

Engineering Guide

IM 32Q01C10-31E

vigilantplant[®]

Introduction

This document is the engineering guide of ProSafe-RS.

This document explains the overview of ProSafe-RS system, the points at the engineering, and the cautionary notes. This document also explains how to design, make, operate, and maintain a safety system using ProSafe-RS, based on the workflow of engineering.

See the Appendix for the terminology in the descriptions of ProSafe-RS.

When using Vnet/IP-Upstream network in the Standard or the Wide-area mode in FAST/TOOLS integrated environment, see section 2.23. For integrating FAST/TOOLS by using SCS57, see Chapter 9.

Notes and precautions regarding the safety control station for Vnet/IP (SCSP1) described in this document also apply to the safety control station for upstream systems (SCSU1).

1. Procedure for Engineering

This chapter explains an outline for the entire engineering of ProSafe-RS.

2. Design of Applications

This chapter explains important issues to consider in designing application of ProSafe-RS system.

3. Creating a New Application

This chapter explains the procedure for creating a new application.

4. Test of Application

This chapter explains the procedure for testing applications.

5. Online Change of Applications

This chapter explains the procedure for Online change of applications.

6. Installation and Start-up

This chapter explains the installation of ProSafe-RS system, the connection to field devices, a procedure of start-up including tests, commissioning and precautions for the start-up.

7. Operation and Maintenance

This chapter explains actions in an emergency, a procedure for collecting information in SOE (Sequence of Events) and a procedure for maintaining the equipment of ProSafe-RS (including I/O modules) and field devices and considerations.

8. Self Document

This chapter explains the Self Document Function.

9. Engineering Works for FAST/TOOLS Integrated System Using SCSU1

This chapter describes the system configuration and the operating environment when setting Vnet/IP-Upstream network as the Narrowband mode in FAST/TOOLS integrated system, the buffering function and the gas flow rate calculation function that can be used in SCSU1, tests, and the maintenance method.


10. Engineering for ProSafe-SLS Communication Function


The ProSafe-RS can communicate with the ProSafe-SLS using subsystem communication. This section describes an overview for each engineering of ProSafe-RS and ProSafe-SLS systems. When performing engineering on the CENTUM integration, you can also monitor the ProSafe-SLS from the CENTUM Integrated System.


Safety Precautions for Use

■ Safety, Protection, and Modification of the Product

- To protect the system controlled by the Product and the Product itself and to ensure safe operation, please observe the safety precautions described in this Manual. Yokogawa Electric Corporation ("YOKOGAWA") assumes no liability for safety if users fail to observe the safety precautions and instructions when operating the Product.
- If the Product is used in a manner not specified in the User's Manuals, the protection provided by the Product may be impaired.
- If any protection or safety circuit is required for the system controlled by the Product or for the Product itself, please install it externally.
- Use only spare parts that are approved by YOKOGAWA when replacing parts or consumables of the Product.
- Do not use the Product and its accessories such as power cords on devices that are not approved by YOKOGAWA. Do not use the Product and its accessories for any purpose other than those intended by YOKOGAWA.
- Modification of the Product is strictly prohibited.
- The following symbols are used in the Product and User's Manuals to indicate the accompanying safety precautions:

 Indicates that caution is required for operation. This symbol is labeled on the Product to refer the user to the User's Manuals for necessary actions or behaviors in order to protect the operator and the equipment against dangers such as electric shock. In the User's Manuals, you will find the precautions necessary to prevent physical injury or death, which may be caused by accidents, such as electric shock resulting from operational mistakes.

 Identifies a protective conductor terminal. Before using the Product, you must ground the protective conductor terminal to avoid electric shock.

 Identifies a functional grounding terminal. A terminal marked "FG" also has the same function. This terminal is used for grounding other than protective grounding. Before using the Product, you must ground this terminal.

 Indicates an AC supply.

 Indicates a DC supply.

 Indicates the ON position of a power on/off switch.

 Indicates the OFF position of a power on/off switch.

■ Notes on Handling User's Manuals

- Hand over the User's Manuals to your end users so that they can keep the User's Manuals on hand for convenient reference.
- Thoroughly read and understand the information in the User's Manuals before using the Product.
- For the avoidance of doubt, the purpose of the User's Manuals is not to warrant that the Product is suitable for any particular purpose but to describe the functional details of the Product.
- Contents of the User's Manuals are subject to change without notice.

-
- Every effort has been made to ensure the accuracy of contents in the User's Manuals. However, should you have any questions or find any errors, contact us or your local distributor. The User's Manuals with unordered or missing pages will be replaced.

■ Warning and Disclaimer

- Except as specified in the warranty terms, YOKOGAWA shall not provide any warranty for the Product.
- YOKOGAWA shall not be liable for any indirect or consequential loss incurred by either using or not being able to use the Product.

■ Notes on Software

- YOKOGAWA makes no warranties, either expressed or implied, with respect to the Software Product's merchantability or suitability for any particular purpose, except as specified in the warranty terms.
- Purchase the appropriate number of licenses of the Software Product according to the number of computers to be used.
- No copy of the Software Product may be made for any purpose other than backup; otherwise, it is deemed as an infringement of YOKOGAWA's Intellectual Property rights.
- Keep the software medium of the Software Product in a safe place.
- No reverse engineering, reverse compiling, reverse assembling, or converting the Software Product to human-readable format may be performed for the Software Product.
- No part of the Software Product may be transferred, converted, or sublet for use by any third-party, without prior written consent from YOKOGAWA.

Documentation Conventions

■ Symbols

The following symbols are used in the User's Manuals.



CAUTION

Identifies instructions that must be observed to avoid physical injury, electric shock, or death.



WARNING

Identifies instructions that must be observed to prevent damage to the software or hardware, or system failures of the Product.



IMPORTANT

Identifies important information required to understand operations or functions.

TIP

Identifies additional information.

**SEE
ALSO**

Identifies referenced content.

In online manuals, you can view the referenced content by clicking the links that are in green text. However, this action does not apply to the links that are in black text.

■ Typographical Conventions

The following typographical conventions are used throughout the User's Manuals.

● Commonly Used Conventions throughout the User's Manuals

- **Δ Mark**
Indicates that a space must be entered between character strings.
Example:

```
.ALΔPIC010Δ-SC
```

- **Character string enclosed by braces { }**
Indicates character strings that may be omitted.

Example:

```
.PRΔTAG{Δ.sheet name}
```

● Conventions Used to Show Key or Button Operations

- **Characters enclosed by brackets []**
When characters are enclosed by brackets in the description of a key or button operation, it indicates a key on the keyboard, a button name in a window, or an item in a list box displayed in a window.

Example:

To alter the function, press the [ESC] key.

● Conventions of a User-defined Folder

- **User-defined folder name enclosed by parenthesis ()**
User definable path is written in a pair of parentheses.

Example:

```
(RS Project Folder)\SCS0101
```

If the RS Project Folder is C:\MYRSPJT, the above path becomes C:\MYRSPJTSCS0101.

■ Drawing Conventions

Drawings used in the User's Manuals may be partially emphasized, simplified, or omitted for the convenience of description.

Drawings of windows may be slightly different from the actual screenshots with different settings or fonts. The difference does not hamper the understanding of basic functionalities and operation and monitoring tasks.

■ Integration with CENTUM

The Product can be integrated with CENTUM VP or CENTUM CS 3000. In the User's Manuals, the integration with CENTUM VP or CENTUM CS 3000 is referred to as "Integration with CENTUM."

In the User's Manuals, the explanations for integrating the Product with CENTUM VP or CENTUM CS 3000, the glossary for various features of CENTUM VP is used instead of the glossary for CENTUM CS 3000. For example, the term "CENTUM VP System Alarm View" is used instead of "CENTUM CS 3000 System Alarm window." Nevertheless, if the features for integrating the Product with CENTUM VP and CENTUM CS 3000 are different, both features will be explained separately.

SEE ALSO

For more information about the functions and usage of CENTUM VP components for integrating the Product with CENTUM VP, refer to:

User's Manuals (IM), Technical Information (TI), and General Specifications (GS) of CENTUM VP

For more information about the features and usage of CENTUM CS 3000 components for integrating the Product with CENTUM CS 3000, refer to:

User's Manuals (IM), Technical Information (TI), and General Specifications (GS) of CENTUM CS 3000

■ Explanation of Hardware and Software Behaviors in the User's Manuals

In the User's Manuals, system behaviors are explained assuming that the latest versions of YOKOGAWA software and hardware at the time of publication of the User's Manuals are installed.

If additional precise information about the safety of legacy versions of software or hardware is required, a link to the corresponding explanation is provided. Please refer to the information according to your system.

■ Station Types

A safety control station (hereafter referred to as SCS) is named according to the type of the safety control unit used in it.

Table Info-1 Names of SCS and Safety Control Unit Used

Name of SCS	Model of the safety control unit
SCSV1-S	SSC10S/SSC10D
SCSP1-S	SSC50S/SSC50D
SCSP2-S	SSC60S/SSC60D
SCSU1-S	SSC57S/SSC57D

In the User's Manuals, the following abbreviations may be used to describe functions of these SCS as a whole.

- SCSV1: Abbreviation of SCSV1-S
- SCSP1: Abbreviation of SCSP1-S
- SCSP2: Abbreviation of SCSP2-S
- SCSU1: Abbreviation of SCSU1-S

Copyright and Trademark Notices

■ All Rights Reserved

The copyright of the programs and online manuals contained in the software medium of the Software Product shall remain with YOKOGAWA.

You are allowed to print the required pages of the online manuals for the purposes of using or operating the Product; however, reprinting or reproducing the entire document is strictly prohibited by the Copyright Law.

Except as stated above, no part of the online manuals may be reproduced, transferred, sold, or distributed to a third party in any manner (either in electronic or written form including, without limitation, in the forms of paper documents, electronic media, and transmission via the network). Nor it may be registered or recorded in the media such as films without permission.

■ Trademark Acknowledgments

- CENTUM, ProSafe, Vnet/IP, and STARDOM are registered trademarks of YOKOGAWA.
- Microsoft, Windows, Windows Vista, Windows Server, Visual Basic, Visual C++, and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.
- Adobe, Acrobat, and Adobe Reader are registered trademarks of Adobe Systems Incorporated.
- Ethernet is a registered trademark of Xerox Corporation.
- HART is a registered trademark of the HART Communication Foundation.
- Modicon and Modbus are registered trademarks of Schneider Electric SA.
- All other company and product names mentioned in the User's Manuals are trademarks or registered trademarks of their respective companies.
- TM or ® mark are not used to indicate trademarks or registered trademarks in the User's Manuals.
- Logos and logo marks are not used in the User's Manuals.

Engineering Guide

IM 32Q01C10-31E 4th Edition

CONTENTS

1.	Procedure for Engineering.....	1-1
1.1	Outline of the Entire Engineering.....	1-2
1.2	Classification of SCS Application.....	1-9
1.3	Type of Project.....	1-10
1.4	System Generation Function.....	1-14
1.5	Maintenance Function.....	1-20
2.	Design of Applications.....	2-1
2.1	System Configuration.....	2-2
2.1.1	Overview of the System Configuration.....	2-3
2.1.2	IT Security.....	2-18
2.2	Hardware Configuration.....	2-20
2.3	Requirements for the Size of System and Installation of Hardware.....	2-30
2.4	Overview of POU.....	2-33
2.5	Structured Text.....	2-41
2.6	Capacity of SCS Applications.....	2-45
2.7	Performance and Scan Period in SCS.....	2-47
2.8	Inter-SCS Safety Communication.....	2-51
2.9	SCS Link Transmission.....	2-57
2.10	Diagnosis Function of SCS.....	2-65
2.11	Monitoring Process and System.....	2-71
2.12	Security.....	2-73
2.12.1	Security for Access to SCS.....	2-74
2.12.2	Security for Project Database.....	2-80
2.12.3	Security for the SCS Maintenance Support Tool.....	2-81
2.13	Access Control / Operation History Management Functions.....	2-83
2.14	Configuration of the SOER.....	2-92
2.14.1	Event Collection Function.....	2-93
2.15	Time Synchronization.....	2-95
2.16	CENTUM Integration.....	2-97
2.17	Connection with Other Systems via Communication Modules.....	2-103
2.17.1	Subsystem Communication Function.....	2-104
2.17.2	Overview of Modbus Slave Communication Function.....	2-108
2.17.3	DNP3 Slave Function.....	2-110

2.18	Connection with Host System Computer via an OPC Server.....	2-115
2.19	Version Control.....	2-118
2.20	Import/Export Function.....	2-120
2.20.1	Precautions Concerning Import/Export.....	2-121
2.20.2	Data Transfer Procedure During Expansions/Remodeling in Modifications where Online Change is Possible.....	2-126
2.20.3	Data Transfer Procedure During Expansions/Remodeling in Modifications Requiring Offline Download.....	2-129
2.20.4	Data Transfer Procedure During SCS Project Regeneration.....	2-131
2.21	System Reaction Time.....	2-135
2.22	HART Communication.....	2-138
2.22.1	Description.....	2-139
2.22.2	PST Engineering.....	2-141
2.23	FAST/TOOLS Integrated Configuration.....	2-143
3.	Creating a New Application.....	3-1
3.1	Procedure of Creating a New Application.....	3-2
3.2	Precautions for Engineering.....	3-9
3.3	Guideline on Creating Application Logic.....	3-15
3.3.1	Use of Analog Input Value.....	3-16
3.3.2	Shutdown due to Channel Failure.....	3-21
3.3.3	Example of Displaying I/O Status.....	3-26
3.3.4	Relations among AIO/DIO, Communication Module and System FBs.....	3-27
3.3.5	Example of Using Bool-type Data Manual Operation Function Block (MOB_*).....	3-28
3.3.6	Construction Example of First-up Alarm Function.....	3-31
4.	Test of Application.....	4-1
4.1	Types of Test.....	4-2
4.2	SCS Simulation Test.....	4-8
4.3	Procedures for Testing.....	4-15
4.3.1	Operation of SCS Simulation Test.....	4-16
4.3.2	Operation of Logic Simulation Tests.....	4-18
4.3.3	Operation of Target Tests (When Online Change is not Executable).....	4-19
4.3.4	Operation of Target Test (When Online Change is Executable).....	4-20
4.4	Precautions for Tests.....	4-21
5.	Online Change of Applications.....	5-1
5.1	Entire Procedure of Online Change of Application.....	5-2
5.2	List of Applicable Items for Online Change.....	5-10
5.3	Precautions for Online Change.....	5-16
6.	Installation and Start-up.....	6-1
6.1	Procedure of Installation and Start-up.....	6-2

7.	Operation and Maintenance.....	7-1
7.1	Operation.....	7-2
7.1.1	Operation in an Emergency.....	7-3
7.1.2	Analyzing Events (SOE Viewer).....	7-6
7.2	Maintenance.....	7-7
7.2.1	Utilizing Forcing and Override Function During Maintenance.....	7-8
7.2.2	Maintenance for ProSafe-RS Equipment.....	7-20
7.2.3	Maintenance of Field Devices.....	7-26
7.2.4	Proof Test.....	7-27
8.	Self Document.....	8-1
9.	FAST/TOOLS Integrated System Using SCSU1.....	9-1
9.1	FAST/TOOLS Integrated System Configuration Using SCSU1.....	9-2
9.2	Narrowband System Environment.....	9-4
9.3	Defining narrowband groups.....	9-9
9.4	Operation in the Narrowband Mode.....	9-12
9.5	Details of the data buffering function.....	9-13
9.6	Gas Flow Rate Calculation Function.....	9-15
9.7	Application Capacities.....	9-20
9.8	Precautions for Engineering and Maintenance.....	9-22
10.	Engineering for ProSafe-SLS Communication Function.....	10-1
10.1	Overview and Flow of the Engineering.....	10-2
10.2	Determination of Events and I/O Data of ProSafe-SLS for Management.....	10-3
10.2.1	Determination of Data and Event and Diagnostic Information of ProSafe-SLS to Monitor.....	10-4
10.2.2	Determination of Time for Time Synchronization.....	10-5
10.3	Engineering ProSafe-RS.....	10-6
10.3.1	Preparation.....	10-7
10.3.2	System Engineering of ProSafe-RS.....	10-8
10.3.3	Engineering to Configure Applications on ProSafe-RS.....	10-10
10.4	Engineering for ProSafe-SLS.....	10-12
10.4.1	Engineering for CO-920.....	10-13
10.4.2	Processing events on CO-920.....	10-15
10.4.3	Initializing CO-920 time.....	10-16
10.4.4	Engineering for Time Setup with DI Input.....	10-17
10.5	Engineering for CENTUM.....	10-18
10.6	Example of Application on ProSafe-SLS Communication Function.....	10-19

Engineering Guide

IM 32Q01C10-31E 4th Edition

CONTENTS

Appendix

Appendix 1. Guidelines for Developing Application Logic.....	App.1-1
Appendix 2. Reuse of SCS Project Databases.....	App.2-1
Appendix 3. Glossary.....	App.3-1

1. Procedure for Engineering

ProSafe-RS is the Safety Instrumented System (SIS) comprising Safety Control Station (SCS) and Safety Engineering PC (SENG).

ProSafe-RS and CENTUM VP/CS 3000 (hereafter called CENTUM) which is a Distributed Control System made by Yokogawa, can be integrated.

This section describes an outline for the entire engineering of ProSafe-RS.

1.1 Outline of the Entire Engineering

This section describes a procedure for engineering the ProSafe-RS system, important issues for basic designs and an outline of the ProSafe-RS Engineering Function.

■ Procedure for Engineering

The regular procedure for engineering, from design to start of operation, including manufacturing, inspecting and commissioning, is shown as follows.

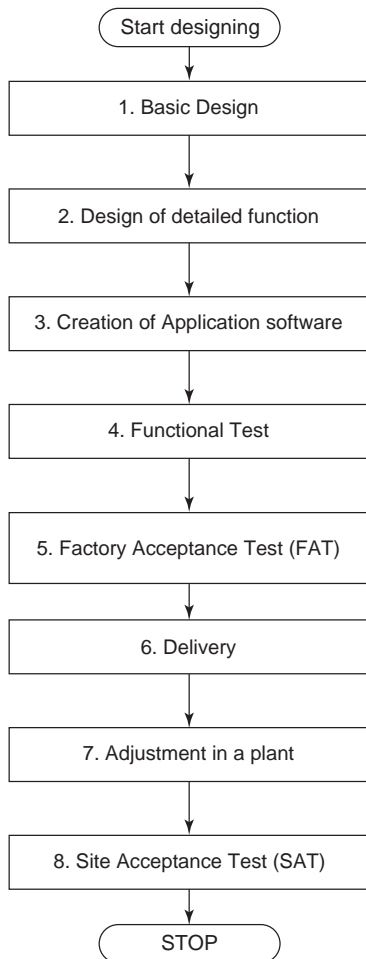


Figure 1.1-1 Procedure for Engineering

1. In Basic Design, the following items are decided based on user's requirements and specifications.
 - The making of safety specification
 - System configuration and hardware
 - The number of I/Os
 - Safety level (SIL) of loops
 - Signal interface with another system

The following documents are made as a result of these work.

- Diagrams of the system structure
- Hardware specifications
- I/O lists

- System basic design document
 - List of interface with other systems
2. Based on the user's requirements and specification, functional specifications are made. Detailed logic like shutdown logic is included in the functional specifications.
 3. ProSafe-RS projects and applications are created on a PC installing the SENG Function.
 4. Functions of the created application are checked. After making a document about the Test Specification, usually testing of functions is conducted in the following order.
 - (1) Desk test
The created applications are checked with self documents on the desk.
↓
 - (2) Unit test-1
Created application logics are verified. SCS simulation and Logic simulation test on SENG can be used for this verification.
↓
 - (3) Unit test-2
In the target test using SCS, the overall logic etc. are verified.
↓
 - (4) Integration test
The integrated final test is conducted on the SCS target. Before the test, it is required to provide an environment, where SCS can be used, in combination with panel, console, a host computer and other subsystems. The testing for system failure such as hardware failure is also conducted.
 5. Hardware and software Factory Acceptance Test (FAT) is conducted in the presence of users.
 6. Hardware and software which the user has confirmed in FAT are delivered.
 7. Hardware and software which are installed in the plant are adjusted.
 8. The Site Acceptance Test (SAT) is conducted to hand over the system to the user.

■ Key Points of Basic Design

In an engineering procedure, elaborate basic design is very important to design and build the safety instrumented system.

Some precautions for basic design are shown as follows. When the user has requirement for the safety integrity level (SIL), the following points should be considered and then PFD (Probability of Failure on Demand) of each safety loop is calculated and basic design is made to meet the required SIL.

● Independence of Safety Instrumented System and Process Control System Function

Establish independence of safety functions in a ProSafe-RS system and of control functions in a Process control system such as DCS.

● Safety Function and Safety Integrity

Consider the following items for Safety Function and Safety Integrity.

- Whether Redundancy for ProSafe-RS is needed or not (CPU and I/O modules)

- The failure rate of each component comprising the safety loop (Sensors, transmitters, relays, logic solver and final elements)
- Requirements for SIL and PFD value of a loop
- Interval between proof tests
- The possibility to easily perform validity check and proof tests for the applied system

● **Architecture (Basic Functions)**

Consider the following items for Architecture.

- Choice of “Normally Open (NO)” or “Normally Close (NC)”
- Choice of “Energize-to-Safe state principle (ETS)” or “De-energize-to-Safe state principle (DTS)”



IMPORTANT

It is recommended that SCS be separated into two SCSs. : One SCS with applications comprised of NC inputs and DTS outputs are performed. The other SCS with applications comprised of NO inputs and ETS outputs are performed.

- Redundant structure of safety loops
- Actions under fault conditions
- Safety time and scan period for process
- Requirements for Sequence Of Event Recorder (SOER) Data Collection and Time Synchronization System
- Man Machine Interface
- Requirements for each communication line
- Consideration for maintenance
- Maintenance override and bypass

● **Power Supply and Grounding**

See and follow the ProSafe-RS Installation Guidance for installation.

**SEE
ALSO**

For more information about power supply and grounding, refer to:

ProSafe-RS Installation Guidance (TI 32S01J10-01E)

● **Common Cause Failure**

Consider the distribution of functions of the ProSafe-RS system in order to deal with common cause failures.

● **Field Input Devices (Sensors, Transmitters and Signal Converters)**

Consider the following items for field input devices:

- Number of points for each signal type (DI or AI)
- Independence from control system
- Process parameter in normal operation and trip point
- Redundancy of input devices: 1oo1, 1oo2, 2oo3 and 2oo4

- Failure rate of input devices, especially the dangerous failure rate
- Whether Wiring Check is needed or not

- **Field Output Devices (Actuator, Solenoid Valve, Shutdown Valve, etc.)**

Consider the following items for field output devices:

- Number of points for each signal type.(DO or AO, voltage value and current value separately)
- Independence from control system
- Choice of Actuator and final element, and their speed of actions (Open direction and Close direction)
- Redundancy of actuators and final elements
- Considering the case of using relay output
- Failure rate of actuators and final elements, especially the dangerous failure rate
- Whether Wiring Check is needed or not

- **Man Machine Interface**

Consider the following items for the Man Machine Interface.

- For Operator Interface
 - Screens such as CRT and LCD
 - Annunciators:
size of display/actions/colors/sounds
 - Switches and lamps for a monitoring board
 - Print items of a printer
- Manual shutdown
- Reset function on recovery
- Interface for maintenance and engineering
 - Configuration definition of system hardware
 - Building application logics and downloading them to SCS
 - Modification, testing and monitoring of the application logics
 - Maintenance override
 - Monitoring system status of SCS and diagnostic information
 - Controlling SCS security level
 - SOER

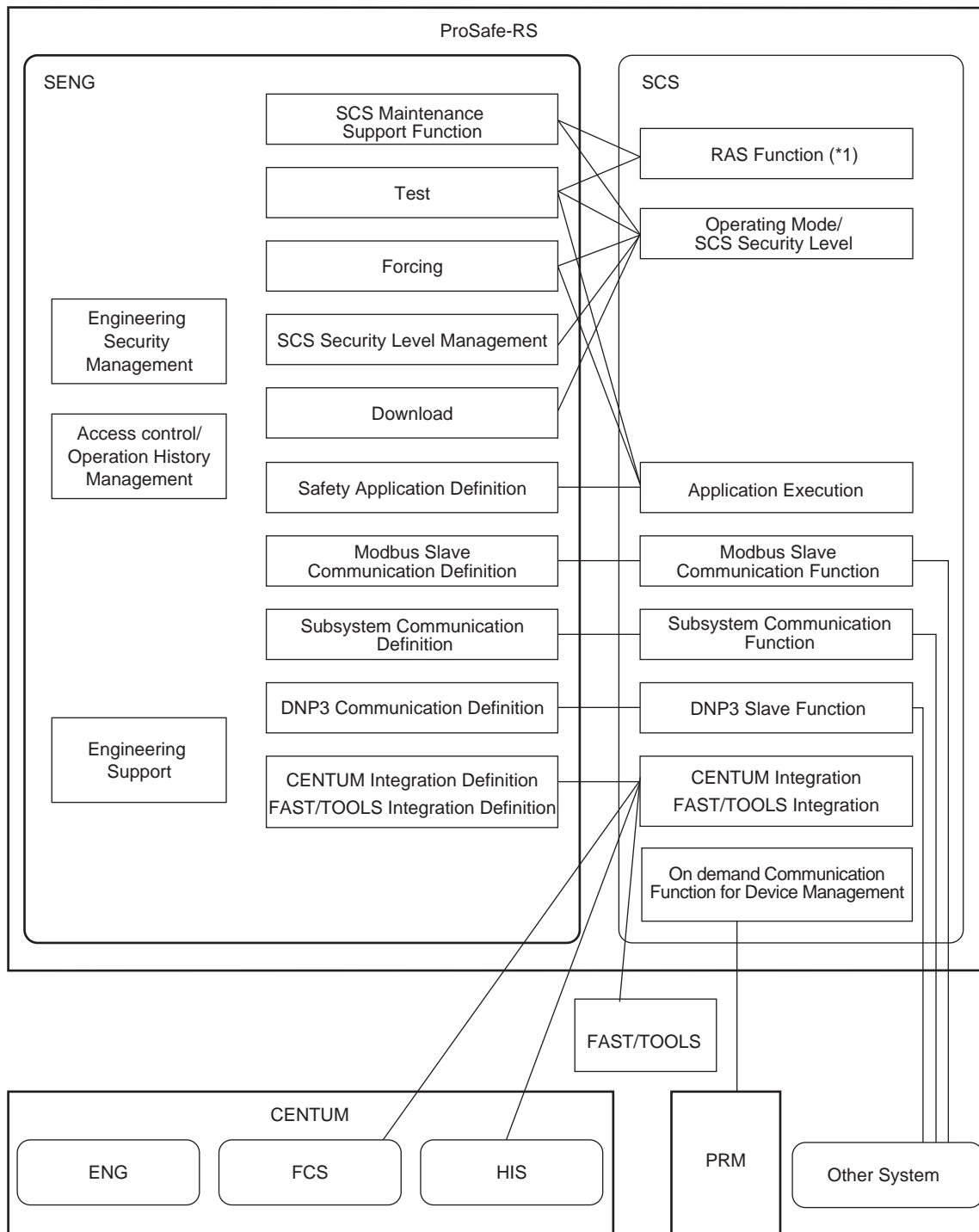
- **Management for Design Documents and Software**

Consider the following items.

- Print and storage management of design documents
- Management of changes for hardware and software

■ Outline of Engineering Functions

This section explains the functions used for engineering of the ProSafe-RS.



*1: RAS represents Reliability, Availability, and Serviceability.

Figure 1.1-2 Relationships Between Functions

● **Safety Application Definition**

This is a SENG function, which is to define safety applications that run on an SCS.

Various builders are used for defining safety applications. After the completion of definition an, SCS database is created to execute the safety application on the SCS. The created SCS database is downloaded to the SCS with the download function.

- **CENTUM Integration Definition**

This is a function defining the connection of an SCS with CENTUM.

This function is used for defining tag names, alarm processing table and alarm priority for monitoring and operating SCS from HIS.

- **FAST/TOOLS Integration Definition**

The function to define the connection of SCSs and FAST/TOOLS systems.

A tag name to refer to data values of SCSs from FAST/TOOLS can be defined.

- **Modbus Slave Communication Definition**

This is a function for setting up definitions for the SCS to communicate with another system (Modbus master) as a Modbus slave.

This function is used for setting Modbus device addresses.

- **Subsystem Communication Definition**

This is a function for setting up definitions for the SCS to connect with other systems using subsystem communication.

- **DNP3 Communication Definition**

This is a function for setting up definitions for the SCS to communicate with DNP3 master as a DNP3 slave.

The DNP3 slave setting and DNP3 data can be defined.

- **Download**

This is a function of downloading the Safety application definition, CENTUM integration definition and Modbus connection definition to the SCS.

- **Test**

This is a function to test engineering work. There are 3 types of tests: the Target Test, to debug using the actual SCS, and the SCS simulation test which simulates SCS and the logic simulation test to debug using simulators application logics on SENG.

- **Forcing**

This function improves the efficiency of commissioning. It contains the Forcing Function and the Fixing All I/O Module Function.

The Forcing Function forcedly fixes and changes I/O variables and internal variables of SCS.

The Fixing All I/O Module Function fixes all input/output values in I/O modules.

The Forcing Function can also be used for maintenance.

- **SCS Maintenance Support Tool**

This is a function of maintaining the SCS. This function allows engineers and maintenance personnel to read SCS diagnostic information, SCS state, and SOE (Sequence of Events). It also has a function of checking Diagnostic information message in SCS.

- **SCS Security Level Management**

This is a function of switching SCS Security Levels. SCS can restrict access from the outside of SCS, depending on security levels.

- **Engineering Security Management**

This is a function of managing the access authority to the databases defined by SENG and the write authority of the SCS maintenance support functions to SCS.

- **Access Control / Operation History Management Function**

Access Control / Operation History Management Function provides user management capability for SENG. Access Control is a function that manages the accesses to SENG or SCS per user. The operation history management function is for recording the operation history of the SENG software and viewing the history that has been recorded.

- **Engineering Support**

This is a function of supporting data construction and improving the efficiency of engineering and maintenance. It provides the following tools for different purposes.

- Version Control
- Master Database Restoring Function
- Test Project Creating Tool
- Project Attribute Tool
- Project Comparing Tool
- Import/Export Function
- Self Document
- Integrity Analyzer
- Cross Reference Analyzer
- Database Validity Check Tool
- SCS Information
- Save Operation Marks/Download Operation Marks

1.2 Classification of SCS Application

This section describes the following three applications running on SCS.

- **Safety Application**
This is an application which executes safety functions. The safety application includes application logic written in the language conforming to the IEC 61131-3 standards.
The following programming languages defined in IEC 61131-3 are available for SCS.
 - Function Block Diagram (FBD)
 - Ladder Diagram (LD)
 - Structured Text (ST)
- **CENTUM Integration Application**
This is an application for exchanging data with CENTUM, which is needed for the CENTUM Integration Structure.
- **Modbus Slave Communication Application**
This is an application for exchanging data with other systems connected via Modbus.
- **DNP3 Communication Application**
This is an application for communicating between the DNP3 master and SCS connected through DNP3.

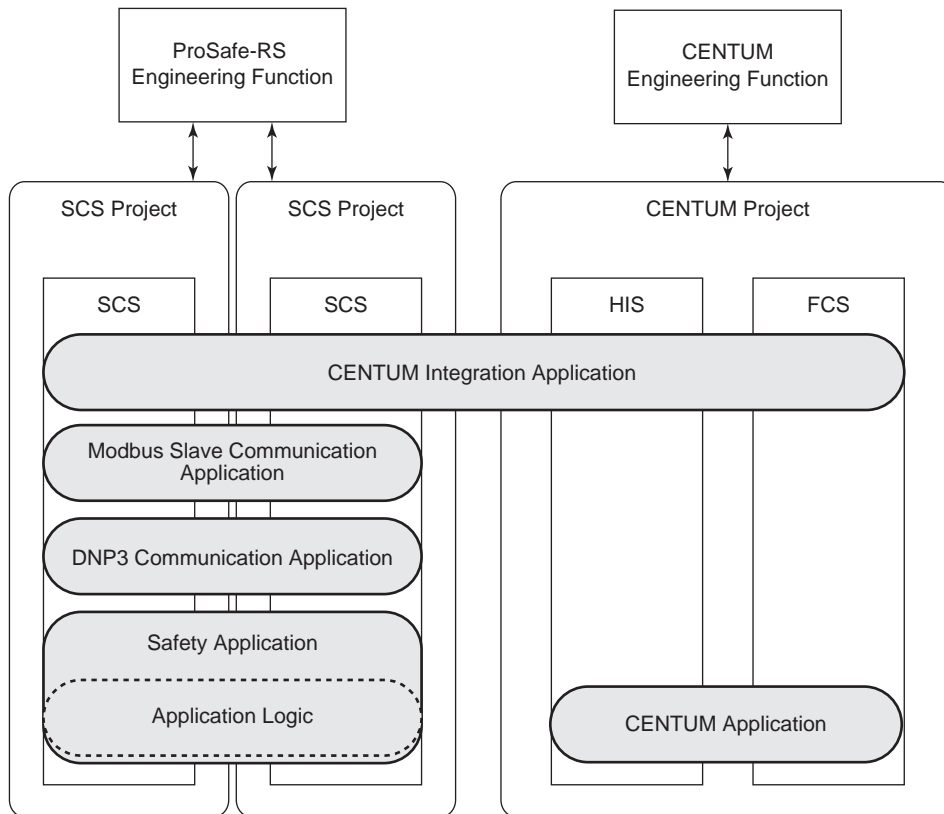


Figure 1.2-1 Classification of Application

1.3 Type of Project

In ProSafe-RS, a set of user-created engineering data called "Project," is collectively managed. This section describes the types of projects and the configuration of the SCS project database.

■ Type of Project

ProSafe-RS has the following two hierarchies of projects.

- RS Project
- SCS Project

For integration with a CENTUM system, a definition to associate the CENTUM Project with SCS Project is required.

Besides these projects, there are library projects, which include engineering data to be used as a library.

● Configuration Example of Projects

The following figure shows the example of SCS projects and RS projects.

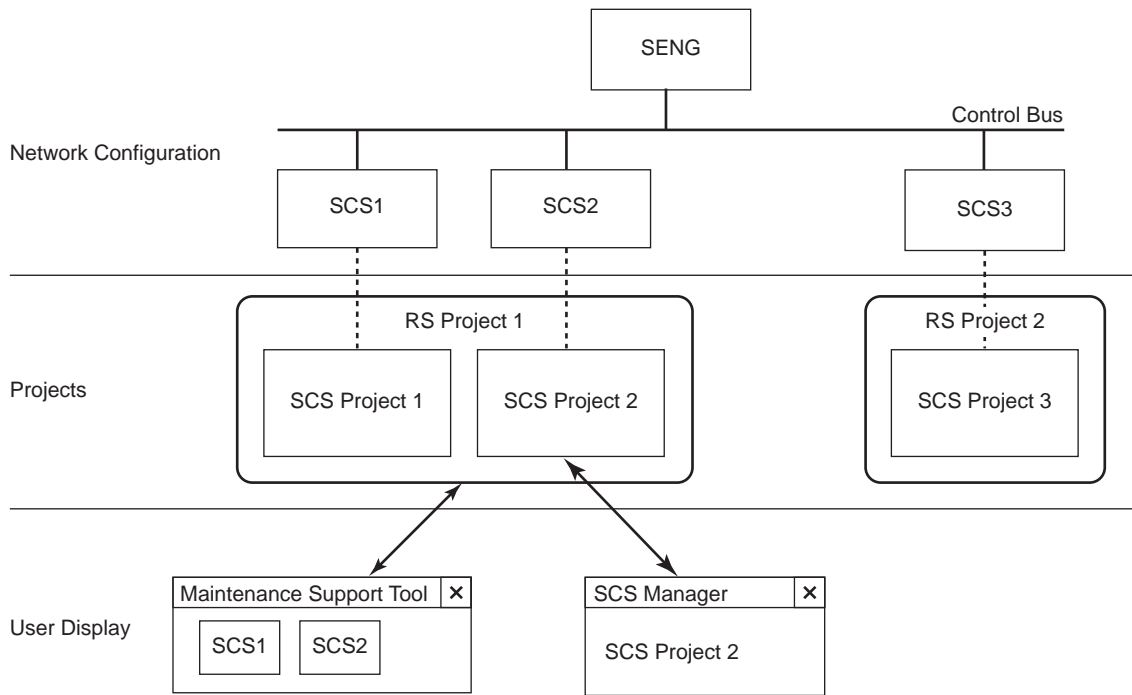


Figure 1.3-1 Outline of SCS Project and RS Project

● RS Project

An RS project is a combination of several SCS projects in order to bundle engineering data of SCS projects. Defining an RS project permits the collective monitoring of the status of the constituent SCSs by using the SCS Maintenance Support Function.

● SCS Project

In ProSafe-RS, one SCS project is defined and managed for one SCS. This allows database to be saved and restored for each SCS.

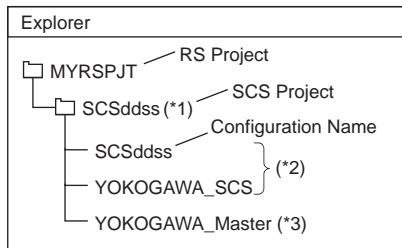
● Relationship between SCS Project and RS Project

An SCS project is included in an RS project. One SCS project, which is always included in one RS project, is not shared with another RS project. In addition, an RS project is not included in another RS project.

● Folder Configuration of RS/SCS Project

The SCS projects that constitute an RS project are specified by the folder configuration.

- RS Project
A folder created in Windows Explorer
- SCS Project
A folder created by using the SCS Manager under an RS project folder. It is placed as one folder.



*1: The folder name must be identical to the SCS project name. (dd: Domain number, ss: Station number)
 *2: This is a work database.
 *3: This is a master database.

Figure 1.3-2 Folder Configuration of RS Project and SCS Project

● Library Project

A library project is a project database that can be used as a library independent of the specific SCS. Library projects can be used for creating application logics and can be debugged only by a logic simulation test. (An individual library project cannot be tested by SCS simulation test or by target test for debugging.)

The functions and function blocks that are used among two or more SCSs can be created as library projects and be copied to each SCS project.

SEE ALSO

For more information about the procedure and remarks in creating library projects, refer to:

6., "Library Projects" in Engineering Reference (IM 32Q04B10-31E)

■ SCS Project Attribute

An SCS project will be defined with the following three attributes.

The attributes of a project determine whether it can be downloaded to actual SCS and whether it can be tested by SCS simulation. However, a logic simulation test can be preformed for any project regardless of its attribute.

● Default Project

A new project created in the SCS Manager will be the default project. The default project should be a project that has not been downloaded to the actual SCS. Engineering works for a new project are always carried out on the default project.

Downloading to actual SCS: Available

Testing by SCS simulation test: Available

● **Current Project**

When offline downloading a default project to an actual SCS, the attribute of the project will change from Default to Current automatically.

Downloading to actual SCS: Available

Testing by SCS simulation test: Unavailable

● **User-defined Project**

A project created using the Test Project Creation Tool will be a user-defined project.

Downloading to actual SCS: Unavailable

Testing by SCS simulation test: Available

■ **Configuration of SCS Project Database**

In ProSafe-RS, one SCS project is defined and managed for each SCS. The following data are stored in each SCS project folder.

- Work Database (SCS database and source files to define SCS)
- Master Database (Current SCS database and source files to define SCS)

On one SENG, the SCS Manager allows editing only one SCS project at a time. Several SCS Managers cannot be opened on one SENG at the same time.

On one SENG, an SCS project stored on another SENG can be edited, but one SCS project can not be referred with several SENGs at the same time.

The following figure shows the configuration of an SCS project.

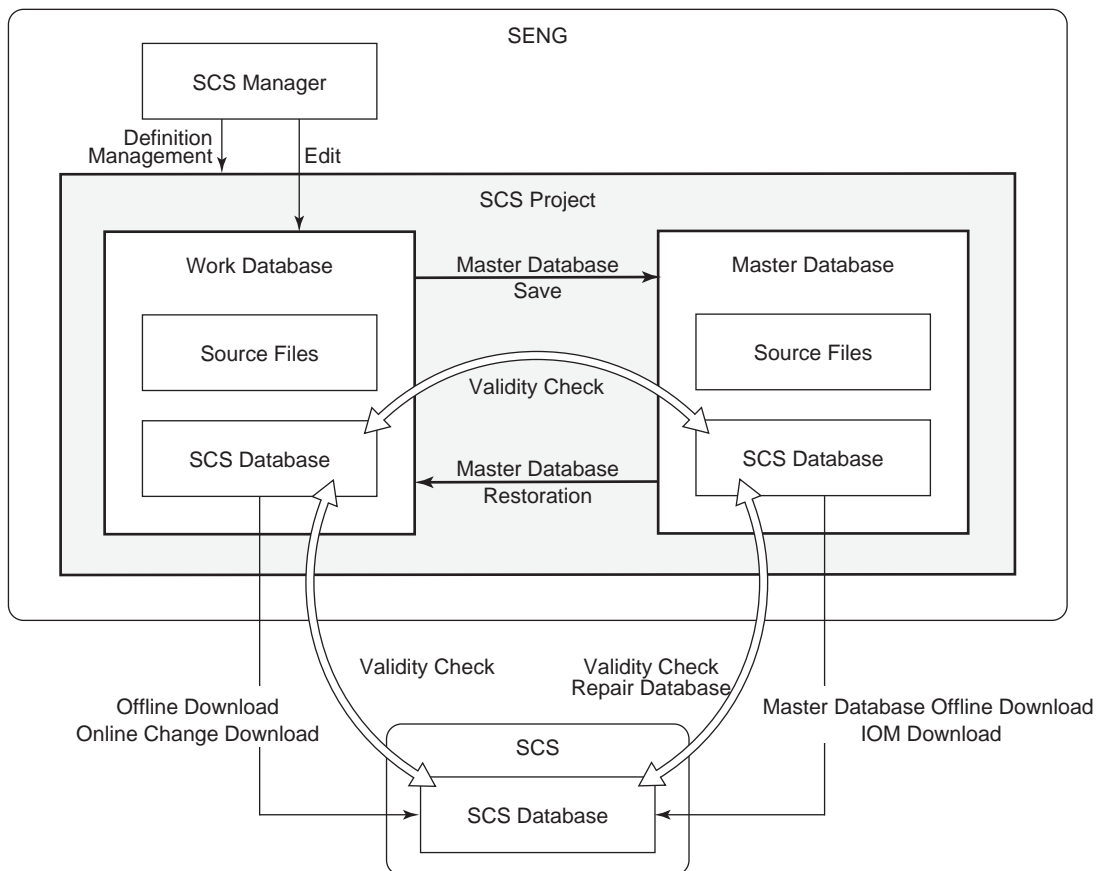


Figure 1.3-3 Configuration of SCS Project

The SCS Manager is used for editing a work database. The edited work database, when being downloaded to SCS with offline download or online change download, is automatically saved in the master database.

The Master Database Restoring Function deletes the SCS database being edited in the work database and replaces it with the master one.

The Database Validity Check Tool is used to check the integrity of the database in the work database, master database, and SCS. Master database offline download enables the database to be downloaded from the master database to SCS. IOM download is available for downloading I/O module information from the master database to a relevant I/O module in the case of I/O module replacement.

1.4 System Generation Function

This section describes the outline of the System Generation Function (Builder Function) and its tools constituting the Engineering Function.

■ Safety Application Definition

A safety application is created with tools and builders called from the SCS Manager.

Various builders and tools used for safety application definition are opened in the SCS Manager.

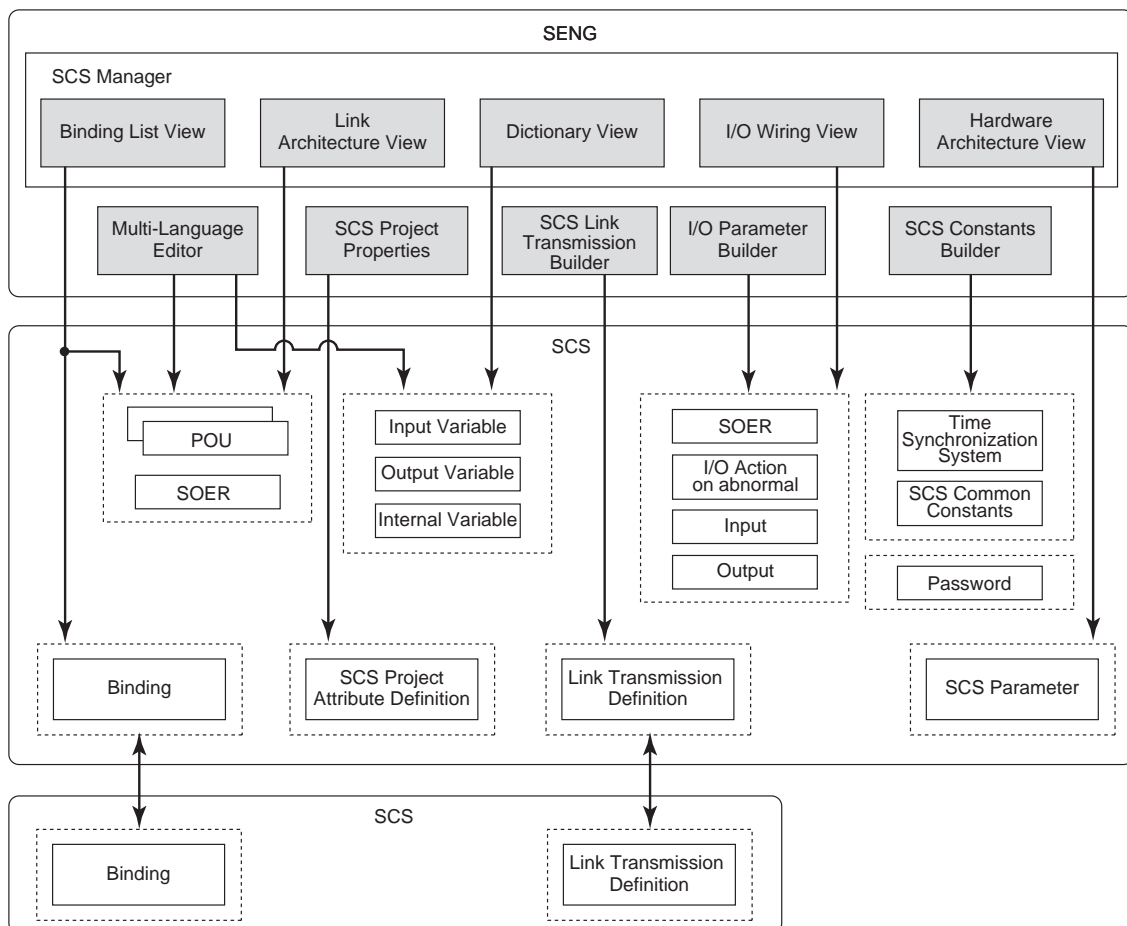


Figure 1.4-1 Overview of Safety Application Definition

● Hardware Architecture View

- Set the configuration name.
- Define the IP address of the SCS.

● I/O Wiring View

- Define the AIO/DIO modules (analog I/O modules and discrete I/O modules) and communication modules.
- Create the wiring from the channels of each module to the I/O variables.

● Link Architecture View

- Configuring the security settings of the SCS project.

- Defining the POU.(*1)
- Adding variable groups.
- Starting the Multi-Language Editor to edit the POU that you have defined.

*1: POU: Program Organization Unit It is a generic term for the programs, function blocks (FB), and functions (FU) that are written with the function block diagram (FBD) and ladder diagram (LD)

● **Multi-Language Editor**

Edit the POUs for the LBD, LD, and ST.

● **Dictionary View**

Declaration of variables and parameters

● **Binding List View**

Binding variables from the producer to the consumer of Inter-SCS safety communication

● **SCS Project Properties**

Defining Project properties including station type, domain number, and station number of SCS

Designating location of the integrated CENTUM project folder, in the case of CENTUM Integration Configuration

● **SCS Constants Builder**

Settings SCS common constants and time synchronization method

● **I/O Parameter Builder**

Setting parameters of nodes, modules, and channels including setting the Actions on Fault Detection of I/O modules and channels SOER collection definition of DI/DO

● **SCS Link Transmission Builder**

Defining SCS link transmission safety communication and SCS global switch communication

■ **CENTUM Integration Application Definition**

The following figure shows the outline of CENTUM integration application definition and the associated builders.

These builders are opened from the engineering launcher of the SCS Manager.

- **Tag Name Builder**
This builder defines tag names for FBs and variables which can be used for CENTUM Integration Configuration, and also defines annunciator messages.
Defining a tag name results in the creation of a mapping block for CENTUM Integration Configuration.
- **Alarm Priority Builder**
This builder defines alarm priority. The condition of alarm activation is set to each alarm priority as in CENTUM.
- **Alarm Processing Table Builder**
On CENTUM Integration, the Alarm Processing Table is used to determine the Alarm Priority of process alarms raised by FBs or mapping blocks.
The Alarm Processing Table Builder is used to import the 'Alarm Processing Table defined in CENTUM' to SCS project.

In a CENTUM integration structure, the application of ProSafe-RS needs to be defined with those builders. Furthermore, engineering of CENTUM including SCS definition and tag list generation needs to be executed on CENTUM ENG. This allows HIS to access SCS data with a tag name and to display annunciator messages.

The following figure provides an overview of CENTUM Integration Application Definition.

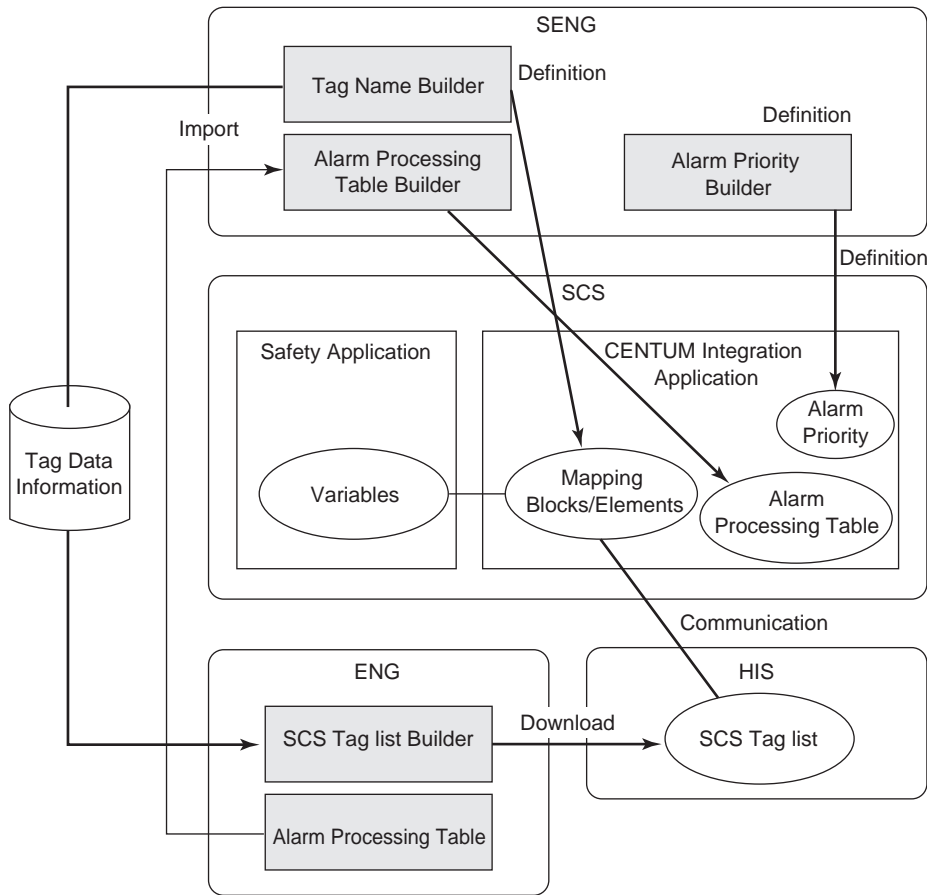


Figure 1.4-2 Outline of CENTUM Integration Application Definition

■ Modbus Slave Communication Application Definition

The outline of the Modbus Slave Communication application definition and the relevant builder are shown below.

- **Modbus Address Builder**
This builder defines Modbus device addresses.

The following figure shows the outline of the definitions of Modbus slave communication application.

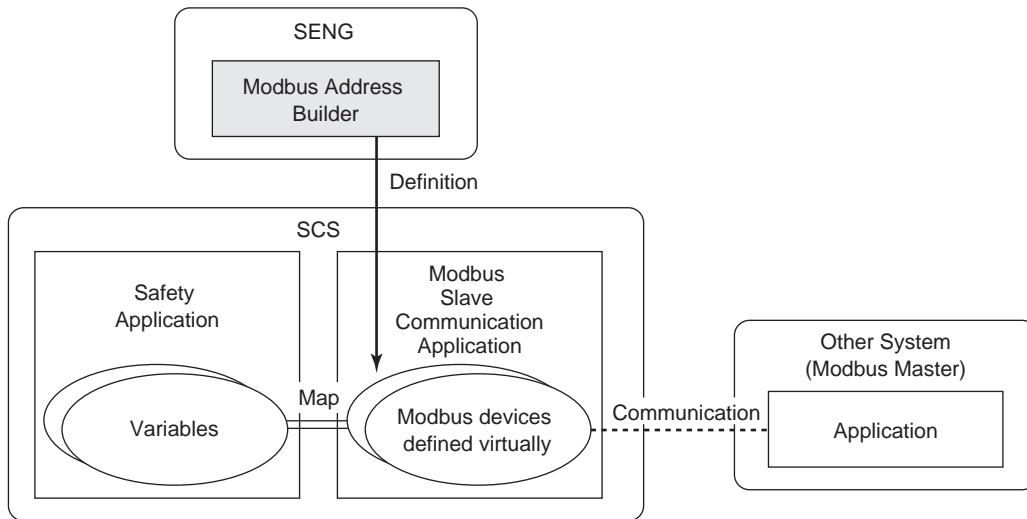


Figure 1.4-3 Outline of Modbus Slave Communication Application Definition

■ DNP3 Communication Application Definition

The following list shows the outline of the DNP3 communication application definition, the builder, and tools.

- The communication I/O module (model: ALE111) required for DNP3 communication is defined. The I/O wiring view and I/O parameter builder are used.
- The parameters needed for the SCS to operate as a DNP3 slave station are set. The DNP3 communication builder is used.
- Instances of DNP3 communication FBs are assigned to DNP3 data so as to reference and set variables of the application logic. The DNP3 communication builder is used.

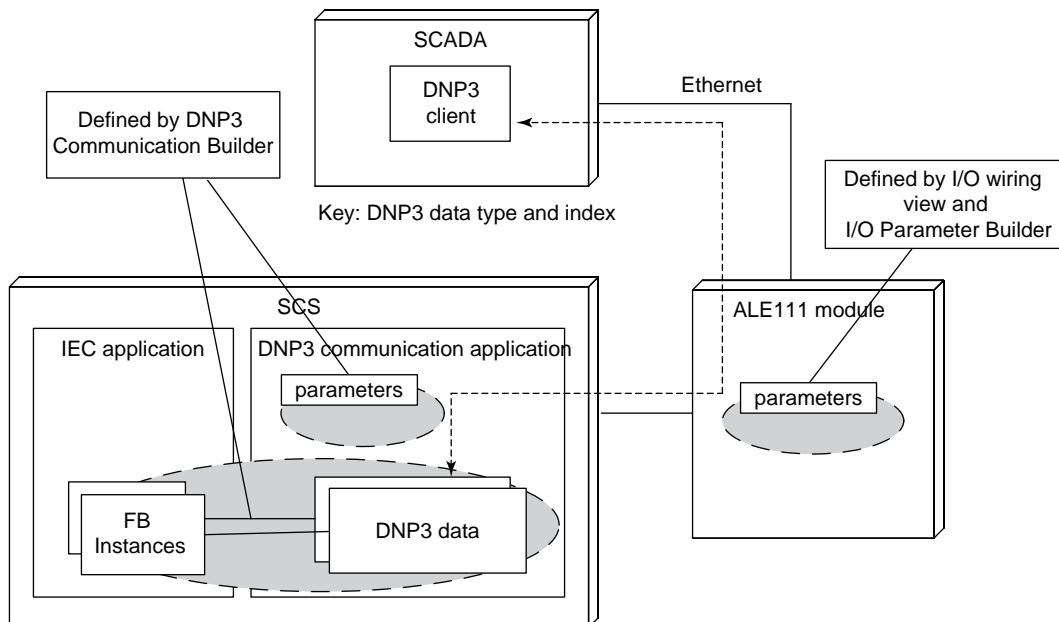


Figure 1.4-4 Outline of DNP3 Communication Application Definition

■ Engineering Tools

The following tools are available.

- **Integrity Analyzer**

The Integrity Analyzer is used to analyze the safety of existing created application logics. It detects unauthorized FB /FU as the safety function, and outputs results of analyzing on screen or on the analysis report.

- **Cross Reference Analyzer**

It shows, on screen or on the analysis report, the difference between the application previously downloaded (which runs currently on SCS) and the application to be downloaded soon as well as the extent of impact in case of downloading. The Cross Reference Analyzer is for limiting the scope of retesting when application logic is modified.

- **Self-Documentation Function**

This is for printing user applications. The entire definitions of an SCS project or any parts can be selected as a printed item.

- **Version Control Tool**

This is for controlling the version history of an SCS project to support the project updates by users.

The Version Control Function is used for saving (check-in) the data of an SCS project at some point by assigning a version number and for restoring (check-out) project data of a certain version.

- **Master Database Restoring Function**

This is for restoring the master database to work database. The Master Database Restoring Function is used to delete the current work database and replace it with the master database.

- **Database Validity Check Tool**

The Database Validity Check Tool is used to check the integrity among the work database and master database of the SCS project, and SCS database on the SCS. With this tool of R3.02.10 or later, you can repair the master database by replacing it with the work database if the master database failed to be updated due to an online downloading error or some other reason.

- **SCS Information**

This function is used to display and print SCS project usage conditions such as POU's used within the SCS and the number of variables. Perform building SCS project before using this function.

- **Save Operation Marks/Download Operation Marks**

Operation marks specified for SCS tags on an HIS in the CENTUM integration structure are initialized and thus lost when offline download to the SCS, master database offline download or SCS restart (including when recovering from power failure) are executed. This function makes it possible to recover initialized operation marks to the status at the last saved operation.

The Save Operation Marks is a function to save operation marks specified for tags on an HIS in the SENG.

The Download Operation Marks is a function to download saved operation marks to the SCS.

**SEE
ALSO**

For more information about Save Operation Marks/Download Operation Marks, refer to:

[2.2.3, "Other builders" in Integration with CENTUM VP/CS 3000 \(IM 32Q01E10-31E\)](#)

- **Import/Export Function**

Import or export functions can be used to import or export SCS project data. Therefore, these data can be used for test functions or for reusing applications.

- **Test Project Creation Tool**

This tool can be used to copy a project that is running at a plant site and create a project for test purpose.

- **Project Attribute Tool**

This tool can be used to display the attribute of an SCS project.

- **Project Comparing Tool**

This tool can be used to detect the difference between two specified SCS projects and to display and print the result.

1.5 Maintenance Function

This section describes the outline of the functions used for maintenance of SCS and field devices.

■ Outline of Functions to Use for Maintenance

● Set SCS Security Level

This is for changing the SCS security level in the case of downloading the database to the SCS or forcing parameters.

● I/O Lock Window

This is for locking/unlocking I/O channels during maintenance, and shows the locking status of the I/O channels. When inputs or outputs are locked, it is possible to set their values.

● Communication I/O Lock Window

This is for locking/unlocking inputs/outputs of subsystem communication during maintenance, and shows the locking status of the inputs/outputs. When inputs or outputs are locked, it is possible to set their values.

● SCS Link Transmission Lock Window

During maintenance, locking or unlocking the communication data of link transmission can be performed on this window. The locking and unlocking status can also be monitored. When a communication data is locked, the value of the communication data can be changed.

● Inter-SCS Communication Lock Window

This is for locking or unlocking inter-SCS safety communication FBs for each SCS during maintenance and shows the locking status of the FBs. When inter-SCS safety communication FBs are locked, it is possible to set their values.

● Restart SCS

This is for restarting SCS.

● Master Database Offline Download

This is for downloading the master database to SCS and restarting the SCS.

● SCS Maintenance Support Tool

The SCS maintenance support tool facilitates the maintenance of SCS. It is not intended for operator's constant monitoring of SCS. It supports maintenance of SCS and the investigation of any cause of failures.

The SCS Maintenance Support Tool allows the user to:

- Recognize the SCS operating status at a glance.
- Set for acquisition and confirmation of diagnostic information messages and SOE event messages and so on by using the Message Cache Tool.
- Recognize the presence of diagnostic information messages and unconfirmed diagnostic information messages at a glance using the diagnostic information window.
- Save the data of the SCS operating status in character strings using the SCS System Report Display Function.
- Set the system clock.

-
- Call the user-defined action guide from help dialogs.
 - Display SCS event information on the SOE viewer.

**SEE
ALSO**

For more information about the SCS maintenance support tool, refer to:

3., [“SCS Maintenance Support Tool” in Utilities and Maintenance Reference \(IM 32Q04B20-31E\)](#)

2. Design of Applications

This section describes important issues to consider in designing application of a ProSafe-RS system.

The ProSafe-RS system can primarily be used for the following applications.

- Emergency Shutdown System (ESD)
- Fire and Gas System (F&G)
- Burner Management System (BMS)

In ProSafe-RS, both types of applications are available: The application consisting of a combination of the NC (NORMALLY CLOSE) inputs and DTS (DE-ENERGIZED TO SHUTDOWN) outputs, and the application consisting of a combination of the NO (NORMALLY OPEN) inputs and ETS (ENERGIZED TO SHUTDOWN) outputs.

2.1 System Configuration

This section describes various kinds of system configuration for ProSafe-RS, requirements for IT Security and an overview of the hardware of ProSafe-RS.

ProSafe-RS consists of Safety Control Station (SCS) and Safety Engineering PC (SENG). ProSafe-RS can communicate with the following DCSs or Supervisory Control And Data Acquisition (SCADA) system.

- CENTUM
- DCS connected through Modbus
- FAST/TOOLS

2.1.1 Overview of the System Configuration

This chapter describes the standard configuration of ProSafe-RS systems.

■ ProSafe-RS Basic Configuration

The basic configuration of ProSafe-RS consists of SENG and SCS. The following figure illustrates an example of the basic configuration of ProSafe-RS consisting of one SENG and two SCSs.

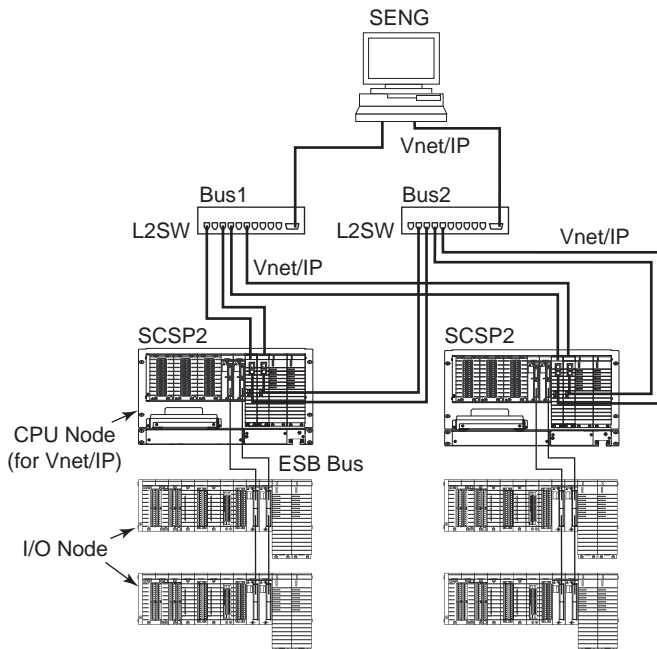
SCS and SENG are connected via control buses. Safety communication through control buses allows data to be sent and received between SCSs.

In SCS, I/O can be expanded by increasing the number of I/O nodes.

In the following figure, each of two SCSs has a Safety Control Unit (CPU node) which is connected to two Safety Node Unit (I/O nodes). I/O modules may also be installed in the CPU node.

● Configuration for Vnet/IP: SCSP2/SCSP1

The following figure shows the basic configuration of a ProSafe-RS system on a Vnet/IP network.

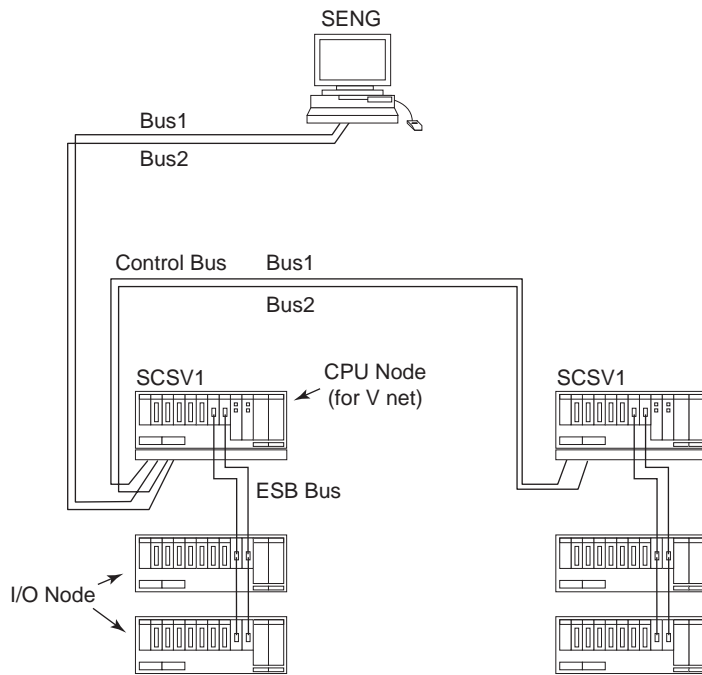


SCSP2: Safety Control Station to perform safety applications (for Vnet/IP)
 SENG: PC for engineering functions like editing applications, downloading, tests and for maintenance.
 L2SW: Layer 2 Switch

Figure 2.1.1-1 Basic Configuration for ProSafe-RS (Vnet/IP)

● Configuration for V net

The following figure shows the basic configuration of a ProSafe-RS system on a V net.

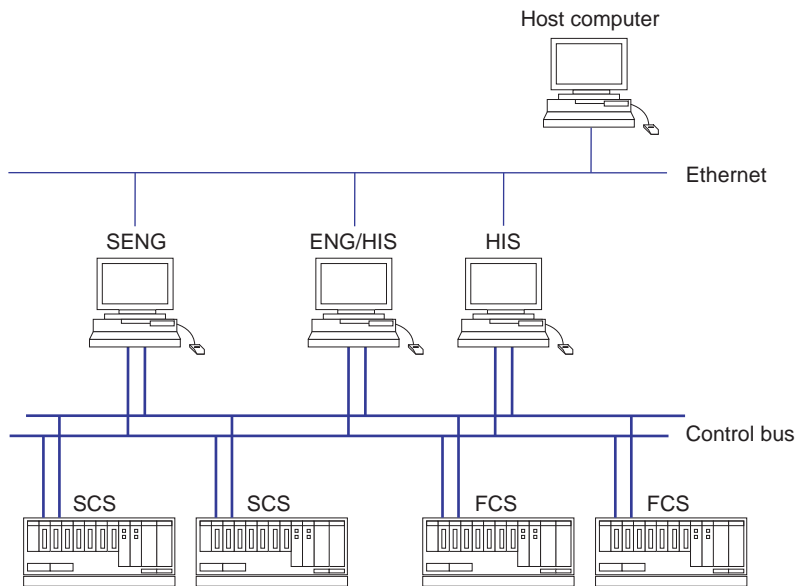


SCSV1: Safety Control Station to perform safety applications (for V net)
 SENG: The computer where you can create applications such as editing, downloading, testing and maintaining applications.

Figure 2.1.1-2 Basic Configuration for ProSafe-RS (V net)

■ CENTUM Integration Configuration

The structure of a ProSafe-RS connected with CENTUM projects is called CENTUM Integration Configuration.



SCS: Control Station to perform safety applications
 SENG: PC for engineering functions like editing applications, downloading, tests, and for maintenance.
 FCS: Field Control Station to execute process control.
 HIS: Human Interface Station
 PC which provides interfaces for operators who monitor and operate the plant
 ENG: PC installing CENTUM engineering function

Figure 2.1.1-3 CENTUM Integration Configuration

- For CENTUM Integration Configuration, both FCS and SCS can be operated and monitored from HIS.
FCS can read or write data in SCS via Control bus. But the SCS is designed so that its safety function is not affected even when data is written by FCS.
- SCS engineering is performed from SENG. FCS and HIS engineering is performed from ENG. Engineering of CENTUM integration function is performed from both SENG and ENG.
SENG functions, ENG functions and HIS functions can be installed in several PCs as well as to the same PC.
- The Exaopc OPC interface package of CENTUM (for installation on HIS) on HIS enables a host computer for production management, to access the data of FCS and SCS by using the OPC Interface.
Moreover, using the ProSafe-RS SOE OPC interface package allows access to SOE information in SCS from the host computer.
- As a type of the CENTUM Integration Configuration, it is possible to connect only HIS function to ProSafe-RS.
In this case, the structure is the same as in the previous figure without FCS.
- SENG is connected to control buses in CENTUM integration configuration. In addition, SENG, HIS and ENG terminals are connected via Ethernet.

**SEE
ALSO**

For more information about CENTUM integration in a Vnet/IP system, refer to:

[A2.2, "System integrated with CENTUM" in ProSafe-RS Vnet/IP \(IM 32Q56H10-31E\)](#)

■ Structure of Connection with Other Systems

SCS supports the Modbus slave communication and subsystem communication functions for connection with other systems. These functions does not affect the safety functions implemented in the SCS.

Interference-free communication modules need to be installed in the SCS nodes to be connected to other systems. Application logic that is created for connection with other systems cannot be used in safety loops.

The functions and configurations for connection are as follows.

- **Modbus Slave Communication Function**
In this type of connection, an external system acts as an Modbus master and the SCS acts as a Modbus slave. It is possible to construct an operator interface for other systems by accessing data in the SCS from the other systems acting as the communication master. To implement redundant Modbus slave communication, you need to create a user application for that purpose on the Modbus master side.

Serial communication modules or Ethernet communication modules need to be installed in the SCS nodes to be connected to other systems.

- **Subsystem Communication Function**
The subsystem communication function allows the SCS to act as the communication master and communicate with other systems. The subsystem communication function of SCS supports the Modbus protocol. The SCS acting as the communication master can read and set input/output data in the subsystems. Subsystem communication can be made dual-redundant.

Serial communication modules need to be installed in the SCS nodes to be connected to other systems.

The following figure shows an example of connection.

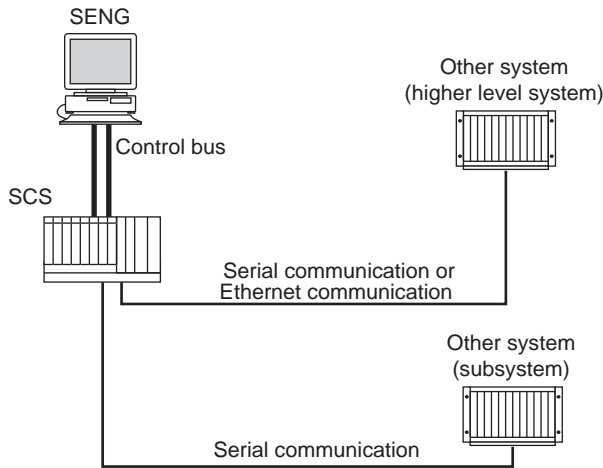


Figure 2.1.1-4 Connection with Systems Except CENTUM

■ Stand-alone SCS Configuration: SCSP2/SCSP1

It is possible to construct a stand-alone SCS configuration system environment without connecting the SCS to the Vnet/IP network while operating. SCS and SENG can be connected temporarily via the network when you perform engineering and maintenance. Only SCSP2/SCSP1 can be used in stand-alone configuration. SCSV1 on a V net cannot be used as a stand-alone system. The following figure shows a stand-alone SCS configuration system.

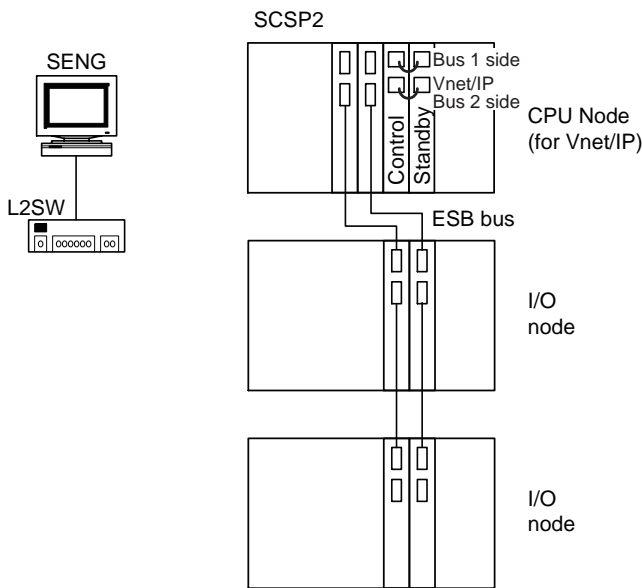


Figure 2.1.1-5 Stand-alone SCS Configuration System

- Prepare an environment where an SENG can be connected to a stand-alone SCS for its maintenance. When connecting an SENG in a stand-alone SCS configuration environment, connect it to the SCS via a Layer 2 switch (L2SW).
- For maintenance, you need to connect an SENG to the SCS. Read through the following procedures and use network cables that are long enough for connection of the SENG.



IMPORTANT

- System status and errors should be notified by outputting them on a hardware-wired panel, or should be checked on the SCS State Management window on a connected SENG.
- In order to enable outputs automatically without using an SENG after turning on the power of the SCS, it is necessary to use SYS_STAT to perform the output enable operation from the application logic. The output module status is available through parameters such as the NRO parameter of SYS_IOALLST.
- While operating in a stand-alone configuration, the SCS itself becomes the Vnet/IP time master and its time may gradually deviate from the absolute time. Check the system time and adjust it accordingly when the SCS is connected to an SENG for maintenance and so forth.
- In a stand-alone SCS configuration system, do not turn on the power to the SCS when the battery of the CPU module has run out. If you do so, the date setting in the SCS will be changed to January 1st, 1970.

● Overview of Procedures to Construct/Maintain Stand-alone SCS Configuration System

This section explains each of the main steps of constructing and maintaining a stand-alone SCS configuration system.

To do the following steps, you need to connect SENG to the Vnet/IP, but note that while a SENG is connected, one of the buses (bus 2) is in an error status.

- Startup of SCS
- Re-connection of SENG
- Disconnection of SENG
- Replacement of one of the redundant CPU modules.



IMPORTANT

Always connect a SENG during maintenance and make sure that you check the following before you disconnect it.

- SCS is normally started.
- SCS inputs and outputs are all normal.
- There is no diagnostic information message indicating errors of the SCS.

● Initial Startup of SCS

The following information explains the procedure for starting SCS for the first time (offline download).

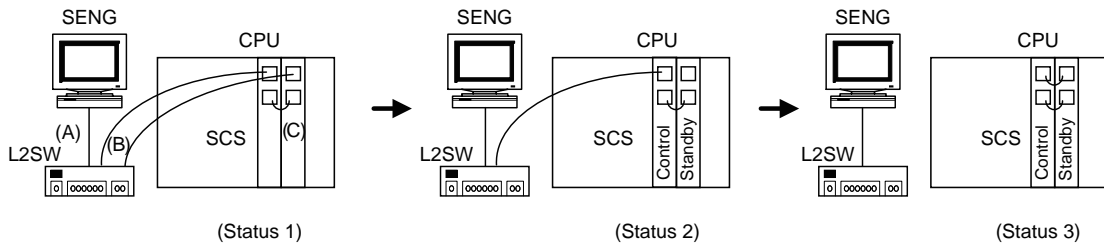


Figure 2.1.1-6 SCS Initial Startup Procedure

1. Perform the following connections using network cables while the SCS is powered off. (Status 1)
 - a. (A) Connection between SENG and L2SW, and powering them on
 - b. (B) Connection of bus 1 connectors on both CPU modules to L2SW
 - c. (C) Connection between bus 2 connectors on both CPU modules
2. Turn on the power of the SCS and perform offline download from SENG.
3. After the offline download is completed, wait until one of the CPU module enters the control state and the other enters the standby state, and then remove the cable between the bus 1 connector of the standby-side CPU module and L2SW (Status 2) (Status 2)
4. Disconnect the bus 1 cable of the control-side CPU module from L2SW and connect it to the bus 1 connector of the standby-side CPU module (Status 3) (Status 3)

● **Reconnection of SENG**

Use the following procedure to connect an SENG to an operating stand-alone SCS for the purpose of maintenance and so forth.

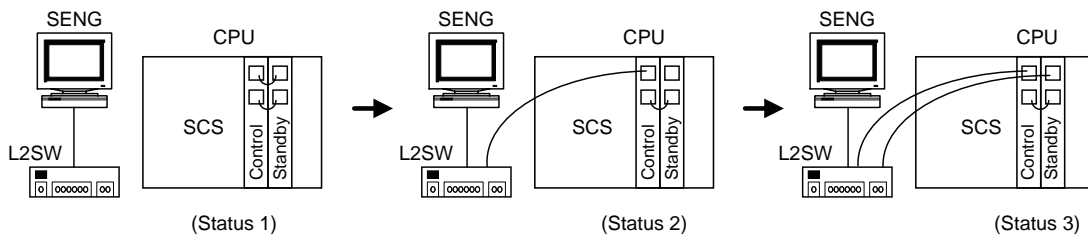


Figure 2.1.1-7 Procedure of Connecting Operating Stand-alone SCS to SENG

(Status 1) above shows SCS operating in stand-alone configuration. At this timing, SENG is not powered and L2SW should be powered.

1. Disconnect the cable from the bus 1 connector of the standby-side CPU module and connect it to L2SW. (Status 2)



IMPORTANT

When you make this connection, if the cable between the bus 1 connectors of the two CPU modules of SCS is not long enough to be connected to the L2SW, you may remove the cable and use a longer cable. However, you must be very careful not to misconnect the cable.

2. Connect the bus 1 connector of the standby-side CPU module to the L2SW with a cable. Then, power on the SENG. (Status 3)

● **Disconnection of SENG**

The SENG can be disconnected after completion of maintenance and other intended operations in the following procedure.

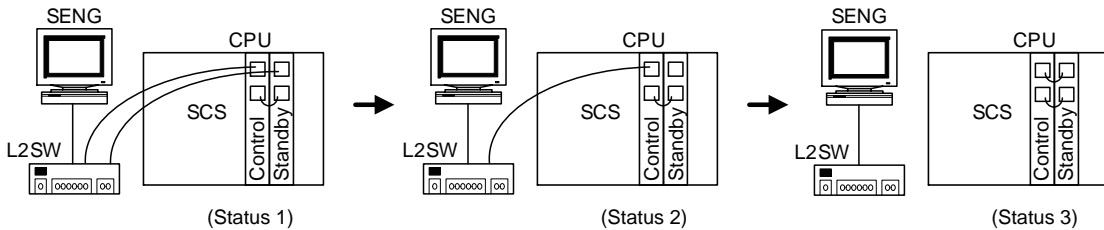


Figure 2.1.1-8 Procedure of Disconnecting SENG

(Status 1) above shows a status where SCS and SENG are connected.

1. Remove the cable between the bus 1 connector of the standby-side CPU module and L2SW (Status 2) (Status 2)
2. Disconnect the bus 1 cable of the control-side CPU module from L2SW and connect it to the bus 1 connector of the standby-side CPU module (Status 3) (Status 3)

● **Replacement of One of the Redundant CPU Modules**

Use the following procedure to replace one of the redundant CPU modules.

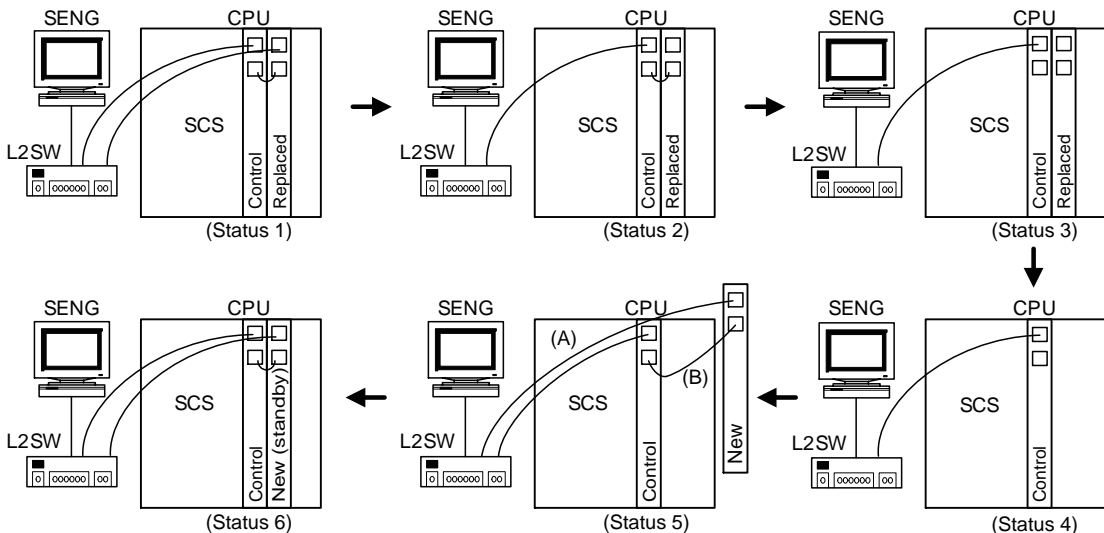


Figure 2.1.1-9 Procedure of Replacing One of the Redundant CPU Modules

(Status 1) above shows a status where an SENG is connected for the purpose of checking diagnostic information.

1. Remove the cable between the bus 1 connector of the CPU module to be replaced (standby-side) and L2SW. (Status 2)
2. Remove the cable between the bus 2 connectors on both CPU modules. (Status 3)
3. Remove the CPU module to be replaced from the node. (Status 4)
4. Prepare a new CPU module as a replacement and perform the following connections. (Status 5)
 - a. (A) Connection between bus 1 connector of the new CPU module and L2SW
 - b. (B) Connection between bus 2 connectors on both CPU modules

- 5. Install a new CPU module in the node. (Status 6)

■ Expandability of System

The ProSafe-RS system can be expanded by using devices such as the V net bus repeater, V net optical bus repeater, V net bus converter (BCV), Communication Gateway Unit (CGW), V net Router, and Wide Area Communication Router (hereafter referred to as WAC router).

Using V net bus repeaters and V net optical bus repeaters can expand the V net connection within one V net domain(*1).

A V net domain can be segmented into several connected V net domains using BCV and CGW. Routing through BCV and CGW enables communications between stations in different V net domains.

WAC routers can connect different Vnet/IP domains through a wide-area network (WAN).

The system connected through BCV, CGW, and WAC routers is a kind of CENTUM Integration Structure.

*1: A V net domain is a collection of stations with one line of V net.

The following figure shows an example of the Expanded System Structure of ProSafe-RS.

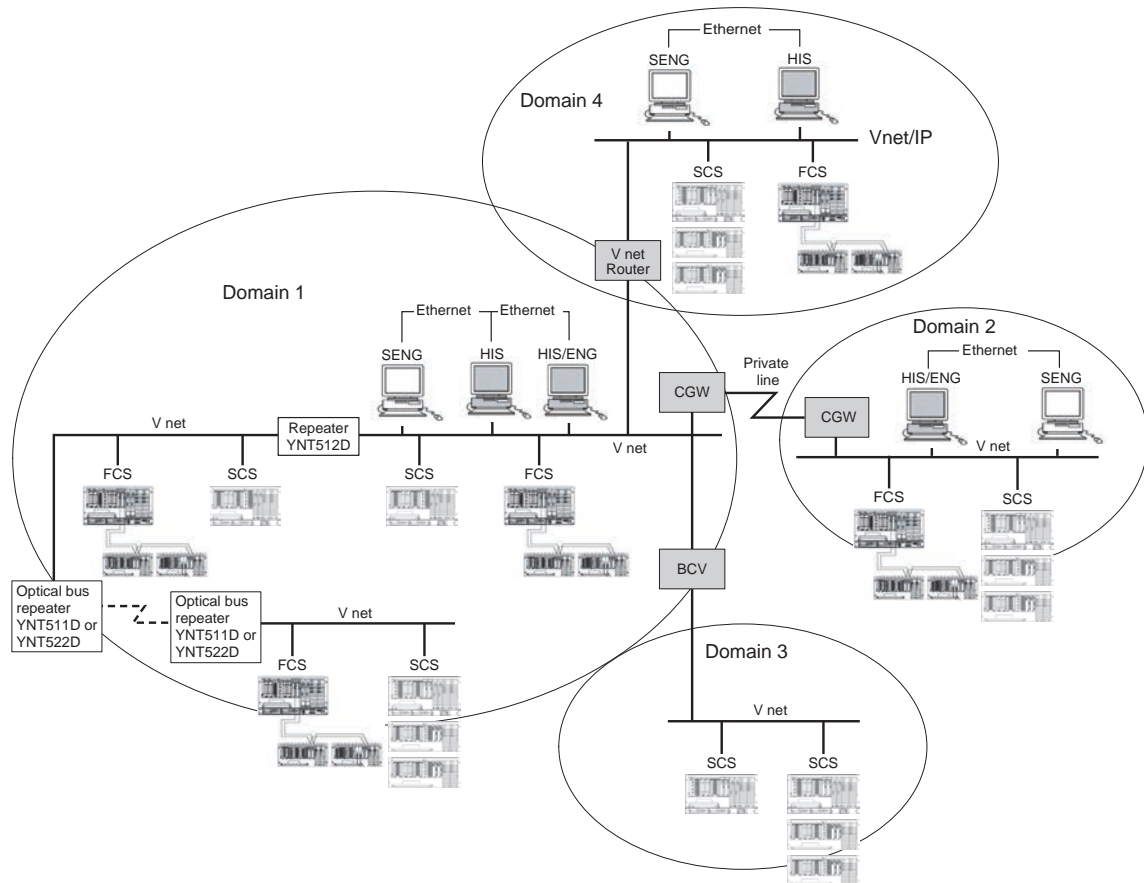


Figure 2.1.1-10 Example of Expanded System Structure

SEE ALSO For more information about expandability of system with Vnet/IP, refer to:

A2., "Vnet/IP network system configuration" in ProSafe-RS Vnet/IP (IM 32Q56H10-31E)

- **System Expansion with BCV**

Connecting two V net domains by BCV allows expanding a system.

As shown in the above figure, CENTUM and ProSafe-RS can be connected within one domain. Also, it is possible to separate CENTUM, as the control system, and ProSafe-RS as the safety system, in different domains and connect them with BCV.

The engineering of BCV can be performed not from SENG but from CENTUM ENG. Therefore, when adding BCV to a system consisting of only SCSs and SENGs to connect the system to another V net domain, the system builder function of CENTUM needs to be added together with BCV.

**SEE
ALSO**

For more information about BCV, refer to:

- CENTUM VP Communication Devices Reference (IM 33K03M10-50E)
- CENTUM VP Reference Communication Devices (IM 33M01A30-40E)
- CS 1000/CS 3000 Reference Communication Devices (IM 33S01B30-01E)

● System Expansion with CGW

Connecting two V net domains by CGW for a wide-area connection makes it possible to expand a system. Using CGW allows remote V net domains to be connected through a dedicated line and so on.

Engineering of CGW is performed by CENTUM ENG. SENG cannot perform CGW engineering. Therefore, when making a wide-area connection by adding CGW to the structure having only SCSs and SENGs, additional CENTUM ENG function is required together with CGW.

Furthermore, when making a wide-area connection with SCSs via CGW, SENG should be placed in the same domain as SCSs.



IMPORTANT

If there are SCSs at both sides of the wide-area connection, it is necessary to consider the location and the number of SENGs to install, paying attention to the performance and reliability of the dedicated line.

**SEE
ALSO**

For more information about CGW, refer to:

- CENTUM VP Communication Devices Reference (IM 33K03M10-50E)
- CENTUM VP Reference Communication Devices (IM 33M01A30-40E)
- CS 1000/CS 3000 Reference Communication Devices (IM 33S01B30-01E)

● System Expansion with V net Router Connection: SCSP2/SCSP1

It is possible for SENG and/or SCS in a Vnet/IP domain to access an SCS in a V net domain. It is also possible to access an SCS in a V net domain from a CENTUM system and/or Ex-aopc client in a Vnet/IP domain via a V net router. The V net router is engineered by using the system builders of CENTUM.

When connecting a V net router, make sure to check that the load on the V net router caused by communication passing through the V net router will not become excessive.

TIP

V net routers (AVR10D) are classified into two types of behavioral specification, based on their hardware style and system software revisions. In this document, the two types are defined as "V net router of style S3 or above" and "V net router of a style below S3" as follows.

- V net router of style S3 or above
The style of AVR10D is S3 or above and the "operating mode" of V net router is set to [Standard mode] in the System View of CENTUM VP R5.01 or later.
- V net router of a style below S3
For all cases other than the condition described in "V net router of style S3 or later"

If no style is mentioned in explanations about the operation of the V net router in this document, the operation is common to all AVR10D styles and ProSafe-RS/CENTUM VP software revisions.

The following functions are implemented in the V net router connection configuration.

- Perform engineering and maintenance of SCS in a V net domain from SENG in a Vnet/IP domain
- Perform engineering and maintenance of SCS in a Vnet/IP domain from SENG in a V net domain
- Perform safety communication between SCS in a Vnet/IP domain and SCS in a V net domain
- Perform operation and monitoring of SCS in a V net domain from an HIS in a Vnet/IP domain
- Perform operation and monitoring of SCS in a Vnet/IP domain from an HIS in a V net domain
- Refer to data in an SCS in a V net domain and write data to an external communication FB from an FCS in a Vnet/IP domain
- Refer to data in an SCS in a Vnet/IP domain and write data to an external communication FB from an FCS in a V net domain
- Collect and display SOE and diagnostic information of an SCS in a V net domain from the CENTUM Sequence of Events Manager or ProSafe-RS SOE Viewer installed on an HIS in a Vnet/IP domain
- Install the ProSafe-RS SOE OPC Interface package on a PC in a Vnet/IP domain or V net domain and use the HIS or SENG as an OPC server to display SCS events on an OPC client (e.g., Exaquantum) in a Vnet/IP domain.
- Set up an Exaopc server in a Vnet/IP domain or V net domain and access data on the SCS from an OPC client (e.g., Exapilot) in a Vnet/IP domain.
- V net router of style S3 or above: Connect multiple Vnet/IP domains on a single V net domain
- V net router of style S3 or above: Execute SCS global switch communication (link transmission between FCS and SCS stations) between a V net domain and a Vnet/IP domain connected to a V net router.
- V net router of style S3 or above: Effect a time transfer from a V net domain to a Vnet/IP domain with the V net domain as the clock master, or vice versa
- The following specifications are applied when using a V net router of a style below S3
The V net domain cannot be made the clock master, which means that you cannot change the time on the Vnet/IP domain even if you set the time from a SENG or HIS on the V net domain

SEE ALSO

For more information about Vnet/IP, refer to:

ProSafe-RS Installation Guidance (TI 32S01J10-01E)

● **System Expansion with WAC Routers**

WAC routers can be used to expand the system by connecting two or more Vnet/IP domains in remote sites using a wide-area network.

You can engineer WAC router by using the System Builders of CENTUM VP. You cannot engineer WAC routers by using the SENG.

Therefore, if you plan to add WAC routers to the system that consists of only SENG and SCS, and connect the system to a wide-area network, the System Builders of CENTUM VP are required.

Moreover, when connecting SCS with wide-area network through WAC routers, install an SENG in each Vnet/IP domain that are connected by WAC routers. Engineering operations such as offline download to SCS must be performed from the SENG that is connected to each Vnet/IP domain.

The following figure shows an example of system expansion using WAC routers.

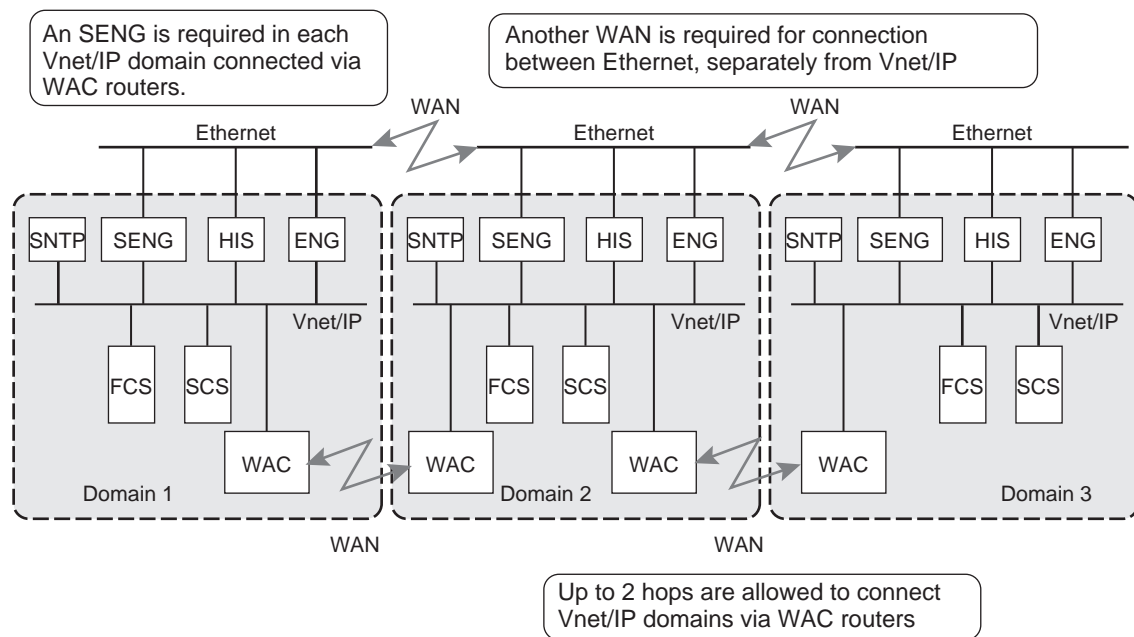


Figure 2.1.1-11 Example of System Expansion with WAC Routers

SEE ALSO For more information about how to set WAC router, refer to:

8., "Wide Area Communication Router " in CENTUM VP Communication Devices Reference (IM 33K03M10-50E)

■ **Communicable Extent**

Safety communications for which SIL3 is guaranteed are possible between SCS stations in V net and Vnet/IP domains.



IMPORTANT

Make sure that the system program release numbers for SCSs to communicate with each other are correct.

SEE ALSO

For more information about the software release numbers allowing for Inter-SCS communications, refer to:

Appendix 4., "Compatibility between Revisions and Cautionary Notes for Upgrading" in Installation (IM 32Q01C50-31E)

● **Inter-SCS Safety Communication in Vnet/IP Domains**

It is possible to perform safety communications between all SCS stations in the same Vnet/IP domain or different Vnet/IP domains. Even if control communication and open communication coexist on Vnet/IP, SIL3 is guaranteed.

● **Inter-SCS Safety Communication in a V net domain**

It is possible to perform Inter-SCS Safety Communication between SCS stations in the same V net domain or different V net domains to a range of up to 2 BCV or CGW hops.

● **Inter-SCS Safety Communication in Systems in which a V net Domain and a Vnet/IP Domain are Connected**

Inter-SCS Safety Communications have different network reach ranges according to the specifications of V net router to be applied.

- Network range for style S3 or above
In a communications route between two stations, network reach is up to 4 hops for connections between a V net domain and a Vnet/IP domain via a V net router, and up to 2 hops for connections between V net domains via a BCV or CGW.

The following figure shows the domain configuration for the maximum network range when V net routers of style S3 or above are used.

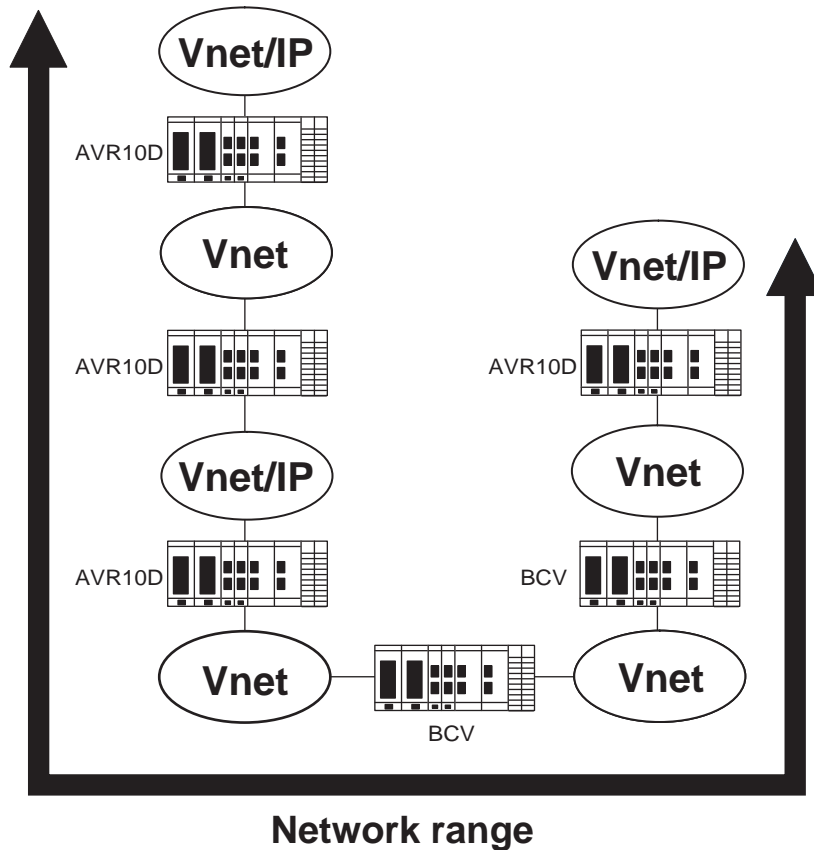


Figure 2.1.1-12 Network Range when a V net Router of Style S3 or Above is Used

- Network range for style below S3

The network reach range for inter-SCS Safety Communications is up to 2 hops for connections between V net domains via a BCV or CGW. It is not possible to have a V net domain on a mid-stream route communicating between Vnet/IP stations. That is, the configuration of SCSs on two Vnet/IP domains with a V net domain in between is not allowed.

