
**User's
Manual**

Safety Manual



IM 32S01S10-21E

vigilantplant.®

Introduction

This document presents the safety requirements for building a safety system with ProSafe-RS. Safety applications that meet the requirements of SIL 3 of the IEC 61508 standard can be realized by following these requirements.

The ProSafe-RS has been certified by TÜV Industrie Service GmbH Business Sector ASI (<http://tuvasi.com/>), TÜV Rheinland Group to fulfill the requirements of SIL 3 of the IEC 61508. The contents of this safety manual have also been approved by TÜV.

For the proper use of ProSafe-RS, also refer to the user's manuals available on our Website (<http://www.yokogawa.com/iss/>).

This document consists of the following chapters.

1. Safety Lifecycle
This chapter explains an overview of the safety conditions for building a safety instrumented system.
2. System Considerations
This chapter explains details of the safety considerations for building a safety instrumented system with the ProSafe-RS.

■ Abbreviations

The following table lists the abbreviations used in this safety manual.

Table Abbreviations

Abbreviation	Definition	Remarks
AI	Analog Input	
AO	Analog Output	
CENTUM	Denotes CENTUM VP and CS 3000 R3, the Integrated Production Control System of Yokogawa.	
CPU	Central Processing Unit	
DI	Digital Input	
DO	Digital Output	
ENG	Engineering Personal Computer	Device of CENTUM
FB	Function Block	Element used in FBD/LD/ST
FBD	Function Block Diagram	IEC 61131-3 language
FCS	Field Control Station	Device of CENTUM
FU	Function	Element used in FBD/LD/ST
HIS	Human Interface Station	Device of CENTUM
I/O	Input/Output	
LD	Ladder Diagram	IEC 61131-3 language
PFD	Probability of Failure on Demand	Defined by IEC 61508
SCS	Safety Control Station	Device of ProSafe-RS system
SENG	Safety Engineering Personal Computer	Device of ProSafe-RS system
SIL	Safety Integrity Level	Defined by IEC 61508
ST	Structured Text	IEC 61131-3 language

ProSafe-RS Document Map

Safety System

Safety Manual

IM 32S01S10-21E

**Engineering
Guide**

IM 32S01C10-21E

Software

**Safety Control Station
Reference**

IM 32S03B10-21E

**Integration with
CENTUM VP/CS 3000**

IM 32S01E10-21E

Open Interfaces

IM 32S05B10-21E

**Engineering
Reference**

IM 32S04B10-21E

**Utilities and
Maintenance
Reference**

IM 32S04B20-21E

Messages

IM 32S02B10-21E

**ProSafe-RS
System Test
Reference**

IM 32S04B30-21E

**Integration with
FAST/TOOLS**

IM 32S56H20-21E

Workbench User's Guide

Hardware

**Safety Control
Stations
(Hardware)**

IM 32S06C10-21E

**Communication
Devices**

IM 32S06H10-21E

Vnet/IP




**ProSafe-RS
Vnet/IP**

IM 32S56H10-21E

Installation

Installation

IM 32S01C50-21E

-  Manual
-  Software Help
-  Read Me First

Safety Precautions

■ Safety, Protection, and Modification of the Product

- In order to protect system controlled by this product, the product itself and ensure safe operation, observe the safety precautions described in this user's manual. We assume no liability for safety if users fail to observe these instructions when operating the product.
- You must use this product according to the instructions described in user manuals. If not, protective functions of this product may not work as expected.
- If any protection or safety circuit is required for system controlled by the product or for the product itself, prepare it separately.
- Be sure to use the parts approved by Yokogawa Electric Corporation (hereafter simply referred to as YOKOGAWA) when replacing parts or consumables.
- Modification of the product is strictly prohibited.
- The following symbols are used on the product and in this user manual to indicate that safety precautions are required:



Indicates that user must take caution. The symbol on the equipment refers the user to the relevant manual to avoid potentially hazardous situations that may result in injury or death. The symbol appears next to the cautionary information in user manuals required to avoid harm to personnel and to the equipment.



Indicates a protective grounding terminal. Before using the product, ground the terminal.



Indicates a functional grounding terminal. Before using the product, ground the terminal.



Indicates an AC supply.



Indicates a DC supply.



