

# Safety Fieldbus Taking Aim at the Process Industries

## Fieldbus in the Process Industries

As end-users discover the benefits of fieldbus with their process automation systems, many are beginning to wonder why they haven't been able to enjoy similar benefits with their safety instrumented systems (SIS). Most customers are reporting that the big benefit of fieldbus is not so much in the upfront installation savings, but in the ongoing operations and maintenance savings made available by advanced diagnostics and asset management tools.

Safety-fieldbus promises advanced diagnostics, as well as capabilities that will make interlock testing easier, a task that must be repeated year after year. Distributed Control System (DCS) users are enjoying these benefits today with standard fieldbus, but ironically, users don't need to test those interlocks with the same frequency as the safety interlocks.

What is preventing customers from using fieldbus technology with their safety systems? This white paper explores the history of safety-fieldbus, the current state of the technology, and speculates on the future impact of safety-fieldbus in the process industries.

process  
SAFETY

**SIEMENS**

### The history of safety-fieldbus

The concept and application of digital communications within a safety system is not new. In fact, safety bus communications have been used in commercial systems since the first programmable safety systems appeared on the market in the late 1980s.

The most common safety-fieldbus found within programmable safety systems is the communications bus between controller modules and I/O modules, often referred to as the system I/O bus. The results of an undiagnosed failure in these communications could be disastrous (e.g., inputs and outputs turning on and off at random). Therefore, the safety integrity level of the entire system requires that these communications occur reliably, timely, and without corruption. Over the years manufacturers have developed a variety of proprietary, safety-certified I/O busses that meet these requirements and have been certified as part of their overall system.

As systems grew larger, it became important to be able to send safety-critical signals between systems. In response, manufacturers developed proprietary communications protocols to support fail-safe, peer-to-peer communications over system-wide communications busses which again were certified as part of the system. Figure 1 depicts a system with both fail-safe, peer-to-peer communications and safety-certified I/O communications.

In the late 1990s, several manufacturers of automation products for the machine safety applications developed safety-certified fieldbusses suitable for use in safety systems up to EN 954-1 Category 4 and SIL 3 applications according to IEC 61508. These busses support a variety of

machine safety sensors such as light curtains, laser scanners, limit switches, and emergency stop pushbuttons. Examples include SafetyBus p, Interbus S, PROFIsafe, AS-i Safety@work, and DeviceNet Safety. Figure 2 shows a typical machine-safety system with integrated safety-fieldbus.

Safety-fieldbus machine safety circuits are less complex and less costly to design, install, and commission due to far fewer cables and connections. Furthermore, they have been shown to improve reliability and lower maintenance costs due to the availability of comprehensive diagnostics. For these reasons the machine automation sector has rapidly adopted safety fieldbus. For example, PROFIBUS International recently announced that the number of PROFIsafe-enabled systems in operation around the world has passed 20,000. In terms of safety devices, this represents nearly 18.8 million nodes.

### Safety communications get approvals for process applications

Why has the process automation sector not adopted safety-fieldbus for process safety applications?

One reason may be that many national and application-specific standards related to the application of safety instrumented systems prohibited the use of bus communications for safety-related signals. For example, clause 7.4.1.3 of ANSI/ISA S84.01-1996 stated "Each individual field device shall have its own dedicated wiring to the system." Another reason may be that clause 4-3.2.3.6 of NFPA 8502-1999 stated, "Signals that initiate mandatory master fuel trips shall be hardwired."

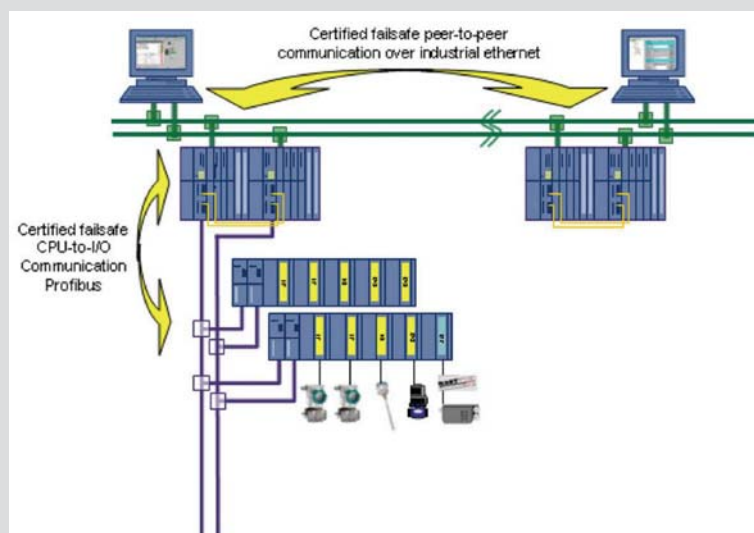


Figure 1: System with fail-safe, peer-to-peer and safety-certified I/O communications



