Edgecross

Security Guidelines for Users, Detailed Version

Ver. 1.0.0

Edgecross Consortium Technical Meeting Security Guideline Formulation WG

ECD-TE4-0006-01-EN

Technical Meeting Security Guideline Formulation WG

Participants (titles omitted, random order)

TACHIBANA ELETECH CO., LTD.

DMG MORI CO., LTD.

NEC Corporation

Hitachi, Ltd.

FUJITSU LIMITED.

Mitsubishi Electric Corporation

McAfee Co., Ltd

Microsoft Japan K.K.

DELTA ELECTRONICS (JAPAN), INC.

Trend Micro Co., Ltd.

Revision History

Ver.	Revisions	Issue Date
1.0.0	First edition	June, 2020

Table of Contents

1. Introduction

1.1 Overview

Nowadays, the manufacturing industry is accelerating the use of IoT(Internet of Things) to strengthen competitiveness and create new value. "Edgecross Consortium" is based on this era, transcending the boundaries between enterprises and industries, and is jointly built by members of the consortium, thus providing an open software platform "Edgecross" in the field of Japanese edge computing coordinated with FA (Factory Automation) and IT (Information Technology). Through the coordination between FA and IT, it is expected to improve the productivity of the factory, but on the other hand, the threat of attacks inside and outside the FA system will also increase. In order to reduce threats, it is best to consider implementing various policies on people, physics and even connected networks on multi-layer networks.

Based on the specific threats envisaged in a typical Edgecross use case, this book presents security considerations when building a FA system using Edgecross as a guideline for security and reassurance. As a security measure recommended for customers to import, the key points summarized from hardware /OS, security software, Edgecross basic software and network viewpoint will be more detailed than those described in the summary version.

1.2 Scope of this document

As the target readers of this document, we expect to be the technicians, managers and operators of the Edgecross system.

This book embodies the guidelines for security measures for Edgecross systems based on the IoT Security Guidelines published by the IoT Promotion Consortium, the Ministry of Internal Affairs and Communications, and the Ministry of Economy, Trade and Industry.

Table 1-1 lists the key points of the Security Guidelines and how to respond to the sections in this document.

Table 1-1 **Key Points and applicable passage of Security Guidelines**

"IoT Security Guidelines" ver 1.0 (IoT Acceleration Consortium/ Ministry of Internal Affairs and Communications / Ministry of Economy, Trade and Industry) Security Countermeasure Guide List			applicable passage in this document
Major Items	**Guidelines**	**Key Points**	
Policy	Guideline 1 Establish a basic policy that takes into account the nature of IoT	Key Point1. Management commits to IoT security	1.3
		Key Point 2. Guard against internal non-compliance or mistakes	1.3
Analysis	Guideline 2 Recognize the risks of IoT	Key Point 3. Specify what to protect	2.2
		Key Point 4. Imagine the risks arising from the connection	2.3, 2.5
		Key Point 5. Imagine the risks affected by the connection	2.3, 2.5
		Key Point 6. Understand physical risks	2.3, 2.5
		Key Point 7. Learn from past examples	2.4
Design	Guideline3 Think about a design to protect what you need to protect	Key Point 8. Use designs that can be protected individually or as a whole	3.1
		Key Point 9. Use designs that don't bother each other	3.1
		Key Point 10. Adopt the conformity design that realizes safe and secure	3.1
		Key Point 11. Use a design that can ensure safety and security even if it is connected to unspecified objects	3.1
		Key Point 12. Verify and evaluate the design to achieve safety and security	3.1
Build and Connect	Guideline4 Think about countermeasures on the network	Key Point 13. Set the function of mastering and recording the status of machines	3.2, 3.3, 3.4
		Key Point 14. Make proper network connection according to function and purpose	3.2, 3.3, 3.4, 3.5
		Key Point 15. Notice initial setting	3.2, 3.3, 3.4, 3.5
		Key Point 16. Import authentication function	3.2, 3.3
Operation and Maintenance	Guideline5 Maintain a safe and secure state, and send and share information	Key Point 17. Maintain a safe and secure state after delivery and release	4.1
		Key Point 18. Once shipped and released, be aware of IoT risks and communicate what you expect related personnel to follow	4.2
		Key Point 19. Let the general user know the risks through the connection	4.2
		Key Point 20. Recognize the role of relevant personnel in IoT system service	4.2
		Key Point 21. Identify vulnerable equipment and alert appropriately	4.2

In addition, as a security document related to FA, there are also security standards IEC62443 of the control system, so please refer to it if necessary.

1.3 Basic Policy

1.3.1 Cybersecurity Management

In cyber security measures for systems utilizing IoT, it is important to establish a basic policy that takes into account the nature of IoT systems. Security measures can be costly, and it is expected that they will face situations where decisions beyond the discretion of the operating floor are required. Therefore, it is necessary for the level of management to take the initiative in presenting the policy of security measures.

Security measures require the establishment of a system for various parties to cooperate and respond, and the development of human resources who can utilize security technologies. In addition, it is necessary to respond to human threats such as the possibility of internal fraud that threatens safety and unintentional errors.

Please work as an organization on security measures by referring to the "Cyber Security Management Guidelines" published by the Information Processing Promotion Agency of the Ministry of Economy, Trade and Industry.

In addition, the Edgecross Consortium provides security information about edgecross systems, so please also refer to it.

1.3.2 Edgecross Consortium

As an organization that promotes the spread of platforms for the development of industry, the Edgecross Consortium will make three initiatives in its core efforts to contribute to the maintenance and improvement of safety and security in the operational environment.

・Building an organization and structure to ensure safety and security

The Consortium has established a system to respond quickly to security issues and cooperate with JPCERT/CC in the event of a security incident to provide prompt response and information to customers. In addition, we will investigate threat trends, technologies, systems, etc., and strive to disseminate information to the consortium member companies and customers in order to maintain correct knowledge and high awareness of security.

・Achieve safe and secure product development

Together with member companies, the Consortium analyzes the assets to be protected and possible threats, designs robust products, develops developer security guidelines, and develops products to ensure that appropriate security measures are taken so that they can remain safe and secure after shipment and release.

・Provide security guidelines for customers

The Consortium believes that it is desirable to take a multi-layer of human, physical, network, and other measures to reduce threats. For this reason, the consortium provides security guidelines for the proper operation of FA systems with Edgecross-enabled products to help implement and maintain security measures in the operational environment of Edgecross.

1.4 Abbreviations

BIOS	Basic Input Output System
C&C	Command and Control
CPU	Central Processing Unit
CSV	Comma Separated Values
DB	Data Base
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DMZ	DeMilitalized Zone
DoS	Denial of Service
ERP	Enterprise Resources Planning
EWS	Engineering WorkStation
FA	Factory Automation
FW	FireWall
GW	GateWay
HDD	Hard Disk Drive
HMI	Human Machine Interface
ID	Identification
IPS	Intrusion Prevention System
I/F	Interface
IoT	Internet of Things
IP	Internet Protocol
IPA	Information-technology Promotion Agency
IT	Information Technology
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center
LAN	Local Area Network
MES	Manufacturing Execution System
MQTT	Message Queuing Telemetry Transport
NC	Numerical Control
OPC	OLE (Object Linking and Embedding) for Process Control
OPC UA	OPC Unified Architecture
OS	Operating System
OSS	Open Source Software
PC	Personal Computer
PIN	Personal Identification Number
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SD	Secure Digital
SNMP	Simple Network Management Protocol
SOC	Security Operation Center
TLS	Transport Layer Security
TPM	Trusted Platform Module
USB	Universal Serial Bus
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network
WWW	World Wide Web

1. 5 Terminology

The terms used in this book are shown in Table 1-2.

Table 1-2 Term

Term	Description
IT System	A system that uses IT to use data from the production site. This book refers to the external system connected with LAN and Internet at the production site.
Edgecross System	A system using Edgecross.
Edgecross Software	The general name of Edgecross basic software, edge application, data collector and IT gateway.
Edgecross Basic Software	Software that implements edgecross functionality. In conjunction with edge applications, it is possible to perform analysis and diagnosis of data at the production site, and to exchange data with on-premise-based and cloud IT systems.
PC Equipped with Edgecross	Industrial PC equipped with Edgecross basic software.
Edge Application	In the edge computing area, software that takes advantage of the functions provided by Edgecross to perform various processes for the utilization of data at the production site. In particular, this book refers to those that have passed the Edgecross Consortium certification exam and have been certified.
Data Collector	A software component that collects production site data through each network, provided by each vendor for various networks and connected devices.
IT Gateway	Software components provided by vendors that communicate with IT systems in order to use data from production sites.

1. 6 Related Materials

The related materials in this book are listed in Table 1-3.

Table 1-3 Related Materials

No.	Material Name	Material No	Access Method
1	IoT Safety Guidelines Ver 1.0 July 2016 IoT Promotion Consortium, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry	-	http://www.soumu.go.jp/main_content/000428393.pdf
2	Cybersecurity Management Guidelines Ver 1.0 December 2015 Information Processing Promotion Organization, Ministry of Economy, Trade and Industry	-	http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf
3	Edgecross Specifications Overview	ECD-TE1-0002	Edgecross Consortium Member Homepage
4	Edgecross Basic Software Windows User's Manual	ECD-MA1-0001	Marketplace (Edgecross Basic Software Windows Product Documentation)
5	Control System Security Risk Analysis Guide, 2nd Edition	-	https://www.ipa.go.jp/files/000069436.pdf
6	Cyber-Physical Security Framework Version 1.0 April 2019 Ministry of Economy	-	https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf

2. Edgecross System

This chapter provides system features, assets to protect, possible threats, and examples of security incidents.

2. 1 Features of the system

Edgecross is an open edge computing software platform for FA-IT coordination. In the field of edge computing, an ecosystem can be built by combining components from multiple vendors.

Edge computing processes data collected from the production site on the production site side. By running applications on industrial PCs that are physically close to the production site, you can realize a system that requires real-time response.

In addition, because IT systems are used to handle data at multiple sites and for long-term periods of time, edge computing enables seamless integration between production sites and IT systems.

2. 2 Assets to protect

Figure 2-1 shows the entire assets that Edgecross should protect. There are four main assets to protect against a variety of security threats: data, hardware/OS, Edgecross software and related software, and networks.

The data contains operation information, sensor information, data generated by machine tools, industrial robots and data required by NC program operation, but Edgecross does not process NC program, etc.

Hardware/OS includes industrial PCs, Windows OS, etc.

The Edgecross software products include Edgecross basic software to perform real-time data processing and data model management, edge applications such as operation monitoring to perform various processing by utilizing the data of the production site, data collector to collect the data of the production site through the FA network described below. There are IT gateways that enable seamless data integration with IT systems, middleware such as Mosquitto and OpenSSL. In addition, there is a development kit etc. as related software.

The network has a control network that transfers data from the production site, an FA network such as a field network, and an information network that works with IT systems such as MES and ERP.

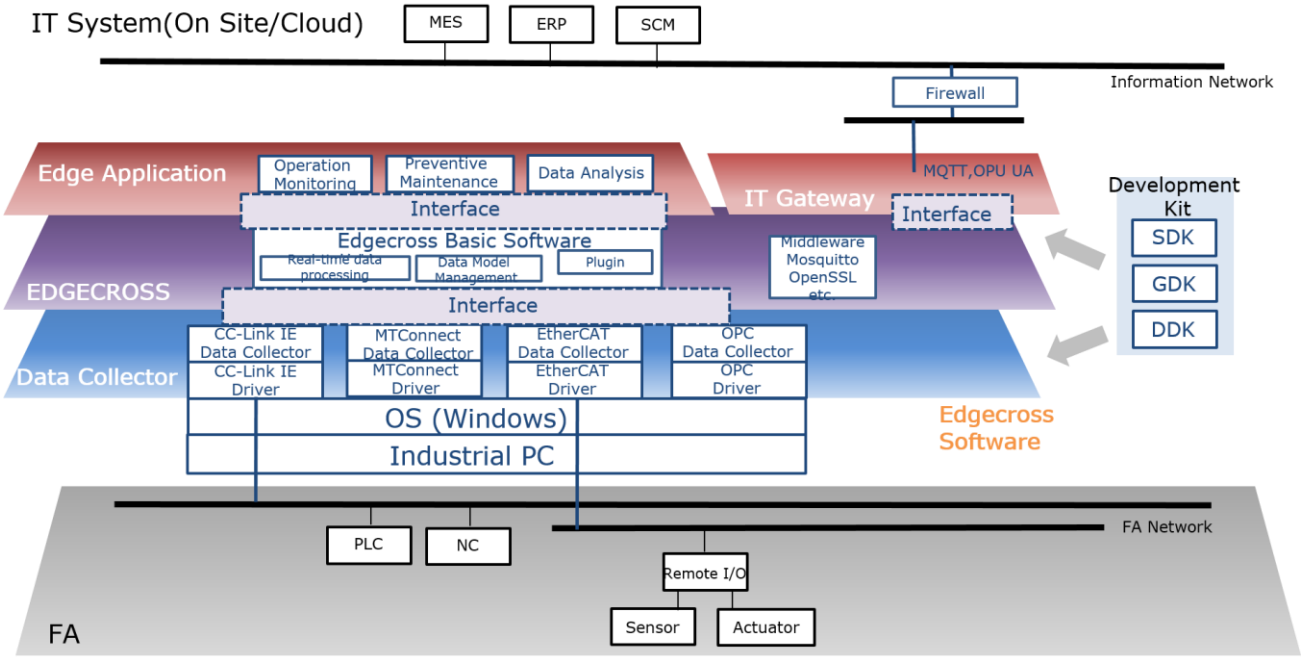


Figure 2-1 Assets to be protected in Edgecross

2. 3 Possible Threats

Lists the possible security threats for the preceding system. These threats are expected to result in product outages, fire accidents, and defective products.

(1) Spoofing

It is assumed that there is a threat that another user's Windows account (ID and password) is obtained illegally or illegally obtained and illegally logged into edgecross PC.

(2) Information theft

It is assumed that the data etc. of the production site collected by Edgecross basic software are read illegally. It also assumes a threat that Edgecross software will be read illegally from a PC with Edgecross.

(3) Malware

Assume that malware will be installed on a PC equipped with Edgecross.

(4) Unauthorized communication

Malware lurking in Edgecross pc is assumed to be a threat to illegally communicate with external devices.

(5) Tampering

Assume that the malicious software hidden on the PC equipped with Edgecross illegally rewrites the Edgecross software, which may threaten the function of the software. In addition, it is assumed that malicious software will illegally tamper with the data on the production site collected by Edgecross basic software, which may produce inappropriate statistical results and threaten to trigger the next processing improperly.

(6) A stepping stone to a high-load attack

A malware-infected Edgecross PC is expected to be used as a stepping stone to a DoS/DDoS attack on the server.

(7) Exploiting vulnerabilities

Vulnerabilities in the operating system and installed software are exploited to assume threats such as malware being installed on a PC with Edgecross.

(8) Physical attacks

Assume there is a threat of physical attacks such as physical intrusion by suspicious persons and theft of PCs equipped with Edgecross.

2. 4 Examples of security incidents in control systems

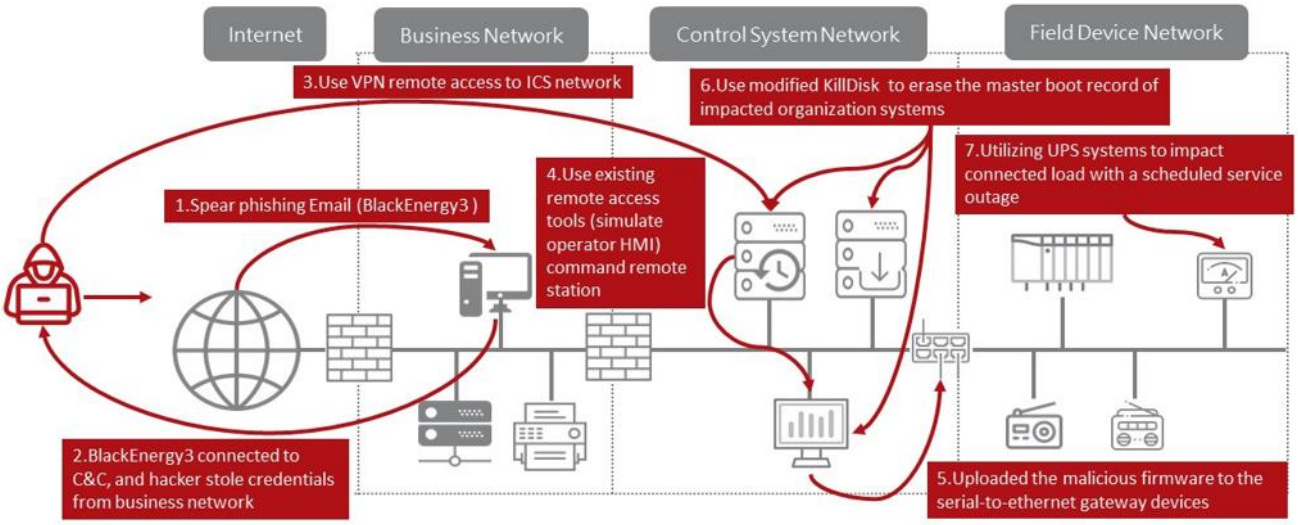
First of all, this is an incident case of a power generation facility that occurred in Ukraine.

In December 2015, three power companies in Ukraine were forced into unexpected power outages caused by multiple cyber attacks. The power outage lasted three hours and was reported to have affected about 250,000 customers.

The attacker took over the Virtual Private Network (Virtual Private Network, VPN) to gain access to the SCADA network and control the power generation facility. This not only drove customers into power outages, but also made the operation of the facility inoperable.

This case shows that even in a control system environment that is not directly connected to the Internet, it can be damaged by a cyber attack.

In a factory environment where edgecross systems are located, you may not be connected to the Internet as well. You must recognize that there are still security risks, even in offline environments, and take security measures to prevent damage.



