Technical Information

Recorders, Data Loggers, and Control Products Security Standard

TI 04A02A01-00EN

Contents

The contents of this document are subject to change without notice.

YOKOGAWA ◆

Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan

5th Edition July 2017

1. Introduction

Security in Yokogawa Electric Corporation and its group companies

Our basic philosophy is to work with customers responding to cyber-threats to ensure that they can safely continue business activities with peace of mind. Yokogawa provides support for customers' initiatives to ensure security throughout the lifecycle, from product developing, through implementation of security measures upon introduction of a system, to security management during operation.

Throughout the product lifecycle, Yokogawa ensures vulnerabilities due to the architectures and technologies of systems and products are reduced. Yokogawa has established a framework and a dedicated workforce that allows for appropriate response to incidents concerning vulnerabilities and new threats.

As one way of countering such cyber threats, Yokogawa continuously handles vulnerabilities with its PSIRT (Product Security Incident Response Team), which is tasked with preventing vulnerabilities from contaminating or becoming inherent in products.

If you notice any vulnerabilities in a YOKOGAWA product, please contact psirt@ml.jp.yokogawa.com.

Furthermore, to protect important data entrusted to us by stakeholders, YOKOGAWA is taking IT-oriented data security measures based on the approach of ISO27001.

This document contains security guidelines for products that Yokogawa's Network Solutions Business Division provides. This document provides generalized risk assessment and security measures for the network (Ethernet) connections of applicable products and uses standard models as a basis for explaining how to manage applicable products.

Because new measures are always being taken to counter today's ever-changing security threats, the contents of this document are subject to change without prior notice.

Why Security Is Essential

In recent years, with the advancement of network and information technology, open information technologies used in operating systems and communication protocols are also being adopted in control systems. This trend is accelerating the close interaction between information systems and control systems.

In this type of environment, control systems can become targets for attackers and are subject to security threats from computer viruses and other malicious programs. Ensuring the safety of measuring systems and control systems is vital to protecting important assets.

Applicable Products

This document applies to the following products.

• Chart recorders	μR10000/μR20000
• Paperless recorders	GX10/GX20/GP10/GP20, DX364, DX1000T/DX2000T, DX1000/DX2000/DX1000N, FX1000, DX3000, CX1000/CX2000
• Data acquisition system	GM
• Data acquisition units	MW100
• Single-loop controllers	YS1000 Series
• Digital indicating controllers/ Program controllers/ Digital indicator with alarms	UTAdvanced

Trademarks

- Ethernet is a registered trademark of Fuji Xerox Corporation.
- Modbus is a registered trademark of Schneider Automation Inc. in the United States.
- Other company and product names are registered trademarks or trademarks of their respective holders.
- In this document, the TM and ® symbols do not accompany their respective registered trademark or trademark names.

2. Assets That Should Be Protected

To safely sucure customer assets, first we must assemble a list of the assets to be protected, clarify ownership, and determine their value.

The higher the value of the asset, the greater the need to take security measures. The following are examples of assets that should be protected.

Data Assets

- Production schedule information
- System configuration information
- Application configuration information
- Control parameter information
- Recipe information
- History information

Device Assets

- Engineering workstations (EWSs)
- Operator consoles (OITs)
- Process controllers (DCSs and PLCs)
- Field devices
- Network devices

Human and Environmental Assets

- Employees
- Factories and plant facilities
- Natural environment

When theses assets are exposed to security threats, the following may result:

- Disturbance or halting of production activities
- Leakage of recipes and other confidential information that relates to production activities
- Personal injury
- Damage to factories and plant facilities
- Environmental damage

These events can inflict tremendous losses on an organization.

The objective of taking security measures is to protect these assets from threats and reduce opportunity losses incurred by the organization.

Priority Classification Example

Below is an example of how asset priorities can be classified.

- Priority A: Extremely high
- Priority B: High
- Priority C: Low
- Priority D: Extremely low

NOTE

This document is based on “ISA 99.00.01-2007: Security for Industrial Automation and Control Systems, Part 1: Terminology, Concepts, and Models.” This document refers to this standard as ISA 99.00.01.

ISA 99.00.01 defines “activity-based criteria” for determining security measures and “asset-based criteria” for determining the assets that need to be protected. This document is based on these criteria.

3. Identifying and Evaluating Threats

Determine all possible security threats to the assets that are on your list of assets that need to be protected. Possible threats need to be considered from the following viewpoints.