PROFIsafe has been TÜV Certified to IEC 61508 SIL 3 and EN 954-1 Category 4 since 1999. PROFIsafe safety measures are realized in software and simply added as a Safety Layer to the devices on top of the PROFIBUS layer 7 (ISO/OSI model) with no change to the other layers. This means, as shown in Figure 3, that PROFIsafe can be used with PROFINET, PROFIBUS-DP, and PROFIBUS-PA (Process Automation). PROFIBUS-PA is used for the connection of process instruments and supports intrinsic safe transmission and power on the wire. The PROFIsafe profile for PA devices in process automation was approved in December 2004, and certification of PROFIsafe-enabled PROFIBUS PA devices has started. This profile follows the recommendations of NE 97. According to Profibus International, almost 10 percent of the installed base of

PROFIsafe devices is in process automation already, where PROFIsafe is used for tasks such as stopping pumping systems and initiating shut downs.

Safety information is packed in the PROFIBUS telegram frame in addition to the standard data, thus forming the PROFIsafe frame which is passed completely unmodified from a PROFIsafe sender to a PROFIsafe receiver. The safety measures are encapsulated in the communicating devices thus forming a 'black channel' as shown in Figure 4. The advantage of a black channel is that the safety integrity of the communications is media independent – meaning it can work over any transmission system, including wireless.

