Edgecross

Security Guidelines Overview

Ver. 1.0.0

Edgecross Consortium Technical Meeting Security Guidelines Formulation WG

ECD-TE4-0004-01-EN

Technical Meeting Security Guidelines Formulation WG Participants (titles omitted, random order)

TACHIBANA ELETECH CO., LTD.

DMG MORI CO., LTD.

NEC Corporation

Hitachi, Ltd.

FUJITSU LIMITED

Mitsubishi Electric Corporation

Revision history

Ver.	Revised Content	Year and Month
1.0.0	First Edition	2019/9

Table of Contents

1. Introduction

1. 1 Overview

In the manufacturing industry, the use of the Internet of Things (IoT) is accelerating to strengthen competitiveness and create new value. Based on this trend, “Edgecross Consortium” goes beyond the boundaries of companies and industries, and consortium members build together to realize collaboration between FA (Factory Automation) and IT (Information Technology). We offer an open edge computing software platform “Edgecross” from Japan. While the collaboration between FA and IT can be expected to improve the productivity of factories and plants, the threat of attack from inside and outside the FA system also increases. In order to reduce threats, it is desirable to take various measures such as human, physical, and connected networks in multiple layers. This document shows security points that should be considered when building an FA system using Edgecross, and it is a guideline for ensuring safety and security. As security measures recommended for customers, the points from hardware / OS, security software, Edgecross basic software and network are listed.

1. 2 Scope of This Document

The intended audience for this document is engineers who build Edgecross systems, administrators of Edgecross systems, and users of Edgecross systems.

This document is a guideline for Edgecross system security measures based on the IoT Security Guidelines published by the IoT Acceleration Consortium / Ministry of Internal Affairs and Communications / Ministry of Economy, Trade and Industry.

Table 1-1 shows the correspondence between the main points of the security countermeasure guidelines and the locations described in this document.

Table 1-1 Key points and description points of security countermeasure guidelines

“IoT Security Guidelines” ver 1.0 (IoT Acceleration Consortium / Ministry of Internal Affairs and Communications / Ministry of Economy, Trade and Industry) List of security measures			Where to find this document
Major item	Guidelines	Main Points	
Policy	Policy 1 Establishing a basic policy that considers the nature of IoT.	Point 1. Manager commits IoT security.	1.3
		Point 2. Avoid internal fraud and mistakes.	1.3
Analysis	Policy 2 Recognize IoT risks.	Point 3. Identify what to protect.	2.2
		Point 4. Assume the risks of being connected.	2.3
		Point 5. Assume the risks of spreading through connections.	2.3
		Point 6. Recognize physical risks.	2.3
		Point 7. Lesson Learnt from the past.	2.4
Design	Policy 3 Think of a design that protects what should be protected.	Point 8. Design for individual and overall protection.	3.1
		Point 9. Designed to avoid confusion for connected people.	3.1
		Point 10. Ensure consistency for safety and security in design	3.1
		Point 11. Ensure safety and security even when connected to unspecified partners in design.	3.1
		Point 12. Verificate and evaluate the designs that realized safety and security.	3.1
Construction and Connection	Policy 4 Think about measures on the network.	Point 13. Provide a function to grasp and record the state of equipment, etc.	3.2, 3.3, 3.4
		Point 14. Connect to the network appropriately according to function and application.	3.2, 3.3, 3.4, 3.5
		Point 15. Pay attention to the initial settings.	3.2, 3.3, 3.4, 3.5
		Point 16. Introduce the authentication function.	3.2, 3.3
Operation And	Policy 5	Point 17. Maintain safety and security even after shipment and releasement.	4.1

"IoT Security Guidelines" ver 1.0 (IoT Acceleration Consortium / Ministry of Internal Affairs and Communications / Ministry of Economy, Trade and Industry) List of security measures			Where to find this document
Major item	Guidelines	Main Points	
Maintenance	Maintain a safe and secure Send and share information safety and confidently.	Point 18. Understand IoT risks even after shipment and releasement, and inform relevant parties what should be protected.	4.2
		Point 19. Let general users know the risks of connecting.	4.2
		Point 20. Recognize the roles of stakeholders in IoT systems and services.	4.2
		Point 21. Identify vulnerable devices and call attention appropriately.	4.2

1. 3 Basic Policy

1. 3. 1 Cyber Security Management

In cyber security measures for systems using IoT, it is important to establish basic policies that take into account the nature of IoT systems. Security measures can be costly, and you may be faced with situations that require judgment beyond the discretion of the operations site. Therefore, it is necessary for the level of management to take the lead in presenting security policy.

