Technical Information

Collaborative Information Server
Product Overview

TI 36K01A10-01EN

YOKOGAWA

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

TI 36K01A10-01EN

3rd Edition Aug. 2024 (YK)

Introduction

Collaborative Information server serves as a platform system that connects to the devices and system within a plant and monitor their operations. Engineers build the operation monitoring system by defining the data and creating screens for monitoring the operations.

This document describes the major features and specifications of CI Server and the engineering details.

Drawing conventions

TI 33J01A11-01EN	CENTUM VP System Overview (HMI Overview)
TI 33J01A12-01EN	CENTUM VP System Overview (FCS Overview)
TI 32P01A10-01EN	ProSafe-RS System Overview

Target Readership for This Manual

The figures used in this document are emphasized, simplified, or omitted for the convenience of description.

Trademark

Trademark Acknowledgment

The names of corporations, organizations, and logos used in this document are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

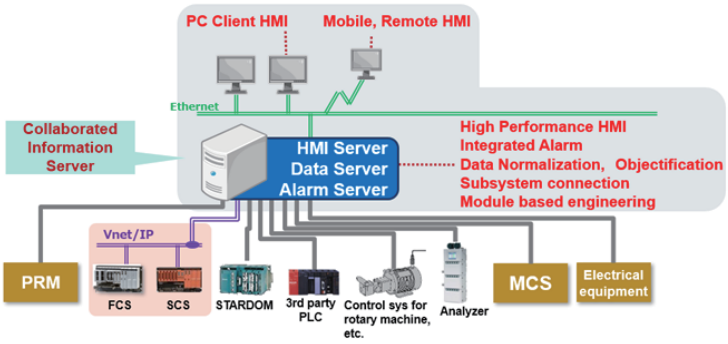
Collaborative Information Server Product Overview

TI 36K01A10-01EN 3rd Edition

CONTENTS

1. Overview

Collaborative Information Server (CI Server) integrates data collected from various controllers such as DCS (Distributed Control System), RTU (Remote monitoring Control Unit), and PLC (Program Logic Controller) that constitute a system and provides the integrated data to the operator.



F010001.ai

The major features of CI Server are as follows:

Web based data operation monitoring

Operation monitoring screen is of two types: 1. Operation monitoring screen using a dedicated application and 2. Operation monitoring screen using Web browser.

F010002.ai

Multi-vendor support

CI Server conforms to industry standards such as OPC UA and ODBC. It also supports controller specific communication drivers. Data can be collected not only from Yokogawa products but also from other company products.

Save historical data

Data that is handled in CI Server can be stored as historical data. Data such as item data, system logs, operation records, report details etc. can be stored as historical data.

Report output

Reports that inform about plant condition and reports such as when an event occurred, or on-demand reports can be sent out.

Alarm management

When data is abnormal, alarms are generated to notify the abnormality. Alarms are listed in the Alarm Overview Page. Operations when an alarm is generated such as alarm confirmation, filtering, renotification, and alarm display can be configured in detail based on data. Also, the alarm data history managed in the data server can be analyzed using System Performance Analysis.

Audit trails

The operations on data can be stored as audit trails.

User management

Users who can monitor the operations of CI Server can be defined and the range of operation management can be configured for each user.

System scalability

The structure of CI Server is capable of handling distribution of functions, and hence supports from small-scale standalone systems to large-scale systems that integrates distributed systems.

Engineering function

It is structured such that data once created can be easily reused. Effective engineering can be performed in large scale systems as well as systems in which expansion is planned. It consists of tools for definitions to build the system and an editor to create different pages/screens.

Vocabulary

No.	Vocabulary	Definitions
1	Operator interface	Operation monitoring screen
2	Engineering module	An engineering tool that is used to configure the system.
3	Edit module	An editor that is used to create operation monitoring screens
4	Nodes and node names	Computers in which CI Server is installed are sometimes called as Nodes. Node name is the name given to the nodes for identification.

2. System architecture

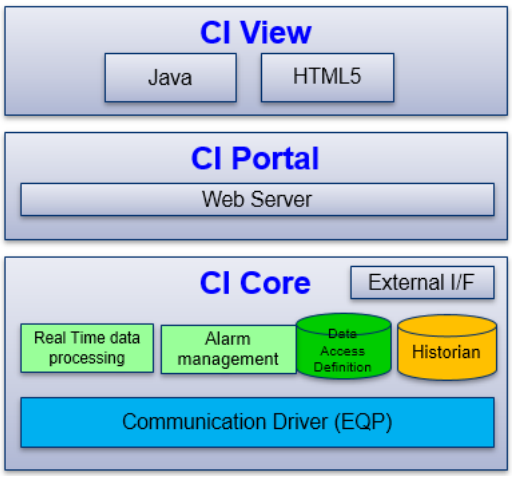
Based on the plant structure and business style, the structure of CI Server can be made flexible; either a standalone structure in which both data collection and operation maintenance are realized in a single computer, or an integrated structure in which multiple servers are configured in layers and all the plant operations are monitored.

2.1 CI Core, CI Portal, and CI View

CI Server is made of three functional components, CI Core, CI Portal and CI View. These components can be installed in computers using functional component unit. Each of the functional components can be installed in a single computer or can be distributed across computers based on the plant structure. Therefore, CI Server supports both standalone structure in which data collection and operation maintenance is carried out in a single computer as well as wide area system structure in which multiple servers are installed in a wide area and are integrated.

Functional component	Role
CI Core	Data server
CI Portal	Web server
CI View	Client

Configuration of CI server functional components



F020101.ai

- **CI Core**

  Functions as a basic part of CI Server. It functions as the data server that collects and stores operation data of a plant. It shares data with other CI cores and communicates with other systems. CI Core provides data to CI Portal. It manages alarms and historical data.

- **CI Portal**

  CI Portal provides the data collected and saved by CI Core to CI View. It performs the role of a Web server.

CI View

It is an HMI that supports various work environment for operation maintenance and can be displayed on Windows computer as well as tablets. It connects to CI Portal and displays the screens. HMI is of two types:

- HMI created in Java application
  The Java application HMI can be further classified into the following two types of usage patterns:
  Opening HMI (Java application) in a computer where both CI Portal and CI View are installed Opening the [Remote Connect] application from the CI View computer and using the HMI application
- HMI displayed in Web browser
  There is no specific software required when using Web browser.

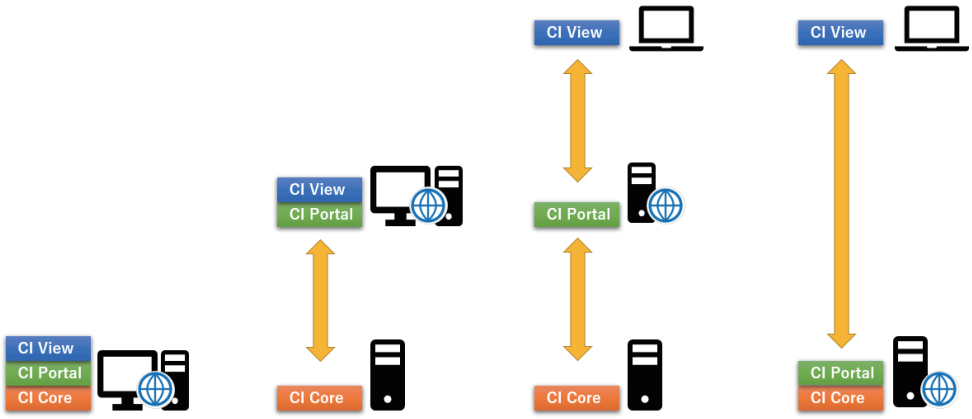
Applications that can be used on these HMIs are as follows:

HMI type	Applications that can be used
Java application	Operator interface
	Engineering module
	Edit module
	Edit module (Enterprise)
	Item search
	Alarm system performance analysis (*1)
Web browser (HTML5)	Operator interface

*1: Cannot be used from Remote Connect application

Distribution arrangement of functional components

The functional components can be distributed as shown below and installed.



F020102.ai

- Standalone Configuration
  Pattern in which CI Core, CI Portal, and CI View are used in a single computer
- Integrated CI View and CI Portal Configuration
  Pattern in which CI Core and the combination of CI Portal and CI View are used in different computers
- Separated CI View, CI Portal configuration 1
  Pattern in which CI Core, CI Portal and CI View are used in different computers

- Separated CI View, CI Portal configuration 2
  Pattern in which the combination of CI Core and CI portal is used in a different computer than the CI View computer.

Note: In an actual CI Core license, CI Portal/CI view is included by default, and there are no computers in which only CI Core is installed. The above descriptions are to represent the roles of the computers used in the project. Similarly, CI View is included by default in the CI Portal license and there are no computers in which only the CI Portal function is installed.

2.2 System architecture pattern

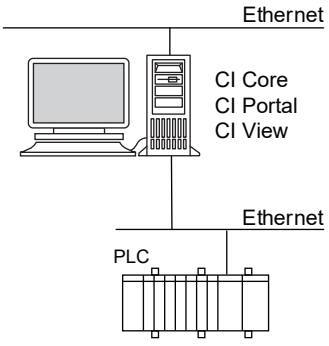
Distributing the functional components enables to build various system architectures. The following system architecture are explained in this document.

- Standalone configuration
- Remote CI Portal/CI View configuration
- Enterprise configuration
- Gateway configuration
- Host-to-host connection configuration
- Yokogawa Cloud Configuration

To increase the usability of the system, server redundancy structure and node to node communication redundancy structure can be combined.

Standalone configuration

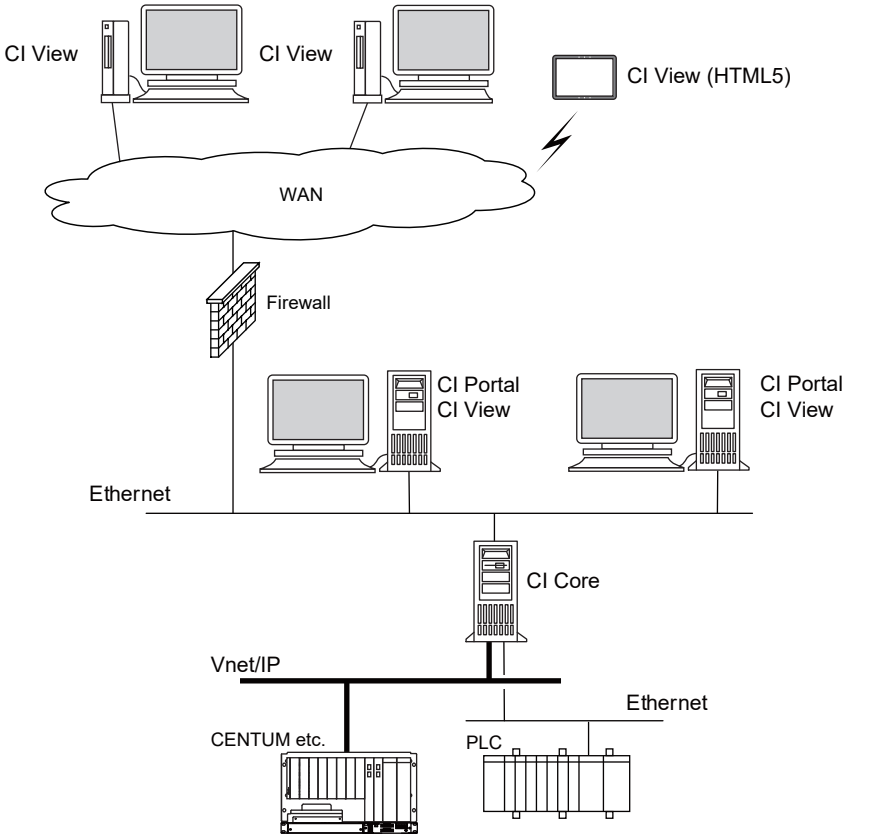
The system configuration in which data collection, monitoring control, engineering environment and operator environment are implemented on a single computer. This type of configuration may be used for relatively small applications where it is acceptable to have only one combined Web HMI Server/Client station for data acquisition, operator supervision and engineering.



F020201.ai

Remote CI Portal/CI View configuration

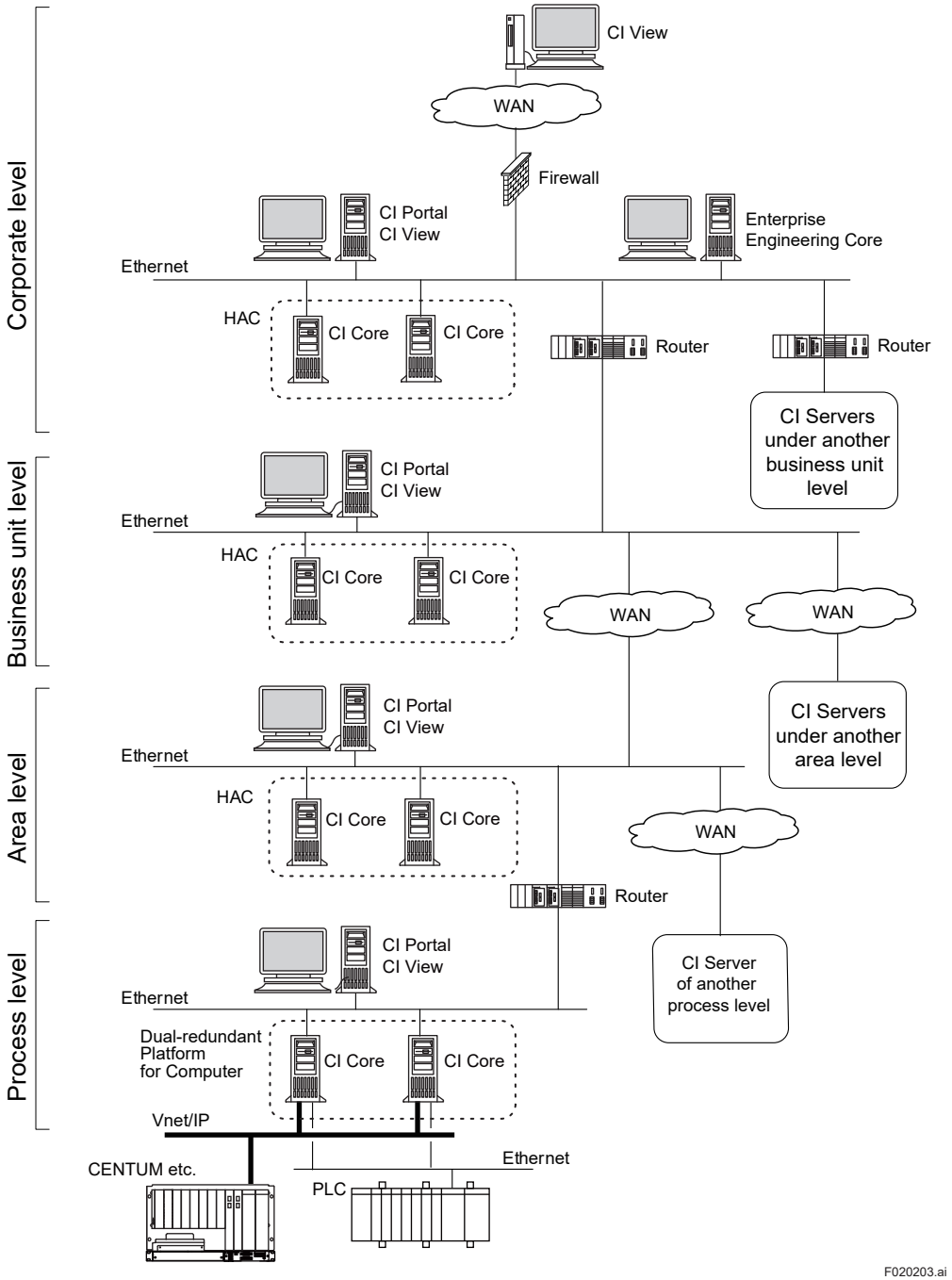
The system configuration in which the data server that collects data, runs application, and maintains database in real time is separated from CI Portal in which engineering and operation monitoring are performed, thus increasing the scalability of the system.



Enterprise configuration

The system configuration for large scale geographically dispersed projects having independent process control systems in layered structure, with each of the process control system responsible for a particular area and are monitored by the systems in the upper level.

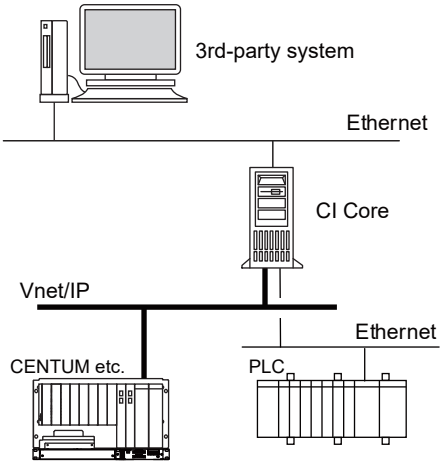
In this configuration, functionalities of server such as data collection and multiple HMI client support can be distributed to many computers.



- Process level
  Process level contains local controllers and other automation control devices/ monitoring devices that communicates with devices in a plant directly or indirectly.
- Area level
  At the area level, all processes are managed graphically to control overall area.
- Business unit level
  The business unit level is typically responsible for all areas within the business unit.
- Corporate level
  At the corporate level, all KPI's and other process data of all the business units are collected and aggregated providing a holistic view of the performance of the enterprise and its operational groups down to process level in real-time.

Gateway configuration

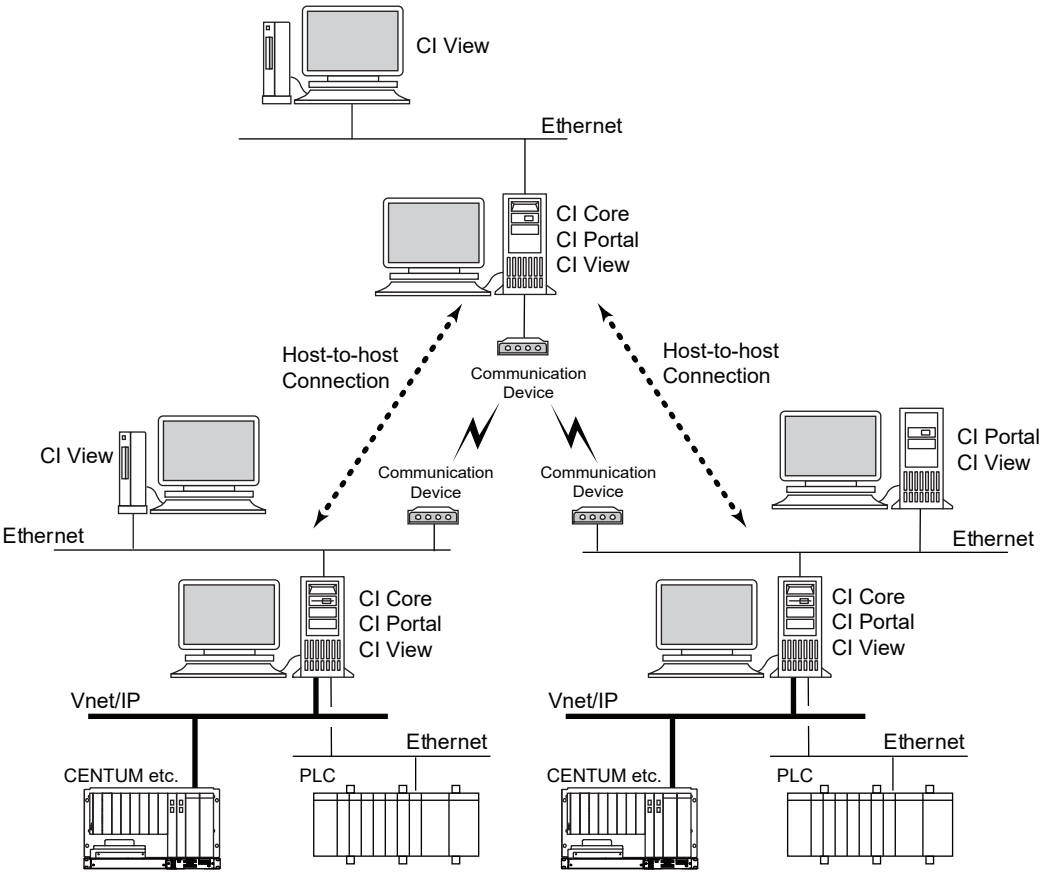
The configuration in which CI Server acts as a gateway to other systems.



F020204.ai

Host-to-host connection configuration

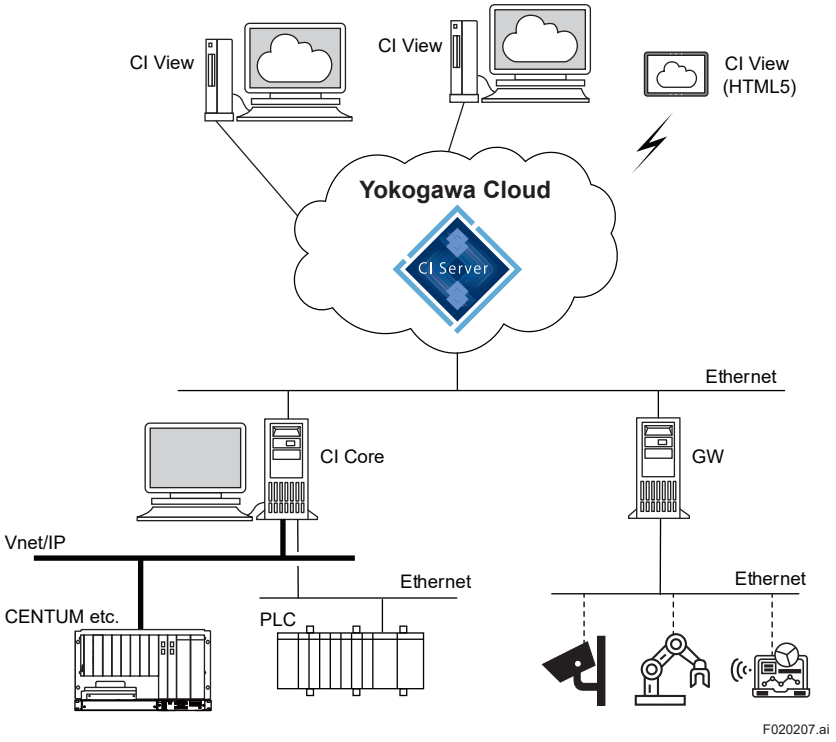
Data can be exchanged in real time between CI Cores that functions independently. This type of configuration may be used for applications where several systems at a central or across dispersed process locations need to be fully independent in terms of maintainability and operations, while at the same time exchange key data with other systems.



F020205.ai

Yokogawa Cloud Configuration

CI Server can use in a PaaS (Platform as a Service) format that combines Yokogawa Cloud, a software license, and maintenance. This solution facilitates the optimized management of production activities across an entire enterprise, while also providing a remote operation environment to ensure efficient plant operations from any location.



2.3 High availability

There are two high availability solutions in CI Server.

- Redundancy through HAC (High Availability Computing) function
- Redundancy through Dual-redundant platform

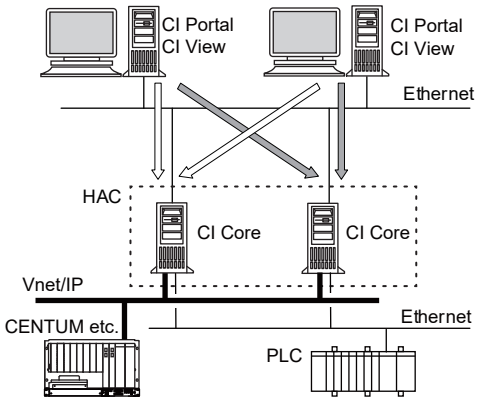
The functions of these two solutions are as described in the table below:

	HAC	Dual-redundant platform
Possible configuration	Dual, Triple, quadruple redundant servers	Dual redundant server
Method	Active/Standby * One server becomes active server and can be operated. Other servers are standby servers in waiting status. * Data from active server is always synchronized to the standby server.	Active/Standby (Always synchronized at I/O level) * One server becomes active server and can be operated. Other servers are standby servers in waiting status. * Memory (such as programs) and data from active server is always synchronized to the standby server. * Abnormality symbol of hardware can be checked.
For HW defects	Automatically switches to standby server	Automatically switches to standby server
For SW errors	Automatically switches to standby server	Cannot be switched
Switch over time	10 seconds to 1 minute When switching over, time is required to start software on the standby side. This time depends upon settings such as data count and data update frequency.	Within 1 second Components that access server (such as other servers, subsystems) are not affected by the switchover.
Data loss at the time of switchover	Data is lost during switchover.	Data is not lost. (Since switchover takes place with I/O level synchronization)
Operating sequence	Operation is suspended when switching over	Operation continues
View on network	Each server has different IP address. When switchover occurs, CI Portal automatically switches the connection destination in the active server and in case of CI View this switching is not required.	Two computers form one logical server. Two servers have the same IP address. Other servers need not recognize which server is active and can access either of them.
Disaster recovery	Possible Backup server can be configured in the remote site.	Not possible
HW model specification	Not present	Present

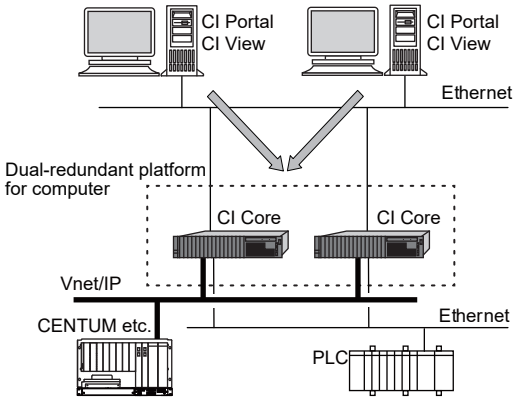
Note: When connecting with Vnet/IP, Dual-redundant platform, redundancy configuration common to all Yokogawa system products is recommended.

Note: The model of the computer used in Dual-redundant platform is restricted to the one specified by Yokogawa. For details, refer “PC redundant platform (GS 30A05C10-01)”.

Configuration example



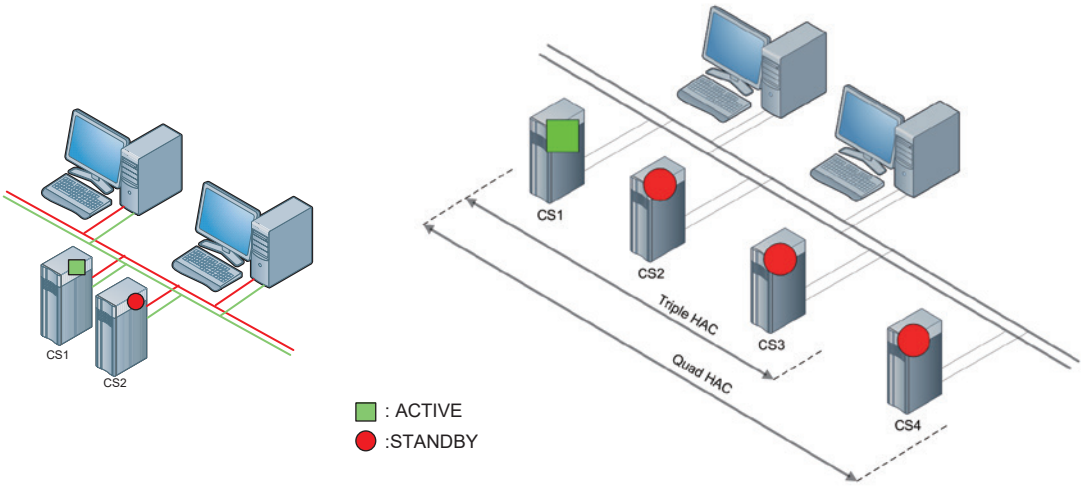
Example of HAC configuration



F020206.ai

2.3.1 HAC (High Availability Computing)

HAC is an Active-Standby type redundant system that is configured on multiple (about 2 to 4) servers. Under normal operating conditions, one server acts as the active server and performs all the processes. The remaining servers act as standby servers and are in the waiting state. If there is any issue in the active server due to which processes could not continue, any of the standby servers becomes active server and runs the processes.



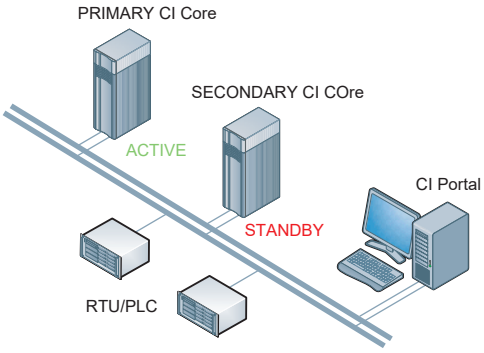
Dual HAC

Triple HAC, Quadruple HAC

F020301.ai

Dual HAC, Triple HAC, Quadruple HAC

Functional overview



F020302.ai

Configuration

The target component of HAC is CI Core. CI Portal cannot be configured with HAC. Generally, when using HAC solution, CI Portal and CI Core are placed in different servers. When HAC based switchover occurs, CI Portal automatically switches the connection destination to the active CI Core. CI View that is connected to CI Portal need not switch.

If you want HAC based switchover of CI Core and want to make CI Portal as redundant, multiple CI Portal needs to be prepared.

Note: In the server in which HAC configuration is adopted, CI View can be connected to CI Portal; but in such cases, the CI portal which is the connection destination of CI View needs to be manually changed when HAC based switchover occurs.

Active, Standby

Active and Standby represents the operation statuses of servers.

All the servers within the redundant structure acts as standby servers when started. Soon, when a server is assigned as primary server, it becomes the active server and all other servers (secondary servers etc.) continues to act as standby servers.

The active server runs all the processes. Other standby servers run minimum functions that are required to monitor itself and the other servers in the redundant system.

Switchover

When there is any abnormality in the active server, it shuts down and standby server switches to active state. This time required for the system to restore depends upon the system configuration and the hardware used.

Note: After switching from primary server to secondary server, if the primary server returns to its normal state, it will not switchover automatically to active state. Switchover takes place only under the following conditions:
* When there is an error in the active server
* When the switchover is done manually

Primary, secondary, tertiary, and fourth servers

Represents the priority order of servers. Immediately after the system is started, when none of the servers is active, primary server becomes active. If primary server does not become active, secondary sever (or subsequent server) becomes active as per the priority order. The priority order of primary, secondary, tertiary and fourth servers are decided corresponding to the physical servers.

Automatic mode and manual mode

Normally CI Server is operated in automatic mode. In the automatic mode, if there is any problem in the active server, switch overtakes place automatically.

In the manual mode, operation check and abnormality detection are carried out, but switch over does not takes place automatically.

The server can be set to operate in automatic mode or manual mode irrespective of connection to other servers. It can be set to manual mode during server maintenance to avoid switching over automatically.

Data synchronization

Data collection is done by active server. Data is always synchronized between active server and standby server and therefore, standby server starts immediately after the switchover.

History merge function

If there is a disconnection among HAC systems, standby server becomes active and sometimes there could be multiple active servers. After the connection is restored from this state, normally the history data of active server remains but the history data of standby server is thrown away. In order to avoid this, the History Merge function enables to merge and use the data collected by standby server.

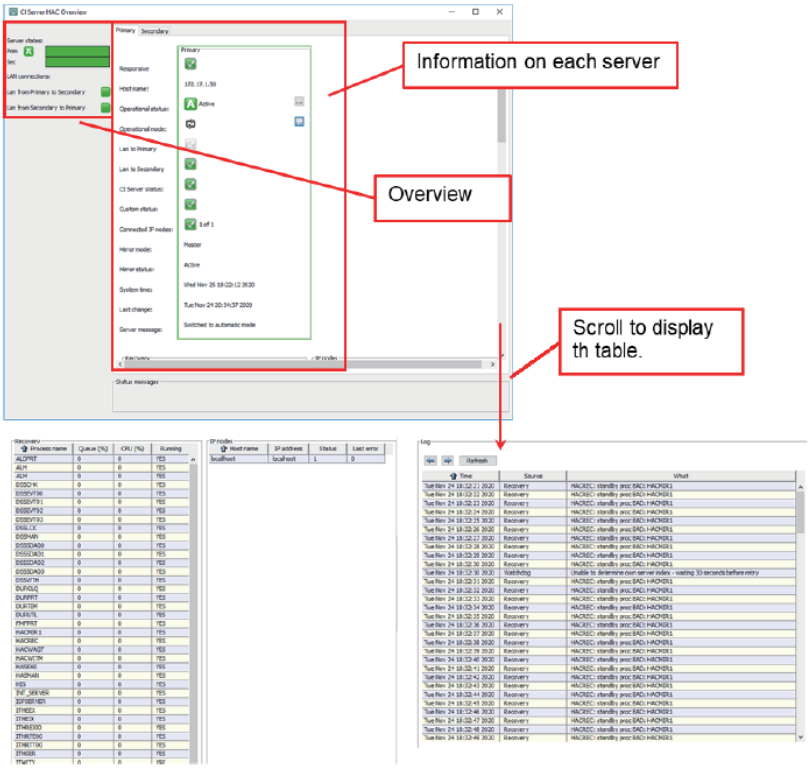
Island state (split brain condition)

The condition where server configured with redundant configuration could not connect to other servers or network devices, the server becomes completely independent and is called is in “Island status”. Since HAC system does not function properly in this state, server shuts down on its own. This is because it does not impact system in worse manner.

HAC management screen (HAC HMI)

HMI is made capable of monitoring the status of redundant server and switching to active server manually.

HAC HMI consists of an Overview panel on the left side and a Tab page that displays server-wise information. The Overview panel displays the server status and the connection status.



F020303.ai

Note: The time taken by a server to detect errors can be adjusted.
Note: In the HAC configuration, the two servers have different IP addresses. The applications that access the HAC servers must switch the IP addresses to be accessed based on the HAC switch over.

Restricted functions

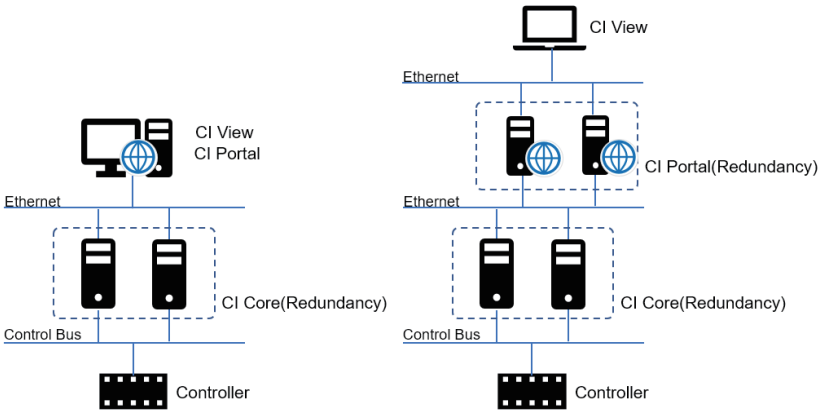
- During the HAC switchover, the external communication session using network is not maintained.
  The following are required to be reconnected.
  - ODBC Client
  - OPC Client
  - OPC UA Client
  - MQTT Client
  - Excel Add-in Report
  - Web browser connected to the CI Portal within the HAC configured servers
- DSS source file is not synchronized. If you have created DSS in a project, copy the source file manually.
- The data file read from DTS is not synchronized.
- The images, symbols, layout file that were created by connecting to CI Portal within the HAC configured servers are not synchronized.