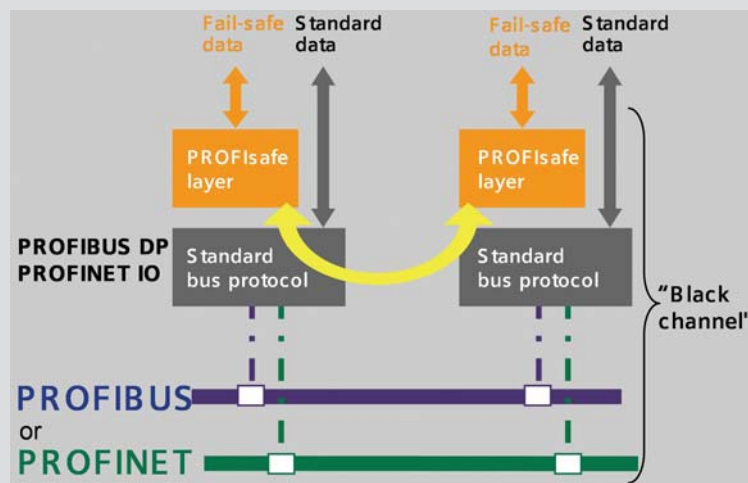


Figure 3: PROFIsafe can be used with PROFINET, PROFIBUS-DP, and PROFIBUS-PA

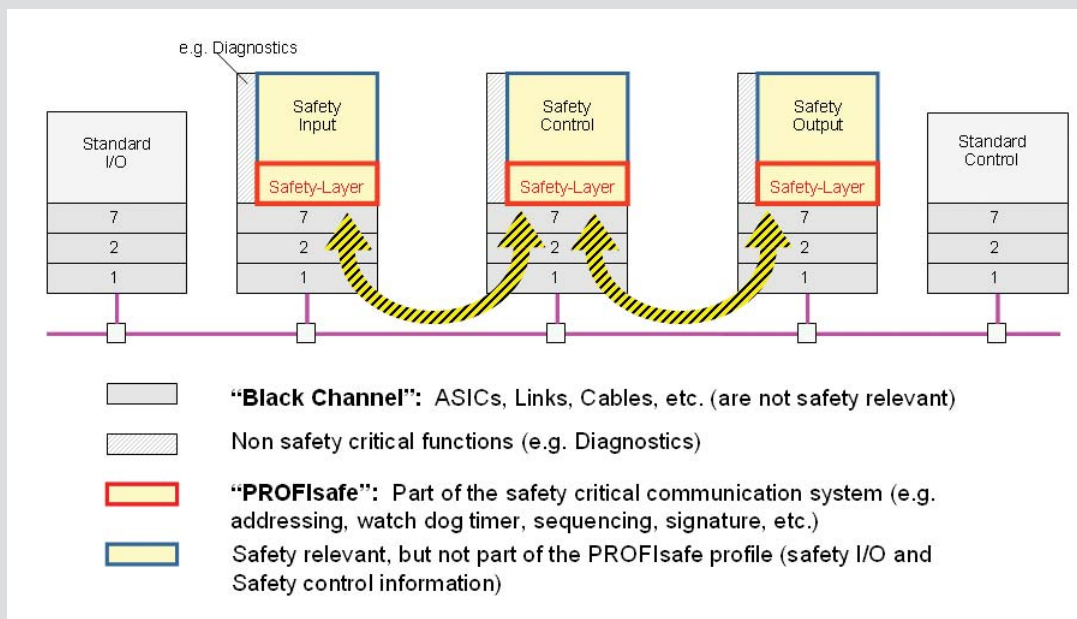


Figure 4: Safety measures are encapsulated in the communicating devices, thus forming a 'black channel,' allowing the network to be media independent.

Another significant benefit of this encapsulation approach, as shown in Figure 5, is that it allows safety and non-safety-related communications to share the same "wire" while still maintaining the necessary degree of functional separation to meet safety requirements.

In addition to PROFIBUS, Foundation Fieldbus announced in January 2006 that TÜV has granted Protocol Type Approval for the Fieldbus Foundation Safety Instrumented Systems (FF-SIS) specifications. The specifications are in

compliance with IEC 61508 standard requirements up to, and including, Safety Integrity Level 3 (SIL 3).

The availability of PROFIsafe and FF-SIS specifications enable manufacturers to build PROFIBUS-PA or Foundation Fieldbus devices in compliance with IEC 61508. Third-party test agencies, such as TÜV and exida.com, will certify that these devices are suitable for use in safety instrumented systems.