The following figure shows the domain configuration for the maximum network range when V net routers of a style below S3 are used.

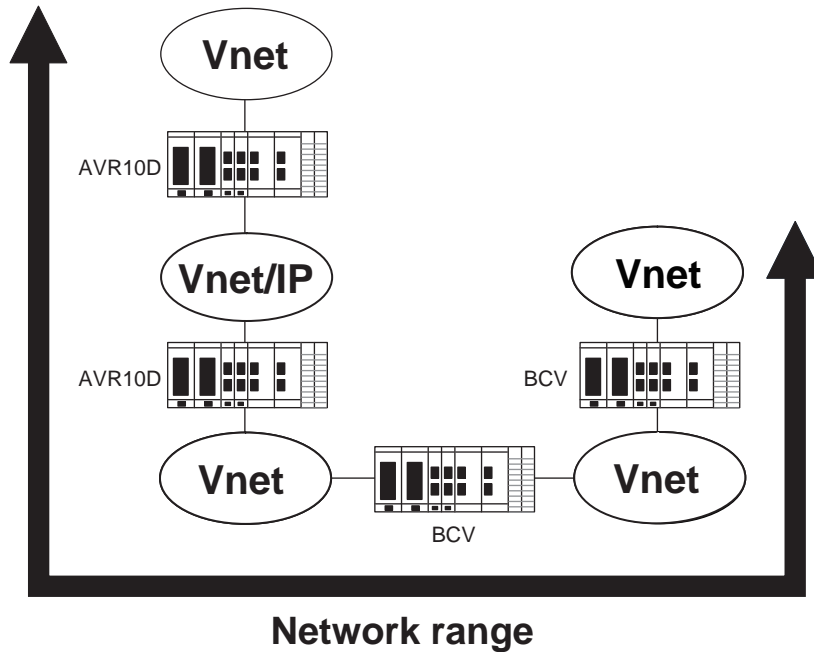


Figure 2.1.1-13 Network Range when a V net Router of a Style Below S3 is Used

- **Communication Between SENG and SCS**

SCS engineering and maintenance is carried out from the SENG via V net or Vnet/IP.

It is possible to perform safety communications between SENG and SCS stations in V net and Vnet/IP domains.

The communicable network range is the same as for executing Inter-SCS safety communication.

At least one SENG should be connected on the V net or Vnet/IP allowing communications with SCS.

- **Communication Between HIS/FCS and SCS**

It is possible to communicate with an SCS in a V net domain or a Vnet/IP domain from an HIS/FCS. The communicable network range is the same as for executing Inter-SCS safety communication.

This communication has no impact on safety functions executed in SCS.

- **Precautions when Engineering CENTUM Systems for Using V net Routers: SCSP2/SCSP1**

V net routers are engineered using CENTUM ENG. Take the following precautions when engineering the routers.

- **TCP/IP Communication Relay Processing**

When the system consists of V net domains and Vnet/IP domains, enable [Transfer TCP/IP to FCS] in the setting items of the V net router (one of the settings of the CENTUM system builder function) to allow the V net router to relay the TCP/IP broadcast frames in both directions. This function allows the TCP/IP communication between the SENG and SCS to be performed across domains.

- **Transferring System Time**

- If you are using a V net router style S3 or above, open the "V net router" property from System View in CENTUM VP R5.01 or later, and specify the Transfer system time ([Transfer upper] or [Transfer lower]). This allows the time on either the V net domain or the Vnet/IP domain connected to the V net router to be transferred to another domain as the master.
- In the case of using a V net router style below S3, the Vnet/IP domain is always the upper domain. It is not possible to transfer the time from the lower domain to the upper domain.

- **Time Discrepancy Between Domains**

A maximum time discrepancy of 5 seconds occurs between two domains connected via a V net router. One way to reduce the time discrepancy is to synchronize each domain with an external absolute time rather than effecting a time transfer via the V net router.

■ Precautions when Engineering CENTUM Systems for Using Vnet/IP Domains: SCSP2/SCSP1

- **TCP/IP Communication Relay Processing**

When the system consists of multiple Vnet/IP domains, enable [FCS TCP] in the setting items of the domain property (one of the settings of the CENTUM system builder function) to allow to relay the TCP/IP broadcast frames in both directions. This function allows the TCP/IP communication between the SENG and SCS to be performed across domains.

■ Precautions when Engineering CENTUM Systems for Using BCV and CGW

BCV and CGW engineering are performed by CENTUM ENG. In this case, follow the precautions below.

- **TCP/IP Communication Relay Processing**

In the CENTUM Integration Configuration, enable the "Transfer TCP/IP to FCS" in the setting items of BCV or CGW (one of the settings of the CENTUM system builder function), to allow the BCV or CGW to relay TCP/IP broadcast frames in both directions. This function allows the TCP/IP communication between the SENG and SCS to be performed across domains.

- **Time-related Function**

BCV and CGW have the function of transferring the time setting when time is set in the Adjust Time dialog on HIS or SENG.

**SEE
ALSO**

For more information about TCP/IP communication relay processing and time-related function, refer to:

- CENTUM VP Communication Devices Reference (IM 33K03M10-50E)
- CENTUM VP Reference Communication Devices (IM 33M01A30-40E)
- CS 1000/CS 3000 Reference Communication Devices (IM 33S01B30-01E)

- **Time Discrepancy Between Domains**

A maximum time discrepancy of 5 seconds occurs between two domains connected via a BCV. Times are not synchronized automatically when the time discrepancy increases between two domains connected via CGWs. One way to reduce the time discrepancy in either case is to synchronize each domain with an external absolute time. In this case, ensure that you do not transfer the time by BCV or receive the system time via CGW.

- **Precautions when Engineering CENTUM VP Systems for Using WAC Router**

A WAC router is engineered on the CENTUM VP side. When connecting the WAC router to ProSafe-RS, be careful of the following points.

- **Priority Control of the Inter-SCS Safety Communication**

A WAC router has the function to give priority to the inter-SCS safety communication, if the communication traffic between Vnet/IP domains exceeds the limit of bandwidth specified in the builder. When performing inter-SCS safety communication through WAC routers, be sure to set WAC routers to enable this function.

**SEE
ALSO**

For more information about how to set WAC router, refer to:

8., "Wide Area Communication Router " in CENTUM VP Communication Devices Reference (IM 33K03M10-50E)

2.1.2 IT Security

This section describes requirements for IT security (supported since R2.01).

For SENG in a ProSafe-RS system, Windows OS is used as a platform. Therefore, it is necessary to prevent, detect and recover from computer viruses and attacks from the external via network. (Measures such as network access control using a firewall and the backup of system.)

In the CENTUM integration structure, it is necessary to consider comprehensive IT security including ProSafe-RS system and CENTUM system.

You can harden the security of the PC designated as a SENG terminal to enhance the ProSafe-RS IT security (PC hardening). This section describes the details regarding PC hardening and the setting guidelines.

TIP

When you attempt to combine ProSafe-RS and CENTUM VP, the security settings need to be performed at the installation of ProSafe-RS and CENTUM VP together.

When ProSafe-RS is integrated with CS 3000, select [Legacy model] in IT Security Tool.

SEE ALSO

For more information about setup procedure of PC security, refer to:

2., "Security Models" in [ProSafe-RS Security Guide \(IM 32Q01C70-31E\)](#)

■ An Example of Registering a User to the User Account

IT security enhancement for a PC can protect the ProSafe-RS system from the illegal access by any user other than the user of ProSafe-RS user groups. For protecting the ProSafe-RS system from the accidental mistaken accesses by the users of ProSafe-RS groups, the ProSafe-RS Security features should be used. By combining IT security enhancement for a PC and ProSafe-RS Security, you can fortify security of ProSafe-RS.

The typical examples of registering a ProSafe-RS user to the user groups are shown as follows:

(A) ProSafe-RS Engineer (Integrated with CENTUM VP)

ProSafe-RS Engineer user should be assigned to both PSF_ENGINEER group of ProSafe-RS and CTM_ENGINEER group of CENTUM VP.

(B) ProSafe-RS Engineer (Not Integrated with CENTUM VP)

ProSafe-RS Engineer user should be assigned only to the PSF_ENGINEER group.

(C) Maintenance and service persons

The user who requires the role for upgrading SENG software to newer versions, maintaining or changing the hardware components such as I/O modules should be assigned only to the PSF_MAINTENANCE group.

(D) Network and System Administrator (User who is responsible for network maintenance)

This user is considered as the administrative user of Windows environment in SENG. This user needs to be assigned only to the PSF_MAINTENANCE group.

(E) User account for emergency attention (For domain or parallel management in standard model)

When ProSafe-RS system is running in an Windows domain environment, if the domain controller encounters an abnormality, no one can logon to the SENG with the domain account. You need to prepare the user accounts who are assigned to the PSF_MAINTENANCE_LCL group for an emergency attention. If the domain controller encounters an abnormality, user can logon to the SENG with this user account, then maintain and operate ProSafe-RS.

Though the users in the above groups are all granted with the Write permission to all the Project folders, in the cases of (C) and (D), the Write permission is not required. An engineer should define a password by using the security feature of the project database and keep the password as secret to the users whom you do not grant the Write permission so as to protect the project database. Moreover, ProSafe-RS provides security features for accessing the SCS and for Maintenance Support Tool. These security features can be utilized in accordance with the role of the users so as to protect the database and SCS from the accidental operation mistakes.

**SEE
ALSO**

For more information about user groups of ProSafe-RS mentioned in the examples, refer to:

[2.2, "User/Group Management" in ProSafe-RS Security Guide \(IM 32Q01C70-31E\)](#)

For more information about user groups of CENTUM VP mentioned in the examples, refer to:

CENTUM VP Installation (IM 33K01C10-50E)

2.2 Hardware Configuration

This section describes the SCS hardware structure of ProSafe-RS and the hardware equipment forming the entire system.

■ Outline of Hardware Configuration

● Hardware Configuration: SCSV1/SCSP1

A SCS is made up of a Safety Control Unit (CPU node) and multiple Safety Node Units (I/O nodes). Up to nine I/O nodes can be connected. When only a few I/O modules are required, the SCS may consist of a CPU node only. The following figure shows the hardware configuration of SCSV1.

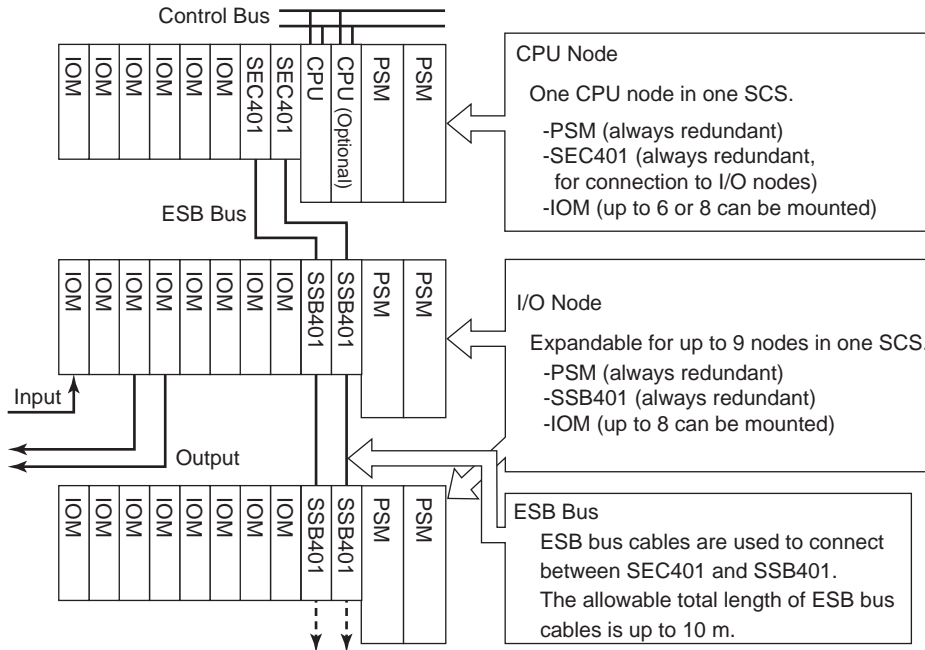


Figure 2.2-1 Hardware Configuration of SCSV1/SCSP1

Table 2.2-1 Main Hardware Module of SCSV1/SCSP1

Name	Description	Note
CPU	CPU Modules	SCP401, SCP451
IOM	Input/Output Modules	-
PSM	Power Supply Module	Model SPW48x always redundant
SEC401	ESB Bus Coupler Module	Installed in Slots 7 and 8 (always redundant)
SSB401	ESB Bus Interface Module	Always redundant
CPU Node	Node which has CPU Module on it	SSC10S/SSC10D, SSC50S/SSC50D
I/O Node	Node which does not have CPU Module on it	Node to which CPU is not mounted
ESB Bus	Extended Serial Backboard Bus	Bus to connect nodes

● Hardware Configuration: SCSP2

When CPU nodes are SSC60D or SSC60S (SCSP2), it is possible to mount SEC401 or SEC402 as ESB bus coupler modules. If SEC402 is mounted, ESB buses can be connected to the upper and the lower connectors, allowing connection of up to 13 I/O nodes. Note that when 10 or more I/O nodes are to be connected, the license of CFS1350 Node Expansion

Package has to be granted to the SENG. The following figure shows the SCS hardware configuration where SEC402 is used to connect I/O nodes.

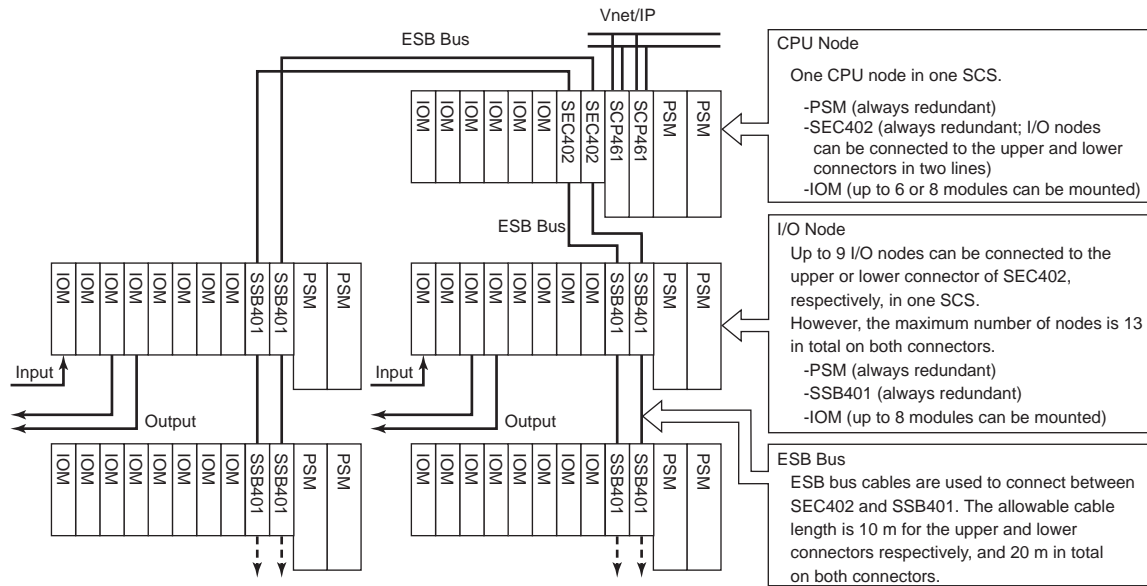


Figure 2.2-2 SCS Hardware Configuration (Example of SCSP2)

Table 2.2-2 Main Hardware Module of SCS (SCSP2)

Name	Description	Note
CPU	CPU Modules	SCP461
IOM	Input/Output Modules	-
PSM	Power Supply Module	Model SPW48x always redundant
SEC402 (*1)	ESB Bus Coupler Module	Used when I/O nodes are used. Installed in slots 7 and 8 of CPU node (always redundant) . Cannot be used for SCSV1/SCSP1.
SSB401	ESB Bus Interface Module	Always redundant
CPU Node	Node which has CPU Module on it	SSC60D/SSC60S
I/O Node	Node which does not have CPU Module on it	Node to which CPU is not mounted
ESB Bus	Extended Serial Backboard Bus	Bus to connect nodes

*1: SEC401 is available on SCSP2. The specification for using SEC401 is the same as that of SCSP2 and SCSP1/SCSV1.

SEE ALSO

For more information about SCS hardware, refer to:

- 1., "Hardware Configuration and Names of Components" in Safety Control Stations (Hardware) (IM 32Q06C10-31E)

■ CPU Node

The following table shows the types of CPU node available.

Table 2.2-3 CPU Node Type

Model	Name	CPU Node fan
SSC60D-S (*1)	Duplexed Safety Control Unit (for Vnet/IP, Rack Mountable Type, Standard Type)	No

Continues on the next page

Table 2.2-3 CPU Node Type (Table continued)

Model	Name	CPU Node fan
SSC60D-F (*1)	Duplexed Safety Control Unit (for Vnet/IP, Rack Mountable Type, Wide Range Temperature Type)	Yes
SSC60S-S (*1)	Safety Control Unit (for Vnet/IP, Rack Mountable Type, Standard Type)	No
SSC60S-F (*1)	Safety Control Unit (for Vnet/IP, Rack Mountable Type, Wide Range Temperature Type)	Yes
SSC50D-S (*2)	Duplexed Safety Control Unit (for Vnet/IP, Rack Mountable Type, Standard Type)	No
SSC50D-F (*2)	Duplexed Safety Control Unit (for Vnet/IP, Rack Mountable Type, Wide Range Temperature Type)	Yes
SSC50S-S (*2)	Safety Control Unit (for Vnet/IP, Rack Mountable Type, Standard Type)	No
SSC50S-F (*2)	Safety Control Unit (for Vnet/IP, Rack Mountable Type, Wide Range Temperature Type)	Yes
SSC10D-S	Duplexed Safety Control Unit (for V net, Rack Mountable Type, Standard Type)	No
SSC10D-F	Duplexed Safety Control Unit (for V net, Rack Mountable Type, Wide Range Temperature Type)	Yes
SSC10S-S	Safety Control Unit (for V net, Rack Mountable Type, Standard Type)	No
SSC10S-F	Safety Control Unit (for V net, Rack Mountable Type, Wide Range Temperature Type)	Yes

*1: Available in R2.03.00 or later

*2: Available in R1.02.00 or later

■ I/O Node

The following table shows the types of I/O Node available.

Table 2.2-4 I/O Node Type

Model	Description
SNB10D	Node Unit for Dual-Redundant ESB Bus (19-inch Rack Mountable)

SEE ALSO

For more information about SCS hardware, refer to:

- Safety Control Units, Duplexed Safety Control Units (for Vnet/IP, Rack Mountable Type) (GS 32Q06D10-31E)
- Safety Control Units, Duplexed Safety Control Units (for Vnet/IP, Rack Mountable Type) (GS 32Q06D20-31E)
- Safety Control Units, Duplexed Safety Control Units (for V net, Rack Mountable Type) (GS 32Q06D30-31E)
- Safety Node Unit (Rack Mountable Type) (GS 32Q06K10-31E)

■ I/O Modules

The following table shows the types of I/O modules that can be installed in a CPU node or I/O node.

Table 2.2-5 I/O Modules

Type	Model	Channels	I/O specification	Remarks
Digital Input Module	SDV144	16	24 V DC, Non-voltage contact input Module Isolation	Safety (SIL3)
Digital Output Module	SDV521 (*1)	4	24 V DC, Module Isolation, 2 A/CH	Safety (SIL3)
	SDV526 (*2)	4	100-120 V AC, Module Isolation, 0.5 A/CH	Safety (SIL3)
	SDV531	8	24 V DC, Module Isolation, 0.6 A/CH	Safety (SIL3)
	SDV531-L (*1)	8	24 V DC, Module Isolation, 0.6 A/CH	Safety (SIL3) Supports long cable connection
	SDV53A (*3)	8	48 V DC, Module Isolation, 0.6 A/CH	Safety (SIL3)
	SDV541 (*4)	16	24 V DC, Module Isolation, 0.2 A/CH	Safety (SIL3)
Analog Input Module	SAI143	16	4-20 mA Module Isolation	Safety (SIL3)
	SAI143-H (*4)	16	4-20 mA Module Isolation	Safety (SIL3)
	SAV144	16	1-10 V Module Isolation	Safety (SIL3)
	SAT145 (*5)	16	Thermocouple / mV, Isolated channels	Safety (SIL3)
	SAR145 (*5)	16	Resistance temperature detector, Isolated channels	Safety (SIL3)
Analog Output Module	SAI533-H (*4)	8	4-20 mA Module Isolation	Safety (SIL3)
Serial Communication Module	ALR111 (*6)	2 (number of ports)	RS-232C	Interference-free
	ALR121 (*6)	2 (number of ports)	RS-422/RS-485	Interference-free
Ethernet Communication Module	ALE111(*7)	1 (number of ports)	10 BASE-T	Interference-free

*1: These I/O modules can be used in R1.03.00 or later.

*2: R2.02.00 or later supports this model. Minimum Output Holding Time must be considered when making applications for SDV526. For the required minimum output holding time, see the following General Specifications (GS) for digital I/O modules.

*3: R2.03.00 or later supports this model.

*4: These I/O modules can be used in R1.02.00 or later.

*5: These input modules can be used in R.3.01.00 or later.

*6: The serial communication module can be used for Modbus communication (Slave) and subsystem communication (Master).

*7: The Ethernet communication module can be used for Modbus slave communication. This module can be used in R3.02.00 or later.

When the CPU node of SCS is SSC10D or SSC10S, do not define ALE111.

I/O modules can have a redundant configuration to improve their availability.

For external equipment such as field power supplies for I/O, sensors, etc. which is connected to the I/O modules, it is recommended to use equipment designed to prevent electrical shock (e.g. SELV or PELV equipment which is IEC950 certified or equivalent).

SEE ALSO

For more information about specifications of I/O modules, refer to:

- [1.4, "Input/Output Modules" in Safety Control Stations \(Hardware\) \(IM 32Q06C10-31E\)](#)
- [ProSafe-RS Outline of I/O Modules \(GS 32Q06K20-31E\)](#)
- [Analog I/O Modules \(for ProSafe-RS\) \(GS 32Q06K30-31E\)](#)
- [Digital I/O Modules \(for ProSafe-RS\) \(GS 32Q06K40-31E\)](#)

■ Devices Related to Optical ESB Bus Repeater

ProSafe-RS allows for locating I/O nodes at remote places by using Optical ESB Bus Repeater modules. I/O nodes are connected on the ESB bus (the I/O bus of the SCS) network which is extended by using Optical ESB Bus Repeater master modules (SNT401/SNT411) and Optical ESB Bus Repeater slave modules (SNT501/SNT511). Both the demand reaction time and fault reaction time are the same as those when I/O nodes are connected with non-optic ESB bus cables.

The following is an outline of the Optical ESB Bus Repeater connection functions.

- Maximum number of nodes (including the CPU node)
When SEC401 is used (SCSV1/SCSP1/SCSP2): 10 nodes/SCS
When SEC402 is used (SCSP2): 14 nodes/SCS
- Topology: Chain, star, or a mix of the two
- Maximum extension distance of fiber-optic cable (*1): 5 km for SCSV1 and 50 km for SCSP1/SCSP2.
- Maximum distance between SNT401 and SNT501 (length of fiber-optic cable between layers): 5 km
- Maximum distance between SNT411 and SNT511 (length of fiber-optic cable between layers): 50 km
- Maximum number of layers in fiber-optic cable connection: 2
For SCSP2/SCSP1, mixed use of SNT401/SNT501 and SNT411/SNT511 is allowed. For example, it is possible to connect 2 layers of SNT401 and SNT501, 5 km each, to extend the distance up to 10 km.
It is also possible to use SNT401/SNT501 for the first layer (5 km), and use SNT411/SNT511 for the second layer (45 km) for extension to a total of 50 km.
- Where to install Optical ESB Bus Repeater modules: Slots 1 to 6 of CPU nodes, slots 1 to 8 on I/O nodes, and slots 1 to 10 on the Unit for Optical ESB Bus Repeater module (SNT10D)
- Redundancy: Both Optical ESB Bus Repeater module and fiber-optic cable are always redundant. (*2)
- Maximum distance of ESB bus cable connection: 10 m; 10 m each for the upper and lower connectors respectively when SEC402 is used.

*1: The "maximum extension distance of fiber-optic cable" refers to the total extension distance of fiber-optic cable from the CPU node to the last I/O node connected.

*2: It is recommended to set the same length for left and right fiber-optic cables as a general rule.

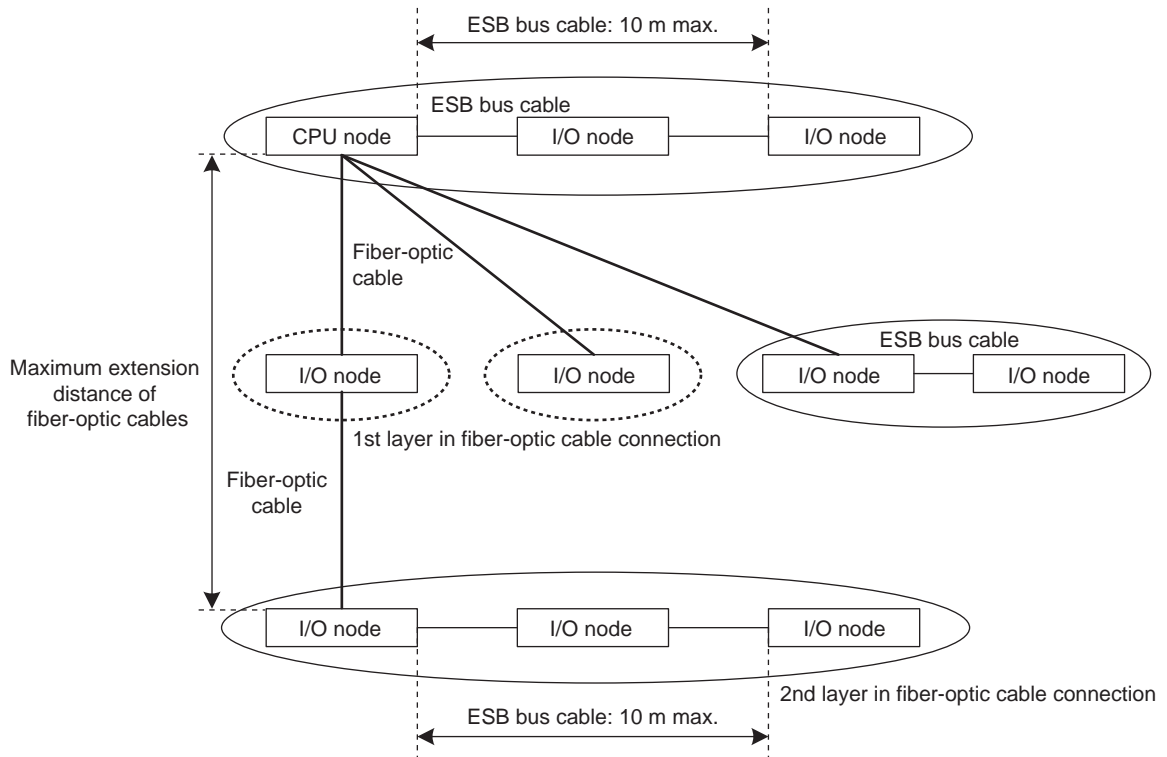


Figure 2.2-3 Overview of Optical ESB Bus Repeater Connection Function (Example of Connection with SEC401)

The following table shows the hardware used in relation to the Optical ESB Bus Repeater.

Table 2.2-6 Hardware Related to Optical ESB Bus Repeater

Model	Name	Description	Remarks
SNT10D	Unit for Optical ESB Bus Repeater Module	Unit dedicated for mounting Optical ESB Bus Repeater modules. This unit has redundant power supply modules mounted. 10 slots are provided for mounting SNT401s/SNT501s and SNT501s/SNT511s.	-
SNT401	Optical ESB Bus Repeater Master Module	Master module for extending ESB bus with fiber-optic cable(s). The distance between SNT401 and SNT501 can be extended up to 5 km (two layers total, up to 10 km for SCSP2/SCSP1)	-
SNT501	Optical ESB Bus Repeater Slave Module	Slave module for extending ESB bus with fiber-optic cable(s).	-
SNT411	Optical ESB Bus Repeater Master Module	Master module for extending ESB bus with fiber-optic cable(s). The distance between SNT411 and SNT511 can be extended up to 50 km.	These modules cannot be installed in SCSV1
SNT511	Optical ESB Bus Repeater Slave Module	Slave module for extending ESB bus with fiber-optic cable(s).	

SEE ALSO

For more information about specifications and installation restrictions of hardware used in relation to the Optical ESB Bus Repeater, refer to:

[1.3, "Configuration of Unit for Optical Bus Repeater Module" in Safety Control Stations \(Hardware\) \(IM 32Q06C10-31E\)](#)

For more information about software setups before using the Optical ESB Bus Repeater, refer to:

[3.1.3, "SCS Constants Builder" in Engineering Reference \(IM 32Q04B10-31E\)](#)

■ Precautions for Mounting the Optical ESB Bus Repeater Module

- Ensure that the optical attenuation between SNT411 and SNT511 meets the conditions in the following table. If the conditions are not met, use an attenuator to ensure that the conditions are met.

Table 2.2-7 Required optical attenuation between SNT411 and SNT511

SNT411/SNT511 style	Required attenuation
Style S2 and above	3 dB or more
Style S1	1 dB or more

- In the case of SCSP2/SCSP1, the time accuracies for SOE data (discrete inputs) are as follows.

Table 2.2-8 Time Accuracies for SOE Data (Discrete Inputs) (In the Case of SCSP2/SCSP1)

Distance of extension by Optical ESB Bus Repeater (One of the two target SCSs, whichever the extension distance is longer.)	Time accuracies
No extension	± 1 ms
Extension within 25 km	± 2 ms
Extension from 25 km to 50 km	± 3 ms

- As the load on the SCS increases when the distance of ESB bus extended by the Optical ESB Bus Repeater module becomes longer, the number of I/O modules that can be installed may be restricted. The time required for IOM download or communication module startup becomes longer compared to the cases where the Optical ESB Bus Repeater module is not used.

Be sure to make the following definitions when using the Optical ESB Bus Repeater modules. Items to be defined vary depending on the SCS type.

- Required settings in SCSV1 and problems that occur if settings are not made
In SCS Constants Builder, set [Optical ESB Bus Repeater] to [Yes] and specify the correct maximum extension distance in [Maximum Extension Distance]. If the Optical ESB Bus Repeater modules are used without these settings, the node data and SOE data will not be updated correctly.
- Required settings in SCSP2 and problems that occur if settings are not made
For SCSP2 in I/O Parameter Builder, set a node setting item [Extends Node Bus] to [Yes] and specify the actual node distance on the ESB bus from the CPU node in [Extends To] for all nodes connected via Optical ESB Bus Repeater modules. Communication errors may occur between CPU modules and the nodes if the Optical ESB Bus Repeater modules are used without these node settings being configured correctly. If this happens, the data of the modules in nodes and SOE data are not updated correctly. As a result, the output modules output the output value at fault.
- Required settings in SCSP1 and problems that occur if settings are not made.
Ensure that the settings are configured in each of the following builders.

Table 2.2-9 Settings required in SCSP1

Builder to be set up	Required settings	Precautions
SCS Constants Builder	Set [Optical ESB Bus Repeater] to [Yes] and specify the correct maximum extension distance in [Maximum Extension Distance].	If the Optical ESB Bus Repeater modules are used without these settings, the node data and SOE data will not be updated correctly.

Continues on the next page

Table 2.2-9 Settings required in SCSP1 (Table continued)

Builder to be set up	Required settings	Precautions
I/O Parameter Builder	Set the node setting item [Extends Node Bus] to [Yes] and specify the actual node distance on the ESB bus from the CPU node in [Extends To] of the I/O Parameter Builder for all nodes connected via Optical ESB Bus Repeater modules.	If you do not specify the distance to the node, the system behaves as if the corresponding I/O node is located at the maximum extension distance. Although I/O modules function correctly, the CPU load fluctuation may become large if abnormalities occur. Be sure to specify the node distance in order to reduce CPU load fluctuation at abnormality occurrence.



IMPORTANT

When performing Modbus slave communication

The following precautions should be observed for nodes on which Optical ESB Bus Repeater modules are mounted.

- In the case of SCSP2/SCSP1, be sure to specify the node extension distance in the I/O Parameter Builder for the I/O nodes where ALR111, ALR121, or ALE111 is mounted.
- ALR111, ALR121, or ALE111 cannot be mounted on I/O nodes located at a distance of 5 km or further.

Precautions when mounting SNT401/SNT411 and SNT501/SNT511

- If SNT401/SNT411 and SNT501/SNT511 are mounted on the SNT10D, set DIP switch 1 (mounting unit setting) on the SNT401/SNT411 and SNT501/SNT511 to "0." If the switch is set to 1, errors on one of the SNT10D power modules will not be reported. (*1)
- If SNT401/SNT411 and SNT501/SNT511 are mounted on the CPU node or I/O node, set DIP switch 1 (mounting unit setting) on the SNT401/SNT411 and SNT501/SNT511 to "1." If it is set to "0," one of the power modules on the CPU node or I/O node will cause the failure of one of the redundant SNT401/411 or SNT501/SNT511. (*1)

*1: The default setting of DIP switch 1 is 0. This setting status can be checked on the LED display on the front of the module. If DIP switch 1 is set to 1, the LED display "NODE-1" is turned on in green.

Precaution when performing HART communication

- If the Optical ESB Bus Repeater node extension distance exceeds 25 km on SCSP1 and HART communication is performed periodically, the scan period must be set to 100 ms or longer.

■ Safety Engineering PC (SENG)

SENG is the PC with Windows, where SCS engineering and maintenance functions are executed.

● PC

For the specifications for recommended PCs, see the General Specifications (GS).

**SEE
ALSO**

For more information about specifications for recommended PC, refer to:

Safety System Generation and Maintenance Package (GS 32Q04C10-31E)

- **Connection to V net**

A V net interface card (VF702 or VF701) is used. VF702 is installed in a PCI Express slot, and VF701 is installed in a PCI slot of SENG.

- **Connection to Vnet/IP: SCSP2/SCSP1**

A Vnet/IP interface card (VI702 or VI701) is used. VI702 is installed in a PCI Express slot, and VI701 is installed in a PCI slot of the SENG.

■ Equipment for Expanding System

Equipment to use for expanding system of ProSafe-RS is shown as follows.

- **V net Bus Repeater (YNT512D)**

A V net Bus Repeater is used to lengthen V net Bus coaxial cables.

**SEE
ALSO**

For more information about maximum number of bus repeaters to use and maximum extended length, refer to:

ProSafe-RS Safety Instrumented System Overview (for V net) (GS 32Q01B20-31E)

- **V net Optical Bus Repeater (YNT511D/YNT522D)**

A V net optical repeater is used to lengthen V net by using fiber-optic cable.

**SEE
ALSO**

For more information about maximum number of bus repeaters to use and maximum extended length, refer to:

ProSafe-RS Safety Instrumented System Overview (for V net) (GS 32Q01B20-31E)

- **V net Bus Converter (BCV) (ABC11D-V)**

A V net Bus Converter is used to divide V net domains. For example, it works efficiently to divide two domains into a domain for control and a domain for safety.

- **Communication Gateway Unit (CGW) (ACG10S-F)**

A Communication Gateway Unit connects between remote V net domains using private lines.

- **V net router (AVR10D): SCSP2/SCSP1**

A V net router is the hardware dedicated to connect a Vnet/IP domain and a V net domain.

TIP

Router operations may vary according to the combination of AVR10D hardware style and system software revisions, therefore the system configurations that can be built will be different.

**SEE
ALSO**

For more information about effect on the system of differences in router operations due to the AVR10D hardware style and revisions to the system software, refer to:

“● System Expansion with V net Router Connection: SCSP2/SCSP1” on page 2-11

- **WAC Router**

A WAC router expands the system by connecting two or more Vnet/IP domains.

**SEE
ALSO**

For more information about engineering of WAC router, refer to:

- [System Expansion with WAC Routers](#) on page 2-13
-

2.3 Requirements for the Size of System and Installation of Hardware

This section describes requirements for the size of system and installation of hardware including I/O modules.

■ Size of System

The number of maximum connectable stations in the system which consists of ProSafe-RS stations only and in ProSafe-RS integrated with CENTUM system is shown below respectively. Each system can be expanded as follows:

**SEE
ALSO**

For more information about FAST/TOOLS Integrated system configuration, refer to:

[2.23, "FAST/TOOLS Integrated Configuration" on page 2-143](#)

● Number of Stations (ProSafe-RS integrated with CENTUM)

- Connectable control bus: V net or Vnet/IP
- Domains that can be connected: 16
- Stations that can be connected in a domain: 64
- Stations that can be connected: 256
- Hierarchy: three-level hierarchy (three levels of control bus) (Up to two BCVs or two pairs of CGWs)

For HIS, 16 stations/domain at maximum.

For multiple domains, system generation function of CENTUM is required. In addition, V net requires BCVs and Vnet/IP requires Layer 3 switches.

● Number of Stations (consists of only ProSafe-RS stations)

- Connectable control bus: V net or Vnet/IP
- Number of domain: 1
- Stations that can be connected in a domain: 64

A system consisting of only ProSafe-RS stations cannot be configured as a multiple-domain system. Only single-domain configuration is supported.

● Number of SENG

One SENG at least is required.

● Number of SCS

The number of stations should be within the limit.

● Vnet/IP Domain Connection Specifications (ProSafe-RS Integrated with CENTUM): SCSP2/SCSP1

Connect Vnet/IP domains on each Bus with a Layer 3 switch (L3SW). This also requires the CENTUM system builder function.

- Number of connectable domains: 16 (Total of Vnet/IP domains and V net domains)
- Number of Layer 3 switches (L3SW) allowed: 15 levels

- **Connection Specifications in a Vnet/IP Domain (ProSafe-RS integrated with CENTUM): SCSP2/SCSP1**

- Number of connectable Vnet/IP stations: Max. 64 (Vnet/IP stations including V net routers)
- General-purpose Ethernet communication devices: Max. 124 (PCs, Routers, etc.)
- Distance between stations in a Vnet/IP domain: Max. 40 km
- Distance between Layer 2 switch and a station: Max. 100 m (for Unshielded Twisted Pair (UTP)); Max. 5 km (for fiber-optic cable)
- Distance between Layer 2 switches: Max. 5 km (for fiber-optic cable)
- Number of connectable Layer 2 switches in a domain: Max. 7 per each Bus. (Multilayer by cascade connection allowed)

- **Restrictions on Installation of Hardware**

There are the following restrictions on the installation of hardware on the SCS.

- In the SCS, the I/O nodes can be connected to the CPU node to expand inputs and outputs. Up to 9 I/O nodes can be connected with SCSP1/SCSV1, and up to 13 I/O nodes with SCSP2. Note that when 10 or more I/O nodes are to be connected, it is necessary to install the CFS1350 Node Expansion Package to the SENG and grant the license to the SCS.
- To connect an I/O node, SEC401s are installed in slots 7 and 8 of the CPU node. To connect 10 or more I/O nodes with SCSP2, install SEC402 instead. If you do not need to expand inputs and outputs, you can install I/O modules in slots 7 and 8.
- When configuring I/O modules in redundant configuration, install them to any slots of the following in pairs: 1 and 2, 3 and 4, 5 and 6, 7 and 8.
- For installation of I/O modules, there are two more limitations other than the above restrictions. One is imposed by electric capacity and another is imposed by ambient temperature conditions (60 to 70 deg. C) for operation.
- The Optical ESB Bus Repeater modules must be mounted within the specified operating temperature range.
- Subsystem communication and Modbus slave communication can not be executed together with a single serial communication module. Dedicated ALR111 or ALR121 is necessary for each communication.
- When the CPU node of SCS is SSC10D or SSC10S, do not define ALE111.
- When using ALE111, use the style S1 module with unit revision U:2 or later. The unit revision is indicated on the top of the module. However, the unit revision is not indicated if it is U:0.
- For subsystem communication, up to 4 serial communication modules (ALR111/ALR121) can be installed per SCS (up to 2 pairs in redundant configuration).
- For Modbus slave communication, up to 2 modules selected from among serial communication modules (ALR111/ALR121) and Ethernet communication modules (ALE111) can be installed.
- In total, up to 6 serial communication modules (ALR111/ALR121) can be installed in an entire SCS.
- With SCSP2/SCSP1, you cannot install serial communication modules (ALR111/ALR121) or Ethernet communication module (ALE111) for the purpose of Modbus slave communication in I/O nodes located further than 5 km using the optical ESB bus repeater module.

- The operating temperature is different between the Safety Control unit for Vnet/IP and the Safety Control unit for V net.

**SEE
ALSO**

For more information about restrictions on SCS hardware installation, refer to:

ProSafe-RS Outline of I/O Modules (GS 32Q06K20-31E)

For more information about the precautions for mounting the Optical ESB Bus Repeater module, refer to:

- Optical ESB Bus Repeater Module (GS 32Q06L15-31E)
- ProSafe-RS Outline of I/O Modules (GS 32Q06K20-31E)

For more information about the operating temperature of the Safety Control Unit, refer to:

ProSafe-RS Installation Guidance (TI 32S01J10-01E)

2.4 Overview of POU

POU (Program Organization Unit) is a general name for programs, function blocks and functions. Use POU properly according to the following list.

Table 2.4-1 Proper Usage for POU

Type of POU	Description	Applicable Language	Remarks
Program	It is the uppermost-level sheet for writing application logic. An engineer writes input variables, logic, and output variables as a program. When the logic is complicated, divide the logic into user-defined function blocks or user-defined functions.	<ul style="list-style-type: none"> Function Block Diagram (FBD) Ladder Diagram (LD) 	As a program does not have I/O parameters, write I/O variables in the program directly. The engineer writes the program combining variables, function blocks and functions.
Function Block	It is used for writing a logic which is shared in some programs. It is used for writing a logic which is common in some programs or for dividing a program when logic is too complicated to be involved in a program. It has two types: standard function block and user-defined function block	<ul style="list-style-type: none"> FBD LD Structured Text (ST) 	Each instance (entity) of a function block has inputs and outputs as parameters and can have local parameters as well. However, function blocks cannot have local variables for each of their definitions. Engineer writes function blocks combining I/O parameters, local parameters, function blocks and functions. When a function block is used in a program, an instance (identity) will be created.
Function	It is used for writing a logic which is shared in some programs. It has two types: standard function and user-defined function	<ul style="list-style-type: none"> FBD LD ST 	A function has I/O parameters, but has only one output parameter. Engineer writes functions combining I/O parameters and functions. Function blocks and internal variables of global attributes cannot be used within a function. Internal variables of local attributes can be used within a function, but such internal variables are initialized every time the function is called. (Initialized to the initial values specified on Dictionary View. If the initial value is absent, 0 or FALSE will be used.)

In this section, lists of function blocks and functions are shown and data types of variables for POU are explained.

■ Application Logics Written in POU

In ProSafe-RS, user can use Function Block Diagram (FBD), Ladder Diagram (LD) or Structured Text (ST) to create a POU for the application logics.

FBD can be used to create a program by using the Functions (FU) or Function Blocks (FB), and FBD can also be used to create user defined FU and FB. Some Ladder elements can be used in FBD.

In LD, programs and user-defined FU and FB are created using Ladder elements. Some FU and FB can also be used concurrently in LD.

Structured Text can be used to create FU/FB using the conditional statements and other statements.

**IMPORTANT**

Structured Text cannot be used for creating a program.

**SEE
ALSO**

For more information about designing, generating and testing the application logics, refer to:

[Appendix 1., "Guidelines for Developing Application Logic" on page App.1-1](#)

■ Function Blocks and Functions

Some FU/FB provided by the ProSafe-RS system can be used in safety loops (Safety FU/FB) and others cannot be used in safety loops (Interference-free FU/FB). FU/FB that cannot be used in safety loops are designed to be interference-free to avoid interference with the safety functions.

● Safety FU/FB

Safety FU/FB are shown as follows. All of them can be used in FBD. Some FU/FB can also be used in the Ladder Diagram.

Table 2.4-2 Safety Functions (FU)

Function Name	Description	Use on Ladder Diagram	Re-remarks
ABS	Gives the absolute (positive) value of a real value	(*1)	
SQRT	Calculates the square root of a real value	(*1)	
+ ADD	+, meaning "addition"	(*1)	
× MUL	×, meaning "multiplication"	(*1)	
– SUB	–, meaning "subtraction"	(*1)	
/ DIV	/, meaning "division"	(*1)	
SHL	Make the bits of an integer shift to the left. Shift is made on 32 bits. Zero is used to replace lowest bit.	(*1)	
SHR	Make the bits of an integer shift to the right. Shift is made on 32 bits. Highest bit is copied at each shift.	(*1)	
ROL	Make the bits of an integer rotate to the left. Rotation is made on 32 bits.	(*1)	
ROR	Make the bits of an integer rotate to the right. Rotation is made on 32 bits.	(*1)	
AND	AND	Yes(*2)	
OR	OR	Yes (*2)	
XOR	Exclusive disjunction (exclusive OR)	Yes (*2)	
NOT	Negation	Yes (*2)	
SEL	Selects one of two input values (INTEGER)	Yes (*2)	
SEL_R	Selects one of two input values (REAL)	(*1)	(*3)
SEL_T	Selects one of two input values (TIME)	(*1)	(*3)
MAX	Selects the larger of two input values (INTEGER)	(*1)	
MIN	Selects the smaller of two input values (INTEGER)	(*1)	
LIMIT	Limits the range of the input values to output (INTEGER)	(*1)	

Continues on the next page

Table 2.4-2 Safety Functions (FU) (Table continued)

Function Name	Description	Use on Ladder Diagram	Remarks
MUX4	Selects one of four input values (INTEGER)	(*1)	
MUX8	Selects one of eight input values (INTEGER)	(*1)	
MUXBOOL4	Selects one of four input values (BOOL)	(*1)	
MUXBOOL8	Selects one of eight input values (BOOL)	(*1)	
MUXREAL4	Selects one of four input values (REAL)	(*1)	
MUXREAL8	Selects one of eight input values (REAL)	(*1)	
GT	>, meaning "greater than"	(*1)	
GE	>=, meaning "greater than or equal to"	(*1)	
EQ	=, meaning "equal"	Yes (*2)	
LE	<=, meaning "less than or equal to"	(*1)	
LT	<, meaning "less than"	(*1)	
NE	≠, meaning "unequal"	(*1)	
SCALER	Converts a 0-100% range of input values into a normalized range for outputting.	(*1)	
1 GAIN	Assignment	(*1)	
IB_TO_V	Converts IO_BOOL-type input to data value	(*1)	(*3)
IB_TO_S	Converts IO_BOOL-type input to data status	(*1)	(*3)
IR_TO_V	Converts IO_REAL-type input to data value	(*1)	(*3)
IR_TO_S	Converts IO_REAL-type input to data status	(*1)	(*3)

*1: Though applicable in Ladder Diagram, since EN and ENO are attached, cannot be applied in Safety loops.

*2: Yes: Available to use

*3: These function blocks can be used in new SCS database created by SENG in R1.01.30 or later.

Table 2.4-3 Safety Function Blocks (FB)

Function Block Name	Description	Use on Ladder Diagram	Remarks
SR	Set dominate bistable	Yes(*1)	
RS	Reset dominate bistable	Yes (*1)	
R_TRIG	Detects a rising edge	Yes (*1)	
F_TRIG	Detects a falling edge	Yes (*1)	
CTU	Count up counter	Yes (*1)	
CTD	Count down counter	Yes (*1)	
CTUD	Count up/down counter.	Yes (*1)	
TP	Pulse timer which outputs pulses for a specified duration after rising edge detection.	Yes (*1)	
TON	On-delay timer	Yes (*1)	
TOF	Off-delay timer	Yes (*1)	
REPEATTIMER	Alternates TRUE and FALSE outputs at specified intervals	Yes (*1)	
FILTER	First-order lag filter	(*2)	
FILTER_S	First-order lag filter with data status analysis capability	(*2)	
ANLG1OO2D	1oo2D analog voter	(*2)	(*3)

Continues on the next page

Table 2.4-3 Safety Function Blocks (FB) (Table continued)

Function Block Name	Description	Use on Ladder Diagram	Remarks
ANLGVOTER	3-input analog voter (IO_REAL)	(*2)	(*3)
BOOLVOTER	3-input BOOL voter (IO_BOOL)	(*2)	
ANG_S	Outputs high/low alarm with scale conversion (with data status input)	(*2)	(*4) (*5) (*6)
ANLGI	Outputs high/low alarm with scale conversion	(*2)	(*4) (*5)
VEL	Detects the velocity limit exceeded	(*2)	(*4) (*5)
SYS_STAT	Manages the SCS status	(*2)	(*5)
SYS_FORCE	Manages forcing	(*2)	(*5)
SYS_DIAG	Outputs diagnosis information	(*2)	(*5)
SYS_SECURE	Manages Security level	(*2)	(*5)
SYS_SEC_CTL	Protects security level	(*2)	(*5) (*7)
SYS_IOALLST	Detects fault in all I/O channels	(*2)	(*5)
SYS_NODEST	Detects fault in all I/O channels in node	(*2)	(*5)
SYS_OUTST	Detects fault in output module channels (for 8 channels)	(*2)	(*5)
SYS_OUTST16	Detects fault in output module channels (for 16 channels)	(*2)	(*5) (*6)
SYS_INST	Detects fault in input module channels	(*2)	(*5)
SYS_CHST	Detects fault in channels	(*2)	(*5)
SYS_CERR	Indicates computation errors	(*2)	(*5) (*8)
SYS_SCA-NEXT	Indicates the extension of scan period	(*2)	(*5) (*8)
SYS_OVR	Manages override function blocks	Yes (*1)	(*5)
SYS_PSWD	Manages password function blocks	Yes (*1)	(*5)
SYS_OUTEN	Indicates Output module output status	(*2)	(*5) (*6)
SYS_ALLSD	Shuts down Station output	(*2)	(*5) (*6)
SYS_IOSD	Shuts down Module output	(*2)	(*5) (*6)
SYS_FORCE_BD	Manages forcing of Inter-SCS safety communication data	Yes (*1)	(*5) (*8)
SYS_FORCE_L T	Manages forcing of SCS Link Transmission	(*2)	(*5) (*9)
SYS_LTSTS	Indicates SCS Link Transmission reception status	(*2)	(*5) (*9)
OVR_B	Overrides from HIS (BOOL)	(*2)	(*4) (*5)
OVR_I	Overrides from HIS (INTEGER)	(*2)	(*4) (*5)
OVR_R	Overrides from HIS (REAL)	(*2)	(*4) (*5)
OVR_IB	Overrides from HIS (IO_BOOL)	(*2)	(*4) (*5)
OVR_IR	Overrides from HIS (IO_REAL)	(*2)	(*4) (*5)
PASSWD	Manipulates BOOL-type data using password from HIS	(*2)	(*4) (*5)
MOB_11	Data manual operation with two-position answerback (BOOL)	(*2)	(*4) (*5) (*6)
MOB_21	Data manual operation with three-position answerback (BOOL)	(*2)	(*4) (*5) (*6)

Continues on the next page

Table 2.4-3 Safety Function Blocks (FB) (Table continued)

Function Block Name	Description	Use on Ladder Diagram	Remarks
MOB_RS	Auto-reset data manual operation (BOOL)	(*2)	(*4) (*5) (*6)
MOA	Analog-type data manual operation	(*2)	(*4) (*5) (*6)
CONS_B	Receives data on consumer side for inter-SCS safety communication (BOOL)	(*2)	(*5)
CONS_I	Receives data on consumer side for inter-SCS safety communication (INTEGER)	(*2)	(*5)
CONS_R	Receives data on consumer side for inter-SCS safety communication (REAL)	(*2)	(*5)
PROD_B	Transmits data on producer side for inter-SCS safety communication (BOOL)	(*2)	(*5)
PROD_I	Transmits data on producer side for inter-SCS safety communication (INTEGER)	(*2)	(*5)
PROD_R	Transmits data on producer side for inter-SCS safety communication (REAL)	(*2)	(*5)
B_TO_IB	Converts data values and status to IO_BOOL-type outputs.	(*2)	(*7)
R_TO_IR	Converts data values and status to IO_REAL-type outputs.	(*2)	(*7)
GOV_B	Grouping overrides from HIS (BOOL)	(*2)	(*4) (*5) (*6)
GOV_IB	Grouping overrides from HIS (IO_BOOL)	(*2)	(*4) (*5) (*6)
LTRCV	Receives Safety Link Transmission data	(*2)	(*5)
LTSND	Sends Safety Link Transmission data	(*2)	(*5)
ANN_FUP	First-up Alarm Annunciator	Yes (*1)	(*4) (*5) (*6) (*8)
FUP_RST	Resets the First-up alarm annunciator	Yes (*1)	(*5) (*8)

- *1: Yes: Available to use
- *2: Though applicable in Ladder Diagram, since EN and ENO are attached, cannot be applied in Safety loops.
- *3: The range limitation of the fail-safe values for SCS System Programs R3.01.00 or later is different from that of earlier versions. In versions earlier than R3.01, the range limitation is from -25.0% to 125.0%. There is no range limitation in R3.01 and later versions.
- *4: FBs that can define tag names for instances. By defining tag names, mapping blocks/elements are created, which can be accessed from the HIS.
- *5: The operation of FBs in an SCS simulation test and a logic simulation test is different from the operation in an actual SCS.
- *6: These functions can be used in new SCS database created by SENG in R1.03.00 or later.
- *7: These function blocks can be used in new SCS database created by SENG in R1.01.30 or later.
- *8: These function blocks can be used in new SCS database created by SENG in R2.03.00 or later.
- *9: These function blocks can be used in new SCS database created by SENG in R1.03.00 or later.

● **Safety Ladder Elements**

Safety Ladder Elements are shown as follows. All of them can be used in Ladder Diagram. Some elements can be used in FBD.

Table 2.4-4 Safety Ladder Elements

Elements Name	Description	Use in FBD
Direct Contact	Direct Contact	Yes
Inverted Contact	Inverted Contact	Yes
Contact with Rising Edge Detection	Contact with Rising Edge Detection	Yes
Contact with Falling Edge Detection	Contact with Falling Edge Detection	Yes

Continues on the next page

Table 2.4-4 Safety Ladder Elements (Table continued)

Elements Name	Description	Use in FBD
Direct Coil	Coil	Yes
Inverted Coil	Inverted Coil	Yes
SET Coil	SET Coil	Yes
RESET Coil	RESET Coil	Yes
Coil with Rising Edge Detection	Coil with Rising Edge Detection	No
Coil with Falling Edge Detection	Coil with Falling Edge Detection	No

● Interference-free FU/FB

The following table shows the Interference-free FU/FB (No interference in safety functions). All of them can be used in FBD and Ladder Diagram. When they are used in Ladder diagrams, EN and ENO terminals are added.

Table 2.4-5 Interference-free Functions (FU)

Function Name	Description	Remarks
ANY_TO_BOOL	Converts to BOOL-type	
ANY_TO_DINT	Converts to INTEGER-type	
ANY_TO_REAL	Converts to REAL-type	
ANY_TO_TIME	Converts to TIME-type	(*1)
POW	Performs power calculation	
POWE	Calculates with a exponential function with base e	(*2)
ACOS	Calculates the Arc cosine of a real value	
ASIN	Calculates the Arc sine of a real value	
ATAN	Calculates the Arc tangent of a real value	
COS	Calculates the Cosine of a real value	
SIN	Calculates the Sine of a real value	
TAN	Calculates the Tangent of a real value	
LOG	Calculates the Common logarithm of a real value	
LOGE	Calculates the Natural logarithm of a real value	(*2)
MOD	Calculates the Modulo of an integer value	(*3)

*1: Can be used regardless the SCS database revision number when SENG software release number is R1.03.00 or later.

*2: These functions can be used in new SCS database created by SENG in R3.02.10 or later.

*3: These functions can be used in new SCS database created by SENG in R1.03.00 or later.

Table 2.4-6 Interference-free Function Blocks (FB)

Function block Name	Description	Remarks
ANN	Transmits annunciator message	(*1)
SYS_SCAN	Outputs scan time information	(*2)
SYS_IOMDSP	Outputs the IOM status	(*2)
SYS_NODEINF	Outputs node status	(*2) (*3)
SYS_ESBINF	Outputs ESB bus status	(*2) (*3)
SYS_NETST	Outputs Control bus status	(*2) (*3)
SYS_ALRDSP	Outputs status of subsystem communication modules	(*2) (*4)
SYS_ALARM	Outputs alarm transmission status	(*2)

Continues on the next page

Table 2.4-6 Interference-free Function Blocks (FB) (Table continued)

Function block Name	Description	Remarks
SYS_TIME	Outputs SCS clock information	(*2)
SYS_FORCE_SC	Manages forcing of subsystem communication data	(*2) (*4)
SYS_STAT_SC	Indicates output enable operation in subsystem communication	(*2) (*4)
SOE_B	BOOL-type SOER	(*2)
SOE_I	INTEGER-type SOER	(*2)
SOE_R	REAL-type SOER	(*2)
ECW_B	Sets data of a BOOL-Type variable from an external device	(*1) (*2)
ECW_I	Sets data of a INTEGER-Type variable from an external device	(*1) (*2)
ECW_R	Sets data of a REAL-Type variable from an external device	(*1) (*2)
AVERAGE	Calculates the average of a specified duration	
LIM_ALRM	Hysteresis on a real value for high and low limits	
SCI_B	Input from a subsystem (BOOL)	(*1) (*2) (*4)
SCI_I	Input from a subsystem (INTEGER)	(*1) (*2) (*4)
SCI_R	Input from a subsystem (REAL)	(*1) (*2) (*4)
SCO_B	Output to a subsystem (BOOL)	(*1) (*2) (*4)
SCO_I	Output from a subsystem (INTEGER)	(*1) (*2) (*4)
SCO_R	Output to a subsystem (REAL)	(*1) (*2) (*4)
LTFCS	Receives Interference-free Link Transmission data	(*2) (*5)
SYS_SETTIME	Sets the time of SCS	(*6)

*1: FBs that can define tag names for instances. By defining tag names, mapping blocks/elements are created, which can be accessed from the HIS.

*2: The operation of FBs in an SCS simulation test and a logic simulation test is different from the operation in an actual SCS.

*3: These function blocks can be used in new SCS database created by SENG in R1.02.00 or later.

*4: These function blocks can be used in new SCS database created by SENG in R1.01.30 or later.

*5: These function blocks can be used in new SCS database created by SENG in R1.03.00 or later.

*6: The function block can be used in a new SCS database created by SENG in R3.02.10 or later.

■ Data Type of Variables

● Basic Data Type

Basic data types are shown as follows.

Table 2.4-7 Basic Data Types

Data Type	Description	Remarks
BOOL	Boolean (true or false) value	TRUE=1, FALSE=0
DINT	Integer value	-2147483648 to +2147483647 (32 bit)
REAL	Real (floating) value	Complies with the IEEE format.(32 bit)
TIME	Time value	Time values from 0 milli-second to 23h59m59s999ms are used.
STRING	Character string	Use this data type only as a literal (character-string constant). Up to 255 characters can be used.

Some data types can be used as arrays in Structured Text but only as one-dimensional arrays.

**SEE
ALSO**

For more information about data types handled as one-dimensional arrays, refer to:

“■ Data Types Available in ST” on page 2-43

● Structure

The types of structure used in ProSafe-RS are shown as follows. A structure is a combination of basic data types.

Table 2.4-8 Structures

Data Type	Description	Remarks
IO_REAL	Used for input variables of analog input.	IO_REAL{ REAL v; BOOL status; }
IO_BOOL	Used for input/output variables of discrete input/output.	IO_BOOL{ BOOL v; BOOL status; }
COM_BOOL	Used for inter-SCS safety communication containing Boolean data.	
COM_DINT	Used for inter-SCS safety communication containing integer-type data.	
COM_REAL	Used for inter-SCS safety communication containing real-type data.	

2.5 Structured Text

Structured Text (ST) language can be used to create user-defined FU and FB.

After downloading the FU and FB created by ST to any SCS, the downloaded FU and FB act as POUs just like those written in Function Block Diagram (FBD) or Ladder Diagram (LD) and can also be called by other POUs.

Since various statements such as the conditional statements and iteration statements are provided by ST language, ST language is more versatile than FBD and LD, sometimes the structure of the logic scripts becomes more complicated. In order to use ST language in ProSafe-RS for safety purpose, some restrictions are applied and some types of descriptions are recommended.

This section explains the restrictions and the recommendations regarding the ST language of ProSafe-RS.

SEE ALSO

For more information about the programming procedure in ST, refer to:

"Project Architecture" in the "Language Reference" of the Workbench User's Guide

For more information about the detailed check items of ST Integrity Analyzer, refer to:

“■ Checking Program Source Code and Object Code” in 8.1.3, “Confirmation of Analysis Results by Project Tree” in Engineering Reference (IM 32Q04B10-31E)

■ Basic Statements

The following table lists the ST statements defined in IEC 61131-3 and the ST statements used in ProSafe-RS.

Table 2.5-1 Basic Statements

Basic ST Statements	IEC 61131-3 Statements (*1)	Safety Usage (*2)	Interference-free Usage(*2)	Remarks
Expression	<Variable>:=<any_expression>;	Yes	Yes	
Call FU	<variable>:=<funct>(<par1>,...<parN>);	Yes	Yes	(*3)
Call FB	<blockname>(<p1>,<p2>...); <result>:=<blockname>.<ret_param1>; <result>:=<blockname>.<ret_paramN>;	No	Yes	(*3) (*4)
Conditional	IF	Yes	Yes	(*5)
	CASE	Yes	Yes	
Iteration	FOR	Yes	Yes	(*6)
	WHILE	No	No	
	REPEAT	No	No	
Control	EXIT	Yes	Yes	(*7)
	RETURN	No	Yes	

*1: Variable (variable declaration) cannot be declared in an ST statements. The dictionary should be used.

*2: Yes: Available
No: Not available

*3: When using ST program to call FU or FB, all the input parameters specified on the block diagram from top to bottom should be designated one by one. No one is omissible. FU or FB cannot be called recursively.

*4: Specify only the ValueExpression in the argument list (for each of <p1>,<p2>...and so on). No need to input parameter names.

*5: If an IF statement contains more than one conditional expression concatenated, all the conditional expressions are always evaluated regardless of the result of the first one.
For example, in the following logic, even if the B is equal to 0, that is, the result of (B<>0) is false, the second expression (A/B>0) is always evaluated and 'division by zero' occurs.

```
if ((B <> 0) and (A/B > 0)) then
```

```
    GTEQ := true;
```

```

else
    GTEQ := false;
end_if;

Instruction: do as follows to avoid 'division by zero'.
if (B <> 0) then
    if (A/B > 0) then
        GTEQ := true;
    else
        GTEQ := false;
    end_if;
else
    GTEQ := false;
end_if;

```

- *6: Nested loops cannot be used. The initial values, end values and step values of a FOR loop should all be constants.
- *7: Except in FOR loop, EXIT statement cannot be used.

SEE ALSO For more information about syntaxes of the statements, refer to:
 "ST Language" of "Language Reference" in the "Language Reference" of the Workbench User's Guide

■ ST Operators

Among the IEC 61131-3 operators, those that can be used in ProSafe-RS ST are shown as follows:

The available operators can be used in either safety purpose or interference-free purpose.

Table 2.5-2 Operators that can be Used in ST

ST Operator (*1)	Description	Availability (*2)(*3)	Remarks
(...)	Parenthesized expression	Yes	
Function(...)	Function calling (*4)	Yes	
**	Exponentiation (Raise to a power)	No(*5)	Use POW and ANY_TO_REAL /ANY_TO_DINT.
-	Negation for either real or integer number	Yes	
NOT	Boolean complement	No (*5)	Use NOT FU
*	Multiplication	Yes	
/	Division	Yes	
MOD	Modulus operation	No (*5)	Use MOD FU
+	Addition	Yes	
-	Subtraction	Yes	
<, >, <=, >=	Comparison operators	Yes	
= <>	Equality Inequality	Yes	
AND, &	Boolean AND	Yes	
XOR	Boolean exclusive OR	Yes	
OR	Boolean OR	Yes	

- *1: The higher the position of an operator in this table is, the higher precedence it has.
- *2: Yes: Available
No: Not available
- *3: The applicable operators can be used for either safety purpose or interference-free purpose.

- *4: Since a function block cannot be called from an expression, only the function is listed.
- *5: A build error will occur if this operator is used in an ST expression.

■ Data Types Available in ST

The data types that can be used in ST are shown as follows:

With ST, some types of data can be used as a single dimensional array with up to 500 elements.

The initial index of an array must be 1.



IMPORTANT

- Only ST can handle arrays. When using other languages to handle arrays, the Integrity Analyzer will treat it as an error, thus downloading cannot be performed.
- Under the following circumstances, Integrity Analyzer will treat it as an error, downloading cannot be performed.
 - When ST program contains an array with two or more dimensions.
 - When a non-usable data type is used in an array.
 - When the number of array elements exceeds the limit.
- If the specification of [Behavior at abnormal calculation] of the SCS Constants Builder is [SCS fails] (default), the SCS stops if access to the outside of an array occurs.

Table 2.5-3 Data Type

Data Type	Availability in ST (*1)				Availability as one-dimensional array Availability in ST (*1)		
	Con- stants	Local varia- bles/Local parameter (*2)	Global vari- able (*2)	I/O pa- rameter (*2)	Local varia- ble/Local pa- rameter (*2)	Global vari- able (*2)	I/O parame- ter (*2)
BOOL	Yes	Yes	Yes	Yes	Yes	Yes	No
DINT	Yes	Yes	Yes	Yes	Yes	Yes	No
REAL	Yes	Yes	Yes	Yes	Yes	Yes	No
TIME	Yes	Yes	Yes	Yes	Yes	Yes	No
STRING	Yes	No	No	Yes	No	No	No
IO_REAL	N/A	Yes	No (*3)	Yes	No	No	No
IO_BOOL	N/A	Yes	No (*3)	Yes	No	No	No
COM_BOO L	N/A	No	No (*3)	No (*3)	No	No	No
COM_DINT	N/A	No	No (*3)	No (*3)	No	No	No
COM_REAL	N/A	No	No (*3)	No (*3)	No	No	No

- *1: Yes: Available (for either safety purposes or interference-free purposes)
No: Not available
N/A: Not applicable
- *2: Local variable: A local variable is variable valid only used within a program or a function. (The value of this variable cannot be accessed from other POU.)
Local parameter: A local parameter is a variable only used within a FB. (The value of this variable cannot be accessed from other POU.)
I/O parameter: An I/O parameter is a variable that allows a FB or FU to access its input or output data. (This variable cannot be accessed from other POU.)
Global variable: This variable can be accessed internally or externally from any POU.
- *3: This variable can be used in FBD or LD but not ST.

SEE
ALSO For more information about data types available in ST, refer to:

“■ [Data Type of Variables](#)” on page 2-39

■ FUs or FBs Used in ST

All the FUs and FBs that can be used in FBD can also be used in ST.

When an FB or FU written by ST program calls an interference-free FU, the FB or FU written by ST will be handled as interference-free. When a FB written by ST program calls an FB or accesses an FB parameter of any types of FB, the FB written by ST will be handled as interference-free.

■ Debugging ST Program

If you want to use the “Breakpoint” or “Steps” in debugging ST, set the [Generate Debug Information] setting to [ON] and run “Build.” This is the same as in LD.

When debugging is complete, if you set [Generate Debug Information] to [OFF], the Cross Reference Analyzer determines that the module has been changed and shows the module in red. (=Instruction Modified). If you want to avoid another test, leave the [Generate Debug Information] unchanged ([ON]).

2.6 Capacity of SCS Applications

This section shows the capacity of applications related to SCS.

Table 2.6-1 Capacity of SCS Applications

Types	Items	SCSP2 Max. capacity	SCSV1, SCSP1 Max. capacity	Note
I/O	Number of nodes	14	10	Node #1 is for CPU node only.
	Number of slots	8 slots/node	8 slots/node	When connecting I/O node, the maximum slot number of CPU nodes is 6.
	Number of communication modules	2	2	For Modbus Slave Communication
		4	4	For Subsystem Communication
	Number of points of I/O	1500 (800 in duplexed I/O module)	1000 (500 in duplexed I/O module)	The numbers are provided only as a guide.
Number of Subsystem Communication Data	500 data	500 data	This is the maximum number of producing and consuming data per SCS.	
Application logic	Number of programs and user-defined FU/FB (number of POU's)	Max. 500	Max. 500	When more than 500 POU's are defined in the SCS Manager, an error occurs in building. It may not be possible to define 500 POU's depending on the type and number of FU/FB or LD elements. A restriction may be imposed depending on SCS performance.
	Definable number of variables	1500 I/O variables. 4500 internal variables	1000 I/O variables. 3000 internal variables.	The numbers are provided only as a guide. It may not be possible to define the maximum number of variables shown in the left columns depending on each type of defined variables and the performance of SCS.
Inter-SCS Safety Communication	Producing data	200 data	200 data	This is the maximum number of producing data per SCS.
	Consuming data	200 data	200 data	This is the maximum number of consuming data per SCS.
SCS Link Transmission	Sending data	128 data	128 data	This is the maximum number of sending data per SCS.
	Receiving data	1000 data	1000 data	This is the maximum number of receiving data per SCS.
CENTUM Integration Function	Annunciators (%AN)	2000	1000	
	Common switches (%SW)	300	200	All are system switches.
	External Communication FB	(*1)	(*1)	

Continues on the next page

Table 2.6-1 Capacity of SCS Applications (Table continued)

Types	Items	SCSP2 Max. capacity	SCSV1, SCSP1 Max. capacity	Note
Mapping block to use for integration with CENTUM	Analog input blocks (ANLG_S, ANLGI)	Total 2700	Total 1800	
	Velocity alarm blocks (VEL)			
	Maintenance override blocks (OVR_*, GOV_*)			OVR_B, OVR_I, OVR_R, OVR_IB, OVR_IR, GOV_B, GOV_IB
	Password blocks (PASSWD)			
	Manual operation blocks (MOB_*, MOA)			MOB_11, MOB_21, MOB_RS, MOA
	Annunciator blocks (ANN, ANN_FUP)	2000	1000	Mapping to %AN element
Communication I/O area	Overall size of %W	4000 Words	4000 Words	1 Word = 16 Bits
	%W: For mapping (BOOL)	200 Words (3200 Bits)	200 Words (3200 Bits)	1 data = 2 words, 100 data
	%W: For mapping (32-bit analog data)	1800 Words	1800 Words	900 data
	%W: For subsystem communication	1000 Words	1000 Words	Up to 500 data in total of bit data and analog data can be assigned.
	%W: Not used	1000 Words	1000 Words	
Modbus Slave	Coil	1000 Bits	1000 Bits	
	Input relay	4000 Bits	4000 Bits	
	Input register	4000 Words	4000 Words	1 word = 16 bits, 1 data = 2 words, 2000 data
	Holding register	1000 Words	1000 Words	500 data
SOE	SOE storage area (RAM)	15000 events	15000 events	
	Back up area on power failure (non-volatile RAM)	Last 1000 events	Last 1000 events	
	Trip signal file (non-volatile RAM)	2 trip signal files of up to 1500 events	2 trip signal files of up to 1500 events	
Diagnostic information message	Area for saving diagnostic information messages (RAM)	5000 messages	5000 messages	
	Back up on power failure (nonvolatile RAM)	Last 200 messages	Last 200 messages	

*1: The maximum capacities that can be defined are as follows:

- When using Modbus, the maximum definable number of external communication FB is up to 1000 for ECW_B and 500 for ECW_I and ECW_R in combination.
- In the tag assignment for CENTUM integration, up to 3200 Boolean internal variables and ECW_B FB in combination can be defined.
- In the tag assignment for CENTUM integration, up to 900 DINT and REAL internal variables, input variables of IO_REAL and FB of ECW_I and ECW_R in combination can be defined.

SEE ALSO

For more information about capacity of Mapping Block/Element, refer to:

[5.3, "Precautions for Online Change" on page 5-16](#)

2.7 Performance and Scan Period in SCS

This section describes the performance and scan periods in SCS.

■ Processing Timing and Scan Period

The periodic processing for SCS falls into two types: Application Logic Execution Function and External Communication Function. They are executed at an individual scan period.

● Application Logic Execution Function

This is the function of monitoring the safety status of a plant and performing operations specified against a fault if it occurs. Main operations are as follows.

- Input of process data from the field device
- Execution of the application logic
- Output of process data to the field device
- Inter-SCS safety communication
- SCS Link Transmission
- Communication data I/O (Subsystem communication)
- Communication with SENG
- Diagnosis

The application logic execution function has the highest priority among the functions of SCS.

TIP

The “Application Logic Execution Function” described in this section does not mean only a function of executing the application logic. This is a general name for all functions mentioned above, including the application logic.

● External Communication Function

This is the function of communicating information with external devices connected to SCS. It does not have any effects on the Application Logic Execution Function. It has the following functions.

- CENTUM Integration Function
- SOER Function
- Modbus Slave Communication Function
- Diagnostic Information Collection Function

The External Communication Function is executed in a part where the Application Logic Execution Function is not executed in the CPU processing period.

SEE ALSO

For more information about SCS scan timing, refer to:

[A3.1.1, “Definition of SCS scan period” in Safety Control Station Reference \(IM 32Q03B10-31E\)](#)

■ Confirmation of CPU Processing Time and Consideration of Idle Time

● CPU Processing Time

The actual processing time of the Application Logic Execution Function can be checked on the SCS State Management window of SENG or Status Display View of HIS. It can also be referred with the application logic by using the SYS_SCAN system function block.

Application execution time is the period of time required for processing the application logic within a scan period. Instantaneous value (%) in each scan calculated by 10 ms resolution is displayed.

CPU idle time is the period of time when the CPU has no task including the External Communication Function. Idle time per 60 seconds is displayed.

These displayed times tend to fluctuate depending on the communication load since the CPU of SCS processes the communication with SENG and communication requests from DCS.

● Consideration of CPU Idle time

You must confirm the above-mentioned Application Logic Execution time and CPU idle time when creating, adding, or changing an application logic for the SCS. The appropriate CPU idle time is necessary to ensure the external communication, the online change, etc.

You can take the following measures when the CPU idle time is insufficient.

- Reduce application logic.
- Lengthen the scan period.
- Divide application logic into two SCS.

● Influence on Application Logics According to the Increase of Communication Load

Processes on communication with SENG (online monitoring, I/O lock window operation, etc.) and communication request from DCS are done by the CPU of SCS so that they consume its idle time. Upon the increase of the frequency of such communication requests, SCS restricts the communication requests to accept to a certain amount. Thus those communications may be delayed.

Therefore when there is no communication, securing the idle time of the CPU to be more than 30 % is recommended to keep the influence on the communication to minimum upon the temporary increase of the communication load.

● Influence when the Execution Load of the Application Logic is Large

Even if the time taken for the processing of application logic execution occupies large portion of the SCS scan period and therefore CPU idle time is steadily less than 30%, the application logic can still be executed when there are no communications with SENG (online monitoring, I/O lock window operation, etc.) nor with DCS. However, if the communication load increases this situation, the following phenomenon will be observed.

- When the idle time is not sufficient
 - Updating the data displayed on HIS window, communication with SENG and FCS may be delayed.
 - Process alarms and annunciator alarm may be delayed.
 - Modbus slave communication may become an error.

As the idle time lessens, the above phenomenon will become more obvious.

- When there is hardly any idle time and the application logic execution time is equal to scan period
 - Updating the data displayed on HIS window, communication with SENG and FCS may be stopped.
 - Sending process alarms and annunciator messages may be stopped.
 - Modbus slave communication may become an error.
- When there is no idle time and the application logic execution time is steadily longer than scan period
 - Inter-SCS safety communication will not be performed properly and timeout errors may be detected on the receiving side. Such phenomenon does not occur in SCS link transmission safety communication because the communication mechanism is different.

■ Automatic Scan Period Extension Function

The purpose of this function is to extend the scan period of the application logic automatically in order to prevent communication functions, such as inter-SCS safety communication, from stopping when the execution of application logic takes longer than the scan period defined in the SENG as a result of online changes of application software that contains engineering mistakes for example. This function can be enabled or disabled on the SCS Constants Builder. It is disabled by default.



IMPORTANT

If a demand occurs while scan period is extended, it can affect safety because, for example, the reaction time may become longer than the process safety time. You need to judge carefully whether or not to enable the automatic scan period extension, taking the process safety time into consideration. If the scan period is extended while the automatic scan period extension is enabled, promptly take countermeasures such as reducing the amount of application logic by online change.

● Precautions when Using Automatic Scan Period Extension Function

The fact that the SCS is running with an automatically extended scan period is important safety information. In projects where no HIS is connected, it is necessary to use the SYS_SCA-NEXT function block to notify the user that the SCS is running with an automatically extended scan period.

SEE ALSO

For more information about the automatic scan period extension function of SCS, refer to:

[A3.1.2, "Automatic extension function for scan period of the application logic execution function" in Safety Control Station Reference \(IM 32Q03B10-31E\)](#)

■ Locking of Internal Variables and Performance: SCSP2

If you lock an internal variable in SCSP2, the application execution time may become longer, i.e., the CPU load increases. Limit the use of locking of internal variables to engineering and maintenance purposes only. In the case of SCSP1 and SCSV1, the CPU load is not affected by locking of internal variables.

● Internal Variables that Affect Performance

Internal variables whose lock status affects the performance are those defined in the Dictionary. I/O variables and the variables that are locked in the Communication I/O Lock window,

SCS Link Transmission Lock window and Inter-SCS Communication Lock window do not affect the performance.

● Locking of Internal Variables

- In SCSP2, internal variables can be locked only when [Extend Scan Period Automatically] is set to [Yes] and [Locking of Internal Variables] is set to [Enable] on the SCS Constants Builder. If you need to lock internal variables, set [Extend Scan Period Automatically] to [Yes] and change the [Locking of Internal Variables] to [Enable] and download to the SCS. After you have completed the required lock operations, set these specifications back to the original settings and download to the SCS. Note that the locking of internal variables can be cancelled regardless of these specifications.
- When the SCS security level is Level 0, internal variables can be locked only when [Extend Scan Period Automatically] is set to [Yes] and [Locking of Internal Variables] is set to [Enable]. However, at Level 0, the application execution can also become longer when the break point function is used during debugging of the application logic. If you use the break point function once, the application execution time does not return to the original length even if you cancel all break points.
- The locked internal variables can be checked with the diagnostic information messages of SENG or system alarm messages of HIS.

● CPU Load due to Locking of Internal Variables

- If you lock internal variables when the CPU idle time is small, the execution time of the CPU may exceed the specified scan period. In such cases, the automatic scan period extension function may be activated in order to extend the scan period so that external communication processing and similar are not affected.
- Even if you lock one internal variable, the CPU load increases by 20% to 30% compared to the status where no internal variables are locked.(The rate of CPU load increase depends on the application)
- If you unlock all internal variables, the application execution time automatically returns to the original value before the internal variables are locked.
- It is recommended to set [Locking of internal variable] to [Disable] on the SCS Constants Builder while the SCS is running in normal operation. This is because there is a risk of locking internal variables without considering the increase of CPU load if [Locking of Internal Variable] is set to [Enable].

2.8 Inter-SCS Safety Communication

This section describes the Inter-SCS safety communication and the precautions for engineering.

■ Outline of The Inter-SCS Safety Communication

In ProSafe-RS, it is possible to perform the Inter-SCS safety communication in the same control bus domain or in different control bus domains. The inter-SCS safety communication is a one-way communication of one-to-one variable between SCSs. The inter-SCS communication can be used to build the safety loop between SCSs.

To perform the Inter-SCS safety communication, the application logic using the dedicated FB is generated in each SCS of the sender and the receiver. Variables called binding variable are used to bind each variable of the sender and the receiver.

The following example explains the inter-SCS safety communication which sets BOOL variable X to variable Y.

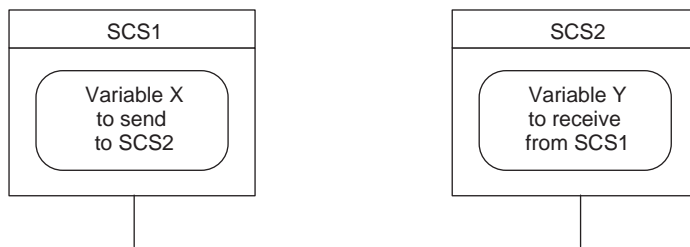


Figure 2.8-1 An Example of a Project

Generate FB (PROD_B, PROD_I, PROD_R) for communication on the sender side (the producer) in SCS, and FB (CONS_B, CONS_I, CONS_R) for communication on the receiver side (the consumer) in SCS in order to implement this Inter-SCS safety communication. To connect the sender and the receiver, define the binding variables ("P0101001" and "C0101001" in the figure shown below) for each side.

The binding variables in pairs are connected in Binding List View.

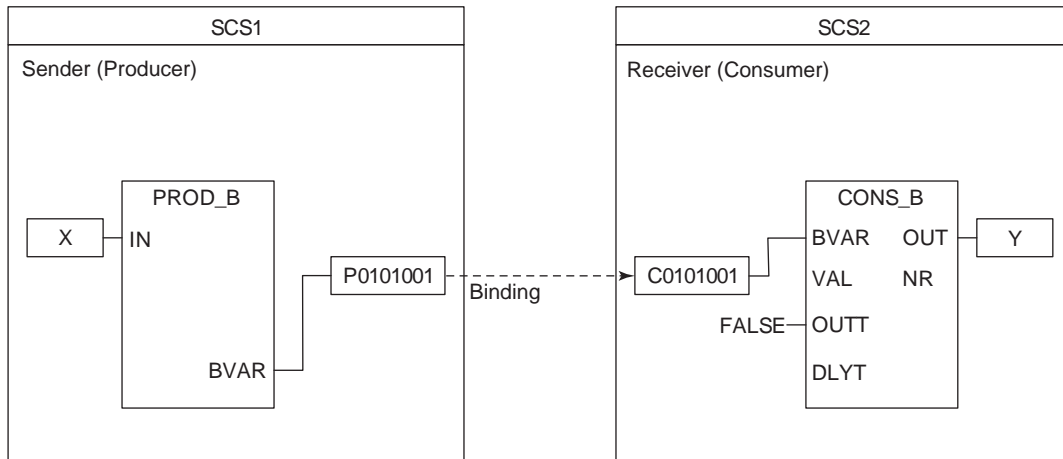


Figure 2.8-2 Inter-SCS Communication Application

The following status indicates how the Inter-SCS safety communication is performed.

- Control bus fault status indicating whether or not the SCS (the producer, the consuming) is communicable.
- Data status and Representative data status showing that data can be received normally (the consumer)

- Diagnostic information message about communication error and recovery (the consumer)

Several data sent in the same scan timing from the producer are certainly received in the same scan timing in the consumer.

**SEE
ALSO**

For more information about the Inter-SCS Communication Function, refer to:

[A5., "Inter-SCS safety communication" in Safety Control Station Reference \(IM 32Q03B10-31E\)](#)

For more information about how to define Inter-SCS communication, refer to:

[5.2, "Inter-SCS Safety Communication Definition" in Engineering Reference \(IM 32Q04B10-31E\)](#)

■ Precaution for Engineering

This section describes precautions and important issues in using the Inter-SCS safety communication.

● Restrictions on the Inter-SCS Safety Communication

- One SCS can communicate with up to 16 other SCSs.
Note that if one SCS communicates in a bi-directional manner, you should count a SCS communicated with as two.
- The maximum number of data that one SCS can send is up to 200.
- The maximum number of data that one SCS can receive is up to 200.
- If Inter-SCS safety communication is executed between the SCSs whose system program release number is prior to R1.02 in the different V net domains, the communication path cannot include Vnet/IP domains.

**SEE
ALSO**

For more information about range to which inter-SCS safety communication is possible, refer to:

- ["■ Communicable Extent" on page 2-13](#)
- ["● Inter-SCS Safety Communication in Vnet/IP Domains" on page 2-14](#)
- ["● Inter-SCS Safety Communication in a V net domain" on page 2-14](#)
- ["● Inter-SCS Safety Communication in Systems in which a V net Domain and a Vnet/IP Domain are Connected" on page 2-14](#)

● Important Issues to Consider

- Value of a binding variable on the producer side of the Inter-SCS safety communication must not be set in two or more locations.
- When an error occurs in Inter-SCS safety communication, a diagnostic information message is output and the fail-safe value (VAL) is set to the output of FB (OUT) for communication on the consumer. Design to set proper value to VAL on the consuming side.
- The FB that is used in Inter-SCS Safety communication does not have a latch function. Therefore, the value of the binding variable is output when returning from the error. If necessary, make the latch function in the application, and control error condition and the release from error condition by the application.
- The above error can be automatically recovered (The diagnostic information message is output at the recovery.) and the output of FB for communication on the consumer is also automatically recovered to the received data from the output value at the occurrence of an error.
- Changing the binding list online causes an error at the builder.
- If you use inter-SCS safety communication, the revision of SCS projects on the consumer SCS and the producer SCS should be upgraded at the same time. That is, if either one of

the SCS projects is opened using an upgraded SCS Manager, the revision of the opened SCS project is upgraded. The SCS project on the other SCS must also be upgraded by opening it with an SCS Manager with the same software release number. If the revisions of the SCS projects do not match, a build error will occur.



WARNING

- The wiring of Inter-SCS safety communication that can be changed online is only between the Inter-SCS safety communication FB and the logic for the communication. This means, for example, that only the wiring for the input of FB or communication on the producer (see wiring A in the following figure) or the wiring for the output of FB for communication on the consumer (see wiring B in the following figure) can be changed. Wiring from FB for communication on the producer to FB for communication on the consumer cannot be changed online. If it is changed online, the communication of FB on the consumer will cause an error and then a fail-safe value will be generated.

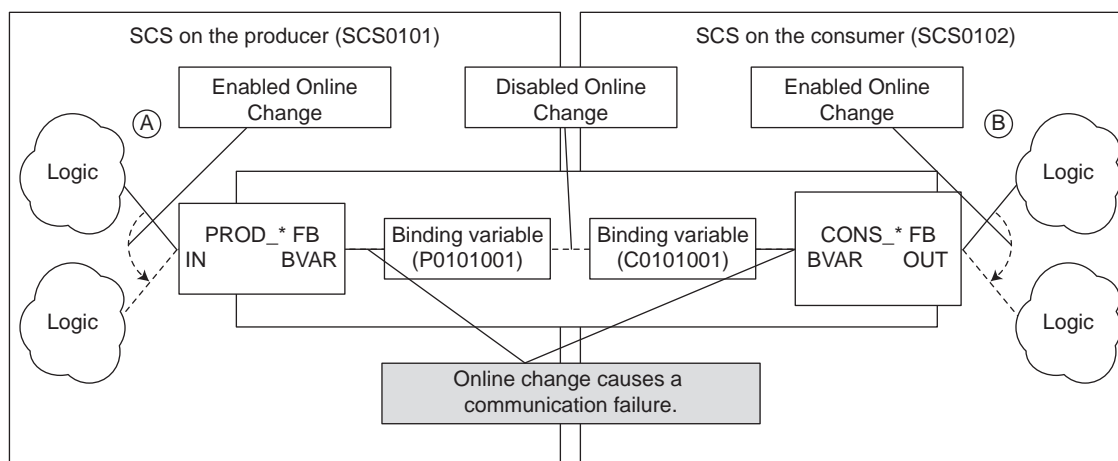


Figure 2.8-3 Wiring of Inter-SCS Safety Communication is Changed Online

- When making a wide-area connection using CGW, consider carefully the necessity of Inter-SCS safety communication through the wide-area network. Especially, when using a satellite connection, which is sensitive to the weather, as an inter-exchange channel, you must pay attentions because a trip may easily occur in inter-SCS safety communication. When the communication line does not have high enough performance or reliability, Inter-SCS safety communication will be delayed. The safety communication will time out because of this delay, and there is a possibility that a false trip may occur.

Moreover, when performing inter-SCS safety communication through WAC routers, be sure to set the value for the bandwidth limit appropriately on the System View so that the inter-SCS safety communication is always given priority.

- Be sure to use the Inter-SCS Communication Lock window to perform lock operation on inter-SCS safety communication. If you lock the binding variables directly from the Multi-Language Editor or Dictionary, an error occurs in the consumer FBs that receive the values of locked variables and fail-safe values are output. This may cause a false trip depending on the application.

- As a general rule, FBs for inter-SCS safety communication should be used after creating their instances with names using the Dictionary. If instance names are not assigned to inter-SCS safety communication FBs, inter-SCS safety communication is performed normally but the instance names that are displayed on the Inter-SCS Communication Lock window and in system alarm messages are automatically assigned by SCS Manager.
- Be sure to connect inter-SCS safety communication FBs and binding variables directly. If you insert any variables, function blocks or parameters between them, forcing and monitoring cannot be performed.

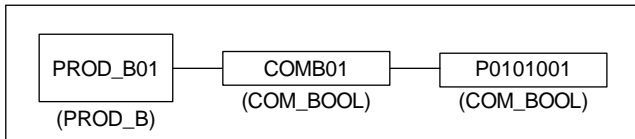


Figure 2.8-4 Example where FB and Variable are not Directly Connected

- Do not use inter-SCS safety communication FBs as parameters of function blocks. If you use inter-SCS safety communication FBs as parameters, they are not displayed on the Inter-SCS Communication Lock window. Forcing cannot be performed as well.

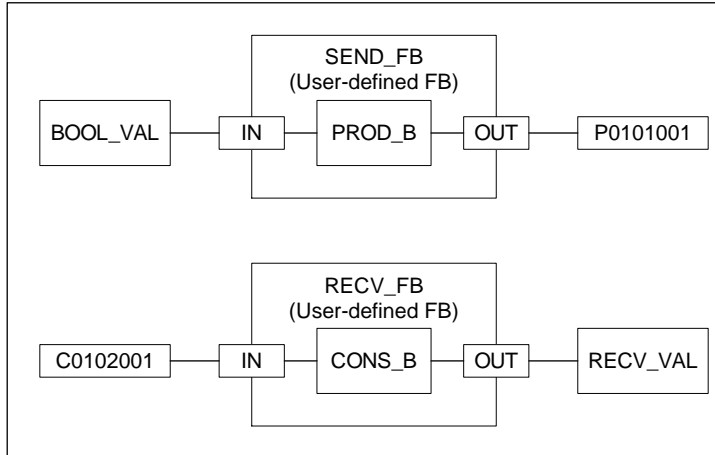


Figure 2.8-5 Example where Inter-SCS Safety Communication FBs are Used as Parameters

- Please note that when multiple binding variables are connected to a single producer FB, if you perform forcing by selecting a line corresponding to a binding variable on the Inter-SCS Communication Lock window, the values of all the binding variables connected to the same producer FB will be changed.

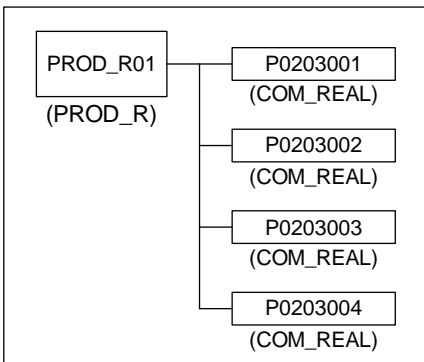


Figure 2.8-6 Example of Multiple Binding Variables Connected to a Single Producer FB

Inter-SCS Safety Communication FB									
Station	L	D	Variable	Variable Type	Instance	FB Type	Logical Value	Physical Value	Variable Comment
SCS0203			P0203001	COM_REAL	PROD_R01	PROD_R	TRUE	TRUE	
			P0203002	COM_REAL	PROD_R01	PROD_R	TRUE	TRUE	
			P0203003	COM_REAL	PROD_R01	PROD_R	TRUE	TRUE	
			P0203004	COM_REAL	PROD_R01	PROD_R	TRUE	TRUE	
SCS0201			C0201001.v	COM_DINT	CONS_I01	CONS_I	TRUE	TRUE	
			C0201001.sts				GOOD	GOOD	
			C0201001.v	COM_DINT	CONS_I02	CONS_I	TRUE	TRUE	
			C0201001.sts				GOOD	GOOD	
		C0201001.v	COM_DINT	CONS_I03	CONS_I	TRUE	TRUE		
		C0201001.sts				GOOD	GOOD		

Figure 2.8-7 Example of the Display on the Inter-SCS Communication Lock Window (Multiple Binding Variables Connected to a Single FB)

● **Inter-SCS Safety Communication Timeout Settings**

There are two timeout settings for monitoring intervals for Inter-SCS safety communication. One is the reception interval timeout value (OUTT) and the other is the transmission delay timeout value (DLYT).

A temporary “transmission delay error” is detectable by OUTT. Set DLYT to detect a constant “transmission delay error.”

- **Reception Interval Timeout Value (OUTT)**
Intervals to receive data are checked in the CONS_* FB for communication on the consumer. When a data reception interval exceeds the timeout value (OUTT), a communication error occurs and then a fail safe-value (VAL) is output.
- **Transmission Delay Timeout Value (DLYT)**
This is the checking of the time taken between the transmission of data by producer FB(PROD_*), and the reception of the data by consumer FB(CONS_*). This time is called Inter-FB transmission delay time. When the time exceeds the timeout value (DLYT) of CONS_* and that situation continues for the time of OUTT, a communication error occurs and a fail safe value (VAL) is output.
- **Setting the Reception Interval Timeout Value (OUTT)**
OUTT accepts a setting of between 3 and 30 seconds. Ensure that you set a value equal to or higher than the value obtained using the following formula. If the result of the calculation is less than 3 seconds, set OUTT to 3 seconds or more.

In case of executing the inter-SCS safety communication through WAC routers, if the calculated OUTT is less than 10 seconds, set OUTT as 10 seconds.

$$OUTT = (\text{select the longer scan period of either the producer or the consumer}) \times 8 + (\text{Additional Delay})$$

Table 2.8-1 Additional Delays by Network Configuration

Network configuration	Additional Delay
V net	No BCV/CGW used: 0 s Via BCV/CGW: number of BCVs used x 1 s + number of pairs of CGWs used x 2 s
Vnet/IP	Within a Vnet/IP domain: 0 s Between Vnet/IP domains (no WAN): 0 s (regardless of the number of Layer 3 switches) Between Vnet/IP domains (with WAN): 1 s (regardless of the number of Layer 3 switches) Between Vnet/IP domains connected via WAC routers (with WAN): 1.3 s (*1)
If a Vnet/IP domain and a V net domain are connected	V net delay (above) + Vnet/IP delay (above) + number of V net routers x 1 s

- *1: When the revisions of two SCSs for inter-SCS safety communication is earlier than R2.03.59, perform either of the following:
 - Install the SNTP server for each domain connected with the WAC routers to synchronize the time.
 - If the SNTP server cannot be added, add 5 seconds to the additional delay of OUTT.
- **Setting the Transmission Delay Timeout Value (DLYT)**
 DLYT accepts a setting of between 3 and 30 seconds. Ensure that you set a value equal to or higher than the value obtained using the following formula. If the result of the calculation is less than 3 seconds, set DLYT to 3 seconds or more.

$$DLYT = (\text{scan period of the producer}) + (\text{scan period of the consumer}) + (\text{Additional Delay})$$

Table 2.8-2 Additional Delays by Network Configuration

Network configuration	Additional Delay
V net	No BCV/CGW used: 300 ms Via BCV/CGW: number of BCVs used x 1.3 s + number of pairs of CGWs used x 2.3 s
Vnet/IP	Within a Vnet/IP domain: 300 ms Between Vnet/IP domains (no WAN): 300 ms (regardless of the number of Layer 3 switches) Between Vnet/IP domains (with WAN): 1.3 s (regardless of the number of Layer 3 switches) Between Vnet/IP domains connected via WAC routers (with WAN): 1.3 s + Transmission delay of WAN
If a Vnet/IP domain and a V net domain are connected	V net delay (above) + Vnet/IP delay (above) + number of V net routers x 1.3 s



IMPORTANT

If DLYT is set to 0 second and the Inter-FB transmission delay check is bypassed, the received data in the corresponding inter-SCS safety communications cannot be used for the purpose of safety.

- When the result of the calculation is $OUTT < DLYT$, OUTT should be changed to DLYT.
- The timeout times of the Inter-SCS Safety Communication must be taken into account to calculate the system reaction time depending on the safety engineering concept.

SEE ALSO

For more information about the communication timeout in Inter-SCS Safety communication, refer to:

C4., "Function blocks for inter-SCS communication (Safety FBs)" in Safety Control Station Reference (IM 32Q03B10-31E)

● **Recommended Guideline for Engineering**

For maintenance of Inter-SCS safety communication, it is recommended that the information on connection with the consume side should be written as a comment at the producer side in a program sheet.

SEE ALSO

For more information about the Inter-SCS Communication Function, refer to:

A5., "Inter-SCS safety communication" in Safety Control Station Reference (IM 32Q03B10-31E)

For more information about procedure for creating Applications of Inter-SCS Safety Communication and Examples, refer to:

5.2, "Inter-SCS Safety Communication Definition" in Engineering Reference (IM 32Q04B10-31E)

For more information about the calculation method of DLYT when the SCS system program release number is earlier than R2.03.51 at either of receiving/sending side, refer to:

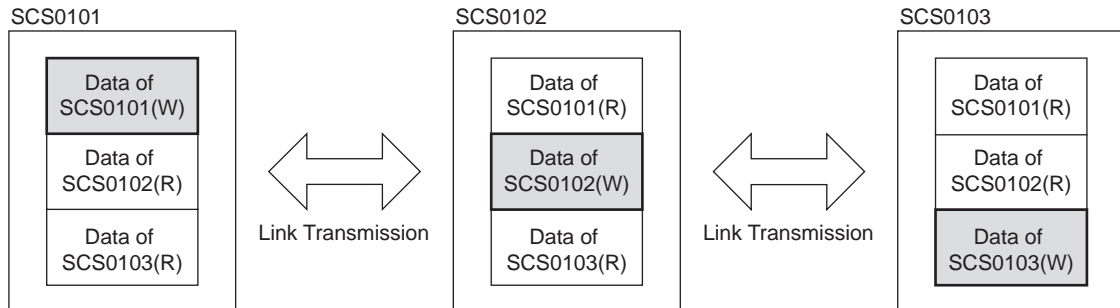
■ Specification Changes Made in SCS System Program Release Number R2.03.51" in Appendix 4.8.2, "Compatibility with Earlier Revisions" in Installation (IM 32Q01C50-31E)

2.9 SCS Link Transmission

This section describes SCS link transmission.