2.3.2 Dual-redundant platform

The Dual-redundant platform is an Active-Standby type redundancy system with two servers.

Configuration

The systems that can form a redundant structure in Dual redundant platform are CI Core and CI Portal.



CI Core Redundancy example **CI Core, CI Portal Redundancy example**

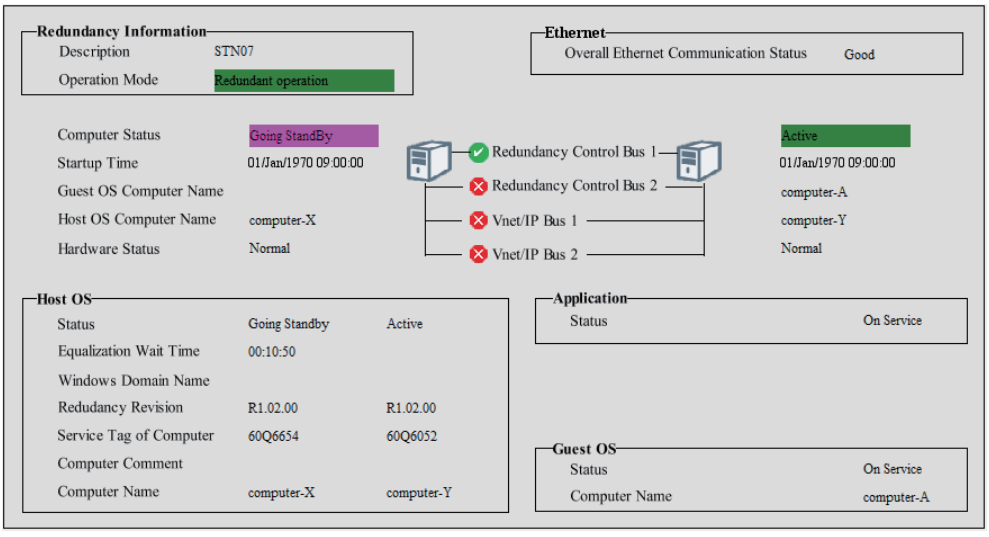
F020304.ai

For details about the specifications of Dual redundant platform, refer “Dual Redundant Platform (GS 30A05C10-01)”.

Note: There are limitations in OS and hardware when using Dual redundant platform. Refer GS mentioned above.

With redundancy management tool configured, manual switch over is possible.

The condition of Dual redundant platform is stored in item and symbols as mentioned in the image below are prepared.

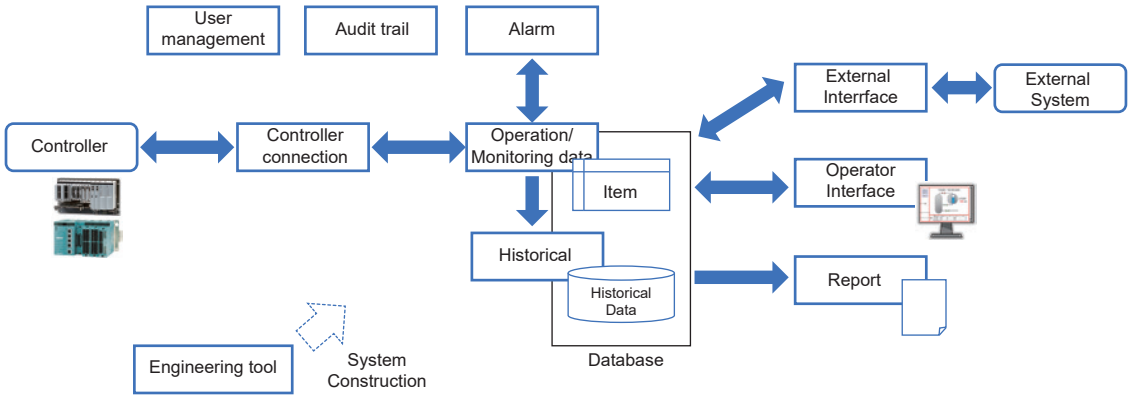


F020305.ai

3. Functional Overview

3.1 List of functions

The major functions are as mentioned in the image below:



F030101.ai

The following major functions are available.

- User management
- Audit trail
- Controller connection
- Operation / Monitoring data
- Alarm
- Historical
- External interface
- Operator Interface
- Report
- Engineering tool

3.2 Engineering tool

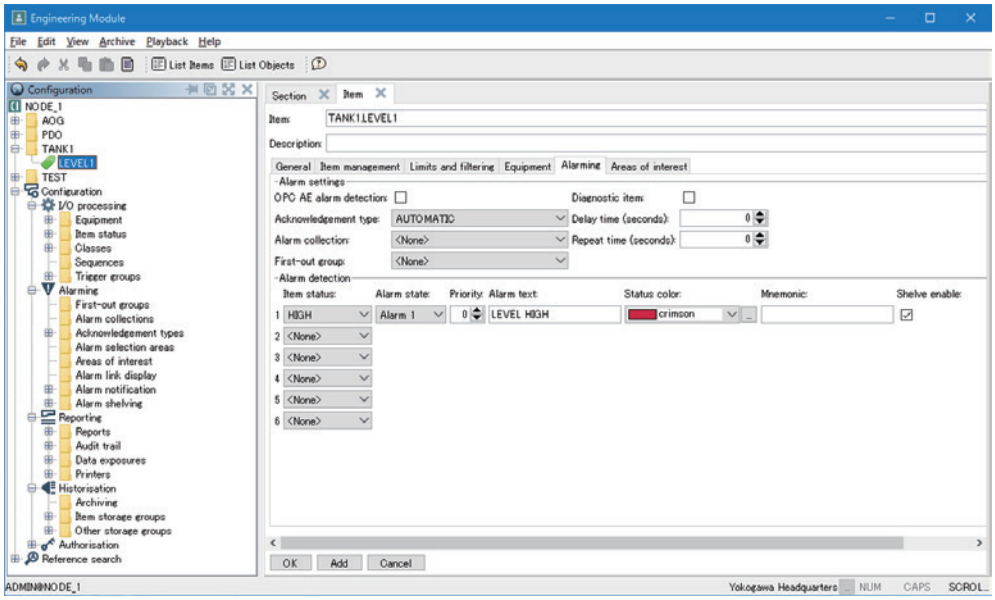
As many of the CI Server functions are configured using the engineering tool, this manual describes about engineering tool in the beginning.

The following tools are available for engineering.

- Engineering Module
  Tool that configures the system. Data and processes are defined using this tool.
- Edit Module
  Tool to create operation monitoring screens.
- Setup File Editor
  Tool to perform basic settings of the system.
- Quick Load Tool
  Import/export tool used for text file-based configurations.
- CI Exchange
  Tool used for configurations and tuning screens for connecting to Yokogawa controllers and for generating faceplate windows.

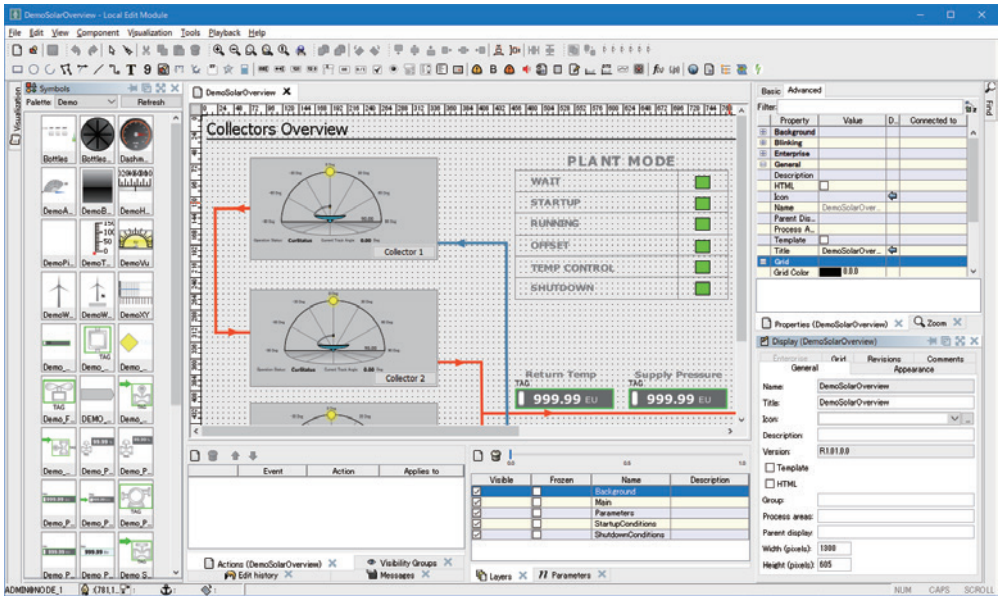
The definition items of each tool are as follows:

Engineering tool	Items that can be defined
Engineering Module	User definitions
	Controller connections
	Operation monitoring data definitions
	Data management definitions
	Alarm settings
	Historical definitions
	Audit trail definitions Report definitions
Edit Module	Operation monitoring screen definitions
Setup File Editor	Basic definitions of system
Quick Load Tool	All items
CI Exchange for CENTUM VP	Extract necessary information from the CENTUM VP project database and converts to CI Server database
CI Exchange for Prodigy	Extract necessary information from the CCC Prodigy project database and converts to CI Server database



F030201.ai

Figure Engineering Module screen



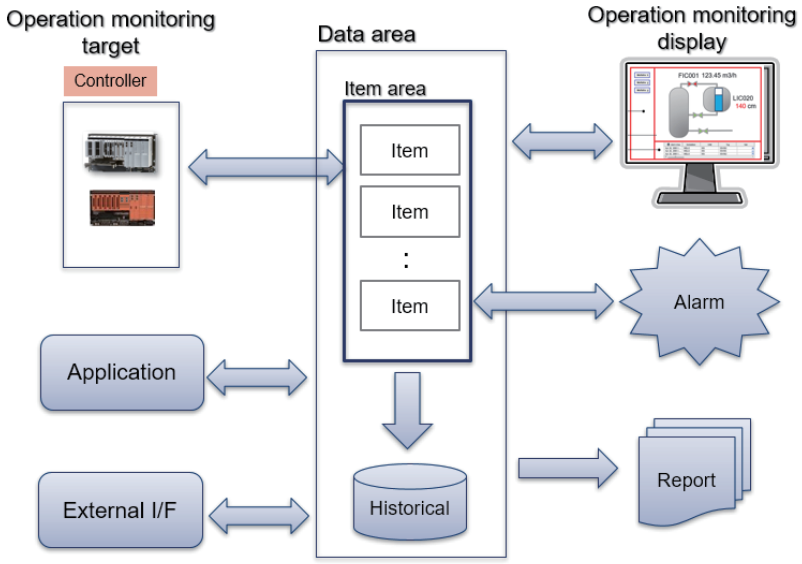
F030202.ai

Figure Edit Module screen

3.3 Item

Item

The data handled in CI Server is stored in the data region called as [Item]. The data collected from controller and the data processed by CI Server system are stored in the 'Item'. The functions of CI Server are configured around 'Item'.



F030301.ai

- The item data can be displayed in screen and output as report.
- If the item is connected to the controller data, the data read from controller is stored in the item. Also, when item value is changed, it is sent to controller. For example, the data entered through display is written to item, it is sent to controller.
- The historical process saves the item data as historical data.
- Alarm is generated when item data value or item status is abnormal.

Item consists of the following attribute data.

- Value
- Data type: Boolean, Integer, Real, String
- Engineering unit
- Item status
- Alarm judgement value, parameter for alarm
- I/O point (data of controller to be connected) etc.

The engineer defines the required items in the Engineering Module. When defining the items, the corresponding attribute data must be configured.

Subitem

Item can contain subitems that belongs to that item. Subitems contains the following functions, and these functions are capable of processing the values of main item (item to which the subitem belongs to).

- Addition
- Pulse counter
- Maximum value/minimum value
- Change ratio
- No type

Section

Item consists of layer structure called section and is defined as below.

Item format: [Section name. Section name. Section name....] Item name

The plant data with layer structure can be defined corresponding to the section and item.

(Ex) EAST.UNIT_A.TANK_1.LEVEL

3.4 User management

User management refers to managing users who can use CI Server and their privileges.

3.4.1 Users

The following attributes are available for each user.

- Username
- Supplementary information
- Password
- Privilege group
- Process area list
- Locale information (language)

Username

It is not case-sensitive. Up to 31 characters can be entered.

Supplementary information

79 bits or lesser

Password

It is not case-sensitive. Up to 31 characters can be entered.

Privilege group

Privilege group defines the user privileges. Allotting the user with a privilege group enables giving the user the privileges. The privileges within the privilege group are pre-defined.

Process area list

Process area denotes the area in which user can perform operations. In this area, the items for which values can be changed and alarms can be acknowledged are specified user-wise. Process area number can be attached to items, and by allotting process area number to each user, the items on which the user can perform operation can be specified.

Locale

Locale denotes the language used in the operator interface. When omitted, the default system language is used.

Currently, the languages that can be used are English (EN) and Japanese (JP).

3.4.2 User privileges

User privileges are allotted to user groups. The following privileges can be configured for users.

- Display, operable screens
- Operable devices and data
- Generatable reports and trends
- Management, notification, and acknowledgement of alarms
- Operation records (automatic or manual)
- Area that can be engineered

For each of the following actions, deletion, insertion, modification, and display privileges are available.

User privilege action (category)	Definitions
AUDIT_TRAIL	Audit trailing
AUTH_GROUP	User privilege group definition
CLASS	Method class definition
CLASS_ATTR_VAL	Method class attribute
DISPLAY	Display definition
FOLDER	Folder definition
HIS_GROUP	Item storage group definition
HIS_UNITS	Storage unit
INSTALL	Installation definition
ITEM	Item definition
ITEM_HISTORY	Definition to search Item data from item storage group
ITEM_HIS	Definition to assign item to item storage group
OBJECT_ATTR_VAL	Method object attribute
OBJECT	Object definition
OPC_GROUP	OPC group definition
REPORT	Report definition
SCAN_TYPE	Scantype definition
SCHEME	Scheme definition
SECTION	Section definition
SEQUENCE	Sequence definition
STATION	Station definition
STATUS	Item status definition
SUB_ITEM	Sub item definition
SYMBOL	Symbol definition
TRIGGER_GROUP	Trigger group definition
UNIT	Unit definition
USER	User definition

Action type	Definitions
_DELETE	Data deletion privilege
_INSERT	Data insertion privilege
_MODIFY	Data modification privilege
_READ	Data display privilege

In addition to the above privileges, the following privileges are also available.

User privilege action	Definitions
ALARM_CHRONO_READ	Read chronological alarm
ALARM_CURRENT_ACK	Acknowledge current alarm
ALARM_CURRENT_READ	Read current alarm
ARCHIVE_ACTIONS_READ	Archive overview function
ARCHIVE_COMMANDS	Execute archive operations
ARCHIVE_GROUPS_READ	Archive overview function
ARCHIVE_TAPES_READ	Archive data function
AUTH_ACTION_READ	Read authorization group
CLASS_INCLUDED_READ	Read included class
CLASS_SIGNALS_READ	Read unit value of class
EXECUTE_GENERAL_COMMANDS	All actions that are not unique to the data set
HIS_GROUP_FORCE_ROLLOVER	Forced rollover of storage group
INSTALL_BLOCK_UNBLOCK	Modify installation blocking
ITEM_ACK_ALARM	Acknowledge item alarm
ITEM_MODIFY_APPLICATION_FLAG	Modify item application flag
ITEM_MODIFY_BLOCKED_VALUE	Modify item block value
ITEM_MODIFY_DEADBAND	Modify item limit
ITEM_MODIFY_HISTORY	Modify historical value item
ITEM_MODIFY_LIMIT_HIGH	Modify item limit
ITEM_MODIFY_LIMIT_HIGH_HIGH	Modify item limit
ITEM_MODIFY_LIMIT_LOW	Modify item limit
ITEM_MODIFY_LIMIT_LOW_LOW	Modify item limit
ITEM_MODIFY_QUALITY_CODE	Modify item quality code
ITEM_MODIFY_STATUS	Modify item status
ITEM_MODIFY_STRING_VALUE	Modify item value
ITEM_MODIFY_ VALUE	Modify item value
ITEM_READ_ALARM_TYPE	Display item alarm
NODE_HOST_READ	Read host node
NODE_LOCAL_READ	Read local node
OBJECT_SIGNALS_READ	Read object signal value
REPORT_DELETE_ANY_GEN_REPORT	Delete all generated reports
REPORT_DELETE_GENERATED_ REPORT	Delete generated report
REPORT_GENERATE_ADHOC	Generate report as required
REPORT_MAINTAIN_LOGBOOK	Record logbook
REPORT_PRINT	Print report
REPORT_READ_GENERATED_REPORT	Display generated report
SECTION_BLOCK_UNBLOCK	Block/Unblock section
STATION_ON_OFF_SCAN	Change station scanning
SYS_LOG_READ	Read system logs
UNIT_BLOCK_UNBLOCK	Change unit blocking

3.4.3 Privileges and authentication of the entire system

Privileges and authentication for the entire system can be configured instead of configuring for each user.

Login methods of user:

Login methods when starting Operator Interface, Engineering Module and Edit Module are as follows:

- Login as the user registered within CI Server
- Login as OS user
  Username and password are managed in OS.
  (However, the same Windows username must be registered in CI Server)
  For example, log-in is not required when starting Operator Interface.
- Login linked with the Windows active directory
  CI Server privilege group is mapped with security group or organization unit.
  Single sign-on with OS user is also possible.
- No login

Privileges and authentication settings:

The following items are available:

- Methods of logging in to the system
- Single sign-on settings
- Active directory settings
- Password rules

etc.

3.5 Audit trail (Audit)

The Audit trail function is used to save data modification and logon/logout records. The saved records can be monitored on Reports or screen.

The saved records are used for the following purposes:

- To find the root cause of issues related to operation and management of processes being monitored.
- To improve the operation procedure of processes that is being monitored.

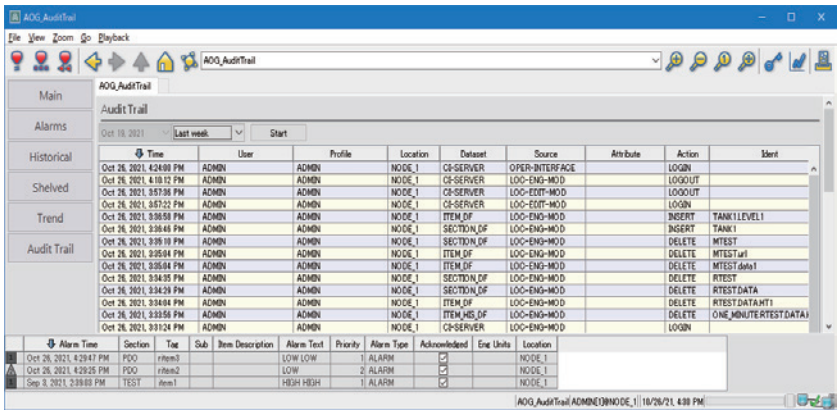
The following details are recorded:

- Operator name or application program that performs modification
- Place of modification
- Date when modification occurred
- Modification details if possible old value and new value
- Operator can enter additional text for description purpose

The following are the examples of operations that are logged:

- Change of set value
- Change of alarm limit
- Acknowledgement of alarms
- Opening/Closing valves
- Login/Logout actions (success or failure)

The records can be viewed on the Audit Trail Viewer.



F030501.ai

Basically, timestamp when the event occurred, and the related data (values before and after modification and occurrence reason) are saved.

The saved events and the retrieved events can be specified.

The saved items are as follows:

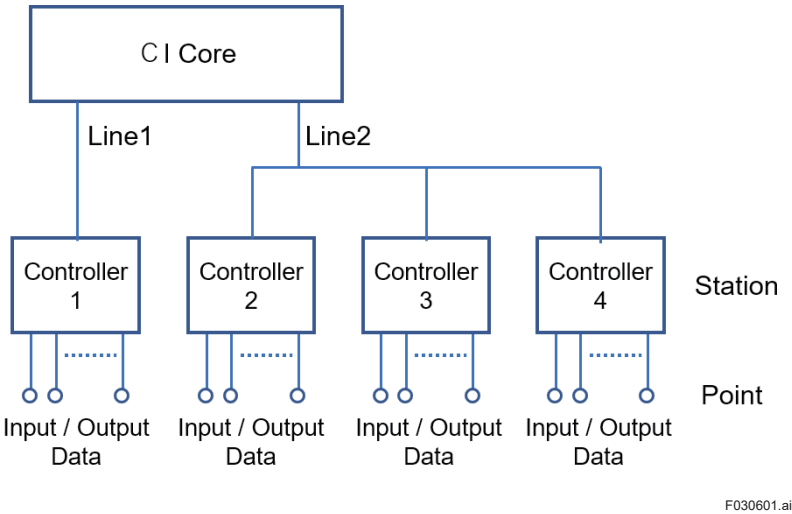
- Events
  - Login, logout, and login failure information
  - Insertion, modification, and deletion (by operator or application) of data
  - Alarm acknowledgement (by operator or application)
  - Shelving and un-shelving operations of alarms

- Timestamp when event occurred
- Username who performed operations
- Terminal name where operations were performed
- Values before and after modification (for example, when changing data, values of that data before and after changing)
- Items related to event
  - Data name
  - Program name
  - Alarm notification destination
  - Alarm notification user
  - User profile
  - Controller interface
- Name of the program that generated the event
- Application-wise information (when creating application in the program)

For details about the saved events, refer “Audit Management Engineering (IM 36K10L25-01JA)”.

3.6 Controller connections

This function defines the controllers that are connected to CI Server. It also selects the controllers and communication protocols. The controllers that are connected to CI Server are called stations. The communication protocol between the controllers and CI Server is called a line. And the I/O data that are connected to CI Server (CI Core) through controllers are called points. The concept of stations, lines, and points are as explained in the figure below.



In the figure above, CI Server is connected to controllers through two types of lines.

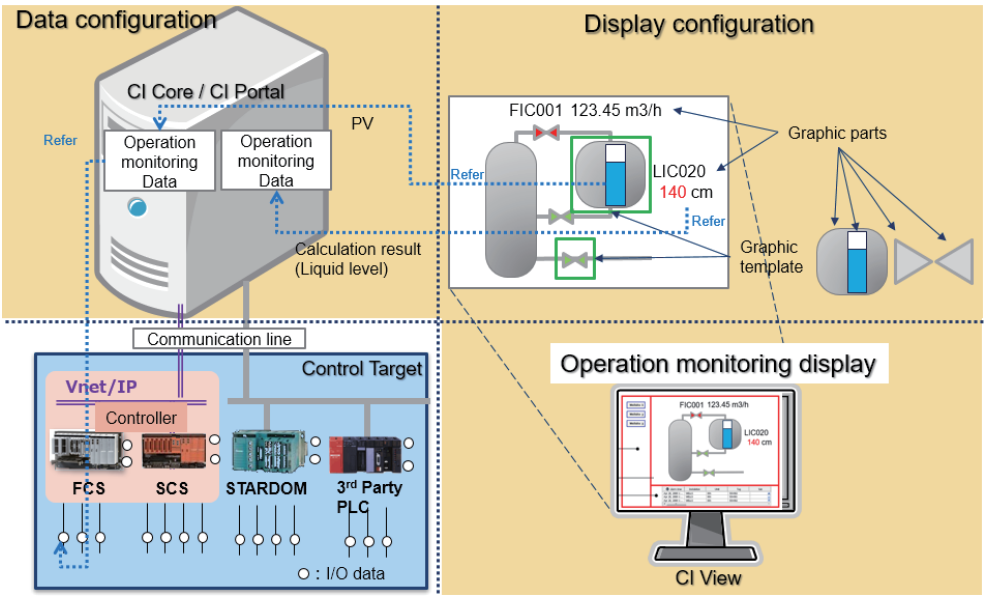
Line 1 is connected to one station and Line 2 is connected to two stations.

In the controller connections, stations, lines, and points are defined based on the system to be connected.

3.7 Operation monitoring data

The operation monitoring data that is collected from controllers and the data processed by CI Server system are stored in item.

The overall picture of operation monitoring is as shown in the figure below.



F030701.ai

3.8 Alarms

Features

The Alarm function of CI server has the following characteristics:

- Acknowledgement of alarms
  Some alarms are required to be acknowledged. Manual/automatic alarm acknowledgement can be configured.
- Suppression and delay of alarms
  Some of the alarms that are generated at the time of starting up the process can be suppressed.
- Repetition of alarms
  Alarms that were not acknowledged can be configured to be repeated.
- Grouping
  Alarms can be grouped. If you acknowledge the representative item of the group, the entire group is acknowledged. If you reset that item, the group is reset.
- First-up alarm
  It is used when focusing the item that is the cause of the first alarm within the alarm group.
- First-out alarm
  Only the first alarm within the group is considered as alarm and the rest of the alarms are suppressed.
- Alarm link display
  When an operator clicks the alarm, immediately the screen switches to the screen containing the alarm tag.

- If an alarm is not acknowledged within the stipulated time, it can be resent to another workstation.
- After the workhours is over, the destination where alarms need to be sent can be modified.
- Alarms can be filtered when operator wants to receive alarms only from specific area (process area).
- Dynamic modification of priority
  If an alarm continues even after the stipulated time and is not acknowledged, its priority can be modified.

Summary

CI Server generates and displays alarms on its own. Alarms generated outside the CI Server can be captured and displayed via OPC A&E or OPC UA A&C. CENTUM alarms can be handled as OPC UA alarms, and alarm color and alarm status can be displayed by acquiring CENTUM engineering information.

The following phenomenon are handled as alarms:

- Abnormality in item value/item status
  Alarms are determined by the upper and lower limit of item value, and the item status.
- OPC A&E alarms
  Alarm information is taken from OPC A&E.
- OPC UA A&C alarms
  Alarm information is taken from OPC UA A&C server.
- CENTUM alarms
  Alarm information is directly taken from Vnet/IP and converted to the OPC UA alarm format. CENTUM alarms are handled as OPC UA alarms.

The following information is included in the alarms and is displayed on screens etc.

- Alarm priority (0-15)
- Alarm status (Alarm, event, acknowledgement, reset, normal etc.)
- Alarm time (Timestamp received from controller or the timestamp generated by CI Server (has precision up to millisecond))
- Item name, item value, item description, alarm description
- Alarm status text (Low, Low-Low, High, High-High, normal, under-range, over-range, offline, blocked etc.)

In this document, basic concept, and structure of alarm process of CI Server is explained. The basic role of an alarm is to detect any abnormality in item value or status and notify the user. To realize this, alarm function consists of the following four major processes.

1. Alarm detection (decision based on limits)
2. Alarm management (acknowledgement, grouping, filter definition etc.)
3. Alarm display/operation (alarm overview, alarm count etc.)
4. Alarm external notification (mail sender etc.)

Terminologies and concept used in these processes are explained.

Limits/Limit value

It is the threshold value configured for the item value. Whenever the item value changes, it is compared with the limit value, and as a result, the item status is determined.

Item status

It shows the status of an item. Limit value is configured for each item, and whenever the item value crosses the range of limit range, as well as when an item that has earlier crossed the limit range and has now returned within the range, item status changes and alarm is generated.

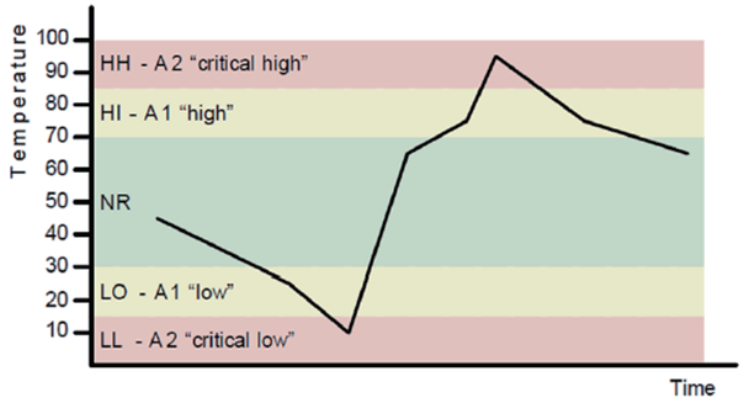
Note: When the item status changes from NORMAL -> HIGH HIGH (at a time), only HIGH HIGH alarm is generated. HIGH alarm is not generated.

Alarm status

The item statuses HIGH, LOW etc. (as well as the generated alarms) are classified into the following four alarm statuses.

Alarm status type	Alarm notification	General item status (part) classified by default
NORMAL	Not notified	NORMAL, BLOCKED
Alarm 1 (A1)	Notify	OFFSCAN etc.
Alarm 2 (A2)	Notify	HIGH, LOW etc.
Alarm 3 (A3)	Notify	HIGH HIGH, LOW LOW etc.

Alarm statuses are classified based not only on system general settings but also on the item-wise settings. Example of item status: (High is classified as A1, HighHigh as A2 etc.)



F030801.ai

Alarm status value is single valued and does not contain multiple values. For example, when status changes from HIGH to HIGHHIGH, status value becomes HIGHHIGH and HIGH condition is deleted.

Priority/Priority value

In addition to the alarm status-based classification, item statuses (or generated alarms) can also be classified based on the priority (or criticality) using the values from 0 to 15. Similar to alarm status, priority settings can also be based on system general settings and item-wise settings.

Priority is used for sorting and filtering the alarms on Alarm Overview.

Also, if an alarm is not acknowledged for the specified time after it is generated, or even after it is acknowledged, the priority value linked to the alarm can be changed to change the criticality of the alarm and the same can be displayed.

Acknowledgement

If a highly critical alarm is generated, that alarm can be made mandatory to be acknowledged by the operator. The alarms to be acknowledged blink on the Alarm Overview.

You can configure the alarms such that they must be acknowledged, or they need not be acknowledged.

Alarm shelving

‘Shelf’refers to the shelf and ‘Shelving’ refers to arranging on the shelf.

In order to avoid the operator getting overloaded when a lot of alarms occur and to avoid time consumption on less-critical alarms, Alarm shelving function can be used to arrange the alarms on the shelf (Shelving).

The alarms shelved by the operator are deleted from the Alarm Overview and are moved to Shelf Alarm Overview.

3.8.1 Alarm functions list

The following table shows the list of alarm functions.

Category	Function	Description
Alarm detection	Limit judgement	Alarms are judged based on the upper and lower limit of alarm values.
	OPC A&E alarm detection	Alarm information is taken from OPC A&E.
	OPC UA A&C alarm detection	Alarm information is taken from OPC UA A&C server.
	CENTUM alarm detection	Alarm information is directly taken from Vnet/IP and converted to the OPC UA alarm format. CENTUM alarms are handled as OPC UA alarms.
Alarm acknowledgement	Alarm acknowledgement	Critical alarms are acknowledged by the operator.
Display/Operate alarms	Alarm Overview	Displays the list of alarms that are generated earlier and the alarms that are currently generated.
	Alarm Sound	Replays the alarm sound based on the generated alarms.
	Area of interest	Alarms are filtered based on the labels attached to data.
	Alarm Selection Area	Alarms are filtered based on the condition format.
	Alarm shelving	Arranges the low-priority alarms on the shelf and processes the high priority alarms.
	Alarms/Display linkage	Displays the alarms generated from the Alarm Overview to the corresponding screens.
	Export to file	Exports the alarms to the files.
	Alarm Suppression	Alarms can be switched off data-wise or device-wise.
Alarm Group	First out group	Displays only the first alarm in a group. Multiple groups can be configured in layers.
	Alarm Collection group	Statuses of alarms can be grouped and can be managed in bulk.
Notification	Alarm notification	Notifies alarms through mails and SMSs.
Reports	Report function	Sends out alarms as reports.

Alarms can be filtered when displaying/operating and notifying them. The following types of filters are available.

Type	Description
Filtering based on date	Alarms can be filtered by specifying the date and duration.
Filtering based on condition	Alarms can be filtered by conditions such as data name, Area of interest, and alarm selection area.

The following display operation settings can be configured for alarms.

Type	Description
Delayed alarms	Displayed as alarm only when the alarm status continues for the specified time.
Repeated alarms	After identified as alarm, if status crosses the specified time, it is displayed as repeat alarm every time it crosses the specified time.

The Alarm Grouping function enables avoiding reoccurrence of same alarm multiple times, thus reducing the load on operators to respond to alarms. The following type of groups are available.

Type	Description
First out group	Displays only the first alarm within a group and suppresses all the other alarms generated within the same group. This helps to avoid flooding of alarms in the Alarm Overview. Multiple groups can be configured in layers.
Alarm Collection group	Occurrence / Acknowledgement / Reset of alarms can be grouped and managed in bulk.

3.8.2 Alarm Overview screen

When an alarm occurs, it is displayed in a list in the Alarm Overview. Alarm Overview is of three types as mentioned below:

Name	Description
Current alarm overview	Displays alarms that are currently generated. Alarms can be confirmed on this screen.
History alarm overview	Displays record and history of alarms generated earlier or returned alarms and acknowledged alarms.
Shelf alarm overview	Displays alarms that were moved from the Current Alarm Overview by performing shelving operation.

Current alarm overview

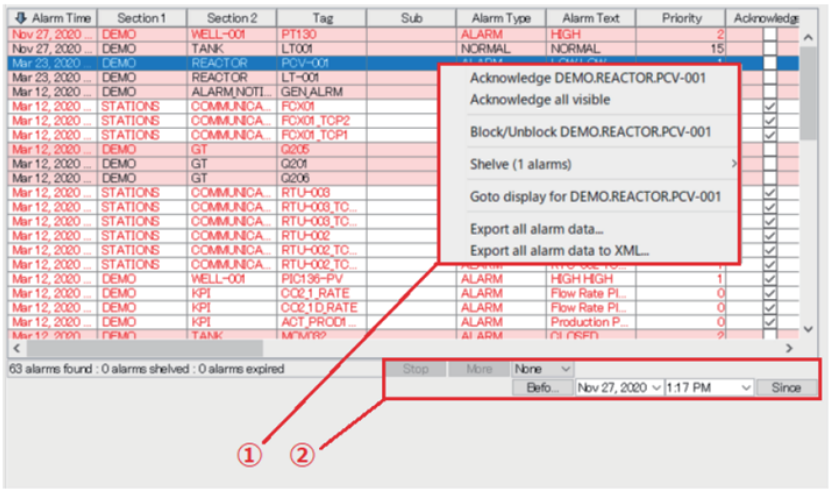
Displays occurrence of current alarms and return status of alarms. Displays the current alarms and the alarms that are not acknowledged. Alarm related operations such as acknowledgement of alarms and alarm shelving (arranging the alarms in shelf temporarily) can be done on this list. You can change the order of items in the displayed list or apply filters on the columns by clicking the column title.

