Evolution of Solution

SAT145/SAR145 Temperature Input Modules Satisfying Safety Integrity Level (SIL) 3

Yuya Itagaki [*1] *Atsushi Terayama* [*1]
Koji Nakaya [*1] *Junichiro Katsu* [*1]

We have developed two types of temperature input module as the I/O function of the ProSafe-RS safety instrumented system. These modules conform to the safety integrity level (SIL) 3, which is defined in the IEC61508 international functional safety standard, and achieve fast response and high reliability. This paper introduces their functions in the safety system and describes how the functions are achieved.

INTRODUCTION

Yokogawa's ProSafe-RS safety instrumented system is used for many applications [(1)] as a system conforming to the safety integrity level (SIL) 3 defined in the IEC61508 international functional safety standard [(2)].

To deal with temperature inputs, systems were conventionally configured using signal conditioners. However, securing enough space for signal conditioners was often difficult in such system configurations. Especially when SIL 3 is required, the problem is serious because a redundant configuration is required. Figure 1 shows an external view of the newly developed temperature input modules conforming to SIL 3: SAT145 for the thermocouple and SAR145 for the resistance temperature detector.

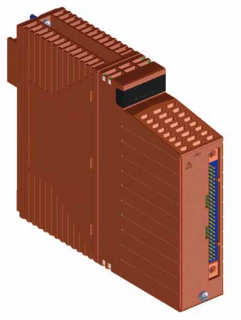

Figure 1 External view of the temperature input module

*1 Field I/F Development & Engineering Dept.,
Industrial Automation Systems Business Headquarters

Using a new temperature input module eliminates the need for a signal conditioner as shown in Figure 2. Combined with the compact terminal board that was concurrently developed, the modules solve the problem of installation space.

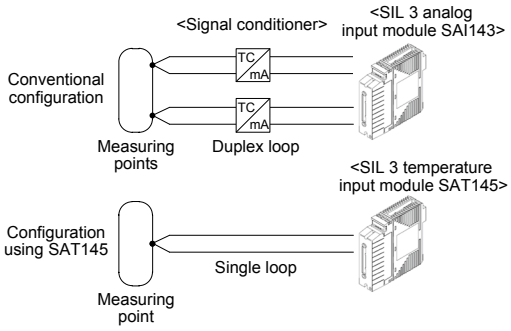

Figure 2 Example of system configuration with SAT145

These newly developed modules are based on the basic specifications and highly reliable technologies of the existing AAT145 and AAR145 temperature input modules for the CENTUM VP integrated production control system. Employing more advanced self-diagnosis, they have achieved conformity to SIL 3, which safety systems are required to meet. The modules have also satisfied the requirements for high-speed input response and fault detection, both of which safety system applications are required to meet. They also have achieved high availability and maintainability to increase plant productivity.

This paper explains the high safety integrity level, high-speed response, high availability, and increased maintainability required for a safety module, which are all achieved in the new modules.

BASIC SPECIFICATIONS OF SAT145/SAR145 TEMPERATURE INPUT MODULES

The basic specifications of the newly developed SAT145/SAR145 temperature input modules are equal to or higher than those of the AAT145 and AAR145 temperature input modules for our CENTUM VP system. Table 1 shows the basic specifications of the new modules.

While there are as many as 16 input points, individual channels are isolated and the data update period is as high as 150 ms.

The burnout (breaking of a wire) detection time is reduced to 1.5 seconds, over ten times faster than the CENTUM VP I/O modules.

Table 1 Basic specifications of temperature input modules

Specification \ Model	SAT145	SAR145
Function	TC/mV input	RTD input
Number of input channels	16-channel	16-channel
Input signal	TC input: J, K, E, T, S, R, N, B mV input: −100 to 150 mV	RTD input: Pt100, Pt50, Pt200, Pt500, Pt1000 Ni100, Ni120
Accuracy	TC: ± 40 μV mV: ± 40 μV	800 Ω range: ± 180 mΩ 4000 Ω range: ± 1700 mΩ
Isolation type	Isolated channels	Isolated channels
Data update period	150 ms	150 ms
Burnout detection time	1.5 sec	1.5 sec

SAFETY DESIGN ARCHITECTURE

1) Requirements for meeting SIL 3

When designing a ProSafe-RS system, the design target to configure a SIL 3-compliant safety loop is keeping the Probability of Failure on Demand (PFD) for the entire safety loop less than 1.5×10^{-4}, or 15% of the required rate for SIL 3 (10^{-3} to 10^{-4}). To achieve this, assuming that the proof test (validation test during a periodic inspection) is conducted every 10 years, the total undetected dangerous failure rate (λ_{DU}) of all the components constituting the safety loop should not exceed 3.4 fit (failure rate of once in 340,000 years). That means the failure rate of a single I/O module has to be extremely small.