(Source: Trend Micro Threat Database Security Blog https://blog.trendmicro.co.jp/archives/14203)

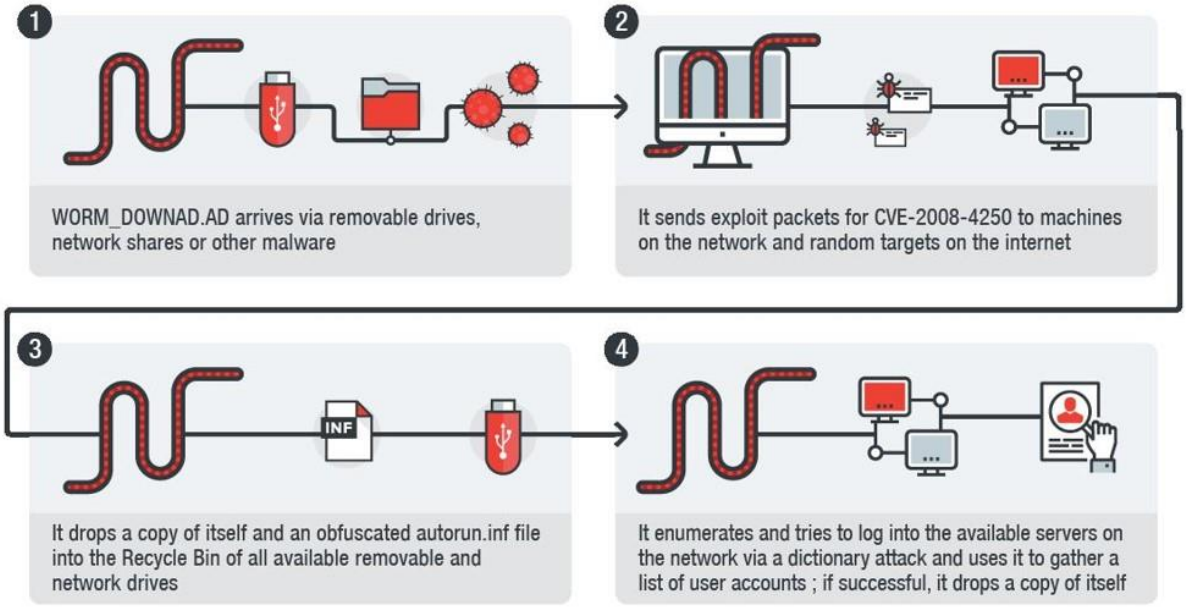
The following is a case of DOWNAD (also known as Conflicker) that is still spreading in factories.

DOWNAD first emerged as a threat in November 2008. Hundreds of thousands of computers around the world have been reported infected with DOWNAD in a blink of an eye since the threat was first identified. The important thing here is that DOWNAD is still ″malware that continues to be powerful against outdated systems″ 12 years after its heyday.

As more modern malware, such as “WannaCry” and “PETYA”, it is not a more modern malware that is of interest to the public, but as long as there are older systems in the network that are unsupported and the vulnerability is not updated, this situation will still remain a threat and this will not change in the future.

This case shows that removable media brought in from the outside can lead to secondary damage that could cause malware to enter into devices and network drives on the LAN.

Even in factory environments where Edgecross systems are located, removable media such as USB memory and CD-ROM may be used for maintenance, maintenance, etc. If you use a carry-on terminal or removable media, you must take security measures such as recognizing that there are still security risks due to the carelessness of the maintenance personnel and performing a proactive check to prevent damage.



(Source: Trend Micro Threat Database Security Blog https://blog.trendmicro.co.jp/archives/16614)

2. 5 Use Cases

2. 5. 1 System Composition

As a typical system composition when Edgecross is used, it is manifested in two situations: large-scale factory and small-scale factory.

【Pattern 1】For large-scale factories (Table 2-2)

In a large-scale factory, it is divided into an information network that connects the progress management personal computer etc. used in the management building and the network used in the factory, and the communication between the information network and the network in the factory and the Internet are carried out through the firewall.

The network in the factory is divided into information control network[1] connected by engineering tools and MES Client, control network connected by machine tools[2], PLC control equipment and local network[3] connected by HMI.

PCs equipped with Edgecross (Edgecross carrier PCs) are used by connecting to a control network or information control network.

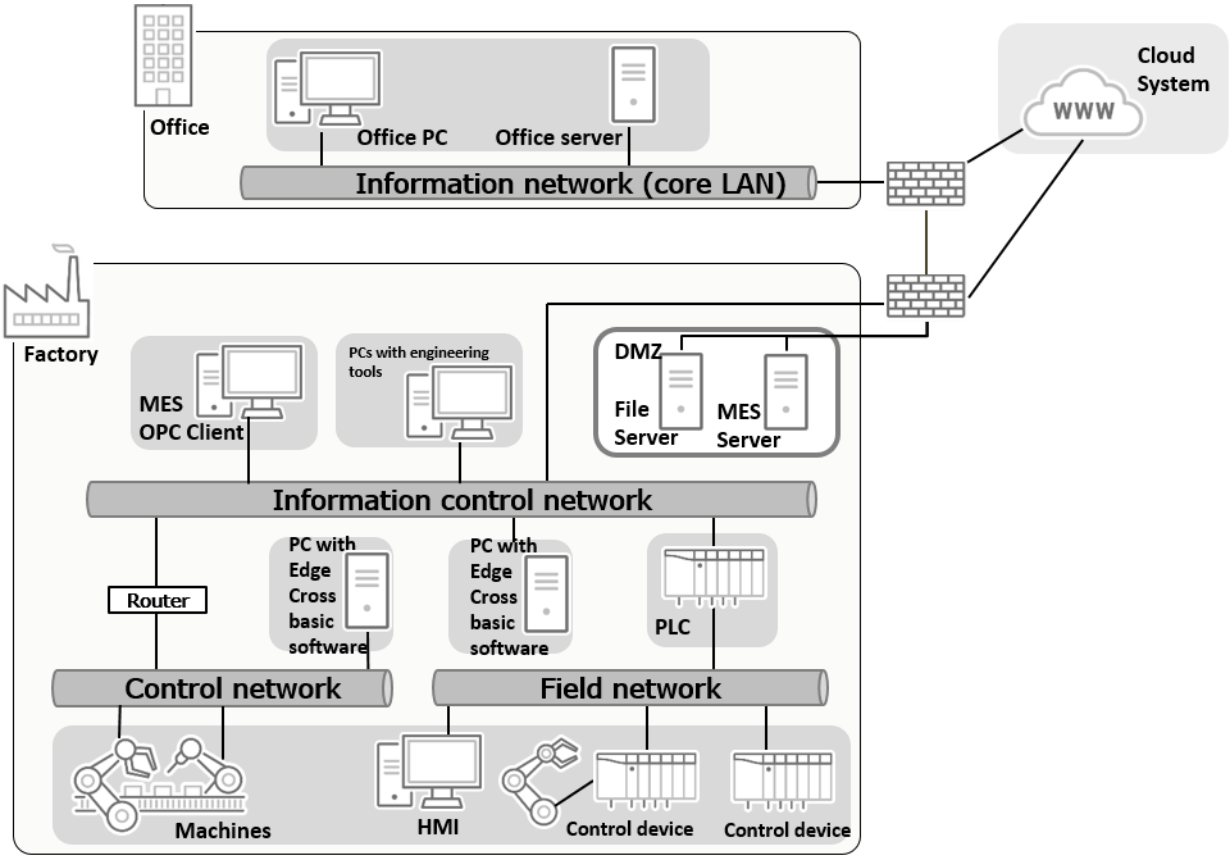


Table 2-2 【Pattern 1】Example of system configuration (large-scale factory)

【Pattern 2】For small-scale factories (Table 2-3)

In small-scale factories, office computers, engineering PCs, FileServer, etc. in the office are connected with machine tools on a network.

PCs equipped with Edgecross are also connected to the same network.

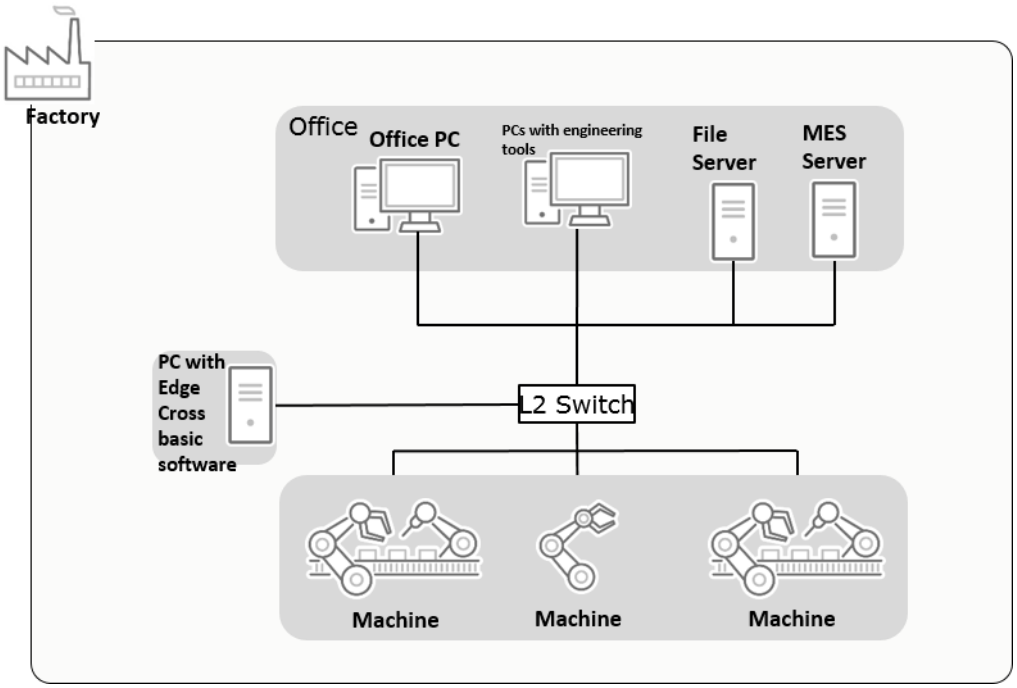


Table 2-3 【Pattern 2】Example of system configuration (small-scale factory)

2.5.2 Example Scenarios

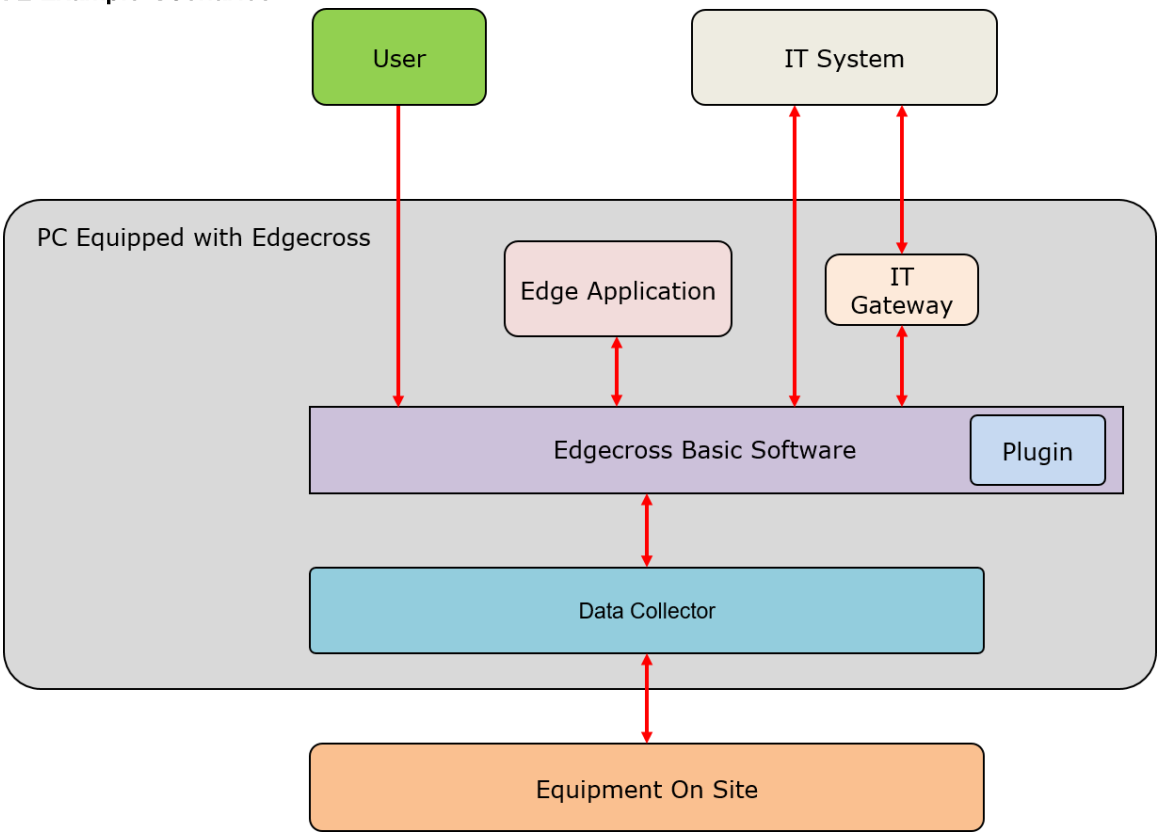


Table 2-4 Edgecross Software Composition Overview

First, the configuration of the Edgecross software is shown in the table above. Edgecross Basic Software collects and provides feedback on production site equipment through a data collector. Edge applications analyze and diagnose data. It also exchanges data with external IT systems.

Edgecross basic software also consists of a real-time flow manager, a real-time flow designer, a management shell, and a management shell explorer.

Real-time flow manager is a software that implements the ability to realize real-time diagnosis and feedback of data in the production site. You can use data collectors (software for collecting production site data through network) to collect data from connected equipment, equipment, or lines, and to process and analyze data. You can also use plug-ins to perform extensibility. It is started/stopped as a Windows service from the Real-time flow designer.

The real-time flow designer is a software that implements the ability to create, store, display, start/stop the real-time flow manager, and diagnose the various settings required to operate the real-time flow manager.

Management shell is software that models the data related to equipment, devices or production lines on the production site and manages it as a hierarchical structure. You can use the data collector to read the data of connected equipment, devices or production lines and write the data. The management shell explorer will be started/stopped as a Windows service。

The management shell explorer sets up and references the data model managed by the management shell and is responsible for starting and stopping the management shell.

Table 2-1 shows example scenarios using Edgecross in Table 2-1.

Table 2-1 Example scenario using Edgecross

	Category	Scenario Name	Remarks
(a)	Settings	System Launch (Real-Time Flow Designer)	Access equipment via real-time flow manager
(b)		System Launch (Management Shell Explorer)	Access equipment via the Management Shell
(c)	Data Collect	Data access from edge applications (such as MES Server) by OPC UA	
(d)		Use historical data in edge applications	
(e)		Data accumulation in FileServer	
(f)		Data analysis in cloud services	Not in Pattern 2
(g)	Feedback	Feedback from edge applications	Diagnostics + feedback in edge applications

(a) System Launch (case using real-time flow designer)

Start the real-time flow designer to configure settings for the real-time flow manager.

① The user starts the real-time flow designer to select the data collector to be used and set the device to which it is accessed.

② Next, configure "Data logging flow setting" or "Data diagnostic flow setting".

③ Finally, apply settings.

④ If you use an edge application for data diagnosis, etc., set the settings.

(b) System Launch (case using management shell explorer)

Start management shell explorer and configure settings for the management shell.

① The user selects the data collector to be used by using the Management Shell resource manager, and sets the access target device.

② Edit the component tree to create a model of the factory system.

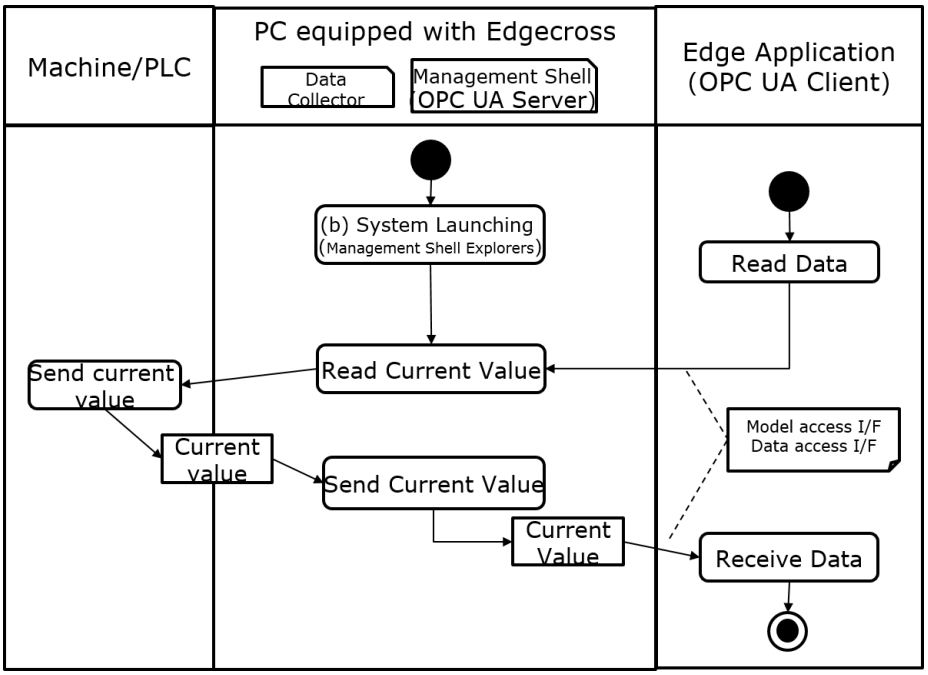
③ When using an IT gateway, configure the gateway settings.

④ When using OPC UA, configure the gateway settings.

⑤ According to the used edge application, make the necessary settings, such as OPC UA communication settings and data model references.

(c) Data access from edge applications (such as MES servers) by OPC UA

Edgecross model access I/F (OPC UA), data access I/F (OPC UA), edge application (such as MES server) refers to the current value of machine tool /PLC.