For security measures, it is also necessary to establish a system for coordinating and responding to various locations and to develop human resources who can utilize security technology. Furthermore, it is also required to respond to human threats such as the possibility of internal fraud that threatens safety and unintentional mistakes.

Please refer to the "Cyber Security Management Guidelines" published by the Information-technology Promotion Agency, Ministry of Economy, Trade and Industry.

The Edgecross Consortium also sends out security information about the Edgecross system, please utilize it per requirement

1. 3. 2 Edgecross Consortium

The Edgecross Consortium is an organization that promotes platforms for the development of industry, and work on for the following three important targets to contribute to maintaining and improving the safety and security of customers' usage environments continuously..

・Building an organization and system to ensure safety and security

This consortium establishes a system for promptly responding to security-related problems, and when security incidents occur, it cooperates with public organizations to provide prompt responses and provide information to customers. In addition, we will investigate in threat trends, technologies, systems, etc., and endeavor to publicize to this consortium member company and all customers in order to maintain correct knowledge and high awareness of security.

・Product development for safety and security

This consortium together with member companies formulates security guidelines for developers and develops products appropriately so that appropriate security measures are taken, through analyzing the threats that may cause threats to the assets that being protected, designing robust products, and maitaining a safe and secure state after shipment and release.

・Provision of security guidelines for customers

The consortium considers that it is desirable to take various measures such as human, physical and network in order to reduce threats. For this reason, this consortium provides security guidelines for the proper operation of FA systems that have introduced Edgecross compatible products, and supports the introduction and maintenance of security measures in the usage environment of Edgecross.

1. 4 Abbreviation

BIOS	Basic Input Output System
CPU	Central Processing Unit
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
I/F	Interface
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
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
PC	Personal Computer
PIN	Personal Identification Number
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
TLS	Transport Layer Security
TPM	Trusted Platform Module
USB	Universal Serial Bus
WWW	World Wide Web

1. 5 Terms

The terms used in this manual are shown in Table 1-1.

Table 1-1 Terms

Terms	Explanation
IT System	A system that uses data from production sites using IT. In this document, it is used in particular to mean an external system connected to the production site via LAN or the Internet.
Edgecross System	System using Edgecross.
Edgecross Software	A general term for Edgecross basic software, edge applications, and data collectors.
Edgecross Basic Software	Software that implements Edgecross functionality. In conjunction with edge applications, it can perform analysis and diagnosis of production site data, and exchange data with on-premises and cloud IT systems.
Edge Application	Software that executes various processes for data utilization at production sites by utilizing the functions provided by Edgecross in the edge computing area.
Data Collector	A software component that collects production site data via each network, and is provided by each vendor for various networks and connected devices.

1. 6 Related Documents

Table 1-2 shows the related documents of this manual.

Table 1-2 Related Documents

No.	Document Name	Document No	How to Get
1	IoT Security Guideline ver 1.0 July, Heisei 28 IoT Acceleration Consortium, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry	－	http://www.soumu.go.jp/main_content/000428393.pdf
2	Cyber Security Management Guidelines Ver 1.0 December, Heisei 27 Ministry of Economy, Trade and Industry, Independent Administrative Institution, Information-technology Promotion Agency	－	http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf
3	Edgecross Specification Overview	ECD-TE1-0002	Edgecross Consortium member-only page
4	Edgecross Basic Software Windows Edition User's Manual	ECD-MA1-0001	Market Place（Edgecross Basic Software Windows Edition Product Document）

2. Edgecross System

This chapter describes the features of the system, assets to be protected, possible threats, and security incident cases.

2. 1 System Features

Edgecross is an open edge computing software platform that enables collaboration between FA and IT. It is possible to build an ecosystem by combining multi-vendor components in the edge computing field.

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

In addition, since IT systems are used to handle multiple sites and long-term data, edge computing also enables seamless collaboration between production sites and IT systems.

