SAFETY TECHNOLOGIES INCORPORATED IN THE SAFETY CONTROL STATION

EMORI Toshiyuki [*1] *KAWAKAMI Shigehito* [*1]

We have developed the ProSafe-RS safety instrumented system, which has been certified by the TÜV German certification organization as meeting Safety Integrity Level (SIL) 3 specified in IEC 61508, the international standard for functional safety. The Safety Control Station (SCS) is a safety controller that is a core component of the ProSafe-RS. This paper describes some of the technologies, including safety functions, protection against interference from non-safety functions, and safety communication, incorporated in the SCS to achieve SIL 3.

INTRODUCTION

Conventional safety instrumented system (SIS) is typically installed separated from a distributed control system (DCS) to eliminate interference from the DCS and assure safety. However, users increasingly wish to integrate SIS with DCS while maintaining the safety of safety controllers.

The safety control station (SCS), a safety controller of the ProSafe-RS, features the same architecture as the field control station (FCS) of our DCS, the CENTUM CS 3000, and inherits the same high reliability and the process data communication interface as the FCS. Furthermore, the SCS implements safety functions and safety communication to achieve SIL3-level safety as well as close integration with the CS 3000 system, and has been certified by the TÜV German certification organization.

SAFETY LOOP AND SCS

Figure 1 shows the SCS functional configuration.

The SCS is a safety logic solver located on a safety loop and captures input data from sensors and outputs data in a fail-safe manner to final control elements.

The SCS consists of safety functions that directly affect a safety loop (safety logic execution, I/O function, diagnostic function, etc.), as well as non-safety functions not directly related to the safety loop (connection to CS 3000 and Modbus communication, etc.). Moreover, use of Inter-SCS safety communication allows a safety loop to be built extending over multiple SCSs via the V net control network.

SCS SAFETY FUNCTION

This section describes the basic safety functions of the SCS as the safety logic solver.

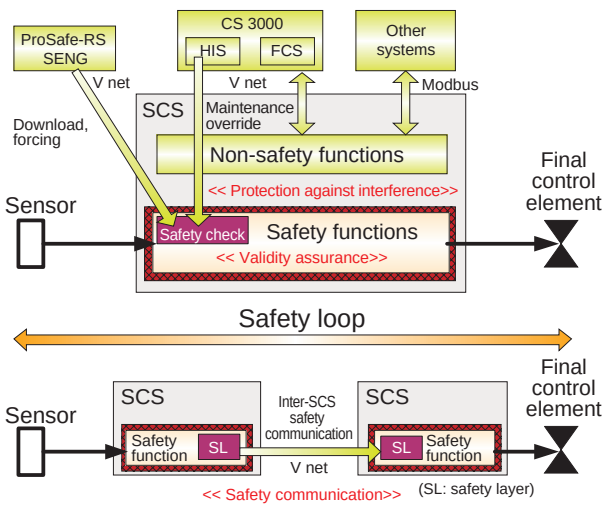

Figure 1 Configuration of SCS Functions

*1 IA Systems Business Division, IA Business Headquarters

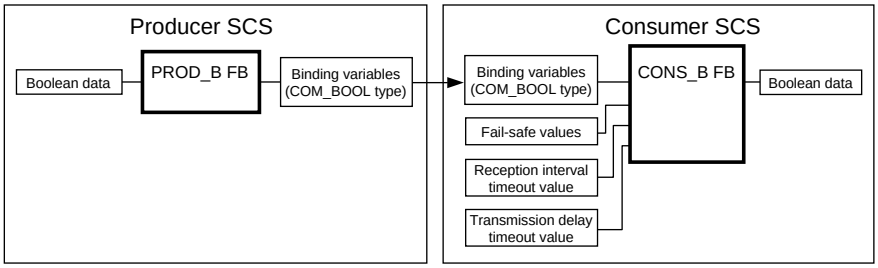

Figure 2 Example of Logic for Inter-SCS Safety Communication

Safety Logic Execution

In the SCS, safety logic described using the IEC 61131-3 international standards compliant function block diagrams (FBD) and ladder diagrams (LD) are run in specified scan period. When the SCS detects demand (event for which the plant should be shut down) from sensors, shutdown processing described using safety logic is run to output shutdown signal to final control element(s) (shutdown valves, etc.).

