



Functional safety and explosion protection

New possibilities in automation

by Stephan Schultz

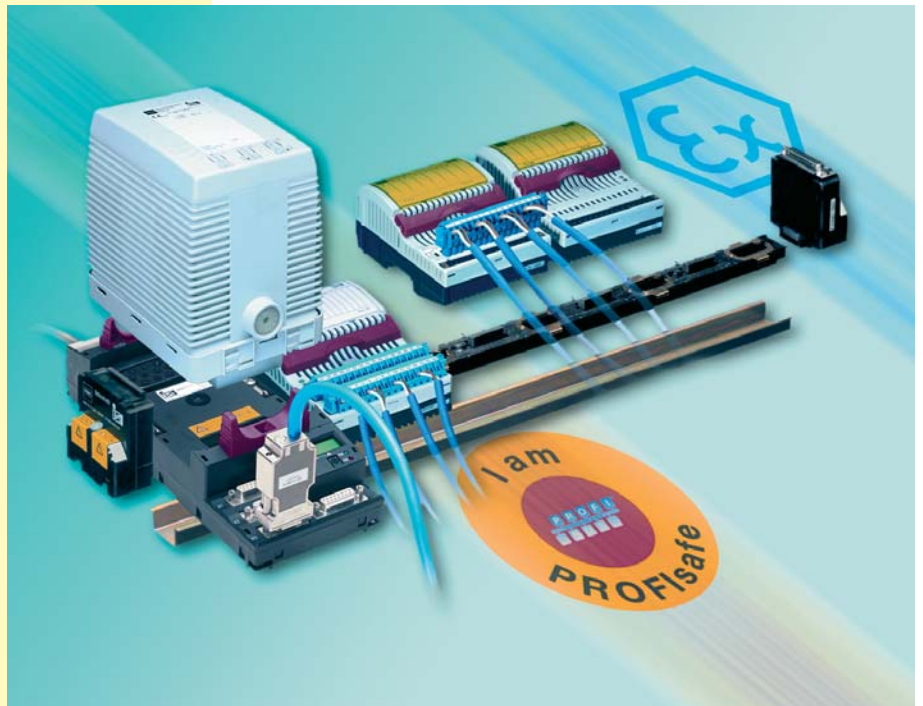


Figure 1: Remote I/O system with ProfiSafe functionality

These days process automation is impossible without components that can be used in combined applications with functional safety in accordance with EN 61508 [1] and EN 61511 [2] (SIL), and explosion protection. The range of solutions that meet these requirements has consequently continuously increased in recent years. In the past discrete isolators were used almost exclusively, for instance, in the ISpac system from R.STAHL. The user was able to draw on a complete range of suitable isolators. However, for a long time suitable bus protocols for usage in Remote I/O and fieldbus systems were not available. This situation has changed dramatically. Today protocols such as ProfiSafe, Foundation Fieldbus

(F-SIF) and other mostly manufacturer-specific protocols are available for bus communication. As a result the door is now open for solutions that range from classic 4...20 mA technology to Remote I/O and to fieldbus technology. For the user the question then arises as to the future, and the advantages and disadvantages of SIL-compliant interface technology.

Isolators – the proven solution

As already mentioned, isolators currently offer the largest range for the integration of field devices that communicate with the aid of intrinsically safe, conventional signals. This area overlaps with the range of sensors and actuators available on the mar-

ket. These are primarily designed for classic transfer signals, such as the 4...20 mA signal.

More than 80 % of the device types in the intrinsically safe ISpac series of isolators are suitable for applications that require functional safety. As a result the standard signals in process automation are largely covered. But this is certainly not a reason to lean back and become complacent. After all better is always the enemy of the good.

In the past direct, complete monitoring of signals on the field side with conventional isolators was only possible to a limited extent for binary signals, e.g. the evaluation of proximity switches with Namur signals and the operation of solenoid valves. Although conventional isolators offer diagnostics for short circuit or open circuit in the field wiring; signalling is however, often limited to an LED indication on the isolator. Due to the I.S. isolator connected in between, the downstream control system technology in the form of a safety PLC could not detect the difference between the ›OFF‹ switch state and a wire break. The only way out: Some devices on the market have separate error messaging contacts that can be evaluated via an additional digital input.

The ISpac series of isolators has, up until now, been based on an integrated solution, that has error messaging using LED, and separate contact and group fault signalling for all variants.