※In this case, in order to use the Management Shell, the system(b) should be started in advance (the case using the Management Shell explorer).

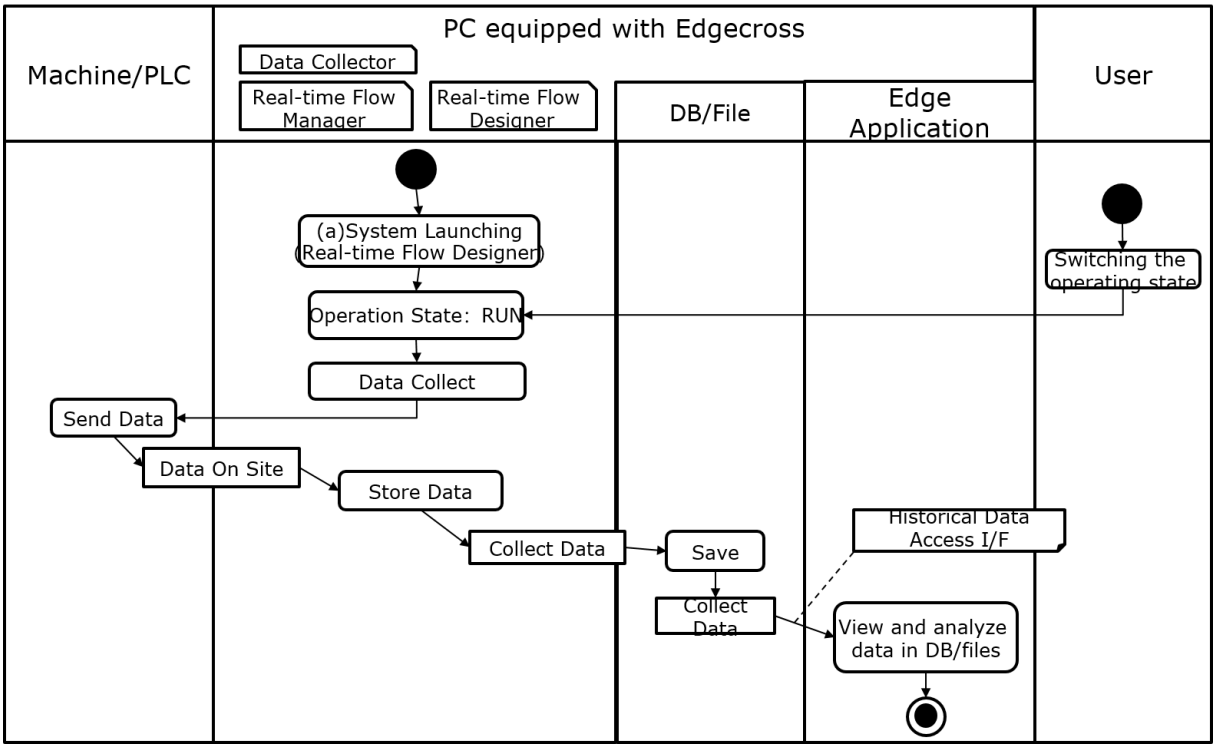
① Edge application reads data to management shell by model access I/F or data access I/F.

② Management Shell reads the current value from the machine tool /PLC through the data collector.

③ Send current value to the requesting edge application.

(d) Usage of historical data in edge applications

Examples of using Edgecross historical data to access I/F and using edge application to analyze historical data and other examples.



※In this case, we will launch (a) system (the case of using the real-time flow designer) in advance to use the real-time flow manager.

① The user switches the operating state of the real-time flow manager from the real-time flow designer to RUN.

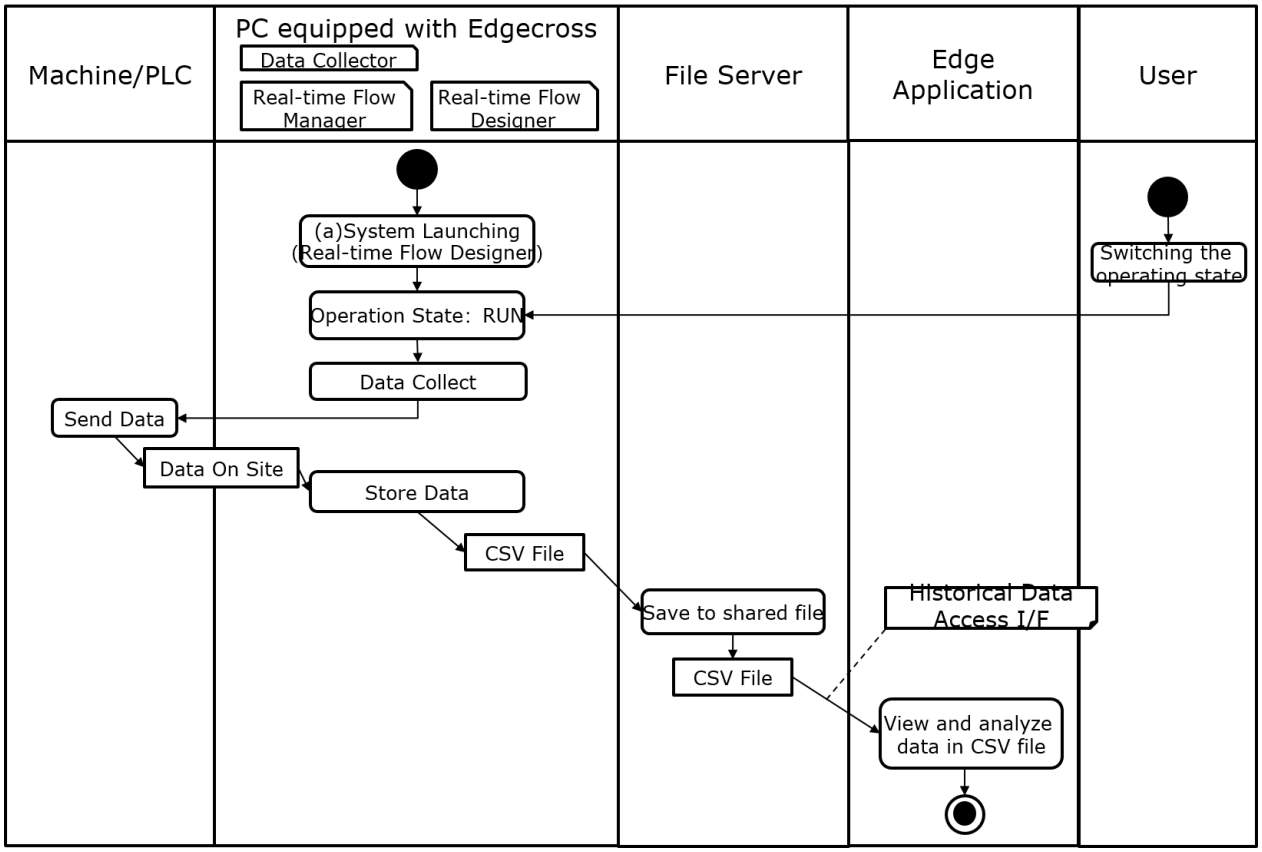
② Real-time flow manager collects data from machine tools/PLC via data collector.

③ The collected site data is stored in the DB/file by the data storing function of the real-time flow manager. (There are also cases where it is saved in a file through the string function.)

④ The edge application accesses I/F through historical data, obtains collected data from DB/ file, and displays and analyzes it.

(e) Data accumulation on FileServer

The data storage function of Real-time Process Manager saves CSV files in the collected data in FileServer, which can be used for the analysis of edge applications and other cases.



※In this case, we will launch (a) system (the case of using the real-time flow designer) in advance to use the real-time flow manager.

① The user switches the operating state of the real-time flow manager from the real-time flow designer to RUN.

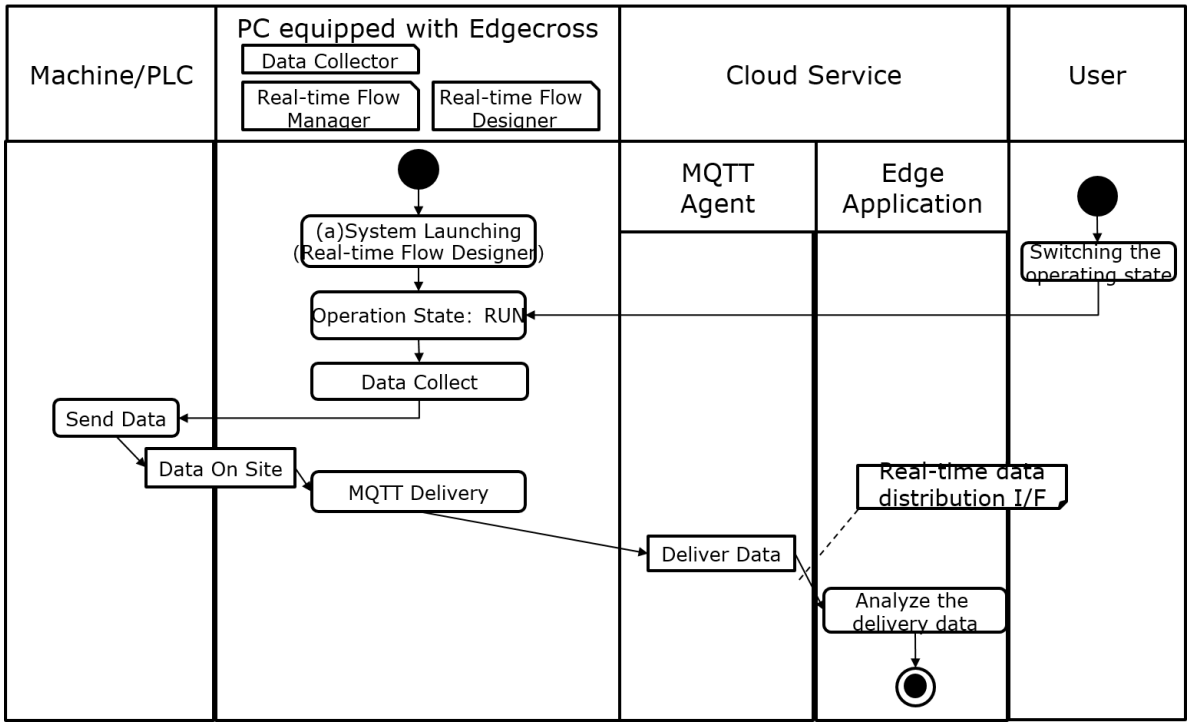
② Real-time flow manager collects data from machine tools/PLC via data collector.

③ The collected field data is generated as CSV file in the shared folder of FileServer through the data storage function.

④ The edge application accesses I/F through historical data, obtains collected data from CSV file on FileServer, and displays and analyzes it.

(f) Data analysis in cloud services

Through the real-time flow manager's data distribution function (MQTT distribution function), data is collected in cloud services in MQTT and analyzed in edge applications that support real-time data distribution I/F.



※In this case, we will launch (a) system (the case of using the real-time flow designer) in advance to use the real-time flow manager.

① The user switches the operating state of the real-time flow manager from the real-time flow designer to RUN.

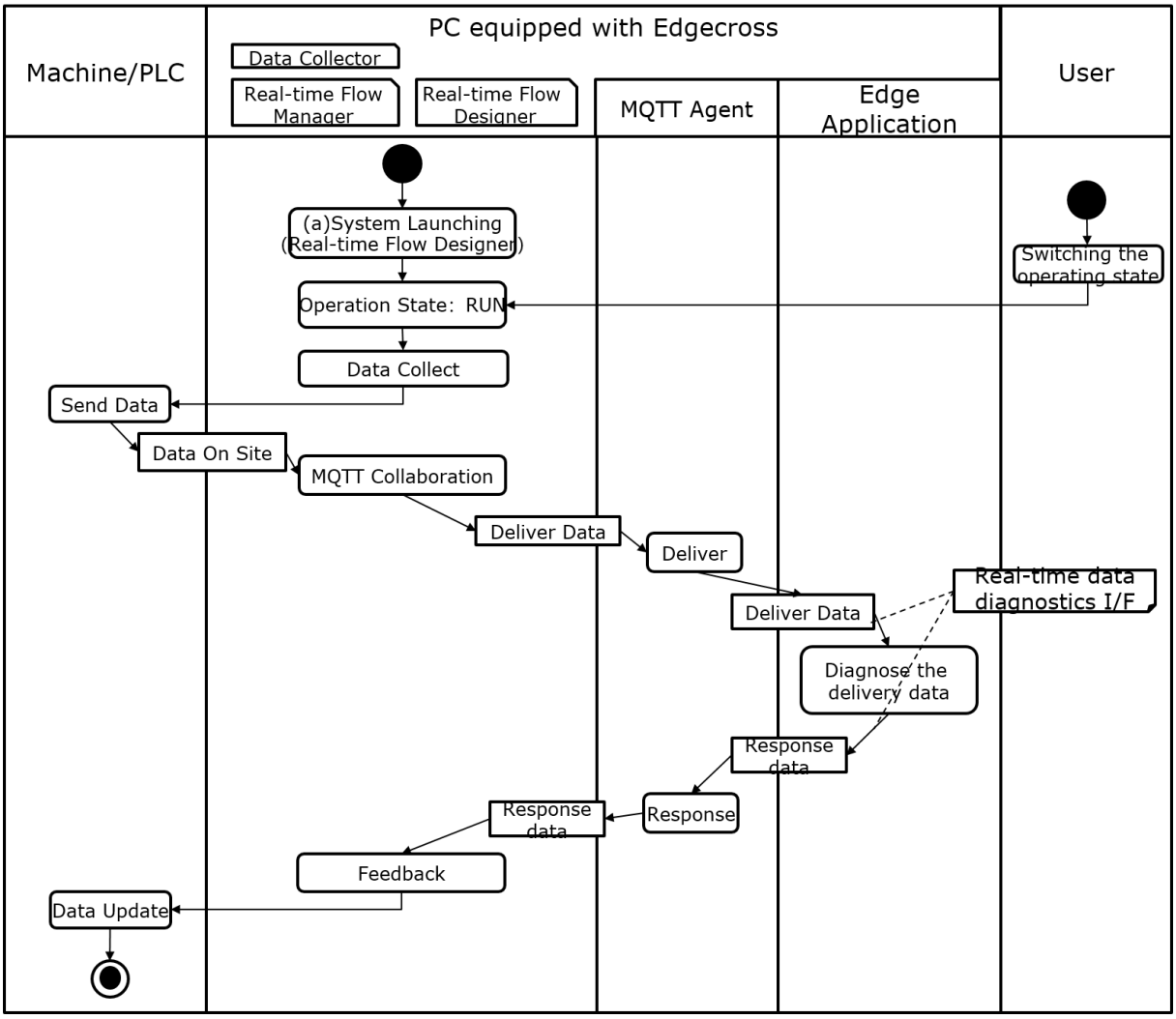
② Real-time flow manager collects data from machine tools/PLC via data collector.

③ The collected field data is sent to the MQTT broker on the cloud service through the MQTT distribution function of real-time process manager.

④ The edge application on the cloud service obtains the sending data from the MQTT broker through the real-time data sending I/F, and displays and analyzes it.

(g) Feedback from edge applications

It is a case to deliver data to edge applications that support real-time data diagnosis I/F (MQTT) by the data diagnosis function (MQTT cooperation) of the real-time flow manager, and to perform diagnosis and feedback.



※In this case, we will launch (a) system (the case of using the real-time flow designer) in advance to use the real-time flow manager.

① The user switches the operating state of the real-time flow manager from the real-time flow designer to RUN.

② Real-time flow manager collects data from machine tools/PLC via data collector.

③ The collected field data is passed to the MQTT broker through the REAL-TIME process manager's MQTT collaboration capabilities.

④ Edge application receives delivery data from MQTT broker with real-time data diagnostics I/F and performs diagnostics.

⑤ Response data when diagnostics are completed is sent from the edge application to the MQTT broker using real-time data diagnostics I/F.

⑥ Real-time flow manager receives response data with MQTT integration function and updates machine tool/PLC equipment data via data collector with feedback execution function.

2. 5. 3 Possible Threats

2.5.1 Table 2-2 lists the threats that are expected for use cases in the system configuration.

The threat categories in the table are in accordance with the classification of threats in the Security Risk Analysis Guide for Control Systems, 2nd Edition, published by the IPA, and the causal relationship between the threat categories described in the guide is shown in Figure 2-5. Patterns 1 and 2 show "large-scale factories" and "small factories" listed in 2.5.1, respectively, and the attack surface is described as well as "○" in the pattern in which the expected threat is applicable. Further, in order to point to the security measures against each threat, 3. Security measures in the construction and 4. The corresponding chapter section number of the security measures in the operation is described.

The following is an overview and incidents for each threat category in Table 2-2. In addition, the security threat of the entire factory, mainly PCs equipped with Edgecross, is described in a separate volume.

(1) Unauthorized access

A malicious third party penetrates an Edgecross PC over a network and performs an attack, such as tampering with stored information.

(2) Physical intrusion

Malicious third parties and intentional insiders (employees and collaborators with access to Edgecross-equipped PCs) illegally enter the location of the Edgecross-equipped PC with restricted entry. Or remove restrictions on Edgecross-equipped PCs with limited physical access by racks, boxes, etc.

(3) Improper operation

After (2), an operation is performed directly on the console of Edgecross-equipped PC, etc., and an attack such as downloading and installing an illegal software from a web site is performed.

(4) Negligent operation

An attack is made by triggering negligent operation of internal related personnel and making an illegal setting for the Edgecross-equipped PC operating system. An external storage device such as a regular USB memory or SD card is connected to an Edgecross-equipped PC, and an attack such as malware infection is performed intentionally。

(5) Illegal media, machine connection

Perform attacks such as connecting an external storage device illegally brought in by a malicious third party or a deliberate insider to an Edgecross-equipped PC and stealing production information and logs.

(6) Process malpractice

(1), (3), (4) illegal execution of normal programs, commands, services and other processes located on the Edgecross-equipped PC.

