AIMS AND FEATURES OF THE ProSafe-RS SAFETY SYSTEM

NISHIDA Jun[*1] *MATSUDA Toshihiko*[*1]

We have developed the ProSafe-RS, a safety system compatible with the SIL3 level of the IEC 61508 international standard. This product alone fulfills the requirements for safe instrumentation. In addition, it is highly compatible with our CENTUM CS 3000 process control system and offers a platform for flexible, comprehensive solutions to users who implement overall process plant designs. This paper outlines the aims and features of the ProSafe-RS.

INTRODUCTION

There is growing recognition of the importance of preventing serious accidents in the process control field in view of the potential scale of impact on society. The IEC 61508 and IEC 61511 international standards call for the reduction of risk using safety instrumented systems (SIS) as well as the configuration of multiple protective layers in a process control system in order to prevent major accidents. Safety systems included in SIS are required to be both safe and highly reliable. Generally, safety and high reliability appear to be similar in meaning. However, the term “safety” as applied to safety systems, means the level of accuracy at which plant shutdown is performed when a problem occurs, and includes the characteristic that safety systems will behave toward the fail-safe side, i.e., plant shutdown, even if they themselves fail. In contrast, reliability refers to the low probability at which a plant is shut down due to failure in a safety system (error trip rate is low). From the user's point of view, both process control and safety instrumentation are conducted for the same plant, requiring solutions that consider both process control and safety instrumentation comprehensively. Our safety system, the ProSafe-RS, has been developed with the following features to meet these requirements.

- Integration with DCS
- Compatibility between the high safety of SIL3 level and high reliability in a single configuration
- IEC 61131-3-compliant engineering tools

*1 IA Systems Business Division, IA Business Headquarters

SYSTEM CONFIGURATION

Figure 1 shows an example of an integrated configuration of the ProSafe-RS safety system and the CENTUM CS 3000 production control system. In the ProSafe-RS, the safety engineering PC (SENG) and safety control station (SCS) are connected directly using a V net control bus.

The SENG is a PC on which software having engineering functions and maintenance functions runs.

The SCS is a safety controller that performs logical operations such as shutdown by downloading application(s) created on the SENG. The architecture of the SCS is based on the flexibility of the CS 3000 FCS, and its I/O modules and CPU modules allow the user to select a dual-redundant configuration (Figure 1-①) or single configuration (Figure 1-②③) in a single station according to the user's objective. Moreover, SCS supports inter-SCS safety communication, allowing a safety loop to be built (Figure 1-④) extending over SCSs via the V net control bus shared by the CS 3000.

Performing CS 3000 tag engineering on the SENG and then downloading these tags to the SCS allows integrated operations handling SCS (Figure 1-⑥) to be performed from the CS 3000 HIS in the same way as the CS 3000 FCS.

INTEGRATION WITH DCS

Architecture Integration

The basic architecture of the ProSafe-RS is the same as that of the CS 3000. This makes the ProSafe-RS easy to use, based on the many years of DCS development and the proven field reliability of the CS 3000.