2. 2 Assets to Protect

Figure 2-1 shows the total assets to be protected based on Edgecross. Assets that need to be protected from various security threats can be roughly classified into four categories: data, hardware / OS, Edgecross software and related software, and networks.

The data include operation information, sensor information, data generated by machine tools and industrial robots, and NC programs that are necessary for operation, but Edgecross does not handle NC programs.

Hardware / OS include industrial PC and Windows OS.

Edgecross software include Edgecross basic software peforming real-time date processing and data model management, edge applications such as operation monitoring that performs various processes by using production site data, and data collector that collects data of the production site via the FA network described later. There is also a development kit as related software.

The network includes FA networks such as control networks and field networks that transfer production site data, and information networks that link with IT systems such as MES and ERP.

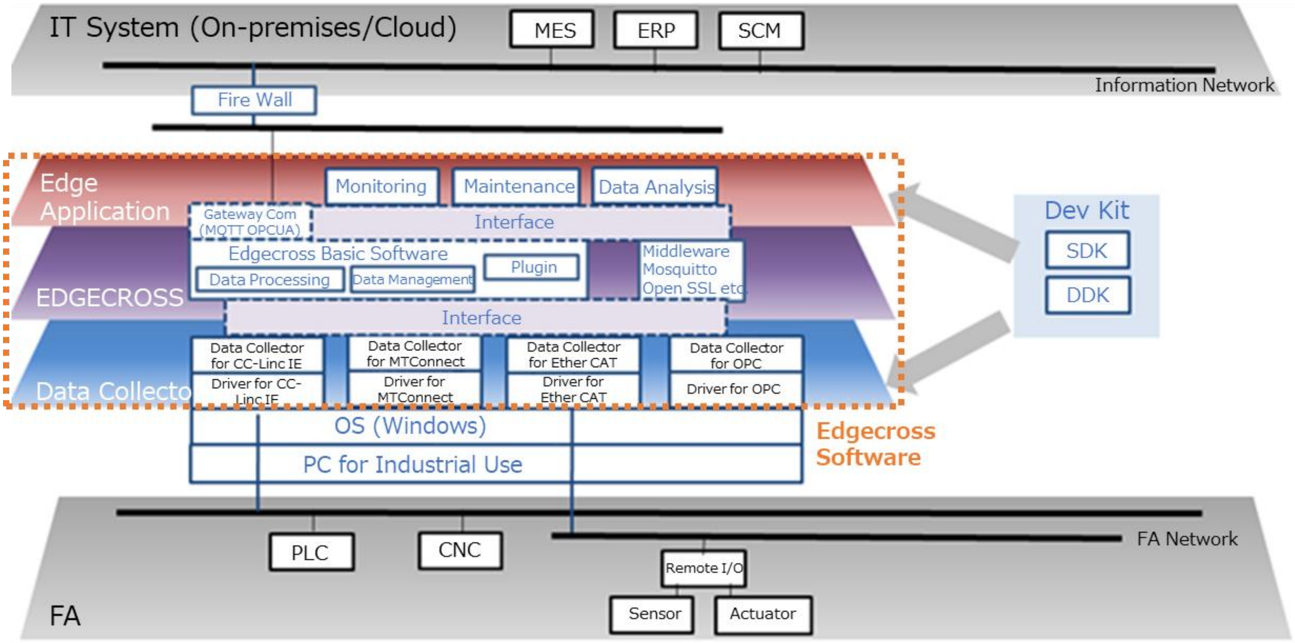

Figure 2-1 Assets to protect at Edgecross

2. 3 Possible Threat

List the possible security threats in the above system. The impacts of these threats are assumed to be product supply interruptions, accidents such as fires, and production of defective products.

(1) Impersonation

There is a threat that another user's Windows account (ID and password) is obtained by analogy or fraudulence, and impersonated by the user, resulting in unauthorized login to an industrial PC.

(2) Information leak

The threat of illegally reading production site data collected by Edgecross basic software is assumed. There is also a threat that software such as edge applications can be read illegally from industrial PCs.

(3) Malware

There is a threat that malicious software such as malware is installed on industrial PCs.

(4) Unauthorized communication

There is a threat that malware lurking on industrial PCs communicates illegally with external devices.

