AUGUST 2012

PHOENIX CONTACT
INSPIRING INNOVATIONS

Building a bridge to safety

Automation safety over a non-safe industrial network

By Zachary Stank

Executive summary

In machine automation, one of the primary objectives is the efficient and flexible integration of safety functions. Every automation system is different, but similar safety solutions are effective when comparing equally scaled applications. For small-scale applications, simple-to-configure safety relays are usually better suited, whereas large-scale applications usually employ highly integrated and networked fail-safe PLCs. A new approach encompassing both flexible and easy network communications would bridge these two solutions and support machine builders during the realization of an efficient, networked safety solution without the need for a full fail-safe PLC.

TABLE OF CONTENTS

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-7388 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
E-mail: info@phoenixcon.com • Website: www.phoenixcontact.com

PHOENIX CONTACT
INSPIRING INNOVATIONS

Introduction

Machine and plant engineers must observe functional safety standards, such as ANSI B11.19, EN ISO 13849, and IEC 61508, when they are constructing their equipment. Safety in today's market has come a long way from the simple, single-function safety relays of the past. Now engineers are left to question which is best for the efficient implementation of the prevailing safety requirements in their process: programmable, network-enabled safety controllers or spatially limited, configurable safety relays? This paper will examine the benefits and shortfalls of both safety PLCs and configurable safety relays. It will also examine a new way of handling safety in industrial automation, "SafetyBridge" technology.

Configurable safety relays

Configurable safety relays are similar to hard-wired safety relays, but contain the logical processing power required to configure multiple safety sensors using a single device. The logic configuration is typically done using a screwdriver on a selector dial, a simple on-board configuration screen or basic software configuration. Technological developments also allow these devices to report status back to a master PLC via an RJ45 or fieldbus module connection.

Easy configuration and communication with logical controllers have greatly contributed to the growth of configurable safety relays in hazardous applications. Customers can now have a customizable safety solution that requires less wiring time and can be integrated without special training or advanced classes in programming languages. This can reduce logistics costs, because one part number can be stocked to handle all safety applications for all machines or processes. Even the safety program can be saved and transferred to replacement devices for easy repair.

Even with all these advantages, configurable safety relays still fall short of safety PLCs in distributed safety applications because they cannot communicate over a safe network. In a distributed safety application, safety inputs and outputs are needed throughout the machine.

To accommodate systems like this, there are two options:

1. The installer can run safe I/O wiring across long distances through the machine back to the configurable safety relay, or
2. Each remote safety application can use separate configurable safety relays. This will lead to increased wiring and setup times, as well as inefficient use of configurable safety relay I/Os.

Because of these shortfalls, the only efficient way to connect a distributed safety system is to use a safe PLC and its associated safety protocol.

PHOENIX CONTACT
INSPIRING INNOVATIONS

Programmable safe PLCs

While configurable safety relays replace simple relay solutions at moderate safety I/O counts, the programmable fail-safe PLC replaces the configurable safety relay at higher safe I/O counts. A programmable fail-safe PLC also has significantly more processing power and safety functionality. These specialized PLCs offer better integration, programming resources and a larger amount of usable safety signals for functions like safe motion and robot control. The fail-safe PLC uses a standardized safety network to communicate to safe I/Os on the network. This allows direct control and monitoring of hazards.

Programmable fail-safe PLCs offer increased computing power and functionality, but they also require certain preconditions that can present challenges in designing and certifying a system.

The first and most important precondition is that the PLC being used has a "fail-safe" version. Though safety technology has grown significantly over the past decade, some PLCs do not have a fail-safe version or add-on processor widely available yet.

Machine builders also need to consider that specific customer control requirements may vary region to region, and different PLCs may be specified altogether. Designing systems for multiple PLCs can be time-consuming and expensive, especially considering change control within each system. If a change is made to the overall design, then each individual safety design must also reflect that change. This could lead to multiple versions of multiple controls systems being in the field at the same time.