Unauthorized Access to Assets by Individuals with Malicious Intent

- Insider
- Outsider
- Via network
- Direct access to assets (direct operation of instruments that contain assets)

Unauthorized Access to Assets by Malicious Software

- Via network
- Via removable media

Inappropriate Access by Valid Users through Operation Errors and Careless, Unintended Acts

- Via network
- Via removable media
- Direct access to assets (direct operation of instruments that contain assets)

For each security threat that you have identified, evaluate the probability of occurrence. Below is an example of how the probabilities of occurrence can be classified.

- Probability level A: High probability that the threat will occur
- Probability level B: Moderate probability that the threat will occur
- Probability level C: Low probability that the threat will occur

Identifying and Evaluating Vulnerabilities

Determine the vulnerability of each asset or the vulnerability of the device that contains the asset. Vulnerabilities are conditions that allow security threats to adversely affect assets. Examples of vulnerabilities are listed below.

- Flaws in the planning of security measures
- Flaws in the execution of security measures
- Flaws in the supervision or improvement of security measures
- Lack of physical protection
- Flaws in the configuration of firewalls
- Failure to exterminate viruses and flaws in the application of security patches
- Flaws in backing up data (system is not being backed up)
- Insufficient understanding of production control systems and their operation and environment
- Lack of system designer and operator awareness about security

Risk Assessment

Assess the security risk for each asset or the device containing the asset. Risk is assumed to be expressible using the following formula.

Risk = threat × vulnerability × expected loss

Risk assessment enables you to prioritize various security measures. Risk assessment includes assessing the business loss incurred due to the halting of system functionality, the expenses required to repair the damage to the production control system, and so on.

Determine the priority of each security measure in accordance with the level of quantitative loss. Doing so will enable you to determine which risks require countermeasures, which risks can be tolerated, and so on.

Note that in some cases, losses are difficult to assess as business losses because they include factors such as environmental contamination, personal injury, and loss of public confidence in the organization.

4. Overview of the Products That This Document Applies To

Applicable Products

This document applies to the following products.

• Chart recorders	μR10000/μR20000
• Paperless recorders	GX10/GX20/GP10/GP20, DX364, DX1000T/DX2000T, DX1000/DX2000/DX1000N, FX1000, DX3000, CX1000/CX2000
• Data acquisition system	GM
• Data acquisition units	MW100
• Single-loop controllers	YS1000 Series
• Digital indicating controllers/	
Program controllers/	
Digital indicator with alarms	UTAdvanced

The communication features implemented on the applicable products vary depending on the product series. This chapter describes the communication features that are implemented on each series of products and the security measures that should be considered.

Features of Applicable Products

All the products covered in this document use microprocessors and real-time OSs to run communication applications. At the factory, different communication applications are embedded in each product series.

In principle, users cannot add new program codes to or create new applications in these instruments. As an exception, some products do allow users to update the embedded software. However, only specific code can be embedded in a specific way, so there is no threat of software updates leading to the introduction of malicious programs into these instruments.

Communication Protocols

Ethernet and TCP/IP Protocol

Applicable products come with standard or optional 10BASE-T or 100BASE-TX Ethernet ports. Ethernet communication uses stable TCP and UDP protocols that are based on IPv4.

The applicable products allow IP addresses, subnet masks, and default gateways to be specified.

In addition, on applicable products equipped with client features, destination server devices can be specified by their IP address or by their DNS (Domain Name System) host name.

The port numbers in the following table are factory default port numbers that have been allotted for the purpose of connecting to the server features of the applicable products. The port numbers of some products are fixed. Fixed port numbers are indicated as “fixed” in the table.

Server Features of GX10/GX20/GP10/GP20 Paperless Recorders and GM Data Acquisition System

Port Number	Maximum Simultaneous Connections	Protocol	Service
502/tcp	4	Modbus	Multi-vendor connection (Modbus server)
21/tcp	4	FTP or FTPS (when Encryption is On)	File transfer (FTP server)
44818/tcp	10	EtherNet/IP	Multi-vendor connection (EtherNet/IP server)
44818/udp, 2222/udp	-		
4840	3 sessions	OPC-UA	Multi-vendor connection (OPC-UA server)
80/tcp or 443/tcp (when Encryption is On)	-	HTTP or HTTPS (when Encryption is On)	www (HTTP server)
123/udp	-	SNTP	Time synchronization (SNTP server)
34434/tcp (fixed)	4	Yokogawa proprietary	General-purpose communication services