(5) Falsification

There is a threat that malware lurking on industrial PCs may illegally rewrite software such as edge applications and hinder the functionality of the software. In addition, it is possible that the production site data collected by Edgecross basic software will be illegally rewritten by malware, creating threats that generate inappropriate tabulation results and triggers for the next process.

(6) DoS / DDoS attack springboard

There is a threat that an industrial PC infected with malware is used as a springboard for DoS / DDoS attacks on servers.

(7) Abuse the vulnerability

Threats such as malware being installed on industrial PCs by abusing the vulnerability of the OS and installed software are assumed.

(8) Physical attack

The threat of a physical attack, such as a suspicious person physically invading and stealing an industrial PC, is assumed.

2. 4 Security Incident Cases

Figure 2-2 shows an example of a power plant incident that occurred in Ukraine. There was a cyber-attack at a power supply company, causing a large-scale blackout in 1.4 million households, including public infrastructure. This attack started with a targeted attack email from the outside, infecting employee terminals, trying to spread inside, and finally causing the power generation facility to malfunction through the SCADA system.

This example shows the possibility of cyber-attacks even in control system environments that are not directly connected to the Internet.

The factory environment where the Edgecross system is located also is not connected with the Internet, but similarly, it should be recognized that security risks remain and security measures must be taken.

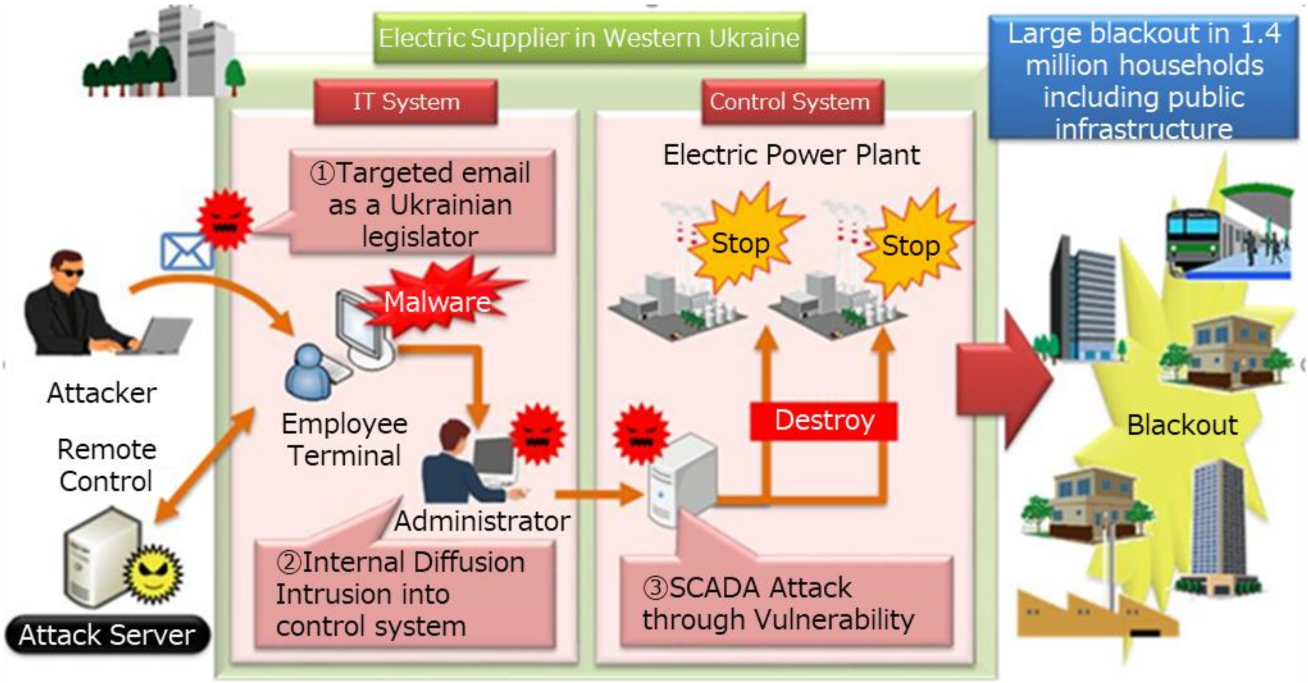
Electric Supplier in Western Ukraine
IT System
Control System
Large blackout in 1.4 million households including public infrastructure
①Targeted email as a Ukrainian legislator
Malware
Attacker
Employee Terminal
Remote Control
Administrator
Attack Server
②Internal Diffusion Intrusion into control system
Electric Power Plant
Stop
Stop
Destroy
③SCADA Attack through Vulnerability
Blackout

Figure 2-2 Incidents at power generation facilities

3. Construction

3. 1 Main Points of Construction

When constructing the Edgecross system, clarify the object to be protected and design the system from the following viewpoints (1) to (5) so that the object can be protected.