F030802.ai

Figure Current alarm overview

When alarms are deleted (manually or automatically) or when the alarms are acknowledged, they disappear from this list.

Foreground color and background color can be selected based on the alarm status. Columns can be positioned arbitrarily and displayed.



F030803.ai

(1): Right-click menu
(2): Filter specification area for alarms to be displayed

FIgure Operations on Current Alarm Overview

Alarms can be acknowledged by one of the following methods:

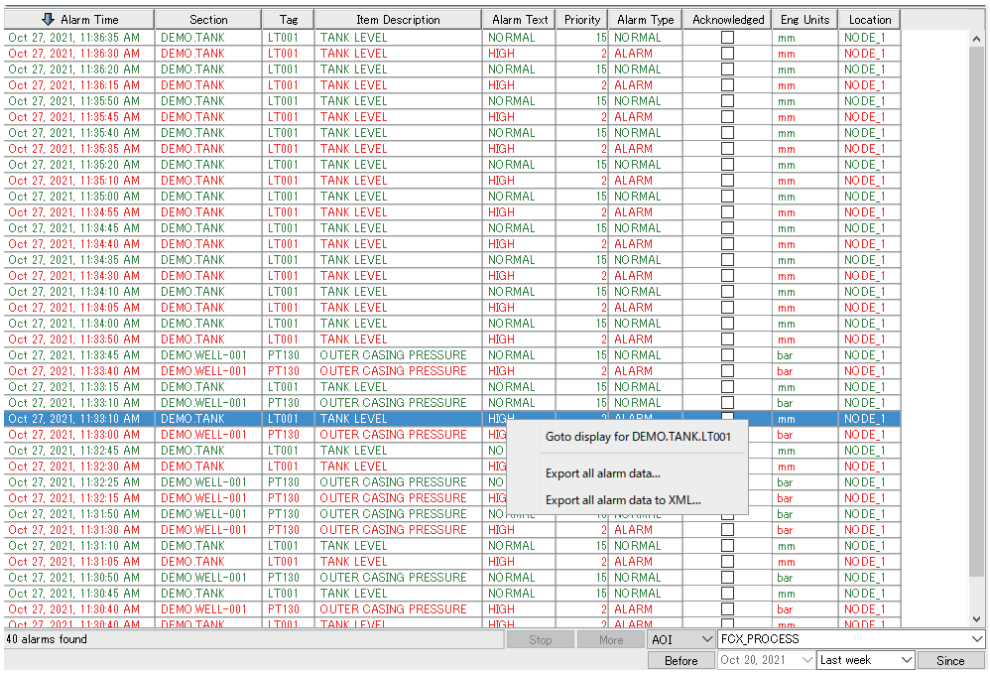
- By clicking the check box on the [Confirm] column on the Overview screen.
- By right-clicking on the corresponding alarm row and selecting [Confirm]. Depending upon the settings, multiple alarms can be acknowledged at the same time. To select multiple alarms, either drag, or use Shift + click or CTRL + click.

The following operations can be performed using the right-click menu:

- Acknowledging the alarms
- Blocking the item on which alarm occurred
- Shelving of alarms
- Linking to display (Displaying the item where alarm is generated)
- Exporting to alarm file

The displayed alarms can be filtered by specifying filter conditions on section □. Alarms can be filtered based on time, section, tags, ASA etc.

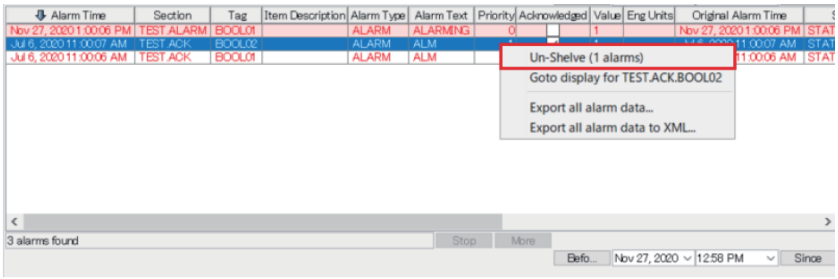
- **Historical alarm overview**The AD Organizer, the main software for engineering for mod-
  Displays records and history of alarms that were generated in the past or returned alarms, acknowledged alarms etc.



F030804.ai

- **Shelved alarm overview**

  Displays alarms that are shelved. Shelving operation can also be cancelled from this screen.



F030805.ai

Display contents

Alarm information that can be displayed on the Current alarm overview /Historical alarm overview are as follows:

Column name	Description
Alarm time	Time when alarm (event) occurred or returned
Section 1	Topmost section on the section layer where alarm (event) items are defined
Section 2	Second section from the top on the section layer where alarm (event) items are defined
Tags	Tag name of alarms (Among items, it is the item name after the section layers are removed)
Subitem	Name of the subitem of alarms (events)
Alarm type	Alarm type of the alarms (events). NORMAL: normal ALARM: Alarm ACKNOWvAcknowledgement DELAY: Delayed alarms DIRECT: Direct alarms FIRSTUP: Firstup alarms etc.
Alarm text	Alarm text of alarms (events)
Priority	Priority order of alarms (events)
Acknowledgement	Acknowledgement conditions. ON when acknowledged, OFF when waiting for acknowledgement
Value	Alarm value when alarm (event) occurred or returned
Quality	Quality value when alarm (event) occurred or returned
Supplementary information	Supplementary information defined in the items of alarms (events)
Engineering unit	Engineering unit defined in the items of alarms (events)
Event source	Generally left blank. OPC event source when used for detecting OPC events.
Event Cat.	Generally left blank. OPC event category when used for detecting OPC events.
Event condition	Generally left blank. OPC event condition when used for detecting OPC events.
Event sub condition	Generally left blank. OPC event sub-condition when used for detecting OPC events.
Event actor	Generally left blank. OPC event actor when used for detecting OPC events.
C Event source	Generally, the same as [Supplementary information] OPC event source when used for detecting OPC events.
C Event Cat.	Generally, the same as [Alarm type] OPC event category when used for detecting OPC events.
C Event condition	Generally, the same as [Alarm text] OPC event condition when used for detecting OPC events.
C Event sub condition	Generally, the same as [Alarm text] OPC event sub-condition when used for detecting OPC events.
C Event actor	Generally displayed as CI_SERVER OPC event actor when used for detecting OPC events.
Item name	Item name of alarms(events) (including section layers)
Acknowledgement users	User who performed acknowledgement of alarms
Original alarm time	Time when alarm (event) is generated (Direct alarm occurred time in case of delayed alarm events)
Section	Section layer where items of alarms (events) are defined
Location	CI Core node number where items of alarms (events) are defined

Column name	Description
Section 1 description	Supplementary information defined in section 1
Section 2 description	Supplementary information defined in section 2
Area☐☐	Name of the Area of interest defined in the items of alarms (events) ☐☐ denotes the number of area of interest of the item definition.
Area☐☐ definition	Supplementary information of the Area of interest defined in the items of alarms (events) ☐☐ denotes the number of area of interest of the item definition.
Section description	Supplementary information of section where items of alarms (events) are defined
Alarm Collection	Name of the alarm collection where items of alarms (events) are defined
Priority Text	By default, the priority value is displayed. If the priority text is configured, the text according to the priority value will be displayed.
<CI attribute name>	CI attributes are user-definable attributes. Vendor-specific attributes can be defined as CI attributes in the OPC AE client settings. The CI attributes selected on the Attributes tab of the Component Properties in the alarm overview are displayed here.

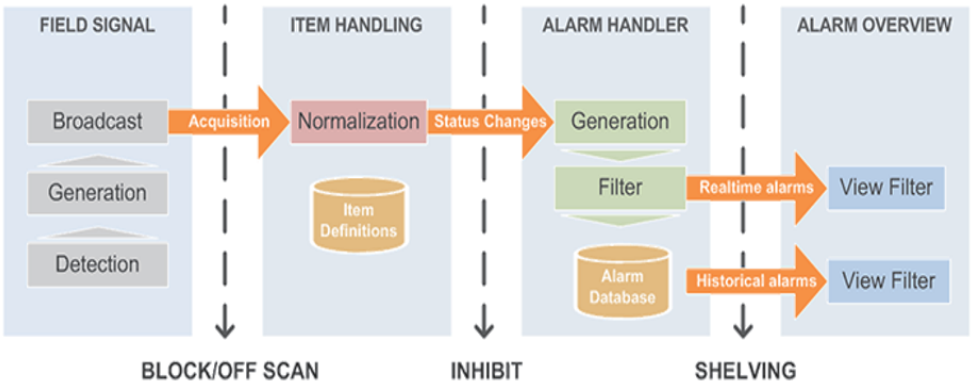
The column type and display contents are common for Current Alarm Overview and History Alarm Overview.

The displayed columns and their order are configured in the engineering phase.

3.8.3 Alarm control

Alarms can be controlled in the following levels:

Stopping data collection	Alarms are suppressed by stopping the data collection. Shown in the SCAN place in the following diagram
Suppressing alarm generation	Alarms are suppressed after data is collected. Shown in INHIBIT place in the following diagram.
Suppressing alarm display	After alarms are generated, they can be suppressed by using the display filter. Shown in SHELVING place in the following diagram. Shelving is a type of filtering.



F030806.ai

3.8.4 Acknowledgment of alarms

When alarms are generated, they are displayed in the Current Alarm Overview. For alarms requiring the operators to acknowledge, the corresponding rows blink and the [Acknowledge] column checkbox is turned OFF. For alarms that do not require to be acknowledged, the corresponding rows do not blink and the [Acknowledge] column checkbox is turned ON.

The alarms that are acknowledged by the operator are recorded as [ACKNOW] in

the History Alarm Overview.

The operator can acknowledge an alarm by turning ON the checkbox in the [Acknowledge] column of the Current Alarm Overview

● Configuring the acknowledgement type setting

Alarms are generated based on the change in the item status. Each item status is classified into four alarm statuses (Normal/Alarm1/Alarm2/Alarm3). Whether the changes in these alarm statuses need to be acknowledged or not can be configured during the engineering phase.

For each change of the alarm status (Ex Normal --> Alarm2), whether acknowledgement process is required (acknowledgement process required) or not required (automatic acknowledgement) is configured. Also, based on the alarm acknowledgement status (acknowledged or not) before the change in alarm status, whether alarm acknowledgement is required or not after the status change is configured. In other words, based on the alarm status 4 types and alarm acknowledgement types (2 types) before the status change, and alarm status 4 types after the change, whether alarm acknowledgement is required after the status change is defined for the combination (4 x 2 x 4). This definition is considered as acknowledgement type.

Several of these acknowledgement types are set and by allotting acknowledgement type for each item, operations at the time of acknowledging the alarms are determined

● Acknowledgment type definition for external alarms

Item-based alarms have four alarm states, “Normal,” “Alarm 1,” “Alarm 2,” and “Alarm 3” while external alarms have two alarm states, “Normal” and “Alarm.”

Therefore, select the External alarm check box when defining acknowledgment types for external alarms. If this check box is selected, there will be eight check boxes for configuration, regarding Inactive and Active. Inactive corresponds to “Normal” and Active corresponds to “Alarm.” Select the check boxes for the state transitions that do not require manual acknowledgment.

3.8.5 Alarm notification

In addition to displaying the occurrence and return of alarms on the Alarm Overview, they are also notified through the following methods:

- Notification through emails
- Notification through SMS

3.8.6 Occurrence conditions of alarms

Alarms are generated under the following conditions:

- Comparison of limit value and item value
- Judgement of status data obtained from controllers (status change through OPC communication)
- Status written through application

3.8.7 Options at the time of alarm occurrence

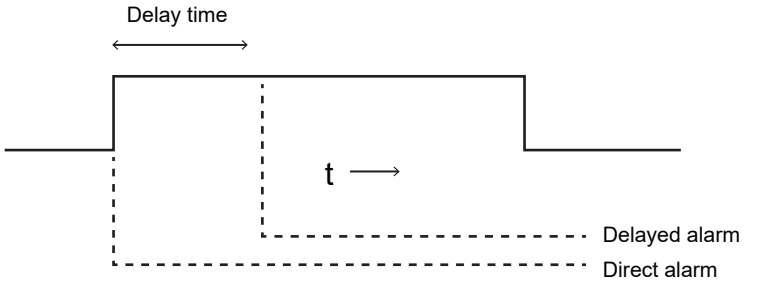
Options at the time of alarm occurrence. The following occurrence options are available.

- Delayed alarms
- Repeated alarms

Delayed alarms

If you want to display as alarm after the same alarm status continues for the specified time, delayed alarm can be used.

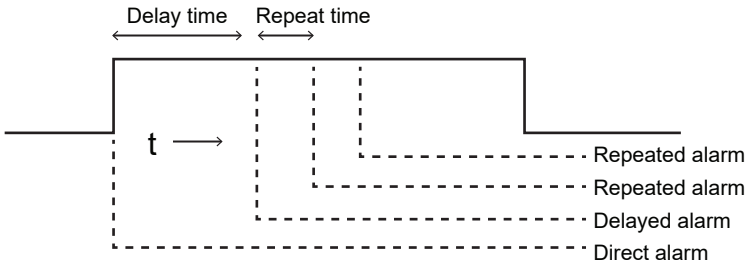
When delayed alarm is configured, the alarm is not displayed on the Alarm Overview until the specified time is crossed after the item status changes to alarm status. After the specified time, the alarm is displayed on the Alarm Overview. At that time, the type of the alarm is displayed as [DELAY].



F030807.ai

Repeated alarms

If you set the repeat time, when item status changes to alarm status and the specified time elapses, repeat alarm is generated. This repeat alarm is repeated every time the specified time is crossed until the alarm status returns to normal status. Repeat alarms can be acknowledged only on the History Alarm Overview.



F030808.ai

3.8.8 Alarm Suppression

Display and notification of section-wise and item-wise alarms need to be suppressed or not can be configures.

3.8.9 Using alarm information

The information created in the alarm function can be used in the other functions of CI Server such as Reports.

3.8.10 Grouping of alarms

In real systems, multiple alarms are generated from a single phenomenon, and these alarms are displayed on the Alarm Overview Screen and it is time consuming for the operator to respond (acknowledgement, judgement etc.) to critical alarms. Also, when multiple alarms are generated, it is time-consuming to respond to each alarm. This situation can be avoided by using the Alarm grouping function, thus reducing the load on the operator to respond to alarms.

The following two grouping methods are available in CI Server.

- First out group
- Alarm collection group

First out group

With this grouping method, only the first alarm within a group can be displayed and all the other alarms generated within the same group can be suppressed. This helps to avoid flooding of alarms in the Alarm Overview. Multiple first out groups can be layered.

Alarm collection group

With this grouping method, alarms of all the items (group items) registered in a group can be managed together.

Status of each alarm collection group (group status) represents the occurrence condition, acknowledgement status and reset status of alarms generated in the group items. Group status is displayed as a combination of three information, occurrence condition of alarms, execution status of acknowledgment operation, and execution status of reset operation.

Since each alarm has statuses [No Alarm/Alarm generated], [waiting for acknowledgment/ Acknowledged], [Waiting for reset operation/reset operation completed], group status can have one of the 8 statuses (2 x2 x2).

- When group status is [Alarm]
  Signifies that one or more alarms are generated in the group items. Even if one alarm is generated among the group items, group status becomes [Alarm].
- When group status is [Acknowledgement required]
  Signifies that one or more unacknowledged alarms are present among the alarms generated in all the group items. Only if all the alarms are acknowledged, group status becomes [Acknowledged].
- When group status is [Reset]
  Signifies that reset operation is performed for the alarm collection group.

3.8.11 Alarm display filter

Alarm filter can be used when extracting the required alarm from several alarms: for example, when referring to historical alarms. In addition to the standard filters such as section name and item name, filter conditions can also be created based on system requirements.

Alarm filters can be used on Alarm Overview, Alarm sound, and alarm notifications. Depending upon the usage, there could be limitations on the type of filter used.

The following filters are available:

- Section and item names
- Area of Interest (AOI)
- Alarm Selection Area (ASA)

Alarm filter usage in each usage area

Filter used on	Filter type		
	Section and item name	Area of Interest (AOI)	Alarm Selection Area (ASA)
Alarm Overview	Yes	Yes	Yes
Alarm Sound	Yes	Yes	Yes
Alarm notification	No	No	Yes
User filter settings (*1)	No	No	Yes

*1: Configuration in which each user is allotted with a filter, and these filters are used as initial display when alarms are displayed on the Alarm Overview.

Area of Interest (AOI)

Area Of Interest (AOI) is a filtering method in which alarms are filtered using the labels attached to alarm definitions.

Each item can have up to 16 labels attached to it.

Since each item is defined independently, this method is used when the items to be filtered are less or when items cannot be filtered through item name and section name or when the conditional expression in the Alarm Selection Area is too long or too complicated.

Alarm Selection Area (ASA)

Alarm Selection Area (ASA) is a filtering method in which alarms are filtered based on the conditional expression that uses information related to alarms and items. If the alarms that are generated satisfies the conditional expression shown on the specified Alarm Selection Area, those alarms are displayed or notified.

In addition to using this filter in the Alarm Overview and Alarm Sound, it can also be used when notifying alarms (sending mails/SMS).

Format of the basic conditional expression is as shown below:

Conditional expression: <Keyword> <Related operator> <constant>

Ex: section = “Plant1.Factory1.Boiler1”

Meaning of the example: All the item alarms included in the Section name “Plant1.Factory1.Boiler1”. (Items defined under the subsection of “Plant1.Factory1.Boiler1” are not included)

<Keyword>, <Related operator>, <constant>that can be used are as follows:

<Keyword> (text within the brackets is the data type that can be used in <constant>)

- ACTOR_ID (character string)
  Source name for OPC acknowledgement request.
- AOI (character string)
  Areas of Interest.
- COLLNAM (character string)
  Alarm collection group.
- COND_NAME (character string)
  OPC condition.
- EAL_ID (EAL id data type of an external alarm)
  EAL id
- EAL_NAME (character string)
  The tag part of external alarm identification. Wildcard can be used for <Constant>.
- EVENT_CAT (character string)
  OPC event category
- INST (character string)
  The installation part of the item identification (for compatibility with old version). Wildcard can be used for <Constant>.
- ITMID (item id data type)
  Item id
- ITMNAM (character string)
  The tag part of item identification. Wildcard can be used for <Constant>.
- ITMSUB (character string)
  The sub-item part of item identification. Wildcard can be used for <Constant>.
- PRIO (integer)
  The priority value of alarm.
- QC (integer)
  The quality code value of alarm.
- SECTION (character string)
  The section part of item identification. Wildcard can be used for <Constant>.
- SOURCE (character string)
  OPC event source (for example, tag name).
- SUBC_NAME (character string)
  Active OPC sub-condition.
- UNIT (character string)
  The unit part of item identification (for compatibility with old version). Wildcard can be used for <Constant>.

<Related operator>

Depending upon the data type used in the keyword, only some operators can be used. Refer the following table for details.

Related operator	Description	Character string	Integer	Item ID Data type
!=	Not equal	Yes	Yes	Yes
=	Equal	Yes	Yes	Yes
>	Greater than	Yes	Yes	No
<	Lesser than	Yes	Yes	No
>=	Equal or greater than	Yes	Yes	No
<=	Equal or lesser than	Yes	Yes	No
|	Bit-wise OR	No	Yes	No
&	Bit-wise AND	No	Yes	No

<constant>

Integer, character string, or item ID data value can be mentioned directly. Character string must be enclosed within double quotations (”). Also, the following wild cards can be used when specifying character string.

- Asterisk (*)
  Represents character of any number. For example, [PT-1*] shows all the character strings that begin with PT-1 (includes “PT-1”).
- Question mark (?)
  Represents any one character. For example, (PT-1??) shows all the character string that start with PT-1 followed by 2 characters.

When conditional expression is mentioned, compile is executed to check if the format of the mentioned content matches.

The following format can be used as data format of item ID. Node number, item group number, item number, sub number, attribute number

(Each item is separated by comma) Ex: itmid = 1, 1, 5, 0, 0

Node number: Node number on which CI Core works

Item group number.Item number: Internal item ID. The two numbers displayed on the “General” tab of the Item definition.

Sub number: 0

fixed attribute number: 0 fixed

Multiple conditional expressions can be combined using logical operators (and/or) and a new conditional expression can be created.

Comment

Comment can be included in the conditional expression. It can be used to leave a note about the conditional expression. Comments are enclosed between [/*] and [*/]. And are ignored when evaluating the conditional expressions.

3.8.12 Alarm shelving

When there is large no. of alarms generated, you may want to focus on high priority alarms leaving the low priority alarms to be dealt later. Alarm shelving can be used to select and shelve the low priority alarms. After responding to the high priority alarms, you can remove the low priority alarms from the shelf and handle those alarms.

3.8.13 Alarm link display

The Alarm and display linking (Alarm link display) function shows the screen to link alarms on the Alarm Overview. The aim of this function is to help the operators with alarm acknowledgement by directly displaying the screen related to an alarm after it is generated.

3.8.14 Alarm Sound

When alarm is generated, audio file can be played.

This is realized by using a graphical alarm sound part in engineering.

3.9 Historical

The Historical function saves data in time series. The saved data (historical data) can be displayed as trends and reports.

The following data can be saved as historical data.

1. Items
2. Item events
3. Audit events
4. System events

3.9.1 Storage group

Items are saved as historical data in units of storage group.

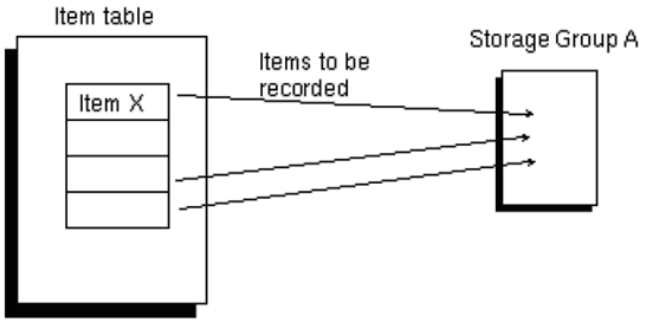
The following settings are required for each storage group.

- Regular saving/Event based saving (saved when data is changed)
- Save period of historical data etc.

The setup procedure to save items as historical data is as follows:

(1) Create storage group. Configure save frequency, save period etc.

(2) Register the items to be saved in the storage group



F030901.ai

3.9.2 Archive

Historical data can be archived in the following storage media.

- CD/ DVD
- USB disk
- Windows folder (including common folder)
- Data media

The following archive operations are available:

- Automatic archive (automatically archived in regular intervals)
- Manual archive

Archived data can be restored.

3.10 Data aggregation

The Data aggregation function aggregates the data after collection to create reports (daily or monthly), trends or for statistical analysis. It generates data such as calculated value, minimum value, maximum value, and average value within the specified data period.

The data aggregation is performed within the historical process.

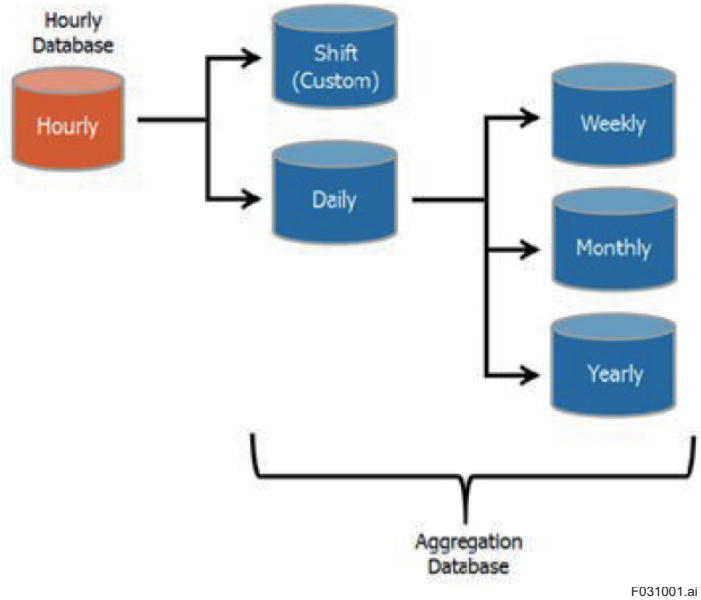
The following data intervals can be set for each storage group.

- 30 minutes closing
- Hourly closing
- shift-based
- Daily closing
- Weekly closing
- Monthly closing
- Yearly closing

The following Data aggregation can be configured for each item:

- Minimum value
- Maximum value
- Average value
- Calculated value
- Standard deviation
- Counter (counts when value changes from 0 to any other value)
- Differential accumulation

Every hour, the Data aggregation function reads all the historical data collected in the past one hour and performs the specified operation.



F031001.ai

Shift-based and daily closing aggregate values are calculated based on the hourly aggregate values.

Weekly, monthly, and yearly aggregate values are calculated based on the daily closing aggregate values.

The timestamps used at the time of saving the data aggregation is the start time of that aggregation period. These timestamps are saved in the data aggregation database.

30 minutes closing data aggregation method is similar to hourly aggregation method. The 30-minute aggregation is calculated few minutes after the 30-minute period is over. This is saved in the hourly database.

The data stored in the hourly database can be managed for lifetime, deleted, or archived through Historical function. The data from daily aggregation (includes shift aggregation also) to yearly aggregation is saved in a different database other than the historical and is not archived.

The data aggregation database needs to be backed up by the user.

Trigger at the time of data completion

The completion of all data aggregation operations for each data period can be notified to items. This function can be used to trigger a class and send out a report when calculation is over and data aggregation value becomes usable.

Overwriting the data aggregation data

The data aggregation function supports override (overwrite) operation by user. The overridden value contains a mark to indicate the same and is taken care such that it is not overwritten again automatically at the time of hourly aggregation operation.

3.11 Reports

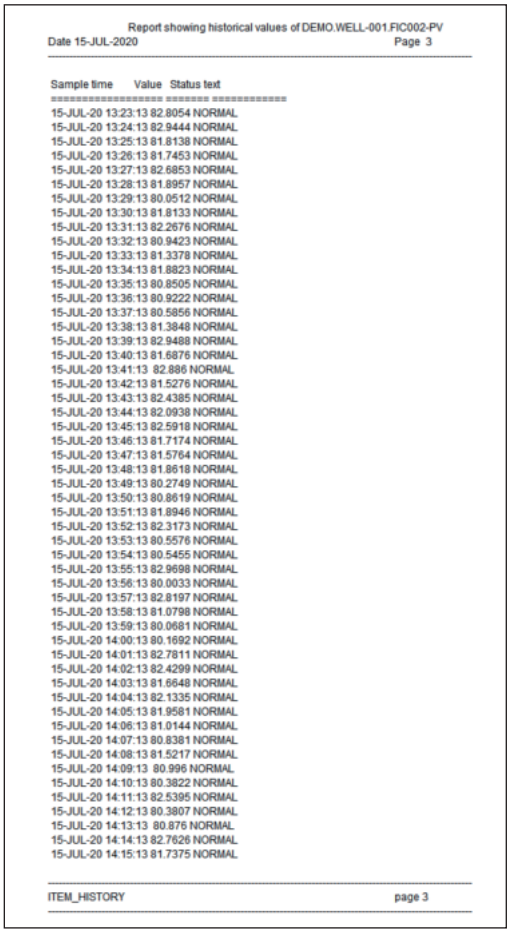
The collected data and configuration information output in a table format is called Reports and the collected data can be displayed in a time series. Reports can be displayed on screens or can be sent out to files and printers. The reports sent to files are in ASCII format and hence the reports can be read using a text editor, edited, and printed. It can also be scheduled to be deleted after the save period is completed.

The following types of reports can be generated:

- Fixed time reports (Ex: Production date report, shift report, monthly report etc.)
- Event based report (Item change Ex: report generation before and after the shutdown event)
- On-demand report
  Pressing a button to generate a prescribed report (Ex: Current Alarm Report)

Defining a new report online and creating a report (Ex: Creating a list of all analog items containing upper limit, lower limit)

Ex) Report in which data value and status are displayed in a time series



Report showing historical values of DEMO.WELL-001.FIC002-PV
Date 15-JUL-2020 Page 3

Sample time	Value	Status text
15-JUL-20 13:23:13	82.8054	NORMAL
15-JUL-20 13:24:13	82.9444	NORMAL
15-JUL-20 13:25:13	81.8138	NORMAL
15-JUL-20 13:26:13	81.7453	NORMAL
15-JUL-20 13:27:13	82.6853	NORMAL
15-JUL-20 13:28:13	81.8957	NORMAL
15-JUL-20 13:29:13	80.0512	NORMAL
15-JUL-20 13:30:13	81.8133	NORMAL
15-JUL-20 13:31:13	82.2676	NORMAL
15-JUL-20 13:32:13	80.9423	NORMAL
15-JUL-20 13:33:13	81.3378	NORMAL
15-JUL-20 13:34:13	81.8823	NORMAL
15-JUL-20 13:35:13	80.8505	NORMAL
15-JUL-20 13:36:13	80.9222	NORMAL
15-JUL-20 13:37:13	80.5856	NORMAL
15-JUL-20 13:38:13	81.3848	NORMAL
15-JUL-20 13:39:13	82.9488	NORMAL
15-JUL-20 13:40:13	81.6876	NORMAL
15-JUL-20 13:41:13	82.886	NORMAL
15-JUL-20 13:42:13	81.5276	NORMAL
15-JUL-20 13:43:13	82.4385	NORMAL
15-JUL-20 13:44:13	82.0938	NORMAL
15-JUL-20 13:45:13	82.5918	NORMAL
15-JUL-20 13:46:13	81.7174	NORMAL
15-JUL-20 13:47:13	81.5764	NORMAL
15-JUL-20 13:48:13	81.8618	NORMAL
15-JUL-20 13:49:13	80.2749	NORMAL
15-JUL-20 13:50:13	80.8619	NORMAL
15-JUL-20 13:51:13	81.8946	NORMAL
15-JUL-20 13:52:13	82.3173	NORMAL
15-JUL-20 13:53:13	80.5576	NORMAL
15-JUL-20 13:54:13	80.5455	NORMAL
15-JUL-20 13:55:13	82.9698	NORMAL
15-JUL-20 13:56:13	80.0033	NORMAL
15-JUL-20 13:57:13	82.8197	NORMAL
15-JUL-20 13:58:13	81.0798	NORMAL
15-JUL-20 13:59:13	80.0681	NORMAL
15-JUL-20 14:00:13	80.1692	NORMAL
15-JUL-20 14:01:13	82.7811	NORMAL
15-JUL-20 14:02:13	82.4299	NORMAL
15-JUL-20 14:03:13	81.6648	NORMAL
15-JUL-20 14:04:13	82.1335	NORMAL
15-JUL-20 14:05:13	81.9581	NORMAL
15-JUL-20 14:06:13	81.0144	NORMAL
15-JUL-20 14:07:13	80.8381	NORMAL
15-JUL-20 14:08:13	81.5217	NORMAL
15-JUL-20 14:09:13	80.996	NORMAL
15-JUL-20 14:10:13	80.3822	NORMAL
15-JUL-20 14:11:13	82.5395	NORMAL
15-JUL-20 14:12:13	80.3807	NORMAL
15-JUL-20 14:13:13	80.876	NORMAL
15-JUL-20 14:14:13	82.7626	NORMAL
15-JUL-20 14:15:13	81.7375	NORMAL

ITEM_HISTORY page 3

F031101.ai

Reports are created (output) by the following procedure:

(1) Report definition

Reports are defined in advance. The following items are specified.

- Name
- Output destination
- Output data
- Data set containing that data
- Layout

The data that is sent out to reports is defined using a [Query language] called RQL.

The data that is output to report is saved as data set. Data is extracted from data set to create a report. The following are the examples of data set.

- Item definition
- Item history
- Current alarm and alarm history

(2) Generating reports

Reports can be generated in the following scenarios:

- Generate reports on demand

  A method where reports can be generated instantly by pointing the report generation on the display.

- Generating reports based on schedule

  Reports can be generated at specified time based on schedule. Reports can be generated periodically such as for every 24 hours.

- Generating reports based on events

  Reports can be generated when a particular event occurs such as when the specified item crosses a particular value.

Reports can be sent out in the following ways:

- Display on screen
- Send to printer
- Send to file

3.12 Data analysis/Reporting tool

Data analysis/Reporting tool is a client tool that produces CI Server data on Microsoft Excel, analyses the process data and creates forms for reports.

Excel is connected to CI Server using Excel Add-in function. With the data search function enabled, this tool extracts the required process data and data aggregation data and can create simple daily reports and monthly reports.

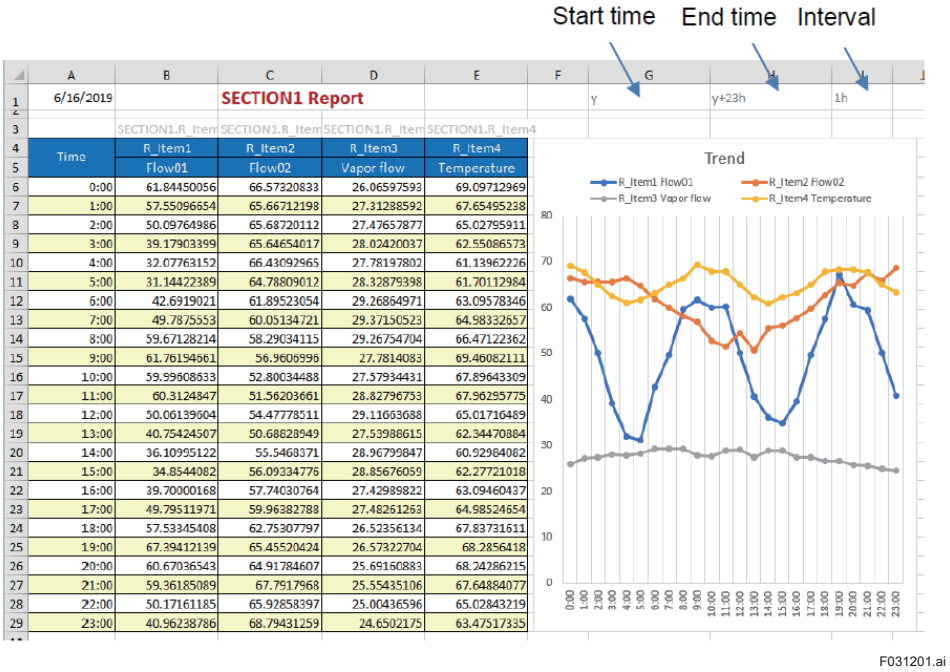


Figure Example of daily report

This tool contains the following functions:

- Function to manage connection with CI Server

  It connects to CI Server. Logon is required at the time of connection. Based on the user rights, there are limitations on the range of data that can be accessed. Data can be extracted securely.