If considering different solutions for different regions, then it is also worthwhile to consider the safety network and communication protocol each solution requires. A system that uses both PROFIBUS and EtherNet/IP will require communication bus couplers, cabling, and safety I/O for each of those protocols. This increases the need for logistical control and stocking for these parts.

Another concern is customers who use their own "home-grown" machine controls. Though they may be using a standard network, they are not using a standard control software. Safe software tools and runtime technologies are available, but these components are based on safe hardware, which the machine builder must then develop.

The programmable fail-safe PLCs offer a significant advantage in safety functionality. The deep integration of safety logic and communication into the central PLC, however, means strong dependences on single-source providers, increased needs for engineering and logistic control, and inflexibility of components – all potential disadvantages.

PHOENIX CONTACT
INSPIRING INNOVATIONS

Bridging Safely – the distributed configurable safety relay

Today, however, a different approach to distributed safety in an automated industrial network is available. New technology makes it possible to eliminate the strong dependencies between the fail-safe PLC and the safety protocol by achieving two conditions:

1. The safe logic must not be an integrated part of central PLC, but rather decentralized and separated from the standard PLC as in the case of a configurable safety relay.
2. The safe logic must communicate via special protocol over an already installed standard network to read safety input signals from distributed sensors and write safety outputs to actuators.

To reach these conditions, a special logic module can act as a standard network device. This logic module is distributed in the network and handles all safety logic processing on-site. Processing this safety data is done via internally redundant processors, much like a configurable safety relay can process its own safety program. Unlike a configurable safety relay, however, the distributed logic module can communicate to its associated safe input and safe output signals via a special protocol on the standard network.

This safety protocol does not contain any network or PLC-specific dependencies, but operates on the "black channel" principle, like that of a PROFIsafe system. The entire network, including the standard PLC and all infrastructure components located in the data path of the safety signals, is part of the black channel. Safety failure detection is only implemented at the end points of communication, which can detect failures within the black channel with a residual failure probability for the highest safety levels (PL e, Cat 4, SIL 3) **(Figure 1).**