The following points are listed in the "IoT Security Guidelines". For the Edgecross system, please refer to the "IoT security guidelines" for construction.

(1) Design that can protect individually and collectively both

Consider countermeasures for individual devices / systems for risks due to external interface / internal / physical contact. Also, if their countermeasures are not enough, consider countermeasures using the higher-level IoT devices / systems that contain them.

(2) Design that won't confuse the users being connected

Design a device / system that can detect abnormalities, and consider the appropriate behavior when abnormalities are detected.

(3) Ensuring the integrality of the design that safety and security be realized

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

(4) Design that ensure safety and security even when connected to unspecified partners

Consider a design that can determine how to connect according to the counterpart to which the device / system is connected.

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

For connected devices and systems, consider the risks unique to the IoT, verify and evaluate the design to achieve safety and security.

In order to reduce threats, it is desirable to take various measures such as human, physical, and connected networks in multiple layers. It is recommended that customers introduce the following security measures.

3. 2 Hardware/OS

3. 2. 1 Hardware

(1) Procurement

Edgecross can be installed on industrial PCs from various manufacturers. For the construction of safe and secure equipment, procure industrial PCs from highly reliable sources.

Supplier has a contact window for device support and is easily accessible, and that technical information such as device specifications and firmware updates is available.

Please be noted that there may be problems with the distribution channel even if the product is from a reliable manufacturer. For example, there may be cases where second-hand goods that are maliciously mixed with malware are sold.

(2) Installation

Also pay attention to protect from physical attacks when installing industrial PCs.

・Measures against physical theft using a lockable PC rack and security wire lock

・Measures for physical connection by USB / LAN physical lock

・Operator entry / exit restrictions

These measures vary depending on the usage environment, so please implement them according to the environment.

(3) Initial setting

Industrial PCs have several security settings. Set appropriately according to the operating environment and the software to be operated. The typical setting items are listed below. For details, refer to the industrial PC manual.

- Password settings such as BIOS password and HDD password
- Boot drive settings
- USB settings
- Setting functions that enable external control such as Wake on Lan
- Security chip settings such as TPM

(4) Update

Update the firmware and BIOS of the CPU and chipset, and the firmware and drivers of the storage and network cards appropriately. When obtaining updated software, use a reliable website to ensure that the software has not been tampered with.

Also, keep in mind that there is a possibility that the firmware etc. may have been updated when each hardware item is shipped to actual use. Please check the update information.

(5) Operation

Check the support period of the hardware (and accompanying software). Operation within the support period is recommended.

If you have to continue operation beyond the support period, be aware of the risk that the support period of the current equipment has passed, and perform appropriate management.

If the device is unused and unmanaged, it may be a security risk that the unmanaged device is operating, so turn off the device.

3. 2. 2 OS

The Edgecross basic software runs on Microsoft® Windows® 10 Operating System (hereinafter referred to as Windows). In this chapter, basic guidelines for Windows operation are described, but the actual implementation details should be selected appropriately according to the operating environment of the Edgecross device.

Windows functions and terminology may change in future updates. For details, refer to the information on the Microsoft website.

(1) Account password

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

For user authentication, in addition to Windows account and password, PIN authentication, biometrics authentication, and two-step authentication / multi-factor authentication combine can also be used.

When a significant change is made to the Windows system, a security function (user account control function) that requires permission from the administrator user is provided. It is recommended to enable this function.

Windows has a function to memorize various user names and passwords. Storing information such as network access credentials and web page usernames and passwords in the system may lead to security risks, so it is recommended not to store them unless necessary.

(2) Setting

Windows includes various applications and services. It is recommended to disable unnecessary functions when using Edgecross. In particular, disable personal use functions that are not necessary for Edgecross, such as camera functions and microphone functions. Also, limit or disable physical access from outside such as USB and Bluetooth as much as possible.

