General Specifications

GS 33J10D40-01EN

VP6E5170
Access Administrator Package
(FDA:21 CFR Part 11 compliant)

CENTUM VP

[Release 6]

■ GENERAL

Part 11 of Code of Federal Regulations Title 21 (21 CFR Part 11) issued by the United States Food and Drug Administration (FDA) provides criteria and rules of accepting electronic records and electronic signatures as equivalent to paper records and handwritten signatures executed on paper. This regulation enables the use of electronic technology for approvals. Two major functions are required for control systems to comply with the FDA:21 CFR Part 11, which are Access Control Functions and Audit Trail Management Functions.

Access control functions (Personnel authentication)
- Protect systems and data from illegal break-ins
- Control individual operations by authenticating operators, system engineers, report package users, and recipe engineers.

Audit trail management functions
- Record operation, recipe creation, maintenance of report definitions, ands system maintenance histories (When, Who, What, How, Why, Where) automatically.

When applying FDA:21 CFR Part 11 to CENTUM VP, four major categories need to be considered which are; for operators (operation and monitoring functions); for operators (system view/builder); for report users (report package); and for recipe engineers (recipe management function). In this document, the system view/builder and the recipe management function are explained.
As for the operators, operation and monitoring functions are included in VP6H1100 standard operation and monitoring function.

For details of the report package for FDA:21 CFR Part 11, refer to the General Specifications (GS) of the “VP6H6530 Report Package” (GS 33J05J20-01EN).

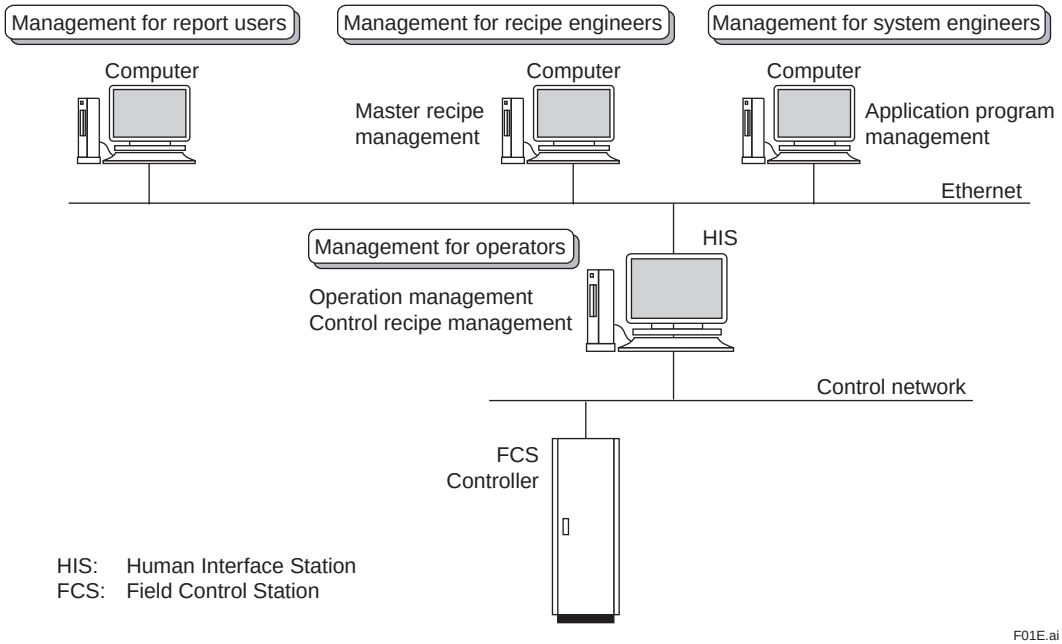


Figure CENTUM VP system configuration

■ FUNCTIONAL SPECIFICATIONS

● Functional Overview

The following shows positioning of the access control function and the audit trail management function.