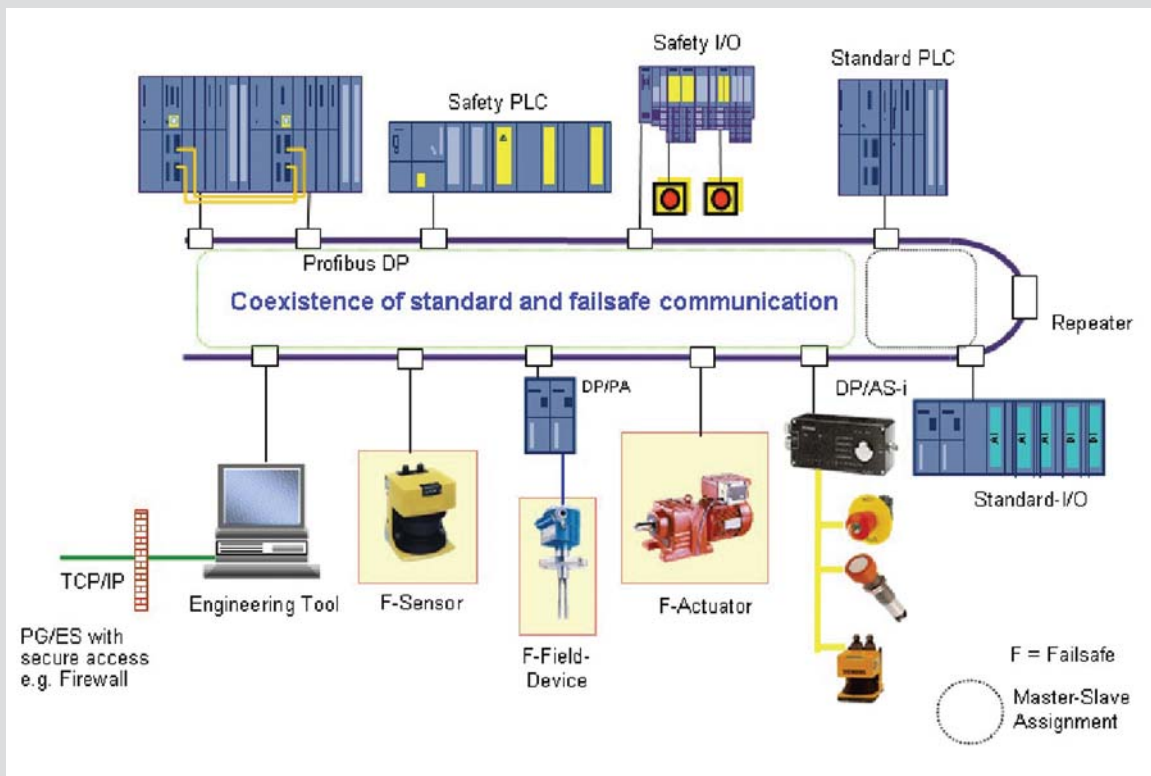


Figure 5: Safety and non-safety-related communications to share the same "wire", reducing installation and commissioning costs.

The first safety-fieldbus-enabled instruments and installation concepts, as shown in Figure 6, were first presented at the Interkama+ Fair in April 2006 and also at the Achema Fair in May 2006. In the U.S., it was introduced at the ISA Fall conference in October 2006 and is now officially available on the market. Of course the

next major step will be the progress of certified field devices (sensors and final control elements) adopting the PROFIsafe protocol in their offerings. While at the time of this paper it is noted the offerings are limited, but there has been a fair amount of investment by some major global manufacturers of devices.

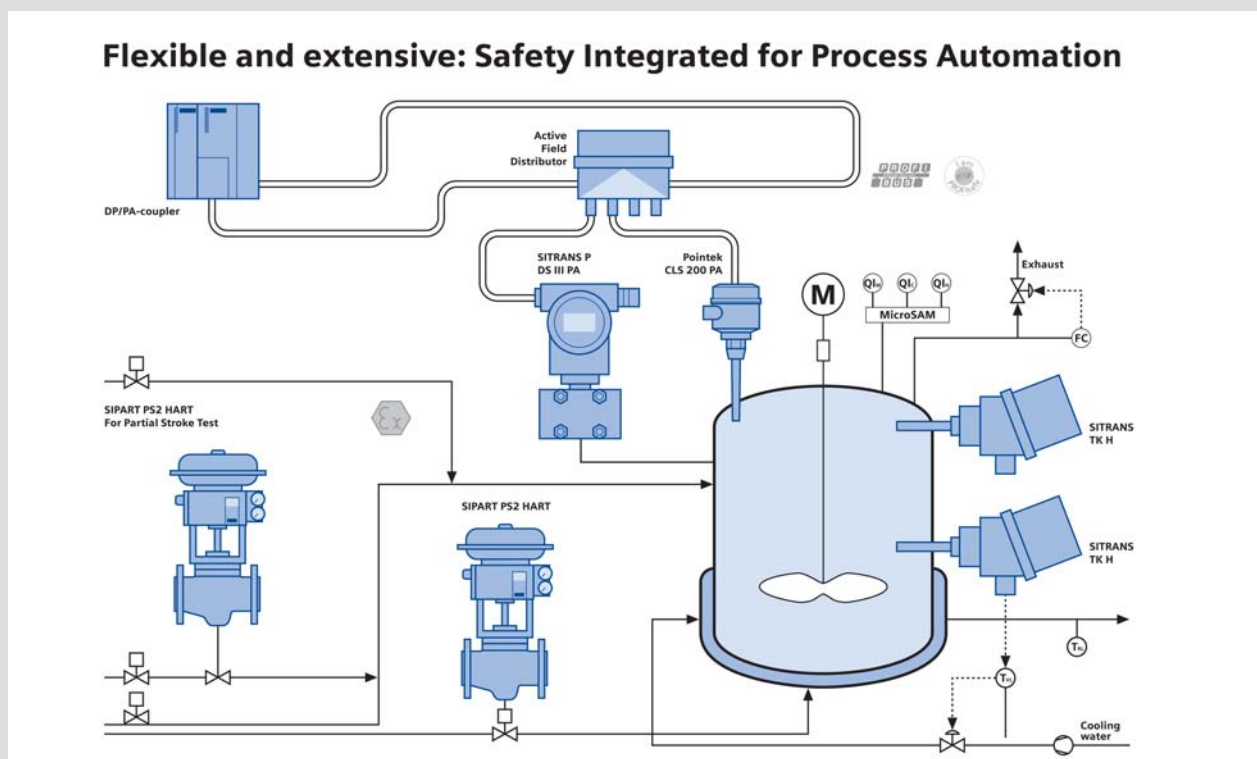


Figure 6: The first safety-fieldbus-enabled instruments shown at Interkama+ Fair in April 2006.