As a countermeasure against malware, use the security function installed in Windows or install third-party security software. It is also recommended to block unnecessary network access with a personal firewall.

(3) Update

Windows has a function to apply updates with Windows Update. It is recommended to update to the latest status according to the environment. However, as a practical matter, some update programs may require restart, some update takes time, some are incompatible with the operating environment, and some have problems, which may hinder Edgecross operations. Keep these conditions in mind.

It is effective to temporarily postpone the application of the update program and prepare test equipment for verifying the operation of the update program.

Microsoft offers Windows Server Update Services (WSUS) as a solution to control the application of updates.

We recommend Windows Update as a part of equipment maintenance and systematic operation.

3. 3 Security Software

Security software is a general term for application software used for computer security measures.

The general function of this software is to prevent entry into the system and infection with malware.

It is recommended to install security software to prevent unauthorized software from starting on Edgecross basic software and certified products, and recommended industrial PCs (to detect and prevent the start and operation of malware).

Before installation, please contact the vendor of security software.

If been infected by malware, etc., in general Windows machines, there are the following effects as examples.

- Malware is installed
- Tampering, disappearance or leakage of various data
- Be used as a springboard to attack other systems

After installing security software, we recommend that you consider the following three points.

(1) Contract renewal

Security software may have a limited usage period such as one year or multiple years depends on the license agreement.

It is necessary to renew the license agreement so that it can be used continuously while the system is running.

(2) Update

Update security software features to improve detection of security threats.

Malware detection patterns are often updated daily, so regular updates are required.

In addition, if security software is enhanced on a large scale, it will be upgraded, so please consider introducing it.

(3) System scan

Regularly scan the entire system. Because the CPU load increases during the scan execution, it is recommended to execute scan according to the system operation performance.

3. 4 Edgecross Basic Software

Edgecross basic software runs on Windows and consists of the following software. By linking with edge applications, you can perform analysis and diagnosis of production site data, or exchange data with on-premises and cloud IT systems.

Table 3-1 Edgecross basic software configuration

Software	Content
Real-time flow manager	Software that implements functions for real-time diagnosis and feedback of production site data. You can use a data collector (software that collects production site data over a network) to collect data from connected equipment, equipment, or lines for data processing and analysis. You can also use plug-ins to enhance functionality.
Real-time flow designer	Software that implements functions for creating, saving, and displaying various settings necessary for Realtime Flow Manager operation, starting / stopping Realtime Flow Manager operation, and performing diagnostics.
Management shell	Software that models device, equipment, or line data on the production floor and manages it as a hierarchical structure. It runs in the background on Windows as a Windows service. Data collectors can be used to read and write data to connected equipment, devices, or lines.
Management shell explorer	Software for setting and referencing the data model managed by the Management shell.

Since the latest Edgecross basic software incorporates countermeasures for known vulnerabilities, please use the latest version of Edgecross basic software. It is recommended to perform the operation after verifying the operation. The main security-related functions and points to note in the Edgecross basic software are as follows. For details, see the Edgecross Basic Software Windows User's Manual.

(1) OPC UA connection function

The management shell operates as an OPC UA server and has a function (OPC UA connection function) that provides model access I / F and data access I / F to edge applications that are OPC UA clients. At this time, it is possible to perform authentication using the client certificate of the edge application.

(2) Edge application linkage function using MQTT

Data (collected data, processed data) can be distributed from the real-time flow manager to the edge application, and encrypted with TLS when response data is received from the edge application.

(3) Event history

Acquires event information generated by the real-time flow manager and the data collector used by the real-time flow manager, and displays the event history and detailed event information, cause, and action method as diagnostic information. Since the event history is saved even if the industrial PC running the real-time flow manager is turned off, it can be used to investigate factors of problems by the confirmation after restarting the industrial PC or the operation information before and after. It can also be used when the error code cannot be confirmed when an error occurs.

(4) File save function

When specifying a remote shared folder as the save destination in the file save function of the data collected / processed by the Realtime Flow Manager or the data of the diagnosis result, it is recommended to restrict access by Windows firewall as appropriate.

3. 5 Network

The following is a method using a network as a security measure for assets to be protected.

[Examples of network security measures]

Figure 3-1 shows an example of network security measures.

