HARDWARE FEATURES OF THE ProSafe-RS

YAMASHIRO Yasuhiko [*1] ***SEKINO Hiroyoshi*** [*1] ***SHISHIBA Ryoutarou*** [*1]
KOBAYASHI Yoshinori [*1]

The new hardware of our ProSafe-RS safety system offers single and dualredundant module configurations, both of which have achieved a safety integrity level (SIL) of 3. Based on the technological heritage and reliability of the CENTUM CS 3000, which has a proven track record in the hardware market, the ProSafe-RS is designed to meet all the safety design requirements of IEC61508, an international functional safety standard. The main feature of the newly developed ProSafe-RS hardware is the application of dual microprocessor technology, not only to the CPU module, but also to the I/O module. This feature affords an SIL 3 in a single configuration as well as in a dual-redundant configuration.

INTRODUCTION

There are already safety systems on the market that have achieved safety integrity level SIL3 of the functional safety standard, IEC61508. However, most of them have achieved SIL3 by conversion of modules into dual-redundant or triplex form. With this method, if one of the modules fails, safety is degraded; the failure must be repaired within a specified time in order to maintain safety. Moreover, because the modules are required to be multiplexed, costs are likely to be relatively high. If SIL3 can be achieved in single configuration, system costs can be reduced to a low level, and if redundancy is available, a high operating ratio can be attained.

This paper primarily introduces the hardware of safety system ProSafe-RS (Figure 1) which has achieved safety integrity level SIL3 in a single module configuration based on the highly reliable technology of the CENTUM CS 3000 series that has a market-proven record. Moreover, flexible redundancy was also available in this system.

*1 IA Systems Business Division, IA Business Headquarters

SAFETY DESIGN ARCHITECTURE AND RELIABILITY

(1) Requirements for meeting SIL3
To be applicable to the SIL3 safety loop in single module

Figure 1 External View of the ProSafe-RS (in Redundancy Configuration)
Upper half: safety control unit
Lower half: safety node unit

configuration, the ProSafe-RS's probability of failure on demand (PFD) value must be limited to 15% (1.5×10^{-4}) or less of the PFD value of the overall SIL3 safety loop (10^{-3} to 10^{-4}). For this, a proof test (operation test to be conducted at regular inspections) is assumed to be 10 years, the undetected dangerous failure rate (λ_{DU}) for the hardware constituting the ProSafe-RS needs to be limited to a value as small as 3.4 fit (probability at which the number of failures occurring in 10^9 hours is 3.4 times) or less.

Furthermore, IEC61508 specifies that the safe failure fraction (SFF) ((total failure ratio - λ_{DU}) ÷ total failure ratio) × 100%) must be 99% or higher. This indicates that all self-diagnostics must be put to full use to limit the undetected dangerous failure rate to less than 1%.

(2) Safety design architecture

When realizing safety integrity level SIL3, an important point is just how to enhance the self-diagnostics. However, IEC61508 defines that microprocessors alone cannot have a self-diagnostic rate of 90% or above. Thus, to achieve a self-diagnostic rate of 99% or above, a means such as the use of two microprocessors to compare calculation results is required.

Therefore, the ProSafe-RS processor modules have adopted the redundant matching method, the 'Pair & Spare' method, of microprocessors that has a proven record in the CENTUM. Also for the input/output modules, microprocessors are used in pairs on the basis of the CS 3000's FIO. In addition, conversion of the input/output circuits to multi-system form, inter-system comparison, and activation diagnostics of the input/output circuits were employed to achieve the high failure detection rate.

Furthermore, SIL3 safety needs to be assured for the I/O buses (ESB/SB buses) that perform data communications between the processor modules and input/output modules. Thus, in the same way as Vnet based safety communication, a safety layer is provided for both the processor modules and input/output modules, and CRC and sequence numbers are appended to safety communication data and strict checks are conducted to assure safety.