■ SCS Link Transmission Overview

You can use the link transmission function of control bus to broadcast data of a station periodically to all other stations in the same domain (simultaneous notification). Vice versa, a station can also receive the broadcasts of other stations and you can use the received data in the application logics.



W: An SCS can write its own data.
R: Data of other SCS are read only.

Figure 2.9-1 SCS Link Transmission

● Communication Specification

The main communication specifications of SCS link transmissions are as follows:

- Communication range: within a domain. However, V net router style S3 or above enables to make SCS Link Transmission Global Switch Communications between V net domain and Vnet/IP domain connected with V net router. Please consult the explanation in the reference link.
- Control bus: V net, Vnet/IP (either of them)
- Max. number of stations: 64 (Max. number of stations to communicate with stations: 63)
- Transmission period: Every 100 ms (fixed)
- Type of data exchanged among SCSs through SCS link transmission: BOOL type data only (Analog-type and integer-type is not supported)

SEE ALSO

For more information about virtual domain link transmission when a V net router style S3 or above is used, refer to:

■ [Virtual Domain Link Transmission](#) on page 2-62

● Read and Write Transmission Data

In SCS link transmission, bits in the received data are assigned to the dedicated FBs as input and read by the application logic. Bits in the data to be sent are assigned to the dedicated FBs as output and sent to other stations.

- Up to 1000 FBs can be used as input FBs of SCS link transmission per SCS (This is irrelevant to the sending station types such as SCS or FCS). The number of FBs for receive data per station is not limited.
- Up to 128 bits can be assigned to the output FB of SCS link transmission per SCS.

● SCS Link Transmission Types

SCS link transmission is mainly for the safety data communications among SCSs, and the interference-free communications between SCS and FCS (including APCS and GSGW). There are two types of communications:

- Data communications among SCSs: SCS link transmission safety communication
- Data communications between SCS-FCS: SCS global switch communication

■ SCS Link Transmission Safety Communication

SCS link transmission safety communication is a feature for communicating safety data among SCSs.

● Safety Communication

SCS link transmission safety communication attaches safety information to the communication data values, therefore, the receiving SCS can validate the received data values according to the safety information (safety-layer). Due to this validation, SCS link transmission safety communication data can be used up to SIL3 safety loops.

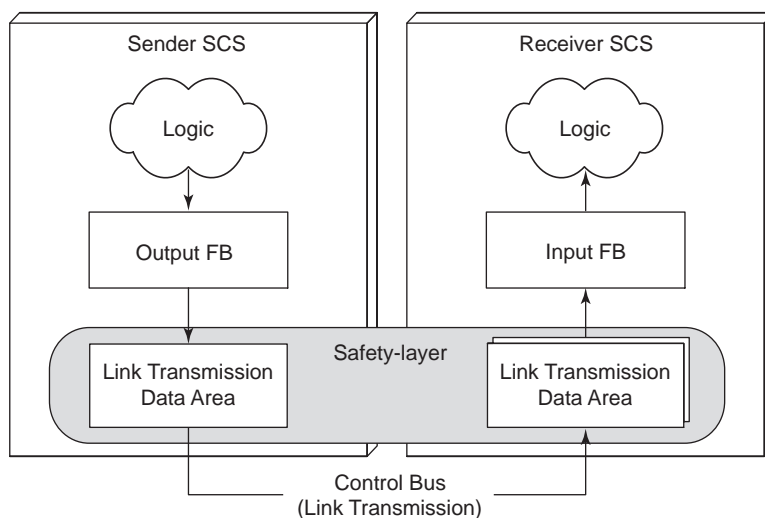


Figure 2.9-2 SCS Link Transmission Safety Communication Overview

● SCS Actions on Abnormality

When an error is detected by safety-layer, SCS will act as follows:

- Initiate a system alarm on the diagnosis error (alarm class 1).
- Set the statuses of the data received from the corresponding station to BAD.
- Use the fail-safe data values specified on the builder to replace the data values of input FBs.

When the diagnosis error is recovered, SCS will act as follows: Since the error status is not latched, it may be necessary to make the application to latch the error status.

- Initiate a system alarm on the recovery.
- Set the statuses of the data received from the corresponding station to GOOD.
- Input FBs use the data values that are refreshed after recovery.

■ SCS Link Transmission Global Switch Communication

● Global Switch Communication

Through link transmission, SCS can read data of FCS global switches. Vice versa, FCS can receive data from SCS as global switches.

Note the following when using global switch data:

- SCS can read 256 bit data of FCS global switches.
- SCS link transmission global switch communication is interference-free communication. For the applications to use the received FCS data, the dedicated FB should be used. The input data from the dedicated FB cannot be used in the safety application logics.
- The global switches in FCS that can accept the SCS link transmission data are the global switches from %GS001 to %GS128. The switches from %GS129 are not available for SCS link transmission data.

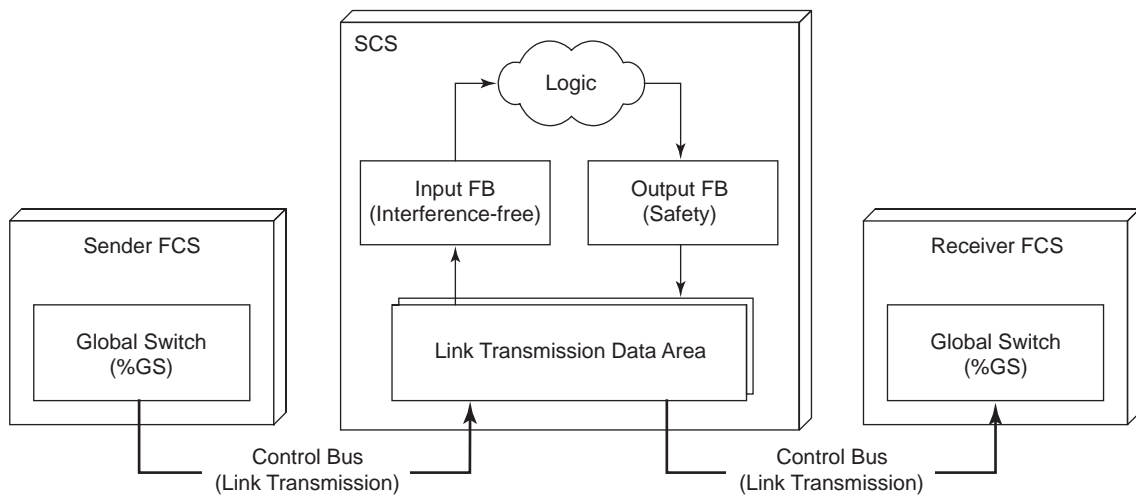


Figure 2.9-3 Data Exchange between SCS and FCS through Link Transmission

● SCS Actions on Communication Error

When a communication error occurs or when the sender FCS stops, SCS will act as follows:

- Initiate a system alarm on the diagnosis error (alarm class 2).
- Set the statuses of the data received from the corresponding station to BAD.
- Use the fail-safe data values specified on the builder to replace the data values of input FBs.

When communication recovers from error, SCS will act as follows:

- Initiate a system alarm on the recovery.
- Set the statuses of the data received from the corresponding station to GOOD.
- Input FBs use the data values that are refreshed after recovery.

■ Precaution for Engineering

This section describes precautions and important issues in using SCS link transmission.

● Intend Purpose of SCS Link Transmission

The following figure illustrates the relationship between SCS link transmission and binding of inter-SCS safety communication for data exchange among SCSs.

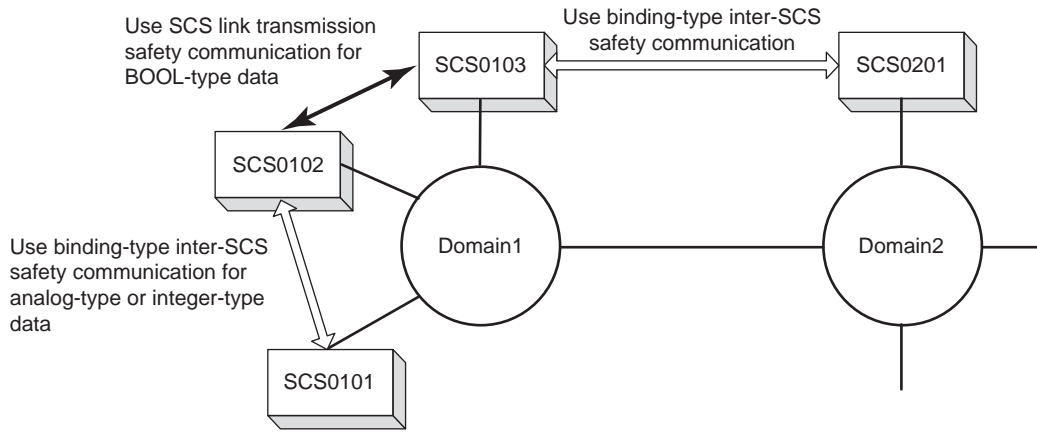


Figure 2.9-4 Relationship with Inter-SCS Safety Communication

The BOOL type data exchange among SCSs in the same domain is recommended to go through the SCS link transmission safety communication. Although the amount of data that can be communicated is limited, use of SCS link transmission safety communication enables for communicating with more stations, and achieves higher performance, compared to when inter-SCS safety communication is used.

For analog-type or integer-type data exchange in the same domain and for inter-SCS data exchange across domains, use binding-type inter-SCS safety communication.

The following table shows the range of communication and the relationships of communication data types and communication methods.

Table 2.9-1 Communication Data Types and Communication Methods

Scope	Data type	Communication Method	Remark
Inter-SCS in the same domain	BOOL	SCS link transmission safety communication	Can communicate with FCS (SCS global switch communication: Interference-free)
	Analog, integer	Binding-type inter-SCS safety communication	-
Inter-SCS across domains	BOOL, analog	Binding-type inter-SCS safety communication	-

● **Communication with FCS through the Inter-station Data Link Block (ADL)**

FCS can read from SCS mapping blocks or write to SCS mapping blocks through the inter-station data link block (ADL). However, data exchange through SCS link transmission does not require the mapping blocks used by data exchange through inter-station data link block (ADL). Consider using SCS link transmission for SCSs exchange data of BOOL type in one domain.

The following cautions need to be noted when reading or writing for data exchange:

- When writing from FCS to SCS through the inter-station data link block (ADL), the periodic writing is restricted. However, periodic writing is possible through SCS link transmission.
- Tag names cannot be assigned for the Input/Output function block of SCS link transmission. For reading the SCS data transmitted through SCS link transmission on HIS, the transmitted data should be linked to the BOOL type internal variables by the application logics and assigned the tag names to the linked variables.

● Time Out Settings of SCS Link Transmission Safety Communication

The time out settings of SCS link transmission safety communication consists of the reception interval timeout value (Reception Timeout, referred to as OUTT hereafter) and transmission delay timeout value (Transmission Timeout, referred to as DLYT hereinafter).

A temporary "transmission delay error" is detectable by OUTT. Set DLYT to detect a constant "transmission delay error."

- Reception Interval Timeout Value (OUTT)

This value is valid only when the communication partner (the sender) is an SCS.

The reception interval is an interval between data received by an SCS. This reception interval timeout value (OUTT) should be specified for each communication partner station. If the communication data from a station are not received within this interval, a communication error is raised and the fail-safe values will be used to replace the communication data values.

- Transmission Delay Timeout Value (DLYT)

This value is valid only when the communication partner (the sender) is an SCS.

Inter-SCS transmission delay time is the elapsed time after the sending side SCS transmits the data until the receiving side SCS receives the data. If SCS transmission delay time exceeds DLYT for the period of time specified to the OUTT, a communication error is raised and the fail-safe values will be used to replace the communication data values.

The guidance for setting the timeout values is as follows:

- Setting the Reception Interval Timeout Value (OUTT)

$OUTT = (\text{Scan period of sender SCS or receiver SCS whichever longer}) \times 8$

If the result of the OUTT calculation is 3 seconds or less, set a value of between 3 and 30 seconds.

- Setting the Transmission Delay Timeout Value (DLYT)

Set the DLYT to between 3 and 30 seconds.

When using 0 to set DLYT, checking for the delay according to the DLYT will not be done.

● Pre-Alarm Setting Value (Pre-Alarm)

This value is valid only when the communication partner (the sender) is an SCS.

A pre-alarm setting value (hereinafter PALT stands for Pre-Alarm) needs to be specified for each communication partner SCS. Specify a value if it is necessary to detect transmission delays before the inter-SCS transmission delay time reaches the DLYT. No system alarm is raised. Even if the DLYT is set to 0, if the PALT is not set to 0, the pre-alarm is checked.

When the Inter-SCS transmission delay time exceeds the time specified by PALT and if the state continues more than the period specified by OUTT, a pre-alarm will occur. The initiated pre-alarm can be notified to the applications by using a system function block of SYS_LTSTS.

The following points should be noted when setting a pre-alarm:

- When PALT is set to 0 second (default), the pre-alarm will not be active.
- If the DLYT is not set to 0, to activate the pre-alarm, set PALT with a value of $0 < PALT < DLYT$, and create a logic using SYS_LTSTS.



IMPORTANT

If both DLYT and PALT are set to 0 second, the SCS link transmission cannot be used for safety purposes.

- **Other Notices**

- When the receiver station accesses data that is not assigned on the sender station, the data value will show FALSE and the data status will show GOOD.
- Builder cannot check the consistency of the data assigned on the sender station and on the receiver station for data exchange, so the assignment of the communication data on both sides must be checked by the communication test.
- By the setting of "Link Transmission Receiving Station" of SCS link transmission, the receiver stations can be limited so as to prevent the performance declination. Other stations with which no communication is required should not be specified as "Receive."

- **Virtual Domain Link Transmission**

If you are using a V net router style S3 or above, SCS Link Transmission Global Switch Communication is possible within a virtual domain by deploying the V net domain and Vnet/IP domain connected to that V net router as a single virtual domain.

To enable this feature, you must set up the V net router by using the CENTUM system builder function.

- **Issues to Consider when Using Virtual Domain Link Transmission**

The following are issues to consider when making a virtual domain link transmission.

- If you are using a V net router style S3 or above and CENTUM VP R5.01 or later, you can enable and disable virtual domain link transmission using the V net router settings included in the system generation function in CENTUM. If you set virtual domain link transmission for the V net router to [Enabled], link transmission is enabled between the V net domain and Vnet/IP domain connected to the V net router.
- To change the Enable/Disable setting for virtual domain link transmission, you will need to perform an offline download to the V net router.
- The guaranteed reach for virtual domain link transmission is within the same virtual domain as the sending station.
- Link transmission is not available between separate virtual domains. When connecting Vnet/IP domain A and B via V net, for example, Vnet/IP(A) – V net and Vnet/IP(B) – V net are discrete virtual domains. Consequently, link transmission can not be made between Vnet/IP(A) and Vnet/IP(B). When connecting V net domain A and B via Vnet/IP, V net(A) – Vnet/IP and V net(B) – Vnet/IP are discrete virtual domains likewise. Consequently, link transmission can not be made between V net(A) and V net(B).
- When you make a virtual domain link transmission, there must be no duplication of the station numbers inside the virtual domain.
- When two or more virtual domains are connected by a domain added to two or more virtual domains, station numbers must be unique in all these virtual domains.

- **Example Use of Virtual Domain Link Transmission**

Virtual domain link transmission is useful in situations such as when migrating part of a V net domain and changing it to a Vnet/IP domain. The following figure shows an example configuration.

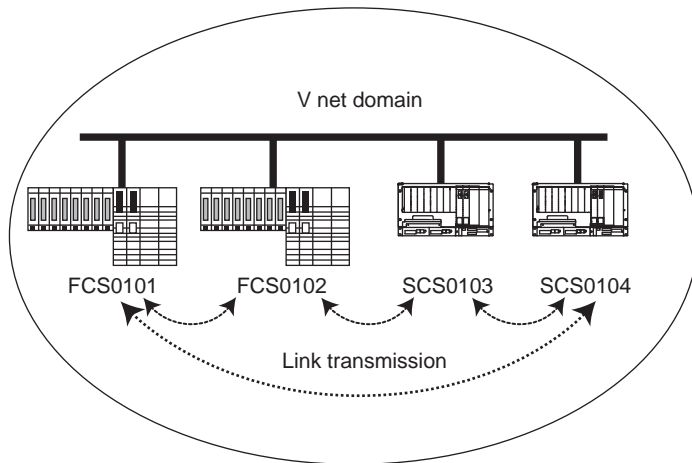


Figure 2.9-5 Example of the Configuration of a Link Transmission in a V net Domain

The following figure shows an example of a migration in which part of a V net domain is split into a Vnet/IP domain and an FCS0102 and SCS0104 are added to the Vnet/IP domain.

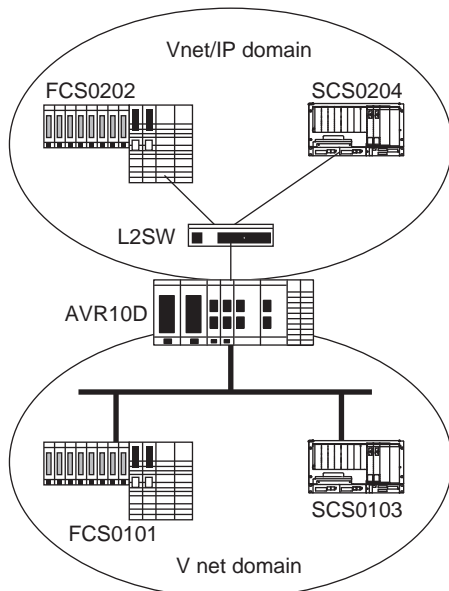
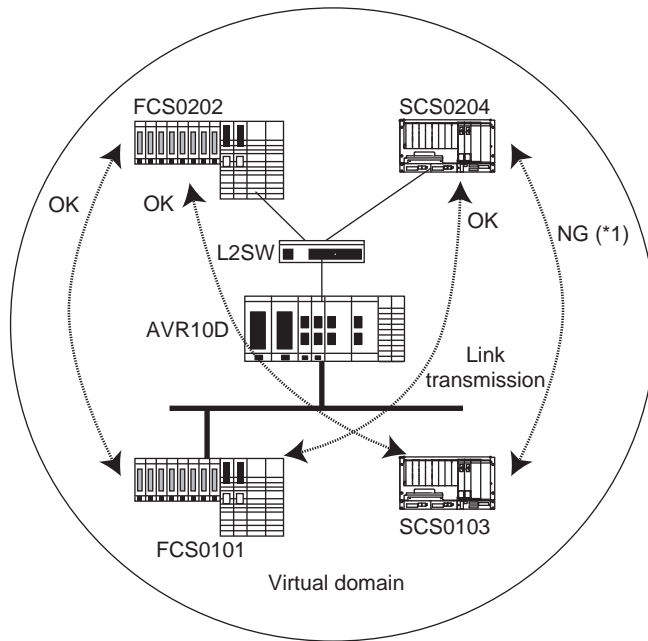


Figure 2.9-6 An Example of a V net Domain Split into V net and Vnet/IP Domains

The following figure shows an implementation of a link transmission.



*1: Virtual link transmission between SCSs (SCS link transmission safety communication) can not be executed.

Figure 2.9-7 Example of a Virtual Domain Link Transmission

If the global switch for an SCS that has been migrated from V net to Vnet/IP is referenced by an FCS, it may, depending on the referencing method, be necessary to re-engineer the application concerned with the global switch in the FCS.

- If the global switch in the SCS is referenced by specifying the FCS as %GSnnnss (nnn: %GS number, ss: station number)

You must re-engineer the FCS application if the SCS station number has been changed. It is not necessary to re-engineer the application if only the SCS domain number has been changed.

Example: In the figure above, if FCS0101 references %GS001 in SCS0204, it is not necessary to change "%GS00104" referred to in the FCS0101 application.

- If the global switch in the SCS is referenced by specifying the FCS as %GSnnnSddss (nnn: %GS number, dd: domain number, and ss: station number) You must re-engineer the FCS application if the SCS domain number or station number has been changed.

Example: In the figure above, if FCS0101 references %GS001 in SCS0204, it is necessary to change "%GS001S0104" referred to in the FCS0101 application to "%GS001S0204."

- If the global switch for an FCS that has been migrated from V net to Vnet/IP is referenced by an SCS. Provided that the station number does not change, it is not necessary to re-engineer the application concerned with the SCS link transmission. If the station number has been changed, you must change the station type in the Other Stations tab sheet of the SCS link transmission definition in SCS Link Transmission Builder, and redefine the wiring in Data Wiring Definition.

2.10 Diagnosis Function of SCS

SCS notifies the user of the status of SCS in operation, the information on detected errors and on operations by the user. Monitoring the notified information enables the user to take appropriate actions. SCS controls to bring the process to a safe state when SCS detects an error in itself.

This section describes the following.

- Overall diagnostic function of SCS
- Error processing that should be considered in application design.

■ Overall Diagnostic Function of SCS

SCS has diagnostic functions for hardware and software.

When SCS detects an error by diagnosis, actions corresponding to the error are taken. A notification of the error appears in the Diagnostic Information Message and Status Display to alert the user.

● Diagnosis for Hardware

SCS carries out diagnosis with the following timing to check whether various types of hardware including I/O modules are in the normal state.

- At the start of the hardware.
- At specified periodical intervals during operation.

● Diagnosis for Software

SCS carries out diagnosis to check that the following actions of software are correctly performed.

- Task actions
- Application execution time

The following table shows an overview of actions when SCS detects an error by diagnosis.

Table 2.10-1 SCS Actions on Fault Detection by SCS Diagnosis

Fault level (*1)	Definition	Overview of SCS actions
Fatal error	Fatal hardware/software errors disabling continuous operation of the SCS.	CPU on both sides stops (SCS FAIL). Stopping CPU results in the change of output values of all output modules to the fail-safe values (All outputs shutdown) (*2)
Major error	This is not a fatal error that stops the CPU, but an error that disables some of the execution function of the application logic.	SCS performs an action against the error and notifies the application logic of the error state. In this case, creating an application by the user allows actions to be performed at the occurrence of an error (Shutdown action(*2), etc.) SCS notifies the user that an error occurs with diagnostic information message and the Status Display.
Minor error	Other errors <ul style="list-style-type: none"> • Error that have no influence on the application logic execution function itself, such as switching in redundant configuration • Errors related to functions not associated with the application logic execution functions • Operation mistakes by users 	The application logic execution function continues. SCS notifies the user with diagnostic information message and the Status Display that an error occurs. Notification to the application logic depends on what kind of error occurs. When a module in a dual-redundant configuration fails, the failed module is regarded as FAIL state and switching-over to the stand-by is executed.

*1: Classification of error level

The SCS classifies the error level according to the result of error analysis, which determines the type of error that occurred, as well as the system state at which the error happened.

*2: Shutdown actions

Shutdown actions control output modules in appropriate conditions. There are three kinds of shutdown actions.

- The Shutdown that is operated with the logic that was created by user.
- Shutdown that makes CPU hold the output value in a failed channel.
- Shutdown of the output modules when they detect an error in communication with the CPU.

When all output modules are shut down by stopping CPU due to a fatal error, this is called All Output Shutdown.

■ Actions on Error Detection

To keep the process in a safety state when an error is detected by the diagnosis of SCS, you need to understand the actions of the system in the case of error and design the safety application appropriately for the error levels.

Major SCS errors and actions of I/O modules against the error status are shown as follows.

They are very important issues in designing the safety applications.

Table 2.10-2 Actions on Error Detection

Failure location	Cause	Configuration	Actions	Fault level
CPU module	Hardware failure CPU node failure Software failure	Single	CPU stops. All output modules output the value at fault.(All output shutdown)	Fatal error
		Dual-redundant	CPU on failure side stops. The control is continued by switching the control right.	Minor error
Input module	Hardware failure	Single	The Input value at fault is set to all input channels of the module and data status changes to BAD.	Major error
		Dual-redundant	The control is continued by switching the control right.	Minor error
Input channel	Failure of Hardware for individual channel Failure on field side	Single (*1)	The Input value at fault is set to failed input channels and data status changes to BAD.	Major error
		Dual-redundant (*2)	When a failure is on the field side, the same action as the single configuration is performed.	Major error
			When a failure other than the above occurs, the control is continued by switching the control right.	Minor error
Output module	Hardware failure	Single	Output of all output channels on the module becomes 0 (*3) and is put in output disable state, and data status changes to BAD.	Major error
		Dual-redundant	The control is continued by switching the control right.	Minor error
Output channel	Failure of Hardware for individual channel Failure on field side	Single (*1)	When the output shutoff switch works (*4): Output of all output channels on the module becomes 0 (*3) and is put in output disable state, and data status changes to BAD.	Major error
			Others except for the above case: Output value at fault is set to physical data of this channel and is put in output disable state, and data status changes to BAD state.	Major error
		Dual-redundant (*2)	When a failure is on the field side, the same actions as the single configuration are performed.	Major error
			When a failure other than the above occurs, the control is continued by switching the control right.	Minor error

*1: When the module is in single configuration

*2: When the module is in dual-redundant configuration

*3: DO module: FALSE AO module: 0.0 [mA]

*4: This works if dangerous failure (DO module channel is fixed to ON) or failures requiring the protection of internal module (such as an overcurrent of AO module) occur. If you want to set the output shutoff switch to go on when dangerous failure requiring no protection of module occur, set the output module channel accordingly with the I/O Parameter Builder window.

● Considering Application Actions on Fault Detection

- In the logic of NC input like ESD application, etc, setting "the input value at the error occurrence" to FALSE permits the application logic to handle a failure of the input module as a demand and perform actions like shutdown.
- For DTS (De-energize To Safe) output in ESD application and so on, it is necessary to set a "fail-safe value" in order that the process is in a shutdown state when all outputs become the "fail-safe value."
- When a failure of an output module occurs, a shutdown action for different related output modules is required depending on the process. In this case, it is necessary to create the application logic to shut down the output of different related modules when the output channel data status changes into a BAD state.

SEE ALSO

For more information about example for creating the application logic to monitor the channel data status and perform a shutdown, refer to:

[3.3.2, "Shutdown due to Channel Failure" on page 3-21](#)

For more information about actions at the occurrence of SCS error and of procedure for recovery, refer to:

[B6., "Actions taken at error occurrence and recovery procedure" in Safety Control Station Reference \(IM 32Q03B10-31E\)](#)

■ Setting of Parameters of I/O Modules

This section explains the precautions to be taken when setting the parameters of an I/O module. Parameters are set with the I/O Parameter Builder.

Parameters of I/O modules include the specifications of actions on error detection. It is necessary to be careful when setting them.

● Issues to Consider when Setting the Parameters (by Channel) of the Analog Input Module (SAI143)

- Select two-wire or four-wire according to field devices for "Field power supply diagnosis." For all specified items for detection, the default settings are recommended.
- When two-wire or four-wire for Field power supply diagnosis is set, specify it to set pins on hardware for the current input module. In the case of different settings in the "Field power supply diagnostics" and hardware pins, the module will not start due to diagnosis error.

SEE ALSO

For more information about parameters by channel for current / voltage analog input module, refer to:

["■ Items set for each channel in the current/voltage analog input module" in A4.4, "Items set for analog inputs" in Safety Control Station Reference \(IM 32Q03B10-31E\)](#)

● Issues to Consider when Setting the Parameters (by Channel) of the Analog Input Module (SAT145, SAR145)

Enter the Input Value at Fault, Threshold of the IOP (High) level, and the Threshold of the IOP (Low) level as % units. If the input signal is engineering data, convert the setting value from engineering data to a % unit based on the upper and lower range values.

Setting (%) = (Setting in engineering data - lower range value) / (upper range value - lower range value) x 100

Example:

When you select [Type K] for the Signal Conversion and select [C] for the Engineering Unit.

- The permissible range is -200 to 1200 deg. C.
- To set the Input Value at Fault to 900 deg. C, set $(900 + 200) / (1200 + 200) \times 100 = 78.6 \%$.



IMPORTANT

You must use the upper and lower range values of the I/O Parameter Builder. Be careful to ensure that you do not use the upper and lower scale values of Tag Name Builder. If you have set the upper and lower scale values to between 0 and 800 deg. C in Tag Name Builder, ensure that you do not specify the Input Value at Fault as a % unit corresponding to between 0 and 800 deg. C.

SEE ALSO

For more information about parameters by channel for thermocouple / resistance temperature detector analog input module, refer to:

“■ Items set for each channel of a thermocouple/resistance temperature detector (TC/RTD) analog input module” in A4.4, “Items set for analog inputs” in Safety Control Station Reference (IM 32Q03B10-31E)

● Issues to Consider when Setting the Parameters (by Channel) of the Analog Output Module (SAI533)

- If the short circuit detection level is not properly set when the wiring resistance exceeds 50 Ω, the short circuit may not be detected on outputting the "Output Value at Fault" or the Tight-shut value. To avoid this problem, set properly the short circuit detection level with reference to the following information.
- The "Output Value at Fault" is output to the field exactly as it was set when the fault is detected. If you want to do Tight-shut or Full-open on fault detection, set the same value as the Tight-shut value or the Full-open value to the "Output Value at Fault." If the Tight-shut value or the Full-open value is changed, check if the "Output Value at Fault" should also be changed.

SEE ALSO

For more information about Tight-shut / Full-open settings for HART communication, refer to:

2.22, “HART Communication” on page 2-138

For more information about the short circuit detection level, refer to:

“● Command Line” in “■ Items set for each channel (analog output)” in A4.5, “Items set for analog outputs” in Safety Control Station Reference (IM 32Q03B10-31E)

For more information about parameters by channel for analog output module, refer to:

“■ Items set for each channel (analog output)” in A4.5, “Items set for analog outputs” in Safety Control Station Reference (IM 32Q03B10-31E)

● Precautions for Setting Module Parameters for the DI Module (SDV144)

- When the software filter is set to 1, if an ON state is detected twice in the scan timing of the DI module, the input value is fixed to ON, and its value referenced by the application logic.
- When a software filter is set to 0, the PV value is effected noise. Ensure that the software filter is not set to 0.
- In addition to the software filter for making the input values, the DI module also has a filter to make SOE events. The filter for verifying the SOE events will be disabled if the software filter is set to 0 (no filter). If set to 1 or a bigger value, the digital filter will be 10 ms filter.

- If you have set Automatically Delete Noisy Event to [Yes] and more events than the specified number occur in the channel in the specified event time, the extra events are automatically deleted.

**SEE
ALSO**

For more information about module parameters for discrete input module, refer to:

“■ Items set for each module (discrete input)” in A4.6, “Items set for discrete inputs” in Safety Control Station Reference (IM 32Q03B10-31E)

● Precautions for Setting Channel Parameters of DI Module

- The Wiring Check Adapter (SCB100) and a sensor switch must be connected in parallel to detect disconnection. When the check adapter is not installed, specify "No detection."
- The following setting is recommended as the disconnection detection value.
 - Specify "No detection of disconnection" (default) for NC (Normally Close) input.
 - Specify "Detection of disconnection" (Wiring Check Adapter is required to be installed.) for NO (Normally Open) input.
- Wiring Check Adapter(SCB110) and a sensor switch must be connected in series to detect a short circuit. When the check adapter is not installed, specify "No detection."
- For specifying the detection of a short circuit, the following settings are recommended. Specify "Detection of a short circuit" (default) for both of NC input and NO input.
(Wiring Check Adapter need to be installed. For detecting both open and short circuits, while NO is selected, Wiring Check Adapters, both SCB100 and SCB110 are necessary.)
- In case of an NC input, to conduct a pulse test, the wiring check adapter (SCB110) and a sensor switch must be connected in series. When the input is NC and the check adapter is not installed, specify "No pulse test." In case of a NO input, a pulse test can be conducted without a check adapter.
- For a pulse test, the following settings are recommended.
In case both of an NC input and a NO input, a pulse test should be conducted.(Default)
(In the case of NC input, the wiring check adapter is required to be installed.)

**SEE
ALSO**

For more information about channel parameters for discrete input module, refer to:

“■ Items set for each channel (discrete input)” in A4.6, “Items set for discrete inputs” in Safety Control Station Reference (IM 32Q03B10-31E)

● Precautions for Setting Channel Parameters of DO Module

- Set a proper value to the "Output value in detecting error" after carefully considering the operation of the application and the operation of the field in error condition.
- The following setting is recommended as the disconnection detection value. Specify "Detect Disconnection circuit" in both cases of DTS (De-energize To Safe) output and ETS (Energize To Safe) output (Default).
- For a pulse test on OFF, the following setting is recommended. Specify "Pulse Test" in both cases of DTS output and ETS output (Default).
- For a pulse test on ON, the following settings are recommended.
 - Specify "No pulse test" in the case of DTS output (Default).
 - Specify "Pulse Test" in the case of ETS output.

**SEE
ALSO**

For more information about channel parameters for discrete output module, refer to:

“■ Items set for each channel (discrete output)” in A4.7, “Items set for discrete outputs” in Safety Control Station Reference (IM 32Q03B10-31E)

2.11 Monitoring Process and System

SCS status and process state can be monitored from SENG and HIS in CENTUM Integration structure.

In CENTUM Integration structure, HIS can monitor both CENTUM System and SCS.

It is possible to monitor faults in the system by annunciator panel put out of SCS.

This section describes the monitoring of the process and the system.

■ Monitoring by Diagnostic Information Message

SCS sends diagnostic information messages for detected faults and for the operation on the safety functions to notify user of events.

You can confirm the time when a fault occurred and the outline of the cause of the fault by reading the information provided in the diagnostic information message.

Diagnostic information messages can be checked as system alarm on SENG and HIS.

■ Monitoring SCS Status

The status of SCS can be checked on SENG and HIS. When a fault occurs in SCS, the fault can be located in a visual way.

■ Monitoring SCS Status with an External Alarm Panel

Creating the application logic of SCS makes it possible to output the data about SCS fault status to the external alarm panel so that the fault status can be informed to an operator.

It is recommended to put such alarm panel in a place where the operator can see the panel for continuous monitoring in order to monitor faults occurring in hardware of SCS.

When the occurrence of a fault in hardware is recognized on the external alarm panel, the detailed information on the fault is confirmed on the Diagnostic Information Window in SENG.

The following example shows the application logic to inform the fault status to the external alarm panel in SCS using a system function block.

● An Example of Using the SYS_DIAG to Output SCS Fault Status to an External Alarm Panel

Diagnostic Information FB (SYS_DIAG) detects all system faults except user's operation mistakes. The following example shows how to use the SYS_DIAG to output system faults, I/O and V net-related faults to an external Alarm Panel.

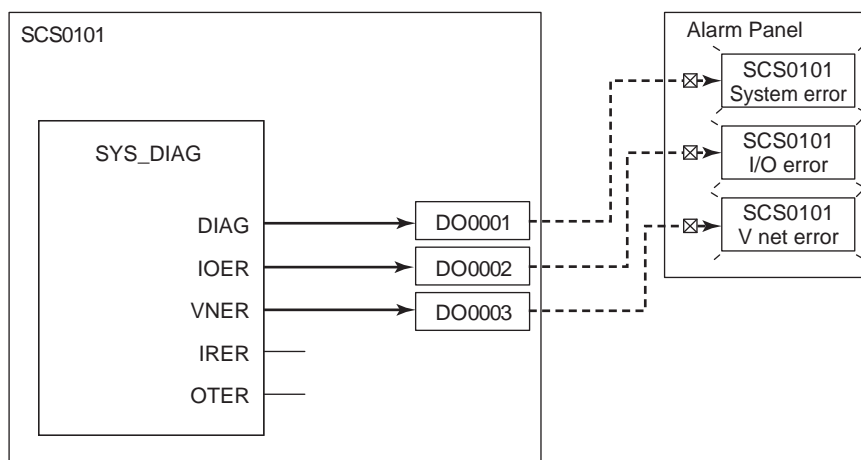


Figure 2.11-1 Example of the Logic to Output SCS Fault Status to External Alarm Panel

SEE ALSO

For more information about detailed function of the SYS_DIAG, SYS_ESBINF and SYS_NODEINF system function block, refer to:

C10.6, "SYS_DIAG (diagnostic information output)" in Safety Control Station Reference (IM 32Q03B10-31E)

■ Monitoring Process with Process Alarm Message and Annunciator Message

In CENTUM Integration configuration, information on a process state can be notified to HIS as a process alarm or annunciator messages from the application logic of SCS.

The process alarm and annunciator messages can be used as a pre-alarm before generating a trip in SCS. In the CENTUM system, they inform the operator that the appropriate action should be taken in the plant.

The following example shows the application logic to output a process alarm and annunciator message.

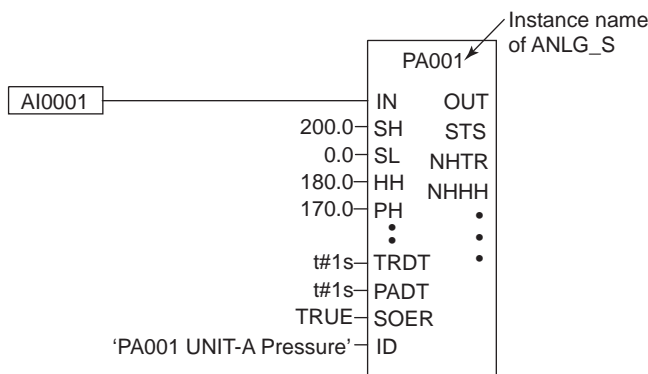


Figure 2.11-2 Example for the Output of Process Alarm of Analog Input to HIS

Creating the above application and then setting a tag name for the Instance name with the Tag Name Builder results in generating a Mapping block for CENTUM Integration. The mapping block allows alarm for the Analog input value (AI001) to be displayed as process alarm on HIS. Note that the alarm setting value (HH/PH/PL/LL) cannot be changed on HIS.

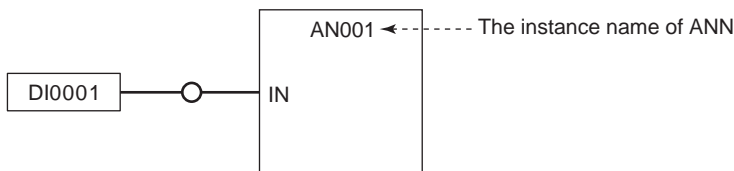


Figure 2.11-3 Example for the Output of Annunciator Message to HIS

Creating ANN in the application logic as shown above and then defining the corresponding mapping element to instance name with the Tag Name Builder results in the automatic generation of mapping element %AN. Specifying a message character string with the Tag Name Builder allows displaying an annunciator message on HIS.

■ Monitoring I/O Data and Application Logic Data

User can monitor I/O data and application logic data from SENG, HIS and external equipment via Modbus.

2.12 Security

This section describes Security features in ProSafe-RS.

ProSafe-RS has the following security to block access to the system from unauthorized users or systems and to prevent unintended changes caused by operators' operation error.

- Security for Project Database
When changing the project database with the SCS manager, it can be set with SENG function that entering a password is needed.(recommended)
- Security for Access to SCS
SCS limits access to SCS from the outside according to SCS security level. Entering a password is required to change SCS security level. (must)
- Security for the SCS Maintenance Support Tool
Writing to SCS with the SCS maintenance support tool is controlled in SENG by a specific password.(recommended)

Furthermore, SENG Function has features of detecting faults in project data and of getting confirmation before important operations to prevent user's misoperations.

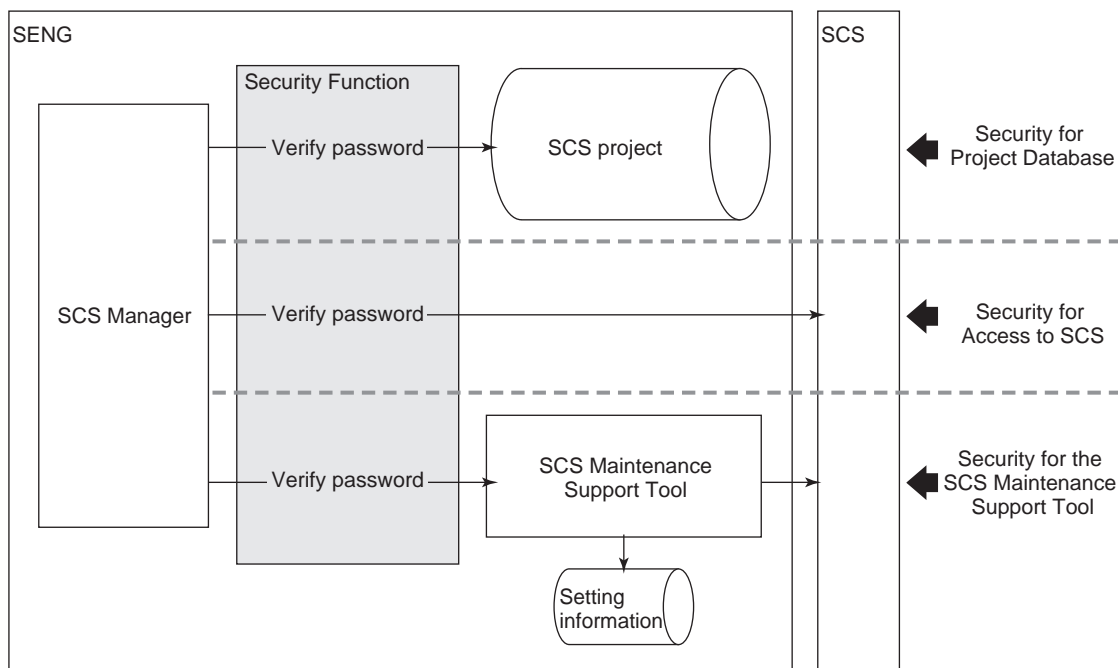


Figure 2.12-1 Security Features with Passwords

2.12.1 Security for Access to SCS

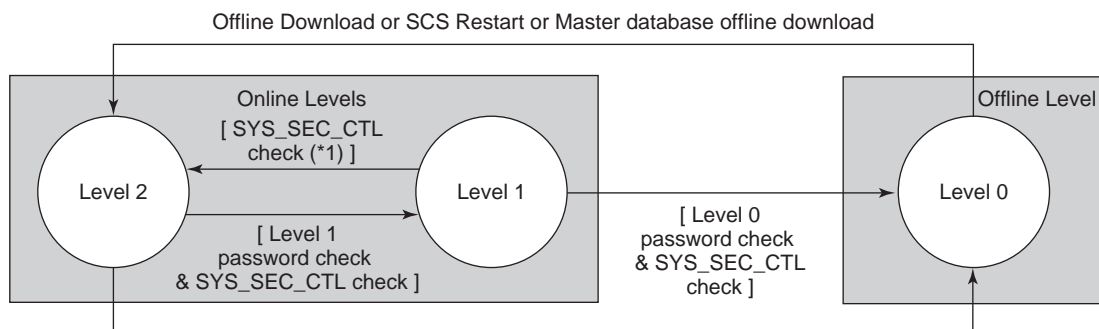
This section describes security for access to SCS.

■ Security Level of SCS

The security level of SCS indicates the level of protection against erroneous writing to the memory in SCS from the connected stations or devices. An overview of SCS security level is as follows:

- One SCS has one security level.
- The security level can be confirmed from LED on the CPU module and the SCS State Management window of SCS Maintenance Support Tool or Status Display View of HIS.
- SCS limits changes made from the outside according to security level.
- Security level can be referred to by applicable logic.
- Security level can be changed by an authorized user with the password using the SCS Manager.
- Using the system function block (SYS_SEC_CTL) makes it possible to control whether or not to allow security level change operations from an SENG with an external hardware switch or similar.
- Security level can be changed under the following conditions:
 - The SCS is either in the Waiting or Running mode, AND
 - The SYS_SEC_CTL is set to allow security level changes or is not used.

The following figure illustrates the transition of states of the security level.



*1: It is allowed to reset the security level from Level 1 to Level 2 via the RST input in the SYS_SECURE block, regardless of the security level change enable/disable status of SYS_SEC_CTL.

Figure 2.12.1-1 Transition of Security Level Status

■ Definition of Each Security Level

There are two classifications of levels; online level and offline level. The Online level is used when SCS is in normal operation. The Offline level is used when SCS is not in normal operation.

● Online Level

The Online Level is a security level to be used when normal operation is performed in SCS. The SCS itself provides security of the Online Level by controlling access to the memory from the outside.

The Online Level is separated into two levels according to limits of functions which can be used.

Table 2.12.1-1 Online Level

Level	Description
Level 2	The highest security level. SCS is usually operated at this security level.
Level 1	A temporary security level used by engineers or authorized users for maintenance of equipment or changing applications online

● **Offline Level**

The Offline Level is a security level to be used when a regular operation is not performed in SCS. This is displayed as "Level 0" on the LED of SCS or the SCS State Management window of SENG. In the Offline Level, SCS does not limit access to SCS from the outside. However, information which was used at test may be stored in SCS databases depending on operations performed by those tools.



IMPORTANT

To restore an SCS to Online Level from Offline Level, restart the SCS or do offline download. This ensures that the system returns to the security level for normal operation.

The Following are operational items in each security level. It is possible to refer to SCS and write information that are not related to the Safety Function at any levels.

Table 2.12.1-2 Operations Performed to SCS and Required Security Levels

Write Operation to SCS	Security Level (*1)			Operation
	Level 2	Level 1	Level 0	
Override from HIS	OK	OK	OK	HIS
Operation on password block from HIS	OK	OK	OK	HIS
Operation on manual operation block	OK	OK	OK	HIS
Confirmation of Process Alarm	OK	OK	OK	HIS
Setting operation mark on mapping element/mapping block	OK	OK	OK	HIS
Confirmation and Deletion of Diagnostic information	OK	OK	OK	SENG
Setting of system time	OK	OK	OK	HIS/SENG
Change of security level	OK	OK	ERROR	SENG
IOM Download (*2)	OK	OK	OK	SENG
Resetting of TRIP signal file	OK	OK	OK	SENG
Change of passwords for security level	OK	OK	OK	SENG
Lock/Unlock of variables	ERROR	OK	OK	SENG
On-demand communication for device management	OK	OK	OK	PRM
Change of variable value with Forcing Function	ERROR	OK	OK	SENG
Online change download of applications	ERROR	OK	OK	SENG
I/O Lock Function	ERROR	OK	OK	SENG
Communication I/O Lock Function	ERROR	OK	OK	SENG
Switching Control right for dual-redundant AIO/DIO Modules	ERROR	OK	OK	SENG
Offline Download	ERROR	ERROR	OK	SENG
Application Debug Function	ERROR	ERROR	OK	SENG

Continues on the next page

Table 2.12.1-2 Operations Performed to SCS and Required Security Levels (Table continued)

Write Operation to SCS	Security Level (*1)			Operation
	Level 2	Level 1	Level 0	
Restart of SCS from SENG	ERROR	ERROR	OK	SENG
Output Enabled Operation	OK	OK	OK	SENG
Save/Download Operation Marks	OK	OK	OK	SENG
Output module starting operation	OK	OK	OK	SENG

*1: OK: Enabling operation
 ERROR: Operation fails

*2: Downloading can be performed on failed I/O modules.

● **Security Level at the Start of SCS**

The security level is Level 2 when SCS starts normally.

■ **Operation of Security Level**

● **Change Operation of Security Level**

To change the security level from Level 2 to Level 1 or to Level 0 or from Level 1 to Level 0, entering a password from SENG is required. When the security level is changed, SCS notifies the user of the change of the security level with the Diagnostic Information Message.

You can change the security level from Level 1 to Level 2 without a password. To change the security level from Level 0 to Level 2, you must restart the SCS.

● **Protection of Security Level by Hardware Switch**

It is possible to use SYS_SEC_CTL to control whether or not to allow changing the security level from a SENG using an external hardware switch or similar.

- When the SYS_SEC_CTL is used, it is not allowed to change security level by password entry from SENG if the FIX parameter input of the SYS_SEC_CTL is set to TRUE. To change the security level of the SCS, the user needs to operate an external key switch or similar and change to the status where security level change operations are allowed (set the FIX parameter of the SYS_SEC_CTL to FALSE), and enter the appropriate password from a SENG.
- The SYS_SEC_CTL also controls whether it is allowed to reset the security level from Level 1 to Level 2 (even though password entry is not required).
- If the security change enable/disable status is changed by the SYS_SEC_CTL, the status is notified to user via a diagnostic information message.
- Resetting of the security level to Level 2 via RST input in the SYS_SECURE block and resetting of the security level to Level 2 via the CPU's restart switch are not affected by the security change enable/disable status of the SYS_SEC_CTL.



IMPORTANT

The situation when the FIX parameter of the SYS_SEC_CTL is constantly set to TRUE by erroneous applications should be surely avoided.

SEE ALSO

For more information about specification of the SYS_SEC_CTL, refer to:

C10.8, "SYS_SEC_CTL (security level protection)" in Safety Control Station Reference (IM 32Q03B10-31E)

● **Reset Function for Security Level**

When a fault occurs in SENG or the communication line while the security level (Level 1) is being changed, it is required to reset the security level (back to Level 2) as soon as possible to ensure security of SCS. The SYS_SECURE block in the application logic can reset the security level with RST input.

- It is possible to reset from Level 1 in the SYS_SECURE block, not from Level 0.
- Connecting a discrete input signal to RST makes it possible to reset the security level with a key switch or a button. When this is not necessary, set FALSE to RST.
- The SYS_SECURE block detects the change of RST input from FALSE to TRUE and resets the security level.

● **Monitoring Function of Security Level**

When the security level of an SCS is in Level 1, the SYS_SECURE block monitors duration of the status. If the status of Level 1 continues longer than the time specified by the CHKT input in the SYS_SECURE block, a diagnostic information message occurs. After notifying the diagnostic information message, the duration is monitored again. The status of Level 0 is not monitored.

The following figure shows an example of application using the SYS_SECURE.

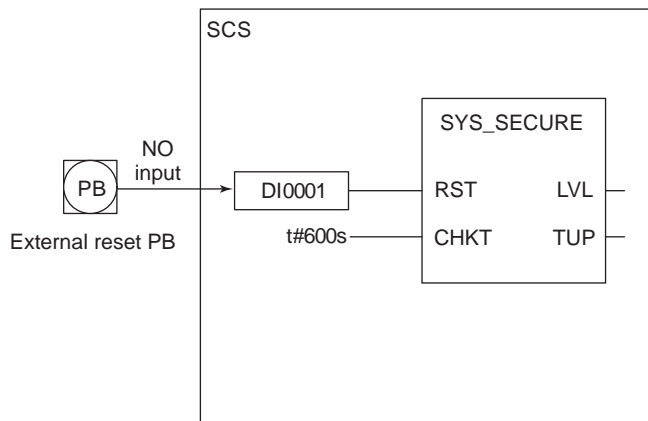


Figure 2.12.1-2 Example of Application Using Security Block

■ **Passwords for Changing Security Level**

● **Specification for Passwords**

- Passwords for the security level are controlled in SCS.
- A password for the security level is set for each security level. It is necessary to set the password to change to Level 1 and Level 0 respectively. A password is not necessary to change to Level 2.
- A password is 16 alphanumeric characters (*1)at maximum, which is upper/lower case sensitive.
- Passwords are maintained during a power cut and restart of SCS.
- Passwords are deleted by SCS offline download.

*1: Including a space character and
 ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~

● **Setting and Changing Passwords**

- Change passwords on the SCS Manager in SENG.

- Passwords can be changed when SCS is in operation.
- To change a password, user must enter the old password before it is changed.
- When a password has been changed, SCS notifies its change with the Diagnostic Information Message.

SEE ALSO

For more information about an operation to change the SCS Security Level and to set passwords, refer to:
[1.3, "Security of SCS" in Utilities and Maintenance Reference \(IM 32Q04B20-31E\)](#)

■ Precautions when Changing SCS Security Level

- Set different passwords for each SCS.
- Set a different password for each security level.
- When the security Level of SCS has been changed, confirm that the change is made to an appropriate level with the SCS State Management Window.
- Do not set the security levels to Level 1 or Level 0 for several SCSs at the same time when SCSs are in operation.
- If setting a password to SCS during APC (All Program Copy), APC restarts. It takes about 10 minutes from setting a password, after offline download, to restarting the operation of the dual-redundant system.
Do not change passwords during APC except the changes required for after offline download.



IMPORTANT

- When a password is not set, entering characters in the Password Entry Dialog causes an error. Considering safety as the safety system, always set passwords to use.
- Power failure or restart does not change or delete passwords.
- Passwords are deleted when offline download is performed. As there is no password after offline download, set new passwords after performing offline download.
- Passwords cannot be referred to after setting them. User should remember the set password. Also, Password should be controlled so that unauthorized users do not know it.

■ Precautions when Using the SYS_SEC_CTL

The SYS_SEC_CTL block can control whether or not to enable the security level change by password entry from SENG. In general, an application containing the following blocks should be created.



Figure 2.12.1-3 General Application Example

Connect the toggle switch signal for controlling the security level change output from a DI module to the FIX parameter input of the SYS_SEC_CTL block. This makes it possible to switch the security change permission status via the external toggle switch. By connecting the output parameter to a lamp or similar, the security level change permission status can be displayed on an external device.

If the external toggle switch is connected to SYS_SEC_CTL, make sure to examine all possible states of the DI module or channel to which the toggle switch signal is input.

If an error occurs in the DI module or channel, SYS_SEC_CTL controls the security level change permission status as follows according to the Input Processing at Fault setting in the I/O Parameter Builder.

Table 2.12.1-3 Security Level Change Control Operations

the Input Processing at Fault	Operation at Errors
1 (TRUE)	Changing security level by password entry via a SENG is disabled until the fault is corrected. (*1) If a fault occurs in Level 1, it is possible to reset to the same security level by the SYS_SECURE block (*2) or reset to Level 2 by restarting the SCS. It is, however, not possible to change to a lower level until the fault is corrected. (*3) (*4)
0 (FALSE)	During a fault, it is possible to change security level by password entry via a SENG.
HOLD	The operation performed before the fault occurred resumes. In other words, if an error occurs in the status where security change is unavailable (FIX is set to TRUE), the status where security change is not allowed is retained after the error occurrence. If an error occurs in the status where security change is allowed (FIX is set to FALSE), the status where security change is allowed is retained after the error occurrence. If an error occurs in the status where security change is unavailable (FIX is set to TRUE), it is necessary to take the same precautions as when inputting TRUE at Input Processing at Fault.

*1: Do not lock the input/output variables connected to FIX and change the security level to Level 2. The variables will not be unlocked even after the causes of errors are removed. (In this case, it is necessary to restart the SCS or reset by SYS_FORCE.)

*2: Use separate DI modules for the DI module for inputting the reset signal of the SYS_SECURE block and the DI module for inputting a toggle switch for security control of the SYS_SEC_CTL block.

*3: It is not necessary to lower the security level during recovery operations. If a DI module fails, replace the module and perform IOM download.

*4: It is necessary to take measures such as incorporating an application in order to avoid situations where the security level cannot be reset to Level 2 due to DI module errors when the security level is Level 1.

2.12.2 Security for Project Database

This section describes security for project databases.

■ Setting a Password for Project Databases

Assigning passwords to a database prevents unauthorized users from making changes to the database in SCS projects. Users without entering the password can be given permission for read only operation.

Passwords can be specified for the following.

- For each SCS Project
- For each POU

The reading and writing right for the whole project and the access right for each POU can be controlled using the security function of the SCS project and the security function of each POU.

Set a different password for each SCS Project.

If higher level of security is required, set a password for each important POU.

The POU passwords should be different from the password for the SCS Security Level setting.

Database files in RS projects should not be changed from other tools than the ProSafe-RS Engineering Function.

**SEE
ALSO**

For more information about setting of a password for security of databases, refer to:

[1.2, "Security of Database" in Utilities and Maintenance Reference \(IM 32Q04B20-31E\)](#)

2.12.3 Security for the SCS Maintenance Support Tool

This section describes security for the SCS Maintenance Support Tool.

■ Setting a Password for the SCS Maintenance Tool

The SCS Maintenance Support Tool requires a password entry every time you start a window to ensure the security of the SCS access. Password needs to be set for each SENG.

Each tool in the SCS Maintenance Support Tool can be operated for security by entering a password at the start of each tool. When the password entry is cancelled, the tools' operations are disabled for security and the window is in the read-only mode.

The following table shows whether tools can be operated or not when the password is entered and when password entry is cancelled.

Table 2.12.3-1 Operation of SCS Maintenance Support Tool

Tool	Operations provided security	Inputting a password	Without inputting a password
SCS State Management Window	IOM Download	Enabling operation	Read Only
	Output Enable Operation	Enabling operation	Read Only
	Output Module Start Operation	Enabling operation	Read Only
	Setting Time	Enabling operation	Read Only
Diagnostic Information Window	Confirmation and Deletion of Diagnostic information	Enabling operation	Read Only
Setup Tool	Setting and change of display font, color and operating methods for confirming or deleting messages	Enabling operation	Read Only
SOE Viewer	Display of events of SCS and generation of report	Enabling operation	Enabling operation
Message Cache Tool	Setting of message collection, initialization of TRIP information in SCS and storage and deletion of cache data.	Enabling operation	Read Only

SEE ALSO

For more information about security for the SCS Maintenance Support Tool, refer to:

[1.4, "Security of SCS Maintenance Support Tool" in Utilities and Maintenance Reference \(IM 32Q04B20-31E\)](#)

For more information about Message Cache Tool, refer to:

[3.4, "Message Cache Tool" in Utilities and Maintenance Reference \(IM 32Q04B20-31E\)](#)

For more information about SOE Viewer, refer to:

[4., "SOE Viewer" in Utilities and Maintenance Reference \(IM 32Q04B20-31E\)](#)

● Specification for Passwords

- A password is 16 alphanumeric characters(*1)consisting of 1 through 16 alphanumeric characters which are case sensitive.
- Set a password for each SENG-installed PC.
- There is no password when SENG is installed for the first time.

- Set a password when starting the SCS Maintenance Support Tool for the first time.

*1: Including a space character and

! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` | ~

2.13 Access Control / Operation History Management Functions

This section describes the Access Control / Operation History Management functions.

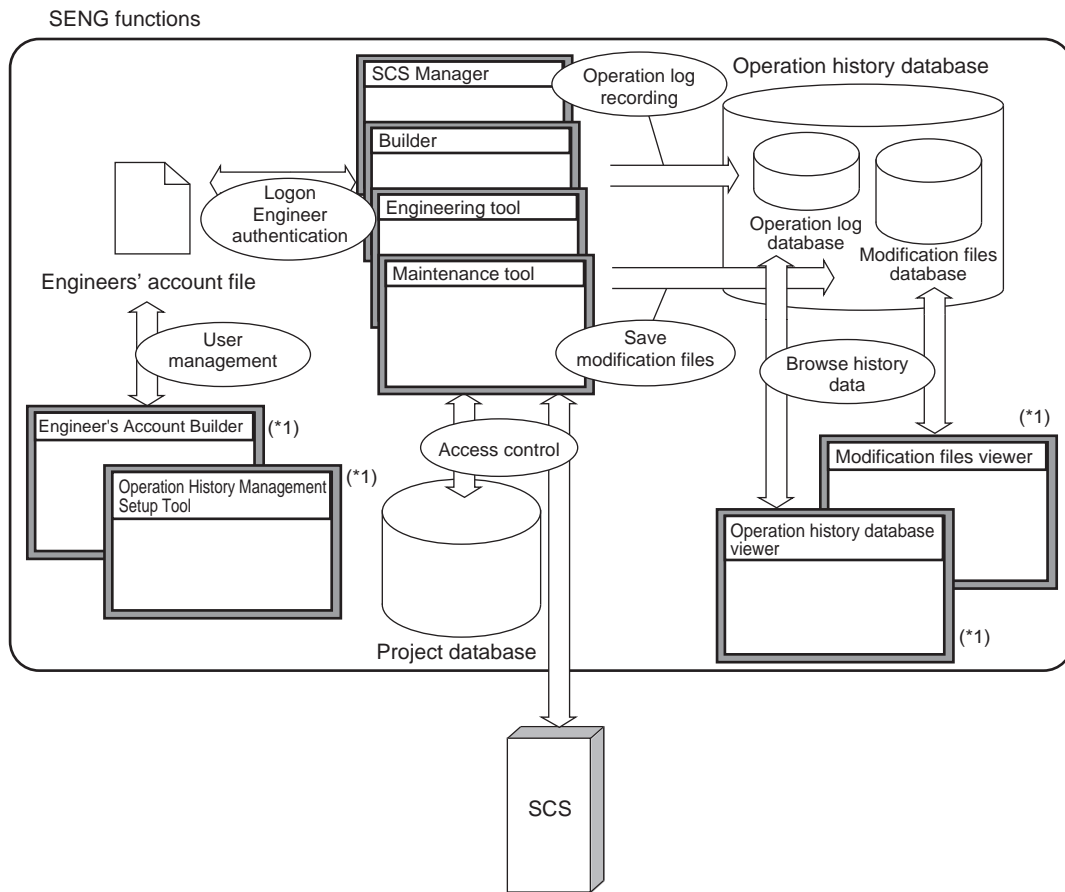
The Access Control/Operation History Management functions provide user-based restrictions to functions of the SENG software and to record or view the operation history of operations in the SENG software.

The Access Control / Operation History Management functions are made up of the following functions.

- **User management**
Manage users (referred to as "engineers" in the following sections) working with SCS Manager and SCS Maintenance Support Tool.
- **Logon / Engineer Authentication**
Logon is a function that prompts the engineer to enter an engineer name and password when starting a SENG function. Engineer Authentication is a function that prompts the engineer to enter a password when executing a specific operation after Logon. The user can select the configuration whether or not to perform Engineer Authentication.
- **Access Control**
A function for specifying whether individual engineers have the authority to perform an operation and to control whether or not the operation is available to perform based on that specification.
- **Record Operation History**
A function for recording operation information in the form of a history when an engineer has performed that operation.
- **View Operation History**
A function for displaying and printing operation histories stored in the History Management Database in order to view them.

■ Configuration

The following figure shows the overall configuration of the Access Control / Operation History Management functions.



*1: These tools are included in the CHS5170 Access Control and Operation History Management Package.

Figure 2.13-1 Overall Configuration of the Access Control / Operation History Management Functions

SEE ALSO

For more information about configuration of the Access Control and Operation History Management Function, refer to:

16.1.2, "Structure of Access Control/Operation History Management Function" in Engineering Reference (IM 32Q04B10-31E)

■ Operating Environment

- **Hardware**
It is recommended that the hard disk of the PC on which the History Management Database is located has at least 100 GB of free space. It is recommended that you provide an auxiliary memory device to back up the History Management Database.

TIP

The size of the History Management Database will increase by up to around 10 MB during a single download. 100 GB of free space therefore equates to 10000 downloads (1000 downloads per SCS if you have 10 SCSs.)

- **Software**
The following package is required on SENGs on which you are running the Access Control / Operation History Management functions, in addition to the CHS5100 Safety System Generation and Maintenance Package.
CHS5170 Access Control / Operation History Management package

The package is not required on PCs that are only for registering the History Management Database.

If the number of connections to the PC on which the History Management Database is installed is five or more, use a server OS on this PC.

■ System Configuration

The following figure shows an example of a system configuration using the Access Control / Operation History Management functions.

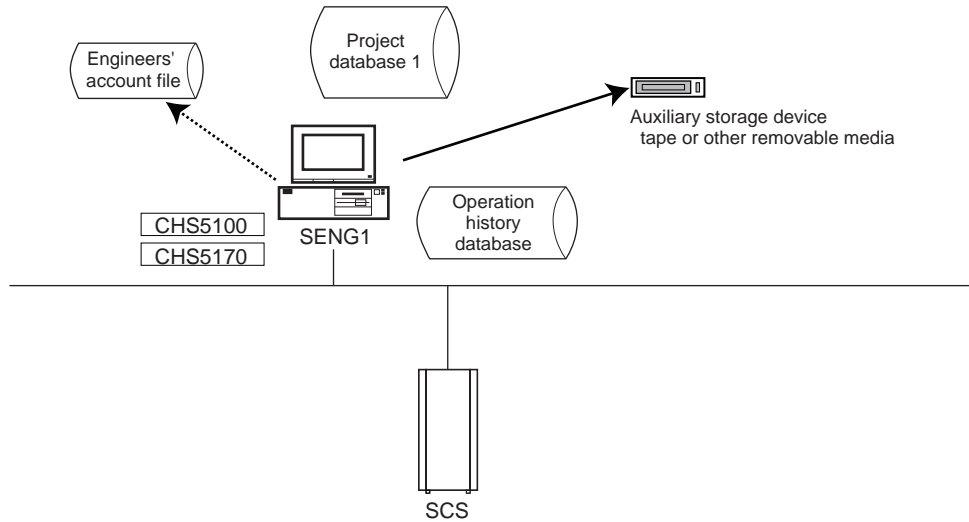


Figure 2.13-2 Example of a Minimum Configuration

The following figure shows an example in which the functions are deployed on multiple SENGs. The History Management database is located on a dedicated PC. The engineer registration information is also located on the dedicated History Management PC so that it is referenced commonly by multiple SENGs, and set as shared.

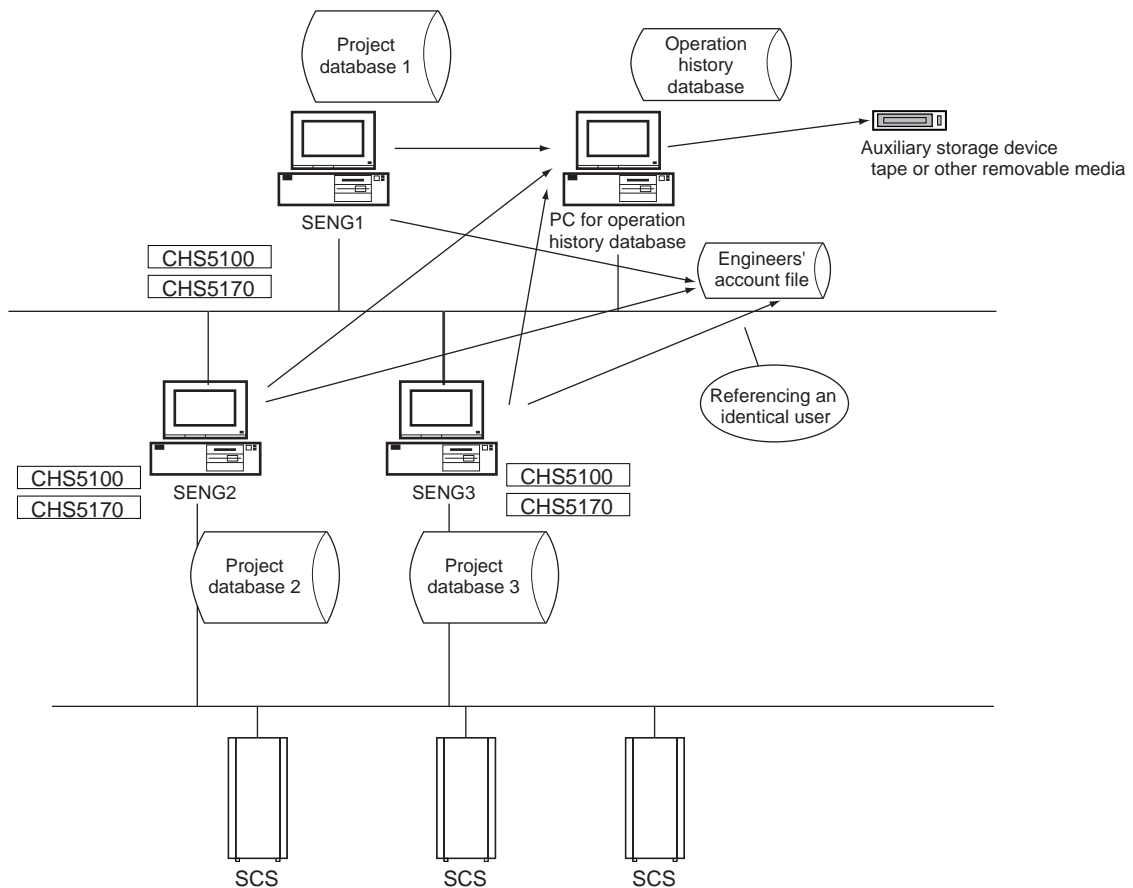


Figure 2.13-3 Example of Use on Multiple SENGs



IMPORTANT

When using the Windows authentication mode, ensure that the system to which Domain management or Combination management is applied consists of a single Windows domain in order to unify user management and passwords on all terminals. Otherwise, a security loophole is created.

● Guidelines for the Locations of the Engineer Registration File and History Management Database

Ensure that the locations of the Engineer Registration File and History Management Database specified in the Operation History Management Settings Tool are fully secure.

Make sure that these folders are not inadvertently opened in Explorer. It is recommended that you set access permissions that give access to no one but administrators and engineers.

- If the PC on which the History Management Database is located does not have a server OS installed on it, make sure that the number of PCs accessing the disks on that PC is no more than four. To perform History Management functions from five or more SENGs, locate the History Management Database on a PC with a server OS installed on it.
- For the PC where the History Management Database is located, you must create the folder for placing the database before applying the IT security tool.
- If the PC where the History Management Database is located does not have a server OS installed on it, ensure that, as a rule, the CENTUM project database is not located on that PC.

The storing of history data in the History Management Database and the clearing of the History Management Database may fail if the History Management Database and the CENTUM project database are on the same PC.

TIP

- If the storage of history data fails during the operation to start History Management, cancel and perform the start operation again.
- If clearing of the History Management Database fails, perform the clear operation again.

SEE ALSO

For more information about setup procedure of the file server, refer to:

[A2.2.3, "Setup Procedure for a File Server" in Installation \(IM 32Q01C50-31E\)](#)

■ Combined Use with Product Security Functions

The Access Control / Operation History Management functions are additional to the Product Security functions provided as standard in ProSafe-RS. They are functionally independent, and can therefore be used in combination. However, if you use the Access Control / Operation History Management functions, the password entry function in the SCS Maintenance Support Tool is suppressed.

When using the Access Control / Operation History Management functions in combination with the Product Security functions, configure the Product Security settings as follows.

- **Project password**
The project password gives permissions to users for opening and viewing the project (except when the project is set to allow Read Only opening). When you need to restrict some registered engineers' access to view the project, manage the project by applying a project password (set not to allow Read Only opening) and circulating it only to engineers who are allowed to view the project.
- **POU password**
The POU password gives permissions to users for opening and viewing specific POU. When you need to restrict some registered engineers' access to open and view the particular POU, manage the project by applying a password to the POU and circulating it only to engineers who are allowed to view the project.
- **SCS security level password**
An SCS security level password is a separate password for each SCS that is independent of the SENG users, and provides a system for determining whether execution is possible on the SCS. Ensure that an SCS security level password is always set.
- **SCS Maintenance Support Tool password**
The password entry function in the SCS Maintenance Support Tool is suppressed when the Access Control / Operation History Management functions are being run. Log on is necessary in Logon / Engineer authentication function instead. Use the password for the SCS Maintenance Support Tool when you are not running the Access Control / Operation History Management functions.

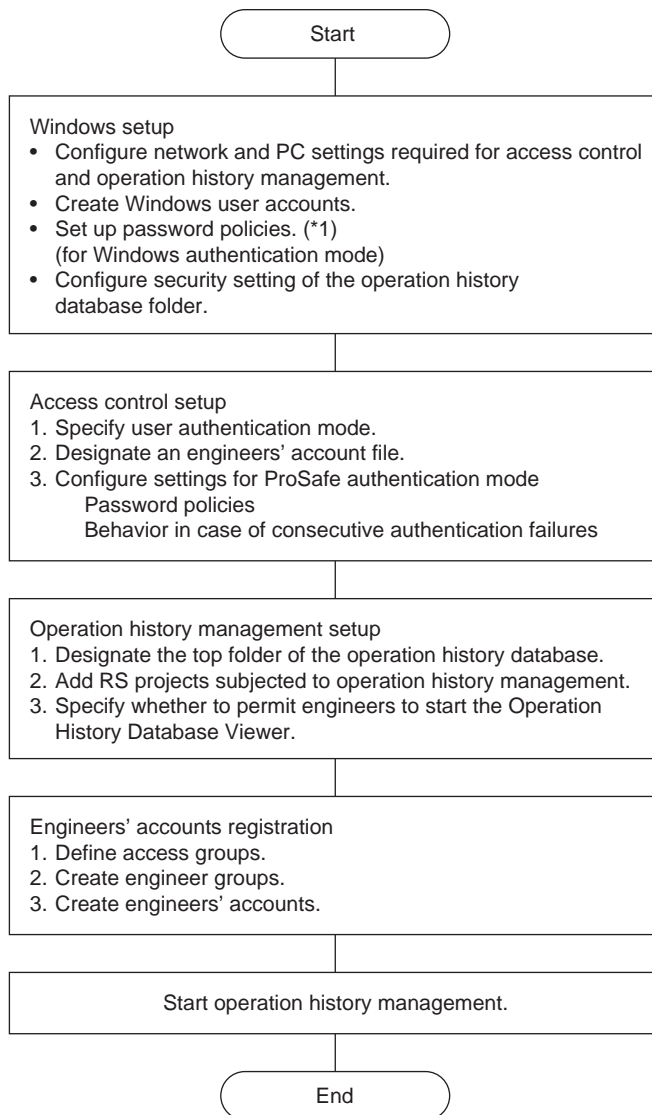
■ Access Control / Operation History Management Procedure

Before you start the first operation, the Access Control/Operation History Management functions need to be set up by an administrator. The following settings are configured, using mainly the Operation History Management Settings Tool.

- Specify the authentication mode
- Register the engineer
- Set the password policy
- Specify whether or not to implement Engineer Authentication

- Specify the path for the History Management Database
- Start / stop History Management

The task sequence is as follows:



*1: You can set password policies any time before operation history management is started.

Figure 2.13-4 Access Control / Operation History Management Sequence

SEE ALSO For more information about the settings, refer to:

[16.2, "Setting Up Access Control/Operation History Management" in Engineering Reference \(IM 32Q04B10-31E\)](#)

■ Executing Operation History Management

Engineers must first log on when starting an operation with a SENG function. Enter an engineer name and password as a logon operation. If the engineer name and password are entered correctly, subsequent SENG operations can be executed. If the engineer chooses Cancel, the operation cannot be executed. After logon, the following processes are executed whenever an engineer performs an operation managed with History Management.

- Access Right Check

The system checks whether the engineer who has logged on has the access right to perform the operation in question. If the engineer has access right, he/she can perform the operation. If the engineer does not have access right, an error occurs and he/she cannot perform the operation.

- Engineer Authentication (only if the option "Do not require engineer authentication on individual operations" is unchecked)
When an engineer executes an operation, he/she enters the engineer password under which he/she is logged on and an optional comment. If the engineer enters the correct password, he/she can execute the operation. If the engineer chooses Cancel, the operation cannot be executed.
- Store Operation History
Once the operation is complete, a history log is recorded for the operation and a modification file is saved based on the type of operation (the modification file is only saved if the option "Do not save modification files" is unchecked.)

The engineering procedures carried out by engineers after History Management is started are the same as the ones when History Management is not being run except for these procedures.

**SEE
ALSO**

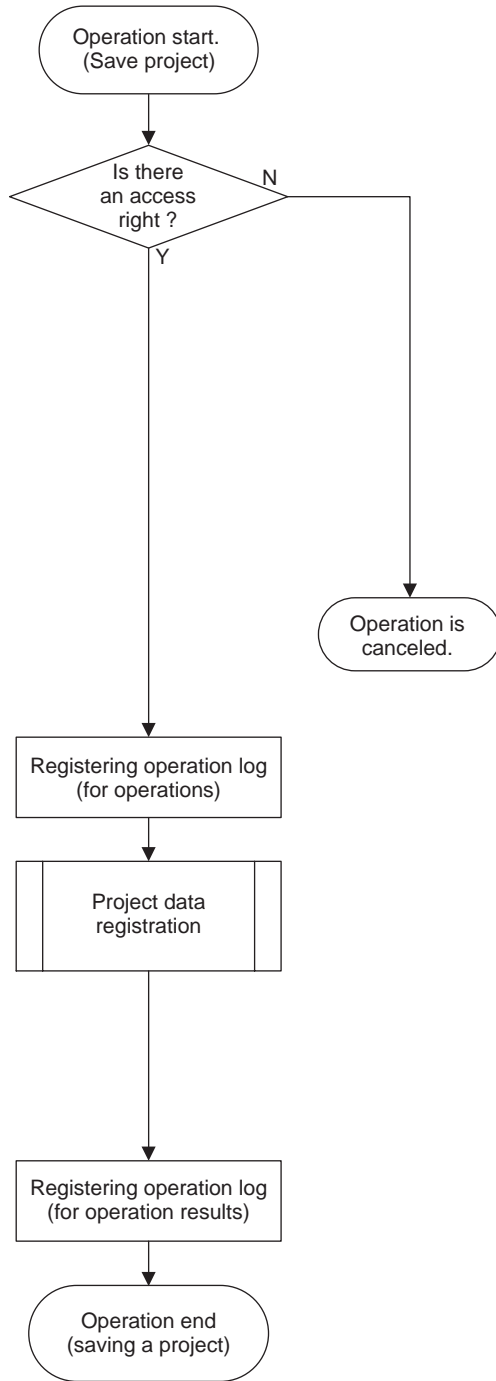
For more information about target operations for access control and Operation History Management, refer to:

[16.1.3, "Access Control/Operation History Management Target Operation List" in Engineering Reference \(IM 32Q04B10-31E\)](#)

■ Operation History Management Process Flow

The History Management process flow is shown in the following figure.

Operation "Saving a project"



Operation "Offline downloading"

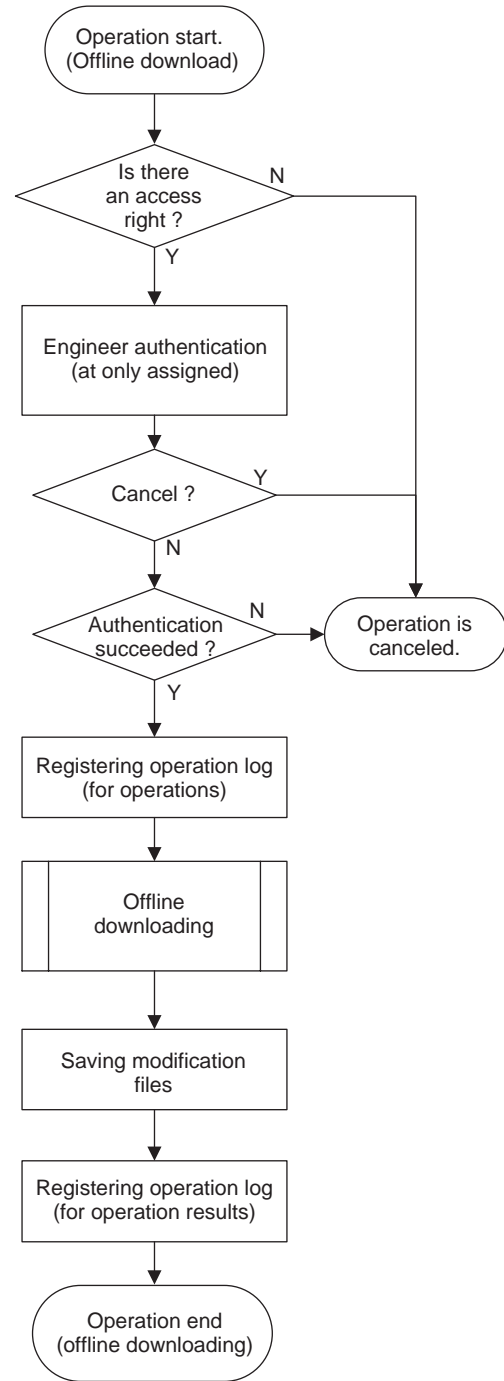


Figure 2.13-5 Example of a History Management Process Flow

■ Access Right

With the SENG Access Control and Operation History Management functions, access rights for project databases and access rights for SCS/SCS simulators are handled. These access rights are further broken down into categories.

**SEE
ALSO**

For more information about categories of access right, refer to:

16.5.2, "Access Rights Category List" in Engineering Reference (IM 32Q04B10-31E)

For more information about setting the access right, refer to:

16.2.3, "Registering Engineers" in Engineering Reference (IM 32Q04B10-31E)

2.14 Configuration of the SOER

This section describes functions of the SOER.

The SOER (Sequence of Events Recorder) is for recording and analyzing events detected by SCS. In ProSafe-RS, the SOER is used for the user to analyze the cause of a trip based on the event information detected right before and after the trip.

The user provides definition related to the SOER on SENG. The definition is downloaded to the CPU and the DI module of SCS. The event collected and saved by SCS is uploaded to the SOE viewer on SENG or HIS.

**SEE
ALSO**

For more information about SOER function, refer to:

[A7., "SOER" in Safety Control Station Reference \(IM 32Q03B10-31E\)](#)

2.14.1 Event Collection Function

This section describes the Event Collection Function.

■ Event to be Collected

SCS can collect events depending on user definitions as follows:

Table 2.14.1-1 Type of Event Collection

Type	Timing and location for event collection	Time stamp Event
Discrete input (DI)	The input module collects events when the input data value to the input module changes.	The time of DI module when the event occurs.
Discrete output (DO)	The CPU collects events when the output data value to the output channel changes.	The time of SCS immediately before an output value is set to DO module.
Variable of application logic	SOER FB (SOE_B / SOE_I / SOE_R) for event collection collect events, which are Boolean, integer-type, and real-type. ANLG_S and ANLGI FB collect events.	The time of SCS when a scan cycle starts.

SEE ALSO

For more information about function block (ANLG_S, ANLGI and SOE_*), refer to:

- C3., “Safety function blocks” in Safety Control Station Reference (IM 32Q03B10-31E)
- C7., “Interference-free function blocks” in Safety Control Station Reference (IM 32Q03B10-31E)

■ Storage of Event

The event information is stored in the SOER event information storage area in SCS. There are two types of file to contain event information: an event log file and trip signal files.

● Event Log File

Up to 15,000 events can be stored in the event log file. When the number of events in one log file exceeds its capacity, the oldest event is overwritten with a new event.

● Trip Signal File

If the trigger signal for the SOE is set to 'trip signal', a trip signal and events before and after the trip are stored in SCS in a trip signal file separately from other events.

The stored trip signal file is not automatically deleted.

- Two trip signal files are saved in SCS. Even when more trip signals occur, no more trip signal file is created. If a trip signal file is created, immediately check if the trip signal file is uploaded from the SENG and initialized.
- The trip signal is an extremely important signal to analyze the cause of the trip. To keep important event information, the settings of trip signals must be sufficiently examined.

SEE ALSO

For more information about resetting of TRIP signal file, refer to:

- 3.4.5, “Initialization of Tripping Information” in Utilities and Maintenance Reference (IM 32Q04B20-31E)

■ Event Collection of Application Logic

The following figure shows an example of an application with FBs for the SOE event collection.

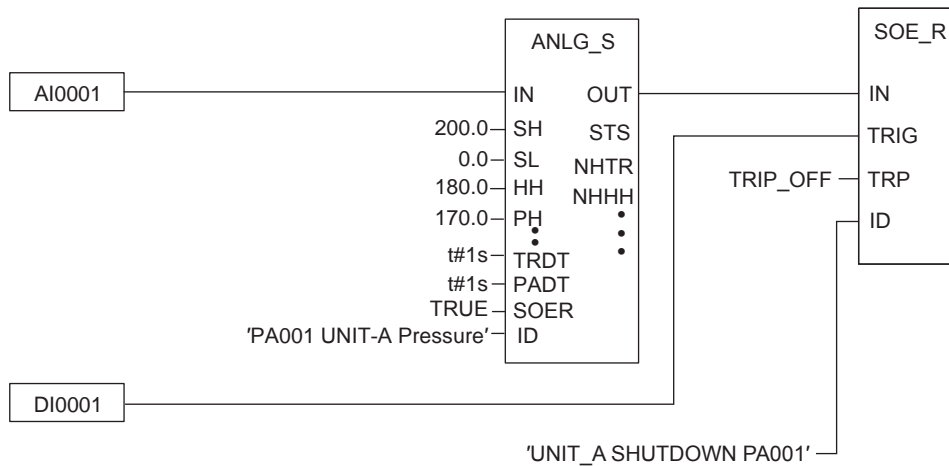


Figure 2.14.1-1 Example of Application with FBs for SOE Event Collection

In the figure, the "SOE_R" FB collects the output value (OUT) of the "ANLG_S" FB together with the character string "UNIT_A SHUTDOWN PA001" when DI0001 changes value. The SOER of the "ANLG_S" is set to TRUE, so that the "ANLG_S" FB collects the alarm status with the character string "PA001 UNIT-A Pressure" when alarm of the FB occurs.

● **Precautions for Creating an Application**

- Comment(s) is added to the DI events and DO events. Comments are bound with input/output variables wired to its channel. (Max. 32 characters) Set character strings that can identify events from the Dictionary View window on the SCS Manager.
- For the function block (ANLG_S/ANLGI/SOE_*) used for acquiring events on variables in application logic, specify the number of characters (max. 32 characters) for comments added to events from the Multi-Language Editor window in SCS Manager. Comments are used to identify events.
- For acquiring analog output value (AO) as events, specify the 'value set to output variable' in SOE_R also. Specify the timing of acquiring events as a trigger signal in application.

2.15 Time Synchronization

SCS is capable of synchronizing the time among SCSs, SCS and DI modules to make the event log accurate.

SEE ALSO

For more information about time synchronization, refer to:

[A3.2, "Time synchronization of SCS" in Safety Control Station Reference \(IM 32Q03B10-31E\)](#)

■ SCS Type and Time Synchronization

SCS for V net synchronizes with different time synchronization methods from SCS for Vnet/IP.

SCS for V net: V net time method or IRIG-B time synchronization is selectable.

SCS for Vnet/IP: Vnet/IP time synchronization is the only option.

Table 2.15-1 Time Synchronization Methods

Type	Target SCS	Description
V net time synchronization (Standard)	For V net	The mechanism that synchronizes the clock of devices connected on V net is used. User sets the V net time from Adjust Time dialog box on SENG or HIS.
IRIG-B time synchronization (Option)	For V net	The GPS unit is used as the standard time server, and the output (IRIG-B) from the unit is connected to each SCS. The IRIG-B time is used for time stamps of events and alarms set by the CPU of the SCS. This method uses GPS and therefore produces more accurate timing for events among SCSs compared to the V net time synchronization method. The time of the CPU module and DI modules are synchronized to the IRIG-B time.
Vnet/IP time synchronization	For Vnet/IP	The system clock of SCSP synchronizes with Vnet/IP time. If SNTP server is connected, the clock synchronizes with more accurate absolute time. All the stations in one time group connected with a control bus have the same time data.

■ Precautions for Time Synchronization

● **When Vnet/IP Time Synchronization is Selected: SCSP2/SCSP1**

- If the Vnet/IP time synchronizes with the SNTP server, time setting from SENG or HIS is ignored.
- Changing the Vnet/IP time may cause the SOE generation order to be reversed. Be sure to take the timing to set the time and the difference of the time into consideration when setting the V net time.



WARNING

Do not change the Vnet/IP time from more than one SENG or HIS concurrently. It may cause the following errors:

- Self-diagnosis function detects a clock error on the running non-redundant SCS and a system alarm is raised.
- Self-diagnosis function detects a clock error on one of the running redundant SCS and the control right is switched to the standby CPU module.

- **When the V net Time Synchronization is Selected**

Changing the V net time may cause the SOE generation order to be reversed. Be sure to take the timing to set the time and the difference of the time into consideration when setting the V net time.

- **If a Vnet/IP Domain and a V net Domain are Connected via a V net Router**

The following precautions apply in a situation where a V net domain and a Vnet/IP domain are connected via a V net router and the V net time synchronization and the Vnet/IP time synchronization are selected as their respective time synchronization methods.

- If you are using a V net router of style S3 or above and have enabled the Transfer system time ([Transfer higher] or [Transfer lower]) in the V net router property of System View for CENTUM VP R5.01 or later, it is not possible to change the time from a SENG in the domain to which the time is transferred.
- If you are using a V net router of a style below S3 and have enabled the [Transfer lower] of Transfer system time ([Transfer System Time - Transfer lower] for CENTUM VP earlier than R5.01), it is not possible to change the time from a SENG in the V net domain that constitutes a lower domain.

- **When the IRIG-B Time Synchronization is Selected**

- It is necessary to synchronize V net clock with IRIG-B clock.
- If the input of the IRIG-B signal fails, SCS updates the time based on the IRIG-B time immediately before the failure. (No synchronization with V net time)
- When the input of the IRIG-B signal recovers, the displayed time may be set back to synchronize with the IRIG-B time again. In this is case, if you want to check the messages and events raised before the recovery, do not sort the messages and events until you finish your check.

**SEE
ALSO**

For more information about time synchronization methods, refer to:

[3.1.3, "SCS Constants Builder" in Engineering Reference \(IM 32Q04B10-31E\)](#)

- **Precautions for Time Setting during a Vnet/IP Network Failure**



WARNING

As a rule, time changes from an HIS/SENG should be made when both buses in the Vnet/IP network are in a normal state.

If you change the time from an HIS/SENG during a network failure, there may be stations on which the time does not change immediately, depending on which area of the network has failed and the circumstances of the failure.

2.16 CENTUM Integration

This section describes the overview and the engineering procedure of CENTUM Integration Configuration.

■ Functions in CENTUM Integration Structure

This section describes the functions of operating SCS from HIS or FCS in the CENTUM integration.

SEE ALSO

For more information about restrictions by software release number of CENTUM systems to be integrated with ProSafe-RS, refer to:

Appendix 1., "Differences in limitations and specifications among software release numbers of CENTUM" in Integration with CENTUM VP/CS 3000 (IM 32Q01E10-31E)

● Monitoring and Operation from HIS

- SCS data can be monitored and operated with tag names through the same interface as the one for FCS, which allows data reference with a faceplate and display of SCS data on a Graphic View.
- SCS data to be collected can be defined as a historical trend by HIS by specifying its tag name and data type, but not as a high-speed trend (1 sec).
- The occurrence/recovery of process alarm and annunciator messages which were detected by SCS can be managed on the Process Alarm View of HIS.
- Diagnostic information messages issued at SCS can be monitored on the System Alarm View of HIS.
- SCS status can be shown on the SCS Status Display View of HIS.
- The values of the variables of the SCS application logic can be overridden by HIS. This is the function of fixing a variable of SCS application logic at the predefined value temporarily.
- Boolean variables of SCS application logic can be set to 1 or 0 by HIS with password authentication.
- CAMS for HIS (Consolidated Alarm Management Software for HIS) is the software for managing the alarms on HIS. When CAMS for HIS is enabled in CENTUM, the System Alarm View and Process Alarm View showing respective alarms generated by ProSafe-RS are integrated with the CAMS for HIS windows.



IMPORTANT

The alarm handling feature in HMI has been made more sophisticated, in response to the needs of users. This makes alarm handling easier and more convenient. However, incorrect usage of this feature might result in the filtering out of important alarms critical to safety. Therefore when configuring alarms, it is important to ensure that critical alarms are always communicated to operators.

**SEE
ALSO**

For more information about override function, refer to:

C5.1, "Override function blocks" in Safety Control Station Reference (IM 32Q03B10-31E)

For more information about data setting function with password authentication, refer to:

C10.10, "SYS_PSWD (password function blocks management)" in Safety Control Station Reference (IM 32Q03B10-31E)

For more information about CAMS for HIS, refer to:

3.1.6, "Message monitor of CAMS for HIS" in Integration with CENTUM VP/CS 3000 (IM 32Q01E10-31E)

● Communication Between FCS and SCS

- The variable of SCS application logic can be set by FCS with SFC blocks. The External Communication Function Block is used for SCS. In this case, the SCS data must be confirmed by reading the data back by FCS. This function does not affect the safety function of SCS.
- SCS data can be read by FCS using tag names and the FCS function of connecting between stations.
- From the Switch Instrument Block or the Motor Control Block, data can be set to the External Communication FB on the SCS using Inter-station Data Link Block (ADL). However, there are some precautions as following: Do not change frequently (every second) the MV in the Switch Instrument Block or Motor Control Block connected to SCS tags using ADL. If you use the three-position type Switch Instrument Block or the Motor Control Block on FCS, note the following:
 - Use enhanced Switch Instrument Block or Motor Control Block. Non-enhanced function blocks cannot connect with three-position type input and output via ADL.
 - In ADL connection, synchronization of open signal and close signal from/to three-position type input and output is not guaranteed. Both open signal and close signal from/to input and output can become ON (PERR status) at the same timing. Mask the PERR alarm using the answer-back inconsistency alarm mask in enhanced Switch Instrument Block or enhanced Motor Control Block for three-position type input and output.
 - For three-position type output, create a logic considering the behavior when both open signal and close signal turn ON at the same timing on the SCS side (which has the priority, for example).
 - When you change the MV in Switch Instrument Block or the Motor Control Block on FCS from 2 to 0, first change it from 2 to 1 then 1 to 0. This will prevent both the ON-open signal and ON-close signal from sending to SCS from FCS. Take enough time when the MV is 1 (twice the time taken in ADL communication period)

■ Limitations on the Number of Data Setting Requests via Tag Name Interfaces

An SCS places priority to executing application logic function within the scan period. Data setting via tag name interface is processed on the basis of maximum 4 packets per second if the scan period is shorter than 250 ms, or one packet per one scan if the scan period is 250 ms or longer. Taking data congestion into consideration, up to 8 packets for setting data can be received and stored as they are generated, and processed internally in sequence at intervals of one scan period of application logic. This number of packets does not include communication via the Modbus slave connection function. If 8 unprocessed packets have accumulated in the SCS, and an additional packet is issued from HIS or FCS, a data setting error is generated.

SCS can process only one communication frame at one time in the order of reception, either from HIS/FCS or from Modbus.

● **Types and Communication Packet of Data Setting Requests**

The types and communication packet of data setting requests are as follows:

- Data setting requests from an associated faceplate and windows of HIS (one data operation constitutes one communication packet)
- Data setting via SEBOL all-data setting statements of SFC blocks of FCS (one all-data setting statement constitutes one communication packet. Up to 32 data items can be set per all-data setting statement.)

● **Operations and Actions to be Taken at Error Occurrence**

The following are operations and actions to be taken if communications become congested and cannot be processed.

- If an error occurs as a result of a data setting request from HIS, the message "Communication error occurred" is displayed. If the reason is that data is set at the same timing as data setting from FCS, avoid the collision and perform data setting again.
- If an error occurs as a result of data setting via a SEBOL statement, an error is stored in the SEBOL error storage variable. A system alarm occurs if no error storage variable has been specified. If large amounts of data need to be set repeatedly with SEBOL statements, the system should be designed accordingly, for example by ensuring that data is set in a specific sequence and confirming that each processing is carried out correctly.



IMPORTANT

Do not set data periodically to SCS from control blocks such as PID or MLD, or from arithmetic/logic calculation blocks such as CALCU, using inter-station data link blocks (ADL) of FCS.

● **Error Codes Returned from SCS in CENTUM Integration Configuration**

When you try to set data from CENTUM stations to an SCS on CENTUM Integration, the following error codes may be returned due to an application error.

Table 2.16-1 Error Codes Returned by SCS

Error code	Meaning (cause)	Action
0x5408	Setting request buffer in SCS is FULL.	Check the applications that periodically set data to SCS.
0x5409	The number of Setting requests exceeded SCS's capacity.	Check the applications that set a number of data to SCS.

■ **Variable and Function Block to which a Tag Name can be Assigned**

In the CENTUM Integration Configuration, the variables or the function blocks of the SCS application logic need to have tag names to be accessed from HIS.

When a tag name is assigned with the tag name builder, a mapping block/element is created. These mapping blocks/elements are accessed from outside.

Tag names can be assigned to I/O variables, internal variables, and certain variables or function blocks including ANLG_S/ANLGI, VEL, OVR_* (Override FB), PASSWD (Password FB), ECW_* (External Communication FB), MOB_* (BOOL-Type Data Manual Operation FB), MOA (Analog-Type Data Manual Operation), and SCS_*, SCI_*, SCO_* (Subsystem Communication I/O FB).

SEE ALSO

For more information about variables to which tag names can be assigned, refer to:

2.1.4, "Defining tag names" in Integration with CENTUM VP/CS 3000 (IM 32Q01E10-31E)

Engineering Procedure of CENTUM Integration Configuration

In the CENTUM Integration Configuration, engineering needs to be performed by using both the SENG functions and the CENTUM system builders. The following figure shows the engineering procedure in the CENTUM Integration Configuration.