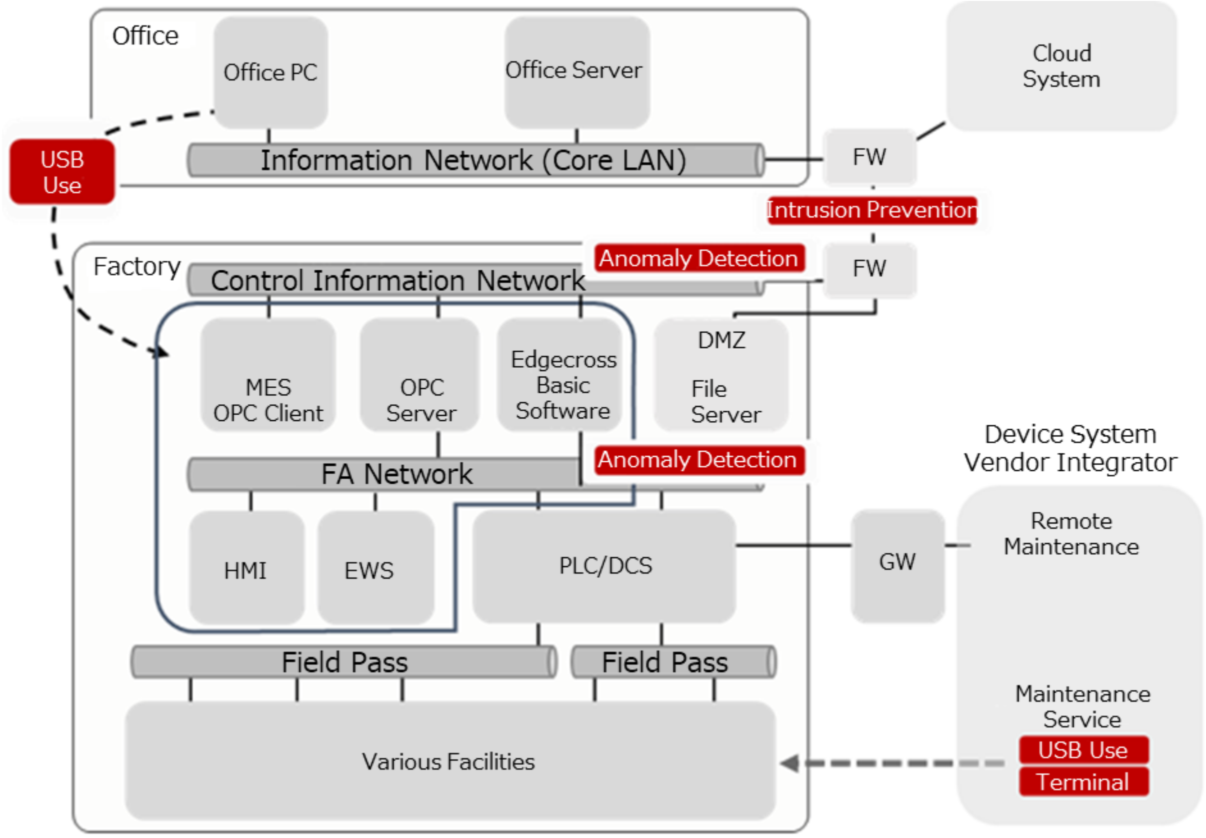

Figure 3-1 Examples of network security measures

[Network measures]

The network that exists in the factory is divided into "Control Information Network", "FA Network", and "Fieldbus" according to the usage location.

(1) Countermeasure policy

It is necessary to eliminate the risks that occur when connected to the network, by taking measures to prevent infection and detect after infection on the network, check the infection status, detect and remove on the terminal side.

(2) Network boundary measures

When connecting the control information network at the factory entrance to the normal company-wide information system network (hereinafter referred to as IT network), a firewall device (hereinafter referred to as FW device) is installed to prevent malware from entering the IT network. However, it is recommended not to be a simple FW device, but to be a FW device equipped with a next-generation intrusion prevention system that considers vulnerability countermeasures.

(3) Early abnormality detection measures

In the control information network, considering the time when a device on the network is infected with malware, it is possible to detect malware infection on the network, visualize the latest threats, detect abnormalities, it is also recommended to install a standard cyber–attack detection sensor.