Actions On Fault Detection

In the CPU modules and I/O modules of the SCS, self-diagnostics are performed periodically by the hardware and software.

The following describes the actions of each module to be performed if a failure is detected in single module operation. When modules are operated in dual-redundant configuration, if a single failure occurs, the module continues to operate singly and does not allow the shutdown processing to run. A failed module and the cause of failure are notified by an alarm, and the failed module can be replaced while online.

(1) Actions on fault detection in CPU module
If a failure is detected in the CPU module in single configuration, the CPU module is stopped and all the output modules output a pre-defined fail-safe value.

(2) Actions on fault detection in Input module
The input modules periodically perform field wiring diagnostics, channel diagnostics, and module common area diagnostics. If any diagnostic detects a failure, an input value for a fault that is pre-defined in the safety logic can be nortified, and the safety logic to be taken in the event of demand occurrence is shared as-is to perform shutdown processing taken in the event of failure.

(3) Actions on fault detection in Output module
The output modules also periodically perform field wiring diagnostics, channel diagnostics, and module common area diagnostics. If any diagnostic detects a failure in the module common area, outputs of all channels of the output module concerned are forcibly turned off.
If a failure occurs in individual channels, a pre-defined fail-safe value is forced to be output. It is also possible to monitor for an output channel that has entered an abnormal status using safety logic, to output a shutdown signal to other output channel(s).

Inter-Scs Safety Communication

The ProSafe-RS allows an integrated system in which safety communication with SIL3-level certification and conventional CS 3000 control communication are mixed to be flexibly built, either in a small- to large-scale configuration or in a wide-area configuration, on the same V net without separating the CS 3000 system's V net control network.

To perform Inter-SCS safety communication, dedicated Inter-SCS safety communication function blocks (FB) are used to describe the safety logic (Figure 2).

Hazardous events that may occur in communication (such as data corruption, omission, or delay) are all checked by the consumer SCS FB (CONS_B in example in Figure 2). If a fault is detected, a pre-defined fail-safe value is output, and information identifying the faulty data and the cause of the fault are notified by an alarm.

Maintenance Override

The maintenance override function is used for bypassing shutdown processing so that it is not executed by safety logic during partial maintenance such as specific input. Creating bypass logic using a dedicated override FB allows the CS 3000's human interface station (HIS) to safely perform maintenance override for SCS (Figure 3).

Generally, a value input to the override FB is output as-is. However, an override execution command from the HIS causes a specified value (OVR_B VAL in Figure 3) to be output.

Moreover, the override FB has an override permission switch (OVR_B SW in Figure 3), and maintenance override cannot be executed from the HIS unless this switch is in the permission status. A combination of the override FB with a dedicated password FB also allows the HIS to make an override permission.

TECHNOLOGIES FOR SIL3-LEVEL SAFETY

To meet the SIL3-level safety for an integrated system having both safety functions and non-safety functions as shown in Figure 1, it is required to assure the validity of the safety functions and safety communication, and assure that non-safety functions do not interfere with safety functions.

Assurance of Validity of Safety Functions

The ProSafe-RS has been developed according to strict development standards in the same way as the CS 3000 to assure high quality. Furthermore, it analyzes the effects of potential risks on the safety functions and incorporates the following mechanisms for detecting faults to check that no hazardous status (condition in which a plant cannot be shut down even if a demand is happened) is caused by systematic failure resulting from a human error, etc.:

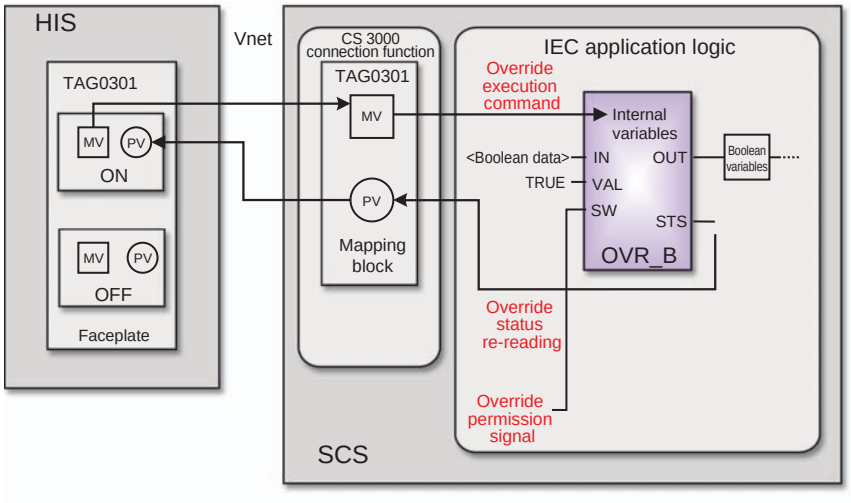

Figure 3 Example of Maintenance Override from HIS

(1) Assurance of validity of safety logic
Safety logic can be downloaded to the SCS only after checking whether user-created safety logic is properly and safely configured, and or checking areas assumed to be affected by logic modification using an analyzer.

(2) Check of validity of data from SENG
The SENG is a component for performing engineering and maintenance of the SCS and is connected to the same V net as the SCS. For communication relating to operation from SENG to SCS, the following mechanisms are employed to assure safety:

- CRC (cyclic redundancy check) codes are appended to individual files and operation data that are loaded from the SENG to SCS to check that the files or data are not corrupted on the SCS side.
- Which part of the SCS is how operated is notified by an alarm for delivery check with respect to operation from the SENG.

(3) Sequence monitoring
The ProSafe-RS monitors processing relating to the safety functions such as safety logic, self-diagnostic that runs in the SCS whether such processing is securely executed in the correct sequence within a specified time. Also, software is monitored for a runaway using a watch-dog timer (WDT).
If a fault occurs, the output modules output a fail-safe value, shutting down the plant securely.

(4) Data space monitoring
For SCS programs and databases used by safety functions, CRC is executed at the start of SCS to check for validity. Monitoring is also performed at periodic intervals to check that no safety-related program or database has been modified (corrupted).

Protection against Interference from Non-safety Functions

The SCS is equipped with the following mechanisms to protect the SCS's safety functions against interference from non-safety functions also existing in the SCS or interference from a non-safety device connected to the SCS via communication:

(1) Memory protection for safety function areas
The memory area used by the safety functions in the SCS is protected against being written from non-safety functions.

(2) Design with the highest priority given to execution of safety functions
The priority of executing a safety functions is set to a higher level than that of the non-safety functions in the SCS. Thus, even if a non-safety function enters an endless loop, the safety functions can be securely executed every scan period.

Furthermore, the design ensures that execution of a safety function is not interfered with by a surge of communication from the CS 3000 station on the V net to the SCS. In the SCS, the processing time of V net communication made per scan period is measured to perform control such that the processing time does not exceed the upper limit of a set processing time. Thus, even if a malicious communication attack on the SCS is made, the safety functions can be executed every scan period.

(3) Security level
The SCS has a security level for permitting operation on the safety functions from the SENG. At the operation level, the SCS does not accept operations that modify a safety function, such as off-line download, online change, or forcing (operation of fixing or changing safety logic data value(s) forcibly). To perform SCS maintenance, it is necessary to input a password that has kept in the SCS, to change the security level to the maintenance level.

(4) Protection against interference from maintenance override
The maintenance override features that the override from the HIS can be executed even if the SCS's security level is at the operation level. To let the HIS, non-safety equipment, change data in the SCS's safety loop directly, the SCS uses the following mechanisms to assure safety.

