as on the Left)	Device Alive Monito		$ \rightarrow $		+'	4
	1		3	2	1 '	A		device.	Application Whitelisting		Same as on the Left)	Log Collection/Log		$ \rightarrow $		<u>+</u> _'	4
	1				1 '				Approval of Important Operations	(8	Same as on the Left)	Integrated Log Manageme	it System	$ \rightarrow $		<b></b>	4
	1			<u> </u>					Antivirun	+		Device Free D	tion	<b></b> +		+'	+
	1			1	1 '		Malware Infection		Anti-virus Application Whitelisting			Device Error Detec Device Alive Monitor		-+		+	-
	1				1 '			the attack target device.	Applying Patches	+-+		Log Collection/Log		$\rightarrow$		+	+
	1		3	2	1 '	A			Avoidance of Vulnerability	++		Integrated Log Manageme		-+		+	1
	l				1 '				Data Signature	+				-+		+	-
	1				1 '					+-+		-		+		<u> </u>	1
l	1			1	1 '		Information Theft	Theft of information (software, authentication information,	Permission Management	· (5	Same as on the Left)	Log Collection/Log	Analysis				1
	1				1 '			configuration settings, encryption keys and other confidential	Access Control	(S	Same as on the Left)	Integrated Log Manageme					
	1		3	2	1 '	A		information) stored on the device.	Data Encryption		Same as on the Left)						
	1				1 '				DLP		Same as on the Left)						
	1				'												1
	1				יך		Unauthorized Modification of	Unauthorized modification of information (software,	Permission Management		Same as on the Left)	Device Error Detec		F	Data Backup	0	_
	1		3	2	1 '	A	Information	authentication information, configuration settings, encryption	Access Control		Same as on the Left)	Log Collection/Log		<u> </u>		<u>+</u> '	4
	1			-	1 '			keys and other confidential information) stored on the device.	Data Signature	(S	Same as on the Left)	Integrated Log Manageme	nt System				4
	l									+ +				<u> </u>	Data Backup		+
	1				1 '		Information Destruction	Destroying of information (software, authentication			Permission Management	<ul> <li>Device Error Detection</li> <li>Log Collection/Log A</li> </ul>		Ē	Јата Баскир	-	-
	1		3	2	1 '	A		information, configuration settings, encryption keys and other			ICCESS CONTION	Integrated Log Manageme		-+		+	-
	1				1 '			confidential information) stored on the device.		+		integrates cog managene	ii oyalalii	-+		+	-
ł	1			+	3		I Inauthorized Transmission	Sending unauthorized control commands (settings changes,	Segmentation/Zoning	(5	Same as on the Left)	Log Collection/Log	Analysis	-+		+	+
	1				° '			power shutdowns, etc.) and unauthorized data to other	Data Signature		Same as on the Left)	Integrated Log Manageme					1
	1		3	3	1 '	A		devices.	Approval of Important Operations	(5	Same as on the Left)						1
	1				'												1
	l				יך		Outage	Stopping device functions.				Device Error Detec			Redundancy		T
	l				1 '					+		Device Alive Monitor		F	Failsafe Design		4
	1		3	3	1 '	A				+		Log Collection/Log					4
	1				1 '					+		Integrated Log Manageme	nt System				4
	l			+					DD-C Caustomeran	+		Davias Free Datas		<u> </u>	Deducdance		+
	1				1 '		DoS Attack	Interruption of regular device operations by sending	DDoS Countermeasures	++		Device Error Detec Device Alive Monitor			Redundancy Failsafe Design	+	-
	1		1	3	1 '	в		processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.		+ +		Log Collection/Log		- ŀ	dilodio Dobigit	+	1
	1			ľ	1 '			the device as a result of a DDoS attack, etc.		+		Integrated Log Manageme		-+		1	1
	,									1 1						-	-
					1					++			Г	└──┼-		+	
					4		Theft	Device theft.	Lock and Key Management	• (S	Same as on the Left)	(Same as on the Le	ft)				+
			1	2	-	с	Theft	Device theft.	Lock and Key Management	• (S	Same as on the Left)	(Same as on the Le	ft)	Ħ		+	+
			1	2		с	Theft					(Same as on the Le	(ft)			E	
			1	2			Theft Information Theft by	Device theft. Theft of information (software, authentication information,	Lock and Key Management Tamper Resistance		Same as on the Left)	(Same as on the Le	:ft)			E	
			-		-	c	Information Theft by Tampering Device at Time	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential	Tamper Resistance Obfuscation	(S	Same as on the Left) Same as on the Left)	(Same as on the Le	ift)				-
			1	2	-	c	Information Theft by	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and	Tamper Resistance Obfuscation	(S	Same as on the Left)	(Same as on the Le	ift)				-
			-		-	с	Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) street on devices which were stolen or disposed of and then disassembled.	Tamper Resistance Obfuscation Zeroization	(S	Same as on the Left) Same as on the Left)				Zeckurdaneu		
			-		-	с	Information Theft by Tampering Device at Time	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassemilied. Communications are blocked by disconnecting the	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management	(S	Same as on the Left) Same as on the Left)	Device Error Detec	tion		Redundancy		
			-			с	Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable.	Tamper Resistance Obfuscation Zeroization	(S	Same as on the Left) Same as on the Left)	Device Error Detec Device Alive Monito	tion		Redundancy		
			-			с	Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) strotes 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	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management	(S	Same as on the Left) Same as on the Left)	Device Error Detec Device Alive Monit Log Collection/Log	tion oring Analysis		Redundancy		
			-			с	Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable.	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management	(S	Same as on the Left) Same as on the Left)	Device Error Detec Device Alive Monit Log Collection/Log , Integrated Log Manageme	tion oring Analysis mt System		Redundancy		
			-			с	Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) strotes 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	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management	(S	Same as on the Left) Same as on the Left)	Device Error Detec Device Alive Monitor Log Collection'Log Untegratel Log Managere Surveillance Came	tion oring Analysis mt System ra		Redundancy		
			-			с	Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) strotes 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	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management	(S	Same as on the Left) Same as on the Left)	Device Error Detec Device Alive Monit Log Collection/Log , Integrated Log Manageme	tion oring Analysis mt System ra		Redundancy		
			-			c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) strored 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	Tamper Resistance Obtiscation Zeroization Entrance and Exit Management Lock and Key management	(S	Same as on the Left) Same as on the Left)	Device Error Detec Device Alive Monte Log Collection/Log Universite Log Managere Surveillance Camer Intrusion Detection	tion oring Analysis nt System ra Sensor				
			-			c	Information Theft by Tampering Device at Time of Theft or Disposal	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) street on devices which were stolen or disposed of and then disassembled. Communication cable are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Tamper Resistance Obtiscation Zeroization Entrance and Exit Management Lock and Key management	(S	Same as on the Left) Same as on the Left)	Device Error Detec Device Alive Monitor Log Collection'Log Untegratel Log Managere Surveillance Came	tion oring Analysis mt System ra Sensor tion		Redundancy Redundancy		
			-		-	c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management Lock and Key management FW (Packet Filtering Type)	(S	Same as on the Left) Same as on the Left)	Device Error Detect Device Alive Monitor Log Collection/Log . Integrated Log Manageme Surveillance Came Intrusion Detection Device Error Detect	tion oring Analysis rit System ra Sensor tion oring				
			-		-	c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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	Tamper Resistance Obtiscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/DS	(S	Same as on the Left) Same as on the Left)	Device Error Detect Device Alive Monitorium Log Collection/Log Integrated Log Manageme Surveillance Came Intrusion Detection Device Error Detect Device Alive Monitor	tion pring Analysis nt System ra Sensor tion pring Analysis				
			-		-	c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management Lock and Key management PW (Packet Filtering Type) FW (Application Gateway Type) WAF	(S	Same as on the Left) Same as on the Left)	Device Error Detec Device Alive Monite Log Collection/Log, Vergate Log Managere Surveillance Camer Intrusion Detection Device Error Detec Device Alive Monit Log Collection/Log	tion pring Analysis nt System ra Sensor tion pring Analysis				
			-			c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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	Tamper Resistance Obtiscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/DS	(S	Same as on the Left) Same as on the Left)	Device Error Detec Device Alive Monite Log Collection/Log, Vergate Log Managere Surveillance Camer Intrusion Detection Device Error Detec Device Alive Monit Log Collection/Log	tion pring Analysis nt System ra Sensor tion pring Analysis				
			-		-	c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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	Tamper Resistance Obtiscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/DS	(S	Same as on the Left) Same as on the Left)	Device Error Detec Device Alive Monite Log Collection/Log, Vergate Log Managere Surveillance Camer Intrusion Detection Device Error Detec Device Alive Monit Log Collection/Log	tion fring Analysis and System France Analysis fra Sensor france Analysis fra Sensor france Analysis fra System fra Syste	R			
	Not applicable (no fui	nctions)	-			c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communication cable 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.	Tamper Resistance Obtiscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/DS	(S	Same as on the Left) Same as on the Left)	Device Error Defect Device Alive Monitor Log Collection/Log Integrate Log Manageme Intrusion Detection Device Error Detec Device Alive Monitor Log Collection/Log Integrated Log Manageme	tion pring Analysis nt System ra Sensor dition pring Analysis nt System tion tion	R	Redundancy		
	Not applicable (no fu	nctions)	-		-	c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communication cable 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.	Tamper Resistance Obtiscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/DS	(S	Same as on the Left) Same as on the Left)	Device Error Detect Device Alive Monit Log CollectionLog. Surveillance Came Intrusion Detection Device Error Detection Device Error Detection Understellang Manageme Device Error DetectionLog Device Error DetectionLog Device Error DetectionLog Device Error Detection Device Error Device Er	tion pring Analysis Analysis Sensor tion pring Analysis Sensor tion pring Analysis Int System to System tion pring Analysis Analysis Ition pring Analysis	R	Redundancy		
	Not applicable (no fu	nctions)	-		-	c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communication cable 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.	Tamper Resistance Obtiscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/DS	(S	Same as on the Left) Same as on the Left)	Device Error Detect Device Aive Monitor Log Collection/Log Vergetate Log Managere Surveillance Came Intrusion Detection Device Error Detect Device Aive Monitor Log Collection/Log Integrated Log Managere Device Error Detect Device Aive Monitor	tion pring Analysis Analysis Sensor tion pring Analysis Sensor tion pring Analysis Int System to System tion pring Analysis Analysis Ition pring Analysis	R	Redundancy		
	Not applicable (no fu	nctions)	-			c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communication cable 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.	Tamper Resistance Obtiscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/DS	(S	Same as on the Left) Same as on the Left)	Device Error Detect Device Alive Monit Log CollectionLog. Surveillance Came Intrusion Detection Device Error Detection Device Error Detection Understellang Manageme Device Error DetectionLog Device Error DetectionLog Device Error DetectionLog Device Error Detection Device Error Device Er	tion pring Analysis Analysis Sensor tion pring Analysis Sensor tion pring Analysis Int System to System tion pring Analysis Analysis Ition pring Analysis	R	Redundancy		
	Not applicable (no fu	nctions)	-			c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communication cable 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.	Tamper Resistance Othuscation Zeroization Entrance and Exit Management Lock and Key management W(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 Error Detect Device Alive Monit Log CollectionLog. Surveillance Came Intrusion Detection Device Error Detection Device Error Detection Understellang Manageme Device Error DetectionLog Device Error DetectionLog Device Error DetectionLog Device Error Detection Device Error Device Er	tion pring Analysis Analysis Sensor tion pring Analysis Sensor tion pring Analysis Int System to System tion pring Analysis Analysis Ition pring Analysis	R	Redundancy		
	Not applicable (no fur	nctions)	-			c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communication cable 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.	Tamper Resistance Obtiscation 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		Same as on the Left) Same as on the Left)	Device Error Detect Device Alive Monit Log CollectionLog. Surveillance Came Intrusion Detection Device Error Detection Device Error Detection Understellang Manageme Device Error DetectionLog Device Error DetectionLog Device Error DetectionLog Device Error Detection Device Error Device Er	tion pring Analysis Analysis Sensor tion pring Analysis Sensor tion pring Analysis Int System to System tion pring Analysis Analysis Ition pring Analysis	R	Redundancy		
	Not applicable (no fu	nctions)	-			c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communication cable 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.	Tamper Resistance Othuscation Zeroization Entrance and Exit Management Lock and Key management W(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 Error Detect Device Alive Monit Log CollectionLog. Surveillance Came Intrusion Detection Device Error Detection Device Error Detection Understellang Manageme Device Error DetectionLog Device Error DetectionLog Device Error DetectionLog Device Error Detection Device Error Device Er	tion pring Analysis Analysis Sensor tion pring Analysis Sensor tion pring Analysis Int System to System tion pring Analysis Analysis Ition pring Analysis	R	Redundancy		
	Not applicable (no fu	nctions)	-			c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communication cable 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.	Tamper Resistance Obtuscation Zeroization Ertrance 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 Data Encryption		Same as on the Left) Same as on the Left)	Device Error Detect Device Alive Monit Log CollectionLog. Surveillance Came Intrusion Detection Device Error Detection Device Error Detection Understellang Manageme Device Error DetectionLog Device Error DetectionLog Device Error DetectionLog Device Error Detection Device Error Device Er	tion pring Analysis Analysis Sensor tion pring Analysis Sensor tion pring Analysis Int System to System tion pring Analysis Analysis Ition pring Analysis	R	Redundancy		
	Not applicable (no fu	nctions)	-			c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communication cable 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.	Tamper Resistance Obtuscation Zeroization Ertrance 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 Data Encryption		Same as on the Left) Same as on the Left)	Device Error Detect Device Alive Monit Log CollectionLog. Surveillance Came Intrusion Detection Device Error Detection Device Error Detection Understellang Manageme Device Error DetectionLog Device Error DetectionLog Device Error DetectionLog Device Error Detection Device Error Device Er	tion oring Analysis ra Sensor tion oring Analysis rit System tion oring Analysis rit System tion oring Analysis rit System	R	Redundancy		
	Not applicable (no fu	nctions)	-			c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Tamper Resistance Odfuscation Zeroization Ercitance and Exit Management Lock and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/IDS DDoS Countermeasures DDoS Countermeasures Encryption of Communications Channels Data Encryption Exclusive Line		Same as on the Left) Same as on the Left)	Device Error Detec Device Aive Monito Log Collection Log , Integrate Log Manageme Intrusion Detection Device Error Detection Device Aive Monito Log Collection Log , Integrated Log Manageme Device Aive Monito Log Collection Log , Integrated Log Manageme Integrated Log Manageme	tion and states and st	R	Redundancy		
	Not applicable (no fu	nctions)	-			c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Tamper Resistance Obtuscation 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 DDoS Countermeasures Encryption of Communications Channels		Same as on the Left) Same as on the Left)	Device Error Detect Device Alve Monit Log Collection/Log Integrate Log Manageme Surveillance Camer Intrusion Detection Device Error Detect Device Alve Monit Log Collection/Log Device Error Detect Device Alve Monit Log Collection/Log Integrated Log Manageme	tion and states and st	R	Redundancy		
	Not applicable (no fur	nctions)	-			c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Tamper Resistance Odfuscation Zerroization Entrance and Exit Management Lock and Key management PW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/IDS DDoS Countermeasures Encryption of Communications Channels Data Encryption of Communications Channels Encryption of Communications Channels Data Sgnature		Same as on the Left) Same as on the Left)	Device Error Detect Device Alve Monit Log Collection/Log Integrate Log Manageme Surveillance Camer Intrusion Detection Device Error Detect Device Alve Monit Log Collection/Log Device Error Detect Device Alve Monit Log Collection/Log Integrated Log Manageme	tion and states and st	R	Redundancy		
	Not applicable (no fu	nctions)	-			c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communication cable 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.	Tamper Resistance Odfuscation Zerroization Entrance and Exit Management Lock and Key management PW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/IDS DDoS Countermeasures Encryption of Communications Channels Data Encryption of Communications Channels Encryption of Communications Channels Data Sgnature		Same as on the Left) Same as on the Left)	Device Error Detect Device Alve Monit Log Collection/Log Integrate Log Manageme Surveillance Camer Intrusion Detection Device Error Detect Device Alve Monit Log Collection/Log Device Error Detect Device Alve Monit Log Collection/Log Integrated Log Manageme	tion oring Analysis et System orige orige or System orige orige or System orige origination orige or	R	Redundancy		
	Not applicable (no fu	nctions)	-			c	Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of Communication Data	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Tamper Resistance         Obtuscation         Zeroization         Entrance and Exit Management         Lock and Key management         PW (Packet Filtering Type)         FW (Application Gateway Type)         PS/DS         DDoS Countermeasures         Encryption of Communications Channels         Data Encryption         Encryption of Communications Channels         Data Signature         Enclysive Line		Same as on the Left) Same as on the Left)	Device Error Detect Device Alive Monite Log Collection/Log Integrated Log Manageme Surveillance Camer Intrusion Detection Device Alive Monite Log Collection/Log Unitegrated Log Manageme Device Error Detect Device Error Detect Device Alive Monite Log Collection/Log Integrated Log Manageme Log Collection/Log Integrated Log Manageme	tion and the set of th	R	Redundancy		

