Technical Information

TI 32P01A10-01EN

Safety Instrumented System ProSafe-RS System Overview

[Release 4]

YOKOGAWA

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

4th Edition Nov. 2024 (YK)

Introduction

ProSafe-RS is a safety instrumented system conforming to IEC 61508. This technical information (TI) document introduces various features and functions of the ProSafe-RS.

■ Document Structure

An overview of the ProSafe-RS system is described in this TI. After reading this TI, go over to read other documents such as General Specifications (GS) or Instruction Manuals (IM) for more details.

This TI consists of five chapters. Chapter 1 discuss about the importance of safety instrumented system, while the remaining chapters will explain the features of ProSafe-RS, system configuration, safety control station, engineering, operation and maintenance.

■ Reference Documents

Refer to the following document for a system integrated with CENTUM VP.

- Integrated Production Control System CENTUM VP System Overview (General Overview) (TI 33J01A10-01EN)

■ Target Readership

- Managers who are considering introduction of a new safety instrumented system.
- Instrumentation, power and computer engineers who evaluate for purchasing or installation of ProSafe-RS.

■ Representation of Drawings

- Drawings in this TI may be emphasized, simplified, or omitted some features for convenience of explanations.
- The screen captures may be slightly modified for the convenience of the better understanding without disturbing the functional understanding or operation and monitoring.

Trademark

■ Trademark Acknowledgment

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

Safety Instrumented System
ProSafe-RS
System Overview

TI 32P01A10-01EN 4th Edition

CONTENTS

1. Necessity of Safety Instrumented System

In this chapter, a plant owner's responsibility, the international standards, positioning of a safety instrumented system and safety evaluation scales are explained.

Plant owner's responsibility

During 1970s and 1980s, serious incidents that occurred at petroleum and chemical plants initiated several countries to legislate that "owners of industrial plants where dangerous materials are handled must evaluate possible risks that may occur in the plants."

These legal regulations stipulate that the plant owners are socially responsible in the entire lifecycle, from planning to disposal, to minimize the risks of causing hazards over "human beings, physical assets and environments." In order to fulfill these social responsibilities, the plant owners are expected to identify risk factors of hazardous elements that cause incidents; to analyze and evaluate them; then to reduce the risks to a socially acceptable level.

The international standards of IEC 61508 and IEC 61511 defined procedures of how to identify, analyze and evaluate risks, then implement the risk reduction measures based on legal regulations of several countries.

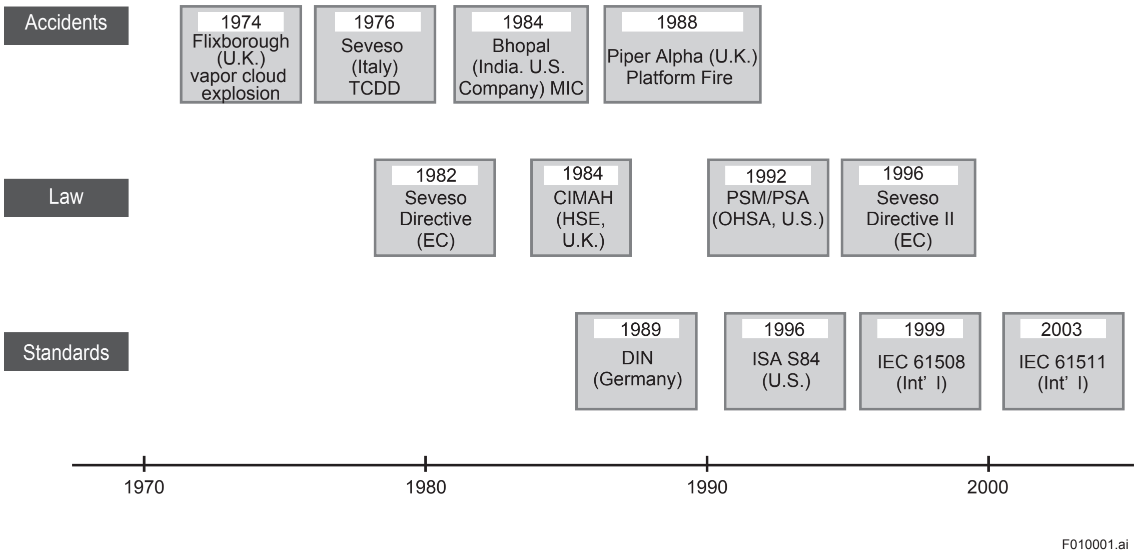

Accidents
1974 Flixborough (U.K.) vapor cloud explosion
1976 Seveso (Italy) TCDD
1984 Bhopal (India. U.S. Company) MIC
1988 Piper Alpha (U.K.) Platform Fire
Law
1982 Seveso Directive (EC)
1984 CIMAH (HSE, U.K.)
1992 PSM/PSA (OHSA, U.S.)
1996 Seveso Directive II (EC)
Standards
1989 DIN (Germany)
1996 ISA S84 (U.S.)
1999 IEC 61508 (Int' l)
2003 IEC 61511 (Int' l)
1970
1980
1990
2000
F010001.ai

Figure Flow from incidents to standardization

IEC 61508 / IEC 61511 international standards

The IEC 61508 defines the basic safety standard for functional safety for all industries. The IEC 61511 is dedicated for the process industry, in reference to the IEC 61508. These safety standards for functional safety are not established on the premise of “100% accident free,” but with some risks always remain. By converting the risks into numerical value by the globally standardized scale, the necessity and effectiveness of safety measures can be verified.

Positioning of the safety instrumented system in the viewpoint of layer of protection

A “layer of protection” approach is adopted as the basis of securing the plant safety that is to reduce risks by combining independent protection layers with the international standards of the IEC 61511, as shown below. Each protection layer has to be independent from each other, sets quantitative target for reducing risks, and establishes means of achieving these goals.
A safety instrumented system is positioned in the prevention layer for reducing the risk of hazardous event occurrence and the mitigation layer for mitigating the influence of a hazardous incident that has occurred.

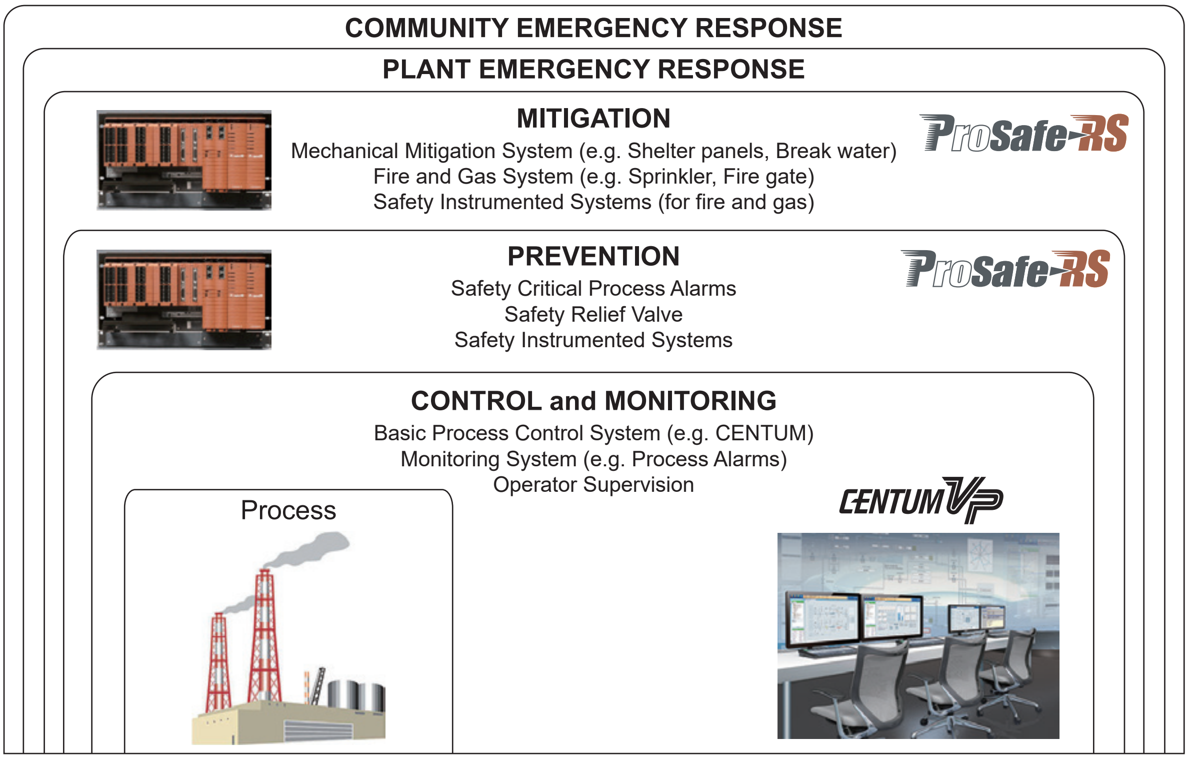
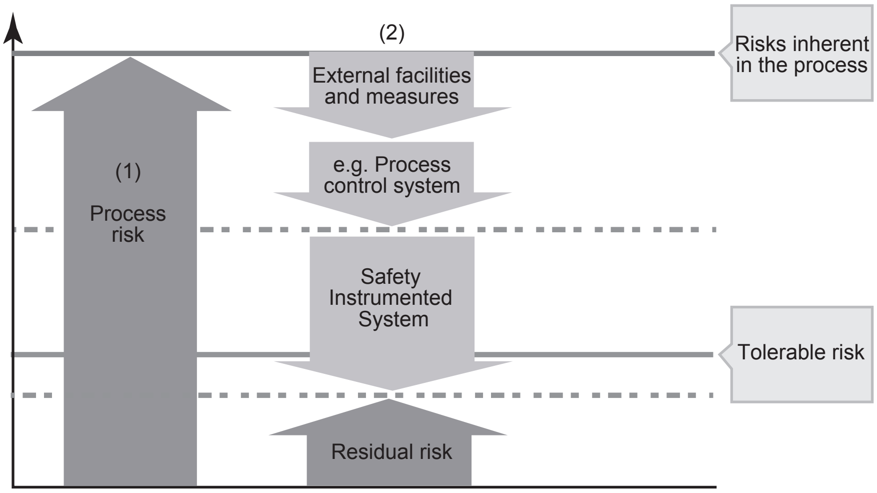

COMMUNITY EMERGENCY RESPONSE
PLANT EMERGENCY RESPONSE
MITIGATION
Mechanical Mitigation System (e.g. Shelter panels, Break water)
Fire and Gas System (e.g. Sprinkler, Fire gate)
Safety Instrumented Systems (for fire and gas)
ProSafe-RS
PREVENTION
Safety Critical Process Alarms
Safety Relief Valve
Safety Instrumented Systems
ProSafe-RS
CONTROL and MONITORING
Basic Process Control System (e.g. CENTUM)
Monitoring System (e.g. Process Alarms)
Operator Supervision
CENTUM VP
Process
F010002.ai

Figure The layer of protection

In order to work out countermeasures for risks based on the layer of protection, risk assessments to the plant must be implemented and essential risk levels inherent in the process must be calculated. (1) In order to reduce the risks to a socially permissible risk level, multiple layers of protection have to be assigned. (2) The figure below shows reducing the risks to the tolerable level by combining external mitigation facilities (e.g. shelter panels, breakwaters, etc.); a process control system (e.g. CENTUM); and a safety instrumented system for emergency shutdown (ESD).