Server Features of MW100 Data Acquisition Units

Port Number	Maximum Simultaneous Connections	Protocol	Service
502/tcp	4	Modbus	Multi-vendor connection (Modbus server)
21/tcp	4	FTP	File transfer (FTP server)
80/tcp	-	HTTP	www (HTTP server)
123/udp	-	SNTP	Time synchronization (SNTP server)
34318/tcp	4	Yokogawa proprietary	General-purpose communication services

Server Features of DX364, DX1000T/DX2000T, DX1000/DX2000/DX1000N, FX1000, DX3000 Paperless Recorders

Port Number	Maximum Simultaneous Connections	Protocol	Service
502/tcp	2	Modbus	Multi-vendor connection (Modbus server)
44818/tcp	10	EtherNet/IP	Multi-vendor connection (EtherNet/IP server) *Except DX364 and FX1000
44818/udp, 2222/udp	-		
21/tcp	2	FTP	File transfer (FTP server)
80/tcp	-	HTTP	www (HTTP server)
123/udp	-	SNTP	Time synchronization (SNTP server)
34260/tcp (fixed)	3	Yokogawa proprietary	Setup and measurement services
34261/tcp (fixed)	1	Yokogawa proprietary	Maintenance and test services
34264/udp (fixed)	-	Yokogawa proprietary	Instrument information service

Server Features of CX1000/CX2000 Paperless Recorders

Port Number	Maximum Simultaneous Connections	Protocol	Service
21/tcp (fixed)	2	FTP	File transfer (FTP server)
80/tcp (fixed)	-	HTTP	www (HTTP server)
34260/tcp (fixed)	3	Yokogawa proprietary	Setup and measurement services
34261/tcp (fixed)	1	Yokogawa proprietary	Maintenance and test services
34264/udp (fixed)	-	Yokogawa proprietary	Instrument information service

Server Features of μR10000/μR20000 Chart Recorders

Port Number	Maximum Simultaneous Connections	Protocol	Service
34260/tcp (fixed)	3	Yokogawa proprietary	Setup and measurement services
34261/tcp (fixed)	1	Yokogawa proprietary	Maintenance and test services
34264/udp (fixed)	-	Yokogawa proprietary	Instrument information service

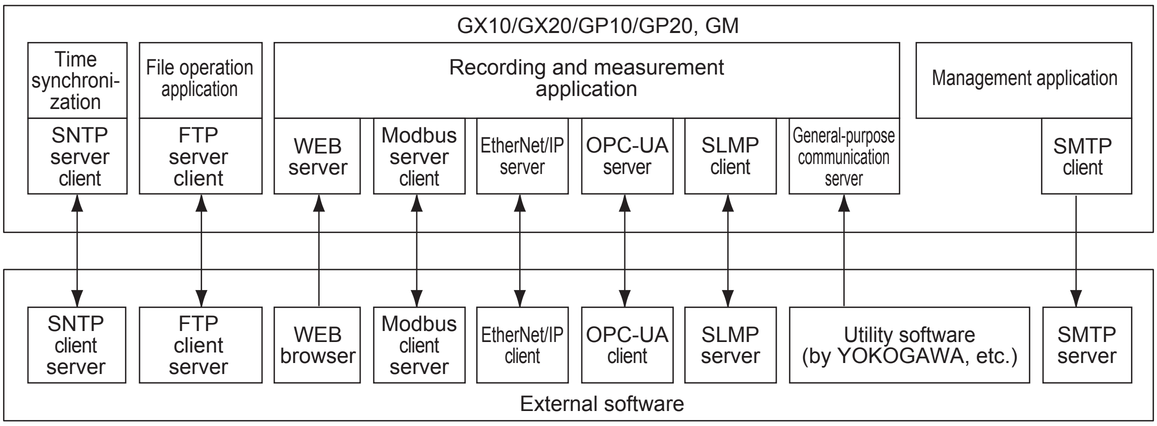
YS1000 Series Single-loop Controllers (Server features)

Port Number	Maximum Simultaneous Connections	Protocol	Service
502/tcp	2	Modbus	Multi-vendor connection (Modbus server)