Indicates that main switch is ON.



Indicates that main switch is OFF.

■ Notes on Handling User Manuals

- Please hand over user manuals to your end users so that they can have them on hand for convenient reference.
- Please read the user manuals thoroughly before using the product.
- The purpose of these user manuals is not to warrant that the product is well suited to any particular purpose but rather to describe the functional details of the product.
- YOKOGAWA reserves the right to make improvements in the user manuals and product at any time, without notice or obligation.
- If you have any questions, or you find mistakes or omissions in the user manuals, please contact our sales representative or your local distributor.

■ Warning and Disclaimer

The product is provided on an “as is” basis. YOKOGAWA shall have neither liability nor responsibility to any person or entity with respect to any direct or indirect loss or damage arising from using the product or any defect of the product that YOKOGAWA can not predict in advance.

■ Notes on Software

- YOKOGAWA makes no warranties, either expressed or implied, with respect to the software’s merchantability or suitability for any particular purpose, except as specified in the terms of warranty.
- This software may be used on one machine only. If you need to use the software on another machine, you must purchase another copy of the software.
- It is strictly prohibited to reproduce the product except for the purpose of backup.
- Store the CD-ROM (the original medium) in a safe place.
- It is strictly prohibited to perform any reverse-engineering operation, such as reverse compilation or reverse assembling on the product.
- No part of the product may be transferred, converted or sublet for use by any third party, without prior written consent from YOKOGAWA.

Documentation Conventions

■ Typographical Conventions

The following typographical conventions are used throughout the user manuals:

● Commonly used Conventions throughout User manuals:

Character strings in the following font and style:

Indicate that user must enter them in the relevant field or text box in the context.

Example:

```
FIC100.SV=50.0
```

“Δ” Mark:

Indicates a space between character strings that must be entered.

Example: Calling the tuning view with the tag name of S0001 on HIS (Human Interface Station of the integrated CENTUM).

```
S0001ΔTUN
```

Character string enclosed by brackets ({ }):

Indicates an option that can be omitted.

Example: Parameters for calling the tuning view on HIS.

```
Tag name ΔTUN {Δ-window size} {Δ=Display position}
```

● Conventions used to show Key or Button Operations:

Characters enclosed by square brackets ([]):

Characters enclosed by square brackets within any description of a key or button operation, indicate either a key on the keyboard, a button name on a window, or an item displayed on a window.

Example:

```
Click the [OK] button.
```

● Conventions of User Defined Folder

User-Defined Folder Name

If the path of a folder can be defined by users, it is written within parentheses.

Example: (RS Project Folder) \SCS0101

If the RS Project Folder is C:\MYRSPJT, the above path becomes: C:\MYRSPJT\SCS0101

■ Symbol Marks

Throughout this user manual, you will find that several types of symbols are used to identify different sections of text. This section describes these icons.



CAUTION:

Indicates instructions that must be observed in order to prevent physical injury and death of operator.



WARNING:

Indicates instructions that must be observed in order to prevent software or hardware from being damaged or system from becoming faulty.



IMPORTANT:

Indicates important information required to understand operations or functions.

TIP:

Indicates additional information.

SEE ALSO :

Indicates a source to be referred to.

Clicking a reference displayed in green can call up its source, while clicking a reference displayed in black cannot.

■ Drawing Conventions

Some drawings in the user manual may be partially emphasized, simplified, or omitted, for the convenience of description.

Note that screen images in user manuals may be slightly different from the actual ones (for example, display positions and case differences), and some show only example images.

■ 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."

For the same features of CENTUM VP and CENTUM CS 3000 that have different feature names, the name used in CENTUM VP will be referred to in the explanations. (For example, CENTUM CS 3000 System Alarm Window and CENTUM VP System Alarm View have the same functions, but only System Alarm View will be referred to when explaining this feature.) Nevertheless, if there is any difference in functionality according to whether ProSafe-RS is integrated with CENTUM VP or CENTUM CS 3000, the feature will be explained separately for both cases.

SEE ALSO

- For information about the functions and usage of CENTUM VP components, see CENTUM VP User's Manuals (IM) and related Technical Information (TI) and General Specifications (GS).
 - For information about the functions and usage of CENTUM CS 3000 components, see CENTUM CS 3000 User's Manuals (IM) and related Technical Information (TI) and General Specifications (GS).
-

Copyright and Trademark Notices

■ All Rights Reserved

The copyright of the programs and online manuals contained in the DVD-ROM or CD-ROM shall remain in Yokogawa.