(3) Safety verification

We verified conformance to SIL3 using a technique known as "failure modes effects and diagnostic analysis" (FMEDA) and analyzed the failure rate, failure mode, and effects caused by the failure of a component on all of the constituting components. Among those failures found in these analyses, we quantitatively estimated the dangerous failure rate (λ_{DU}) that could not be detected by self-diagnostics, calculated the PFD value and verified that it was 1.5×10^{-4} or less, meaning it was less than the target value. We proved that this estimation was correct by conducting equipment verification such as fault insertion tests witnessed by the safety certification agency TÜV Rheinland.

(4) High reliability

To achieve high reliability and a high operating ratio with SIL3 safety maintained, the ProSafe-RS has adopted the redundancy technology of the CS 3000 that can be applied on a module basis. All of the processor module, input/output modules, power module, and communication buses can be made redundant. However, the power module and communication buses are provided in redundant configuration as standard to enhance the reliability of the platform section. For environmental resistance, the ProSafe-RS has met the requirements of IEC61131-2 (Programmable Controllers-Equipment requirements and test) in which test conditions stricter than general DCS are required, EN298 (burner management standards), and EN54-2 (fire protection and fire extinguishing system standards). Furthermore, the ProSafe-RS's corrosion resistance meets the G3 specifications of ANSI/ISA S71.04 as standard.

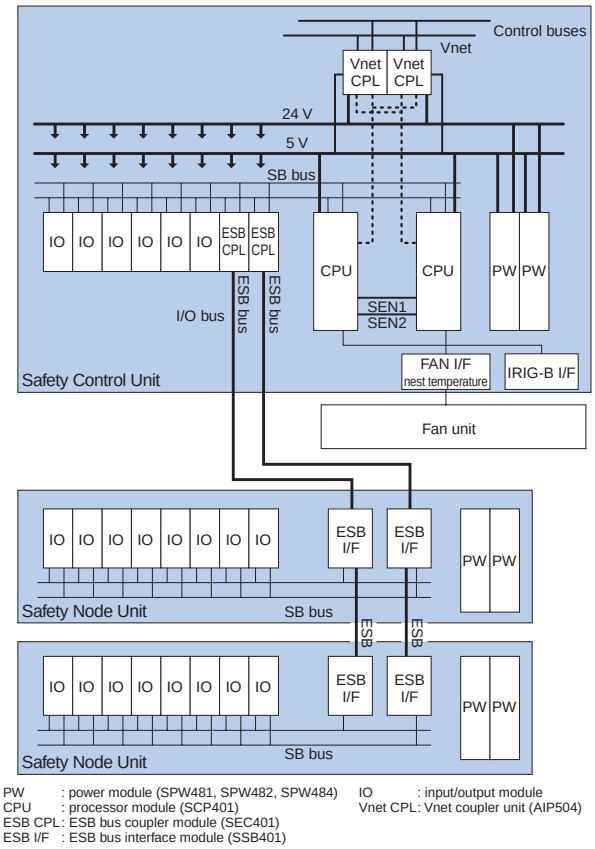

Figure 2 SCS Configuration

SCS HARDWARE CONFIGURATION

The safety control station (SCS) consists of one safety control unit and safety node units that can be extended to a maximum of nine units. The control buses and I/O buses have adopted the same Vnet and ESB/SB buses as those of the CENTUM CS 3000. Figure 2 shows the configuration of ProSafe-RS's SCS.

At the time of development, CS 3000's FFCS and FIO were employed as the platform taking into account integral operation with CS 3000, maintainability, and productivity as well as a high degree of safety and reliability. Thus, the ProSafe-RS's outer dimensions are the same as those of FFCS and FIO.