(7) Malware infection

(1), (3), (4), (5) infect and operate malware on the target Edgecross-equipped PC.

(8) Information theft

(6) and (7) steal information stored in Edgecross-equipped PC (production information, logs, software, authentication information, configuration setting information, encryption keys, etc.) stored in the PC equipped with Edgecross.

(9) Information tampering

(6) and (7) tamper with the information stored in the Edgecross-equipped PC.

(10) Information destruction

(6) and (7) destroy information stored in Edgecross-equipped PC.

(11) Unauthorized transmission

(6) and (7) make Edgecross-equipped PC transmit unauthorized control commands (change of setting value, power supply interruption, etc.) and illegal data (unauthorized value, illegal format, etc.) to machine tools and PLC-related devices.

(12) Machine Stop

(6), (7), (13) stop the function of the Edgecross-equipped PC.

(13) High-load attack

(7) makes Edgecross-equipped PC infected with malware by participates in DDoS attack or the like, transmits a large amount of data to other devices such as File Server, interfere with the normal operation of the device. In addition, infected malware requires more processing than the processing power of the Edgecross PC, interfering with the normal operation of the PC.

(14) Theft

After (2), steal the PC equipped with Edgecross.

(15) Break down and steal information when stealing or scrapping

After (14), the stolen Edgecross-equipped PC and the discarded PC are broken down and information stored in the PC is stolen.

(16) Eavesdropping and communication data tampering

Malicious third parties eavesdrop on or tamper with information flowing over the network between Edgecross-powered PC and File Servers.

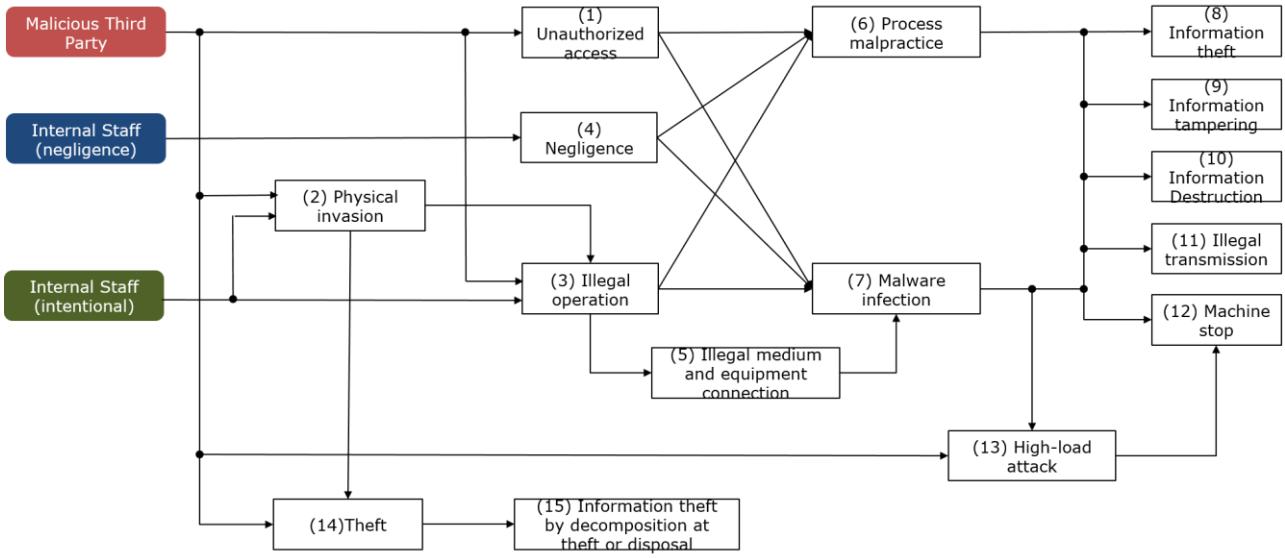


Figure 2-5 Causality of threat categories

Table 2-2 List of Assumed Threats in Edgecross Use Cases

No.	Threat Category	Assumed Threats	STRIDE Classification ※	Pattern 1 (Attack Surface)	Pattern 2 (Attack Surface)	Countermeasure
1	01. Unauthorized Access	Illegal access to PC equipped with Edgecross from outside the factory (Internet) by stealing passwords or using vulnerability.	Disguise	○ (Internet-Edgecross)+GG5H40		3.2.2 (1)(3) 3.4.2 (1) 3.4.3 (1) 3.4.4 (1)
2		Unauthorized access to the inside of an Edgecross PC from a legitimate server PC that has been stolen by the external illegal personnel.	Disguise	○ (Server-Edgecross)		3.5 (5)
3		The inside of the PC equipped with Edgecross is illegally accessed from the information control network through the client PC and other devices in the factory, illegally connected machines, infected malware in the factory, etc..	–	○ (Machine-Edgecross)	○ (Machine-Edgecross)	3.5 (5)(9)
4		Even if there is illegal access and operation to the PC equipped with Edgecross, the loss will enlarge due to late discovery or omission.	–	○ (People/Machine-Edgecross)	○ (People/Machine-Edgecross)	3.5 (5)(6)
5		There is no mechanism to authenticate the communication object on the terminal that can remotely operate the PC equipped with Edgecross, and an illegal command is executed, so the PC equipped with Edgecross is illegally operated.	Disguise	○ (Remote Terminal-Edgecross)	○ (Remote Terminal-Edgecross)	3.5 (5)(12)
6		An Edgecross PC receives illegal instructions from an attacker impersonating MES.	Disguise	○ (MES-Edgecross)	○ (MES-Edgecross)	3.5 (6)
7	02. Physical Invasion	The access rules in the area where the terminal can remotely operate the Edgecross PC are not properly managed, and the PC equipped with Edgecross is operated illegally by personnel other than the specified operators.	–	○ (Remote Terminal-Edgecross)	○ (Remote Terminal-Edgecross)	3.2.1 (2)
8	03. Illegal Operation	During the departure of the regular user,the operating PC equipped with Edgecross is accessed by operators without operation authority.	Disguise	○ (People-Edgecross)	○ (People-Edgecross)	3.2.2 (1)
9		A terminal capable of remotely operating a PC equipped with Edgecross is set in an area without special management, and the PC equipped with Edgecross is illegally operated by a staff member other than the specified one.	Disguise	○ (Remote Terminal-Edgecross)	○ (Remote Terminal-Edgecross)	3.2.1 (2) 3.4.2 (1) 3.4.3 (1)
10		Staff members other than specified ones peek at the images of the PC equipped with Edgecross.	–	○ (People-Edgecross)	○ (People-Edgecross)	3.2.1 (2)
11		Due to the direct operation of the attacker posing as the operator, the illegal software is installed on the PC equipped with Edgecross.	Disguise	○ (People-Edgecross)	○ (People-Edgecross)	3.2.2 (1) 3.3.1
12		Illegal software is installed on the PC equipped with Edgecross due to the privilege escalation attack that break through the vulnerability.	Privilege Escalation	○ (People/Machine-Edgecross)	○ (People/Machine-Edgecross)	3.3.1 3.4.4 (1) 4.1
13		Staff installs illegal software obtained from the Internet on the PC equipped with Edgecross.	–	○ (People-Edgecross)		3.3.1 3.3.2
14	04. Negligent Operation	Abnormal settings, information loss, improper execution of software, etc. will happen to the PC equipped with Edgecross due to the operation error of the regular access authority.	–	○ (People-Edgecross)	○ (People-Edgecross)	3.3.1
15	05. Unauthorized Media and Equipment Connections	Unauthorized devices (USB devices, Ethernet devices, wireless devices, etc.) are connected to the external communication path of a PC equipped with Edgecross or an Edgecross PC, and unauthorized operation is performed.	–	○ (Machine-Edgecross)	○ (Machine-Edgecross)	3.2.2 (2) 3.5 (3)(8)(11)(12)
16	06. Process Malpractice	Due to illegal access, illegal operation, malware infection, etc., unintended processes are executed in the PC equipped with Edgecross.	–	○ (People/Machine-Edgecross)	○ (People/Machine-Edgecross)	3.4.3 (4)
17	07. Malware Infection	An external carry-on terminal (maintenance terminal) that has not been security checked is connected, and a PC equipped with Edgecross is infected with malware via an external carry-on terminal (maintenance terminal).	–	○ (External Terminal-Edgecross)	○ (External Terminal-Edgecross)	3.3.1 3.5 (9)(12)
18		The idle port of the network device is placed in a connectable state, connected to an illegal terminal, and sends malicious software to a PC equipped with Edgecross.	–	○ (Machine-Edgecross)	○ (Machine-Edgecross)	3.3.1 3.5 (5)
19		External media (USB, etc.) and external carry-on terminals (maintenance terminals) that have not been security checked on the server are connected, and Edgecross-equipped PCs are infected with malware via them.	–	○ (External Terminal-Edgecross)	○ (External Terminal-Edgecross)	3.3.1 3.5 (8)(9)(12)
20		PCs equipped with Edgecross are infected with malicious software through files obtained from FileServer.	–	○ (FileServer-Edgecross)	○ (FileServer-Edgecross)	3.3.1 3.5 (4)(5)
21		PCs equipped with Edgecross are infected with malware through files obtained from the Internet.	–	○ (Internet-Edgecross)		3.3.1 3.5 (4)
22		PCs equipped with Edgecross are infected with malware and affect production by spreading infection to other devices.	–	○ (Edgecross-Machine)	○ (Edgecross-Machine)	3.3.1 3.5 (5)
23		Illegal software was installed on the PC equipped with Edgecross because of being infected with malicious software.	–	○ (People/Machine-Edgecross)	○ (People/Machine-Edgecross)	3.3.1
24	08. Information Theft	Illegal access, illegal operation, malware infection, etc., resulting in the information in the PC equipped with Edgecross being stolen/tampered/destroyed.	Information Leakage	○ (People/Machine-Edgecross)	○ (People/Machine-Edgecross)	3.3.2
25	09. Information Tampering	Due to the direct operation of the attacker posing as the operator, the settings of the PC equipped with Edgecross are illegally changed.	Tampering	○ (People-Edgecross)	○ (People-Edgecross)	3.3.2
26	10. Information Destruction	Due to illegal access, the necessary log data in the PC equipped with Edgecross is deleted.	Denial	○ (People/Machine-Edgecross)	○ (People/Machine-Edgecross)	3.3.1
27		Obstruct service by deleting authentication information in PC equipped with Edgecross.	–	○ (People/Machine-Edgecross)	○ (People/Machine-Edgecross)	3.3.1
28	11. Illegal Transmission	Entering a target value that is not appropriate for the PLC via an Edgecross-equipped PC, the equipment is destroyed by illegal operation.	–	○ (Edgecross-PLC)	○ (Edgecross-PLC)	3.4.2 (1)(2)(3) 3.4.3 (1)(2)(3)(5)(6) 3.5 (5)
29		The PC equipped with Edgecross is infected with malicious software and execute illegal instructions, which adversely affects the production.	–	○ (Edgecross-PLC)	○ (Edgecross-PLC)	3.3.1 3.5 (5)
30		The PC equipped with Edgecross is infected with malware and sends illegal instructions to PLC.	–	○ (Edgecross-PLC)	○ (Edgecross-PLC)	3.3.1 3.5 (5)
31		Due to malware infection, illegal files will be uploaded from the PC equipped with Edgecross to the FileServer.	–	○ (Edgecross-FileServer)	○ (Edgecross-FileServer)	3.3.1 3.5 (4)(5)
32		Illegal files will be uploaded from the PC equipped with Edgecross to the FileServer through the direct operation of the attacker disguised as an operator.	Disguise	○ (Edgecross-FileServer)	○ (Edgecross-FileServer)	3.2.2 (1) 3.5 (4)(5)
33		Through infected malicious software, the information in the PC equipped with Edgecross is sent to the Internet.	–	○ (Edgecross-Internet)		3.3.1 3.3.2 3.4.2 (4) 3.4.3 (2)(7) 3.5 (4)(5)(6)
34		Through the direct operation of the attacker disguised as an operator, the information in the PC equipped with Edgecross is sent to the Internet.	Disguise	○ (Edgecross-Internet)		3.2.2 (1) 3.3.2 3.4.2 (4) 3.4.3 (2)(7) 3.5 (4)(5)(6)(12)
35		Connect a server or PC disguised as a legitimate server or PC and send data from a PC equipped with Edgecross.	Disguise	○ (Edgecross-Server)	○ (Edgecross-Server)	3.3.2 3.4.2 (4) 3.4.3 (2)(7) 3.5 (4)(5)
36	12. Function Stop	Due to the direct operation of the attacker disguised as a staff, the PC equipped with Edgecross is in a stopped state.	Disguise	○ (People-Edgecross)	○ (People-Edgecross)	3.2.2 (1)
37		PC equipped with Edgecross is overloaded and stopped due to malware infection.	–	○ (People/Machine-Edgecross)	○ (People/Machine-Edgecross)	3.3.1
38	13. High-load Attack	For the IT gateway and the data model management function, high-load communication is carried out, and the service is obstructed.	DoS Attack	○ (Internet-Edgecross)	○ (Internet-Edgecross)	3.5 (4)(5)
39	14. Theft	The PC equipped with Edgecross is physically attacked and stolen by intrusion into the factory.	–	○ (People-Edgecross)	○ (People-Edgecross)	3.2.1 (2)
40	15. Stealing information by decomposing it when stolen or abandoned	Stealing information through reverse engineering of abandoned and stolen PC equipped with Edgecross.	Information Leakage	○ (People-Edgecross)	○ (People-Edgecross)	3.3.2
41	16. Information theft by decomposition at theft and disposal	Leakage and tampering occurred in the data sent and received from PC equipped with Edgecross to FileServer.	Information Leakage Tampering	○ (Edgecross-FileServer)	○ (Edgecross-FileServer)	3.3.2
42	17. Windows Related	Without compatibility verification, unexpected Windows Update is executed, unexpected Shutdown, reboot or system failure occurs.	–	○	○	3.2.2 (3) 4.1 (3)
43		The execution of Windows Update causes the resource exhaustion of the PC equipped with Edgecross and cannot perform the necessary processing.	–	○	○	3.2.2 (3) 4.1 (3)
44		The Windows evaluation process is overloaded and cannot perform necessary processing.	–	○	○	3.2.2 (3) 4.1 (3)
45		Windows Update is not implemented, and known vulnerabilities accumulate.	–		○	3.2.2 (3) 3.5 (7) 4.1 (3)
46		As Windows continues to be used after the end of support services, known vulnerabilities will accumulate.	–	○	○	3.2.2 (3) 3.5 (7) 4.1 (3)

※STRIDE is one of the initial threat analysis methods for spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS attack), and Elevation of privilege.

3. Security Measures in Construction

3. 1 Main Points

The Edgecross system is located at the boundary between the FA and IT areas. Therefore, from a security point of view, access to both production site equipment and IT systems must be considered.

In addition, the user can define the operation by edgecross basic software, and by combining various software such as data collector, edge application, and plug-in, it is possible to build a system with a high degree of freedom. To ensure security, users need to take the lead in what systems to build and how to protect them.

When building edgecross systems, please design the system from the following (1) to (5) perspective so that you can identify what you want to protect and protect them.

The IoT Security Guidelines contain the following key points: Please refer to "IoT Security Guidelines" to build edgecross systems.

(1) A design that can be protected individually or entirely

Consider measures on individual devices and systems against risks caused by external / internal / physical contact. In addition, if individual devices and systems are not available, consider countermeasures with their higher-level IoT devices and systems.

(2) Design that won't bother the objects involved

Design to detect equipment and system abnormalities, and consider appropriate behavior when abnormalities are detected.

(3) Ensure design consistency for safety and security

Visualize the design to realize safety and security. Also, check the mutual impact of the design to achieve safety and security.

(4) Designed to ensure safety and security even if connected to an unspecified partner

Please discuss the design of connection method that can be judged according to the connected object and connection condition of machine and system.

(5) Verification and evaluation of designs that realize safety and security

Please verify and evaluate the design that realizes safety and security by taking into account the unique risks of IOT for connected devices and systems.

In order to reduce threats, we believe that it is desirable to take various measures such as human, physical, and even connected networks in multiple layers. We recommend that you implement the following security measures.

3. 2 Hardware/OS

3. 2. 1 Hardware

(1) Procurement

Edgecross is available on various manufacturers' industrial PCs. For the construction of safe and secure equipment, industrial PC should be procured from a reliable source.

Make sure that you have access to the procurement equipment and have easy access to the vendor.

Please also note that there may be a problem with the distribution channel, even if the product is from a reliable manufacturer. For example, there may be cases where used products that are maliciously contaminated with malware are sold.

The Edgecross Consortium introduces recommended industrial PCs that have been certified for the operation of the Edgecross basic software Windows version. For more information, please visit the Edgecross Consortium website (https://www.edgecross.org/).

(2) Settings

When installing industrial PCs, be aware of the protection against physical attacks.

・Security wire locking and lockable PC racks to prevent physical theft
・USB/LAN physical lock to prevent physical connectivity
・Operator entry and exit restrictions

These measures vary depending on the environment in which they are used, so please implement them according to your environment.

(3) Initial setting

Industrial PCs have several security settings. Set it appropriately according to your environment and the software you want to run. Typical settings are listed below. For details, please refer to the manual of the industrial PC, etc.

・BIOS password settings such as password, HDD password, etc.
・Set up the boot drive
・USB setting
・Set up functions to enable external control, such as Wake on Lan
・Configure security chips such as TPM
※Recommend to use TPM.

(4) Update

Update the firmware BIOS of the CPU and chipset, storage and network card firmware and drivers, etc. appropriately. To obtain update software, take steps to ensure that it has not been tampered with, such as using a reliable website.

Also, keep in mind that the firmware, etc. may have been updated during the period from the time each hardware is shipped to the actual use, and be sure to check the firmware and other updates at the time of construction, even if it is the latest hardware.

(5) Operation

Check the support period for your hardware (and ancillary software). We recommend that you operate within the support period.