You are allowed to print out the required pages of the online manuals for using the product, however, you are not allowed to print out the entire document.

Except as stated above, no part of the online manual may be reproduced, either in electronic or written form, registered, recorded, transferred, sold or distributed (in any manner including without limitation, in the forms of paper documents, electronic media, films or transmission via the network).

■ Trademark Acknowledgments

- CENTUM, ProSafe, Vnet/IP and STARDOM are registered trademarks of YOKOGAWA.
- Microsoft, Windows, Windows Vista, Visual Basic, Visual C++ and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Adobe, Acrobat and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.
- Ethernet is a registered trademark of XEROX Corporation.
- Modicon and Modbus are registered trademarks of Schneider Electric SA.
- PLC is a registered trademark of Rockwell Automation, Inc.
- HART is a registered trademark of the HART Communication Foundation.
- All other company and product names mentioned in this user's manual are trademarks or registered trademarks of their respective companies.
- We do not use TM or ® mark to indicate those trademarks or registered trademarks used in this user's manual.

ProSafe-RS Safety Manual

IM 32S01S10-21E 2nd Edition

CONTENTS

1.	Safety Lifecycle	1-1
2.	System Considerations	2-1
2.1	Overview of ProSafe-RS.....	2-1
2.2	Hardware Configuration.....	2-2
2.3	Application Development	2-6
2.4	Security	2-9
2.5	On-line Change	2-10
2.6	Forcing	2-11
2.7	Maintenance Override	2-12
2.8	Replacement of Modules in SCS.....	2-13
Appendix A	Product Support.....	App.A-1

1. Safety Lifecycle

The IEC 61508 requires the use of its safety lifecycle for configuring and maintaining safety systems properly. This chapter explains the overview of the safety lifecycle.

■ Overview of the Safety Lifecycle

The safety lifecycle, which consists of sixteen phases that start at the concept phase of a system and end at the systems usage expiration, defines necessary activities for these phases. As the safety lifecycle is considered as a framework to minimize the systematic failure caused by human errors, persons involved in the implementation of the safety functions need to understand the requirements of the safety lifecycle well and follow them.

As part of the safety lifecycle, the three planning phases for operation and maintenance, safety validation, and installation and commissioning are required prior to actual implementation phases. This is because adequate preparations that include the procedures and measures derived from the impact analysis are important to ensure functional safety and/or to prevent an unsafe state during the implementation.

The standard also requires that the functional safety management runs in parallel with the safety lifecycle phases with emphasis on the importance of the documentation. The information about all activities and the results of each phase need to be documented in such way that the descriptions are accurate and easy to understand for users. The document of one phase is used as an input of the subsequent phase of the safety lifecycle in principle. This makes it possible to maintain the consistency of the lifecycle and trace the activities afterward.

Another requirement of the functional safety management is to manage competence. The organizations and/or persons involved in the safety lifecycle must be competent for their activities that they have responsibilities for. Adequate experience and training are necessary for this purpose.

This safety manual provides information for all planning phases of the safety lifecycle to ensure the correct use of ProSafe-RS to reach the aimed safety integrity by the end user.

2. System Considerations

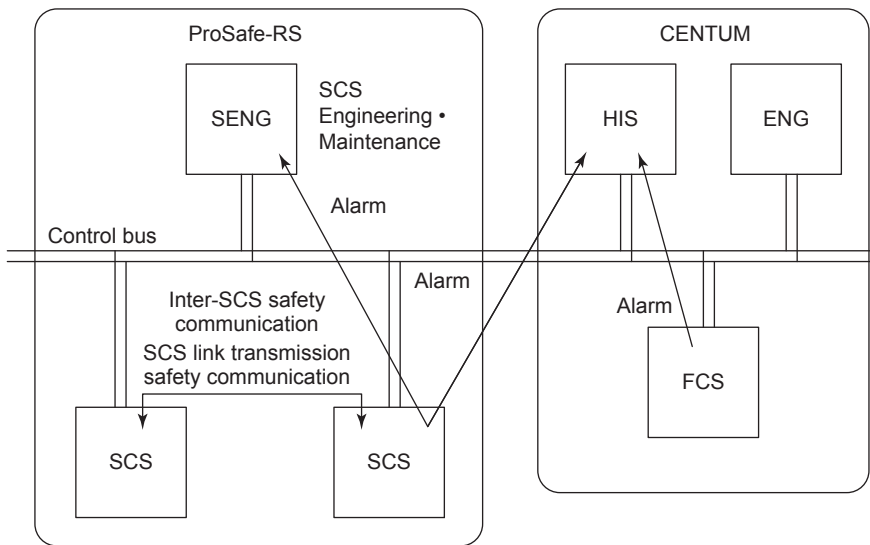
This chapter provides details of the safety considerations for building the safety system with the ProSafe-RS.