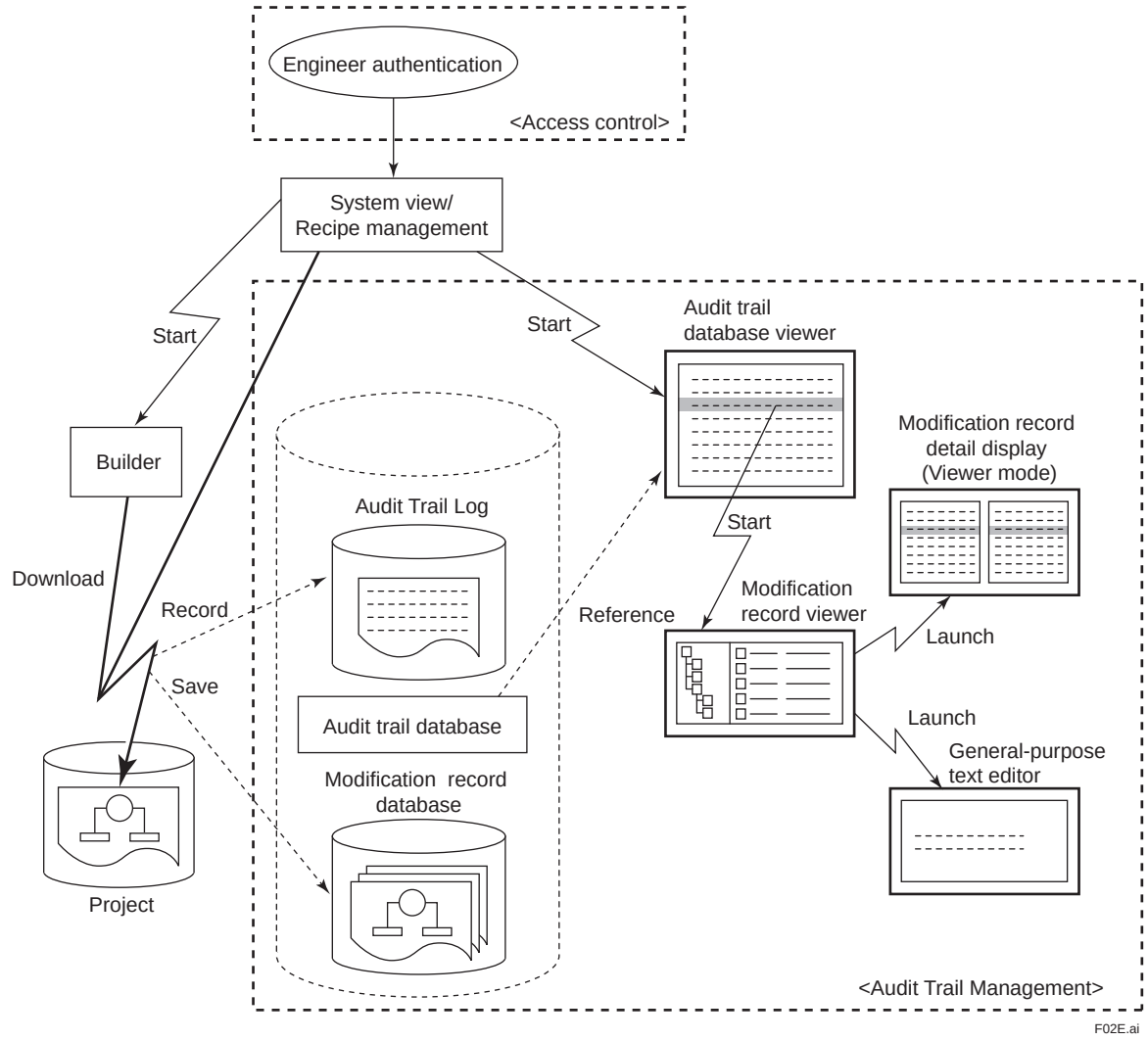
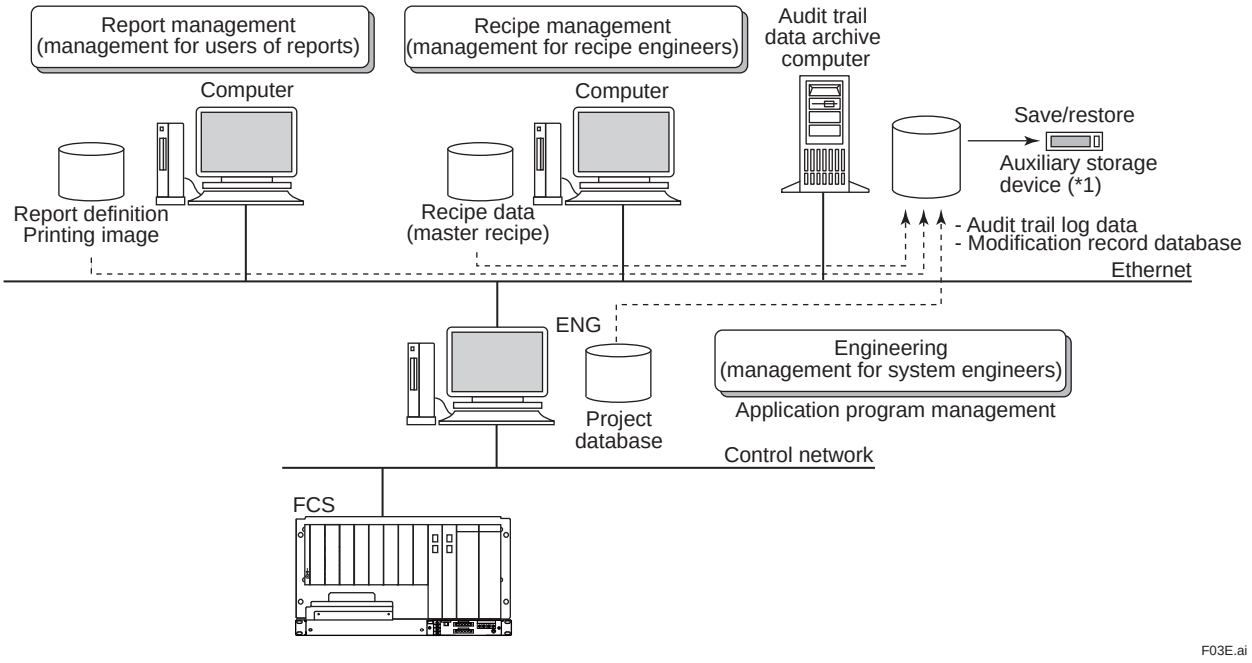