- Item search function
  Item search function is used to select the required items from the connected CI Server.

- Data extraction function
  The following item data can be extracted from the CI Server database and can be copied to the specified cells on the Excel worksheet.

  - Current value
    Latest data can be extracted.

  - History value
    History value can be extracted by specifying extraction period, extraction interval, and timestamp.

  - Data aggregation value
    Data aggregation data such as hourly closing data and daily closing data can be extracted by specifying the timestamp.

  - Item attribute value
    Attribute values of an item such as supplementary information, status, quality code, update time can be extracted by specifying the item name.

3.13 Operator interface (operation monitoring screen)

Operator interface of CI Server has the following features:

Operability

You can create operation monitoring screen on your own based on ergonomics and guidelines defined by the organization and projects. Further, screen operation functions such as zoom, scroll etc. are provided as basic features.

HTML5 support

The operation monitoring screen supports HTML5 and can be displayed on Web browser as well as mobile devices.

Free style structure

By combining the standard parts such as process data, alarms, historical trends, real time trends, faceplates, reports, event history and the project specific parts, structure of operation monitoring screen can be determined freely. Multiple layers and visual groups can be configured for each screen and can be displayed or hidden based on user rights, process conditions, zoom levels etc.

HMI with high visual effects

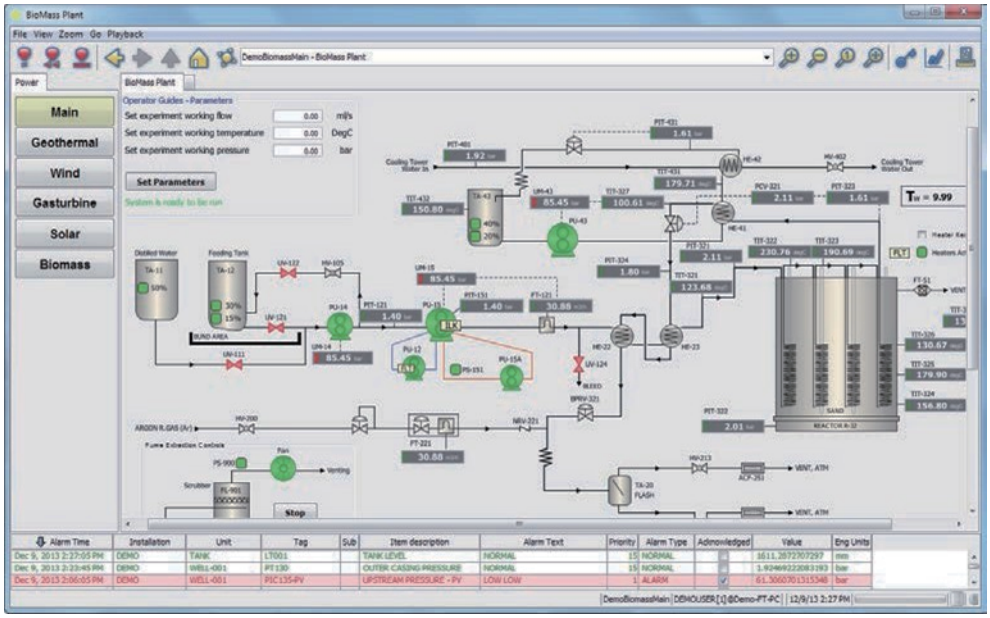
You can easily create an HMI with high visual effects using the in-built ISA-101 compliant symbol library. You can also create Advanced Operating Graphics (AOG) HMI easily.

Multiple data sources

Information from multiple data sources such as video streaming (video camera etc.), Web site, PDF document etc. can be displayed.

Multi-node input

Data collected from multiple CI Cores can be integrated and displayed on a single Operation Monitoring screen. For example, data requested from a particular management level can be collected from each CI Core and displayed.



F031301.ai

F031302.ai

Operator interface can be created using the Edit module.

Major definition items:

- Placement of screen components (figures, text, data display, bar graph)
- Placement of symbols (image of installed pump and tank, ISA symbols etc.)
- Placement of HMI components (Alarm Overview, Trends, Reports etc.)
- Configuration of attributes (Display/setting data, screen development, color change, animations etc.) of placed components

There are multiple ways of creating an effective screen on the Edit Module.

- Images of frequently used equipment and devices are registered as reusable symbols. Symbols can be created and registered.
- There are no limitations on the number of screen components placed on the screen and the size can also be freely selected.
- Screen for template can be created.
- Screen and parts of the screen (symbols, screen components etc.) can be easily copied.

3.13.1 HTML display

There are two types of Operator Interfaces in CI Server. Operation Monitoring screen can be displayed on the Web browser.

- Normal display that is displayed on the CI Server Operator Interface application
  Display that is displayed on the CI View.
- HTML display that is displayed on the Web browser
  Display that uses Web browser.

For details about the types of HMI that include operator interface, refer “2.1 CI Core, CI Portal and CI View”.

Note: There are functional limitations on HTML display when compared to normal display.

3.13.2 Components

The following components are available for developing the screen.

Figures and text display
Rectangle, ellipse, arc, polygon, curves, lines, links, border text, numbers, icons (image display)

Display/Input
Spinner, slider, button, toggle button, checkbox, radio button, combo box, list, text area, Date/Time text field, password field, numerical field

Data display
Scale, rounded scale, radial (radar chart), data bar

Logic
Calculation, function, JavaScript function

Alarm
Alarm Overview, Shelf Alarm Overview, list of blocked items and sub items, alarm sound

Trends
Trend, DTS trend micro trend

Reports
Reports

Viewer series
Web browser map viewer

Data set
Data set form, data set table

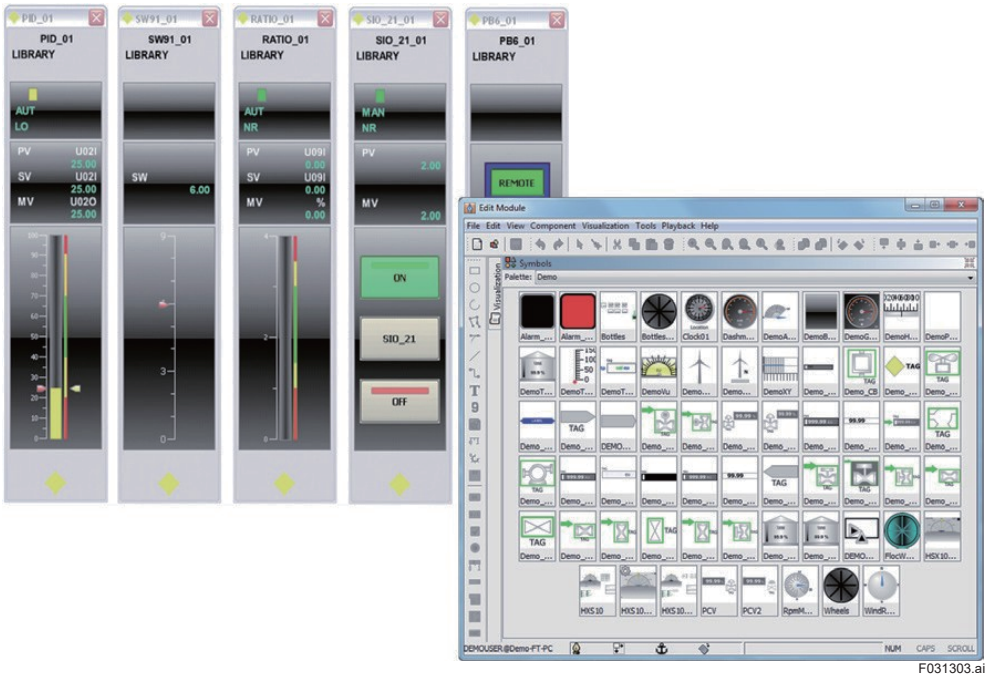
Navigation
Navigation tree

Playback
Playback display

3.13.3 Symbol figures

Frequently used equipment and device figures can be registered in the Edit Module as symbols and callable & reusable figures. More than 3000 such symbols for use in factories and industries have been created.

Faceplate for CENTUM VP is also created.



F031303.ai

Some of the symbols created are mentioned below:

Process symbol:

Airflow/Blower/Chemical industry/Conveyor/Heating Symbol/Hydraulic/Logical/Duct/ Airconditioner/Electricity/Flexiblewires/Controller/Material handling/Pipes/Mixer/motor/Cool down process/Heating process/Thermo/Pump/Sensor/Tank/Valve/Wires & cables

Industrial symbols:

General product symbol/Factory/plant equipment/Power/Water treatment Standards & guideline symbols

ISA symbol/ISA symbol 3D/ASHRAE control & equipment, ASHRAE duct/ASHRAE piping/ HVAC (Heating, ventilation exhaust, cooling)

General symbols:

Building Structures / Arrows / Aviation / Buildings / Basic Shapes / Computer Hardware / Containers / Nature / Numbers / Maps & Flags / International Symbols / Operator Interface / Safety / Scales / Telecom Hardware / Vehicles / Other Symbols

Symbols for AOG:

3.13.4 Alarm Overview

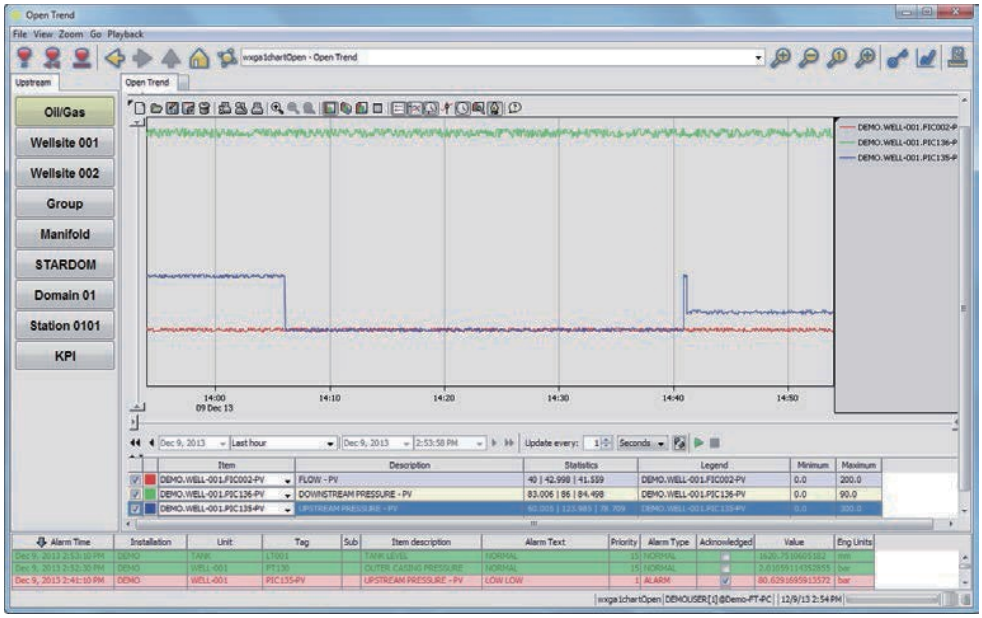
Alarm overview components can be used to create a screen that includes Alarm Overview. For details about Alarm Overview screen, refer “Alarm Overview Screen”.

3.13.5 Trends

Trend components can be used to create screens that include trend graphs. Historical data and real time data can be continuously displayed.

Pen allotment, property setting, changing display items etc. for trends can be done in advance in the Edit Module during engineering or it can also be done on the Operator Interface screen during operation monitoring.

Also, trend definition can be created, saved, saved trends can be called and displayed from the trend screen on the Operator Interface.



F031304.ai

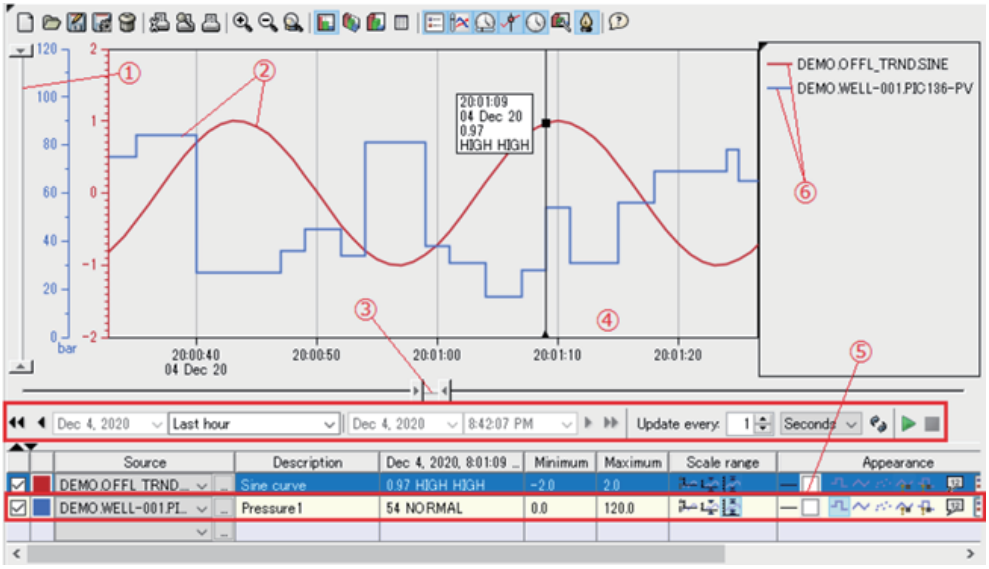
Major features:

- Max. no. of pens: 50 pens per trend
- Minimum time unit in which trends can be displayed: 1ms
- Minimum update cycle: 1 second
- Maximum display time width: No limitations
- No. of trends that can be saved: Depends upon the disk space
- Save/call trends, print, protect
- Export trend data and images (bit map, CSV files)
- Usable user settings
- High speed historical trends
- 2D/3D/table type drawing
- Line graph/Step graph/Scatter plot/Area graph
- X-Y plot

- Display/Hide Legends/Scale
- Swap display of time axis and value axis
- Scale font
- Display trends on time axis of absolute time/relative time and shift time
- Display of alarm status on hairline
- Link display of trends and Alarm Overview
- Pen allotment through drag & drop
- Range width & time width zoom function (XY axis can be zoomed simultaneously by selecting rectangle)
- Display or hide value slider, time slider, time control, 3D control, hairline and pen panel
- Scroll by dragging the mouse. Both horizontal drag (time interval) and vertical drag (value interval) are possible.
- Microtrend (small-sized simplified trends that can be used on ISA-101 compliant screen)
- DTS trend (Displays 3D data (Temperature, distance, time at each point along the optical fiber) obtained from Yokogawa DTSX optical fiber temperature sensor devices)

Trend screen configuration

Trend displays multiple item values on graph. Display consists of values, time slider, legend, and time controller.

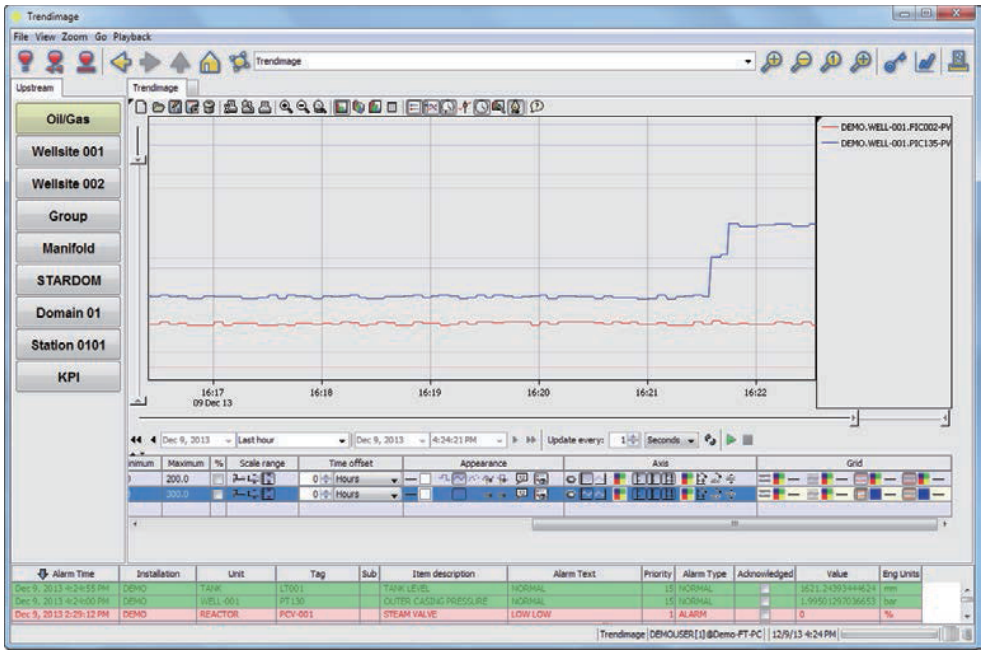


F031305.ai

Figure items description
(1): Value slider
Slider to change the display width of the vertical axis.
(2): Plot
(3): Time slider
Slider to change the display width of the horizontal axis.
(4): Time control
Area to configure displayed time width and display update frequency.
(5): Pen settings
Area to configure the pens to be displayed and display format of each pen.
(6): Trend legend

History values and current value are continuously displayed on the trend. The following item attributes can also be displayed.

- High high limit
- High limit
- Low limit
- Low low limit
- Deadband

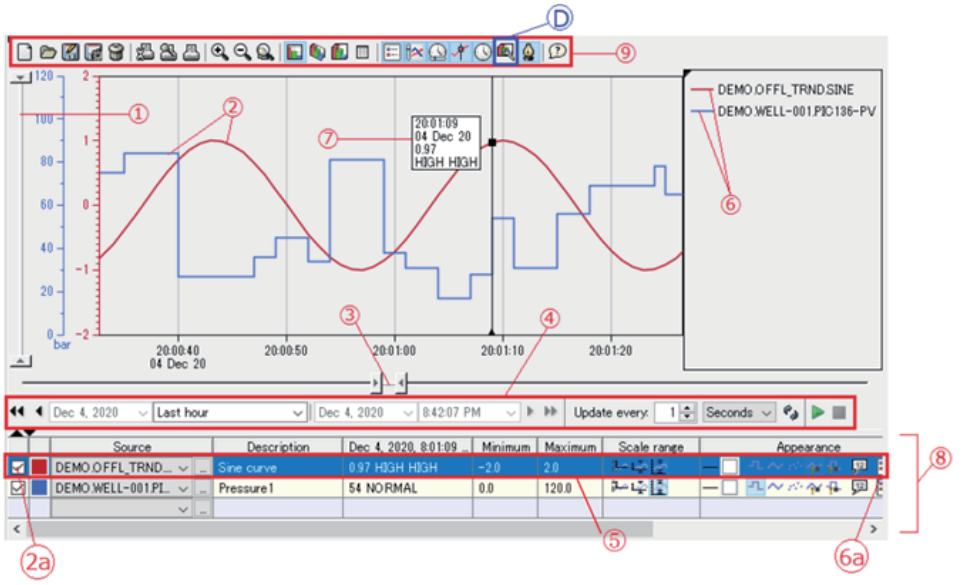


F031306.ai

Display/Hide screen components

Components that constitute the screen can be arbitrarily displayed or hidden. This can be configured during engineering or can be switched during operation monitoring.

The items (1) to (9) in the figure below can be set to be hidden.



F031307.ai

Figure items description
(1): Value slider
(2): Plot. Not displayed if (2a) is not checked.
(3): Time slider
(4): Time control
(5): Pen settings
(6): Trend legend for each pen. Displayed when [Open eye] symbol is selected in (6a).
(7): Hair line
(8): Pen panel
(9): Tool bar
(2a): Plot display/hide checkbox
(6a): Display/Hide check box of trend legend

X-Y plot

From the various data collected in the time series, one type of data is plotted in X axis and the other type of data is plotted in Y axis and displayed.

For example, from the wind power data and power generated data of a windmill collected to the time series, wind power can be plotted on X axis and the power generated can be plotted on Y axis.

Alarm and trend link display

Alarm status and trend data display can be synchronized. When you click an alarm in the Alarm Overview, you can display hairline at the time position of data corresponding to that alarm on the trend. When you click the alarm event, hairline moves to the time when alarm occurred. On the other hand, when you click on the trend, hairline is displayed at the correct position of alarm and the corresponding alarm event occurs.

F031308.ai

Offline status display

The offline status part of trend value can be depicted as a thick line.

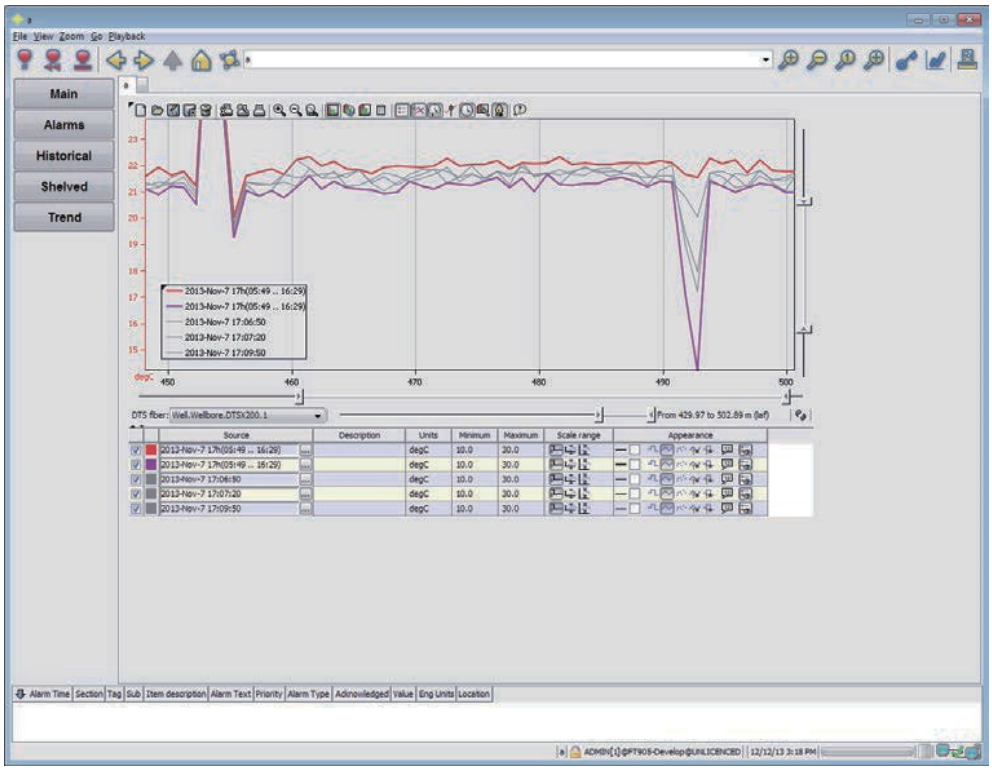
Trend data/Image export

Data can be directly exported from trend screen to CSV file. Trend images can also be exported to JPG file.

3.13.6 DTS trends

Connection to Yokogawa optical fiber temperature sensor is supported. 3D data (temperature, distance, time of each point along the optical fiber) can be read from DTSX and displayed on the trend.

Supported DTS: DTSX200, DTSX3000



F031309.ai

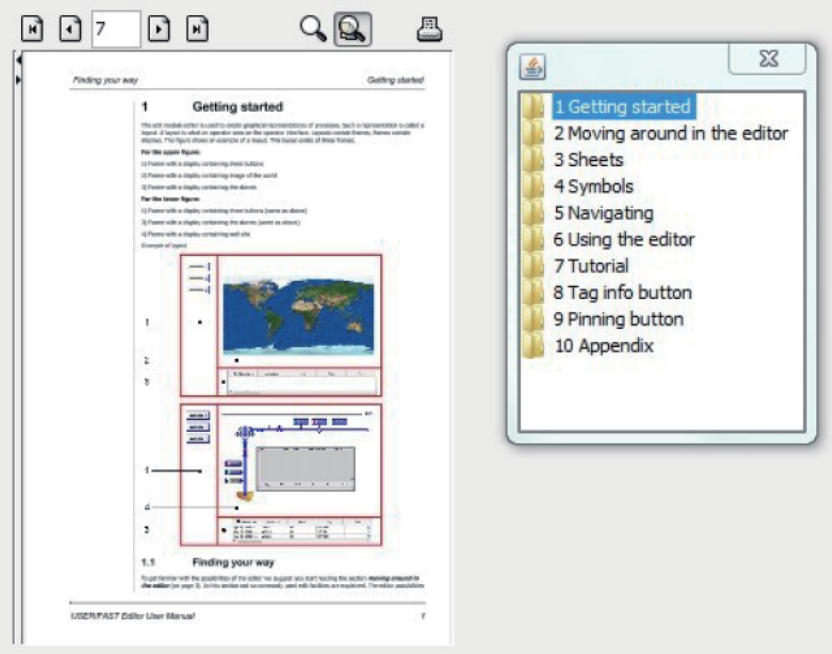
3.13.7 Web browser

A web browser component is available to display web page on Operator Interface.

You can view a media (video) file that includes an HTML file on the Web browser component.

3.13.8 Pdf display

Operator Interface consists of a pdf component that displays the pdf file.



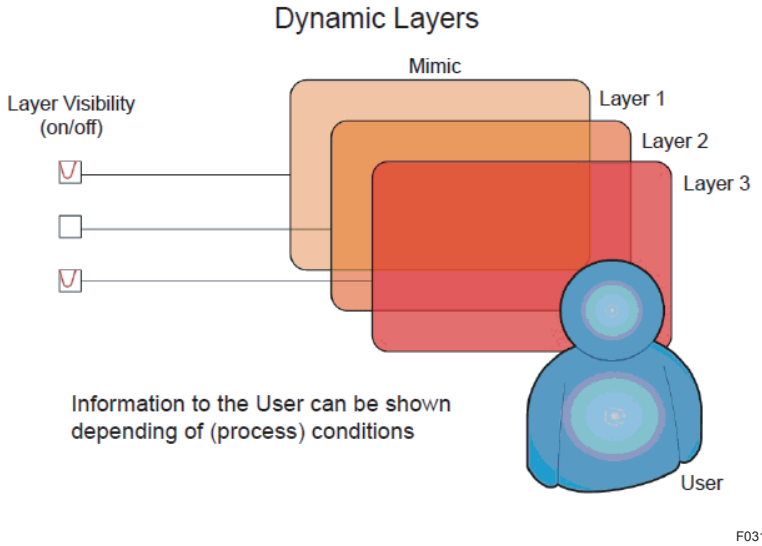
F031310.ai

3.13.9 Navigation tree

Operator interface consists of a navigation tree component that displays the list of display names in a tree format. You can call the display by clicking the display name on the tree.

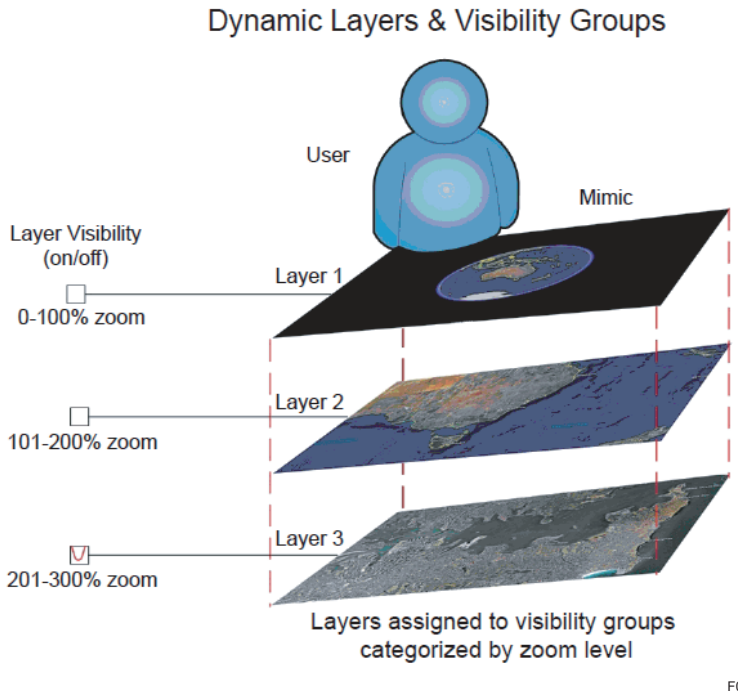
3.13.10 Dynamic layers

The Operation Monitoring screen can have multiple layers and can be overlaid on top of each other.



Operation information and maintenance information can be arranged in layers for maintenance purpose. For example, process flow diagram can be arranged on layer 1, equipment diagram details on layer 2, and power series on layer 3. Also, display and access to specific layers can be permitted based on different user rights.

The layers displayed can be swapped based on the zoom level of display. Zoom based swapping of display contents can be done like Google Earth.



3.13.11 Multi-language support

Operator interface supports display in multiple languages. It can be displayed in the language set as locale for the user.

For example, for Japanese users, locale is set as JP and for English users, locale is set as EN. Operator Interface is displayed in the language set for the user.

At the time of engineering, when creating multi-language supported display in the Edit Module, text is removed from the display and the multi-language table is saved as a language file. Extended character languages such as Japanese, Chinese, and Russian are also supported.

3.14 External application link list

Interface	Provision method	Notes
OPC Classic client 31	Standard	OPC DA v2.04 OPC A&E v1.02
OPC Classic Server（*1）	Option	OPC DA v2.04 OPC A&E v1.02
OPC Classic Tunneller（*1）	Option	OPC DA Tunnelle (Client/Server） v2.04 OPC A&E Tunneller (Server） v1.02 When connecting OPC Classic Server/Client (other company products) to CI Server using the secure communication that is used in the communication between CI Servers, this function is used in the PC run by the other company products.
OPC UA Client（*2）	Standard	OPC UA DA v1.04 OPC UA A&C v1.04 Redundancy support for communication with OPC UA Server
OPC UA Server（*2）	Option	OPC UA DA v1.04 OPC UA A&C v1.04 OPC UA HA v1.04
OPC UA PubSub（*2）	Option	OPC UA v1.04
ODBC Server（*1）	Option	ODBC API compatibility level corresponding to process and configuration data supports level 1 and SQL compatibility level supports 32-bit/64-bit supports
MQTT（*1）	Standard	MQTT 3.1.1 Lower level and upper-level support (IIOT device) and MQTT protocol communication
RDB（Relational Database） connection （*1）	Standard	Supported RDB: MS SQL Server 2016 SP2 or later. Data is transferred through RDB and application that uses RDB. CI Core is connected to RDB and data is synchronized between CI Core and RDB. When CI Core data is changed, data is copied to RDB. When RDB data is changed, data is reflected on the CI Server.

*1: only Windows OS is supported
*2: Both Windows OS and Linux OS are supported

3.15 OPC Classic

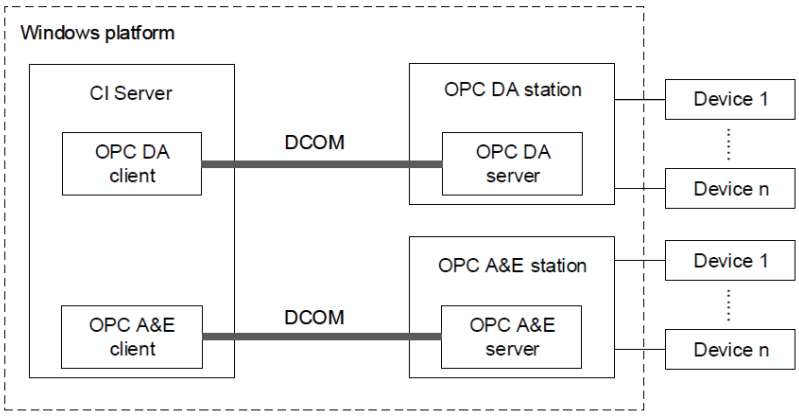
OPC is the standard communication protocol for process control systems. When OPC Interface is used, you can access data of all OPC supported applications that run on Windows OS.

CI Server has the following specifications:

- OPC Classic Client: OPC Data Access (OPC DA), OPC Alarms & Events (OPC A&E)
- OPC Classic Server: OPC Data Access (OPC DA), OPC Alarms & Events (OPC A&E)

Note: Since the basic COM/DCOM technology is implemented by default in the Windows platform, CI Server OPC Classic Server/Client is supported only on the Windows platform.

Connection example when CI Server is the OPC Client is shown below:



F031501.ai

OPC Classic Server

OPC Server collects data from field and sends the data to OPC Client through OPC Interface. The different communication protocols that are used in the field devices are replaced with the standard communication protocol. This enables devices and system from different manufacturers to interact between each other. OPC Server can also update the field device value based on the request from OPC Client.

OPC Classic Client

The OPC Client that is present within the CI Server updates the CI Server internal database based on the data obtained from OPC Server. The values of field devices can also be updated through OPC Server.

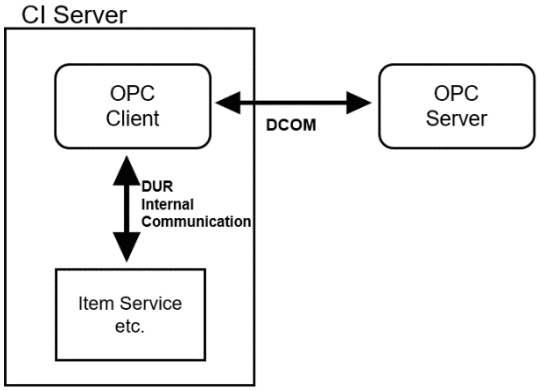
OPC Classic Station

OPC Classic station functions as the controller of process control system. CI Server supports the following types of OPC Classic station.

- OPC Data Access (DA) station
  With these stations, CI Server can replace tag data information such as device values, status, quality code etc. through OPC DA server.
- OPC Alarm & Event (A&E) station
  With these stations, CI Server can receive alarm and event information through OPC A&E server. The alarms and events from OPC A&E station are prioritized through CI Server alarm detection function.

3.15.1 OPC Classic Client

CI Server OPC Client acts as an interface for the OPC Server (third party products) to access the data.



F031502.ai

Item service is a function that manages item values and status values. Based on the requests, it sends/receives item values and status values with other functions and modifies the item values and status values.