2.1 Overview of ProSafe-RS

This section explains the overview of ProSafe-RS.

■ Overview of ProSafe-RS

ProSafe-RS is a safety system consisting of a safety controller, SCS, and a engineering and maintenance PC, SENG. The minimum configuration includes one SCS and one SENG.



020101E.ai

Figure Example of System Configuration

An SCS in which both CPU and I/O modules are in single configuration can be used for applications that meet the requirements of SIL 3 of the IEC 61508. To increase the system availability, CPU modules and/or I/O modules can be duplexed (dual-redundant).

Inter-SCS safety communication and SCS link transmission safety communication allow a safety loop that meets the requirements of SIL 3 to be built between different SCSs connected via the control bus.

The ProSafe-RS can be integrated seamlessly into a CENTUM VP or CS 3000 (hereafter, referred to as "CENTUM") system connected on the same control bus. This allows operators to monitor the SCSs through the HIS.

■ Safety Application

ProSafe-RS is primarily intended to be used for the following safety applications. The use of ProSafe-RS conforming to the standards for each application is also certified by TÜV.

For the details of the requirements, refer to each standard.

- ESD (Emergency Shutdown System) / PSD (Process Shutdown System)
- F&G (Fire and Gas detection System: EN 54, NFPA 72)
- BMS (Burner Management System: EN 298, NFPA 85, EN 50156)

2.2 Hardware Configuration

This section explains the hardware structure.

■ Safety Requirement and System Availability

An SCS in which both CPU and I/O modules are in single configuration can be used for applications that meet the SIL 3 requirements. For the models and revisions of each module, refer to our Website (<http://www.yokogawa.com/iss/>).

To increase the availability, CPU modules and/or I/O modules can be duplexed (dual-redundant). When a fault is detected in one module in a dual-redundant configuration, the other module takes over control to continue operation.

■ SCS Hardware

● SCS Basic Components

The basic components of the SCS hardware include the following.

- Safety Control Unit
 - CPU Module
 - Power Supply Module (dual-redundant)
 - ESB BUS Coupler Module (dual-redundant)
 - Control Bus Interface (dual-redundant)
- Node Unit
 - Power Supply Module (dual-redundant)
 - ESB Bus Interface Slave Module (dual-redundant)

● I/O Modules

The following table lists the I/O modules used for the ProSafe-RS system.

Use safety I/O modules for safety loops.

Table Safety I/O Module List

Digital Input Module (24 V DC)
Digital Output Module (24 V DC)
Digital Output Module (100-120 V AC)
Analog Input Module (4-20 mA)
Analog Input Module (1-5 V/1-10 V)
Analog Output Module (4-20 mA)
Serial Communication Module (RS-232C) (*1)
Serial Communication Module (RS-422/RS-485) (*1)

*1: Interference free

● Environmental Requirements

Refer to ProSafe-RS Installation Guidance (TI 32S01J10-01E, TI 32S51J10-01E) for details of the permissible environmental conditions for ProSafe-RS, and its connection with external devices.

■ Fault Detection and Reaction

● Basic Behaviour

CPU modules and I/O modules are diagnosed by the hardware and software periodically. Errors in communication between CPU module and I/O modules and in inter-SCS safety communications are detected by various measures.

When an error is detected, the failsafe value is used for the output value and a diagnostic information message is issued. The diagnostic information message, which is sent to the SENG and HIS (when integrated with CENTUM) via the control bus, is useful for identifying the details and the cause of the error.