(2)
Risks inherent in the process
External facilities and measures
(1)
Process risk
e.g. Process control system
Safety Instrumented System
Tolerable risk
Residual risk

F010003.ai

Figure The risk reduction level of the plant

Safety evaluation scales

The IEC 61508 introduces the Safety Integrity Level (SIL) as a method of describing the safety integrity requirements required at each layers of protection. The SIL is classified into four levels according to the value of average Probability of a dangerous Failure on Demand (PFDavg). The PFDavg of manual operation is 1/10 or so, which means a failure may occur out of 10 operation requests and unable to perform its safety operation.

On the other hand, enhanced self-diagnostics and fault analysis in safety instrumented systems ensure that PFDavg can be reduced to as low as possible. This means a safety instrumented system with the SIL3 guarantees to perform the operation compared with manual operations.

Table Safety integrity level (SIL)

SIL	PFDavg	Description
4	$\geq 10^{-5}$ to $<10^{-4}$	Frequency of risk occurrence is reduced to the ranges in between 1/10000 and 1/100000 under the current conditions.
3	$\geq 10^{-4}$ to $<10^{-3}$	Frequency of risk occurrence is reduced to the ranges in between 1/1000 and 1/10000 under the current conditions.
2	$\geq 10^{-3}$ to $<10^{-2}$	Frequency of risk occurrence is reduced to the ranges in between 1/100 and 1/1000 under the current conditions.
1	$\geq 10^{-2}$ to $<10^{-1}$	Frequency of risk occurrence is reduced to the ranges in between 1/10 and 1/100 under the current conditions.

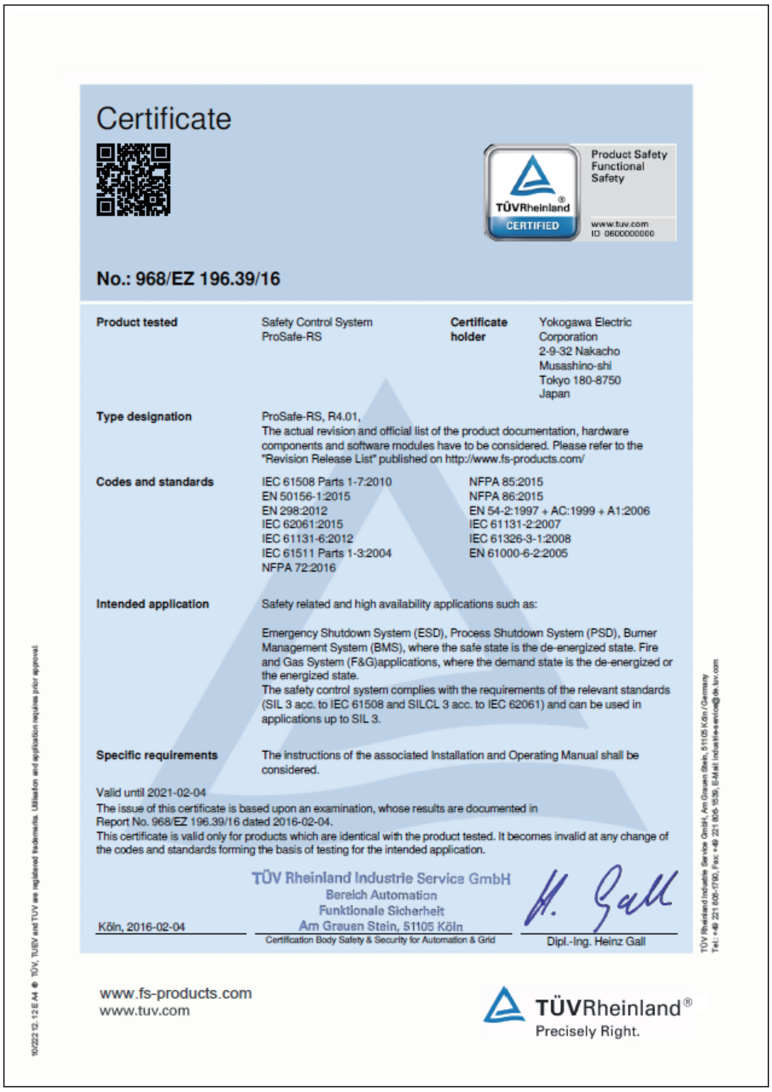
2. Features of the ProSafe-RS

This chapter describes about the features of the ProSafe-RS safety instrumented system which conforms to the Safety Integrity Level 3 (SIL3) defined by the IEC 61508.

■ Achieving SIL3 in single configuration

ProSafe-RS is a safety instrumented system which achieves the SIL3 in a single configuration and its performance is certified by TÜV Rheinland, an external certification organization.

Each of the processor and input/output modules of the ProSafe-RS contain built-in computation matching function and self-diagnostic function, which keeps the modules failure rates to extremely low. The ProSafe-RS flexibly complies with customers' requirements with its single configuration and the SIL3 certification.



Certificate

Product Safety
Functional
Safety

TÜVRheinland®
CERTIFIED

www.tuv.com
ID 0600000000

No.: 968/EZ 196.39/16

Product tested
Safety Control System
ProSafe-RS

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

Type designation
ProSafe-RS, R4.01,
The actual revision and official list of the product documentation, hardware components and software modules have to be considered. Please refer to the "Revision Release List" published on http://www.fs-products.com/

Codes and standards
IEC 61508 Parts 1-7:2010
EN 50156-1:2015
EN 298:2012
IEC 62061:2015
IEC 61131-6:2012
IEC 61511 Parts 1-3:2004
NFPA 72:2016
NFPA 85:2015
NFPA 86:2015
EN 54-2:1997 + AC:1999 + A1:2006
IEC 61131-2:2007
IEC 61326-3-1:2008
EN 61000-6-2:2005

Intended application
Safety related and high availability applications such as:

Emergency Shutdown System (ESD), Process Shutdown System (PSD), Burner Management System (BMS), where the safe state is the de-energized state. Fire and Gas System (F&G)applications, where the demand state is the de-energized or the energized state.
The safety control system complies with the requirements of the relevant standards (SIL 3 acc. to IEC 61508 and SILCL 3 acc. to IEC 62061) and can be used in applications up to SIL 3.

Specific requirements
The instructions of the associated Installation and Operating Manual shall be considered.

Valid until 2021-02-04
The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/EZ 196.39/16 dated 2016-02-04.
This certificate is valid only for products which are identical with the product tested. It becomes invalid at any change of the codes and standards forming the basis of testing for the intended application.

Köln, 2016-02-04

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln
Certification Body Safety & Security for Automation & Grid

H. Gall
Dipl.-Ing. Heinz Gall

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-1790, Fax: +49 221 806-1539, E-Mail: industrie-service@de.tuv.com

10/222 12. 12 E A4 ® TÜV, TUEV and TUV are registered trademarks. Utilisation and application requires prior approval.

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

F020001.ai

Redundancy achieves higher reliability

ProSafe-RS allows selecting dual-redundant module configurations in order to achieve higher reliability. Since the system already achieves SIL3 with a single configuration, the SIL3 is maintained even when one of the modules fails.

System integration with CENTUM VP

By integrating with the CENTUM VP system, the operation status of the ProSafe-RS are monitored on the CENTUM VP's operation and monitoring screen. ProSafe-RS and CENTUM VP synchronize time, share data, and notify event & alarm in a single step.

Segregating functions of CENTUM VP from ProSafe-RS

International safety standards require that control and safety functions are independent of each other. Even when the ProSafe-RS and the CENTUM VP systems are integrated, the control and the safety functions are securely segregated. The operation of the CENTUM VP has no influence over safety functions of the ProSafe-RS.