Figure Positioning of the access control function and the audit trail management function

● System Configuration

The recipe management function is performed by using VP Batch functions.



*1: Removable media

Figure System configuration

A computer dedicated for archiving audit trail data has to be prepared. In this computer, refrain from installing the operation and monitoring function, recipe management function, engineering function and such. Depending on the number of computers installed with the builder function or the recipe management package, the audit trail data archive computer has to be a server. For details, refer to the GS of the “Integrated Production Control System CENTUM VP System Overview” (GS 33J01A10-01EN).

In a project with the Recipe management function, the audit trail data archive computer manages historical data of both the engineering and the recipe management.

● System Administrator

When using the Access control function and the Audit trail management function, various settings must be done. These settings can be performed only by a system administrator who has administrator’s authority of the computer, and not by engineers who performs actual engineering. The roles of the system administrator are as shown below:

System Administrator

- Network administration
- Specifying and editing of engineers’ account files
  - Registration of engineers’ names
  - Setting the authority for each engineer group
  - Specifying and updating locations of the audit trail management-database
- Starts and stops audit trail
- Performs audit trail database backup and deletes past engineering data when the database is full
- Viewing the audit trail database

Access Restriction Settings

The table below shows the functions that the system administrator has to set. This table includes the items required by VP6H1100 standard operation and monitoring function and VP6H6530 report package. The functions required for access-control are categorized into four groups:

A: User ID registration management: handling of user IDs and passwords
B: Access control: setting conditions for accessing the system
C: Password policy: conditions of setting passwords, etc.
D: Direct access to Windows: computer's desktop environment

User group		HIS group		Engineering group (system builder, recipe builder, report builder) (*1)
Location		Security builder (*2)	HIS utility (each HIS)	Access control utility (each Computer)
Optional packages required		Not required (included in standard applications)		VP6E5170 packages for FDA 21CFR Part 11
Function				
A	User ID registration and deletion	X (*3)		X
	Authorization setting for each user ID	X (*3)		X
	Password management (Local control/Common control)	X		
B	Automatic user logoff /automatic screen lock	X		X
	Check illegal logon attempts		X (*3)	X
	User lockout		X	X
	User ID release during lockout	X		X
	Password resetting	X		X
	Reconfirmation with double authentication		X (*3)	
	Biometric authentication		X (*4)	
C	Check expiration date of passwords		X (*3)	X
	Check obsolete passwords		X	X
	Check password-length		X	X
D	Automatic logon Windows		X (*3)	X
	CENTUM desktop		X (*3)	X