If you are forced to continue operating after the support period, be aware of the risk that the support period for working equipment has passed and take appropriate management.

If the device becomes unused and is out of control, it may be a security risk that the unmanaged equipment is running, so turn off the equipment.

3.2.2 OS

Edgecross Basic Software Windows version runs on Microsoft® Windows® 10 Operating System (hereinafter referred to as Windows). This chapter provides basic guidelines for windows operations, but you should choose the actual implementation appropriately according to the production environment of your Edgecross equipment.

Windows features and terminology may change in future updates. Please refer to Microsoft's homepage for details.

(1) Account password

Windows has the ability to manage accounts and passwords for each user. Set up an account according to the user's role, and implement appropriate management, such as setting a password that is difficult for others to estimate.

In addition to the Windows account password, you can also use PIN authentication, biometrics authentication, or two-factor authentication / multi-factor authentication combined with the Windows account password.

There are security features (user account control features) that allow administrator authority users to grant permission when important changes to Windows systems are made. It is recommended to enable this feature.

Windows has the ability to store various usernames and passwords. Storing information such as network access credentials and web pages' usernames and passwords in a system may lead to security risks, so it is recommended not to be stored unless necessary.

(2) Setting

Windows contains a variety of applications and services. We recommend that you disable unnecessary features when running Edgecross. In particular, disable personal use functions that are not necessary for Edgecross, such as camera and microphone functions. In addition, physical access from outside such as USB and Bluetooth should be restricted or disabled as much as possible.

As an anti-malware measure, take advantage of the security features installed in Windows or deploy third-party security software. It is also recommended that you block unnecessary network access through a personal firewall.

(3) Update

Windows has the ability to apply updates with Windows Update and keep it up-to-date. We recommend that you keep it up to date in a generic environment.

However, some updates may take a long time to update, some that involve a restart. Since there are some problems with the operating environment and problems, we recommend that you update it after making sure that there is no problem with the operation of Edgecross.

For industrial PCs used in certain applications, it is effective to postpone the application of the update and prepare the test equipment for the verification of the operation of the update. Microsoft provides Windows Server Update Services (WSUS) as a solution for controlling the application of windows updates within an organization。

If you choose WSUS as the source of Windows updates, use Group Policy to set your Windows PC to the WSUS server. Updates from Windows Update are periodically downloaded to the WSUS server, managed, approved, and deployed through the WSUS Management Console or Group Policy to streamline the management of corporate updates.

If you can't do a timely Windows Update, you can take advantage of next-generation IPS to take temporary measure with virtual patches.

3. 3 Security Software

Security software is a generic name for application software used to protect computer security and is used to prevent malware intrusions and infections, and to prevent unauthorized access, information theft or tampering, and attacks against other systems. We recommend that customers implement appropriate security software for Edgecross basic software and certified products, recommended industrial PCs, etc.

3. 3. 1 Anti-malware software

For specific consideration, it is necessary to select security software according to the application and operation of the system. As anti-malware software, please refer to the following methods. For more information, contact your product distributor or sales agency to proceed with the introduction.

Blacklist method

Strengths: Implementation of rich multi-layer defense technology.

Weaknesses: Timely updates to respond to the latest threats. Product support in accordance with the OS support lifecycle.

Whitelist method(Lock down with specific applications)

Strengths: The length of the support lifecycle. Updates according to the system update cycle. Resource leveling.

Weaknesses: Matching with system characteristics (for example, if there are frequent executable changes or exports)

In the unlikely event that an infection with malware, the following effects will occur, for example, as in the case of an infection of a general Windows machine. If you suspect such symptoms, we recommend that you use them as needed because there is a USB malware check and removal tool that allows you to check for malware without installing the application.

- ・Malicious software is installed
- ・Tampering, loss, or leakage of various types of data
- ・Be a stepping stone to an attack on another system

After you deploy antimalware software, it is recommended that you consider the following three points:

(1) Renew contract

Antimalware software has a limited license period for one year or several years. It is necessary to update the license agreement so that it can be used continuously during the system operation.

(2) Update

Antimalware software may require updates to improve functionality in order to respond to changes in external threats. Malware detection patterns are often updated on a daily basis, so regular updates are required when using blacklisted anti-malware software. If you use whitelisted anti-malware software, you will need to update the list at the time of system change. When an antimalware software vulnerability is disclosed, product updates and security patches may be provided separately. Be aware of the vulnerability information and consider applying it.

(3) System scan

Periodically scan the entire system. It is recommended that you run it according to the health of the system because the CPU load is high during the scan. Resident type is to install anti-malware software and non-resident type (USB malware inspection and recovery tool) that do not require software installation.

3.3.2 Other Security Software

We recommend the introduction of personal firewalls with built-in operating systems and third-party communication access control software as countermeasures against unauthorized access and stepping stone.

For information theft and tamper prevention, please refer to the 3.4 edgecross basic software encryption for edgecross PC and external communications. It is recommended to introduce third party encryption software and tampering software. In relation to this, distribution, management, and disposal of encryption keys and certificates are cumbersome as the edgecross system is larger, so we recommend that you use third-party key management software as needed.

3. 4 Edgecross Basic Software

3. 4. 1 Composition

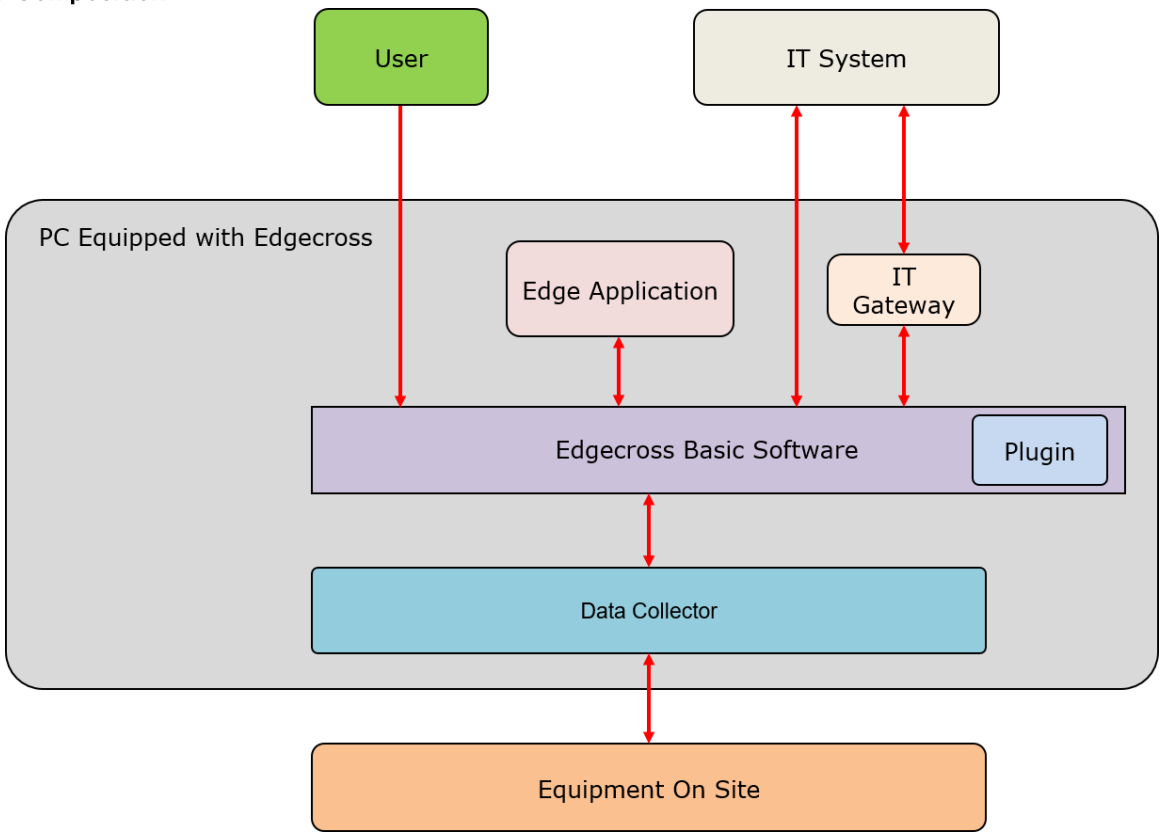


Figure 3-1 Edgecross Software Structure Schematic Diagram

The figure above is a schematic view of the Edgecross software structure.

Edgecross Basic Software collects and provides feedback on production site equipment through a data collector. Edge applications analyze and diagnose data. It also exchanges data with external IT systems.

Data collector is a software that can directly control production site equipment. Edge applications and IT gateways, which are data collectors and software accessible to data collectors (through Edgecross basic software), use reliable software.

There are two forms of access to Edgecross from external IT systems.

The first is a form of direct access to edgecross basic software. In this form, the interface between Edgecross basic software and edge applications is exposed to external IT systems. Keep in mind the security risks of exposing the interface to the outside world. For more information about interfaces, please refer to 3.4.2 Data Model Management and 3.4.3 Real-Time Data Processing.

The other way is access to Edgecross basic software through an IT gateway. In this form, access to Edgecross is limited via the IT gateway. You can also take advantage of security features in your IT gateway.

The user logs in to the OS and performs various operations of Edgecross basic software.

The operation of edgecross basic software is not only information browsing but also access to the production site equipment through the data collector. Please note that users accessible to edgecross basic software are accessible to production site equipment (i.e., it is possible to manipulate the production site equipment illegally). Edgecross basic software does not have the ability to control accounts for each user, so please use OS account control.

Table 3-1 Edgecross Basic Software Composition

Function	Software	Contents
Real-time Data Processing	Real-time Flow Manager	Software that realizes real time diagnosis and feedback of data in production site. You can use data collectors (software to collect data from a production site via a network) to collect connected equipment, devices, or line data, and then process and analyze data. You can also use the plugin to extend functionality. Real time flow designer starts / stops as a Windows Service.
	Real-time Flow Designer	This software implements the ability to create, store, display, start/stop the real-time flow manager, and diagnose various settings required for the operation of the real-time flow manager.
Data Model Management	Management Shell	It is a software that can be used as a hierarchical structure to model data on equipment, devices, or lines in a production site. Data collectors can be used to read and write data from connected machines, devices, or lines. Management shell Explorer starts / stops as a Windows service.
	Management Shell Explorer	Set and refer to the data model of management shell management, and be responsible for the start / stop of management shell.

Edgecross basic software consists of the software listed above. For more information, please refer to the Edgecross Basic Software User Manual Windows Version.

Edgecross basic software is roughly divided into two functions: real time data processing and data model management. Details of each feature and security considerations will be described below.

3. 4. 2 Data Model Management

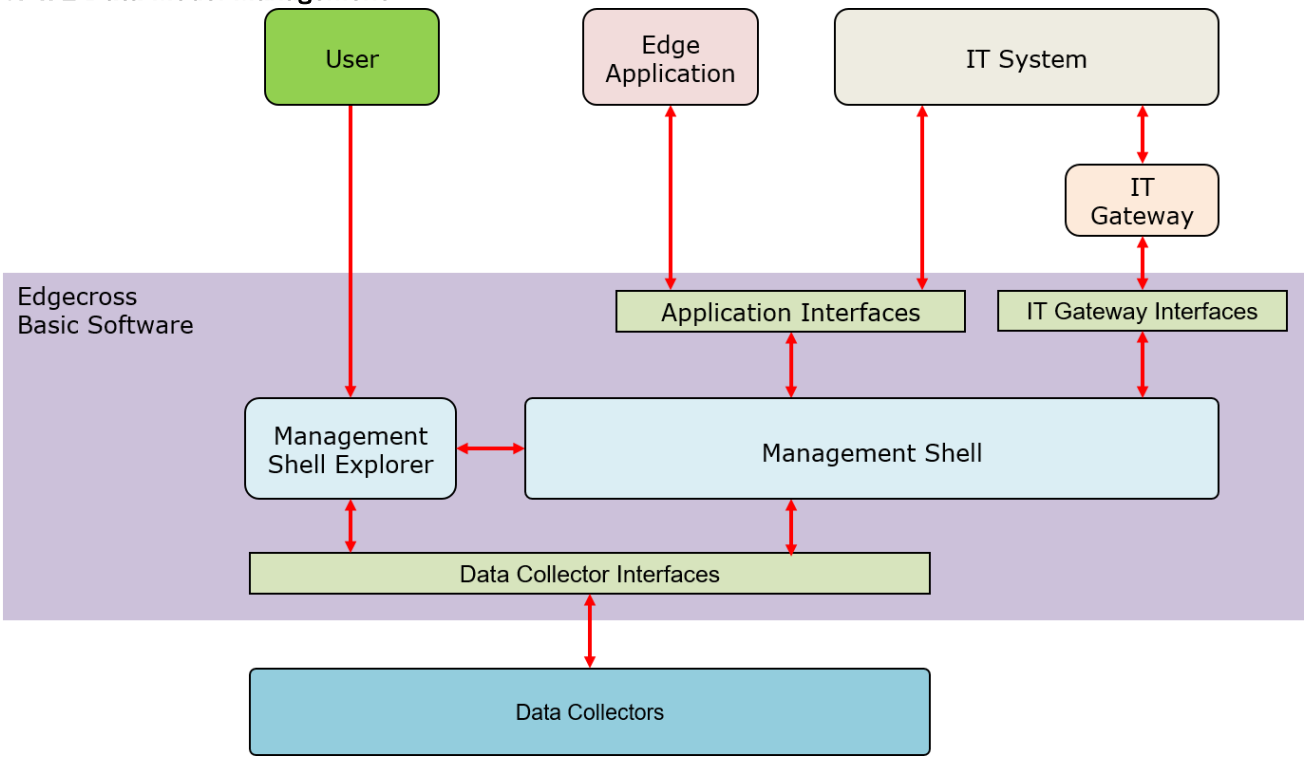


Figure 3-2 Data Model Management Schematic

Data model management is a function to model and manage data about equipment, devices, or lines in a production site as a hierarchical structure, allowing you to use a data collector to read and write data for connected equipment, devices, or lines. From a security perspective, keep in mind that you have the ability to operate production-site equipment through a data collector.

There are three entities that perform data model management: user, edge application, and external IT system.

The user operates the Management Shell Explorer as a user interface.

Edge applications operate the OPC UA server as an application interface.

External IT systems operate OPC UA servers and IT gateways as interfaces.

(1) Management Shell Explorer

Management shell Explorer enables you to configure and reference a data model managed by the management shell. That is, it is possible to read and write data from devices and equipment of production site. If the Management Shell Explorer is manipulated by an unauthorized user, it may cause the suspension of the production site, the leakage of data, tampering, etc. As a countermeasure, please configure edgecross PC so that only trusted users can log in (log in to Windows).

In addition, the startup and stop of the management shell, and the configuration of the OPC UA server are executable for the users with Windows administrator rights (or users who know the password of the administrator account).

(2) OPC UA

The Management Shell acts as an OPC UA server and has the ability to provide model access I/F and data access I/F to edge applications that are OPC UA clients (OPC UA connection function). In this case, it is possible to authenticate using the client certificate of the edge application. You can also encrypt while communicating.

Note that the OPC UA interface is also capable of operating production equipment via the data collector. The owner of the client certificate of the OPC UA is also able to operate the production site equipment.

(3) Edge Applications

The edge application can operate data model management via the OPC UA. In addition, it works as an application on Windows, and it is possible to perform other behaviors than the data model management. When malicious edge application is introduced, it may cause stop of production site, leakage or tampering of data.

Edge applications are recommended to be obtained from trusted sources, such as Edgecross Marketplaces.

(4) IT Gateway

IT gateway is a software component that provides communication between the external IT system and edgecross basic software.

If IT gateway is available, the above OPC UA is recommended to disable access from outside of edgecross PC and to deploy edge applications in edgecross PC. With this configuration, access to edgecross from an external IT system can be limited via IT gateways, so it is possible to build a robust system for external access. To learn how to use the IT gateway, please refer to the IT gateway manual from the IT gateway provider.

3. 4. 3 Real-time Data Processing

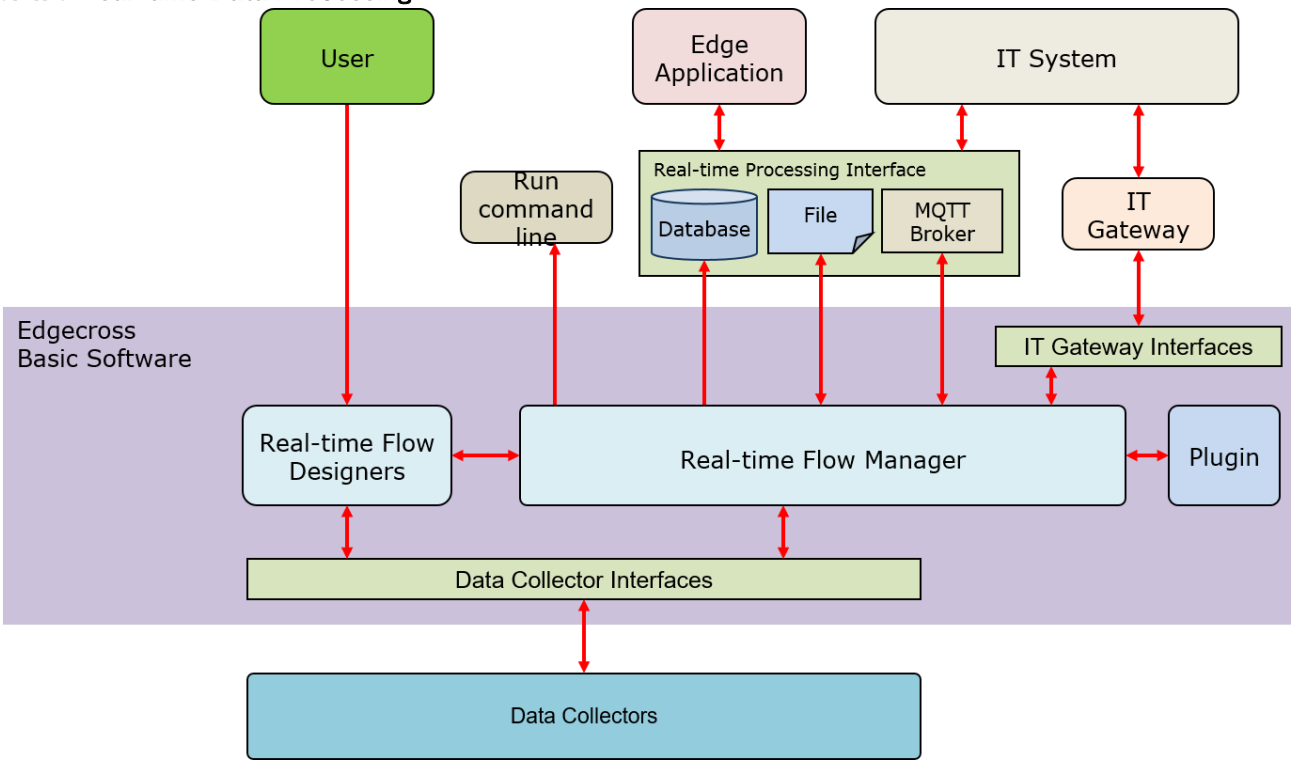


Figure 3-3 Real-time Data Processing Schematic

Real-time data processing collects data from the data collector at the production site and processes and analyzes the data. You can also feed back the results of processing and analysis of data to production equipment (via a data collector). In addition, data can be sent and received from IT systems. It also has the ability to run command-line programs on the OS.