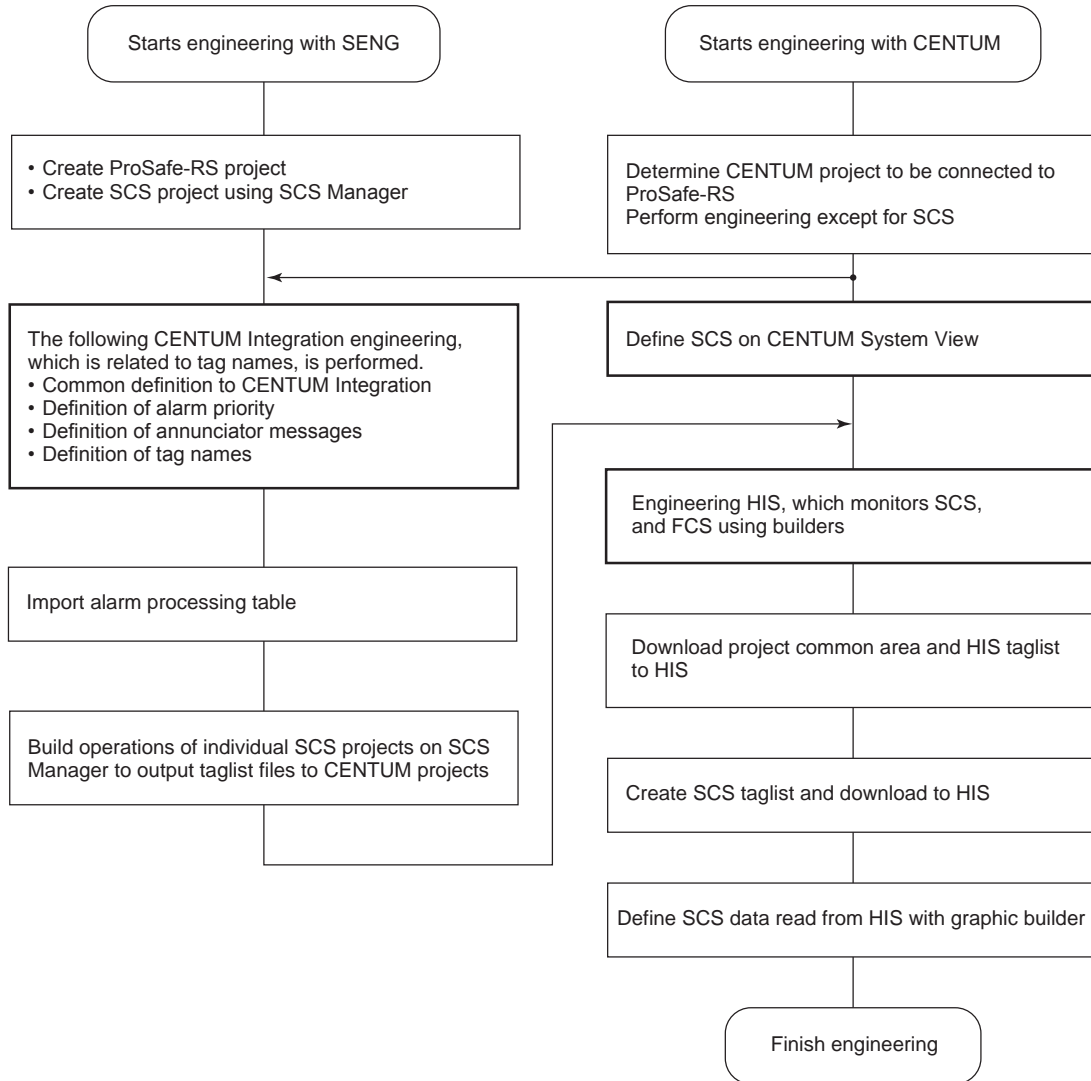


Figure 2.16-1 Engineering of CENTUM Integration

The following are the engineering items performed by SENG and CENTUM.

Table 2.16-2 Engineering with SENG

Engineering	Details	Builder to be used
Common definition of CENTUM Integration	Defines the top folder of the CENTUM project for CENTUM Integration	SCS Project Properties
Definition of alarm priority	Defines the handling of SCS process alarms in SCS, which appear on HIS	Alarm Priority Builder

Continues on the next page

Table 2.16-2 Engineering with SENG (Table continued)

Engineering	Details	Builder to be used
Definition of alarm processing table	Import the alarm processing table, which defined on CENTUM	Alarm processing Builder
Definition of annunciator messages	Defines the contents of process alarms, which appear on HIS	Tag Name Builder
Definition of tag names	Allows CENTUM to access the variables of application logic by assigning tag names	Tag Name Builder

Table 2.16-3 Engineering with CENTUM

Engineering	Description	Builder to be used
Definition of SCS	Defines the SCS as one station of CENTUM projects for connecting SCS project and CENTUM project	System View
Generation of SCS Taglist	Connects the SCS project and CENTUM project. The SCS project is included in the CENTUM project	System View
Definition of SCS data reference from HIS	Creates a Graphic View shown on HIS	Graphic Builder

Perform other engineering for HIS, which includes the trend definition and the operation mark definition for the operation and monitoring function of HIS, and data settings of SCS from FCS as necessary.

Even if SCS project and CENTUM project are not connected, you can define SCS using the builders for CENTUM; you can also edit the tag name-related application programs and create a database of SCS mapping blocks/elements using the SCS Manager. However, duplication check for tag names using System View or creating database for operating and monitoring mapping blocks/elements from HIS is not possible if SCS project and CENTUM project are disconnected.

SEE ALSO

For more information about engineering of CENTUM Integration, refer to:

2., “Engineering for CENTUM integration” in *Integration with CENTUM VP/CS 3000 (IM 32Q01E10-31E)*

For more information about SCS property, refer to:

2.1.1, “Setting of SCS project property” in *Integration with CENTUM VP/CS 3000 (IM 32Q01E10-31E)*

For more information about Alarm Priority builder, refer to:

2.1.2, “Defining alarm priorities” in *Integration with CENTUM VP/CS 3000 (IM 32Q01E10-31E)*

For more information about Tag Name builder, refer to:

2.1.4, “Defining tag names” in *Integration with CENTUM VP/CS 3000 (IM 32Q01E10-31E)*

For more information about the security operation, refer to:

1.3, “Security of SCS” in *Utilities and Maintenance Reference (IM 32Q04B20-31E)*

Relationship between Projects

An SCS project is held by the ProSafe-RS system. An RS project, which includes one or more SCS projects, is the unit handled by the SCS Maintenance Support Tool for SCS Status Overview. A CENTUM project is held by the CENTUM system. SCS projects can be connected with CENTUM projects.

When an SCS project is connected with a CENTUM project, SCS is regarded as one station in the CENTUM project. The following figure shows the relationship between projects. It shows, from the top to the bottom, the station structure, projects, and the display on the SCS Maintenance Support Tool, the SCS Manager, and the System View.

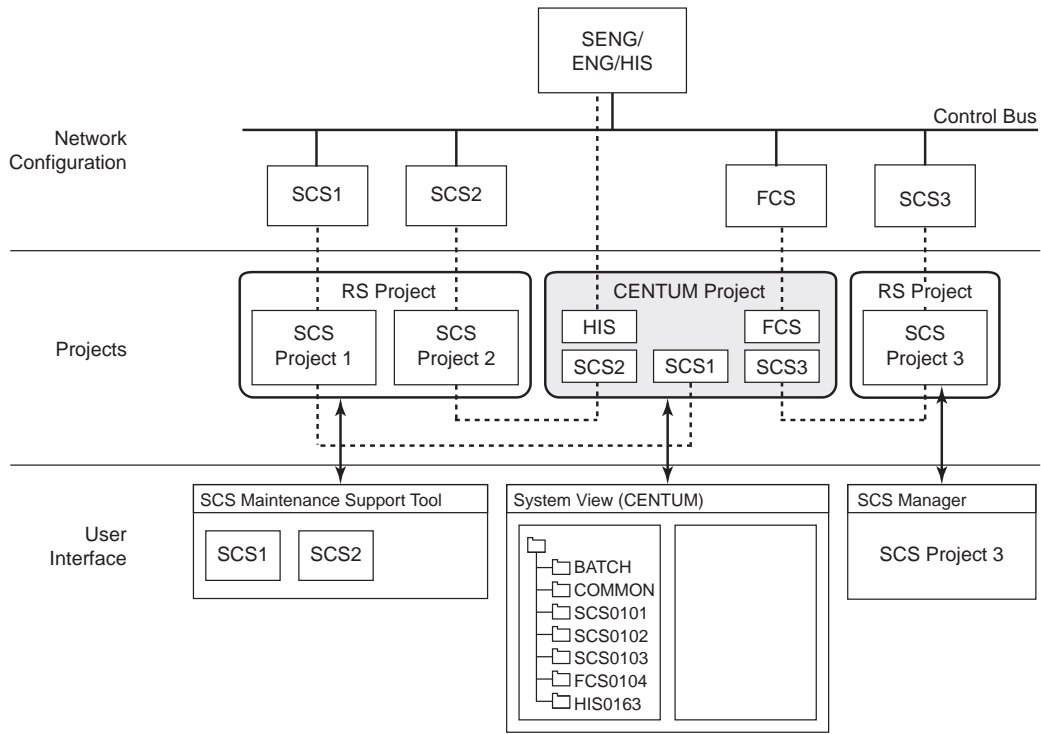


Figure 2.16-2 Relationship between RS Projects, SCS Projects and CENTUM Projects

2.17 Connection with Other Systems via Communication Modules

This section describes the connection of ProSafe-RS with other systems including DCS and DNP3 Master by using communication modules.

SCS supports subsystem communication, Modbus slave communication, and DNP3 slave functions.

2.17.1 Subsystem Communication Function

The subsystem communication function is used to read and set input/output data in subsystems from an SCS. SCS supports the Modbus communication protocol.

Mount a serial communication module on the SCS to connect to other systems. By accessing data of other systems via the subsystem communication from the SCS, connection with PLCs, outputs to LED and so forth can be established. Communication data from subsystems is handled by using subsystem communication input/output FBs in the application logic. The subsystem communication function does not affect the safety functions executed in the SCS.

The following two types of serial communication modules can be used:

- RS-232C serial communication module (ALR111)
- RS-422/RS-485 serial communication module (ALR121)

■ Application Capacities

The application capacity regarding subsystem communication is shown as follows:

Table 2.17.1-1 Application Capacities

Item	Maximum number	Remarks
Number of communication modules that can be mounted	4 modules (2 pairs)/SCS	Up to 4 modules can be mounted if all modules are not applied in redundant configuration (*1)
Dual-redundancy	Possible	
Number of communication data items	500 data items/SCS	(*2)
Communication input/output size	1000 words/SCS	(*3) (*4)
Communication size per communication module	1000 words	
Number of ports used per communication module	2 ports	Same protocol for the 2 ports
Number of subsystem stations that can be communicated per port	30 stations	
Number of communication definitions per module	128 definitions	

*1: The number of ALR111/ALR121 modules that can be mounted on a single SCS is determined by the total number of ALR111/ALR121 modules mounted on the same SCS. Be sure that the total number of ALR111 and ALR121 modules does not exceed the value specified in the table. Communication modules for the Modbus slave communication are not included in the count.

*2: This specifies the number of data items that can be wired to subsystem communication input/output FB instances.

*3: The maximum total size of data that can be assigned to discrete inputs/outputs is 256 words (4096 bits).

*4: It is not allowed to wire the subsystem communication I/O FB instances and the allocated areas beyond the limitation on total number of communication data.

**SEE
ALSO**

For more information about requirements of the entire SCS for installing ALR111/ALR121, refer to:

■ [Restrictions on Installation of Hardware](#) on page 2-31

■ Dual-Redundancy of Communication

Communication can be made dual-redundant by using two adjacent serial communication modules (an odd numbered slot and the slot with the same number plus 1). This redundancy method makes the communication module and communication paths to the subsystem dual-redundant. When a communication module or subsystem error occurs (including the communication errors caused by a communication routing error, subsystem interface error and so on), the dual-redundancy scheme automatically chooses the normal module as the controlling module.

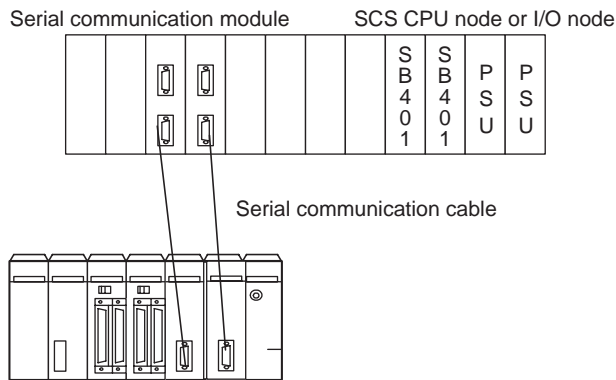


Figure 2.17.1-1 Example of Dual-Redundant Communication

Two dual-redundant serial communication modules are controlled by the basic software in the CPU on the control side in order to determine which is the control side and which is the standby side. A communication module that operates normally and communicates normally with the subsystems is selected to be the control side.

The module on the control side performs read and write communication.

The module on the standby side performs read communication to diagnose the communication path.

The control right is switched from the serial communication module on the control side to the serial communication module on the standby side if either one of the following conditions is met.

- An error has been detected in the communication module on the control side and the communication module on the standby side is normal.
- An error has occurred on the control side and all communication on the standby side (2 ports) is normal.

■ Conditions for Dual-Redundancy

Modules on both sides (paths on both sides) must be able to read and write devices of subsystems. If the subsystem side is dual-redundant and reading and writing are restricted due to control rights of subsystems, communication modules cannot be made dual-redundant.

Only packages performing readback communication can make an output dual-redundant. In Modbus communication, if readback communication is disabled using the Communication I/O Builder, dual-redundancy cannot be applied.

■ Precautions for Dual-Redundant Modules

The control right is determined by checking each module. This means that even if a communication error occurs on the control side, the control right is not switched unless all communication (all communication via both ports if two ports are used by one communication module) on the standby side is normal.

Data update is stopped from the time a communication error occurs and is detected on the control side until the time the control right is switched. For example, when the control right is switched due to no response from serial communication module, a communication error occurs after the following "Elapsed Time" passes.

- Elapsed Time = Response time x (number of retries + 1)

■ Definition of Dual-Redundancy

- Definition of Communication Modules

A communication module should be defined using an odd number slot. If redundancy is specified, the even number slot immediately to the right is automatically defined as a communication module as well.

- **Communication Definition**
The same communication definition is used for both communication modules.

The communication definition should be assigned to the communication module placed in the odd number slot. The same communication definition as the odd number slot is automatically assigned to the communication module in the even number slot as well.

SEE ALSO For more information about the subsystem communication function, refer to:

[B1., "Common items regarding subsystem communication functions" in Open Interfaces \(IM 32Q05B10-31E\)](#)

■ About Impact of Online Change Download

The following table shows the impact of online change download of items related to the subsystem communication that can be changed online on communication modules or subsystems communication input/output FB.

Table 2.17.1-2 Impact of Online Change Download

Items that can be changed online	Impact on communication modules	Impact on logic (communication input/output FBs)
Modification of transmission definition Addition of communication definition Deletion of communication definition Change of communication definition	Communication modules whose definitions are changed are restarted. No impact on other communication modules.	Communication input/output FBs wired to changed communication modules become faulty during restarting of the communication modules. They return to normal after completion of communication module restarting. No impact on other communication input/output FBs.
Addition of subsystem communication input/output FB (*1)	No impact.	Added communication input/output FBs take fixed values during online change. They return to normal operation after completion of online change.
Change of wiring for subsystem communication input/output FB	No impact.	The change is reflected. No impact on other communication input/output FBs.
Deletion of subsystem communication input/output FB Change of input operation at errors	No impact.	No impact on other communication input/output FBs.

*1: Recreating communication input/output FBs after deleting existing communication input/output FB instances is also regarded as addition of communication input/output FB.

SEE ALSO For more information about impact of online change download, refer to:

[B1.7, "Online change" in Open Interfaces \(IM 32Q05B10-31E\)](#)

■ About Readback Communication Operations

If readback communication is enabled, outputs on the subsystem side are read and write communication is not performed unless the readback value is different from the value to be written. If the output value is changed in the CPU, and this causes the readback value to be different from the value to be written, write communication to the subsystem side is performed. If the output value is changed on the subsystem side while normal communication, and this causes the readback value to be different from the value to be written, write communication to the subsystem side is performed.

If readback communication is disabled, write communication is only performed at the timing of communication periods where the previous output value and the current output value are different. This means that even if the output value is changed on the subsystem side, a communication module does not perform write communication again.

Note that the function code of the address specified by Communication I/O Builder determines whether or not to perform readback in the Modbus communication.

Table 2.17.1-3 Readback Communication Operation

Item	With readback	Without readback
CPU initialization start (Output disabled status)	If outputs are disabled, the physical data of the communication input/output data is set to the value read back from the subsystem. The value read back from the subsystem is output until the output enable operation is performed.	If outputs are disabled, the initial value of the physical communication input/output data is set to 0. No output is made until the output value is changed. The value is output when it changes to a non-zero value after the output enable operation. (*1)
Error in locked communication module (at communication module error, online change causing a communication module to reset)	If errors occur in the ALR111/ALR121 modules or in the communication, or online changes are made while communication modules are locked, the physical data of the communication input/output data is set to the value read back from a subsystem. The value on the subsystem side is set to the output value by locking the output when performing maintenance and online change.	In the same way as in the case of initialization start, the output value is set to 0 and the value is output when it changes to a non-zero value. (*1)
Communication error	The status becomes BAD if a communication error occurs.	Even if a communication error occurs, the BAD status may not be notified. When a communication error occurs, no output is made and the output of the CPU and the output of a subsystem become different.
Dual-redundant	Dual-redundancy is supported.	Dual-redundancy is not supported if addresses without readback are used.

*1: This is handled by a function that suppresses writing for 70 seconds after restart if ALR111/ALR121 modules are restarted. This function can be disabled by changing the Option 2 setting.

SEE ALSO

For more information about option settings, refer to:

[B3.1, "Communication specifications" in Open Interfaces \(IM 32Q05B10-31E\)](#)

2.17.2 Overview of Modbus Slave Communication Function

The Modbus slave communication function of SCS is for a Modbus master (external device) reading and setting SCS data via Modbus protocols. DCSs supplied by other manufacturers can function as a Modbus master to be connected with SCS. The Modbus slave communication function of an SCS does not affect the safety functions of it.

For Modbus connection, the following communication modules need to be installed in SCS nodes to be connected to other systems.

- RS-232C serial communication module (ALR111)
- RS-422/RS-485 serial communication module (ALR121)
- Ethernet communication module (ALE111)
When the CPU node of SCS is SSC10D or SSC10S, do not define ALE111.

To set data in SCS from an external device, the External Communication Function Block is used. The External Communication FB allows setting data of a variable of application logic from a Modbus master. In this case, the SCS data must be confirmed by Modbus master by reading back the data.

**SEE
ALSO**

For more information about Modbus connection function, refer to:

[C1., "Common items regarding the Modbus slave communication function" in Open Interfaces \(IM 32Q05B10-31E\)](#)

For more information about engineering of Modbus slave communication, refer to:

[C., "Modbus slave communication" in Open Interfaces \(IM 32Q05B10-31E\)](#)

■ Redundancy of Modbus Communication

To implement redundant Modbus slave communication, you need to create a user application for that purpose on the Modbus master side.

For serial communication, it is possible to duplex the path of Modbus communication in the following ways.

- Using two serial communication modules
The communication modules and communication paths are both duplexed. When one module fails, communication can be continued with the other module.
- Using two ports on one module
When Ports 1 and 2 on the same communication module are used, only the communication paths are duplexed.

For Ethernet communication, it is possible to duplex the path of Modbus communication by using two Ethernet communication modules. The communication modules and communication paths are both duplexed. When one module fails, communication can be continued with the other module.

■ Data Setting and Reading from Modbus Master

The Modbus slave communication function of SCS allows an external device to read the internal variables of SCS (BOOL, DINT, and REAL) and its I/O variables (DI/DO, AI, etc). The External Communication Function Block is used for setting data of these variables. Attention is needed for data handling when accessing to SCS from the Modbus master. In addition, SCS data is 32-bit, however, access from the Modbus master that handles 16-bit data only is available depending on the settings.

**SEE
ALSO**

For more information about data access from the Modbus master that handles 16-bit data only, refer to:

“■ 16-bit Modbus master support mode” in C1.2, “Data access using the Modbus communication functions” in Open Interfaces (IM 32Q05B10-31E)

■ Retry for a Communication Error

The application in Modbus master must be implemented so as to make retry when an error occurs in Modbus communication.

■ Response Timeout Period Setting on the Modbus Master when Communicating with SCSP2

When performing Modbus slave communication with an SCSP2 installed with dual-redundant CPU modules (model: SCP461) and an Ethernet communication module, you must set a five seconds or longer response timeout period on the Modbus master device.

If the control right is switched to the standby-side SCP461 while the control-side SCP461 is processing for Modbus slave communication, the SCSP2 processes the communication data again. As a result, it can take a maximum of five seconds from the time the Modbus master sends a request to the SCSP2 until it receives a response.

2.17.3 DNP3 Slave Function

The DNP3 slave function of the SCS allows the DNP3 master to refer data from the SCS or set data to the SCS through DNP3 communication. The DNP3 slave function of an SCS does not affect the safety functions of it.

To perform DNP3 communication with the DNP3 master, install the Ethernet communication module (model: ALE111) on an SCS node.

To use the DNP3 slave function, use DNP3 communication FBs. By assigning instances of DNP3 communication FBs to DNP3 data, SCS data can be referred or set from the DNP3 master.

The SCS generates and buffers an event that includes a time stamp and data the moment a variable of the application logic changes. This prevents missing data when a communication failure occurs, because the DNP3 master can read the relevant event from the SCS's event buffer following the recovery.

SEE ALSO

For more information about DNP3 slave function, refer to:

[D.](#), “DNP3 slave function” in *Open Interfaces (IM 32Q05B10-31E)*

For more information about engineering of DNP3 slave function, refer to:

[D3.](#), “Engineering and maintenance with SENG” in *Open Interfaces (IM 32Q05B10-31E)*

■ Transmission Specifications of Ethernet Communication Modules

The following table describes the transmission specifications of the Ethernet communication module (model: ALE111) that is needed to use the DNP3 slave function.

Table 2.17.3-1 Transmission Specifications of ALE111

Item	Specification
Interface	Ethernet (IEEE 802.3)
	10 BASE-T
Baud rate	10 Mbps



IMPORTANT

- One ALE111 per SCS can be used for DNP3 communication.
- The ALE111 cannot be installed in any I/O node 5 km or further away from the CPU node.
- For the Ethernet network that is used in DNP3 communication, use a network of line quality equivalent to or better than that of the Vnet/IP-Upstream network, which requires bandwidth of 2 Mbps or more, transmission delay of 500 ms or less.

■ Data referencing and setting from DNP3 master

Use DNP3 communication FBs to reference data from or set data to the SCS from the DNP3 master. The following table shows the relationship between the DNP3 communication FBs and DNP3 data that can be referenced and set from the DNP3 master.

Table 2.17.3-2 Relationship between the DNP3 communication FBs and DNP3 data that can be referenced and set from the DNP3 master

DNP3 communication FB	DNP3 data	Referencing and setting from DNP3 master
DNP3_BI	Binary Input	Referencing
DNP3_BO	Binary Output	Referencing, setting
DNP3_CT_16, DNP3_CT_32	Binary Counter, Frozen Counter	Referencing (*1)
DNP3_AI_16, DNP3_AI_32, DNP3_AI_SF	Analog Input	Referencing
DNP3_AO_16, DNP3_AO_32, DNP3_AO_SF	Analog Output	Referencing, setting

*1: Binary Counter can only be referenced, whereas the Frozen Counter can be referenced and cleared.

■ Data Settings from the DNP3 Master

When setting data from the DNP3 master, use the Operate - With Acknowledgment command unless there is a specific reason.

● Precautions for Using Operate - With Acknowledgment Command

When setting data by using the Operate - With Acknowledgment command, wait for an acknowledgment before issuing the next data setting request. If the next data setting request is issued consecutively without waiting for an acknowledgment, the following status code will be returned:

PROCESSING_LIMITED

If PROCESSING_LIMITED is returned, issue the data setting request again because the target data may not have been set.

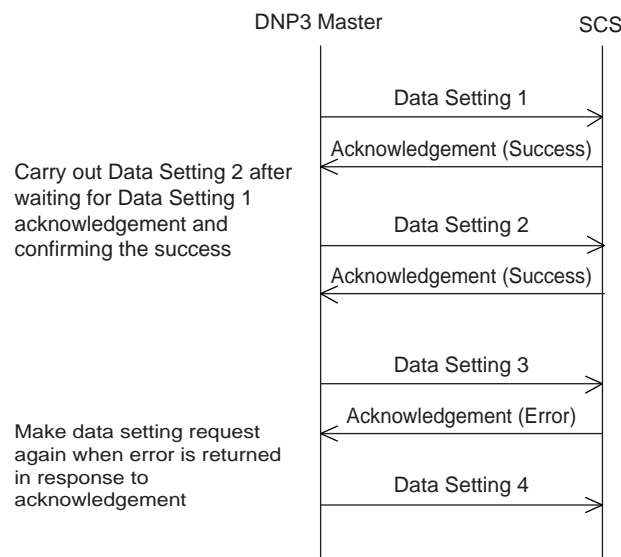


Figure 2.17.3-1 Data Setting Request with Acknowledgment

● Precautions for Using Operate - Without Acknowledgment Command

When setting data by using the Operate - Without Acknowledgment command, read back the event or current value to confirm that the target value has been set, before issuing the next data setting request.



IMPORTANT

It takes time before the set value can be read, so ensure a sufficiently long wait time before the read-back. If the value is not yet set when checked after waiting for sufficiently long time, issue the data setting request again.

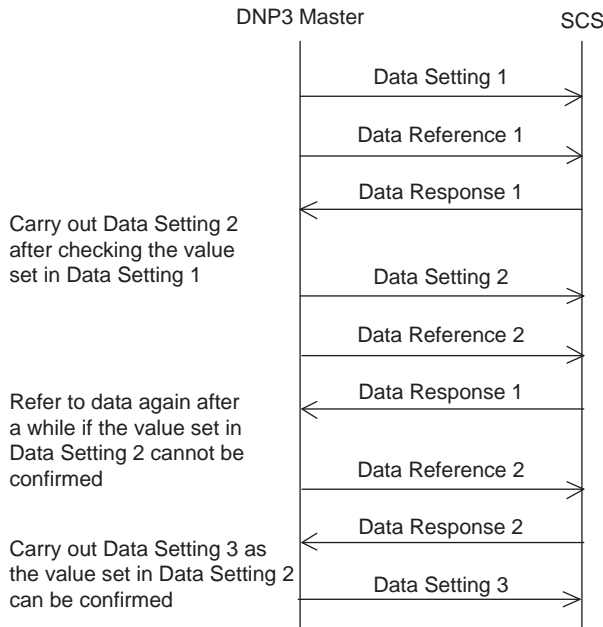


Figure 2.17.3-2 Data Setting Request Without Acknowledgment

SEE ALSO

For more information about time until the set value can be read, refer to:

- [“Maximum Time Before the Set Value Can Be Referenced” on page 2-112](#)

● **Maximum Time Before the Set Value Can Be Referenced**

After setting data, the event or current value can be read back to confirm that the target value has been set. The following time must elapse before the set value can be read.

The maximum time that must elapse before the set value can be referenced is the sum of the maximum time needed for the set data to be set to the variable of the application logic, and the maximum time needed for the value to be referenced using DNP3 communication after the variable of the application logic is set.

- **Maximum time needed for the set data to be set to the variable of the application logic**

$$\text{Scan period of application logic} \times \text{Number of data setting requests from external connection function}$$
- **Maximum time needed for the value to be referenced using DNP3 communication after the variable of the application logic is set**

$$\text{Scan period of the external communication function}$$
- **Maximum Time Before the Set Value Can Be Referenced**

$$\text{Maximum time before the set value can be referenced} = \text{Scan period of application logic} \times \text{Number of data setting requests from external connection function} + \text{Scan period of external connection function}$$

■ Method of Response Upon Event Acquisition

To acquire events from the SCS, set the event response method of the SCS to "Single fragment."

Setting "Multiple fragments" as the event response method of the SCS allows the DNP3 master to acquire events efficiently, but it may disable data setting request and other processes.

TIP

"Data setting" includes setting data using Modbus or other communication.

SEE

ALSO For more information about how to set single fragment, refer to:

“■ Type of response message fragmentation” in D3.3, “DNP3 slave setting” in Open Interfaces (IM 32Q05B10-31E)

■ Precautions When Setting the Time Through DNP3 Communication

Assume multiple SCSs are connected to the Vnet/IP-Upstream network. If the time of the SCSs is set by using DNP3 communication, set the time for just one SCS in each Vnet/IP-Upstream domain. An attempt to set the time of multiple SCSs all at once using DNP3 communication may take up to 10 seconds before the time of all stations connected to the Vnet/IP-Upstream network are synchronized.

SEE

ALSO For more information about time synchronization using DNP3 communication when the SCS is connected to the Vnet/IP-Upstream network, refer to:

“■ Time synchronization using DNP3 communication (The SCS is connected to the Vnet/IP-Upstream network)” in D2.4, “Time synchronization” in Open Interfaces (IM 32Q05B10-31E)

For more information about time synchronization of Vnet/IP, refer to:

A4., “Time synchronization of Vnet/IP” in ProSafe-RS Vnet/IP (IM 32Q56H10-31E)

■ Engineering for DNP3_CT_16/DNP3_CT_32

To use the DNP3_CT_16/DNP3_CT_32 as a counter, create a calculation application using the output value of the DNP3_CT_16/DNP3_CT_32 from the previous scan and input value of an external device, and so on.

Define a variable, connect to the input of the DNP3_CT_16/DNP3_CT_32 the result of calculation by using such as the defined variable and the input value of an external device and then write the output of the DNP3_CT_16/DNP3_CT_32 to the defined variable.

Create an application that clears to 0 the value held by the DNP3_CT_16/DNP3_CT_32 when it counts up from the maximum number of data it can handle.

- DNP3_CT_16
Data range: 0 to 65535 of DINT type
- DNP3_CT_32
Data range: 0 to 2147483647 of DINT type

Use the DNP3 communication function to clear to 0 the value held by the DNP3_CT_16/DNP3_CT_32. In the scan period during which the clear request is received from the DNP3 communication function, clear to 0 the value held by the DNP3_CT_16/DNP3_CT_32 and reset to 0 the defined variable.

The following figure shows an example of engineering for DNP3_CT_16.

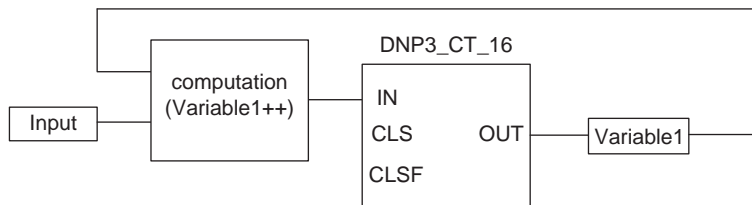


Figure 2.17.3-3 Engineering Example for DNP3_CT_16

■ Precautions When Assigning DNP3 Data

It is recommended for efficient DNP3 communication that when DNP3 data is assigned, the Indexes must be defined consecutively from 0 without missing number.

2.18 Connection with Host System Computer via an OPC Server

ProSafe-RS connects with a supervisory computer via OPC interface. The following two OPC interfaces are available.

- SOE OPC interface package (CHS2200)
Enables OPC-compatible application (client) on the supervisory computer to access diagnostic data and event data (SOE) on SCS.
- Exaopc OPC interface (LHS2411 for HIS, or NTPF100)
Enables OPC-compatible application (client) on the host computer to access various data such as process data and alarm messages on SCS in the same manner as for data on the FCS.

This section primarily describes the SOE OPC Interface Function.

SEE ALSO

For more information about SOE OPC interface, refer to:

[A1., "Overview of SOE OPC Interface" in Open Interfaces \(IM 32Q05B10-31E\)](#)

For more information about the Exaopc OPC interface, refer to:

NTPF100 Exaopc OPC Interface Package (IM 33J02A11-01E)

■ Overview of OPC Interface

The following figure shows the overview of the OPC Interface.

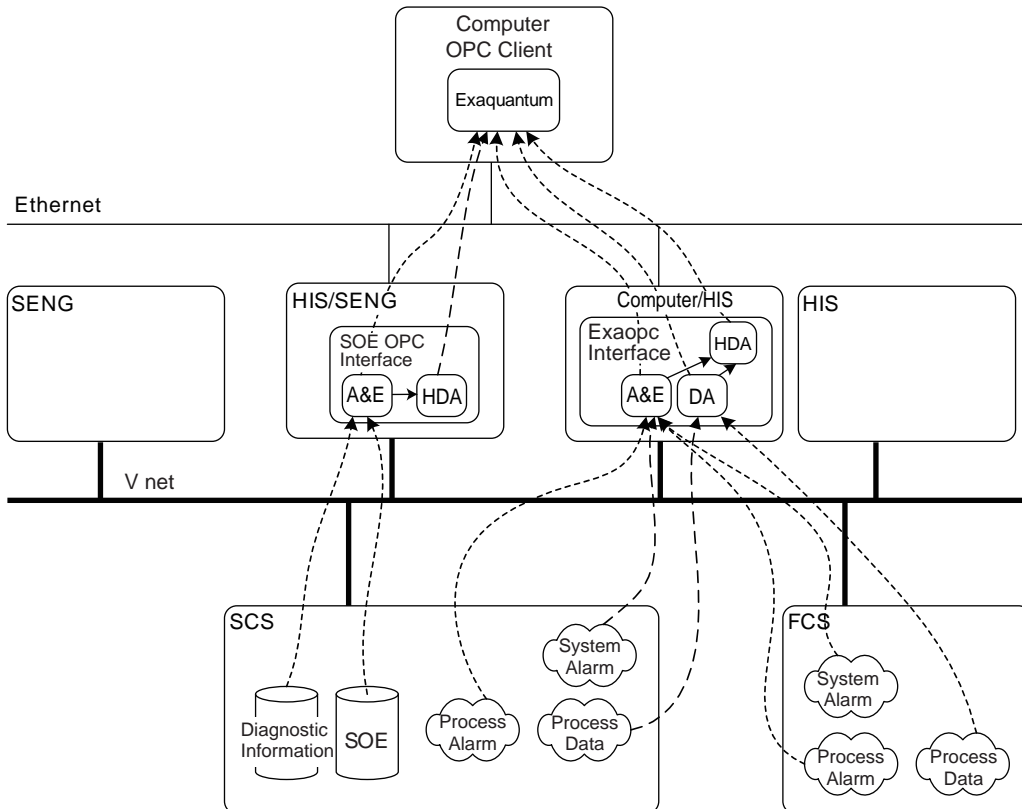


Figure 2.18-1 Overview of OPC Interface

■ SOE OPC Interface (CHS2200)

SOE OPC Interface package for ProSafe-RS notifies the client computer of diagnostic data and event data (SOE) on SCS via OPC A&E interface. The major OPC client is Exaquantum, but general-purpose OPC clients (provided by other manufacturers) can also be connected with SCS.

Together with Exaquantum, HDA interface becomes available.

SOE OPC Interface works on a PC. It also works on HIS. It consists of the OPC server, which sends data to clients, and an SOE-dedicated cassette of ProSafe-RS, with which SCS data is obtained (hereafter referred to as a cassette). The specifications for the OPC server are identical to the one for the A&E server, which is essentially part of Exaopc. The A&E server is a function which creates notifications in the occurrence of an event affecting the OPC client.

■ Exaopc OPC Interface (LHS2411 for HIS, or NTPF100)

Exaopc OPC Interface enables OPC client to access process data, alarms, and messages on SCS.

Exaopc OPC Interface supports the following three interfaces.

- **OPC DA Interface**

Enables OPC client to access SCS process data.

- **OPC HDA Interface**

Enables OPC client to access historical SCS process data kept by Exaopc OPC Interface.

- **OPC A&E Interface**

Enables OPC client to access SCS alarms and messages such as process alarms and system alarms.

■ Precautions

This section provides the precautions for engineering the SOE OPC Interface.

- **Coexistence of SOE-dedicated OPC Server with Exaopc OPC Interface Package**

Minimize the chance of coexistence of the SOE-dedicated OPC Server of ProSafe-RS with the HIS "Exaopc OPC Interface Package (for HIS)." Otherwise, this can cause lower performance of the SOE-dedicated OPC Server depending on the frequency of using the Exaopc OPC Interface Package. This problem can be avoided by distributing the load on several HISs.

- **CPU Load Distribution**

To reduce the communication load and CPU load caused by sending a large amount of data to the client, the cassette has a function of distributing the CPU load by restricting the communication traffic to the client. The cassette computes the maximum number of events that can be sent simultaneously (1-1000) from the delay time per one transmit event (user defined value, the default is 40 ms) with the following expression and alternates transmission and delay.

- Maximum number of transmitted events = Maximum delay time (fixed at 2000 ms) /Event transmission delay time (ms)
- Delay time =Event transmission delay time (ms) x Number of transmit events (n)

The default is the repetition of 50 (2000/40) event transmissions and two second delays (40 x 50).

This case requires 40 seconds for transmitting 1000 events.

The default setting can be changed according to the performance of PC.

- Longer "event transmission delay time" causes delayed event transmission and lower CPU load.
- Shorter "event transmission delay time" causes faster event transmission and higher CPU load.

**SEE
ALSO**

For more information about the SOE OPC interface , refer to:

[A1., "Overview of SOE OPC Interface" in Open Interfaces \(IM 32Q05B10-31E\)](#)

2.19 Version Control

This section describes the Version Control Function.

The Version Control Function is intended for controlling the version history of SCS projects to support users' system update.

The Version Control Function is used for saving (check-in) the data of an SCS project at some point by assigning a version number and for restoring (check-out) project data of a certain version.

The Version Control Function performs the following functions.

- Check-in of project data
- Check-out of project data
- Deletion of Versions
- Deletion of check-in projects
- Reading of version information
- Printing of version information
- Designation of check-in folders
- Designation of SCS projects to be version controlled

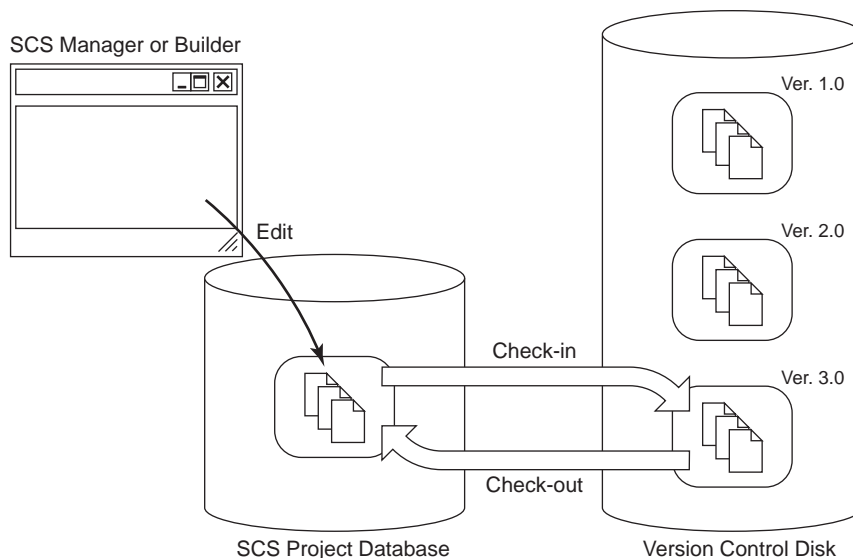


Figure 2.19-1 Functions of Version Control Tool

■ Using Version Control Tool

Version Control tool assigns a version number to an SCS project downloaded to SCS and stores the data with the version number in a separate disk. Using the Version Control tool for saving SCS projects after changing and downloading them, you can manage revision history. You also can use SCS Projects stored by the Version Control tool as backups.

● Assigning Version Numbers

Implement appropriate version number management. For example, you can apply different rules of numbering versions between major changes and minor changes. Examples of assigning version numbers are as follows:

Example

Rev1.0 First engineering

Rev1.1 Version after a minor change

Rev1.2 Version after a minor change

Rev2.0 Saved version under engineering for a major change

■ Related Functions and Files

The Version Control Tool runs independently of the other engineering functions (SCS Manager, Multi-Language Editor, builder, etc.). However, projects opened in the SCS Manager cannot be handled with Check-in/out.

The following files are related to the Version Control Tool.

- Version information file to hold version history
- Project attribute file to record version numbers of each project
- Project database files to be recorded
- Project database files that have been recorded

■ Unit of Version Control (Object Files of Check-in)

The Version Control Function can handle individual SCS projects for check-in. A whole RS project can not be saved for check-in.

**SEE
ALSO**

For more information about the operation of the Version Control, refer to:

[13., "Version Control" in Engineering Reference \(IM 32Q04B10-31E\)](#)

2.20 Import/Export Function

The application data of a project can be exported to an external file, and the application data in an exported file can also be imported to a project. This function can be used when diverting or regenerating SCS projects during SCS expansion or reformation.

2.20.1 Precautions Concerning Import/Export

This section summarizes the precautions to take when you perform an import or export. You must observe these precautions when carrying out the actual operation.

■ Precautions on Handling CSV Files

Do not use an editor to directly edit CSV files that have been exported from SCS project data. Operation cannot be guaranteed if you have imported an edited CSV file in SCS project data.

■ Notice on Sequence of Importing

When importing individual global variables or individual POUs, the sequence of importing is as follows:

1. POU (Function Block)
 2. POU (Other than Function Block)
 3. Global Variables
- If you import global variables before importing the POU (Function Block), the Type information regarding the imported global FB instance may be missing. As a result, "???" will be shown in the Type column of Dictionary.
 - If you import POU (other than Function Block) before importing the POU (Function Block), the Type information regarding the imported local FB instance may be missing. As a result, "???" will be shown in the Type column of Dictionary.
 - If a user-defined function block (such as FB1) is using another user-defined function block (FB2) as a local parameter and FB1 is imported before FB2, the Type information regarding the imported local parameter type may be missing. As a result, "???" will be shown in the Type column of the parameter in Dictionary. The function blocks used as parameters should be imported before.

If the above sequence is not observed when importing the individual global variables or POUs, a build error will occur. In this case, import again in the above-mentioned order.

■ Use Cross Reference Analyzer to Check the Imported POU

If the POU to be imported has an identical name with an existing POU, the Cross Reference Analyzer will act as follows:

If the POU to be imported is exactly the same as the existing POU, the Cross Reference Analyzer will mark the POU as "Unchanged POU" and display it in green icon. If the POU to be imported is discrepant from the existing POU, the Cross Reference Analyzer will mark the POU as "Changed POU" and display it in red (Modified) icon.

■ Notice on Compatibility (Including Importing Builder)

- When importing the files created in the previous software release number of SENG, the setting values for the new items supported only in the newer software release number of SENG will be the default values.
- The files exported from the project created on newer software release number SENG cannot be imported to the project opened on the older software release number SENG.
- When the software of SENG is upgraded to R1.03, SCS project created on the SCS Manager of the older software release number can be imported and exported.

■ Notice on Password

When importing a project to replace an old project, the passwords of project and POUs are also imported and the old passwords will be replaced.

Therefore, when using export and import, you should manage the project password and the passwords of POUs for exported project.

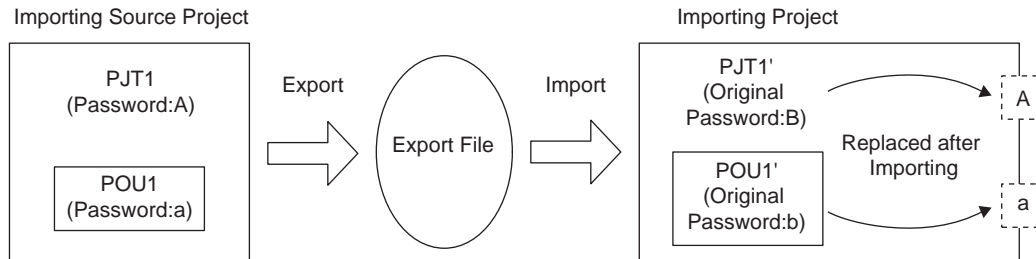


Figure 2.20.1-1 Passwords Replaced after Importing

The effects regarding passwords after importing are shown as follows:

- When importing the exported project files with passwords, the passwords of exported project and POUs are also imported and the existing passwords will be replaced. After importing, the passwords of the imported project will be required to open the project, without the passwords, the imported project cannot be opened for editing.
- When importing those POUs that are protected by passwords, the passwords of the existing POUs will be replaced by the passwords of the imported POUs. So, after importing, the passwords of the imported POUs will be required to open the POUs, without the passwords, the imported POUs cannot be opened for editing.

■ Unit for Exporting and Sequence of Importing

This section describes the file formats that are used when exporting SCS project data and actions that are carried out while importing. SCS projects can be exported as binary (PXF format) files. SCS project properties and SCS constant data can be exported in CSV files.

SEE ALSO

For more information about units and formats used for export, refer to:

“■ SCS Project Application Data Exportable By SCS Manager” in 14., “Import/Export” in Engineering Reference (IM 32Q04B10-31E)

● Import/Export in PXF Format

Even if you have exported data for individual SCS projects in binary (PXF format) files, you can import data selectively (you can import the POUs you need) from the exported data.

The actions during importing are shown in the following table.

Table 2.20.1-1 Actions during Importing

Imported Contents	Actions during Importing
Project	Deletes the existing project first and then adds the imported project in PXF files. Importing projects is only possible when the project name, configuration name and resource name of the source project match with those of the existing project.(*1)

Continues on the next page

Table 2.20.1-1 Actions during Importing (Table continued)

Imported Contents	Actions during Importing
POU	<ul style="list-style-type: none"> • Deletes the existing POU with the identical name when adding the POUs from PXF files. • POU name can be changed during importing. • When you import multiple POUs at one time, you can choose whether to import them without changing their name (by deleting any existing POUs and adding them with the same name) or by automatically renaming any POUs with the same name to non-duplicate names. • When importing a local instance where the FB is not defined in the existing project, the variables with unknown types will be generated and build error will occur. To solve this problem, you can either define a new FB before importing or import the FB.
Resource Properties	Overwrites all the existing properties of the resource.
I/O Device Instances	<ul style="list-style-type: none"> • If the imported I/O device has different index number with the existing I/O modules, the imported I/O device will be added as a new I/O module. • If the imported I/O device has an identical index number with the same type of existing I/O module, the IOM parameters (node address, slot numbers and redundancy setting) of the imported I/O device will be added to replace the existing I/O module. • If the imported I/O device has an identical index number with a different type of existing I/O module, a warning message will be displayed and the I/O device will not be imported. The existing I/O module will not be changed.
Global Variables	<ul style="list-style-type: none"> • If the imported variable is different from the existing variable, the imported variable will be added as a new variable. • If the name and scope of the imported variable are identical with the existing variable, the imported variable will be added to replace the existing variable. • If the existing variable is wired with other variable in the same channel, the imported variable will replace the existing variable and be wired with the other variable. • When importing an instance where the FB is not defined in the existing project, the variable with an unknown type will be generated and a build error will occur. To solve this problem, you can either define a new FB before importing or import the FB.
Wired Variables (I/O variables)	<ul style="list-style-type: none"> • If the imported variable is different from the existing variable, the imported variable will be added as a new variable. • If the name and scope of the imported variable are identical with the existing variable, the imported variable will be added to replace the existing variable. • If the existing variable is wired with other variable in the same channel, the imported variable will replace the existing variable and be wired with the other variable. • When importing an instance where the FB is not defined in the existing project, the variable with an unknown type will be generated and a build error will occur. To solve this problem, you can either define a new FB before importing or import the FB.
Binding	<ul style="list-style-type: none"> • If the imported binding group has a different group ID from the existing binding group (either Consumer Group or Producer Group), the imported group will be added as a new group. • If the imported binding group has an identical group ID to an existing binding group (either Consumer Group or Producer Group), the imported group will be added to replace the existing group. • If the imported binding variable has different name from the existing binding variable, the imported binding variable will be added in a binding group.
Defined words	<ul style="list-style-type: none"> • If the imported defined words have a different name from the existing defined words, the imported defined words will be added as a new defined words. • If the imported defined words have an identical name with the existing defined words, the imported defined words will be added to replace the existing defined words.

*1: When importing the entire projects, an error dialog box appears if any one of the project name, configuration name and resource name of the importing source project does not match with that of the existing project. For instance, if the entire SCS project of SCS0101 is exported, it is not allowed to import the entire project as SCS0102. If you wish to export the entire project and import it to an SCS project with a different name, create a new project with the same name as the importing source project, perform import operation, and then change the project name, configuration name and resource name to the desired names before using the project.

● **Import/Export of SCS Project Properties**

You can export SCS Project Properties as a CSV file, but this does not mean that all of the data will be applied when you import it. Actions during import are shown in the following table:

Table 2.20.1-2 Actions when Importing SCS Project Properties

Items	Actions during Import
Station Type	Reflected only when importing during new project creation
Database Type	Not reflected
Station Address	Reflected
Domain Number	Reflected
Station Number	Reflected
IP Address	Not reflected
Component Number	Reflected
Version	Not reflected
CENTUM Project Folder	Reflected
SCS Project Attribute	Not reflected
Originally Created	Not reflected

● **Import/Export of SCS Constants**

SCS constants can be exported in a CSV file. However, when you import the constants, the default value may be used if the setting does not exist, depending on the software release number of your system and the SCS type. If the settable values are different, they will need to be changed. If you do not change them, an error will occur at build time.

■ **How to Check When Project Data is Migrated by Export or Import**

How to check differences in the imported data after migration of project data by import/export is as follows:

Table 2.20.1-3 Builder Definitions and How to Verify

Builder	Data	How to Verify
SCS Manager	POU	Cross Reference Analyzer
	I/O Wiring	Cross Reference Analyzer
	Binding	Cross Reference Analyzer
SCS Project Properties	Domain/Station number	Project Comparing Tool
	CENTUM Project Folder	Project Comparing Tool
Configuration Properties	Target	Project Comparing Tool
	Memory size for temporary variables	Project Comparing Tool
Connections	IP Address	Project Comparing Tool
Resource Properties	Resource Number	Project Comparing Tool
	Cycle Timing	Project Comparing Tool
	Memory size for online changes-Code	(Fixed value) (*1)
	Memory size for online changes-User variable size	Project Comparing Tool

Continues on the next page

Table 2.20.1-3 Builder Definitions and How to Verify (Table continued)

Builder	Data	How to Verify
SCS Constants Builder	Interval of Repeated Warning Alarms	Project Comparing Tool
	Synchronous Mode	Project Comparing Tool
	Scan Period for External System	Project Comparing Tool
	Modbus Word Order	Project Comparing Tool
	Alarm Notify Action when AOF Released	Project Comparing Tool
	PV Status of S_ANLG_S	Project Comparing Tool
	Optical ESB Bus Repeater/Maximum Extension Distance (*1) SCS Constants Builder	Project Comparing Tool
	Extend Scan Period Automatically (*1)	Project Comparing Tool
	Behavior at Abnormal Calculation (*1)	Project Comparing Tool
	Automatic IOM Download (*1)	Project Comparing Tool
	Locking of Internal Variables (*1)	Project Comparing Tool
	16-bit Modbus master support mode (*2)	Project Comparing Tool
	DNP3 Slave Function (*3)	Project Comparing Tool
I/O Parameter Builder	Node parameter (Extends Node Bus/Extends To (Km) in optical ESB bus repeater) (*1)	Project Comparing Tool
	Module parameter	Cross Reference Analyzer
	Channel parameter	Cross Reference Analyzer
Communication I/O Builder	Communication I/O definition	Cross Reference Analyzer
	Communication I/O wiring	Cross Reference Analyzer
SCS Link Transmission Builder	SCS Link transmission data definition	Cross Reference Analyzer
	Wiring definition	Cross Reference Analyzer
Modbus Address Builder	-	Project Comparing Tool
DNP3 Communication Builder (*3)	-	Project Comparing Tool
Tag Name Builder	-	Project Comparing Tool
Alarm Priority Builder	-	Project Comparing Tool
Alarm Processing Table Builder	-	Project Comparing Tool

*1: The corresponding item may not exist or the configurable value may be different depending on the software release number of the system or SCS type. Such items may therefore be picked up as discrepancies by the Project Comparing Tool.

*2: It can be used in SCS database created by SENG R3.02.10 or later.

*3: It can be used in SCSU1 database created by SENG R3.02.20 or later.

2.20.2 Data Transfer Procedure During Expansions/ Remodeling in Modifications where Online Change is Possible

This section describes the procedure for applying the results of making a modification that can be changed online from a user-defined project to the current project. This procedure involves exporting the results from the user-defined project and only importing the data that has been modified into the current project.



IMPORTANT

- Do not forget to import all the modified content.
- Confirm that the current project has not been changed manually before importing.
- Modifications with a newly added POU cannot be made through online change downloads. Carry out the expansions/remodeling by offline download.

The overall flow of the procedure is as follows:

1. If a POU included in a library has been modified, first update the original library project with the modifications required, and then copy the modifications to the library of the current project.
2. If an SCS project has been modified, apply the modifications from the user-defined project to the current project.
3. Perform an online change download of the SCS project.

■ Library POU Data Transfer in Modifications where Online Change is Possible

If you are using library POUs, use the Import/Export function to apply the modifications from the library in the user-defined project to the original library.

- By way of preparation, back up the original library using the Version Control Tool.

● Exporting Library POU Source Data where Online Change is Possible

First export the library POU source data.

1. In the user-defined project, export the library so as to create the following PXF files.
 - A PXF file containing the whole library project.
 - If you are reflecting the addition or modification of global variables used in a library project, a PXF file containing the global variables
 - If you are reflecting the addition or modification of defined-words used in a library project, a PXF file containing the defined words

● Importing Library POU Data where Online Change is Possible

1. Use the SCS Manager to open the original library, and then import the required content from the exported PXF files.
 - 1-1. In the Import dialog, specify the PXF file containing the entire exported library project and import only the modified POUs. (*1)

*1: In the course of importing, if the POU contains any FB that does not exist in the current project, the following warning message will be displayed. In such a case, a build error will occur when building the project.
Warning: Type 'UFB' for symbol 'iUFB' was not found in this project.
or

Warning: Type 'UFB1' for Parameter 'iUFB1' was not found in this project.
 'UFB', 'UFB1': FB Name
 'iUFB', 'iUFB1': FB Instance Name

- 1-2. To import the global variables, in the import dialog box, specify the PXF file containing the global variables, and import.
- 1-3. To import defined words, in the import dialog box, specify the PXF file containing the defined words, and import.
2. Delete any global variables and defined words that are not required after importing. The variables that are not used in POU can be checked in the Browser. Start the Browser and generate (or refresh) the cross-reference information for checking the unused variables.
3. Perform build.
4. Validate the contents on the Integrity Analyzer.
5. Copy the original library to the LIBRARIES folder of the current project.

■ SCS Project Data Transfer in Modifications where Online Change is Possible

Apply the modifications from the modified user-defined project to the current project using the Import/Export function.

- By way of preparation, back up the current project using the Version Control Tool.

● Exporting SCS Project Source Data Where Online Change is Possible

First export the SCS project data from the import source project.

1. Export the source project to the following PXF files.
 - PXF file containing the entire project
 - If you are reflecting the addition or modification of global variables, a PXF file containing the global variables
 - If you are reflecting the addition or modification of defined words, a PXF file containing the defined words
2. If you have modified "Component Number" or "CENTUM Project Folder" in the SCS Project Properties, export the SCS Project Properties to a CSV file. Items other than "Component Number" and "CENTUM Project Folder" cannot be modified via an online change in SCS Project Properties.

● Importing SCS Project Data where Online Change is Possible

1. Use the SCS Manager to open the original current project, and then import the required data using the exported PXF files.
 - 1-1. In the Import dialog, specify the PXF file containing the entire exported project and import only the modified POUs. (*1)
 - 1-2. To import the global variables, in the import dialog box, specify the PXF file containing the global variables, and import.
 - 1-3. To import the defined-words, in the import dialog box, specify the PXF file containing the defined-words, and import.

*1: In the course of importing, if the POU contains any FB that does not exist in the current project, the following warning message will be displayed. In such a case, a build error will occur when building the project.

Warning: Type 'UFB' for symbol 'iUFB' was not found in this project.
 or
 Warning: Type 'UFB1' for Parameter 'iUFB1' was not found in this project.
 'UFB', 'UFB1': FB Name
 'iUFB', 'iUFB1': FB Instance Name

2. After importing, the unnecessary global variables and defined words should be deleted. The variables that are not used in POU can be checked on the Browser. Start the Browser and generate (or refresh) the cross-reference information to check the unused variables.
3. If you have modified "Extends Scan Period Automatically", "Behavior at Abnormal Calculation", or "Automatic IOM Download", correct each of them in the builder. There are no other items in SCS Constants Builder that can be modified via an online change.
4. Regarding the following builders, import the builder files if required.

Table 2.20.2-1 Builder Files for Import (Modifications where Online Change is Possible)

Builder	Builder File Location (*1)
I/O Parameter Builder	SCS Project\YOKOGAWA_SCS\SAFETY\IOM\IOMDEFSB.edf
Communication I/O Builder	SCS Project\YOKOGAWA_SCS\SAFETY\CONFIGURATION\CommIO.edf
Link Transmission Builder	SCS Project\YOKOGAWA_SCS\SAFETY\CONFIGURATION\LinkTrans.edf
Modbus Address Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION\Modbus-Def.edf
DNP3 Communication Builder (*2)	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION\DNP3Def.edf
Tag Name Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\TAG\TAG.edf

*1: (relative path under SCS project top directory)

*2: Because the event buffer size cannot be modified by an online change, import the event buffer size and then restore and save the original value.

Alarm Priority Builder and Alarm Processing Table Builder cannot be modified via an online change. Do not import them.

5. If "Component Number" or "CENTUM Project Folder" have been changed in the SCS Project Properties, import the CSV file that you exported to in advance.

● **Online Change Downloads During SCS Project Expansions/Remodeling**

When you have applied the library POU data and SCS project data to the current project, run the online change download.

1. Perform build.
2. Use the Project Comparing Tool to check that the original project after import is the same as the source user-defined project.
 - a. Launch the Project Comparing Tool to compare the original project after import and the source user-defined project and check that there are no discrepancies. When you do so, check that the project paths which you are comparing are correct in the project path display area of Project Comparing Tool or in the printed summary report of the discrepancies.
 - b. If a discrepancy is found, check that it is appropriate.
3. On Integrity Analyzer, validate the contents.
4. On Cross Reference Analyzer, validate the modified contents. Modifications must also be tested after download.
5. Perform online change downloading.

SEE ALSO

For more information about the procedure for online change download, refer to:

5., "Online Change of Applications" on page 5-1

2.20.3 Data Transfer Procedure During Expansions/ Remodeling in Modifications Requiring Offline Download

This section describes the procedure for making a modification that requires offline download and importing the results of testing in the import source project into the current project on a project-by-project basis. Offline download is necessary because the entire project is being imported.

The overall flow of the procedure is as follows:

1. If a POU included in a library has been modified, first apply the modifications to the library project to the original library project, and then copy the modifications to the library of the current project.
2. If the import source project has been modified, apply the modifications to the current project.
3. Download the SCS project offline.

■ Library POU Data Transfer in Modifications Requiring Offline Download

Apply the modifications from the library in the import source project to the original library and copy it to the LIBRARIES folder of the current project.

- By way of preparation, back up the original library using the Version Control Tool.
1. Open the library of the importing source project side on the SCS Manager, and change the target name to SCS_TARGET and then save the change.
 2. Export the entire project containing the library to PXF files.
 3. Use the SCS Manager to open the original library, specify the PXF files thus created in the Import dialog, and then import the whole project containing the library.
 4. Execute the build of the original library.
 5. Check the integrity of the original library using the Integrity Analyzer.
 6. Copy the original library to the LIBRARIES folder of the current project.

■ SCS Project Data Transfer in Modifications Requiring Offline Download

Reflect the modifications on the current project from the modified importing source project.

- By way of preparation, back up the current project using the Version Control Tool.
- **Exporting SCS Project Source Data Requiring Offline Download**
 1. Open the importing source project on the SCS Manager, and change the target name to SCS_TARGET and then save the change.
 2. Export the entire source project to PXF files.
 3. If you have modified "Component Number" or "CENTUM Project Folder" in the SCS Project Properties of the import source project, export the SCS Project Properties to a CSV file.
 4. If you have modified SCS Constants Builder in the import source project, export it to a CSV file.

● **Importing Source SCS Project Data that Requires Offline Download**

1. In SCS Manager, open the current project, import the whole project specifying the PXF file exported from the source project.
2. Redefine the library path to the current project.
3. Import the CSV file if there is an exported CSV file of the SCS Constants Builder.
4. Import the builder files if required.

Table 2.20.3-1 Builder Files for Import

Builder	Builder File Location (*1)
I/O Parameter Builder	SCS Project\YOKOGAWA_SCS\SAFETY\IOM\IOMDEFSB.edf
Communication I/O Builder	SCS Project\YOKOGAWA_SCS\SAFETY\CONFIGURATION\CommIO.edf
Link Transmission Builder	SCS Project\YOKOGAWA_SCS\SAFETY\CONFIGURATION\LinkTrans.edf
Modbus Address Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION\Modbus-Def.edf
DNP3 Communication Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION\DNP3Def.edf
Tag Name Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\TAG\TAG.edf
Alarm Priority Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION\Alm-Pri.edf
Alarm Processing Table Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION\AlmTbl.edf

*1: (relative path under SCS project top directory).

5. Import the CSV file if there is an exported CSV file of the SCS Project Properties of source SCS project.

● **Offline Download During Expansions/Remodeling**

Execute offline download in an SCS project that you have finished importing.

1. Perform build.
2. Use the Project Comparing Tool to check that the original project after import is the same as the user-defined source project.
 - 2-1. Launch the Project Comparing Tool to compare the original project after import and the user-defined source project, then check that there are no discrepancies. When you do so, check the path in the project path display area of Project Comparing Tool or in printed summary report of the discrepancies that you are comparing are correct.
 - 2-2. If a discrepancy is found, check that it is appropriate.
3. Validate the contents on the Integrity Analyzer.
4. Validate the modified contents on the Cross Reference Analyzer. Modifications must also be tested after download.
5. Perform offline download.

TIP

- Possibilities of online change download
Whether or not it is possible to perform online change download when the current project has been modified by import is the same as when the same modifications are made manually on the current project. Therefore, in some cases, online change download is possible even when the entire project has been imported. Whether or not it is possible to perform online change download is found when you run a build or try to run online change download after importing.

2.20.4 Data Transfer Procedure During SCS Project Regeneration

In order to apply the new features on the newer SENG software release number to the existing SCS project or to reuse the existing project, the existing project needs to be ported (or regenerated).

When porting (or regenerating) a project, the original project needs to be entirely exported into PXF format binary files. Then import the PXF files into a new project.

The overall flow of the procedure is as follows:

1. If the library needs to be regenerated, regenerate the library first.
2. Regenerate the SCS project.
3. Check that the regenerated project is equivalent to the original project.

■ Regenerating Library Data when Regenerating an SCS Project

Implement the following procedure if you need to regenerate a library as part of regenerating an SCS project.

1. Back up the original library on the Version Control Tool if necessary.
2. Open the source library in SCS Manager and export the whole project containing the library to PXF files.
3. In Windows Explorer, delete the original library, or move it to a different place.
4. Create a new library using the same name as the original library on the SCS Manager, and change the resource name and configuration name to the same names as the original library.
5. In the SCS Manager, import the whole project containing the source library. In the Import dialog, specify the PXF files to which the project has been exported.
6. Build the library.
7. Check the integrity of the library using the Integrity Analyzer.

■ Regenerating the SCS Project

The process flow for regenerating SCS projects is as follows:

1. Export all of the data in the source SCS project.
2. Create a new target SCS project to import the data to and prepare the necessary libraries.
3. Import all of the exported data to the target SCS project.

● Exporting SCS Project Data when Regenerating an SCS Project

1. Back up the original project on the Version Control Tool if necessary.
2. Open the original project on the SCS Manager, and export the whole project and create the PXF files.
3. Export the SCS Project Properties from the source project to create a CSV file.
4. Export the SCS Constants Builder data from the source project to create a CSV file.
5. In Windows Explorer, delete the original project, or move it to a different place.

● **Generating an SCS Project and Importing SCS Project Data**

1. Create a new SCS project using the same name as the original project on the SCS Manager, and change the resource name and configuration name to the same names as the original project.
2. Copy any libraries used in the original project to the LIBRARIES folder of the newly created SCS project. Also copy any libraries that you have regenerated.
3. In SCS Manager, open the newly created SCS project, specify the PXF file to which the whole original project was exported, and import the whole project.
4. Open the SCS Constants Builder and import the exported CSV file in the original project.
5. Import the builder files.

Table 2.20.4-1 Builder Files to be Imported (Project Regeneration)

Builder	Builder File Location (*1)
I/O Parameter Builder	SCS Project\YOKOGAWA_SCS\SAFETY\IOM\IOMDEFSB.edf
Communication I/O Builder	SCS Project\YOKOGAWA_SCS\SAFETY\CONFIGURATION\CommIO.edf
Link Transmission Builder	SCS Project\YOKOGAWA_SCS\SAFETY\CONFIGURATION\LinkTrans.edf
Modbus Address Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION\Modbus-Def.edf
DNP3 Communication Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION\DNP3Def.edf
Tag Name Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\TAG\TAG.edf
Alarm Priority Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION\AlmPri.edf
Alarm Processing Table Builder	SCS Project\YOKOGAWA_SCS\INTEGRATION\CONFIGURATION\AlmTbl.edf

*1: (relative path under the SCS project top directory)

6. Open SCS Project Properties and import the exported CSV file in the original project.

**IMPORTANT**

- If you export the entire SCSP1/SCSV1 project and import it to a newly created project of SCSP2, the values of the original project are applied to the following definitions related to application capacity. Change the values to the fixed values or default values of SCSP2 after importing.

Table 2.20.4-2 Definition Items Related to Application Capacity

Definition item	Value of SCSP1/SCSV1	Value of SCSP2	Remarks
Online change code size (*1)	1700000 (fixed value)	2550000 (fixed value)	A build error will occur if the value is not changed after importing.
Online change user variable size (*2)	32768 (default) 8192 to 65536 (allowable specification range)	131072 (default) 8192 to 262144 (allowable specification range)	A value different from the default SCSP2 value is set after importing.
Constant/temporary variable size (*3)	32768 (default) 8192 to 65536 (allowable specification range)	131072 (default) 8192 to 262144 (allowable specification range)	A value different from the default SCSP2 value is set after importing.

*1: [Code size] in the Advance settings dialog box of the Settings tab in Resource Properties of the SCS Manager

*2: [User variable size] in the Advanced settings dialog box of the Settings tab in the Resource Properties of the SCS Manager

*3: [Memory size for temporary variables] in the Target tab of Resource Properties in the SCS Manager or [Memory size for temporary variables] in the Hardware tab of Configuration Properties in the SCS Manager

- In an SCSP2 project using Optical ESB Bus Repeater modules, if you import the project data from an SCSP1/SCSV1 project, you must configure the node settings in the I/O Parameter builder for all nodes connected to the CPU node via the Optical ESB Bus Repeater modules. If [Extends Node Bus] is set to [No], change it to [Yes] and specify the actual node distance on the ESB bus from the CPU node in [Extends To (Km)].
- If you import SCSP2 applications to an SCSP1/SCSV1 project, do not import the entire project. Import individual POUs or other units as required.

SEE ALSO

For more information about cautionary notes using Optical ESB Bus Repeater modules, refer to:

■ [Devices Related to Optical ESB Bus Repeater](#) on page 2-24

■ Confirming a Regenerated Project

Check that the regenerated project is equivalent to the original project using the following procedure.

1. Open the regenerated SCS project on the SCS Manager and perform build.
2. Check the validity using the Integrity Analyzer.
3. Using the Cross Reference Analyzer's function for comparison with the original project, check that all POUs are equivalent to those of the original project. Open the regenerated SCS project on the SCS Manager and compare it with the original SCS project using the Cross Reference Analyzer. Confirm that all POUs are displayed in green (retesting or review is not required). At this point, check whether the path in the title bar of Cross Reference Analyzer or in the report is correct.
4. For data that cannot be checked with Cross Reference Analyzer, use the Project Comparing Tool to ensure that the regenerated SCS project is equivalent to the original SCS project. Launch the Project Comparing Tool and compare the regenerated SCS project with the original SCS project, so that there is no difference in all items. When you do so, check

that the project paths which you are comparing are correct in the project path display area of Project Comparing Tool or in the printed summary report of the discrepancies.

- If no difference is detected with the Cross Reference Analyzer or the Project Comparing Tool, re-test of SCS application is not required.
- If the following differences are detected with the Project Comparing Tool, check the details and modify as needed.
 - If you import an SCS project that is created using a SENG with an older software release number, definitions that do not exist in the original project are set to the default values in the regenerated project. These items are picked up as discrepancies by the Project Comparing Tool. When you change the default value, the items must be tested.
 - If you import an SCS project that is created for a different model, definitions that do not exist on the model used for the original project are set to the default values in the regenerated project. Moreover, definitions with different configurable values will produce an error at build in the regenerated project.

5. Perform an offline download to the SCS and make sure that the SCS starts.

TIP

If you have modified a regenerated project after verifying that the regenerated project is equivalent to the original project by using the Cross Reference Analyzer and Project Comparing Tool, ascertain the range for re-testing in the usual manner by using the Cross Reference Analyzer, Project Comparing Tool, or the self-document printout, and conduct the tests.

**SEE
ALSO**

For more information about how to check Project Data Migrated by Export or Import, refer to:

“■ [How to Check When Project Data is Migrated by Export or Import](#)” on page 2-124

2.21 System Reaction Time

This section describes Reaction Time and PFD Calculation.

■ System Reaction Time

The system reaction time of SCS consists of the reaction time for the external demand (Demand reaction time) and the reaction time when a fault is detected in the SCS (Fault reaction time).

- Tr: system reaction time
- Tscan: scan period for application logic execution

● Demand Reaction Time

The demand reaction time differs as follows, depending on whether the loop includes safety communication.

- When Not Using the Inter-SCS Safety Communication

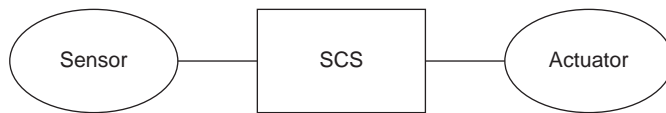


Figure 2.21-1 Reaction Time 1

$$Tr = Tscan \times 2 + \text{Input processing time} + \text{Output processing time-Idle time}$$

$$\text{Idle time} = Tscan - \text{Application logic execution time}$$

- When Using the Inter-SCS Safety Communication
When the inter-SCS safety communication is used, the calculation formula varies depending on whether the scan period of the SCS on the producing side or the scan period of the SCS on the consuming side is larger.
 - If Tscan on the producing side > Tscan on the consuming side:
 $Tr = Tscan \text{ on the producing side} \times 2 + Tscan \text{ on the consuming side} \times 2 + \text{transmission delay}$
 - If Tscan on the producing side \leq Tscan on the consuming side:
 $Tr = Tscan \text{ on the producing side} \times 2 + Tscan \text{ on the consuming side} \times 3 + \text{transmission delay}$

Transmission delay (V net)

- No BCV/CGW used: 10 ms
- BCV/CGW used: number of BCV used x 50 ms + number of pairs of network levels via CGWs x 500 ms

Transmission delay (Vnet/IP)

Table 2.21-1 Transmission Delay in the Case of Vnet/IP

Range	Value to be set
Within a Vnet/IP domain	10 ms
Between Vnet/IP domains without WAN connection (*1)	50 ms (Regardless of the number of L3SWs)
Between Vnet/IP domains with a WAN	250 ms (Regardless of the number of L3SWs and existence of WAC routers)
If the Vnet/IP domain and V net domain are connected using a V net router	Number of the hops of V net router x 50 ms

*1: Connecting two domains through wide-area network is called "WAN connection."



Figure 2.21-2 Reaction Time 2

- When using SCS link transmission safety communication
 $Tr = \text{Sender Tscan} \times 2 + \text{Receiver Tscan} \times 2 + \text{Transmission Delay}$
 Transmission Delay: 100 ms

● **Fault Reaction Time**

How to calculate the fault reaction time of the ProSafe-RS system is shown as follows:

- In the case of faults within the Safety Control Station
 Basically, fault reaction time (maximum) is calculated by the following formula:
 $Tr = \text{Fault detection time} + \text{Tscan} \times 2 + \text{Output response time} - \text{Idle time}(*1)$

- *1: The maximum value of Fault detection time in the formula is the following. It depends on the module type.
- SDV144, SDV521, SDV526, SDV531, SDV53A, SDV541: 520 ms
 - SAI143, SAI533: 600 ms
 - SAV144: 1360 ms
 - SAT145, SAR145: 2100 ms

In addition, Tr in the case of communication fault between the CPU module and input/output modules is defined as below.

- $Tr = 1 \text{ s}$ (Tscan \leq 250 ms)
- $Tr = \text{Tscan} \times 2 + 0.5 \text{ s}$ (Tscan $>$ 250 ms)

After the time (Tr above) passed since the faults, the output module outputs the fail safe value.

- In the case of faults with field wiring or devices
 The following table shows the types of faults and the fault detection time (maximum). Apply this fault detection time in the above formula.

Table 2.21-2 Fault Detection Time of Field Wiring and Devices

Type of Fault	Module	Fault detection time (Maximum)
Short circuit between channels	SDV144, SDV521, SDV531, SDV53A, SDV541	1460 ms (*1)
	SAI533	600 ms
Short circuit in output wiring (while outputting OFF signals)	SDV531, SDV541	1460 ms (*1)
	SDV521	10 s (*1) (*2)
	SDV53A	10 s (*1) (*3)
Open circuit	SAT145, SAR145	1.5 s (*4)
Inputting the signal out of the range	SDV144	1020 ms (*5)
Open circuit or Short circuit with the power supply line (while outputting OFF signals)	SDV526	302 s
Overload of field device	SDV526	1.5 s

*1: Only detectable when the pulse test is enabled.
 *2: Value for style S3 and above.
 *3: Value for style S2 and above.
 *4: Only detectable when burnout detection is enabled.
 *5: This value applies when the modules are in dual redundant configuration. The value for non-redundant configuration is 520 ms as noted in the above explanation.

- Inter-SCS Safety Communication
The reaction time of Inter-SCS safety communication is the timeout time specified in the FB for Inter-SCS Safety communication.

$$Tr = OUTT + DLYT$$

- OUTT: Reception Interval Timeout value
- DLYT: Transmission Delay Timeout Value

- SCS Link Transmission Safety Communication
SCS link transmission safety communication reaction time equals to the timeout time specified for the receiver SCS.

$$Tr = OUTT + DLYT$$

- OUTT: Reception Interval Timeout value
- DLYT: Transmission Delay Timeout Value

SEE ALSO

For more information about OUTT and DLYT, refer to:

- “● Inter-SCS Safety Communication Timeout Settings” on page 2-55
- “● Time Out Settings of SCS Link Transmission Safety Communication” on page 2-61

● **Example of Calculating the Fault Reaction Time (Tr)**

Conditions:

Scan period of application logic

Idle time: 30%

DO module: SDV531 (output response time = 30 ms)

- Case 1 (Fault with the DI module)
 $Tr \text{ (max.)} = 520 \text{ ms} + 200 \text{ ms} \times 2 + 30 \text{ ms} - (200 \text{ ms} \times 0.3) = 890 \text{ ms}$
- Case 2 (Communication fault between the CPU module and the output module)
 $Tr \text{ (max.)} = 1 \text{ s}$ (because $T_{scan} < 250 \text{ ms}$)
- Case 3 (Short circuit fault between DI channels)
 $Tr \text{ (max.)} = 1460 \text{ ms} + 200 \text{ ms} \times 2 + 30 \text{ ms} - (200 \text{ ms} \times 0.3) = 1830 \text{ ms}$

■ **PFD Calculation**

The average PFD (System PFDavg) of a system is calculated with the model in the following figure.

$$\text{System PFDavg} = \text{Sensors PFDavg} + \text{Controller PFDavg} + \text{Valves PFDavg}$$



Figure 2.21-3 PFD Calculation Model

When the interval between proof tests is 10 years and the DIO module is used, the Controller PFDavg is indicated as follows.

$$\text{Controller PFDavg} = 6.63 \times 10^{-6}$$

Further information about PFD calculation is available on request.

2.22 HART Communication

Analog I/O module with HART communication (hereinafter called HART modules) on Pro-Safe-RS allows Plant Resource Manager (PRM) to control the HART communication devices connected to input and output on SCS. Also, HART modules allow PRM to conduct Partial Stroke Test (hereinafter called PST) on HART-supported valve positioner equipped with the PST function.

The HART modules on ProSafe-RS are interference-free and have no impact on the safety functions on SCS.

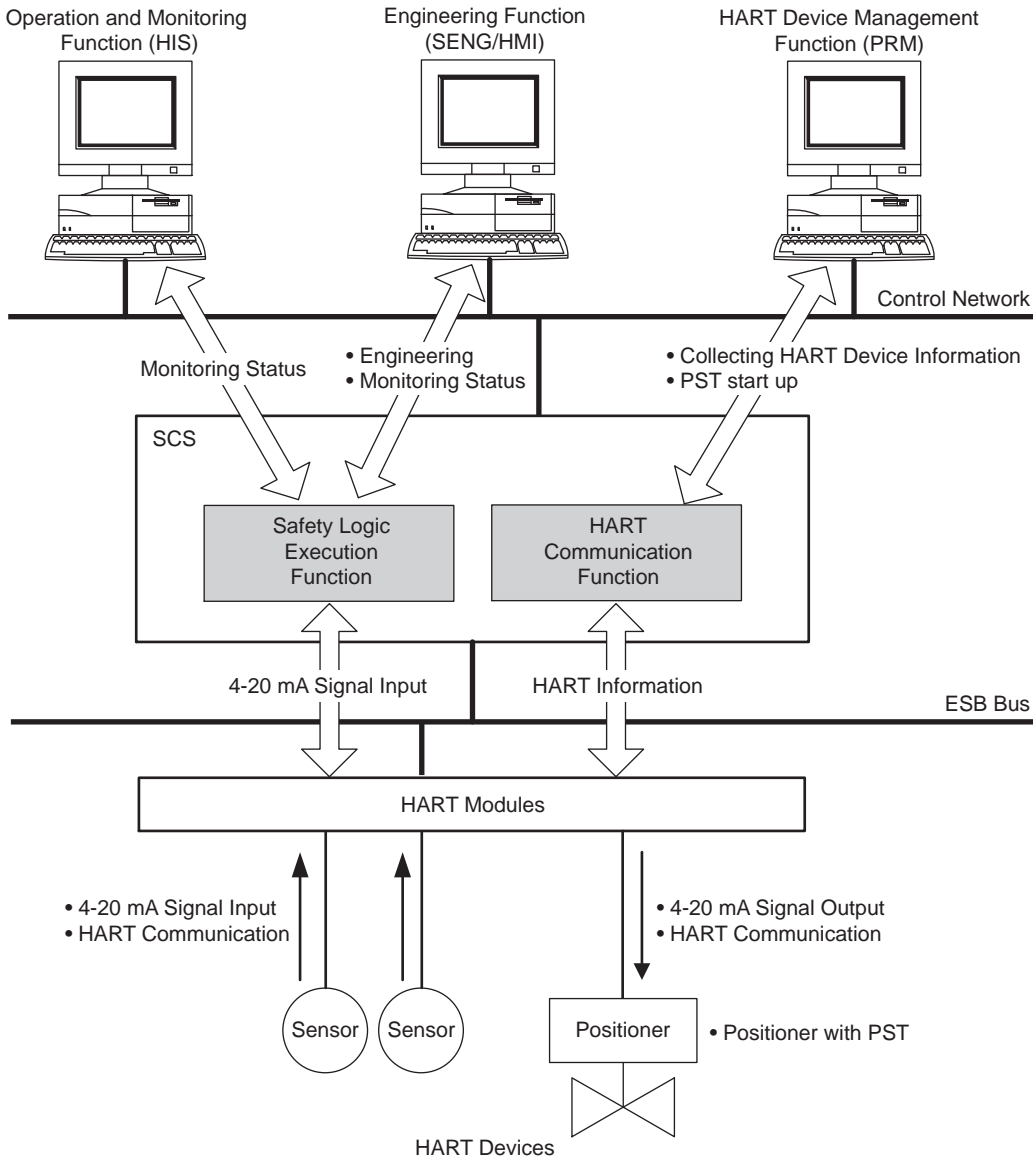


Figure 2.22-1 HART Communication Function

2.22.1 Description

This section introduces input and output modules supporting HART communication functions and provides precautions to perform HART communications.

■ AI/AO Modules for HART Communication Function

The following table shows the AI/AO modules for HART communication available to ProSafe-RS.

Table 2.22.1-1 AI/AO Modules for HART Communication Function

Module	Model	Description	Remark
Analog input module (Current input)	SAI143-H	16 channel; 4 to 20 mA, Isolated	HART communication function
Analog output module (Current output)	SAI533-H	8 channel; 4 to 20 mA, Isolated	HART communication function

One HART device is connectable for each channel. Each channel is equipped with a power supply function to the HART device.

Each module has only one HART modem and is communicable concurrently with only one HART device.

■ ProSafe-RS Software Setting Items

No setting items on ProSafe-RS for HART communications is required. However, some HART-supported valve positioners are capable of HART communications even during shutdown outputs (Valve full close) (*1). If you set the Shutdown output value for the analog output module on ProSafe-RS in accordance with the specifications of the valve positioner, HART communications continue even after the valve is shutdown. To do so, set the following parameters for the analog output module on ProSafe-RS based on the specifications of the valve positioner.

- Shutdown output value
- Tight-shut output value
- Output value at fault

*1: For example, specifications of some HART-supported valve positioners are defined as: 14 mA or more: Full open; 5.6 mA or less: Full close; 3.8 mA or more: HART communications allowed. In this case, set 'Shutdown output value', 'Tight-shut output value', and 'Output Value at Fault' to 3.8 mA (within the range where HART communications are allowed and safety shutdown is guaranteed), and HART communications continue even after the valve is full-closed.

■ Precautions for Using HART Devices

There are certain precautions to be taken regarding any HART devices that you are using and to be observed during their use.

● Precautions Regarding HART Devices

If HART devices (such as sensors, multiplexers, positioners, and handy terminals) are used in Safety loop, the devices must meet the requirements for the Safety loop (such as SIL certified: Self-diagnosable for HART circuit failure and capable of notifying it to external devices).

A failure in HART devices may affect field signals and cause errors such as false trip or no demand responding. If HART devices are incapable of notifying the errors, ProSafe-RS has no way to recognize them.

You must use devices not-constantly connected to the system such as a handy terminal only when the plant is shutdown or when maintenance work is being performed while no hazardous situation is created even if field signals are affected. If you have to use a handy terminal

while the plant is in operation, make sure that the handy terminal works correctly and take the above mentioned risks into account.

- **Dealing with HART Communication Errors**

If an error occurs in communication via a HART module between a HART communication device and PRM and there is nothing wrong in the communication route between the HART communication device and the HART module, the HART circuit inside the HART module may have failed. When an error occurs in the HART circuit, the control rights for the module are not switched, even if the HART module has a redundant configuration. In such cases, use the IOM Control Right Switching Tool to switch the control rights for the module and check whether communication is restored. If communication returns to normal as a result of switching the control rights, it is possible that the problem was caused by a HART circuit failure in the module on standby. In this case, ensure that the module is replaced.

**SEE
ALSO**

For more information about the IOM Control Right Switching Tool, refer to:

[5.2, "IOM Control Right Switching Tool" in Utilities and Maintenance Reference \(IM 32Q04B20-31E\)](#)

2.22.2 PST Engineering

From a PC integrated with PRM in which PST supported Plugin Software (hereinafter called Plugin for PST) is installed, you can execute PST on the valve positioner that supports the Plugin. Operations for and configuration of the PST are performed from the Plugin for PST. Plugin for PST communicates with the valve positioner via HART communications protocol. The valve positioner executes PST based on the information from the Plugin for PST and stores the test results inside. You can refer to the stored result by Plugin for PST, so you can determine the status of the valve (normal/abnormal) based on the result.

To build such a PST environment, consideration must be given to the following:

- PRM Configuration
- PST Engineering

■ PRM Configuration

PRM configuration includes:

- Register devices connected to ProSafe-RS in PRM.
- Register the 'Plugin for PST' software in PRM.
- Set the handling manner of errors raised by ProSafe-RS (such as system or device alarms) (*1)
- Customize to distinguish SIS devices from DCS devices.

All engineering work for PRM is done on PRM. For details, see User's Manuals for PRM.

*1: Error handling here means setting parameters for PRM's Fault Notification functions (such as Device Patrol and Maintenance Alarms). PRM is an interference-free product including its error handling functions.

■ PST Engineering

PST engineering includes the following parameter settings:

- Interval of PSTs
- Valve close level in PST (Percentage)
- Criteria for raising errors
- How to activate PST (Manual or Auto)
- If PST is automatically activated, how to notify errors (*1)

*1: If PST is automatically activated, available error notification methods are: sending alarms to HIS via PRM or using the output contacts equipped with the valve positioner. For the specifications of the output contacts on the valve positioner, see its specifications.

All the PST engineering work is done from Plugin for PST or Valve positioner. For details of the engineering work, see the User's Manuals for the Valve positioner.

Some Plugin for PST are capable of working in conjunction with PRM client. For details, see the User's Manuals for Plugin for PST.

Safety Integrity Level (SIL)-certified and PST-supported valve positioner is provided with a manual which describes precautions for conducting PSTs. Be sure to read the manual and follow the given procedures for conducting PSTs.

■ Precautions for Building PST Environment

The following must be observed when PST environment is built:

- Specifications of the valve positioner define that the shutdown output from ProSafe-RS has the highest priority (even in a PST).

-
- When the Analog output module configuration is online changed, ProSafe-RS is temporarily disconnected from HART communications. So, avoid online changing the module while the Plugin for PST software is running (i.e., during HART communications). If a HART communication error is raised while an online change is being made, run the Plugin for PST again after the module is recovered.
 - According to the manual for the valve positioner, setup the ProSafe-RS.

2.23 FAST/TOOLS Integrated Configuration

The configuration in which FAST/TOOLS is integrated with ProSafe-RS using a FAST/TOOLS Integration Engineering package is called "FAST/TOOLS Integrated configuration." When ProSafe-RS is integrated with FAST/TOOLS, they are connected via Vnet/IP-Upstream network. V net is not supported.

You can use SCS, the network modes, and the functions shown in the following table, on the assumption that it is used in the upstream process of oil or gas. "Yes" in the table indicates the supported function, while "-" indicates the function is not supported. The available Vnet/IP-Upstream network modes and function vary depending on the type of SCS.

Table 2.23-1 Function by SCS Type

Type of SCS	Vnet/IP-Upstream network mode			Function for the upstream process of oil and gas	
	Standard	Wide-area	Narrow-band	Gas Flow Rate Calculation Function	Data buffering function
SCSP1/SCSP2	Yes	Yes	-	-	-
SCSU1	Yes	Yes	Yes	Yes	Yes

This section describes the items of FAST/TOOLS integrated configuration common to SCSP1, SCSP2, and SCSU1. Descriptions for SCSU1 in the Narrowband mode or in upstream process are excluded.

The following figure shows the example of system configuration using the Wide-area mode of FAST/TOOLS integrated configuration.

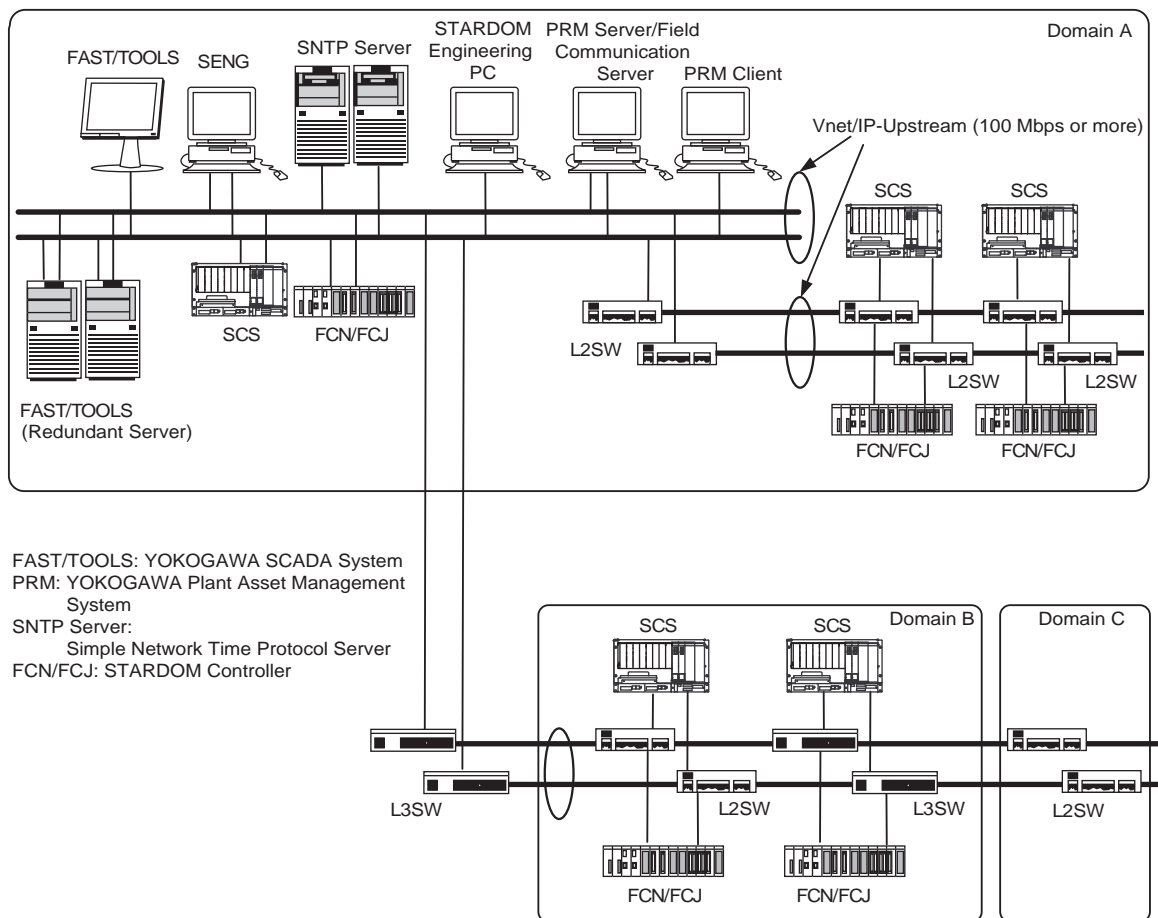


Figure 2.23-1 Example of System in the Wide-area Mode of FAST/TOOLS Integrated Configuration

**SEE
ALSO**

For more information about FAST/TOOLS integration and the Narrowband mode specification by using SCSU1 when using narrowband mode or the function for upstream process, refer to:

[9., "FAST/TOOLS Integrated System Using SCSU1" on page 9-1](#)

For more information about gas flow rate calculation function, refer to:

[B2., "Gas flow rate calculation function" in Integration with FAST/TOOLS \(IM 32Q56H20-31E\)](#)

■ Considerations on the Configuration

- SCS engineering is performed on SENG, and FAST/TOOLS engineering is performed on FAST/TOOLS.
Software packages of FAST/TOOLS and SENG must be installed on separate computers. They cannot be installed on the same computer.
- Because the network of FAST/TOOLS integrated configuration is Vnet/IP-Upstream, CENTUM station cannot be connected to it. Vnet/IP of CENTUM system and Vnet/IP-Upstream network of FAST/TOOLS integrated configuration system must be physically separated.
- In an SENG computer, a CENTUM VP/CS 3000 Integration Engineering package and FAST/TOOLS Integration Engineering package cannot be installed together.
- It is only the FAST/TOOLS integrated configuration using the FAST/TOOLS Integration Engineering package that can expand the distance between stations within Vnet/IP-Upstream network domain up to 1000 km (the Wide-area mode) or 10000 km (the Narrowband mode).
- In a FAST/TOOLS integrated system, SCS simulator cannot be used.
- For Vnet/IP hardware installed in Vnet/IP station, use the firmware of Rev. 12 or higher for the standard and the Wide-area mode, and Rev. 19 or higher for the Narrowband mode.
- If you have added a Vnet/IP station to the network, you must obtain the actual domain properties using the Domain Properties Setting Tool and confirm that the network setting for the domain that includes the new station is correct as follows: The Wide-area mode can be set for each domain. The Narrowband mode can be set for whole system only.
When the Standard mode is set Network Mode: Standard
When the Wide-area mode is set Network Mode: WideArea
When the Narrowband mode is set Network Mode: Narrowband

**SEE
ALSO**

For more information about how to obtain the setting status using the Domain Property Setting Tool, refer to:

[C2.4, "Obtaining actual domain property settings" in Integration with FAST/TOOLS \(IM 32Q56H20-31E\)](#)

■ Size of the System

The sizes of the system in standard and wide-area modes using integration with FAST/TOOLS are as follows:

- Connectable control bus: Vnet/IP-Upstream
- Number of connectable domains: 31
- Number of connectable stations within one domain: 64
- Stations that can be connected: 1984(*1)
- Layers: 16

*1: The number in theory. In practice, you need to determine the number of stations that are connected to Vnet/IP-Upstream network considering communications load.

When Wide-Area domain is selected in the domain properties dialog box, a part of the specifications of Vnet/IP-Upstream network is expanded as follows:

- Distance between stations in one domain: max. 1000 km
- Transmission delay: 40 ms or less
- Number of layer2 switches connectable between stations in one domain: unlimited

■ Reaction Time

The value of the Transmission Delay used for calculating Demand Reaction Time in inter-SCS safety communications is changed as follows depending on the settings of the Area in the domain:

Transmission Delay in inter-SCS safety communications:

- Standard is selected for the domain: 10 ms
- Wide area(*1) is selected for the domain: 40 ms

*1: [Wide-Area] is selected for Area in the Domain Properties Setting Tool.

**SEE
ALSO**

For more information about formula to calculate reaction time, refer to:

[2.21, "System Reaction Time" on page 2-135](#)

■ Extended Network Configuration

For extending your network to a larger area using the line provided by a common carrier, we recommend your network should be capable of self-isolation.

Example:

Digital leased line, wide area Ethernet, and so on.

For extending your network to a larger area without using the line provided by a common carrier, we recommend you use optical fiber cables.

In either case, the following specifications must be satisfied.

- Communications speed: 100 Mbps or more
- Transmission delay
 - In a domain: 40 ms or less
 - Inter-domain: 80 ms or less

3. Creating a New Application

This section describes the procedure for creating a new application.

3.1 Procedure of Creating a New Application

The following figure illustrates a procedure of engineering RS projects and SCS project from the creation of a project to backup of the completed project (Check-in).

For modifying the application, it is necessary to considerably analyze any effects caused by modifications in advance and take required measures against the effects.

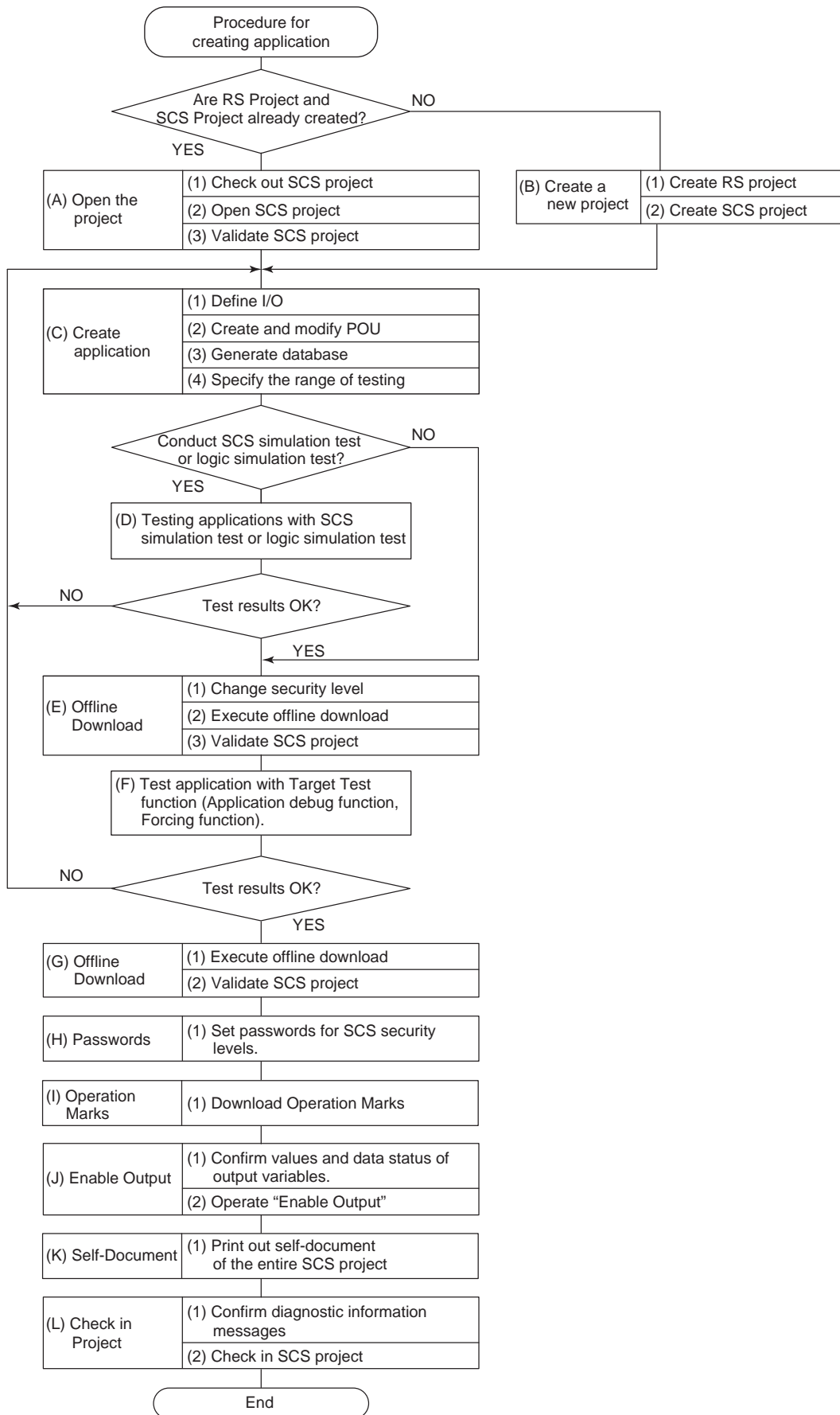


Figure 3.1-1 Procedure of Creating a New Application

■ Detailed Procedure for Creating a New Application

● (A) Opening the Project

Table 3.1-1 Procedure for Opening the Project

Item	Description
(1) Check out SCS project	<ul style="list-style-type: none"> Check out the existing SCS project with the Version Control Tool.(If the SCS project was checked in before creation of the application is completed.)
(2) Open SCS project	<ul style="list-style-type: none"> Start the SCS Manager. Open the SCS project. Enter the password for the SCS project.
(3) Validate SCS project	<ul style="list-style-type: none"> Run the Database Validity Check Tool and check that the CRC codes and generation times of the databases are consistent between the SCS and SCS project. Repair a database if there is a discrepancy in the database.