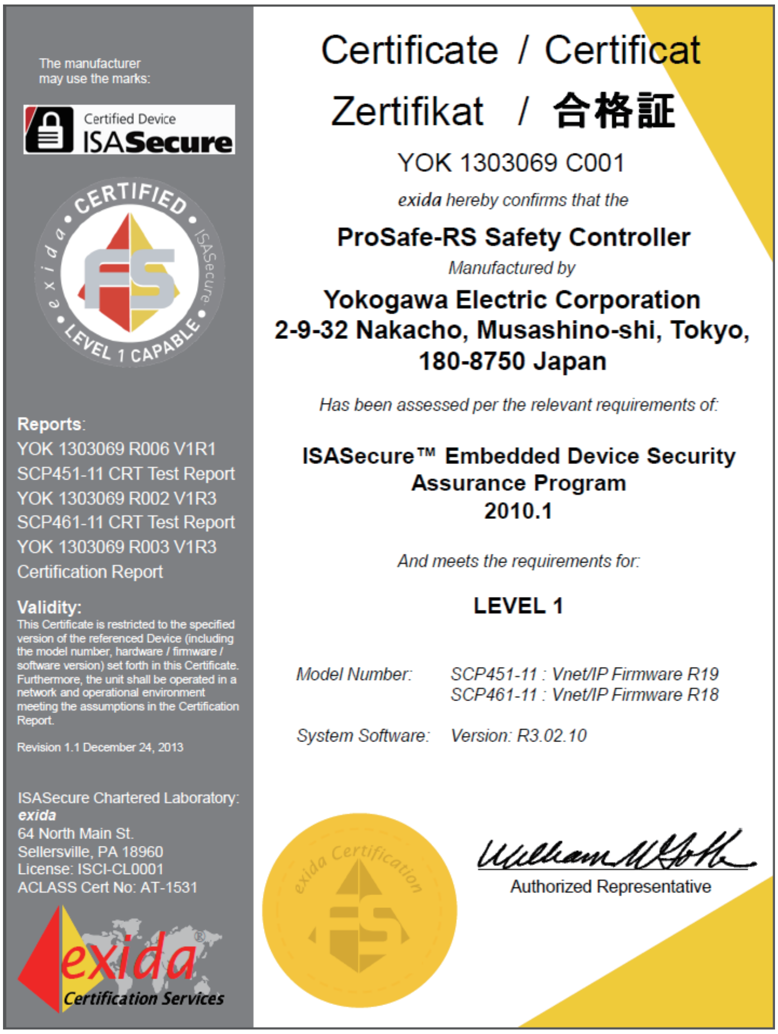
Connecting with other systems

The operating status and data of the ProSafe-RS can be referred to by a supervisory computer or Modbus master via an OPC interface (*1), or a Modbus slave communication. Furthermore, the subsystem data such as sequencers can be set or referred by the ProSafe-RS via a Modbus communication.

*1: The OPC is a way of communication among standard applications of Windows OS applied to process control. The OPC enables to send/receive process data among multiple Windows applications.

■ Security measures

The ProSafe-RS is accredited with the ISASecure Embedded Device Security Assurance (EDSA) of the ISASecurity Compliance Institute (ISCI), an international accreditation organization. The exida, an American accreditation organization certified by the ISASecure EDSA performed the Communication Robustness Test (CRT), the Fabricated Security Assessment (FSA) and the Software Development Security Assessment (SDSA). Then the ISCI evaluated and verified the conformity to the standard. The ISASecure EDSA certification certifies that the ProSafe-RS's controllers have adequate security measures against threats of cyberattacks.


CERTIFIED
exida
ISASecure
LEVEL 1 CAPABLE
FS
exida Certification

The manufacturer
may use the marks:

Certified Device
ISASecure

Reports:
YOK 1303069 R006 V1R1
SCP451-11 CRT Test Report
YOK 1303069 R002 V1R3
SCP461-11 CRT Test Report
YOK 1303069 R003 V1R3
Certification Report

Validity:
This Certificate is restricted to the specified version of the referenced Device (including the model number, hardware / firmware / software version) set forth in this Certificate. Furthermore, the unit shall be operated in a network and operational environment meeting the assumptions in the Certification Report.

Revision 1.1 December 24, 2013

ISASecure Chartered Laboratory:
exida
64 North Main St.
Sellersville, PA 18960
License: ISCI-CL0001
ACLASS Cert No: AT-1531

exida
Certification Services

Certificate / Certificat

Zertifikat / 合格証

YOK 1303069 C001

exida hereby confirms that the

ProSafe-RS Safety Controller

Manufactured by

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

Has been assessed per the relevant requirements of:

ISASecure™ Embedded Device Security
Assurance Program
2010.1

And meets the requirements for:

LEVEL 1

Model Number:	*SCP451-11 : Vnet/IP Firmware R19* *SCP461-11 : Vnet/IP Firmware R18*
System Software:	*Version: R3.02.10*

William M Goble
Authorized Representative

F020002.ai

Figure ISASecure EDSA certification

3. System Configuration of the ProSafe-RS

In this chapter the system configuration of the ProSafe-RS is explained. The ProSafe-RS consists of Safety Control Station (SCS), Safety Engineering Station (SENG), Automation Design Server (AD Server) and others. AD Server is a Database Server which preserve the project data in a system. A minimum configuration system consists of an SCS and a SENG (including an AD Server).

3.1 Typical configuration

The figure below shows an example of the ProSafe-RS system configuration.

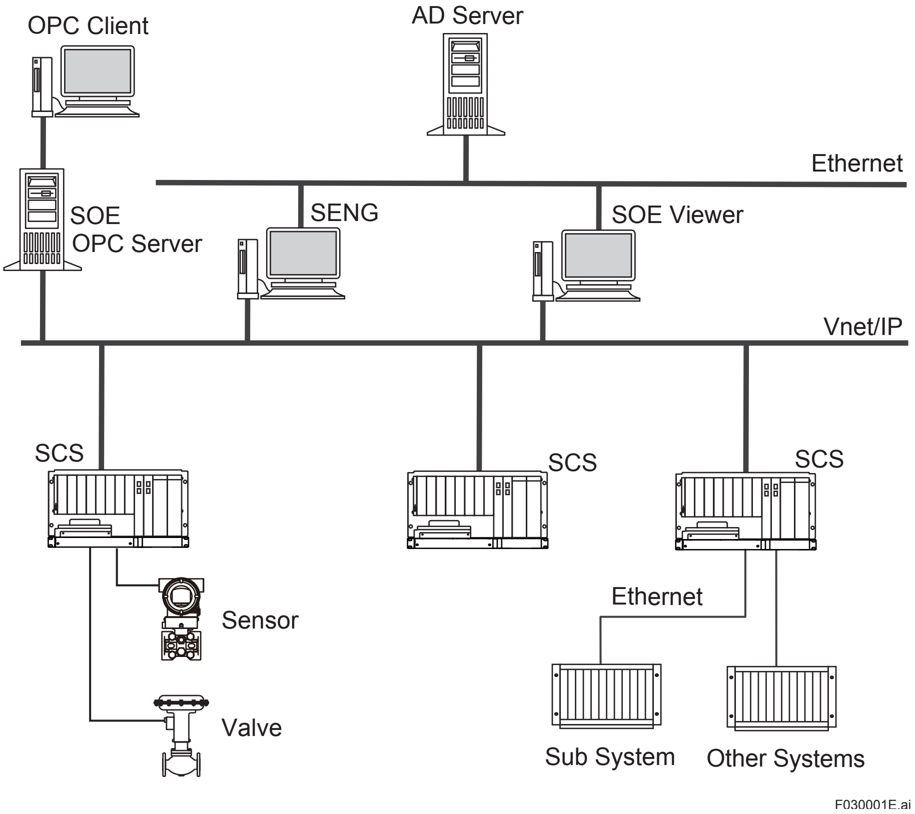


Figure Example of ProSafe-RS system configuration

■ Safety control station (SCS)

An SCS is a controller to perform safety control of the ProSafe-RS.

Main features

- Executes safety control function
- Receives input datas from field devices
  (e.g. temperature, pressure, flow, ON/OFF status of a switch)
- Transmits output instructions to field devices
  (e.g. open/close of valves, instruction of equipments' ON/OFF)
- Performs inter-station communications
  (e.g. inter-SCS safety communication, SCS link transmission safety communication)
- Communicates with field devices (HART communication)
- Communicates with other systems
  (e.g. Modbus communication)

■ Safety engineering station (SENG)

The SENG is a computer for performing SCS's engineering and maintenance tasks.

Main features

- Creates and verifies safety control functions (application programs)
- Downloads the created application programs to SCSs
- SCS Status monitoring
- Receives and displays alarm messages from SCSs

3.2 Integration with the CENTUM VP

The ProSafe-RS and the CENTUM VP systems can be integrated. The figure below shows an example of a system configuration that the ProSafe-RS and the CENTUM VP are integrated.

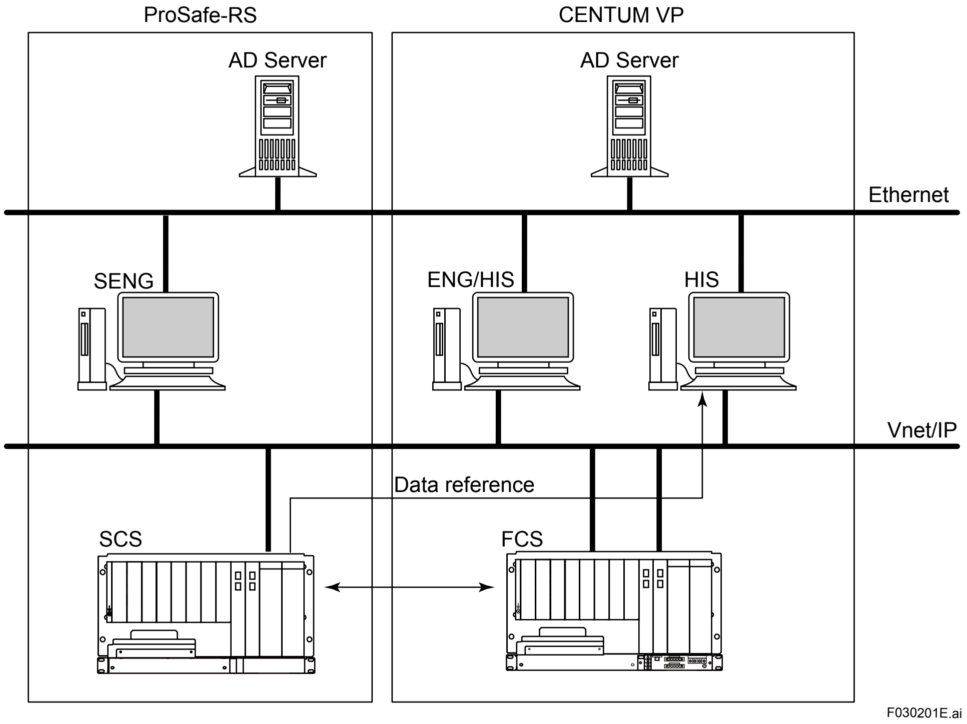


Figure System configuration example of ProSafe-RS integration with CENTUM VP

HIS
An operation and monitoring station of CENTUM VP for operating a plant.