The Real-time flow manager is a service that is responsible for the flow of data, and the Real-Time Flow Designer allows the user to create a flow of operations.

Data processing and analysis can be extended by introducing edge applications and plugins.

Edge applications communicate with real-time flow managers via MQTT, files and databases.

Plug-ins are called directly from the real-time flow managers.

External IT systems and Edgecross basic software communicate via the same interface (MQTT, files, database) and IT gateway via edge applications.

Real-time data processing, like data model management, must be prepared for unauthorized user interaction. In addition, keep in mind that real-time data processing handles and operates on the data from the production site and the data that processes them. In other words, it is necessary to prepare for illegal access by illegal data besides operation by an illegal user.

For example, if the flow of data delivered to MQTT is transferred to the on-site equipment via the data collector, the illegal data delivery to the mqtt may cause an illegal operation of the on-site equipment. In this case, the data to be delivered to the on-site equipment must be taken to prevent illegal data access, such as building a flow so as to be limited to normal data generated within a reliable edge application.

(1) Real-time Flow Designer

By manipulating the real-time flow designer, users can create various settings necessary for the behavior of the real-time flow manager. As with data model management, if the real-time flow designer is manipulated by an unauthorized user and the real-time flow manager settings are rewritten, it may lead to the stop of the production site, data leakage, tampering, etc. As a countermeasure, please configure Edgecross PC so that only trusted users can log in (log in to Windows).

(2) MQTT

MQTT is used to deliver data (collected data, machining data) from real-time flow managers to edge applications, and to receive response data from edge applications. It is also used for communication with external IT systems.

MQTT is a widely used communication standard, but it often poses a security risk due to improper configuration. In 2018, there were reports of the discovery of tens of thousands of vulnerable MQTT servers (brokers) on the Internet. In edgecross systems, it may not only lead to information leakage, but also unauthorized operation of field equipment due to unauthorized data injection, so be careful not to disclose MQTT in a vulnerable state.

Below is a typical example of the mqtt configuration in the Edgecross system.

①Data transmission between real time flow managers and edge applications

Edge applications and MQTT brokers are deployed in PCs with Edgecross and do not expose MQTT outside the PC (personal firewall prohibits communication in the internal of MQTT).

②Sending data to external IT systems

The MQTT broker is deployed on the external IT system side, it limits the data transmission from the edgecross system to the external IT system, and it encrypts between edgecross and MQTT brokers in TLS。

Both (1) and (2) above are configured to avoid data injection into the Edgecross system by not externally exposing the MQTT on the Edgecross system side.

(3) File/Database

Communication with files and databases as an interface has the same nature as MQTT communication. In other words, the disclosure of a file can lead to information disclosure, and writing a file can lead to the injection of malicious data. Publish files/databases should be treated as carefully as MQTT.

As a function of Edgecross basic software, it is possible to place files in a remote shared folder. Set the appropriate user account/password for the shared folder.

You can also use a shared folder that does not use a user account, but keep in mind that in this case, the access rights of the remote shared folder will be "ANONYMOUS LOGON". This means that all users who have access to the remote PC can access the file without authentication.

We recommend that you use remote shared folders that do not use user accounts only in a reliable network or do not use such remote shared folders.

(4) Run Command Line

The Real-Time Flow Manager provides the ability to run the specified program from the command line. You can also specify diagnostic data as program arguments. The specified program operates with system privileges, so most of the Edgecross PC can be operated.

The ability to run command-line programs with diagnostic data as arguments means that from a security perspective, an attacker could have the opportunity to manipulate the system by injecting malicious data. When using this feature, consider thoroughly and consider the possibility that malicious data will be executed in the program.

It is recommended that you do not use the function of specifying diagnostic data to program arguments if you cannot dispel concerns about data injection attacks.

(5) Edge Application

Edge applications are responsible for processing and analyzing data via MQTT, files, and databases, but because they act as applications on Windows, it is also possible to perform operations other than data processing and analysis. Deploying malicious edge applications may lead to stop production sites, leakage, tampering of data, etc.

Edge applications are recommended to be obtained from trusted sources, such as Edgecross marketplaces.

(6) Plug-in

Plug-ins are software that is placed under real-time data processing execution control and called from real-time data processing. The plug-in operates with system privileges and allows most operations of the Edgecross PC. If a malicious plug-in is mixed in, it may cause the stop of the production site and the leakage or tampering of the data.

Plug-ins are recommended to be obtained from trusted sources, such as Edgecross marketplaces.

(7) IT Gateway

IT gateway is a software component that provides communication between external IT systems and Edgecross basic software.

3.4.2(3) and described in "IT Gateway", it is possible to build a robust system through an IT gateway to access Edgecross from an external IT system. To learn how to use the IT gateway, please refer to the IT gateway manual from the IT gateway provider.

3. 4. 4 Maintenance and Operation

(1) Software Update

As the latest Edgecross basic software is compliant with known vulnerabilities, make sure that the Edgecross basic software uses the latest version. It is recommended to perform the version upgrade after the operation verification. You should also address the vulnerability of the relevant OSS.

For more information, please refer to 4.1 "Vulnerability Countermeasures".

(2) Preservation

Event information often provides useful information not only in the event of a security incident, but also in the event of a failure or software failure. Edgecross system administrators should check the history of event information.

Edgecross Basic Software captures event information that occurs in real-time flow managers, management shells, and the data collectors they use, and displays event history and event details, causes, and action methods as diagnostic information. The event history is stored even if the power of the industrial PC running the real-time flow manager is turned off, so it can be used to investigate the cause of the problem by checking after restarting the industrial PC or by checking the operation information before and after. It can also be used if the error code cannot be verified when an error occurs.

3. 5 Network

A network based approach as a security measure for protected assets is shown below.

[Example of Security Measures for the Network]

Figure 3-4provides an example of a security measure to network.

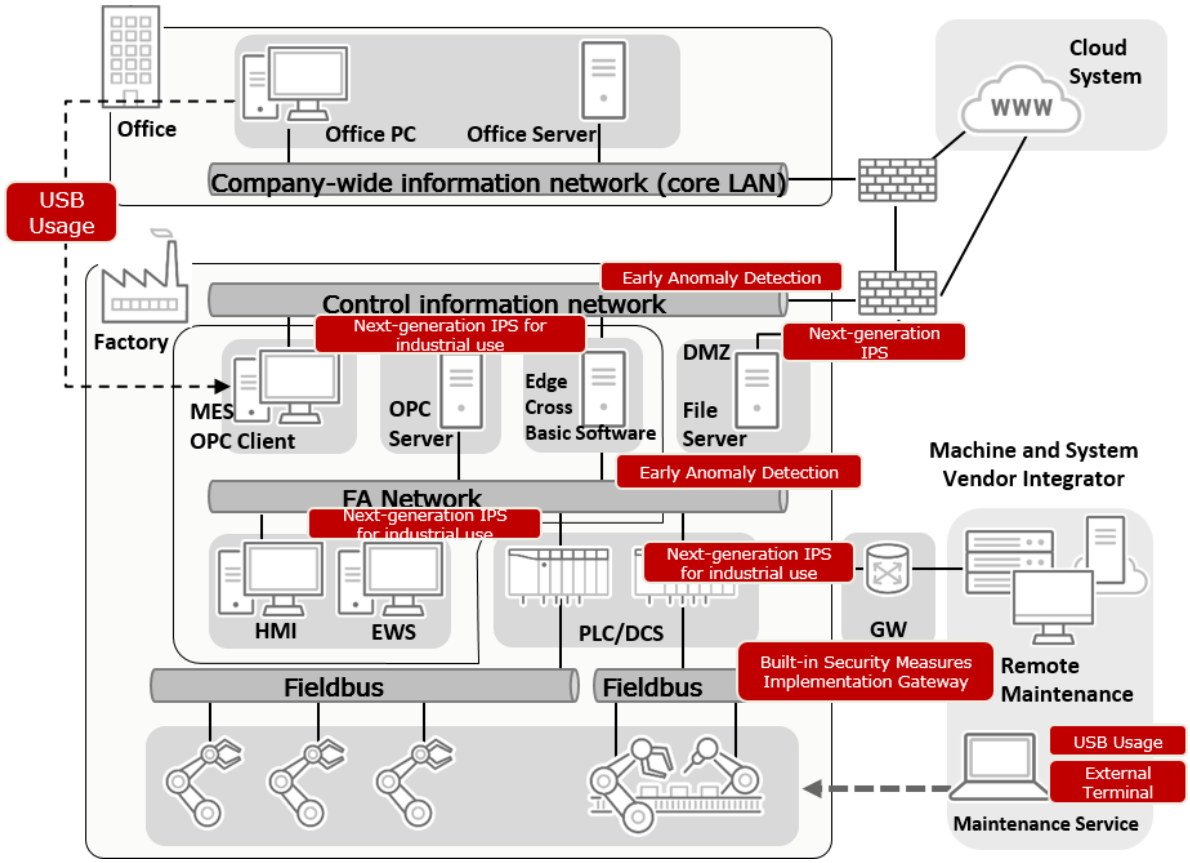


Figure 3-4 Example of Security Measures for the Network

[Network Measures]

The existing networks in the factory are divided into "control information network", "FA network" and "field bus" according to the utilization location.

(1) Countermeasure Policy

It is necessary to remove the risk of being connected to the network by taking countermeasures to prevent infection, detect after infection, and take measures to confirm, detect, and control infection conditions on the terminal.

(2) Asset Management

If you don't know which assets you need to protect, there is a possibility that there is a security measure leak or the situation cannot be confirmed at the time of an incident. Therefore, it is necessary to list information such as the control information network, equipment on the FA network, and the applications (Communication Protocols) used by the devices on the FA network, and create an asset management list. We recommend the installation of network visualization devices that can detect devices on the network from communication packet monitors, etc., and enable asset management, etc., which do not affect existing systems or existing networks.

(3) Network Composition Management

If you can't grasp the composition of the network, you may not be able to quickly confirm the scope of influence in case of emergency. Therefore, it is necessary to make a network structure diagram which can understand the physical composition, logical composition and data flow of control information network and FA network. It is recommended to set up network monitoring device and network visualization device. Network composition diagram can be drawn through data collection such as communication packet monitor and SNMP.

(4) Network Boundary Countermeasure

When connecting the control information network of the factory entrance and exit with a regular company-wide information system network (hereinafter referred to as IT system network), in order to prevent malicious software from entering the IT system network, firewall device (hereinafter referred to as FW device) should be set. In addition, it is not just the setting of FW devices. In view of the vulnerability countermeasures of industrial control system subordinate to control information network, it is recommended to add intrusion prevention system (next generation IPS) or install the next generation FW with the same function.

(5) Countermeasures for Early Anomaly Detection

In consideration of the event that a device on the network is infected with malicious software, the control information network recommends the installation of an internal countermeasure device (cyber attack detection sensor) that detects unauthorized behavior and abnormalities from network communications and visualizes risk threats and response priorities.

(6) Countermeasures for Illegal Communication Detection

In the application of factory network, besides human error, it can also be expected that people with malice will lead to serious situations. In addition, in the aspect of importing countermeasures, it must be considered not to increase the burden on the existing systems and networks, but also to simply import them later, so as to avoid involving excessive network knowledge, consuming set man-hours and so on. By preventing wrong operation and suspicious communication, it is effective to have the switch policy of automatically generating white list (access permission list) with setting function which can also prevent unauthorized internal access besides external attacks.

(7) Measures for SCADA, HMI (panel, etc.) and IPC using general-purpose operating system requiring long-term availability

Depending on the equipment, SCADA and HMI may be operated using panels with limited system resources. For control terminals where it is difficult to add security software due to circumstances, we recommend that you connect industrial next-generation IPS to the LAN port of the device as an alternative. This not only mitigates vulnerability countermeasures, but also leverages protocol whitelisting capabilities that support industrial control protocols and control commands to reduce the high-level communication of IPCs implemented by Edgecross basic software to MQTT and OPC-UA only.

(8) Countermeasures for USB Usage

Even if the IT system network which becomes the malware approach route is intercepted by the FW equipment, there is the necessity of the early abnormality detection countermeasure because when the device is connected to the network by the installation of Edgecross, the entry path from the USB device used in the operation of the site is not lost.

Even if you start collecting information via the network, it is difficult to remove the operation of USB from all points, and because it takes some time to complete. Even though you remove it, if there is a USB device in the site, at the point of data collection using a USB device, using a malware search and removal tool that does not require installation to ensure the health of your device.

The reason for using the tool which does not need to be installed is to suppress the load influence on the terminal by the installation of the anti-malware software, and there is a case where the installation of the anti-malware software is not allowed in the embedded terminal etc. provided by the manufacturer.

(9) Countermeasures for Portable PC

It has been reported that factory workers connected personal computers infected with malware to the network in the factory, leading to the spread of infection within the company. It is necessary to restrict not only in the safe operation rules, but also the connection to the factory network. In order to protect the factory network, do not affect the existing network structure, and prevent the connection between unregistered terminals and registered NG terminals, the network type countermeasures are effective. By blocking unregistered personal computers and private smart phones from the factory network, the factory network is protected from information disclosure caused by illegal access and malicious software infection.

(10) Importance of Introduction Design of Laying Network

The measures described so far are cases where the network status is known when laying the network in an existing environment.

・Current network environment is not clear

・Individual optimal network environments are built in units of equipment and can not be interconnected

・Laying a new network

When introducing Edgecross as an opportunity to promote the networking of factories, in order to effectively and safely use the network, we can adopt the method of effectively connecting devices without changing the address from the IP address repetition state between devices, and use the special method of micro-segment for the purpose of preventing malicious software from spreading.

Therefore, it is recommended to build professional integration to IP network, convey the purpose of network import and future utilization method, and rely on the design to realize the construction of network.

(11) Wireless Network

Since the spread of radio signals is a threat in wireless communications such as AGV, it is recommended to place radio signals in a factory network environment.

(12) Maintenance Services of Machine and System Integration Suppliers

In order to ensure security in providing a maintenance service in a large scale network environment, the remote GW connection is minimized and the following defense measures are recommended.

1. Use Dynamic virtual private network (D-VPN)
2. Whitelist access control of the equipment to be connected
3. Internet connection via industrial next-generation FW and GW

In addition, the system vendor integrator should be consulted with the operator of the factory to restrict the time.

Figure 3-5provides an example of where security measures for a network with a minimum configuration.

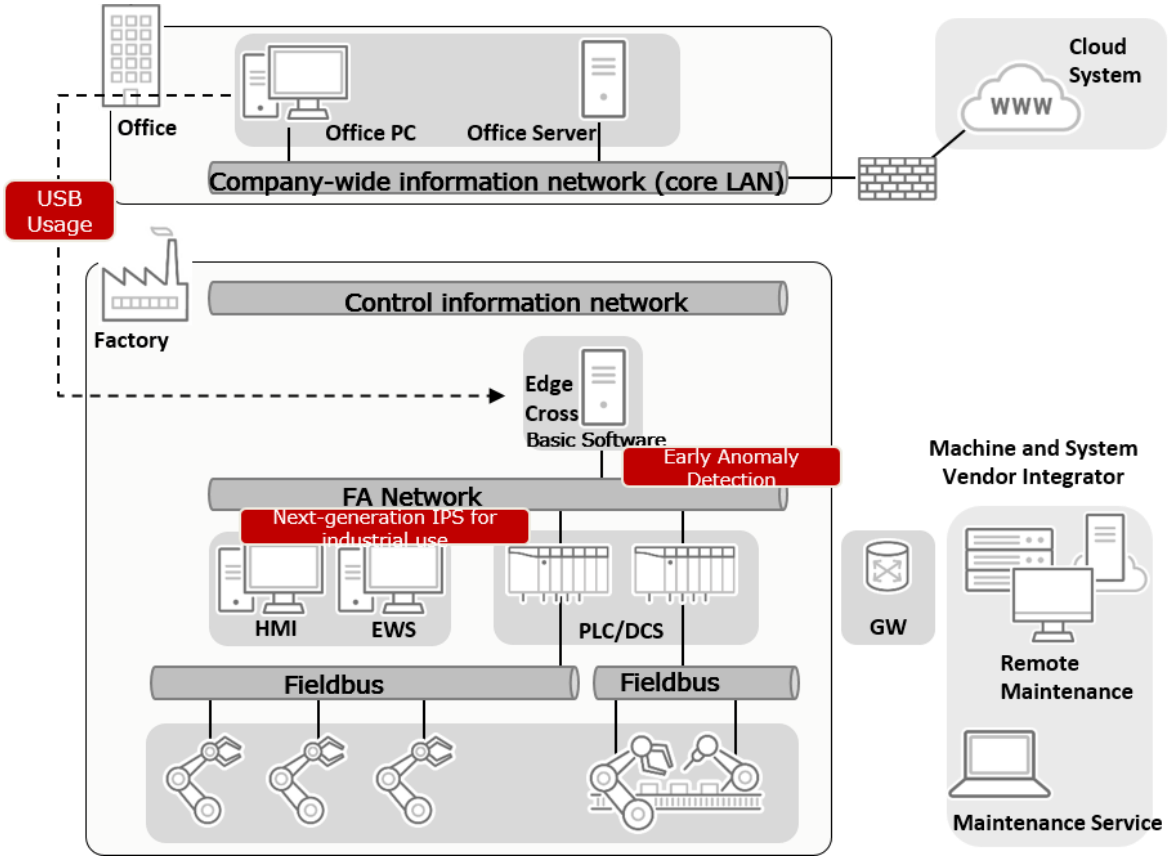


Figure 3-5 Example of security measures for a network with a minimum configuration

[Network Measures]

The network present in the factory is divided into "Control Information Network" "FA Network" and "Fieldbus" according to the place of use.