*1: VP6H6530 Report Package is required in addition to perform report functions.
*2: For operation of the security builder, registration and authorization of an engineer are needed in addition to the system administrator authorization (of the computer).
*3: The System administrator authorization is required.
*4: Contact Yokogawa for details about biometric authentication.

● Managing System Engineer (System view/Builder)

Access control
Access control over the project database can be defined for each system engineer, which enables to assign roles of each system engineer in details.

For instance, system engineer A can modify from one to ten of the FCS0101 drawing files. System engineer B cannot modify FCS data but can create, delete, and modify the entire graphics of HIS.

Unit of access control
The access control is assigned by the computer.

Applicable project of access control
The access control works only for the default or the current project, and not for user-defined project(s).

System engineer group and system engineer
A system engineer group is a fundamental unit for specifying authorities to perform engineering.
All the system engineers must belong to one of the groups and register the engineers' names (ID); passwords; and legal names. The system engineer performs an engineering within the authority entitled to its group.

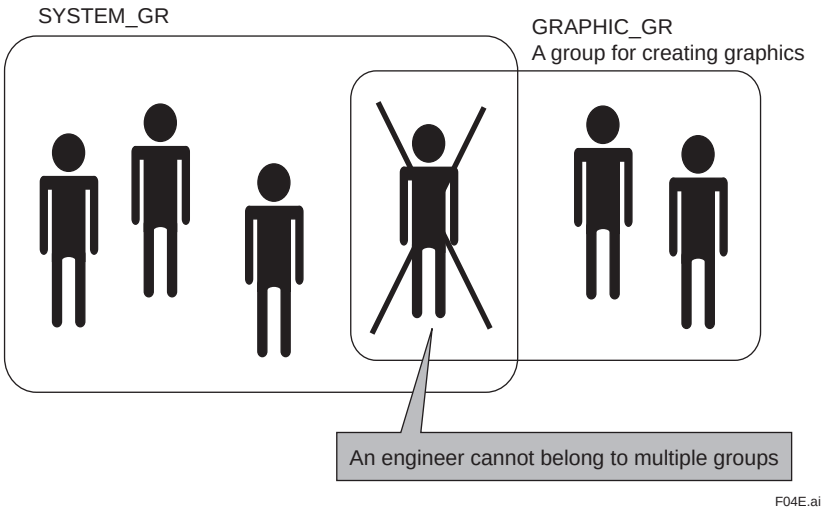


Figure System engineers and engineer groups

Scope of authority
The minimum unit of authorities entitled to a system engineer group is by the builder such as graphics or drawings.

Types of authority

Read:	Reading files is allowed. If only Read is entitled, "Overwrite and Save" or "Download" cannot be selected. An engineering group without Read authority cannot be created.
Write:	Writing into files is allowed. "Save" and "Download" of the existing files can be performed.
Create:	Creating and deleting an object on the System view is allowed. This authority is required for creating stations and deleting windows.

System engineer authentication and Authority check
This function verifies identity of a system engineer and if the system engineer has the authority to perform the tasks.

Table System engineer authentication and the Timing of authority check

Timing	Engineer authentication	Authority check
Logging in to the System View	X	–
Creating and Deleting a project on the System View	– (*2)	X
Starting the Builder	–	X
Overwriting and saving from the Builder (*1)	– (*3)	–
Downloading from the Builder (*1)	X	–
Logging off from the System View	–	–

X: Performed –: Not performed

*1: When starting the Builder, the System View verifies the Write authority of a system engineer. If the engineer does not have the authority, Read Only mode starts, which prevent the engineer from selecting the menu.
*2: The authentication is checked when downloading the project database.
*3: The authentication is checked when downloading to the Builder is not performed.

Audit Trail Management
Modified engineering data is automatically saved in the pre-defined database.