### **Will safety-fieldbus be accepted in the process industries?**

One of the first hurdles that must be overcome, before safety-fieldbus is readily adopted by the process industries, is proving that safety-fieldbus can be as safe and reliable as traditional 4-20 mA systems.

The issue of safety is easier to address because the dangerous failure rates of an IEC 61508 certified safety-fieldbus have been quantified. Therefore, most experts agree that SIF can be designed to provide up to SIL 3 protection, provided they utilize an IEC 61508 certified protocol with a defined PFDavg. This can be modeled by assigning a PFDavg value to the "wire" and associated communication equipment between the instrument and the system when analyzing the SIF. One often overlooked advantage of safety-fieldbus is that the I/O card is no longer necessary, so the card and its associated PFDavg can be eliminated. In fact, the elimination of hardware could actually make a safety-fieldbus SIF safer than a 4-20 mA equivalent.

The issue of availability is more difficult to address because data and modeling tools are not yet available that can analyze the mean time to spurious trip (MTTFs) of both traditional and safety-fieldbus architecture options. However, as the technology emerges, users can expect suppliers of SIL verification software to branch into this area as well. Users can also expect suppliers to develop improved fault-tolerance for fieldbus systems, both standard and safety.

### **The future of safety-fieldbus in the process industries**

One clear message from end-users is that they are looking forward to the ability to integrate their SIS instrumentation into their asset management systems. Continuous access to the condition information in intelligent SIS components will enable analysis of the safety performance of the SIS, helping users avoid spurious trips.

In the absence of an available digital safety-fieldbus for process automation, some end-users have turned to HART® technology as an interim method of achieving this goal. However, since HART is not, and most likely never will be, a safety-certified protocol, the challenge is finding a way to use the HART data in a way that won't interfere or degrade the safety function. In the long run, users will gain the most benefit from being able to use the same basic fieldbus for both their basic process control system and safety instrumented system instrumentation.

The subject of periodic proof testing is one of the first topics to arise in discussions with users about safety-fieldbus and asset management for SIS. This is because while most companies are able to design safety instrumented systems that work fairly well, many of them cannot be tested without extraordinary effort. Smart SIFs with their advanced diagnostics, promise to deliver advanced tools to help users minimize, plan, execute, and document their manual testing. For example, a smart SIF could use predictive methods to alert users when a manual proof test is necessary or provide notification when an opportunity presents itself, due to process conditions, to test an SIF without impacting production. Of course all testing, whether automatic, manual, planned, or unplanned, needs to be documented. Safety-fieldbus enables access to the data and diagnostic information needed for an automatic reporting system.

While it remains to be seen how quickly it will be adopted, there is no question that safety-fieldbus technology is growing. Strong support from the major process fieldbus organizations (Profibus and Foundation Fieldbus) and process automation suppliers, coupled with advantages in reduced installation, maintenance, and testing costs, will certainly propel this technology along the same path as standard fieldbus—perhaps even faster.

## References

1. ANSI/ISA S84.01-1996 "Application of Safety Instrumented Systems for the Process Industries," Instrument Society of America S84.01 Standard, Research Triangle Park, NC, 27709, February 1996.
2. IEC 61511, Part 1 & 2 "Functional Safety: Safety Instrumented Systems for the process industry sector," International Electrotechnical Commission, FDIS Issue, January 2002.
3. IEC-61508 1-7, "Functional Safety of electrical/electronic/programmable electronic safety related systems," International Electrotechnical Commission, International Standard, 1998-12
4. EN 954-1 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design, 1996
5. ARC White Paper, PROFIsafe: Networked Safety for Process and Factory Automation, April 2006
6. ISA SP84 WG 1, "Safety Bus Design Considerations for Process Industry Sector Applications," Draft Technical Report, Oct. 28, 2003.
7. NFPA 85, Boiler and Combustion Systems Hazards Code, 2007

Charles M. Fialkowski  
National Process Safety Manager  
Siemens Energy & Automation, Inc.  
charles.fialkowski@siemens.com

John Cusimano  
Process Automation Market Manager  
Siemens Energy & Automation, Inc.  
john.cusimano@siemens.com