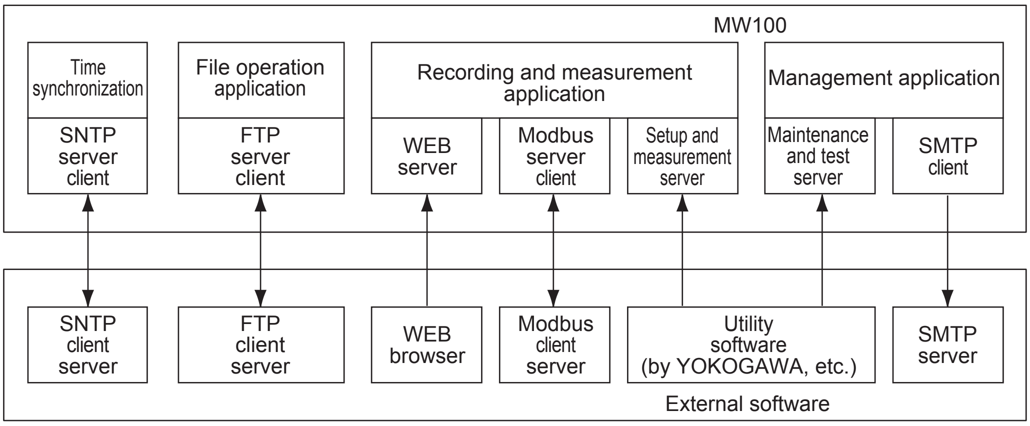
Server Feature of UTAdvanced Digital Indicating Controllers/Program Controllers/Digital Indicator with Alarms

Port Number	Maximum Simultaneous Connections	Protocol	Service
502/tcp	2	Modbus	Multi-vendor connection (Modbus server)

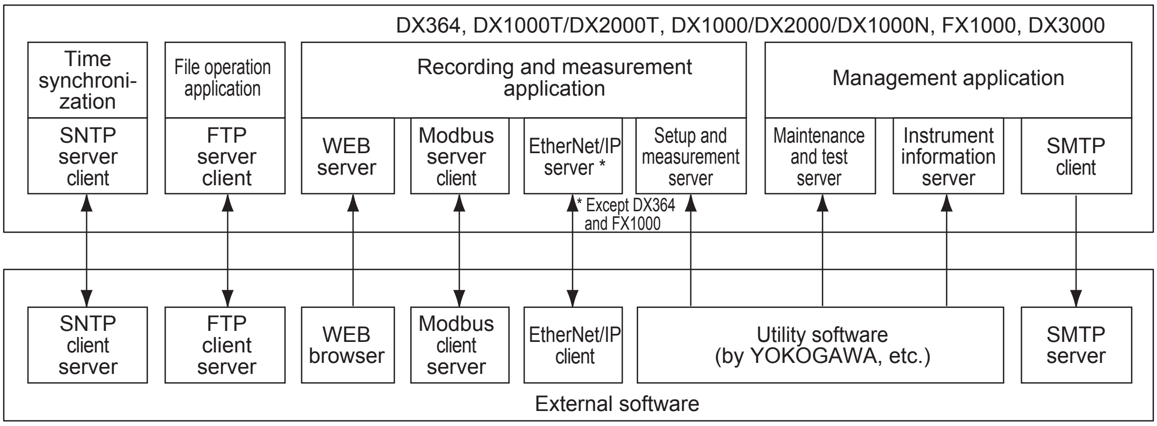
The following figure summarizes the client and server features of each instrument. An overview of each protocol is given in the later pages.



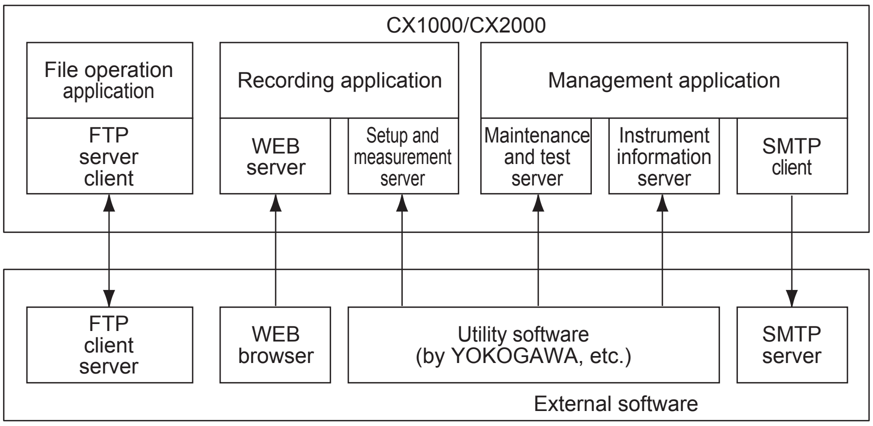
GX10/GX20/GP10/GP20 Paperless Recorders and GM Data Acquisition System