By simultaneously recording the audit trail log the audit trail management provides a method to identify WHEN, WHO, WHAT, HOW, WHY, and WHERE the data is modified. The detailed information on WHAT is changed and HOW it is changed can be confirmed along with the audit trail log.

When the Builder is started in viewing mode after selecting a file to be modified, differences in the Builder can be displayed in different colors. (*1)

*1: The differences cannot be displayed by some Builders. See the table of “Builder view mode functions” for details.

Audit trail management policy (Recording timing)
The audit trail management in CENTUM VP is to save the modified data to the pre-assigned database only when the engineering that affects the product quality is performed (downloading to the target machine). At the same time, the data is saved in the Audit trail log file.

Saving modified data of the current project
The modified data is saved in the default or current project. The engineering data under the user-defined project is not saved.

Out of scope of Builder
Fieldbus Tools and OPC

Table Builder Functions in View Mode (1/2)

Project Hierarchy	Builder Name	Supported Functions	
		Difference Display	Other Functions
Project Common	Station configuration	X	–
	System-fixed status character string	X	–
	Security	X	–
	Alarm priority	X	–
	Alarm processing table	X	–
	Alarm status character string	X	–
	Block status character string	X	–
	Plant hierarchy	X	–
	Engineering unit symbol	X	–
	Switch position label	X	–
	Multiple project connection	X	–
	Operation mark	X	–
	Tag name hierarchy	–	--
	Status change command character string	X	–
	CAMS for HIS alarms	–	--
	CAMS for HIS alarm group	–	--
	CAMS for HIS message monitor definition	–	--
	CAMS for HIS shelf	–	--
	State transition matrix	X	–
	Buzzer assignment	X	–
BATCH	Process management configuration	X	–
	Unit common block	X	–
	Common block	X	–
	Product control	–	–
	Train	X	–
FCS	FCS constants	X	–
	Process cell	X	–
	SEBOL	–	–
	SFC sequence	–	–
	Unit procedure	–	–
	IOM (other than Fieldbus)	Δ (*1)	–
	Fieldbus	Δ (*2)	–
	Communication input/output	X	–
	Extended communication input/output	X	--
	Global switch	X	–
	Common switch	X	–
	Communication input/output Tag	X	–
	Extended communication input/output tag	X	---
	Annunciator	X	–
	Signale	X	–
	Operator guide	X	–
	Print message	X	–
	Drawing	–	Detail Start
	Function block overview	Δ (*3)	Detail Start
	Function block detail	Δ (*4)	–
	Drawing/Logic chart status display (option)	–	–

X: Supported Δ : Partly supported –: Not supported

*1: The differences of the detailed setting information of each terminal cannot be displayed.
*2: The differences of the block parameters of Fieldbus blocks cannot be displayed
*3: The differences of the details of each function block cannot be displayed.
*4: The differences in sequence tables, general-purpose arithmetic expressions, logic charts, SFC, and SEBOL cannot be displayed.

Table Builder Functions in View Mode (2/2)

Project Hierarchy	Builder Name	Supported Functions	
		Difference Display	Other Functions
HIS	Assign function keys	X	–
	Sequence message request	X	–
	HIS constants	X	–
	Panel set	X	–
	Scheduler	X	–
	Trend acquisition pen assignment	–	–
	Graphic	–	–
	Help	–	–
STN	Tag-list generation (Operator guide message)	X	–
	Tag-list generation (Print message)	X	–
	Tag-list generation (Sequence message)	X	–
	Tag-list generation (Tag name)	X	–
	Tag-list generation (Area name)	X	–

X: Supported –: Not supported

● Recipe engineer management (Recipe management)

Access Control
Access to create and modify Master recipe for each recipe engineer can be specified.

Unit of access control
The access control is performed for each computer.

Subject to access control
The access control for the recipe management is performed for all the projects. The project attributes in the engineering functions do not affect.

Recipe engineer group and Recipe engineer
A recipe engineer group is a fundamental unit for specifying the authorities to operate the recipe management functions. All recipe engineers must belong to one of the groups and register the recipe engineer's name, password, and legal name. The recipe engineer can operate the recipe management functions by the authority given to the recipe engineer group.

Scope of authority
The authority entitled to the recipe engineer group is a project at the maximum and a recipe as the minimum. Subgroups are out of scope of the authority.