In a dual-redundant configuration, the other module that is working normally takes over control to continue the operation. The diagnostic information message that is issued at the same time helps identify the failed module.

The user can define the fail-safe behavior of the system when faults are detected in I/O modules. The following section describes the details.

● Diagnosis and Reaction

This section explains the fault detection and reaction of the system in the single configuration.

In a dual-redundant configuration, the other module that is working normally takes over control to continue the operation.

- CPU Module
The major components in the CPU module are duplexed, and their operation results are always compared between the two. This enables to detect a fault in a very short time. The detection of a fault causes a shutdown of the CPU module. Accordingly, the output modules detect a communication halt of the CPU module and outputs the failsafe value predefined for each channel.
- Input Module
Diagnostic tests of input modules are performed by the firmware periodically. When one of the following faults is detected, the status of input channel changes to “bad” and a predefined value (input value of error occurrence) is transferred to the application logic. This means, faults in input modules, as well as demands (changes in input values), can be handled by application logic.
 - Fault in the common part of an input module
 - Fault in an input channel
 - Failure in communication between an input module and a CPU module
- Output Module
Diagnostic tests of output modules are performed by the firmware periodically. When one of the following faults is detected, the Output Shutoff Switch is activated to force all the output channels to OFF (0).
 - Fault in the common part of an output module
 - Stuck-at-ON, the case where the output cannot be turned to OFF (digital output module (24 V DC))
(In the case of digital output module (100-120 V AC), only the fault-detected channel is turned to OFF.)
 - Output current read back error (analog output module)

In case of a communication fault between an output module and a CPU module or channel faults other than the above, the failsafe value for each channel is output.

- **Diagnosis of Field Wiring**
A diagnostic function is provided to detect open and short circuits in wiring between field devices and I/O modules.
The behavior after detection of such a fault is the same as the case of a fault in the channel of the I/O modules.

For this diagnosis with a DI module, connect a dedicated diagnostic adaptor with the wiring close to the field device. The diagnostic adaptors are available for “Normally Energized” and for “Normally De-energized” respectively.
- **Inter-SCS Safety Communication and SCS Link Transmission Safety Communication**
The receiver side of SCS can detect failures caused by faults in the SCSs and the relay devices on the communication path.
When a failure in inter-SCS safety communication and/or SCS link transmission safety communication is detected, the predefined value is transferred to the application logic in the receiver side of SCS. This is implemented by the dedicated FBs for inter-SCS safety communication and SCS link transmission safety communication respectively.

■ System Timing

● System Reaction Time

The system reaction time of SCS includes the reaction time for the external demand and the reaction time when a fault is detected in the SCS. For more details, refer to Engineering Guide (IM 32S01C10-21E).

● Process Safety Time

The process safety time is the period from the time of fault occurrence in the process until the time process enters a dangerous state. The safety system needs to transfer the process to a safe state within the process safety time after the demand (process error).

The reaction time of the safety system, which is the total of the reaction time of the sensor, actuator, and safety controller, needs to be shorter than the process safety time. Consider the system reaction time of SCS as the reaction time of the safety controller.

■ PFD Calculation

The ProSafe-RS has been designed to meet the requirements for PFD of SIL 3 that are defined as a fraction of 10^{-4} to 10^{-3} in the IEC 61508, with the condition that the interval between proof tests is ten years. For further information on this, refer to Engineering Guide (IM 32S01C10-21E).

■ Check List for Hardware Engineering

Table Check List for Hardware Engineering

No.	Description	Check
1	Have the modules for safety and the ones for non-safety been used appropriately?	
2	Have the devices and wiring been installed according to ProSafe-RS Installation Guidance (TI 32S01J10-01E, TI 32S51J10-01E) ?	
3	Has the mechanism of the fault detection and reaction been understood?	
4	For diagnosis of the field wiring of DI modules, have the dedicated adaptors for wiring diagnostics been connected?	
5	Has the system reaction time and the process safety time been understood?	

SEE ALSO For each No. of the check list, see the following:

“■ SCS Hardware”

2.3 Application Development

This section explains about the application development.

■ Parameter Settings

To ensure normal operation of the system, you should select the appropriate parameters by using the engineering function.