Contro	pe of Assets	Target Device		essment Me			Threat (Attack Type)	Description		tection			Detection/Understanding Dar	mage	Business Continuity	
Contro			Threat Level	Vulnerability Level	Importance of Assets	Risk Value			Intrusion/Spreading Phase		Objective Achievement Pha	ase		age	Duarioss Continully	
Contro	ol System Asset	HMI (Operator Terminal)					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							
			2	2		в			WAF							
			-	-		-			Peer-to-Peer Authentication	0						
									IPS/IDS							
									Applying Patches							
									Avoidance of Vulnerability							
4					1											
							Physical Intrusion	Unauthorized access of sections/areas (device installation locations,	Entrance and Exit Management (IC Card)	0			Surveillance Camera	0		
						в		etc.) with access restrictions. It also refers to removing restrictions on devices with physical	Lock and Key Management	Ŭ			Intrusion Detection Sensor	Ŭ		
			2	2		P		access restrictions (devices installed in racks, cabinets, etc.).								
1					1	<u> </u>	Unauthorized Operation	Intrusion through direct operation of the device's console or other	Operator Authentication	-						
			2	3		A		component to execute an attack.								
1					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							
			2	3		A		device).								
								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)			
			3	3		A	Media or Device	device, etc.) brought in from outside the organization with the					Log Collection/Log Analysis			
			l °	- <b>-</b>				device to execute an attack.					Integrated Log Management System			
4					4	L	-		D	1	0					
1			1					Unauthorized execution of legitimate programs, commands,	Permission Management	1	(Same as on the Left)		Device Error Detection			
1			l .			.	Processes	services, and other processes found on the attack target	Access Control	1	(Same as on the Left)		Device Alive Monitoring			
			3	3		A		device.	Application Whitelisting	-	(Same as on the Left)		Log Collection/Log Analysis			
									Approval of Important Operations	1	(Same as on the Left)		Integrated Log Management System			
			<b>—</b>		-	L			Artivirus	1			Davias Free David			
							Malware Infection		Anti-virus Annlication Whitelisting	-		-	Device Error Detection Device Alive Monitoring			
								the attack target device.	Application Whitelisting	-			*			
			3	3		A			Applying Patches	-			Log Collection/Log Analysis			
			1	-					Avoidance of Vulnerability	-			Integrated Log Management System			
									Data Signature	-						
			<b>—</b>		-	L	Information Th 10	The first section (a first section for the sec	Permission Management	-	(Same as on the Loff)		I on Collection/Lon Applysia			
							Information Theft	Theft of information (software, authentication information,	Permission Management Access Control	1	(Same as on the Left) (Same as on the Left)		Log Collection/Log Analysis Integrated Log Management System			
						l .		configuration settings, encryption keys and other confidential	Data Encryption	-	(Same as on the Left)		integrated Eog Management System			
			3	3		A		information) stored on the device.	DLP	-						
									DLP	-	(Same as on the Left)					
					-		Line destined Madification of		Permission Management	-	(Same as on the Left)		Device Error Detection		Data Backup	
								f Unauthorized modification of information (software,	A O I I		(Same as on the Left)		Log Collection/Log Analysis		Data Dackup	
			3	3		A	Information	authentication information, configuration settings, encryption	Data O's sat as	-	(Same as on the Left)		Integrated Log Management System			
								keys and other confidential information) stored on the device.	Data Signature	-	(Same as on the Left)		incgrated cog management oystem			
					-		Information Destruction	Destroying of information (a offware, outbantication		-	Permission Management		Device Error Detection		Data Backup	
							Information Destruction	Destroying of information (software, authentication information, configuration settings, encryption keys and other			Access Control		Log Collection/Log Analysis			
			3	3		A				-			Integrated Log Management System			
								confidential information) stored on the device.								
1					1		I Inauthorized Transmission	Sending unauthorized control commands (settings changes,	Segmentation/Zoning	-	(Same as on the Left)		Log Collection/Log Analysis			
					3			power shutdowns, etc.) and unauthorized data to other	Data Signature		(Same as on the Left)		Integrated Log Management System			
			3	3		A		devices.	Approval of Important Operations		(Same as on the Left)					
					1		Outage	Stopping device functions.					Device Error Detection		Redundancy	
1					1								Device Alive Monitoring		Failsafe Design	
					1					1			Log Collection/Log Analysis			
			3	3		A							Integrated Log Management System			
			3	3		A										
			3	3												
			3	3	-		DoS Attack	Interruption of regular device operations by sending	DDoS Countermeasures				Device Error Detection		Redundancy	
					-		DoS Attack	processing requests that exceed the processing capacity of	DDoS Countermeasures				Device Alive Monitoring		Redundancy Failsafe Design	
-			3	3	-		DoS Attack		DDoS Countermeasures				Device Alive Monitoring Log Collection/Log Analysis			
-					-		DoS Attack	processing requests that exceed the processing capacity of	DDoS Countermeasures				Device Alive Monitoring			
-					-			processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.					Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System			
-			1	3	-	в	DoS Attack	processing requests that exceed the processing capacity of	DDoS Countermeasures	0	(Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis			
					-			processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.		0	(Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System			
			1	3	-	в	Theft	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft.	Lock and Key Management	0			Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System			
-			1	3	-	в	Theft Information Theft by	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information,	Lock and Key Management Tamper Resistance	0	(Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System			
			1	3	-	B	Theft Information Theft by Tampering Device at Time	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential	Lock and Key Management Tamper Resistance Obfuscation	0 0	(Same as on the Left) (Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System			
			1	3	-	B	Theft Information Theft by	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information,	Lock and Key Management Tamper Resistance Obfuscation	0 0	(Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Failsafe Design	
			1	3	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Lock and Key Management Tamper Resistance Obfuscation	0 0	(Same as on the Left) (Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System			
			1	3	-	B	Theft Information Theft by Tampering Device at Time	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassemided. Communications are blocked by disconnecting the	Lock and Key Management Tamper Resistance Obfuscation Zeroization	0 0	(Same as on the Left) (Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left)		Failsafe Design	
			1	3	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management	0 0 0	(Same as on the Left) (Same as on the Left)		Device Error Detection		Failsafe Design	
			1	3	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management	0	(Same as on the Left) (Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring		Failsafe Design	
			1	3	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management	0 0	(Same as on the Left) (Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis Hegrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis		Failsafe Design	
			1	3	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management	0 0 0 0	(Same as on the Left) (Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis inequated Log Management System (Same as on the Left) Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Failsafe Design	
			1	3	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management	0 0 0 0 0 0	(Same as on the Left) (Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera		Failsafe Design	
			1	3	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable.	Lock and Key Management Tamper Resistance Obliscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type)	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	(Same as on the Left) (Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera		Failsafe Design	
			1	3	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management 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 Management System (Same as on the Left) Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor		Failsafe Design	
			1	3	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encyption 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.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management 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 (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Intrusion Detection Sensor Device Error Detection Device Error Detection Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis		Failsafe Design	
			1	3	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encyption 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.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type)	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	(Same as on the Left) (Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis inequated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Error Detection Device Alive Monitoring		Failsafe Design	
			1	3	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encyption 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.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management 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 (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Intrusion Detection Sensor Device Error Detection Device Error Detection Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis		Failsafe Design	
			1	3	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encyption 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.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF FPS/IDS		(Same as on the Left) (Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Intrusion Detection Sensor Device Error Detection Device Error Detection Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis		Failsafe Design	
			1	3		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encyption 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.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF FPS/IDS		(Same as on the Left) (Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Intrusion Detection Sensor Device Error Detection Device Error Detection Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	Image: Constraint of the sector of	Redundancy	
Nota	upplicable (no fun	ctions)	1	3		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF FPS/IDS		(Same as on the Left) (Same as on the Left)		Device Error Detection Survival Management System Intrusion Detection Device Error Detection Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Intrusion Detection Sensor Device Camera Device Error Detection Device Alive Monitoring Device Alive Monitoring Device Ling Management System Intrusion Detection Sensor	Image: Constraint of the sector of	Failsafe Design	
Nota	upplicable (no fun	ctions)	1	3	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF FPS/IDS		(Same as on the Left) (Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis Imegrated Log Management System Game as on the Left) Game as on the Left) Gevice Error Detection Device Alive Monitoring Log Collection/Log Analysis Intrusion Detection Device Camera Intrusion Detection Device Camera Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Alive Monitoring	Image: Constraint of the sector of	Redundancy	
Nota	upplicable (no fun	ctions)	1	3		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF FPS/IDS		(Same as on the Left) (Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) 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 Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	Image: Constraint of the sector of	Redundancy	
Nota	upplicable (no func	ctions)	1	3		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF FPS/IDS		(Same as on the Left) (Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis Imegrated Log Management System Game as on the Left) Game as on the Left) Gevice Error Detection Device Alive Monitoring Log Collection/Log Analysis Intrusion Detection Device Camera Intrusion Detection Device Camera Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Alive Monitoring	Image: Constraint of the sector of	Redundancy	
Nota	-pplicable (no fun	ctions)	1	3		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management Cock 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 (Same as on the Left) 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 Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	Image: Constraint of the sector of	Redundancy	
Nota	pplicable (no fun	ctions)	1	3	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PSrIDS 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 (Same as on the Left) 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 Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	Image: Constraint of the sector of	Redundancy	
Nota	spplicable (no fun	ctions)	1	3		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Lock and Key Management Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management Lock and Key management FW (Apolication Gateway Type) FW (Apolication Gateway Type) WAF PS/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 (Same as on the Left) 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 Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	Image: Constraint of the sector of	Redundancy	
Nota	spplicable (no fun	ctions)	1	3		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PSrIDS 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 (Same as on the Left) 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 Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Image: Constraint of the sector of	Redundancy	
Nota	upplicable (no fun	ctions)	1	3		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encyption keys and other confidential information) stored on devices which were stelen or disposed of and then disassembled. Communications are blocked by disconnecting the 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.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management Lock and Key management FW (Application Gateway 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 instruction (Same as on the Left)  Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Instruction Detection Device Alive Monitoring Log Collection/Log Analysis Instruction Detection Device Alive Monitoring 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 Integrated Log Management System	Image: Constraint of the sector of	Redundancy	
Nota	spplicable (no fun	ctions)	1	3		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Lock and Key Management Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management Lock and Key management Exit Management FW (Application Gateway Type) WAF PS/IDS DDoS Countermeasures DDoS 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 (Same as on the Left) 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 Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Image: Constraint of the sector of	Redundancy	
Nota	upplicable (no fun	ctions)	1	3		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encyption keys and other confidential information) stored on devices which were stelen or disposed of and then disassembled. Communications are blocked by disconnecting the 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.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management Lock and Key management FW (Application Gateway 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 instruction (Same as on the Left)  Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Instruction Detection Device Alive Monitoring Log Collection/Log Analysis Instruction Detection Device Alive Monitoring 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 Integrated Log Management System	Image: Constraint of the sector of	Redundancy	
Nota	-pplicable (no fun	ctions)	1	3		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encyption keys and other confidential information) stored on devices which were stelen or disposed of and then disassembled. Communications are blocked by disconnecting the 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.	Lock and Key Management Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management Lock and Key management Exit Management FW (Application Gateway Type) WAF PS/IDS DDoS Countermeasures DDoS 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 Imegrated Log Management System Gamma as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Intrusion Detection Device Alive Monitoring Device Error Detection Device Alive Monitoring Device Alive Monitoring Device Alive Monitoring Device Error Detection Device Alive Monitoring Device Error Detection Device Error Detection Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Image: Constraint of the sector of	Redundancy	
Nota		ctions)	1	3		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encyption keys and other confidential information) stored on devices which were stelen or disposed of and then disassembled. Communications are blocked by disconnecting the 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.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF FPS/IDS DDoS Countermeasures Encryption of Communications Channels Data Encryption of Communications Channels Encryption of Communications Channels Encryption of Communications Channels Encryption of Communications Channels Data Signature		(Same as on the Left) (Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis Imegrated Log Management System Gamma as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Intrusion Detection Device Alive Monitoring Device Error Detection Device Alive Monitoring Device Alive Monitoring Device Alive Monitoring Device Error Detection Device Alive Monitoring Device Error Detection Device Error Detection Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Image: Constraint of the sector of	Redundancy	
Nota	spplicable (no fun	ctions)	1	3		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of Communication Data	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Lock and Key Management Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management Lock and Key management Exclusive Line Encryption of Communications Channels Data Signature Exclusive Line E		(Same as on the Left) (Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis Imegrated Log Management System Gamma as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Intrusion Detection Device Alive Monitoring Device Error Detection Device Alive Monitoring Device Alive Monitoring Device Alive Monitoring Device Error Detection Device Alive Monitoring Device Error Detection Device Error Detection Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Image: Constraint of the sector of	Redundancy	
Nota	spplicable (no fun	ctions)	1	3		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of Communication Data Connecting Unauthorized	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encyption keys and other confidential information) stored on devices which were stelen or disposed of and then disassembled. Communications are blocked by disconnecting the 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.	Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF FPS/IDS DDoS Countermeasures Encryption of Communications Channels Data Encryption of Communications Channels Encryption of Communications Channels Encryption of Communications Channels Encryption of Communications Channels Data Signature		(Same as on the Left) (Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis Megrated Log Management System Gamma Source System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Megrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Megrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Megrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Megrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Megrated Log Management System Device Alive Monitoring Log Collection/Log Analysis Metry and Log Management System Device Alive Monitoring Log Collection/Log Analysis Metry and Log Management System Device Alive Monitoring Log Collection/Log Analysis Metry and Log Management System Device Alive Adminent System Device Adminent System D	Image: Constraint of the sector of	Redundancy	
Nota	pplicable (no fun	ctions)	1	3		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of Communication Data	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Lock and Key Management Lock and Key Management Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management Lock and Key management Exclusive Line Encryption of Communications Channels Data Signature Exclusive Line E		(Same as on the Left) (Same as on the Left)		Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Intrusion Detection Gensor Device Error Detection Device Error Detection Device Error Detection Device Error Detection Device Error Detection Device Alive Monitoring Device Error Detection Device Alive Monitoring Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	Image: Constraint of the sector of	Redundancy	

+	Type of Assets	Target Device	Ass			Threat (Attack Type	Description	Protect	tion	measures	-		
			Threat Level	Vulnerability Level	Importance of Assets			Intrusion/Spreading Phase	Objective Achievement Ph	Detection/Understanding I	Damage	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	s		
L								One-way Gateway		Integrated Log Management System			
L.								Proxy Server			-		
ι.								WAF			-		
								Peer-to-Peer Authentication			_		
L								IPS/IDS			_		
											+		
L								Applying Patches			_		
ι.								Avoidance of Vulnerability			_		
-					4 - 1			Enternance and Evit Management		Current Company	_		
						Physical Intrusion	Unauthorized access of sections/areas (device installation locations,			Surveillance Camera	-		
							etc.) with access restrictions. It also refers to removing restrictions on devices with physical	Lock and Key Management		Intrusion Detection Sensor	_		
							access restrictions (devices installed in racks, cabinets, etc.).						
							access restrictions (devices installed in racks, cabinets, etc.).						
-					4 1	Use the fact of Osciety	Intrusion through direct operation of the device's concele or other	Operator Authentication			_		
ι.						Unauthorized Operation	Intrusion through direct operation of the device's console or other component to execute an attack.	Operator Admenication			_		
					1 1	Human Error in Operati		URL Filtering/Web Reputation			_		
								Mail Filtering					
ι.							device).				-		
ι.							An act equivalent to an attack is performed on the device as a result				-		
L.							of a proper media or device connection.				-		
-					4 1			Destriction on Connection Device and its Users	(Same as on the Left)	Restriction on Connecting Device and its Usage	_		
ι.						Connecting Unauthorize			(Same as on the Leit)	Log Collection/Log Analysis	_		
ι.						Media or Device	device, etc.) brought in from outside the organization with the						
ι.							device to execute an attack.			Integrated Log Management System			
-					4 1						_		
L								Permission Management	(Same as on the Left)	Device Error Detection	-		
L					I	Processes	services, and other processes found on the attack target	Access Control	(Same as on the Left)	Device Alive Monitoring	-		
L							device.	Application Whitelisting	(Same as on the Left)	Log Collection/Log Analysis			
1								Approval of Important Operations	(Same as on the Left)	Integrated Log Management System			
1					1 L								
E					I [	Malware Infection	Infection or running of malware (unauthorized programs) on	Anti-virus		Device Error Detection			
L							the attack target device.	Application Whitelisting		Device Alive Monitoring			
E								Applying Patches		Log Collection/Log Analysis			
1								Avoidance of Vulnerability		Integrated Log Management System			
1					I			Data Signature					
1													
1					ן ן	Information Theft	Theft of information (software, authentication information,	Permission Management	(Same as on the Left)	Log Collection/Log Analysis	S		
1							configuration settings, encryption keys and other confidential	Access Control	(Same as on the Left)	Integrated Log Management System			
L							information) stored on the device.	Data Encryption	(Same as on the Left)				
L							information) stored on the device.	DLP	(Same as on the Left)				
L									(		-		
					1 1	Linauthorized Modificati	n of Unauthorized modification of information (software,	Permission Management	(Same as on the Left)	Device Error Detection	-	Data Backup	
L						Information		Access Control	(Same as on the Left)	Log Collection/Log Analysis			
ι.						information			(Same as on the Left)	Integrated Log Management System			
L							keys and other confidential information) stored on the device.	Data Olgi latti e	(Game as on the cert)	integrated bog management of stern	-		
E													
ł					4 H	Information Destruction	Destroying of information (or finance of the stington)		Permission Management	Device Error Detection		Data Backup	
ι.						Information Destruction	Destroying of information (software, authentication		Access Control	Log Collection/Log Analysis	_	Data Backup	
ι.							information, configuration settings, encryption keys and other		Access Control	Integrated Log Management System			
ι.							confidential information) stored on the device.			integrated Log Management System	_		
					4 1		· · · · · · · · · · ·				_		
ι.					3	Unauthorized Transmis	ion Sending unauthorized control commands (settings changes,		(Same as on the Left)	Log Collection/Log Analysis Integrated Log Management System	5		
ι.							power shutdowns, etc.) and unauthorized data to other	Data Signature	(Same as on the Left)	Integrated Log Management System	-		
ι.							devices.	Approval of Important Operations	(Same as on the Left)		_		
					4					Device Error Detection	_		
						Outage	Stopping device functions.			Device Alive Monitoring	_	Redundancy	
											_	Failsafe Design	
L										Log Collection/Log Analysis			
L													
										Integrated Log Management System			
						DoS Attack	Interruption of regular device operations by sending	DDoS Countermeasures		Device Error Detection		Redundancy	
						DoS Attack	Interruption of regular device operations by sending processing requests that exceed the processing capacity of	DDoS Countermeasures				Redundancy Failsafe Design	
						DoS Attack		DDoS Countermeasures		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	5		
						DoS Attack	processing requests that exceed the processing capacity of	DDoS Countermeasures		Device Error Detection Device Alive Monitoring	5		
						DoS Attack	processing requests that exceed the processing capacity of	DDoS Countermeasures		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	5		
-						DoS Attack	processing requests that exceed the processing capacity of	DDoS Countermeasures	<ul> <li>(Same as on the Left)</li> </ul>	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	5		
-							processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.		<ul> <li>(Same as on the Left)</li> </ul>	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	5		
							processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.		<ul> <li>(Same as on the Left)</li> </ul>	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	5		
							processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.		<ul> <li>(Same as on the Left)</li> <li>(Same as on the Left)</li> </ul>	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	5		
						Theft	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential	Lock and Key Management Tamper Resistance Obfuscation	(Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	5		
						Theft Information Theft by	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of	Lock and Key Management Tamper Resistance Obfuscation	(Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	5		
-						Theft Information Theft by Tampering Device at Ti	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential	Lock and Key Management Tamper Resistance Obfuscation	(Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	5	Failsafe Design	
						Theft Information Theft by Tampering Device at Ti	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of	Lock and Key Management Lock and Key Management Tamper Resistance Obfuscation Zeroization Ensues and Eit Wagenet (Clock Bonetic Addenticate)	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left)	5		
						Theft Information Theft by Tampering Device at Ti of Theft or Disposal	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, the configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Lock and Key Management Tamper Resistance Obfuscation Zeroization	(Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection(Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring	S	Failsafe Design	
						Theft Information Theft by Tampering Device at Ti of Theft or Disposal Route Blocking	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the	Lock and Key Management Lock and Key Management Tamper Resistance Obfuscation Zeroization Ensues and Eit Wagenet (Clock Bonetic Addenticate)	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Megrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	5	Failsafe Design	
			3	2		Theft Information Theft by Tampering Device at Ti of Theft or Disposal	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information,     configuration settings, encryption keys and other confidential     information) stored on devices which were stolen or disposed of and     then disassembled.     Communications are blocked by disconnecting the     communication cable.	Lock and Key Management Lock and Key Management Tamper Resistance Obfuscation Zeroization Ensues and Eit Wagenet (Clock Bonetic Addenticate)	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection(Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring	5	Failsafe Design	
			3	2		Theft Information Theft by Tampering Device at Ti of Theft or Disposal Route Blocking	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information, the configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.     Communications cable.     Alternatively, communications are blocked by pulling out the	Lock and Key Management Lock and Key Management Tamper Resistance Obfuscation Zeroization Ensues and Eit Wagenet (Clock Bonetic Addenticate)	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Megrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	5	Failsafe Design	
			3	2		Theft Information Theft by Tampering Device at Ti of Theft or Disposal Route Blocking	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information, the configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.     Communications cable.     Alternatively, communications are blocked by pulling out the	Lock and Key Management Lock and Key Management Tamper Resistance Obfuscation Zeroization Ensues and Eit Wagenet (Clock Bonetic Addenticate)	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		Failsafe Design	
			3	2		Theft Information Theft by Tampering Device at Ti of Theft or Disposal Route Blocking	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information, the configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.     Communications cable.     Alternatively, communications are blocked by pulling out the	Lock and Key Management Lock and Key Management Tamper Resistance Obfuscation Zeroization Ensues and Eit Wagenet (Clock Bonetic Addenticate)	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection(Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection(Log Analysis Integrated Log Management System Surveillance Camera		Failsafe Design	
			3	2		Theft Information Theft by Tampering Device at Ti of Theft or Disposal Route Blocking	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information,     configuration settings, encryption keys and other confidential     information joted on devices which were stolen or disposed of and     then diassembled.     Communications are blocked by disconnecting the     communication cable.     Alternatively, communications are blocked by pulling out the     communication cable from the device.	Lock and Key Management  Tamper Resistance Obfuscation Zeroization Entrace and Key management Lock and Key management	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection(Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Error Detection Device Alive Monitoring Log Collection(Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor		Fallsafe Design	
			3	2		Theft Information Theft by Tampering Device at Ti of Theft or Disposal Route Blocking	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information, organization) settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then diassembled.     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	Lock and Key Management  Tamper Resistance Obfuscation Zeroization Entrace and Ent Meagement (C Carl, Bondra Admeticator) Lock and Key management  FW (Packet Filtering Type)	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Error Detection		Failsafe Design	
						Theft Information Theft by Tampering Device at Tr of Theft or Disposal Route Blocking Network Congestion	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information,     configuration settings, encryption keys and other confidential     information joted on devices which were stolen or disposed of and     then diassembled.     Communications are blocked by disconnecting the     communication cable.     Alternatively, communications are blocked by pulling out the     communication cable from the device.	Lock and Key Management Tamper Resistance Obtuscation Zeroization Ecroization Lock and Key management For Cast tends Attention For (Packet Filtering Type) FW (Application Gateway Type)	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Error Detection Device Error Detection Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring	5 5 5 5 5	Fallsafe Design	
			3	2		Theft Information Theft by Tampering Device at Ti of Theft or Disposal Route Blocking	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information, organization) settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then diassembled.     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	Lock and Key Management  Tamper Resistance Obfuscation Zeroization Entering Tot Margament (C Carl, Bonets Antendator, Lock and Key management  FW (Packet Filtering Type) FW (Application Gateway Type) WAF	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection(Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection(Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Error Detection Device Error Detection Device Alive Monitoring Log Collection(Log Analysis	5	Fallsafe Design	
						Theft Information Theft by Tampering Device at Tr of Theft or Disposal Route Blocking Network Congestion	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information, organization settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then diassembled.     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	Lock and Key Management Lock and Key Management Tamper Resistance Obfuscation Zeroization Exercise and Ext Meagement (C.Carl, Breats Antendard Exercise and Ext Meagement (C.Carl, Breats Antendard) Exercise and Ext Meagement (C.Carl, Breats Antendard) Exercise antendard Exercise antendard Exercise antendard Exercise antendard) Exercise antendard Exercise a	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Error Detection Device Error Detection Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Alive Monitoring	5	Fallsafe Design	
						Theft Information Theft by Tampering Device at Tr of Theft or Disposal Route Blocking Network Congestion	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information, organization settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then diassembled.     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	Lock and Key Management  Tamper Resistance Obfuscation Zeroization Entering Tot Margament (C Carl, Bonets Antendator, Lock and Key management  FW (Packet Filtering Type) FW (Application Gateway Type) WAF	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection(Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection(Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Error Detection Device Error Detection Device Alive Monitoring Log Collection(Log Analysis	5	Fallsafe Design	
						Theft Theft Information Theft by Tampering Device at Ta of Theft or Disposal Route Blocking A Network Congestion A	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information,     configuration settings, encryption keys and other confidential     information) stored on devices which were stolen or disposed of and     then disassembled.     Communications cable.     Alternatively, communications are blocked by guiling 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.	Lock and Key Management Lock and Key Management Tamper Resistance Obfuscation Zeroization Exercise and Ext Meagement (C.Carl, Breats Antendard Exercise and Ext Meagement (C.Carl, Breats Antendard) Exercise and Ext Meagement (C.Carl, Breats Antendard) Exercise antendard Exercise antendard Exercise antendard Exercise antendard) Exercise antendard Exercise a	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Error	5	Failsafe Design	
(	Not applicable (confi	netionsl				Theft Information Theft by Tampering Device at Tr of Theft or Disposal Route Blocking Network Congestion	processing requests that exceed the processing capacity of the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information, organization settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then diassembled.     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	Lock and Key Management Lock and Key Management Tamper Resistance Obfuscation Zeroization Exercise and Ext Meagement (C.Carl, Breats Antendard Exercise and Ext Meagement (C.Carl, Breats Antendard) Exercise and Ext Meagement (C.Carl, Breats Antendard) Exercise antendard Exercise antendard Exercise antendard Exercise antendard) Exercise antendard Exercise a	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection 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 Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection	5	Fallsafe Design	
	Not applicable (no fu	.nctions)				Theft Theft Information Theft by Tampering Device at Ta of Theft or Disposal Route Blocking A Network Congestion A	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information,     configuration settings, encryption keys and other confidential     information) stored on devices which were stolen or disposed of and     then disassembled.     Communications cable.     Alternatively, communications are blocked by guiling 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.	Lock and Key Management Lock and Key Management Tamper Resistance Obfuscation Zeroization Exercise and Ext Meagement (C.Carl, Breats Antendard Exercise and Ext Meagement (C.Carl, Breats Antendard) Exercise and Ext Meagement (C.Carl, Breats Antendard) Exercise antendard Exercise antendard Exercise antendard Exercise antendard) Exercise antendard Exercise a	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection 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 Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Error Detec	5 5 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	Failsafe Design	
	Not applicable (no fu	unctions)				Theft Theft Information Theft by Tampering Device at Ta of Theft or Disposal Route Blocking A Network Congestion A	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information,     configuration settings, encryption keys and other confidential     information) stored on devices which were stolen or disposed of and     then disassembled.     Communications cable.     Alternatively, communications are blocked by guiling 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.	Lock and Key Management Lock and Key Management Tamper Resistance Obfuscation Zeroization Exercise and Ext Meagement (C.Carl, Breats Antendard Exercise and Ext Meagement (C.Carl, Breats Antendard) Exercise and Ext Meagement (C.Carl, Breats Antendard) Exercise antendard Exercise antendard Exercise antendard Exercise antendard) Exercise antendard Exercise a	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection 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 Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection	5 5 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	Failsafe Design	
	Not applicable (no fu	.nctions)				Theft Theft Information Theft by Tampering Device at Ta of Theft or Disposal Route Blocking A Network Congestion A	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information,     configuration settings, encryption keys and other confidential     information) stored on devices which were stolen or disposed of and     then disassembled.     Communications cable.     Alternatively, communications are blocked by guiling 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.	Lock and Key Management Lock and Key Management Tamper Resistance Obfuscation Zeroization Exercise and Ext Meagement (C.Carl, Breats Antendard Exercise and Ext Meagement (C.Carl, Breats Antendard) Exercise and Ext Meagement (C.Carl, Breats Antendard) Exercise antendard Exercise antendard Exercise antendard Exercise antendard) Exercise antendard Exercise a	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Surveillance Camera Intrusion Detection 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 Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Error Detec		Failsafe Design	
	Not applicable (no fu	inctions)				Theft Theft Information Theft by Tampering Device at Ta of Theft or Disposal Route Blocking A Network Congestion A	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information,     configuration settings, encryption keys and other confidential     information) stored on devices which were stolen or disposed of and     then disassembled.     Communications cable.     Alternatively, communications are blocked by guiling 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.	Lock and Key Management Lock and Key Management Tamper Resistance Obfuscation Zeroization Exercise and Ext Meagement (C.Carl, Breats Antendard Exercise and Ext Meagement (C.Carl, Breats Antendard) Exercise and Ext Meagement (C.Carl, Breats Antendard) Exercise antendard Exercise antendard Exercise antendard Exercise antendard) Exercise antendard Exercise a	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis		Failsafe Design	
	Not applicable (no fu	nctions)				Theft     Information Theft by     Tampering Device at Ta     of Theft or Disposal     Route Blocking     A     Network Congestion     Jamming	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information,     ordiguration 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.     Causing congestion by generating the communications traffic     that exceeds the capacity of the device.     Interference with radio communications.	Lock and Key Management  Tamper Resistance Obfuscation Zeroization Extract and Key management Extract and Key management Extract and Key management EXT (Application Gateway Type) FW (Application Gateway Type) WAF PS/IDS DDoS Countermeasures	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis		Failsafe Design	
	Not applicable (no fu	inctions)	2	3		Theft     Information Theft by     Tampering Device at Ta     of Theft or Disposal     Route Blocking     Network Congestion     Jamming     Jamming     Packet Sniffing	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information,     configuration settings, encryption keys and other confidential     information) stored on devices which were stolen or disposed of and     then disassembled.     Communications cable.     Alternatively, communications are blocked by guiling 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.	Lock and Key Management  Tamper Resistance Obfuscation  Zeroization  Exercization  Exercization  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) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis		Failsafe Design	
	Not applicable (no fu	nctions)				Theft     Information Theft by     Tampering Device at Ta     of Theft or Disposal     Route Blocking     A     Network Congestion     Jamming	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information,     ordiguration 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.     Causing congestion by generating the communications traffic     that exceeds the capacity of the device.     Interference with radio communications.	Lock and Key Management         Image: Control of Contro	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis		Failsafe Design	
	Not applicable (no fu	nctions)	2	3		Theft     Information Theft by     Tampering Device at Ta     of Theft or Disposal     Route Blocking     Network Congestion     Jamming     Jamming     Packet Sniffing	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information,     ordiguration 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.     Causing congestion by generating the communications traffic     that exceeds the capacity of the device.     Interference with radio communications.	Lock and Key Management  Tamper Resistance Obfuscation  Zeroization  Exercization  Exercization  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) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis		Failsafe Design	
	Not applicable (no fu	nctions)	2	3		Theft     Information Theft by     Tampering Device at Ta     of Theft or Disposal     Route Blocking     Network Congestion     A     Jamming     Jamming     Packet Sniffing     A	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information,     configuration settings, encryption keys and other confidential     information taxed on devices with were stolen or deposed of and     then disassembled.     Communications are blocked by disconnecting the     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.	Lock and Key Management           Tamper Resistance           Obfuscation           Zeroization           Zeroization           Elexication Elexity           Lock and Key management           Lock and Key management           FW (Packet Filtering Type)           FW (Application Gateway Type)           PS/IDS           DDoS Countermeasures           Encryption of Communications Channels           Data Encryption           Exclusive Line	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection 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 Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	S	Failsafe Design	
(	Not applicable (no fu	inctions)	2	3		Theft     Information Theft by     Tampering Device at Ta     of Theft or Disposal     Route Blocking     A     Network Congestion     Jamming     Jamming     Dacket Sniffing     Unauthorized Modificati	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information,     ordiguration 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.     Causing congestion by generating the communications traffic     that exceeds the capacity of the device.     Interference with radio communications.	Lock and Key Management  Tamper Resistance Obfuscation Zeroization  Enclose and Key management  Lock and Key management  Finance and Key manag	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) 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 Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System 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 Lo	S C C C C C C C C C C C C C C C C C C C	Failsafe Design	
	Not applicable (no fu	.nctions)	2	3		Theft     Information Theft by     Tampering Device at Ta     of Theft or Disposal     Route Blocking     A     Network Congestion     A     Jamming     Jamming     Packet Sniffing     A     Unsuthorized Modificati     Communication Data	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information,     configuration settings, encryption keys and other confidential     information taxed on devices with were stolen or deposed of and     then disassembled.     Communications are blocked by disconnecting the     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.	Lock and Key Management           Tamper Resistance           Obfuscation           Zeroization           Zeroization           Elexication Elexity           Lock and Key management           Lock and Key management           FW (Packet Filtering Type)           FW (Application Gateway Type)           PS/IDS           DDoS Countermeasures           Encryption of Communications Channels           Data Encryption           Exclusive Line	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection 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 Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System	S C C C C C C C C C C C C C C C C C C C	Failsafe Design	
	Not applicable (no fu	inctions)	2	3		Theft     Information Theft by     Tampering Device at Ta     of Theft or Disposal     Route Blocking     A     Network Congestion     Jamming     Jamming     Dacket Sniffing     Unauthorized Modificati	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information,     configuration settings, encryption keys and other confidential     information taxed on devices with were stolen or deposed of and     then disassembled.     Communications are blocked by disconnecting the     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.	Lock and Key Management  Tamper Resistance Obfuscation Zeroization  Enclose and Key management  Lock and Key management  Finance and Key manag	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) 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 Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System 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 Lo	S C C C C C C C C C C C C C C C C C C C	Failsafe Design	
	Not applicable (no fu	incions)	2	3		Theft     Information Theft by     Tampering Device at Ta     of Theft or Disposal     Route Blocking     A     Network Congestion     A     Jamming     Jamming     Packet Sniffing     A     Unsuthorized Modificati     Communication Data	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.     Device theft.     Theft of information (software, authentication information,     configuration settings, encryption keys and other confidential     information taxed on devices with were stolen or deposed of and     then disassembled.     Communications are blocked by disconnecting the     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.		(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) 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 Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System 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 Lo	S C C C C C C C C C C C C C C C C C C C	Failsafe Design	
	Not applicable (no fu	.nctions)	2	3		Theft       Information Theft by Tampering Device at Ti of Theft or Disposal       Route Blocking       A       Jamming       Jamming       Packet Sniffing       A       Unauthorized Modification Data	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.      Device theft.      Theft of information (software, authentication information,     configuration satings, encryption keys and other confidential     information) stored on devices which were stolen or desposed of and     then deasembled.     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.	Lock and Key Management  Tamper Resistance Obfuscation Zeroization  Eroization  FW (Packet Filtering Type) FW (Application Gateway Type) FW (Application Gateway Type) FW (Application Gateway Type) FW (Application Gateway Type) Ext (Application Gateway Type) FS/IDS DDoS Countermeasures  Encryption of Communications Channels Data Encryption Encryption of Communications Channels Data Signature Exclusive Line	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) 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 Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System 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 Lo	S C C C C C C C C C C C C C C C C C C C	Failsafe Design	
	Not applicable (no fu	Inctions)	2	3		Theft       Information Theft by Tampering Device at Ti of Theft or Disposal       Route Blocking       A       Jamming       Jamming       Packet Sniffing       A       Communication Data       Connecting Unauthorize Device	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.      Device theft.      Theft of information (software, authentication information,     configuration satings, encryption keys and other confidential     information) stored on devices which were stolen or desposed of and     then deasembled.     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.		(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection     Device Alive Monitoring     Log Collection/Log Analysis     Integrated Log Management System     System     System     System     Device Error Detection     Device Error Detection     Device Alive Monitoring     Log Collection/Log Analysis     Integrated Log Management System     Device Error Detection     Devic		Failsafe Design	
	Not applicable (no fu	inctions)	2	3		Theft       Information Theft by Tampering Device at Ti of Theft or Disposal       Route Blocking       A       Jamming       Jamming       Packet Sniffing       A       Unauthorized Modification Data	processing requests that exceed the processing capacity of     the device as a result of a DDoS attack, etc.      Device theft.      Theft of information (software, authentication information,     configuration satings, encryption keys and other confidential     information) stored on devices which were stolen or desposed of and     then deasembled.     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.	Lock and Key Management  Tamper Resistance Obfuscation Zeroization  Eroization  FW (Packet Filtering Type) FW (Application Gateway Type) FW (Application Gateway Type) FW (Application Gateway Type) FW (Application Gateway Type) Exclusive Line Encryption of Communications Channels Data Encryption Encryption of Communications Channels Data Signature Exclusive Line	(Same as on the Left) (Same as on the Left) (Same as on the Left)	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Vitegrated Log Management System Log Collection/Log Analysis Vitegrated Log Management System	S	Failsafe Design	