SEE ALSO

For more information about the databases, refer to:

“■ Relationship among Inter-Database Checks” in 11., “Database Validity Check Tool” in Engineering Reference (IM 32Q04B10-31E)

For more information about how to repair a database, refer to:

- “■ Repair database” in 11., “Database Validity Check Tool” in Engineering Reference (IM 32Q04B10-31E)
- “■ Repairing the Database That Does Not Match” in 11., “Database Validity Check Tool” in Engineering Reference (IM 32Q04B10-31E)

● (B) Creating a New Project

Table 3.1-2 Procedure for Creating a New Project

Items	Description
(1) Create RS project	<ul style="list-style-type: none"> A folder of RS project is automatically created when the Engineering Function is installed. If Concurrent Engineering is performed in some SENGs, the folder in RS project is changed to a shared folder.
(2) Create SCS project	<p>Set the following items with the SCS Manager when a new SCS project is created.</p> <ul style="list-style-type: none"> Folder for SCS project Properties of SCS project Resource Configuration P address

SEE ALSO

For more information about creating a project , refer to:

3.1, “Creation of New SCS Projects” in Engineering Reference (IM 32Q04B10-31E)

● (C) Creating an Application

Table 3.1-3 Procedure for Creating an Application

Items	Description
(1) Define Input/Output	<ul style="list-style-type: none"> Define I/O variables.(Dictionary View) Define I/O modules.(I/O Wiring View) Define links between channels and I/O variables.(I/O Wiring View) Set parameters for nodes, I/O modules and channels.(I/O Parameter Builder)
(2) Create and modify POU	<ul style="list-style-type: none"> Open POU which you want to create and modify. Edit POU. Save POU. Print POU. Confirm that the logic on Multi-Language Editor is the same as the logic printed with the Self-Document Function. Confirm that the execution order of FB/FU is correct.
(3) Generate database	<ul style="list-style-type: none"> Perform Build. Analyze that FU/FB which have been written in the safety application are for safety by using the Integrity Analyzer and then authorize them.
(4) Specify the range of testing	<ul style="list-style-type: none"> Check the modified POU and the affected POU with the Cross Reference Analyzer and then authorize them. Then, visually check the following setting items, which are critical for safety, to be sure that there are no unintended changes, because changes in these items cannot be detected by the Cross Reference Analyzer. <p>Item in Resource Properties window:</p> <p>Items in SCS Constants Builder:</p> <ul style="list-style-type: none"> [Cycle Timing] [Optical ESB Bus Repeater] (for SCSP1/SCSV1) [Maximum Extension Distance] (for SCSP1/SCSV1) [Extend Scan Period Automatically] [Behavior at Abnormal Calculation] [Automatic IOM Download] [Locking of Internal Variable] (for SCSP2)

SEE ALSO

For more information about Integrity Analyzer, refer to:

[8.1, "Integrity Analyzer" in Engineering Reference \(IM 32Q04B10-31E\)](#)

For more information about Cross Reference Analyzer, refer to:

[8.2, "Cross Reference Analyzer" in Engineering Reference \(IM 32Q04B10-31E\)](#)

● (D) Testing the Application with the SCS Simulation Test or Logic Simulation Test Function

User applications should be tested in the simulator running on SENG by using the SCS simulation test or the logic simulation test. Use the SCS Manager to perform control and operation, status display and results display for testing.

Application logic can be debugged with the Application Debug Function, Forcing of I/O variable and Online Monitoring Function. In the SCS simulation test or the logic simulation test, I/O channels are equivalent to being locked all the time.

SEE ALSO

For more information about operation of logic simulation tests, refer to:

[2., "Logic simulation test operations" in ProSafe-RS System Test Reference \(IM 32Q04B30-31E\)](#)

For more information about operation of SCS simulation test, refer to:

[3., "SCS simulation tests" in ProSafe-RS System Test Reference \(IM 32Q04B30-31E\)](#)

● (E) Offline Download

Table 3.1-4 Procedure for Offline Download

Items	Description
(1) Change Security Level	<ul style="list-style-type: none"> Start the SCS Maintenance Support Tool which monitors the SCS from the SCS Manager. Set the SCS security level to 0. Entering a password is required. Confirm that the SCS Security Level is 0 on the SCS State Management window of the SCS Maintenance Support Tool. Confirm the diagnostic information message indicating the security level at 0 with the SCS Maintenance Support Tool.
(2) Execute Offline Download	<ul style="list-style-type: none"> Execute offline download. When integrated with CENTUM, choosing offline downloading menu will pop up a dialog box to prompt for saving the operation marks. The operation marks may be saved as necessary. Confirm that SCS has started normally on the SCS State Management window of the SCS Maintenance Support Tool.
(3) Validate SCS project	<ul style="list-style-type: none"> Start the Database Validity Check Tool to check that CRC and generation time of four kinds of databases for SCS and SCS project are correct. Repair a database if there is a discrepancy in the database.

SEE ALSO

For more information about operation of the offline download, refer to:

9.1, "Offline Download" in Engineering Reference (IM 32Q04B10-31E)

For more information about how to repair a database, refer to:

- “■ Repair database” in 11., “Database Validity Check Tool” in Engineering Reference (IM 32Q04B10-31E)
- “■ Repairing the Database That Does Not Match” in 11., “Database Validity Check Tool” in Engineering Reference (IM 32Q04B10-31E)

● (F) Testing the Application with the Target Test Function

In a target test, user application logics are executed on the SCS. The SCS Manager is used for the operation of the test, the display of the status, and the display of the result. When the SCS security level is set to 0, all the following test functions can be used.

- Application logic can be debugged with the Application Debug Function, Forcing of I/O variable and Online Monitoring Function.
- Application can be executed without mounting I/O modules or wiring field devices when the Forcing Function for the I/O modules is used.
- Application logic can be debugged using the Forcing Function for I/O variables by changing conditions of the application logic.

With target test, it is highly recommended to test all signal paths and logic (FU/FB).

SEE ALSO

For more information about operation of the target test, refer to:

4.2, “Target test operation (in case online change download is not possible)” in ProSafe-RS System Test Reference (IM 32Q04B30-31E)

● (G) Offline Download

Table 3.1-5 Procedure for Offline Download

Items	Description
(1) Execute Clean Project and Build	<ul style="list-style-type: none"> • Before you execute offline download, you should perform Clean Project. Then perform build to create the database for downloading.
(2) Execute Offline Download	<ul style="list-style-type: none"> • Execute offline download. • When integrated with CENTUM, choosing offline downloading menu will pop up a dialog box to prompt for saving the operation marks. Save the operation marks as necessary. • Confirm that SCS has started normally on the SCS State Management window of SCS Maintenance Support Tool.
(3) Validate SCS project	<ul style="list-style-type: none"> • Run the Database Validity Check Tool and check that the CRC codes and generation times of the databases are consistent between the SCS and SCS project. • Repair a database if there is a discrepancy in the database.



IMPORTANT

Perform Clean Project in a timely manner; specifically, before FAT (Factory acceptance tests) or SAT (Site acceptance tests). Before you execute offline download, we recommend you perform Clean Project.

SEE ALSO

For more information about Clean Project, refer to:

“Cleaning Projects” in “Build” in “Code Generator” of “Workbench” of the Workbench User’s Guide

For more information about the databases, refer to:

“■ Relationship among Inter-Database Checks” in 11., “Database Validity Check Tool” in Engineering Reference (IM 32Q04B10-31E)

For more information about how to repair a database, refer to:

- “■ Repair database” in 11., “Database Validity Check Tool” in Engineering Reference (IM 32Q04B10-31E)
- “■ Repairing the Database That Does Not Match” in 11., “Database Validity Check Tool” in Engineering Reference (IM 32Q04B10-31E)

● (H) Setting Passwords

Table 3.1-6 Procedure for Setting Passwords

Items	Description
Set passwords for Security Levels	<ul style="list-style-type: none"> • Set passwords for security levels 1 and 0 from the SCS Manager. • Confirm the diagnostic information message from SCS for which passwords for the security levels have been set with the SCS Maintenance Support Tool.

● (I) Download Operation Marks

Table 3.1-7 Procedure for Downloading Operation Marks

Items	Description
Download Operation Marks	<ul style="list-style-type: none"> • In the case of the CENTUM integration structure, the operation marks saved in advance are downloaded to the SCS.

● (J) Enabling Output

Table 3.1-8 Procedure for Enabling Output

Items	Description
(1) Confirm values and data status of output variables	<ul style="list-style-type: none"> • Confirm which output channels are disabled on the SCS State Management window of SCS Maintenance Support Tool. • Start the I/O Lock Window.(This can be performed at security level 2.) • Confirm that values and statuses of logical data and physical data for output variables are correct.
(2) Operate "Enable Output"	<ul style="list-style-type: none"> • Perform the Output Enable Operation for output modules on the SCS State Management window of SCS Maintenance Support Tool. • Confirm that the diagnostic information message on the Output Enable Operation for output modules is displayed. • Confirm that Output Channels are enabled on the SCS State Management window. • Confirm that the SCS operating mode is "Running" on the SCS State Management window.

SEE ALSO For more information about the Output Enable Operation, refer to:

- ["Enable Output" Operation](#) on page 3-11

● (K) Self-Document

Table 3.1-9 Procedure for Self-Document

Items	Description
(1) Print out whole SCS project using self-document	<ul style="list-style-type: none"> • In preparation for the desk check performed at application software changes in the future, print out the latest SCS project database as self-documents.

● (L) Checking in Project

Table 3.1-10 Procedure for Check in Project

Items	Description
(1) Confirm the diagnostic information message	<ul style="list-style-type: none"> • Confirm whether any diagnostic information messages you have not confirmed are displayed or not with the SCS Maintenance Support Tool.
(2) Check in SCS project	<ul style="list-style-type: none"> • Close the SCS Manager. • Check in the SCS project with the Version Control Tool.

SEE ALSO For more information about Check-in operation, refer to:

- 13.3, ["Checking in Project Data"](#) in Engineering Reference (IM 32Q04B10-31E)

3.2 Precautions for Engineering

This section describes precautions for creating an application.

■ Precautions for Creating an Application

- **Edit of Project Files**

Files in the SCS project folder must be edited only in the SCS Manager.

- **Creating Application Logic**



IMPORTANT

- A value must be set to each input parameter in the FU and FB. Also to each output parameter in the FU. They cannot be omitted.
 - The data type of variables received by FU and FB must be in accord with that of input/output parameters in FU and FB.
-
- Arrays cannot be used in a program of FBD or LD. When the Integrity Analyzer finds an array, it generates an error.
 - In the application logic, POU called from a program can have a hierarchy of up to 8 levels. If the hierarchy exceeds 8 levels, the Integrity Analyzer generates an error.
 - Instance names connected in the hierarchy should be defined so as to have up to 80 characters.
 - Four FBs (ANN, SOE_B, SOE_I, and SOE_R) are Interference-free. However, the Integrity Analyzer does not issue any alarms. As the four FBs do not have output parameters, using the FBs in FBD (Function Block Diagram) has no effects on the safety loop. On the other hand, these FBs have ENO output parameters when used in LD (Ladder Diagram) and thus make sure that they do not affect the safety loop.
 - When looping the output of FU/FB back without using intermediate variables as shown in left of the following figure, a warning is issued at building. To avoid this, use a variable in looping back the output, specified in right of the following figure. Place the output variable on the right of FU/FB in the loop back.

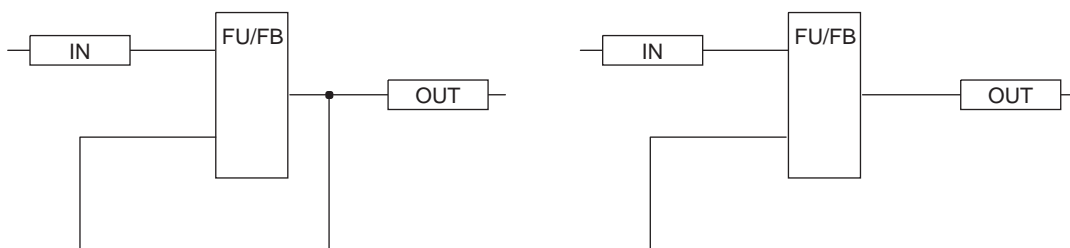


Figure 3.2-1 Example when a Warning is Output (Left) and Example when a Warning is not Output (Right)

- Integrity Analyzer displays yellow warning icons if it detects Null functions of LD. Null functions refer to diagrams where one of the signals that branch out in a parallel coupling is directly connected and the value of the contact connected to the other line is ignored. In the example in the following figure, the value of variable bIN is ignored.

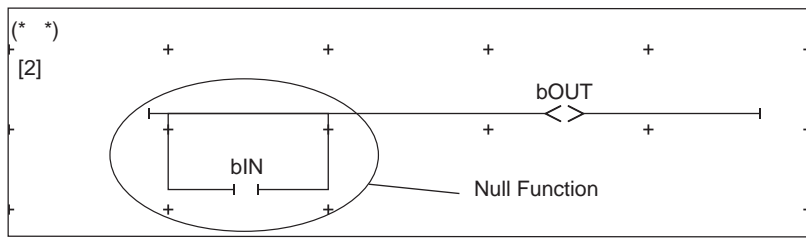


Figure 3.2-2 Example of Null Function in LD

- An FB with a variable name assigned must not be called more than once. Be especially careful when you copy and paste an FB. For example, if the same REPEATTIMER is used in two programs, the timer may count at double-speed. If Integrity Analyzer detects one instance that is called multiple times, it raises a warning.
- If a calculation of equal (=) or Not equal (<>) is used for real numbers, the Integrity Analyzer will display a warning message.
- If variables of COM_BOOL type, COM_DINT type, or COM_REAL type undefined in Binding List View are used in POU, the Integrity Analyzer displays a warning message.
- At least one output parameter must be wired for function blocks that have no input parameter, or such function blocks are not executed. Following FBs are appropriate; ECW_B, ECW_I, ECW_R, SYS_DIAG, SYS_IOALLST, SYS_TIME, SYS_ALARM, SYS_NETST, SYS_ESBIN, SCI_B, SCI_I, SCI_R, LTRCV, LTFCS
- If you repeat building operations on the SCS Manager, the database size of SCS projects become larger. If the database size becomes too large, phenomena such as the build time becoming very long occur. In order to avoid this, execute [Compact Database] at an appropriate timing.

● At Occurrence of Abnormal Calculations



IMPORTANT

If abnormal calculations such as division by zero, access to the outside of an array, overflow in floating-point calculation, and overflow in casting occur during POU execution, SCS behaves according to the specification made by [Behavior at Abnormal Calculation] in the SCS Constants Builder. If this specification is [SCS fails] (default), the SCS stops. If you specify [SCS continues], the SCS continues the operation without failing, but there is a potential risk that it cannot properly respond upon generation of a demand related to the corresponding POU while an abnormal calculation persists. Be sure to take measures to prevent abnormal calculations in applications and, if necessary, specify [SCS continues] just in case.

If SCS continues operating under the conditions where it cannot properly respond to related demands due to occurrence of abnormal calculation, the user must identify the condition immediately and take corrective measure to solve the error by modifying the application. If [SCS continues] is specified and an abnormal calculation occurs, the occurrence of error and the cause are notified to SENG and HIS via diagnostic information messages. Moreover, if you use the SYS_CERR function block, it is possible to output the abnormal calculation status to external devices by the application.

- If division by zero occurs in division of REAL- or DINT-type, SCS behaves according to the specification of [Behavior at Abnormal Calculation] in the SCS Constants Builder.
- If you specify a positive constant or 0 to an array index, index range check is performed at building and a build error will occur if the index points to the outsides of the array. On the other hand, if you specify a variable, expression, or negative constant for an array index, the range check is not performed at building. In this case, if access to the outside of

the array occurs, SCS behaves according to the specification of [Behavior at Abnormal Calculation] in the SCS Constants Builder.

- If you convert floating point data to DINT with the ANY_TO_DINT function, SCS behaves according to the specification of [Behavior at Abnormal Calculation] in the SCS Constants Builder if the converted result is larger than the maximum value or smaller than the minimum value of integer-type data (that is, when an overflow occurs).
- Always use DINT-type for ANY_TO_TIME to restrict the value in the range from 0 to 86400000. If you enter a value outside this range, a correct TIME value cannot be obtained. In particular, if you specify a REAL value larger than 4294967295 (i.e., the maximum unsigned 32-bit integer) or a REAL value smaller than -2147483648 (i.e., the minimum signed 32-bit integer), SCS behaves according to the specification of [Behavior at Abnormal Calculation] in the SCS Constants Builder.

Note that, in the following cases, SCS continues the operations regardless of the specification of [Behavior at Abnormal Calculation] but the intended calculation result cannot be obtained.

- If you input 0 or less to LOG, a fixed value (-1E35) is output.
- If you input 0 or less as the denominator for MOD, a fixed value (-1) is output. In this case, there is no distinction from the case where -1 is obtained from the correct calculation.
- If an overflow occurs in calculation of integer values, the calculation result is not limited by the maximum value. Be sure to apply limits on the result of calculation if it is expected that the maximum value is exceeded.
- Be sure to specify the TIME-type value to less than 24 hours. No error occurs at building even if 24 hours is exceeded. Since the timer returns to 0 hours when it reaches 24 hours, it never reaches time beyond 24 hours. For example, if you set the timeout of TON to 25 hours, TON will no longer time out, which will be different from the intended operation.

**SEE
ALSO**

For more information about considerations on abnormal calculations, refer to:

“■ Coding” on page App.1-1

For more information about the behavior of SCS at abnormal calculation, refer to:

B6.1.3, “Behavior at abnormal calculation” in Safety Control Station Reference (IM 32Q03B10-31E)

● Library Project

If you use a library project, be sure to copy it to an SCS project.

- If you refer to an SCS project from a remote PC, specify the library project path of the Dependencies in the UNC format.

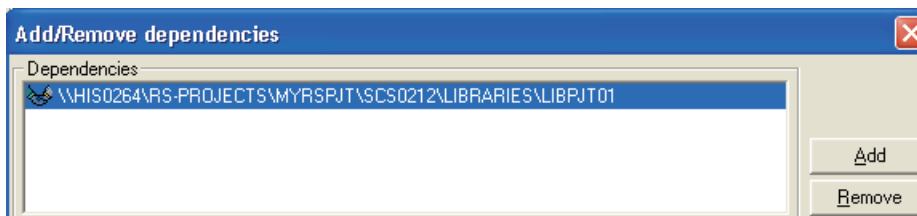


Figure 3.2-3 Specification Example of UNC-format Library Project Path

● “Enable Output” Operation

- Each output channel of SCS has two statuses, Enabled Output and Output Disabled, when the output is disabled, the output from application logic is not connected to the actual output channel, and OFF or pre-specified fail safe value is output to the field. Perform the Enable Output Operation to connect the output values from the application logic to the output channels. All normal outputs (DO module channels, AO module chan-

nels, Subsystem Communication output) are enabled by the output enable operation from an SENG.

When SCS starts, all output channels are in the output disabled status.

- Transmission is started in the inter-SCS safety communication and subsystem communication output by the first output enable operation after SCS startup.
- When an output module fails, all output channels on the output module enter the output disabled status.
When an output channel fails, the output channel enters the output disabled status.
- In the case of subsystem communication, it does not result in the output disabled status even if an error occurs in the subsystem communication (communication module error or communication error).
- The output enable operation can be performed from the application logic using a system function block. There are two types of function blocks that can perform the output enable operation: SYS_STAT, which enables safety outputs and outputs in inter-SCS safety communication, and SYS_STAT_SC, which enables subsystem communication outputs. Use these system function blocks and perform the output enable operation if it is desired to have different output start timings for output modules and the subsystem communication.

**SEE
ALSO**

For more information about specifications of SYS_STAT, refer to:

[C10.1, "SYS_STAT \(SCS status management\)" in Safety Control Station Reference \(IM 32Q03B10-31E\)](#)

For more information about specifications of SYS_STAT_SC, refer to:

[C11.11, "SYS_STAT_SC \(subsystem communication output status indicator\)" in Safety Control Station Reference \(IM 32Q03B10-31E\)](#)

● **System Alarms for the Inter-SCS Safety Communications and Link Transmission at the SCS Startup**

During SCS startup, no system alarm is raised for an error in the inter-SCS safety communications and SCS link transmission. System alarm is sent for the first error after the startup procedure and the error during the startup procedure turns to normal. System alarms related to inter-SCS safety communications and SCS link transmission are sent from the receiving station only.

At SCS startup, make sure that both the inter-SCS safety communications and link transmission are normal.

Do the following to check the normalcy:

- Check the communication status of the receiving function block (NR status of CONS FB, STS of LTRCV FB, and STS of LTFCS FB).
- Check the CMER of the system function block, SYS_DIAG.

● **Considerations on Using the 16-bit Modbus Master Support Mode in Modbus Slave Communication**

When executing the following functions by using the function code from the Modbus master, set 16-bit Modbus master support mode for the definition of SCS Constants Builder to Enable.

- Writing to a single holding register by using the function code 06 from the Modbus master
- Reading one-word data or specifying even reference numbers by using the function codes 03 and 04 from the Modbus master
- Writing one-word data or specifying even reference numbers by using the function code 16 from the Modbus master

The function code 06 allows data to be written to the upper or lower word of 32-bit data. To use the written data as 16-bit data, create an application for extracting the upper or lower word of the 32-bit data.

When 16-bit Modbus master support mode is Enable in the SCS Constants Builder, the simultaneity of the upper and lower words is not assured because writing to the upper and lower words can be performed independently. If you intend to use the data as 32-bit data, write the data in units of 32 bits without using the function code 06 or 16.

■ Considerations on Using Time Synchronization Block (SYS_SETTIME)

Observe the following usage limitations and considerations when you set the system time of SCS and the Vnet/IP or V net time by using the function block (SYS_SETTIME).

The following figure shows an example to set 2:00:00 on input of a trigger signal by using the SYS_SETTIME function block.

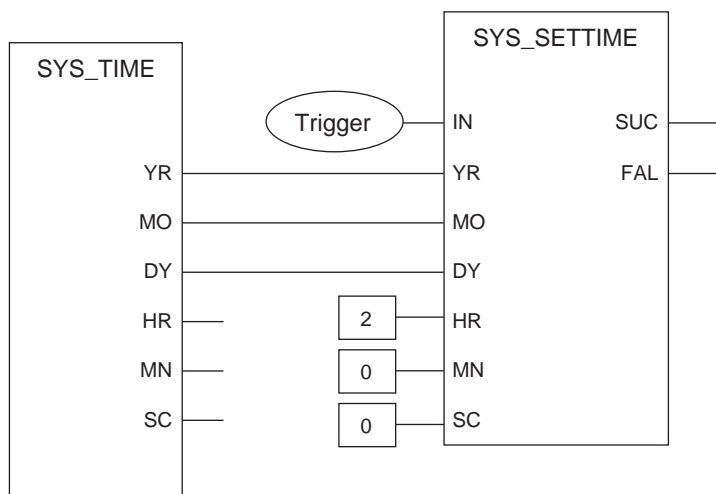


Figure 3.2-4 Usage Example of SYS_SETTIME

Considerations on setting the time in the usage example are as follows:

- At the moment the time setting is executed, the date must match between the trigger signal providing side and the SCS to which the time is set. To ensure matching dates, offset more than one minute from 0:00 A.M. If the time is set around 0:00 A.M. If the function block is used to set a time around 0:00 A.M. If the date of the trigger signal providing side and the date of the SCS may become different. Therefore, a wrong date may be set to the SCS.
- Before using the time synchronization function block, set the time using the time setting function of SENG or HIS.

SEE ALSO

For more information about time synchronization function block (SYS_SETTIME), refer to:

[C11.3, "SYS_SETTIME \(SCS time setting\)" in Safety Control Station Reference \(IM 32Q03B10-31E\)](#)

● Usage Limitations of Time Synchronization Function Block

Do not use the time synchronization function block under the following states: An alarm may occur, due to resetting of the time or time diagnostic error in inter-SCS safety communication.

- Using IRIG-B time synchronization in the time synchronization method
- Using the time synchronization function block in two or more SCSs.
- Using two or more time synchronization function blocks in one SCS.

- A station with Vnet/IP firmware earlier than Rev. 8 is connected to Vnet/IP. The time synchronization function block can be used when the Vnet/IP firmware of the station is updated to Rev. 9 or later.
- SCS with SCS system program R2.03.58 or earlier is connected to the same control bus. The time synchronization function block can be used when all SCS system program release numbers of all SCSs are updated to R2.03.59 or later.

In addition, if the SNTP server is connected to Vnet/IP, the time setting by the time synchronization function block is disabled.

- **Time span for the Time Synchronization Function Block Detects DI Input and It Sets the SCS Time**

Use the DI input that is connected to the SCS using this function block as the input signal for IN.

The maximum time (Tsettime), which is from detection of DI input to change of the SCS time, is obtained from the following formula:

$$Tsettime = Tscan \times 2 + \text{Processing time of Input module} + 50 \text{ ms} - \text{Idle time}$$

$$\text{Idle time} = Tscan - \text{Application logic execution time}$$

**SEE
ALSO**

For more information about check application logic execution time, refer to:

- [“CPU Processing Time” on page 2-48](#)

For more information about application logic execution time, refer to:

- [C11.1, “SYS_SCAN \(execution time indicator\)” in Safety Control Station Reference \(IM 32Q03B10-31E\)](#)
-

3.3 Guideline on Creating Application Logic

This section provides the guideline on creating application logic. Keep this section on hand when creating application logic.

3.3.1 Use of Analog Input Value

Analog input modules include modules to handle current and voltage and modules to handle data from a thermocouple (TC) and Resistance Temperature Detector (RTD). Modules to handle input from TC or RTD hereinafter called TC/RTD input module.

Input signals input to the current/voltage input module are normalized and passed to the application logic in the form of 0.0-100.0% data. The user can convert this data into engineering data in the application.

Input signals input to the TC/RTD input module are passed directly to the application logic in the form of engineering data.

The following shows an example of application logic for comparison between an analog input value and a constant value.

■ Example 1 - Application Logic Using the Analog Input Values of the Current / Voltage Input Module

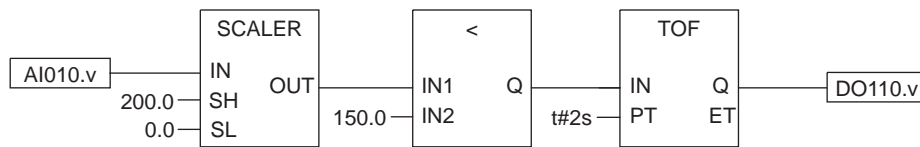


Figure 3.3.1-1 Example 1 - Using Current / Voltage Analog Input Value

In example 1 above, only Analog values are input. These are then converted to values in engineering units for comparison. If the Analog input value is larger than the reference value (150.0) for the specified period of time in Off Delay Timer (2 s), output is turned OFF.

■ **Example 2 - Application Logic Using the Analog Input Values of the Current / Voltage Input Module**

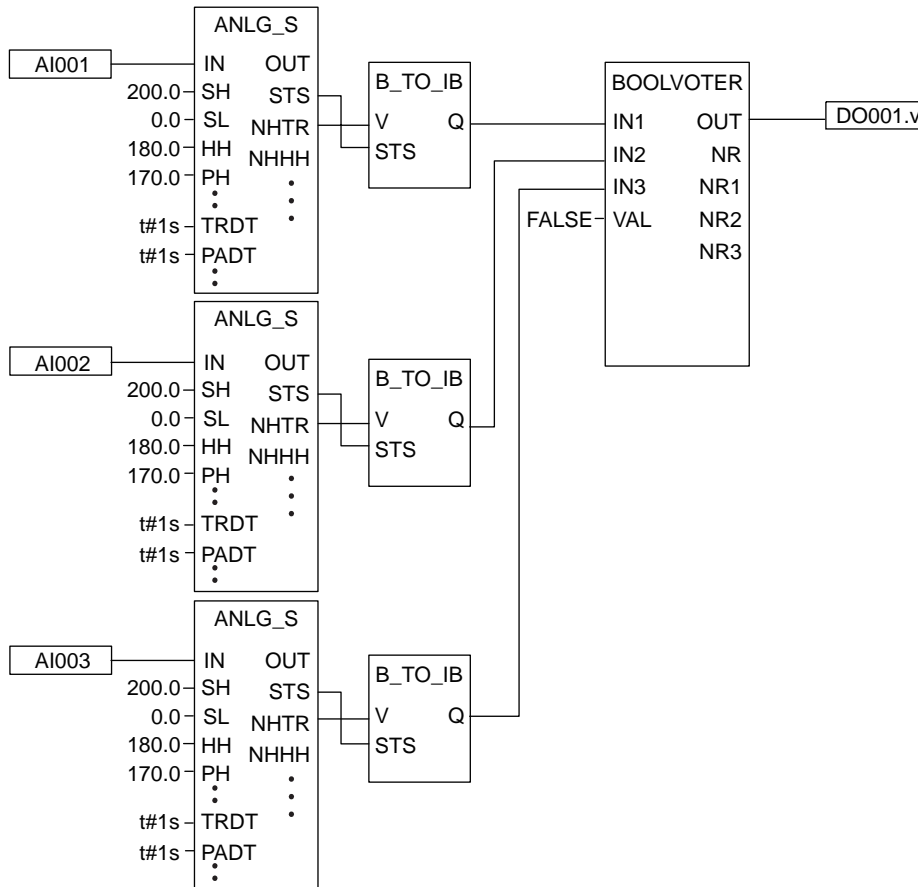


Figure 3.3.1-2 Example 2 - Using Current / Voltage Analog Input Value

In example 2, each of the three analog inputs is scale-converted by each ANLG_S and output. 2oo3 (2 out of 3) Voting result of the Trip outputs (NHTR) or a Fail-safe value is output as DO. Each ANLG_S produces a Trip output when the input value exceeds the Trip limit value for the period that is set in Off-Delay Timer (TRDT = 1 s in Example 2).

■ **Example 3 - Application Logic Using the Analog Input Values of the Current / Voltage Input Module**

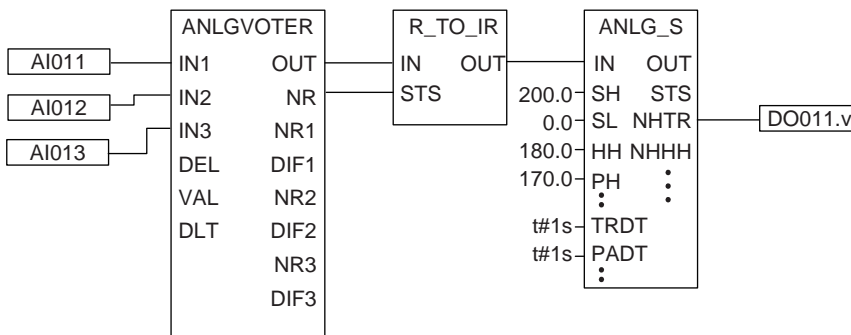


Figure 3.3.1-3 Example 3 - Using Current / Voltage Analog Input Value

The ANLGVOTER gets an intermediate value of analog inputs or a fail-safe value. The R_TO_IR converts the value to IO_REAL type and inputs it to the ANLG_S. The ANLG_S out-

puts the Voting result and Hi-Trip (NHTR). The ANLG_S produces a Trip output when the input value exceeds the Trip limit value for the period that is set in Off-Delay Timer (TRDT = 1 s in Example 3).

■ **Example of Application Logic Using the Analog Input Values of the Thermocouple / Resistance Temperature Detector(TC/RTD)**

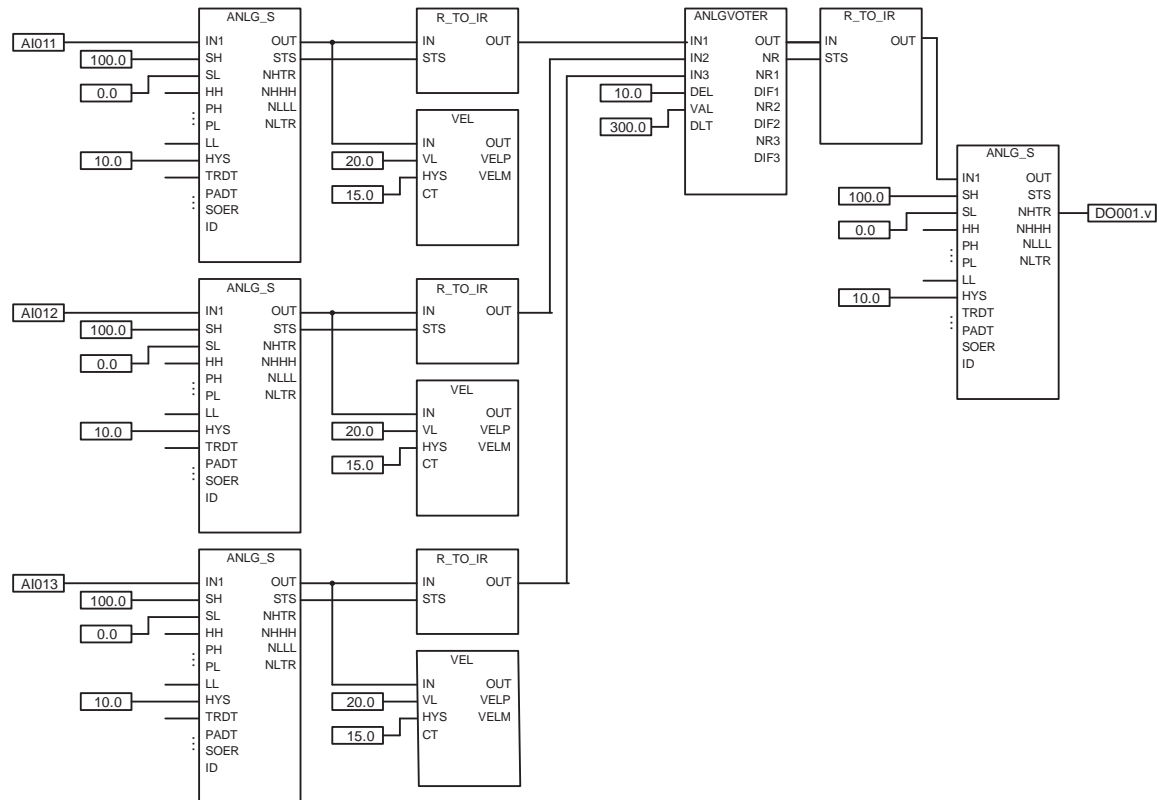


Figure 3.3.1-4 Example of Application Logic Using the Analog Input Values of the TC/RTD Input Module

In the above logic example, the following processes are carried out.

1. Three analog inputs from TC/RTD input modules are each indicated by ANLG_S and the rate of change of each value is simultaneously monitored by VEL to ascertain whether the rate of change is exceeded from allowable range.
2. The intermediate values of the three types of data or the fail-safe values are obtained with ANLGVOTER.
3. The results are indicated by ANLG_S, monitored HI trip status and output to DO.

The input data from TC/RTD input module to ANLG_S is engineering data, which means that 100.0 and 0.0 are input to SH and SL respectively, and input to HYS is in the form of engineering data. The indicated value for ANLG_S (input value to VEL) is engineering data, and so VL and HYS of VEL should be input in engineering data. The same value should be converted to IO_REAL type using R_TO_IR. In R_TO_IR, there is no difference in the handling of input data, whether it is normalized or engineering data. The converted values are each input to ANLGVOTER and the median value or fail-safe value obtained, but since this value is also engineering data, the values input to DEL and VAL in ANLGVOTER are also engineering data. The value obtained is again converted to IO_REAL type using R_TO_IR and input to ANLG_S. In the same way, 100.0 and 0.0 are input to SH and SL respectively and the values input to HYS in the form of engineering data. The Voting result is indicated based on the input value and Hi-Trip (NHTR) is output to DO.

■ Precautions when Using the Analog Input Values from the Thermocouple / Resistance Temperature Detector (TC/RTD)

The input signal entered into the TC/RTD analog input module is passed to the application logic in the form of direct engineering data rather than normalized data.

Caution is required in the case of the ANLG_S, VEL, ANLG1OO2D, and ANLGVOTER, because there are differences in the way of making application logic whether the input data is engineering data or normalized data.

● Case of ANLG1OO2D

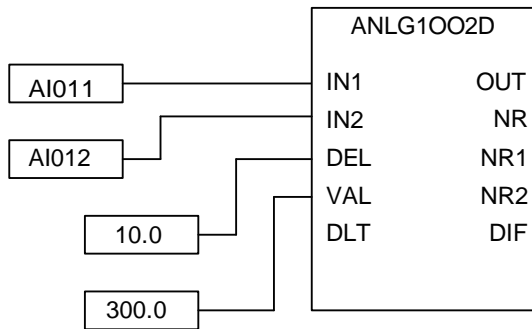


Figure 3.3.1-5 Example of ANLG1OO2D Application Logic

The data (AI011, AI012) from the TC/RTD input module is engineering data, and so the input values (IN1, IN2) and output value (OUT) are also engineering data. In this case, DEL and VAL are also entered as engineering data.

This means that, in the figure above, the values of DEL and VAL are specified as 10.0 deg. C and 300.0 deg. C respectively (if the engineering unit specified in I/O Parameter Builder is deg. C).

● Case of ANLGVOTER

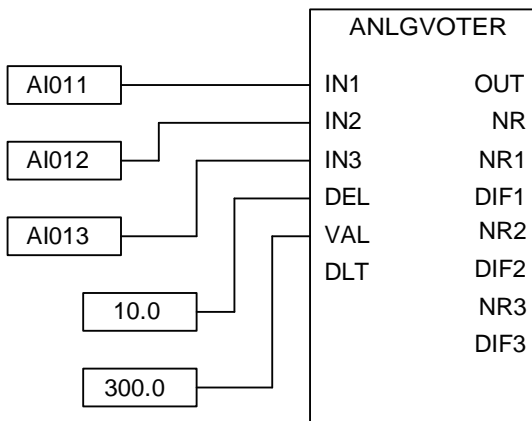


Figure 3.3.1-6 Example of ANLGVOTER Application Logic

As with ANLG1OO2D, if the input values (IN1, IN2, IN3) are engineering data, the output value (OUT) will also be engineering data.

DEL and VAL are also entered as engineering data.

● **Case of VEL**

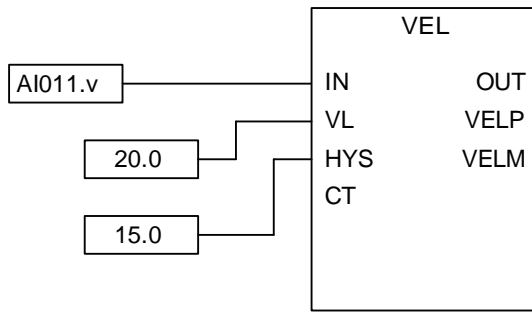


Figure 3.3.1-7 Example of VEL Application Logic

If the input value (IN) is engineering data, the output value (OUT) will also be engineering data.

VL and HYS are entered as engineering data.

● **Case of ANLG_S**

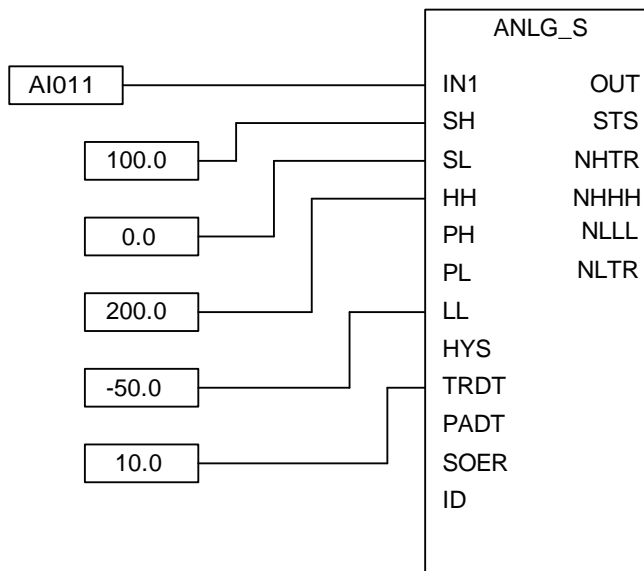


Figure 3.3.1-8 Example of ANLG_S Application Logic

In ANLG_S, make sure that you enter the following value if the input value (IN) is engineering data.

SH=100.0

SL=0.0

HYS is entered as engineering data.

TIP When using ANLGI, apply the same process as ANLG_S.

3.3.2 Shutdown due to Channel Failure

The following examples show three types of application logic for shutdown due to a channel failure (mainly output channel).

■ Overview

The following figure shows the overview of function blocks for creating application logic for shutdown due to a channel failure.

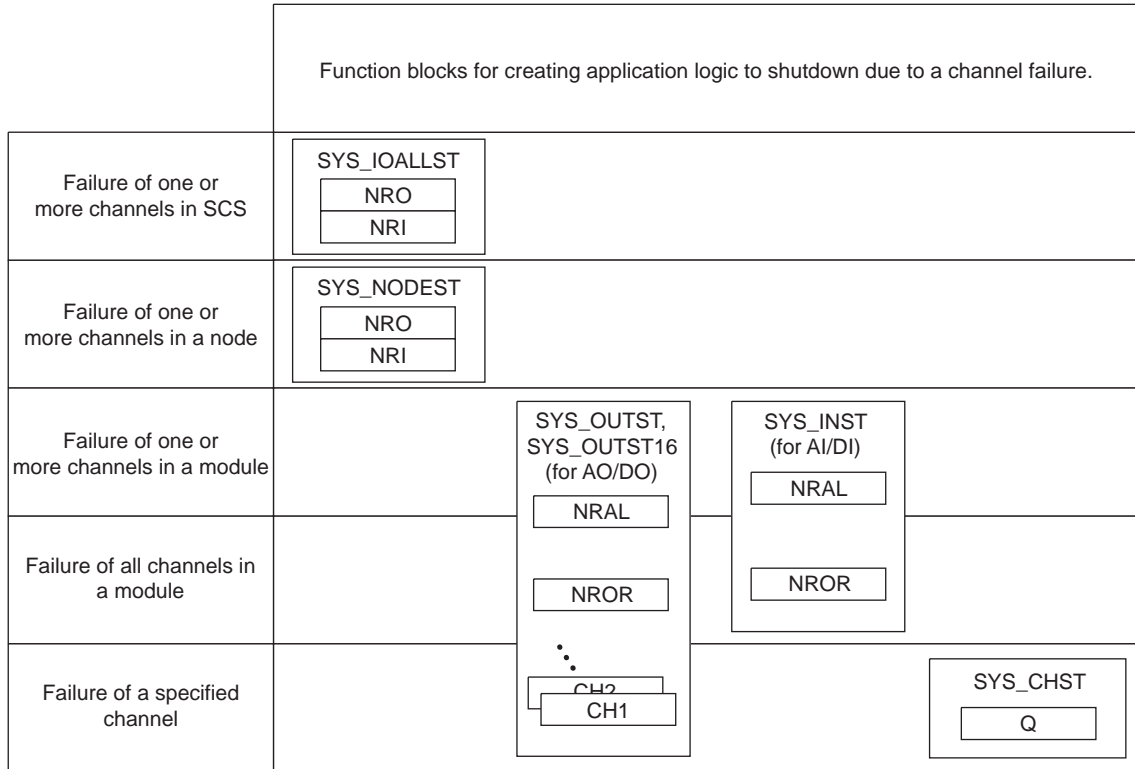


Figure 3.3.2-1 Function Blocks for Shutdown due to a Failure of Channels

A failure in any channel of a whole SCS or one node as well as a failure in a specific channel can be used as the condition for shutdown. If necessary, combine these two conditions.

For maintenance of an I/O module, locking the appropriate module prevents shutdown logic from being activated. (For maintenance of an output module, the actuator connected with the output channels needs to be bypassed.)

■ Shutdown after Detection of any Channel Failures in a Specified Unit

The application logic can be created so that shutdown is executed if any output channel has failed in a certain unit (a whole SCS or specified node).

● Shutdown due to Any Output Channel Failures in a Node

The SYS_NODEST is available to create application logic to execute shutdown in case of a failure of any output channel in a node.

First, add important outputs to one specific node as shown in the following figure, create SYS_NODEST, designate a node number as an input parameter for the SYS_NODEST, and then connect the output parameter with the shutdown logic.

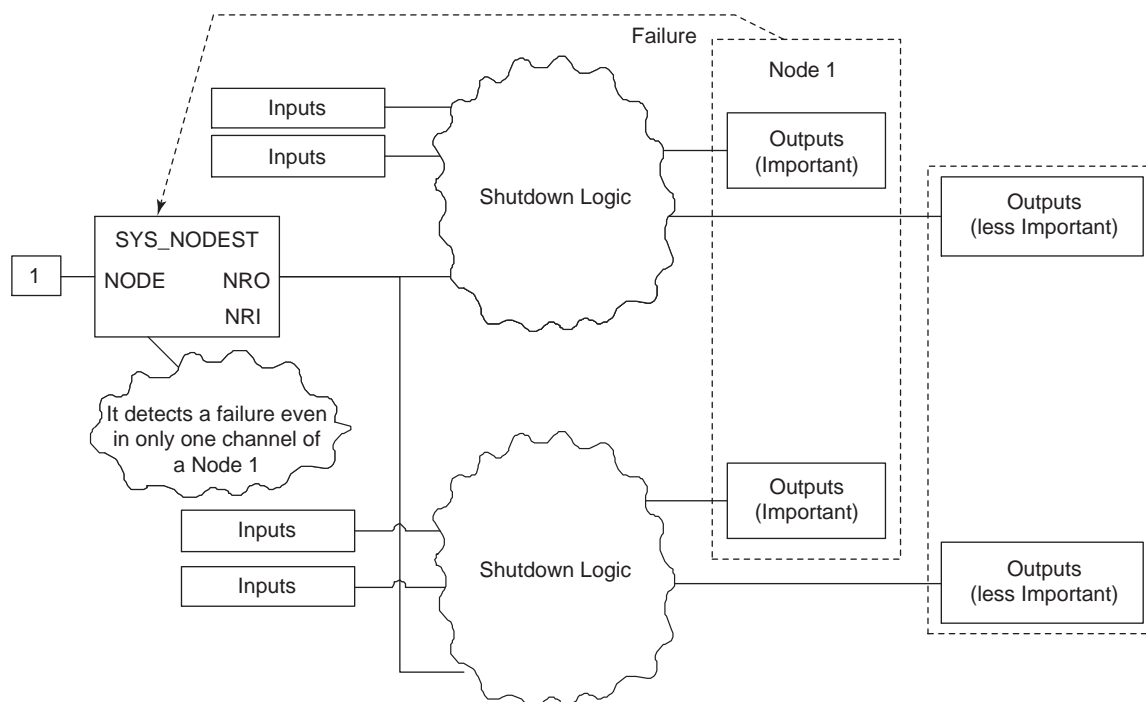


Figure 3.3.2-2 Example of Shutdown in Cases of a Failure of Any Output Channel in a Node

● **Shutdown due to Any Output Channel Failures of an SCS**

The SYS_IOALLST is available to create application logic to execute shutdown in case of a failure in any output channel of an SCS.

The creation method of application logic is the same as the one for detecting a failure in a node. However, take appropriate care when using this logic, as the output channels that are not important are also checked for failure by this logic.

SEE ALSO For more information about SYS_NODEST, refer to:

C10.14, “SYS_NODEST (all I/O channels of node status indicator)” in Safety Control Station Reference (IM 32Q03B10-31E)

For more information about SYS_IOALLST, refer to:

C10.13, “SYS_IOALLST (all I/O channels of SCS status indicator)” in Safety Control Station Reference (IM 32Q03B10-31E)

■ **Shutdown after Detection of a Failure in a Specific Channel**

The application logic can be created to execute shutdown in case of a failure in specific I/O channels. This allows control of shutdown by responding to the failures of individual I/O channels.

● **Shutdown due to Failures in Several Specific Output Channels**

The SYS_OUTST or SYS_CHST is available to create application logic to execute shutdown in case of a failure in specific output channels.

As shown in the following figure, create SYS_OUTST and designate the installation location (Node number and slot number) of the output module as an input parameter to detect a failure in the output channels that acts as the shutdown trigger. The output parameter receives the failure status of each channel. Connect only the necessary channels with the shutdown logic.

For checking fewer channels, the SYS_CHST can be used instead of the SYS_OUTST. To use the SYS_CHST, specify installation locations of the channels (Node number, slot number, and channel number).

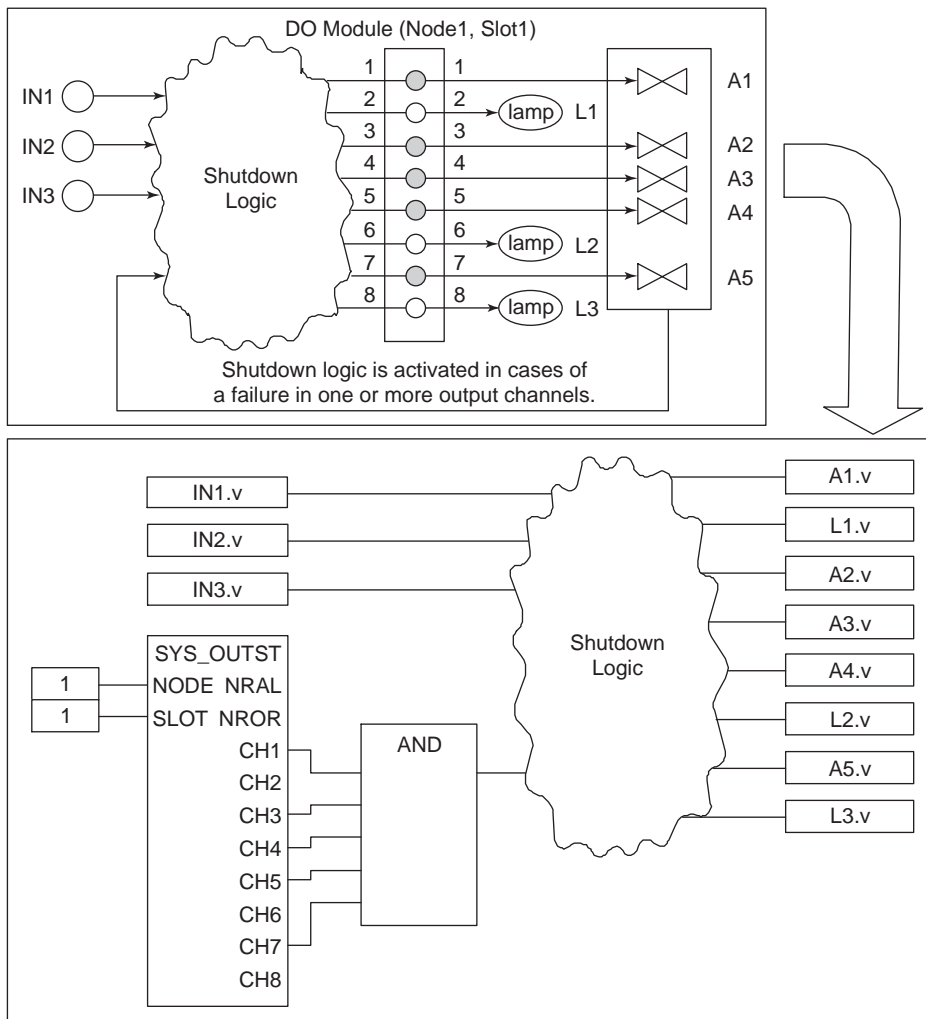


Figure 3.3.2-3 Example of Shutdown Logic to which a Failure in Each Output Channel is Inputted

SEE ALSO

For more information about SYS_OUTST, refer to:

- C10.15, “SYS_OUTST (output module 8 channels indicator)” in Safety Control Station Reference (IM 32Q03B10-31E)
- C10.16, “SYS_OUTST16 (output module 16 channels indicator)” in Safety Control Station Reference (IM 32Q03B10-31E)

● **Shutdown due to a Failure in Important Input Channels**

The I/O parameter builder is available to create application logic for shutdown in case of a failure in important input channels. Specify the channel’s input value for a failure which invokes the shutdown demand. Additional application logic is not necessary.

When failure in an input channel is expected, after multiplexing inputs, use the Voter FB including BOOLVOTER, to create application logic.

■ **Shutdown When All Input Channels Fail**

The SYS_INST FB or SYS_CHST FB is available to create application logic to execute shutdown when all multiplexed input channels fail.

For this type of application logic, the channel’s input value for a failure needs to be specified as a value that keeps the channel’s NORMAL status in order to avoid shutdown due to only one input channel failure.

● **Shutdown When All Input Channels Fail**

There are two methods of creating this type of application logic.

One is implementing all multiplexed inputs on one input module with the other channels kept unused. This method detects the failures of all channels with simple logic using the SYS_INST FB.

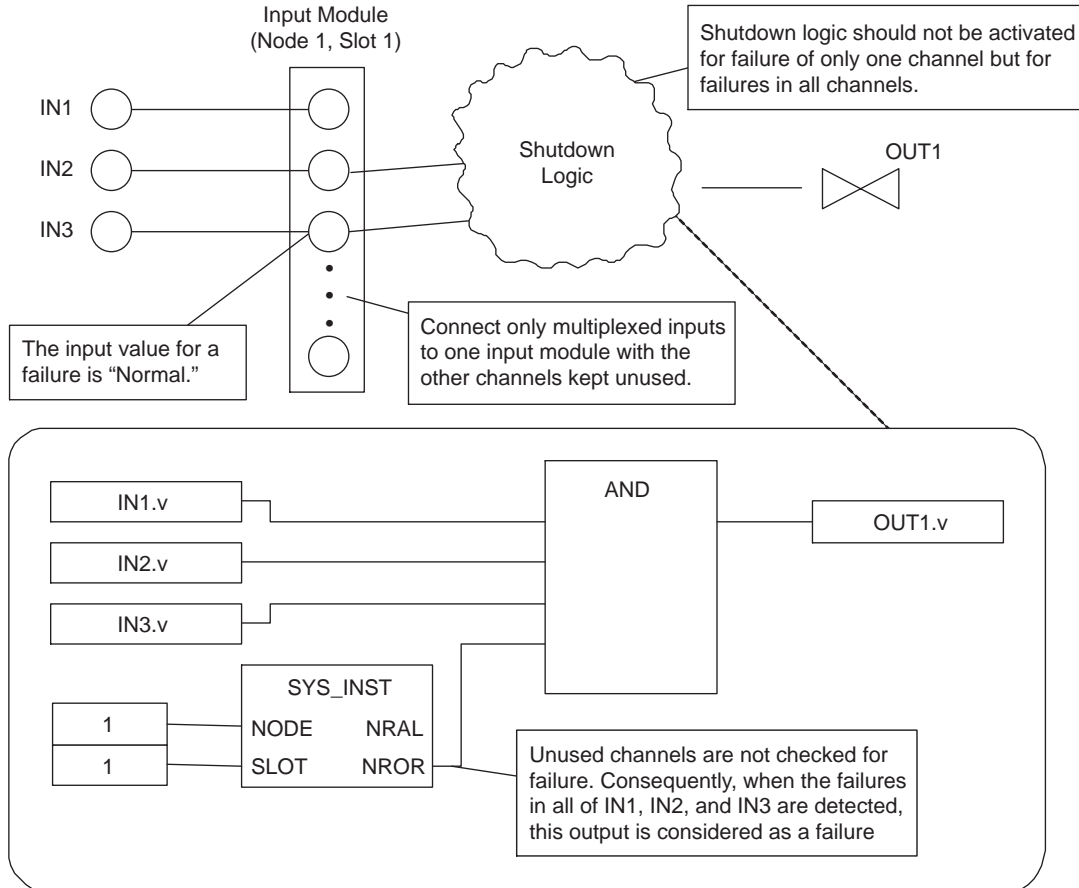


Figure 3.3.2-4 Example of Application to Execute Shutdown when All Input Channels Fail 1

The other method is implementing several multiplexed inputs on separate input modules. The advantages of this method are easier maintenance of modules and resistance to module failures. However, the logic is more complex than Example 1. This case needs an AND operation after detecting the failure status of all channels by using SYS_CHST.

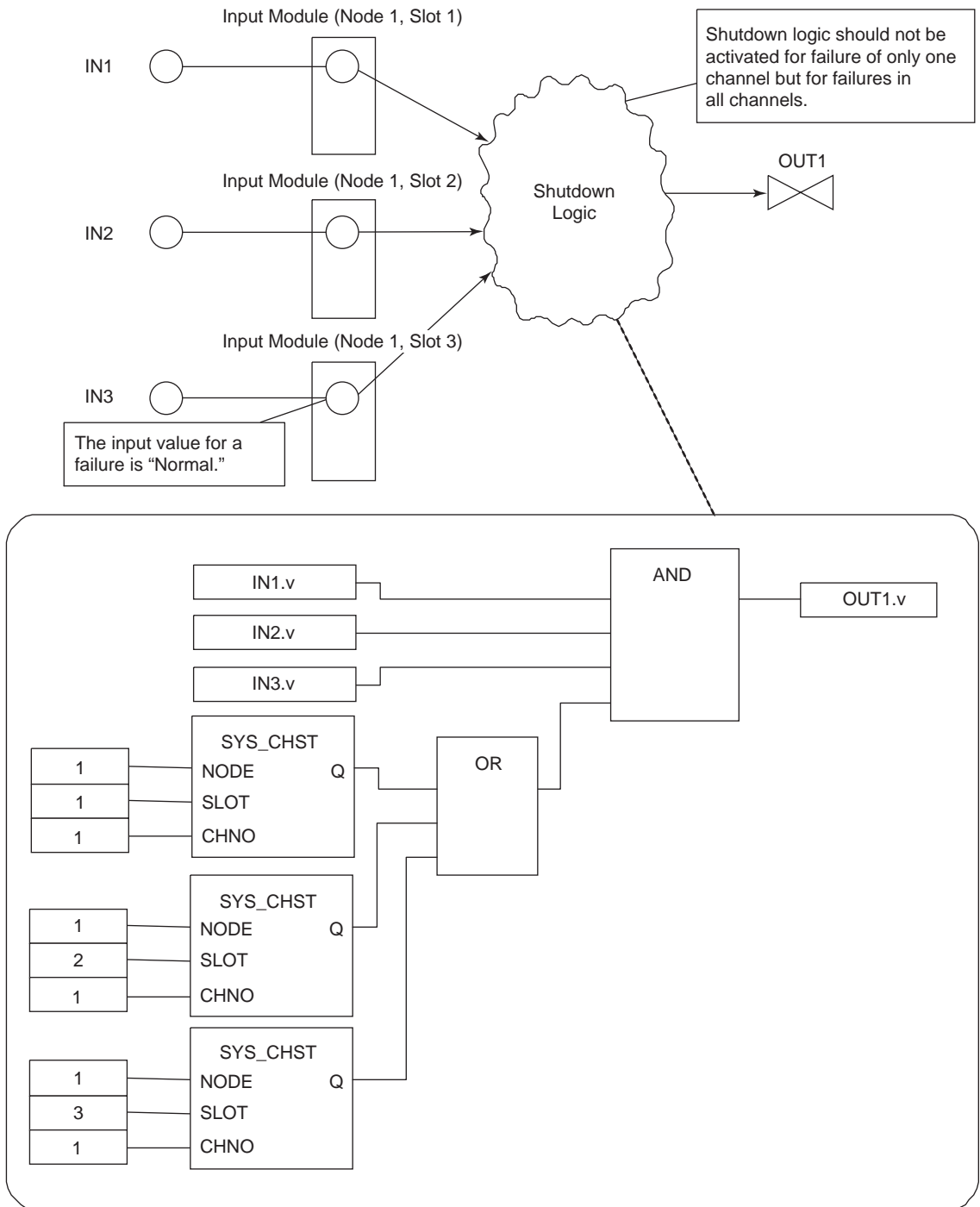


Figure 3.3.2-5 Example of Application to Execute Shutdown when All Input Channels Fail 2

SEE ALSO

For more information about SYS_INST, refer to:

C10.17, "SYS_INST (input module status indicator)" in Safety Control Station Reference (IM 32Q03B10-31E)

For more information about SYS_CHST, refer to:

C10.18, "SYS_CHST (channel status indicator)" in Safety Control Station Reference (IM 32Q03B10-31E)

3.3.3 Example of Displaying I/O Status

This section provides an example of displaying I/O module status using function blocks.

TIP This type of application is rarely needed to be created because I/O status is displayed on SENG.

■ Example of Displaying I/O Operating Status

The SYS_DIAG FB or SYS_IOMDSP FB is available if I/O operating status needs to be indicated on an external display.

To detect a failure in a whole SCS, the SYS_DIAG is available.

To display the status of individual modules, the SYS_IOMDSP is used. One function block is needed to display the status of one module.

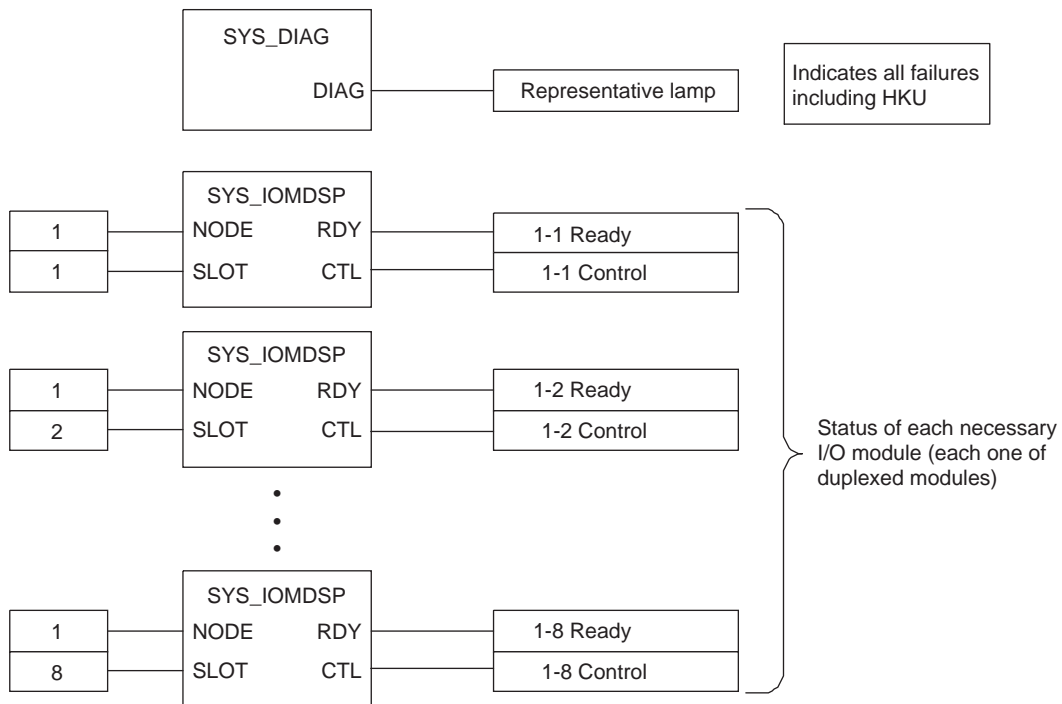


Figure 3.3.3-1 Example of Displaying I/O Operating Status

SEE ALSO For more information about SYS_DIAG, refer to:

C10.6, “SYS_DIAG (diagnostic information output)” in Safety Control Station Reference (IM 32Q03B10-31E)

For more information about SYS_IOMDSP, refer to:

C11.8, “SYS_IOMDSP (IOM status indicator)” in Safety Control Station Reference (IM 32Q03B10-31E)

3.3.4 Relations among AIO/DIO, Communication Module and System FBs

This section describes the relationship between AIO/DIO modules that can be used in SCSs, communication modules and system function blocks. “Related” in this context refers to cases where an output value of an FB is changed if an error occurs in a module or data, or the data output to a module changes depending on the operation of the FB.

Table 3.3.4-1 Safety FBs

	Input module (*1)	Output module (*1)	Subsystem communication module (communication input/output data) (*1)	Modbus Slave communication module (*2)
SYS_STAT	No	Yes	No (Related: SYS_STAT_SC)	No
SYS_FORCE	Yes	Yes	No (Related: SYS_FORCE_SC)	No
SYS_DIAG (*3)	Yes	Yes	Yes	Yes
SYS_IOALLST (*4)	Yes	Yes	No	No
SYS_NODEST (*4)	Yes	Yes	No	No
SYS_OUTST (*4)	No	Yes	No	No
SYS_OUTST16	No	Yes	No	No
SYS_INST (*4)	Yes	No	No	No
SYS_CHST (*4)	Yes	Yes	No	No
SYS_ALLSD	No	Yes	No	No
SYS_IOMSD	No	Yes	No	No

*1: Yes: Related
 No: Not related

*2: Yes: Related
 The Modbus slave communication function refers to and sets data in an SCS. It does not store any data of its own. Functions related to them are thus not necessary for the Modbus slave communication modules themselves.

*3: If a failure or data error occurs, the output parameter IOER is set to TRUE.

*4: When errors occurred in the communication route between CPU and I/O modules (except for the error occurred in one of the redundant ESB buses with that routed properly), the output becomes FALSE.

Table 3.3.4-2 Interference-free FBs

	Input module (*1)	Output module (*1)	Subsystem communication module (communication input/output data) (*1)	Modbus slave communication module (*1)
SYS_IOMDSP (*2)	Yes	Yes	Yes	Yes
SYS_ALRDSP (*2)	No	No	Yes	No (*3)
SYS_STAT_SC	No	No (Related: SYS_STAT_SC)	Yes	No (*3)
SYS_FORCE_SC	No (Related: SYS_FORCE)	No (Related: SYS_FORCE)	Yes	No (*3)

*1: Yes: Related
 No: Not related

*2: When errors occurred in the communication route between CPU and I/O modules (except for the error occurred in one of the redundant ESB buses with that routed properly), the output of the I/O modules will hold the previous output values.

*3: The Modbus slave communication function refers to and sets data in an SCS. It does not store any data of its own. Functions related to them are thus not necessary for the Modbus slave communication modules themselves.

3.3.5 Example of Using Bool-type Data Manual Operation Function Block (MOB_*)

The Bool-type Data Manual Operation Function Block with Answerback (MOB_11/MOB_21) allows you to manipulate valve(s) using switch-type face plate from HIS.

In addition to allowing switch operation from HIS, these function blocks are capable of outputting a shutdown instruction immediately regardless of the manipulated output value from the HIS if a shutdown event occurs. They also have the function to check the answerback input against the manipulated command value, security password function, manual operation enabling function and so on. The manual operation of MOB_11/MOB_21 from HIS can be used for manipulating valves at the startup of a plant or for testing the behavior of devices when you perform maintenance work. Note that when you manually operate MOB_11/MOB_21, entry of password is always required.

The Auto-Reset Bool-type Data Manual Operation FB (MOB_RS) allows a CENTUM HIS to output pulse status. This FB is used to reset from the shutdown status or to reset alarms.

SEE ALSO

For more information about Bool-type Data Manual Operation FB, refer to:

C5., "Function blocks for integration with CENTUM (Safety FBs)" in Safety Control Station Reference (IM 32Q03B10-31E)

■ Example of Using Bool-Type Data Manual Operation FB (MOB_21)

This is an example where the MOB_21 FB is used under the following conditions:

- During the start-up of the plant.
- Shutdown of the SCS occurred and the cause of the shutdown has been cleared.
- The valve is opened one by one using manual operation from HIS.

This example is applicable if a shutdown event is the only criterion to disable manual operation, and if manual operation is enabled whenever the shutdown event is solved.

For DTS, SHDN is connected to signals from the shutdown logic, SS to FALSE.

To enable the manual operation immediately after the shutdown event is solved, connect TRUE to SW. If the SW is always TRUE, the value of IN never be referenced, so set any value to IN.

Since the shutdown signal has higher priority, when the input value of SHDN becomes FALSE, the manual operation becomes disabled even if the SW is always TRUE.

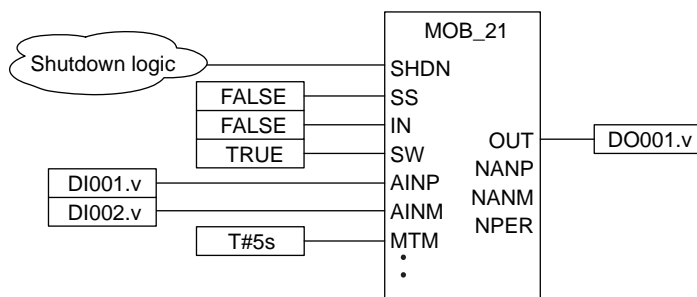


Figure 3.3.5-1 Example of Using Bool-Type Data Manual Operation FB (MOB_21)

The above figure is an example of DTS. For ETS, set the SS input to TRUE.

■ Example of Valve with only Full Close Limit Switch

For manipulating the valve with only Full Close Limit Switch, use the Bool-type Data Manual Operation with Two-Position Answerback (MOB_11) and enter an inverted Full Close Limit Switch signal into AIN.

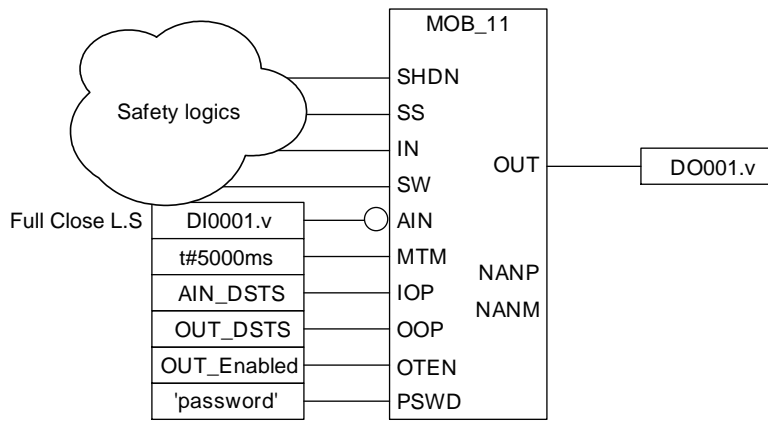


Figure 3.3.5-2 For Valve with only Full Close Limit Switch

■ Example of manipulating Two-Position Analog Valve

Connect analog signal to SCS. To allow an HIS to manipulate an analog valve having only two statuses, Full Open and Full Close, configure the loop as shown in the following figure.

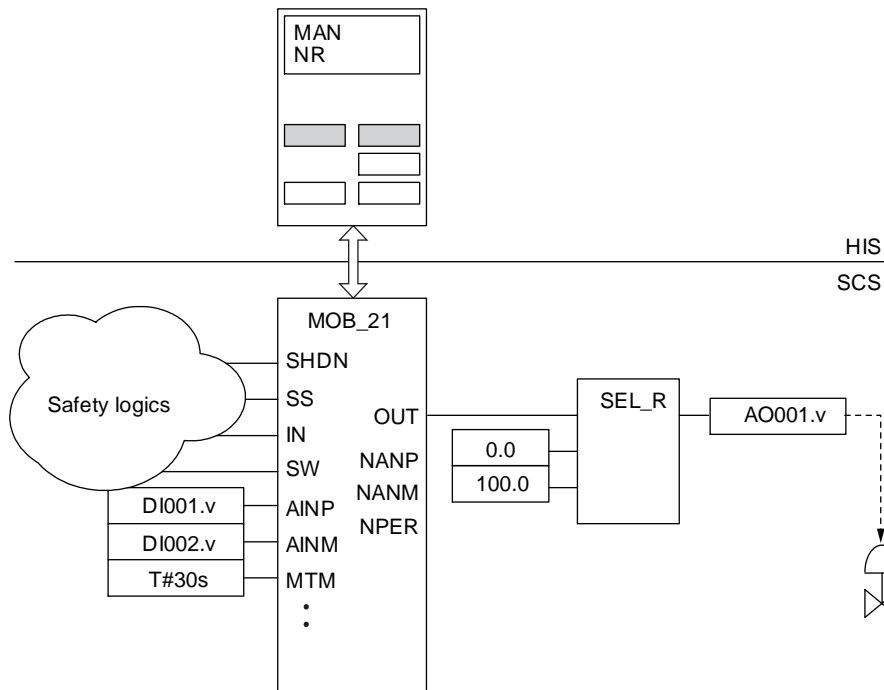


Figure 3.3.5-3 For Manipulating Two-Position Analog Valve

■ Example of No Answerback Check

If Answerback check is not required, looping back the output value to Answerback input disables the Answerback check function. In this case, PV can be used for checking (visually) operations from CENTUM.

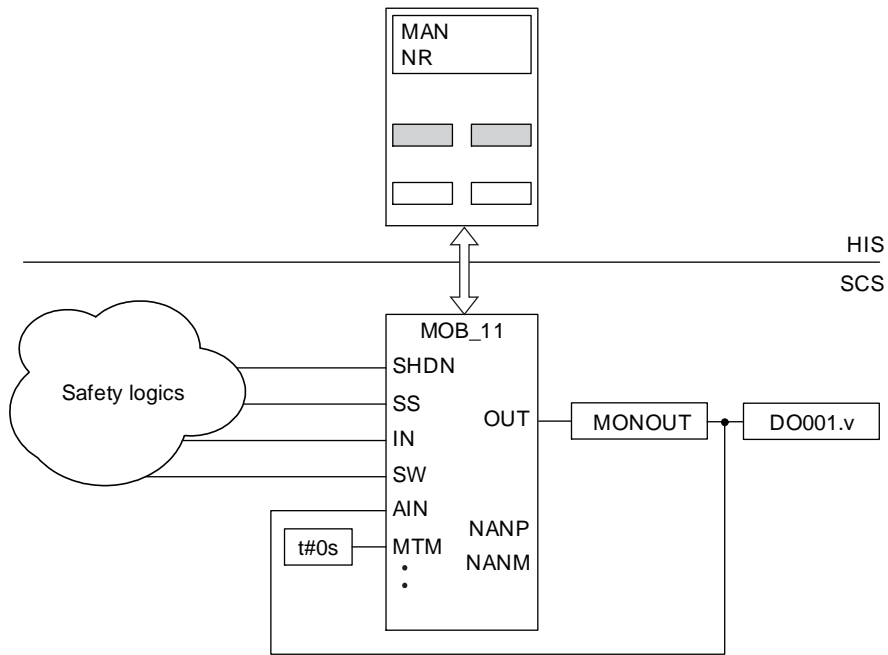


Figure 3.3.5-4 Case where No Answerback Check Required

3.3.6 Construction Example of First-up Alarm Function

In ESD applications and similar, even if the system is shut down due to a certain cause, it might lead to other shutdown causes immediately or multiple shutdown-causing factors may mutually interact in the application logic. As a result, it is not always possible to identify the first cause.

The first-up function allows you to identify the event (factor) that was generated first among grouped events.

■ Overview of First-up Alarm Function and Application Examples

The first-up alarm function is constructed by combining First-up Alarm Annunciator (ANN_FUP) and First-up Alarm Annunciator Reset (FUR_RST). A First-up Alarm Annunciator (ANN_FUP) allows identifying and outputting events that occurred first and second among grouped events. If a CENTUM HIS is connected, an annunciator message is output for the event that occurred first. A First-up Alarm Annunciator Reset (FUP_RST) is used to reset the first-up alarm status of ANN_FUP.

An example of constructing the first-up alarm function using these FBs is shown below.

● Example of First-up Alarm and Outputting Failure of Rest Operation to HIS

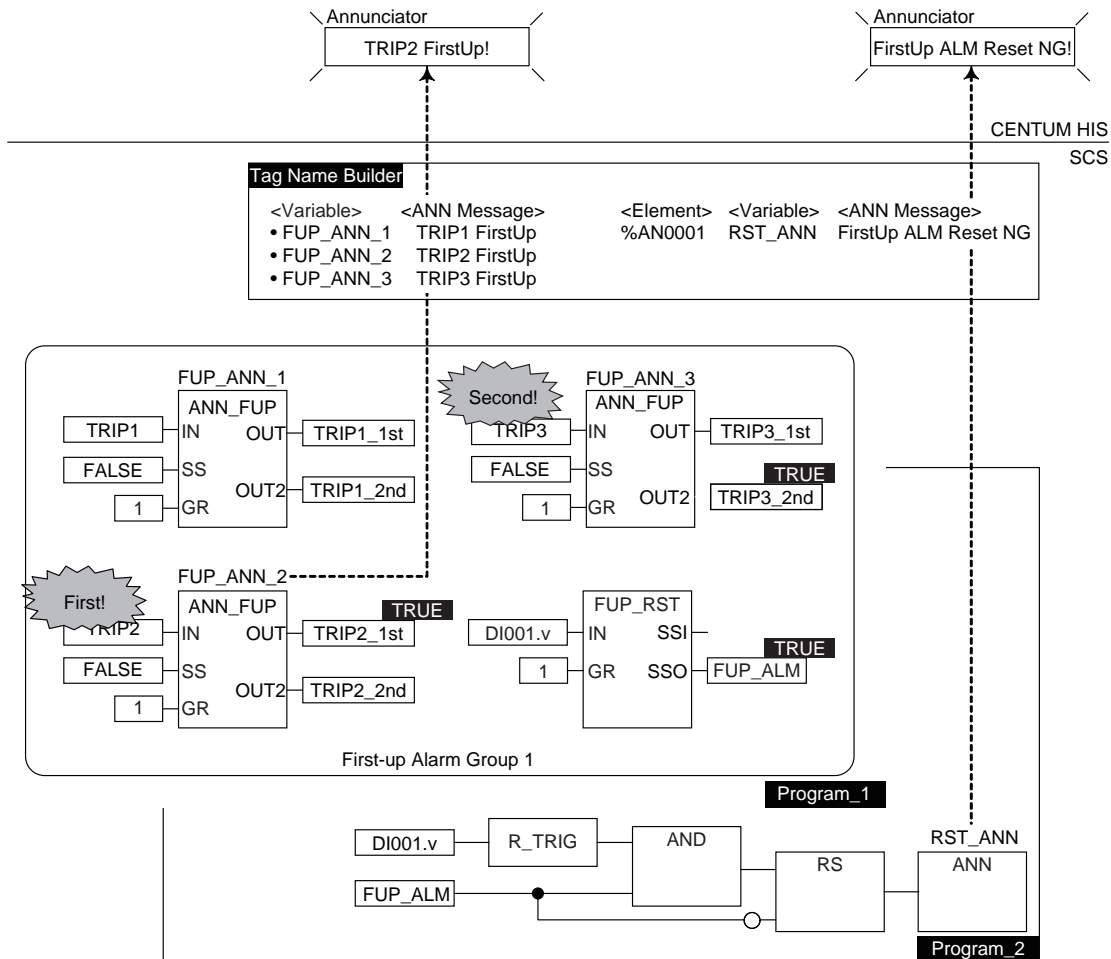


Figure 3.3.6-1 Application of Detecting First-up Alarm

Program_1 inputs events TRIP1, TRIP2, and TRIP3 to their respective ANN_FUPs and set them as First-up alarm group 1. Each ANN_FUP is assigned an instance name. A DI signal DI001, which is operated by a hardware console, etc. and input to SCS for alarm reset, is input to FUP_RST.

Program_2 creates logic to check if the first-up alarm status is cancelled when alarm reset operation is performed.

Annunciator messages corresponding to each instance shall be defined in the Tag Name Builder.

In the example above, events are generated in the order of TRIP2, TRIP3, and then TRIP1. In this case, OUT (TRIP2_1st) of the instance name FUP_ANN_2 and OUT2 (TRIP3_2nd) of FUP_ANN_3 become TRUE and the annunciator message for the first-up alarm (annunciator message of FUP_ANN_2) is output to HIS. When the first-up alarm is generated, SSO (FUP_ALM) of FUP_RST becomes TRUE. In the status where FUP_ALM is TRUE, the first-up alarm status is not cancelled even if the alarm reset signal (DI001) is received. In such cases, an annunciator message notifying that the alarm reset operation failed is output. Since ANN_FUP does not have SOE functions, connect SOE FB as required.

4. Test of Application

This section describes the procedure for testing applications.

4.1 Types of Test

The test function of ProSafe-RS is for debugging applications efficiently when a new application is created or an existing application is modified.

The tests consist of three tests. They are target test, SCS simulation test and logic simulation test.

Table 4.1-1 Types of Test

Types of Test	Description
Target Test	Tests applications on actual SCS.
SCS Simulation Test	Tests applications using the SCS simulator. SCS simulator is a program to simulate SCS actions on a PC. Moreover, during the SCS simulation test, the SCS simulator and virtual HIS on a PC are performed without connecting the control bus.
Logic Simulation Test	Tests performed on the applications using the logic simulator. Logic simulator is a program to simulate logic actions of POU's on a PC.

The following figure illustrates the examined ranges of each test type.

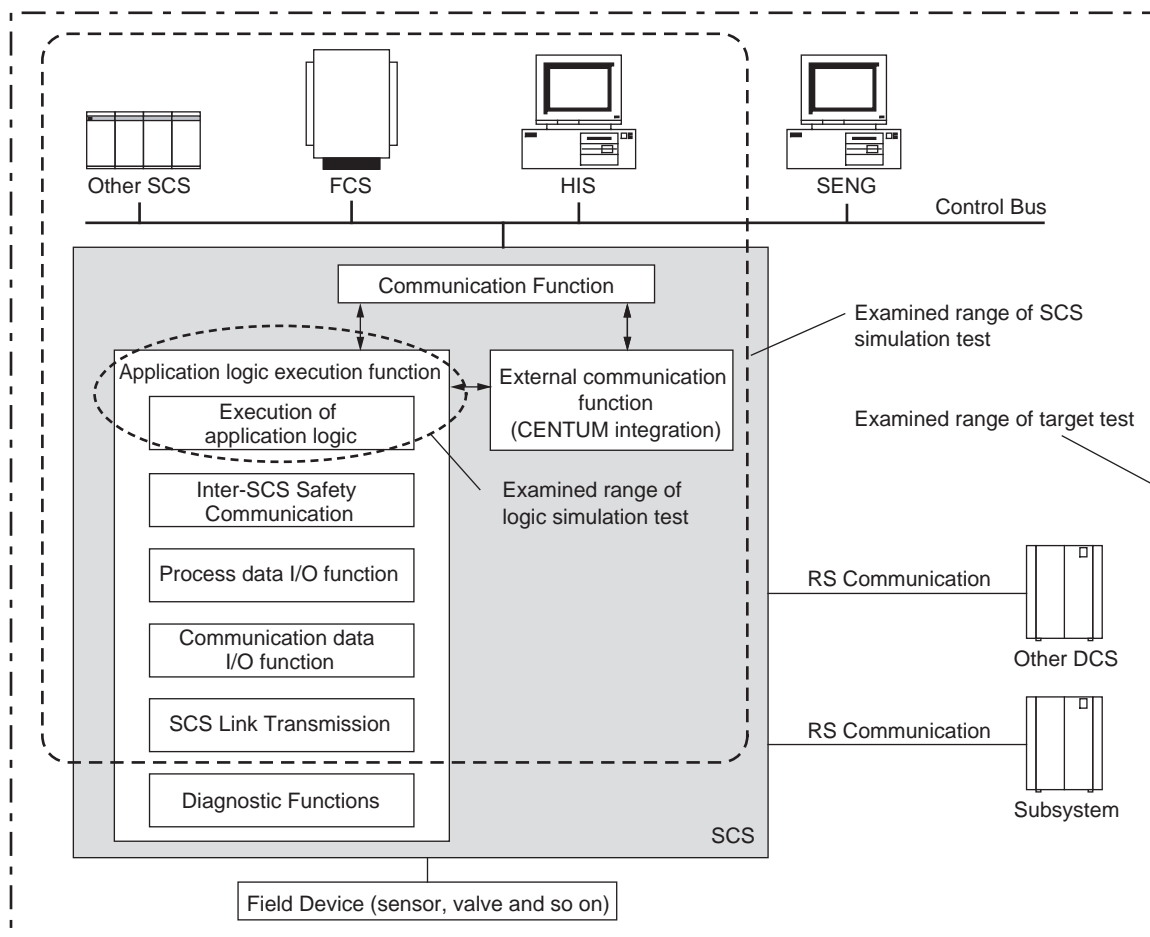


Figure 4.1-1 Examined Range of the Test

The items that can be examined only by target test are shown as follows:

The final stage of a comprehensive test must be conducted by target test using actual SCS.

Table 4.1-2 Examined Range of Target Test

Items	Examination
Performance	CPU load, communication load, network load, demand reaction time and so on.
Field Device and Field Communication	Validation of the communication paths between field devices and I/O modules.
Communication with other vendor DCS or subsystem	Modbus communication
HART Communication	HART Communication
Inter-SCS Safety Communication (For abnormal cases)	Communication behavior when the communication target SCS encounters abnormalities.
SCS Link Transmission (For abnormal cases)	Communication behavior when the communication target SCS encounters abnormalities.
Applications that is connected to the System Function Blocks	System function blocks for indicating the abnormalities. When examine the logics without using the internal variables, target test becomes necessary.
Hardware	CPU, I/O modules, communication bus, control bus, power supplies and so on under both normal and abnormal situations.

The test support tools are listed in the following table. The test supporting tools can be used not only for debugging the applications but also for plant maintenance and monitoring.

Table 4.1-3 Test Support Tools

Tool	Description
Forcing Function	Function that fixes the variable data and changes the value. Forcing function can be used for online changing of applications and maintenance of devices.
Application Debug Function	Changes the behavior of application logics for debugging.
Online Monitoring Function	Displays values of variables on the SCS Manager.

■ Outline of Test Function

The following table shows the executable test functions for various SCS security levels:

Table 4.1-4 Test Modes and SCS Security Levels

Test Function		Logic Simulation Test (*1)	Target Test, SCS Simulation Test (*1)			
			Online		Offline	
Security Level		Irrelevant	Level2	Level1	Level0	
Application Debug Function		Yes	No	No	Yes	
<ul style="list-style-type: none"> • Specifies Running Mode (Real Time /Cyclic) • Specifies Cycle Time • Uses Breakpoint, Step Execution (*2) 						
Forcing Function	Lock	Variable (*3)	Yes	No	Yes	Yes
		Module (*3)	Yes	No	Yes	Yes
	Unlock	Variable (*3)	Yes	No	Yes	Yes
		Module (*3)	Yes	No	Yes	Yes
	Variable Setting	Variable	Yes	No	Yes	Yes
Online Monitoring Function		Yes	Yes	Yes	Yes	Yes

*1: Yes: Operation is available

- No: Operation is unavailable
- *2: The tests using breakpoints or steps is available for the LD and ST applications only.
- *3: Operation is available but the statuses of all the channels of an I/O module during an SCS simulation test and a logic simulation test are equivalent to being locked all the time.

The following table lists the differences between operation of the SCS simulator, the logic simulator and the actual SCS.

Table 4.1-5 Differences between SCS Simulator/Logic Simulator and Actual SCS

Types	Items	SCS simulator	Logic simulator
Scan Period	Execution Timing of Applications	Application logic can only run at 1 second scan period even if the application logic scan period is specified with a scan faster than 1 second from SCS Manager.	Same as SCS target
	Execution Timing of External Communication Function	Runs at 1 second period regardless the setting on builder.	N/A
I/O function	I/O	<ul style="list-style-type: none"> No communication with I/O modules Initial data status is GOOD. 	<ul style="list-style-type: none"> No communication with I/O modules Initial data status is GOOD.
	Subsystem Communication	<ul style="list-style-type: none"> No communication with I/O modules Initial data status is GOOD. 	<ul style="list-style-type: none"> No communication with I/O modules Initial data status is GOOD.
	Modbus Slave	N/A	N/A
	HART Communication	No communication	No communication

Continues on the next page

Table 4.1-5 Differences between SCS Simulator/Logic Simulator and Actual SCS (Table continued)

Types	Items	SCS simulator	Logic simulator
POU	TON, TOF, TP, VEL, ANLG_S, REPEATTIMER, ANLG1OO2D, ANLGVOTER, MOB_11, MOB_21, MOB_RS, SYS_FORCE, SYS_FORCE_SC, SYS_SECURE, SYS_OVR, SYS_PSWD	The scan period is fixed at 1 second. So, if the POU is specified with a scan period faster than 1 second, the time until time-up occurs will be prolonged. For example, if the time-up of a TIME type input parameter is 5 seconds under the condition of 200 ms scan period, the time-up will take 25 seconds under 1 second scan period.	Same as SCS target
	CTU, CTD, CTUD, FILTER, FILTER_S	The outputs of these FBs are determined by the number of executions, and are updated 5 times per second in the actual SCS if the scan period is 200 ms. However, they are updated only once per second in the SCS simulator.	Same as SCS target
	SYS_ALLSD, SYS_IOSD	Same as SCS target	N/A
	SYS_NETST, SYS_ESBINF, SYS_NODEINF, SYS_IOMDSP, SYS_ALRDSP	Always indicates normal.	Always indicates normal.
	SYS_DIAG	Diagnosis for hardware always indicates normal.	Diagnosis for hardware always indicates normal.
	SYS_SCAN	CPU idle time always indicates 0%. Execution time equals to the application logic scan period.	CPU idle time or execution time always indicates 0%.
	SYS_SCANEXT	A fixed value is always output because the automatic scan period extension function is not active.	The automatic scan period extension function is inactive. The scan period specified by the Resource Properties is output to ESCA and OSCA.
	SYS_CERR	Floating point overflow cannot be detected.	The abnormal calculation detection function is disabled. FALSE is output for all.
SYS_SETTIME	SUC or FAL is output at the rising edge of IN, but the time is not set.	SUC or FAL is output at the rising edge of IN, but the time is not set.	
Inter-SCS safety communication	Binding	<ul style="list-style-type: none"> If another SCS simulator is running as the communication partner SCS, the SCS link transmission safety communication can be performed as same as the actual SCS. However, the diagnoses for reception interval time out value (OUTT) and transmission delay time out value (DLYT) are not performed. If the SCS simulator is not running as the communication partner SCS, the communication error will occur. Once SCS simulators communicate normally, if the partner SCS simulator stops, no error is issued. 	N/A

Continues on the next page

Table 4.1-5 Differences between SCS Simulator/Logic Simulator and Actual SCS (Table continued)

Types	Items	SCS simulator	Logic simulator
SCS Link Transmission	SCS Link Transmission Safety Communication	<ul style="list-style-type: none"> If another SCS simulator is running as the communication partner SCS, the SCS link transmission safety communication can be performed as same as the actual SCS. However, the diagnoses for reception interval time out value (OUTT) and transmission delay time out value (DLYT) are not performed. If the SCS simulator is not running as the communication partner SCS, the communication error will occur. Once SCS simulators communicate normally, if the partner SCS simulator stops, no error is issued. 	N/A
	SCS Global Switch Communication	<ul style="list-style-type: none"> If another FCS simulator is running as the communication partner FCS, the SCS global switch communication can be performed as same as the actual SCS. If the communication partner does not exist, it will indicate error as same as the actual SCS. 	N/A
Security	SCS Security Level	Security level will be 0 right after starting simulator. It can be changed to level 2 without stopping the simulator from SCS Manager.	N/A
	Security Password	When the simulator is launched, the security password is cleared.	N/A
Diagnosis	SCS Self-diagnostic	N/A	N/A
	Hardware Diagnosis	Simulated as always "Normal."	N/A
	HKU	Simulated as always "Normal."	N/A
System	Starting Output Module	Operation fails	Operation fails
	Switching between Redundantly Paired AIO/DIO Modules	N/A	N/A
	System Report	Operation fails	Operation fails
	IOM Download	Operation fails	Operation fails
	Restart of SCS	Operation fails	Operation fails
	Master database offline download to SCS	Operation fails	Operation fails
SOE	At SCS Starting	The events before shutdown will not be restored.	N/A
	Event	Events from DI modules are not collected.	N/A
Diagnostic Information	At SCS Starting	The diagnostic information before shutdown will not be restored.	N/A
%SW	System Switch	Switches for indicating the hardware statuses always show normal.	N/A

Continues on the next page

Table 4.1-5 Differences between SCS Simulator/Logic Simulator and Actual SCS (Table continued)

Types	Items	SCS simulator	Logic simulator
Others	Floating-point Computation	The calculation accuracy may vary with CPU types.	The calculation accuracy may vary with CPU types.
		When overflow occurs, the actual SCS will stop, while SCS simulator will not stop but show the calculation results as infinities.	When overflow occurs, the actual SCS will stop, while logic simulator will not stop but show the calculation results as infinities.
	Performance	CPU idle time will be indicated as 0 second, and execution time will be indicated as 100%.	N/A
	Time synchronization	No time synchronization among the PCs. Time synchronization status always shows normal. For Vnet/IP, a display meaning "sync with Vnet/IP time" is shown.	N/A

4.2 SCS Simulation Test

As the following shows, SCS simulation tests can be used for a wider range of tests than logic simulation tests.

- Because communication with the CENTUM VP virtual HIS is possible, a wide range of application operations, such as override function blocks and manual operation function blocks, can be tested. It is not possible to execute an SCS simulation test in the case of integration with a CS 3000.
- Since multiple SCS simulators can run simultaneously so that the tests for the inter-SCS safety communication and SCS link transmission can be performed.
- Since SCS simulator and FCS simulator can run simultaneously, the combination test of the two can be performed.
- Application debugging, forcing and online monitoring can be utilized as for SCS target tests.
- The SCS security levels and the range that can be changed during online maintenance are the same as the SCS target test.
- In order to run the SCS simulation test, the project data is required for the SCS simulator.

■ Components

The software components in the PC required for the SCS simulation test are illustrated as follows:

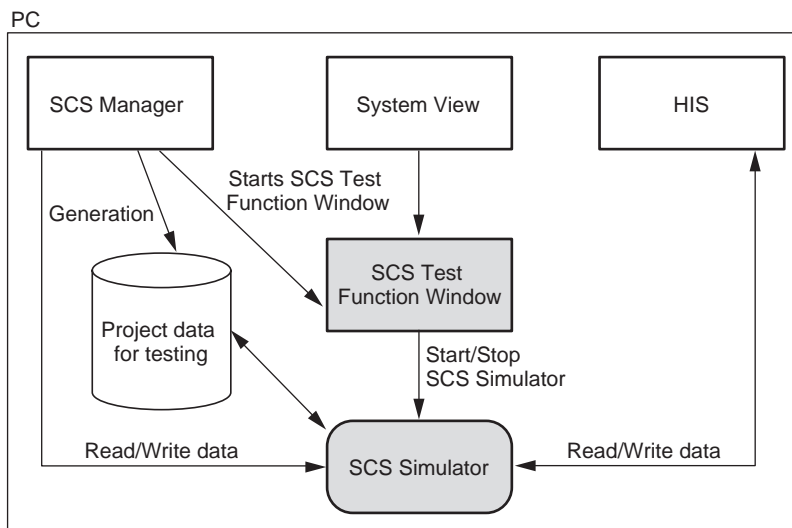


Figure 4.2-1 Software Components for SCS Simulation Test

Table 4.2-1 Software Components for SCS Simulation Test

Components	Functions in SCS Simulation Test
SCS Manager	<ul style="list-style-type: none"> • Produces SCS project data for test. • Starts SCS Test Function window. • Interfaces for forcing or application debugging tools. • Monitors for application logics. • Interfaces for changing applications of ProSafe-RS
SCS Simulator	Simulates SCS actions.
SCS Test Function Window	Starts or stops SCS simulator

Continues on the next page

Table 4.2-1 Software Components for SCS Simulation Test (Table continued)

Components	Functions in SCS Simulation Test
System View	<ul style="list-style-type: none"> Starts virtual HIS Starts SCS Test Function window Starts FCS Test Function window Interfaces for changing applications of CENTUM VP.
HIS	Interfaces for operation and monitoring
Project database	The project database for SCS simulation test.

SEE ALSO

For more information about the software components for SCS simulation test, refer to:

1.3, "Hardware/software environment" in [ProSafe-RS System Test Reference \(IM 32Q04B30-31E\)](#)

● **Regarding a Stand-Alone System**

The SCS simulator cooperates with the CENTUM VP system, and so requires CENTUM VP system configuration. Therefore, you cannot execute SCS simulation test in a stand-alone system which consists of only SCSs and SENGs.

■ **Start and Exit SCS Simulation Test**

A user can start SCS Test Function window from the SCS Manager or the System View. When the Test Function window is started, the SCS simulator for simulating the SCS actions on a PC will also be started. SCS simulator status can be checked from the SCS Maintenance Support Tool in an SENG or from HIS (virtual HIS).

When closing the SCS Test Function windows, the SCS simulator will also be terminated.

● **SCS Test Function Window**

SCS Test Function window is managing SCS simulator. The SCS simulator can be stopped or restarted from the SCS Test Function window.

- As long as an SCS Test Function window is opened, the SCS simulator can be stopped or restarted for as many times as you want.
- One SCS Test Function window is only for one SCS simulator. When an SCS simulator is started from one SCS Test Function window, if you want to start another SCS simulator, you need to open a new SCS Test Function window.
- Multiple SCS Test Function windows cannot be started for one station at the same time.
- SCS Test Function windows for different CENTUM VP projects cannot be started at the same time.
- SCS simulator cannot communicate with the actual SCS, therefore, a combination test of SCS simulator and SCS target cannot be performed.

● **Setting Data Values**

When SCS simulator is started, data values and data statuses of all variables are set to the initial values and statuses. The values and statuses can be defined after locking them.

Table 4.2-2 Setting Data Procedure

Type	Procedure
I/O Variable	<ul style="list-style-type: none"> Lock the variable on I/O Lock Window Set the data values and statuses on I/O Lock Window.
Communication I/O data	<ul style="list-style-type: none"> Lock the I/O variable on Communication I/O Lock Window Set the data values and statuses on Communication I/O Lock Window.

Continues on the next page

Table 4.2-2 Setting Data Procedure (Table continued)

Type	Procedure
Inter-SCS safety communication	If the SCS simulator of the sender SCS is not running, the internal variables connected to the Consumer function block should be locked and set with new values same as for the actual SCS.
SCS Link Transmission	<ul style="list-style-type: none"> If the SCS or FCS simulator of the sender does not exist, on the SCS Link Transmission Lock Window to lock the SCS link transmission data of receiver SCS. Set the initial data values and statuses in the same window.
Operation Marks	Download the operation marks same as for the actual SCS.

● **Output Enable Operation**

After the SCS simulator is started, output is disabled. This is the same behavior as the actual SCS. Outputs need to be enabled on the I/O channel status dialog box of the SCS Maintenance Support Tool. When they are enabled, the data sending through the inter-SCS safety communication and the SCS link transmission will start.

■ **Expanded SCS Simulation Test**

● **FCS Simulator and SCS Simulator are Testing Together**

SCS simulation test can be performed using multiple SCS simulators so that the inter-SCS safety communication and the SCS link transmission safety communication can be tested. Moreover, by starting FCS simulator at the same time, testing for the applications using the global switches, ADL, SEBOL and other data exchanged with FCS can be performed.