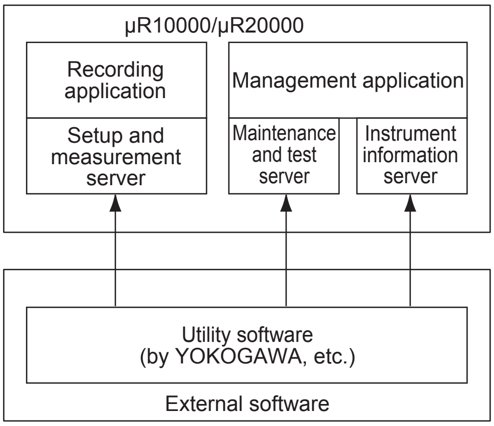
MW100 Data Acquisition Units


DX364, DX1000T/DX2000T, DX1000/DX2000/DX1000N, FX1000, DX3000
Time synchroni-zation
File operation application
Recording and measurement application
Management application
SNTP server client
FTP server client
WEB server
Modbus server client
EtherNet/IP server *
Setup and measurement server
Maintenance and test server
Instrument information server
SMTP client
* Except DX364 and FX1000
SNTP client server
FTP client server
WEB browser
Modbus client server
EtherNet/IP client
Utility software (by YOKOGAWA, etc.)
SMTP server
External software

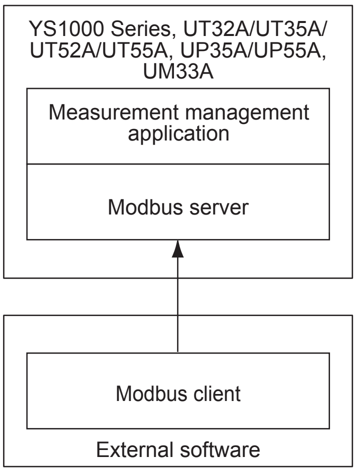
DX364, DX1000T/DX2000T, DX1000/DX2000/DX1000N, FX1000, DX3000 Paperless Recorders



CX1000/CX2000 Paperless Recorders


μR10000/μR20000
Recording application
Setup and measurement server
Management application
Maintenance and test server
Instrument information server
Utility software (by YOKOGAWA, etc.)
External software

μR10000/μR20000 Chart Recorders


YS1000 Series, UT32A/UT35A/ UT52A/UT55A, UP35A/UP55A, UM33A
Measurement management application
Modbus server
Modbus client
External software

YS1000 Series Single-loop Controllers, UTAdvanced Digital Indicating Controllers/Program Controllers/ Digital Indicator with Alarms

EtherNet/IP Protocol (GX10/GX20/GP10/GP20, GM, DX1000T/DX2000T/DX1000/DX2000/DX1000N/DX3000)

The EtherNet/IP Protocol is used in communication between industrial devices. The procol is also used to connect these devices to PLCs, etc. For the GX10/GX20/GP10/GP20, GM, and DX1000T/DX2000T/DX1000/DX2000/DX1000N/DX3000, the EtherNet/IP protocol can be used to access internal data of these devices from clients.

OPC-UA (GX10/GX20/GP10/GP20, GM)

The OPC-UA Protocol is used in communication between industrial deveices. The protocol is also used to connect these devices to SCADAs, MESs, etc. For the GX10/GX20/GP10/GP20, and GM, the OPC-UA server function enables OPC-UA clients of a host system (SCADA, MES,etc.) to access the I/O channels, math channels, and communication channels of a GX/GP/GM for data reading and writing through Ethernet.

SLMP Protocol (GX10/GX20/GP10/GP20, GM)

The SLMP Protocol is used in communication between industrial deveices. The protocol is also used to connect these devices to Mitsubishi PLCs. The SLMP communication of the GX, GP, and GM is a function for reading and writing data by connecting to an SLMP server through Ethernet.