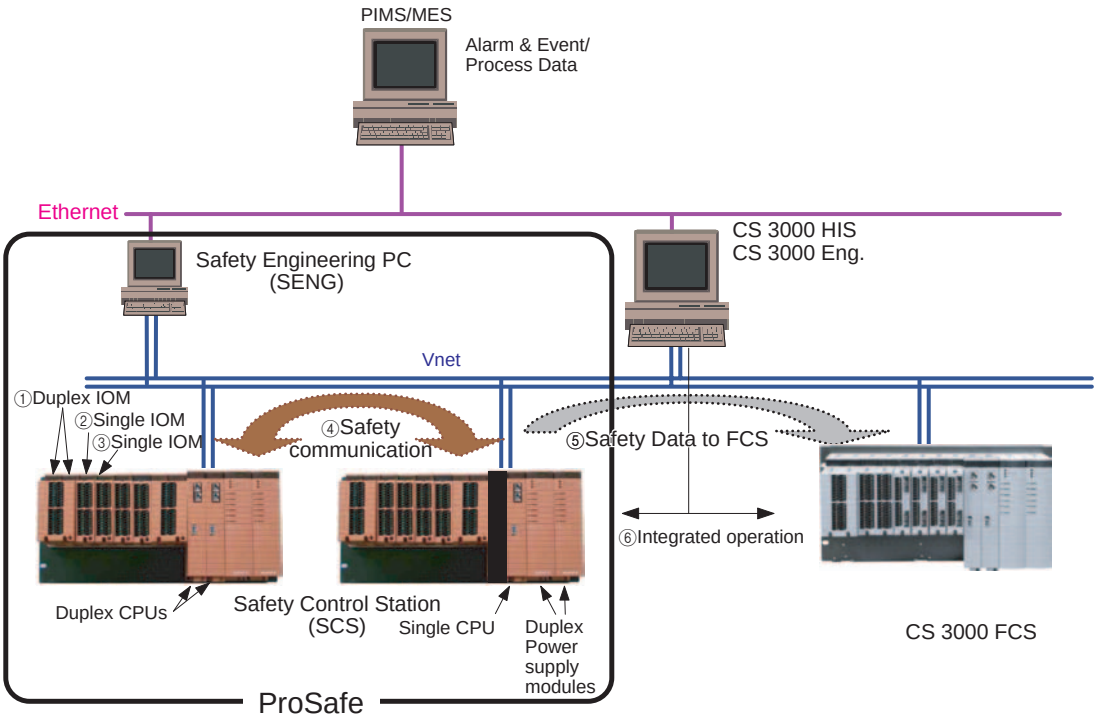

Figure 1 Example of ProSafe-RS/CS 3000 Integrated System Configuration

Users also benefit, as the concept of hardware installation, maintenance methods, etc., is the same between DCS and SIS by applying the CS 3000 and ProSafe-RS in the same plant.

Moreover, architecture integration allows the SIS and DCS to be connected using the V net common control bus. This simplifies system building and mutual interface design, thus significantly improving total engineering efficiency including the design and installation costs of system building and interface design.

In addition, the design concept of providing the same interface with the HIS operator station and MES domain for the DCS and SIS provides a platform offering a total solution using the DCS and SIS with virtually no distinction, as well as sophisticated functional enhancement (such as equipment management) in the future.

Operation Integration

The SIS is a system that immediately shuts down a plant safely if a problem occurs in the plant and neither the DCS nor humans can handle it. In other words, cases where SIS operation or monitoring is required are very rare, and it is inconvenient to always monitor both SIS-specific HMI and DCS-specific HMI for that purpose alone. If the SIS and DCS can be operated and monitored using the same HMI, the operators do not have to remember the operations of both HMIs, and when needed, the operator can take accurate action using the HMI of the DCS he/she usually uses. Therefore, routine SIS monitoring should ideally be performed using the same DCS HMI.

To meet these user requirements, the ProSafe-RS provides an integrated operating environment having the following features:

- The operator can check pre-alarms sent from the SIS using the same CS 3000's HMI
- The operator can perform operations using the same method as the CS 3000 during periodic inspection.
- The system structure allows the CS 3000's HMI or FCS to easily refer to SCS data, so DCS and SIS integrated applications can be built easily. For example, in some applications SIS data is successfully used on the DCS side, such as comparing SIS and DCS sensor information on the DCS side to check that DCS-side sensors are correct.
- Higher-level management using OPC can be performed in the same way as DCS.
- By comprehensively analyzing DCS and SIS event information (sequence of event: SOE), the causes of abnormality can be analyzed on a plant-wide scale.

Integration of DCS and SIS, and Segregation Thereof

Integration of DCS and SIS has the advantages described above. However, the international safety standards require DCS and SIS to be segregated in order to protect the function of safety protective layers even if control functionality is lost, as is apparent in risk assessment analysis (Layer of Protection Analysis, LOPA) using multiple protective layers.