● Scan Period

A safety application runs at intervals of a defined scan period.

Determine a scan period to meet the requirements for the process safety time.

● Input Value for a Fault and Failsafe Value

Define the input value to the application logic when a fault in an input module is detected (input value for a fault) and the output value from an output module when a fault in the communication between CPU and output module is detected (Failsafe value). These can be individually defined on each channel.

These values, that determine the safety state, should be cautiously defined depending on the application. In general, 0 for De-energize to trip system and 1 for Energize to trip system is used. If different values are used, the immediate repair after a failure occurs should be considered.

● Activation of Output Shutoff Switch

The Output Shutoff Switch in the output module is a common switch to all channels and normally closed. The switch is activated to shut off all channels of the output module when a stuck-at-ON fault that the channel can not output OFF (0) for a digital output module (24 V DC) or an output current read back error for an analog output module is detected by the diagnostic test, if the setting of the channel is the default value.

The behavior of the Output Shutoff Switch is definable per channel. Select the default value to all channels for a safety application, which activates the switch when the fault mentioned above is detected in a channel.

● Diagnostics of Field Wiring

Define whether to perform diagnostic tests of field wiring of a digital I/O module for each channel.

● Timeout Settings for Inter-SCS Safety Communication and SCS Link Transmission Safety Communication

Set the proper timeout values for the inter-SCS safety communication dedicated FB and SCS link transmission safety communication parameter.

For calculation of the timeout values, refer to Engineering Guide (IM 32S01C10-21E).

■ Programming

The engineering function of the ProSafe-RS provides the programming languages conforming to the IEC 61131-3 standard. The following languages are used to program safety application logic.

- FBD (Function Block Diagram)
- LD (Ladder Diagram)
- ST (Structured Text)

Use proper FU/FB, LD elements, and ST statements of these languages. Some of them can be used for safety applications, but the others cannot, which is shown in Engineering Guide (IM 32S01C10-21E).

■ Application Test

After programming an application, you need to verify if it operates according to the specifications.

- After programming the application, save it, print it out using the Self-Documentation Function, and check that the inputs of programming and the contents of the printout match.
- Use the Integrity Analyzer to check whether the FU/FB, etc. used for programming the safety application are applicable to safety use. Confirm that the result is as intended.
- The simulator on SENG can test the application for debugging, without the need of the actual SCS.
- Testing the safety application logic can be done with the Target Test Function on the target SCS even when no I/O modules are installed in the SCS or when no field devices are connected.
- You should perform the final test on the target system with the necessary devices installed.
- When loading the application into SCS, make sure that the correct application has been loaded with the version information shown on the SENG.
- When starting the operation after completion of the test at the security level 0, perform the off-line download and change the security level to Level 2.

When a part of the application is modified, the impact of the modification needs to be analyzed before a test. Unintended result of the modification can be detected with the Cross Reference Analyzer before the test. This helps identify the part to be tested, so that only the modified part needs to be tested. The procedure is as follows:

- After modifying the application using the engineering tool, print it out and make sure that the inputs of programming and the contents of the printout match.
- Make sure that the check results by the Cross Reference Analyzer are as intended.
- Check the operation of the application with the SCS simulator, if necessary, then validate it on the target SCS.

To modify the application correctly, the modification history of the current application needs to be managed. For this purpose, the version control function is provided.

■ Check List for Application Development

● Parameter Settings and Programming

Table Check List for Parameter Settings and Programming

No.	Description	Check
1	Has the scan period been determined to meet the requirements for the process safety time?	
2	Has the Output Shutoff Switch of the output module been selected to be activated?	
3	Have the input values for faults and failsafe values been determined?	
4	For inter-SCS safety communication and SCS link transmission safety communication, has the application logic been written with the dedicated FB?	
5	For inter-SCS safety communication and SCS link transmission safety communication, have the proper timeout values been set?	
6	Has the application logic been written with the proper language or language element?	

● Procedure for Application Test

The following check list shows the procedure after application input. When an error is found at a step, go back to a proper step, the application input step in principle.

Table Check List for Procedure for Application Test

No.	Description	Check
1	Save the application on SENG, print it out with the Self-Documentation Function, and compare the inputs with the printout.	
2	Use the Integrity Analyzer and check the results.	
3	Use the Cross Reference Analyzer and check the results.	
4	Use simulator on the SENG for debugging.	
5	Download the application into SCS.	
6	Test the application on target.	