ENG
An engineering station to perform system configuration and maintenance management of the CENTUM VP.

FCS
A controller that controls a process.

- An HIS operates and monitors both FCSs and SCSs.
- The SCS's data can be referred from HISs or FCSs.
- The SENG performs engineering of SCSs and the ENG performs engineering of FCSs and HISs. The engineering of the CENTUM VP integration systems are performed by both the SENG and the ENG. The SENG, ENG and HIS functions can be resided on a single computer or independently installed on different computers.
- The SCS's data setting can be performed from HISs or FCSs; however, the data setting for the SCS is managed with the special security scheme.

■ System scale

In a ProSafe-RS and CENTUM VP integrated system, the maximum number of station that can be configured is as follows:

- Number of connectable domains: 16
- Number of connectable stations (*1) per domain: 64
- Number of connectable stations: 256

Note: For a Vnet/IP system configuration, refer to General Specifications of “ProSafe-RS Safety Instrumented System Overview (for Vnet/IP)” (GS 32P01B10-01EN).

*1: A station is a generic name for SENG, SCS, ENG, HIS and FCS.

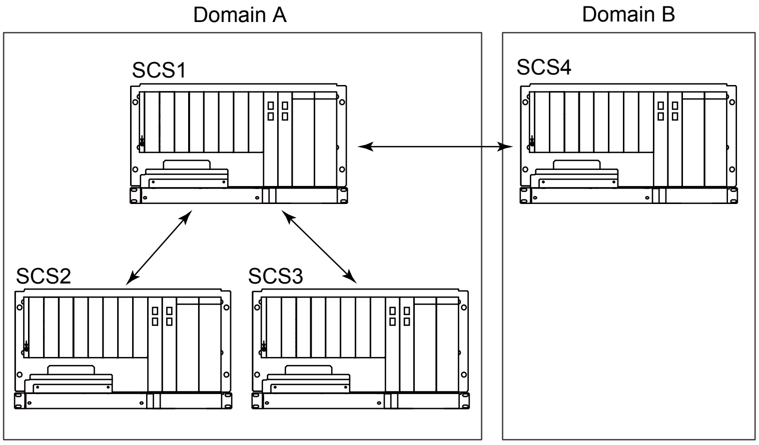
3.3 Communications among stations

“Inter-SCS safety communication,” “SCS link transmission safety communication,” and “SCS global switch communication” are used for communications among control stations.

■ Inter-SCS safety communication

The Inter-SCS Safety Communication can be established between an SCS and another SCS (in the same or in the different domain). (*1) Transmission of essential data at the SIL3 level can be performed while maintaining the communication quality.

*1: In order to perform the Inter-SCS safety communication while inter-domain, the integration with CENTUM VP system is needed.

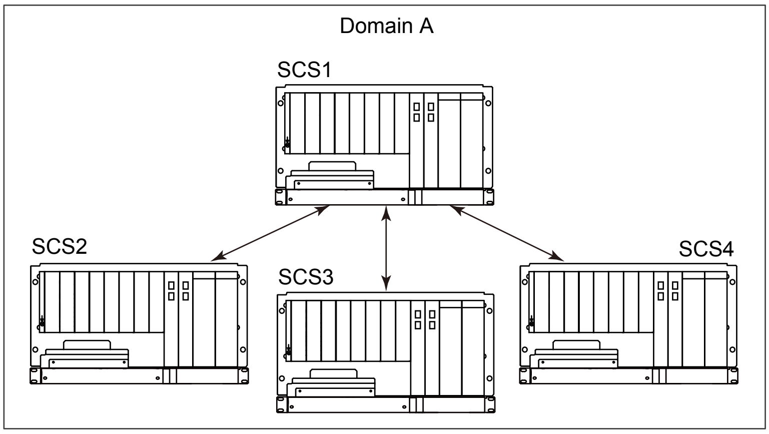


F030301E.ai

Figure Inter-SCS safety communication

■ SCS link transmission safety communication

The SCS Link Transmission Safety Communication is a safety communication to concurrently broadcast Boolean data from an SCS to multiple SCSs (in the same domain). By this communication, broadcasting of essential data at the SIL3 level can be performed.

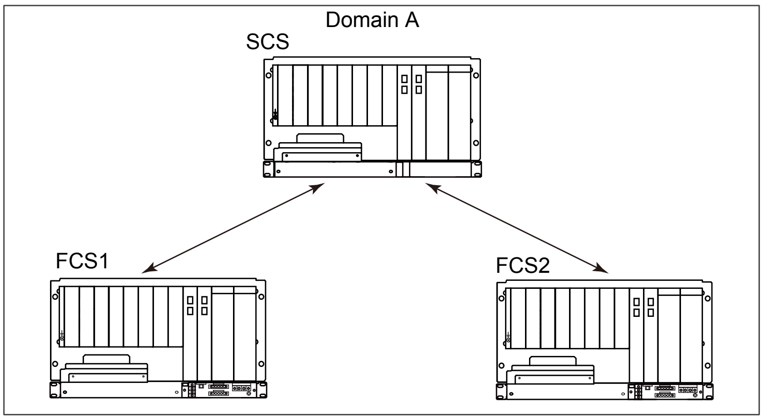


F030302E.ai

Figure SCS link transmission safety communication

■ SCS global switch communication

The SCS Global Switch Communication concurrently broadcasts data from an SCS to multiple FCSs, which is an interference-free communication that has no influence over safety control.



F030303E.ai

Figure SCS global switch communication

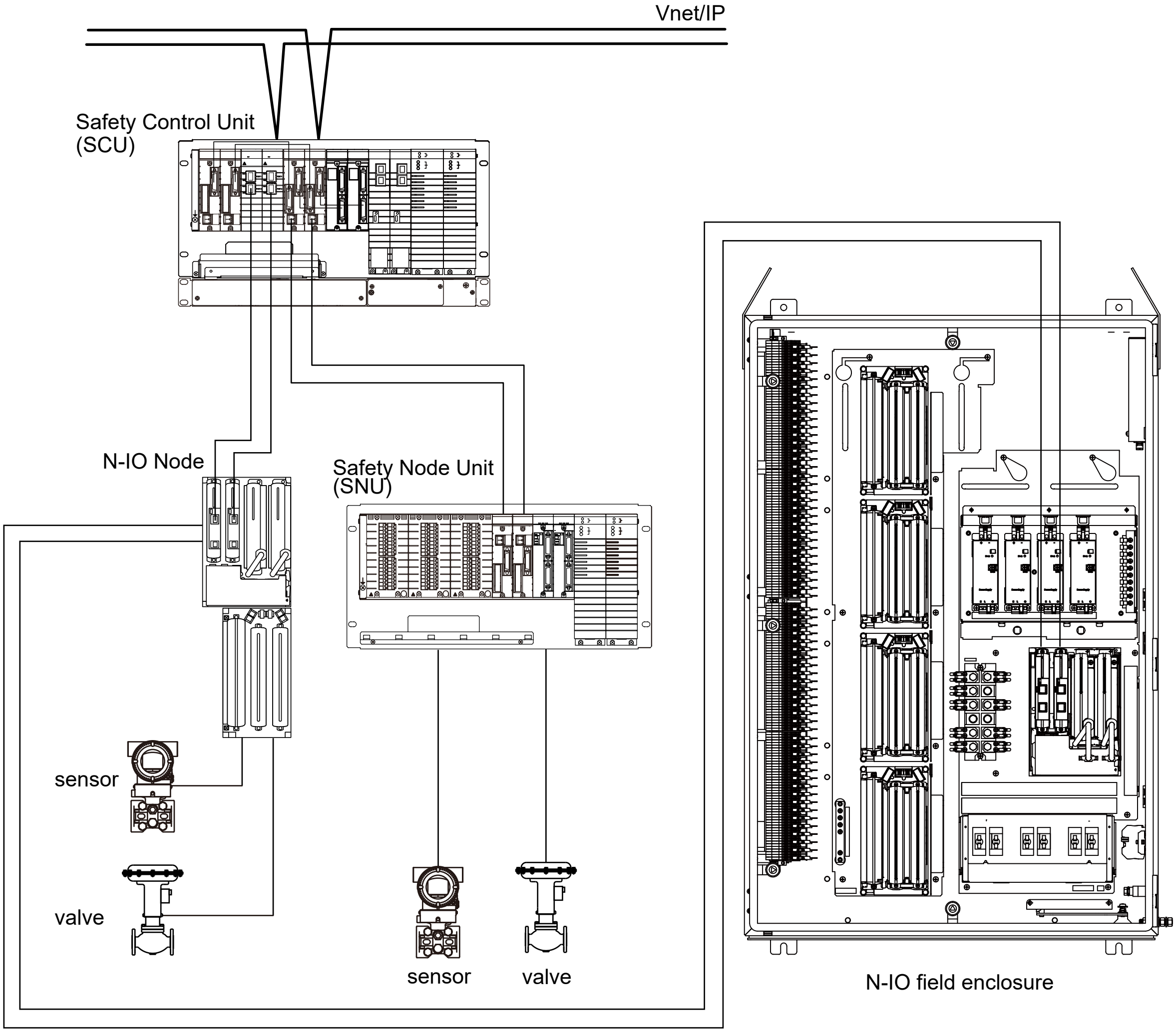
4. Safety Control Station (SCS)

This chapter explains the hardware configuration of a safety control station (SCS) that provides SIL3 in single configuration.

4.1 Hardware configuration of the SCS

The SCS is a safety controller of the ProSafe-RS. The SCS is composed of Safety Control Units (SCU), Safety Node Units (SNU) and N-IO Nodes. (including N-IO field enclosure) N-IO field enclosure is a standardized remote I/O enclosure for outdoor use, in which N-IO nodes are equiped.

The figure below shows an example of a system configuration.



F040101E.ai

Figure System configuration example of SCS

4.2 Safety control unit (SCU)

■ Overview

The SCU implements safety control function by executing the application programs downloaded from the SENG. By using the Vnet/IP communication function, inter-station communications can be performed. Input/output modules mounted on SCU perform for input/output of field devices' data.