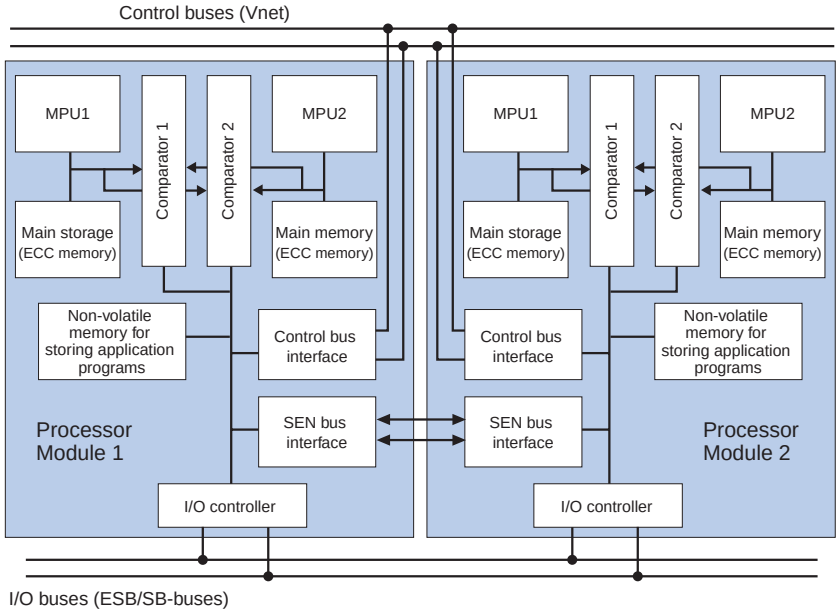

Figure 3 Configuration of the Processor Modules (in Redundant Configuration)

Unit Configuration

The safety control unit can singly configure SCS, incorporating eight input/output modules in addition to the processor modules. Alternatively, it can have six input/output modules and incorporate the ESB bus coupler module (SEC401) to set up configuration that extends the capability of the safety node unit. The operating ambient temperature of the safety control unit is from -20ºC to 50ºC as standard, but wider temperature-capable specifications that are equipped with cooling fans and can cope with a maximum of 70ºC are also available.

Moreover, the IRIG-B (GPS connection) interface for realizing high-precision time-of-day synchronization between SCSs is also available as an option.

The safety node unit can incorporate up to eight input/output modules, coping with a temperature environment of from -20ºC to 70ºC as standard.

I/O Buses

The I/O bus (ESB/SB bus) specifications are the same as those of CENTUM. Because isolation between safety communication and non-safety communication is realized on the same bus using the noted safety layers, it is also possible to use the conventional FIO by connecting it on the same buses. However, it is necessary in this case to obtain the TÜV certification for the fact that FIO connection does not interact with the safety functions. Thus, only the RS communication modules are made connectable at present.

Processor Modules

Figure 3 shows the configuration of the processor modules (in redundant configuration). The processor module was developed based on the CS 3000 FFCS's processor modules (CP401) that employ the redundant matching method, or 'Pair & Spare' method. In the CP401's redundant matching method, two processors perform the same computation, the results of which are compared by one comparator at signal-line levels to detect temporary computation errors. This alone is enough to achieve high reliability. In the ProSafe-RS, however, the comparators, main storages, groups of associated registers, WDT, etc., are made completely dual-redundant to thoroughly eliminate factors that might result in a common-cause failure. This allows the processor modules to be designed such that the undetected dangerous failure rate (λ_{DU}) is minimized. To incorporate these functions into the same size as that of the CP401, we have developed a new highly integrated ASIC, and most of the redundancy-related functions are incorporated into this one-chip ASIC with the exception of the microprocessor (MPU) and main storage (ECC memory). This ASIC design was also made such that a variety of safety design requirements specified by IEC61508 have been satisfied.

In addition, the CP401 uses chargeable secondary batteries to back up the main storage against a power failure and backup time is approximately 48 hours. However, IEC61131-2 requires that the retention time of the application program be 1000 hours or

Table 1 Input/Output Module Types

Model	Module Type	Specifications
SAI143	Analog input module	4-20 mA, 16 ch
SAV144	Analog input module	1-10 V, 16 ch
SDV144	Digital input module (with SOE function)	No-voltage contacts, 16 ch
SDV531	Digital output module	24 VDC, 8 ch,0.6 A/ch
ALR111*	RS-232 communication module	2 ports
ALR121*	RS-422/-485 communication module	2 ports

* These modules can be installed in SCS for use, but cannot be applied to the safety loop.