SNTP Protocol (MW100, GX10/GX20/GP10/GP20, GM, DX1000T/DX2000T/DX1000/DX2000/DX1000N/DX3000/DX364)

The protocol is also used to synchronized to the time between computer systems. For the MW100, GX10/GX20/GP10/GP20, GM, and DX1000T/DX2000T/DX1000/DX2000/DX1000N/DX3000/DX364, these device’s time can be synchronized to the time on an SNTP server. These devices can also function as an SNTP server.

FTP Protocol (Paperless recorders, data acquisition system and data acquisition units)

The file management application saves data residing in the main memory to files on an external storage medium. Depending on how the instrument is configured, the file management application generates daily, weekly, and other types of report files. These files are saved to an external storage medium (disk or memory card) that is inserted into the instrument.

The FTP server feature can be used to manipulate the files and directories in the external storage medium. The measurement and report files described above are stored in specified directories. Authenticated users can retrieve and delete existing files and save new files. If the FTP client feature is enabled, files can be automatically transferred to registered FTP servers when the files are created or when specific events occur. The FTP server has a user authentication feature. When the server’s login feature (described later) is enabled, users can use the FTP server only when they enter the appropriate user name and password.

Up to two connection destination servers (primary and secondary) can be specified. For each, the user sets the server name (host name or IP address), user name, password, and initial directory. Under normal conditions, the instrument attempts to transfer files to the primary server. If the transfer fails, the instrument attempts to transfer files to the secondary server.

HTTP Protocol (Paperless recorders, data acquisition system and data acquisition units)

The recording application displays recording screens and messages on a remote Web browser. It also allows the instrument to be controlled remotely (only when the user logs in as an operator) via a Web browser. Microsoft Internet Explorer has been tested for operational compatibility. The HTTP server has a user authentication feature. When the server’s login feature (described later) is enabled, users can use the HTTP server only when they enter the appropriate user name and password.

SMTP Protocol (Paperless recorders, data acquisition system and data acquisition units)

The management application transmits emails to an SMTP server in accordance with how the instrument has been set up. On the applicable products, emails are transmitted:

(1) Periodically

(2) When a hardware malfunction or other system error occurs

(3) When an hourly, daily, monthly, or other report is created

(4) When an alarm occurs due to measurement errors or other reasons

For each situation, you can set (1) whether to send an email, (2) the subject, (3) the destinations (whether to send email to each of two groups), (3) the body message, and (4) whether to include the Web address (URL) and measured values of each instrument.

Modbus protocol

(YS1000 Series, UTAdvanced, MW100, GM, GX10/GX20/GP10/GP20, DX364, DX1000T/DX2000T/DX1000/DX2000/DX1000N, FX1000 and DX3000)

The Modbus protocol is widely used in communications between industrial devices. The protocol is also used to connect these devices to DCSs, PLCs, SCADAs, etc. For the GX10/GX20/GP10/GP20, GM, DX364, DX1000T/DX2000T, DX1000/DX2000/DX1000N, FX1000 and DX3000 the Modus protocol can be used to output measured data and to start and stop measurements. For the YS1000 Series and UTAdvanced, the Modbus protocol can be used to change an instrument's settings, such as the SP, through the access and modification for the instrument's register values.

Yokogawa Proprietary Protocol

(Chart recorders, paperless recorders and data acquisition units)

The server feature in the recording application and management application uses a command-response protocol. This protocol makes it possible to read measured values, setup and measurement information, maintenance and test information, and instrument information. Commands and responses are primarily exchanged using ASCII character strings, but for some commands, binary response data is returned. The syntax and operations of commands and responses are defined in the user's manual of each instrument. The Yokogawa proprietary protocol has a user authentication feature. When the protocol's login feature (described later) is enabled, users can use the protocol only when they enter the appropriate user name and password.

5. Security Threats

Notable security threats are listed below.

Malware (Virus) Infection Threats

The operating system (OS) of products relevant to this document is a special embedded edition, and because it is does not include the office, mail, and browser software targeted by most viruses and macros, the possibility of infection by malware is very limited. Nevertheless, instruments that have external media such as the DX and MW are in danger of being used as stepping stones for virus infected files, therefore we urge caution when using external media.

Intrusion Threats

Logging in to a product avails you of multiple server functions. To ensure that these server functions, measured values, and settings are not subject to unauthorized access by third parties, direct local access and network access to these products can be password protected. To use password protection, please turn on the Login function in advance. Since user names and passwords for logging in via HTTP and FTP are sent as plain text, there is a danger that passwords will be leaked if a network is tapped. When accessing the network from the Internet or untrusted locations, use a secure communication protocol such as HTTPS or FTPS. Of course, there is always a danger of leaks due to carelessness.