To close the gap mentioned above, new variants of the switching repeater type 9170 LFT and the digital outputs type 9175 LFT were placed on the market. With the new devices, malfunctions from the field side are forwarded directly to the interface, to the PLC or control system. The usage of a separate contact and the related digital input is, as a result, unnecessary. Faults are forwarded reliably and the engineering is simplified.

Safe limits for temperatures and 4...20 mA signals

Along with pure isolating repeaters that convert an intrinsically safe signal into a signal that is not intrinsically safe, the ISpac series of isolators includes a transmitter and a limit switch that make it possible to further process the field signal. This type of device is used particularly in plant

engineering and machine building. Here a need quickly developed among users for devices that provide both explosion protection and functional safety. To address this trend, in the first half of 2009 two old acquaintances from the ISpac series of isolators came onto the market as SIL-compliant devices – the temperature transmitter type 9182 and the transmitter supply unit with limit contacts type 9162.

Both isolators comply with the requirements in accordance with SIL 2 and are therefore suitable for a large number of applications. The temperature transmitter makes it possible to connect intrinsically safe temperature sensors, such as Pt100 or thermocouples, and converts the measured signal into a standard 4...20 mA signal as the interface to the control system. The values measured can be monitored with the aid of limit value contacts using limits set by the user. In the case of the transmitter supply unit with limit value adjustment, the device is primarily used for the supply of the widely used intrinsically safe 2-wire transmitter. Unlike the standard device, this device offers the evaluation of limit values using a contact. Both devices feature a uniquely compact design with a width of only 17.6 mm, which is particularly in de-

mand in plant engineering and mechanical engineering. Installation in Zone 2 and div 2 is possible in both cases. Further isolators are available to planners and users of process plant; these can be used not only for the intrinsically safe integration of field devices into an automation system, but for mastering all the challenges related to functional safety at the same time. A further application is in the area of explosion protection for non-electrical devices, such as pumps or fans with protection by control of ignition source ›b‹ in accordance with EN 13463-6.

Control of ignition source and SIL

The usage of machinery and plant in hazardous areas the requirement on planners and users to meet the regulations for the explosion protection of both electrical and non-electrical equipment. Here the explosion protection for non-electrical equipment and features often represents a difficult challenge. The evaluation of normal operation (failure-free operation), as required in the case of installation in Zone 2, is in general easy to tackle. It must be determined whether, in this case, the related device is generating sparks or has hot surfaces that could result in the ignition of an explosive mixture. →



Figure 2: Compact I.S. transmitter supply unit type 9162 with limit contacts and SIL 2

For usage in hazardous areas in Zone 1 or 0, however, the topic turns out to be significantly more complex, because here fault analysis is required. It must be assessed whether sparks capable of causing ignition or a hot surface can be caused in one of the pieces of equipment as a result of malfunctions during the occurrence of faults.

One possible method of dealing with this issue is the continuous monitoring of such sources of ignition using automation technology. The monitoring device used reacts in critical situations by alarming the operators or placing the installation in the safe state. In the majority of cases this will mean the shut down of the related installation. This technology has been defined as the type of protection ›control of ignition source‹ with the standard EN 13463-6 [3].

This type of monitoring device can comprise in this case, a temperature sensor and temperature transmitter with limit value function. The function is straightforward: If a critical temperature, set previously, is reached, an alarm is signaled or shut down is triggered. Both devices must be explosion protected so that they do not also present any potential sources of ignition.

A further aspect in the safety assessment is the reliability of the protective equipment used. The related question is: What happens if the worst case occurs and the monitoring does not detect it or does not react? For this reason ignition source monitoring must be assessed and tested for compliance with one of the Ignition Prevention Levels (IPL) required in accordance with EN 13463-6 (Table 1). The user is then faced with the next question: Does the automation equipment used need to be certified and the IPLs certified similarly to an equipment category for the explosion protection of electrical equipment by a type examination?

Here the standard EN 13463-6 offers a solution that refers to the subject of functional safety with reference to related existing standards. In practice the following possible ways of performing the evaluation exist: Evaluation of the monitoring equipment based on proven reliability of operation or validation in accordance with EN 61508. This may be, for example, a device designed in accordance with EN 13849 [4] in relation to mechanical engineering, or in

accordance with EN 61508 / 61511 for process automation. Which of the two standards is applied depends primarily on the application area and the probability of how often the safety device must intervene. Here the terms ›high demand‹ and ›low demand‹ are used where the latter is defined by a frequency of ›once per year‹ or ›seldom‹. Machinery and installations in the process industry mostly fall under the ›low demand‹ criterion in which case they must be designed for high availability, and as a result, low failure rates.