The input/output modules can be increased by adding safety node units and N-IO nodes.

The following types of the SCU are available.

S2SC70S/D: For large-scale systems or small to medium-scale systems, applicable to N-IO node

SSC60S/D: For large-scale systems or small to medium-scale systems

SSC57S/D: For wide-area systems such as oil and gas production facilities (wellheads) or small to medium-scale systems

SSC50S/D: For small to medium-scale systems

The following figure shows an example of the SCU configuration.

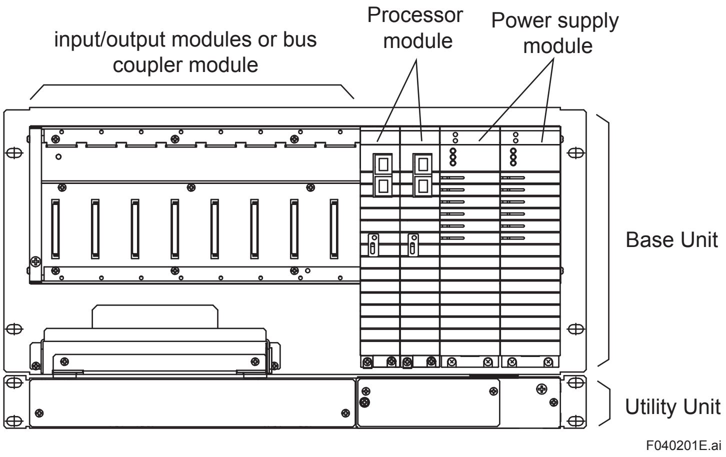


Figure Configuration of safety control unit (S2SC70D)

4.3 N-IO node, N-IO field enclosure, and safety node unit (SNU)

■ N-IO node

An N-IO node consists of an N-IO node interface units and N-IO Input/Output units. The N-IO node interface unit transmits field device signals received by the N-IO I/O unit to the SCU and the SCU data to field devices via an N-IO I/O unit. Input/output modules can be mounted on the N-IO I/O unit.

The figure below shows an example of N-IO node unit configuration.

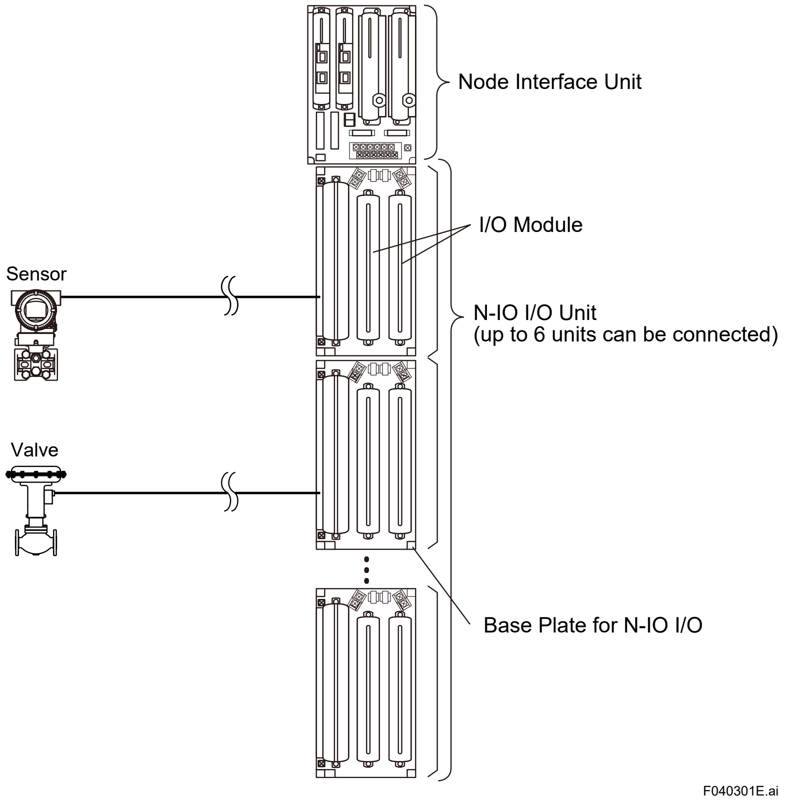


Figure System configuration N-IO node unit

● Input/Output modules

AI, AO, DI, or DO signal can be assigned to the input/output modules by the channel by software.

Model	Function	Remarks
Analog Digital Input/Output Module		
S2MMM843	(AI) Analog Input	4-20 mA , HART Communication function, Module isolation
	(AO) Analog Output	4-20 mA , HART Communication function, Module isolation
	(DI) Digital Input	no-voltage contact, Module isolation
	(DO) Digital Output	24 V DC/0.66 A (*1), Module isolation
S2MDV843	(DI) Digital Input	no-voltage contact, Module isolation
	(DO) Digital Output	24 V DC/0.66 A (*1), Module isolation

*1: The maximum load current up to 2 A device can be connected to DO by multiple channels parallel use.

Field wiring

The terminal(s) provided with the N-IO input/output unit is used for wiring directly to field devices.

N-IO field enclosure

N-IO field enclosure is a standardized remote I/O enclosure for outdoor use, which provides the accessories including field power supply units with optimized design. The N-IO field enclosure consists of two components, one is a dedicated enclosure with terminal blocks and the other is a base unit with an N-IO node including field power supply units. It is possible to order the enclosure and the base unit individually.

Safety node unit (SNU)

The input/output modules can be mounted on the SNU, and the SNU transmits analog input signals and contact signals of field devices to the SCU.

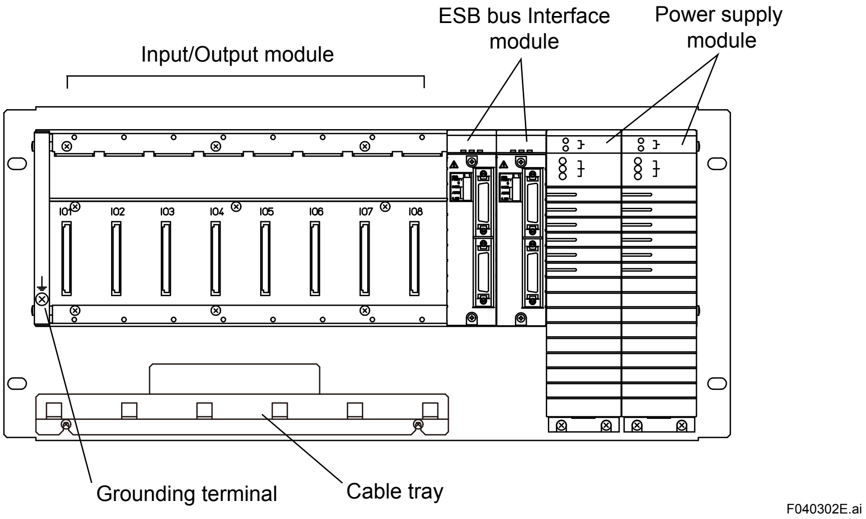


figure Configuration of safety node unit

Input/Output modules

The following table shows the input/output modules available for the ProSafe-RS. The input/output modules can take a dual-redundant configuration in order to improve the availability.

Table

Model	Name	Remarks
Analog Input/Output Modules		
SAI143	Analog input module	4-20mA, Module isolation, HART Communication function
SAV144	Analog input module	1 to 5 V/1 to 10 V, Module isolation
SAT145	TC/mV Input module	Isolated Channels
SAR145	RTD Input Module	Isolated Channels
SAI533	Analog output module	4-20mA, Module isolation, HART Communication function
Digital Input/Output Module		
SDV144	Digital input module	no-voltage contact, Module isolation
SDV521	Digital output module	24 V DC/2 A, Module isolation
SDV526	Digital output module	100-120 V AC, Module isolation
SDV531/SDV541	Digital output module	24 V DC, Module isolation
SDV53A	Digital output module	48 V DC, Module isolation
Communications Module		
ALR111/ALR121	Serial communication module	RS-232C, RS-422/RS-485
ALE111	Ethernet communication module	
S2LP131	Fire and Gas communication module	

Field wiring

For connecting a field device and an input/output module can be done by directly wiring using a pressure clamp terminal block or wiring via a terminal board using a cable-interface. Or, connecting a user-provided MIL cable with an MIL connector terminal block is available.

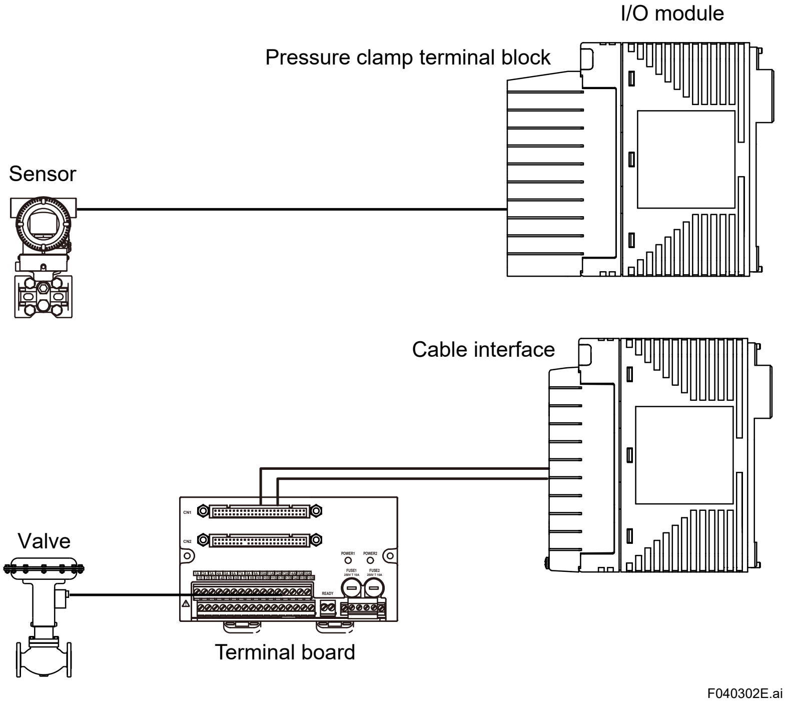


Figure Example of field wiring

5. Engineering and Operation & Maintenance

The engineering and operation & maintenance of the SCS are described in this chapter.