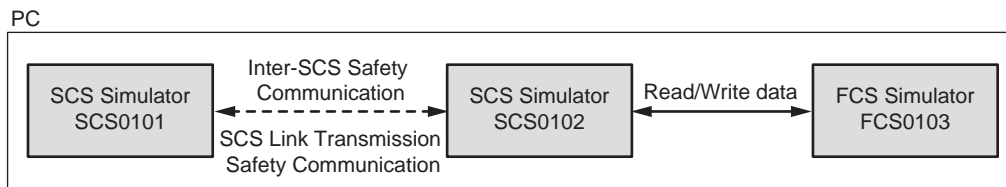


Figure 4.2-2 Testing with Multiple Simulators

● **Tests Using Expanded Test Functions with Multiple PCs**

As with CENTUM VP virtual test, SCS simulation test can be performed on multiple SCS simulators running on multiple PCs using expanded test functions.

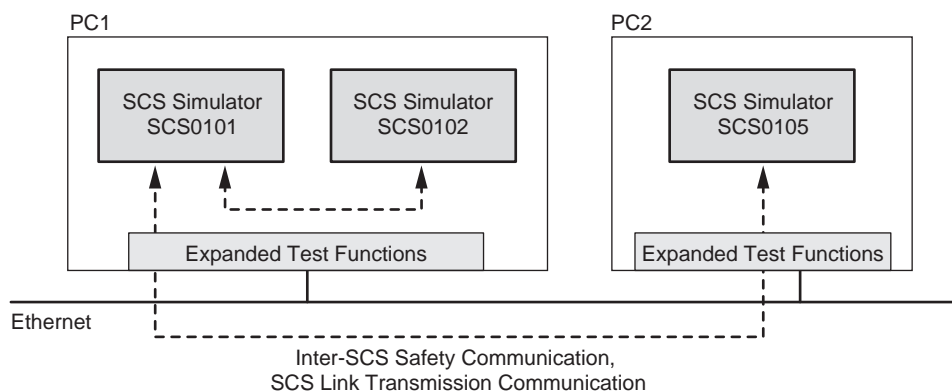


Figure 4.2-3 Test Using Multiple Simulators on Multiple PCs

● **Communicate with Started SCS Simulator from Another SENG**

From an SENG, if you want to monitor the SCS simulator that is running on another SENG PC, you need to start the virtual HIS on the monitoring PC.

SEE ALSO For more information about starting virtual HIS, refer to:

3.4, "Expanded test functions" in ProSafe-RS System Test Reference (IM 32Q04B30-31E)

Capacity

The SCS simulation test capacities are shown as follows. However, the performances are not guaranteed.

- Number of simulators can be started in one PC: Max. 8 (Including both SCS simulators and FCS simulators)
The maximum number of simulators that can be started at the same time is also dependent on the CPU performance of the PC and the load of other software applications in the PC.
- Number of SCS/FCS simulators that can communicate using Expanded Test Functions: Maximum 128 (when integrated with CENTUM VP R4.01.60 or later) (*1)
- Number of connectable HIS stations when Expanded Test Functions are used: Max. 32
- Number of domains when Expanded Test Functions are used: Maximum 8 (when integrated with CENTUM VP R4.01.60 or later)
- Number of connectable PCs when Expanded Test Functions are used: Max. 48 (*2)

*1: When used with FCS simulator, the total number of SCS and FCS simulators should not exceed the maximum number.

*2: PCs installed with the Exaopc OPC Interface Package are included.

- The maximum number of SCS/FCS simulators that can be started from a SENG that is assigned licenses for the CENTUM VP's Standard Builder Functions, Test Functions, and Expanded Test Functions packages is 40. This maximum assumes the case where only the test function-related software is running on the PC. When other software is running, you can start fewer simulators. The following table shows the relation between the Windows OS type and the versions of CENTUM VP that can be integrated.

Table 4.2-3 Windows OS Type and Connectable Versions of CENTUM VP

OS	CENTUM VP version
Windows 7 Professional	Only usable when integrated with CENTUM VP R5.01.00 or later.
Windows Vista Business Edition	Only usable when integrated with CENTUM VP R4.01.60 or later.
Windows Server 2008 R2	Only usable when integrated with CENTUM VP R5.01.00 or later.
Windows Server 2008	Only usable when integrated with CENTUM VP R4.02.00 or later.

SEE ALSO For more information about the configuration of PCs and the number of SCS/FCS simulators that can be started when Expanded Test Functions are used in a large-scale system if integrated with CENTUM VP, refer to:

Models LHS5425, LHS5426, LHS5427: Expanded Test Functions, FCS Simulator Package, HIS Simulator Package (GS 33M10D60-40E)

SCS Project Attributes

The following table shows the relationship between SCS project attributes and various tests.

Table 4.2-4 SCS Project Attributes and Various Tests

SCS Project Attributes	Target Test (*1)	SCS Simulation Test (*1)	Logic Simulation Test (*1)
Default Project	No	Yes (*2)	Yes

Continues on the next page

Table 4.2-4 SCS Project Attributes and Various Tests (Table continued)

SCS Project Attributes	Target Test (*1)	SCS Simulation Test (*1)	Logic Simulation Test (*1)
Current Project	Yes	No	Yes
User-defined Project	No	Yes (*2)	Yes

*1: Yes: Available for test
 No: Not available for test

*2: Under the condition that the target name of the SCS Project is SCS_SIMULATOR.

The following table shows the combinations of SCS project attributes and CENTUM VP project attributes available for testing.

Table 4.2-5 Relationship between SCS Project Attributes and CENTUM VP Project Attributes

SCS Project	CENTUM VP Project		
	Default Project (*1)	Current Project (*1)	User-defined Project (*1)
Default Project	Yes	No	Yes
Current Project	No	Yes	No
User-defined Project	Yes	No	Yes

*1: Yes: Available for test
 No: Not available for test

● **Testing Newly Created Project**

When a new SCS project is created, the attribute of the newly created project is set as the Default project.

The SCS simulation test can be executed by executing the build for the project after the target name is changed from SCS_TARGET to SCS_SIMULATOR.

If you want to offline download the database to an actual SCS after simulation test is completed, you need to change the target name of the project from SCS_SIMULATOR to SCS_TARGET and then build the project again.

After offline downloading a database with the default project attribute, the attribute of the project becomes current project.

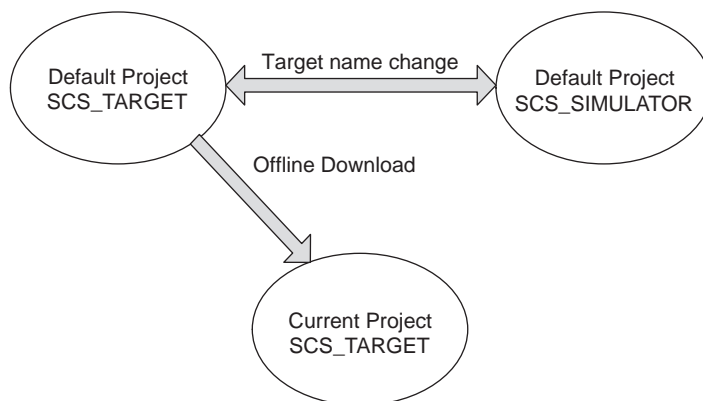


Figure 4.2-4 Testing Newly Created Project

● **Testing Modified Project**

In a current project, you cannot change the target name.

If you want to change the current project and perform SCS simulation tests on the change, you must create a user-defined project separately using the Test Project Creating Tool, change the user-defined project, and run build.

This user-defined project can be tested using SCS simulator.

After testing, the contents of the user-defined project can be imported to the current project using the import function.

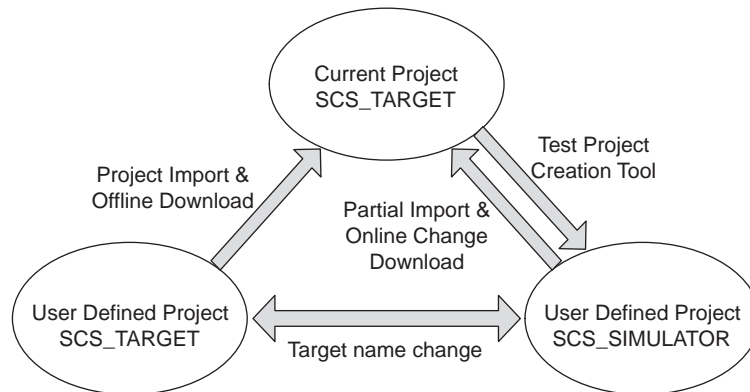


Figure 4.2-5 Testing Modified Project

■ Application Logic Execution Function

● Application Logic Actions

On SCS simulator, safety application logics are executed at the 1 second scan period even though the scan period specified on SCS Manager is faster than 1 second. Note that the action timings of application logics on the SCS simulator are different from the actual SCS.

- For the TIME type input parameters of standard function block such as TON or TOFF, it may take more time to reach timeup. The prolonged time is a multiplication of the scan period in the ratio of "1000/scan period (ms)." For example, if the original scan period is 200 ms, the specified 5 seconds for timeup (t#5s) will take 25 seconds to reach timeup on an SCS simulator.

Applicable FBs: TON, TOF, TP, VEL, ANLG_S, REPEATTIMER, ANLG1002D, ANLG-VOTER, MOB_11, MOB_21, MOB_RS, SYS_FORCE, SYS_FORCE_SC, SYS_FORCE_BD, SYS_SECURE, SYS_OVR, SYS_PSWD

- For the FB with counter outputs such as CTU or CTD, on the actual SCS it counts 5 counts per second under the condition of a 200 ms scan period. On SCS simulator, it counts only 1 count per second.

Applicable FBs: CTU, CTD, CTUD, FILTER, FILTER_S

The following figure shows the output NHTR from the ANLG_S and its equivalent logics using TON and CTU each to output NHTR_A and NHTR_B. (In the figure, input parameters of ANLG_S are omitted.)

When the scan period is 200 ms on the actual SCS, and when input value of AI01 is greater than 80.0, the outputs of NHTR, NHTR_A, NHTR_B become FALSE at the same time.

When this application logic is tested using SCS simulator, though the outputs of NHTR, NHTR_A, NHTR_B become FALSE at the same time, they will become FALSE after 25 seconds from the time when the value of AI01 exceeds 80.0.

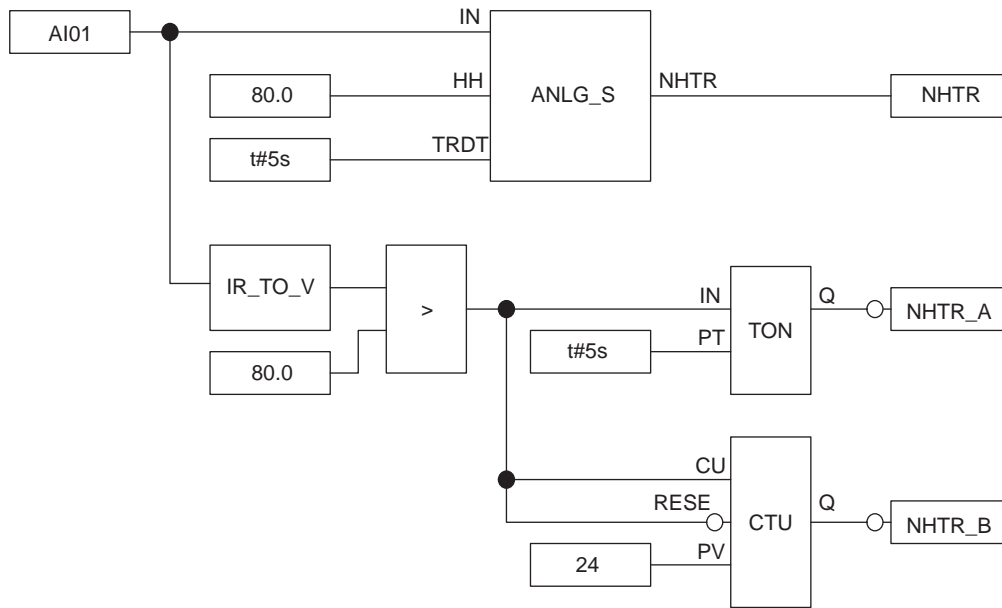


Figure 4.2-6 Timing of Application Actions

● **User-Defined POU Actions**

Undergoing the SCS target test and SCS simulation test, either user-defined program POU or function block POU, may act differently though the difference may vary with scripts.

The following figure shows a simple counter logic. When the scan period is 200 ms, it counts for 5 times per second in the actual SCS target test. Consequently, the count up (CT) will be increased by 5 per second. However, in the SCS simulator, the function block is executed only once per second regardless the actual scan period specified on SCS Manager. Consequently, the count up (CT) will only be increased by 1 per second.

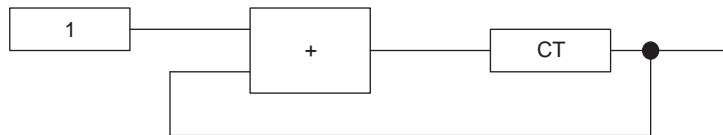


Figure 4.2-7 Example of Counter

● **Actions when Integrated with CENTUM**

When using SCS simulator to test a project that integrated with CENTUM, though the scan period for the external communication function may be specified as 1 second or 2 seconds, the period for executing the CENTUM integration function on the SCS simulator will be 1 second.

4.3 Procedures for Testing

This section describes procedures for the SCS simulation test, the logic simulation test and the target test.

The procedures of the target test vary depending on whether the Online change is executable or not.

4.3.1 Operation of SCS Simulation Test

This section describes how to perform the SCS simulation test.

■ Newly Created Project

Testing of a newly created project is carried out as follows:

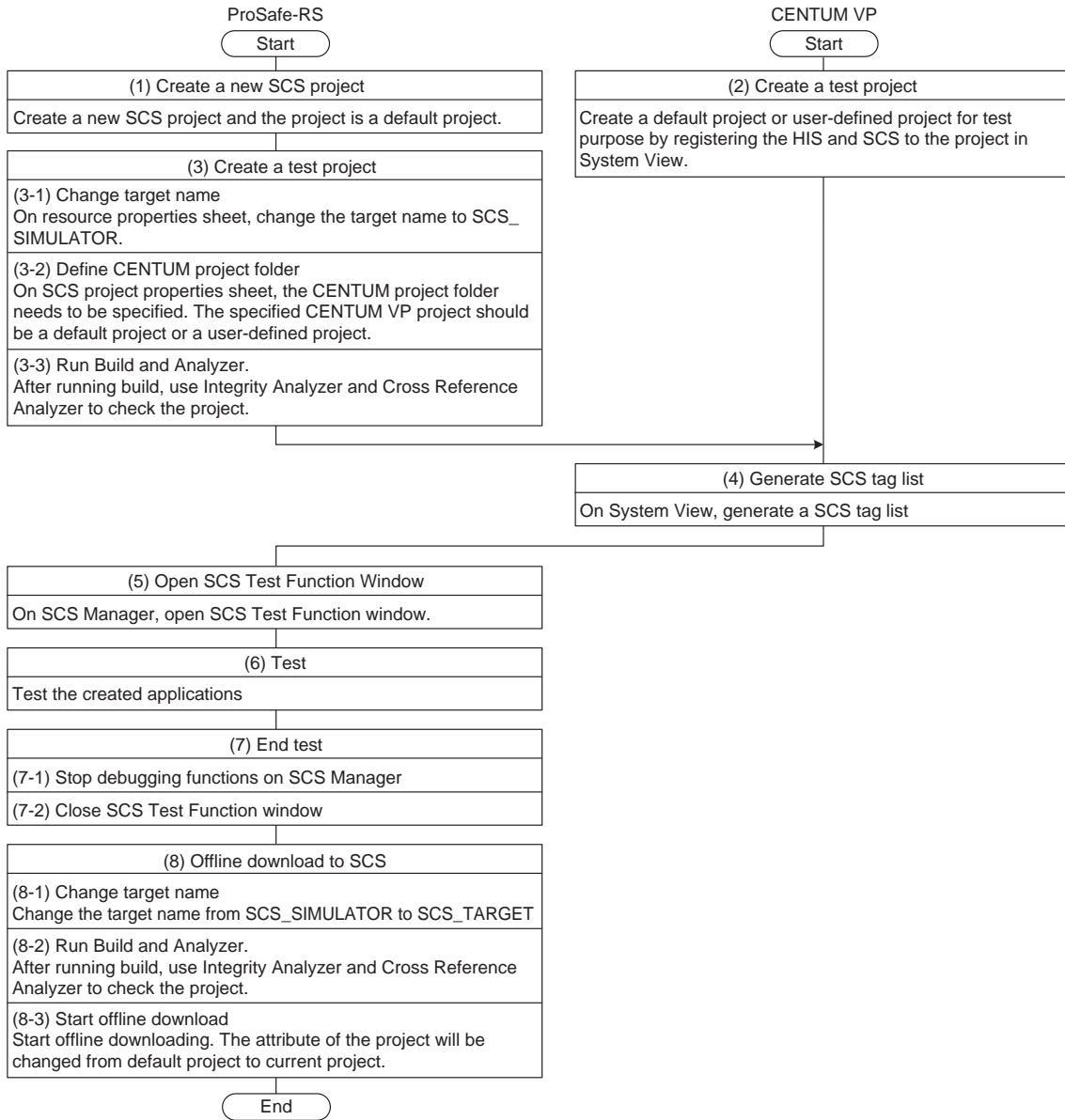


Figure 4.3.1-1 Testing Newly Created Project

■ Testing Modified Project

Testing of a modified project is carried out as follows:

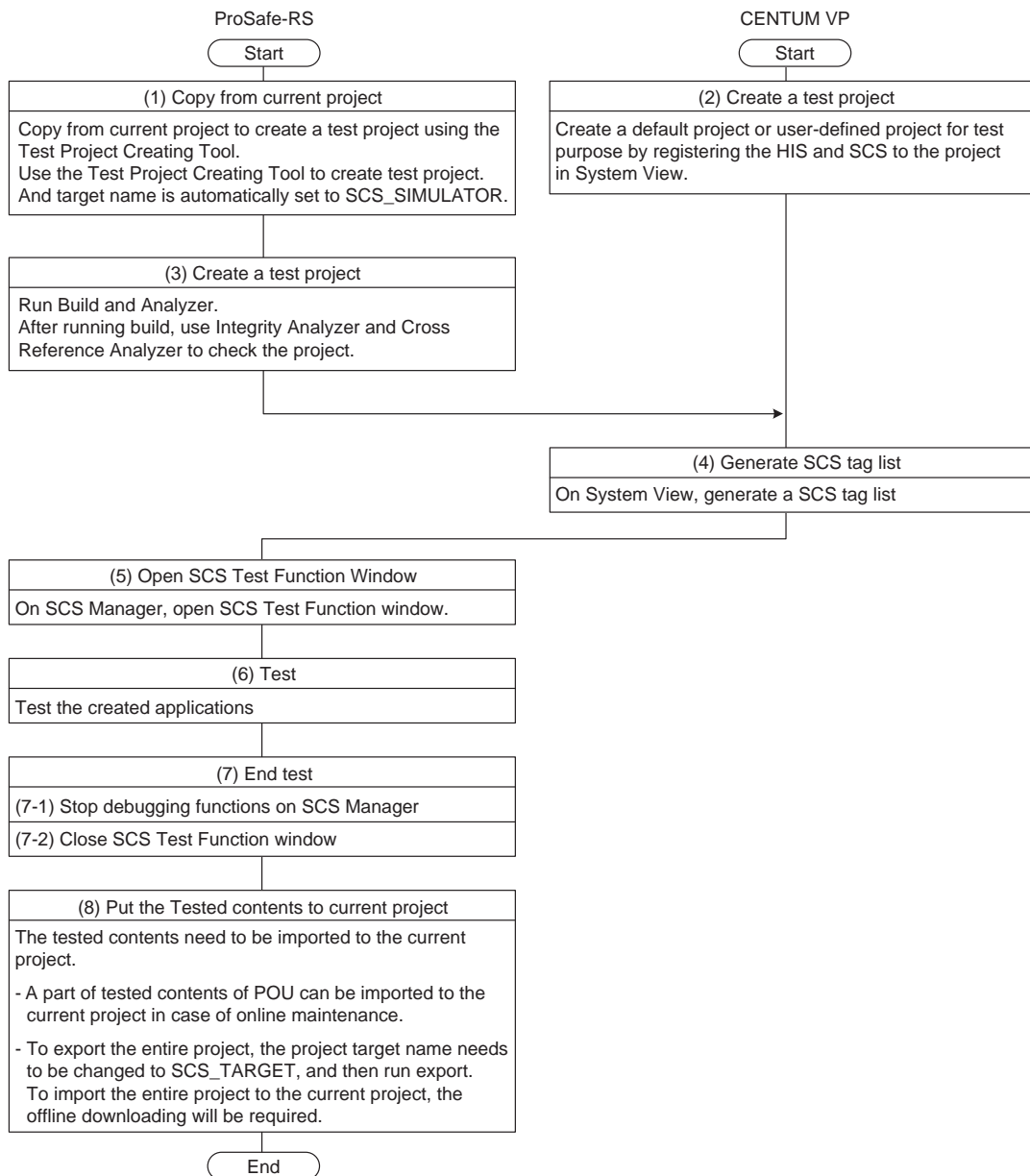


Figure 4.3.1-2 Testing Modified Project

SEE ALSO

For more information about importing the tested contents to the current project, refer to:

[2.20, "Import/Export Function" on page 2-120](#)

4.3.2 Operation of Logic Simulation Tests

The procedure of the logic simulation test is as follows.

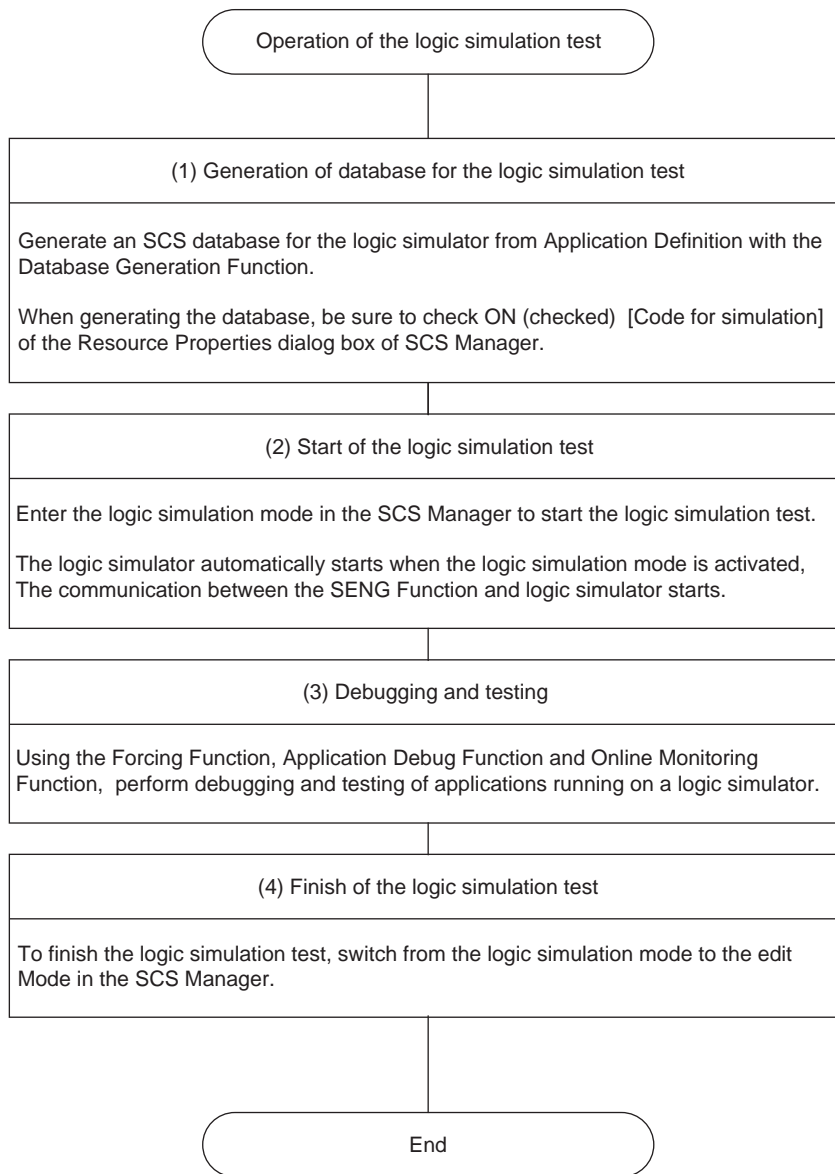


Figure 4.3.2-1 Operation of Logic Simulation Tests

4.3.3 Operation of Target Tests (When Online Change is not Executable)

The target test is performed in accordance with the following procedure for large-scale modifications for which the online change cannot be executed.

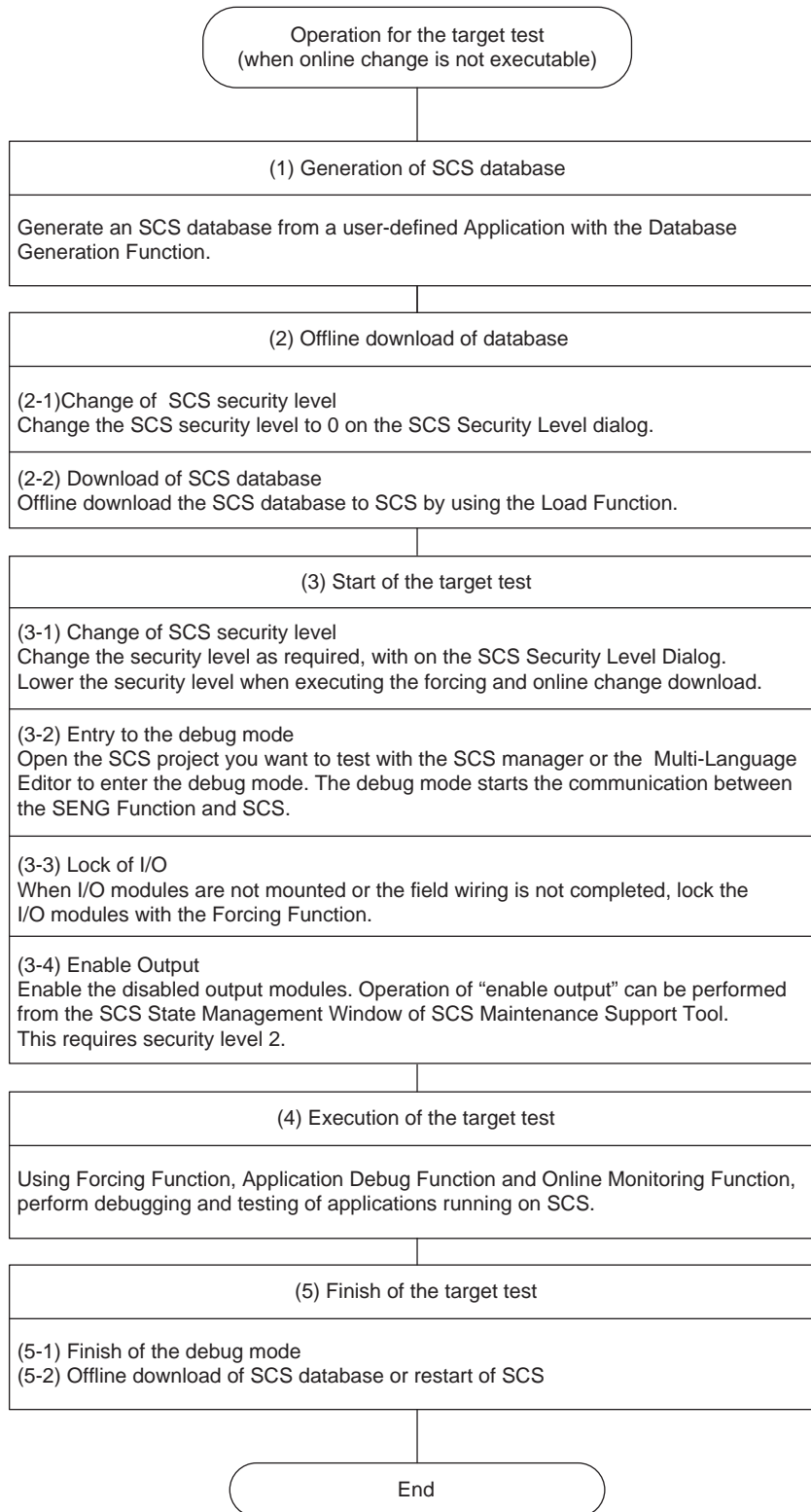


Figure 4.3.3-1 Operation of Target Tests (When Online Change is not Executable)

4.3.4 Operation of Target Test (When Online Change is Executable)

The target test is performed in accordance with the following procedure for small-scale modifications for which the online change can be executed.

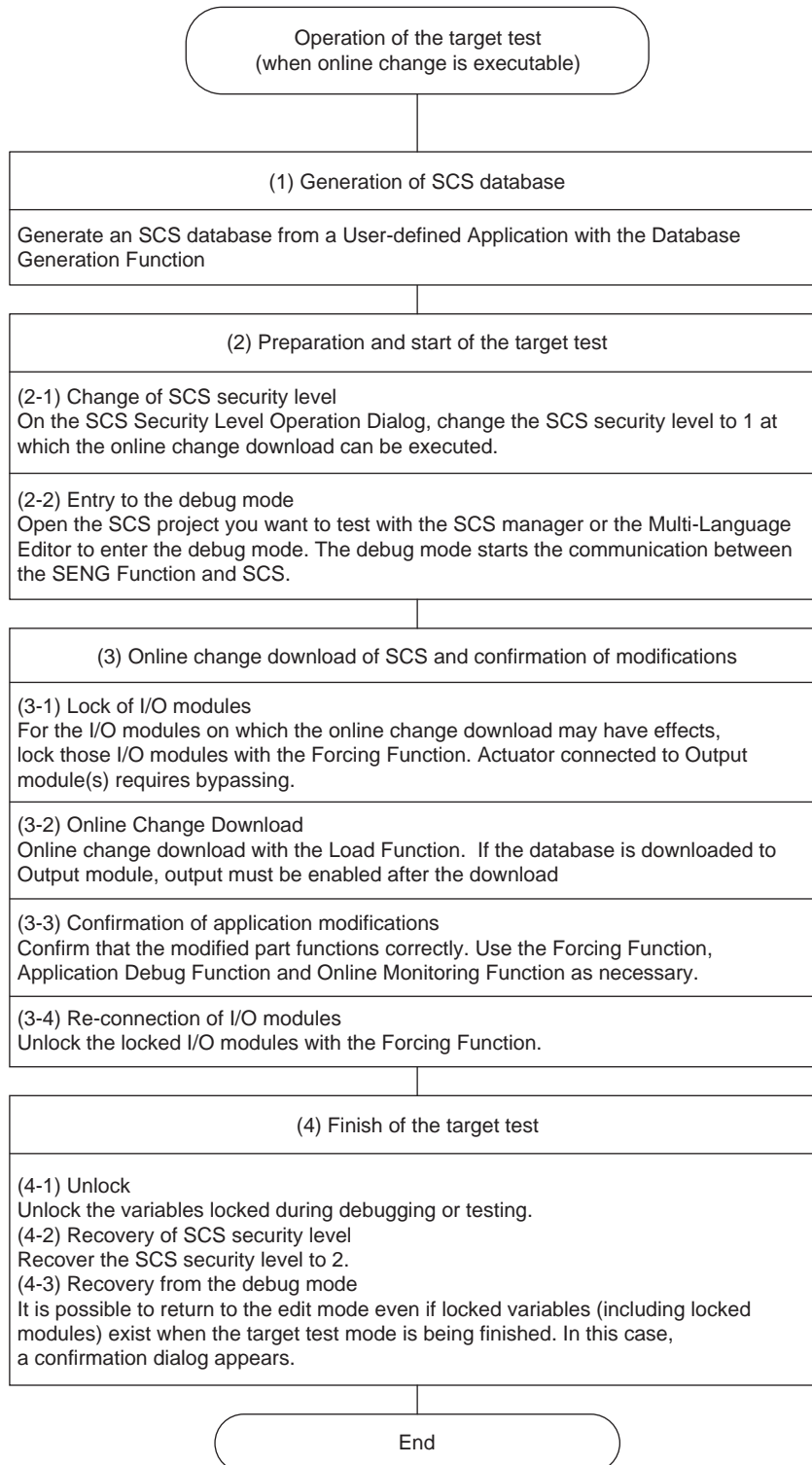


Figure 4.3.4-1 Operation of Target Test (When Online Change is Executable)

4.4 Precautions for Tests

This section describes precautions for testing applications.

■ Test Items

Carefully check the following items when testing applications. Prepare the test procedures in consideration of these items.

- Range of input channels
- Range of output channels
- Check of all paths of application logic
- Check of timers and timing
- Check of combinations of FB/FU input parameters
- Check of the order of executing FB
- Scan period of application logic
- Confirm actions against a fault (a failure in SCS).
- Throughput of the Inter-SCS safety communication
- Confirmation of actions for the Inter-SCS safety communication failure
- SCS Link Transmission

■ Detailed Precautions for Logic Simulation Test

● Modifications in Logic Simulator

Modifications of an application cannot be reflected in the logic simulator during the logic simulation test. To reflect the modifications in the logic simulator, finish the logic simulation test first, then change the application to execute the logic simulation test again.

● The Logic Simulation Test Conducted with Two SENGs or More

With two or more SENGs, the test function can be executed on different SCSs at the same time by start in each simulator. However, communications among two or more logic simulators (“binding”) cannot be executed.

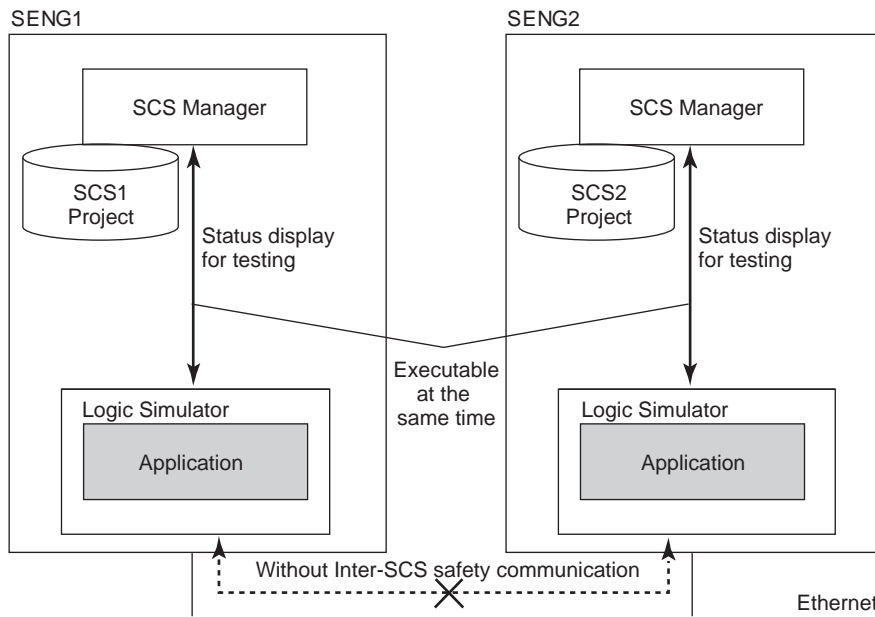


Figure 4.4-1 The Logic Simulation Test Conducted with Two SENGs or More

● **Coexistence of the Logic Simulation Test and the Target Test**

When there are multiple SENG(s), some PCs can be used for conducting the logic simulation test and the others for the target test. The specifications for this case are as follows:

- The logic simulation test and the target test cannot be executed on a single SCS at the same time.
- Logic simulator and SCS in the target test cannot communicate with each other.

■ **Detailed Precautions for Target Test**

● **Effects Caused by Virtual Test of CENTUM VP when CENTUM VP ENG and SENG are Installed in One PC**

When ENG and SENG are installed in one PC, the virtual test of CENTUM VP must not be started during the communication between SENG and SCS.

● **Number of SCS**

The target test can be performed on one SCS project from one SENG at a time. Other SCS projects can also be tested by closing the project being tested and then opening another project.

● **Target Test Conducted with Two SENGs or More**

With two or more SENG, the target test can be performed on different SCSs at the same time. Binding among those SCSs is executed on the control bus.

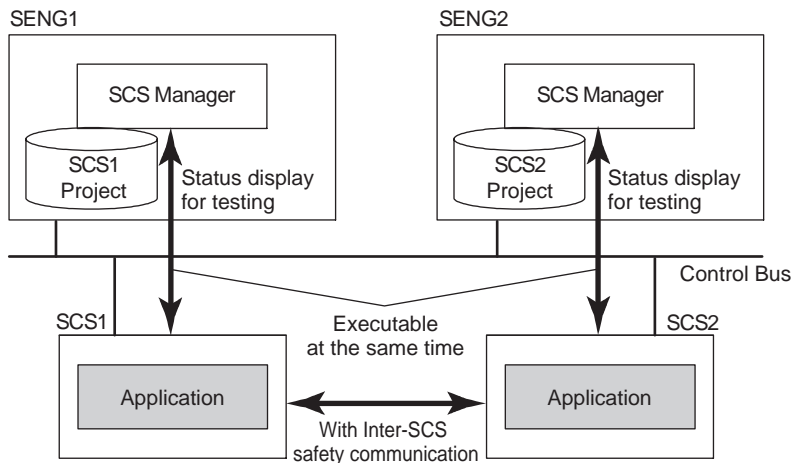


Figure 4.4-2 Target Test Conducted with Two SENGs or More

● **Changing Scan Time while the Debug Application Function is Running**

The following must be observed when you change Scan Time using the Specify Scan Time function while the Debug Application function is running:

- Do not change Scan Time from 250 ms or lower to 500 ms or higher.
- Max Scan Time must be 1 s.

If you do not observe the above two, IOM Alarm/Recover may occur.

● **Using Break Point and Cycle to Cycle Mode while Debug Application Function is Running**

- If the target SCS is connected to IOM with field wiring, do not use Break Point. If used, an IOM error may be triggered by the halt at the Break Point and the output module generates a Failsafe value.
- If the target SCS is performing inter-SCS communication, do not use Break Point or Cycle to Cycle mode. If used, the data of inter-SCS communication is not updated and an inter-SCS communication error occurs at the connected SCSs.

■ **Detailed Precautions for SCS Simulation Test**

● **Precautions at Startup**



IMPORTANT

Do not perform the SCS simulation test on the PC that connected on the control bus (V net, Vnet/ IP) where the plant is running.

- While SCS simulation test is running, the SCS Manager for the project of the actual SCS cannot be started.
- While SCS simulation test is running, do not run the SCS logic Simulation Test.

● **SCS Simulation Test Conducted with Two SENGs or More**

With two or more SENGs, the SCS simulation test can be performed on different SCSs at the same time. Communication among multiple SCSs (binding) is executed on the Ethernet.

Note, however, that if inter-SCS communication is performed among multiple PCs, the expanded test function is required.

- **Library Project for SCS Simulation Test**

- You must change the target name of library project to match the target name of SCS project. If the target names of the two do not match, an error is raised in running build.

- **Database for SCS Test**

- When starting the SCS Test Function window from System View, if the generation time of SCS project and the time of SCS test database are not matching with each other, a warning dialog will be displayed. If you ignore the warning and continue to start the SCS Test Function, the SCS Test Function may start but cannot properly function. Under this situation, you need to run the [Update SCS Test Database] on SCS Manager. After generating a SCS tag list, you need to stop and then start the SCS simulator on SCS Test Function window. When starting SCS Test Function window from the SCS Manager, this problem will not occur since the SCS Manager regenerated the SCS test database when starting the test functions.

- **Operation Marks**

- The operation marks saved during the SCS simulation test cannot be put into the current project.

- **Put Tested Contents to Current Project**

- If the target name of a project is SCS_SIMULATOR, when exporting the entire project contents and then importing the tested contents into a current project, you cannot build the imported contents in the current project since the target name of the project is SCS_SIMULATOR. Changing the target name of the project from SCS_SIMULATOR to SCS_TARGET will solve this problem.
- For the current project of which changes allow online change, the tested contents of the user-defined project need to be exported into PXF binary files and then imported partially to the current project. In this case, do not forget to import all the required contents.

5. Online Change of Applications

This chapter describes the procedure for online change of applications.

5.1 Entire Procedure of Online Change of Application

This section describes a procedure for online change of an application.

■ Procedure for Online Change of an Application

Before performing an online change of an application, analyze possible effects caused by the change carefully and take the appropriate measures. This section describes the procedures for online changes of applications for cases where addition of I/O modules is required and not required, respectively.

**SEE
ALSO**

For more information about operation of SCS Simulation Test, refer to:

[4.3, "Procedures for Testing" on page 4-15](#)

● Online Change without Addition of I/O Modules

The following flowchart illustrates the procedure for online change of an application without addition of I/O modules.

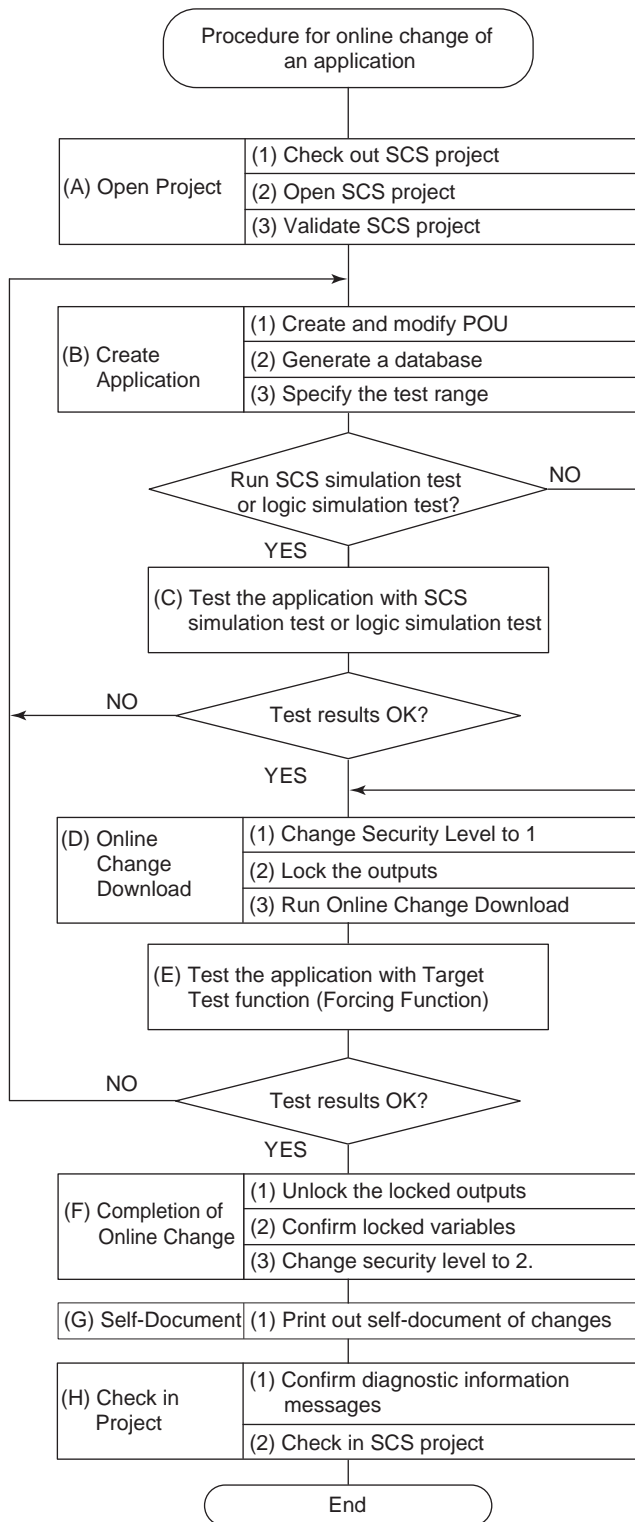


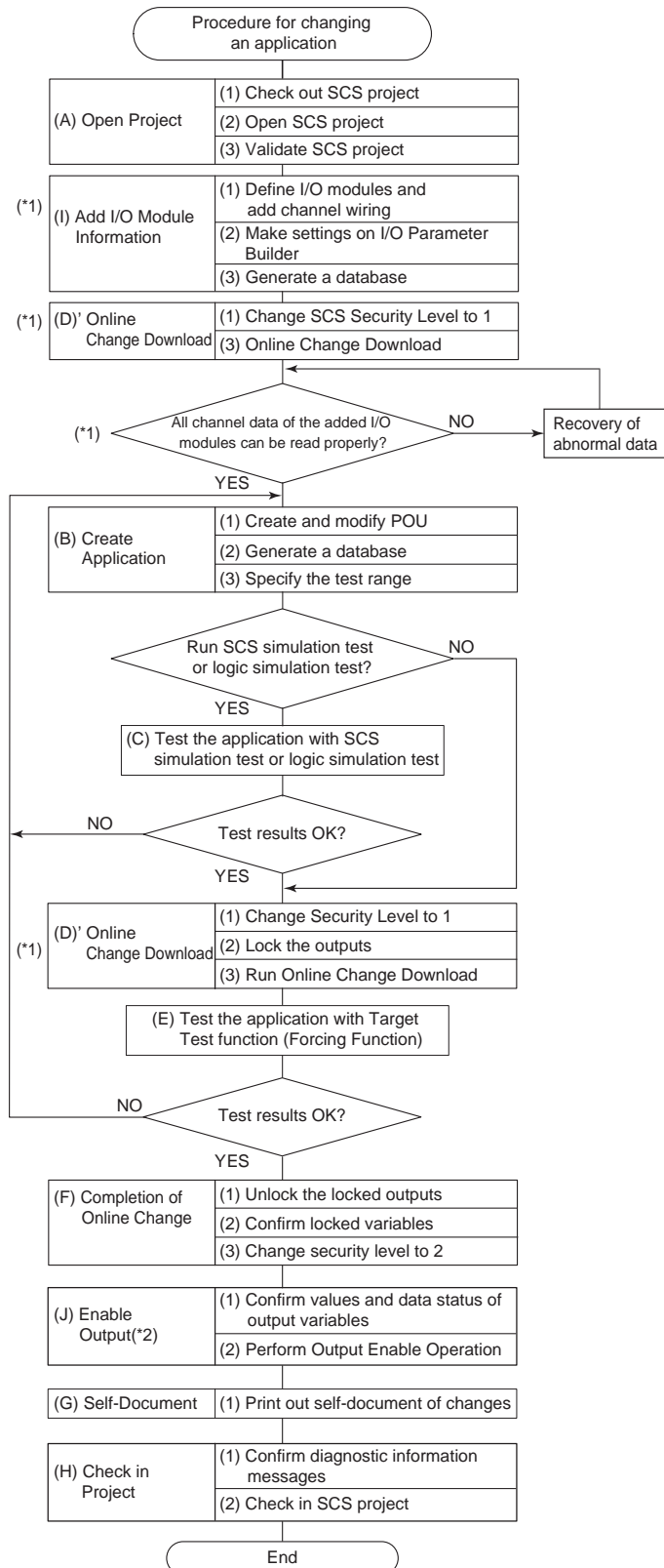
Figure 5.1-1 Procedure for Online Change of an Application

● **Online Change with Addition of I/O Modules**

This section shows the procedure for online changes of the application where any input/output modules are added.

Before you carry out the following procedure, install the input/output modules in the I/O nodes and finish the required hardware setups, such as field wiring and connection of power supply. Next, by following the procedure shown in the flowchart below, make sure that all the data of

the added modules' channels are normal, then generate the application and download the changes.



*1: These steps are different from the procedure for online change without adding input/output modules.
 *2: This is required only when you add output channels or output modules.

Figure 5.1-2 Procedure for Online Change of an Application (With addition of input/output modules)

SEE ALSO

For more information about how to add the hardware of input/output modules online, refer to:

7.5, "Adding Safety Node Unit" in Safety Control Stations (Hardware) (IM 32Q06C10-31E)

● **(A) Opening the Project**

Table 5.1-1 Procedure for Opening a Project

Item	Description
(1) Check out SCS project	<ul style="list-style-type: none"> Check out the existing SCS project with the Version Control Tool.
(2) Open SCS project	<ul style="list-style-type: none"> Start the SCS Manager. Open the SCS project. Enter the password for the SCS project.
(3) Validate SCS project	<ul style="list-style-type: none"> Start the Database Validity Check Tool to check CRC and generation time of four kinds of databases for SCS and SCS project are correct. Repair a database if there is a discrepancy in the database.

SEE ALSO

For more information about how to repair a database, refer to:

- “■ Repair database” in 11., “Database Validity Check Tool” in Engineering Reference (IM 32Q04B10-31E)
- “■ Repairing the Database That Does Not Match” in 11., “Database Validity Check Tool” in Engineering Reference (IM 32Q04B10-31E)

● **(B) Creating an Application**

Table 5.1-2 Procedure for Creating an Application

Items	Description
(1) Create and modify POU	<ul style="list-style-type: none"> Open POU which you want to create and modify. Edit POU. Save POU. Print POU. Confirm that the logic on Multi-Language Editor is the same as the logic printed with the Self-Document Function. Confirm that the execution order FB/FU is correct.
(2) Generate database	<ul style="list-style-type: none"> Perform Build. Check that FU/FB which have been written in the safety application are for safety by using the Integrity Analyzer and then authorize the FU/FB.
(3) Specify the range of testing	<ul style="list-style-type: none"> Check the modified POU and the affected POU with the Cross Reference Analyzer and then authorize them. Use the Project Comparing Tool to check that there are no unintended changes to the following settings, which are critical on safety, because changes to these items cannot be detected by the Cross Reference Analyzer. <ul style="list-style-type: none"> Item in Resource Properties window: <ul style="list-style-type: none"> [Cycle Timing] Items in SCS Constants Builder: <ul style="list-style-type: none"> [Optical ESB Bus Repeater] (for SCSP1/SCSV1) [Maximum Extension Distance] (for SCSP1/SCSV1) [Extend Scan Period Automatically] [Behavior at Abnormal Calculation] [Automatic IOM Download] [Locking of Internal Variable] (for SCSP2) I/O Parameter Builder <ul style="list-style-type: none"> [Extends Node Bus] [Extends To (km)]

● **(C) Testing Applications with the SCS Simulation Test and the Logic Simulation Test Function**

In the SCS simulation test and the logic simulation test, an application is executed by the simulator running on SENG. Use the SCS Manager to perform control and operation, status display, and results display for testing.

Application logic can be debugged with the Application Debug Function, Forcing of I/O variable and Online Monitoring Function. In the SCS simulation test and the logic simulation test, I/O channels are equivalent to being locked all the time.

For performing SCS simulation test, the attribute of the SCS project must be the attribute of user-defined project.

● **(D) (D') Online Change Download**

Table 5.1-3 Procedure for Online Change Download

Items	Description
(1) Change SCS Security Level	<ul style="list-style-type: none">• Start the SCS Maintenance Support Tool which monitors the SCS from the SCS Manager.• Set the security level to 1. Entering a password is required.• Confirm that the SCS Security Level is 1 on the SCS State Management window of SCS Maintenance Support Tool.• Confirm the diagnostic information message indicating the security level at 1 with the SCS Maintenance Support Tool.
(2) Fix the output	<ul style="list-style-type: none">• Locks all the channels of the output modules connected to the modified POU or to be modified POU.• Use the SCS Maintenance Support Tool to confirm that a diagnostic information message is output, indicating that the abovementioned modules have been locked.
(3) Online Change Download	<ul style="list-style-type: none">• Perform online change download.• Establish a communication. Confirm that no communication error occurs.• Confirm that the diagnostic information message is not issued, which is caused by a write error to the flash memory of SCS. If it is issued, perform Offline download.• Use the Database Validity Tool to confirm that CRC and generation time of four kinds of databases for SCS project databases are correct. Confirm that CRC of four kinds of databases and generation time are correct.• Repair a database if there is a discrepancy in the database.• Confirm that the total number of POU notified in the diagnostic information message about the change of resources (No.4172) is identical to the total number of POU shown in the Database Validity Tool.• If downloaded to Output module, validate the output after the download.



WARNING

I/O Lock is a function to prevent unnecessary shutdowns due to the following causes:

- System malfunction caused by unintended errors in application programs
- Temporary halt of I/O module when settings of I/O module are changed (*1)

If you lock the output, you can conduct target tests to check the behavior of a modified logic. However, if you are sure in advance that the above mentioned system malfunction or temporary halt does not occur, or that even if it occurs it will cause no problem, there is no need to lock I/O.

The explanations in Instruction Manuals (IM) for ProSafe-RS rest on the premise that you use the I/O Lock function.

*1: In online change downloads, I/O modules behave differently in R2.02 from earlier SCS system program release number.

SEE ALSO

For more information about how to repair a database, refer to:

- “■ Repair database” in 11., “Database Validity Check Tool” in Engineering Reference (IM 32Q04B10-31E)
- “■ Repairing the Database That Does Not Match” in 11., “Database Validity Check Tool” in Engineering Reference (IM 32Q04B10-31E)

For more information about considerations on online change, refer to:

5.3, “Precautions for Online Change” on page 5-16

For more information about how to repair a database, refer to:

- “■ Repair database” in 11., “Database Validity Check Tool” in Engineering Reference (IM 32Q04B10-31E)
- “■ Repairing the Database That Does Not Match” in 11., “Database Validity Check Tool” in Engineering Reference (IM 32Q04B10-31E)

● **(E) Testing Applications with Target Test Function**

In the target test, an application is executed by the SCS. Use the SCS Manager to perform control and operation, status display, and results display for testing. When the security level is 1, Debug Function of applications cannot be used. Applications can be tested by locking internal and I/O variables using the forcing function and online monitoring function.

● **(F) Completion of Online Change**

Table 5.1-4 Procedure for Completion of Online Change

Items	Description
(1) Unlock the locked outputs	<ul style="list-style-type: none"> • Confirm that, for the digital output modules concerned, the values and statuses of logical data agree with those of physical data. • Unlock the output modules concerned. • Confirm that the diagnostic information message which indicates the output modules concerned have been unlocked is output with the SCS Maintenance Support Tool. • Disable the bypass to the actuator.
(2) Confirm locked variables	<ul style="list-style-type: none"> • Confirm the number of locked variables is 0 with the SCS Maintenance Support Tool. • Confirm that no diagnostic information message is issued except for one you confirmed, with the SCS Maintenance Support Tool.

Continues on the next page

Table 5.1-4 Procedure for Completion of Online Change (Table continued)

Items	Description
(3) Change the security level to 2	<ul style="list-style-type: none"> Set the security level to 2. Confirm that the security level is 2 in the SCS State Management window of the SCS Maintenance Support Tool. Confirm the diagnostic information message which indicates that the security level went back to 2 with the SCS Maintenance Support Tool.

● **(G) Self-Document**

Table 5.1-5 Procedure for Self-Document

Items	Description
(1) Print out modified parts of the project using self-document	<ul style="list-style-type: none"> In preparation for the desk check performed at application software changes in the future, print out the latest SCS project database as self-documents.

● **(H) Check in Project**

Table 5.1-6 Procedure for Check in Project

Items	Description
(1) Confirm the diagnostic information message	<ul style="list-style-type: none"> Confirm that diagnostic information message other than one you confirmed is not issued with the SCS Maintenance Support Tool.
(2) Check in the SCS project	<ul style="list-style-type: none"> Close the SCS Manager. Check in the SCS project with the Version Control Tool.

● **(I) Adding I/O Module Information**

Table 5.1-7 Procedure for Adding I/O Module Information

Items	Description
(1) Define I/O modules and add channel assignment	<ul style="list-style-type: none"> Define I/O variables with the Dictionary. Add I/O module definitions and define parameters with the I/O Wiring View. Connect I/O variables to channels in the I/O Wiring View.
(2) Make settings on the I/O Parameter Builder	<ul style="list-style-type: none"> Define parameters of nodes, modules, and channels with the I/O Parameter Builder.
(3) Generate a database	Execute the same operations as in step (2) of item (B).

● **(J) Enabling Output**

Table 5.1-8 Procedure for Enabling Output

Items	Description
(1) Confirm values and data status of output variables	<ul style="list-style-type: none"> Confirm which output channels are disabled on the SCS State Management window of SCS Maintenance Support Tool. Start the I/O Lock Window.(This can be performed at security level 2.) Confirm that values and statuses of logical data and physical data for output variables are correct.
(2) Operate "Enable Output"	<ul style="list-style-type: none"> Perform the Output Enable Operation for output modules on the SCS State Management window of SCS Maintenance Support Tool. Confirm that the diagnostic information message on the Output Enable Operation for output modules is displayed. Confirm that Output Channels are enabled on the SCS State Management window. Confirm that the SCS operating mode is "Running" on the SCS State Management window.

**SEE
ALSO**

For more information about the Output Enable Operation, refer to:

- [“Enable Output” Operation](#) on page 3-11
-

5.2 List of Applicable Items for Online Change

This section describes the items which can be changed while SCS is in operation online and those which require offline download. If stopping SCS control is not allowed, setting items that require offline download must not be changed.



IMPORTANT

If you change setting items that require offline download, even if you reverse the change, on-line change download is not allowed. If this happens, use Master Database Restoring tool to recover the database to a state where online change download is allowed.

SEE ALSO

For more information about how to use the Master Database Restoring Tool, refer to:

12., “Master Database Restoring Function” in Engineering Reference (IM 32Q04B10-31E)

For more information about the online changeable setting items in the case of SCS whose SCS system program revision is R2.02 or earlier, refer to:

“■ Online Changeable Information” in Appendix 4.7.2, “Compatibility with Earlier Revisions” in Installation (IM 32Q01C50-31E)

■ Online Change of POU Information

There are changes that enables you to execute online change download or offline download according to each POU type.

● Changing POU

The following table shows whether POU can be changed online: for operations on POU, on-line change download can be used for changes of Program name only. If you try to perform online download change on the item that No is described in the table, an error is notified at the time of online change download.

Table 5.2-1 Whether or Not Online Change Can be Used for POU Operations

Type of POU	Changing a name	Creating, deleting
Program	Yes	No
User-defined FU	No	No
User-defined FB	No	No

Since a new program can not be created online, we recommend that you create dummy programs in advance and change the name of the program online as you need.

● Changing POU Logic

When you perform a change operation on POU described in the following table, you can perform an online change download to SCS.

Table 5.2-2 Logic Change Operations that Can be Changed Online on POU

Corrected item	Description
Adding/deleting the standard FU call	-

Continues on the next page

Table 5.2-2 Logic Change Operations that Can be Changed Online on POU (Table continued)

Corrected item	Description
Adding/deleting the user-defined FU call	Including FU defined in the library. A project that is created with the revision earlier than R3.02.00 will be in the same condition as R3.02.00 when clean project is executed. Therefore, you can perform an on-line change download.
Changing logic	-

● **Changing a Library**

When a library is added to or deleted from SCS project, offline download is needed. A warning is displayed at the build operation, and an error occurs at online change download operations.

A project that is created with the revision earlier than R3.02.00 will be in the same condition as R3.02.00 when clean project is executed. Therefore, you cannot perform online change download when the library is added or deleted.

● **Changing Program**

The following table shows the operations that can perform online change download to SCS for global variables, global instances, local variables, and local instances that are used in Program.

Table 5.2-3 Operations that Can be Changed Online for Variables and Instances Used in Program

Corrected item	Description
Adding/deleting a variable	-
Deleting variables and adding variables with the same names as the deleted variables	-
Changing the types of variables	-
Changing attributes of variables	-
Adding/deleting I/O variables	-
Adding/deleting the standard FB instances	-
Adding/deleting the user-defined FB instances	Including FB defined in the library. A project that is created with the revision earlier than R3.02.00 will be in the same condition as R3.02.00 when clean project is executed. Therefore, you can perform online change download.
Deleting FB instances and adding FB instances with the same names as the deleted ones	
Changing the types of FB instances	

● **Changing User-defined FB**

The following table shows the corrections that need offline download to SCS for the parameters of user-defined FB. A warning is displayed at the build operation when performing the correction in the table. An error occurs at online change download operations.

Table 5.2-4 Operation of Parameters that Need Offline Download in User-defined FB

Modification	Description
Adding/deleting a parameter	-
Deleting parameters and adding parameters with the same names as the deleted parameters	-
Changing the types of parameter	-

Continues on the next page

Table 5.2-4 Operation of Parameters that Need Offline Download in User-defined FB (Table continued)

Modification	Description
Changing the attributes of parameter	As the attributes of user-defined FB parameters, the following items cannot be changed online. Direction, () (specification of the number of characters for STRING variables: [Not supported]), Dimension
Adding/deleting the standard FB instances	If you add FB instances without names (not appearing in the Dictionary) in user-defined FB, the FB instances become parameters and thus cannot be changed online.
Adding/deleting the user-defined FB instances	-
Deleting FB instances and adding FB instances with the same names as the deleted ones	
Changing the types of FB instances	

The following table shows the corrections that you can execute online change download to SCS for the global variables and the global instances used in user-defined FBs.

TIP

Normally, global variables and global instances are not used in user-defined FBs.

Table 5.2-5 Operations that Can be Changed Online for Global Variables and Global Instances Used in User-defined FB

Modification	Description
Adding/deleting a variable	-
Deleting variables and adding variables with the same names as the deleted variables	-
Changing the types of variables	-
Changing the attributes of variables	-
Adding/deleting the standard FB instances	-
Adding/deleting the user-defined FB instances	Including FB defined in the library. A project that is created with the revision earlier than R3.02.00 will be in the same condition as R3.02.00 when clean project is executed. Therefore, you can perform online change download. When adding user-defined FU/FB, the added user-defined FU/FB must be tested. When adding pre-validated user-defined FB, testing of the FB itself is not required.
Deleting FB instances and adding FB instances with the same names as the deleted ones	Including FB defined in the library. A project that is created with the revision earlier than R3.02.00 is in the same state as R3.02.00 when clean project is executed. Therefore, it can perform online change download.
Changing the types of FB instances	

- **Changing User-defined FU**

The corrections that you can execute online change download for parameters or local variables in user-defined FU are as follows:

- Adding/deleting
- Deleting variables and adding variables with the same names as the deleted variables
- Changing the types of variables
However, when the type of output parameter is changed, offline download is required.
- Changing attributes of local variables

SEE ALSO

For more information about the precautions that should be taken when deleting a variable or function block and then adding it again, refer to:

“Declared Variables” in “Variables” in “Online Change” in “Debug” in “Workbench” of “Workbench User’s Guide”

I/O Module Information that is Changeable Online

Table 5.2-6 I/O Module

Modification	Online Change (*1)
Adding nodes	Yes
Deleting nodes	Yes
Changing parameters of nodes	Yes
Adding I/O modules	Yes
Deleting I/O modules	Yes
Changing redundant I/O modules	Yes
Changing parameters of I/O modules	Yes
Changing parameters of channels	Yes
Changing parameters of serial communication modules	Yes
Defining wiring between a variable and an idle channel	Yes
Deleting wiring between a channel and a variable	Yes
Changing wiring between a channel and a variable	Yes
Adding, changing or deleting subsystem communication definitions	Yes
Changing wiring of communication input/output FBs	Yes
Adding or deleting ESB bus coupler modules	Yes

*1: Yes: Online change download is possible.

SEE ALSO

For more information about the effect of online maintenance to the communications, refer to:

■ [About Impact of Online Change Download](#) on page 2-106

Constants and Network Information that are Changeable with Online

Table 5.2-7 Constant and Network

Classification	Modification	Online Change (*1)
Configuration	Name	No
	Password	No (*2)
Resource	Name	No
	Resource Number	No
	Cycle Timing	Yes
	Memory size for online changes	No
	Memory size for temporary variable	No
Network	IP address	No
	Station address	No
	Inter-SCS safety Communication (Binding)	No

- *1: Yes: Online change download is possible.
No: Offline download is required.
- *2: Setting and changing passwords is ignored.

■ Builder Definitions that are Changeable with Online

The following table shows whether online change download is possible after definition information has been changed using builders.

Table 5.2-8 Builder Definitions that are Changeable with Online

Items	Online Change (*1)
SCS Constants Builder	Yes (*2)
I/O Parameter Builder	Yes
Communication I/O Builder	Yes
SCS Link Transmission Builder	Yes
Modbus Address Builder	Yes
DNP3 Communication Builder (*3)	Yes (*4)
Tag Name Builder	Yes
Alarm Priority Builder	No
Alarm Processing Table Builder	No

- *1: Yes: Online change download is possible.
No: Offline download is required.
- *2: Some items are enabled. A breakdown showing which items are and are not enabled is provided in "Table of SCS Constants Builder online change."
- *3: Usable only when the version of SCSU1 is R3.02.20 or later
- *4: Some items are enabled. A breakdown showing which items are and are not enabled is provided in "Table of DNP3 Communication Builder online change."

Table 5.2-9 SCS Constants Builder online change

Items	Online Change (*1)
Interval of Repeated Warning Alarms	No
Synchronous Mode	No
Scan Period for External System	No
Modbus Word Order	No
16-bit Modbus master support mode	No
Alarm Notify Action when AOF Released	No
PV Status of S_ANLG_S	No
DNP3 Slave Function (*2)	No
Optical ESB Bus Repeater	No
Maximum Extension Distance	No
Extend Scan Period Automatically	Yes
Behavior at Abnormal Calculation	Yes
Locking of Internal Variables (*3)	Yes
Automatic IOM Download	Yes

- *1: Yes: Online change download is possible.
No: Offline download is required.
- *2: Displayable only when the version of SCSU1 is R3.02.20 or later
- *3: Only for SCSP2

Table 5.2-10 DNP3 Communication Builder Online Change

Items	Online Change (*1)
DNP3 slave station address	Yes
DNP3 master station address	Yes
Timeout value for Select Before Operate (sec)	Yes
Binary Input event buffer size	No
Binary Output event buffer size	No
Binary Counter event buffer size	No
Frozen Counter event buffer size	No
Analog Input event buffer size	No
Analog Output event buffer size	No
Event to be removed when event buffer overflows	Yes
Generate an event when Freeze and Clear command changes data values	Yes
Include Frozen Counters in Class 0 response	Yes
Type of response message fragmentation	Yes

*1: Yes: Online change download is possible.
No: Offline download is required.

5.3 Precautions for Online Change

This section describes precautions for online change of an application.

■ Cautionary Items for Online Change Operation



IMPORTANT

If you change setting items that require IOM download in I/O Parameter Builder and execute online change download to an SCS in R2.01 or earlier system program release number, inputs and outputs of I/O modules stop and their data status changes to BAD. And output module outputs 0.

In the SCS in R2.02 or later system program release number, even if you change setting items that require IOM download in I/O Parameter Builder and execute online change download, data status does not change to BAD and I/O modules continue their tasks.

● Cross Reference Analyzer

- User should confirm locations required for a retest by checking the output of Cross Reference Analyzer.
- For interference -free applications, it is also required to analyze and test parts that are potentially affected by application modifications as with safety applications.

● Online Change Download

- When Online Change Download is executed on I/O modules, confirm that download is executed on the correct I/O modules by checking the diagnostic information message from SCS.
- In CENTUM Integration engineering, even if the correspondence of an instance name and tag name is changed, the modified location may not be displayed in the Cross Reference Analyzer nor in the diagnostic information message. User should conduct tests with care.
- Confirm that CPU idle time of SCS is sufficient and the scan timing is appropriate after an online change.
- During APC (All Program Copy), avoid performing online change download as much as possible. When online change is executed during APC, APC is interrupted and starts again after the online change is finished. Until completion of APC, only one CPU is working even in the redundant configuration. This behavior has no impact on safety. The status of APC operation can be confirmed with LED on CPU, SCS State Management window of SENG or Status Display View of HIS. The start and end of APC are notified by diagnostic information messages.
- When assigning tag names to function blocks that allow the assignment of mapping blocks (e.g., ANLG_S and PASSWD) and annunciators (ANN/ANN_FUP) using the Tag Name Builder, the maximum number of tag names is as follows:
 - Up to 2600 tag names can be assigned when using SCSP1/SCSV1
 - Up to 4500 tag names can be assigned when using SCSP2

The maximum number of online changes that can be made to these mapping blocks and elements with the Tag Name Builder at one time is 200.

The limit on the number of function blocks when using SCSP1/SCSV1 is as follows:

(Number of mapping blocks) + (number of annunciator blocks with tag names) + (total number of mapping blocks/elements changed online at one time) ≤ 2800

The limit on the number of function blocks when using SCSP2 is as follows:

(Number of mapping blocks) + (number of annunciator blocks with tag names) + (total number of mapping blocks/elements changed online at one time) ≤ 4700

If this condition is not met, an error occurs in the check performed before online change and the following error code is displayed in the message display area of the SCS Manager.

```
error code=9448-8ec9
```

Note that tag names are not mandatory for annunciators. It is recommended to set tag names only for those that are referenced by tag names.

- If online change download is executed while the Communication I/O Lock Window is open, close the Communication I/O Lock Window once and open the window again after the completion of the online change download. A database mismatch error may occur if the Communication I/O Lock Window is not closed.
- If you change the range of an input channel in I/O Parameter Builder and execute an online change download, the input value on the channel to which the change was made may change during the download and IOP may occur.
- While an Output Value at Fault is being output, if you change any parameter related to the Output Value at Fault in I/O Parameter Builder and execute an online change download, output value on the channel to which the change was made may change during the download.

● SCS Actions After Changing the Types of FB Instances

The SCS actions during online change download after the types of FB instances or variables are changed are as follows:

- When integrated with CENTUM
SCS data keeps the values before online change download. When reading with the Tag Name interface from CENTUM station, the read values are the values before executing online change download. Values cannot be written from CENTUM station.
- Modbus Slave Communication
Loading/writing values from the Modbus master causes an error. The error code is 13 (hexadecimal).

SEE ALSO

For more information about the error code in Modbus slave communication, refer to:

“● Response message under abnormal conditions” in “■ Response message from SCS” in C1.7, “Messages communication” in Open Interfaces (IM 32Q05B10-31E)

● Precautions for Changing Instance Name in Online Change

If you add/change/delete Instance name(s) to/in/from a function block used in POU and online change download, it affects the behavior of the changed function block.(*1) Do not make unnecessary changes to Instance name(s). Adding of Instance name(s) to a function block is required only if External communication function is used.

*1: Each function block is affected differently by online change. Adding/changing/deleting Instance name(s) involves deleting the existing Instance name(s) together with its previous input/output value and internal status, which affects the behavior of FB. Function Blocks that require measures against instance name changes are as follows:

Table 5.3-1 Impact of Instance Name Change(s)

Function Block	Impact	How to Recover/Avoid
OVR_B, OVR_I, OVR_R, OVR_IB, OVR_IR, GOV_B, GOV_IB	If Override is on, it turns off.	Override is repeated from HIS.
PASSWD	If activated, it gets deactivated.	Activate it again from HIS.
PROD_B, PROD_I, PROD_R	An Inter-SCS communication error and recovers later.	Before online change download, lock the output of Consume side.
MOB_11, MOB_21, MOA	If Data Manual Operation is enabled, output gets FALSE or "0."	Before online change download, lock the variable of OUT connected to MOB_* or MOA.

● Precautions for Reusing Instances

If you delete an instance of an FB or instance of a variable from a Program and perform online change downloading without deleting it (instance of FB or variable) from the Dictionary and then add it again to the Program, the data in the instance are those before the deletion. If you need to initialize the instance data, restart the SCS.

● Precautions Related to Initial Values of Variables

Initial values of variables and FB instance parameters are used when fixing values without re-writing them via logic and specifying values before execution of the first scan after starting SCS.

If Type, Dimension, Scope, and Direction, among types and attributes of variables, are changed online, the values are initialized to the initial values specified by Init.Value of the Dictionary. Changes to values are not reflected if only Init.Value of the Dictionary is changed and online change is executed in order to change the initial values.

If you wish to change only the initial values of variables or FB instance parameters via online changes, change the variable names or delete the variables or FB instances once, perform online change download and then perform online change download to add them again.

● Writing to Flash Memory of SCS

- If an error occurs during writing operation to a flash memory, offline download is required.
- If writing operation to the flash memory is interrupted by pulling out the CPU module or cutting off the power, hardware of the flash memory may fail. Before removing the CPU module or cutting off power, confirm that the LED on the CPU module indicating the flash memory writing status, is lit up (not writing).

● Online Change of Scan Period

- In the case of SCS whose revision of SCS system program is R2.03 or later, it is possible to change the scan period of the application logic execution function via online change download. When you change to a shorter scan period by online change download, a confirmation dialog box displays the estimated CPU idle time after changing the scan period. Note that the estimated CPU idle time does not take into account the impact of changing applications other than in the scan period.
- Do not change both the scan period of the application logic execution function and applications (e.g., addition of logics and I/O modules) at the same time in a single online change download operation. First, change the scan period and perform online change download, check the CPU load of SCS and then change applications.

● Reception Interval Timeout Value (OUTT) for Inter-SCS Safety Communication

In principle, if you set a longer scan period, the transmission interval of inter-SCS safety communication becomes longer. When you change the scan period by online change download,

you need to re-adjust the reception interval timeout values (OUTT) of the SCSs that communicate, by inter-SCS safety communication with the SCS for which the scan period is changed. (This includes the case where the SCS for which the scan period is changed receives data by inter-SCS communication.)

SEE ALSO

For more information about how to decide the OUTT, refer to:

- [“Inter-SCS Safety Communication Timeout Settings” on page 2-55](#)

● Reception Interval Timeout Value (OUTT) for SCS Link Transmission Safety Communication

If you set a longer scan period, the transmission interval of SCS link transmission safety communication becomes longer. Therefore, you also need to re-adjust the OUTT for SCS link transmission safety communication, as should be done for inter-SCS safety communication.

SEE ALSO

For more information about how to decide the OUTT, refer to:

- [“Time Out Settings of SCS Link Transmission Safety Communication” on page 2-61](#)

● Online Change of Single/Dual-redundant Specification of AIO/DIO Modules

Perform the following procedure to change two adjacent AIO/DIO modules in single configuration into dual-redundant configuration by online change download.

1. Disconnect the I/O cables (or terminal blocks) of the modules.
2. If you change two adjacent existing single modules into dual-redundant configuration, pull out one of the modules and then insert it again.
3. Change the definition in the I/O Wiring View and perform online change download.
4. Connect the I/O cables (or terminal blocks).

Immediately after the online change download, the AIO/DIO modules shift to the status described in the following WARNING, but they will recover when I/O cables (or terminal blocks) are connected.

**WARNING**

- Input module
An IOM fail occurs, the “input values at error occurrence” specified with the I/O Parameter Builder are set, and the data status changed to BAD.
- Output module
An IOM fail occurs, the “output values at fault” specified with the I/O Parameter Builder are set as the physical data of all output channels, and the module goes to an output disabled state.

● Online Change of I/O Module Device Index

In order to change device index set with the I/O Wiring View, it is necessary to delete I/O modules once and define them again. At the point I/O modules are deleted, the lock status of each channel of the modules is also canceled.

If you change a device index for a module of the same model installed in the same position by online change download, in the case of input modules, 0s (0 for DI and 0.0 for AI) are input to the application logic at first and then the values from the field are input. In the case of output modules, the channels' outputs are disabled. FALSE for DO and tight-shut value for AO are output. After performing “output enabled operation”, the modules start to output the values of application logic.

■ Online Change of Channel Wirings

This section explains the system behavior when channel assignment is added, deleted, or changed and then online change download is executed. Note that the following cases are also included, in addition to simply adding, deleting, or changing channel assignments.

- When AIO/DIO module definitions are added, channel assignments are also performed at the same time
- When AIO/DIO module definitions are deleted, channel assignments are deleted
- When AIO/DIO module models are changed (when AIO/DIO module definitions are deleted once, then new AIO/DIO module definitions are added, and channel assignments are also performed at the same time)



IMPORTANT

If you change the channel assignment and download the change, IOM downloading will not start automatically.

However, if the I/O parameters are also changed, IOM downloading may automatically start for some types of parameters.

● Online Change of Input Channels

After online changing the input channel assignments, the logical data values of the assigned input variables will be set with the initial value of 0 (DI:FALSE; AI:0.0). Then, the values from the I/O modules will be used.



IMPORTANT

If you add the input channel assignment and the application accessing the input variable, and then the two are online change downloaded at once to SCS, 0 is set to the input variable for an instant before the actual values.

In this case, do the online change according to the procedure below:

1. Run online change downloading right after adding input channels.
2. Lock input variables.
3. Run online change downloading right after changing applications.

When the variable names of the previously assigned input variables are changed and online change downloaded, the input variables will immediately take the values from the I/O modules.

● Online Change of Output Channels

When the output channel assignments are added online, the added channels will not be able to output the logic values. The logic values can be output only after performing the “Output enable operation.”

When the output channel assignments are changed, after online change downloading, the output values may be different from the previous values.

In this case, do the online change downloading according to the procedure below:

1. Lock the output variables.
2. Run online change downloading.

When the variable names of the previously assigned output variables are changed and online change downloaded, the output channels will continuous to output the values through I/O modules.

- **Lock Status at Online Changing of Channels**

When a locked channel is deleted from the assignment, the lock status of that channel will be released and deleted from the total number of locked channels of the whole station. Once a locked channel is deleted from the assignment and online change downloaded, the lock status of the channel will not be kept even when the channel is added to the assignment and online downloaded again.

- **Channel Status at Online Changing**

If the definition of assigned channels is deleted in online change to make them unassigned, the changed channels behave same as the other channels that are unassigned. As the result, channel status outputs for the system function block (such as CHn of SYS_OUTST or Q of SYS_CHST) become FALSE. Also the changed channels are excluded from representative alarm for the system function block (such as NRAL of SYS_OUTST, NRO of SYS_IOALLST, IOER of SYS_DIAG) and are not considered for diagnostic information marks on the SCS State Management window.

- **System Alarm Messages at Online Changing**

When a channel that is causing an error is deleted from the assignment and online change downloaded, the recovery message for the channel will not be raised.

- **Operating Mode at Online Changing**

When an output disabled channel is deleted from the assignment and then online change downloaded, and the operating mode of the station may become Running due to the station does not have any output disabled channel. When an output channel is added to a station that in Running mode, and then online change downloaded the assignment, the status of the station may become Waiting due to the added channel is started in the output disabled status.

■ Online Change of SCS Link Transmission

- **Sequence of Adding and Deleting**

When adding a new data, it should be added first on the sender station. When deleting a data, it should be deleted from the receiver station. Doing this way is to avoid the application to access the deleted data.

- **Lock the Link Transmission Data**

The link transmission data can only be locked together for the whole station. Locking one link transmission data, all the link transmission data in the station will be locked.

Thus, when performing online change (adding or deleting) for link transmission data, the influence of the change to the logics should be properly checked, and then lock the proper variables at the proper places (such as link transmission data of sender station, link transmission data of receiver station or other individual internal variables).



IMPORTANT

For applications that require individual lock, connect the internal variable to lock them as follows:

- On Sender Station: Connect an internal variable to the input parameter of the link transmission output FB, and then lock it.

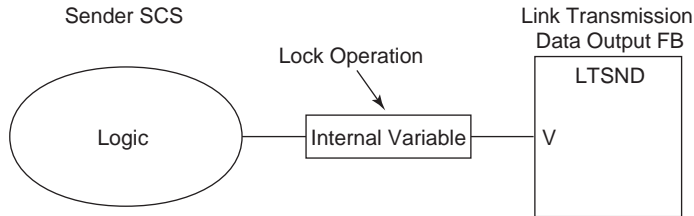


Figure 5.3-1 Lock on Sender Station

- On Receiver Station: Connect an internal variable to the output parameter of the link transmission input FB, and then lock it.

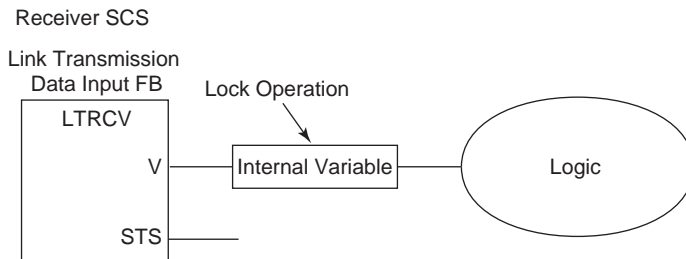


Figure 5.3-2 Lock on Receiver Station

- Add a logic that uses a link transmission data input FB



IMPORTANT

Do not add a link transmission data input FB and the logics connected to the FB at the same time during the online change. The influence to other logics may occur even if the link transmission received data are properly locked.

In this case, do the online change according to the procedure below:

1. Create a link transmission data input FB.
 2. Online Change Download
 3. Add a logic connecting to the link transmission data input FB.
- Change the Link Transmission Data Input FB Instance Name
When a link transmission data input FB instance name is online changed, note that the output of the FB may become different.

When changing the instance name online is necessary, do it according to the procedure below:

1. Lock the internal variable that connected to the link transmission data input FB.
2. Online Change Download

If you cannot find a proper internal variable to lock, you need to add an internal variable to the output parameter of the link transmission data input FB, and then lock the variable. Then you can online change the instance name.

- Delete Link Transmission Data Output FB
When a Link Transmission Data Output FB is deleted, the output data will be reset to 0. Even if the local station is locked to avoid bad influence, the receiver side is still affected since the linked data is reset to 0. Therefore, the FB in the receiver side should be deleted first.
- When Sending Definition of the SCS Link Transmission is Disabled
When sending definition of the SCS link transmission is disabled during online change, data sending to other stations will stop. If another station is receiving data from the stopped station, the actions are shown as follows.

Table 5.3-2 Actions of Receiver Station

Receiver Station	Description
SCS	Since the updating of the safety information (such as sequence numbers or transmission timestamps) sent through the link transmission are stopped, an error will be indicated. The statuses of related input data will become BAD.
FCS	The last received data will be kept. The statuses of the related data will not become BAD.

Moreover, when the transmission size of the sender FCS is online changed to 0, the receiver station on SCS side will keep the last received data values. The data statuses will not become BAD.

■ Locking Inter-SCS Safety Communication and SCS Link Transmission Data at Online Change

False trips caused by online changes can be prevented by locking inter-SCS safety communication data or link transmission data on the station where online change is performed. It is not necessary to lock data on the stations that receive data from the station where online change is performed.

The following figure illustrates an overview and the procedure for performing online changes.

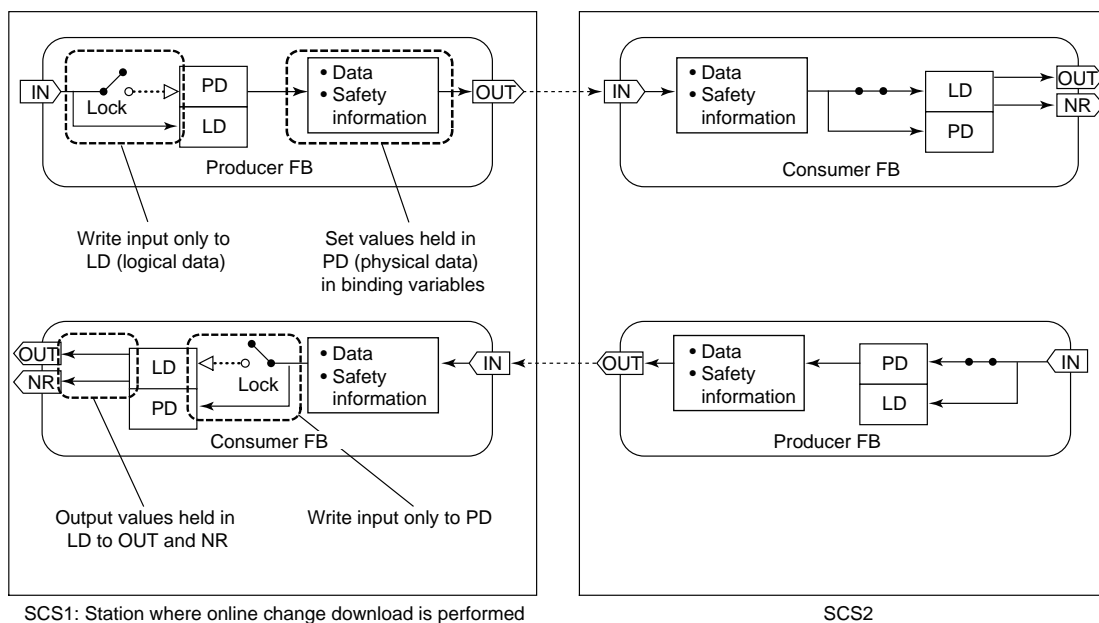


Figure 5.3-3 Example of Locking Inter-SCS Safety Communication at Online Change

Follow these steps to perform online changes:

1. Set the security level of the SCS for which online change is to be performed to 1.
Check that the SCS's security level has changed to 1 with diagnostic information messages.
2. Open the Inter-SCS Communication Lock Window or SCS Link Transmission Window of the SCS for which online change is to be performed and lock the sending and receiving data.
Check that inter-SCS safety communication or link transmission safety communication has been locked with diagnostic information messages.
3. Execute online change download.
4. Check that the logical data and physical data match and that the data status is GOOD in the Inter-SCS Communication Lock window or SCS Link Transmission Lock window.
5. Unlock the sending and receiving data in the SCS in the Inter-SCS Communication Lock window or SCS Link Transmission Lock window.
Check that the inter-SCS safety communication is unlocked with diagnostic information messages.
6. Set the security level of the SCS for which online change has been performed to 2.
Check that the SCS's security level has changed to 2 with diagnostic information messages.

6. Installation and Start-up

This chapter describes the installation of ProSafe-RS system, the wiring to field devices, a procedure of start-up including tests, commissioning and precautions for the start-up.

6.1 Procedure of Installation and Start-up

This section describes a general procedure of the start-up of ProSafe-RS system ranging from the installation of equipment to the completion of commissioning.

■ Installation and Start-up

The regular procedure from the installation of equipment to the completion of commissioning is as follows.

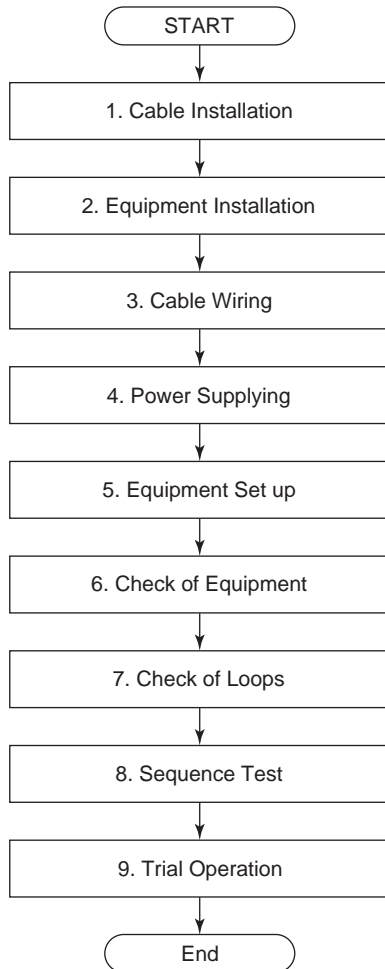


Figure 6.1-1 Installation and Start-up

1. Install control bus, optical cables and cables between panels.
2. Install ProSafe-RS and other equipment.
3. Wire for networks such as V net and ESB buses, as well as I/O modules and field devices.
4. Supply power to ProSafe-RS and other equipment.
5. Turn on ProSafe-RS and other equipment to start.
6. Check individual hardware of ProSafe-RS and other equipment (including I/O modules).
7. Check loops from the field to I/O modules.
8. Test application logic of ProSafe-RS.
9. Perform a trial operation for the entire system to confirm actions of the ProSafe-RS system itself.

● Commissioning

In commissioning, procedures from No.6 “Check of Equipment” to No. 9 “Trial Operation” in the flowchart of “Installation and start-up” are performed. Confirm the following items in this series of procedures.

- All modules in SCS, wiring to field devices and wiring of power supply are correctly installed.
- All modules in SCS, field devices and power supply work without faults.
- Sensor measurement values are correct.
- Input values to SCS and output values from SCS are correct. (Including tests of high/low limits)
- Application logic works correctly according to changes of input values.
- Operations for failure occurrence take place as intended on the basis of each field device and SCS module.
- Safety application logic works correctly between actual SCSs when Inter-SCS safety communication is used.
- Confirm Demand Reaction Time.
- Confirm actions against a fault (a failure in SCS).

● Precautions

- When executing offline download on a suspended SCS, confirm that the SCS is being suspended with the SCS State Management window in SENG so as not to download the database to a different SCS by mistake.
- Confirm that the SCS works normally after offline download with the SCS State Management window in SENG.
- Confirm that database is downloaded correctly with the Database Validity Check Tool in SENG.
- Set new passwords for security levels 0 and 1 after offline download.
- Precautions for LED display of CPU of SCS
LEDs of CPU have a structure which switches between V net or Vnet/IP address display and SCS Status Display. Set LED to the SCS Status Display when SCS is in operation.
- While SDV526 is outputting Off signals, it takes max. 5 minutes to detect open circuit and max. 2 minutes to detect the recovery.
Because of this, if any of the following event occurs before the cause of open circuit error is eliminated after a diagnosis information message of an abnormal status caused by the open circuit is generated, a diagnosis information message of recovery is generated first. And after about 5 minutes, a diagnosis information message of an abnormal status is generated again.

TIP

If you perform output enable operation before the abnormal status is re-detected, open circuit is detected about 5 minutes after a diagnosis information message of recovery is informed if the output signal is OFF. If the signal is ON, open circuit is immediately detected.

- SDV526 recovers from power supply error (the power to the I/O node or the field power supply is turned off and on.)
- Dismounting and remounting of SDV526 or re-connection of a cable connector that was disconnected (both modules in redundant configuration.)
- Recovery of ESB bus communication. (SDV526 recovers from a state where it outputs fail-safe values.)

- In the case of SDV521 (style S3 or above)/SDV53A (style S2 or above), if a short circuit has occurred while the module is outputting an Off signal, it takes max. 10 seconds to detect the short circuit.
- In the case of SDV521 (style S3 or below)/SDV53A (style S2 or below), if a short circuit is detected while the module is outputting an Off signal and a diagnosis information message indicating the abnormal status is generated, a diagnosis information message of recovery may be generated if either of the following events occurs before the short circuit is repaired.
 - The module is powered off and on (due to dismounting and remounting of the module or turning on and off the power to the I/O node)
 - Switch over to the standby module (when modules are in redundant configuration)

Also note that if the module is powered on while it has a short circuit, the short circuit may not be detected. After the short circuit is repaired, it becomes possible to detect short circuits that occur afterward.

- In the case of SDV521/SDV53A, if a short circuit is detected while the module is outputting an On signal and a diagnosis information message indicating the abnormal status is generated, a diagnosis information message of recovery may be generated before the short circuit is repaired. Even after the recovery message is generated, an Off signal is output to the channel and the channel remains in the output disabled status.

**SEE
ALSO**

For more information about repair database, refer to:

[“■ Repair database” in 11., “Database Validity Check Tool” in Engineering Reference \(IM 32Q04B10-31E\)](#)

For more information about how to repair database, refer to:

[“■ Repairing the Database That Does Not Match” in 11., “Database Validity Check Tool” in Engineering Reference \(IM 32Q04B10-31E\)](#)

7. Operation and Maintenance

This chapter describes the actions in an emergency and the procedure for collecting information by using the SOE Viewer. It also describes the procedures and precautions for maintenance of ProSafe-RS equipment (including I/O modules) and field devices.

7.1 Operation

This section describes the procedures for operations in an emergency during plant operation and the procedure for collecting information by using the SOE Viewer.

7.1.1 Operation in an Emergency

It is required to plan the operation procedure beforehand for emergencies including the occurrence of a shutdown demand or an equipment failure.

An emergency operation is required in case of the following. Referring to these operation flows, plan the emergency operation specifically.

■ Operation at the Occurrence of a Process Failure

- Operation when SCS Issues a Pre-alarm because of a Signal from the Field

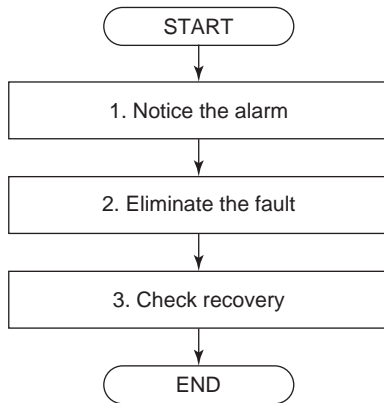


Figure 7.1.1-1 Operation when SCS Issues a Pre-alarm because of a Signal from the Field

1. Confirm the alarm with an alarm panel or HIS (for CENTUM Integration Structure).
2. Operate the DCS or field devices to eliminate the fault by following the operation manual.
3. Confirm the recovery of normal operation at the plant or DCS.

- Operation when Plant is Shutdown because of a Demand from the Field

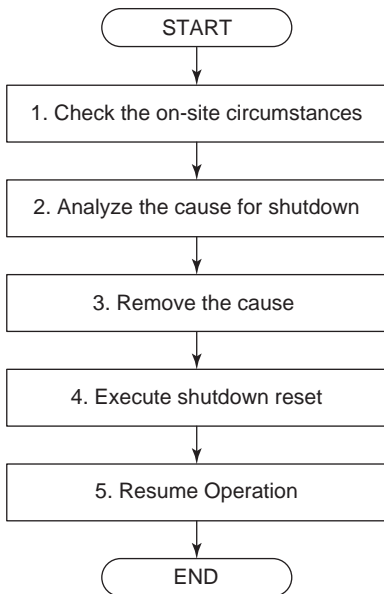


Figure 7.1.1-2 Operation when Plant is Shutdown because of a Demand from the Field

1. Maintenance personnel check the present state in the plant.
2. An engineer analyzes a cause of the shutdown with the SOE Viewer in SENG. The engineer identifies the cause of the fault with the diagnostic information message at the time when a diagnostic fault occurs and event information is displayed in the SOE Viewer. For

CENTUM Integration structure, the engineer can display the process alarm message issued by SCS as a historical message on the SOE Viewer to facilitate the identification of the cause. The engineer then makes a procedure for removing the cause of the fault for recovery. The messages can also be stored as a record by outputting them to a file.

3. The maintenance personnel remove the cause of the fault according to the work procedure.
4. The maintenance personnel execute a shutdown reset operation from the ESD console.
5. Confirm the state of the plant again to restart the plant according to the operation manual.

● **Operation when a User Manually Execute a Shutdown**

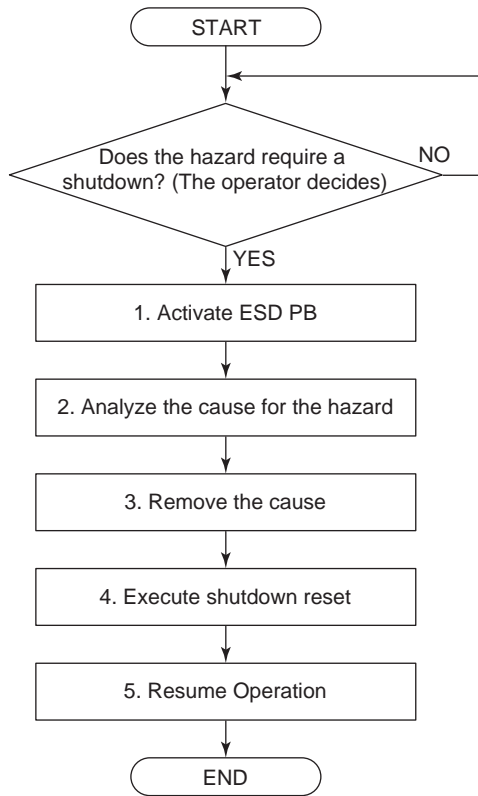


Figure 7.1.1-3 Operation when a User Manually Execute a Shutdown

1. Maintenance personnel confirm the state in the plant and operate ESD PB (Emergency shutdown button) installed in the ESD console in order to avoid dangerous accidents.
2. The engineer analyzes the cause of the hazard with historical messages or trend data of the DCS and the SOE Viewer in SENG, and makes a work procedure for removing the cause of the fault.
3. The maintenance personnel remove the cause of the fault according to the work procedure.
4. The maintenance personnel operate a shutdown reset from the ESD console.
5. Confirm the state of the plant again to restart the plant according to the operation manual.

■ Operations at the Occurrence of a System Failure

● Operation when ProSafe-RS Equipment Fails

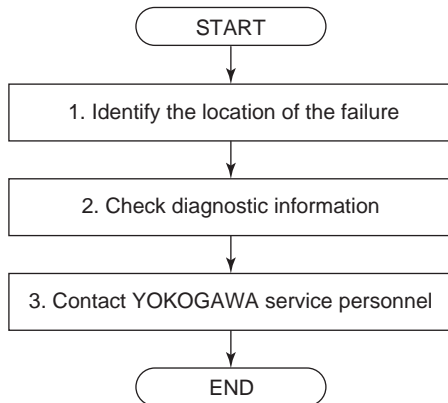


Figure 7.1.1-4 Operation when ProSafe-RS Equipment Fails

1. The engineer starts the SCS State Management window from SENG of the SCS where a fault occurs and confirms the present status on the display. A diagnostic information mark is displayed for I/O modules having a diagnostic fault. The engineer selects the I/O module, and display Diagnostic Information window of the I/O modules to confirm a Diagnostic Information Message related to the I/O modules.
2. The engineer confirms the messages generated by the diagnostic function of SCS. Double-click the message for the corresponding measures. This opens the Help dialog box in which the measures are indicated. Clicking a relevant message in the Diagnostic Information Window and then a [confirmation] button on the Toolbar opens the Confirmation dialog box. Diagnostic Information Messages can be confirmed by pressing the [confirmation] button on this dialog box (Operation for confirming individual messages).
3. Inform the service section at YOKOGAWA of the above information.

7.1.2 Analyzing Events (SOE Viewer)

On the SOE Viewer, events of ProSafe-RS can be analyzed. The event log in the specified SCS is uploaded to be displayed as event messages.

The SOE Viewer functions are as follows.

- The Event log (SOE event information and Diagnostic Information message) stored in SCS is uploaded to be displayed as event messages.
- Data sources of eight SCSs (including HIS for CENTUM Integration Structure) can be specified.
- Only event messages that you want to see can be filtered.
- A trip report can be generated. The report can be printed or exported as a CSV file.
- In case of CENTUM Integration Structure, process alarm messages from SCS can also be displayed.