ber	Type of Assets	Target Device	Ass	essment Me	etrics		Threat (Attack Type)	Description	Prote	ection	Counterme			D	_
	.,,,		Threat Level	Vulnerability Level	Importance of Assets	Risk Value			Intrusion/Spreading Phase		Dijective Achievement Phas	e Detection/Understanding Da	image	Business Continuity	
	Network Asset	Field Network					Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type)			IPS/IDS			
									FW (Application Gateway Type) One-way Gateway	+		Log Collection/Log Analysis Integrated Log Management System			<u> </u>
									Proxy Server	+		Integrated Log Management System	+		<u> </u>
									WAF				+ +		<u> </u>
									Peer-to-Peer Authentication						
									IPS/IDS						
									Applying Patches						
									Avoidance of Vulnerability						
					-		<b>D</b>	Unauthorized access of sections/areas (device installation locations,	Entrance and Evil Management			Current Commercia	+		<u> </u>
							Physical Intrusion	etc.) with access restrictions.	Lock and Key Management	+		Surveillance Camera Intrusion Detection Sensor	+		<u> </u>
								It also refers to removing restrictions on devices with physical							
								access restrictions (devices installed in racks, cabinets, etc.).							
					-		Unauthorized Operation	Intrusion through direct operation of the device's console or other	Operator Authentication	$\vdash$			+		<u> </u>
							Chautionzed Operation	component to execute an attack.							
					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	+			+		<u> </u>
								device). An act equivalent to an attack is performed on the device as a result		+			+		<u> </u>
								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	(Sar	me 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			
								device to execute an attack.				Integrated Log Management System	+		
					-		Execution of Lineuthorized	Unauthorized execution of legitimate programs, commands,	Permission Management	(Sar	me as on the Left)	Device Error Detection	++		_
							Processes	services, and other processes found on the attack target	Access Control		me as on the Left)	Device Alive Monitoring			
								device.	Application Whitelisting	(Sar	me as on the Left)	Log Collection/Log Analysis			
									Approval of Important Operations	(Sar	me as on the Left)	Integrated Log Management System	$\square$		
					- 1		M.1		Antivirus			Davias Error Datastica	$\vdash$		
							Malware Infection	Infection or running of malware (unauthorized programs) on the attack target device.	Anti-virus Application Whitelisting			Device Error Detection Device Alive Monitoring			
								uno attaon target device.	Applying Patches			Log Collection/Log Analysis			
									Avoidance of Vulnerability			Integrated Log Management System			
									Data Signature						
					-		Information The fi	The first state (a.f.	Permission Management	10	me as on the Loft)	Lon Collection Los Arely	+		
							Information Theft	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential	Permission Management Access Control		me as on the Left) me as on the Left)	Log Collection/Log Analysis Integrated Log Management System			
								configuration settings, encryption keys and other confidential information) stored on the device.	Data Encryption		me as on the Left)				
								state of the dense.	DLP		me as on the Left)				
								Unauthorized modification of information (software,	Permission Management		me as on the Left)	Device Error Detection		Data Backup	
							Information	authentication information, configuration settings, encryption	Access Control Data Signature		me as on the Left) me as on the Left)	Log Collection/Log Analysis Integrated Log Management System			
								keys and other confidential information) stored on the device.	Solo Signatoro	(Sar		integrates and interruption of Stelli			
					1		Information Destruction	Destroying of information (software, authentication			mission Management	Device Error Detection	D	Data Backup	
L								information, configuration settings, encryption keys and other		Acc	ess Control	Log Collection/Log Analysis			
1								confidential information) stored on the device.				Integrated Log Management System	$\vdash$		
ł					1		I Inauthorized Transmission	Sending unauthorized control commands (settings changes,	Segmentation/Zoning	(Sar	me as on the Left)	Log Collection/Log Analysis	++		
					3		Straution2eu Transmission	power shutdowns, etc.) and unauthorized data to other	Data Signature		me as on the Left)	Integrated Log Management System			
								devices.	Approval of Important Operations		me as on the Left)				
					4							Davias Feet Data tit		Deductore	
							Outage	Stopping device functions.				Device Error Detection Device Alive Monitoring		Redundancy Failsafe Design	
												Log Collection/Log Analysis	l f	anouro Doorgin	
1												Integrated Log Management System			
							DoS Attack	Interruption of regular device operations by sending	DDoS Countermeasures			Device Error Detection	R	Redundancy	
								processing requests that exceed the processing capacity of				Device Alive Monitoring	F	Failsafe Design	<u> </u>
								the device as a result of a DDoS attack, etc.				Log Collection/Log Analysis Integrated Log Management System			
					1		Theft	Device theft.	Lock and Key Management	(Sar	me as on the Left)	(Same as on the Left)			
									Taman David						
							Information Theft by	Theft of information (software, authentication information, configuration settings, encryption keys and other confidential	Tamper Resistance Obfuscation		me as on the Left) me as on the Left)				
							Tampering Device at Time of Theft or Disposal	information settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and			me as on the Left)				
							or more or praposar	then disassembled.							
					1		Route Blocking	Communications are blocked by disconnecting the	Entrance and Exit Management (on the Premises Only)	0		Device Error Detection	R	Redundancy	—
								communication cable.	Lock and Key management	•		Device Alive Monitoring	+		<u> </u>
				2				Alternatively, communications are blocked by pulling out the		++		Log Collection/Log Analysis Integrated Log Management System	+		<u> </u>
			3	<b>_</b>		A .		communication cable from the device.		++		Surveillance Camera	+		<u> </u>
												Intrusion Detection Sensor			<u> </u>
															Ē
							Network Congestion	Causing congestion by generating the communications traffic				Device Error Detection	R	Redundancy	<u> </u>
								that exceeds the capacity of the device.	FW (Application Gateway Type)	+		Device Alive Monitoring			<u> </u>
			2	3		A			WAF	+ +		Log Collection/Log Analysis	+		<u> </u>
									IPS/IDS DDoS Countermeasures	+		Integrated Log Management System	+		<u> </u>
									Counter measures				+		<u> </u>
(			H	-	-		Jamming	Interference with radio communications.				Device Error Detection	R	Redundancy	
	Not applicable (no fur	nctions)										Device Alive Monitoring			
												Log Collection/Log Analysis			
l												Integrated Log Management System			
<				-	-								ļ		
							Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels	$\vdash$			+		<u> </u>
			2	3		A			Data Encryption	+			+		<u> </u>
									Exclusive Line	+ +			+		<u> </u>
					1		Unauthorized Modification of	Maliciously modifying information flowing on the network.	Encryption of Communications Channels			Log Collection/Log Analysis			<u> </u>
							Communication Data		Data Signature			Integrated Log Management System			
			2	3		A			Exclusive Line						_
															-
								Connecting unauthorized device on the network	Restriction on Connecting Device and its Usage			Restriction on Connecting Device and its Usage	$\square$		<u> </u>
			2	3	1		Device					Log Collection/Log Analysis			<u> </u>
			2			A						Integrated Log Management System			