OPC DA Client

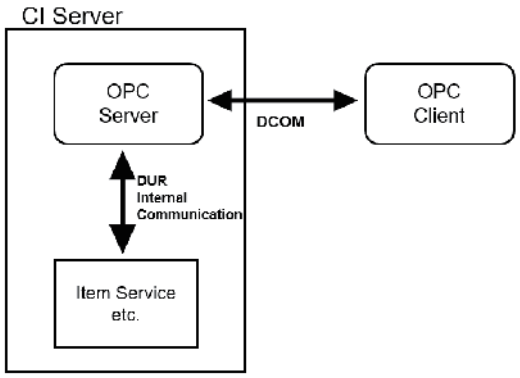
CI Server can access OPC DA Servers (third part servers) and can read/write the values/quality codes provided by such servers. Values/quality data is reflected on the CI Server items.

OPC A&E Client

CI Server can access OPC A&E servers (third party servers) and can receive the condition events sent by such servers. The information in these condition events is reflected in the CI Server items.

3.15.2 OPC Classic Server

CI Server OPC server acts as a gateway for the CI Server name space and item data for the OPC Client (third party products).



F031503.ai

OPC DA Server

- OPC DA Client (third party products) can access (read/write) CI Server item data (value and quality information) through either synchronous or asynchronous methods. DA Client can obtain dynamic item data in event base.
- OPC DA Client (third party products) can refer CI Server system name space to refer the item names defined in the CI Server system.

OPC A&E Server

- OPC A&E Client (third party products) can obtain OPC condition events of CI Server items. If required, it can also confirm the condition events. Further, OPC A&E Client refers to the usable event source of CI Server.

3.15.3 Conversion of quality code

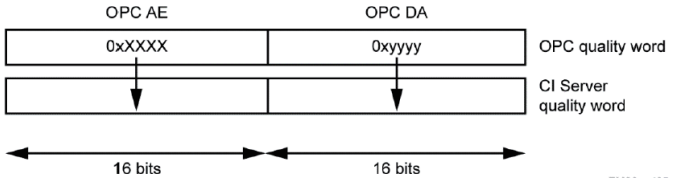
CI Server uses 32-bit word for representing item quality code and OPC quality code is of 16-bit data type. Hence, it is necessary to define the notations of CI Server quality code and OPC quality code.

In this section, conversion, and reverse conversion of OPC quality code word and CI Server quality code word is explained.

Conversion from OPC quality to CI Server quality

OPC quality word is converted into CI Server quality word by the following methods:

- If the OPC quality word is provided from the OPC A&E Client, OPC quality word information gets directly copied to the upper 16 bits of the 32-bit CI Server quality code word.
- If the OPC quality word is provided from the OPC DA Client, OPC quality word information gets directly copied to the lower 16 bits of the 32-bit CI Server quality code word.

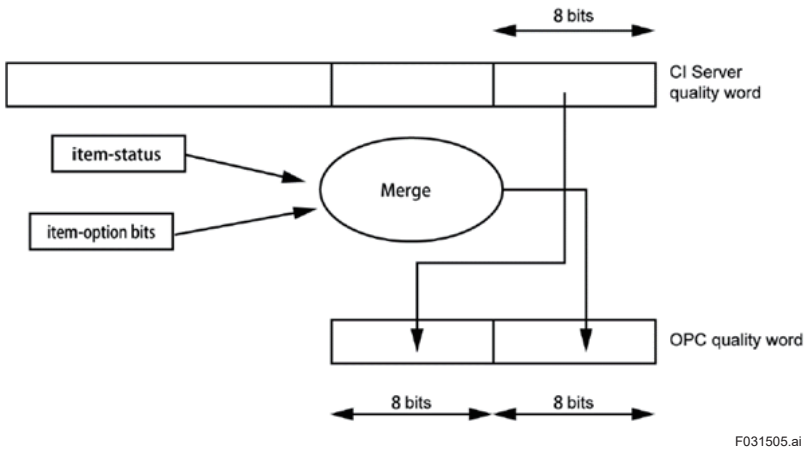


Conversion from CI Server quality to OPC quality

When CI Server item value/quality code attribute is written to OPC DA tag, the 32-bit CI Server quality code is converted to 16-bit OPC quality word.

- Based on the OPC specifications, the top 8 bits of the OPC quality word can be freely used by the application. Therefore, the bottom 8 bit of the CI Server quality word is saved in the top 8 bits of the OPC quality word.
- The bottom 8 bits of the OPC quality word contains the result of merging CI Server item status and bit attributes of item options.

Merged item status and item option attribute	Bottom 8 bits of OPC quality word
ITM_ST_OFFLINE or ITM_ST_UPD_OFF	OPC_QUALITY_LAST_KNOWN
ITM_ST_BLOCKED or ITM_ST_UPD_BLK	OPC_QUALITY_LOCAL_OVERRIDE
ITM_ST_NOT_INIT	OPC_QUALITY_NOT_CONNECTED
<Others>	OPC_QUALITY_GOOD



3.15.4 Data type mapping

Several data types are defined in the OPC DA. OPC data type must be mapped to the CI Server data type. User can use strict mapping as well as lenient mapping. When using the lenient mapping, data types defined for CI Server items is mapped as much as possible. In the strict mapping, only the OPC data type that corresponds to the CI Server item data is mapped. If the type is not supported, it is displayed as [Not supported] in the HMI.

The following table shows the mapping between OPC data type and CI Server data type.

OPC DA data type	CI Server data type
VT_UI1	REP_LONG
VT_UI2	REP_LONG
VT_UI4	REP_DOUBLE
VT_UINT	REP_DOUBLE
VT_INT	REP_LONG
VT_I1	REP_LONG
VT_I2	REP_LONG
VT_I4	REP_LONG
VT_R4	REP_DOUBLE
VT_R8	REP_DOUBLE
VT_BSTR	REP_STRING
VT_BOOL	REP_BOOLEAN

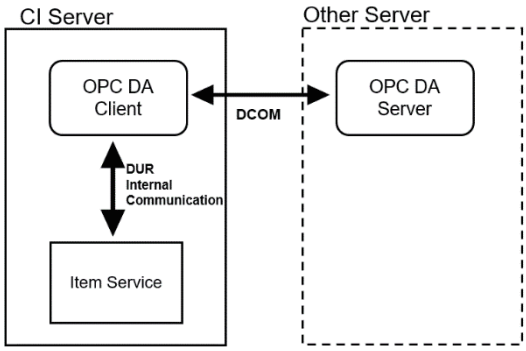
3.16 OPC Classic Tunneller

OPC Classic Tunneller replaces the DCOM communication on the network to the CI Server internal communication (DUR communication) and intends to perform the following actions:

- Avoid DCOM security issues
- Improve communication performance

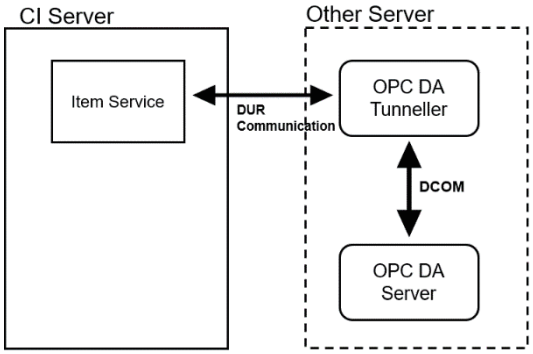
3.16.1 OPC DA Client Tunneller

The general configuration when CI Server becomes OPC DA Client is as shown below:



F031601.ai

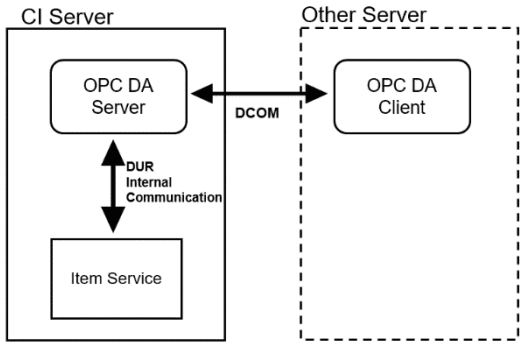
Configuration using OPC DA Tunneller is as shown below. OPC DA Tunneller is installed on other servers.



F031602.ai

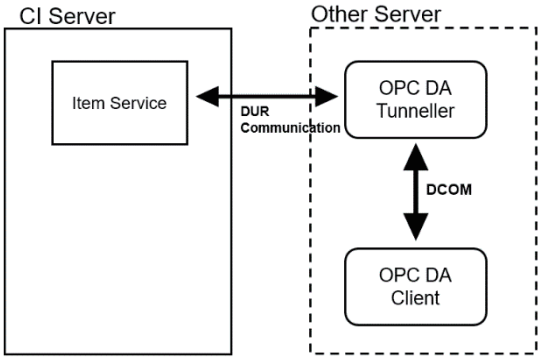
3.16.2 OPC DA Server Tunneller

The general configuration when CI Server becomes OPC DA Server is as shown below:



F031603.ai

Configuration using OPC DA Tunneller is as shown below. OPC DA Tunneller is installed on other servers.



F031604.ai

3.17 OPC UA

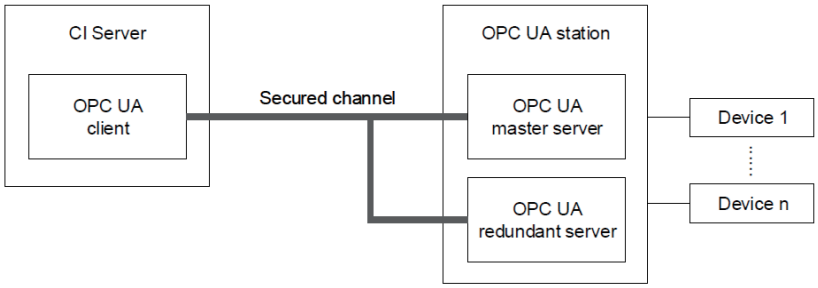
The OPC Unified Architecture (UA) is an improved version of OPC Classic, a platform-independent standard communication protocol based on a service-oriented architecture. It also supports communication security and redundancy.

CI Server supports the following specifications:

- OPC UA Client : OPC UA Data Access (OPC UA DA)
  OPC UA Alarms & Condition (OPC UA A&C)
- OPC UA Server: OPC UA Data Access (OPC UA DA)
  OPC UA Alarms & Condition (OPC UA A&C)
  OPC UA Historical Access (OPC UA HA)

Note: OPC UA Client/Server is supported in Windows and Linux.

Connection structure when CI Server is the OPC UA Client is shown below:



OPC UA Server

OPC UA server function provides integrated model that includes data item value alarm and historical data of the connected devices.

OPC UA Client

OPC UA Client function replaces tag data information such as device values, status, alarms, and quality code. OPC UA Client also establishes secured and protected communication channels and refers to OPC UA Server address space.

OPC UA Station

In addition to the features of OPC Classic station, the OPC UA station supports secure channel communication using a built-in certificate store.

Also, redundant communication can also be configured for the OPC UA station.

3.17.1 OPC UA Client

Protocol

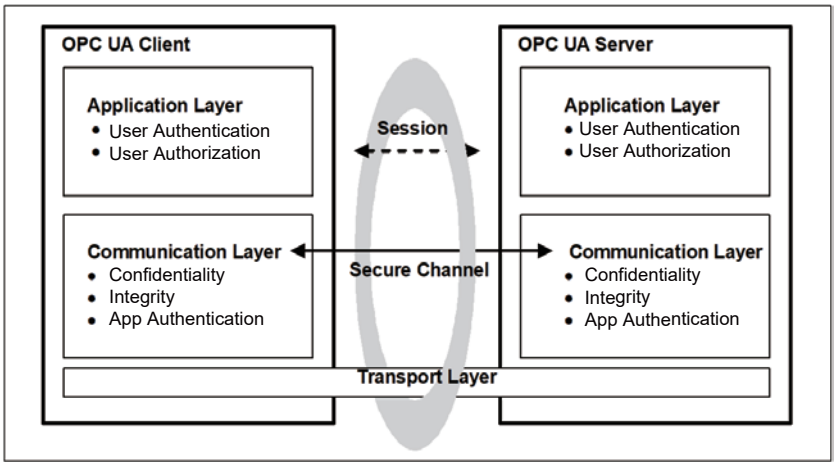
CI Server OPC UA Client only supports the OPC UA TCP protocol.

Security

OPC UA is a platform independent standard and relies on cross platform security measures. OPC UA security is based on a Public Key Infrastructure (PKI) that uses industry standard X.509 digital certificates and addresses authentication, authorization, confidentiality, and integrity.

The following figure shows an overview of the security management method in OPC UA.

The user authority and authentication are executed in the application layer.



F031702.ai

Authentication

OPC UA application instances are uniquely identified by their X.509 certificates, and a session can only be created between two OPC UA applications if each trusts the other's certificate.

For example, a client cannot initiate a session with a server that provides certificate that the client does not trust. Trust can be established in one of two ways

1. Directly:
   Each application copies the certificate of the other party (public) to any of the trust folders that is inspected by that application.
2. Via a tree of trust:
   This allows the application to trust the authority that granted the other application's certificate.

   CI Server OPC UA Client supports both the authentication methods.

Authorization

The CI Server OPC UA client supports the anonymous and the user name and password authorization methods.

Confidentiality and integrity

OPC UA defines public/private key encryption and message signing (integrity) that the client and server must implement to ensure a secure channel.

The following options are available for encryption and signing

- None - No encryption. Security is turned off. Messages can be read or tampered by third parties.
- Sign - Messages are signed to ensure data integrity, but the message itself is not encrypted. Third party can read the messages.
- SignAndEncrypt - Same as above, but the message itself are encrypted; Messages are maintained as confidential, and their integrity is guaranteed and secure.

The following table shows the security policies supported by the CI Server OPC UA client:

Table Security Policy

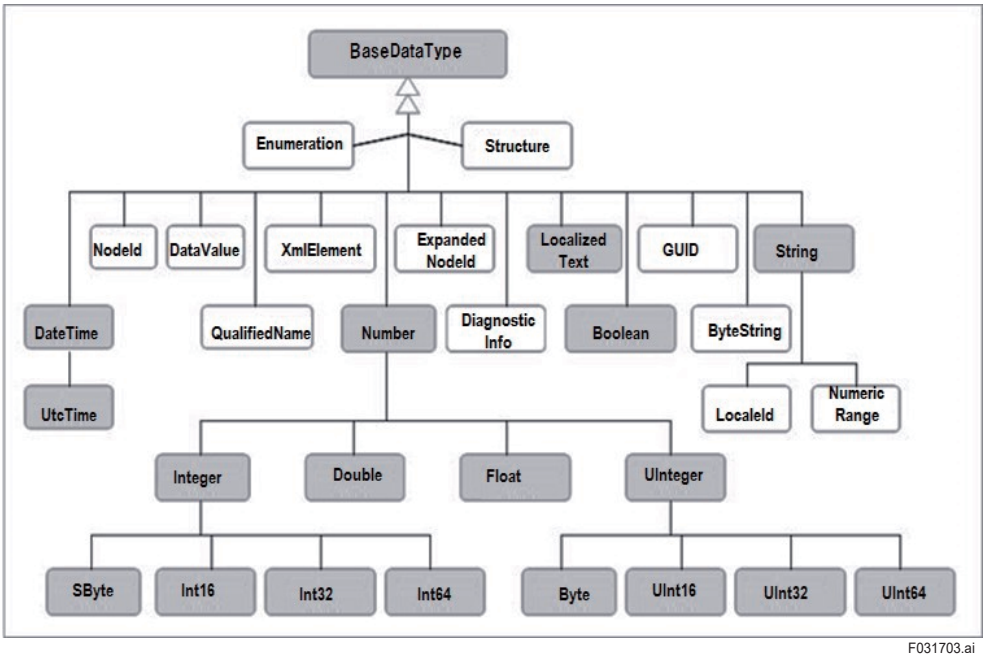
Security Policy	Encryption and signing	Recommendation	Description
None	No	No	No security is applied
Basic128Rsa15	Yes	No	No longer considered as secure
Basic256	Yes	No	No longer considered as secure
Basic256Sha256	Yes	Yes	
Aes128-Sha256-RsaOaep	Yes	Yes	
Aes256-Sha256-RsaPss	Yes	Yes	

CI server OPC UA client supports the data encryption and signing described above.

Data structures supported by CI Server and OPC UA Client

The following figure shows some of the OPC UA data types.

CI server OPC UA client supports only the data types that are filled in gray. Data types with a white background and data types that are not shown in this figure are out of scope. In the server diagnostics, you can map individual elements of the server diagnostic structure to CI server items.



F031703.ai

Mapping of variable types

Variable values are always mapped to CI server item values. Variable properties are also mapped to CI server item values. Properties of OPC UA variables can be accessed by their NodeId in the same way as other OPC UA variables.

CI Server OPC UA Client supports one-dimensional array variable and two-dimensional array variable by specifying the individual array element in the point definition of the engineering module. The array element is treated as a scalar type and set to the CI Server item.

Mapping status code

OPC UA status code indicates the quality of the data read by the client and is stored in a 32-bit unsigned integer (Uint32). This value is mapped with the following values to the quality code of CI Server items.

0: OPXC_QUALITY_CODE_GOOD

1: OPXC_QUALITY_CODE_BAD

2: OPXC_QUALITY_CODE_UNCERTAIN

OPC UA Alarms & Conditions

The CI Server OPC UA client supports the OPC UA Alarms & Conditions.

The CI Server OPC UA client provides the following configurable filters:

- Event type
- Component
- Event node

Alarms that users need can be displayed in the alarm overviews by properly configuring filters.

3.17.2 OPC UA Server

The CI Server OPC UA server cannot operate on its own. OPC UA clients interact with the OPC UA server through the OPC UA TCP protocol. These OPC UA clients can reside on the same node as the OPC UA server but can also reside on another node connected to the same network. In addition, the UA server interacts with other components of CI Server to get the requested information and to write information to the CI Server system.

SDK

CI Server OPC UA server is implemented using Unified Automation's OPC UA Server SDK. This SDK makes a distinguishes between toolkit level use and SDK level use. However, the CI Server OPC UA Server is implemented using parts of both levels. The toolkit level is mainly used for OPC UA-type system namespaces, while the SDK level is used for all communication with CI server data, such as browsing, monitoring, reading, and writing values, etc.

Mapping from CI Server item status to OPC UA status

The item status of CI Server is mapped to the OPC UA status to ease sending and receiving messages.

Item status	Value	OPC UA status code	Value
NORMAL	9	Good	0
NOT_INIT	13	BadNoCommunication	0x80310000
UPD_OFF	15	BadNoCommunication	0x80310000
OFFSCAN	22	BadNoCommunication	0x80310000
OFFLINE	14	BadNoCommunication	0x80310000
UNREACH	83	BadNoCommunication	0x80310000
BAD_VALUE	24	Bad	0x80000000

Mapping of CI Server data type and OPC UA data type

Items and properties of CI Server has internal data type. Mapping between these types and OPC UA data types are as follows:

Table Mapping from CI Server data type to OPC UA data type

CI Server data type	OPC UA data type
Boolean	OpcUaType_Boolean
Integer	OpcUaType_Int32
Real	OpcUaType_Double
String	OpcUaType_String

Table Mapping from OPC UA data type to CI Server data type

OPC UA data type	CI Server data type
OpcUaType_Boolean	Boolean
OpcUaType_Int32	Integer
OpcUaType_Double	Real
OpcUaType_String	String

Authentication and authorization

OPC UA client supports the anonymous and the user name and password authorization methods. The user name and password defined in the CI Server can be used as credentials to connect to the CI Server OPC UA server from the external OPC UA client.

The following table describes the operations that the external OPC UA client can perform depending on the user authorization.

Authorization action of CI Server	Access level of OPC UA	Available operation by external OPC UA client
None	None	The external OPC UA client cannot use this user to connect to the CI Server OPC UA server.
OPC_UA_SERVER_READ (Permissions to view data on the OPC UA server)	CurrentRead (The current value is readable)	The external OPC UA client can use this user to perform following operations: • Browse the CI Server OPC UA address space • Read attribute values for currently occurring item-based alarms, external alarms, and informational events • Read current item values • Read historical data
	HistoryRead (The history of the value is readable)	
OPC_UA_SERVER_MODIFY (Permissions to change data on the OPC UA server)	CurrentRead (The current value is readable)	The external OPC UA client can use this user to perform following operations: • Available operations by the authorization action OPC_UA_SERVER_READ • Write current item values • Execute the methods published by CI Server
	CurrentWrite (The current value is writable)	
	HistoryRead (The history of the value is readable)	

3.17.3 Redundancy of OPC UA client

Client redundancy

The redundancy of the CI server OPC UA client is not implemented.
The switching of OPC UA sessions from one client to another is not currently supported by the CI server OPC UA client.
However, client redundancy can be achieved using the CI server HAC.

Server-side redundancy

The server-side redundancy can be divided into transparent server redundancy and non-transparent server redundancy. Both can be supported by the OPC UA client of the CI server.

- Transparent server redundancy
  Server side takes charge of switching to backup server side. Client need not recognize the interruption in communication.
- Non-transparent server redundancy
  Server side consists of 2 servers, active server and backup server and the client identifies these 2 servers.
  CI Server OPC UA Client supports the so-called cold backup mode. If the connection with the first server fails, it is disconnected, and connection is established with the 2nd server.

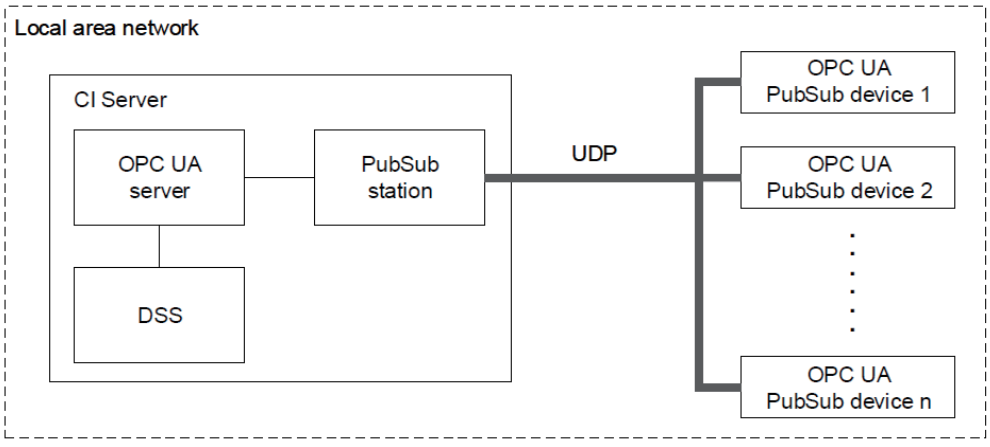
3.17.4 OPC UA Subscription

OPC UA client can register a subscription for data changes to the OPC UA server. When data is changed, OPC UA server delivers a notification to the OPC UA client. OPC UA server continues to distribute notifications until the subscription is cancelled.

The following types of monitoring items can be registered by subscription.

- Variable value data change subscription: Common type.
- Event subscription
- Aggregate value subscription: This type is not supported by the CI Server OPC UA client.

System configuration of OPC UA subscription is as follows:



F031704.ai

3.17.5 OPC UA Profile

Profiles supported in the OPC UA Server and Client are as follows:

Item Name	OPC UA Client	OPC UA Server
Profiles	Minimum UA Client Profile	Standard 2017 UA Server Profile
Facets	Core 2017 Client Facet, Base Client Behavior Facet, Discovery Client Facet, Subnet Discovery Client Facet, AddressSpace Lookup Client Facet, Entry Level Support 2015 Client Facet, Attribute Write Client Facet, Method Client Facet, DataChange Subscriber Client Facet	
Security Policies	SecurityPolicy-None, SecurityPolicy-Basic128Rsa15, SecurityPolicy-Basic256, SecurityPolicy-Basic256Sha256, SecurityPolicy-Aes128-Sha256-RsaOaep, SecurityPolicy-Aes256-Sha256-RsaPss	SecurityPolicy-None, SecurityPolicy-Basic128Rsa15, SecurityPolicy-Basic256, SecurityPolicy-Basic256Sha256, SecurityPolicy-Aes128-Sha256-RsaOaep, SecurityPolicy-Aes256-Sha256-RsaPss
User Identity Tokens	UserToken-Username_Password	UserToken-Username_Password, UserToke-X509Certificate

3.18 ODBC

CI Serve supports ODBC 32-bit/64-bit version.

CI Server uses SimbaServer as ODBC Server.

ODBC compliance level

Compliance levels are prescribed in the ODBC standards. API compliance level defines core functions. There are three levels, Core, Level 1, and Level 2 and are used in data source.

SQL compliance level defines SQL syntax. There are three levels, Minimum, Core and Extended.

The ODBC function in ACCESS Service is based on the following conformance levels:

- API compliance level : Core
- SQL compliance level : Minimum

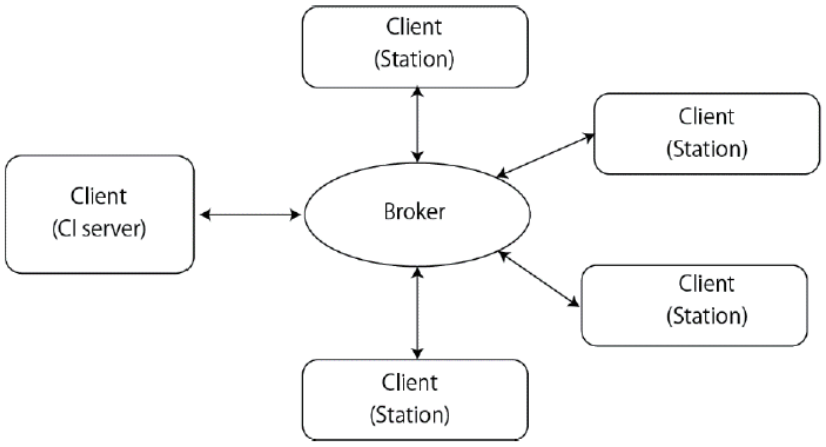
3.19 MQTT

MQTT is a lightweight publish/subscribe messaging protocol.

CI server supports version 3.1.1 of the MQTT protocol and can connect to the MQTT brokers that support this version.

(CI server uses the library of Mosquitto broker version 1.6.9.)

The structure of communication device of MQTT protocol is as follows:



In communications using the MQTT protocol, there are devices that have the roles of broker and client. Client sends and receive messages to other clients via the broker. CI servers and other devices (stations) are also clients. Brokers are responsible for sorting messages. The client who receives messages specifies the messages he wants to receive. The broker receives the message from a client and sends it to the client who requires it. All messages are delivered to the client through the broker.

Messages

Messages consists of Topic (heading that represents the data content) and Payload (data body).

Topic:

Topic is the character string used by the broker to filter the messages from a client. Topic has layered structure separated by “/”.

The following table shows the relevance between Topic and CI Server item.

MQTT topic	CI Server item name
Temperature/heater1	Temperature.heater1
Plant1/Pump/State	Ptant1.Pump.State

Payload:

In CI Server, Payload is used as data value. The following two types of Payloads are used in CI Server.

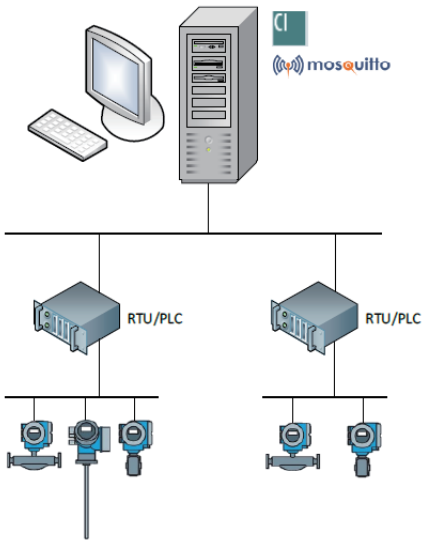
Payload format	Description
Text format	Data value is stored as character string
JSON (Java Script Object Notation)	File format of JSON. [Key] character string and value character string are enumerated in parenthesis. CI Server contains data value, data status, and timestamp. Key character string can be specified by the user. Ex: {“value”:”98.6”.”status”:”11”,”timestamp”:”2020-08-6T08:34:00+00:00”]

After receiving the message from station, CI Server writes the Payload value to the item corresponding to the Topic. If the Payload format is JSON (one of the methods of entering data), item status and item update are updated with the received data.

System structure

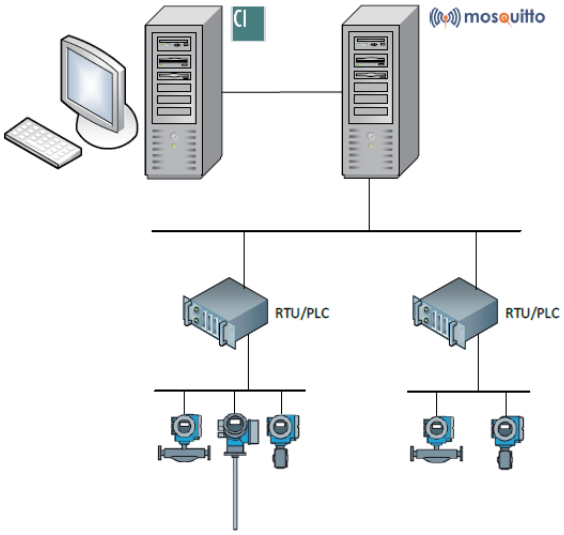
In this example, mosquitto broker is used as the MQTT broker.

(1) When CI Server and MQTT broker are in the same station



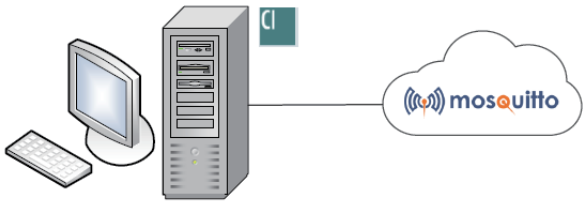
F031902.ai

(2) When CI Server and MQTT broker are in different stations



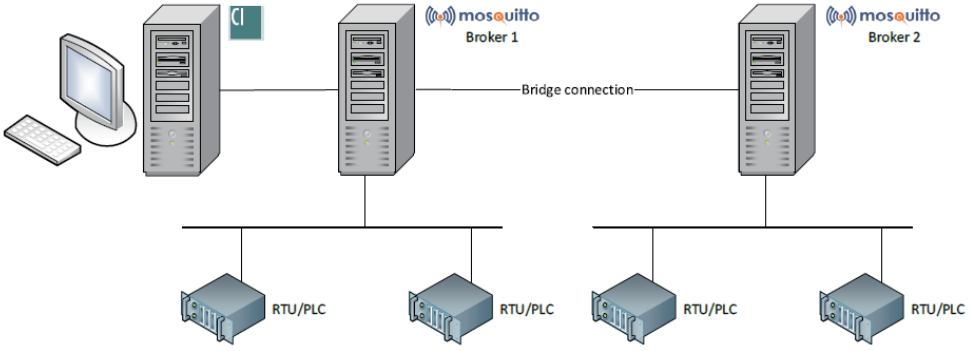
F031903.ai

(3) When MQTT broker is in cloud



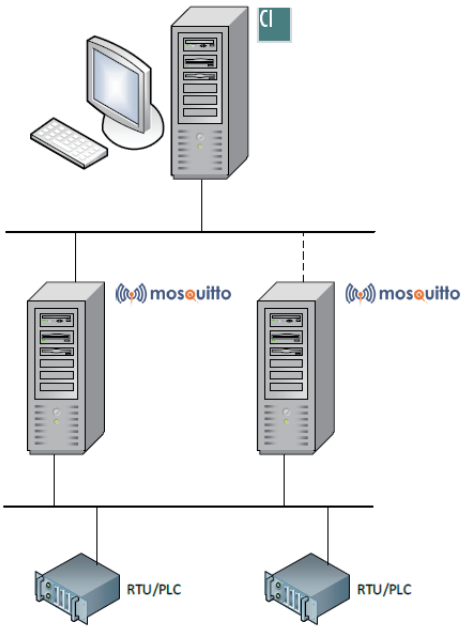
F031904.ai

(4) When MQTT broker is connected through bridge



F031905.ai

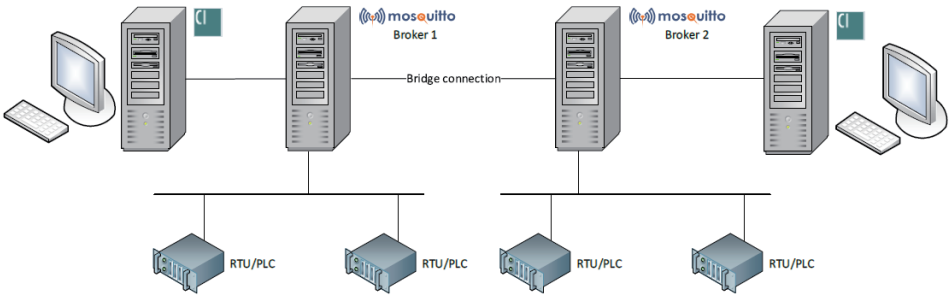
(5) When MQTT broker is in redundant configuration



F031906.ai

CI Server can configure MQTT broker in redundant configuration.

(6) When data is exchanged between CI Servers through MQTT broker



F031907.ai

3.20 RDB connection

RDBMS data copy function is available to connect with RDB (Relational Database).

Supported RDB

MS SQL Server 2016 SP2 or later

Function

The following functions are available.

- Copy current value
  The specified item data (current value) is copied to RDB in regular intervals. Frequency: From 60 seconds to 7 days
  In addition, minimum value, maximum value, average value, data number are calculated and copied to RDB.
- Copy historical data
  Historical data can be specified and copied. Data and period are specified and copied. This operation is carried out on the Engineering Module.
- Changing CI Server item data from RDB
  Item data can be modified from RDB. RDB has a table for items. When this table value is modified, it is reflected on the item of CI Server. However, when item value is changed in CI Server, it is not reflected in the table.
- Copying another database within CI Server
  When data is modified, it is copied to RDB. For example, in case of item database (ITEM_DF) copy, whenever a new item is created, it is copied to RDB.

3.21 PI data trend display

The PI data trend display function assigns the historical data of PI system as the trend pen of the CI server and displays it on the trend.

In the source selection window that appears when selecting trend pens, select the PI historical data.

SSO can be used by linking the CI server and PI system with the Active Directory.