The SOE Viewer has the following operation modes.

- Event Mode Operation
It displays a list of event messages of SCS.
In the case of CENTUM Integration Structure, HIS historical messages (process alarm messages of SCS) can also be displayed.
- Trip Mode Operation
It displays a list of trip events of SCS. Detailed information about trip signals are also displayed.

**SEE
ALSO**

For more information about the usage of SOE Viewer, refer to:

[4., "SOE Viewer" in Utilities and Maintenance Reference \(IM 32Q04B20-31E\)](#)

7.2 Maintenance

Give consideration to the items described in this section and follow the procedures and precautions specified herein when maintaining the ProSafe-RS equipment, software or any field devices as part of maintenance of the safety system.

Before commencing the maintenance work, take the necessary measures to prevent the field devices from being affected by the maintenance. For these measures and during maintenance, the forcing function and override function can be used.

7.2.1 Utilizing Forcing and Override Function During Maintenance

For the purpose of SCS maintenance, it may be necessary to fix or forcibly change the input/output values or values used in application logics. In such cases, the forcing and override functions can be used.

Forcing allows fixing channel input/output values of I/O modules (locking values) from the SCS Manager of SENG and forcibly changing the values (setting values). The following items are the targets of forcing.

- Input/output channels of AIO/DIO modules
- Subsystem communication data
- Variable included in application logic
- Inter-SCS safety communication data
- SCS link transmission data

In addition, it is possible to monitor the lock status in the application logics and forcibly cancel the lock status by using system function blocks (SYS_FORCE, SYS_FORCE_LT, SYS_FORCE_BD, SYS_FORCE_AC).

In the case of integration with CENTUM, variable values can be set by overriding them from HIS.

The following table shows the difference between forcing and override.

Table 7.2.1-1 Difference between Forcing and Override

Items where there is a difference between the two functions	Forcing	Override
Purpose	Maintenance of SCS and debugging of applications that are done through SENG	Maintenance of SCS through HIS in the CENTUM Integration Structure
SCS Security Level	The security level has to be set to 1 or 0.	An override is executable when the security level is 2.
Necessity of Programming	Programming is not necessary.	Application logic needs to be programmed with override function blocks.
Designation of output values	Output values can be specified in the I/O Lock Window, etc.	When an override is activated during execution of application, the preprogrammed value is output as an overridden value.
Conditions for locking a variable	Whether or not forcing can be performed depends on the SCS security level.	A program can be written that enables and disables override by using such as a mechanical key switch.

■ Forcing Function

The forcing function consists of the lock function and value setting function. With this function, values are first locked and then set.

To operate forcing, security level of SCS is required to be set to 1.

By locking an input variable, a wiring test can be conducted without informing the application logic about changes of the input channel value and the status of the input loop (Field wiring and device). The actual input value can be confirmed with the I/O Lock Window. Similarly, by locking an output variable, a wiring test of the output loop can be conducted without informing the output channel about changes of the output value from application logic. Actions of the loop at the output side can be checked by changing the output variable at this time.

In the case of inter-SCS safety communication, you can use the Inter-SCS Communication Lock Window to lock the producer and consumer function blocks for inter-SCS safety communication. By locking the function blocks appropriately, you can prevent the false trip that may occur on a station during the following downloads:

- Online change download on local station
- Online change download on other station
- Offline download on other station

Note that, when the security level is 0, variable values can be set without locking for any application logic variables (including FB parameters) other than input/output variables.

The following table shows the items that can be forced and the main purposes.

Table 7.2.1-2 Forcing Targets and Main Purposes

Target	Main purpose
Input/output channels of AIO/DIO modules	<ul style="list-style-type: none"> • Disconnecting input and output at testing field devices and input/output wiring • Disconnecting input at input module maintenance • Debugging application logic • Fixing input/output at online change download
Variables in application logic	<ul style="list-style-type: none"> • Debugging application logic
Subsystem communication data	<ul style="list-style-type: none"> • Disconnecting input/output at subsystem communication module maintenance • Debugging application logic • Fixing subsystem communication input/output at online change download
Inter-SCS safety communication data	<ul style="list-style-type: none"> • Disconnecting data at communication data at offline download and online change download • Debugging application logic
SCS link transmission data	<ul style="list-style-type: none"> • Disconnecting data at communication data at offline download and online change download • Debugging application logic

● **Lock Function**

The lock function fixes (locks) the values of individual forcing targets to constant values regardless of input from the actual input device or logic output operation result.

The following table shows the lock function for each type of forcing targets.

Table 7.2.1-3 Forcing Target and Lock Function

Target	Unit of locking	Related system function block and function	Precaution at locking
Input/output channels of AIO/DIO modules	Each channel or each module	SYS_FORCE <ul style="list-style-type: none"> • If the total number of locked variables exceeds the pre-defined limit, this function block can issue a diagnostic information message to notify the user. • If the duration of locking exceeds the pre-defined time limit, this function block allows generating a diagnostic information message to notify the user. • It is possible to unlock all locked variables. 	If I/O variables are locked, even when an error occurs in the corresponding channel of the input/output devices, it is not notified to the logic. (*1)
Variables in application logic	Each variable		In the case of SCSP2, if you lock internal variables, the CPU load (execution time) increases compared to the status where no internal variables are locked.

Continues on the next page

Table 7.2.1-3 Forcing Target and Lock Function (Table continued)

Target	Unit of locking	Related system function block and function	Precaution at locking
Subsystem communication data	Each module	<p>SYS_FORCE_SC (*2)</p> <ul style="list-style-type: none"> • If the duration of locking exceeds the pre-defined time limit, this function block can issue a diagnostic information message to notify the user. • It is possible to unlock all locked variables. It is also possible to cancel the lock status of variables that are deleted by online change while being locked. 	If subsystem communication is locked, even when an error occurs in the data status, it is not notified to the logic.
Inter-SCS safety communication data	Each SCS	<p>SYS_FORCE_BD</p> <ul style="list-style-type: none"> • If the total number of stations whose inter-SCS safety communication data is locked exceeds the pre-defined limit, this function block can issue a diagnostic information message to notify the user. • If the duration of locking inter-SCS safety communication data exceeds the pre-defined time limit, this function block can issue a diagnostic information message to notify the user. • It is possible to unlock all locked producer FBs and consumer FBs. It is also possible to cancel the lock status of producer FBs and consumer FBs that are deleted by online change while being locked. 	If inter-SCS safety communication data is locked, even when an error occurs in the data status, it is not notified to the logic.
SCS link transmission data	Each SCS	<p>SYS_FORCE_LT</p> <ul style="list-style-type: none"> • If the total number of stations whose SCS link transmission data is locked exceeds the pre-defined limit, this function block can issue a diagnostic information message to notify the user. • If the duration of locking SCS link transmission data exceeds the pre-defined time limit, this function block can issue a diagnostic information message to notify the user. • It is possible to unlock all locked link transmission data. It is also possible to cancel the lock status of link transmission data that are deleted by online change while being locked. 	If SCS link transmission data is locked, even when an error occurs in the data status, it is not notified to the logic.

*1: Diagnostic information messages notifying abnormality are generated, however. Some system function blocks detect errors without being affected by locking.

*2: In the case of subsystem communication data, the number of locked data is not counted but only the existence of the locked data is detected.

SEE ALSO

For more information about CPU load of SCSP2 when internal variables are locked, refer to:

■ [Locking of Internal Variables and Performance: SCSP2](#) on page 2-49

● Variable Value Setting Functions

This function is used to set value of each item of forcing targets. If you set a value for a locked item when the SCS security level is 1, the item value is fixed to the set value. An error occurs if it is attempted to specify values of input/output variables and internal variables that are not locked.

If the SCS security level is 0, it is possible to set variable values for all applications (excluding I/O variables, inter-SCS safety communication data, etc.) and parameters of function blocks without locking them. Values of internal variables placed within the logic are overwritten by the logic unless they are locked, however. Lock the variables and then specify the values to make sure that data values are changed.

● Forcing Function Block Parameters

If the SCS security level is 0, parameters of FBs whose instance names are defined can be forced without locking them via Multi-Language Editor or Dictionary.

Using this function allows performing tests more efficiently such as forcing the ET (Elapsed Time) parameter of TOF function blocks (off-delay timing) to advance the time. Data values of FBs without instance names can also be changed without locking the parameters from Multi-Language Editor.

● Forcing the User-Defined Function Block Parameter

Data values of user-defined FBs of which instance names are defined can be changed by locking parameters of the instances in Multi-Language Editor or Dictionary if the security level is 1 or less.

● Example of Procedure for Setting Data with Forcing

1. Set the security level of SCS to 1.
Check that the security level of SCS is set to 1 with the Diagnostic Information Message
2. Lock I/O variables or internal variables.
Check that the names of the locked variables are correct with the Diagnostic Information Message.
3. Set a value to the I/O variables or internal variables.
Check that the variable names and the data set are correct with the Diagnostic Information Message.
4. Check applications with the set data.
5. Set the I/O variables and the internal variables so as not to cause any effects on the applications when another value to the variables are unlocked.
 - Check that the variable names and the data set are correct with the Diagnostic Information Message.
 - Check that the logical data of I/O variables are the same as the physical data and the data status is GOOD.
6. Unlock the I/O variables or the internal variables.
Check that the unlocked variable names are correct with the Diagnostic Information Message.
7. Set the security level of SCS back to 2.
Check that the security level of SCS is set to 2 with the Diagnostic Information Message

● Using Inter-SCS Safety Communication Data Lock Function at Offline Download

When executing offline download of the producer SCS of inter-SCS safety communication, it is possible to prevent false trips caused by the offline download by locking inter-SCS safety communication at the consumer stations of the inter-SCS safety communication. An overview of the locking and the procedure for executing offline download is described as follows.

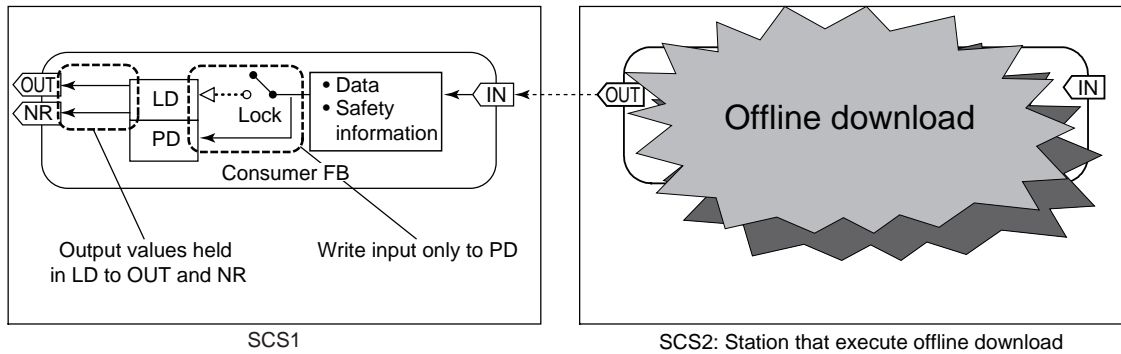


Figure 7.2.1-1 Example of Locking Inter-SCS Safety Communication at Offline Download

1. Set the security level of SCS that receives inter-SCS safety communication data from the SCS that executes offline download to 1.
Check that the security level of SCS is set to 1 with the diagnostic information messages.
2. Lock the consumer FB of the station where offline download is performed using the Inter-SCS Communication Lock window of the SCS that receives inter-SCS safety communication data.
Check that inter-SCS safety communication has been locked with diagnostic information messages.
3. Set the security level of SCS that executes offline download to 0.
Check that the security level of SCS is set to 0 with the diagnostic information messages.
4. Execute offline download.
5. Perform the output enable operation on the SCS that executed offline download.
Check the output enabled status with diagnostic information messages.
6. Check that the logical data and physical data match and that the data status is GOOD in the Inter-SCS Communication Lock window of the SCS that receives inter-SCS safety communication data.
7. Unlock the consumer FB in the Inter-SCS Communication Lock window.
Check that the inter-SCS safety communication is unlocked with diagnostic information messages.
8. Set the security level of the SCS that receives inter-SCS safety communication data to 2.
Check that the security level of SCS is set to 2 with the diagnostic information messages.

SEE ALSO

For more information about procedure of I/O Lock Window at forcing, refer to:

2., "Forcing Function" in Utilities and Maintenance Reference (IM 32Q04B20-31E)

For more information about operating Dictionary View, refer to:

"Dictionary View" of the Workbench User's Guide

For more information about a function at forcing, refer to:

C10.2, "SYS_FORCE (forcing status management)" in Safety Control Station Reference (IM 32Q03B10-31E)

● Precautions for Forcing



IMPORTANT

If you lock an internal variable in SCSP2, the application execution time may become longer, i.e., the CPU load increases. Limit the use of locking of internal variables to engineering and maintenance purposes only.

- When physical data of an output channel are changed by forcing, consider possible effects on the field before performing forcing.
- During forcing, avoid conflict with override operations from an HIS. Check the output values of the SYS_OVR function block to see whether any overridden instances and instances in a status where they can be overridden exist.
Check the diagnostic information messages indicating that the switch input of an override FB was turned ON and the diagnostic information messages showing that values were overridden, and make sure not to affect the same loop unintentionally.
- When displaying variable names in a system alarm, no more than 80 single-byte characters can be displayed. Choose variable names that do not exceed this maximum length, so that variables can be identified when locking/unlocking forcing and overriding.

SEE ALSO

For more information about CPU load when internal variables are locked, refer to:

“■ Locking of Internal Variables and Performance: SCSP2” on page 2-49

■ Override

In the CENTUM Integration structure, I/O values can be set to a specified value that is different from the actual I/O value by operation from HIS while the system is controlled normally by SCS. This operation is called override.

Override can be executed at an SCS security level of 2.

Executing override requires to create application logic with the override FB.

- There are two types of override FBs. One type is grouping override FB which can handle override actions in a group. The other is override FB which does not handle override in a group.
- If the total number of override FBs and grouping override FBs in the ready state for overriding exceeds the limit specified by the SYS_OVR function block, a diagnostic information message is issued to inform user of it.
- If the total number of overridden override FBs and grouping override FBs exceeds the limit specified beforehand by the SYS_OVR function block, a diagnostic information message is issued to inform user of it.
- If the duration in the ready state for overriding exceeds the limit specified beforehand by the SYS_OVR function block, a diagnostic information message is issued to inform user of it.
- If the duration of override exceeds the limit specified beforehand by the SYS_OVR function block, a diagnostic information message is issued to inform user of it.
- Using the SYS_OVR FB can forcefully cancel override for all variables.

SEE ALSO For more information about handling the override FBs, refer to:

D3.5, "Status management of function blocks used for override" in Safety Control Station Reference (IM 32Q03B10-31E)

● **Example of Application of Override**

The following figure illustrates an example of application where override is executed.

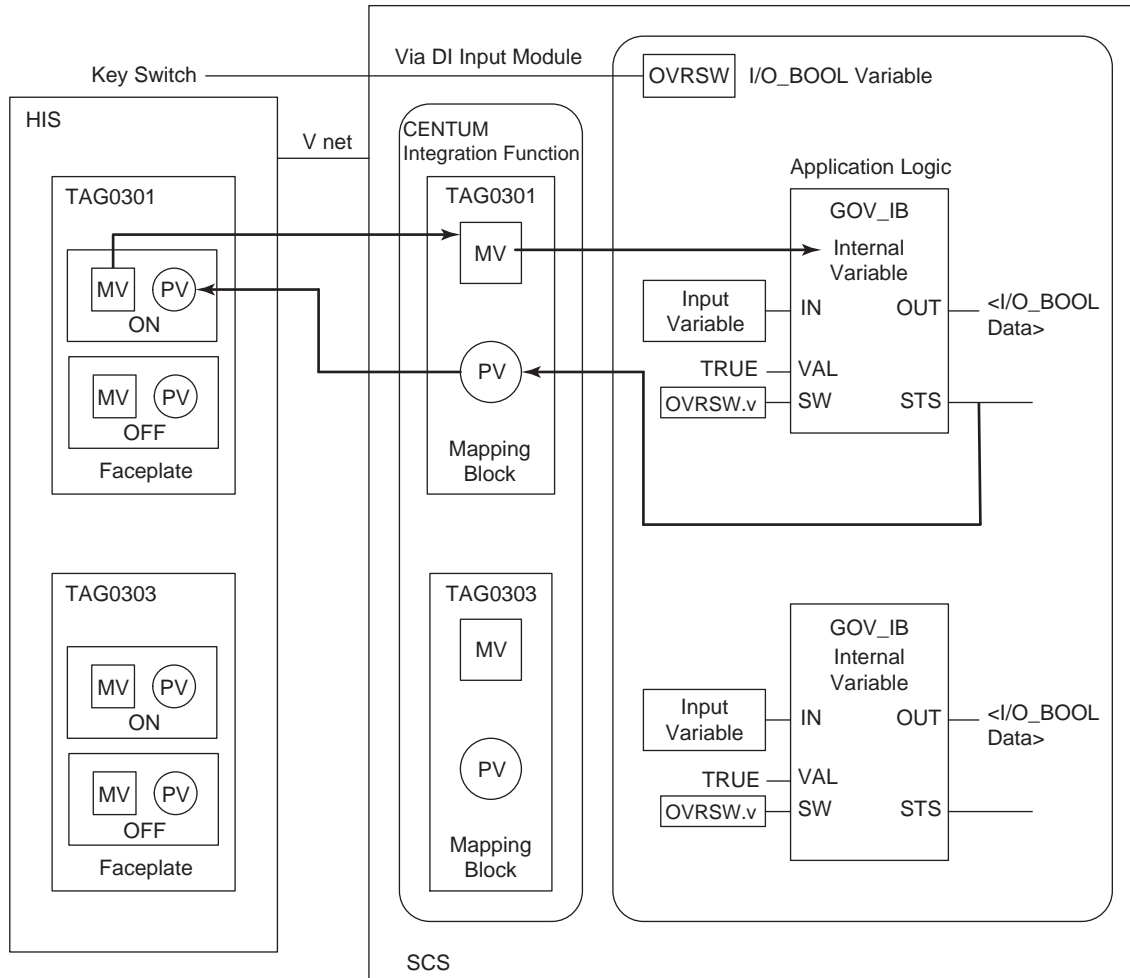


Figure 7.2.1-2 Override from HIS (Example of GOV_IB)

This describes the Override function with the GOV_IB function block.

Override from HIS is executed with the override function block (e.g. OVR_IB). Different Override FBs are available corresponding to the type of overridden variable. Mapping blocks (e.g. TAG0301) help override operation from a faceplate of HIS to the override FB.

Action of Override FB

- Without being overridden, data input from the IN parameter is output from the OUT parameter without any changes.
- When override is used, the override FB outputs data specified to the VAL input parameter, from the OUT parameter. This means the data is locked to the value which has already been defined to VAL.
- When override is cancelled, the override FB outputs the data input from IN again to OUT.
- To execute override, it is required that the override FB's SW parameter which enables override is TRUE and that override is operated from HIS.

- When user executes override from a faceplate of HIS while SW is TRUE, the Data Item MV of mapping block is set to 1 (override instruction). Then, the content of MV is reflected on the internal variable of override FB. The override FB checks the validity of the set data. When the test is passed, the override FB goes into the override status.
- A system alarm message is output if override is enabled for an FB while there are no override-enabled FBs. A system alarm message is also output if override is disabled for the last remaining override-enabled FB, resulting in no override-enabled FBs.
- When the override FB goes into the override status and when the status is cancelled, a diagnostic information message including the instance name and tag name of override FB is issued.

SEE ALSO

For more information about overrides, refer to:

D3.3, "Overview of grouping override function block" in Safety Control Station Reference (IM 32Q03B10-31E)

● Create Applications for Override

To execute override, it is necessary to create application logic with the override FB.

1. Function blocks that meet the requirements of override FB or grouping override FB should be used.
2. Use the override function blocks, which correspond to the type of variables on which override will be executed.
3. Connect an input variable to the IN input parameter. Connect the variable on which override is executed to the OUT output parameter.
4. Define the overriding value to the VAL input parameter.
5. Use the SW input so that override cannot be executed without permission. Do not connect the TRUE value to the SW input.

● Operational Procedure of Override

In this operational procedure, override is enabled/disabled by connecting a discrete input from a key switch with the SW input parameter of the override function blocks. Using the Password FB allows you to switch override through a password from HIS without the key switch.

1. The override function block goes into the ready status for overriding by turning the key switch to "Ready for override from HIS."
Confirm from HIS that a system alarm is output, which indicates override is enabled.
2. Switch the MV of a faceplate on HIS from which override is operated, to "ON." When override becomes effective, the value of the VAL input parameter specified by the override function block is output from the OUT output parameter.
 - A system alarm which notices override is displayed. As instance name and tag name in the override function block are included in this system alarm, confirm they are appropriate.
 - PV of the faceplate reads back the output from the STS parameter in the override function block. Confirm that both MV and PV are "ON."
3. Provide necessary maintenance while override is being performed.
4. Set MV to "OFF" from the faceplate after maintenance to cancel override. When override is canceled, the value from the IN input parameter is output from the OUT output parameter without any changes. The STS output parameter of GOV_IB changes from 1 to 0.
 - Confirm that a system alarm indicating override has been canceled on HIS is displayed. As instance name and tag name in the override function block are included in this system alarm, confirm they are appropriate.
 - Confirm that both MV and PV are "OFF" on the a faceplate.

5. Turn the key switch to the original position to disable override from HIS.
Confirm that the system alarm indicating override is disabled.

● **Differences between Override FB and Grouping Override FB**

The differences between the override FB and the grouping override FB are listed. The override FB and the grouping override FB act differently when the override permission signal becomes OFF during override. Therefore, it is recommended not to mix the two types of override FBs. Moreover, between override FB and grouping override FB, the exclusive override cannot be executed.

Table 7.2.1-4 Differences between Override FB and Grouping Override FB

Feature	Override FB	Grouping Override FB
Grouping function of grouping override FB	No	Yes
Action when override permission (SW) becomes OFF	Override continues	Override stops when permission signal changes from TRUE to FALSE.
Status display on mapping block	No	MAN: Override executable (operational from HIS) AUT: Override not executable (non operational from HIS)
MV of mapping block when override is automatically released (*1)	MV=1 (Answerback error)	MV=0 (Auto reset)
Manipulating the MV of mapping block when permission (SW) is OFF	Can be changed to MV=1, but it indicates answerback error.	Since the block mode is in AUT, an operation error message will be displayed. MV cannot be changed.
Overridden variables	BOOL(OVR_B) IO_BOOL(OVR_IB) DINT(OVR_I) REAL(OVR_R) IO_REAL(OVR_IR)	BOOL(GOV_B) IO_BOOL(GOV_IB)

*1: Automatic release of override
Under the following circumstances, the override will be automatically released.

- SYS_OVR sent a forcibly release override signal(to override FB or grouping override FB)
- Permission signal changes from TRUE to FALSE (grouping override FB)
- Group numbers are changed (grouping override FB)

In the grouping function of override FB with grouping function, override groups can be created by assigning group numbers to grouping override FBs. When the override permission signal changes to TRUE, the override FB becomes overridable. If multiple grouping override FBs have the identical group number, only one of the grouping override FBs can be overridden at a time. In other words, other grouping override FBs in the same group cannot be overridden until the currently overridden FB is released. Grouping management is not applied to the override FBs whose group number is 0.

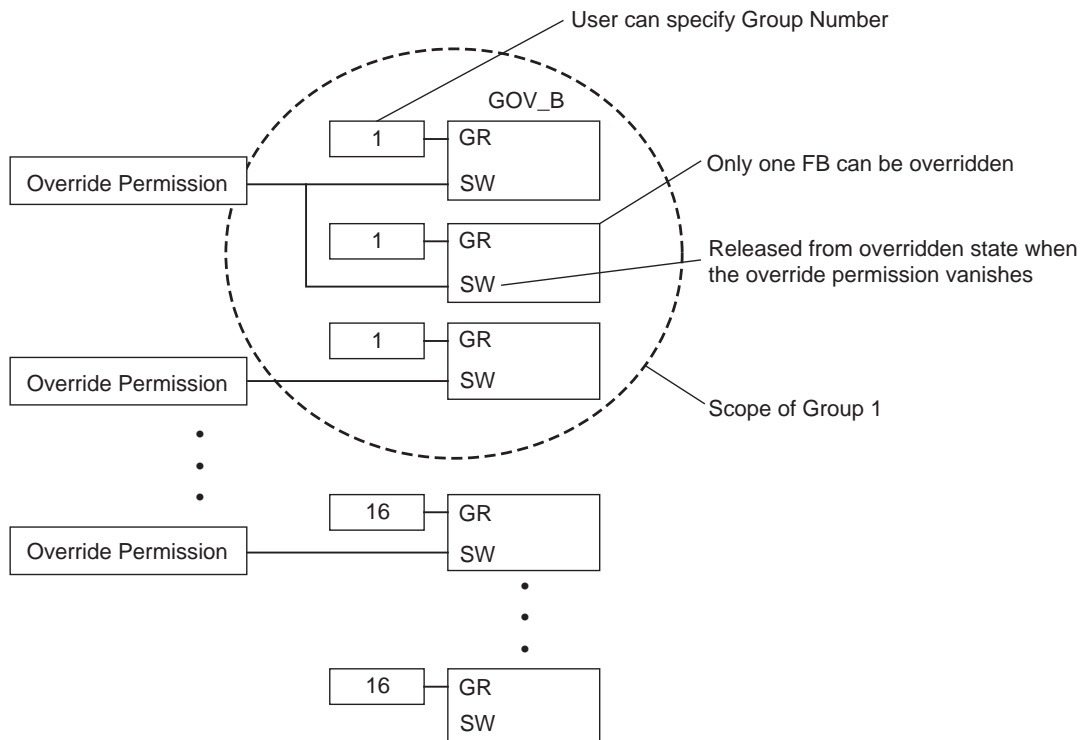


Figure 7.2.1-3 Grouping Override FB Overview

SEE ALSO

For more information about a procedure of override, refer to:

[D3., "Override operation from HIS" in Safety Control Station Reference \(IM 32Q03B10-31E\)](#)

● **Precautions for Override**

- The length of variable name displayed as a system alarm is 80 characters at maximum. Set a variable name length not to exceed the maximum so that the variable name can be identified when forcing and override are enabled/disabled.
- Do not execute online change while executing override from HIS.
- When using the Password FB, set different passwords for each FB.
- If a permission signal SW is from a DI, and the permission signal becomes FALSE due to a DI related device fault, the override will be automatically released.
- When group number is mistakenly specified, the system cannot find this error. Therefore, during the logic test, if the group numbers have been properly specified or not must be carefully inspected.
- During override, do not use online change to change the group number and run online change downloading. If you do, override is automatically deactivated. If you assign a variable to a group number and change the variable value, override is automatically deactivated.

■ **Locking for Online Change Download**

When online change has to be executed on an I/O module and application logic while SCS is in operation, investigate the need to lock the I/O module to avoid a nuisance tripping, and lock the I/O module if necessary.

The following figure shows the procedure to lock the I/O module prior to online change download.

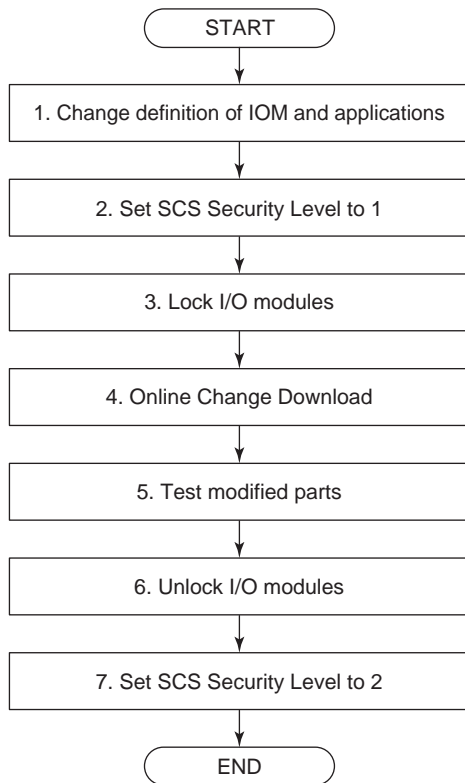


Figure 7.2.1-4 Procedure to Lock I/O Module Prior to Online Change Download

1. The engineer modifies the SCS database with the SCS Manager of SENG and uses the Integrity Analyzer and Cross Reference Analyzer to analyze the modified application. If the application logic has also been modified, use the logic simulation test to check the modifications.
2. Change the SCS security level to Level 1 by using the SCS Security Level Operation Dialog.
3. Locking all I/O modules related to online change with the I/O Lock Window is recommended.
4. Perform an online change download.
5. Start the Debug mode for checking the modified parts.
6. Unlock all locked I/O modules with the I/O Lock Window. At this time, check with great care whether the output values are changed or not. Finish the Debug mode after unlocking the I/O modules.
7. Return the SCS security level to Level 2 by using the SCS Security Level Operation Dialog.



WARNING

If you change some settings of an output module and perform an online change download to an SCS in R2.01 or earlier system program release number, you need to prevent the system from an unexpected shutdown when the value of the output module becomes 0. Preventive measure should be taken on the field device side in advance.

**SEE
ALSO**

For more information about online change, refer to:

5., "Online Change of Applications" on page 5-1

For more information about I/O Module lock/unlock operation, refer to:

2., "Forcing Function" in Utilities and Maintenance Reference (IM 32Q04B20-31E)

7.2.2 Maintenance for ProSafe-RS Equipment

With SCS, procedures for maintenance vary depending on faults such as when dual-redundant CPU module or I/O module is replaced because of a fault or when a module in a single configuration fails. Take care for the maintenance procedure not to cause a nuisance tripping when maintenance is performed during running the plant.

■ Actions to be Taken Upon Device Errors

The following list describes the actions to be taken when you detect hardware errors by system alarms on an HIS or alarm devices such as alarm lamps indicating generation of diagnostic information messages that notify errors.

1. Use the SCS Maintenance Support Tool of the SENG to identify the failed location and cause.
2. Repair the failed location. When a CPU module or I/O module of an SCS stops, you may need to replace the module. Replace the module by following the applicable procedure and precautions specified in the user's manual.
3. Check in the SCS State Management window, or from the fact that the alarm statuses of alarm devices are reset, that all hardware has been serviced properly.

● Precautions for ProSafe-RS Device Maintenance

Exercise caution when maintaining the ProSafe-RS device that each device operates as described as follows:

- It takes about 8 seconds for an I/O module to be back to the normal state when I/O module recovers from a failure such as when applying the power to I/O module.
- When executing the APC operation for dual-redundant SCS, a COPY message is issued twice.
- When one power supply module of the "CPU node" fails, it is reported that the power supply modules of "CPU node" and of "I/O node 1" fail. As a result, two diagnostic information messages are issued.

■ Maintenance of CPU Modules

The procedure to be taken when the CPU module fails varies depending on whether the CPU module is of single configuration or dual-redundant configuration.

● CPU Module Failure (Single Configuration)

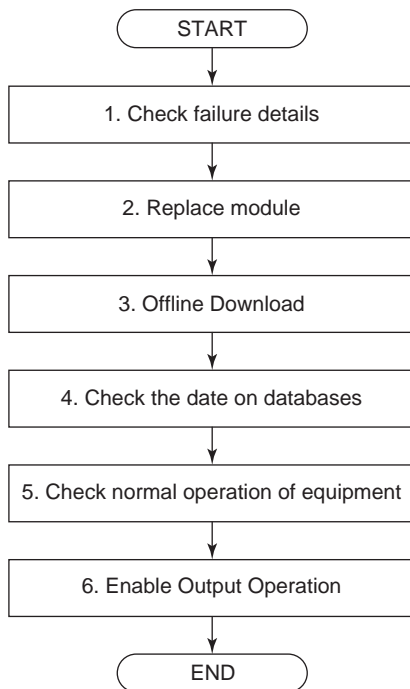


Figure 7.2.2-1 CPU Module Failure (Single Configuration)

1. The engineer starts the SCS State Management window from SENG of the SCS where a fault occurs and confirms the diagnostic information message. Confirm the measures against the fault with the Help Dialog of Diagnostic Information Message and determine whether to replace the CPU module.
2. If the module needs to be replaced as a result of the step 1, the maintenance personnel removes the failed CPU module from the node and installs a new CPU module.
3. The engineer executes master database offline download from SENG. (If downloading to the CPU module has been executed even once, the last application remains in the flash memory of the CPU module. Be sure to execute master database offline download after replacing the CPU module.)
4. The CPU module starts after the download is completed. The engineer displays date of each database for POU DB, Variable DB, System DB and Integration DB on the Database Validity Check Tool, when the SCS is in waiting mode, to confirm that latest version is loaded.
5. The maintenance personnel confirm that the CPU module has started normally from the SCS State Management window in SENG or from LED of the CPU module. Furthermore, the engineer confirms that all SCS equipment are in normal state with the SCS State Management window.
6. The maintenance personnel perform the enable output operation from the SCS State Management window.

**SEE
ALSO**

For more information about the Output Enable Operation, refer to:

[3.1.6, "Output Enable Operation" in Utilities and Maintenance Reference \(IM 32Q04B20-31E\)](#)

● CPU Module Failure (Dual-Redundant Configuration)

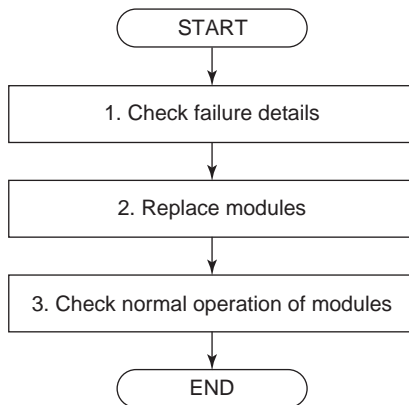


Figure 7.2.2-2 CPU Module Failure (Dual-Redundant Configuration)

1. The engineer starts the SCS State Management window from SENG of the SCS where a fault occurs and confirms the diagnostic information message. Confirm the measures against the fault with the Help Dialog of Diagnostic Information Message and determine whether to replace the CPU module.
2. If the module needs to be replaced as a result of the step 1, the maintenance personnel removes the failed CPU module (on standby) from the node and installs a new CPU module.
3. When the new CPU module is installed, programs and databases of the CPU module on control are automatically copied to the new CPU module. The maintenance personnel confirms with LED of the module or the SCS State Management window in SENG that the module has started normally.



IMPORTANT

Do not pull out the CPU module online and turn off the power while the module is writing to the flash memory. Whether the CPU module is writing can be confirmed by using LED of the CPU module.

SEE ALSO

For more information about the actions when an error has occurred and the procedure for recovery, refer to:

[B6. "Actions taken at error occurrence and recovery procedure" in Safety Control Station Reference \(IM 32Q03B10-31E\)](#)

● Password Setting in Replacing CPU

- If CPU is in dual-redundant configuration and you must replace the standby side, there is no need to re-set passwords for the work. After the Standby side is replaced, the passwords for changing Security level stored in the control side are automatically copied to the standby side.
- In a single CPU configuration, if the CPU is replaced and programs remain in the memory on the new CPU module, the CPU starts. Its Operating mode is Waiting, so output value of application logic is not output to the field.
In this status, press Reset switch, stop the CPU, and offline download the master database. After completion of the download and the CPU is started, set the passwords. The passwords in the memory on the CPU module is initialized, so there is no need to enter the previous passwords.

- In a single CPU configuration, if the CPU is replaced and no program remains in the CPU memory on the new CPU module, the CPU is in a halt status. In that status, offline downloads the master database. After completion of the download and the CPU is started, set the passwords. There is no need to enter the previous passwords.

■ Maintenance of I/O Modules

If the I/O module generates an error, use the IOM Report to investigate the cause before commencing troubleshooting. Note that a failure on the field side is sometimes reported as an error of the I/O module of the ProSafe-RS. If this is the case, the I/O module may not have to be replaced once the failure on the field side is reset, even when the IOM Report error code indicates a hardware failure of the I/O module.

SEE ALSO

For more information about Details on IOM Report, refer to:

[B4., "Notification of diagnostic information using the IOM Report" in Safety Control Station Reference \(IM 32Q03B10-31E\)](#)

● Overview of I/O Module Maintenance Procedure and Precautions

If the I/O module stops, follow these steps to perform maintenance.



IMPORTANT

Observe the following precautions when fixing one stopped module of the dual-redundant I/O modules:

- Do not pull out and insert the stopped I/O module again.
- Do not insert the I/O module that is not assured as normal when exchanging I/O modules.

Failure to observe the above-mentioned cautions may lead to an impact on the field side.

1. Use the IOM Report of the SCS Maintenance Support Tool to check the error code of the I/O module failure.
2. If the error code does not indicate a hardware failure, take the action described in the IOM Report.
3. If the error code indicates a hardware failure that cannot be caused by a failure on the field side, follow the correct procedure to replace the faulty I/O module with one functioning normally. If the error code indicates a hardware failure that may have been caused by a failure on the field side, investigate the field side first.
 - a. If a cause is found on the field side, remove the cause and then restore the I/O module.
 - b. If no cause is found on the field side and it is determined that the I/O module hardware is faulty, follow the correct procedure to replace the faulty I/O module with one functioning normally.

SEE ALSO

For more information about Procedure for replacing the I/O module, refer to:

“● Procedure for Replacing the I/O Module” on page 7-25

● Hardware Failure Error Codes Possibly Caused by Failures on the Field Side

The cause of the I/O module stopping can be checked in the IOM Report.

Even when the IOM Report shows an error code for hardware failure, the module may have actually stopped due to a failure on the field side, not a hardware error. If the IOM Report shows any of the following error codes, follow the troubleshooting procedure that applies when there is a possibility of a failure on the field side.

Table 7.2.2-1 IOM Report Error Codes Possibly Caused by Failures on the Field Side

Code (hexadecimal)	Display	Description
0101 5502 0401 5502 (*1)	Output Readback Error	An error has been detected in the readback process for the output value. Check the field wiring of the analog output module for any abnormality such as inter-channel short circuit, and also confirm that the total resistance of all connected cables and devices does not exceed the allowable output load resistance of the output module, which is specified in the General Specifications (GS).
0101 5504 0401 5504	Output Channel Failed ON	A failure that the output channel is unable to change from ON to OFF has been detected. Check if there are any field wiring errors such as inter-channel short circuit.
0107 5507 0407 5507 (*1)	IOM Channel Fail	There have been some errors with the channel area of the input/output module. Check if there is any input of a signal value at a level between ON and OFF or chattering.

*1: For a channel failure, the error codes and the statuses of failures vary depending on whether the input/output module is in the redundant configuration or non-redundant configuration.

- The upper error code is for a redundantly configured I/O module, while the lower error code is for a non-redundantly configured I/O module.
- If the input/output module is in a redundant configuration, this error will be an IOM Fail error. In a non-redundant configuration, the error will occur only to the failed channel.

● **Troubleshooting Procedure When Error is Possibly Caused by Failures on the Field Side**

If the IOM Report shows an error code indicating a hardware failure that may have been caused by a failure on the field side, investigate the cause on the field side first. If the cause explained in the IOM Report is found on the field side, the I/O module will return to normal once the cause is removed and the module is reset.

The following list describes the troubleshooting procedure to be followed after a cause of failure on the field side is found.

1. Repair the wiring error or failure on the field side to remove the cause of error corresponding to the error code.
2. Reset the I/O module that has stopped. The resetting method differs depending on the system program release number of the SCS. Perform IOM reset for the applicable release number.
 - SCS system program release number is R3.02.00 or later
Select the stopped I/O module and execute IOM download manually. IOM reset is performed at the same time.

TIP

IOM reset only covers AIO/DIO modules of single configuration and standby AIO/DIO modules of dual-redundant configuration when HRDY of both configurations is turned OFF.

- SCS system program release number is earlier than R3.02.00
Pull out and insert the I/O module again. IOM reset is performed.
3. Check that the I/O module has recovered to normal in the SCS State Management window.

4. After an output module has recovered normally, perform the output enable operation in the SCS State Management window.

**SEE
ALSO**

For more information about IOM Download operation, refer to:

[3.1.7, "IOM Download Tool" in Utilities and Maintenance Reference \(IM 32Q04B20-31E\)](#)

● Procedure for Replacing the I/O Module

1. If it is determined that the I/O module hardware is faulty, replace the faulty I/O module with one that is functioning normally.
2. After replacing the module, perform IOM download.
However, in the case where you replace the standby side module of dual-redundant AIO/DIO modules of an SCS installed with the system program release number of R2.03 or later, you do not need to execute IOM download manually if you have specified the "Automatic IOM Download" setting to Enable.

TIP

To enable automatic IOM download, set "[Automatic IOM Download]" to "[Enable]" in the SCS Constants Builder. Once it's set, the SCS automatically downloads configuration information from the control side module to the standby side module after the module is replaced.

3. Check in the SCS State Management window, or from the fact that the alarm statuses of alarm devices are reset, that the replaced module is operating correctly.

**SEE
ALSO**

For more information about how to replace input/output modules, refer to:

[7.3, "Replacing Input/Output Modules" in Safety Control Stations \(Hardware\) \(IM 32Q06C10-31E\)](#)

■ Procedure of Changing Single/Dual-redundant Specification of AIO/DIO Modules

Follow these steps to offline change the single/dual-redundant specification of AIO/DIO modules:

1. Disconnect the I/O cables (or terminal blocks) of the modules.
2. If you change two adjacent existing single modules to dual-redundant configuration, pull out one of the modules and insert it again.
3. Change the definition in the I/O Wiring View and perform offline download.
4. Connect the I/O cables (or terminal blocks).

7.2.3 Maintenance of Field Devices

For maintenance of field devices, it is necessary to take measures on the ProSafe-RS side so as not to cause a nuisance tripping due to field signals changed by maintenance. The procedure for maintenance of field devices is as follows.

1. Take required bypass to avoid generating a nuisance tripping due to maintenance.
2. Perform maintenance of field devices.
3. Test field devices.
4. Remove the bypass taken in step 1.

In ProSafe-RS, I/O values related to maintenance are locked with either of the following ways to avoid a nuisance tripping during maintenance.

- Forcing from SENG
- Override from HIS in CENTUM Integration Structure

7.2.4 Proof Test

A proof test is a periodic test to verify that the functions of safety loops, which consist of a sensor, logic solver and final element, work without fails.

The proof test items for logic solvers (ProSafe-RS) are described as follows.

■ Checking the Channels of Input/Output Modules

Change the input value or output value of each channel of the modules and check if the modules work as intended.

For dual-redundant modules, check on both modules.

■ Control Right Switch Over (for Redundant CPU Modules and Input/Output Modules)

To ensure high availability, use the following procedures to check that switchover takes place properly on dual-redundant modules.

● CPU Modules

1. To make a switch over, press the START/STOP switch in the front of the control-side CPU module to stop it.
2. Press the START/STOP switch of the failed module once again to restart it. The module should start up as a standby-side.

● Input/Output Modules

Use the IOM Control Right Switching Tool to make switchover on AIO/DIO modules. This tool switches the control right of dual-redundant AIO/DIO modules from the SENG.

By using this tool, the control right will be switched over to the modules on the standby-side.

However, you cannot use this tool on dual-redundant serial communication modules (ALR111, ALR121).

You can start the IOM Control Right Switching Tool from Explorer. Switch over can be made either for a selected pair of AIO/DIO modules or collectively on a node-by-node basis.

**SEE
ALSO**

For more information about the START/STOP switch of the CPU module and status display, refer to:

[4.2, "Processor Module" in Safety Control Stations \(Hardware\) \(IM 32Q06C10-31E\)](#)

For more information about the IOM Control Right Switching Tool, refer to:

[5.2, "IOM Control Right Switching Tool" in Utilities and Maintenance Reference \(IM 32Q04B20-31E\)](#)

8. Self Document

This chapter describes the Self Document Function.

■ Outline of Self Document Function

Self Document is a function of printing applications as documents.

Self Document enables the following things.

● Selecting Print Data

Source files of work databases in an SCS project can be printed. All contents of the definitions or any parts can be selected.

The following table shows an outline of data which can be printed.

Table 8-1 Data to be printed

Data to be printed	Details of Definition
Cover	
Table of Contents	
SCS project information(*1)	Data defined with SCS Manager (Project/Configuration/Resource/Properties of each project)
SCS constant data	Data defined with SCS Constants Builder
I/O parameter data	Data defined with I/O Parameter Builder
Subsystem communication I/O information (*2)	Data defined with Communication I/O Builder
SCS Link Transmission data	Data defined with SCS Link Transmission Builder
Global variable data	Data defined with SCS Manager (Global variable data)
Binding data	Data defined with SCS Manager (Binding data)
Modbus address information(*3)	Data defined with Modbus Address Builder
DNP3 communication definition information (*4)	Data defined with DNP3 Communication Builder
Tag name information (*5)	Data defined with Tag Name Builder
Alarm Priority data(*5)	Data defined with Alarm Priority Builder
Alarm Processing Table data(*5)	Data defined with Alarm Processing Table Builder
POU data	<ul style="list-style-type: none"> • Data defined with SCS Manager • Data defined with Multi-Language Editor

*1: It includes the data concerning the CENTUM connection function.

*2: This is the data concerning the subsystem communication.

*3: This is the data concerning the open interface.

*4: Printable only when the version of SCSU1 is R3.02.20 or later.

*5: This is the data concerning the CENTUM connection function.

● Customizing what to Print

The content to print can be customized as follows:

- Cover and contents pages can be created.
- Headers and footers can be created.
- Page numbers can be included.
- Font types can be specified.
- Paper orientation (landscape or portrait) for FBD and LD can be specified.

- **Confirming Preview**

Printing images can be confirmed.

- **Selecting Printer**

A printer directly connected to SENG and connected via networks can be used.

**SEE
ALSO**

For more information about Self document function and its operation, refer to:

[10., "Self-documentation" in Engineering Reference \(IM 32Q04B10-31E\)](#)

■ **Precautions for Using Self Documents**

Save files which are being edited before printing the application.

9. FAST/TOOLS Integrated System Using SCSU1

SCSU1 is the station dedicated for use in systems integrated with FAST/TOOLS. Its functions to realize integration with FAST/TOOLS are basically the same as those of SCSP1 and SCSP2. By using SCSU1, you can implement the following specifications that are not available with SCSP1 or SCSP2:

- **System configuration**
SCSU1 can be connected to Vnet/IP-Upstream networks only. SCSU1 cannot be connected to Vnet/IP or V net of systems that are integrated with CENTUM. It must be physically separated.
- **Specification of narrowband communication**
Bandwidth of 2 Mbps or higher and lower than 100 Mbps is defined as narrowband. SCSU1 can perform communication in the Narrowband mode. For Narrowband mode communication, you must build the network by using a communication line with BER (Bit Error Rate) of 10^{-6} or lower. If a public line is used as inter-exchange channel, VPN (Virtual Private Network) cannot be used. Because SCSP1 and SCSP2 cannot perform communication in the Narrowband mode, they cannot be connected to Vnet/IP-Upstream domains in the Narrowband mode. To realize narrowband communication by using SCSU1, set up all the connected Vnet/IP-Upstream domains in the Narrowband mode.
- **Narrowband system**
A system that contains narrowband lines in communication paths and operates in the Narrowband mode is defined as a narrowband system.
- **Narrowband group definitions**
Grouping SCSU1 stations that share the same narrowband line in communication paths is called narrowband group definition. In a narrowband group definition, the communication traffic on the network is restricted by limiting the number of the window of SENG which displays the information on SCS.
- **Data buffering function**
The data buffering function buffers application logic data of SCSU1 with time stamp so that they can be collected from FAST/TOOLS.
- **Gas flow rate calculation**
The gas flow rate calculation function calculates gas flow rates according to the AGA (American Gas Association) specification and creates hourly and daily reports.

The system should be engineered so that all abnormalities occurred in SCSU1 are notified to users through FAST/TOOLS. When an abnormality occurs in SCSU1, the user must start the SENG used to engineer the concerned SCSU1 to check the details of the abnormality and take corrective actions.

**SEE
ALSO**

For more information about basic specification of FAST/TOOLS integrated systems, refer to:

[2.23, "FAST/TOOLS Integrated Configuration" on page 2-143](#)

For more information about precautions to assign a tag name to function blocks and annunciators, refer to:

["● Online Change Download" on page 5-16](#)

9.1 FAST/TOOLS Integrated System Configuration Using SCSU1

A Vnet/IP-Upstream network is used in FAST/TOOLS integrated system configuration. For a system using SCSU1, you can set up the Vnet/IP-Upstream network in the Narrowband mode. Connections are limited in the Narrowband mode.

■ Example of Narrowband System Configuration

In a Narrowband mode Vnet/IP-Upstream network, you can include lines with bandwidth of 2 Mbps or higher and lower than 100 Mbps and connect two or more Vnet/IP-Upstream domains through a L3SW. All Vnet/IP-Upstream domains connected must be in the Narrowband mode. You cannot set other modes for individual domains.

In the Narrowband mode, the number of stations that can be connected and the amount of communication traffic varies depending on the bandwidth of the line. The Narrowband mode uses the same communication interface as the Standard mode, however, the hardware and the drivers that perform communication operate according to the specification of the Narrowband mode.

To accommodate the delay in response due to the narrow bandwidth of the line, you can set a limit on the number of SCSs from which the SENG collects data at a time.

The following figure shows an example of the narrowband system configuration.

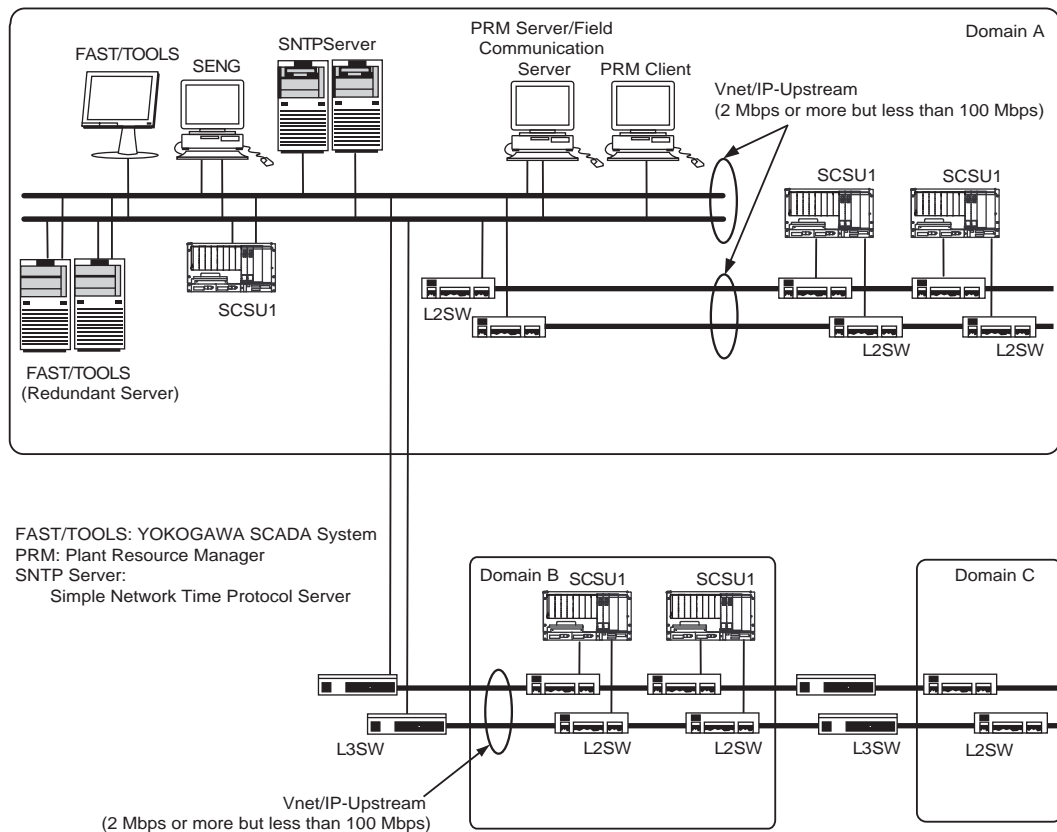


Figure 9.1-1 Example of Narrowband System Configuration

The firmware version of CPU modules of SCSU1 and the Vnet/IP interface cards connected to a Vnet/IP-Upstream network must be Rev. 19 or later.

For Narrowband mode communication, you must build the network by using a communication line with BER (Bit Error Rate) of 10^{-6} or lower. When the line quality of the Narrowband mode is guaranteed, offline download can be performed.

For information about how to check the firmware version, please contact Yokogawa.

**SEE
ALSO**

For more information about basic specification of FAST/TOOLS integrated systems, refer to:

[2.23, "FAST/TOOLS Integrated Configuration" on page 2-143](#)

■ Limitations of Connection

The limitations of connection in the Narrowband mode are as follows:

- A ProSafe-RS system integrated with CENTUM cannot be connected to a Vnet/IP-Upstream network.
- A Vnet/IP-Upstream network in the Narrowband mode and another Vnet/IP-Upstream network in a different mode cannot be connected each other.
- Devices, except for FCN/FCJ, that perform open communication cannot be connected to a Vnet/IP-Upstream network.
- SCSP1 and SCSP2 cannot be connected on a Vnet/IP-Upstream network in the Narrowband mode.
- PRM servers cannot be connected on a Vnet/IP-Upstream network in the Narrowband mode.

■ Avoiding Mixture of Narrowband Mode with Other Modes



IMPORTANT

The prohibitions to prevent mixing Narrowband mode with other modes are as follows:

- Do not connect Vnet/IP devices that do not support the Narrowband mode to the Vnet/IP-Upstream network in the Narrowband mode. If they are connected, excessive communication traffic is generated on the network, which can cause communication errors in the narrowband network because the communication is performed using the same bandwidth as the Standard mode.
- Do not connect two networks that operate in different modes.

If a network in the Narrowband mode is mixed with a network in a different mode, FAST/TOOLS notifies a user with an alarm. Devices that do not support the Narrowband mode or networks operating in other modes must be isolated from the network operating in the Narrowband mode.

**SEE
ALSO**

For more information about procedures to add stations to Vnet/IP-Upstream, refer to:

[C5.2, "Procedures and precautions for adding a station or domain" in Integration with FAST/TOOLS \(IM 32Q56H20-31E\)](#)

9.2 Narrowband System Environment

To engineer a narrowband system, information on the operating environment, hardware specifications, and station configuration are needed.

The following figure shows an example of a narrowband system connected on a Vnet/IP-Upstream network.

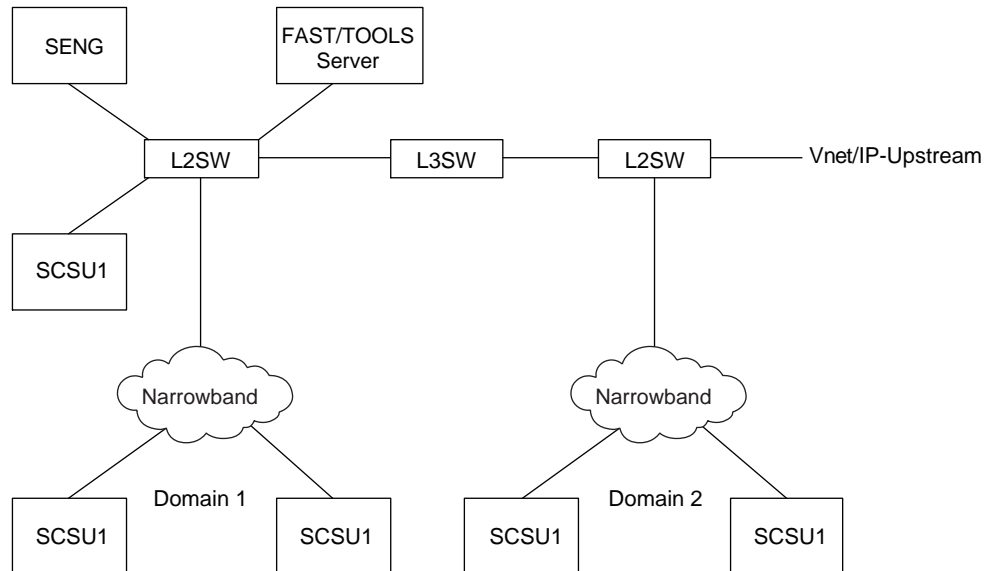


Figure 9.2-1 Example of Narrowband System Configuration Connected on a Vnet/IP-Upstream network

When narrowband networks with 2 Mbps or higher and lower than 100 Mbps are included in the Vnet/IP-Upstream network, use Vnet/IP-Upstream in Narrowband mode. The narrowband mode of Vnet/IP-Upstream supports two or more Vnet/IP-Upstream domains through a L3SW. Because the bandwidth used in Narrowband mode is low compared with Standard and Wide-area modes, the number of stations and available functions are limited.

■ Operating Environment

To use a Vnet/IP-Upstream network in Narrowband mode for a FAST/TOOLS integrated system, the hardware and software must be configured for Narrowband mode. To perform communication in Narrowband mode, use only SCSU1 as SCSs. If SCSP2 or SCSP1 exists, in the network communication cannot be performed in Narrowband mode.

■ Hardware Specification to Communicate in the Narrowband Mode

In the stations that are connected in a narrowband system, install the Vnet/IP device with the following specifications. Stations that include Vnet/IP devices that do not comply with the following specifications cannot be connected in narrowband systems.

- VI702/VI701 (Vnet/IP interface card installed in PC components such as SENG)
Firmware revision (F) should be 19 or later.
- SCP451 (Processor module installed in SSC57S/SSC57D)
Firmware revision (F1) should be 19 or later.

■ Software Specification to Communicate in the Narrowband Mode

Use ProSafe-RS software of release number R3.02.10 or later on SENG.

■ Scale of the System

The scale of FAST/TOOLS-integrated systems in the Narrowband mode is as follows:

- Connectable control bus: Vnet/IP-Upstream
- Number of connectable domains: Up to 31 Vnet/IP-Upstream domains
- Number of connectable stations within one domain: 64
- Number of connectable stations: Limited by estimated communication bandwidth
- Hop count in connected domains: Up to 15 hops via L3SW
- Distance between stations within a domain: max. 10000 km
- Propagation delay: 500 ms or less
- Number of Layer 2 switches that connect stations within a domain: unlimited

■ Overview of the communication procedure in Narrowband mode for SCS Maintenance Support Tool

This section describes an overview of the communication procedure in Narrowband mode, comparing with the procedure in Standard/Wide-area modes.

In Standard/Wide-area modes, Message Cache Service periodically creates a list of SCSs it actually communicate with, and will communicate with all the SCSs in the list one by one.

In Narrowband mode, Message Cache Service creates a list of SCSs to communicate with, and then verifies each SCS in the list referring to the narrowband group definition information. As a result of verification, the SENG will communicate only with the SCSs that meet all the following conditions:

- The SCS belongs to a narrowband group.
- The number of SCSs allowed for communication that is set for the narrowband group to which the SCS belongs is not exceeded.
- Automatic data acquisition is not suspended for the narrowband group to which the SCS belongs.
- Automatic data acquisition is enabled for the SCS, or the SCS is included in the background data acquisition.

For SENG in Narrowband mode, there is a limit on the number of windows that can be displayed by using SCS Maintenance Support Tool.

In Standard/Wide-area modes, the SENG is collecting data from SCSs while the SCS Maintenance Support Tool window is displayed. As for SOE viewer and the Diagnostic Information window, the data collection from the SCSs displayed in the window will continue in the background even after the window is closed. The automatic data acquisition function of Message Cache Tool periodically collects SOE events and diagnostic information messages from SCSs.

In Narrowband mode, you can start only one SOE viewer and only one Diagnostic Information window. For the collection of SOE events and diagnostic information messages, there are limits on the number of SCSs and limits of timing in which you can perform collection simultaneously. If you close the Diagnostic Information window or SOE viewer, collection in the background is stopped.

**SEE
ALSO**

For more information about definitions of a narrowband group, refer to:

C3., "Defining narrowband groups" in *Integration with FAST/TOOLS (IM 32Q56H20-31E)*

For more information about the definition method of a narrowband group, refer to:

C3.1, "Narrowband mode settings and precautions for narrowband group definition" in *Integration with FAST/TOOLS (IM 32Q56H20-31E)*

For more information about SCS Maintenance Support Tool, refer to:

3., "SCS Maintenance Support Tool" in *Utilities and Maintenance Reference (IM 32Q04B20-31E)*

● SCS status display in the Narrowband mode

In the Standard and Wide-area modes, the update cycle of SCS Status Overview window of SCS Maintenance Support Tool is 1 second. In the Narrowband mode, because the number of SCSs allowed for communication per display update cycle to retrieve status information is limited; therefore, updating of the status display is delayed depending on the limited number of communicated SCSs for each narrowband group.

The behaviors of SCS Status Overview window in the Narrowband mode are as follows:

- The SCS Status Overview window obtains SCS statuses through periodical communication with SCSs within the number of SCSs allowed for communication per display update cycle, which is set using the SCS Maintenance Support Tool.

Example:

When 20 SCSs are displayed in the SCS Status Overview window and the number of SCSs allowed for communication per display update cycle is set to 10, the SENG communicates with 10 SCSs every second to obtain the status. As a result, the status display for each SCS is updated at two second intervals.

TIP

The number of SCSs allowed for communication per display update cycle is limited by the setting in the Narrowband Group Definition window. Therefore, even if an alarm occurs in an SCS, the status of the SCS may be displayed as normal until the communication for obtaining the status of that SCS is completed.

Example:

Even if a diagnostic information message indicating Fail is broadcasted and displayed for a certain SCS, the status of that SCS remains READY.

- Blank will be displayed for the "SCS Status," "CPU Status" and "Comment" of the SCS whose status is not obtained.
- When navigating from SCS State Management window to SCS Status Overview window and then returning to SCS State Management window again, the statuses are obtained from the beginning of the SCS list of the SCS Status Overview window.
- The Diagnostic Information button for SCS whose status is not obtained is displayed in gray until the status is obtained, but the button is operational. Clicking the button displays the Diagnostic Information window to enable to check received messages.
- Even if the status in the SCS Status Overview window is not updated, SCS State Management window can be called for the SCS.
- If a narrowband group where automatic acquisition is paused exists in the Narrowband Group Definition window of the Message Cache Tool, "(Pause)" is displayed at the head of the window title of the SCS Status Overview window.
- The Suspended data acquisition checkbox does not affect update of the SCS Status Overview window. Display of SCS state list is also updated even for SCS that belongs to a narrowband group with pause state. The purpose of the Suspended data acquisition checkbox is to pause the collection of SOE events and diagnostic information messages.
- The SENG only obtains the status of SCSs that are displayed in the SCS Status Overview window and also contained in the SCS list of a narrowband group. The SENG does

not communicate with SCSs that became hidden as a result of scrolling or resizing the SCS Status Overview window.

- When the SCS displayed at the top of the list is changed by scroll operation or change of the window size, statuses are obtained again from the SCS that newly comes to the top of the list.
- When the SCS that is displayed at the top of the list is not changed by changing the window size, including by stretching the window downward to expand the display area, statuses are not obtained again from the top SCS but update of statuses is continued from the SCS next to the one that was updated before the change of the window size.
- When a displayed SCS is deleted from a narrowband group, the SCS Status Overview window continues to display the status before the SCS is deleted.
If you have deleted an SCS or a narrowband group definition in the Narrowband Group Definition window, display the window again to display the latest state.

● Behaviors of Message Cache Tool in Narrowband mode

Behaviors of the Message Cache Tool in Narrowband mode are as follows:

- Cache data that is stored in other SENG cannot be referred. The controls on Setup dialog box that adds other SENG to be referred is disabled.
For example, you cannot add stations in the Setup dialog box in Narrowband mode.
- The Narrowband Group Definition Window button on the Setup dialog box becomes active.
- If a narrowband group where the automatic acquisition is paused exists in the Narrowband Group Definition window of the Message Cache Tool, "(Pause)" is displayed at the head of the window title of the Message Cache Tool.

● Behaviors of the Diagnostic Information window in the Narrowband mode

The following are limitations on the Diagnostic Information window in Narrowband mode:

- Only one Diagnostic Information window can be displayed.
- When the Diagnostic Information window is closed, the background acquisition of diagnostic information messages on the displayed SCS is stopped.
To display the latest diagnostic information messages on SCS for which automatic data acquisition is not specified in the Narrowband Group Definition window of the Message Cache Tool, keep the Diagnostic Information window opened.
- Because the number of SCSs allowed for communication in each data acquisition cycle is limited, the Narrowband mode takes more time to display all the previous diagnostic information messages, compared to Standard mode and Wide-area mode.
- Because the number of SCSs allowed for communication in each data acquisition cycle is limited, if the SENG fails to receive any latest diagnostic information messages, the Narrowband mode takes more time to display the missing messages in the Diagnostic Information window, compared to Standard mode and Wide-area mode.
- If a narrowband group where automatic acquisition is paused exists in the Narrowband Group Definition window of the Message Cache Tool, "(Pause)" is displayed at the head of the title of the Diagnostic Information window.
- When an SCS is deleted from a narrowband group while its diagnostic information message is being displayed, the messages of that SCS will no longer be updated in the Diagnostic Information window. In this situation, ACK and DEL operations have no effect on the messages of the deleted SCS.
When you have deleted an SCS or a narrowband group definition in the Narrowband Group Definition window, display the window again to display the latest state.

- Diagnostic information messages of SCSs that do not belong to any narrowband group are not displayed. For such SCSs, cached messages and broadcast messages are not displayed, either.

- **Behaviors of SOE viewer in the Narrowband mode**

Behaviors of the SOE Viewer in the Narrowband mode are as follows:

- Only one window of SOE viewer can be displayed.
- Background data acquisition for the SCS displayed in SOE viewer is stopped after the viewer is closed. To display the latest diagnostic information messages of SCS not specified for automatic data acquisition, keep the SOE viewer window opened.
- If SOE viewer is kept opened, collection from the SCSs for which automatic data acquisition is enabled delays because the number of SCSs allowed for communication in each data collection cycle is limited.
- Since the number of SCSs allowed for communication in each data collection cycle is limited, it takes more time to display the latest SOE events, compared to the Standard or Wide-area mode.
- If there is any narrowband group where data acquisition is paused, "(Pause)" is displayed on title bar of the SOE Viewer.

- **Behaviors of SOE OPC interface in the Narrowband mode**

Behaviors of the SOE OPC interface in the Narrowband mode are as follows:

- The SCSs specified in the SOE OPC interface setting receive a request for data collection from the OPC server via the message cache service at a fixed cycle. Therefore, such SCSs are in the same condition as the SCS for which automatic data acquisition by the message cache service is specified.
The SCS specified in the SOE OPC interface setting must be added to a narrowband group beforehand.
- Up to 100 SCSs can be specified in the SOE OPC interface setting.
- The timing of data collection depends on the number of SCSs allowed for communication that is specified in the Narrowband Group Definition window of the Message Cache Tool. Therefore, it takes more time in the Narrowband mode, compared to the Standard or Wide-area mode.

- **Collecting Data From SCS That Is Not Routed Through Narrowband Lines**

When an SENG that is connected in a narrowband system communicates with an SCS that is not routed through narrowband lines in the communication path, you can collect SOE events and diagnostic information messages from that SCS as in the case with the Standard and Wide-area modes by configuring the Message Cache Tool.

**SEE
ALSO**

For more information about the method of collecting data from SCS that is not routed through narrowband lines, refer to:

C3.8, "Collecting data from SCSs in a narrowband system in the same way as in the Standard and Wide-area modes" in *Integration with FAST/TOOLS (IM 32Q56H20-31E)*

9.3 Defining narrowband groups

A set of SCSs that share the same narrowband communication paths is defined as a narrowband group. The following figure shows the position of a narrowband group definition.

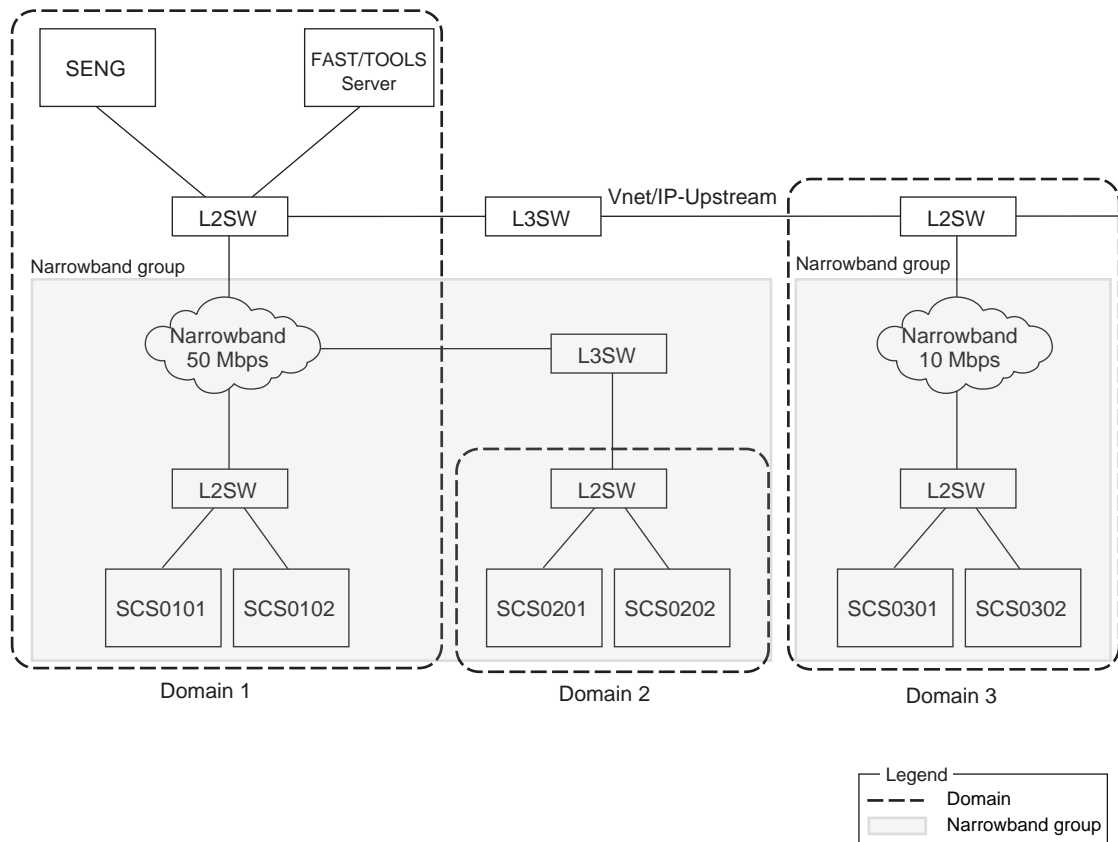


Figure 9.3-1 Position of a narrowband group definition

SCSs connected in a narrowband system must belong to a narrowband group. It is not possible to display the status or collect SOE events and diagnostic information messages from an SCS that does not belong to a narrowband group.

In a narrowband group definition, the following items should be specified to restrict communication for each narrowband group in consideration of network load:

- SCS name included in the narrowband group
- Number of SCSs that can communicate per acquisition cycle of the message caching service
- Number of SCSs that can communicate per display update cycle of the SCS Status Overview window.

■ Examples of Narrowband Group Definition

The conditions and examples to define a narrowband group are as follows:

- SCSs that are connected to two or more narrowband lines can be included in one narrowband group. However, if the bandwidth differs in each narrowband line, configure the narrowband group definition considering the slowest communication speed.

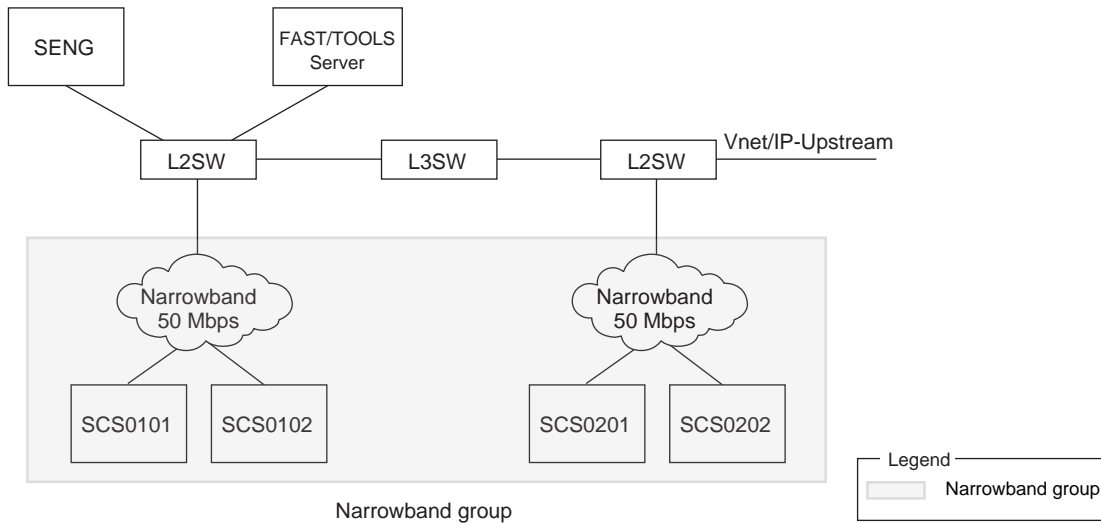


Figure 9.3-2 Example of Two Narrowband Lines in One Narrowband Group

- When two Vnet/IP-Upstream domains are connected to one narrowband line, include the SCSs of the two domains in one narrowband group.

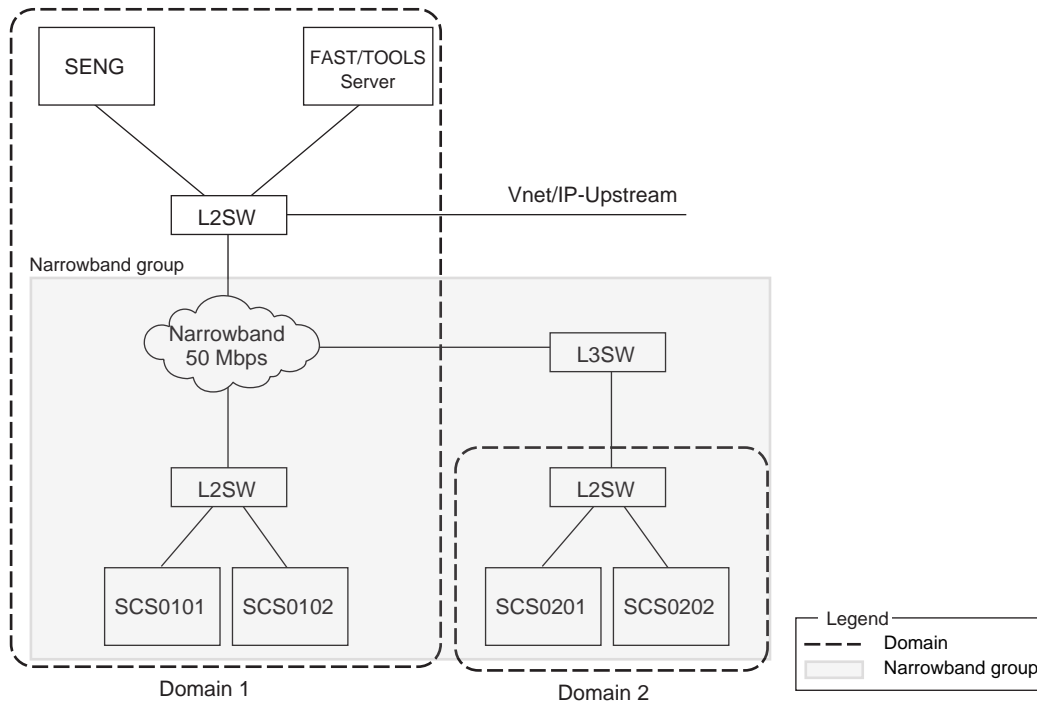


Figure 9.3-3 Example of Two Vnet/IP-Upstream Domains Connected to One Narrowband Line

■ Examples of Invalid Narrowband Group Definition

To avoid invalid narrowband group definition, observe the following prohibition:

Do not group SCSs that are routed through the same narrowband line into two or more narrowband groups.

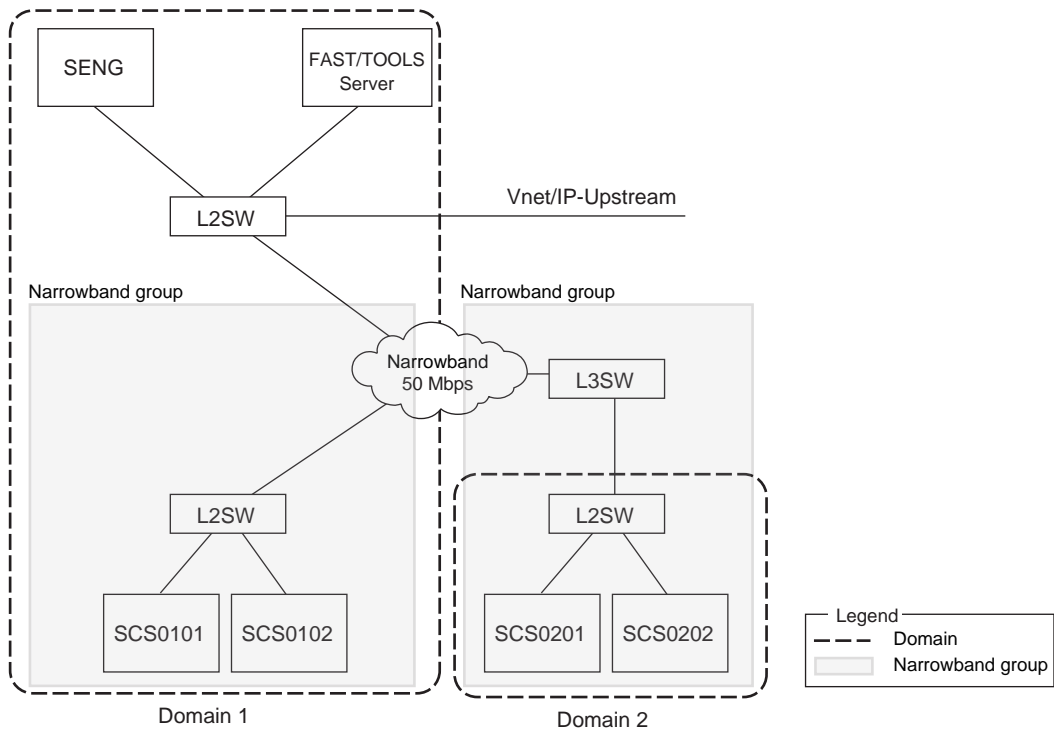


Figure 9.3-4 Examples of Invalid Narrowband Group Definition

9.4 Operation in the Narrowband Mode

In the Narrowband mode, the following limitations are applied to reduce the communication traffic on the network.

- The number of SCSs that perform communication for data collection from SENG is limited for each narrowband group
- Display in SCS Maintenance Support Tool windows is limited for each narrowband group

The Narrowband mode is set by using the Domain Properties Setting Tool.

■ Switching the SCS Maintenance Support Tool into the Narrowband Mode

The SCS Maintenance Support Tool operates in the Narrowband mode when all of the following conditions are satisfied:

- The license for the FAST/TOOLS Integration Engineering Package is distributed and activated on the SENG.
- Narrowband mode is set by using the Domain Properties Setting Tool.

■ Operation of SENG Software in the Narrowband Mode

In the Narrowband mode, the window actions and communications are limited because the bandwidth of line is narrower compared to the Standard mode and the Wide-area mode.

The limited functions are as follows:

- SCS status display
- Message Cache Tool
- Display of the Diagnostic Information window
- Display of the SOE Viewer
- Function to collect diagnostic information messages and SOE events
- SOE OPC interface
- Number of changes that can be made to mapping blocks or mapping elements by one online change download

9.5 Details of the data buffering function

The data buffering function saves application logic data of SCS with time stamps and allows FAST/TOOLS to collect the data. Even if the communication between FAST/TOOLS and SCSs is disconnected, the data buffering function enables you to view the change in data during disconnected communication through the operator interface of FAST/TOOLS after the recovery of communication. This function is useful for an environment where the communication between the FAST/TOOLS and the SCS is unstable or FAST/TOOLS is used in Narrowband.

The following figure shows the configuration of the data buffering function.

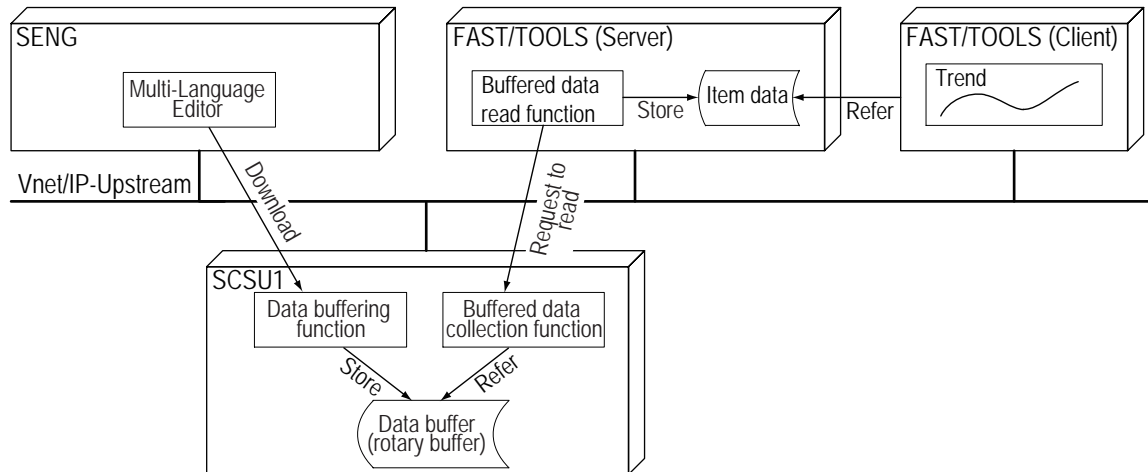


Figure 9.5-1 Configuration of the data buffering functions

SEE ALSO

For more information about data buffering, refer to:

“■ Data buffering function” in B2.1, “Functional configuration of the Gas flow rate calculation function” in Integration with FAST/TOOLS (IM 32Q56H20-31E)

■ Limitation on the Number of Events Saved in the Buffer

FAST/TOOLS collects saved events from SCSs. Consider the following items in the engineering of FAST/TOOLS:

- Event scan interval
- Catch up scan interval

The maximum number of events that can be saved in the buffer is 135000. If the number of saved events exceeds the maximum number, the events are overwritten in chronological order.

■ Engineering for Data Buffering

The following figure shows the relation between ProSafe-RS and FAST/TOOLS. The numbers in parentheses in the figure correspond to the same numbers in parentheses that appear in the engineering steps described below.

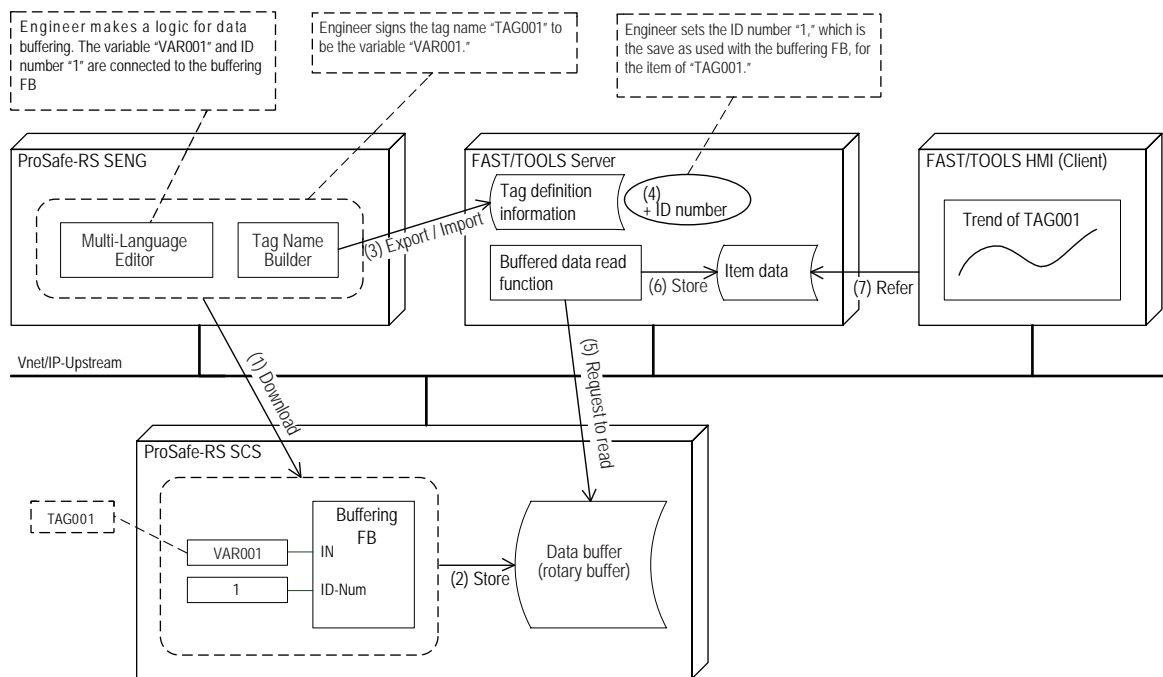


Figure 9.5-2 Relation between ProSafe-RS and FAST/TOOLS

1. Determine the data for which to use the data buffering function.
2. Determine the interval for event collection for FAST/TOOLS so as to prevent data buffer overflow.
3. Calculate required amount of communication traffic and make sure that there is no problem with it.
4. Create application logic for data buffering on SENG.
5. Bind the variables to be buffered and their identification numbers to data buffering function blocks.
6. Use Tag Name Builder to define a tag name for the variable that is to be saved in the buffer.
7. Download the created application logic to SCS. (1)
In SCS, the data buffering function blocks save data in the buffer of SCS along with the time stamp and the identification number. (2)
8. Export the information that is defined in Tag Name Builder of SENG.
9. Import the exported data into FAST/TOOLS.
The tag names defined on SENG are imported to FAST/TOOLS. (3)
10. In FAST/TOOLS, for the items corresponding to the tag names assigned to the variables to be buffered, set the identification numbers that are the same as the numbers specified in the application logic. (4)
You can find out the identification numbers specified in the application logic from the Tag Name Builder definitions and the application logic definitions on the SENG.
11. Set the interval for event collection and the number of events to collect in FAST/TOOLS Server.
FAST/TOOLS Server collects data from the buffer by the number of events to collect in each in the specified period. (5)
FAST/TOOLS Server sorts and saves the collected data into the corresponding items according to the identification numbers. (6)
Then, data of SCSs can be monitored through FAST/TOOLS HMI (Client) by accessing the data saved in the FAST/TOOLS Server as needed. (7)

9.6 Gas Flow Rate Calculation Function

The gas flow rate calculation can be performed in SCSU1. This is the function to calculate gas flow rates according to the AGA (American Gas Association) specification and to create daily and hourly closing data including the volume totals of gas flow rates. When you use the function block for the gas flow rate calculation function, set a scan period of SCS more than 200 ms.

The gas flow rate calculation function is Interference-free.

The engineering for gas flow rate calculation is as follows:

- Creating an Application Logic
- Defining tag names
- Exporting Tag Name Information

SEE ALSO

For more information about the gas flow rate calculation function, refer to:

[B2., "Gas flow rate calculation function" in Integration with FAST/TOOLS \(IM 32Q56H20-31E\)](#)

■ Examples of Gas Flow Rate Calculation Application Logic

To engineer the gas flow rate calculation to be executed at the time of SCS start-up, perform the preparatory tasks for the engineering and then start the SCS. The operation procedures of SCS differ between start-up and restart.

- Example of creating an application logic
 1. Connect ECW_B to EXEC of AGA_* block so that a value can be set from FAST/TOOLS.
 2. Connect ECWR_* to SET, PARA (parameters to be set) and COMP (gas composition data) of AGA_* block so that values can be set from FAST/TOOLS.
 3. Take a backup of the parameter values to be set and gas composition data for AGA_* block in FAST/TOOLS so that they can be set again.
- Example of procedure for starting the gas flow rate calculation function at an initial startup of SCS

Example of operation to start the gas flow rate calculation function at restart of SCS The values of SET, PARA, and COMP to which ECWR_* is connected are restored. When the retainable data is held, the Step 1 and 2 in "Example of procedure for starting the gas flow rate calculation function at initial start-up of SCS" are not necessary.

 1. From FAST/TOOLS, set the parameter values and gas composition data for AGA_* in ECWR_*.
 2. Set the SET flag of AGA_* to TRUE to reflect the parameters in the AGA_* block.
 3. Set the EXEC flag of AGA_* to TRUE to perform the calculation.

Function blocks AGA_3 and AGA_7 are available for gas flow rate calculation. Example usage of these function blocks is described as follows:

- Example of AGA_3 usage

The following figure shows an example of application logic using AGA_3. The arguments in gray hatching are structure type arguments.

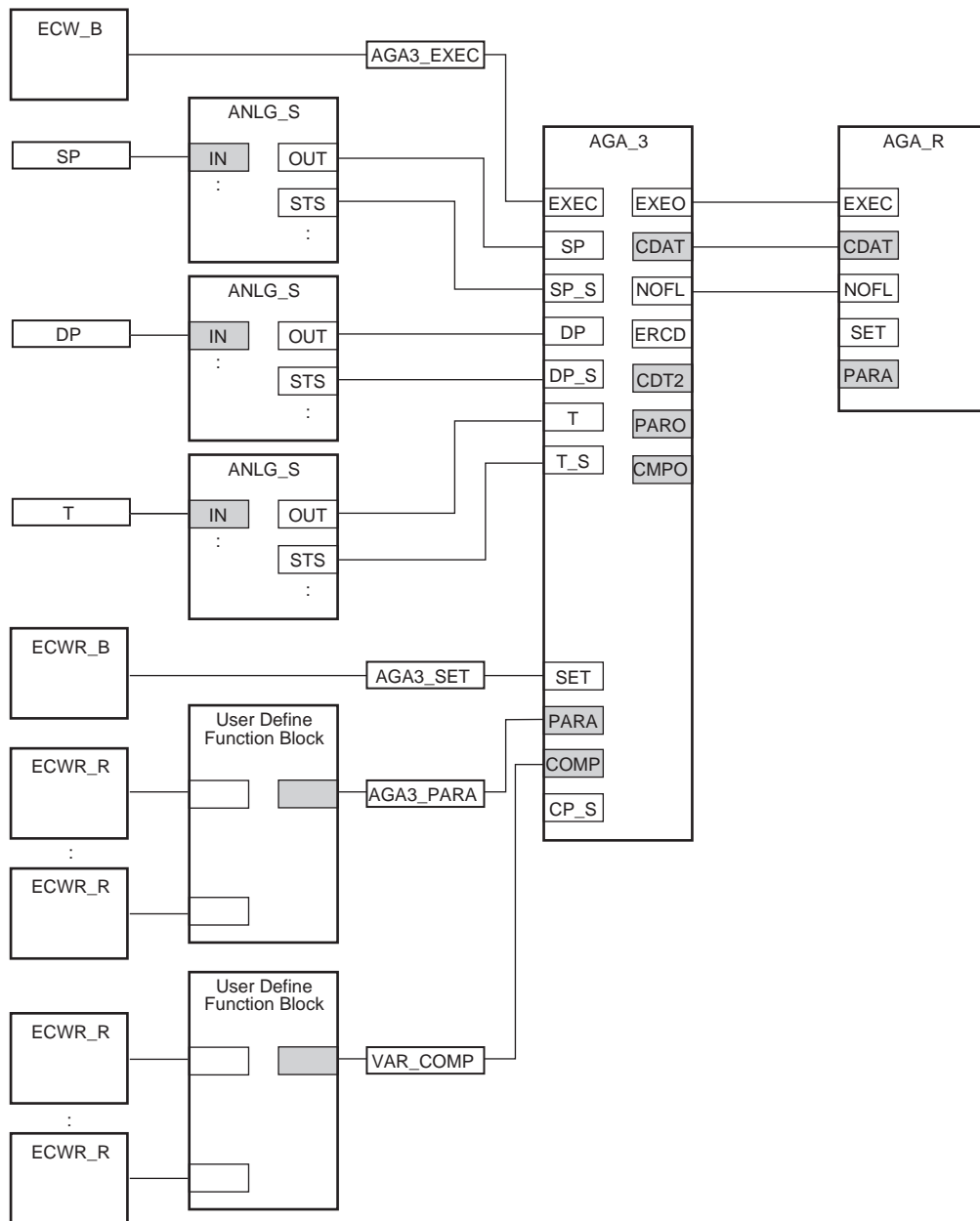


Figure 9.6-1 Example of Application Logic Using AGA_3

Usage example of AGA_3 function block is as follows:

- To SP, DP, and T, input values that are converted into engineering data by using ANLG_S block.
- PARA and COMP are the structure type data. Convert the parameters for calculation and gas composition data into the structure type by using user-defined FB and input to PARA and COMP.
- AGA_3 calculates the gas flow rate based on SP, DP, T, PARA, and COMP, and then outputs it to CDAT and CDT2.
- CDAT is an argument that provides a set of output values needed to create a report. Connect CDAT to the CDAT of AGA_R block.
- By using ECWR_* or ECW_* block, you can change parameters from FAST/TOOLS or a Modbus master device. The setting values are retained at the time of SCS restart by using ECWR_* with the data retaining function.
- Example of AGA_7 usage

The following figure shows an example of application logic using AGA_7. The figure shows an example that converts the uncorrected instantaneous flow rate ("Flow" in the figure), which was entered from the field by analog signal, into the pulse count per scan period by using the user-defined FB, and then enters it in PULS. The arguments in gray hatching in the figure are structure type arguments.

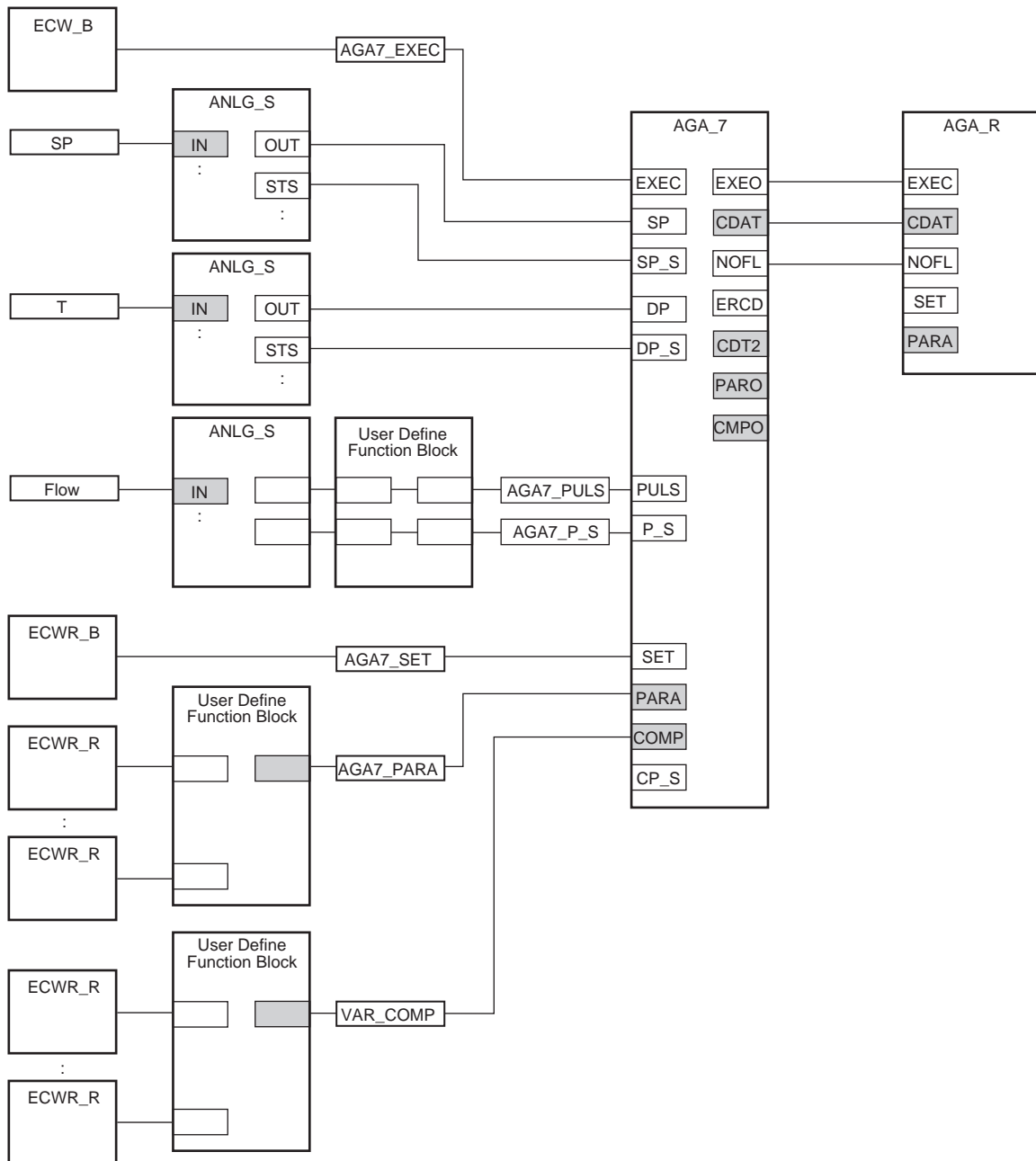


Figure 9.6-2 Example of AGA_7 Application Logic

An usage example of AGA_7 function block is as follows:

- AGA_7 calculates the gas flow rate based on SP, T, PULS, PARA, and COMP, and then outputs it to CDAT and CDT2.
- To SP and T, input values that are converted into engineering data by using ANLG_S.
- Input the external setting values in PARA and COMP by using ECWR block. Convert them into a structure type by using the user-defined function block.
- CDAT is an argument that organizes output values needed to create a report. Connect CDAT to the CDAT of AGA_R block.

- When you want to always use input values to calculate AGA_7 without using the status (P_S) of PULS data, always enter TRUE for the status (P_S) of PULS data.

SEE ALSO

For more information about the specification of function blocks, refer to:

Appendix 2., “Structure of function blocks of gas flow rate calculation function” in Integration with FAST/TOOLS (IM 32Q56H20-31E)

■ Example of Conversion from the Uncorrected Instantaneous Flow Rate to Pulse Count

The following figure shows the example of conversion from the uncorrected instantaneous flow rate to pulse count.