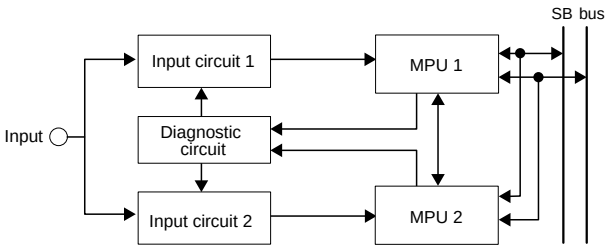

Figure 4 Input Module

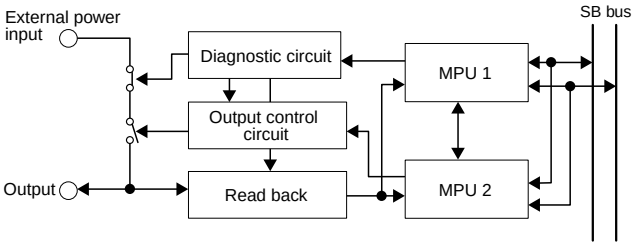

Figure 5 Output Module

more at normal temperature, or 300 hours or more even at high temperatures. To meet these requirements, we have adopted the method of storing application programs in a non-volatile memory (flash memory).

Input/Output Modules

We have developed four types of new SIL3-compliant input/output modules based on FIO and have taken steps such that two types of the existing FIO communication modules can be installed in the same SCS as interference-free modules for safety function. Table 1 shows the types of the input/output modules.

Figure 4 shows the schematic configuration of an input module, while Figure 5 shows that of an output module. Each input/output module is equipped with two MPUs and operates by comparison collating the soundness of commands or input/output data from the processor modules between the MPUs. Unlike hardware-based comparison collation made by comparators in the processor modules, MPU-to-MPU comparison collation operations in the input/output modules are achieved by performing inter-MPU communication using firmware installed in each MPU to make synchronization at a high level. This method is one of the significant features of the safety input/output modules.

Input Modules

An input module consists of two microprocessors (MPUs), two input circuits per channel, and a diagnostic circuit checking the input circuits and peripheral circuits. Input signals from the field are input to the two MPUs via the two independent input circuits. The MPUs check if data input to each MPU matches each other by mutual collation, to assure the soundness of the input circuits and MPUs themselves. When they agree with each other, the data is transmitted to the processor modules via the safety layers configured by the firmware. Moreover, because an input signal handled by the safety system does not change unless a shutdown request is generated, if a component of the input channel circuit gets stuck and fails and cannot be detected, the output cannot be shut down in the event of an occurrence of demand. To avoid such a hazardous situation, the input channel circuits are periodically activated to check for a sticking failure all the time.

Output Modules

An output module receives an output-instructing command sent from the processor modules via the I/O buses using two MPUs and checks the soundness of the command at each MPU making use of the safety layers. The module also compares the results of the check between the MPUs. After verifying the soundness of the command, the module outputs an instruction value. The output value is read back by the two MPUs to check if it agrees with the instruction value all the time. Because an output signal also does not change unless a shutdown request occurs, the output channel circuit is periodically activated to check for a sticking failure in the output switches and read-back circuits. If an output switch is stuck to ON and fails, the other switch arranged in series with that output switch is turned off. This allows the output to be forcibly shut off.

Field Wiring Diagnosis

The soundness of cables connecting the ProSafe-RS and field devices is also an important point in building the safety loop. Even if the ProSafe-RS itself is sound, if wiring is short-circuited or has a break, field wiring cannot properly function as a safety loop. Thus, the ProSafe-RS input/output modules are provided with a function for detecting short-circuits or breaks in wiring. If an input/output module detects a problem, an alarm is generated to inform the operator of the occurrence of a problem, allowing the problem to be resolved.

CONCLUSION

This paper has introduced the hardware configuration and design architecture of the ProSafe-RS SCS. In the future, it is expected that the development of technologies for improving safety and reliability of sensors and actuators will accelerate in the market. These devices occupy a considerable portion of the safety loop's PFD value.

We will enhance a lineup of input/output modules for the ProSafe-RS that can handle such field devices and offer higher safety solutions to users. ◆

REFERENCES

(1) IEC61508 First Edition; Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
(2) Komiya Hiroyoshi, et al., “FFCS Compact Control Station in CENTUM CS 3000 R3”, Yokogawa Technical Reports, No. 38, 2004, pp. 5-8