5.1 Engineering

Application logics need to be generated to activate ESD or fire and gas (FAG) protection systems.

■ Engineering procedure

The procedures of how to create applications to activate ESD or FAG systems as well as how to perform operational tests are as shown in the following figure.

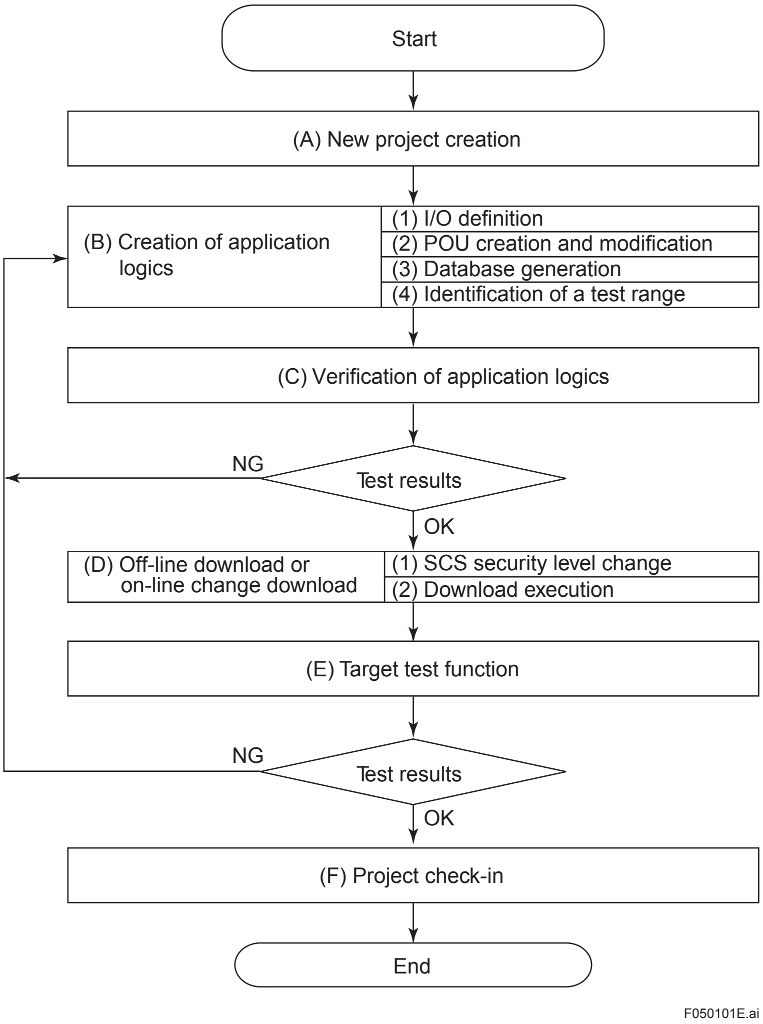

Start
(A) New project creation
(B) Creation of application logics
(1) I/O definition
(2) POU creation and modification
(3) Database generation
(4) Identification of a test range
(C) Verification of application logics
NG
Test results
OK
(D) Off-line download or on-line change download
(1) SCS security level change
(2) Download execution
(E) Target test function
NG
Test results
OK
(F) Project check-in
End
F050101E.ai

Figure Procedures for creating a ProSafe-RS standard application

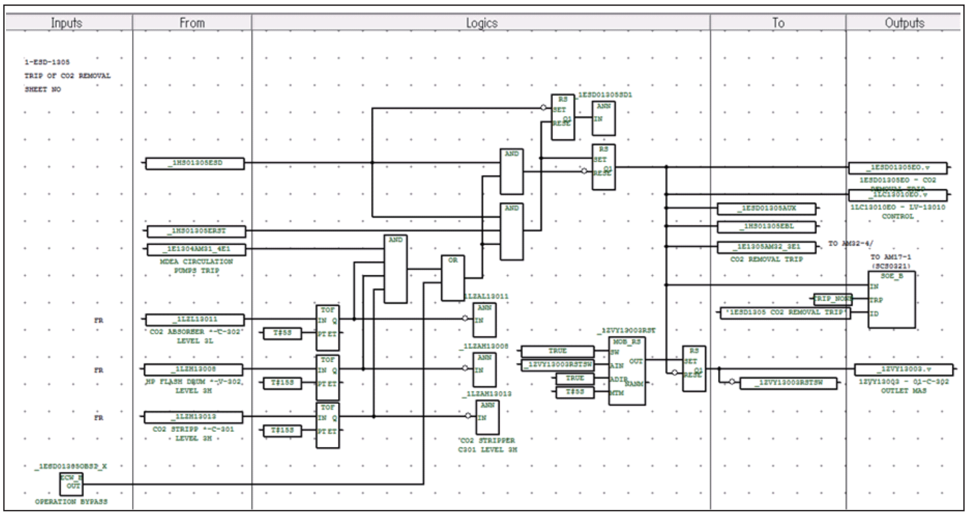
(A) New project creation

Create a new project to manage application logics. Creation of the application logic is enabled only after a creation of a new project.

(B) Creation of application logics

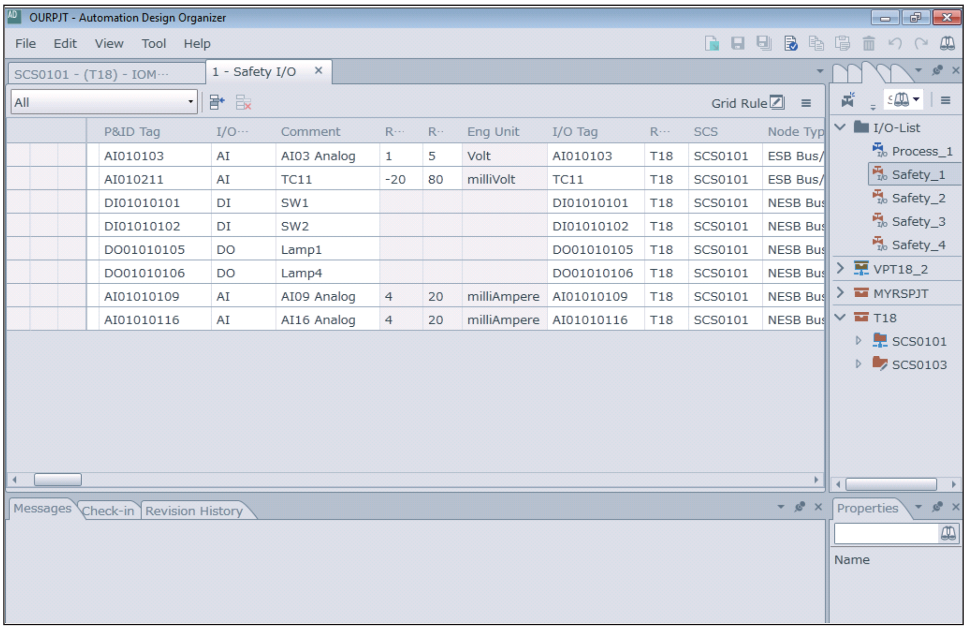
Create an application logic to materialize the designed SCS operation, by using function block diagram (FBD) or ladder diagram (LD) which conform to the IEC 61131-3 international standard.

Use the multi-language editor to create FBD. By connecting boxes of functional units called function blocks (FB) with lines, application logics from input to output can easily be created.



F050102.ai

Figure Example of creation of application logics by using multi-language editor



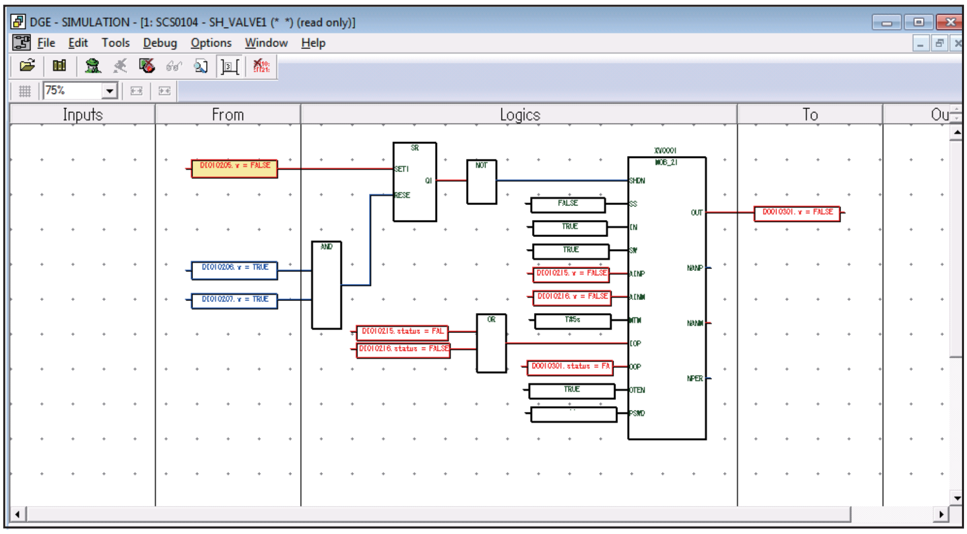
P&ID Tag	I/O···	Comment	R···	R··	Eng Unit	I/O Tag	R···	SCS	Node Typ
AI010103	AI	AI03 Analog	1	5	Volt	AI010103	T18	SCS0101	ESB Bus/
AI010211	AI	TC11	-20	80	milliVolt	TC11	T18	SCS0101	ESB Bus/
DI01010101	DI	SW1				DI01010101	T18	SCS0101	NESB Bus
DI01010102	DI	SW2				DI01010102	T18	SCS0101	NESB Bus
DO01010105	DO	Lamp1				DO01010105	T18	SCS0101	NESB Bus
DO01010106	DO	Lamp4				DO01010106	T18	SCS0101	NESB Bus
AI01010109	AI	AI09 Analog	4	20	milliAmpere	AI01010109	T18	SCS0101	NESB Bus
AI01010116	AI	AI16 Analog	4	20	milliAmpere	AI01010116	T18	SCS0101	NESB Bus

F050103.ai

Figure Define of I/O

(C) Verification of application logics

The application logic made in step (B) can be verified by using the virtual test function. The virtual test function performs the verification of the application logics on a computer without having an actual SCS. With the virtual test function displays the computation results of the application logics intuitively as TRUE (blue) and FALSE (red) on a screen. The logic simulation test and the SCS simulation test are available for the virtual test.