Type of As Control System	Turne I	As	sessment Me	etrics		Thread (Attack Toron			ootia	Counterm	easures				Secur
Control System	sets Target Device	Threat Leve	Vulnerability Leve	el importance of Assets	Risk Value	Threat (Attack Type)	Description	Prote Intrusion/Spreading Phase	ection	Objective Achievement Pha	Detection/Understanding	Damage	Business Continuity		By '
	n Asset Controller, Controller	Thirda Coro			Tubic Fuldo	Unauthorized Access	Intrusion of the device via the network to execute an attack.	FW (Packet Filtering Type)			IPS/IDS			T	-
	(Master)							FW (Application Gateway Type)			Log Collection/Log Analys	is			1
								One-way Gateway			Integrated Log Management Syster	n			
								Proxy Server				_		<u> </u>	-
		2	3		A			WAF							-
								Peer-to-Peer Authentication IPS/IDS				-			-
								Applying Patches						<u> </u>	-
								Avoidance of Vulnerability						-	1
								, , , , , , , , , , , , , , , , , , , ,						-	1
1				1		Physical Intrusion	Unauthorized access of sections/areas (device installation locations,	Entrance and Exit Management (IC Card)	0		Surveillance Camera	0			-
							etc.) with access restrictions.	Lock and Key Management	0		Intrusion Detection Sensor	• •		<u> </u>	4
		2	2		В		It also refers to removing restrictions on devices with physical access restrictions (devices installed in racks, cabinets, etc.).								
							access restrictions (devices installed in facks, cabillets, etc.).								
1		2	2	1	в	Unauthorized Operation	Intrusion through direct operation of the device's console or other	Operator Authentication (ID/Pass)	0						-
-				4	-		component to execute an attack.					_		<u> </u>	
						Human Error in Operation	An attack triggered by a human error in operation by internal	URL Filtering/Web Reputation Mail Filtering				-			-
		2	3		A		personnel (an employee or partner with access privileges to the device).	Mail Filtering						<u> </u>	-
		-					An act equivalent to an attack is performed on the device as a result							-	1
							of a proper media or device connection.								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)				_
		2	3		A	Media or Device	device, etc.) brought in from outside the organization with the				Log Collection/Log Analys			–	-
							device to execute an attack.				Integrated Log Management Syster	n		–	-
				4		Execution of Linguthorized	Unauthorized execution of legitimate programs, commands,	Permission Management		(Same as on the Left)	Device Error Detection	-		<u>+</u>	+
						Processes	services, and other processes found on the attack target	Access Control		(Same as on the Left)	Device Alive Monitoring				1
		2	3	1	A		device.	Application Whitelisting		(Same as on the Left)	Log Collection/Log Analys	is			1
		_		1				Approval of Important Operations		(Same as on the Left)	Integrated Log Management Syster				1
				1											1
				1		Malware Infection		Anti-virus			Device Error Detection			1	1
							the attack target device.	Application Whitelisting			Device Alive Monitoring			<u> </u>	4
		1	3	1	в			Applying Patches			Log Collection/Log Analys				-
				1				Avoidance of Vulnerability			Integrated Log Management Syster	n	+	<u> </u>	-
				1				Data Signature					1	+	-
			1	1		Information Theft	Theft of information (software, authentication information,	Permission Management		(Same as on the Left)	Log Collection/Log Analys	is	1	+	+
			1	1			configuration settings, encryption keys and other confidential	Access Control		(Same as on the Left)	Integrated Log Management Syster	n			]
		3	3		A		information) stored on the device.	Data Encryption		(Same as on the Left)					1
								DLP		(Same as on the Left)					
							Unauthorized modification of information (software,	Permission Management		(Same as on the Left)	Device Error Detection		Data Backup	<u> </u>	-
		3	3		A	Information	authentication information, configuration settings, encryption	Access Control		(Same as on the Left)	Log Collection/Log Analys			+	-
							keys and other confidential information) stored on the device.	Data Signature		(Same as on the Left)	Integrated Log Management Syster	n		+	-
				4		Information Destruction	Destroying of information (software, authentication			Permission Management	Device Error Detection	-	Data Backup	+	+
						Information Destruction	information, configuration settings, encryption keys and other			Access Control	Log Collection/Log Analys	is		-	1
		3	3		A		confidential information) stored on the device.				Integrated Log Management Syster				
															1
				3		Unauthorized Transmission	Sending unauthorized control commands (settings changes,	Segmentation/Zoning		(Same as on the Left)	Log Collection/Log Analys				_
		3	3	°	A		power shutdowns, etc.) and unauthorized data to other	Data Signature		(Same as on the Left) (Same as on the Left)	Integrated Log Management Syster	n		+	-
							devices.	Approval of Important Operations		(Same as on the Leit)				+	-
1				1		Outage	Stopping device functions.				Device Error Detection		Redundancy		+
											Device Alive Monitoring		Failsafe Design		1
		2	3		A						Log Collection/Log Analys			<u> </u>	_
											Integrated Log Management Syster	n		_	4
				1		DoS Attack	Interruption of regular device operations by conding	DDoS Countermeasures			Device Error Detection		Redundancy	+	+
			1				Interruption of regular device operations by sending processing requests that exceed the processing capacity of	bboo countermeasures			Device Alive Monitoring		Failsafe Design	<u> </u>	1
		-									Log Collection/Log Analys				1
		3	3							I		is		_	1
		3	3				the device as a result of a DDoS attack, etc.				Integrated Log Management Syster				
		3	3		A									+-	1
		3	3		A			Lock and Key Management	0	(Same as on the Left)				E	+
		3	3		A		the device as a result of a DDoS attack, etc.	Lock and Key Management	0	(Same as on the Left)	Integrated Log Management Syster				-
		-			в	Theft	the device as a result of a DDoS attack, etc.				Integrated Log Management Syster				-
		-			в	Theft	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information.	Tamper Resistance		(Same as on the Left)	Integrated Log Management Syster				
		-		-	в	Theft Information Theft by Tampering Device at Time	the device as a result of a DDoS attack, etc. Device theft. 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)	Integrated Log Management Syster				- - - - -
		2	2	_	в	Theft Information Theft by Tampering Device at Time of Theft or Disposal	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and	Tamper Resistance Obfuscation		(Same as on the Left)	Integrated Log Management Syster				- - - - - -
		2	2	-	В	Theft Information Theft by Tampering Device at Time of Theft or Disposal	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled.	Tamper Resistance Obfuscation		(Same as on the Left) (Same as on the Left)	Integrated Log Management Syster		Redundancy		
		2	2	-	В	Theft Information Theft by Tampering Device at Time of Theft or Disposal	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and	Tamper Resistance Obfuscation Zeroization		(Same as on the Left) (Same as on the Left)	Vitegrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring	n	Redundancy		
		2	2		В	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management		(Same as on the Left) (Same as on the Left)	Integrated Log Management System (Same as on the Left)  Device Error Detection Device Alive Monitoring Log Collection/Log Analys	n	Redundancy		
		2	2	-	В	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable.	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management		(Same as on the Left) (Same as on the Left)	Vtegrated Log Management System (Same as on the Left) (Same as on the Left) Device Error Detection Device Airve Monitoring Log Collection/Log Analys Integrated Log Management System	n	Redundancy		
		2	2		В	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communications are blocked by pulling out the	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management		(Same as on the Left) (Same as on the Left)	Vitegrated Log Management System (Same as on the Left) (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection.Log Analys Integrated Log Management System Surveillance Camera	n	Redundancy		
		2	2	-	В	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communications are blocked by pulling out the	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management		(Same as on the Left) (Same as on the Left)	Vtegrated Log Management System (Same as on the Left) (Same as on the Left) Device Error Detection Device Airve Monitoring Log Collection/Log Analys Integrated Log Management System	n	Redundancy		
		2	2	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembid. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Tamper Resistance Obtiscation Zeroization Entrance and Exit Management Lock and Key management		(Same as on the Left) (Same as on the Left)	Vtegrated Log Management System (Same as on the Left) Device Error Detection Device Aire Monitoring Log Collection/Log Analys Integrate Log Management System Surveillance Camera Intrusion Detection Sensor	n			
		2	2	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	the device as a result of a DDoS attack, etc. Device theft. Theft of information (coftware, authentication information, 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	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type)		(Same as on the Left) (Same as on the Left)	Vitegrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection/Log Analys Integrated Log Management System Surveillance Camera Intrusion Detection Sensor Device Error Detection	n	Redundancy Redundancy		
		2	2	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembid. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable from the device.	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management Unck and Key management EW (Packet Filtering Type) FW (Application Gateway Type)		(Same as on the Left) (Same as on the Left)		n			
		2	2	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	the device as a result of a DDoS attack, etc. Device theft. Theft of information (coftware, authentication information, 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	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF		(Same as on the Left) (Same as on the Left)	Vtegrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection-Log Analys Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Error Detection Device Error Detection Device Collection-Log Analys	n			
		2	2	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	the device as a result of a DDoS attack, etc. Device theft. Theft of information (coftware, authentication information, 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	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/DS PS/DS		(Same as on the Left) (Same as on the Left)		n			
		2	2	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	the device as a result of a DDoS attack, etc. Device theft. Theft of information (coftware, authentication information, 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	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF		(Same as on the Left) (Same as on the Left)	Vtegrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection-Log Analys Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Error Detection Device Error Detection Device Collection-Log Analys	n			
		2	2	-	B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	the device as a result of a DDoS attack, etc. Device theft. Theft of information (coftware, authentication information, 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	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/DS PS/DS		(Same as on the Left) (Same as on the Left)	Vitograted Log Management System (Same as on the Left) Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analys VitograteLog Management System Device Error Detection Device Error Detection Device Error Detection Device Alive Monitoring Log Collection/Log Analys Vitograted Log Management System	n	Redundancy		
Not applicable	(no functions)	2	2		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/DS PS/DS		(Same as on the Left) (Same as on the Left)	Vtegrated Log Management System (Same as on the Left) Device Error Detection Device Alive Monitoring Log Collection-Log Analys Surveillance Camera Intrusion Detection Sensor Device Error Detection Device Error Detection Device Error Detection Device Collection-Log Analys	n			
Not applicable	(no functions)	2	2		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/DS PS/DS		(Same as on the Left) (Same as on the Left)		n	Redundancy		
Not applicable	(no functions)	2	2		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/DS PS/DS		(Same as on the Left) (Same as on the Left)		n	Redundancy		
Not applicable	(no functions)	2	2		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications.	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/IDS DDoS Countermeasures		(Same as on the Left) (Same as on the Left)		n	Redundancy		
Not applicable	(no functions)	2	2		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Tamper Resistance         Obfuscation         Zeroization         Entrance and Exit Management         Lock and Key management         Entrance         FW (Packet Filtering Type)         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)		n	Redundancy		
Not applicable	(no functions)	2	2		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications.	Tamper Resistance Obtiscation Zeroization Eroization Eroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/IDS DDoS Countermeasures Encryption of Communications Channels Data Encryption		(Same as on the Left) (Same as on the Left)		n	Redundancy		
Not applicable	(no functions)	2	2		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications.	Tamper Resistance         Obfuscation         Zeroization         Entrance and Exit Management         Lock and Key management         Entrance         FW (Packet Filtering Type)         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)		n	Redundancy		
Not applicable	(no functions)	2	2		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (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)		n	Redundancy		
Not applicable	(no functions)	2	2		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. Communications are blocked by disconnecting the communication cable. Alternatively, communications are blocked by pulling out the communication cable. Causing congestion by generating the communications traffic that exceeds the capacity of the device. Interference with radio communications.	Tamper Resistance Obtiscation Zeroization Eroization Eroization FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/IDS DDoS Countermeasures Encryption of Communications Channels Encryption of Communications Channels Encryption of Communications Channels		(Same as on the Left) (Same as on the Left)		n	Redundancy		
Not applicable	(no functions)	2	2		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Tamper Resistance Othuscation Zeroization Entrance and Exit Management Lock and Key management EW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/IDS DDoS Countermeasures Encryption of Communications Channels Data Encryption Encryption of Communications Channels Data Signature		(Same as on the Left) (Same as on the Left)		n	Redundancy		
Not applicable	(no functions)	2	2		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Tamper Resistance Obtiscation Zeroization Eroization Eroization FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/IDS DDoS Countermeasures Encryption of Communications Channels Encryption of Communications Channels Encryption of Communications Channels		(Same as on the Left) (Same as on the Left)		n	Redundancy		
Not applicable	(no functions)	2	2		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of Communication Data	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/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)		n	Redundancy		
Not applicable	:(no functions)	2	2		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of Communication Data Connecting Unauthorized	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Tamper Resistance Othuscation Zeroization Entrance and Exit Management Lock and Key management EW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/IDS DDoS Countermeasures Encryption of Communications Channels Data Encryption Encryption of Communications Channels Data Signature		(Same as on the Left) (Same as on the Left)		n	Redundancy		
Notapplicable	(no functions)	2	2		B	Theft Information Theft by Tampering Device at Time of Theft or Disposal Route Blocking Network Congestion Jamming Packet Sniffing Unauthorized Modification of Communication Data	the device as a result of a DDoS attack, etc. Device theft. Theft of information (software, authentication information, configuration settings, encryption keys and other confidential information) stored on devices which were stolen or disposed of and then disassembled. 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.	Tamper Resistance Obfuscation Zeroization Entrance and Exit Management Lock and Key management FW (Packet Filtering Type) FW (Application Gateway Type) WAF PS/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)		n i i i i i i i i i i i i i	Redundancy		

Type of Assets	Target Device	As	ssessment Me	etrics		Threat (Attack Type)	Description	Prote	Counter	measures				Securi By T
Type of Assets	Talget Device	Threat Level	Vulnerability Level	el Importance of Asseta	Risk Value	Theat (Attack Type)	Description	Intrusion/Spreading Phase	Objective Achievement Ph	betection/Understanding	Damage	Business Continuity		By
Control System Asse	t Controller (Slave)					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 Analys		l	—	-
								One-way Gateway		Integrated Log Management System	n		<u> </u>	-
								Proxy Server WAF				(	<u> </u>	1
		2	3		A			Peer-to-Peer Authentication				[	-	1
								IPS/IDS						1
								Applying Patches				ļ		_
								Avoidance of Vulnerability				l	_	-
-				-		Physical Intrusion	Unauthorized access of sections/areas (device installation locations,	Entrance and Exit Management		Surveillance Camera		<u> </u>	+	+
						r nysical initiasion	etc.) with access restrictions.	Lock and Key Management	0	Intrusion Detection Senso		[	-	1
		3	2		A		It also refers to removing restrictions on devices with physical					Í		
							access restrictions (devices installed in racks, cabinets, etc.).					í .		
4			+			Line that and One section	Intrusion through direct operation of the device's console or other	Operator Authentication (ID/Pass)	0			l	<u> </u>	_
		3	2		A	Unauthorized Operation	component to execute an attack.	Operator Authentication (ID/Pass)				i	-	1
1			1	1 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					─	-
		2	3		A		device). An act equivalent to an attack is performed on the device as a result				-	l		-
							of a proper media or device connection.					i	-	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)	(Same as on the Left)		[		1
		2	3		A	Media or Device	device, etc.) brought in from outside the organization with the			Log Collection/Log Analys		L	—	-
		-					device to execute an attack.			Integrated Log Management System	n		─	-
-			+	- +		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
		2	3		A		device.	Application Whitelisting	(Same as on the Left)	Log Collection/Log Analys			<u> </u>	-
								Approval of Important Operations	(Same as on the Left)	Integrated Log Management System	n	l	—	-
		<b>—</b>	+	4 }		Malware Infection	Infection or running of malware (unauthorized programs) on	Anti-virus		Device Error Detection	-	i	+	+
							the attack target device.	Application Whitelisting		Device Alive Monitoring				1
			<b>,</b>		в			Applying Patches		Log Collection/Log Analys				]
		1	3		5			Avoidance of Vulnerability		Integrated Log Management System	n		+	1
								Data Signature		+ +		l	<u> </u>	-
			+			Information Theft	Theft of information (software, authentication information,	Permission Management	(Same as on the Left)	Log Collection/Log Analys	is	i	+	+
						anormation met	configuration settings, encryption keys and other confidential	Access Control	(Same as on the Left)	Integrated Log Management System				1
		3	3		A		information) stored on the device.	Data Encryption	(Same as on the Left)					1
							,	DLP	(Same as on the Left)			ļ		1
				4				Demission Management	(Company on the Left)	Davias Free Datastica		Data Daaluur	<u> </u>	+
							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 Analys	is	Data Backup		1
		3	3		A	Information	authentication information, configuration settings, encryption keys and other confidential information) stored on the device.	Data Signature	(Same as on the Left)	Integrated Log Management System		í	<u> </u>	1
							keys and other connuential mornation) stored on the device.					[		1
				1 [		Information Destruction	Destroying of information (software, authentication		Permission Management	Device Error Detection		Data Backup		-
		3	3		A		information, configuration settings, encryption keys and other		Access Control	Log Collection/Log Analys Integrated Log Management System				-
							confidential information) stored on the device.			integrates cog management oyster			<u> </u>	1
-			-	1.1		Unauthorized Transmission	Sending unauthorized control commands (settings changes,	Segmentation/Zoning	(Same as on the Left)	Log Collection/Log Analys		i		+
		3	3	3	A		power shutdowns, etc.) and unauthorized data to other	Data Signature	(Same as on the Left)	Integrated Log Management System	n	ļ	<u> </u>	4
			1		~		devices.	Approval of Important Operations	(Same as on the Left)			l	<u> </u>	4
-						Outage	Stopping device functions.			Device Error Detection	-	Redundancy	0	+
						Oulage	Stopping device functions.			Device Alive Monitoring		Failsafe Design	0	1
		3	3		A					Log Collection/Log Analys				1
										Integrated Log Management System	n		<u> </u>	4
-			+			DoS Attack	Interruption of regular device operations by sending	DDoS Countermeasures		Device Error Detection		Redundancy	0	+
						DOS Allack	processing requests that exceed the processing capacity of	bboo countermeasures		Device Alive Monitoring		Failsafe Design	0	1
		3	3		A		the device as a result of a DDoS attack, etc.			Log Collection/Log Analys				]
										Integrated Log Management System	n	ļ	<u> </u>	4
				4		-						ļ	—	╇
		3	2		A	Theft	Device theft.	Lock and Key Management	<ul> <li>(Same as on the Left)</li> </ul>	(Same as on the Left)		i	+	-
		ľ	1		^					+ +			+	1
			+	1 1		Information Theft by	Theft of information (software, authentication information,	Tamper Resistance	(Same as on the Left)			i <u> </u>	<u> </u>	+
		3	2		A	Tampering Device at Time	configuration settings, encryption keys and other confidential	Obfuscation	(Same as on the Left)		-		+	4
			1			of Theft or Disposal	information) stored on devices which were stolen or disposed of and then disassembled.	Zeroization	<ul> <li>(Same as on the Left)</li> </ul>		-		<u> </u>	+
			<u> </u>	- +		Route Blocking	Communications are blocked by disconnecting the	Entrance and Exit Management		Device Error Detection		Redundancy	<u> </u>	t
				L 1			communication cable.	Lock and Key management		Device Alive Monitoring				1
				L 1			Alternatively, communications are blocked by pulling out the			Log Collection/Log Analys				4
							communication cable from the device.			Integrated Log Management System	n		1	4
										Surveillance Camera Intrusion Detection Senso			-	4
										Intrasion Detection Senso				1
				1 1		Network Congestion	Causing congestion by generating the communications traffic	FW (Packet Filtering Type)		Device Error Detection		Redundancy		t
							that exceeds the capacity of the device.	FW (Application Gateway Type)		Device Alive Monitoring				1
				1 I				WAF		Log Collection/Log Analys				4
								IPS/IDS		Integrated Log Management System	n			4
				L 1				DDoS Countermeasures					-	4
			-			Jamming	Interference with radio communications.			Device Error Detection		Redundancy		+
	functions)						Contraction of the state of the			Device Alive Monitoring				1
Not applicable (no										Log Collection/Log Analys	is			1
Not applicable (no										Integrated Log Management System				4
Not applicable (no			-										4	4
Not applicable (no				L 1		Packet Sniffing	Theft of information flowing on the network.	Encryption of Communications Channels						4
Not applicable (no				L 1				Data Encryption					-	4
Not applicable (no				L 1				Exclusive Line						4
Not applicable (no				4 k		Unauthorized Modification of	Maliciously modifying information flowing on the network.	Encryption of Communications Channels		Log Collection/Log Analys	s			t
Not applicable (no				1 1			and the second s	Data Signature		Integrated Log Management System				1
Not applicable (no						Communication Data								
Not applicable (no						Communication Data		Exclusive Line						
Notapplicable (no								Exclusive Line						1
Notapplicable (no				-		Connecting Unauthorized	Connecting unauthorized device on the network			Rastriction on Connecting Device and its Usage				-
Not applicable (no							Connecting unauthorized device on the network	Exclusive Line			is			

This page has intentionally been left blank.

## 3.3. Summary of Risk Values

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

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

[Output 3.3①]

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

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

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

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

## [Output 3.32]

			•								-		
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	С	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		

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

## 4. Business Impact-based Risk Analysis

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

Section In this Volume	Outputs for Preparations Used	Guide
2.1	List of Assets	3.1.5. Table 3-9
2.2	System Configuration Diagram	3.2.3. Figure 3-8
2.3.①	Dataflow Matrix	3.3.1. Table 3-10
2.3.2	Dataflow Chart	3.3.2. Figure 3-14
2.6	Evaluation Criteria for	4.3.2. Table 4-11
2.0	Business Impact Levels	4.3.2. Table 4-11
2.7	List Detailing Business Impacts	4.2.2. Table 4.12
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
	Business Impact-based Risk	664 to 611
4.4	Assessment Sheet	6.6.4. to 6.11.
4.5	Summary of Risk Values	6.11.3.

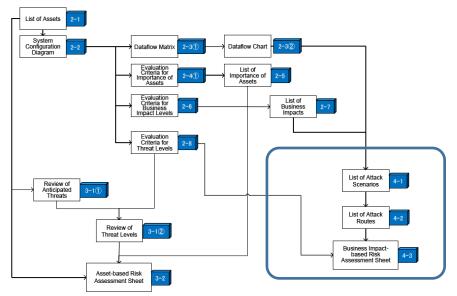


Figure 4-1: Business Impact-based Risk Analysis Work Flow

## 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.

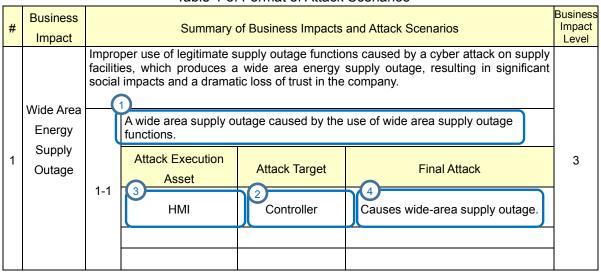


Table 4-3: Format of Attack Scenarios

# [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.

ltem Number	Business Impact		Summary of Busin	ess Impacts and Attack S	icenarios (*1)		Business Impact Lev						
		• •	legitimate supply outage functions caused by a cyber impacts and a dramatic loss of trust in the company.	attack on supply facilities,	which produces a wi	de area fuel supply outage, resulting in							
1	Wide Area Fuel	Scenario #	Attack Scenario	Attack Execution Asset	Attack Target	Final Attack	3						
·	Supply Outage	1-1	A wide area supply outage caused by the use of	нмі	Controller	Causes wide-area supply outage.	(*2)						
		1-2	wide area supply outage functions. A wide area supply outage caused by supply outage	Controller (Master)	Controller (Slave)	Sends malicious control command to cause							
			commands being sent to multiple controllers. s and explosions due to control abnormalities and a los		. ,	supply outage.							
			cilities. Such attacks impact local residents and the en										
		Item Number	Attack Scenario	Attack Execution Asset	Attack Target	Final Attack							
			Outbreak of fires and explosions due to control abnormalities in facilities for handling hazardous	нмі	Controller	Sets incorrect target value for controller.							
		2-1	materials caused by the setting of improper target values.	Control Server	Controller	Sets incorrect target value for controller.							
2	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 HMI.							
		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.							
			Outbreak of fires and explosions caused by a loss of monitoring and monitoring control at facilities for	Control Network (Field	Control Network	Maliciously modifies network settings and disables communications.							
		2-4	handling hazardous materials due to congestion in the control network (field side).	Side) Connected Device		Infects with malware causing unauthorized communications, and disables communications.							
		Manufacturing a	nd supply of fuel that does not meet quality standards	caused by a cyber attack	on manufacturing fac								
		customers, sign	ficant losses in compensation claims, and a dramatic lo	oss of trust in the company	1.								
		Item Number	Attack Scenario	Attack Execution Asset	Attack Target	Final Attack							
			Production of fuel that does not meet quality standards due to control abnormalities in production	нмі	Controller	Sets incorrect target value for controller.							
		3-1	facilities caused by the setting of improper target values.	Control Server	Controller	Sets incorrect target value for controller.							
3	Supply of Defective Fuel	3-2	Production of fuel that does not meet quality standards due to control abnormalities in production	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 standards due to control abnormalities in production	нмі	нмі	Tampers with and alters data/software in HMI.							
		3-3	facilities caused by tampering with and altering data/software.	Control Server	Control Server	Tampers with and alters data/software in control server.	4						
		Manufacturing/production disrupt/suspend and damages due to forcibly terminated processes due to process control abnormalities and operation monitoring failures caused by a cyber attack on manufacturing facilities.											
		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.							
4	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)						
		4-3	Operational abnormalities in production facilities caused by tampering with and altering data/software.	НМІ	НМІ	Tampers with and alters data/software in HMI.							
			This leads to processes being terminated for safety reasons.	Control Server	Control Server	Tampers with and alters data/software in control server.							
		4-4	A destructive malware or ransomware infection that disables monitoring of production facilities and prevent monitoring control. This leads to processes being terminated for safety reasons.	НМІ	НМІ	Infects the system with destructive malware and ransomware, disabling monitoring operations.							
		-	on the control system, resulting in an external leak of co leading to a deterioration in competitive strength.	ompany production secret	s, impacting the comp	pany's competitive edge against other							
		1											
	Leak of	Item Number	Attack Scenario	Attack Execution Asset	Attack Target	Final Attack							
5	Leak of confidential information	Item Number			Attack Target	Final Attack Theft of confidential information stored on the EWS.	3						

61

\*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".

62

## 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 4.2] Listing the attack entry points for the attack execution asset "HMI" in attack scenario 1-1.

[Task 4.2<sup>(2)</sup>] 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 4.2(4)] Carrying out tasks (1) to (3) for all attack scenarios.

Attack	Who	From Where		How		Attack Execution	Attack	Final Attack
Scenario	Attacker	Attack Entry Point	Attack Path 1	Attack Path 2	Attack Path 3	Asset	Target	FINALALIACK
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	()			2	Controller (M)	Controller (S)	Sends malicious control command to cause supply outage.
1-2						Controller (M)	Controller (S)	Sends malicious control command to cause supply outage.
1-2						Controller (M)	Controller (S)	Sends malicious control command to cause supply outage.

This page has intentionally been left blank.