Types of authority
The recipe engineers are entitled to use the following authorities.

Read (*1): Start the recipe builder/recipe procedure builder and view recipes and recipe operations. The recipe builder and recipe procedure builder are for read-only.
Write: Create and edit recipes and recipe operations. Deleting and downloading of recipes and recipe operations are not allowed. Create, delete, and edit of projects and recipe groups are not allowed.
Delete: Delete recipes and recipe operations. Downloading of a recipe is not allowed. Create, delete, and edit of projects and recipe groups are not allowed.
Download: Download recipes from the Recipe view and the Recipe builders. Create, delete, and edit projects and recipe groups are not allowed.
Engineering (*2):
Create, delete, and edit projects and recipe groups; and delete all the recipe operations. Start the recipe builder/recipe procedure builder and view recipes. Create, edit, delete, and download recipes are not allowed.

*1: All recipe engineers are automatically entitled the Read authority and the scope of the authority cannot be set.
*2: The engineering authority can be used in combination with recipe-related authorities such as Read, Write, Delete and Download. (e.g. A recipe engineer with the engineering and the download authorities)

Recipe engineer authentication and rights check
When the recipe engineer performs the recipe management, the system checks the engineer's identification and checks if the engineer has the appropriate authority (right) to perform the task. The timing of the authority check is as shown below.

Table Recipe engineer authentication and the timing of rights check

Timing	Recipe engineer authentication	Rights check
Logging onto recipe view	X	–
Creating and deleting projects or recipe groups in the recipe view Change of properties Deleting all the recipe operations	X	X
Creating and deleting a recipe/recipe operation in the recipe view	–	X
Starting recipe related builders	–	X
Saving files in recipe related builders	–	X
Downloading	X	X
Logging off from recipe view	–	–

X: Performed –: Not performed

Audit trail management
Modified recipe data is automatically saved in the pre-defined database.

By simultaneously recording the audit trail log the audit trail management provides a method to identify WHEN, WHO, WHAT, HOW, WHY, and WHERE the data is modified. The detailed information on WHAT is changed and HOW it is changed can be confirmed along with the audit trail log.

When the Builder is started in viewing mode after selecting a file to be modified, differences in the Builder can be displayed in different colors. (*1)

*1: The differences cannot be displayed by some Builders. See the table of "Builder view mode functions" for details.

Audit trail management policy (Recording timing)
The audit trail management in CENTUM VP is to save the modified data to the pre-assigned database only when the engineering that affects the product quality is performed (downloading to the target machine). At the same time, the data is saved in the Audit trail log file.

Saving modified data of the current project
The modified data of all the projects is saved.

Table Builders in viewer mode functions

Project level	Builder name	Supported functions	
		Difference display	Other functions
Recipe	Recipe builder	X	–
	Recipe procedure builder	–	–

X: Supported –: Not supported

■ OPERATING ENVIRONMENT

● Hardware requirements

Hardware requirements for running the VP6E5170 Access administrator package are as the same as for VP6E5100 Standard engineering function.

For a computer to save the audit trail database, a hard disk with sufficient capacity (e.g. 40 GB or larger) is recommended.

An external storage medium for saving backup of the audit trail database is also required.

● Software requirements

Software requirements for running the VP6E5170 Access administrator package are as the same as for the VP6E5100 Standard engineering function.

Access Administrator Package (FDA:21 CFR Part 11 compliant) can be used with VP6E5100 Standard engineering function. This package can also be used with VP6H6530 Report package or VP6E5166 Recipe management package.

Adobe Acrobat is required to convert the audit trail management data base into PDF files.

Refer to the GS of the “Standard Engineering Function” (GS 33J10D10-01EN) for software requirements of the Adobe Acrobat.

■ MODELS AND SUFFIX CODES

		Description
Model	VP6E5170	Access Administrator Package (FDA:21 CFR Part 11 compliant)
Suffix Codes	-V	Software license
	1	Always 1
	1	English version

Note: VP6E5110 Access control package is not required as it is included in the VP6E5170.

■ ORDERING INFORMATION

Specify model and suffix codes.

■ TRADEMARK ACKNOWLEDGMENT

The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.