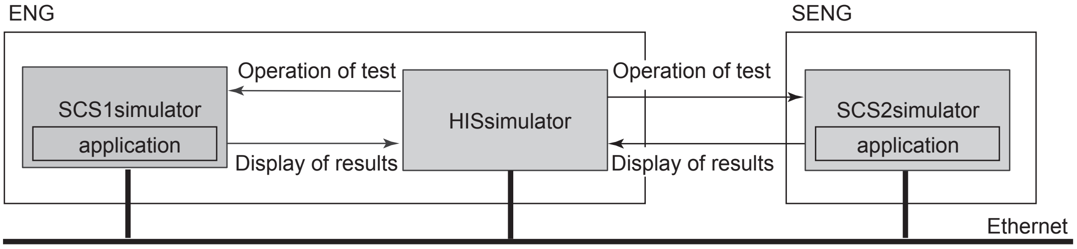


F050104.ai

Figure Example of a test window

During the logic simulation test, the SENG executes the application logic using the logic simulator. The SCS security level is disregarded when verifying the application logic of each SCS.

When the SCS simulator on the ENG or the SENG executes application logic during the SCS simulation test, can also be conducted in accordance with the SCS's security level, integrated operation environment with CENTUM VP is required. Alarm confirmation on the HIS window enabled by temporarily overwritng application logic variables using override function of the HIS simulator. And if two or more of the SCS simulators are used, the inter-SCS safety communication test can be performed as well.



F050106E.ai

Figure SCS simulation test

(D) Off-line download or on-line change download

Download the application program verified in Step (C) from SENG to SCSs. An engineer is to compare the application program on the SENG and the data base in the SCS and confirm if the downloading has been correctly executed.

(E) Target test function

The application logic can be verified on the actual SCS using the target test function. The test can also be performed without mounting input/output modules by using the forcing function (see chapter 5.2 Maintenance Functions) and manually simulate input/output signal status. The target test function can be performed in reference to the security level of the SCS.

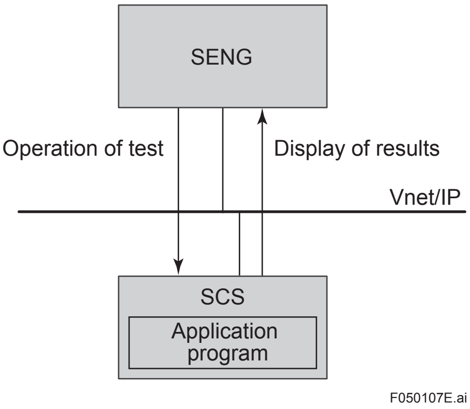


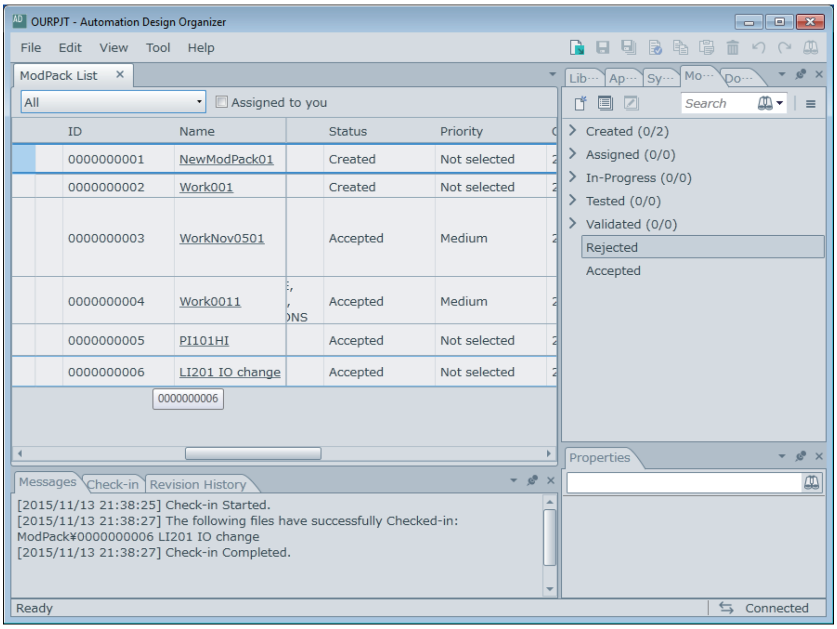
Figure Target test function

(F) Project check-in

Save the projects including the application logics created to the version management database for change management.

■ Change management function

The change management function an engineering support tool to manage change requirements generated during engineering work. By recording the changes in planning, execution, and testing, overlooking of the changes in the application programs can be prevented.



ID	Name		Status	Priority	C
0000000001	NewModPack01		Created	Not selected	2
0000000002	Work001		Created	Not selected	2
0000000003	WorkNov0501		Accepted	Medium	2
0000000004	Work0011	E, , ONS	Accepted	Medium	2
0000000005	PI101HI		Accepted	Not selected	2
0000000006	LI201 IO change		Accepted	Not selected	2

```
[2015/11/13 21:38:25] Check-in Started.
[2015/11/13 21:38:27] The following files have successfully Checked-in:
ModPack¥0000000006 LI201 IO change
[2015/11/13 21:38:27] Check-in Completed.
```

F050108.ai

Figure Change management function window

5.2 Operation and maintenance of SCS

Status of SCS and its operations in response to the plant's operating conditions and maintenance of the safety system are described in this section.

■ SCS status and operation

A safety system is expected to run properly and safely to prevent operators without authorities from making erroneous operations. The ProSafe-RS manages the SCS's operation and operational authorities by the operating mode and the SCS security level. The override and alarm window functions permits operation and monitoring of the SCS from CENTUM VP's HIS.

● Operating modes

The operating modes indicate the operating statuses of the SCS. Depending on the kinds of operating mode determines how the SCS system program performs.

Table Operating modes

Operating Modes	
Name	**Status**
Stop Mode	The initial state of the SCS
Loading Mode	Downloading a program or database information from the SENG to the SCS.
Initial Mode	Executing diagnosis, database initialization, I/O module booting and others that are needed for starting initialization of the SCS.
Waiting Mode	Waiting for all the output modules to activate.
Running Mode	The SCS is operating normally.

● SCS security levels

The SCS security level limits changes made by the operations to the SCS from outside.

Enable or disable of the user operation is controlled by the application logics depending on the defined security level.

Two categories of the security levels are available; one is the On-line level to be used during normal operation of SCS and the other is the Off-line level to be used when offline download is required. The security levels are password protected and only the authorized user with specific privileges can change.

On-line level:

Level 2
The highest security level with which the normal operation of the SCS is executed.

Level 1
The security level is temporarily used by an engineer or a specially authorized user for maintenance of the system and changing applications online.

Off-line level:

Level 0
The security level to be used when off-line download is required.

● Operation and monitoring of SCS by HIS (Override and alarm windows)

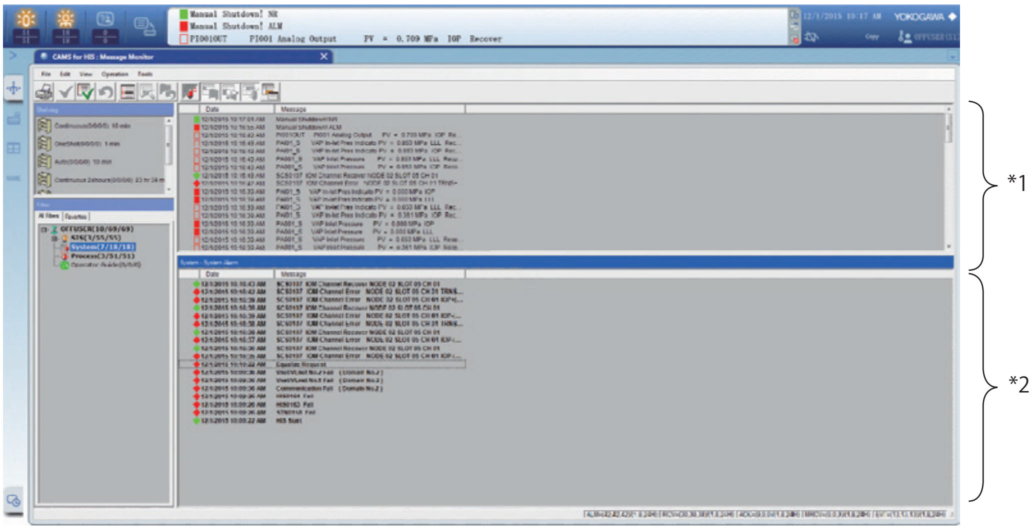
ProSafe-RS allows CENTUM VP’s HIS to control and monitor the SCSs so that the safety instrumented systems perform its functions by knowing the overall plant operation status.

Override

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 the SCS. This operation is called override. This override can be created in the application logic using safety function blocks.

Alarm window

The Alarm window is to notify operators essential alarms to sustain the plant safety. By displaying only the SCS alarms extracted from all alarms, operators are able to recognize the important alarms easily.



YOKOGAWA
CAMS for HIS : Message Monitor
File Edit View Operation Tools
Date
Message
System - System Alarm
*1
*2

```
Manual Shutdown! NR
Manual Shutdown! ALM
PI001OUT     PI001 Analog Output     PV  =  0.709 MPa  IOP  Recover
```

F050201.ai

*1: Alarms that the SCS extracted.
*2: All alarms.