# [Output 4.2]

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

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

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

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

Attack			- 110			· · ·	-		•
Tree	Scenario	Who	From Where		1	1	۲	low	
Number	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	нмі	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						
1-3	4-3	Malicious Third Party	Information Network	FW			НМІ	НМІ	Tampers with and alters data/software in HMI.
1-4	4-4	Malicious Third Party	Information Network	FW			нмі	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	4-3	Malicious Third Party	Information Network	FW			Control Server	Control Server	Tampers with and alters data/software in control server.
		-	-						
1-14	5-1	Malicious Third Party	Information Network	FW			Control Server	Control Server	Theft of confidential information stored on the control server.
1-15	2-1	Malicious Third Party	Information Network	FW			Control Server	Controller	Sets incorrect target value for controller.
1-16	3-1	Malicious Third Party	Information Network	FW			Control Server	Controller	Sets incorrect target value for controller.
		-							-
1-17	4-1	Malicious Third Party	Information Network	FW			Control Server	Controller	Sets incorrect target value for controller.
1-18	5-1	Malicious Third Party	Information Network	FW			EWS	EWS	Theft of confidential information stored on the EWS.
1-19	2-2	Malicious Third Party	Information Network	FW			EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
1-20	3-2			FW			EWS		Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
		Malicious Third Party	Information Network					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
			-			. Laon Fairo			
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	3-3	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		нмі	НМІ	Tampers with and alters data/software in HMI.
2-3	4-3	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		нмі	нмі	Tampers with and alters data/software in HMI.
2-4				,			нмі	НМІ	
	4-4	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian				Infects the system with destructive malware and ransomware, disabling monitoring operations.
2-5	1-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		HMI	Controller	Causes wide-area supply outage.
2-6	2-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		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	-	-	,	Data Historian		Control Conver	Control Server	Tenners with and alters data (software in control conver
	-	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)			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.
	_		Monitoring Terminal	,					
2-15	2-1	Malicious Third Party	ivionitoring i erminal	Data Historian (Relay)	Data Historian		Control Server	Controller	Sets incorrect target value for controller.
2-16	3-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		Control Server	Controller	Sets incorrect target value for controller.
2-17	4-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		Control Server	Controller	Sets incorrect target value for controller.
2-18	5-1	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		EWS	EWS	Theft of confidential information stored on the EWS.
		-					-	-	
2-19	2-2	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
2-20	3-2	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
2-21	4-2	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian		EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
2-22	1-2	Malicious Third Party	Monitoring Terminal	Data Historian (Relay)	Data Historian	EWS	Controller (M)	Controller (S)	Sends malicious control command to cause supply outage.
		-	_						
Tree #	Scenario #	Attacker	Attack Entry Point	Attack Path 1	Attack Path 2	Attack Path 3	Attack Execution Asset	Attack Target	Final Attack
3-1	2-3	Insider (Human Error)	HMI (Physical Intrusion)				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	1-1	Insider (Human Error)	HMI (Physical Intrusion)				нмі	Controller	Causes wide-area supply outage.
3-6							нмі		
	2-1	Insider (Human Error)	HMI (Physical Intrusion)					Controller	Sets incorrect target value for controller.
3-7	3-1	Insider (Human Error)	HMI (Physical Intrusion)				НМІ	Controller	Sets incorrect target value for controller.
3-8	4-1	Insider (Human Error)	HMI (Physical Intrusion)				нмі	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.
	3-1	Insider (Human Error)	Control Server (Physical Intrusion)				Control Server	Controller	Sets incorrect target value for controller.
3-16									
	4-1	Insider (Human Error)	Control Server (Physical Intrusion)				Control Server	Controller	Sets incorrect target value for controller.
3-17		Insider (Human Error)	EWS (Physical Intrusion)				НМІ	НМІ	Infects the system with destructive malware and ransomware, disabling monitoring operations.
	4-4	(					EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
3-17	4-4 2-2	Insider (Human Error)	EWS (Physical Intrusion)						
3-17 3-18 3-20	2-2	Insider (Human Error)					EWR	Controller	Maliciously modifies settings of controllar (such as therebold values). Tame
3-17 3-18 3-20 3-21	2-2 3-2	Insider (Human Error) 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.
3-17 3-18 3-20	2-2	Insider (Human Error)					EWS EWS	Controller Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller. Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.
3-17 3-18 3-20 3-21	2-2 3-2	Insider (Human Error) Insider (Human Error)	EWS (Physical Intrusion)						
3-17 3-18 3-20 3-21 3-22 3-23	2-2 3-2 4-2 2-4	Insider (Human Error) Insider (Human Error) Insider (Human Error) Insider (Human Error)	EWS (Physical Intrusion) EWS (Physical Intrusion) EWS (Physical Intrusion)				EWS EWS	Controller Control Network (Field Side)	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller. Maliciously modifies network settings and disables communications.
3-17 3-18 3-20 3-21 3-22	2-2 3-2 4-2	Insider (Human Error) Insider (Human Error) Insider (Human Error)	EWS (Physical Intrusion) EWS (Physical Intrusion)				EWS	Controller	Maliciously modifies settings of controller (such as threshold values). Tampers with and alters data/software in controller.

66

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.

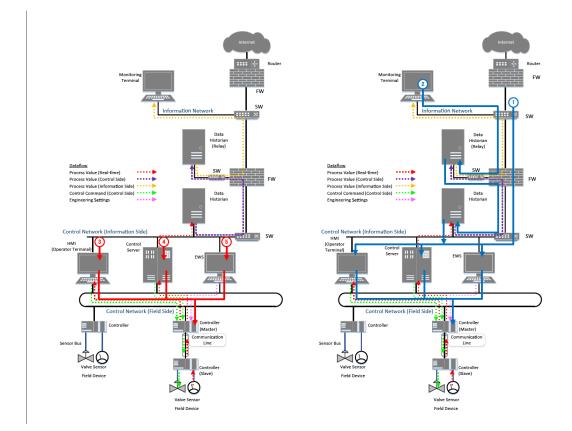


Figure 4-2: Attack Route Diagram

## 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 4.3<sup>(2)</sup>] 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 Impactbased 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 easyto-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

Ŧ (	Attack	Scenario		Assessme	ent Metrics		Countern		Security Level		Attack T	ree Number	
	1.1	Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Level	Pro Intrusion/ Spreading Phase	tection Objective Achievement Phase	Detection/ Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuratio Steps (iter Number)
	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".		ns.		FW O Peer-to-Peer Authentication Applying Patches Avoidance of Vulnerability Permission Management O	(Same as on the left)	IPS/IDS Log Colection/Log Analysis rilegiated Log Management System Device Alive Monitoring		2			
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 O Applying Patches Avoidance of Vulnerability Permission Management		IPS/IDS Log Collection/Log Analysis Hegrated 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     O       Applying Patches     O       Avoidance of Vulnerability     Permission Management     O	(Same as on the left)	IPS/IDS Log Collection/Log Analysis Hegrated 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     O       Applying Patches     Avoidance of Vulnerability       Permission Management     O		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 O Applying Patches Avoidance of Vulnerability Permission Management		IPS/IDS Log Collection/Log Analysis Hegrated 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
B		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		Device Error Detection Device Alive Monitoring Log Cotection/Log Analysis Integrated Log Management System		1 *2			
9	1-1	Supply outage encompassing a wide area caused by malware triggering wide area supply outage functions from the HMI.	2	3	3 A	Data Signature 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	1	#1-3	8,9
0	<u>1-2</u>	A wide area supply outage caused by supply outage commands be 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 sent to m	ultiple control	llers.	Same as item number 1							
1		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 Hitigrated Log Management System Device Alive Monitoring		1			
2		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 Hegrated Log Management System	Data Backup	] 1			
3	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 Hegrated Log Management System		1	2	#1-4	10,11,12 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' vacuation of unauthorized processes' (privilege escalation). Countermeasures used for the two threats are merged, Italic text is used to denote the "execution of unauthorized processes".					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".					Same as ite	em number 5		2			
6		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 O Applying Patches Permission Management Application Whitelisting	(Same as on the left) (Same as on the left)	IPS/IDS Log Collection/Log Analysis Hegrated Log Management System Device Alive Monitoring		2			
7		Tampering with and altering data/software in controller (M) from the EWS by a malicious third party.					Same as iter	m number 12		1			
8	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	3 В		Same as iter	m number 13		1	2	#1-5	14,15,1 7,18
9		Attack Entry Point = EWS Due to human error by an insider, the EWS is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".				Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature		Device Error Detection Device Alive Monitoring Log Cotlection/Log Analysis Hingrated 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 Hegrated Log Management System	Data Backup	1			
:1	1-2	Issuing of commands to stop the controller (S) via the controller (M) by malware infection. Supply outage encompassing a wide area.	2	3	3 A	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Hegrated Log Management System		1	1	#1-6	19,20,2
×													

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

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

### 2. Occurrence of Fires and Explosion Incidents

		ice of Fires and Explosion Incidents Scenario		Assessment Metrics			Counter		Securit	y Level	Attack T	ree Number	
ltem Number		Attack Tree/Attack Steps	Threat Level	Vulnerability Business Level Impact Lev	el Risk Value	Intrusion/ Spreading Phase	Objective Achievement Phase	Detection/ Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Attack Attack Tree Number	Configuration Steps (Item Number)
22	2-1	Outbreak of fires and explosions due to control abnormalities in facil 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".	ities for hand	ling hazardous materials	caused by the	e setting of improper ta	-	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 it	em number 2		2			
24	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the HMI by a malicious third party.	2	2 3	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	#2-1	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	(Same as on the left)	IPS/IDS Log Collection/Log Analysis Integrated Log Management System		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	Application Whitelisting         •           Segmentation/Zoning         •           Data Signature         •           Approval of Important Operations         •	(Same as on the left) (Same as on the left) (Same as on the left) (Same as on the left)	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management Bystem		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 it	em number 4		2 *1			
28		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as it	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					Same as it	em number 6		2			
30	2-1	processes". 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 ite	em number 24		1	2	#2-3	27,28,29,3 0
31		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".				Peer-to-Peer Authentication  Applying Patches Avoidance of Vulnerability Permission Management		IPS/IDS Log Collection/Log Analysis Integrated Log Management Bystem Device Alive Monitoring		2			
32	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the control server by a malicious third party.	2	2 3	В	Permission wanagement	Same as ite	em number 26		1	2	#2-4	27,28,31,3 2
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							
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 ite	em number 24		1	1	#2-5	33,34
35		Attack Entry Point = Control Server Due to human error by an insider, the control server is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".				Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		2 *2			
36	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the control server by a malware infection.	2	2 3	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 Bystem		1	2	#2-6	35,36
37	2-2	Outbreak of fires and explosions due to control abnormalities in facil 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".	ities for hand	ling nazardous materials	caused by the	a 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).					Same as ite	em 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 Bystem	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. <sup>1</sup> 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			
41		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item number 5						
42		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		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	В		Same as ite	em number 39		1	2	#2-8	40,41,42,4 3
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".	tack Entry Point = EWS te to human error by an insider, the EWS is infected with malware after being nnected to a malware-infected USB storage device. Is this is the result of actions by an insider, it is assumed that there is no threat										

			or a delibe	hate attempt at connecting to unautionzed media.				• • • • • • • • • • • • • • • • •		_					• • • • • • • • • • • • • • • • •	• • • • • • • • • • • • • • • • •	• • • • • • • • • • • • • • • • • • • •
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	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 Integrated Log Management System	 Data Backup	 1	1	#2-9	44,45

### 2. Occurrence of Fires and Explosion Incidents

		nce of Fires and Explosion Incidents Scenario		Assessme	nt Matrica			Countor	neasures		Securit	y Level	Attack T	ree Number
Item Number		Attack Tree/Attack Steps	Threat Level	Vuinerability Levei	Business Impact Level		Intrusion/ Spreading Phase	ection Objective Achievement Phase	Detection/	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
		Outbreak of fires and explosions due to control abnormalities in facil Outbreak of fires and explosions due to erratic behavior in facilities f Attack Entry Point = Information Network							ents a proper response	e, even when operations	are perfor	med corre	ctly.	
46		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						Same as ite	em number 1		2 *1			
47		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 ite	em number 2		2			
48	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	Data Backup	1	2	#2-10	46,47,48
49		Unauthorized access of the control server via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escatation).							m number 25		2			
50	2-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	3	В	Permission Management O Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	2	2	#2-11	46,49,50
51		Attack Entry Point = Monitorian (relay) from a monitoring terminal by a malicious third party. Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escatation). Countermasures used for the how threats are mored. Talks their tals used to denote the "execution" of unauthorized access.							em number 4	+	2 *1			
52		Unauthorized access of the data historian from the data historian (relay) by a     malicous third party.     " Unauthorized access includes "execution of unauthorized processes".						Same as iter	m number 28		2			
53		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access of the HMI from the data historian by a						Same as ite	em number 6		2			
54	2-3	processes". Tampering with and altering data/software in the	2	2	3	в		Same as ite	m number 48		1	2	#2-12	51,52,53,5
		HMI by a malicious third party. Unauthorized access of the control server from the data historian by a malicious third party.							I	1 1				4
55		* Unauthorized access includes "execution of unauthorized processes".						Same as iter	m number 31		2			51,52,55,5
56	2-3	Attack Entry Point = HMI	2	2	3	В		Same as ite	m number 50	1 1	1	2	#2-13	6
57		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	em number 8		1 *2			
58	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	57,58
59		Attack Entry Point = Control Server Due to human error by an insider, the control server is infected with malware after being connected to a malware-infected USB storage device.						Same as ite	m number 35		2			
		* 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".					Permission Management O	(Same as on the left)	Device Error Detection	Data Backup	*2			
60	<b>2-3</b>	Tampering with and altering data/software in the control server by malware infection.	2 monitoring c	2 ontrol at facili	3 ties for hand	B Iling hazardou	Access Control Data Signature Is materials due to con	(Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System etwork (field side).		2	2	#2-15	59,60
61		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution	_					Same as ite	em number 1		2 *1			
62		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 ite	em number 2		2			
63	2-4	Tampering with and altering the control network (field side) settings from the HMI to cause network congestion in the control network by a malicious third party. This prevents the monitoring of the control system.	2	2	3	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	#2-16	61,62,63
64		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	2	2	3	В	Anti-virus Application Whitelisting		Device Error Detection Device Alive Monitoring		1	2	#2-17	61,62,64
	2-4	communications. This prevents the monitoring of the control system.	-	-		5	Applying Patches Avoidance of Vulnerability Data Signature		Log Collection/Log Analysis Integrated Log Management System			-		01,02,01
65		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. " Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".						Same as ite	em number 4		2 *1			
66		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".						Same as ite	em number 5		2			
67		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".						Same as ite	em number 6		2			
68	2-4	processes . Tampering with and altering the control network (field side) settings from the HMI to cause network congestion in the control network by a malicious third party. This prevents the monitoring of the control system.	2	2	3	B		Same as iter	m number 63		1	2	#2-18	65,66,67,6 8
69	2-4	Infection of the HMI with malware by a malicious third party to cause unauthorized communication with the control network (field side) and prevent control network communications. This prevents the monitoring of the control system.	2	2	3	В		Same as iter	m number 64		1	2	#2-19	65,66,67,6 9
70		Attack Entry Point = HMI Due to human error by an insider, the HMI is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".						Same as ite	em number 8		1 *2			
71	2-4	Tampering with and altering the control network (field side) settings from the HMI to cause network congestion in the control network by malware infection. This prevents the monitoring of the control system.	2	3	3	A		Same as iter	m number 63		1	1	#2-20	70,71
72	2-4	Malware infection causing unauthorized communication with the control network (field side), and preventing control network communications. This prevents the monitoring of the control system.	2	3	3	A		Same as iter	m number 64		1	1	#2-21	70,72
73		Attack Entry Point = EWS Due to human error by an insider, the EWS is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to nuarthorized media".						Same as iter	m number 19		1 *2			
74	2-4	Tampering with and altering the control network (field side) settings from the EWS to cause network congestion in the control network by malware infection. This prevents the monitoring of the control system.	2	3	3	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	#2-22	73,74
75	2-4	Matware infection causing unauthorized communication with the control network (field side), and preventing control network communications. This prevents the monitoring of the control system.	2	3	3	A	Permission Management Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	1	#2-23	73,75
x														

 [Note]

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

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

#### 3. Supply of Defective Product

3. Sı		of Defective Product											
ltem	Attack	k Scenario		Assessme	ent Metrics		Counterme	asures		Security	y Level	Attack T	ree Number
m Number		Attack Tree/Attack Steps T	Threat Level	Vuinerability Levei	Business Impact Level Risk Value		e Achievement Phase	Detection/ Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (item Number)
-	3-1	Production of a product that does not meet quality standards/criteria d Attack Entry Point = Information Network	due to contro	ol abnormaliti	es in production facilities o	caused by the setting of improper	er target values.						
76		Unauthorized frewall access by a malicious third party. <sup>a</sup> 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 r	number 1		2 *1			
77		Unauthorized access of the HMI via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item	number 2		2			
78	3-1	Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the HMI by a malicious third party.	2	2	2 C	Segmentation/Zoning (Same as on Data Signature (Same as on Approval of Important Operations (Same as on	n the left) Integr	g Collection/Log Analysis rated Log Management System		1	2	#3-1	76,77,78
79		Unauthorized access of the control server via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Same as item 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 C	Segmentation/Zoning (Same as on Data Signature (Same as on Approval of Important Operations (Same as on	n the left)	g Collection/Log Analysis rated Log Management System		1	2	#3-2	76,79,80
81		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item i	number 4		2 *1			
82		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item i	number 5		2			
83		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized					Same as item r	number 6		2			
84	3-1	processes". Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the HMI by a malicious third party.	2	2	2 C		Same as item n	number 78		1	2	#3-3	81,82,83,8 4
85		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item n	number 31		2			
86	3-1	Production of a product that does not meet quality Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the control server by a malicious third party.	2	2	2 C		Same as item n	number 80		1	2	#3-4	81,82,85,8 6
87		Attack Entry Point = HMI Due to human error by an insider, the HMI is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item r	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 item n	number 78		1	1	#3-5	87,88
89		Attack Entry Point = Control Server Due to human error by an insider, the control server is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item 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 C		Same as item n	number 80		1	2	#3-6	89,90
	3-2		due to contro	o <mark>l abnormaliti</mark>	es in production facilities c	caused by the malicious modifica	ation of settings (	(thresholds, etc.) or t	ampering with and alter	ing progra	ms.		
91		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".					Same as item r	number 1		2 *1			
92		Unauthorized access of the EWS via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Same as item 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 C	Permission Management (Same as on Access Control (Same as on Data Signature (Same as on	n the left) Log	vice Error Detection g Collection/Log Analysis rated Log Management System	Data Backup	1	2	#3-7	91,92,93
94		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a mallicious third party. <sup>1</sup> 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 r	number 4		2 *1			
95		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item i	number 5		2			
96		Unauthorized access of the EWS from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as item 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 C		Same as item n	number 93		1	2	#3-8	94,95,96,9 7
98		Attack Entry Point = EWS Due to human error by an insider, the EWS is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					Same as item 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 B		Same as item n	number 93		1	1	#3-9	98,99

#### 3. Supply of Defective Product

₹ /	Attack	Scenario			Assessme	ent Metrics			Counterm	easures		Securit	y Level	Attack 1	Tree Number
ŝ								Prot	ection	Detection/				Attack	Configuration
Item Number			Attack Tree/Attack Steps	Threat Level	Vuinerability Level	Business Impact Level	Risk Value	Intrusion/ Spreading Phase	Objective Achievement Phase	Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Tree Number	Steps (Item Number)
₽	3-1	Production of a p	product that does not meet quality standards/criteria	due to contro	l abnormaliti	es in product	tion facilities c	aused by the setting o	of improper target values	i.					
_	3-3		product that does not meet quality standards/criteria	due to contro	<mark>l abnormalit</mark> i	es in product	tion facilities c	aused by tampering v	vith and altering data/sof	tware.		r			
00		Unauthorized firewall * Unauthorized acces escalation). Counterm	Information Network laccess by a malicious third party. ss includes "execution of unauthorized processes" (privilege measures used for the two threats are merged. Italic text is used to n of unauthorized processes".						Same as iter	n number 1		2 *1			
01			rized access of the HMI via the FW by a malicious third party. orized access includes "execution of unauthorized processes".						Same as iter	n number 2		2			
02	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
03		third party * Unautho	rized access of the control server via the FW by a malicious y. orized access includes "execution of unauthorized processes" escalation).						Same as iten	n number 25		2			
04	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
05		* Unauthorized access inc	he data historian (relay) from a monitoring terminal by a malicious third party. cludes "execution of unauthorized processes" (privilege escalation). for the two threats are merged. Italic text is used to denote the "execution of						Same as iter	m number 4		2 *1			
06		by a malic	rized access of the data historian from the data historian (relay) icious third party. orized access includes "execution of unauthorized processes".						Same as iter	n number 5		2			
07			Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".						Same as iter	n number 6		2			
80	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
09			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			
10	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
11		connected to a malv * As this is the result	<b>It = HMI</b> If by an insider, the HMI is infected with malware after being ware-infected USB storage device. It of actions by an insider, it is assumed that there is no threat mpt at "connecting to unauthorized media".						Same as iter	n number 8		1 *2			
12	3-3	Tamperin infection.	ng 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
13		connected to a malwa * As this is the result of	t = Control Server by an insider, the control server is infected with malware after being are-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	number 35		3 *2			
14	3-3	Tamperin malware i	ng with and altering data/software in the control server by infection.	2	2	2	с		Same as iten	n number 60		2	2	#3-15	113,114
x												~			

11 It is recommended to refer to "Section 9.4 Firewall Settings" in the Guide for evaluating countermeasures.
12 It is recommended to refer to "Section 9.5 Security Measures for External Storage Media" in the Guide for evaluating

countermeasures.