The IEC61508 also stipulates that the Safe Failure Fraction (SFF: (Total failure rate - λ_{DU}) / total failure rate × 100%) required for SIL 3 shall be 99% or higher. In other words, the undetected dangerous failure rate has to be below 1% using every possible self-diagnosis.

2) Safety design

A high fault detection rate has been achieved by inheriting the method proven in the existing I/O modules for the ProSafe-RS, which compares calculation results using two microprocessors.

In addition, the new modules have achieved high fault-detection capability by appropriately implementing diagnosis functions in each channel: the activation diagnostics, i.e., intentional change in the operating condition of the input circuit, and the comparison among multiple input circuits. Both are effective for detecting failures.

3) Safety verification

We have confirmed the conformity to SIL 3 by the Failure Modes Effects and Diagnostic Analysis (FMEDA). The validity of the analysis was proved by tests on actual equipment, such as fault insertion testing.

MODULE CONFIGURATION AND DIAGNOSIS

■ Module configuration

Figure 3 shows the configuration of the entire temperature input module. The system side is isolated from the channel side and individual channels are isolated. Both microprocessors read the input of each channel and convert it to temperature data. The converted results of the microprocessors are compared to verify the validity of input data and integrity of the microprocessors.

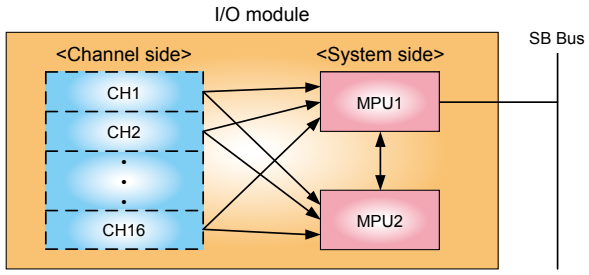

Figure 3 Configuration of entire module

Figure 4 shows the detailed configuration of a channel of the SAT145 and Figure 5 shows that of the SAR145. Each channel is provided with its own input circuit and A/D converter.

■ Diagnosis of input channel

Each module has a diagnosis function appropriate for its channel circuit configuration to maximize the fault detection capability. The input circuit receives a signal from a sensor. It is an analog circuit comprising analog filters, op-amps and others.

a) SAT145

The SAT145 reads a voltage generated in a thermocouple (TC) and converts it to a temperature.

As shown in Figure 4, two input circuits are provided for a channel. Data read from these two input circuits are compared to detect a failure in the input circuits.

b) SAR145

The SAR145 supplies a current to a resistance temperature detector (RTD), reads the produced voltage and converts it to a temperature.

As shown in Figure 5, a channel consists of an input circuit and a current source. The current supplied to the resistance temperature detector is changed intentionally, thereby activating the input circuit, to detect a failure in the circuit.

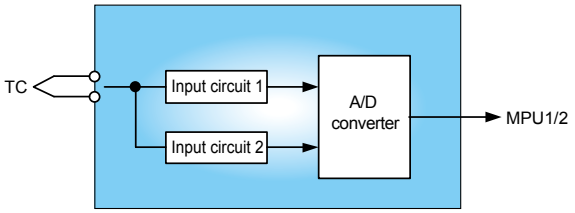

Figure 4 Channel configuration of SAT145

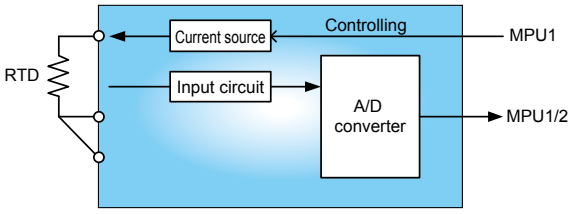

Figure 5 Channel configuration of SAR145

ACHIEVEMENT OF HIGH SPEED RESPONSE

As described above, each channel is provided with its own A/D converter so that all the channels can perform A/D conversion simultaneously, reducing the cycle time of data acquisition and accelerating the input response.

Quick self-diagnosis was implemented to achieve a fault reaction time within three seconds, which is specified in the EN298 (a standard for burner management) and required for a safety instrumented system.

Although the time for most of the self-diagnosis has been successfully reduced by reducing the data acquisition cycle time like that for data input, the time for burnout detection to detect breaking of a wire cannot be reduced by this method alone. We have solved this by the following method.

When a wire in a sensor or field wiring breaks, the PV is intentionally shifted in the predefined upward or downward directions. The host system detects breaking of a wire based on the PV value.

Even when a wire breaks, the input voltage to the I/O module is usually kept unchanged for a while due to stray capacitance among the field wirings or in the I/O module circuits, thus breaking of a wire cannot be detected immediately. To quickly detect burnout, the current for burnout detection is supplied to shift the input voltage intentionally. However, in the CENTUM VP system, it has taken a long time to detect breaking of a wire because of the specific circuit configuration of the temperature input module.