There is a possibility of direct intrusion into instruments that are installed at remote sites and connected via telephone lines. The potential damages include data leaks, corruption of settings, and unauthorized manipulation of output systems resulting in damage to production equipment and instruments.

Threats of Information Leaks and Sabotage

Chart recorders, single-loop controllers, and digital indicating controllers hold very limited information about networks (IP addresses, subnet masks, default gateways, products' host and domain names, and DNS server addresses).

On the other hand, paperless recorders and data acquisition units have FTP client and SMTP features. Therefore, these instruments have access information for external FTP servers and SMTP servers.

If credentials are leaked or stolen throuugh eavesdropping and an attacker gains unauthorized access, they can obtain information that may lead to unauthorized access into relevant servers. Intrusions into instruments also poses a danger of someone extracting measured values, corrupting settings, and improperly manipulating output (control signals). For example, if a setting is changed externally and the controlled temperature is raised abnormally, produced goods may be damaged. Also, recorded data may be erased or tampered with.

As these kinds of data leaks and destructive processes frequently originate from unauthorized access to instruments, using the included Login function and secure communications via HTTPS and FTS are effective countermeasures.

6. Product-Specific Security Features

This chapter explains the security features of each system product. They should be assessed when security measures are put in place. Each product has features that enhance security.

GX10/GX20/GP10/GP20 Paperless Recorders and GM Data Acquisition System

Login Feature

This Login function restricts access for this product group to users registered in advance. By turning ON the Login function and specifying administrator and user rights, you can limit the people who can access instruments to browse measured data or change measurement settings.

This means that even if someone accesses a server over the network, directly, or by physically stealing a terminal, unauthorized third parties cannot manipulate data or settings, and theft, tampering, and deletion of important data such as measured values and settings can be prevented.

There are two user levels (privileges).

Administrator privileges:

All features can be used.

Administrators can specify which functions to assign to general users, individualized user restrictions on operations and settings.

Normal user privileges:

Writing to external media via FTP and other features are restricted. Measured data, report data, log information, status information, etc., can be retrieved. Operation / setting authority can be set up individually.

To ensure security, assign the minimum rights needed to each user.

Assign appropriate login privileges to users to ensure security. Up to 50 administrators and normal users can be registered in these instruments.

SSL Communication Function

For remote access, you can use communication employing the SSL (secure socket layer) data encryption and sending/receiving protocol. Public key encryption and certificates are used to encrypt communication and authenticate connections. These tools restrict access to authenticated, legitimate terminals/users, and prevent theft, tempering, and deletion of crucial data through unauthorized access by third parties. HTTPS and FTPS communications are supported for encrypted communication of HTTP and FTP servers.

IP Access Limitation Function

Only Modbus access from a registered IP address is allowed. Access from an unregistered IP address is rejected.

By using these functions, you can block unauthorized access via Modbus, and prevent theft, tempering, and deletion of crucial data.

Log Information

By referring to communication logs, operation logs, FTP logs, etc., you can determine how the instruments have been operated.

By doing so, you can analyze causes and take appropriate actions in the unlikely event that someone improperly manipulates or configures instruments.

Robustness against cyber attacks

The recording functions of the GM10, GM20, GX20, GP10, and GP20 soundly passed communication tests equivalent to Achilles level 1 certification, which certifies the robustness of industrial instruments.

- The above have been verified on the following revisions.

  GM10: R4.01.01

  GX10: R4.01.01

  GX20: R4.01.01

  GP10: R4.01.01

  GP20: R4.01.01
- For details on Achilles certification, see the following.

  http://www.wurldtech.com/certifications/achilles-communications-certification

MW100 Data Acquisition Units

Login Feature

The login feature allows only registered users to access the MW100. There are two user levels (privileges).

Administrator privileges:

All features can be used.

User privileges:

Writing to external media via FTP and other features are restricted. Measured data, report data, log information, status information, etc., can be retrieved. Measurement range adjustments require administrator privileges.

By enabling the login feature and assigning administrator and user privileges, you can control who is able to access the MW100 and view measured data and who is able to access the MW100 and change the measurement setup. Assign appropriate login privileges to users to ensure security. Up to 10 users can be registered in the MW100.

Log Information

By referring to communication logs, operation logs, FTP logs, etc., you can determine how the instruments have been operated.