The system configuration of the ProSafe-RS integrates the DCS and SIS using the V net control bus, while keeping DCS and SIS functions securely separated. When considering the segregation between the DCS and SIS, the key points are how to prevent interference from the DCS to SIS and how to prevent a failure affecting both systems. The following describes how the

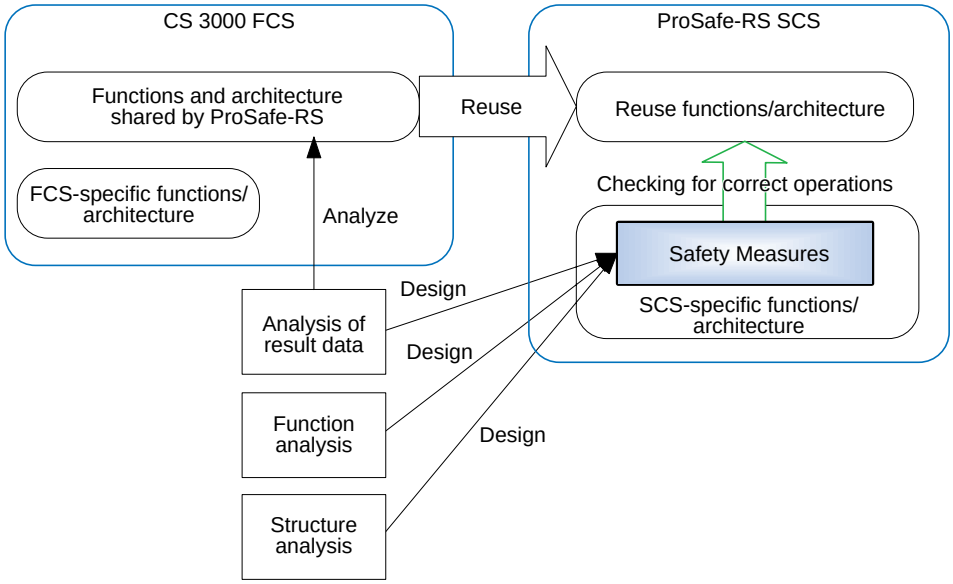

Figure 2 Common Cause Failures and Safety in Reuse

ProSafe-RS protects itself against interference from DCS and common cause failures.

- Prevention of interference from DCS to SIS
  For example, assume that two interconnected SCSs and three FCSs are directly connected to the same V net. Possible cases of interference by the FCS with the SCS via the V net bus include attacking the SCS by the erroneous transmission of a large amount of data to the V net bus and mistakenly transmitting incorrect frames. However, the reliability of the V net bus and FCSs has been proved by the proven-in-use data provided by the CS 3000, so the FCS is very unlikely to have adverse effects on the SCS, as is the case with the CS 3000. Even if a V net bus failure occurs, the safety measures, in, which is implemented focusing on detecting the V net bus failure, can protect SCSs from communication attacks or shut down a safety loop configured by SCS-to-SCS connection. This means that any effects from the DCS via the V net do not cause a dangerous failure in the ProSafe-RS. That is, non-interference from the DCS to SIS (DCS does not cause loss of SIS safety functions) is assured.
- Protection of DCS and SIS against common cause failures
  Because the ProSafe-RS is based on the CS 3000 architecture, it is important to assume common systematic failure in both the DCS and SIS and consider the possibility of common-cause failure and preventive measures. Figure 2 shows the basic concept in regard to preventing such failures. For both SCS hardware and software, the modules' proven-in-use data shared by the CS 3000 has been analyzed, and measures are taken for areas judged to adversely affect safety such as implementing a diagnostic scheme or multiplexing these areas. Moreover, if an abnormality in each section could have adverse effects on the safety functions in view of the functions and architecture of the ProSafe-RS, then safety measures are incorporated in the same way. These safety measures have been newly developed for the ProSafe-RS, and their effectiveness and sufficiency have been discussed and recognized by a certification body (TÜV).
  In other words, even if there is a systematic failure common to both the CS 3000 and ProSafe-RS, the ProSafe-RS is capable of detecting such a failure (or error caused by it) and taking pre-determined actions.

SAFETY AND RELIABILITY AT SIL3 IN SINGLE CONFIGURATION

The ProSafe-RS incorporates the redundant matching mechanism and self-diagnostic mechanism in one I/O module and CPU module to comply with the SIL3 level defined in IEC 61508 by a single component. That is, both the CPU module and I/O module can realize a safety loop meeting SIL3 in a single configuration. This provides the following additional engineering options:

- No damage in safety functions against one side failure in dual-redundant configuration
  The ProSafe-RS, in which no safety function is damaged even if a component on one side fails in dual-redundant configuration, meets the SIL3 level in a single configuration. Thus, if one of the CPU modules or I/O modules fails in dual-redundant configuration, the SIL3 level safety is still maintained.
  In general, for systems realizing the SIL3 level in the dual-redundant configuration, if a single-side failure occurs, the failure detection ratio drops until repair is completed. In this case, the upper limit of the time taken to repair the hardware concerned is determined (for example, 8 hours), and if the hardware is not repaired within that time, overall system

safety deteriorates. That is, the user must repair the failure within the specified time, and if this is not possible, then the user must take safety actions such as manually shutting down the plant. Therefore, the user must consider the running costs involved in ensuring the repair time, such as putting engineer(s) on standby, increasing the number of engineers, quickly identifying and replacing the faulty area and then establishing a system to conduct tests, throughout the entire plant's operation period. The ProSafe-RS overcomes these limitations; the dependence of safety on humans can be reduced, and running costs can also be reduced. Moreover, the flexibility of engineering is broadened, such as installation in difficult-to-maintain locations (remote locations, within wells, etc.).

- High reliability
  For systems meeting the SIL3 level by dual-redundant CPU module configuration, safety is often secured by performing data collation between the two CPU modules. If nonconformity is detected during this data collation, it is difficult to determine which module is faulty. Thus, both modules are generally assumed to be faulty and measures are taken to shut down the system. In other words, any single fault causing collation nonconformity results in an error trip. However, because the ProSafe-RS performs SIL3-level diagnosis in each module, no inter-CPU module collation is made. This means that no error trip occurs unless two failures simultaneously occur in both CPU modules, making the system exceptionally reliable.
- Flexible action in single configuration
  The ProSafe-RS has a function for preventing an error trip in the event of an I/O module failure even in a single I/O module configuration. For digital input modules (DI), it is possible to define that “1” is input if a failure is detected in the relevant channel of an I/O module when the signal input is set to “1” during normal condition and to “0” in the event of plant failure. In this case, no error trip is caused in the event of failure in the I/O module even in a single configuration, and only the occurrence of failure is notified using an alarm. This maintains plant reliability. In addition, the user can replace a faulty area within a specified repair time to secure safety.

IEC 61131-3-COMPLIANT ENGINEERING FUNCTIONS

The ProSafe-RS engineering functions support languages compliant with the IEC 61131-3 international standard. This allows applications having a hierarchical structure to be created and so users can benefit from the advantages of IEC 61131-3, such as reusability and conversion to parts.

The ProSafe-RS supports the following functions for efficient engineering and maintenance.

- IEC 61131-3 languages and CS 3000 integrated tools
  As a function for integration with the CS 3000, the ProSafe-RS supports tools that correlate the IEC 61131-3 function blocks with CS 3000 tags and work in conjunction with the CS 3000 engineering functions. This ensures the efficiency of CS 3000 integrated engineering.
- On-line modification
  The ProSafe-RS function of modifying an application without stopping the safety controller, i.e., without shutting down the plant, and continuing operations has been officially certified.
  Furthermore, there is an engineering tool (Cross Reference Analyzer) for minimizing areas to be tested during on-line modification. This eliminates the need for retesting all applications after partial modification of an application, which is compulsory in many SISs in terms of certification.
- Function for quick maintenance work
  The ProSafe-RS supports maintenance-specific HMIs (SCS maintenance support function) to simplify identification of a failed area in the event of an SCS hardware failure.

CONCLUSION

This paper has outlined the features of the ProSafe-RS and their objectives. The ProSafe-RS provides a powerful platform for achieving safety instrumentation and total DCS solutions. In the future, we will study the following functional enhancements to meet various user needs:

- Expansion of I/O types and coordination with field devices
- Functional enhancement for reducing engineering costs
- Support for value-added functions such as operator training environment ◆

REFERENCES

(1) Sekiguchi Takashi, Sato Yoshinobu, Practical Manual for Mechanical and Functional Safety, Nikkan Kogyo Shimbun, 2001, 271p. in Japanese
(2) Komiya Hiroyoshi, et al.,“FFCS Compact Control Station in CENTUM CS 3000 R3,” Yokogawa Technical Report, No.38, 2004, pp. 5-8
(3) Feature Story about Safety Systems, Yokogawa Giho, Vol. 49, No. 4, 2005, pp. 147-158 in Japanese

◆◆◆