#### 4. Manufacturing/Production Disrupt/Suspend

. Man		ring/Production Disrupt/Suspend	1										
ltem	Attack	Scenario	Assess	ment Metrics			Counterm	neasures	Γ	Securit	y Level	Attack T	ree Numbe
n Number		Attack Tree/Attack Steps	Threat Level Vulnerability Level	y Business Impact Level	Risk Value		tection Objective Achievement Phase	Detection/ Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configuratio Steps (Iten Number)
117	<u>4-1</u>	Control abnormalities in production facilities caused by the setting 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".		<u>. This leads to p</u>	processes be	eing terminated for safe	ety reasons. Same as iter	m 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 iter	m number 2		2			
19	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the HMI by a malicious third party.	2 2	1	D	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis		1	2	#4-1	117,118 9
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	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#4-2	117,118 0
21		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 iter	m number 4		2 *1			
22		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 iter	m number 5		2			
23		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as iter	m number 6		2			
24	4-1	Abnormalities in the manufacturing facilities requiring an emergency atop 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	ı number 119		1	2	#4-3	121,122 3,124
25		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			
26	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 thrid party.	2 2	1	D		Same as item	ı number 120		1	2	#4-4	121,12 5,12
27		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 iter	m number 8		1 *2			
28	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the HMI by a malware infection.	2 3	1	D	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis		1	1	#4-5	127,1
29		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 iten	n number 35		2 *2			
30	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the control server by a malware infection.	2 2	1	D	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management Bystem		1	2	#4-6	129,1
	4-2	Control abnormalities in production facilities caused by the malicious	s modification of settings	<mark>s (thresholds, et</mark>	c.) or tampe	ring with and altering p	rograms. This leads to p	rocesses being termin	ated for safety reasons				
31		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 iter	m number 1		2 *1			
32		Unauthorized access of the EWS via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Same as iten	n number 11		1			
33	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	···· ·································	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup	1	2	#4-7	131,13 3
34		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 iter	m number 4		2 *1			
35		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			
36		Unauthorized access of the EWS from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Same as iten	n number 16		2			
37	4-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2 2	1	D		Same as item	number 133		1	2	#4-8	134,13 6,13
38		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 iten	n number 19		1 *2			
9	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	(Same as on the left) (Same as on the left)	Device Error Detection	Data Backup	1	1	#4-9	138, <i>*</i>

controller from the EWS. Data Signature (Same as on the left) Integrated Log Management System	

#### 4. Manufacturing/Production Disrupt/Suspend

Alease = benefab         Alease = benefab<	Atta	ps Tree	Attack	Configuration Steps (Item
1    	2			
Image: set of the state of	2			
Image: control in the second seco		1		
4     4     Image: bootstand in the part of any of	1			
143 A A A A A A A A A A A A A A A A A A A		2	#4-10	140,141,14 2
141       143       144       145       1	2	• •		
Image: Second Secon	2	2	#4-11	140,143,14
146       147       1 <td>2</td> <td></td> <td></td> <td></td>	2			
147       148       149       1	2			
148       4-3	2	2		
149       A       Important of the party indication of the party indindit party indication of the party indication of the par	1	2	#4-12	145,146,14 7,148
190       4.3	2	2		
111       Area       De to be more the year indice. It all is inficited with malayear allowing outside of a stateward with the in or the total of a stateward with the in or the total of a stateward with the in or the total of a stateward with the in or the total of a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside. If a stateward with the inficited with malayear allowing outside.	1	2	#4-13	145,146,14 9,150
192     102     103     1     D     Same as tem number 35       153     Attack Entry Point = Control Server     2     3     1     D     Same as tem number 35       153     Attack Entry Point = Control Server     2     2     1     D     Same as tem number 35       154     4.4     Attack Entry Point = Control Server     2     2     1     D     Same as tem number 35       154     4.4     Attack Entry Point = Control Server is information that disables monitoring of production facilities and prevent monitoring control. This leads to processes being terminated for safety reasons.       156     Attack Entry Point = Monitation the data setuing analyzables monitoring of production facilities and prevent monitoring control. This leads to processes being terminated for safety reasons.       156     Attack Entry Point = Monitation the data setuing analyzables monitoring of production facilities and prevent monitoring control. This leads to processes being terminated for safety reasons.       156     Attack Entry Point = Monitation the data setuing analyzables monitoring of production facilities and prevent monitoring control. This leads to processes being terminated for safety reasons.       157     Attack Entry Point = Monitation the data setuing analyzable matrice facilities and processes?     2     2     1     D     Same as tem number 3       158     Attack Entry Point = Monitation the data setuing analyzable for party. This prevents the monitoring of the control system.     2	1	2		
153       Aug       Description for your instruct your instruct with makes affecting connected with makes	1	1	#4-14	151,152
154     4.3     Tangeng with and altering data/software in the control server by maker infection.     2     2     1     D     Same as item number 60       164     A destructive or ransomware infection that disables montoined or portunation factoring or particular factoring or portunation factoring or portunating factoring or portuna	3	5.0.0.0.0.0.0.0.0.0		
156     Attack Entry Point = Information Network Unauthorized access includes "seculation of unauthorized processes" (privinge scalation). Contermessures used for the two treats are merged. Ball: ball to all to benche the "seculion of unauthorized access includes" seculation of unauthorized processes".     Image: Same as item number 1       156     Image: Same as item number 2       157     4.4       168     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     Device Enrol Detection     Data Backup       158     Attack Entry Point = Monitoring romainal ty a malicious third party. "Unauthorized access of the data historian (relay) by a malicious third party. This prevents the monitoring of the control system.     2     2     1     Device Enrol Detection     Data Backup       158     Infection of the thMI with destructive malware (ransomware, etc.) by a malicious third party. This prevents the monitoring of the control system.     2     2     1     Device Enrol Detection     Data Backup       158     Infection of the thMI with destructive malware (ransomware, etc.) by a malicious third party. "Unauthorized access of the data historian (relay) then a monitoring terminal ty unauthorized access of the data historian from the data historian (relay) by a malicious third party. "Unauthorized access includes "execution of unauthorized processes".     Image: Same as item number 4       159     Unauthorized access of the data historian from the data historian (relay) by a malicious third party. "Unauthorized access in thu	1	2	#4-15	152,154
156       A4       Inductorized access includes "execution of unauthorized processe" (priving escatation) Countements usuad for the two thread are merged. Italic text is used to denote the "execution of unauthorized processes".       Image: Same as item number 1         156       Image: Same as item number 2       Same as item number 2         157       Image: Same as item number 2       Image: Same as item number 2         158       Image: Same as item number 1       Image: Same as item number 2         158       Image: Same as item number 2       Image: Same as item number 2         158       Image: Same as item number 1       Image: Same as item number 2         158       Image: Same as item number 1       Image: Same as item number 2         158       Image: Same as item number 1       Image: Same as item number 2         158       Image: Same as item number 1       Image: Same as item number 2         158       Image: Same as item number 4       Image: Same as item number 4         158       Image: Same as item number 4       Image: Same as item number 4         158       Image: Same as item number 4       Image: Same as item number 4         159       Image: Same as item number 4       Image: Same as item number 4         159       Image: Same as item number 4       Image: Same as item number 4         159       Image: Same as item number 4				
156       A.4       A	2	2+0+0+0+0+0+0+0+0+0+0+0+0+0+0+0+0+0+0+0		
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     0	2			-
158       Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. Unauthorized access of the data historian from the data historian (relay) by a malicious third party. Unauthorized access of the data historian from the data historian (relay) by a malicious third party. Unauthorized access of the data historian from the data historian (relay) by a malicious third party.       Image: Construction of unauthorized access of the data historian from the data historian (relay) by a malicious third party.       Image: Construction of unauthorized access of the data historian from the data historian (relay) by a malicious third party.       Image: Construction of unauthorized access of the data historian from the data historian (relay) by a unauthorized access of the data historian from the data historian (relay) by a unauthorized access of the data historian by a malicious third unauthorized access of the data historian by a malicious third unauthorized access of the data historian by a malicious third unauthorized access of the data historian by a malicious third unauthorized access of the data historian by a malicious third unauthorized access of the data historian by a malicious third unauthorized access of the data historian by a malicious third unauthorized access of the data historian by a malicious third unauthorized access of the data historian by a malicious third unauthorized access of the data historian by a malicious third unauthorized access of the data historian by a malicious third unauthorized access of the data historian by a malicious third unauthorized access of the data historian by a malicious third unauthorized access of the data historian by a malicious third unauthorized access of the data historian by a malicious third unauthorized access of the data historian by a malicious third unauthorized access of the data historian by a malicious thi	1	2	#4-16	155,156,1 7
159 Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes". Unauthorized access of the HMI from the data historian by a malicious third	2			
	2			
160 party. * Unauthorized access includes *execution of unauthorized processes*.	2			
Infection of the HMI with destructive malware (ransonware, etc.) by a malicious third party. This prevents the monitoring of the control system.     2     2     1     D	1	2	#4-17	158,159,10 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*.	1			
163     4-4               Data destroyed by destructive malware (ransomware, etc.). This prevents the monitoring of the control system.      2     3     1              Destar (a fragment) Access Control               Device Error Detection               Data Backup                 Auti-Virus               Access               Access               Device Error Detection               Data Backup	1	1	#4-18	162,163
Image: Note that the second of a second s	1	21212121212121212121		
166       1000 connection to unauthorized media".       2000 connection to the HML Data destroyed by destructive malware (ransomware, etc.). This prevents the monitoring of the control system.       2       3       1       Anti-Virus       Anti-Virus       Anti-Virus       Anti-Virus       Device Error Detection       Data Backup         1000       A-44       A-44       Anti-Virus       Anti-Vir	1	1	#4-19	164,165
X         Data Signature         I		0-		

[Note]
\*11 t 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.

#### 5. Leak of Confidential Information

₹ /	Attack	k Scenario		Assessm	ent Metrics			Countern	neasures		Securit	y Level	Attack 1	Free Numbe
ž							Prot	tection	Detection/				Attack	Configurati
Item Number		Attack Tree/Attack Steps T	Threat Level	Vuinerability Level	Business Impact Level	Risk Value	Intrusion/ Spreading Phase	Objective Achievement Phase	Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Tree Number	Steps (ite Number)
•	5-1	Theft of company production secrets stored on the control system, res	<mark>sulting in an</mark>	external info	ormation leak.									
66		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 ite	m number 1		2 *1			
57		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			
38	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) (Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis		2	2	#5-1	166,167 8
<b>59</b>		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			
0	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) (Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#5-2	166,16 0
'1		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. <sup>1</sup> Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasure 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			
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 ite	m number 5		2			
3		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".						Same as iter	n number 31		2			
<b>′</b> 4	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 iten	n number 168		1	2	#5-3	171,17 3,17
75		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	·	1			
76	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 iten	n number 170		1	2	#5-4	171,17: 5,17
<														

\*11 tis recommended to refer to "Section 9.4 Firewall Settings" in the Guide for evaluating countermeasures.
 \*21 tis 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

ľ	Attack	<mark>CScenario</mark>			Assessme	ent Metrics	1			ermeasures			Securit	y Level	Attack T	ree Numbe
			Attack Tree/Attack Steps	Threat Level	Vuinerability Level	Business Impact Level	Risk Value	Prote Intrusion/ Spreading Phase	Objective Achievem Phase	Detection/ ent Understanding Damage	Business Continu	ity	Attack Steps	Attack Tree	Attack Tree Number	Configurati Steps (ite Number)
	1-1 1-2		area supply outage caused by the use of wide area sup area supply outage caused by supply outage command			ontrollers.										
:	2-1 2-2	2-2: Outbrea	ak of fires and explosions due to control abnormalities in ak of fires and explosions due to control abnormalities in	n facilities for h	nandling haza	ardous mater	ials caused b	y the malicious modifica	ation of settings (thre			-				
	2-3 2-4 3-1	2-4: Outbrea	ak of fires and explosions due to erratic behavior in facil ak of fires and explosions caused by a loss of monitorin tion of a product that does not meet quality standards/cr	g and monitor	ring control at	facilities for	handling haza	ardous materials due to	congestion in the co	ntrol network (field side).	se, even when ope	eration	is are pe	normed co	mecuy.	
	3-2 3-3	3-3: Product	tion of a product that does not meet quality standards/cr tion of a product that does not meet quality standards/cr	riteria due to c	ontrol abnorr	malities in pro	oduction facili	ties caused by tamperin	<mark>g with and altering d</mark>		or tampering with a	nd alte	ering pro	grams.		
	4-1 4-2 4-3	4-2: Control	I abnormalities in production facilities caused by the setti I abnormalities in production facilities caused by the mali ional abnormalities in production facilities caused by tan	icious modific	ation of settir	ngs (threshold	ds, etc.) or tar	mpering with and altering	programs. This lea		ninated for safety r	easor	ns.			
	4-4 5-1	4-4: A destru	uctive malware or ransomware infection that disables m f company production secrets stored on the control syst	ionitoring of p	roduction fac	ilities and pre	vent monitori				S.					
		Unauthorized firew	<pre>tolnt = Information Network wall access by a malicious third party. ccess includes "execution of unauthorized processes" (privilege escalation).</pre>					FW o Peer-to-Peer Authentication 0 Applying Patches 0		IPS/IDS Log Collection/Log Analysis Integrated Log Management System			2			
		Countermeasures of unauthorized pr	s used for the two threats are merged. Italic text is used to denote the "execution rocesses".					Avoidance of Vulnerability Permission Management Peer-to-Peer Authentication O	(Same as on the left)	Device Alive Monitoring			*1			
2			authorized access of the HMI via the FW by a malicious third party. nauthorized access includes "execution of unauthorized processes"					Applying Patches Avoidance of Vulnerability		Log Collection/Log Analysis Integrated Log Management System			2			
3	2-3		Tampering with and altering data/software in the HMI by a	2	2	3	в	Permission Management Permission Management Access Control	(Same as on the left) (Same as on the left)	Device Alive Monitoring Device Error Detection Log Collection/Log Analysis	Data Backup		1	2	#1-1	1,2,3
=			malicious third party. Tampering with and altering data/software in the HMI by a					Data Signature	(Same as on the left)	Integrated Log Management System						
•	3-3		malicious third party.	2	2	2	С		Same as	; item number 3		_	1	2	#1-2	1,2,4
;	4-3		Tampering with and altering data/software in the HMI by a malicious third party.	2	2	1	D			item number 3			1	2	#1-3	1,2,5
6	4-4		Infection of the HMI with destructive malware (ransomware, etc.) by a malicious third party. This prevents the monitoring	2	2	1	D	Anti-virus Application Whitelisting Applying Patches	Permission Management Access Control	Device Error Detection Device Alive Monitoring Log Collection/Log Analysis	Data Backup		1	2	#1-4	1,2,6
			of the control system.					Avoidance of Vulnerability Data Signature		Integrated Log Management System						
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 Integrated Log Management System			1	2	#1-5	1,2,7
в	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	Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System			1	2	#1-6	1,2,8
,	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 HM by a malicious third party.	2	2	2	с		Same as	item number 8			1	2	#1-7	1,2,9
0	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 MM by an analicous third party.	2	2	1	D		Same as	; item number 8			1	2	#1-8	1,2,1
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 a	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	#1-9	1,2,1
╡			malicious third party. This prevents the monitoring of the control system. Infection of the HMI with malware by a malicious third party					Data Signature Anti-virus	(Same as on the left)	Device Error Detection						
2	2-4		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		Device Alive Monitoring Log Collection/Log Analysis Hitegrated Log Management Bystem			1	2	#1-10	1,2,1
╡			authorized access of the control server via the FW by a malicious					Data Signature Peer-to-Peer Authentication Applying Patches		IPS/IDS Log Collection/Log Analysis						
3		* Un	d party. nauthorized access includes "execution of unauthorized processes" vilege escalation).					Permission Management Application Whitelisting O	(Same as on the left) (Same as on the left)	htterated Log Management System Device Alive Monitoring			2			
4	2-3		Tampering with and altering data/software in the control server by a malicious third party.	2	2	3	В	Permission Management O Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Httgrated Log Management System	Data Backup		2	2	#1-11	1,13,1
5	3-3		Tampering with and altering data/software in the control server by a malicious third party.	2	2	2	с		Same as	item number 14			2	2	#1-12	1,13, <i>1</i>
6	4-3		Tampering with and altering data/software in the control server by a malicious third party.	2	2	1	D		Same as	item number 14			2	2	#1-13	1,13,
7	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	(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis http://www.collection/Log Management System			1	2	#1-14	1,13,1
8	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 thrift party.	2	2	3	В	DLP Segmentation/Zoning Data Signature Approval of Important Operations	(Same as on the left) (Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis http://www.collection/Log Management System			1	2	#1-15	1,13,1
9	3-1		Production of a product that does not meet quality standards/criteria due to the setting of inappropriate target values for the controller from the control server by a malicious third party.	2	2	2	с	yesses and the second s		item number 18	<u> </u>		1	2	#1-16	1,13, <i>1</i>
0	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	2	2	1	D	I	Same as	item number 18	11	+	1	2	#1-17	1,13,2
			malicious third party.					Peer-to-Peer Authentication O		IPS/IDS Log Collection/Log Analysis						
:1			nauthorized access includes "execution of unauthorized processes" vilege escalation).					Permission Management Application Whitelisting	(Same as on the left) (Same as on the left)	Hegrated Log Management System Device Alive Monitoring			1			
2	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	(Same as on the left) (Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System			1	2	#1-18	1,21,
3	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,
4	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			item number 23			1	2	#1-20	1,21,
5	4-2		A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software	2	2	1	D		Same as	item number 23		+	1	2	#1-21	1,21,
6			in controller from the EWS. Tampering with and altering data/software in controller (M)					Permission Management Access Control	(Same as on the left) (Same as on the left)	Device Error Detection	Data Backup		1			
.0	1-2		from the EWS by a malicious third party. Issuing of commands to stop the controller (S) via the controller (M) by a malicious third party. Supply outage	2	2	3	в	Data Signature Segmentation/Zoning Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)				1	2	#1-22	1,21,26
'	2		encompassing a wide area.					Approval of Important Operations	(Same as on the left)					-		.,21,20
				Here and the second	l i i i i i i i i i i i i i i i i i i i											

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

		a Product Supply Outage, 2 <mark>Scenario</mark>	. Occurrence of Fires and E	•		. Supply of ant Metrics		Products, 4. Ma		iction Disrupt/Suspe termeasures	end, 5. Leak of Co		l Informa urity Leve		Tree Number
		Attack Tree//	Attack Steps	Threat Level	Vuinerability Level	Business Impact Level	Risk Value	F Intrusion/ Spreading Phase	Protection Objective Achieven e Phase	Detection/ nent Understanding Damage	Business Continu	ity Attac Step		Attack Tree Number	Configuration Steps (item Number)
	1-1 1-2		aused by the use of wide area sup aused by supply outage command			ontrollers.		oproading r has		Damago				Humber	
ltem N	2-1 2-2	2-2: Outbreak of fires and explosion		facilities for h	nandling haza	ardous materi	als caused b	y the malicious mo	dification of settings (th			-	a na da ma	d oomootly.	
Number	2-3 2-4 3-1	<ul><li>2-3: Outbreak of fires and explosit</li><li>2-4: Outbreak of fires and explosit</li><li>3-1: Production of a product that d</li></ul>	ons caused by a loss of monitoring	g and monitori	ing control at	facilities for h	nandling haza	irdous materials du	e to congestion in the	control network (field sid		erations a	е репогте	a correctly.	
	3-2 3-3	3-3: Production of a product that d	loes not meet quality standards/cri loes not meet quality standards/cri	iteria due to c	ontrol abnorr	nalities in pro	duction facilit	ies caused by tam	pering with and altering	<b>0</b> (	tc.) or tampering with	and alterin	g programs		
	4-1 4-2 4-3	4-2: Control abnormalities in produ	uction facilities caused by the settin uction facilities caused by the malic production facilities caused by tam	cious modifica	ation of settin	ngs (threshold	s, etc.) or tar	npering with and all	tering programs. This le		terminated for safety	reasons.			
	4-4 5-1	4-4: A destructive malware or rans 5-1: Theft of company production						ng control. This lead	ds to processes being	terminated for safety rea	asons.				
28		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from * Unauthorized access includes "execution of unauth Countermeasures used for the two threats are merge	norized processes" (privilege escalation).					Applying Patches Avoidance of Vulnerability	•	Log Collection/Log Analysis Integrated Log Management System		2			
			ata historian from the data historian (relay)					Permission Management Peer-to-Peer Authentication Applying Patches	(Same as on the left)	Device Alive Monitoring IPS/IDS Log Collection/Log Analysis					
29			es "execution of unauthorized processes".					Avoidance of Vulnerability Permission Management Peer-to-Peer Authentication	0	Integrated Log Management System Device Alive Monitoring IPS/IDS		2			
30		malicious third party. * Unauthorized acce	ss of the HMI from the data historian by a ess includes "execution of unauthorized					Applying Patches Avoidance of Vulnerability		Log Collection/Log Analysis Integrated Log Management System		2			
31	2-3		g with and altering data/software in the	2	2	3	в	Permission Management	Same	Device Alive Monitoring		1	2	#2-1	28,29,30,3
			malicious third party.					1							1 28,29,30,3
32	3-3		malicious third party.	2	2	2	С		Same	as item number 3		1	2	#2-2	2
33	4-3		g with and altering data/software in the malicious third party.	2	2	1	D	1	Same	as item number 3		1	2	#2-3	28,29,30,3
34	4-4	(ransomw	of the HMI with destructive malware vare, etc.) by a malicious third party. This the monitoring of the control system.	2	2	1	D		Same	as item number 6		1	2	#2-4	28,29,30,3 4
35	1-1	malicious th	age encompassing a wide area caused by a hird party using wide area supply outage functions roller from the HMI.	2	2	3	В		Same	as item number 7		1	2	#2-5	28,29,30,3 5
36	2-1	due to the se	ontrol of facilities for handling hazardous materials atting of inappropriate target values for the controller I by a malicious third party.	2	2	3	В		Same	as item number 8		1	2	#2-6	28,29,30,3 6
37	3-1	standards/cri	of a product that does not meet quality iteria due to the setting of inappropriate target values aller from the HMI by a malicious third party.	2	2	2	С		Same	as item number 8		1	2	#2-7	28,29,30,3 7
38	4-1	emergency s the setting of HMI by a ma	es in the manufacturing facilities requiring an stop of the manufacturing/production system due to finappropriate target values to the controller from the allicious third party.	2	2	1	D		Same	as item number 8		1	2	#2-8	28,29,30,3 8
39	2-4	settings from	with and altering the control network (field side) the HMI to cause network congestion in the control a malicious third party. This prevents the monitoring I system.	2	2	3	В		Same a	as item number 11		1	2	#2-9	28,29,30,3 9
40	2-4	third party with the c control ne	of the HMI with malware by a malicious / to cause unauthorized communication ontrol network (field side) and prevent twork communications. This prevents oring of the control system.	2	2	3	В		Same a	is item number 12		1	2	#2-10	28,29,30,4 0
41		historian by a malicio	ss of the control server from the data ous third party. ass includes "execution of unauthorized					Peer-to-Peer Authentication Applying Patches Avoidance of Vulnerability	•	IPS/IDS Log Collection/Log Analysis relegated Log Management Bystem		1			
42	2-3	Tamperin	g with and altering data/software in the erver by a malicious third party.	2	2	3	В	Permission Management	Same a	Device Alive Monitoring		1	2	#2-11	28,29,41,4
43	3-3		g with and altering data/software in the rver by a malicious third party.	2	2	2	С		Same a	as item number 14		1	2	#2-12	28,29,41,4 3
44	4-3		g with and altering data/software in the erver by a malicious third party.	2	2	1	D		Same a	is item number 14		1	2	#2-13	28,29,41,4 4
45	5-1	third party	ata on the control server by a malicious /. n retrieved by following the reverse	2	2	3	В		Same a	is item number 17		1	2	#2-14	28,29,41,4 5
46	2-1	Abnormal co due to the se	ontrol of facilities for handling hazardous materials atting of inappropriate target values for the controller trol server by a malicious third party.	2	2	3	В		Same a	is item number 18		1	2	#2-15	28,29,41,4
47	3-1	standards/cri	of a product that does not meet quality iteria due to the setting of inappropriate target values oller from the control server by a malicious third party.	2	2	2	С		Same a	is item number 18		1	2	#2-16	28,29,41,4 7
48	4-1	of the manufac	in the manufacturing facilities requiring an emergency stop cturing/production system due to the setting of inappropriate to the controller from the control server by a malicious third	2	2	1	D		Same a	is item number 18		1	2	#2-17	28,29,41,4 8
49		a malicious third par * Unauthorized acce processes".	ess includes "execution of unauthorized						Same a	is item number 21		2			
50	5-1	party.	ata on the EWS by a malicious third n retrieved by following the reverse	2	2	3	В		Same a	is item number 22		1	2	#2-18	28,29,49,5 0
51	2-2	A malicious values) of c	third party modifies settings (such as threshold controller or tampers with and alters data/software from the EWS.	2	2	3	В		Same a	is item number 23		1	2	#2-19	28,29,49,5
52	3-2	threshold v	is third party modifies settings (such as values) of controller or tampers with and /software in controller from the EWS.	2	2	2	С		Same a	is item number 23		1	2	#2-20	28,29,49,5 2
53	4-2	threshold v	is third party modifies settings (such as values) of controller or tampers with and /software in controller from the EWS.	2	2	1	D		Same a	is item number 23		1	2	#2-21	28,29,49,5 3
54			g with and altering data/software in (M) from the EWS by a malicious third						Same a	is item number 26		1			
55	1-2		Issuing of commands to stop the controller (S) via the controller (M) by a malicious third party. Supply outage encompassing a wide area.	2	2	3	В		Same a	is item number 27		1	2	#2-22	28,29,49,5 4,55
x		Note] 1 It is recommended to refer to "Section 9.4 Fi	irewall Settings" in the Guide for evaluating co	ountermeasures.											