3.22 List of external controller connections

		Communication methods		
Communication driver	**Provided method**	**TCP/IP**	**Terminal server**	**Serial**
Yokogawa Vnet/IP (*1)	Option	X		
Yokogawa STARDOM (*1)	Standard	X		
Yokogawa DAQMASTER (*1)	Standard	X		
Yokogawa SMARTDAC+ (*1)	Standard	X		
Yokogawa FA-M3 (*1)	Standard	X		
Modbus slave (*1)	Standard	X	X	X
Modbus master (*1)	Standard	X	X	X
Yokogawa Vnet/IP Software Stack (*1)	Option	X		
IEC 60870-5-101 (*1)	Option		X	X
IEC 60870-5-102 (*1)	Option		X	X
IEC 60870-5-103 (*1)	Option		X	X
IEC 60870-5-104 (*1)	Option	X		
IEC 61850	Option	X		
DNP3 master	Option	X	X	X
WITS level 0 slave (*1)	Option		X	X
WITS level 0 master (*1)	Option		X	X
HEX repeater	Option		X	
Rockwell Allen Bradley CIP	Option	X		
Rockwell Allen Bradley DF1	Option		X	X
Rockwell Allen Bradley DH+	Option	X		
Allen Bradley PLC5	Option	X		X
Siemens 3964R (*1)	Option			X
Siemens SAPI-S7 (*1)	Option	X		
Emerson BSAP	Option		X	X
Emerson Fisher ROC	Option		X	X
MELSEC(*2)	Option	X (TCP/IP, UDP)		X
OMRON FINS	Option	X (UDP only)		
Telemetry integration environment	Custom			X
HART router	Custom		X	
Beckhoff ADS	Custom	X		
Beckhoff BK8100	Custom		X	
Bachmann M1COM	Custom			X

*1: Windows version driver only
*2: Supports only Windows Client OS

3.23 Redundancy communication support

In the controller connection, communication lines can be made redundant in the communication established with common items such as TCP/IP, UDP, DUR (CI Server internal communication). In case of TCP/IP, UDP, 2 IP addresses can be configured. In case of DUR, two node numbers can be configured.

Note: Depending upon the station type, redundancy cannot be performed in some cases.

3.24 Modbus

The following communication methods are supported. CI Server supports Client (master) as well as Server (Slave).

- TCP/IP communication (Open Modbus TCP protocol)

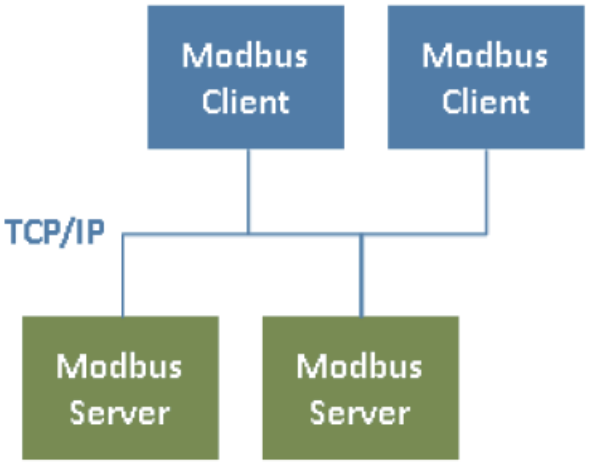


Figure: Modbus over TCP/IP network

F032401.ai

- Serial (ASCII/RTU protocol)

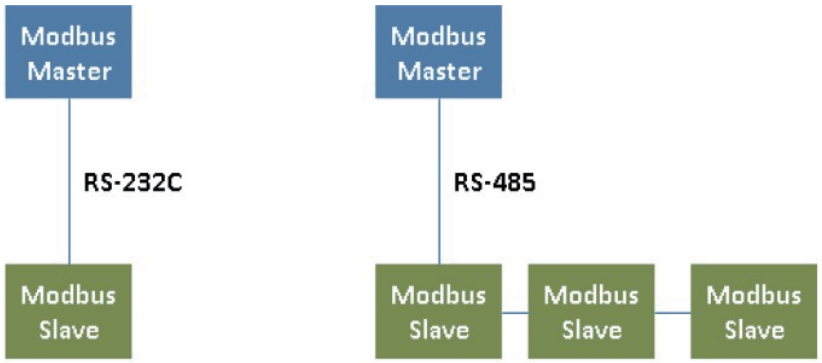


Figure: Modbus over serial line

Figure: Modbus over serial line (Multi-drop networks)

F032402.ai

- Terminal server

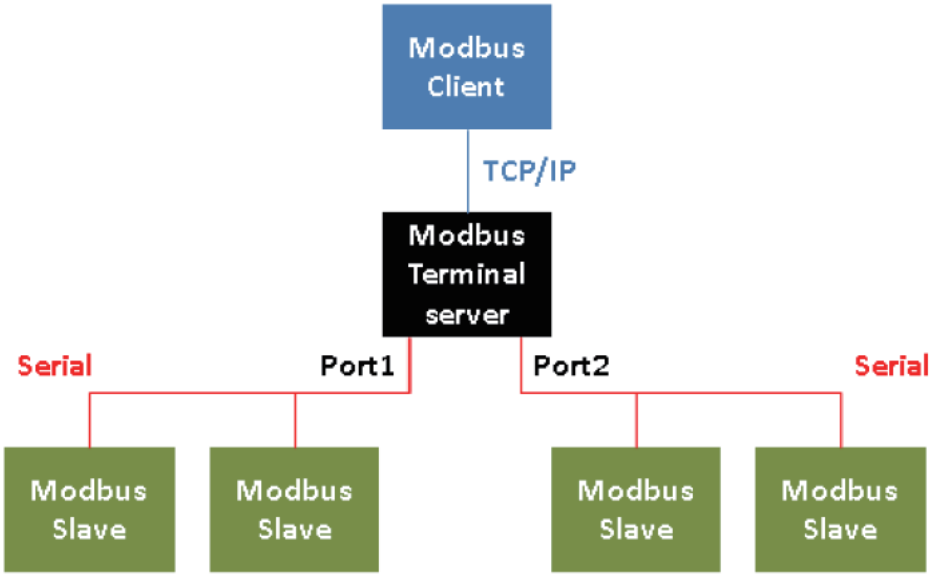


Figure: Modbus terminal server

F032403.ai

3.25 IEC61850

Supported functions

Only the following functions are supported.

- Read
  Reading data through scanning
- Write
  Data writing to event, direct writing, writing to controller model

3.26 DNP3

DNP3 with authentication

CI Server supports the following secured authentication versions.

- Secured Authentication mechanism Version 2 (SAv2)
- Secured Authentication mechanism Version 5 (SAv5)

DNP V3.0 Device Profile

Information of the device profile is as mentioned in the following table.

DNP V3.00
DEVICE PROFILE DOCUMENT

Vendor Name:	**Yokogawa**
Device Name:	**CI Server**

Highest DNP Level Supported:	Device Function:
For Requests: **Level 3** For Responses: **Level 3**	☒: **Master** ☐: Slave

Notable objects, functions, and/or qualifiers supported in addition to the Highest DNP Levels Supported (the complete list is described in the attached table):

16-bit and 32-bit and Float Analog Change Events with Time are supported.

Maximum Data Link Frame Size (octets):	Maximum Application Fragment Size (octets):
Transmitted: **292** Received: **292**	Transmitted: **2048** Received: **4096**

Maximum Data Link Re-tries:	Maximum Application Layer Re-tries:
☐: None ☐: Fixed at ____ ☒: **Configurable from 0 to 255**	☒: **None** ☐: Configurable

Requires Data Link Layer Confirmation:

☒: **Never**
☐: Always
☐: Sometimes
☐: Configurable

Requires Application Layer Confirmation:

☒: **Never**
☐: Always
☐: When reporting Event Data
☐: When sending multi-fragment responses
☐: Sometimes
☐: Configurable

Timeouts while waiting for:

Data Link Confirm:	☒: **None**	☐: Fixed at ____	☐: Variable	☐: Configurable
Complete Appl. Fragment:	☒: **None**	☐: Fixed at ____	☐: Variable	☐: Configurable
Application Confirm:	☒: **None**	☐: Fixed at ____	☐: Variable	☐: Configurable
Complete Appl. Response:	☐: None	☐: Fixed at ____	☐: Variable	☒: **Configurable**

Sends/Executes Control Operations:

DNP V3.00

DEVICE PROFILE DOCUMENT

WRITE Binary Outputs	☒: **Never**	☐: Always	☐: Sometimes	☐: Configurable
SELECT/OPERATE	☐: Never	☐: Always	☐: Sometimes	☒: **Configurable**
DIRECT OPERATE	☐: Never	☐: Always	☐: Sometimes	☒: **Configurable**
DIRECT OPERATE – NO ACK	☒: **Never**	☐: Always	☐: Sometimes	☐: Configurable
Count > 1	☒: **Never**	☐: Always	☐: Sometimes	☐: Configurable
Pulse On	☐: Never	☐: Always	☐: Sometimes	☒: **Configurable**
Pulse Off	☐: Never	☐: Always	☐: Sometimes	☒: **Configurable**
Latch On	☐: Never	☐: Always	☐: Sometimes	☒: **Configurable**
Latch Off	☐: Never	☐: Always	☐: Sometimes	☒: **Configurable**
Queue	☒: **Never**	☐: Always	☐: Sometimes	☐: Configurable
Clear Queue	☒: **Never**	☐: Always	☐: Sometimes	☐: Configurable

Expects Binary Input Change Events:

☐: Either time-tagged or non-time-tagged for a single event
☐: Both time-tagged and non-time-tagged for a single event
☒: **Configurable, target database may be designed to handle either or both.**

Unsolicited Events

☒: **Unsolicited events are supported**
☐: Unsolicited events are not supported

Sequential File Transfer Support:

Append File Mode	☐: Yes	☒: **No**
Custom Status Code Strings	☐: Yes	☒: **No**
Permissions Field	☐: Yes	☒: **No**
File Events Assigned to Class	☐: Yes	☒: **No**
File Events Poll Specifically	☐: Yes	☒: **No**
Multiple Blocks in a Fragment	☐: Yes	☒: **No**
Max Number of Files Open	**0**	

Authentication Support:

☒: Authentication SAv2 supported
☒: Authentication SAv5 supported

DNP V3.0 Implementation Table

OBJECT			REQUEST (CI Server may send)		RESPONSE (CI Server will parse)	
Object Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
1	0	Binary Input – Any Variation	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)		
1	1	Binary Input packed format	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
1	2	Binary Input with Flags	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
2	1	Binary Input Change without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
2	2	Binary Input Change with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
2	3	Binary Input Change with Relative Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
3	0	Double Bit Input – Any Variation	1 (read)			
3	1	Double Bit Input packed format	1 (read)		129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
3	2	Double Bit Input with Flags	1 (read)		129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
4	1	Double Bit Input Change without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
4	2	Double Bit Input Change with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
4	3	Double Bit Input Change with Relative Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
10	0	Binary Output Status – Any Variation	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)		
10	1	Binary Output	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
10	2	Binary Output With Flags	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
11	1	Binary Output Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)

OBJECT			REQUEST (CI Server may send)		RESPONSE (CI Server will parse)	
Object Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
11	2	Binary Output Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
12	1	Control Relay Output Block	3 (select) 4 (execute) 5 (direct op)	17, 28, 39 (index)	129 (response)	echo of request
13	1	Binary Output Command Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
13	2	Binary Output Command Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
20	0	Binary Counter – Any Variation	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)		
20	1	32-Bit Binary Counter (with Flag)	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
20	2	16-Bit Binary Counter (with Flag)	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
20	3	32-Bit Delta Counter (with Flag)	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
20	4	16-Bit Delta Counter (with Flag)	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
20	5	32-Bit Binary Counter without Flag	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
20	6	16-Bit Binary Counter without Flag	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
20	7	32-Bit Delta Counter without Flag	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
20	8	16-Bit Delta Counter without Flag	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
21	0	Frozen Counter – Any Variation	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)		
21	1	32-Bit Frozen Counter (with Flag)	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
21	2	16-Bit Frozen Counter (with Flag)	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)

OBJECT			REQUEST (CI Server may send)		RESPONSE (CI Server will parse)	
Object Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
21	3	32-Bit Frozen Delta Counter (with Flag)	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
21	4	16-Bit Frozen Delta Counter (with Flag)	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
21	5	32-Bit Frozen Counter (with Flag and Time)	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
21	6	16-Bit Frozen Counter (with Flag and Time)	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
21	7	32-Bit Frozen Delta Counter (with Flag and Time)	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
21	8	16-Bit Frozen Delta Counter (with Flag and Time)	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
21	9	32-Bit Frozen Counter without Flag	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
21	10	16-Bit Frozen Counter without Flag	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
21	11	32-Bit Frozen Delta Counter without Flag	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
21	12	16-Bit Frozen Delta Counter without Flag	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
22	1	32-Bit Counter Change Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
22	2	16-Bit Counter Change Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
22	3	32-Bit Delta Counter Change Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
22	4	16-Bit Delta Counter Change Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
22	5	32-Bit Counter Change Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)

OBJECT			REQUEST (CI Server may send)		RESPONSE (CI Server will parse)	
Object Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
22	6	16-Bit Counter Change Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
22	7	32-Bit Delta Counter Change Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
22	8	16-Bit Delta Counter Change Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
23	1	32-Bit Frozen Counter Change Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
23	2	16-Bit Frozen Counter Change Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
23	3	32-Bit Frozen Delta Counter Change Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
23	4	16-Bit Frozen Delta Counter Change Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
23	5	32-Bit Frozen Counter Change Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
23	6	16-Bit Frozen Counter Change Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
23	7	32-Bit Frozen Delta Counter Change Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
23	8	16-Bit Frozen Delta Counter Change Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
30	0	Analog Input - Any Variation	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)		
30	1	32-Bit Analog Input	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
30	2	16-Bit Analog Input	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
30	3	32-Bit Analog Input without Flag	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)

OBJECT			REQUEST (CI Server may send)		RESPONSE (CI Server will parse)	
Object Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
30	4	16-Bit Analog Input without Flag	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
30	5	Short floating Analog Input	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
30	6	Long floating Analog Input	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
31	0	Frozen Analog Input - Any Variation	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)		
31	1	32-Bit Frozen Analog Input with Flags	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
31	2	16-Bit Frozen Analog Input with Flags	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
31	3	32-Bit Frozen Analog Input with Flags and Time	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
31	4	16-Bit Frozen Analog Input with Flags and Time	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
31	5	32-Bit Frozen Analog Input without Flag	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
31	6	16-Bit Frozen Analog Input without Flag	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
31	7	Short floating Frozen Analog Input	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
31	8	Long floating Frozen Analog Input	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
32	1	32-Bit Analog Change Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
32	2	16-Bit Analog Change Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
32	3	32-Bit Analog Change Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)

OBJECT			REQUEST (CI Server may send)		RESPONSE (CI Server will parse)	
Object Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
32	4	16-Bit Analog Change Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
32	5	Short floating point Analog Change Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
32	6	Long floating point Analog Change Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
32	7	Short floating point Analog Change Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
32	8	Long floating point Analog Change Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
33	1	32-Bit Frozen Analog Change Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
33	2	16-Bit Frozen Analog Change Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
33	3	32-Bit Frozen Analog Change Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
33	4	16-Bit Frozen Analog Change Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
33	5	Short floating Frozen Analog Change Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
33	6	Long floating Frozen Analog Change Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
33	7	Short floating Frozen Analog Change Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
33	8	Long floating Frozen Analog Change Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
34	0	Analog Input Deadband	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)		

OBJECT			REQUEST (CI Server may send)		RESPONSE (CI Server will parse)	
Object Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
34	1	Analog Input Deadband 16 Bit	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
			2 (write)	00, 01, 02 (start-stop) 17, 28, 39 (index)		
34	2	Analog Input Deadband 32 Bit	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
			2 (write)	00, 01, 02 (start-stop) 17, 28, 39 (index)		
34	3	Analog Input Deadband Single Float	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
			2 (write)	17, 28, 39 (index)		
40	0	Analog Output Status (Variation 0 is used to request default variation)	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)		
40	1	32-Bit Analog Output Status	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
40	2	16-Bit Analog Output Status	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
40	3	Short floating point Analog Output Status	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
40	4	Long floating point Analog Output Status	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
41	1	32-Bit Analog Output Block	3 (select) 4 (execute) 5 (direct op)	17, 28, 39 (index)	129 (response)	echo of request
41	2	16-Bit Analog Output Block	3 (select) 4 (execute) 5 (direct op)	17, 28, 39 (index)	129 (response)	echo of request
41	3	Short floating point Analog Output Block	3 (select) 4 (execute) 5 (direct op)	17, 28, 39 (index)	129 (response)	echo of request
41	4	Long floating point Analog Output Block	3 (select) 4 (execute) 5 (direct op)	17, 28, 39 (index)	129 (response)	echo of request
42	1	32-Bit Analog Output Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
42	2	16-Bit Analog Output Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)

OBJECT			REQUEST (CI Server may send)		RESPONSE (CI Server will parse)	
Object Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
42	3	32-Bit Analog Output Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
42	4	16-Bit Analog Output Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
42	5	Short floating point Analog Output Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
42	6	Long floating point Analog Output Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
42	7	Short floating point Analog Output Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
42	8	Long floating point Analog Output Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
43	1	32-Bit Analog Output Command Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
43	2	16-Bit Analog Output Command Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
43	3	32-Bit Analog Output Command Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
43	4	16-Bit Analog Output Command Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
43	5	Short floating point Analog Output Command Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
43	6	Long floating point Analog Output Command Event without Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
43	7	Short floating point Analog Output Command Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)

OBJECT			REQUEST (CI Server may send)		RESPONSE (CI Server will parse)	
Object Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
43	8	Long floating point Analog Output Command Event with Time			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
50	1	Time and Date	2 (write)	07 (quantity = 1)		
51	1	Time and Date CTO			129 (response)	07 (quantity = 1)
51	2	Unsynchronized Time and Date CTO			129 (response)	07 (quantity = 1)
60	1	Class 0 Data	1 (read)	06 (no range, or all)		
60	2	Class 1 Data	1 (read)	06 (no range, or all) 07 (quantity = 1-255) 08 (quantity = 256-x)		
60	3	Class 2 Data	1 (read)	06 (no range, or all) 07 (quantity = 1-255) 08 (quantity = 256-x)		
60	4	Class 3 Data	1 (read)	06 (no range, or all) 07 (quantity = 1-255) 08 (quantity = 256-x)		
80	1	Internal Indications	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
			2 (write)	00 (start-stop,element 7, 16-255) 28, 39 (index,element 256-up)		
101	0	Binary Coded Decimal	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)		
101	1	Binary Coded Decimal 4 digits	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
			2 (write)	00, 01, 02 (start-stop) 17, 28, 39 (index)		
101	2	Binary Coded Decimal 8 digits	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
			2 (write)	00, 01, 02 (start-stop) 17, 28, 39 (index)		
101	3	Binary Coded Decimal 16 digits	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
			2 (write)	17, 28, 39 (index)		
102	0	Unsigned Integer	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)		
102	1	Unsigned Integer 8 Bit	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
			2 (write)	17, 28, 39 (index)		

OBJECT			REQUEST (CI Server may send)		RESPONSE (CI Server will parse)	
Object Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
110	string length	Octet String Object	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
			2 (write)	17, 28, 39 (index)		
111	string length	Octet String Event Object			129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
121	0	Security statistic	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)
121	1	Security statistic 32 bit	1 (read)	00, 01, 02 (start-stop) 17, 28, 39 (index)	129 (response)	00, 01, 02 (start-stop) 07, 17, 27, 37, 08, 18, 28, 38, 09, 19, 29, 39 (index)

3.27 MELSEC

MELSEC PLC is developed and maintained by Mitsubishi Electric Corporation. There are multiple CPU types and connection types in MELSEC PLC. For more details, refer the website of Mitsubishi Electric Corporation.

Supported OS

When using the MELSEC driver, use Windows client-based OS for CI Core. (Server-based OS cannot be used).

Supported OS

The following table shows the supported MELSEC CPUs.

Product series	CPU unit name
A series	A0J2HCPU, A1SCPU, A1SCPUC24-R2, A1SHCPU(-SI), A1SJCPU, A1SJHCPU, A1NCPU, A2CCPU, A2CJCPU, A2CCPUC24(-PRF), A2NCPU(-S1), A2SCPU, A2SHCPU, A3NCPU, A2ACPU(-S1), A2ACPUP21/R21(-S1), A3ACPU, A3ACPUP21/R21, A1FXCPU, A2UCPU(-S1), A3UCPU, A4UCPU, A2USCPU(-S1), A2USHCPU-S1
QnAseries	Q2ACPU(-S1), Q2ASCPU(-S1), Q3ACPU, Q4ACPU, Q2ASHCPU(-S1), Q4ARCPU
Q series (A mode)	Q02CPU-A, Q02HCPU-A, Q06HCPU-A
Q series (Q mode)	Q02(H)CPU, Q06HCPU, Q12HCPU, Q25HCPU, Q00JCPU, Q00CPU (*1), Q01CPU (*1), Q12PHCPU, Q25PHCPU, Q12PRHCPU, Q25PRHCPU, Q00UJCPU, Q00UCPU, Q01UCPU, Q02UCPU, Q03UDCPU, Q04UDHCPU, Q06UDHCPU, Q10UDHCPU, Q13UDHCPU, Q20UDHCPU, Q26UDHCPU, Q03UDECPU, Q04UDEHCPU, Q06UDEHCPU, Q10UDEHCPU, Q13UDEHCPU, Q20UDEHCPU, Q26UDEHCPU, Q02PHCPU, Q06PHCPU, Q50UDEHCPU, Q100UDEHCPU, Q03UDVCPU, Q04UDVCPU, Q06UDVCPU, Q13UDVCPU, Q26UDVCPU, Q04UDPVCPU, Q06UDPVCPU, Q13UDPVCPU, Q26UDPVCPU
PC CPU	009PPC-CPU686, 009PPC-CPU852
WinCPU	009PPC-100-DC, Q10WCPU-W1
L series	L02CPU, L02CPU-P, L02SCPU, L02SCPU-P, L06CPU, L06CPU-P, L26CPU, L26CPU-P, L26CPU-BT, L26CPU-PBT, LJ72MS15
FX series	FX0, FX0S, FX0N, FX1, FX1S, FX1N, FX1NC, FX2, FX2C, FX2N, FX2NC, FX3UC, FX3U
iQ-R series	R04CPU, R08CPU, R16CPU, R32CPU, R120CPU, R08PCPU, R16PCPU, R32PCPU, R120PCPU, R04ENCPU, R08ENCPU, R16ENCPU, R32ENCPU, R120ENCPU, R00CPU, R01CPU, R02CPU
iQ-F series	FX5U
Motion controller	A273UHCPU(-S3), A173UHCPU(-S1), A171SHCPU, A172SHCPU, Q172(H)CPU, Q173(H) CPU, Q172DCPU, Q173DCPU, R16MTCPU, R32MTCPU, R64MTCPU
GOT (*2)	A985GOT(-V), A975GOT, A970GOT, A960GOT, A956WGOT, A956GOT(-M3), A953GOT, A951GOT, A950GOT, F920GOT-K, F920 handy GOT RH type, F93 □ GOT, F930GOT-K, F94 □ GOT, F940WGOT, F94 □handy GOT, F94 □ handy GOT RH type GT1150, GT1155, GT1550, GT1555, GT1565, GT1575, GT1585, GT2103, GT2508, GT2510, GT2512, GT2708, GT2710, GT2712, GT2715
Sequencer function in-built inverter	FR-C500(A0J2HCPU equivalent)
MELDAS CNC series	C64 (*3)
C language controller	Q12DCCPU-V, Q06CCPU-V-H01, R12CCPU-V

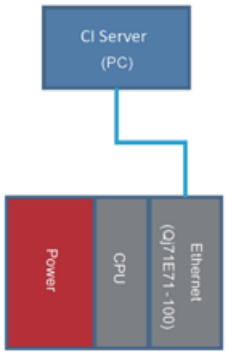
*1: Q00CPU, Q01CPU units corresponding to multi-CPU configuration are the units of functional version B and later.
2: A900GOT series can be connected only to version 9.0 and later.
In case of F900GOT series, OS version 1.10 or later of F900GOT main unit is required.
*3: Top 5 digits of serial no. supports 12042 or later.

Connection type

The following connection types are available.

- Ethernet port connection through ethernet unit

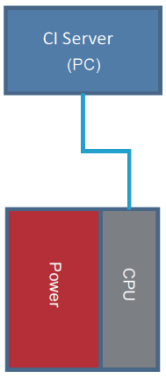
  This is a simple system configuration in which CI Server is connected to MELSEC CPU through MELSEC ethernet unit.



F032701.ai

- Ethernet port connection through CPU unit

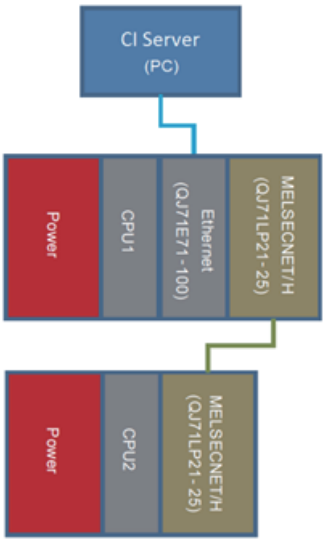
  This is a simple system configuration in which CI Server is connected MELSEC CPU through the ethernet port on MELSEC CPU.



F032702.ai

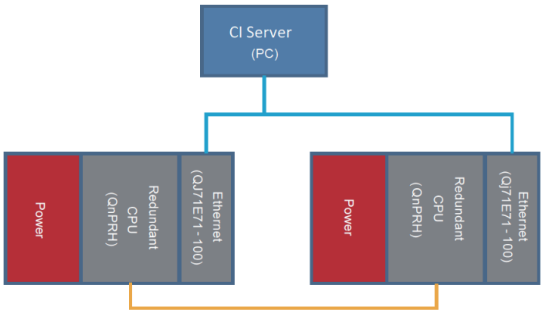
- Multi network connection through ethernet unit

  In this type, CI Server is connected to MELSEC CPU through multiple networks. The following example shows MELSECNET/H



F032703.ai

- CPU redundancy connection using ethernet



F032704.ai

3.28 Omron FINS

Connects to devices that use the Omron FINS protocol.

Connection format:

Connects to the interface card of Omron RTU and uses UDP protocol.

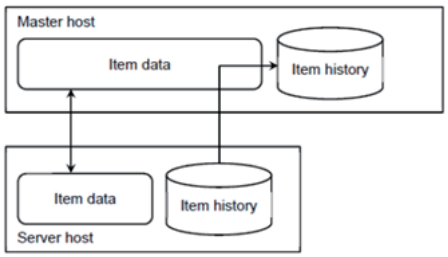
Supported functions:

Read/write to CIO, WR, HR, and DM areas on the RTU in CS and CJ modes.

3.29 Host-host connection

The function that connects CI Core and CI Core is called host-host connection. In the host-host connection, multiple CI Cores are connected and the item data in CI Cores is synchronized. In the host-host connection, other CI Cores are connected as external station.

(Connection is defined within the equipment definitions in the Engineering Module.) The system that provides data is called Server host and the system to which data is provided is called Master host.



F032901.ai

The host-host connection provides the following functions:

- The item data of server host is transferred to the item of the master host.
- When the master host item data is changed, the change is reflected in the server host item.
- The item data that was not transferred due to communication failure etc., is transferred from the server host to the master host after communication is restored.
- Multiple CI Cores on the server side can be connected to a single CI Core on the master side.
- The communication between the master host and the server host is encrypted.
- The master host and the server host can be connected with redundant lines.

Notes:

- The supported item data types are Boolean, integer, real, and string data.
- The supported historical item data types are Boolean, integer, real, and string data. String data is not supported because it cannot be stored in the item storage group.
- Data transfer from the master host to the server host is also supported, but performance is not optimized, and historical data transfer is not supported.

When using host-host connection

In the host-host connection, data transfer and command transmission are performed between CI Cores and can be used even when the quality of the connected network is poor. (Ex: offshore system and onshore system)

Enterprise systems have a feature similar to a host-host connection, where database is shared among the servers in the system.

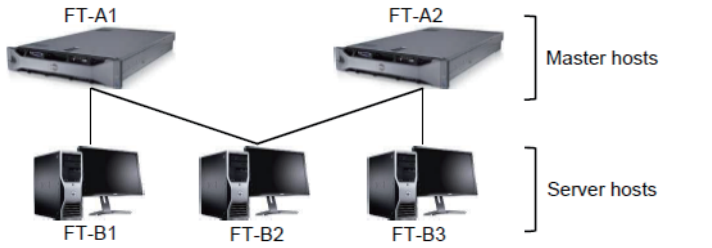
Example of system configuration

In addition to the simple Master host - Server host configuration, the following system configuration can also be used.

N:(master host)-N:(server host) connection

FT-A1 is the master host of FT-B1 and FT-B2, and the data from FT-B1 and FT-B2 is transferred to FT-A1.

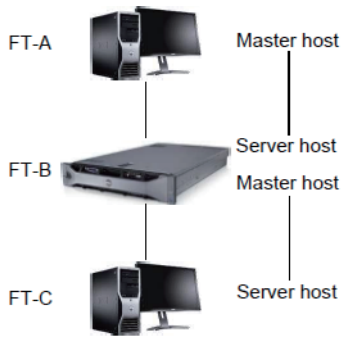
FT-A2 is the master host of FT-B2 and FT-B3, and the data from FT-B2 and FT-B3 is transferred to FT-A2.



F032902.ai

Master host and server host integrated configuration

Data from FT-C is transferred to FT-B and data from FT-B is transferred to FT-A. FT-B is the master host of FT-C and server host of FT-A.



F032903.ai

Note: A tool to estimate the load on network is provided.

3.30 CENTUM VP connection

CI server is connected to Vnet/IP and communicates with FCS, SCS, and UGS.

Notes:

- The stations of CENTUM VP (FCS, HIS, SCS, UGS, etc.) cannot access the data of CI server.
- Vnet/IP connection is not suitable to write large amount of data (such as data of RTU connected to CI Server) frequently to FCS.

Fixed scan

CI Server collects (scans) data from controllers (FCS, SCS, UGS) regularly.

Note: The maximum amount of data that can be processed differs depending on the Vnet/IP station. (Refer table below). The total com munication amount to FCS, SCS and UGS can be adjusted such that it does not exceed the processing capacity of each station.

Station type	Polling rate	Notes
FCS	3,200	AFV10
	12,800	AFV10 / AFV 30 / AFV40 and later models
UGS	6,400	
SCS	1,280	SSC50 / SSC60

The scan cycle can be set to three scan types: fast, medium, and slow.

For example, you can set to scan high-severity data every second, medium-severity data every two seconds, and low-severity data every five to ten seconds.

This can be set for each type of data such as PV, MV, SV, etc.

The following table shows default settings during normal operation.

Scan type	Interval	Item	Notes
Slow	10,000 msec	AOFS, BSET, BSTS, COMMENTS, DL, DIALOGE, DV, HH, LL, MODE, MSH, MSL, PH, PHASE, PL, SH, SL, UNIT, VL	
Medium	5,000 msec	FV, SV	
High speed	1,000 msec	ALRM, CPV, MV, PV	

User can define each scan type controller-wise and item-wise.

Dynamic scan

In addition to the fixed scan cycles (fast, medium, and slow), there are dynamic scan cycles. In addition to the normal scan cycle, you can speed up the scan cycle only while the item is displayed in the graphic.

The dynamic scan period is typically used for tuning parameters. Tuning parameters generally do not change. For example, the normal scan period is once every 30 minutes, but you can change it to every second while the parameter setting screen is displayed.

Two scan periods are defined in the dynamic scan period:

* Normal scan period

* Special scan period (when item is displayed on the screen)

Supported CENTUM version

CENTUM VP R5.01.20 and later are supported.

Configuration

When connecting with CENTUM VP, the following tools are used to define CENTUM tag data as CI server items at once.

- CI Exchange for CENTUM VP
  In this tool, in addition to items, tuning panel and faceplates of CENTUM function block are generated as screens on the CI Server.

Data that cannot be accessed with the CI Exchange tool can be accessed by defining a point in the usual way.

Supports Vnet/IP multi domain.

3.30.1 CI Exchange for CENTUM VP

To manage a CENTUM VP project in CI Server, the CENTUM VP project must be equalized in the CI Server environment. Also. the CENTUM VP engineering data must be converted to CI Server engineering data. The CI Exchange for CENTUM VP tool enables you to convert

CENTUM VP engineering data such as tags, function blocks, or alarms to CI Server engineering data. This tool also generates the displays of the engineering data.

The CI Exchange for CENTUM VP tool supports the following solutions.

- RGS solution
  The RGS polls @ALARM data from the CENTUM VP system via Vnet/IP network, which can be monitored in CI Server. Alarms can be generated if something changed.
- RGS with EAL solution
  CI Server is equipped with VAGW (Vnet Alarm Gateway). VAGW receives alarm events or alarm status information from Vnet/IP, converts them into a format that CI Server can process, and then sends them to the Alarm service. The OPC UA model is adopted to send the data so that the Alarm service can handle the CENTUM VP alarm as an OPC UA alarm. Moreover, the alarm acknowledgement operation can be synchronized between CI Server and CENTUM VP through the OPC UA A&C interface.