(1) Countermeasure Policy

At the initial stage of introduction of the policy, when a single network is configured and there is no Internet connection, USB used for data acquisition between office and factory. Industrial next-generation FW measures are taken for early detection of infection when using USB, etc.

For specific measures, please check the USB measures and early abnormality detection measures shown in the previous section.

4. Security Measures in Operations

Prior to operation, it is important to develop composition management as described above, user/administrator/administrator management, access management, log management, etc., and to continuously implement security management such as vulnerability/threat information collection and vulnerability management in addition to these managements after the start of operation. In addition, in order to respond quickly to emergencies, monitoring, anomaly detection, problem response (emergencies, permanent), and recovery systems must be in place.

In particular, we will discuss vulnerability countermeasures, security management, and incident response.

4. 1 Vulnerability Countermeasures

In recent years, malware has entered the factory site, and there have been many cases where factory operations are stopped due to diffusion activities. Malware penetrates from USB devices and carry-on devices and exploits vulnerabilities in devices on the network to spread the infection to other devices.

In order to reduce malware infection and spread activity, it is necessary to properly manage the assets of each device's operating system, applications, etc., and to apply the security patches timely.

Vulnerabilities can be addressed by versioning software for industrial PCs where Edgecross basic software is introduced and, if necessary, updates to Edgecross basic software, operating systems, and other applications. Here's how to update for each of the following areas.

(1) Edgecross Basic Software

To reduce the vulnerability, please use the latest version of Edgecross basic software. It is recommended that security patches be applied or upgraded after operation verification.

The latest version of Edgecross basic software is available on Edgecross marketplace.

The related OSS of the Edgecross basic software Windows version is shown in the table below.

From the security point of view, the operation has been confirmed, and it is best to use the new version.

In addition, if a vulnerability is exposed to the OSS you are using, the Edgecross Consortium will check the operation as soon as possible to ensure prompt disclosure of information.

OSS can be used in two ways.

One is the use of OSS source code and libraries in the edgecross basic software. If the vulnerability of this form is exposed to the vulnerability of this type of OSS and needs to be addressed, an update to the Edgecross basic software is required. See Edgecross Consortium Support for Edgecross Basic Software Updates.

The other is OSS, which operates independently outside of Edgecross basic software. It is up to the user to address this form of OSS vulnerability. Please obtain an update work after obtaining information of OSS and conducting the operation verification.

Please refer to the below url for the latest information.
https://www.edgecross.org/ja/data-download/

Table 4-1 Related OSS list of Edgecross basic software

	OSS Name	Usage Form
1	Eclipse Mosquitto	Used in Edgecross basic software
2	OpenSSL	Used in Edgecross basic software
3	PostgreSQL	Outside of Edgecross basic software
4	PSQLODBC.DLL	Outside of Edgecross basic software
5	pthread	Used in Edgecross basic software

(2) Edge Applications and Data Collectors

Edgecross member companies are developing edge applications and data collectors, so get information

from the developer or marketplace to take vulnerability countermeasures.

It is recommended to apply and upgrade security patches after verification of operation.

Edgecross Marketplace:
https://www.marketplace.edgecross.org/

(3) OS

Windows has the power to apply updates through Windows Update to keep them up-to-date. We recommend that you always keep up-to-date in a general-purpose environment.

However, some updates involve a restart, while others take a long time to update. Because there are some problems with the operating environment and compatibility, we recommend that you update it after confirming that there is actually no problem with the operation of Edgecross.

For industrial PCs and other applications, measures such as temporarily postponing the application of updates and providing test equipment to verify the operation of updates are effective. Microsoft provides Windows Server Update Services (WSUS) as a solution to control the application of Windows updates in your organization.

If you choose WSUS as the source for Windows updates, use Group Policy to set your Windows PC to the WSUS server. Windows Update periodically downloads updates to WSUS servers for management, approval, and deployment through the WSUS Management Console or Group Policy to simplify management of corporate updates.

(4) Hardware, BIOS, driver

Bios and drivers for industrial PCs and devices connected to them must also be addressed if they are vulnerable. We recommend that you obtain information from the developer, verify its operation, and apply it.

4. 2 Security Management and Incident Response

In the Edgecross system, various devices exist, and equipment and systems that are used for a long period of more than 10 years are also assumed. There are concerns about the occurrence of vulnerabilities associated with many environmental changes, such as adding equipment to the system, updating settings, and changing the network environment. In addition, new vulnerabilities may be discovered even if the equipment is not changed.

It is important to continuously manage security and respond even after the operation of edgecross system is started. In the whole system, there are many parties such as administrators, network administrators, system operators, suppliers of software and equipment. Organize the roles of parties in advance and establish a system so that they can systematically manage and respond to security.

- Consider and apply methods to properly implement critical equipment updates, etc. at the necessary time.
- The builders and operators of the edgecross system collect and analyze system vulnerabilities and send information to the parties concerned.
- Please inform relevant personnel of the risks arising from inadvertent connection to the system and what you want them to comply with.
- Please organize the role of the parties such as various equipment manufacturers, providers, system administrators and operators in the Edgecross system.
- Build a mechanism to understand vulnerable devices and systematically monitor them regularly.
- If you identify a vulnerable device, alert the administrator of the device and take the vulnerability response as soon as possible.

Reference:「IoT Security Guidelines ver 1.0」
2.5【[Operation and maintenance】Guideline 5 Maintain a safe and secure state, send and share information

Please be equipped with a system to respond quickly to incidents in advance.

- Please establish a mechanism to confirm the history of 3.4 edgecross basic software and 3.5 network log, monitor regularly and detect incidents as soon as possible. In addition, due to the requirement of highly professional monitoring, external SOC services can also be used flexibly when personnel are difficult to ensure.
- When detecting incidents, use pre-established response procedures to minimize damage.
- Quickly investigate the cause of the incident and perform recovery work by contacting and working with relevant personnel.

5. Summary

Use these guidelines to ensure the safety and security of FA systems using Edgecross.

If you have any questions about the information in this document, please fill out the inquiry form on the Edgecross Consortium website.

Edgecross Consortium Inquiry Form https://www.edgecross.org/ja/contact/form/

Appendix（Assets Statement）
Style1

No.		1	2	3	4	5	6	7	8
Asset Name		Progress Management Computer	Laptop (Wireless)	Firewall (Internet)	Firewall (Management Building)	Firewall (Factory)	File Server	MES Server	MES Client
Assets Class	Information Assets	○	○				○	○	○
	Control Assets								
	Network Assets			○	○	○			
Assets Function	Input/Output	○	○				○	○	○
	Data Storage						○		
	Order Publication							○	○
	Door			○	○	○			
Line Category		LAN(Wired)	LAN(Wired／Wireless)	LAN／WAN(Wired)	LAN／WAN(Wired)	LAN／WAN(Wired)	LAN(Wired)	LAN(Wired)	LAN(Wired)
Installation Site		Management Building	Management Building		Management Building	Factory(DMZ)	Factory(DMZ)	Factory(DMZ)	Factory
Connect to NW	Information Network	○	○	○	○				
	DMZ			○		○	○	○	
	Control Information Network			○		○			○
	Control Network								
	Network between controllers								
	Internet		○	○	○	○			
Management Port's Connection Destination		×	×	Information Network	Information Network	DMZ	×	×	×
Operation or Not I/F		○	○	×	×	×	○	○	○
USB/Deliver Letter I/F Usage		○(USB)	○(USB)	○(LAN)	○(LAN)	○(LAN)	○(USB)	○(USB)	○(USB)
Stable Use of Media, Equipment Connection or Not		×	×	×	×	×	×	×	×
Wireless function or not		×	○	×	×	×	×	×	×
Stable Operation, Unstable Operation		Stable Operation	Stable Operation	Stable Operation	Stable Operation	Stable Operation	Stable Operation	Stable Operation	Stable Operation
Data Types and Paths		Record separately							
Build Suppliers/Equipment Manufacturers		Company A／Company X	Company A／Company X	Company A／Company Y	Company A／Company Y	Company A／Company Y	Company A／Company X	Company A／Company X	Company A／Company X
OS Type/Version		Windows 10	Windows 10	Independent OS	Independent OS	Independent OS	Windows Server 2016	Windows Server 2016	Windows 10
Protocol		TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP
Security Policy(※)		Equipment connection and use restrictions[19], Authority management[23]	Equipment connection and use restrictions[19], Authority management[23]	FW(Packet filtering type)[1]	FW(Packet filtering type)[1]	FW(Packet filtering type)[1]	Equipment connection and use restrictions[19], Authority management[23]	Equipment connection and use restrictions[19], Authority management[23]	Equipment connection and use restrictions[19], Authority management[23]

※IPA records the safety countermeasures in "table 4-29 List of Safety Countermeasures Items" in "Guide for Safety Risk Analysis of Control System, 2nd Edition"

Appendix（Assets Statement）
Style1

No.		9	10	11	12	13	14	15	16
Asset Name		Engineering PC	Router	Edgecross Carrier PC 1	Edgecross Carrier PC 2	HMI	PLC	Control Machine 1	Control Machine 2
Assets Class	Information Assets	○		○	○				
	Control Assets					○	○	○	○
	Network Assets		○						
Assets Function	Input/Output	○		○	○	○			
	Data Storage								
	Order Publication	○		○	○	○	○		
	Door		○						
Line Category		LAN(Wired)	LAN(Wired)	LAN(Wired)	LAN(Wired)	LAN(Wired)	LAN(Wired)	LAN(Wired)	LAN(Wired)
Installation Site		Factory	Factory	Factory	Factory	Factory	Factory	Factory	Factory
Connect to NW	Information Network								
	DMZ								
	Control Information Network	○	○		○		○		
	Control Network		○	○					
	Network between controllers					○	○	○	○
	Internet			○	○				
Management Port's Connection Destination		×	Control Information Network	×	×	×	×	×	×
Operation or Not I/F		○	×	○	○	○	×	×	×
USB/Deliver Letter I/F Usage		○(USB)	○(LAN)	○(USB)	○(USB)	×	×	×	×
Stable Use of Media, Equipment Connection or Not		×	×	○	○	×	×	×	×
Wireless function or not		×	×	×	×	×	×	×	×
Stable Operation, Unstable Operation		Stable Operation	Stable Operation	Stable Operation	Stable Operation	Stable Operation	Stable Operation	Stable Operation	Stable Operation
Data Types and Paths		Record separately							
Build Suppliers/Equipment Manufacturers		Company A／Company X	Company A／Company Y	Company A／Company X	Company A／Company X	Company A／Company Z	Company A／Company Z	Company A／Company Z	Company A／Company Z
OS Type/Version		Windows 10	Independent OS	Windows 10	Windows 10	Independent OS	Independent OS	Independent OS	Independent OS
Protocol		TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	CC-LinkIE	TCP,UDP,CC-LinkIE	CC-LinkIE	CC-LinkIE
Security Policy(※)		Equipment connection and use restrictions[19], Authority management[23]		Equipment connection and use restrictions[19], Authority management[23]	Equipment connection and use restrictions[19], Authority management[23]				

Appendix（Assets Statement）
Style1

No.		17	18
Asset Name		Work Machine 1	Work Machine 2
Assets Class	Information Assets		
	Control Assets	○	○
	Network Assets		
Assets Function	Input/Output		
	Data Storage		
	Order Publication		
	Door		
Line Category		LAN(Wired)	LAN(Wired)
Installation Site		Factory	Factory
Connect to NW	Information Network		
	DMZ		
	Control Information Network		
	Control Network	○	○
	Network between controllers		
	Internet		
Management Port's Connection Destination		×	×
Operation or Not I/F		○	○
USB/Deliver Letter I/F Usage		×	×
Stable Use of Media, Equipment Connection or Not		×	×
Wireless function or not		×	×
Stable Operation, Unstable Operation		Stable Operation	Stable Operation
Data Types and Paths			
Build Suppliers/Equipment Manufacturers		Company A／Company Z	Company A／Company Z
OS Type/Version		Independent OS	Independent OS
Protocol		TCP,UDP	TCP,UDP
Security Policy(※)			

Appendix（Assets Statement）
Style 2

No.		1	2	3	4	6	7	8	9	10
Asset Name		Office PC	Engineering PC	File Server	Production Management Application	L2 Switch	Edgecross Carrier PC	Work Machine 1	Work Machine 2	Work Machine 3
Assets Class	Information Assets	○	○	○	○		○			
	Control Assets							○	○	○
	Network Assets					○				
Assets Function	Input/Output	○	○	○	○		○			
	Data Storage			○						
	Order Publication		○		○		○			
	Door					○				
Line Category		LAN(Wired)	LAN(Wired)	LAN(Wired)	LAN(Wired)	LAN(Wired)	LAN(Wired)	LAN(Wired)	LAN(Wired)	LAN(Wired)
Installation Site		Office	Office	Office	Office	Factory	Factory	Factory	Factory	Factory
Connect to NW	Information Network									
	DMZ									
	Control Information Network	○	○	○	○	○	○	○	○	○
	Control Network									
	Network between Controllers									
	Internet									
Management Port's Connection Destination		×	×	×	×	×	×	×	×	×
Operation or Not I/F		○	○	○	○	×	○	×	×	×
USB/Deliver Letter I/F Usage		○(USB)	○(USB)	○(USB)	○(USB)	×	○(USB)	×	×	×
Stable Use of Media, Equipment Connection or Not		×	×	×	×	×	○	×	×	×
Wireless function or not		×	×	×	×	×	×	×	×	×
Stable Operation, Unstable Operation		Stable Operation	Stable Operation	Stable Operation	Stable Operation	Stable Operation	Stable Operation	Stable Operation	Stable Operation	Stable Operation
Data Types and Paths		Record separately								
Build Suppliers/Equipment Manufacturers		Company A／Company X	Company A／Company X	Company A／Company X	Company A／Company X	Company A／Company Y	Company A／Company X	Company A／Company Z	Company A／Company Z	Company A／Company Z
OS Type/Version		Windows 10	Windows 10	Windows 10	Windows 10	Independent OS	Windows 10	Independent OS	Independent OS	Independent OS
Protocol		TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP
Security Policy		Equipment connection and use restrictions[19], Authority management[23]	Equipment connection and use restrictions[19], Authority management[23]	Equipment connection and use restrictions[19], Authority management[23]	Equipment connection and use restrictions[19], Authority management[23]		Equipment connection and use restrictions[19], Authority management[23]			

※IPA records the safety countermeasures in "table 4-29 List of Safety Countermeasures Items" in "Guide for Safety Risk Analysis of Control System, 2nd Edition"

Appendix (Attack Script) Style 1

※1：Attack stronghold refers to the machine and place where the target can be finally attacked
※2：The target of attack refers to the machine that is assumed to be the ultimate target of attack

No.	Business Loss	Business Loss Level	Summary of Business Loss and Attack Script								
1	Stop Wide-area Product Supply	3	Summary of Business Losses	Due to the network attack on manufacturing equipment, the supply of products stopped in the wide area, which brought great influence to the society and caused high losses such as compensation expenses. At the same time, the company's trust also dropped significantly.				Affected A,I,C		
			Script#	Attack Script	Attack Stronghold(※1)	Attack Target(※2)	Final Attack	Availability	Integrity	Confidentiality
			1-1	Due to the communication interference between MES Server and various devices, the production management data disappears, and the management of manufacturing processes and instructions to operators cannot be carried out, resulting in the production stop.	Information Network DMZ Control Information Network	MES Server	Due to the communication interference between MES Server and each device, the production management data disappears	○	○	-
			1-2	MES Server is infected with malicious software, which leads to the disappearance of production management data, unable to give instructions to the management and operators of manufacturing process, and leads to the stop of production.	Internet Information Network DMZ Control Information Network	MES Server	MES Server is infected with malware, and production management data disappears.	○	○	-
			1-3	PC equipped with Edgecross is infected with malicious software, and the production is stopped.	Internet DMZ Control Information Network Control Network	Edgecross Carrier PC	The PC equipped with Edgecross is infected with malware and performs production stop operation.	○	-	-
2	Stop the Supply of Products in Limited Areas	2	Summary of Business Losses	Due to the network attack on manufacturing equipment, the supply is stopped in a limited area, which has an impact on the society, resulting in compensation expenses and other losses, while the company's reliability is reduced.				Affected A,I,C		
			Script#	Attack Script	Attack Stronghold(※1)	Attack Target(※2)	Final Attack	Availability	Integrity	Confidentiality
			2-1	Unlicensed applications are installed on the PC equipped with Edgecross, which leads to processing performance failure and access delay.	Control Information Network Control Network	Edgecross Carrier PC	Unlicensed applications are installed on PCs equipped with Edgecross.	○	○	-
			2-2	Because HMI is infected with malicious software, it is impossible to carry out monitoring operations, so some production stopped.	Network between Controllers	HMI	HMI is infected with malicious software, which makes monitoring operations and other operations impossible.	○	-	-
			2-3	The vulnerability of the system is not fully understood, and it is still in a state of remaining vulnerability, and the vulnerability of the system is attacked.	Internet	Edgecross Carrier PC	The factory stopped due to non-compliant operation of servers and control machines.	○	-	-
			2-4	The identity confirmation and action monitoring of staff members are insufficient, and they are attacked by internal staff members.	Control Information Network Control Network	Edgecross Carrier PC	The factory stopped due to non-compliant operation of servers and control machines.	○	-	-
			2-5	Due to inadequate management of internal lines, they are accessed into non-compliant external lines without authorization, and are subjected to non-compliant connection and attack through external networks outside the supervision.	Internet	Edgecross Carrier PC	The factory stopped due to non-compliant operation of servers and control machines.	○	-	-
			2-6	Because the security policy of the information system terminal connected to the external network is not sufficient, it leads to the attack on the facility through the information system terminal.	Internet	Edgecross Carrier PC	The factory stopped due to non-compliant operation of servers and control machines.	○	-	-
			2-7	The security countermeasures of the network equipment used for external connection are not enough and are attacked by the external network connection.	Internet	Edgecross Carrier PC	The factory stopped due to non-compliant operation of servers and control machines.	○	-	-
			2-8	PCs equipped with Edgecross are not equipped with special management zones, which leads to non-compliance operation by personnel other than the specified operators.	Control Information Network Control Network	Edgecross Carrier PC	The factory stops, the set value is tampered, the information is leaked, etc. due to non-compliant operation.	○	○	○
			2-9	The entry and exit of the division set by the PC equipped with Edgecross is not properly managed, and non-compliant operation is carried out by personnel other than the specified operators.	Control Information Network Control Network	Edgecross Carrier PC	The factory stops, the set value is tampered, the information is leaked, etc. due to non-compliant operation.	○	○	○
			2-10	The PC equips with Edgecross does not authenticate the communication object, executes the non-compliant command, and is operated non-compliant.	Internet DMZ Control Information Network Control Network	Edgecross Carrier PC	The factory stops, the set value is tampered, the information is leaked, etc. due to non-compliant operation.	○	○	○