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

1-2         1           2-1         2           2-2         2           2-3         2           2-4         2           3-1         3           3-1         3           4-1         4           4-2         4           4-3         4           4-4-4         4           5-1         5           56	Scenario         Attack Tree/Attack Steps         1-1: A wide area supply outage caused by supply outage command         1-2: A wide area supply outage caused by supply outage command         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 control abnormalities in         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/crist         3-2: Production of a product that does not meet quality standards/crist         3-3: Production of a product that does not meet quality standards/crist         3-3: Production of a product that does not meet quality standards/crist         3-3: Production of a product that does not meet quality standards/crist         3-3: Production abnormalities in production facilities caused by the setti         4-2: Control abnormalities in production facilities caused by the malite         4-3: Operational abnormalities in production facilities caused by the malite         5-1: Theft of company production secrets stored on the control system         Attack Entry Polt = 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 "conn	Is being sent facilities for h facilities for handli g and monitor iteria due to c iteria due to c citeria due to c ong of imprope cious modific ipering with a onitoring of pl	Level inctions. to multiple co- handling haza ing hazardous ring control at control abnorm control abnorm control abnorm control abnorm re target value ration of settin and altering da roduction faci	Business Impact Level Indous materia rodous materia s materials wh facilities for ha nalities in proc nalities in proc as. This leads ggs (thresholds tat/software. T lities and prev	als caused b here the unau andling haza duction facilit duction facilit duction facilit to processe s, etc.) or tam his leads to tent monitorin tak.	y the malicious modification of settings (threshold thorized modification of data and programs pre- rdous materials due to congestion in the control es caused by the setting of improper target value es caused by the malicious modification of settin es caused by the malicious modification of settin es caused by tampering with and altering data/s s being terminated for safety reasons. upering with and altering programs. This leads to processes being terminated for safety reasons.         age control. This leads to processes being terminated Application Whitelisting       Dev Applying Patches	Detection/ Understanding Damage Business Continuity lis, etc.) or tampering with and altering pro- ents a proper response, even when oper network (field side). es. gs (thresholds, etc.) or tampering with ar oftware. processes being terminated for safety re	Attack Steps		Attack Tree Number	Free Number Configuration Steps (Item Number)
1-2       1         2-1       2         2-2       2         2-3       2         2-4       3         3-1       3         3-2       3         3-2       3         3-2       3         3-1       4         4-2       4         4-3       4         4-4       4         56       2-3         57       2-3         58       3-3         59       4-3         60       4-4         61       1-1	1-2: A wide area supply outage caused by supply outage command 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 control abnormalities in 2-3: Outbreak of fires and explosions caused by a loss of monitoring 3-1: Production of a product that does not meet quality standards/cri 3-2: Production of a product that does not meet quality standards/cri 3-2: Production of a product that does not meet quality standards/cri 4-1: Control abnormalities in production facilities caused by the settil 4-2: Control abnormalities in production facilities caused by the settil 4-3: Operational abnormalities in production facilities caused by the mali 4-3: Operational abnormalities in production facilities caused by the mali 4-4: A destructive malware or ransomware infection that disables med- 5-1: Theft of company production secrets stored on the control syste 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". Tampering with and altering data/software in the HMI by malware infection. Tampering with and altering data/software in the HMI by malware infection. Data destroyed by destructive malware (ransomware, etc.). This	s being sent facilities for f facilities for f facilities for f ties for handli g and monitor iteria due to c iteria due to c	to multiple co handling haza handling hazardous ring control at control abnorm control abnorm control abnorm er target value ation of settin nd altering da roduction faci in an external	Irdous materia Irdous materials wh facilities for hi- nalities in proc nalities in proc nalities in proc alities in proc s. This leads Igs (thresholds ta/software. T lities and prev information le	als caused b here the unau andling haza duction facilit duction facilit duction facilit to processe s, etc.) or tam his leads to tent monitorin tak.	/ the setting of improper target values.         / the malicious modification of settings (threshold thorized modification of data and programs previdues materials due to congestion in the control es caused by the setting of improper target values caused by the malicious modification of setting es caused by the malicious modification of setting escaused by tampering with and altering the target values, is being terminated for safety reasons.         pering with and altering programs. This leads to processes being terminated for safety reasons.         ng control. This leads to processes being terminated for safety measons.         Anti-virus       Dev         Application Whitelisting       Dev         Applying Patches       Ico	Is, etc.) or tampering with and altering pro- ents a proper response, even when oper network (field side). es. sgs (thresholds, etc.) or tampering with an oftware. processes being terminated for safety re- ted for safety reasons.	and altering p easons.			
item     2-1     2       2-2     2     2       3-1     3       3-2     3       3-2     3       3-4-1     4       4-2     4       4-2     4       4-3     4       57     2-3       58     3-3       59     4-3       60     4-4       61     1-1	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 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/cri     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     3-3: Production of a product that does not meet quality standards/cri     4-1: Control abnormalities in production facilities caused by the settil     4-2: Control abnormalities in production facilities caused by the malid     4-3: Operational abnormalities in production facilities caused by the malid     4-3: Operational abnormalities in production facilities caused by the malid     4-3: Operational abnormalities in production facilities caused by the malid     4-4: A destructive malware or ransomware infection that disables m     5-1: Theft of company production secrets stored on the control syste     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".     Tampering with and altering data/software in the HMI by malware     infection.     Tampering with and altering data/software in the HMI by malware     infection.     Data destroyed by destructive malware (ransomware, etc.). This	facilities for h facilities for handli g and monitor iteria due to c iteria due to c iteria due to c ng of imprope cious modific ipering with a onitoring of pr am, resulting i 2	handling haza handling hazardous ring control at control abnorm control abnorm er target value ation of settiin ind altering da roduction faci in an external	Irdous materia Irdous materials wh facilities for hi- nalities in proc nalities in proc nalities in proc alities in proc s. This leads Igs (thresholds ta/software. T lities and prev information le	als caused b here the unau andling haza duction facilit duction facilit duction facilit to processe s, etc.) or tam his leads to tent monitorin tak.	y the malicious modification of settings (threshold thorized modification of data and programs pre- rdous materials due to congestion in the control es caused by the setting of improper target value es caused by the malicious modification of settin es caused by the malicious modification of settin es caused by tampering with and altering data/s s being terminated for safety reasons. upering with and altering programs. This leads to processes being terminated for safety reasons.         age control. This leads to processes being terminated Application Whitelisting       Dev Applying Patches	ents a proper response, even when oper network (field side). es. ggs (thresholds, etc.) or tampering with an oftware. processes being terminated for safety re ated for safety reasons.	and altering p easons.		correctly.	
Number       2-3       2         3.1       3       3       3         3.3       3.3       3       4         4.1       4       4       4         4.2       4       4       4         56       2-3       8         57       2-3       8       8         58       3-3       9       9         59       4-3       9       9         60       4-4       4       4       9         61       1-1       1       1       1	2-3: Outbreak of fires and explosions due to erratic behavior in facili     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     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 mali     4-2: Control abnormalities in production facilities caused by the mali     4-3: Operational abnormalities in production facilities caused by the mali     5-1: Theft of company production secrets stored on the control syste     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".     Tampering with and altering data/software in the HMI by malware     infection.     Tampering with and altering data/software in the HMI by malware     infection.     Data destroyed by destructive malware (ransomware, etc.). This	ties for handli g and monitor iteria due to c iteria due to c iteria due to c cious modific pering with a conitoring of pr am, resulting 2 2	ing hazardous ring control at control abnorm control abnorm ontrol abnorm er target value ration of settin ind altering da roduction faci in an external	s materials wh facilities for ha nalities in prod nalities in prod es. This leads gs (thresholds ta/software. T lities and prev information le	nere the unau andling haza duction facilit duction facilit duction facilit to processe s, etc.) or tan his leads to rent monitorin tak.	thorized modification of data and programs preventions materials due to congestion in the control es caused by the setting of improper target values caused by the malicious modification of setting es caused by the malicious modification of setting es caused by the malicious modification of setting set of the set of th	ents a proper response, even when oper network (field side). es. ggs (thresholds, etc.) or tampering with an oftware. processes being terminated for safety re ated for safety reasons.	and altering p easons.		correctly.	
3-2       3         3-3       3         4-1       4         4-2       4         4-3       4         4-4       4         56       2-3         57       2-3         58       3-3         59       4-3         60       4-4         61       1-1	3-1: Production of a product that does not meet quality standards/cri         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         3-4: Control abnormalities in production facilities caused by the setti         4-2: Control abnormalities in production facilities caused by the malid         4-3: Operational abnormalities in production facilities caused by the malid         4-4: A destructive malware or ransomware infection that disables m         5-1: Theft of company production secrets stored on the control syste         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.         * A shis 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".         Tampering with and altering data/software in the HMI by malware infection.         Tampering with and altering data/software in the HMI by malware infection.         Data destroyed by destructive malware (ransomware, etc.). This	teria due to c iteria due to c iteria due to c iteria due to c ng of imprope cious modific pering with a onitoring of p em, resulting 2 2	control abnorm control abnorm control abnorm er target value cation of settin ind altering da roduction faci in an external	nalities in prod nalities in prod nalities in prod s. This leads gs (thresholds ta/software. T lities and prev information le	duction facilit duction facilit duction facilit to processe s, etc.) or tan "his leads to rent monitorin ak.	es caused by the setting of improper target valu es caused by the malicious modification of settin es caused by tampering with and altering data/s s being terminated for safety reasons. upering with and altering programs. This leads to processes being terminated for safety reasons. ig control. This leads to processes being termina Anti-virus Application Whitelisting Dev Applying Patches Ico	es. Igs (thresholds, etc.) or tampering with an oftware. processes being terminated for safety re- ated for safety reasons. Inter Enror Detection Ice Enror Detection Ice Alive Monitoring	easons.	rograms.		
3-3       3         4-1       4         4-2       4         4-3       4         56       2-3         57       2-3         58       3-3         59       4-3         60       4-4         61       1-1	3-3: Production of a product that does not meet quality standards/crif 4-1: Control abnormalities in production facilities caused by the settil 4-2: Control abnormalities in production facilities caused by the malie 4-3: Operational abnormalities in production facilities caused by tam 4-4: A destructive malware or ransomware infection that disables me 5-1: Theft of company production secrets stored on the control syste Attack Entry Polnt = 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". Tampering with and altering data/software in the HMI by malware infection. Tampering with and altering data/software in the HMI by malware infection. Tampering with and altering data/software in the HMI by malware infection. Data destroyed by destructive malware (ransomware, etc.). This	iteria due to c ng of imprope cious modific pering with a onitoring of pi em, resulting 2 2	control abnorm er target value ation of settin ind altering da roduction faci in an external	nalities in prod es. This leads gs (thresholds ta/software. T lities and prev information le	duction facilit to processe s, etc.) or tan "his leads to rent monitorin eak.	es caused by tampering with and altering data/s s being terminated for safety reasons. Inpering with and altering programs. This leads to processes being terminated for safety reasons. Ing control. This leads to processes being termina Anti-virus Dev Application Whitelisting Dev Applying Patches Log	oftware. processes being terminated for safety re ted for safety reasons.	easons.	rograms.		
4-2       4         4-3       4         4-3       4         5-3       5         57       2-3         58       3-3         59       4-3         60       4-4         61       1-1	4-2: Control abnormalities in production facilities caused by the mali 4-3: Operational abnormalities in production facilities caused by tam 4-4: A destructive malware or ransomware infection that disables me 5-1: Theft of company production secrets stored on the control syste 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". Tampering with and altering data/software in the HMI by malware infection. Tampering with and altering data/software in the HMI by malware infection. Tampering with and altering data/software in the HMI by malware infection. Data destroyed by destructive malware (ransomware, etc.). This	cious modific ipering with a onitoring of pr m, resulting i 2 2	ation of settin nd altering da roduction faci in an external	gs (thresholds ata/software. T lities and prev information le	s, etc.) or tan This leads to rent monitorin eak.	Anti-virus Applying Patches Constraints of the second seco	ited for safety reasons.				
4-4     4       5-1     5       56	4-4: A destructive malware or ransomware infection that disables meta-1: Theft of company production secrets stored on the control system of the secret store store of the secret store store of the secret st	onitoring of pr am, resulting 2 2	roduction faci in an external	lities and prev information le	<mark>ent monitorii</mark> ak.	Anti-virus Dev Application Whitelisting Dev Applying Patches Log	ice Error Detection				
56	Attack Entry Point = HMI         Due to human error by an insider, the HMI is infected with malware after being connected to a malware-infected USB storage device.         * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".         Tampering with and altering data/software in the HMI by malware infection.         Tampering with and altering data/software in the HMI by malware infection.         Tampering with and altering data/software in the HMI by malware infection.         Data destroyed by destructive malware (ransomware, etc.). This	2				Application Whitelisting Dev Applying Patches Log	ice 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 of a deliberate attempt at "connecting to unauthorized media". Tampering with and altering data/software in the HMI by malware infection. Tampering with and altering data/software in the HMI by malware infection. Tampering with and altering data/software in the HMI by malware infection. Tampering with and altering data/software in the HMI by malware infection. Data destroyed by destructive malware (ransomware, etc.). This	2	3	3		Applying Patches					
57     2-3       58     3-3       59     4-3       60     4-4       61     1-1	* 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". Tampering with and altering data/software in the HMI by malware infection. Tampering with and altering data/software in the HMI by malware infection. Tampering with and altering data/software in the HMI by malware infection. Data destroyed by destructive malware (ransomware, etc.). This	2	3	2			·····	*2			
57     2-3       58     3-3       59     4-3       60     4-4       61     1-1	Tampering with and altering data/software in the HMI by malware infection.         Tampering with and altering data/software in the HMI by malware infection.         Tampering with and altering data/software in the HMI by malware infection.         Data destroyed by destructive malware (ransomware, etc.). This	2	3	2			grated Log agement System	<u> </u>			
58       3-3         59       4-3         60       4-4         61       1-1	infection. Tampering with and altering data/software in the HMI by malware infection. Tampering with and altering data/software in the HMI by malware infection. Data destroyed by destructive malware (ransomware, etc.). This	2	3	2		Data Signature					
59     4-3       60     4-4       61     1-1	Infection. Tampering with and altering data/software in the HMI by malware infection. Data destroyed by destructive malware (ransomware, etc.). This			3	A	Same as item r	umber 3	1	1	#3-1	56,57
60 4-4 61 1-1	Data destroyed by destructive malware (ransomware, etc.). This	2	3	2	В	Same as item r	umber 3	1	1	#3-2	56,58
61 1-1			3	1	D	Same as item r	umber 3	1	1	#3-3	56,59
_		2	3	1	D	Same as item r	umber 6	1	1	#3-4	56,60
_											
62 2-1	Supply outage encompassing a wide area caused by malware triggering wide area supply outage functions from the HMI.	2	3	3	Α	Same as item r	umber 7	1	1	#3-5	56,61
_	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	Α	Same as item r	umber 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 r	umber 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 r	umber 7	1	1	#3-8	56,64
65 2-4	Tampering with and altering the control network (field side) settings from the HMI to cause network congestion in the control network by malware infection. This prevents the monitoring of the control system.	2	3	3	A	Same as item n	umber 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 n	umber 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".					Application Whitelisting O Dev Applying Patches Log	ice Error Detection Colection Colect	2 *2			
68 2-3	Tampering with and altering data/software in the control server by matware infection.	2	2	3	В	Same as item n	umber 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 n	umber 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 n	umber 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 n	umber 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 n	umber 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 n	umber 18	1	2	#3-16	67,73
74	Attack Entry PoInt=EWS Due to human error by an insider, the EWS is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it assumes that there is no threat of a deliberate attempt to					Application Whitelisting Dev Applying Patches Log	Ice Error Detection CelectionLog Analysis Int Log Management System				
	"connect to unauthorized media".					Avodance of vulnerability reages Data Signature					
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 r	umber 6	1	1	#3-17	74,75
76 2-2	A malware infection maliciously modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	3	3	A	Same as item n	umber 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 n	umber 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 n	umber 23	1	1	#3-20	74,78
79 2-4	Tampering with and altering the control network (field side) settings from the EWS to cause network congestion in the control network by malware infection. This prevents the monitoring of the control system.	2	3	3	A	Access Control (Same as on the left) Log	Icce Error Detection Data Backup Collection/Log Analysis Include Management System	1	1	#3-21	74,79
80 2-4	Malware infection causing unauthorized communication with the control network (field side), and preventing control network communications. This prevents the monitoring of the control system.	2	3	3	A	Permission Management (Same as on the left) Dev Access Control (Same as on the left) Log	Ice Error Detection Data Backup Collection/Log Analysis Edulus/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 n	umber 26	1			
	Issuing of commands to stop the controller (S) via the										
82 1-2	controller (M) by malware infection. Supply outage encompassing a wide area.	2	3	3	А	Same as item n	umber 27	1	1	#3-23	74,81,82

[Note] \*11 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

#### 1. Wide Area Product Supply Outage

F I	Attack	Scenario		Assessm	ent Metrics	<b>;</b>				Counte	ermeasures		Securit	y Level	Attack 1	Free Number
Kan Number		Attack Tree/Attack Steps	Threat Level	Vulnerability Level	Business Impact Leve	Risk \	/alue	F Intrusion/ Spreading Phase		oction Objective Achieveme Phase	Detection/ nt Understanding Damage	Business Continuity	Attack Steps	Attack Tree	Attack Tree Number	Configurati Steps (Iter Number)
•	1-1 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			ontrollers.											
		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						FW Peer-to-Peer Authentication Applying Patches Avoidance of Vulnerability	•		IPS/IDS Log Collection/Log Analysis Hegrated Log Management System Device Alive Monitoring		2 *1			
		used to denote the "execution of unauthorized processes".						Permission Management	0	(Same as on the left)	IPS/IDS					
		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			
;	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	3	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 Bystem		1	2	#1-1	1,2,3
,		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 triggated Log Management System Device Alive Monitoring		2			
		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 Analys is Integrated Log Management System	Data Backup	1			
;	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	3	Segmentation/Zoning Data Signature Approval of Important Operations		(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		1	2	#1-2	1,4,5
		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	0 0 0	(Same as on the left)	IPS/IDS Log Collection/Log Analysis Integrated Log Management System Device Alive Monitoring		2 *1			
		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	0		IPS/IDS Log Collection/Log Analysis Hitgrated Log Management System Device Alive Monitoring		2			
		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 tegrate( Log Management System Device Alive Monitoring		2			
)	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	3			Same a	is item number 3		1	2	#1-3	7,8,9,
1		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 http://dc.gov.org/analysis Device Alive Monitoring		2			
2		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			
3	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	3			Same a	is item number 6		1	2	#1-4	7,8,11, 3
1		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			
5	1-1	Supply outage encompassing a wide area caused by malware triggering wide area supply outage functions from the HMI.	2	3	3	A	<b>\</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 Bystem		1	1	#1-5	14,1
;		Attack Entry Point = EWS Due to human error by an insider, the EWS is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".						Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature			Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Hegrated Log Management System		1 *2			
,		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			
	1-2	Issuing of commands to stop the controller (S) via the controller (M) by malware infection. Supply outage encompassing a wide area.	2	3	3	A		Segmentation/Zoning Data Signature Approval of Important Operations		(Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis titegrated Log Management System		1	1	#1-6	16,17
:																