DX364, DX1000T/DX2000T, DX1000/DX2000/DX1000N, FX1000, DX3000 Paperless Recorders

Login Feature

The login feature allows only registered users to access the paperless recorders. There are two user levels (privileges).

Administrator privileges:

All features can be used. Administrators can specify which features to make available to normal users.

Normal user privileges:

Writing to external media via FTP and other features are restricted. Measured data, report data, log information, status information, etc., can be retrieved. Measurement range adjustments require administrator privileges.

By enabling the login feature and assigning administrator and user privileges, you can control who is able to access the paperless recorders and view measured data and who is able to access the paperless recorders and change their measurement setups. Assign appropriate login privileges to users to ensure security. Up to 5 administrators and 30 normal users can be registered in these paperless recorders.

IP Access Limitation Function

(Available on the DX1000T/DX2000T/DX1000/DX2000/DX1000N Release 3 or later, and DX3000 restricts access to Modbus server)

Only Modbus access from a registered IP address is allowed. Access from an unregistered IP address is rejected.

By using these functions, you can block unauthorized access via Modbus, and prevent theft, tempering, and deletion of crucial data.

Log Information

By referring to communication logs, operation logs, FTP logs, etc., you can determine how the instruments have been operated.

By doing so, you can analyze causes and take appropriate actions in the unlikely event that someone improperly manipulates or configures instruments.

CX1000/CX2000 Paperless Recorders

Login Feature

The login feature allows only registered users to access the paperless recorders. There are two user levels (privileges).

Administrator privileges:

All features can be used.

User privileges:

Writing to external media via FTP and other features are restricted. Measured data, report data, log information, status information, etc., can be retrieved. Measurement range adjustments require administrator privileges.

By enabling the login feature and assigning administrator and user privileges, you can control who is able to access the paperless recorders and view measured data and who is able to access the paperless recorders and change their measurement setups. Assign appropriate login privileges to users to ensure security. One administrator and up to six users can be registered in these paperless recorders.

Log Information

By referring to communication logs, operation logs, FTP logs, etc., you can determine how the instruments have been operated.

UTAdvanced Digital Indicating Controllers/Program Controllers/ Digital Indicator with Alarms

Write Access to Modbus Registers

Writing to Modbus registers over communication lines can be enabled or disabled. Disabling the feature will prevent outsiders with malicious intent from changing the controller settings. When the feature is disabled, settings must be changed manually onsite.

IP Access Limitation Function

Only Modbus access from a registered IP address is allowed. Access from an unregistered IP address is rejected. This feature prevents unauthorized access and enhances security.

YS1000 Series Single-loop Controllers

Write Access over Ethernet

Writing to Modbus registers over Ethernet can be enabled or disabled. Disabling the feature will prevent outsiders with malicious intent from changing the controller settings. When the feature is disabled, settings must be changed manually onsite.

Robustness against cyber attacks

The control functions of the YS1000 soundly passed communication tests equivalent to Achilles level 1 certification, which certifies the robustness of industrial instruments.

- The above have been verified on the following revisions.

  YS1000: MCU R2.01.01, DCU R2.01.02, NCU R2.01.02

- For details on Achilles certification, see the following.

  http://www.wurldtech.com/certifications/achilles-communications-certification

7. Staff Security

One of the most important security threats is “people.” Human error can pose major security threats.

Education

The purpose of education is to ensure that staff members develop knowledge and skills about security and are able to carry out daily operations in accordance with security guidelines. Education should include the following objectives.

- Staff members deepen their understanding about security.
- Staff members recognize threats and influences on production control systems.
- Staff members can carry out appropriate security measures and improvements.
- Staff members understand the proper operation and management of production control systems. For example, staff members should learn how to check logs to determine whether a system has been attacked.

Education should be provided at the following occasions.

- At the time of employment
- When the staff members that access the applicable instruments change because of personnel changes or other reasons

Revision Information

Title : Recorders, Data Loggers, and Control Products Security Standard
Manual number : TI 04A02A01-00EN

June 2012/1st Edition
Newly published

October 2012/2nd Edition
Addition of the models (SMARTDAC+ GX/GP)

August 2015/3rd Edition
Addition of the models (SMARTDAC+ GM)

November 2016/4th Edition
Addition of the models (Daqstation DX364 and DX3000)

July 2017/5th Edition
Review of contents

Written by Yokogawa Electric Corporation
Published by Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN

Blank Page