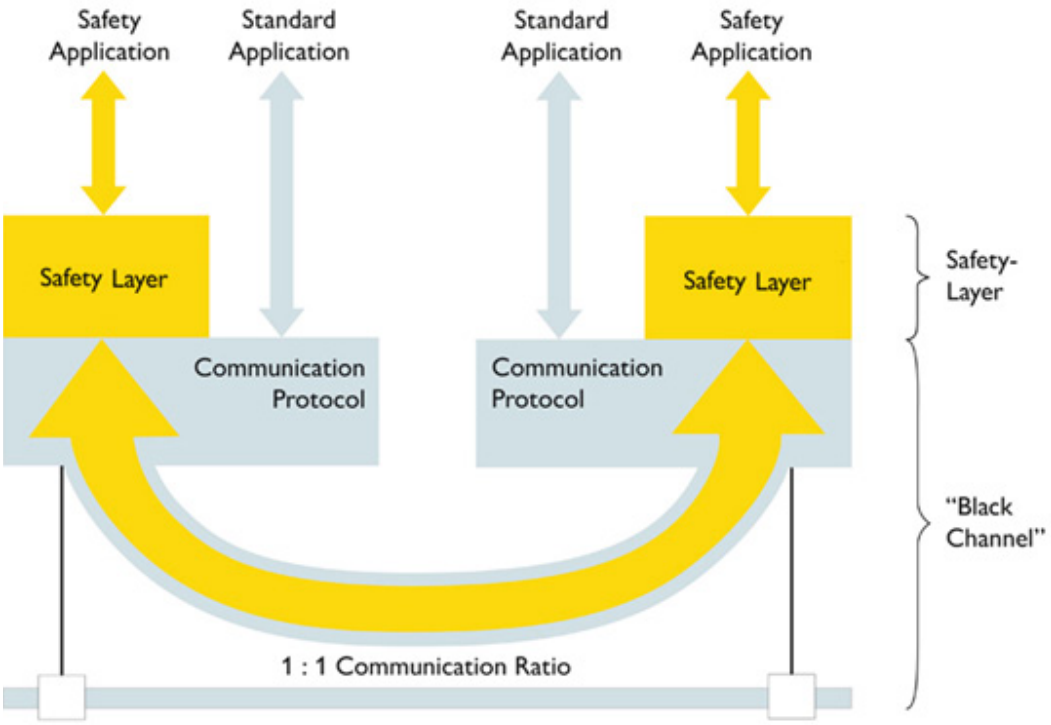

Figure 1 **The black channel principle separates safety from the standard communication protocol, effectively "bridging" the safety application across the network**

BRIDGING SAFELY continued »

Using this communication principle, the safe I/O can be distributed throughout the network, while still communicating back to the same logic module. This creates even more system flexibility. Input and output devices can be wired where they are needed, eliminating the need for long bundled sensor and actuator wire runs throughout the system. Having the standard PLC on the black channel also brings about several advantages:

- The standard PLC has direct readable access to all safe input signals coming from the input devices.
- The standard PLC has direct readable access to all safe output signals, which are mirrored as standard inputs by the safe output devices.
- The standard PLC can directly access all diagnostics information from all distributed safety modules.
- Standard I/O can be used inline with safe I/O modules.

From the user's point of view, the safety logic module and its associated safe I/O modules are realized into one configurable safety relay function responsible for all safety functions. A detailed network view isn't necessary for the configuration of the safety function because of the black channel communication philosophy.

SafetyBridge technology

This new approach combines the advantages of programmable and networked fail-safe PLCs with those of configurable safety relays. Phoenix Contact's new SafetyBridge technology meets these specifications.

SafetyBridge is as flexible as a fail-safe PLC and as easy to handle as a safety relay. The free and simple SAFECONF configuration tool, which is also used to program Phoenix Contact configurable safety relays, is used to create, check, and simulate the safety system on an engineer's computer and is then easily integrated into the standard PLC software.

The SafetyBridge system has been since 2009 by TÜV Rheinland and is usable for safety applications up to Category 4, SIL 3, PL e. It combines the advantages of safe network communication with the simplicity of configurable safety relays. Due to the strict separation of the safety functionality from the standard PLC and network, there is no need for changes on safety relevant configuration and parameters if the standard PLC and network configurations are changed or adapted. This means that an approved safety application remains unchanged and is reusable in various machines with various PLC types.

PHOENIX CONTACT
INSPIRING INNOVATIONS

Conclusion

SafetyBridge technology is a new approach to safe network communication in automation networks. The SafetyBridge system works independently of the relevant network and the standard control system used. Both simply act as a transport medium for safe data packets, which are exchanged between the safe input and safe output modules. The safe inputs and outputs are distributed in the network and do not require a higher-level safety controller or a separate safety bus system. Therefore, instead of having to choose safe networks with safety controllers available accordingly, it is very easy for users to integrate into the systems or technologies they have come to rely on.

SafetyBridge technology is truly the bridge between configurable safety relays and programmable fail-safe PLCs.

Learn more at:
www.phoenixcontact.com/safetybridge.

ABOUT PHOENIX CONTACT

Phoenix Contact develops and manufactures industrial electrical and electronic technology products that power, protect, connect and automate systems and equipment for a wide range of industries. Phoenix Contact GmbH & Co. KG, Blomberg, Germany, operates 50 international subsidiaries, including Phoenix Contact USA in Middletown, Pa.

For more information about Phoenix Contact or its products, visit www.phoenixcontact.com, call technical service at 800-322-3225, or e-mail info@phoenixcon.com.

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-7388 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
E-mail: info@phoenixcon.com • Website: www.phoenixcontact.com