For the stated requirements in a monitoring device – detection and monitoring of measured values, explosion-protected design, functional safety for ›low demand‹ applications – limiting value indicators represents an economical and compact solution. The isolator system ISpac from R.STAHL offers, with the temperature transmitter type 9182 and the transmitter supply unit with limit value adjustment type 9162, suitable devices that are particularly suitable for general applications in mechanical and installation engineering, particularly due to their low space requirement, high resistance to vibration and the possibility of installation in Zone 2.

Safe signal transfer with Remote I/O System IS1

Can communication signals based on bus protocols be used for functional safety? The answer is clear: Yes, and it also makes sense from an economical point of view to consider this technology. In the case of conventional automation concepts, safety functions are achieved using time consuming, expensive, and material consuming point-to-point wiring. Therefore, even in the case of large numbers of signals, new approaches offer more convenience and also meet current requirements for functional safety.

In applications specified to SIL 2 in accordance with EN 61508 in a hazardous area it is possible to use, for instance, the Remote I/O System IS1 that in the latest generation offers comprehensive support for the ProfiSafe protocol (Figure 1). An IS1 system provides, on the one hand, analogue input modules making it possible to communicate via ProfiSafe in compliance with SIL 2 and, on the other hand, there is a digital output module making it possible to immediately shut down all outputs with a separate, software-independent intrinsically safe input.

ProfiSafe offers a major advantage: It is based on the Profibus standard or Profinet protocol. The functional safety for ProfiSafe is achieved using additional safety procedures that act on the end points for the communication. These points are in this case the analogue input module for the IS1 system at the one end and the safety PLC at the

Occurrence of potential ignition source	Category 3	Category 2	Category 1
In normal operation	IPL1	IPL2	-
During foreseeable malfunction	not relevant	IPL1	IPL2
During rare malfunction	not relevant	not relevant	IPL1

Table 1: Minimum ignition prevention level (IPL) requirements for an ignition prevention system used to protect Group II equipment acc. EN 13463-6



other end. The communication takes place over Profibus DP. This means that both the process data and the data for the functional safety can be transmitted over one and same connection path. Along with cables and connectors this aspect also includes repeaters, isolating repeaters, and optical fibre isolating repeaters. Additional parallel communication is unnecessary. Other advantages for the user further increase the level of convenience: In the case of SIL requirements the system is, for instance, completely Hart-transparent such that there is also nothing in the way of Hart-based asset management functions. In parallel with the general process control system functions, it is also possible to continuously monitor the state of all equipment to adjust maintenance intervals to actual needs, and to prevent potentially expensive failures in good time.

Conclusion

The application area for the combination of explosion protection and functional safety is growing continuously and with it, the range and variety of the equipment used. There are hardly any limitations that users have to accept and they can use the solution that is suitable for the specific application – whether it be isolators, Remote I/O or fieldbus. In the coming years isolators will continue to dominate in this application area. This technology is widespread and has proven itself in numerous SIL circuits. The range of matching field devices with classic communication signals is also the largest.

The new Remote I/O System IS1 with ProfiSafe functionality represents a successful start to usage for SIL applications. With it, it is possible to exploit the advantages of Remote I/O systems not only for explosion protection, but also in the case of the combination of explosion protection and functional safety. With the implementation of Profi-Safe interfaces in a growing number of safety PLCs in the future, there is nothing in the way of the success of this system.

Last but not least, usage in fieldbus protocols for Foundation Fieldbus is under discussion. Protocols for safety-related signal circuits are already available as are the first products. Correct function has been demonstrated in cross-manufacturer trial installations. However, at the moment there is a limited selection of devices that support this protocol available to the user. R.STAHL is therefore endeavouring to continuously expand the range for this critical application area with innovative and efficient products, true to the motto:

Your safety – our reality.

References

- [1] IEC/EN 61508– Functional safety of electrical/electronic/ programmable electronic safety-related systems
- [2] EN 61511– Functional safety. Safety instrumented systems for the process industry sector
- [3] EN 13463-6 Non-electrical equipment for use in potentially explosive atmospheres – Part 6: Protection by control of ignition source
- [4] EN/ISO 13849 Safety of machinery – Safety related parts of control systems. Part 1: General principles for design, Part 2. Validation