Tag information supported in CI Exchange

Tag Property in CENTUM VP	Data Type	Supported for Conversion
Tag Name	String (max length=16 characters)	Yes
TagComnt	String (max length=24 characters)	Yes
AlarmType	8-bit Unsigned Integer	Yes
InstType	8-bit Unsigned Integer	Yes
DP	8-bit Unsigned Integer	Yes
MV_DP	8-bit Unsigned Integer	Yes
LabelCode (Label1, Label2, Label3, Label4)	8-bit Unsigned Integer	Yes (Label4 is not supported)
UserCode2	8-bit Unsigned Integer	Yes
UserCode3	8-bit Unsigned Integer	Yes
MV_Unit	16 bit Unsigned Integer	Yes
EngUnit	16-bit Unsigned Integer	Yes
SH	32-bit Signed Integer	Yes
SL	32-bit Signed Integer	Yes
RH	32-bit Signed Integer	Yes
RL	32-bit Signed Integer	Yes
MVH	32-bit Signed Integer	Yes
MVL	32-bit Signed Integer	Yes
StationName	String (max length=8 characters)	Yes
AccessLevel	8-bit Unsigned Integer	No
ElemType1	8-bit Unsigned Integer	No
ElemType2	8-bit Unsigned Integer	No
ElemNo	16-bit Unsigned Integer	No
HelpNo	16-bit Unsigned Integer	No
InstNo	16-bit Unsigned Integer	No
PlantNo	16-bit Signed Integer	No
AuxPointer	32-bit Unsigned Integer	No
AuxCode1	8-bit Unsigned Integer	No

Tag Property in CENTUM VP	Data Type	Supported for Conversion
DataDisp	8-bit Unsigned Integer	No
AuxCode1	8-bit Unsigned Integer	No
InstMark	8-bit Unsigned Integer	No
TagMark	8-bit Unsigned Integer	No
TP	8 bit Unsigned Integer	No
RP	8-bit Unsigned Integer	No
OCMark	8-bit Unsigned Integer	No
DivideNo	8-bit Unsigned Integer	No
UserCode1	8-bit Unsigned Integer	No
StatusAdr	32-bit Unsigned Integer	No
StatusBitAdr	16-bit Unsigned Integer	No
CPUNo	8-bit Unsigned Integer	No
HMLDivision	8-bit Unsigned Integer	No
DevCode	16-bit Unsigned Integer	No
DevInf	16-bit Unsigned Integer	No
UpperPanel	String (max length=16)	No

Functional block FCS supported by the CI Exchange tool

Control blocks

Category	Function Block	Description	Supported (Yes/No)
Input indicators	PVI	Input indicator block	Yes
	PVI-DV	Input indicator block with deviation alarm	Yes
Controllers	PID	Controller block	Yes
	PI-HLD	Sampling PI controller block	Yes
	PID-BSW	PID controller block with batch switch	Yes
	ONOFF	2-Position ON/OFF controller block	Yes
	ONOFF-E	Enhanced 2-position ON/OFF controller block	Yes
	ONOFF-G	3-position ON/OFF controller block	Yes
	ONOFF-GE	Enhanced 3-position ON/OFF controller block	Yes
	PID-TP	Time-proportioning ON/OFF controller block	Yes
	PD-MR	PD controller block with manual reset	Yes
	PI-BLEND	Blending PI controller block	Yes
	PID-STC	Self-tuning PID controller block	Yes
	ZWOPID	PID Controller with Output Loss Compensation for Wireless Block	No
Manual loader	MLD	Manual loader block	Yes
	MLD-PVI	Manual loader block with input indicator	Yes
	MLD-SW	Manual loader block with Auto/Man switch	Yes
	MC-2	2-position motor control block	Yes
	MC-2E	Enhanced 2-position motor control block	Yes
	MC-3	3-position motor control block	Yes
	MC-3E	Enhanced 3-position motor control block	Yes
Signal setters	RATIO	Ratio set block	Yes
	PG-L13	13-zone program set block	Yes
	PG-L13	13-zone program set block with copy	Yes

Category	Function Block	Description	Supported (Yes/No)
Signal setters	BSETU-2	Flow-totalizing batch set block	Yes
	BSETU-3	Weight-totalizing batch set block	Yes
Signal limiters	VELLIM	Velocity limiter block	Yes
Signal selectors	AS-H/M/L	Autoselector block	Yes
	SS-H/M/L	Signal selector block	Yes
	SS-DUAL	Dual-redundant signal selector block	Yes
Signal distributors	FOUT	Cascade signal distributor block	Yes
	FFSUM	Feedforward signal summing block	Yes
	FFSUM	Feedforward signal summing block (with balanced operation)	Yes
	XCPL	Non-interference control output block	Yes
	SPLIT	Control signal splitter block	Yes
Alarm	ALM-R	Representative alarm block	Yes
Pulse count input connection	PTC	Pulse count input block	Yes
YS instrument	SLCD	YS controller block	No
	SLPC	YS programmable controller block	No
	SLMC	YS programmable controller block with pulse-width output	No
	SMST-111	YS manual station block with SV output	No
	SMST-121	YS manual station block with MV output lever	No
	SMRT	YS ratio set station block	No
	SBSD	YS batch set station block	No
	SLCC	YS blending controller block	No
	SLBC	YS batch controller block	No
	STLD	YS totalizer block	No
Foundation Fieldbus	FF-AI	Analog input	Yes
	FF-DI	Digital input	Yes
	FF-AO	Analog output	Yes
	FF-DO	Digital output	Yes
	FF-CS	Control Selector	No
	FF-PID	PID Control	No
	FF-RA	Ratio	No
	FF-OS	Output Splitter	No
	FF-SC	Signal Characterizer	No
	FF-IT	Integrator (Totalizer)	No
	FF-IS	Input Selector	No
	FF-MDI	Multiple Discrete Input	No
	FF-MDO	Multiple Discrete Output	No
	FF-MAO	Multiple Analog Output	No
	FF-MAI	Multiple Analog Input	No
	FF-SUNV	Simple Universal	No

Operation blocks

Category	Function Block	Description	Supported (Yes/No)
Arithmetic calculation	ADD	Addition block	Yes (*1)
	MUL	Multiplication block	Yes (*1)
	DIV	Division block	Yes (*1)
	AVE	Averaging block	Yes (*1)
Analog calculation	SQRT	Square root block	Yes (*1)
	EXP	Exponential block	Yes (*1)
	LAG	First-order lag block	Yes (*1)
	INTEG	Integration block	Yes (*1)
	LD	Derivative block	Yes (*1)
	RAMP	Ramp block	Yes (*1)
	LDLAG	Lead/lag block	Yes
	DLAY	Dead-time block	Yes
	DLAY-C	Dead-time compensation block	Yes
	AVE-M	Moving-average block	Yes
	AVE-C	Cumulative-average block	Yes
	FUNC-VAR	Variable line-segment function block	Yes
	TPCFL	Temperature and pressure correction block	Yes (*1)
	ASTM1	ASTM correction block: old JIS	Yes
	ASTM2	ASTM correction block: new JIS	Yes
Logic operation	AND	Logical AND block	Yes (*1)
	OR	Logical OR block	Yes (*1)
	NOT	Logical NOT block	Yes
	SRS1-S	Set-dominant flip-flop block with 1 output	Yes (*1)
	SRS1-R	Reset-dominant flip-flop block with 1 output	Yes (*1)
	SRS2-S	Set-dominant flip-flop block with 2 outputs	Yes (*1)
	SRS2-R	Reset-dominant flip-flop block with 2 outputs	Yes (*1)
	WOUT	Wipeout block	Yes (*1)
	OND	ON-delay timer block	Yes (*1)
	OFFD	OFF-delay timer block	Yes (*1)
	TON	One-shot block (rising-edge trigger)	Yes (*1)
	TOFF	One-shot block (falling-edge trigger)	Yes (*1)
	GT	Comparator block (greater than)	Yes (*1)
	GE	Comparator block (greater than or equal)	Yes (*1)
	EQ	Equal operator block	Yes (*1)
	BAND	Bitwise AND block	Yes (*1)
	BOR	Bitwise OR block	Yes (*1)
	BNOT	Bitwise NOT block	Yes (*1)
General purpose calculation	CALCU	General-purpose calculation block	Yes
	CALCU-C	General-purpose calculation block with string	Yes
Auxiliary	SW-33	Three-pole three-position selector witch block	Yes
	SW-91	One-pole nine-position selector switch block	Yes
	DSW-16	Selector switch block for 16 data	Yes
	DSW-16C	Selector switch block for 16 string data	Yes

Category	Function Block	Description	Supported (Yes/No)
Auxiliary	DSET	Data set block	Yes
	DSET-PVI	Data set block with input indicator	Yes
	BDSET-1L	One-batch data set block	Yes
	BDSET-1C	One-batch string data set block	Yes
	BDSET-2L	Two-batch data set block	Yes
	BDSET-2C	Two-batch string data set block	Yes
	BDA-L	Batch data acquisition block	Yes
	BDA-C	Batch string data acquisition block	Yes
	ADL	Inter-station data link block	Yes

*1: Newly supported block in this revision

Sequence control blocks

Category	Function Block	Description	Supported (Yes/No)
Sequence table	ST16	Sequence table block	Yes
	ST16E	Rule extension block	Yes
	M_ST16	Sequence table block (Medium Capacity)	No
	M_ST16E	Rule extension block (Medium Capacity)	No
	L_ST16	Sequence table block (Large Capacity)	No
	L_ST16E	Rule extension block (Large Capacity)	No
Logic chart	LC64	Logic chart	Yes
	LC64-E	Enhanced Logic chart	No
Switch instrument	SI-1	Switch instrument block with 1 input	Yes
	SI-2	Switch instrument block with 2 inputs	Yes
	SIO-11	Switch instrument block with 1 input and 1 output	Yes
	SIO-12	Switch instrument block with 1 input and 2 outputs	Yes
	SIO-21	Switch instrument block with 2 inputs and 1 output	Yes
	SIO-22	Switch instrument block with 1 input and 2 outputs	Yes
	SIO-12P	Pulse switch instrument block with 1 input and 2 outputs	Yes
	SIO-22P	Pulse switch instrument block with 1 input and 2 outputs	Yes
	SO-1	Switch instrument block with 1 output	Yes
	SO-2	Switch instrument block with 2 outputs	Yes
	SI-1E	Switch instrument block with 1 input	Yes
	SI-2E	Switch instrument block with 2 inputs	Yes
	SIO-11E	Enhanced Switch instrument block with 1 input and 1 output	Yes
	SIO-12E	Enhanced Switch instrument block with 1 input and 2 outputs	Yes
	SIO-21E	Enhanced Switch instrument block with 2 inputs and 1 output	Yes
	SIO-22E	Enhanced Switch instrument block with 1 input and 2 outputs	Yes
	SIO-12PE	Enhanced Pulse switch instrument block with 1 input and 2 outputs	Yes
	SIO-22PE	Enhanced Pulse switch instrument block with 1 input and 2 outputs	Yes
	SO-1E	Enhanced Switch instrument block with 1 output	Yes
	SO-2E	Enhanced Switch instrument block with 2 outputs	Yes
	SI-1ALM	Switch Instrument Block with 1 Input Discrete- status Alarm	No
Sequence element	TM	Timer block	Yes
	CTS	Software counter block	Yes
	CTP	Pulse train input counter block	Yes
	CI	Code input block	Yes
	CO	Code output clock	Yes
	RL	Relational expression block	Yes
	RS	Resource scheduler block	Yes
Valve monitoring	VLVM	Valve monitoring block	Yes
Local Switch	LSW	Local Switch Block	No

Faceplate blocks

Category	Function Block	Description	Supported (Yes/No)
Faceplate	PBS5C	Extended 5-Push-Button Switch Block	Yes
	PBS10C	Extended 10-Push-Button Switch Block	Yes
	INDST2	Dual-Pointer Indicating Station Block	No
	INDST2S	Dual-Pointer Manual Station Block	No
	INDST3	Triple-Pointer Manual Station Block	No
	BSI	Batch Status Indicator Block	Yes
	HAS3C	Extended Hybrid Manual Station Block	No

SFC blocks

Category	Function Block	Description	Supported (Yes/No)
SFC	_SFCSW	Three-position switch SFC block	Yes
	_SFCPB	Pushbutton SFC block	Yes
	_SFCAS	Analog SFC block	Yes

Unit measurement blocks

Category	Function Block	Description	Supported (Yes/No)
Unit Instrument	_UTAS	Analog Unit Instrument	No
	_UTAS-N	Analog Non-Resident Unit Instrument	No
	_UTAS-SN	Analog Non-Resident Unit Instrument with Recipe Operation	No
	_UTPB	Unit Instrument with Five-Pushbutton Switch	No
	_UTPB-N	Analog Non-Resident Unit Instrument	No
	_UTPB-SN	Non-Resident Unit Instrument with Five-Pushbutton Switch and Recipe Operation	No
	_UTSW	Unit Instrument with Three-Position Switch	No
	_UTSW-N	Non-Resident Unit Instrument with Three- Position Switch	No
	_UTSW-SN	Non-Resident Unit Instrument with Three- Position Switch and Recipe Operation	No
Unit Instrument Operation	UTOP-SN	Non-Resident Unit Operation Function Instrument	No
	OPSFC	SFC Operation	No
	OPSFCP1	SFC operation with floating-data parameters	No
	OPSFCP2	SFC operation with character-data parameters	No
	OPSFCP3	SFC operation with floating/character-data parameters	No
	OPSFCP4	SFC operation with integer/character-data parameters	No
	OPSFCP5	SFC operation with floating/integer-data parameters	No
	OPSBL	SEBOL Operation	No

Valve Pattern Monitoring blocks

Category	Function Block	Description	Supported (Yes/No)
Valve Pattern Monitoring	VPM64	64-Data Valve Pattern Monitor	No
	VPM128	128-Data Valve Pattern Monitor	No
	VPM256	256-Data Valve Pattern Monitor	No
	VPM512	512-Data Valve Pattern Monitor	No
	VPM64A	64-Data Valve Pattern Monitor with Alarm	No
	VPM128A	128-Data Valve Pattern Monitor with Alarm	No
	VPM256A	256-Data Valve Pattern Monitor with Alarm	No
	VPM512A	512-Data Valve Pattern Monitor with Alarm	No

Offsite blocks

Category	Function Block	Description	Supported (Yes/No)
Offsite blocks	FSBSET	Batch Set Control Block	No
	BLEND	Blending Master Control Block	No

System functional blocks

Category	Function Block	Description	Supported (Yes/No)
System Function blocks	FCS_CPU	CPU Load Information Block	No
	FCS_COM	Communication Load Information Block	No
	FCS_IOC	I/O Load Information Block	No
	FCS_SBL	SEBOL Related Information Block	No

Link blocks

Category	Function Block	Description	Supported (Yes/No)
System Function blocks	FCS_CPU	CPU Load Information Block	No
Link blocks	PIO		No
	AREAIN		No
	AREAOUT		No

Advanced regulatory blocks

Category	Function Block	Description	Supported (Yes/No)
Advanced regulatory blocks	ZSSVC	Shell Surge Volume Controller	No
	ZBALANCE	Furnace Pass/Coil Balancing Algorithm	No
	ZCTL	Column Tray Loading Algorithm	No
	ZMVC	Measurement Validation and Comparison	No

Element type-wise support

Category	Function Block	Supported (Yes/No)
Annunciator	%AN	Yes
Process I/O	%ZN	No
Communication I/O	%Z	No
	%WW	No
	%WB	No
Fieldbus I/O	%Z	No
Common SW	%SW	Yes
Global SW	%GS	Yes
Print SW	%PR	No
Operation guide	%OG	No
Multimedia start	%VM	No
Sequence message request	%RQ	No
Computer event message	%CP	No
Picot computer event message	%M3	No
Signal event message	%EV	No
Process I/O	%Y	No

SCS function blocks supported in the CI Exchange tool

Extension communication blocks

Category	Function Block	Description	Supported (Yes/No)
External Communication Blocks	ECW_B	External Communication Bock (BOOL type)	Yes
	ECW_I	External Communication Bock (Integer type)	Yes
	ECW_R	External Communication Bock (Real type)	Yes

Safety control functional blocks

Category	Function Block	Description	Supported (Yes/No)
External Communication Blocks	ANLG_S	Analog input	Yes
	ANLGI	Analog input function blocks with data status	Yes
	HSDTR	Analog input FB for smoke and heat detectors)	No
	GASDTR	Analog input FB for gas and flame detectors	No

Speed control alarm functional blocks

Category	Function Block	Description	Supported (Yes/No)
Velocity Alarm Limit Blocks	VEL	Velocity Limit Alarm	Yes

Grouping override functional blocks

Category	Function Block	Description	Supported (Yes/No)
Grouping Override	GOV_B	BOOL type Grouping Override	Yes
	GOV_IB	Grouping Override	No

Manual operation blocks

Category	Function Block	Description	Supported (Yes/No)
Manual Operation Blocks	MOB_11	BOOL-type data manual operation with three-position answerback	Yes
	MOB_21	BOOL-type data manual operation with two-position answerback	Yes
	MOB_RS	Auto-reset BOOL-type data manual operation	Yes
	MOA	Analog-type data manual operation	No

Annunciator blocks

Category	Function Block	Description	Supported (Yes/No)
Annunciator Blocks	ANN	Annunciator	Yes
	ANN_FUP	First Up Annunciator	No
	ANN_SUP	First Up Annunciator	No
	FUR_RST	First Up Alarm Annunciator Reset	No
	FUP_RST	First Up Alarm Annunciator Reset	No

UGS Function blocks supported in the CI Exchange tool

UGS function blocks

Category	Function Block	Description	Supported (Yes/No)
UGS	USY-US	Station monitor block	Yes
	USY-CTR	Controller monitor block for OPC DA server, Mod- bus controller, and Ether- net/IP controller	Yes
	USR-ASH	Auto Selector POU	No
	USR-ASL	Auto Selector POU	No
	USR-ASM	Auto Selector POU	Yes
	USR-AST1	ASTM Correction (Old JIS) POU	No
	USR-AST2	ASTM Correction (New JIS) POU	No
	USR-AVEC	Cumulative-Average POU	No
	USR-AVEM	Moving-Average POU	No
	USR-BBFR	Real Data Buffer POU	Yes
	USR-BBFT	Time Data Buffer POU	Yes
	USR-CT	Counter POU	Yes
	USR-DLAY	Dead-Time POU	Yes
	USR-FSM	Feed-forward Signal Ad- dition	No
	USR-FSMB	Feed-forward Signal Ad- dition with Balance Action	Yes
	USR-FOUT	Cascade Signal Distribu- tor POU	Yes
	USR-FNVR	Variable Line-segment Function POU	Yes
	USR-LDLG	Lead/Lag POU	No
	USR-MLD	Manual Loader POU (without output push- back)	Yes
	USR-MLDP	Output Pushback Type MLD	Yes
	USR-MLDB	Bias Tracking Type MLD	Yes
	USR-OO	2-position ON/OFF Con- troller POU	Yes
	USR-OOG	3-position ON/OFF Con- troller POU	Yes
	USR-PCFL	Pressure Correction POU	Yes
	USR-P30	30-zone Program Set POU	Yes
	USR-P30B	30-zone Program Set POU (with bumpless function)	Yes
	USR-PIHL	Sample PI Controller POU	Yes
	USR-PID	PID Controller POU	Yes
	USR-PVI	Input Indicator POU	Yes
	USR-RTO	Ratio Set POU	Yes
	USR-RTOR	Ratio Set POU (with ratio tracking function)	No
	USR-I1	Switch Instrument	Yes
	USR-I2	Switch Instrument	Yes
	USR-IO11	Switch Instrument	Yes
	USR-IO12	Switch Instrument	Yes
	USR-IO21	Switch Instrument	Yes
	USR-IO22	Switch Instrument	Yes
	USR-O1	Switch Instrument	Yes
	USR-O2	Switch Instrument	Yes
	USR-SW13	1-pole 3-position Selector Switch POU	No
	USR-SW19	1-pole 9-position Selector Switch POU	No
	USR-SW31	3-pole 1-position Selector Switch POU	No
	USR-SW91	9-pole 1-position Selector Switch POU	No

Category	Function Block	Description	Supported (Yes/No)
UGS	USR-TCFL	Temperature Correction POU	Yes
	USR-TM	Timer POU	Yes
	USR-TPCL	Temperature and Pres- sure Correction POU	Yes
	USR-VLM	Velocity Limiter POU	Yes
	USR-VLMP	Output Pushback VEL- LIM	Yes
	USR-XLMD	Double Cross-limit POU	Yes
	USR-XLMS	Single Cross-limit POU	Yes
	USD-I16	Signed 16-bit integer	Yes
	USD-U16	16-bit unsigned integer	Yes
	USD-I32	32-bit signed integer	Yes
	USD-U32	32-bit unsigned integer	Yes
	USD-F32	32-bit floating point	Yes
	USD-F64	64-bit floating point	Yes
	USD-CHR	16-byte (or less) charac- ter string data	Yes
	USD-BOOL	ON/OFF data (1-bit, True:1 False:0)	Yes
	USG_ANNP	When the specified bit value in RAW changes from 0 to 1, annunciator messages are generated.	Yes
	USG_ANNI	When the specified bit value in RAW changes from 1 to 0, annunciator messages are generated.	Yes
	USG_VB32	Bit array faceplate block	No
	_UNxxxxx	User-defined faceplate block without alarm	No
	_UGxxxxx	User-defined faceplate block with alarm	No

3.31 Geographic Information System link (GIS)

By overlapping the CI Server symbol on the map image of the external GIS (Geographic Information System) Web mapping server, CI Server information can be displayed on the map.

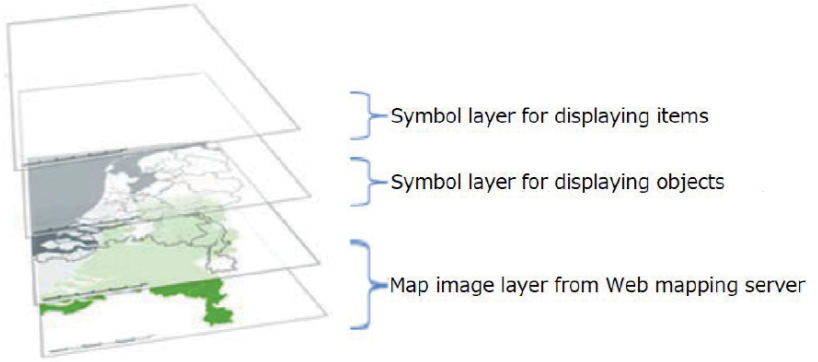


Figure Image of layer structure of Map Viewer

System configuration

The Map Viewer obtains the map image from the Web mapping server of the external server through Web HMI Server proxy service.

The following figure shows the system configuration when map viewer is used.

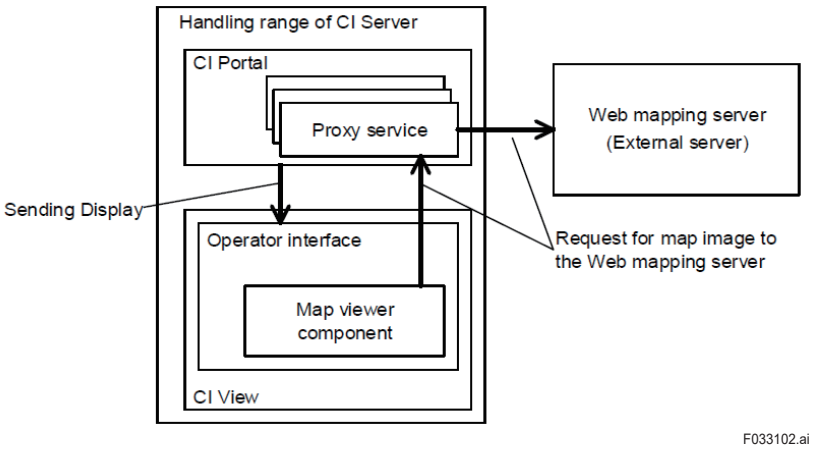


Figure System configuration when map viewer is used

By using a proxy service, Map Viewer can even be used in environments where the Web HMI client cannot connect to external Web server.

In the environment where Web HMI can connect to the external Web Server, map image can be requested directly on the Web mapping server from the Web HMI Client without using proxy server.

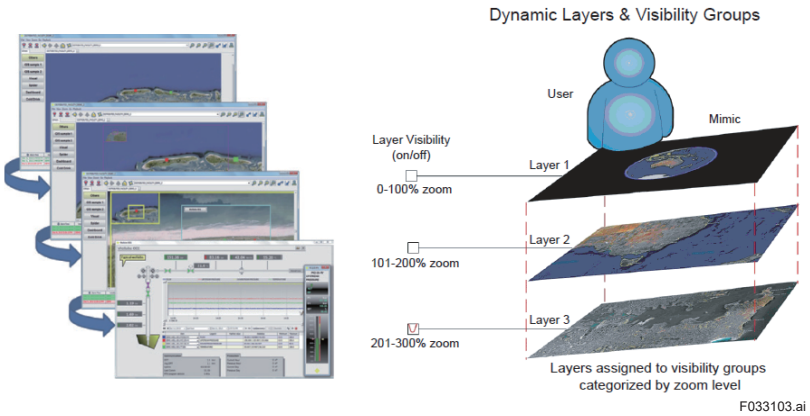
Communication protocol to Web mapping server

Communication protocol to the following Web mapping server is supported.

- Operator Interface
- HTML display
  OGC specification version 1.3

With this method, CI Server can provide an integrated environment in which GIS map and CI Server Operator screen can be linked and synchronized and thus the layers of CI Server operator environment can be switched between display and hide. User can perform the following actions:

- Display GIS map on CI Server
- Display process status on GIS map
- Synchronize GIS data on CI Server project



It supports zoom and pan features similar to Google Earth.

Fast and smooth (Performance is high because it changes in a continuous manner and there is no need to open a new window)

Scatter / Converge (Depending on the zoom level of the display, details are displayed one after the other)

3.32 Gas Flow Calculation (AGA)

CI Server is equipped with programming language (CI Server unique language) library for standard calculation of gas flow stipulated by the American Gas Association (AGA).

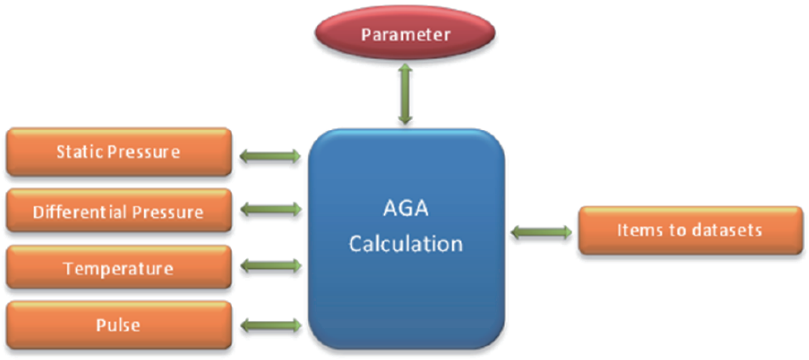
The AGA calculation function includes the following standards:

- AGA3 - Orifice metering of natural gas and related hydrocarbon gases
- AGA7 - Measurement of gas by turbine meters
- AGA8 - Compressibility factors of natural gas and other related hydrocarbon gases
- AGA9 - Measurement of gas by multipath ultrasonic meters
- AGA10 - Speed of sound in natural gas and other related hydrocarbon gases
- AGA11 - Measurement of natural gas by Coriolis meter
- V-Cone - V-cone based natural gas calculation
- Wafer - Cone - Water-cone based natural gas calculation

It includes the following additional calculation function:

Calculation of gross heating value, relative density, and compressibility factor for natural gas mixtures from composition analysis by AGA5 or GPA2172 method.

Calculation of atmospheric pressure depending on latitude and altitude



F033201.ai

The integrated AGA Calculation engine can profile an amount of 1000 calculations show less than a second. An AGA calculation takes less than an average of 0.1 millisecond.

This process is based on legacy PLC/RTU input that is not based on AGA calculation standards.

3.33 EAS (Enterprise Automation Solution)

Enterprise Automation Solution (EAS) provides real-time and historical data from the plant/field level to the enterprise level. Through its unified visualization environment, it provides and combines information from any geographically dispersed asset and enables real-time collaboration and interaction across roles and locations.

For example, it is an effective solution for companies that do business across countries, regions, or on a global scale.

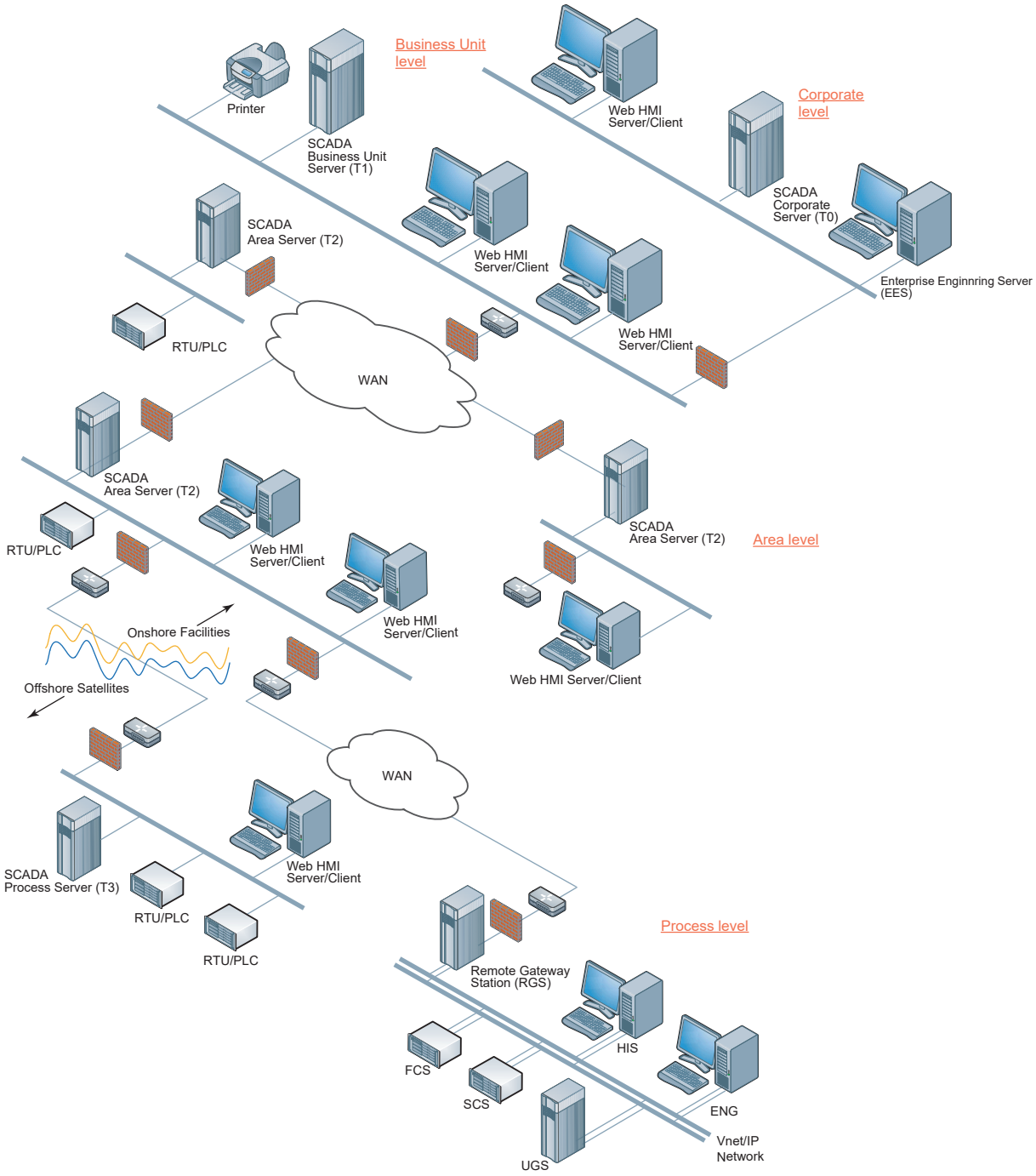
Positioning

For large scale geographically dispersed projects, there may be a hierarchy of individual Process Automation Systems, which in turn are each responsible for a specific region and are managed by a higher-level system. For these applications CI Server provides a flexible, scalable architecture for EAS, by supporting multi-level/multi-node configurations. It is possible to balance server functions over multiple machines, for example for data acquisition or for supporting many HMI clients. This architecture lends itself very well to Enterprise-wide remote operations, - monitoring and - maintenance projects for dispersed production sites and supply chain infrastructures such as oil and gas fields, pipeline grids, water distribution, energy generation, etc.

Enterprise architecture

By placing functional components on multiple computers, large-scale integrated operations monitoring is possible, allowing each business tier to gather only the information it requires.

Example structure:

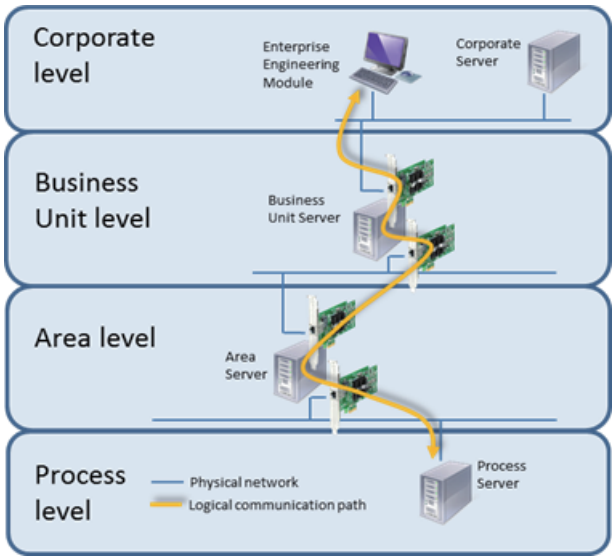

Business Unit level
Printer
SCADA Business Unit Server (T1)
Web HMI Server/Client
Corporate level
SCADA Corporate Server (T0)
Enterprise Enginnring Server (EES)
SCADA Area Server (T2)
Web HMI Server/Client
Web HMI Server/Client
RTU/PLC
WAN
SCADA Area Server (T2)
RTU/PLC
Web HMI Server/Client
SCADA Area Server (T2)
Area level
Web HMI Server/Client
Onshore Facilities
Offshore Satellites
Web HMI Server/Client
WAN
SCADA Process Server (T3)
Web HMI Server/Client
RTU/PLC
RTU/PLC
Process level
Remote Gateway Station (RGS)
HIS
FCS
SCS
ENG
Vnet/IP Network
UGS

F033202.ai

Enterprise operation

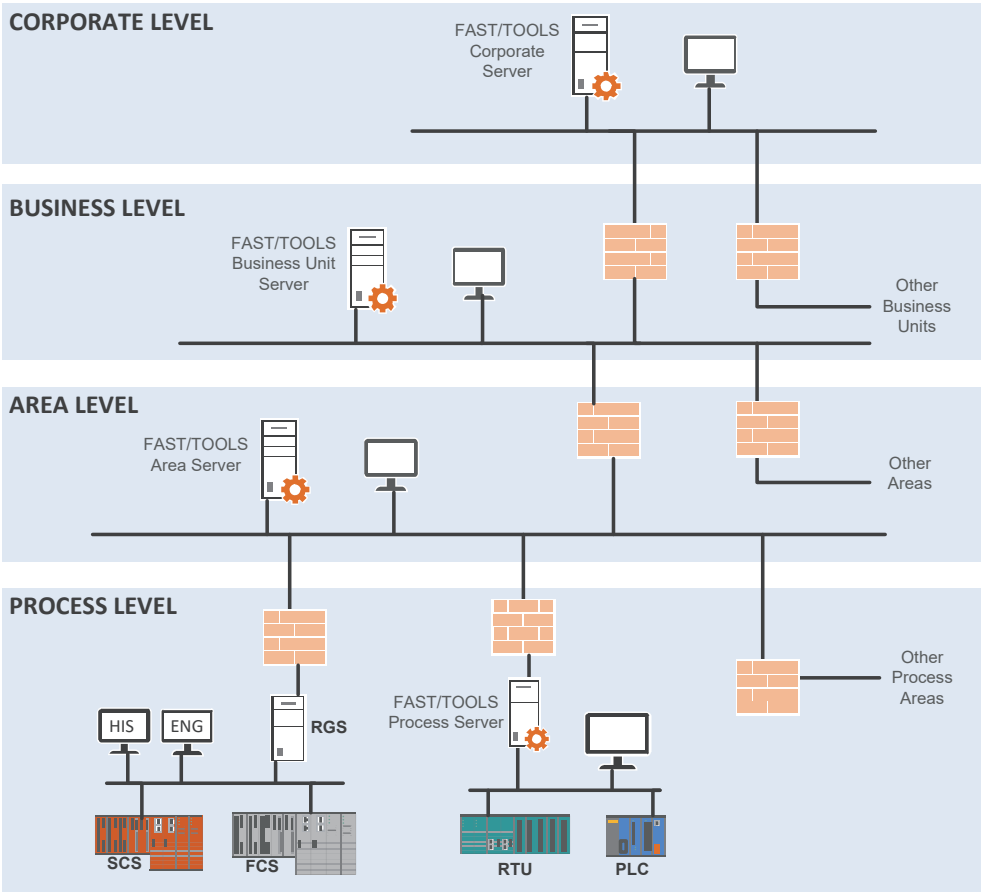
CI Server uses name space server to establish the most optimal path to access data that must be displayed for providing process data at each level. It tries to find alternative paths to the data if access to a certain server is temporarily interrupted. In the figure below, four networks are depicted: The Corporate network, the Business Unit network, the Area network, and the Process network. These networks can be one physical network where the sections are separated by routers and firewalls. In such cases, Business Unit server may have two network cards, one that connects the server to the Business Unit network, and one that connects the Business unit server to the Corporate network.