(4) USB usage measures

Even if the IT network that is the malware entry route is blocked by the FW device, there is a need for early anomaly detection. This is because the entry path from the USB device to be used is not lost~~,~~ when the devices are connected to the network by installing Edgecross.

Even if you start collecting information via the network, it is difficult to remove the USB operation from all points, and even if it is removed, it will take some time to complete the operation. If there is a device, it is necessary to use a malware search and removal tool that does not require installation at the point of data collection using a USB device to ensure the health of the device.

The reason for using tools that do not require installation is to reduce the impact on the device due to the installation of anti–malware software, and there are cases where installation of anti–malware software is not allowed on embedded devices provided by manufacturers.

(5) Importance of the network design to be constructed

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

・Current network environment is not clearly known

・Individual optimal network environment is constructed for each unit of equipment and cannot be interconnected

・New network will be constructed

When promoting the networking of factories with the introduction of Edgecross, in order to use the network efficiently and securely, it is necessary to confirm that the facilities can be connected efficiently without changing the address from IP address overlapping state between facilities. A dedicated network design method using micro–segmentation to prevent malware spread is also necessary.

For this reason, we recommend that you tell an integrator who specializes in IP network construction about the purpose of network introduction and how to use it in the future so that you can design and construct the network you want to realize.

4. Operation

4. 1 Vulnerability Countermeasure

In recent years, malware has also invaded factory site, and there have been many cases in which factory operations have stopped due to diffusion activities. Malware invades from USB devices and brought−in devices and uses the vulnerabilities of devices on the network to spread infection to other devices.

In order to suppress malware infection and spread activities, it is necessary to appropriately manage assets such as OS and applications of each device and apply the security patches in a timely manner.

Vulnerability can be dealt with by performing version control of industrial PC software where Edgecross basic software is installed, and updating Edgecross basic software, OS, and other applications as necessary. The following describes how to update each part.

(1) Edgecross Basic Software

To eliminate the vulnerability, please use the latest version of Edgecross basic software. It is recommended to perform the operation after verifying the operation.

Security information is available on the Edgecross website, so check the content and take action if necessary.

(2) Edge application and data collector

Edge applications and data collectors are developed by Edgecross member companies, so please obtain information from the developer and deal with the vulnerability.

Please execute it after verifying the operation in the version upgrade.

(3) OS

The OS supported by Edgecross basic software is Windows. Vulnerabilities are regularly announced, and OS fixes are regularly released by Microsoft. It is recommended to update regularly.

In the update, obtain information on OS update from the target industrial PC manufacturer or Microsoft, and execute it after verifying the operation.

(4) Hardware, BIOS, driver

If there are vulnerabilities in the BIOS and drivers of industrial PCs and devices connected to them, it is necessary to deal with them. It is recommended to apply after obtaining information from the developer and verifying the operation.

4. 2 Security Management and Response

A variety of devices exist in the Edgecross system, and devices 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 devices to the system, updating settings, and changing the network environment. In addition, new vulnerabilities may be discovered even if the device is not changed.

It is important to continue to manage and respond to security even after the operation of the Edgecross system. There are many stakeholders in the entire system, such as various device administrators, network administrators, system operators, and software and device suppliers. Organize the roles of the related parties in advance, and prepare a system so that security management and response can be organized systematically.

- Consider and apply a method to properly implement updates that are important for device security at the required timing.
- The Edgecross system builder / operator should collect and analyze system vulnerability information and send it to relevant parties.
- Inform people concerned about the risks of careless connection to the system and what you want them

to protect.

- ･Please organize the roles of related parties such as various equipment manufacturers and providers of Edgecross systems, system administrators and users.
- ･Establish a system to identify vulnerable devices, and conduct regular monitoring systematically.
- ･If a vulnerable device is identified, alert the administrator of the device and take action on the vulnerability as soon as possible.

Reference: “IoT Security Guidelines ver 1.0”

2.5【Operation and Maintenance】 Guidelines 5 Maintain a safe and secure state, and send and share information

5. Summary

Using this guideline is to ensure the safety and security of FA systems when implements Edgecross.

If you have any questions regarding this document, please submit the inquiry form on the Edgecross Consortium home page.

Edgecross consortium inquiry form https://www.edgecross.org/ja/contact/form/