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

#### 2. Occurrence of Fires and Explosion Incidents

2.00		nce of Fires and Explosion Incidents		-											
	Attack	Scenario		Assessme	ent Metrics				measures		1	Security	y Level		ree Number
Item Nu		Attack Tree/Attack Steps	Threat Level	Vuinerability Level	Business Impact Level	Risk Value	Pro Intrusion/ Spreading Phase	tection Objective Achlevement Phase	Detection/ Understanding Damage	Business Continu		Attack Steps	Attack Tree	Attack Tree Number	Configuration Steps (Item Number)
Number	2-2 2-3	2-1: Outbreak of fires and explosions due to control abnormalities in 1 2-2: Outbreak of fires and explosions due to control abnormalities in 1 2-3: Outbreak of fires and explosions due to erratic behavior in faciliti 2-4: Outbreak of fires and explosions caused by a loss of monitoring	facilities for h ies for handlii	andling haza	ardous materi s materials w	ials caused b /here the una	y the malicious modifi uthorized modification	ication of settings (thres of data and programs	orevents a proper resp	ponse, even when o			erformed c	correctly.	
19		Attack Entry Point = Information Network Unauthorized firewall access by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".						Same as it	em number 1			2 *1			
20		Unauthorized access of the HMI via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".						Same as it	em number 2			2			
21	2-1	Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate target values for the controller from the HMI by a malicious third party.	2	2	3	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 Managament System			1	2	#2-1	19,20,21
22	2-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	3	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	#2-2	19,20,22
23	2-4	Tampering with and altering the control network (field side) settings from the HMI to cause network congestion in the control network by a malicious third party. This prevents the monitoring of the control system.	2	2	3	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	#2-3	19,20,23
24	2-4	Infection of the HMI with malware by a malicious third party to cause unauthorized communication with the control network (field side) and prevent control network communications. This prevents the monitoring of the control system.	2	2	3	В	Anti-virus Application Whitelisting Applying Patches Avoidance of Vulnerability Data Signature		Device Error Detection Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System			1	2	#2-4	19,20,24
25		Unauthorized access of the control server via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).					Peer-to-Peer Authentication  Applying Patches Permission Management Application Whitelisting	(Same as on the left) (Same as on the left) (Same as on the left)	IPS/IDS Log Collection/Log Analysis Integrated Log Management System Device Alive Monitoring Log Collection/Log Analysis			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)	Integrated Log Management System			1	2	#2-5	19,25,26
27	2-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	3	В	Permission Management O Access Control Data Signature	(Same as on the left) (Same as on the left) (Same as on the left)	Device Error Detection Log Collection/Log Analysis Integrated Log Management System	Data Backup		2	2	#2-6	19,25,27
28		Unauthorized access of the EWS via the FW by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation).						Same as it	em number 4	_		2			
29	2-2	A malicious third party modifies settings (such as threshold values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	3	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	19,28,29
30		Attack Entry Point = Monitoring Terminal Unauthorized access of the data historian (relay) from a monitoring terminal by a malicious third party. * Unauthorized access includes "execution of unauthorized processes" (privilege escalation). Countermeasures used for the two threats are merged. Italic text is used to denote the "execution of unauthorized processes".						Same as it	em number 7			2 *1			
31		Unauthorized access of the data historian from the data historian (relay) by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".						Same as it	em number 8			2			
32		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes". Abnormal control of facilities for handling hazardous materials						Same as it	em number 9			2			20.01.00.0
33	2-1	due to the setting of inapprovate target values for the controller from the HMI by a malicious third party. Tampering with and altering data/software in the HMI by a	2	2	3	В		Same as ite	m number 21			1	2	#2-8	30,31,32,3 3 <u>30,31,32,3</u>
34	2-3	malicious third party. Tampering with and altering the control network (field side)	2	2	3	В		Same as ite	m number 22			1	2	#2-9	4
35	2-4	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 ite	m number 23			1	2	#2-10	30,31,32,3 5
36	2-4	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 ite	m number 24			1	2	#2-11	30,31,32,3 6
37		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Peer-to-Peer Authentication         O           Applying Patches         Avoidance of Vulnerability           Permission Management         O		IPS/IDS Log Collection/Log Analysis Integrated Log Management System Device Alive Monitoring			2			20.04.07.0
38	2-1	Abnormal control of facilities for handing 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		Same as ite	m number 26			1	2	#2-12	30,31,37,3 8
39	2-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	3	В		Same as ite	m number 27			1	2	#2-13	30,31,37,3 9
40		Unauthorized access of the EWS from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes". A malicious third party modifies settings (such as threshold						Same as ite	m number 11			2			30,31,40,4
41	2-2	values) of controller or tampers with and alters data/software in controller from the EVVS.	2	2	3	В		Same as ite	m number 29			1	2	#2-14	1

#### 2. Occurrence of Fires and Explosion Incidents

Attac	k Sc	enario		Assessme	ent Metrics	,		Counte	rmeasures			Securi	ty Level	Attack	Free Number
		Attack Tree/Attack Steps	Threat Level	Vuinerability Level	Business Impact Level	Risk Value	Prot Intrusion/	tection Objective Achieveme	Detection/ nt Understanding	Business Contin	uity	Attack Steps	Attack Tree	Attack Tree	Configuration Steps (Iter
	_						Spreading Phase	Phase	Damage					Number	Number
2-1		1: Outbreak of fires and explosions due to control abnormalities in		-					abalda ata \ artama	arian with and alterian					
2-2 2-3		<ol> <li>Outbreak of fires and explosions due to control abnormalities in</li> <li>Outbreak of fires and explosions due to erratic behavior in facil</li> </ol>											performed	correctly	
2-4		4: Outbreak of fires and explosions due to enally behavior in facility		-							pera	tions are	Senonned	conectly.	
		ack Entry Point=HMI													
	Du	e to human error by an insider, the HMI is infected with malware after being													
		nnected to a malware-infected USB storage device.						Same as	item number 14			*2			
		s this is the result of actions by an insider, it is assumed that there is no threat a deliberate attempt at "connecting to unauthorized media".													
	-	Abnormal control of facilities for handling hazardous materials due to					Segmentation/Zoning	(Same as on the left)	Log Collection/Log Analysis						
2-1		the setting of inappropriate target values for the controller from the HMI	2	3	3	А	Data Signature	(Same as on the left)	Integrated Log Management System			1	1	#2-15	42,4
		by a malware infection.					Approval of Important Operations	(Same as on the left)				]			
		Tampering with and altering data/software in the HMI by malware	_	_		_	Permission Management	(Same as on the left)	Device Error Detection	Data Backup					
2-3		infection.	2	3	3	A	Access Control	(Same as on the left)	Log Collection/Log Analysis			1	1	#2-16	42,44
							Data Signature	(Same as on the left)	Integrated Log Management System	Data Daalaas					
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	2	3	3	А	Permission Management Access Control	(Same as on the left) (Same as on the left)	Log Collection/Log Analysis	Data Backup		1	1	#2-17	42,4
		the monitoring of the control system.	_	Ŭ	Ŭ		Data Signature	(Same as on the left)	Integrated Log Management System			1 .			,
							Anti-virus		Device Error Detection						
		Malware infection causing unauthorized communication with the control					Application Whitelisting		Device Alive Monitoring		~~~~~	1			
2-4		network (field side), and preventing control network communications.	2	3	3	A	Applying Patches		Log Collection/Log Analysis			1	1	#2-18	42,46
		This prevents the monitoring of the control system.					Avoidance of Vulnerability		Integrated Log Management System			j			
							Data Signature								
	Att	ack Entry Point = Control Server					Anti-virus		Device Error Detection						
		e to human error by an insider, the control server is infected with malware after					Application Whitelisting O		Device Alive Monitoring			2			
		ng connected to a malware-infected USB storage device.					Applying Patches		Log Collection/Log Analysis			*2			
		s this is the result of actions by an insider, it is assumed that there is no threat a deliberate attempt at "connecting to unauthorized media".					Avoidance of Vulnerability		Integrated Log Management System						
	-						Data Signature Segmentation/Zoning	(Same as on the left)	Log Collection/Log Analysis						
2-1		Abnormal control of facilities for handling hazardous materials due to the setting of inappropriate 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	47,4
		control server by a malware infection.	-	-	Ŭ	5	Approval of Important Operations	(Same as on the left)				1 .	-		,
							Permission Management O	(Same as on the left)	Device Error Detection	Data Backup					
2-3		Tampering with and altering data/software in the control server by malware infection.	2	2	3	В	Access Control	(Same as on the left)	Log Collection/Log Analysis			2	2	#2-20	47,49
							Data Signature	(Same as on the left)	Integrated Log Management System						
		ack Entry Point = EWS								·					
		e to human error by an insider, the EWS is infected with malware after being						Como os	to a success of C			1			
		nnected to a malware-infected USB storage device. s this is the result of actions by an insider, it is assumed that there is no threat						Same as	item number 16			*2			
		a deliberate attempt at "connecting to unauthorized media".													
							Permission Management	(Same as on the left)	Device Error Detection	Data Backup					
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	А	Access Control	(Same as on the left)	Log Collection/Log Analysis		1	1	1	#2-21	50,5
							Data Signature	(Same as on the left)	Integrated Log Management System						
		Tampering with and altering the control network (field side) settings from the EWS to					Permission Management	(Same as on the left)	Device Error Detection	Data Backup					
2-4		cause network congestion in the control network by malware infection. This prevents the monitoring of the control system.	2	3	3	A	Access Control	(Same as on the left)	Log Collection/Log Analysis			] 1	1	#2-22	50,52
		une monitoring or the control system.					Data Signature	(Same as on the left)	Integrated Log Management System						
•		Malware infection causing unauthorized communication with the control network (field	-	-	~		Permission Management	(Same as on the left)	Device Error Detection	Data Backup					F0 -
2-4		side), and preventing control network communications. This prevents the monitoring of the control system.	2	3	3	A	Access Control Data Signature	(Same as on the left) (Same as on the left)	Log Collection/Log Analysis			1	1	#2-23	50,53
	_						cara ognature	(outrie as on the left)	- Agreen Log mendgement bysem		-				
	ſ	Note]										4			
	:	room 1 It is recommended to refer to "Section 9.4 Firewall Settings" in the Guide for evaluating counter 2 It is recommended to refer to "Section 9 Security Measures for External Storage Media" in the (						<u> </u>							200

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

#### 3. Supply of Defective Product

3. 30		f Defective Pro	oduct													
Item Number	Attack	Scenario	Attacl	k Tree/Attack Steps	Threat Level	Vulnerability	Business	Risk Value	P Intrusion/ Spreading Phase	rotection Objective Achieveme	Ormeasures Detection/ Understanding Damage	Business Continuity	Securit Attack Steps	y Level Attack Tree	Attack T Attack Tree Number	Tree Number Configuration Steps (item Number)
mber				uct that does not meet quality standards/cr uct that does not meet quality standards/cr					es caused by the s	etting of improper targe		etc) or tampering with an	d altering p	rograms		
				uct that does not meet quality standards/cr												
54			cess by a ma ncludes "exe for the two th							Same as	s item number 1		2 *1			
55				ss of the HMI via the FW by a malicious third party. ess includes "execution of unauthorized processes".							s item number 2		2			
56	3-1		to the settin	of a product that does not meet quality standards/criteria due ag of inappropriate target values for the controller from the HMI ous 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 Bystem		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 Integrated Log Management System	Data Backup	1	2	#3-2	54,55,57
58		third party * Unautho	1.	ss of the control server via the FW by a malicious ess includes "execution of unauthorized processes" ).							item number 25		2			
59	3-1		to the settin	of a product that does not meet quality standards/criteria due g of inappropriate target values for the controller from the ere 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		ss of the EWS via the FW by a malicious third party. ess includes "execution of unauthorized processes" ).						Same as	s item number 4		2			
62	3-2		values) of	us third party modifies settings (such as threshold f controller or tampers with and alters data/software ler 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	ne data historia cludes "execut	ermInal 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	s item number 7		2 *1			
64		by a malic	cious third p	ss of the data historian from the data historian (relay) party. ess includes "execution of unauthorized processes".					Same as item number 8				2			
65		Vnauthorized access includes "execution of unauthorized processes".  Production of a product that does not meet quality						Same as	s 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 as	item number 57		1	2	#3-7	63,64,65,6 7
68			historian b	ized access of the control server from the data by a malicious third party. orized access includes "execution of unauthorized s". [Production of a product that does not meet quality						Same as	item number 37		2			
69	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	item number 59		1	2	#3-8	63,64,68,6 9
70	3-3			Tampering with and altering data/software in the control server by a malicious third party.	2	2	2	С		Same as	item number 60		1	2	#3-9	63,64,68,7 0
71			a maliciou * Unautho processes	I						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 2
73		connected to a make * As this is the result	by an insid ware-infect t of actions	der, the HMI is infected with malware after being ted USB storage device. Is by an insider, it is assumed that there is no threat necting to unauthorized media".						Same as	item number 14		1 *2			
74	3-1	due to the	e setting of	duct that does not meet quality standards/criteria inappropriate target values for the controller from are infection.	2	3	2	В		Same as	item number 56		1	1	#3-11	73,74
75	3-3	Tampering infection.	g with and	l altering data/software in the HMI by malware	2	3	2	В		Same as	item number 57		1	1	#3-12	73,75
76		to a malware-infected US	in insider, the SB storage d actions by a	e control server is infected with malware after being connected levice. In insider, it is assumed that there is no threat of a deliberate						Same as	item number 47		2 *2			
77	3-1	the setting		ct that does not meet quality standards/criteria due to briate target values for the controller from the control infection.	2	2	2	С		Same as	item number 59		1	2	#3-13	76,77
78	3-3	Tampering malware ii		altering data/software in the control server by	2	2	2	С		Same as	item number 60		1	2	#3-14	76,78
79		connected to a malw * As this is the result	by an insid ware-infect t of actions	der, the EWS is infected with malware after being ed USB storage device. by an insider, it is assumed that there is no threat necting 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 as	item number 62		1	1	#3-15	79,80
x																
	_										1	I	- 1			<u>, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,</u>

[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.

### 4. Manufacturing/Production Disrupt/Suspend

4. M		turing/Production Disrupt/Suspend		•									
ltem Nu	Attack	Scenario Attack Tree/Attack Steps	Threat Level	Assessme Vulnerability Level	Business Impact Level	Risk Value	C Protection Intrusion/ Objective Act Spreading Phase Phas		Business Continuity	Securit Attack Steps	y Level Attack Tree	Attack T Attack Tree Number	Cree Number Configuration Steps (Item Number)
Number		4-1: Control abnormalities in production facilities caused by the setting of improper 4-2: Control abnormalities in production facilities caused by the malicious modificat the set of the set of t	ion of settings (th	nresholds, etc.)	or tampering wi	th and altering p	rograms. This leads to processes being term	ninated for safety reasons.					
81		4-3: Operational abnormalities in production facilities caused by tampering with and     4-4: A destructive malware or ransomware infection that disables monitoring of pro     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 access of the HMI via the FW by a malicious third party.					ocesses being terminated for safety reason	Same as item number 1		2 *1			
82		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	_	_		_	Segmentation/Zoning (Same as on the lef			2	_		
83	4-1	inappropriate target values to the controller from the HMI by a malicious third party.	2	2	1	D	Data Signature (Same as on the lef Approval of Important Operations (Same as on the lef	)		1	2	#4-1	81,82,83
84	4-3	Tampering with and altering data/software in the HMI by a malicious third party.	2	2	1	D	Permission Management (Same as on the lef Access Control (Same as on the lef Data Signature (Same as on the lef Anti-virus Permission Managem	Log Collection/Log Analysis     vrtegraded Log Management System	Data Backup Data Backup Data Backup	1	2	#4-2	81,82,84
85	4-4	Infection of the HMI with destructive malware (ransomware, etc.) by a malicious third party. This prevents the monitoring of the control system.	2	2	1	D	Application WhiteInstring Access Control Applying Platches II Avaidance of Valuerability II Data Signature III	Device Alive Monitoring Log Collection/Log Analysis Integrated Log Management System		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).					5	Same as item number 25		2			
87	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the control server by a malicious third party.	2	2	1	D	Segmentation/Zoning (Same as on the lef Data Signature (Same as on the lef Approval of Important Operations (Same as on the lef	() Integrated Log Management System		1	2	#4-4	81,86,87
88	4-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	1	D	Permission Management O (Same as on the lef Access Control (Same as on the lef Data Signature (Same as on the lef	Log Collection/Log Analysis	Data Backup	2	2	#4-5	81,86,88
89		Unauthorized access of the EWS via the FW by a malicious third party.  * Unauthorized access includes "execution of unauthorized processes" (privilege escalaton).  A malicious third party modifies settings (such as threshold					Permission Management (Same as on the lef	Same as item number 4	Data Backup	1			
90	4-2	values) of controller or tampers with and alters data/software in controller from the EWS.	2	2	1	D	Access Control (Same as on the lef Data Signature (Same as on the lef	b) Log Collection/Log Analysis	Data Dackip	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".						2					
93		Unauthorized access of the HMI from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".							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 malicous third party.	2	2	1	D	5	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	Ę	Same as item number 84		1	2	#4-8	91,92,93,9 5
96	4-4	Infection of the HMI with destructive malware (ransomware, etc.) by a malicious third party. This prevents the monitoring of the control system.	2	2	1	D	5	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".					I [	Same as item number 37		2			
98	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the control server by a malicious third party.	2	2	1	D	ξ	1	2	#4-10	91,92,97,9 8		
99	4-3	Tampering with and altering data/software in the control server by a malicious third party.	2	2	1	D	Ę	1	2	#4-11	91,92,97,9 9		
100		Unauthorized access of the EWS from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".					Ę	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	5	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".					S	Same as item number 14		1 *2			
103	4-1	Abnormalities in the manufacturing facilities requiring an emergency stop of the manufacturing/production system due to the setting of inappropriate target values to the controller from the HMI by a malware infection.	2	3	1	D	Segmentation/Zoning (Same as on the lef Data Signature (Same as on the lef Approval of Important Operations (Same as on the lef	i) Integrated Log Management System		1	1	#4-13	102,103
104	4-3	Tampering with and altering data/software in the HMI by malware infection.	2	3	1	D	Permission Management (Same as on the lef Access Control (Same as on the lef Data Signature (Same as on the lef	b) Log Collection/Log Analysis	Data Backup	1	1	#4-14	102,104
105	4-4	Data destroyed by destructive malware (ransomware, etc.). This prevents the monitoring of the control system.	2	3	1	D	Anti-virus Permission Manage Application Whitelisting Access Control Applying Patches Audiance of Vulnerability Data Signature E	ment Device Error Detection Device Alive Monitoring Log Collecton.Log Analysis Haywel Log Mangement Bystem	Data Backup	1	1	#4-15	102,105
106		Attack Entry Point = Control Server Due to human error by an insider, the control server is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate						Same as item number 47		2 *2			
107	4-1	attempt at "connecting to unauthorized media". 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 (Same as on the lef Data Signature (Same as on the lef Approval of Important Operations (Same as on the lef	() Integrated Log Management System		1	2	#4-16	106,107
108	4-3	Tampering with and altering data/software in the control server by malware infection.	2	2	1	D	Permission Management O (Same as on the lef Access Control (Same as on the lef Data Signature (Same as on the lef	) Log Collection/Log Analysis	Data Backup	1	2	#4-17	106,108
109		Attack Entry Point = EWS Due to human error by an insider, the EWS is infected with malware after being connected to a malware-infected USB storage device. * As this is the result of actions by an insider, it is assumed that there is no threat of a deliberate attempt at "connecting to unauthorized media".					5	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 lef Access Control (Same as on the lef Data Signature (Same as on the lef	) Log Collection/Log Analysis	Data Backup	1	1	#4-18	109,110
111	4-4	Malware infection of the HMI. Data destroyed by destructive malware (ransomware, etc.). This prevents the monitoring of the control system.	2	3	1	D	Anti-vhus Permission Managu Application Whitelisting Access Control Applying Patches Avoidance of Vulnerability Data Signature D	ment Device Error Detection Device Alive Monitoring Log CollectionLog Analysis Integrate Log Management System	Data Backup	1	1	#4-19	109,111
x		[Note] 1 It is recommended to refer to "Section 9.4 Firewall Settings" in the Guide for evaluating cou 2 It is recommended to refer to "Section 9.5 sentity Manuscree for Externet Storage Media" to 1											
		*2 It is recommended to refer to "Section 9 Security Measures for External Storage Media" in t	ne Guide for evalua	aung countermeas	urës.								

### 5. Leak of Confidential Information

Item	Attack	s Scenario		Assessme	ent Metrics			Counterr	neasures		Securit	y Level	Attack T	ree Number
J Z				Vulnerability	Business	]	Pro	otection	Detection/		Attack	Attack	Attack	Configuration
Number		Attack Tree/Attack Steps	Threat Level	Level	Impact Level	Risk Value	Intrusion/ Spreading Phase	Objective Achievement Phase	Understanding Damage	Business Continuity	Steps	Тгее	Tree Number	Steps (Item Number)
ě,	5-1	5-1: Theft of company production secrets stored on the control syste	em, resulting i	n an externa	I information	leak.								
12		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".						Same as ite	em number 1		2 *1			
13		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	m number 25		2			
14	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) (Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analysis Integrated Log Management System		2	2	#5-1	112,113,1 4
15		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 4		1			
16	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) (Same as on the left) (Same as on the left) (Same as on the left)	Log Collection/Log Analys is Integrated Log Management System			2	#5-2	112,115,1 6
17		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 7		2 *1			
18		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 8		2			
19		Unauthorized access of the control server from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".						Same as iter	m number 37		2			
120	5-1	Theft of data on the control server by a malicious third party. (Data then retrieved by following the reverse route.)	2	2	3	В		Same as iten	n number 114		1	2	#5-3	117,118,1 9,120
121		Unauthorized access of the EWS from the data historian by a malicious third party. * Unauthorized access includes "execution of unauthorized processes".						Same as iter	m number 11		2			
122	5-1	Theft of data on the EWS by a malicious third party. (Data then retrieved by following the reverse route.)	2	2	3	В		Same as iten	n number 116		1	2	#5-4	117,118,1 1,122
x		[Note] •1 It is recommended to refer to "Section 9.4 Firewall Settings" in the Guide for evaluating counter	ermeasures.								-			

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 impactbased risk analysis.

[Output 4.4]

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

Risk Value	Total Number of Attack Trees		Business Impact Scenario	Number of Attack Trees (By Business Scenario)
		1	Wide Area Product Supply Outage	2
A	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
В	29	3	Supply of Defective Product	3
		5	Leak of Confidential Information	4
С	12	3	Supply of Defective Product	12
D	D 19		Manufacturing/Production Disrupt/Suspend	19
E	0		-	0

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

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	А	HMI (Physical Intrusion)	4	0
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	E	(Omitted)	0	0

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

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

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

[Output 5.1①]

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

#	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	- нмі	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		after being connected to a malware- infected USB storage device.	B Applicable Tree = 1 (Table 4-12#6)		(Vulnerability Level 3 -> 2)	C Applicable Tree = 1
3		Due to human error by an insider, the EWS is infected with malware	A Applicable Trees = 5 (Table 4-12#2)	N 1	Applying whitelist	B Applicable Trees = 5
4	EWS	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)		<ul> <li>(Proposal 1)</li> <li>Strengthening firewall administrator authentication.</li> <li>Applying additional countermeasures, such as restricting screen access to access attempts that pass through a secure jump server, and using two-factor authentication.</li> <li>(Vulnerability Level 2 -&gt; 1)</li> <li>(Proposal 2)</li> <li>Shifting the administrator interface from the information network to the control network, and blocking firewall access from the information network.</li> <li>(Vulnerability Level 2 -&gt; 1)</li> <li>* This assumes that firewall patch updates can be applied offline.</li> </ul>	C Applicable Trees = 11
6		Unauthorized access of assets on the control network via the data historian (relay) in the DMZ by a malicious third party.	B Applicable Trees = 11 (Table 4 <sup>-</sup> 12#4)	<ul> <li>Keeping communication connections to an absolute minimum (IP packet level restrictions)</li> </ul>	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)	<ul> <li>Application whitelisting to restrict the execution of unauthorized processes.</li> </ul>	(No additional countermeasures)	B Applicable Trees = 2

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

[Output 5.12]

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

Risk Value	Current Number of Attack Trees	Number of Attack Trees after Improvements
А	9	0
В	27	11
С	12	27
D	19	17
E	0	12

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

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

		Who	From Where		How					В	efore Cour	ntermeasur	es	A	After Counter	ermeasure	€S
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. <u>https://www.ipa.go.jp/security/controlsystem/riskanalysis.html</u>





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/