To reduce the time taken to detect breaking of a wire, the following methods are introduced in these new modules.

a) SAT145

For the SAT145, we have increased the burnout detection current to reduce the transition time, thereby reducing the detection time.

The burnout detection current is supplied at a timing when it will not affect the A/D conversion of the input voltage, and this will not affect the PV accuracy.

b) SAR145

The SAR145 is provided with two current sources for the resistance temperature detector, thus eliminating the effect of stray capacitance and enabling faster detection.

The alternate use of the two current sources helps compensate the effect of a relative error of the current sources and minimize the effect on the accuracy.

HIGH AVAILABILITY AND GOOD MAINTAINABILITY

A safety system is required to have high availability and good maintainability as a whole system as well as to meet the safety integrity level and achieve a high-speed response. Therefore, the system must have high noise-resistance capability, and in case of a failure, the causes must be easily identified.

High availability

To improve noise-resistance capability, we have taken both hardware and firmware measures. An appropriate A/D conversion sampling rate is applied to suppress noise especially for data susceptible to the field environment among all acquired data. Transient noise that cannot be suppressed by this measure is reduced by a filter.

A failure in the system or abnormality in the field wiring can be notified while the PV value immediately before the trouble is held. Thus, it is possible to optimize the system behavior in the case of trouble for every application. Especially in a redundant configuration, the PV value can be bumplessly switched in the case of failure, which enables seamless system control operation.

With these measures, we have achieved high availability.

Good maintainability

Prompt and adequate maintenance is required to respond to a failure. Therefore, the system must be able to accurately identify the fault point.

Especially, it is important to distinguish failures caused by external factors such as breaking of a wire in the field wiring, and those caused by internal factors such as a failure of a component in a module. To achieve this, we have added a diagnostic circuit and strengthened the function to identify the causes of failures by acquiring more diagnostic information. Thus, we have enhanced the maintainability.

FEATURES OF COMPACT TERMINAL BOARDS FOR INPUT MODULES

This section introduces the features of the SBT4D and SBR4D compact terminal boards developed for the TC and RTD input modules.

Figure 6 shows an external view of the compact terminal board and Table 2 shows the basic specifications.

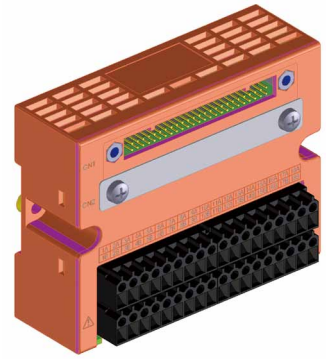

Figure 6 External view of compact terminal board

Table 2 Basic specifications of compact terminal boards

Specification \ Model	SBT4D	SBR4D
Function	TC/mV input with reference junction compensation	RTD input
Number of connection points	16-channel	16-channel
Size	4.3-inch wide (110 × 90 × 35 mm)	4.3-inch wide (110 × 90 × 35 mm)

In order to utilize the limited mounting space, the terminal board is required not only to increase the number of points per unit area but also to freely arrange each module.

The newly developed compact terminal boards save space. A terminal board with the width of 4.3 inches is connected to one I/O module.

These compact terminal boards can be mounted either vertically or horizontally. They can also be mounted on universal DIN rails, flexibly meeting various market needs.

Tables 3 and 4 show the maximum number of input points accommodated in the 19-inch wide space. Compared with those of the AET4D and AER4D terminal boards for temperature input for the CENTUM VP, their mounting efficiency per width of 19 inches is improved by two times for the SBT4D and four times for the SBR4D.

Table 3 Number of connection points of TC/mV input

Specification \ Model	SBT4D	AET4D
Number of connection modules	1 module	2 modules
Number of input points per width of 19 inches	64 channels (max. 4 units)	32 channels (max. 1 unit)

Table 4 Number of connection points of RTD input

Specification \ Model	SBR4D	AER4D
Number of connection modules	1 module	1 module
Number of input points per width of 19 inches	64 channels (max. 4 units)	16 channels (max. 1 unit)

CONCLUSION

This paper has explained the basic specifications and features of the SIL 3-compliant temperature input modules for the ProSafe-RS.

While adding new I/O modules satisfying market needs to the lineup for the ProSafe-RS, we will continue to improve system usability for safety system applications and seek further evolution and advances in safety solutions.

REFERENCES

(1) Yasuhiko Yamashiro, et al., "Hardware Features of the ProSafe-RS," Yokogawa Technical Report English Edition, No. 40, 2005, pp. 47-50
(2) IEC 61508 ed2.0:2010, Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-related Systems.