Figure Integrated alarm window

Maintenance functions

A safety instrumented system is required to have regular maintenance because it has to function without fail when an abnormality occurs. For the maintenance of the ProSafe-RS, maintenance support tools and forcing are provided.

SCS maintenance support tools

The SCS maintenance support tools have been developed for the purpose of simplifying the maintenance of the SCS. Equipped with a user interface to easily spot on a failure section, the function chronologically displays maintenance data necessary for analysis in the form of diagnostic information messages.

The SCS maintenance support tools are as described below:

SCS status display:	Displays the operating status of the SCS
Diagnostic information display:	Displays diagnostic information in the SCS
Online monitoring:	Displays the operating status of the application logic on the SCS
Message cache tool:	Acknowledges the diagnostic information message and accumulation of SOE events
SOE Viewer:	Displays event information stored on the SCS
Setup Tool:	Customizes how to display and use the SCS maintenance support tools.

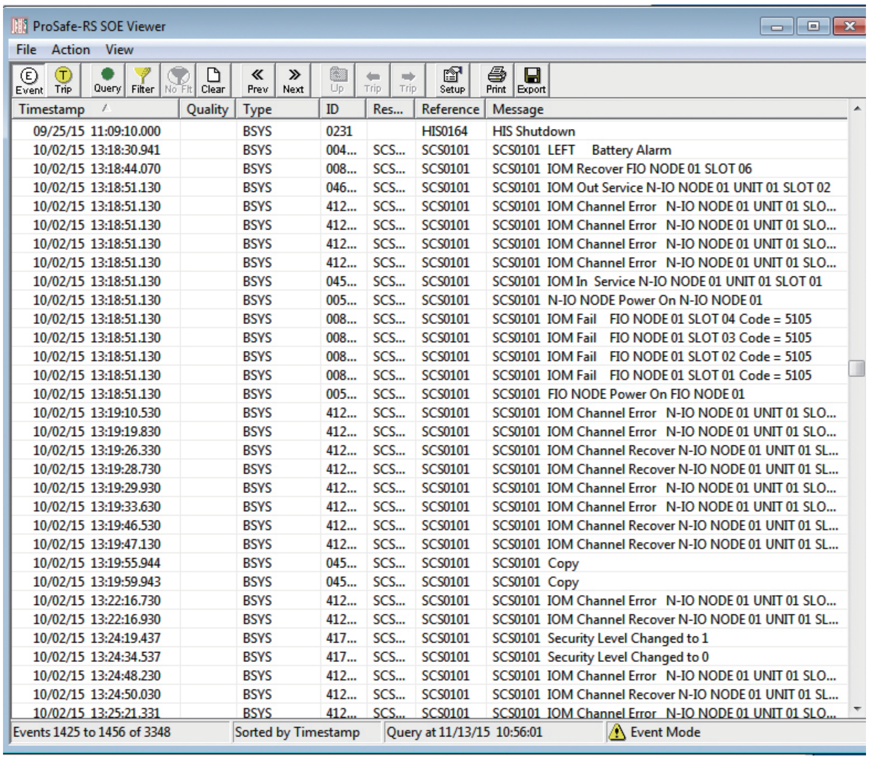
Forcing

The forcing is a function to fix or forcibly change values of input/output modules and application logic for the purpose of maintenance of the SCS or verification of application logics. Different from the override function, a dedicated user interface is used and creation of an application logic is not required.

5.3 Sequence of events recorder (SOER)

The sequence of events recorder (SOER) is a function to record the events (*1) that the SCS detects. Especially when the safety instrumented system is triggered, the SOER can be utilized for analyzing the causes of the plant's emergency shutdown. The SOER function consists of the event collection, the event storage and the time synchronization functions.

*1: The term an "event" refers to a change to the predefined application logic.



Timestamp	Quality	Type	ID	Res...	Reference	Message
09/25/15 11:09:10.000		BSYS	0231		HIS0164	HIS Shutdown
10/02/15 13:18:30.941		BSYS	004...	SCS...	SCS0101	SCS0101 LEFT Battery Alarm
10/02/15 13:18:44.070		BSYS	008...	SCS...	SCS0101	SCS0101 IOM Recover FIO NODE 01 SLOT 06
10/02/15 13:18:51.130		BSYS	046...	SCS...	SCS0101	SCS0101 IOM Out Service N-IO NODE 01 UNIT 01 SLOT 02
10/02/15 13:18:51.130		BSYS	412...	SCS...	SCS0101	SCS0101 IOM Channel Error N-IO NODE 01 UNIT 01 SLO...
10/02/15 13:18:51.130		BSYS	412...	SCS...	SCS0101	SCS0101 IOM Channel Error N-IO NODE 01 UNIT 01 SLO...
10/02/15 13:18:51.130		BSYS	412...	SCS...	SCS0101	SCS0101 IOM Channel Error N-IO NODE 01 UNIT 01 SLO...
10/02/15 13:18:51.130		BSYS	412...	SCS...	SCS0101	SCS0101 IOM Channel Error N-IO NODE 01 UNIT 01 SLO...
10/02/15 13:18:51.130		BSYS	045...	SCS...	SCS0101	SCS0101 IOM In Service N-IO NODE 01 UNIT 01 SLOT 01
10/02/15 13:18:51.130		BSYS	005...	SCS...	SCS0101	SCS0101 N-IO NODE Power On N-IO NODE 01
10/02/15 13:18:51.130		BSYS	008...	SCS...	SCS0101	SCS0101 IOM Fail FIO NODE 01 SLOT 04 Code = 5105
10/02/15 13:18:51.130		BSYS	008...	SCS...	SCS0101	SCS0101 IOM Fail FIO NODE 01 SLOT 03 Code = 5105
10/02/15 13:18:51.130		BSYS	008...	SCS...	SCS0101	SCS0101 IOM Fail FIO NODE 01 SLOT 02 Code = 5105
10/02/15 13:18:51.130		BSYS	008...	SCS...	SCS0101	SCS0101 IOM Fail FIO NODE 01 SLOT 01 Code = 5105
10/02/15 13:18:51.130		BSYS	005...	SCS...	SCS0101	SCS0101 FIO NODE Power On FIO NODE 01
10/02/15 13:19:10.530		BSYS	412...	SCS...	SCS0101	SCS0101 IOM Channel Error N-IO NODE 01 UNIT 01 SLO...
10/02/15 13:19:19.830		BSYS	412...	SCS...	SCS0101	SCS0101 IOM Channel Error N-IO NODE 01 UNIT 01 SLO...
10/02/15 13:19:26.330		BSYS	412...	SCS...	SCS0101	SCS0101 IOM Channel Recover N-IO NODE 01 UNIT 01 SL...
10/02/15 13:19:28.730		BSYS	412...	SCS...	SCS0101	SCS0101 IOM Channel Recover N-IO NODE 01 UNIT 01 SL...
10/02/15 13:19:29.930		BSYS	412...	SCS...	SCS0101	SCS0101 IOM Channel Error N-IO NODE 01 UNIT 01 SLO...
10/02/15 13:19:33.630		BSYS	412...	SCS...	SCS0101	SCS0101 IOM Channel Error N-IO NODE 01 UNIT 01 SLO...
10/02/15 13:19:46.530		BSYS	412...	SCS...	SCS0101	SCS0101 IOM Channel Recover N-IO NODE 01 UNIT 01 SL...
10/02/15 13:19:47.130		BSYS	412...	SCS...	SCS0101	SCS0101 IOM Channel Recover N-IO NODE 01 UNIT 01 SL...
10/02/15 13:19:55.944		BSYS	045...	SCS...	SCS0101	SCS0101 Copy
10/02/15 13:19:59.943		BSYS	045...	SCS...	SCS0101	SCS0101 Copy
10/02/15 13:22:16.730		BSYS	412...	SCS...	SCS0101	SCS0101 IOM Channel Error N-IO NODE 01 UNIT 01 SLO...
10/02/15 13:22:16.930		BSYS	412...	SCS...	SCS0101	SCS0101 IOM Channel Recover N-IO NODE 01 UNIT 01 SL...
10/02/15 13:24:19.437		BSYS	417...	SCS...	SCS0101	SCS0101 Security Level Changed to 1
10/02/15 13:24:34.537		BSYS	417...	SCS...	SCS0101	SCS0101 Security Level Changed to 0
10/02/15 13:24:48.230		BSYS	412...	SCS...	SCS0101	SCS0101 IOM Channel Error N-IO NODE 01 UNIT 01 SLO...
10/02/15 13:24:50.030		BSYS	412...	SCS...	SCS0101	SCS0101 IOM Channel Recover N-IO NODE 01 UNIT 01 SL...
10/02/15 13:25:21.331		BSYS	412...	SCS...	SCS0101	SCS0101 IOM Channel Error N-IO NODE 01 UNIT 01 SLO...

Events 1425 to 1456 of 3348 | Sorted by Timestamp | Query at 11/13/15 10:56:01 | ⚠ Event Mode

F050301E.ai

Figure SOE Viewer

■ Event collection

Not only digital inputs (DI) but also changes in digital outputs (DO) and analog inputs (AI) are collected as event information. By using the SOER function blocks with the application logic, changes in application logics can be acquired as event information, which enables to record changes in communication data with other SCSs.

■ Event storage

A certain volume of event information is stored in the SCS, and a computer for the data storage is not required to be activated all the time. On the other hand, the essential event information before and after the ESD are stored separately.

Revision Information

- Title : Safety Instrumented System ProSafe-RS System Overview
- Manual No. : TI 32P01A10-01EN

Nov. 2024/4th Edition

Introduction	Updated descriptions of trademark.
1.	Necessity of Safety Instrumented System ■ Safety evaluation scales [Correction of description]
3.2	Typical configuration [Correction of errors]

Dec. 2018/3rd Edition

Front page	ProSafe-RS Logo change
4.1	Added the description of N-IO field enclosure. Added the figure of N-IO field enclosure in the Figure “System configuration example of SCS”.
4.3	Added the description of S2MDV843, S2LP131, and N-IO field enclosure.

July 2016/2nd Edition

All pages, Clerical error correction.

Dec. 2015/1st Edition

Newly published.

Written by Yokogawa Electric Corporation

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