Appendix (Attack Script) Style 1

※1：Attack stronghold refers to the machine and place where the target can be finally attacked
※2：The target of attack refers to the machine that is assumed to be the ultimate target of attack

No.	Business Loss	Business Loss Level	Summary of Business Loss and Attack Script								
3	Supply of Products with Poor Specifications	2	Summary of Business Losses	Because of the network attack on manufacturing equipment, customers are provided with products that do not meet the specified specifications, which affects the society, causes losses such as compensation expenses, and at the same time reduces their trust in company.				Affected A,I,C		
			Script#	Attack Script	Attack Stronghold(※1)	Attack Target(※2)	Final Attack	Availability	Integrity	Confidentiality
			3-1	Because MES Server is infected with malicious software, the production management data is falsified, and the management of manufacturing processes and instructions to operators become meaningless instructions, resulting in the supply of products with poor specifications.	Internet Information Network DMZ Control Information Network	MES Server	MES Server is infected with malicious software and tampered with production management data.	○	○	－
			3-2	MES Client is infected with malicious software, and the production management data is tampered, which makes the management of manufacturing process and the instructions to operators become meaningless instructions, resulting in the supply of products with poor specifications.	DMZ Control Information Network Control Network	MES Client	MES Server is infected with malicious software and tampered with production management data.	○	○	－
4	Destruction of equipment	3	Summary of Business	Due to the network attack on manufacturing equipment, the equipment is destroyed and the supply stopped. At the same time, there are deaths and injuries of employees and nearby residents, which had a great impact on the society, caused high losses such as compensation expenses, and greatly reduced the trust in our company.				Affected A,I,C		
			Script#	Attack Script	Attack Stronghold(※1)	Attack Target(※2)	Final Attack	Availability	Integrity	Confidentiality
			4-1	By inputting inappropriate target values to PLC, the control of equipment is abnormal and the equipment is destroyed.	Control Information Network Network between Controllers	PLC	Enter an incorrect target value into the PLC	○	○	－
			4-2	Because the engineering PC is infected with malicious software, it is set as an unsuitable project, the equipment control is abnormal, and the equipment is destroyed.	DMZ Control Information Network Control Network	Engineering PC	The engineering PC is infected with malicious software, and the engineering settings are tampered with	○	○	－
			4-3	The vulnerability of HMI is not fully understood, and it is still in a state of remaining vulnerability, and the system vulnerability is attacked.	Network between Controllers	HMI	The stop of HIM leads to the occurrence of unsupervised state	○	－	－
			4-4	For the terminal setting place, the permitted entrants and exits are not restricted, and people other than the specified operators peek at the pictures and conduct non-compliant operations.	Factory	Engineering PC	Non-compliant operation leads to equipment stop, set value tampering, information leakage, etc	○	○	○
			4-5	The authority management and operation monitoring of the system are insufficient, and the specified operators overstep their authority and improperly operate the system and terminal/control panel.	Factory	Engineering PC	Non-compliant operation leads to equipment stop, set value tampering, information leakage, etc	○	○	○
			4-6	The login management and login information management of HMI are inadequate, and non-compliant login and operation are performed by people other than regular operators.	Factory	HMI	The equipment stops or the set value is tampered with due to illegal operation.	○	○	－
			4-7	The authority management and operation monitoring of HMI are not sufficient, and the specified operators overstep their authority and conduct non-compliant operation on the system and terminal.	Factory	HMI	The equipment stops or the set value is tampered with due to illegal operation.	○	○	－
			4-8	When connecting to external media such as USB without security confirmation, it is invaded by malicious software through external media.	External Media	Edgecross Carrier PC	Stop of PC equipped with Edgecross, tampering of settings, information leakage, etc.	○	○	○
			4-9	When connecting to an external import terminal without security confirmation, it is invaded by malicious software through the external import terminal.	External Import Terminal	Edgecross Carrier PC	Stop of PC equipped with Edgecross, tampering of settings, information leakage, etc.	○	○	○
			4-10	Idle ports of network devices are placed in a connectable state, connected by non-compliant terminals, and malware is imported.	FW's Blank Port	Edgecross Carrier PC	Stop of PC equipped with Edgecross, tampering of settings, information leakage, etc.	○	○	○
			4-11	Due to insufficient understanding of the vulnerability of the server, it is still in a state of remaining vulnerability, and the vulnerability of the system is attacked.	Internet Information Network DMZ Control Information Network	Edgecross Carrier PC	Stop of PC equipped with Edgecross, tampering of settings, information leakage, etc.	○	○	○
			4-12	PLC has no mechanism to authenticate the communication object, executes non-compliant orders and is forced to execute non-compliant actions.	Control Information Network Network between Controllers	PLC	The equipment stops or the set value is tampered with due to illegal operation.	○	○	－
			4-13	The ID and password of PLC are not set properly, so it is easy to be accessed by intruders for non-compliance operation.	Factory	PLC	The equipment stops or the set value is tampered with due to illegal operation.	○	○	－
			4-14	The vulnerability of machine tools and control machines is not fully understood, and the vulnerability remains, and the system vulnerability is attacked.	Control Network Network between Controllers	Machine tools, control machines	Stop of machine tool and control machine due to attack	○	－	－
			4-15	The gateway device has no mechanism to restrict the communication target, executes non-compliant commands and is forced to perform non-compliant actions.	Control Information Network Control Network	Router	The equipment stops or the set value is tampered with due to illegal operation.	○	○	－
			4-16	There are keys widely used in the industry on various control panels and distribution boards, which are easy to be unlocked, and non-compliant operation is carried out by personnel other than specified operators.	Factory	Each device	The equipment stops or the set value is tampered with due to illegal operation.	○	○	－
			4-17	The setting place of the switch and other network equipment is in a state that is not safely managed and can be touched by anyone. Personnel other than the designated operator shall carry out non-compliant operation.	Factory	FW, router	The equipment stops or the set value is tampered with due to illegal operation.	○	○	－

Appendix (Attack Script) Style 1

※1：Attack stronghold refers to the machine and place where the target can be finally attacked
※2：The target of attack refers to the machine that is assumed to be the ultimate target of attack

No.	Business Loss	Business Loss Level	Summary of Business Loss and Attack Script							
5	The cost of large-scale countermeasures	1	Summary of Business Losses	Under the network attack, although there is no disaster of stopping the supply of products, the vulnerability of the current countermeasures becomes obvious, and huge countermeasures cost is incurred in order to solve this problem.				Affected A,I,C		
			Script#	Attack Script	Attack Stronghold(※1)	Attack Target(※2)	Final Attack	Availability	Integrity	Confidentiality
			5-1	Because of maintenance and other reasons, they are connected without knowing the external connection, and they are infected and illegally invaded by malicious software through the external network connection outside the management.	Internet	MES Server	Data has been tampered with and information leaked due to malware infection and hacking	-	○	○
			5-2	The firewall has inadequate security measures and is invaded by external network.	Internet	MES Server	Data tampering and information leakage due to illegal intrusion	-	○	○
			5-3	Because the cloud server credit information management is not sufficient and outflow, the system was illegally accessed.	Internet	Server on Cloud	Data tampering and information leakage due to illegal intrusion	-	○	○
6	Leakage of confidential information	1	Summary of Business Loss and Attack Script	_				Affected A,I,C		
			Script#	Attack Script	Attack Stronghold(※1)	Attack Target(※2)	Final Attack	Availability	Integrity	Confidentiality
			6-1	Secretive information is leaked to the outside by physically invading the factory or stealing the production data of MES Server through the Internet.	Internet Factory	MES Server	Extract the production data of MES Server	-	-	○
			6-2	Physical intrusion into the factory, or stealing confidential information from FileServer through the Internet, and leaking it to the outside.	Internet Factory	FileServer	Stealing confidential information from FileServer	-	-	○
			6-3	Physical intrusion into the factory, or stealing confidential information from the PC equipped with Edgecross through the Internet, and leaking it to the outside.	Internet Factory	PC equipped with Edgecross	Stealing confidential information from a PC equipped with Edgec	-	-	○

Appendix (Attack Script) Style 2

※1：Attack stronghold refers to the machine and place where the target can be finally attacked
※2：The target of attack refers to the machine that is assumed to be the ultimate target of attack

No.	Business Loss	Business Loss Level	Summary of Business Loss and Attack Script								
1	Stop Wide-area Product Supply	3	Summary of Business Losses	Due to the network attack on manufacturing equipment, the supply of products stopped in the wide area, which brought great influence to the society and caused high losses such as compensation expenses. At the same time, the company's trust also dropped significantly.				Affected A,I,C		
			Script#	Attack Script	Attack Stronghold(※1)	Attack Target(※2)	Final Attack	Availability	Integrity	Confidentiality
			1-1	Due to the communication interference between production management application and various devices, the production management data disappears, and the management of manufacturing processes and instructions to operators cannot be carried out, resulting in the production stop.	Control Information Network	Production Management Application	Due to the communication interference between production management application and each device, the production management data disappears	○	○	-
			1-2	Production management application is infected with malicious software, which leads to the disappearance of production management data, unable to give instructions to the management and operators of manufacturing process, and leads to the stop of production.	Control Information Network	Production Management Application	Production management application is infected with malware, and production management data disappears.	○	○	-
			1-3	PC equipped with Edgecross is infected with malicious software, and the production is stopped.	Control Information Network	Edgecross Carrier PC	The PC equipped with Edgecross is infected with malware and performs production stop operation.	○	-	-
2	Stop the Supply of Products in Limited Areas	2	Summary of Business Losses	Due to the network attack on manufacturing equipment, the supply is stopped in a limited area, which has an impact on the society, resulting in compensation expenses and other losses, while the company's reliability is reduced.				Affected A,I,C		
			Script#	Attack Script	Attack Stronghold(※1)	Attack Target(※2)	Final Attack	Availability	Integrity	Confidentiality
			2-1	Unlicensed applications are installed on the PC equipped with Edgecross, and the processing performance fails and the access is delayed.	Control Information Network	Edgecross Carrier PC	Unlicensed applications are installed on PCs equipped with Edgecross.	○	○	-
			2-2	The identity confirmation and action monitoring of staff members are insufficient, and they are attacked by internal staff members.	Control Information Network	Edgecross Carrier PC	The factory stopped due to non-compliant operation of servers and control machines.	○	-	-
			2-3	PCs equipped with Edgecross are not equipped with special management zones, which leads to non-compliance operation by personnel other than the specified operators.	Control Information Network	Edgecross Carrier PC	The factory stops, the set value is tampered, the information is leaked, etc. due to non-compliant operation.	○	○	○
			2-4	The entry and exit of the division set by the PC equipped with Edgecross was not properly managed, and non-compliant operation was carried out by personnel other than the specified operators.	Control Information Network	Edgecross Carrier PC	The factory stops, the set value is tampered, the information is leaked, etc. due to non-compliant operation.	○	○	○
			2-5	The PC equipped with Edgecross has no authenticated communication object, and has executed non-compliant commands and been subjected to non-compliant operations.	Control Information Network	Edgecross Carrier PC	The factory stops, the set value is tampered, the information is leaked, etc. due to non-compliant operation.	○	○	○
3	Supply of Products with Poor Specifications	2	Summary of Business	Due to the network attack on manufacturing equipment, products that do not conform to the specified specifications are provided to customers, which has an impact on the society and losses such as compensation expenses, while the company's reliability is reduced.				Affected A,I,C		
			Script#	Attack Script	Attack Stronghold(※1)	Attack Target(※2)	Final Attack	Availability	Integrity	Confidentiality
			3-1	Because the production management application program is infected with malicious software, the production management data is tampered, and the instructions to the operators in the management of the manufacturing process become unintentional instructions, resulting in the supply of products with poor specifications.	Control Information Network	Production Management Application	The production management application is infected with malicious software and falsifies the production management data	○	○	-

Appendix (Attack Script) Style 2

※1：Attack stronghold refers to the machine and place where the target can be finally attacked
※2：The target of attack refers to the machine that is assumed to be the ultimate target of attack

No.	Business Loss	Business Loss Level	Summary of Business Loss and Attack Script							
4	Destruction of equipment	3	Summary of Business	Due to the network attack on manufacturing equipment, the equipment was destroyed and the supply stopped. At the same time, there were deaths and injuries of employees and nearby residents, which had a great impact on the society, caused high losses such as compensation expenses, and greatly reduced the reliability of our company.				Affected A,I,C		
			Script#	Attack Script	Attack Stronghold(※1)	Attack Target(※2)	Final Attack	Availability	Integrity	Confidentiality
			4-2	Because the engineering PC was infected with malicious software, it was set as an unsuitable project, the equipment control was abnormal, and the equipment was destroyed.	Control Information Network	Engineering PC	The engineering PC was infected with malware and the engineering Settings were tampered with.	○	○	-
			4-4	For the terminal setting place, the permitted entrants and exits are not restricted, and people other than the specified operators peek at the pictures and conduct non-compliant operations.	Factory	Engineering PC	Non-compliant operation leads to equipment stop, set value tampering, information leakage, etc	○	○	○
			4-5	The authority management and operation monitoring of the system are insufficient, and the specified operators overstep their authority and improperly operate the system and terminal/control panel.	Factory	Engineering PC	Non-compliant operation leads to equipment stop, set value tampering, information leakage, etc	○	○	○
			4-8	When connecting to external media such as USB without security confirmation, it is invaded by malicious software through external media.	External Media	Edgecross Carrier PC	Stop of PC equipped with Edgecross, tampering of settings, information leakage, etc.	○	○	○
			4-9	Malicious software intrudes into the external bring-in terminal when connecting the external bring-in terminal without security confirmation.	External Bring-in Terminal	Edgecross Carrier PC	Stop of PC equipped with Edgecross, tampering of settings, information leakage, etc.	○	○	○
			4-10	Idle ports of network devices are placed in a connectable state, connected by non-compliant terminals, and malware is imported.	L2 Switch's Blank Port	Edgecross Carrier PC	Stop of PC equipped with Edgecross, tampering of settings, information leakage, etc.	○	○	○
			4-11	Due to insufficient understanding of the vulnerability of the server, it is still in a state of remaining vulnerability, and the vulnerability of the system is attacked.	Internet Information Network DMZ Control Information Network	Edgecross Carrier PC	Stop of PC equipped with Edgecross, tampering of settings, information leakage, etc.	○	○	○
			4-14	The vulnerability of machine tools and control machines is not fully understood and is in the state of residual vulnerability, and the vulnerability of the system is attacked.	Control Information Network	Machine Tool	Stop of machine tool due to attack	○	-	-
			4-16	There are keys widely used in the industry on various control panels and distribution boards, which are easy to be unlocked, and non-compliant operation is carried out by personnel other than specified operators.	Factory	Each device	The equipment stops or the set value is tampered with due to illegal operation	○	○	-
			4-17	The setting places of network equipment such as switches are in a state where anyone can contact them without safety management, and non-compliant operation is carried out by personnel other than the specified operators.	Factory	L2 Switch	The equipment stops or the set value is tampered with due to illegal operation	○	○	-
5	The cost of large-scale countermeasures	1	Summary of Business	Although there is no disaster of stopping the supply of products due to cyber attacks, the vulnerability of existing countermeasures becomes obvious, and huge countermeasures costs are incurred to solve this problem.				Affected A,I,C		
			Script#	Attack Script	Attack Stronghold(※1)	Attack Target(※2)	Final Attack	Availability	Integrity	Confidentiality
6	Disclosure of confidential information	1	Summary of Business Losses	_				Affected A,I,C		
			Script#	Attack Script	Attack Stronghold(※1)	Attack Target(※2)	Final Attack	Availability	Integrity	Confidentiality
			6-1	Due to physical intrusion into the factory, confidential information is obtained from File Server and leaked to the outside.	Factory	File Server	Stealing confidential information from File Server	-	-	○
			6-2	Due to physical intrusion into the factory, confidential information was obtained from the PC equipped with Edgecross and leaked to the outside.	Factory	Edgecross Carrier PC	Stealing confidential information from a PC equipped with Edgecross	-	-	○