When a server is added to the physical network at any level, then the logical automation network will discover this and update its routing tables with the new server.

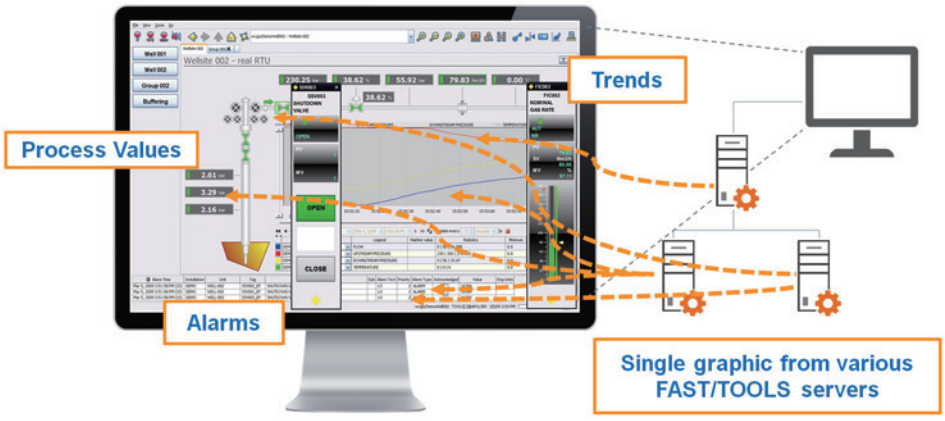


F033203.ai

In the figure above a logical connection between an Enterprise Operation Module located at the corporate level and one of the process servers from which its visualization environment is gathering information from is shown. This allows the Enterprise Operations Module to connect to multiple CI Servers across several levels and to visualize the gathered information in one Mimic as illustrated here below.



F033204.ai



F033204.ai

Enterprise engineering

Engineering multiple servers is required in the enterprise structure. Enterprise engineering server is provided for performing engineering of multiple servers on a single server.

3.34 Alarm System Performance Analysis (ASPA)

The Alarm System Performance Analysis tool is an application that analyses and reports alarm history data. Hereinafter referred as ASPA.

This tool can be used for the following purposes:

- Identify alarms with high occurrence frequency.
- Recognize alarm patterns.
- Evaluate load on operator caused by alarms.
- Evaluate operator response (acknowledge alarms) on alarms.
- Assist reconstructing events that occurred in the past.
- Compare alarm occurrences and responses for similar control periods.

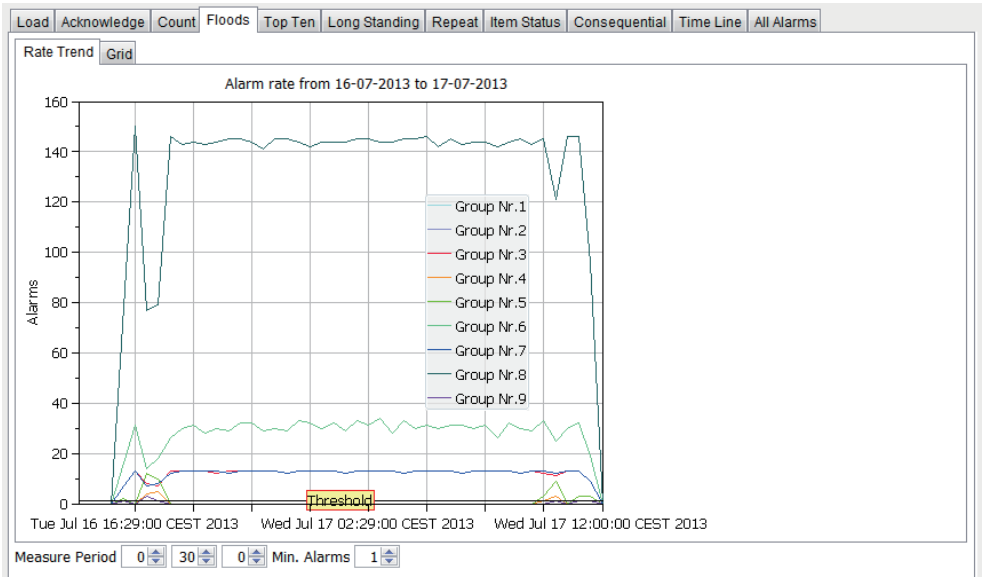
ASPA analyses the performance based on the guidelines of EEMUA 191 directives and the ISA 18.2 standard that ensures quality and result of alarm systems. ASPA supports the alarm system performance improvement processes to avoid operator overload and reduce the risk of critical alarms being overlooked, causing wrong or to late decisions putting safety as well as the continuity and quality of production at stake.

Major analysis items:

- Operator load KPI (EEMUA191 section 4.1.1)
- Operator load performance (EEMUA191 section 4.1.2)
- Alarm rate and alarm flooding (EEMUA191 appendix A12.7)
- Top 10 causes of alarms (EEMUA191 appendix A12.6)
- Prolonged alarms (EEMUA191 appendix A12.8)
- Interrelation of critical alarms (EEMUA191 appendix A12.11)

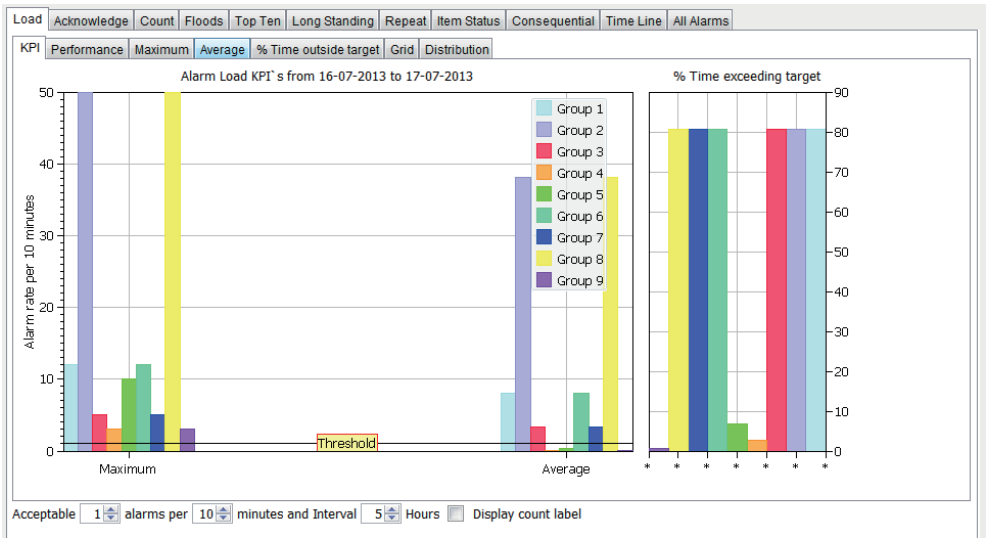
ASPA metrics are the basis in the assessment of whether operators will find the alarm system easy to work with and does not exceed the ergonomically acceptable workload and quality.

Display example of alarm flooding



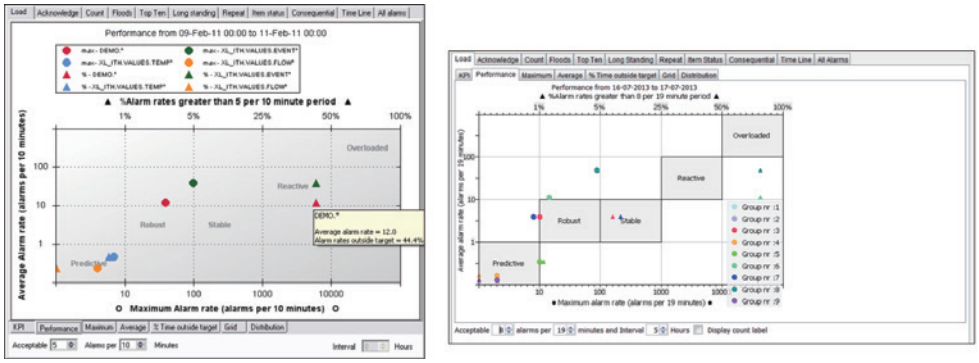
F033401.ai

Display example of operator load status



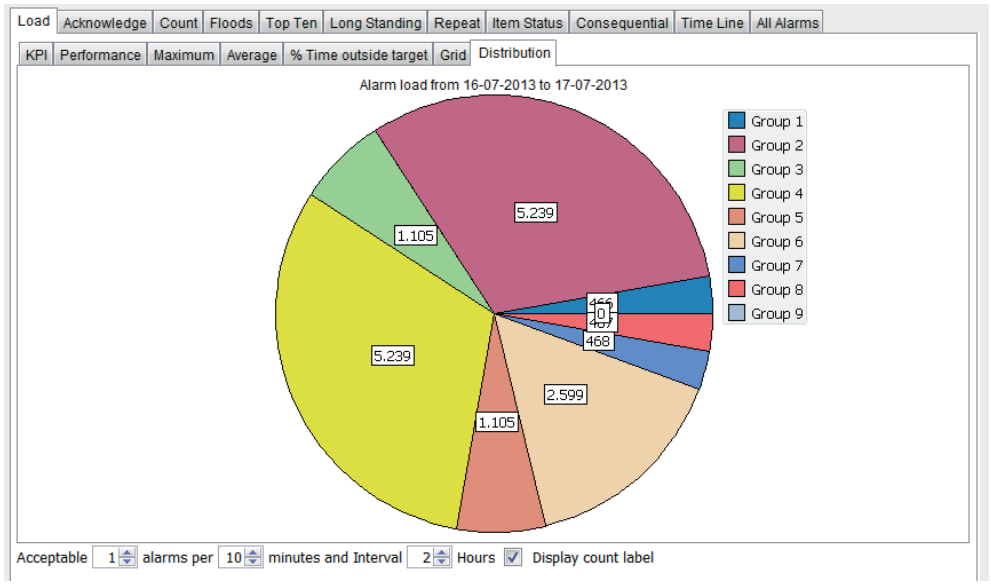
F033402.ai

Display example of operator load performance



F033403.ai

Display example of alarm distribution



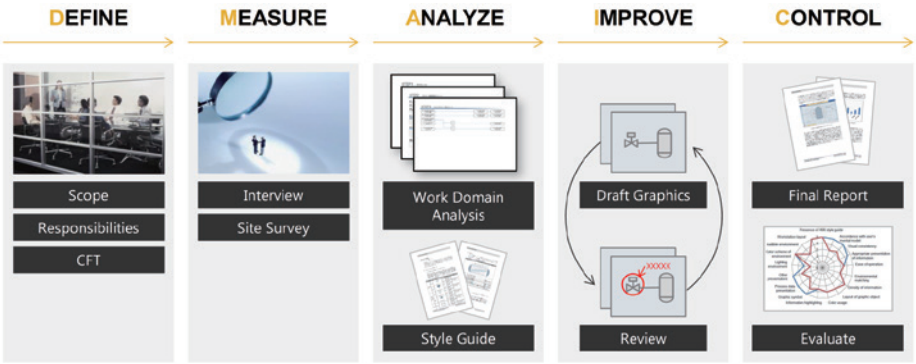
F033404.ai

3.35 Advanced Operating Graphics (AOG)

Advanced Operating Graphics (AOG) is a consulting service provided by Yokogawa to design PCS user interface based on human factors and knowledge engineering in order to improve users' situation awareness.

- Identify user, task and functional requirements for operation that require HMI support.
- Analyze the requirements to determine the needs and conditions to meet for the project.
- Provide guidance on designing and developing user interface including display layout, navigation, hierarchy, color pallet, data visualization, etc.
- Submit final report of achievements in the project.

The following figure shows AOG consulting process.



F033501.ai

To support a more effective HMI strategy we have developed a symbol library adopting the ISA-101 philosophies. The ISA-101 standard helps users understand what those concepts mean and how to implement them. It is designed to develop and establish a consistent approach to effective

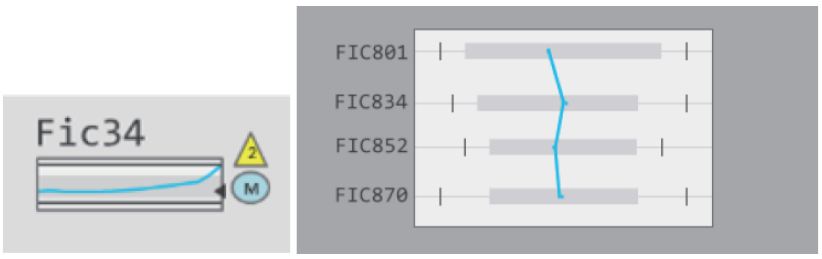
HMI development and implementation for manufacturing and especially process industries. End users, automation suppliers and system integrators can use this standard to create more effective HMIs, which will lead to higher productivity and a safer operating environment.

Therefore, the emphasis is on showing meaningful information rather than just numbers facilitating Advanced Operating Graphics (AOG).

The high-performance HMI is governed by the following principles:

Emphasis on information

Data in general are just numbers. In order to give meaning to those numbers that are useful information for users, context is needed.



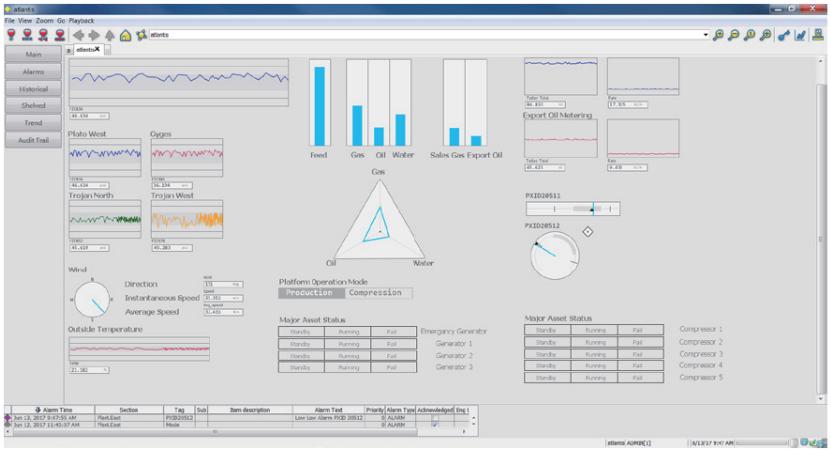
F033502.ai

When data are shown within a context, they become relevant for performing a particular task. Therefore, context and relevance are the keywords to convert data into information.

Seek the operator's attention only when required

Showing a colorful display is difficult for the operator to observe abnormal situations. By limiting the use of color and relevant information, operator can immediately find out what is happening.

AOG symbol library and templates are standards available within the Edit Module.



F033503.ai

For details about AOG consulting service, contact our Business center.

3.36 Playback function

Operator Interface, Engineering Module and Edit Module are equipped with playback function. Menu bar contains [Playback] menu. Recording and playback function of this [Playback] menu can be used to record the display contents on the screen and the operations performed on the device (mouse operations and key inputs). You can also set to start recording automatically.

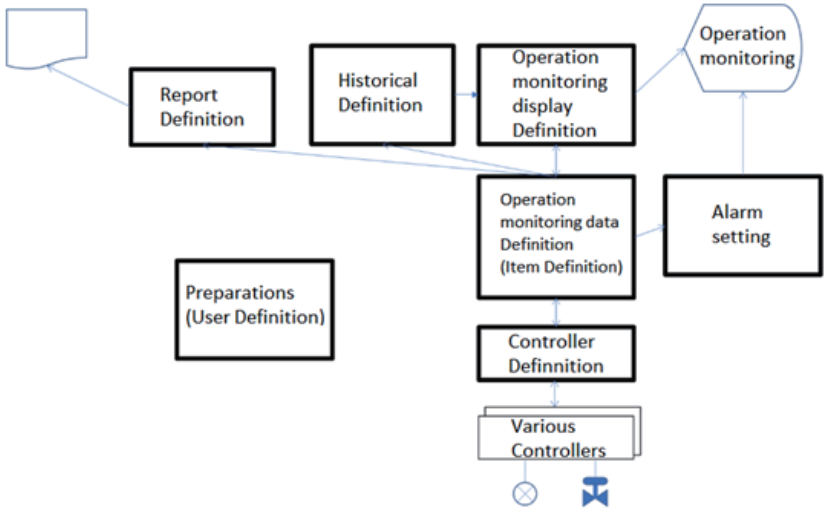
Recordings can be viewed on the Playback Viewer.

4. Functional definition of CI Server (Engineering function)

The functions to be executed by CI server are defined using the CI server engineering functions. Although CI server has a variety of functions, this chapter describes the functions that can be realized in CI server by explaining the items to be defined to realize the basic functions and the CI server engineering functions used for the definitions.

For details about operating methods of engineering functions and items to be defined, refer the IM.

The items defined by using engineering functions for realizing the functions of CI Server are denoted by the thick-framed boxes in the following diagram.



User definition

As an engineering preparation, the users who access CI Server are defined. Operation range and accessible data range can be restricted based on users.

Controller connection

Controller to be connected and the communication protocol to be used for the connection can be selected here. Also, data to be imported to the CI server from the data handled by the controller to be connected is selected here.

Operation monitoring data definition

This section defines the storage location of the operation monitoring data to be handled by the CI server and performs naming of data. It also links the controller data with the operation monitoring data.

Alarm setting

When a limit value is set for an item, alarm is generated when the limit value is crossed. For each item, alarm related operations can be set in detail. In addition to setting limit value, item status and alarm display information such as color and message string on the alarm display screen, and alarm acknowledgement methods can be defined.

Report definition

Format of the output report, report output timing and report output destination can be defined.

Historical definition

Definitions and storage methods of historical data region of item data are defined.

Operation monitoring display definition

Operation monitoring display is created.

Item

External interface

Data collection

HMI

Trend screen

Alarm screen

Historical Reports

Alarms

User management

Security

RDB connection

HostHost connection

OPC Tunneller

OPC-UA

AGA calculation

GIS

MELSEC

Excel Add-in version report

5 Security measures

CI Server consists of IT security function using Windows security function and CI Server specific security function. Also, Yokogawa Endpoint security measures service can also be used.

The functions related to CI Server specific security has encrypted communication, user management and audit trails.

For details about security measures, refer “System product security measures standard (TI 33Y01B30-01)”.

5.1 IT security functions

This function uses Windows OS security function to fortify CI server components. For example, you can set up a Windows Firewall to restrict communication types and port numbers, stop unnecessary services, and control access to folders and files by using the access control function for Windows users and groups.

IT security tool can be used to configure this function. This tool is common to all Yokogawa System products and allows you to configure security with simple operations. The following threats are supported: IT Security Version 2.0 for CI Server R1.01 and later.

Threat	Description
Attack over the network	Threat by unauthorized persons impacting the system or stealing critical data via network
Direct attack through devices	Threat by unauthorized persons operating the devices that impact the system or steal critical data.
Computer/data theft	Threat of computer theft containing important data

The following table shows the types of security measures that can be used.

Security measures	Description
Access control	Restricts access to files, folders, registry, and programs.
Personal firewall settings	Controls the communication among computers over network.
Stopping unused Windows services	Stops unused programs and services.
Modification of IT environment settings.	Enables stable Windows security measures.
Applicable group policy settings	Settings for central management of security policies of computers connected to the same domain.

5.2 CI Server specific security function

The following CI Server specific security functions are available.

Encrypted communication function

The following security measures can be incorporated in the communication routes of CI Server.

- Communication between CI Portal and CI View
  CI View and CI Mobile View displays the operational data via CI Portal. Secure Socket Layer (SSL) can be used in CI Portal to make this data transfer secure.
- Communication between CI Core and CI Core / CI Core and CI Portal

  Communication between servers use industry standard technology that is used for secure internet communication such as DTLS and public/private key encryption.
- OPC UA encrypted communication function
  Secure and highly reliable communication can be established using OPC UA encrypted function.

User management

CI server has security mechanism that recognizes role-based application security. This allows for user management that recognizes functional as well as administrative area privileges, from data reference only privileges to full system configuration privileges. CI server also supports user management through Active Directory (AD).
By mapping the user group on AD to the user group names on CI Server, refined user management is possible. CI Server can also realize single sign on using AD.

The following privileges can be set for users:

- Display, operable screens
- Operable devices and data
- Generatable reports and trends
- Management, notification, and acknowledgement of alarms
- Operation records (automatic or manual)
- Area that can be engineered

For details, refer “User management”.

The following user authentication methods are available:

- CI Server authentication (Windows authentication and combined authentication)
- Combination of Windows user authentication process and account settings

Single SignOn (SSO) can be used by integrating with Active Directory. Uses SPNEGO (Simple and Protected GSS-API Negotiation mechanism) which is the standard user authentication method of Web Server and supports HTTP requested SSO Web authentication.

Audit trails

Operation records for logon/logout records and data are saved as audit trails. Audit trails can be displayed on screen and sent out as reports. Operations and data saved as audit trails can also be defined.
For details, refer “Audit trails”.

5.3 Endpoint security service

Yokogawa endpoint security service can be applied which reduces the risk of malware infection on Windows PCs and servers and supports the maintenance of system health throughout the lifecycle.

- **Yokogawa standard anti-virus software**

  Yokogawa standard anti-virus software is based on McAfee's anti-virus technology and is used as the standard anti-virus software for our control systems. This product is used as the standard antivirus software for our IA systems.

- **Yokogawa standard whitelisting software**

  Yokogawa standard whitelisting software is a whitelisting security countermeasure software that uses McAfee's application control technology and is provided with optimal settings for our control systems. This product is used in our IA systems for anti-fraud services.

  For details, refer "Endpoint security measure service" (GS43D02T30-02).

6 Performance

6.1 Performance reference data

Performance reference value is displayed in the following five types of structure:
A: Standalone type

B: CI View distributed architecture

C: CI Portal / CI View distributed architecture

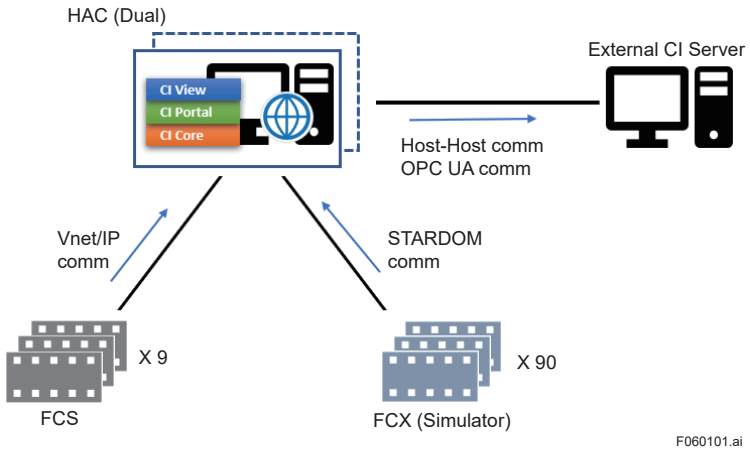
D-1: CI Core / CI Portal / CI View distributed architecture type 1
D-2: CI Core / CI Portal / CI View distributed architecture type 2

*A - D-1 uses HAC and D-2 uses Dual redundant platform

Structure

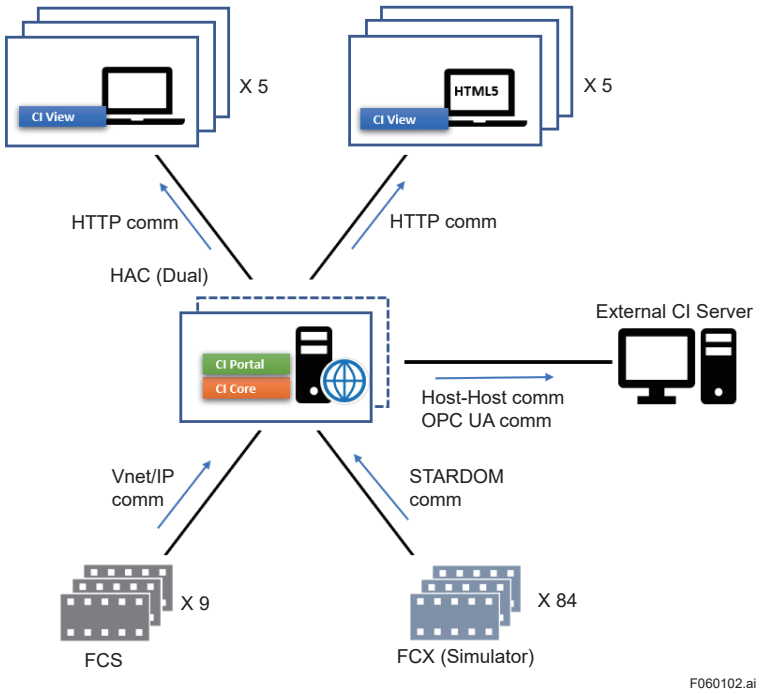
A: Standalone type

Architecture in which CI Core/CI Portal / CI View are installed in the same computer.



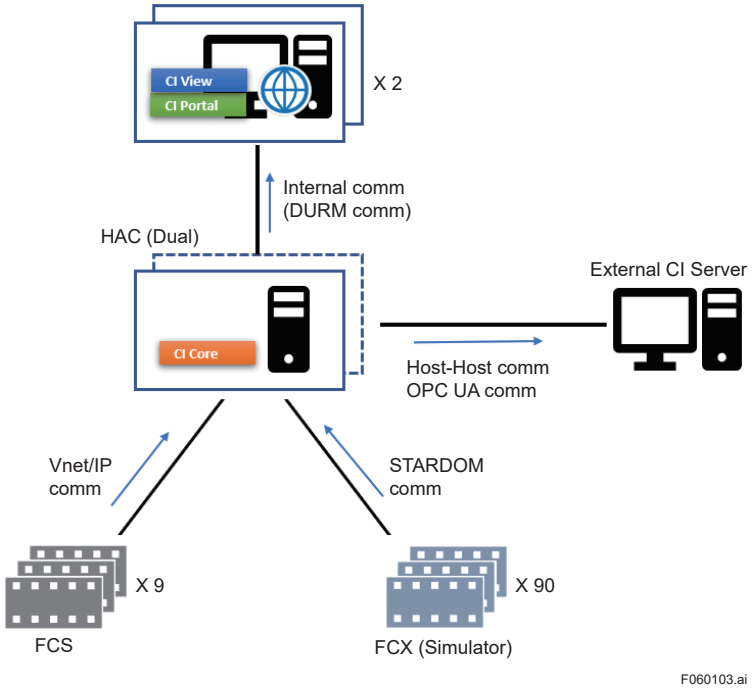
B: CI View distributed structure

Structure in which CI View is placed in a different PC than CI Core/CI Portal combination



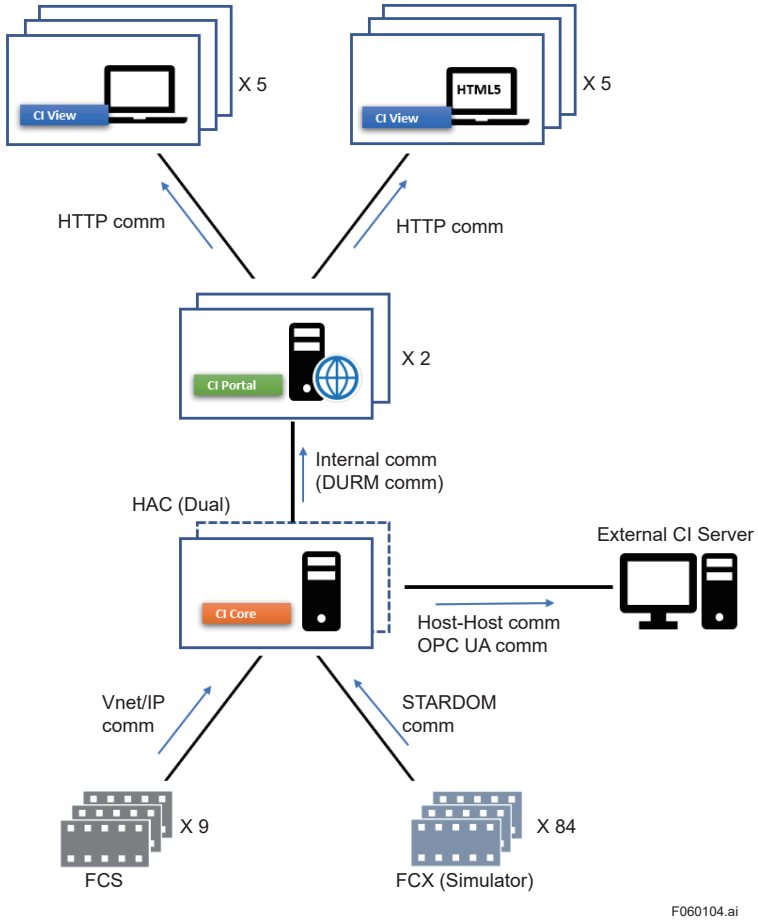
C: CI Portal / CI View distributed structure

Structure in which CI Portal/CI View combination PC is placed in a different PC than CI Core



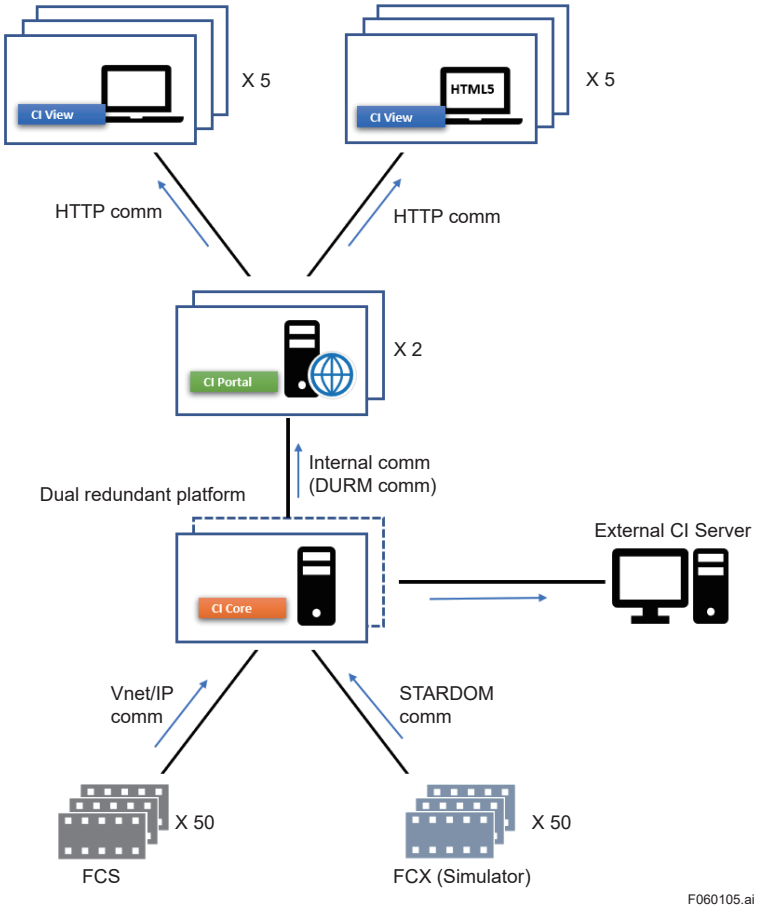
D-1: CI Core, CI Portal and CI View in distributed structure type 1

CI Core, CI Portal, and CI View are installed in separate computers.



D-2: CI Core, CI Portal and CI View in distributed structure type 2

CI Core, CI Portal, and CI View are installed in separate computers. Dual redundant platform is used for redundancy structure.



Performance reference value

		Structure A	Structure B	Structure C	Structure D-1	Structure D-2
		All-in-one (HAC)	CI Core /CI Portal (HAC) | CI View	CI Core (HAC) | CI Portal/CI View	CI Core (HAC) | CI Portal | CI View	CI Core (Redundant PC) | CI Portal | CI View
Item	No. of items	1M	1M	1M	1M	1M
Data collection	Vnet/IP I/O count (points/sec)	4,500	4,500	4,500	4,500	12,500
	STARDOM I/O count (points/sec)	10,500	10,500	10,500	10,500	2,500
	Total I/O count (points/sec)	15,000	15,000	15,000	15,000	15,000
	Line count	20	20	20	20	20
	Stations count: Per line	5 or 4	5 or 4	5 or 4	5 or 4	5
	Station count: Total	93	93	93	93	100
Object	Object count	50,000	50,000	50,000	50,000	50,000
	Trigger (Objects/sec)	5,000	5,000	5,000	5,000	5,000
Alarms	Alarm status change (alarms/sec)	100	100	100	100	20
History	Scan base (items/sec)	5,000	5,000	5,000	5,000	5,000
	Event base (items/sec)	5,000	5,000	5,000	5,000	5,000
External communication	Host-Host communication (send) (items/sec)	1,000	1,000	1,000	1,000	1,000
	OPC UA Server (send) (items/sec)	5,000	5,000	5,000	5,000	5,000
Graphics	C Portal count	1	1	2	2	2
	CI View count: Total	1	5	2	5	5
	CI View count (HTM5): Total	0	5	0	5	5
	Active screen count	5	10	10	30	30
	Active screen count: per screen	500	500	500	500	500
	Active screen count: Total	2,500	5,000	5,000	15,000	15,000

Revision Information

- Title : Collaborative Information Server Product Overview
- Manual No. : TI 36K01A10-01EN

Aug, 2024/3rd Edition
3.8 OPC UA A&C Alarms and CENTUM Alarms [added descriptions]

Apr. 2022/2nd Edition
2.3.1 ● Automatic mode and manual mode [Correction of errors]

Dec. 2021/1st Edition
Newly published

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