This example of conversion is a calculation example that uses the FB function of AGA_7 as it is. Calculates PULS that is an input FB argument of AGA_7 from the flow rate at moment before correction by using the user-defined FB, and then enters inputs the calculation result into AGA_7.

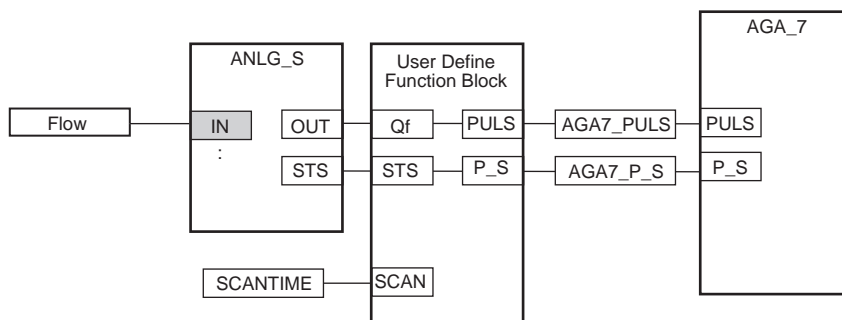


Figure 9.6-3 Example of Conversion into Pulse Number

An example of calculation in the user-defined FB is as follows:

- $PULS = Qf \times SCAN / 1000.0$
 Qf: Flow rate at moment before correction. The unit is [m³/s] for SI unit system, [ft³/s] for US unit system.
 SCAN: Scan period. The unit is [ms]
- $P_S = STS$

When using AGA_7 for this way, specify the parameters relating to the pulse number of PARA that is the input argument of AGA_7, as follows:

PULSE_K: Fix to 1

PULS_CUTOFF: Lower cut-off value for the uncorrected instantaneous flow rate per scan period. The unit is [m³/scan] for SI unit system, [ft³/scan] for US unit system.

In addition, set PULS_CUTOFF again when you change the scan period.

■ Example of an Application to Create a Report

Function block AGA_R is available for report creation.

The following figure shows an example of application logic using AGA_R. The arguments in gray hatching in the figure are the structure type arguments.

AGA_R performs accumulation, average, closing processing based on the calculation result of AGA_3 or AGA_7 block, and then creates a report data.

Connect the output parameter CDAT of AGA_3 or AGA_7 block to CDAT.

Input the parameters into PARA of AGA_R. These parameters are externally set via the ECWR blocks and covered into a structure type by the user-defined function block.

AGA_R outputs the report data to CURH, PREH, TDAY, YDAY and CMON, and reflect to the data item of mapping block. You can collect the report data in FAST/TOOLS by using the tag access and the Data Buffering function.

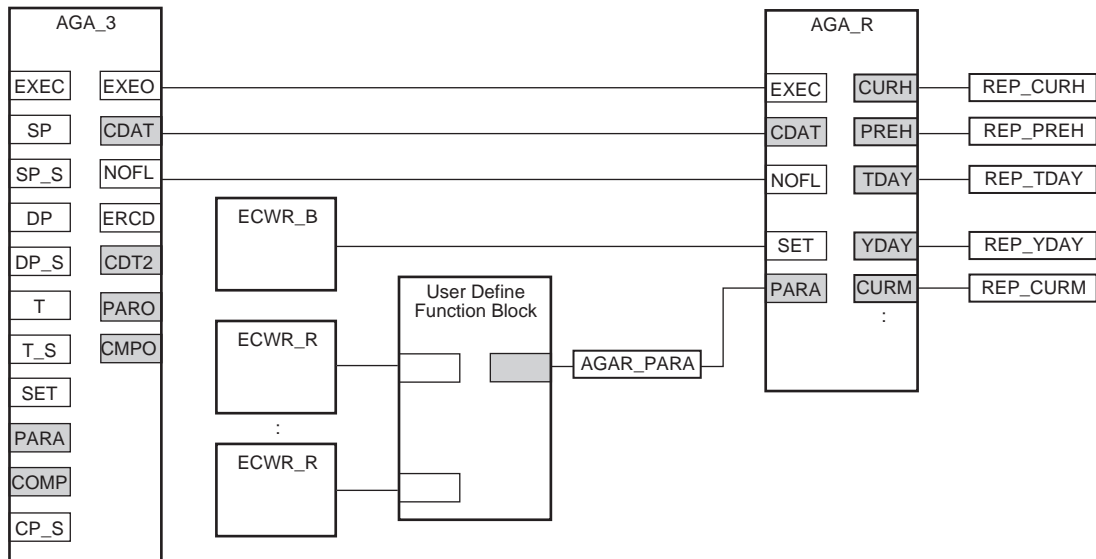


Figure 9.6-4 Example of AGA_R Application Logic

You can make use of the application logic to prevent accumulation of the calculation result in AGA_R in case of input error that causes an abnormal status. The handling method is as follows:

- When SP_S/DP_S/T_S of AGA_3 is BAD, set NOFL (gas production suspended) entered in AGA_R to TRUE.
- When SP_S/DP_S/T_S of AGA_3 is GOOD, set NOFL (gas production suspended) entered in AGA_R to FALSE.
- When SP_S/T_S/P_S of AGA_7 is BAD, set NOFL (gas production suspended) entered in AGA_R to TRUE.
- When SP_S/T_S/P_S of AGA_7 is GOOD, set NOFL (gas production suspended) entered in AGA_R to FALSE.

SEE ALSO

For more information about the specification of function blocks, refer to:

[Appendix 2., “Structure of function blocks of gas flow rate calculation function” in Integration with FAST/TOOLS \(IM 32Q56H20-31E\)](#)

9.7 Application Capacities

The following table shows the capacity of applications for SCSU1.

Table 9.7-1 Capacity of SCS Applications

Types	Items	SCSU1 Max. capacity	Remarks
I/O	Number of nodes	10 nodes	Node #1 is for CPU node only.
	Number of slots	8 slots	When connecting an I/O node, the maximum slot number of CPU nodes is 6.
	communication module	2	For Modbus slave communication (Total number of ALR111/ALR121/ALE111)
		4	For Subsystem Communication
	Number of I/O points	1000 (500 in duplexed I/O module)	The numbers are provided only as a guide.
Number of Subsystem Communication Data	500 data	The maximum number of transmitted and received data per SCS	
Application logic	Number of programs and user-defined FU/FB (number of POU's)	Max. 500	When more than 500 POU's are defined in the SCS Manager, an error occurs during the building time. It may not be possible to define 500 POU's depending on the type, number and complexity of the connection of FU/FB or LD elements. A limitation may be imposed depending on SCS performance.
	Number of variables to be defined	I/O variables. 1000 Internal variables 3000	The numbers are provided only as a guide. You may not be able to define up to the maximum capacity depending on the type of variable defined. A limitation may be imposed depending on SCS performance.
Inter-SCS safety Communication	Number of sending data	200 data	Maximum number of sending data per SCS.
	Number of receiving data	200 data	Maximum number of receiving data per SCS
SCS Link Transmission	Number of sending data	128 data	Maximum number of sending data per SCS.
	Number of receiving data	1000 data	Maximum number of receiving data per SCS
FAST/TOOLS Integrated Function	Annunciators (%AN)	1000	
	Common switches (%SW)	200	All are system switches.
	External Communication FB	(*1)	
	External communication FB (with Data Retaining function)	(*1)	It is also limited by the size of area for retaining.
Gas Flow Rate Calculation Function	Number of FBs for gas flow rate calculation (Total of AGA_*)	1	SCSU1 only
	Report data creation FB (AGA_R)	1	SCSU1 only

Continues on the next page

Table 9.7-1 Capacity of SCS Applications (Table continued)

Types	Items	SCSU1 Max. capacity	Remarks
Mapping block	Analog input blocks (ANLG_S, ANLGI)	Total 1800 including AGA* and AGA_R blocks	
	Velocity alarm blocks (VEL)		
	Gas Flow Rate Calculation Function (AGA*)	1	
	Report function of Gas Flow Rate Calculation Function (AGA_R)	1	
	Annunciator blocks (ANN, ANN_FUP)	1000	Mapping to %AN element
Communication I/O area	Overall size of %W	4000 Words	1 word = 16 bits
	%W: For mapping (BOOL)	200 words (3200 bits)	1 data = 2 words, 100 data
	%W: For mapping (32-bit analog data)	1800 Words	900 data
	%W: For subsystem communication	1000 Words	Up to 500 data in total of bit data and analog data can be assigned.
	%W: Not used	1000 Words	
Modbus Slave	Coil	1000 Bits	
	Input relay	4000 Bits	
	Input register	4000 Words	1 word = 16 bits, 1 data = 2 words, 2000 data
	Holding register	1000 Words	500 data
SOE	SOE storage area (RAM)	15000 events	
	Back up area on power failure (non-volatile RAM)	Latest 1000 events	
	Trip signal file (non-volatile RAM)	2 trip signal files of up to 1500 events	
Diagnostic information message	Area for saving diagnostic information messages (RAM)	5000 messages	
	Back up on power failure (nonvolatile RAM)	Latest 200 messages	Diagnostic information message
Data buffering	Number of buffers	135000	
Area for retaining	Size of data area for retaining	6 Kbyte	

*1: The number that can be defined differs depending on the use condition.

- When using in Modbus, the maximum number is 1000 for ECW_B and ECWR_B in total. Up to 500 for ECW_I, ECWR_I, and ECW_R, ECWR_R in total can be defined.
- Up to 3200 tag names can be defined in total for Boolean internal variables and FBs of ECW_B and ECWR_B.
- Up to 900 tag names can be defined in total of DINT and REAL type internal variables, IO_REAL type input variables, and FBs of ECW_I, ECWR_I, ECW_R, and ECWR_R.

9.8 Precautions for Engineering and Maintenance

You need to secure enough bandwidth so that FAST/TOOLS and SCS can communicate normally, and to enable offline download to SCS through narrowband in the narrowband system environment.

In an environment in which it is difficult to collect SCS information through a narrowband line, consider bringing a portable computer set up as SENG to the site to collect necessary information.

■ How to Reduce Bandwidth Usage Before Offline Download

Reduce the bandwidth usage before performing offline download to SCS. Allowance for the bandwidth may decrease during some communication such as SCS data collection from FAST/TOOLS through narrowband. If enough bandwidth for communication is not secured, data may be lost or offline download may fail. To reduce the bandwidth usage, perform either of the following:

- Extend the period of data collection from SCS
- Stop data collection from SCS

If the handling is difficult, bring a portable computer set up as SENG to the site to perform offline download.

■ Bandwidth for Offline Download and Initialization of Retain Data

Bandwidth of 1.2 Mbps is required for offline download. When performing offline download through narrowband, first stop data collection by FAST/TOOLS. However, when there is enough allowance of 1.2 Mbps or higher while FAST/TOOLS in operation, you can perform offline download without stopping data collection by FAST/TOOLS.

If offline download fails, retry the procedure.

If offline download fails no matter how many times you retry, bring the SENG to the site to perform offline download without passing through the narrowband lines, or bring a CPU module that you have performed offline download locally to the site and install it.



IMPORTANT

When you perform offline download, the retainable data is initialized.

SEE ALSO

For more information about online change download, refer to:

- [“Online Change Download” on page 5-16](#)

■ Precautions for Using Inter-SCS Communication

The following table shows the additional delay that is used for calculating the time-out setting value for inter-SCS safety communication when the network is in Narrowband mode.

Table 9.8-1 Additional Delay for Inter-SCS Safety Communication When the Network is in Narrowband Mode

Type of time-out monitoring time	Additional Delay
Reception Interval Timeout Value (OUTT)	15 seconds
Transmission Delay Timeout Value (DLYT)	Transmission delay of the narrowband line

The following table shows the delay time to be taken into consideration when deciding the time-out setting value for SCS link transmission safety communication when the network is in Narrowband mode.

Table 9.8-2 Delay Time of SCS Link Transmission When the Network is in Narrowband Mode

Type of time-out monitoring time	Delay time
Reception Interval Timeout Value (OUTT)	Not applicable
Transmission Delay Timeout Value (DLYT)	Transmission delay of the narrowband line

**SEE
ALSO**

For more information about time-out values of Inter-SCS Safety Communication, refer to:

- [Inter-SCS Safety Communication Timeout Settings](#) on page 2-55

For more information about time-out values of Link Transmission Inter-SCS Safety Communication, refer to:

- [Time Out Settings of SCS Link Transmission Safety Communication](#) on page 2-61
-

10. Engineering for ProSafe-SLS Communication Function

By using the ProSafe-SLS communication function, ProSafe-SLS events and data can be acquired by subsystem communication.

Events acquired from the ProSafe-SLS can be handled as SOE events, while data acquired from the ProSafe-SLS can be handled as subsystem communication data. If the ProSafe-RS is integrated with the CENTUM, you can build an application logic in the SCS and cause the HIS to monitor alarms. ProSafe-SLS events can also be displayed in the SOE Viewer of the HIS.

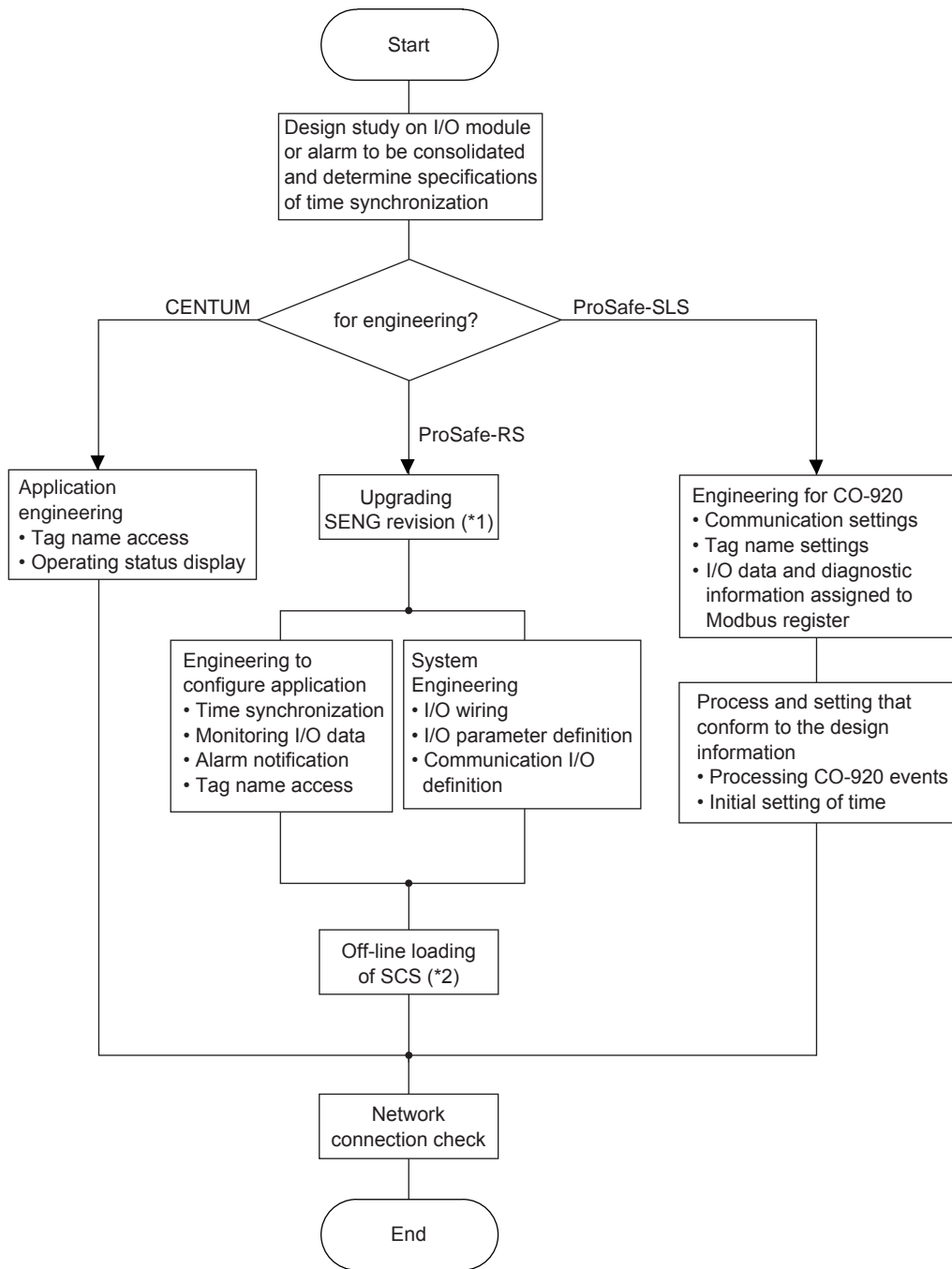
**SEE
ALSO**

For more information about system configuration for ProSafe-SLS communication function, refer to:

[B4.2, "System configuration" in Open Interfaces \(IM 32Q05B10-31E\)](#)

10.1 Overview and Flow of the Engineering

The following figure shows an image of engineering flow such as connecting ProSafe-SLS to ProSafe-RS, checking ProSafe-SLS events on the SOE viewer of ProSafe-RS and monitoring I/O data or operating status of ProSafe-SLS on CENTUM HIS.



- *1: You do not need to upgrade the revision for a new project. If you intend to upgrade the revision of existing project to use ProSafe-SLS functions, you must perform offline download.
- *2: If you have performed offline download of the project database in R3.02.20 or later, you can perform online download.

Figure 10.1-1 Engineering Flow of ProSafe-SLS Communication

10.2 Determination of Events and I/O Data of ProSafe-SLS for Management

When the ProSafe-SLS communication function is used, determine I/O data, diagnostic information and events of ProSafe-SLS that you want to apply the comprehensive management in ProSafe-RS. Examine ways to keep the application capacity to or less than the applicable maximum capacity shown in the following table.

Table 10.2-1 Application capacity

Application element	Maximum capacity	Description
Number of ALR121 to install	4 per one SCS	Total number including ALR111 (*1)
Number of communication data units per SCS	500 data units	This specifies the number of data items that can be wired to subsystem communication FB instances. Maximum 256 words (4096 bits) are allowed for the total assignment size of discrete input/output.
Size of communication I/O per SCS	1000 words	A word holds two bytes.
Allowable number of communication attempts per ALR121	1000 words	-
Number of ports per ALR121	2 ports	-
Allowable number of subsystem stations to communicate per port	30 stations	One CO-920 is considered as a station.
Number of communication definitions per ALR121	Number of definitions in the range that can be calculated by using the following formula (Number of SLSEVENT type communication definitions) x 2 + (Number of non-SLSEVENT type communication definitions) ≤ 128	-
Number of data sets for event acquisition per ProSafe-SLS	24 words	To acquire the events from ProSafe-SLS, assign 24 words of communication definition for event acquisition per ProSafe-SLS.

*1: Available number of ALR111 and ALR121 to be installed to an SCS is determined according to the total number of ALR111 and ALR121 that are installed in the same SCS. Ensure the total number of ALR111/ALR121 does not exceed the applicable value shown in the table. Communication modules for the Modbus slave communication are not included in the count.

10.2.1 Determination of Data and Event and Diagnostic Information of ProSafe-SLS to Monitor

Internal error information of the ProSafe-SLS and CO-920 are collectively referred to as diagnostic information of ProSafe-SLS. Determine the diagnostic information of ProSafe-SLS to monitor on ProSafe-RS. Diagnostic information can be handled as both Modbus communication data and events.

Errors of devices connected to the ProSafe-SLS can also be handled as Modbus communication data and events.

● Monitoring the Data of ProSafe-SLS-connected Devices

The following describes how the data of ProSafe-SLS-connected devices should be handled. When performing engineering from the COM-SET, set the "Data acquisition area (DAR)" field of the tag name to monitor as the information of the connected device, at "Taglist part" in the TAG file on the CO-920, to "YIS."

● Determination of Diagnostic Information of ProSafe-SLS to Monitor

Diagnostic information of CO-920 includes self-diagnosis information of Y-net and each module in the ProSafe-SLS, available space of event buffer and other information of the CO-920. The diagnostic information of the CO-920 indicates the current statuses and values, and these statuses and values are retained while an error is present.

Some diagnostic information of ProSafe-SLS changes even when an error does not occur, and if such information is to be monitored as events, important events may remain unnoticed. Among the diagnostic information of ProSafe-SLS, therefore, make sure the following items are monitored.

- Communication status of COM port
- Y-net network integrity

If you want to select other items, investigate the need to do so by referring to the ProSafe-SLS manual.

● How to Monitor Changes in Diagnostic Information of ProSafe-SLS

If diagnostic information of ProSafe-SLS is input to the SCS as Modbus communication data, and the diagnostic information changes multiple times at a rate faster than the Modbus communication cycle, the ALR121 may not acquire the changes in diagnostic information and missing data may occur. The alarm notification application cannot notify an alarm for missing data.

Missing data will not occur at the SOE so long as diagnostic information of ProSafe-SLS is input to the SCS as SLS events. In this case, SOE events are recorded even when no alarm is notified based on Modbus communication data.

To input changes in the applicable diagnostic information as SLS events, enable event generation when you set information on the tag names corresponding to the applicable diagnostic information of CO-920. To be specific, when performing engineering from the COM-SET, set the "Generate event" field of the tag name to monitor as diagnostic information, at "Taglist part" in the TAG file on the CO-920, to "Y."

After event generation is permitted, SOE is logged at the timing of a change on diagnostic information. On SOE Viewer, the tag name is indicated on Reference.

SEE ALSO

For more information about diagnostic information of ProSafe-SLS, refer to:

CO-920 manual

10.2.2 Determination of Time for Time Synchronization

To use ProSafe-SLS communication function, specify the time synchronization that is triggered by output pulse from SCS and performed between ProSafe-SLS and SCS once a day at a certain time. You need to specify the time for synchronization separately for ProSafe-SLS and SCS. Determine the time according to the universal time coordinated (UTC) before you start engineering.

10.3 Engineering ProSafe-RS

This section describes the preparation and engineering of the ProSafe-RS that are needed to use the ProSafe-SLS communication function.

10.3.1 Preparation

You need to upgrade ProSafe-RS to R3.02.20 or later.

ProSafe-SLS communication function is also applicable to the existing SCS projects. After you upgrade SENG to R3.02.20 or later, specify related definitions to build and run off-line download. ProSafe-SLS communication function becomes available then.

10.3.2 System Engineering of ProSafe-RS

This section describes the wiring and builder setting of the ProSafe-RS that are required to use the ProSafe-SLS communication function. The views and builders that are required to use the ProSafe-SLS communication function are as follows:

- I/O wiring view
- I/O parameter builder
- Communication I/O builder

■ Setting I/O Wiring View

Define ALR121M to slots of nodes in which ALR121 is installed for ProSafe-SLS communication.

ALR121 used for ProSafe-SLS communication function supports only non-redundant configuration.

Set "IsRedundant" to "FALSE."

■ Setting I/O Parameter Builder

On Module tab, set "Connection Device" to "S_SLSMOD."

On Port1 tab and Port2 tab, set as follows:

- Ensure that communication settings for each ALR121 port match those for CO-920.
- "Baud Rate" on CO-920 is set to 57600 bps by default and not supported by the ProSafe-RS, thus the baud rate for CO-920 may need to be set again.
- "Parity" is set to "Even" by default. "None" is set to CO-920 by default. To ensure the communication reliability, "Even" is the recommended Parity setting to ALR121 and CO-920.
- Ensure that "Data Bits" is always set to 8 bit because Modbus protocol (RTU mode) is applied for communications.
- Set "2-Wire/4-Wire" according to the connection method for RS-485 communications between ALR121 and CO-920.
- The following items can be used in the default setting.
"Reception Inter-Character Time", "Response Timeout", "Communication Retry" and "Interval of Connection Retries"
- Options between "Option1" and "Option4" are not applied to ProSafe-SLS communication function. Set them to 0 on a constant basis.

■ Setting Communication I/O Builder

To enable an SCS to acquire I/O data, diagnostic information and events from CO-920, set communication I/O definitions by considering the limitation on application capacity.

S_SLSMOD is the program to communicate with ProSafe-SLS. Set "Program Name" to "S_SLSMOD."

TIP

If any of the following conditions applies, correct the program name in the communication I/O builder. If the program name is not corrected, a build error will occur.

- The "Connection Device" definition of the ALR121M was changed in the I/O parameter builder
- The ALR121M defining the S_SLSMOD was deleted and the ALR111M was created at the same installation position by using the I/O wiring view

Data types that can be assigned to the communication I/O definition are listed on the following table.

Table 10.3.2-1 Accessible Data Types for ProSafe-RS Through SLS Communication Function

Data type	Description
Input (16-Bit Unsigned)	Analog input (16-bit unsigned integer)
Output (16-Bit Unsigned)	Analog output (16-bit unsigned integer)
Input (Discrete)	Discrete input
Output (Discrete)	Discrete output
SLSEVENT	Event type applicable only in S_SLSMOD

Input (16-Bit Unsigned), Output (16-Bit Unsigned), Input (Discrete) and Output (Discrete) can be assigned to the communication I/O definition through the same procedures as those in S_MODBUS.

Be aware of the following conditions when you assign SLSEVENT to communication I/O definition.

- One Station Number of each port accepts only one definition.
- The size must be 24 words.
- Set the address of other devices to "SLSEVENT."

**SEE
ALSO**

For more information about Application Capacity, refer to:

[10.2, "Determination of Events and I/O Data of ProSafe-SLS for Management" on page 10-3](#)

10.3.3 Engineering to Configure Applications on ProSafe-RS

Configure applications for time synchronization, I/O data monitoring and alarm notification. Engineering for tag name is required to monitor the data on CENTUM HIS.

■ Configuring an Application for Time Synchronization

To perform time synchronization between ProSafe-SLS and ProSafe-RS, configure an application on ProSafe-RS enabling ProSafe-RS DO module to output the trigger once a day to ProSafe-SLS DI module. Settings of Trigger, for example rising and/or falling edge of pulse must match the Trigger of time synchronization events on CO-920.

● Example of Application on ProSafe-RS

The following figure shows an example of application logic to output trigger from the SCS DO module at 3:00 universal time coordinated (UTC) every day.

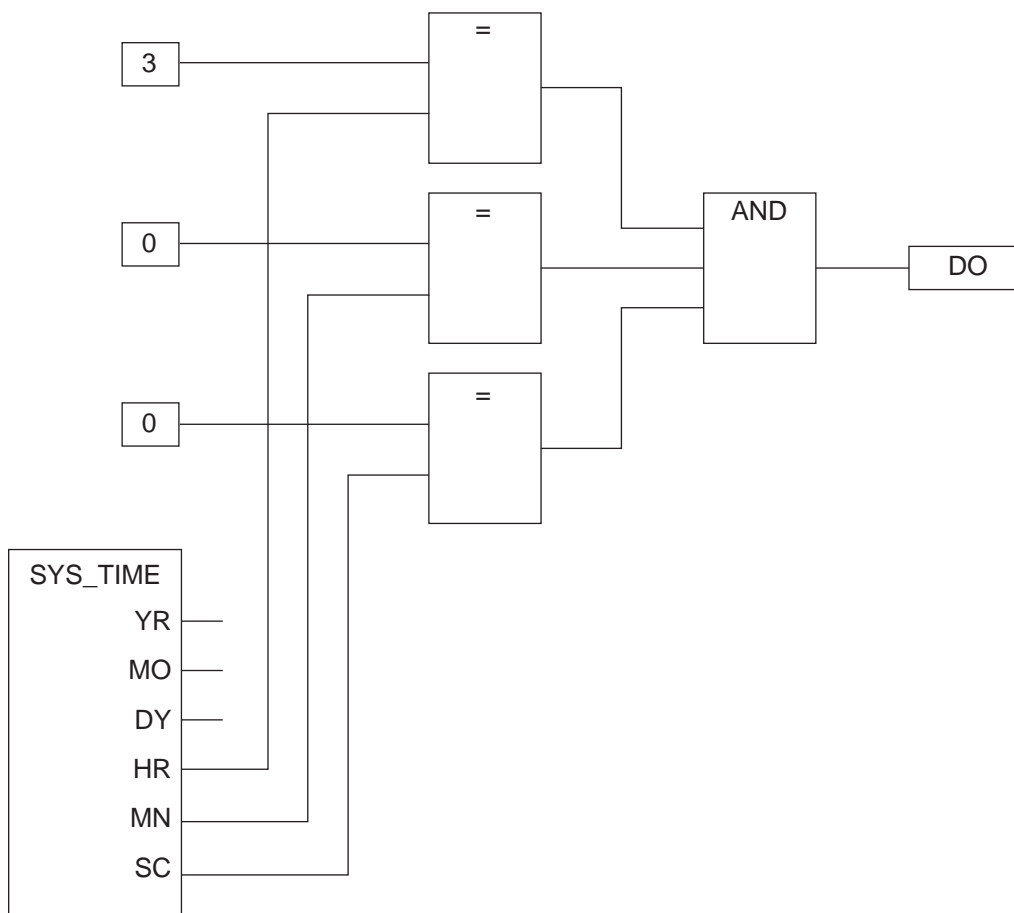


Figure 10.3.3-1 Example of Creating an Application Logic to Output Trigger for Time Synchronization From DO

To apply the application logic provided as an example for time synchronization, engineering is required on ProSafe-SLS.

● Example of Engineering on ProSafe-SLS

1. Define a DI that applies the rising edge of pulse input as a time setting event to DI module on ProSafe-SLS.

- 2. Set 3:00 universal time coordinated (UTC) to ProSafe-SLS for input of rising edge of DI pulse.

■ Engineering to Monitor I/O Data

The I/O data acquired from ProSafe-SLS can be handled as subsystem communication data on ProSafe-RS. On ProSafe-RS, create an application to monitor the subsystem communication data.

Create an application for CENTUM Integration to monitor on HIS.

■ Configuring an Application for Alarm Notification

The following figure shows an example of ProSafe-RS application that notifies an alarm to HIS at an error of a certain I/O module on ProSafe-SLS and that outputs recovery alarm.

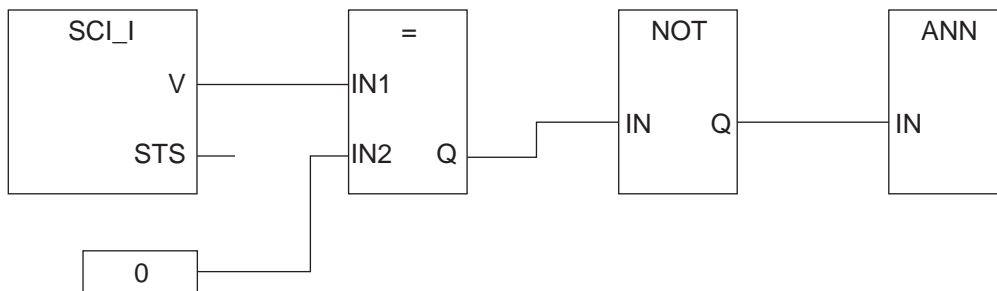


Figure 10.3.3-2 Example of Application to Notify ProSafe-SLS Error Alarm

This application loads the data status of a certain I/O module of ProSafe-SLS and acquires DINT value by using SCI_I in the function block.

DINT turns to a value except for 0 when the I/O module fail occurs and it remains during the failure. It turns to 0 when the failure recovers.

■ Engineering for Tag Name Access

To allow CENTUM HIS to access I/O data acquired from CO-920, define tag names on SENG.

10.4 Engineering for ProSafe-SLS

The following items are required for ProSafe-SLS engineering.

- Engineering for CO-920
- Processing events on CO-920
- Initializing CO-920 time
- Engineering for time setup with DI input

10.4.1 Engineering for CO-920

Use the COM-SET to edit the communication setting file and tag name setting file to perform CO-920 engineering.

■ Engineering Flow of CO-920

Perform CO-920 engineering from the COM-SET based on the I/O data, alarms and other design information of the ProSafe-SLS.

The task is performed according to the following steps:

1. Connect COM-SET to RS-232C port on CO-920 and perform CO-920 engineering. Use COM-SET and edit CNF file and TAG file.
2. Compile the edited texts on COM-SET.
3. Download the compiled binary data from COM-SET to CO-920.
4. When the settings have been downloaded, reset and restart the CO-920 from the COM-SET.
Communication between the ALR121 and CO-920 is disabled while the CO-920 is being reset and restarted. If CO-920 is running, you must be careful for any affects on a system of upstream connection.

SEE ALSO

For more information about Items to edit and recommended settings, refer to:

- “■ Editing CNF File” on page 10-13
- “■ Editing TAG File” on page 10-14

For more information about engineering for ProSafe-SLS, refer to:

ProSafe-SLS manual

■ Setting Communication

Set communication setting for CO-920 and SCS ensuring that parameters match between them.

Among communication settings, you must be careful particularly with baud rate and parity settings.

SCS does not support the default baud rate settings (57600 bps) for CO-920. CO-920 parity is set as None by default, which is different from SCS default (Even).

■ Editing CNF File

CNF file contains I/O data, diagnostic information, time synchronization and the information relative to communication settings of each port and they are described on System part, Communication part, and Data acquisition part.

● System part

In communication with ProSafe-RS, set External Clock to "Y" and Time to the target time for time synchronization from SCS. Make Trigger slope match to DO wave that is applied to the trigger for time synchronization on SCS.

● Communication part

It describes setting information for items and types of event character string about RS-232C port (COM1) and RS-422/RS-485 (COM2, COM3).

Modbus slave address is equivalent to Station Number for subsystem communication on ProSafe-RS. It must match the Station Number that is set at ProSafe-RS engineering.

Baud rate, Word length, Parity and Stop bits are communication settings of RS-485. Make them match to the communication settings for subsystem specified at ProSafe-RS engineering.

Recommended specification is Format11 for Event format that does not contain Description and applies 10 character type for status.

- **Data acquisition part**

Set behaviors when CO-920 acquires the data from each I/O module.

Set the Module type, Network address and I/O type for each YIS-net module installed.

■ Editing TAG File

TAG file contains the Description corresponding to tag name and the information about Modbus register assignment for Tag name monitored on ProSafe-RS and they are describe on Taglist part.

Setting items of Taglist part and their details are provided as follows:

- I/O data or Tag name for diagnostic information is set to TAG_NAME. Recommended maximum characters are 22 for a Tag name because SOE on SCS reads up to 22 characters. Duplicate tag names are not permitted within one CO-920.
- The SOE of the SCS does not read TAG_DESCRIPTION. Include the necessary information in the tag name.
- Specify the data source or the initial value of the corresponding Tag name to TAG_SOURCE.
- Specify the Modbus register address to which Tag name is assigned to TAG_LOGIC_ADDRESS. Each TAG_LOGIC_ADDRESS corresponds to the Logic address of Modbus register that is set on CNF file.

You must consider the previous descriptions and ensure that the following requirements are satisfied to set ProSafe-SLS tag name.

- Maximum 22 characters are allowed.
- Overview of an event can be determined.

■ Assigning I/O Data to Modbus Register

Assign the I/O data of ProSafe-SLS monitored on ProSafe-RS to Modbus register on CO-920.

■ Assigning Diagnostic Information to Modbus Register

If you intend to detect errors in ProSafe-SLS and notify alarms, assign diagnostic information of ProSafe-SLS to Modbus register on CO-920. Make an alarm notify when the previous information is read through an SCS application and an error is judged.

10.4.2 Processing events on CO-920

If events are stored on CO-920 before events are acquired from ProSafe-RS, SCS requires a long time to acquire events. To avoid slow event acquisition, process the events according to the policy during design study.

TIP For example, ALR121 contains communication definitions as much as the maximum application capacity and event acquisition runs only for one communication definition, approximately maximum 15 hours is expected for SCS to acquire 10000 events from a CO-920.

■ Acquiring or Deleting Events Stored in CO-920

SCS starts acquiring at the event next to the last one acquired from CO-920.

If you do not need the events generated on ProSafe-SLS before you connect ProSafe-RS, acquire all events from COM-SET and delete them in advance.

● How to Acquire Events that are Stored in CO-920

Before you connect SCS to CO-920, connect COM-SET to the maintenance port (COM1) of CO-920 and acquire all events from CO-920.

TIP Even though all events are acquired from the maintenance port (COM1) of CO-920, locations of event read pointer for COM2 and COM3 remain unchanged.

If you connect a system for event acquisition to COM2 and COM3 and acquire events, the events on CO-920 disappear.

Events are stored in the rotary buffer on CO-920 and they remain until they are overwritten with new events.

● How to Delete Events that are Stored in CO-920

On COM-SET menu, select [ProSafe-SSCC] > [Reset] to delete all events.

Note that this action resets CO-920 and CO-920 cannot communicate with ProSafe-RS for several seconds.

10.4.3 Initializing CO-920 time

When engineering the time setting to use ProSafe-SLS communication function, remember that all references to time are based on the Universal Time Coordinated (UTC).

Before you connect DO module on SCS to DI module on ProSafe-SLS for time synchronization, specify year, month, day, hour, minute, and second from COM-SET to CO-920 to make CO-920 time match to SCS time. The time to match should be specified according to the information in the design study.

If time synchronization is performed between SCS and ProSafe-SLS, CO-920 uses DO output from SCS as a trigger and corrected to the predefined time. At that timing, date is corrected within 12 hours gap between the current time and the setting time. For that reason, the time difference between SCS and CO-920 must be less than 12 hours before time synchronization is performed.

The following figure shows an image of correcting date.

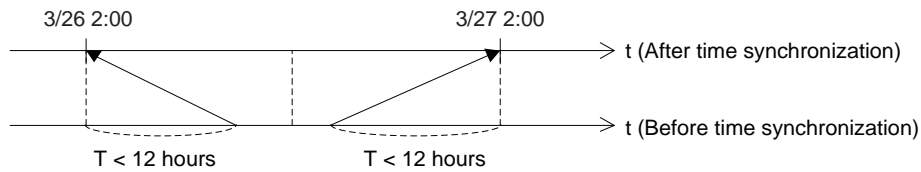


Figure 10.4.3-1 Image of Correcting Date

10.4.4 Engineering for Time Setup with DI Input

If you want to use the application logic for time synchronization created on ProSafe-RS to perform time synchronization for ProSafe-SLS, you also need to perform engineering on ProSafe-SLS.

**SEE
ALSO**

For more information about Engineering example for time synchronization, refer to:

- [Example of Engineering on ProSafe-SLS](#) on page 10-10
-

10.5 Engineering for CENTUM

If CENTUM is integrated, perform engineering to enable tag name access and build an application to display the operating status so that the ProSafe-SLS communication function can be used.

■ Tag Name Access

To attain the access to tag names that are assigned to I/O data of CO-920 and defined in ProSafe-RS, perform the tag name access engineering.

■ Configuring Application to Show Operating Status

Because the ProSafe-SLS and CO-920 are devices on the other end of subsystem communication for the SCS, they are not displayed in the operating status display windows of the HIS and SENG. If necessary, engineer the CENTUM Integrated System so that, for example, ProSafe-SLS or CO-920 data that has been read by using subsystem communication will be determined and graphics will be displayed accordingly.

10.6 Example of Application on ProSafe-SLS Communication Function

The ProSafe-SLS communication function cannot directly notify diagnostic information of ProSafe-SLS or errors of devices connected to the ProSafe-SLS, as alarms. ProSafe-SLS events are acquired and recorded as SOE events of the SCS. Note, however, that they are not notified to the HIS as alarms. These events can be referenced in the SOE Viewer or through the SOE OPC server.

To notify the operator, as alarms, of diagnostic information of ProSafe-SLS or errors of devices connected to the ProSafe-SLS, enable such data to be acquired from the CO-920 as Modbus communication data. In addition, create in the SCS a determination logic that uses this data, and create an application that uses the ANN FB or annunciator FB to notify the operator of error alarms and recovery alarms.

■ Application to Notify ProSafe-SLS Alarms to the HIS

The SCS determines the diagnostic information that is read from the CO-920 as Modbus communication data and the device data that is connected to the ProSafe-SLS. The CENTUM integration configuration allows the determination results at the SCS to be notified to the HIS by using the annunciator FB. The HIS handles the notified alarms as process data.

By performing CO-920 engineering to generate an event when the value of the diagnostic information associated with the applicable alarm has changed, changes in the diagnostic information can be managed as events.

The following figure shows an example of notifying ProSafe-SLS errors to the HIS as alarms.

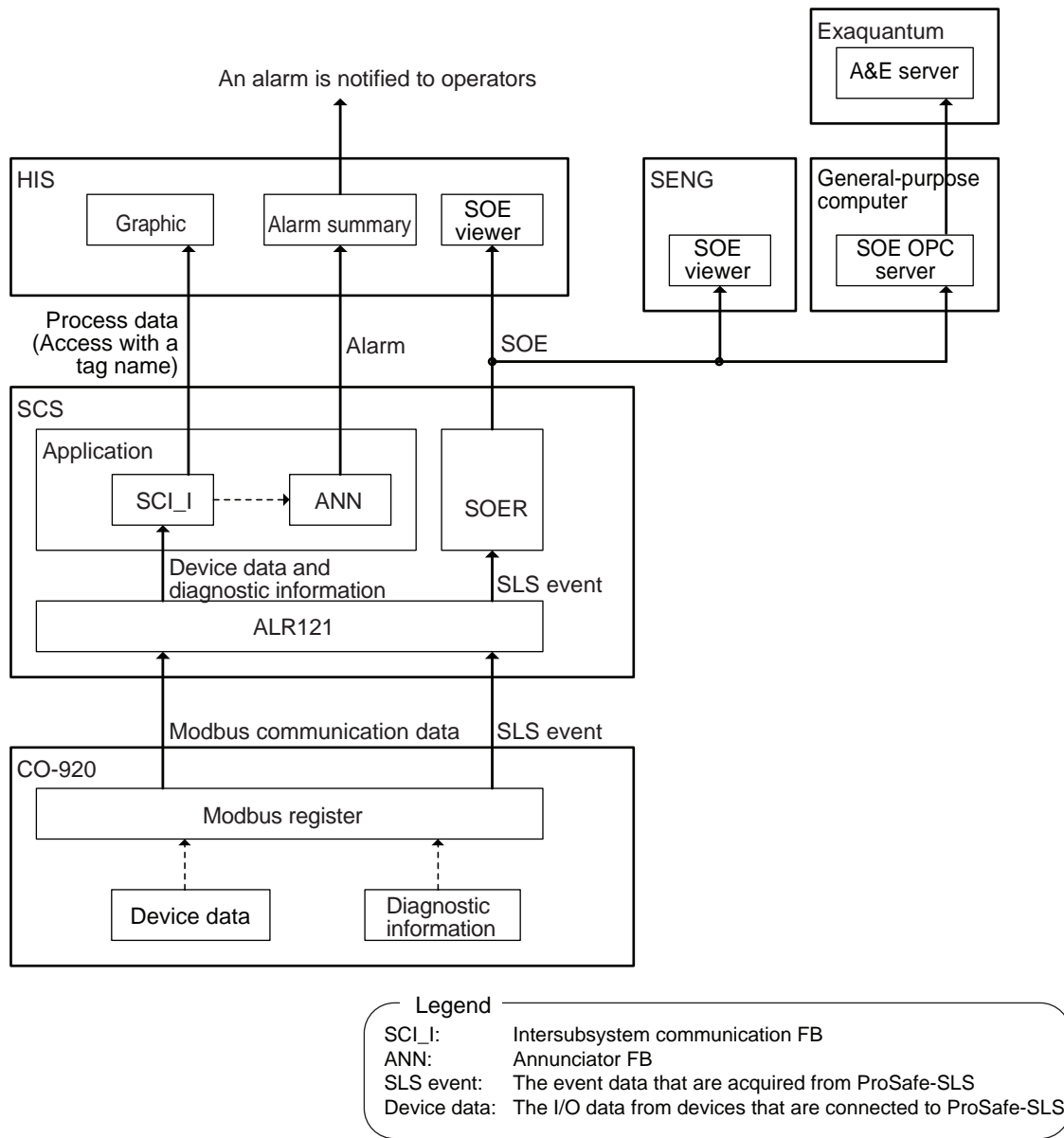


Figure 10.6-1 Example of Notifying ProSafe-SLS Alarms to the HIS

■ Application to Notify ProSafe-SLS Alarms to the FAST/TOOLS

In the FAST/TOOLS integration environment, you must configure an application on FAST/TOOLS that enables the FAST/TOOLS to acquire through the SCS, and determine, diagnostic information of CO-920 and data of devices connected to the ProSafe-SLS and then notify alarms to the operator.

The following figure shows an example of an application that prompts the FAST/TOOLS to notify ProSafe-SLS alarms to the operator in the FAST/TOOLS integration environment.

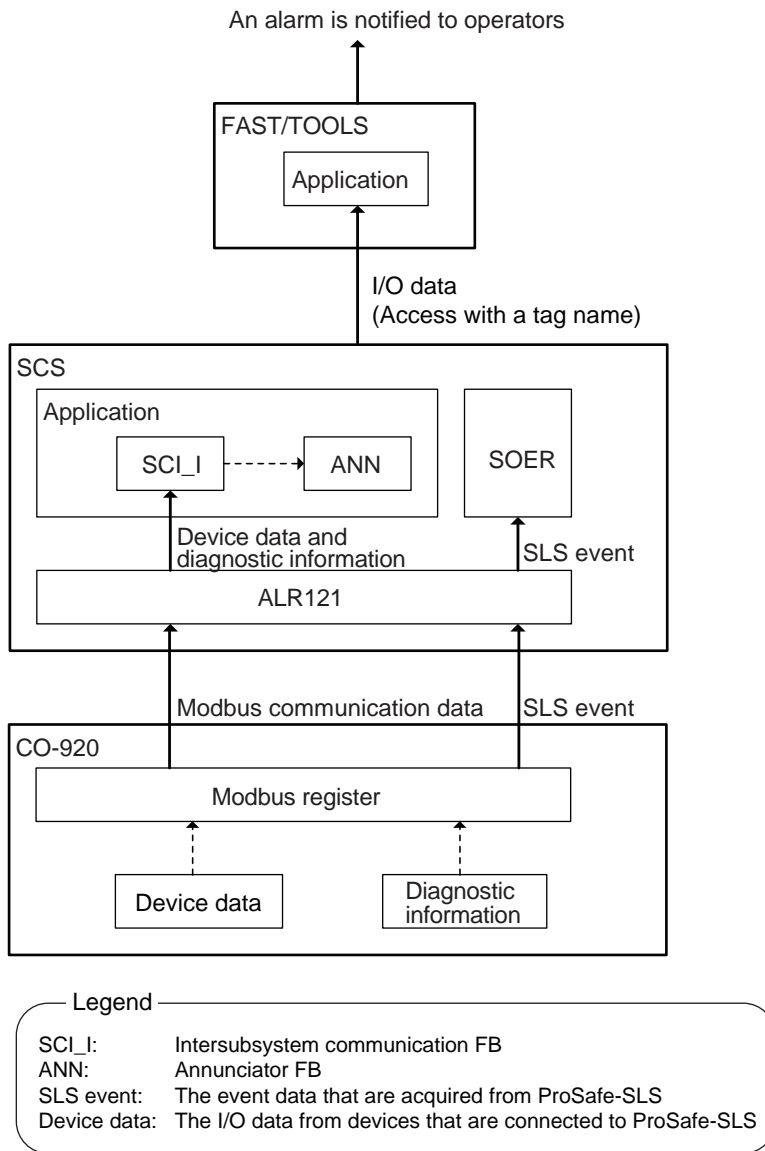


Figure 10.6-2 Example of Notifying ProSafe-SLS Alarms to the FAST/TOOLS

■ Application to Notify ProSafe-SLS Alarms to Field Devices

If alarm lamps and other field devices are used, configure an application that outputs the determination results of diagnostic information at the SCS from the DO module to the field devices.

The following figure shows an example of notifying ProSafe-SLS alarms to field devices.

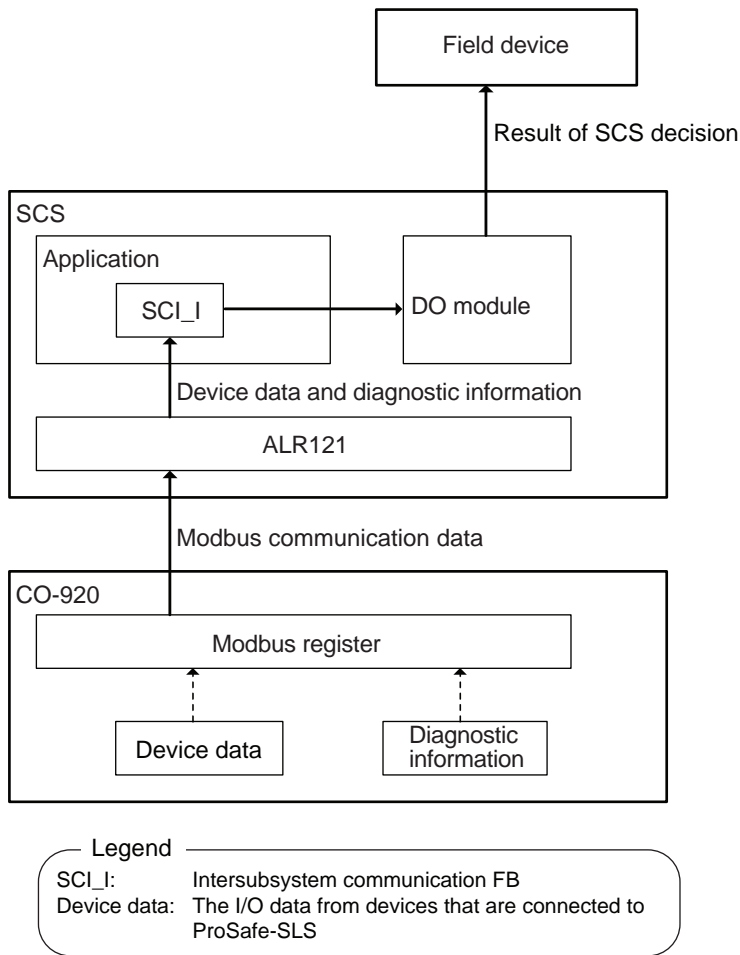


Figure 10.6-3 Example of Notifying ProSafe-SLS Alarms to Field Devices

Appendix 1. Guidelines for Developing Application Logic

This appendix provides guidelines for designing, coding, and testing application logics where Function Block Diagram (FBD), Ladder Diagram (LD), or Structured Text (ST) is used. For the development process of application software, check the conformity with the V-Model development process defined in IEC 61511.

Before using ST, you must understand its features well before developing application logics based on them. The ST implemented in the ProSafe-RS is a subset of the ST specification defined in IEC 61131-3, and can be used as a Limited Variability Language (LVL) defined in the IEC 61511.

You can use ST to simplify the coding of computation components (that is, FUs and FBs) by applying conditional statements, iteration statements, and array variables, where the drawing typically becomes complex if FBD or LD is used. On the other hand, a variety of combinations of conditional branches, iteration statements, and arrays, could produce highly complicated codes. When you use ST, take note of the following in creating user-defined FUs and user-defined FBs.

- ST must be used for computation components (i.e. FU or FB that computes output values from input values). (Use FBD or LD for logics; separate the use.)
- ST must be as simple, local, and readable as possible.

■ Designing

Note the following points when you design application logic:

- Define input parameters and output parameters of FB/FU, and create interface specifications.
- Minimize the number of parameters for FB/FU to realize a simple structure.
- Use Local variables whenever possible. Minimize the use of Global variables. Try to modularize and localize.
- Create FB/FU of simple function to shorten the run time.
An example of simple function is a calculation function of combination of four arithmetic operations. On the other hand, an example of complex function is a complex calculation function such as PID control calculation or convergence calculation. To make simple function, the followings are important.-
 - Put one role to a FU/FB to have easily understandable code
 - Write structured code for readability easily readable code with structured code
 - Reduce conditional branches as much as possible
- If one of multiple scripts is selected conditionally and executed, minimize variation of run-time among the scripts.

■ Coding

● Coding Rules

Define coding rules in advance, and code according to the rules.

Guidelines for coding rules are as follows:

Table Appendix 1-1 Guidelines for Coding Rules

Types	Item	Guidelines for Coding Rules
Common to FBD, LD, and ST	Naming	<ul style="list-style-type: none"> • Variable names must indicate their purposes. For example, variable name can be formatted as AAABBBB_CC_D AAA : Short name of equipment which the logic is applied for. BBBB : Equipment number CC : Shutdown point number D : Attribute • Differentiate Global variables from Local variables. For example, prefix of "G_" for global variable can be effective to differentiate global variables from local variables. And global variable can be differentiated by checking the "scope" field of the Dictionary View of the SCS Manager. • Variable names must be specific. • Variables having different purposes must have distinctly different names.
	Placing and wiring in FBD	<ul style="list-style-type: none"> • Basically, place and wire FU/FB according to the areas shown in Multi-Language Editor following these definitions: Inputs : Input variable(s), or FB instance(s) for external communications, and others. From : Global variable(s) (Variable(s) set by other programs) To : Global variable(s) (Variable(s) passed to other programs) Outputs : Output variable(s) or ANN FB instance(s) Logics : FU/FB, Global variables, and Local variables that are not listed in this cell.
	POU size	<ul style="list-style-type: none"> • Divide functions and organize into simple structure. A warning is displayed by Integrity Analyzer if it exceeds 4000 bytes.
	Floating-point arithmetic and Integer arithmetic	<ul style="list-style-type: none"> • Avoid rounding errors caused by repeated floating-point operations. • Avoid 'division by zero' in both floating-point operations and integer operations. • Avoid overflows in both floating-point operations and integer operations.(See the IMPORTANT section below.) • Use comparison operators ">", "<", ">=", and "<=" for comparing two floating-point variables. • A warning is displayed by Integrity Analyzer if "=" or "<>" (inequality) is detected in comparison of two floating-point variables.
	Data type conversion	<ul style="list-style-type: none"> • Avoid whenever possible. • If it is unavoidable, use 'FU dedicated to converting types' and check if the precision of the converted is acceptable. • Confirm that no overflow occurs. • No data conversion on Defined Words.
	Setting values	<ul style="list-style-type: none"> • For the following variables, their value must be set only once in one scan. <ul style="list-style-type: none"> • OUTPUT variables • Outputting from the SCS such as the output binding variables • Global Variables This is to avoid crash of a variable by writing data to the variable more than once. Use the Integrity Analyzer and check that values are not written to the same variable from multiple locations. Note that the SCS Manager's Dictionary View can display the scope of each variable. Browser can display every POU which accesses the variable.

Continues on the next page

Table Appendix 1-1 Guidelines for Coding Rules (Table continued)

Types	Item	Guidelines for Coding Rules
ST-specific	Control statements (IF, Case), and Iteration statements (FOR)	<ul style="list-style-type: none"> • Avoid complicated structures. Simplify. • Minimize the number of iterations.(A warning is displayed by Integrity Analyzer if the number in a FOR statement exceeds 500.) • No EXIT statement outside FOR loops.
	Number of lines	<ul style="list-style-type: none"> • Reduce the number of statements in each component of FB and FU so that they are contained in one window giving an overview of a processing. • If the number of statements (excluding comments) exceeds 500, a warning is displayed by Integrity Analyzer.
	Indents	<ul style="list-style-type: none"> • Use indentation to help grasp the structure of codes.
	Parentheses (brackets)	<ul style="list-style-type: none"> • Use parentheses to show the precedence of operators and to make statements easy to read.
	IF statements and CASE statements	<ul style="list-style-type: none"> • In IF statements or CASE statements, always use ELSE to specify the behavior when the conditions are not met.
	Output parameters	<ul style="list-style-type: none"> • In IF statements or CASE statements, no data must be set to output parameters.
	Calling FB	<ul style="list-style-type: none"> • In conditional statements and iteration statements, FB must not be called. (See the IMPORTANT section below.)
	Use of arrays	<ul style="list-style-type: none"> • Do not access outside the range of arrays.



IMPORTANT

- Floating-point arithmetic and Integer arithmetic

Define rules for avoiding errors in floating point operations (guidelines for reduced number of operations), overflows, underflows, and ‘division by zero’ (such as ensuring operations within the range where arithmetic exception never occurs or checking data before operations).

If an overflow or ‘division by zero’ occurs in operations with REAL-type variables, or ‘division by zero’ occurs in operations with integer-type variables, SCS behaves according to the specification in [Behavior at Abnormal Calculation] made in the SCS Constants Builder. If this specification is [SCS fails] (default), the SCS stops. If you specify [SCS continues], the SCS continues the operation without failing, but there is a potential risk that it cannot respond properly at demand generation related to the corresponding POU while an abnormal calculation persists. Also, if an overflow occurs in DINT operations, the result will be an unexpected value, and thereby the logic may not function normally.

To avoid this, the numeric values handled by the application must satisfy the following. Values of constants, of operation results, and of operation process must be within the recommended range (*1), and ‘division by zero’ never occurs.

To guarantee this, the following must be taken into consideration. If the requested operation contains division(s) and ‘division by zero’ or an overflow of operation result is possible, make sure to avoid that problem by providing a workaround referencing the example below. Consider the following two solutions in implementing a workaround:

- Validity of operation results after avoiding ‘division by zero’ or an overflow (Shutdown is executed or not.)
- If ‘division by zero’ or an overflow is averted, whether or not the plant operator should be notified that the arithmetic operation is not normal.

*1: Recommended range for REAL type:
 0.0, from 1.0×10^{-12} (=an extremely small value near 0) through 1.0×10^{12} (a large value), and from -1.0×10^{12} through -1.0×10^{-12} .
 Recommended range for DINT type: From -2,147,483,648 through 2147483647

An example of workaround for this problem is shown as follows:

If the ratio of the two analog input values, F1 and F2, from field devices exceeding “0.5” triggers a shutdown, the shutdown logic must be tested by the formula, “ $F1/F2 > 0.5$.” In this formula, the following measures can be considered.

Measures 1: Multiply both sides of the expression by F2, and use no division.

```
a:=0.5*F2;
IF (F1>a)
THEN
  (*Shutdown Logic*)
  :
  :
ELSE
  :
  :
END_IF;
```

Measures 2: If the denominator is 0.001 or less, replace it with 0.001 and calculate.

```
IF (F2<0.001)
THEN
a:=0.001;
ELSE
  a:=F2;
END_IF;
b:=F1/a;
IF (b>0.5)
THEN
  (*Shutdown Logic*)
  :
  :
ELSE
  :
  :
END_IF;
```



IMPORTANT

- Calling FB
FB has internal status such as the previous data. If an FB is called, a change is made to its internal status. If an FB is included in an IF statement, the FB is called only if the condition(s) of the IF statement is met. If the condition(s) of the IF statement is not met, the FB is not called. As a result, unexpected output may occur depending on the internal status of the FB. To avoid this, you should not use FB in conditional statements and iteration statements.

If you still have to use FB in an IF statement, remember the possible problem mentioned above and extra care must be taken.

● **Reviewing Codes**

When you finish coding, review the code (static analysis included) to make sure you coded correctly complying with the coding rules and the structure is not too complex. The guidelines for reviewing application logics are as follows:

Table Appendix 1-2 Guidelines for Reviewing Application Logics

Types	Item	Guidelines
Common to FBD, LD, and ST	Print	<ul style="list-style-type: none"> For effective reviews, print the codes in advance.
	Static analysis (Syntax)	<ul style="list-style-type: none"> Integrity Analyzer and compiler are used for static analysis. Based on the warning messages that are output by Integrity Analyzer and compiler, find coding errors and check the validity of the codes.
	Check codes	<ul style="list-style-type: none"> Check that the codes comply with the coding rules.
	FU/FB interfaces	<ul style="list-style-type: none"> Check the input and output parameters of FB/FU are valid. <ul style="list-style-type: none"> Names of input and output parameters match with those defined in the Design spec. The number and the sequence of input and output parameters match with those defined in the Design spec.
	Structure	<ul style="list-style-type: none"> Check that the structure is simple. To make simple structure, the followings are important. <ul style="list-style-type: none"> Put one role to a FU/FB to have easily understandable code. Keep easily readable code with structured code. Reduce conditional branches as much as possible.
	Conformity to Design spec	<ul style="list-style-type: none"> Check that the codes conform to the Design spec.
	Initialize variables	<ul style="list-style-type: none"> Check that local variables and global variables have been initialized before they are used.
	Unused variables	<ul style="list-style-type: none"> Check if unused variables exist. How to check: Use "browser" in SCS Manager to detect them.
	Setting values	<ul style="list-style-type: none"> Check if the following values are set only once in one scan. <ul style="list-style-type: none"> OUTPUT variables Outputting from the SCS such as the output binding variables. Global Variables
ST-specific	Number of steps	<ul style="list-style-type: none"> Check that the number of steps is not large. Reduce the number of statements in each component of FB and FU so that they are contained in one window giving an overview of a processing. If the number of statements (excluding comments) exceeds 500, a warning is displayed by Integrity Analyzer. If branches are included, the number of steps in each branch must be about the same. FU in a FOR statement may cause great disparity in the overall process amount because the size of each FU varies. Therefore, avoid calling FU whenever possible in the loop statements.

■ **Module Tests**

Guidelines for testing application logic as modules are given below. If ST is used, validity of all the conditional statements in the ST must be guaranteed.

Table Appendix 1-3 Guidelines for Testing Application Logic with Modules

Types	Items	Guidelines
Common to FBD, LD, and ST	Paths	<ul style="list-style-type: none">On Logic simulator or SCS simulator, or actual SCS, change the input value of all the logic elements to the following values, and check the output value. Analog data: Values within the range of normal operations (max. min. mean values), and values near the boundary value (Example: such as a branch point) Digital data: Values 0 and 1
	Run time	<ul style="list-style-type: none">On an actual SCS, check the load on CPU during runtime.
ST-specific	Paths	<ul style="list-style-type: none">On Logic simulator or SCS simulator, or actual SCS, conduct C2 coverage 100% tests using debugger. (*1)
	Run time	<p>Check the number of steps executed in ST as a means to learn the runtime.</p> <ul style="list-style-type: none">The number of steps in the longest processing.If a FOR statement is used, the number of iterations.

*1: C2 coverage (Condition Coverage) is a coverage level. It tests all the sub-conditions in a conditional statement one by one for true or false.

Appendix 2. Reuse of SCS Project Databases

The procedure for copying an existing SCS project database in order to reuse it for an SCS project with a different domain/station number is described as follows.

■ Copying an SCS Project

1. Copy an SCS project in order to reuse it.
 - a. Using Windows Explorer, copy the entire source SCS project to the target RS project folder.
 - b. Change the folder name ddss in the copied SCS project to SCSddss, using the new Domain Number and Station Number.
2. Change the Domain Number and Station Number of the copied SCS project database. The procedure for changing the Domain Number and Station Number of the copied SCS project database is almost the same as that for creating a new project.
 - a. Open the copied SCS project in SCS Manager and change the Domain Number and Station Number in SCS Project Properties. The following messages are displayed.
Domain Number or Station Number has changed.
Delete Master Database and update Domain Number and Station Number.
Are you sure?
 - b. Click [OK].
3. Change the Name (Resource Name) and Resource Number in Resource Properties.
4. Change the Name in Configuration Properties (Configuration Name).
5. Change the IP Address in Connection Properties.

■ Modifying an Application

The following modifications to the application are required on the copied station.

1. Modification of inter-SCS safety communication
Modify the inter-SCS safety communication application.
 - a. The domain number and station number on the consumer and producer will change. Modify the variable names accordingly.
 - b. Delete the existing binding table and regenerate it.
2. Modification of SCS link transmission
Modify the receiving station as appropriate.

■ Checking Copied Projects

Check that the copied SCS project is equivalent to the original project.

1. Build the copied SCS project from SCS Manager.
2. Launch the Integrity Analyzer from SCS Manager and check the integrity.

3. Launch the Cross Reference Analyzer from SCS Manager and check that all POUs are equivalent to those of the project before it was copied.
 - a. Use the Cross Reference Analyzer's function for comparison with the original project to compare the copied SCS project with the original SCS project. Check that all POUs are displayed in green, excluding the sections in which you have modified the inter-SCS safety communication and related areas. At this point, use the display on the title bar or the report of the Cross Reference Analyzer to check that the path to the original project to be compared is correct.
 - b. Validate the modified content.
Each modification must be tested at an appropriate timing.
4. For data that cannot be checked with the Cross Reference Analyzer, use the Project Comparing Tool to ensure that the copied SCS project is equivalent to the original SCS project.
 - a. Launch the Project Comparing Tool and compare the copied SCS project with the original SCS project. Ensure that there are no discrepancies, except in sections that you have modified. When you do so, check in the results printed from the Project Comparing Tool for the project path display area and the summary of discrepancies to make sure that the project paths that you are comparing are correct.
 - b. If a discrepancy is found, check that it is appropriate.
5. Perform an offline download to the SCS and make sure that the SCS starts.

TIP

Run the Cross Reference Analyzer, Project Comparing Tool, self-document printout and other functions on any modifications other than the inter-SCS safety communication and SCS link transmission in the copied SCS project, and ascertain the range for retesting in the usual manner.

Appendix 3. Glossary

The following terminologies are used within ProSafe-RS.

Table Appendix 3-1 Terminologies used in ProSafe-RS

Terminology	Meaning
Access control	A functionality to restrict user operations in each SENG. A SENG terminal where access control is applied requires an engineer name and password entry to perform particular operations. When an engineer tries to make an engineering operation, the engineer can not execute the desired action unless the engineer has the permission to perform the operation. CHS5170 Access Control and Operation History Management Package is required.
ADL	Inter-station data link block of CENTUM FCS
AIO module	Generic term for analog input/output modules
AIO/DIO module	Generic term for analog input/output modules and discrete input/output modules. Communication modules are not included.
Alarm class	Alarm information added to diagnostic information messages. On SENG, diagnostic information messages are displayed in different colors with different alarm marks according to the alarm class. <ul style="list-style-type: none"> • Class 1 (serious alarm) • Class 2 (moderate alarm) • Class 3 (minor alarm) • Class 4 (notification alarm)
Alarm priority	Process alarm information that is needed when ProSafe-RS is integrated with CENTUM. Alarm priorities are in five levels: high-priority alarm, medium-priority alarm, low-priority alarm, logging alarm, and reference alarm.
Alarm Priority Builder	The builder used to define process alarm priority levels when ProSafe-RS is integrated with CENTUM. For each alarm priority level, you can define the output style and alarm action on occurrence/recovery of process alarms generated in SCS.
Alarm processing table	The table that defines the process alarms' display color and alarm priority corresponding to the alarm status on CENTUM HIS. On ProSafe-RS, you can import the alarm processing table defined on CENTUM to use it for reference.
Alarm Processing Table Builder	The builder used to import the Alarm Processing Table defined on CENTUM into SCS project.
All output shutdown	To shut down all the output modules when the CPU stops due to a fatal error. During all output shutdown, the fail-safe values are output.
All Program Copy (APC)	In dual-redundant CPU modules, to copy the memory contents of the control-side module to the stand-by-side module.
Analog Input/Output modules with HART function	An analog input/output module that supports HART communication

Continues on the next page

Table Appendix 3-1 Terminologies used in ProSafe-RS (Table continued)

Terminology	Meaning
Application logic execution function	<p>The function that monitors the safety condition of the plant and performs pre-determined safety operations on detecting any hazards. Specifically, it denotes the following features and is used as the generic term for these features:</p> <ul style="list-style-type: none"> • Input processing of the process data from the field • Execution of user-defined application logic • Outputting process data to the field • Communication data I/O (Subsystem communication) • Inter-SCS safety Communication • SCS Link Transmission • Self-diagnosis
Application run time	<p>The proportion of the time in a scan period of the SCS during which the CPU is working for the application execution functions. (Represented in percentage.)</p>
Automatic IOM download	<p>For dual-redundant AIO/DIO modules of a running SCS, if only the standby-side AIO/DIO module is replaced for maintenance, the configuration information is automatically downloaded from the control-side module to the standby-side module after replacement. This function is called automatic IOM download.</p>
Behavior at abnormal calculation	<p>The setting item of an SCS that specifies whether the SCS is stopped when an abnormal calculation, such as an overflow in floating-point data calculation, has occurred due to a defect in the application logic. It also refers to the behavior of the SCS specified with this setting.</p>
Binding List View	<p>The view on SCS Manager that is used to associate the variables for inter-SCS safety communication between producer SCS and consumer SCS. See Workbench User's Guide for more information.</p>
Binding variable	<p>Variables that link variables of producer SCS and variables of consumer SCS performing inter-SCS safety communication. The producer variables of a producer SCS need to be grouped for each consumer SCS that receives them. The consumer variables of a consumer SCS also need to be grouped for each producer SCS that sends them. These groups are called "binding groups."</p>
Build	<p>The operation that is run on SCS Manager to generate the database to be downloaded to a target SCS.</p>
Burnout	<p>One of input module action specifications when Thermocouple or Resistance Temperature Detector input has an open circuit. Selectable options at open circuit are to clamp the input to an upper or a lower limit or to disable burnout actions. Clamping to an upper limit is called burnout upscale and clamping to a lower limit is called burnout downscale.</p>
CENTUM	<p>In the user's manuals of ProSafe-RS, the generic term that refers to CENTUM VP and CENTUM CS 3000.</p>
CENTUM project folder	<p>The folder storing the data of the CENTUM project to be connected to SCS projects. When the system is integrated with CENTUM, you need to specify this folder in the SCS Project Properties dialog box.</p>

Continues on the next page

Table Appendix 3-1 Terminologies used in ProSafe-RS (Table continued)

Terminology	Meaning
Clean Project	The command on SCS Manager that deletes the files created in the previous run of the build command. After Clean Project is run, only offline downloading is possible.
Communication I/O Lock Window	The window used to lock/unlock the input/output data for subsystem communication. You can set values to the input/output data locked through this window. This window is used on SENG for maintenance and testing purposes.
Communication module	A module used to implement communications with systems (such as PLCs) from other companies. It is treated as one of the input/output modules.
Consumer SCS	SCS which receives data in inter-SCS safety communication.
Control bus driver	A driver software on a PC necessary to perform control bus communications via V net or Vnet/IP network.
Control bus interface card	An interface card installed to a PC to allow it connecting to V net.
CPU module	The main module that works to implement the control performed by SCS.
CPU node	A component of SCS in which CPU modules are mounted. It is also called "Safety Control Unit."
Cross Reference Analyzer	<p>One of the Safety Analyzers. A Safety Analyzer which shows the following information in the screen or in an analysis report.</p> <ul style="list-style-type: none"> • Differences between the previously downloaded application (which is currently running on the SCS) and the application that is to be downloaded • The scope that will be affected by downloading the new application <p>This tool enables you to narrow the scope of re-testing when the application logic has been modified.</p>
Cycle Time	Another name for the scan period of application logic execution functions. It is defined by setting the [Cycle Timing] in the Resource Properties dialog box of SCS Manager.
Database Validity Check Tool	The tool that checks the mutual validity of the work database, the master database and the SCS database within an SCS. In addition, database can be repaired.
Debug mode	A mode of SCS Manager that is used in target tests. See Workbench User's Guide for more information.
Defined word	Definition of a constant expression, TRUE/FALSE Boolean expression, or keyword. Defined words are replaced by their corresponding expressions during compiling.
Diagnostic information message	SCS sends diagnostic information messages for detected faults and for the operation on the safety functions to notify user of events. In a system integrated with CENTUM, diagnostic information messages of ProSafe-RS are sent to HIS and treated as system alarms.
Dictionary View	The view on SCS Manager used to set parameters and define variables of POU's. See Workbench User's Guide for more information.

Continues on the next page

Table Appendix 3-1 Terminologies used in ProSafe-RS (Table continued)

Terminology	Meaning
Digital input/output module	The name of the modules that handle discrete inputs/outputs.
DIO module	The generic term for discrete input/output (digital input/output) modules
Discrete input	Input of a discrete (ON/OFF) signal
Discrete output	Output of a discrete (ON/OFF) signal
ENG	A computer installed with engineering function packages for system generation and maintenance of CENTUM.
Engineers' account builder	The builder used to register engineers that are managed by the access control/operation history management function. It is also used to define access rights of engineers. All the settings made on this builder are saved in the Engineers' account file.
Error level	The level of errors occurred in SCS. Errors are classified in three levels: fatal error, major error, and minor error. With a fatal error, the SCS cannot continue operation. With a major error, the SCS can continue operation but some of the safety functions are disabled. Minor errors do not affect safety functions of the SCS. The users are notified of the error level by diagnostic information message.
ESB bus (Extended serial backboard bus)	The bus for connecting the CPU node and I/O nodes of SCS. ESB bus coupler modules are installed in the CPU node while ESB bus interface modules are installed in I/O nodes. These modules are connected using ESB bus cables.
Ethernet communication module	The name of a module that supports Modbus TCP communication protocol. SCS uses this module to perform Modbus slave communication.
Event log file	The file containing SOE (Sequence Of Event) events which is stored in SCS. You can save this file to SENG.
Expanded test function	The function to perform SCS simulation tests using SCS simulators on multiple computers and running them in coordination. This function is available with the use of the Expanded Test package of CENTUM.
Extend scan period automatically	The function that automatically extends the scan period of application logic execution functions when the load of SCS becomes heavy.
External communication function	The function of SCS for exchanging data with external systems. It is designed so as not to affect the application logic execution functions and comprises the following features: <ul style="list-style-type: none"> • CENTUM Integration Function • SOER Function • Modbus Slave Communication Function • Diagnostic information collection • PRM-supported HART on-demand communication
External communication function block	Function blocks used as the interface for data setting to SCS from Modbus master in Modbus slave connection or data setting to SCS from a CENTUM station when ProSafe-RS is integrated with CENTUM. External communication function blocks are interference-free.

Continues on the next page

Table Appendix 3-1 Terminologies used in ProSafe-RS (Table continued)

Terminology	Meaning
FAST/TOOLS:	SCADA system developed by Yokogawa
FCS simulator	A simulator program offered for CENTUM systems. It simulates the behavior of FCS on a computer.
Field Control Station (FCS)	A component of CENTUM system which performs process control in plants.
Forcing	The function to lock and change the values of inputs/ outputs or variables of SCS. It is used on SENG for maintenance of SCS or debugging of application logic. This function is available while the security level of the target SCS is set to 1 or 0.
Function Block Diagram (FBD)	A language defined in IEC 61131-3.
Function Block (FB)	POU defined in IEC 61131-3. Constituents incorporated in FBD/LD/ST.
Function (FU)	POU defined in IEC 61131-3. Constituents incorporated in FBD/LD/ST.
Generation time	The time at which build was run for an SCS project to generate SCS database. In the SCS State Management window or a system report, a generation date is shown for each type of database: POU DB, Variable DB, System DB, and Integration DB.
Global switch	An element of CENTUM FCS which can be set to the same logical value in all the FCSs within a domain. By using the SCS global switch communication feature of SCS link transmission, values of some global switches can be sent or received between CENTUM stations (FCS, APCS, or GSGW) and SCS.
Global variable	A variable which can be accessed by any POU.
Grouping override function block	A special type of override function block. Grouping override function blocks belonging to the same group can be controlled so that no more than one function block within the group is overriding at the same time.
Hardware Architecture View	A view on SCS Manager that graphically displays the SCS and the network. See Workbench User's Guide for more information.
Human Interface Station (HIS)	A component of CENTUM system. It is a computer installed with a set of operator interface package software that enable operation and monitoring. Monitoring of SCS is also possible from HIS.
I/O Lock Window	The window used to lock/unlock the input/output channels of the AIO/DIO modules in SCS. You can set values to the input/output variables connected to the channels that have been locked through this window. This window is used on SENG for maintenance and testing purposes.
I/O node	A component of SCS in which input/output modules are mounted. It is used when you want to add input/output modules. It is also called "Safety Node Unit."
I/O Parameter Builder	The builder used to make settings for nodes and input/output modules of SCS and parameters that specify the behavior of the channels of the input/output modules (I/O parameters).
I/O Wiring View	The view on SCS Manager used to create or delete input/output modules in SCS, set node addresses, define wiring between channels and variables. See Workbench User's Guide for more information.

Continues on the next page

Table Appendix 3-1 Terminologies used in ProSafe-RS (Table continued)

Terminology	Meaning
Input module	Generic term for analog input modules and discrete input modules.
Input valuable	Variables connected to the channels of an input module, which are used in POU's.
Input value at error occurrence	A predefined value that is output when a value from an input module becomes abnormal.
Input/Output module	Generic term for AIO/DIO modules and communication modules.
Integration with CENTUM	ProSafe-RS can be used by integrating with CENTUM VP or CENTUM CS 3000. In the User's Manuals of ProSafe-RS, the integration with CENTUM VP or CENTUM CS 3000 is referred to as "Integration with CENTUM."
Integrity Analyzer	One of the Safety Analyzers. The tool used to analyze the safety of the created application logic. The users are required to use this tool to detect the use of FB/FU that are unacceptable as safety functions. The results of analysis can be shown on the screen or output in the analysis report.
Interference-free	Does not interfere safety application.
Internal variable	Variables not connected to an input/output module, which are available for use in POU's.
Inter-SCS Communication Lock Window	The window used to lock/unlock the input/output data for inter-SCS safety communication on an SCS by SCS basis. You can set values in the inter-SCS safety communication FB of the SCS locked through this window. This window is used on SENG for maintenance and testing purposes.
Inter-SCS safety communication	Safety communication used to implement safety loops among multiple SCS. Safety communication by SCS link transmission is not included in this communication. Safety loops are implemented by defining the function blocks dedicated for inter-SCS safety communication (producer FB and consumer FB) and binding variables.
IOM Control Right Switching Tool	The tool used for switching the control right of AIO/DIO modules placed in redundant configuration. Redundantly configured communication modules cannot be switched with this tool.
IOM download	Processing which downloads the input/output configuration information such as I/O parameters to input/output modules. This processing may occur during online change download after changing I/O parameters of input/output modules using I/O Parameter Builder.
IOM download tool	A tool that is needed when input/output modules have been replaced due to a malfunction, etc. It is run from the SCS State Management window and downloads the input/output configuration information stored in the master database of the SCS project to the input/output modules.
IOM Report	A dialog box which shows the status and error-related diagnostic information about an individual input/output module. IOM Report is called up from the SCS IOM Maintenance Tool.

Continues on the next page

Table Appendix 3-1 Terminologies used in ProSafe-RS (Table continued)

Terminology	Meaning
IOM Reset Function	A function that allows you to restore an I/O module from SENG. Only in the cases when an I/O module stops because of failures on the field side, you can restore the module by manually executing IOM download from SENG.
Ladder Diagram (LD)	A language defined in IEC 61131-3.
Legacy model	A model of information security settings set on SENG. This model should be used when the standard model of security settings is too tight or when compatibility with other system is required.
Library project	A project database that can be used as a library independent of specific SCS. The functions and function blocks that are used in multiple SCSs can be created as library projects and be copied to each SCS project.
Link Architecture View	A view on SCS Manager which graphically shows the resources of SCS project and data links among the resources. On this view, you can define POU, add variable groups, etc. See Workbench User's Guide for more information.
Local variable	Variables that can be used in only one POU.
Logic simulation test	Tests performed by running a logic simulator from SCS Manager. The logic simulator is a program that simulates the behavior of POUs on a computer.
Logical data	For input variables, the data passed from an input variable to the application logic. For output variables, the data passed from the application logic to an output variable. For internal variables, the data to be output from that internal variable. Normally, the values of physical data and logical data match. However, while a variable is under forcing, the connection between its physical data and logical data is disconnected, and therefore they may not match.
Manual operation function block	Function blocks used to output values to the application logic by manual operation from CENTUM HIS when the system is integrated with CENTUM. These function blocks output either BOOL-type data or analog-type data and can be used for valve operation.
Mapping element/Mapping block	In a system integrated with CENTUM, a mapping element or mapping block is created if you assign a tag name to an internal variable, input/output variable, or a specific type of function block of the application logic using the Tag Name Builder. This scheme enables access to the data in SCS from CENTUM by specifying a tag name.
Master database	The database stored in SENG and is running on a target SCS. It consists of source files containing definitions for the SCS and the SCS database generated by running a build of the source files.
Master database offline download	The function to download, to the CPU modules of an SCS, the SCS database saved on SENG as the master database, which was previously downloaded to the SCS for actual run. You need to run this download when you replace both CPU modules in the SCS. You do not need to run this download when you replace one of the dual-redundant CPU modules.

Continues on the next page

Table Appendix 3-1 Terminologies used in ProSafe-RS (Table continued)

Terminology	Meaning
Master Database Restoring function	This tool restores the SCS project being edited to the state it was last downloaded to the target SCS. It is used to discard the changes made to the work database so far and revert it to the master database as the new work database for engineering. This tool is helpful when you have accidentally changed any settings that require offline download.
Modbus Address Builder	The builder that is used to define Modbus device addresses for Modbus slave connection.
Modbus slave connection	Connection for communications where SCS acts as a Modbus slave and the data in the SCS are read or set by the Modbus master (external device) via Modbus protocol. This communication is called Modbus slave communication.
Modification files viewer	A viewer to view modification files saved in an operation history database.
Multi-Language Editor	The editor used to create and edit application logic for SCS. In ProSafe-RS, application logic can be created using the following three languages, which are defined in IEC 61131-3. <ul style="list-style-type: none"> • Function block diagram (FBD) • Ladder diagram (LD) • Structured Text (ST) See Workbench User's Guide for more information.
Narrowband system	FAST/TOOLS integrated environment that sets the network mode of Vnet/IP-Upstream as narrowband mode.
Network mode	Indicates the operating mode of Vnet/IP-Upstream. The operating mode that supports the line characteristic is selected from the following operating modes by using the Domain Property Setting Tool. <ul style="list-style-type: none"> • Standard mode • Wide-area mode • Narrowband mode
Offline download	The function to download the system program of SCS and the database generated using the engineering functions of SENG to a target SCS while the CPU of the SCS is stopped. The SCS is restarted after the offline download is completed.
Online change download	The function to download only the changes made to the application to a target SCS while the CPU of the SCS is running. Online change download is not possible depending on which items of the application have been changed.
Online monitoring function	The function to monitor the application logic running on SCS. You can monitor the values of variables and function blocks of a running program and the status of whether conditions are met or not. The online monitoring function is available through the following windows: FBD window, LD window, and ST window of Multi-Language Editor, Dictionary View, and SPY List Window.
Operating mode	Operating mode of SCS. There are five operating modes: Stop mode, Loading mode, Initial mode, Waiting mode, and Running mode. SCS normally runs in the Running mode.
Operation history database viewer	A viewer to view operation log saved in an operation history database.

Continues on the next page

Table Appendix 3-1 Terminologies used in ProSafe-RS (Table continued)

Terminology	Meaning
Operation history management	Functionality to record operations performed by each SENG user into the operation log. When downloading to SCS, the information of the modified project data (modification file) is saved. These operation log or change information are saved into the operation history database. CHS5170 Access Control and Operation History Management Package is required.
Operation history management setup tool	A tool to setup access control and operation history management functionality.
Operation mark	A frame-shaped mark attached to a faceplate displayed on CENTUM HIS. It is used to make certain elements or function blocks easy to be distinguished. You can save in SENG the operation marks set for elements or function blocks of SCS and download the saved operation marks to SCS.
Optical bus repeater	The device used to extend the distance of V net by using fiber-optic cable.
Optical ESB bus repeater module	Generic term for the modules mounted in nodes in SCS when nodes in the SCS are connected with fiber-optic cables for the purpose of extending the distance of ESB bus. Optical ESB bus repeater master modules can be mounted in CPU nodes or I/O nodes, while Optical ESB bus repeater slave modules can be mounted only in I/O nodes. A master module and a slave module are connected on a one-to-one basis using a fiber-optic cable.
Output disable status	The status of output modules in SCS in which the output values of the application logic are not output from the modules. Channels of all the output modules are in this status immediately after the SCS is started up. To enable outputs from the output modules in this status, it is necessary to perform the output enable operation. The output disable/enable status is controlled for each output channel.
Output enable operation	The operation to connect outputs from the application logic to the channels of output modules. You can perform this operation from the I/O Channels Status dialog box of SCS Maintenance Support Tool on SENG. This operation places all the channels of all the output modules on the SCS in the Output Enable status, and output values of the application logic are output from output channels. However, channels generating errors remain in the Output Disable status. Performing the output enable operation immediately after an SCS is started also initiates inter-SCS safety communication, SCS Link Transmission, and subsystem communication.
Output module	Generic term for analog output modules and discrete output modules.
Output Shutoff Switch	The switch to shutoff all the outputs of a module when a dangerous failure that can prevent normal output of signals has occurred to the module. This switch can be activated automatically by setting the parameter for the output module.
Output value at fault	The value that is output as the fail-safe value when an output module detects an error.
Output variable	Variables connected to the channels of an output module, which are used in POU's.

Continues on the next page

Table Appendix 3-1 Terminologies used in ProSafe-RS (Table continued)

Terminology	Meaning
Override	The operation to forcibly fix the value of a variable of SCS to a predefined value while the SCS is running normally. In order to enable override operations from CENTUM HIS, create application logic for performing override operation by using override function blocks.
Partial Stroke Test (PST)	Inspection of emergency shutdown valves, which do not need to work in normal conditions. PST is performed by slightly moving the valve to check if the valve is not stuck at one position and that it can work properly when required.
Physical data	For input variables, the data read from an input module. For output variables, the data to be set into an output module. For internal variables, the data input to the variable. Normally, the values of physical data and logical data match. However, while a variable is under forcing, the connection between its physical data and logical data is disconnected, and therefore they may not match.
Plant Resource Manager (PRM)	A software product of Yokogawa that is used to manage field devices and other equipment used in a plant online.
Process data	In ProSafe-RS, process data means analog input/output data and discrete input/output data.
Producer SCS	SCS which sends data in inter-SCS safety communication.
Program Organization Unit (POU)	Generic term for program, function block, and function that are defined in IEC 61131-3.
Project Attribute Tool	The tool that shows the attributes of SCS projects. It is mainly used when using test functions.
Project comparing tool	A tool to detect differences between two SCS projects, display and print them. This tool is able to compare work database and the master database of any SCS project.
ProSafe authentication mode	A user authentication mode to provide separate user management for ProSafe-RS users apart from Windows users when using access control and operation history management functionality.
RAS function	RAS means Reliability, Availability, and Serviceability. This is an important standard when evaluating the system performance. Reliability indicates robustness against error occurrence, availability indicates shortness of downtime and serviceability indicates ease of repair at failure. The RAS function diagnoses whether hardware and software of SCS are running normally and handles maintenance of them if any errors are detected. It is one of the most essential SCS functions which shuts down the system, changes the status of SCS, and takes other actions according to the situation.
Resource	A set of application logic that is defined for a single SCS.
RS Project	A group of SCS projects that is defined in order to manage engineering data of multiple SCS projects together. The status of SCSs belonging to the same RS project can be monitored collectively by using the SCS Maintenance Support Tools.

Continues on the next page

Table Appendix 3-1 Terminologies used in ProSafe-RS (Table continued)

Terminology	Meaning
Safety application	Application which monitors the safety status of the plant and, if any abnormality is detected, performs the safety action that is programmed for the abnormality.
Safety Control Station (SCS)	A station which performs safety control in ProSafe-RS systems. SCS consists of a CPU node and I/O nodes.
Safety Control Unit	A component of SCS in which CPU modules are mounted. (Hardware product name)
Safety Node Unit	A component of SCS in which I/O modules are mounted. It is used when you want to add I/O modules. (Hardware product name)
Scan period of the application logic execution function	Of the two types of scan periods of SCS, the scan period at which the application logic execution functions are executed. It is defined by setting the [Cycle Timing] in the Resource Properties dialog box of SCS Manager.
Scan period of the external communication function	Of the two types of scan periods of SCS, the scan period at which the external communication functions are executed. This scan period is defined by setting [Scan Period for External System] on the SCS Constants Builder.
SCS Constants Builder	The builder used to set the constants and the mode of time synchronization of an SCS.
SCS database	Database in a format executable on SCS, which stores the results of engineering works done on SENG. SCS database consists of POU DB, Variable DB, System DB, and Integration DB.
SCS global switch communication	An interference-free type of SCS link transmission that is used to communicate with CENTUM FCS.
SCS Information dialog	The dialog box which shows the numbers of the POU's and variables used in the SCS project or the size of the area for storing them. It is a dialog box of the SCS Maintenance Support Tool.
SCS link transmission	The function of SCS that a local SCS broadcasts its data periodically to other stations within the domain. By using this function, a local SCS can also receive the data broadcasted by other stations and the received data can be referenced by the application logic. SCS link transmission is available in two modes: SCS link transmission safety communication and SCS global switch communication.
SCS Link Transmission Builder	The builder used to define SCS link transmission safety communication and SCS global switch communication.
SCS Link Transmission Lock Window	The window used to lock/unlock the data for SCS link transmission on an SCS by SCS basis. You can set values to the SCS link transmission communication data of the SCS locked through this window. This window is used on SENG for maintenance and testing purposes.
SCS link transmission safety communication	A type of SCS link transmission that can implement safety loops.

Continues on the next page

Table Appendix 3-1 Terminologies used in ProSafe-RS (Table continued)

Terminology	Meaning
SCS Maintenance Support Tool	A set of tools to facilitate maintenance of SCS. These tools are for supporting maintenance tasks and analysis to find out the cause of errors, not provided for the monitoring of SCS by the operator.
SCS Manager	The main window used to define SCS projects. It is also called "Workbench."
SCS Project	A project database corresponding to a single SCS. In ProSafe-RS, engineering data are managed for each SCS project. Within an SCS project, the database consists of master database and work database, which are managed separately.
SCS project attribute	Attributes given to SCS projects for the testing of SCS. You can specify one of three attributes: default project, current project, and user-defined project. The project attribute determines whether the project can be downloaded to a target SCS, whether the project can be tested by SCS simulation, etc.
SCS Project Properties	This is the title of the dialog box on SCS Manager that is used to define SCS properties such as the model name, domain number, and station number. When the system is integrated with CENTUM, the location of CENTUM project folder is also defined in this dialog box. See Workbench User's Guide for more information.
SCS security level	The numeric value which shows the degree of how the data in the SCS is protected against data setting access from external devices or by personnel. The security levels are 0, 1, or 2, and SCS usually runs at level 2, which is the highest level. Level 0 is called the offline level, and levels 1 and 2 are called the on-line level.
SCS simulation test	Testing with SCS Simulators. SCS simulator is a program to simulate SCS actions on a computer.
SCS taglist generation	The function to generate an SCS taglist, which is required for monitoring SCS from CENTUM HIS. SCS taglist generation is run by selecting the [SCS Taglist Import] command on System View of CENTUM. SCS taglist is a database that is defined based on the tag names assigned to function blocks and other elements of SCS.
SCS Test Function Window	A window which manages starting and quitting of SCS simulator. You can start this window from SCS Manager or System View of CENTUM.
SCSP1-S (SCSP1)	SCS which uses SSC50S/SSC50D as the CPU node.
SCSP2-S (SCSP2)	SCS which uses SSC60S/SSC60D as the CPU node.
SCSV1-S (SCSV1)	SCS which uses SSC10S/SSC10D as the CPU node.
SCSU1-S (SCSU1)	SCS which uses SSC57S/SSC57D as the CPU node.
Self document	A function of SENG which prints out the definitions of SCS projects in certain formats.

Continues on the next page

Table Appendix 3-1 Terminologies used in ProSafe-RS (Table continued)

Terminology	Meaning
Self-diagnosis	The schema of SCS for detecting abnormality in hardware and software by itself. It is run periodically and if any abnormality is detected, a diagnostic information message and status information are generated. The diagnostic information messages are sent to SENG and CENTUM HIS. The status information can be referenced by the application logic.
SENG	A computer installed with the SCS engineering functions, test functions, and maintenance functions. On SENG, you can perform engineering works, such as creation, downloading, and testing of the application logic, and maintenance of SCS.
Sequence of Event Recorder (SOER)	A function that records events detected by SCS so that the user can analyze them. The collected and saved event information can be shown on the SOE viewer of SENG or CENTUM HIS.
Serial communication module	The name of a module that supports Modbus communication protocol (RTU mode). SCS uses this module to perform subsystem communication or Modbus slave communication.
Stand-alone SCS configuration	A system configuration where an SCS which is connectable to Vnet/IP network runs alone without being connected on Vnet/IP network.
Stand-alone system	A system in which only ProSafe-RS stations (SCS and SENG) are connected on the control bus.
Standard model	A model of IT security settings set on SENG. The standard model is categorized into two types according to the management of computers on the Windows network: Windows domain type and stand-alone type.
Start output module operation	The operation to recover the outputs of a module that were shut off by the activation of the output shut-off switch. This operation is performed using the SCS maintenance support tool. After recovery, all the channels of the output module are in the output disable status, so the output enable operation is required to deliver outputs.
Structured Text (ST)	A language defined in IEC 61131-3.
Subsystem communication	Communications performed between SCS and a subsystem. In this communication, SCS acts as the communication master and reads/writes data from/to the subsystem. Modbus protocol is supported in subsystem communication.
Subsystem communication module	Another name of serial communication module. This name is used when the serial communication module is used for subsystem communication.
System function block	Function blocks which indicate the status of SCS. System function blocks have a name beginning with "SYS_."
System View	The main window of the system generating functions of CENTUM. System View plays a central part in CENTUM engineering works.

Continues on the next page

Table Appendix 3-1 Terminologies used in ProSafe-RS (Table continued)

Terminology	Meaning
Tag Name Builder	The builder used to define tag names for function blocks and variables for use in a system integrated with CENTUM. Annunciator messages are also defined on this builder. By defining tag names using this builder, their mapping blocks or elements are created.
Target test	Testing of created application on an actual SCS by using the test functions.
Test Project Creating Tool	The tool used to create projects for SCS simulation test.
Time synchronization method	<p>Method of system time synchronization. For SCSV, V net time synchronization or IRIG-B time synchronization can be selected. For SCSP, only Vnet/IP time synchronization is used.</p> <ul style="list-style-type: none"> • V net time synchronization: The V net time is set to the CPU modules and input modules of the SCS. • IRIG-B time synchronization: Time information is acquired via IRIG-B from the standard clock installed outside the system and set to the CPU modules and input modules of the SCS. • Vnet/IP time synchronization: The network time on Vnet/IP is set to the CPU modules and input modules of the SCS.
Trip signal file	A file on SCS that stores the SOE data of the event specified as the trip signal and the data of the events before and after that event. This file can be saved into SENG. The signals that can be specified as trip events are the signals of DI/DO modules and the signals of function blocks dedicated to SOE.
Unit for optical ESB bus repeater module	A unit which is connected to SCS and exclusively used for mounting ESB bus optical repeater modules.
User-defined function	Functions defined by the user. You can create user-defined functions by using Multi Language Editor.
User-defined function block	Function blocks defined by the user. You can create user-defined function blocks by using Multi Language Editor.
User-defined project	A project created using Test Project Creating Tool. This project is for SCS simulation tests and cannot be downloaded to actual SCS.
Vnet/IP device	The device that is connected with Vnet/IP. Vnet/IP interface card (model: VI701 and VI702) and processor module (model: SCP451, SCP461) are included.
V net bus repeater	The device used to extend the distance of V net bus coaxial cable.
V net router	The device used to connect a V net domain and a Vnet/IP domain. Engineering of V net router is done on the CENTUM system.
Version Control Tool	A function that manages the change history of SCS projects and assists the user with system updating tasks. By using the Version control tool, you can save the SCS project data at a certain point with a version number and restore the project data of a certain version.

Continues on the next page

Table Appendix 3-1 Terminologies used in ProSafe-RS (Table continued)

Terminology	Meaning
Virtual domain link transmission	Virtual domain link transmission provides virtual domain capability to V net domain and Vnet/IP domain connected with V net router style S3 or above. SCS global switch communications are allowed between SCS and FCS in the virtual domain and these communications are called virtual domain link transmission.
Vnet/IP interface card	An interface card installed to a PC to allow it connecting to Vnet/IP network.
Vnet/IP open communication driver	A driver software on a PC necessary to perform open communications (Ethernet communications) on Vnet/IP network.
Watch Dog Timer (WDT)	A mechanism which allows a system to self-diagnose to check if it is running normally at a constant period. SCS also has a WDT.
Windows authentication mode	A user authentication mode to manage a ProSafe-RS user as a Windows user when using access control and operation history management functionality.
Wiring check adapter	An element used to detect faults in the wiring between discrete input modules and field devices. Two types of wiring check adapters are available: SCB100 for detecting disconnections and SCB110 for detecting short-circuits.
Work database	The results of engineering are first saved in a work database. A work database consists of source files containing definitions for the SCS and the SCS database generated by running a build of the source files.
Workbench	Another name of SCS Manager. Workbench User's Guide is the help file that explains the development environment of SCS application. You can read Workbench User's Guide while you perform engineering works in the development environment called up from SCS Manager. (However, Workbench User's Guide does not include explanations about the tools started from the launchers selected in the [Tools] menu of SCS Manager.)

Revision Information

Title : Engineering Guide

Manual No. : IM 32Q01C10-31E

Jan. 2015/4th Edition/3.02.20 or later*

*: Denotes the release number of the Software Product corresponding to the contents of this Manual. The revised contents are valid until the next edition is issued.

Introduction	ProSafe-RS Document Map has been deleted, and a description of Safety, Protection, and Modification of the Product has been changed
1.1, 1.2, 1.4, 2.17, 2.20, 5.2, Chapter 8	DNP3 slave function has been added
Chapter 10	Added the new description

Oct. 2013/3rd Edition/R3.02.10 or later

All	Term integration "General Specifications (GS)" "Installation" "Domain Controller"
Introduction	Changed the description of station types
1.5	Added the description of Operation of SCS Maintenance Support Tool
2.4	Changed and added the description of FB and FU
2.2, 5.2	Changed the name of setting item for SCS Constants Builder
2.23	Supported Vnet/IP-Upstream
3.1, 5.1	Supported the database repairing function of the Database Validity Check Tool
6.1	Added the precautions
Chapter 9	Added the new description

Dec. 2012/2nd Edition/R3.02.00 or later

All	Changed descriptions to use the term "SCS State Management window" consistently.
2.3	Added information on Ethernet communication modules.
2.17	Added description of the response timeout period setting on the Modbus master.
2.20	Added information on a new item of builder definitions.
3.2	Added "Precautions for Using the Function Code 06 in Modbus Slave Communication."
5.2	Added a new item of SCS Constants Builder that is changeable online.
Appendix	Added new terms.

Aug. 2011/1st Edition/R3.01 or later*

Newly published

■ For Questions and More Information

Online Query: A query form is available on the following URL for online query.

<http://www.yokogawa.com/iss>

■ Written by Yokogawa Electric Corporation

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