2.4 Security

To prevent accesses from unauthorized users or devices during the operation and unintended changes due to user's operation errors, consider the security mentioned in this section.

■ SCS Security Level

The SCS controls the security levels for the safe operation of the system.

Set the security level to Level 2 during the normal operation of SCS to protect the SCS against illegal access. It needs to be set to Level 1 for maintenance, and to Level 0 for off-line operation. To prevent erroneous changes of the security level, password authorization is required.

Assign different passwords for authorization to individual security levels and SCSs. Check that the security level on the display of SENG is correct when changing the security level.

■ Access to SCS

Changing the security level enables SCS to be accessed. To prevent erroneous access to SCS, correct operation on SENG is needed. For this purpose, SENG is provided with the display of the system alarms and SCS status to indicate which part of SCS is to be accessed. When accessing SCS, use these functions to ensure the correct access for its safe operation.

■ Access Control on SENG

The safety application stored in SENG is protected with a password, so that only authorized users are allowed to operate and modify it. The passwords for operating the safety application need to be different for each SCS.

■ Check List for Security

Table Check List for Security

No.	Description	Check
1	Is the usage of the SCS Security Levels understood?	
2	Have different passwords for changing SCS Security Levels been assigned to individual security levels and individual SCSs?	
3	Has the Security Level of the SCS in operation been set to Level 2?	
4	Have you confirmed that the settings and the state of SCS are the same as you intended?	
5	Have different passwords for operating safety application on the SENG been assigned to individual SCSs?	

2.5 On-line Change

ProSafe-RS allows both the application to be modified and the I/O module settings to be changed on-line. Before On-line Change, analyze its impact on the system, provide external measures when necessary or appropriate, and then execute it with much caution.

■ On-line Change Consideration

After modifying the application and completing the check, you need to perform On-line Change Download and test the modified part. Before On-line Change Download, change the SCS Security Level to Level 1, and return it to Level 2 after completion of the test.

To prevent a system error, On-line Change Download must not be performed while maintenance override operation by HIS is going on.

If the modified application contains any unintended changes, On-line Change can lead to unexpected system behavior. To prevent adverse influence on the parts outside of SCS caused by the unexpected behavior, use the Forcing Function as necessary, and also provide appropriate measures outside of SCS to deal with emergency situations in advance.

**SEE
ALSO**

For the detailed procedure for On-line Change, refer to Engineering Guide (IM 32S01C10-21E)

■ Check List for On-line Change

Table Check List for On-line Change

No.	Description	Check
1	Has the plan of modification been reviewed and approved?	
2	Does the modification need to be done on-line?	
3	Has the impact of the on-line change on the system been analyzed and the results fully understood?	
4	Are the Integrity Analyzer and Cross Reference Analyzer used for change verification?	
5	Has the Forcing Function or Fixing All Output Function been taken into account?	
6	Have the adequate measures for an emergency situation been prepared outside SCS?	
7	Has the procedure for the on-line change been clearly established?	

2.6 Forcing

This section explains the consideration at the time of performing the Forcing Function.

■ Forcing Function

The forcing function of the SENG is for locking and forcing the values on I/O channels and the variables used in the application logic.

To start the forcing function, change the SCS Security Level to Level 1.

When operating from the SENG, make sure that the correct variables are locked.

To return to the normal operation, unlock all the I/O channels and variables, and change the SCS Security Level to Level 2.

Using the dedicated FB helps management of the forcing condition, such as the number of locked variables and forced unlocking of locked variables.

Before performing the forcing function, which is used for maintenance of devices and for On-line Change, analyze the impact on the system and take adequate measures beforehand.

■ Check List for Forcing

Table Check List for Forcing

No.	Description	Check
1	Has the impact of the forcing on the system been analyzed and the results fully understood?	
2	Has the use of the dedicated FB for managing the forcing condition been taken into account?	
3	Has the procedure for forcing been clearly established?	
4	Does the procedure include the instruction that all the variables must be unlocked and backed to normal after the end of forcing?	
5	Have the adequate measures for emergency situations been prepared outside SCS?	