- An override execution command from the HIS cannot be accepted unless the override FB is in the permission status.
- Override execution to the SCS is possible only from HIS's dedicated override faceplate. Since this faceplate displays the operation status and read-back status from the SCS, correct execution can be checked.
- If the permission or execution status of the override FB changes, an alarm is reported from the SCS to the HIS, so that it is possible to check which override FB is operated and what condition it has entered.
- Override request data from the HIS to SCS is assigned a CRC code, and the validity of the data is checked by the SCS.
- To prevent neglect of canceling an override execution status,

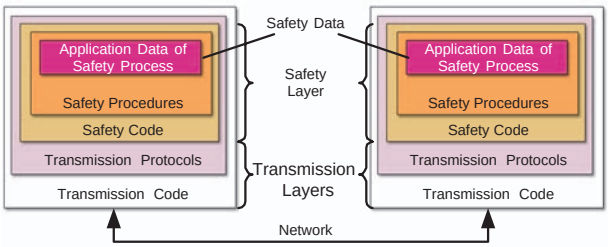

Figure 4 Configuration of Safety Communication

an alarm is reported from the SCS to HIS if the override condition continues for more than a specified time.

- The number of overrides that are being executed simultaneously is also monitored and, if an override exceeding a specified number of overrides is executed, an alarm is reported from the SCS to HIS.

Safety Communication in the SCS

Safety communication is a communication method that has a mechanism for checking that safety-related data is passed to the communication counterpart without fail on an existing non-safety communication system. (See the EN50159 European standards concerning safety communications.)

In safety communication, a safety layer is arranged in the place of the application layer in communication to separate the safety functions from the outside non-safe world. Figure 4 shows the configuration of general safety communication.

In the SCS, the safety layer is arranged within the Inter-SCS safety communication FBs (see Figure 2) that are executed by safety logic to ensure safety communication. The producer-side safety layer (producer FB) appends information such as a sequence number, time stamp, and CRC codes to each safety data to be sent, while the consumer-side safety layer (consumer FB) strictly checks for transmission errors.

Table 1 shows transmission errors that may occur in communication and check measures conducted in the Inter-SCS safety communication.

V net's high reliability and high responsiveness have already been proven in the CS 3000's control communication. The Inter-SCS safety communication further improves the communication reliability and safety assurance under an environment having both safety communication and control communication.

Table 1 Check Measures for Transmission Errors in the Inter-SCS Safety Communication

Possible Transmission Errors	Measures for Checking			
	Appending of Information Identifying Transmission Source and Destination	Appending of Sequence No. to be Updated Every Sending	Appending of Time Stamp upon Sending on the Transmission Side	Appending of CRC Codes to Data and Information Appended as Noted at the Left
Repetition of same message	—	○	○	—
Missing of necessary message	—	○	—	—
Insertion of unexpected message	—	○	—	—
Transposed message order	—	○	○	—
Message has been corrupted	—	—	—	○
Delay in message arrival	—	—	○	—
Confused as message from a non-safety device	○	—	—	—

○: transmission error that can be checked by a measure,
—: transmission error that cannot be checked by a measure

CONCLUSION

In the ProSafe-RS, not only the mechanism of safety measures implemented on the SCS but also precautions and operating procedures for safe engineering and operations are described in safety manuals and engineering guides to assure safety from various aspects for obtaining safety certification.

Yokogawa will continue to develop DCS and SIS in integrated form, to keep providing total solutions that satisfy users. ◆

REFERENCES

(1) Ando Tadaaki, et al., “Safety Instrumented Systems and ProSafe Diagnostic Functions,” Yokogawa Giho, Vol. 43, No. 4, 1999, pp. 175-180 in Japanese
(2) Emori Toshiyuki, et al., “Communication Bus V-net for the CENTUM CS,” Yokogawa Technical Report, No. 23, 1997, pp. 21-24
(3) EN50159-1/-2: Railway applications–Communication, signaling and processing systems: Safety-related communication in closed/open transmission systems (March 2001)