2.7 Maintenance Override

This section explains the consideration at the time of performing the maintenance override.

■ Maintenance Override

The maintenance override, which is used for device maintenance, assigns a predefined value or state to an I/O variable.

For a maintenance override from the HIS in a CENTUM-integrated system, build the safety application logic beforehand, using the dedicated FB for maintenance overrides.

The maintenance override operation has two steps: the authorization command and the execution command of the override. After completion of maintenance, clear the maintenance override.

Perform a series of operations from the HIS by operator's confirming the contents and the message on the display.

■ Check List for Maintenance Override

Table Check List for Maintenance Override

No.	Description	Check
1	Has the effect of the maintenance override been analyzed and the results fully understood?	
2	Has the application logic been written with the dedicated FB for the maintenance override?	
3	Has the operation manual been prepared and confirmed by the operators?	
4	Does the operation manual include the instruction that all overrides must be removed at the completion of the maintenance?	
5	Has an alternative method for removing overrides been prepared?	
6	Have adequate measures for emergency situations been prepared outside SCS?	

2.8 Replacement of Modules in SCS

This section explains the consideration at the time of replacement of modules.

■ Replacement of Modules

When a module failure occurs, identify the failed location in SCS using the LED display of modules or the diagnostic information of the SENG to replace the relevant module.

After replacing the CPU module in a single configuration, perform Master Database Off-line Download and ensure the correct application has been downloaded.

In case a module failure does not lead to a shutdown in a single configuration, the replacement of the module should take place within Mean Time To Repair (MTTR).

Even in case of a failure in one module of a duplex configuration, the SIL 3 is guaranteed. The failed module can be replaced while the SCS is in operation.

■ Check List for Replacement of Modules

Table Check List for Replacement of Modules

No.	Description	Check
1	Has the diagnostic information of the SENG been confirmed?	
2	Is the LED display of the relevant module showing the failure?	
3	Is the procedure of replacing the module understood correctly?	
4	After replacing a CPU module, has the application been confirmed correct (in the single configuration)?	
5	Has Master Database Off-line Download been performed to load the correct application if necessary?	

Appendix A Product Support

Please contact our offices listed below for the technical support of the ProSafe-RS system.

Yokogawa Electric Corporation
Process Automation Product Marketing Dept.
Industrial Automation Systems Business Div.
2-9-32 Nakacho, Musashino-Shi, Tokyo
180-8750 Japan
Tel.: +81 422 52 5552
Fax: +81 422 52 9802
E-mail: 200502prosafe_com@yg.jp.yokogawa.com

Yokogawa System Center Europe B.V.
Lange Amerikaweg 55, 7332 BP Apeldoorn
P.O. Box 20020, 7302 HA Apeldoorn
The Netherlands
Tel.: +31 (0) 55 5389 500
Fax: +31 (0) 55 5389 511
E-mail: info@nl.yokogawa.com

Yokogawa Engineering Asia Pte Ltd
Safety Excellence Center
5 Bedok South Road
Singapore 469270
Tel.: +65 6241 9933
Fax: +65 6241 2606
E-mail: prosafe@sg.yokogawa.com

Revision Information

- Title : Safety Manual
- Manual No. : IM 32S01S10-21E

Dec.2008/2nd Edition/R2.02 or later*

* : Denotes the release number of the software corresponding to the contents of this user's manual. The revised contents are valid until the next edition is issued.

Overall "CS 3000" was changed to "CENTUM," which refers to both CENTUM VP and CS 3000.

2.1 Standards NFPA8501, NFPA8502 were changed to NFPA85.

2.2 Descriptions of the digital output module (100-120 V AC) were added.
Description in "● System Reaction Time" was modified.

2.3 Description in "● Activation of Output Shutoff Switch" was modified.

2.5 Description in "■ On-line Change Consideration" was modified.

Appendix A Phone numbers and e-mail address for Yokogawa Electric Corporation were changed.

May 2008/1st Edition/R2.01 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/>

If you want more information about Yokogawa products, you can visit

Yokogawa's homepage at the following web site.

Homepage: <http://www.yokogawa.com/>

- Written by Process Automation Product Marketing Dept.
Industrial Automation Systems Business Div.
Yokogawa Electric Corporation

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