White Paper

PLC® vs. Safety PLC – Fundamental and Significant Differences

Bringing Together Leading Brands in Industrial Automation

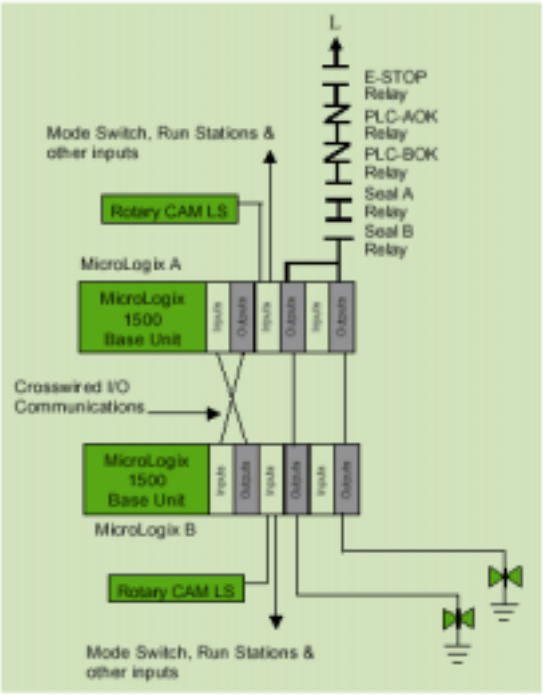
PLC vs. Safety PLC – Fundamental and Significant Differences

Introduction

Safety systems have traditionally required hard wiring and the use of electro-mechanical components, as required by the National Fire Protection Association “Electrical Standard for Industrial Machinery” (NFPA79). Section 9.6.3 states that a Category 0 stop shall only have hard-wired electro-mechanical components and shall not depend on electronic components (hardware or software) or the transmission of commands over a communications network. Likewise, a Category 1 stop shall be accomplished by electro-mechanical means. Although this requirement is stipulated for emergency stop circuits, both redundant standard PLCs and safety PLCs have begun replacing the other safety-related hard-wired circuits.

For example, there are many applications where the Programmable Logic Controller (PLC®) has been used to control equipment, including the safety-related parts of the control system. Typically, standard PLC controllers used in safety applications are configured in pairs. The redundant controller is used to support a safe and orderly shutdown in the event the primary controller fails. In addition to multiple controllers, safety applications designed using standard PLCs utilize additional I/O inputs to monitor safety system output signals, and more outputs to generate test pulses for the safety system’s input modules. Also, applications designed around standard PLCs require custom software to monitor, control and diagnose the safety system. To summarize, designing safety systems around standard controllers requires additional engineering time, I/O hardware, and wiring to support the safety portion of the application, in addition to the hardware and software required to run the application.

Figure 1



Allen-Bradley 6556 MicroLogix Clutch/Brake Controller for Mechanical Stamping Presses

Redundant PLC-based packages are available that drastically reduce engineering effort and eliminate the controller certification phase by providing complete software/hardware kits certified for use in press control applications. For example, Rockwell Automation’s Clutch/Brake control package based on redundant MicroLogix™ processors has been certified by TÜV as "suitable as a control and monitoring system for mechanical presses according to ANSI B11.1-1988 and EN 692-1996." Using two PLCs provides redundancy to improve the safety integrity of the system. The inputs and outputs are cross-wired to provide self-monitoring and checking of the operation as the block diagram in Figure 1 shows.

These concepts improve the safety integrity of the system as compared to the use of a single PLC. The dual, cross-wired PLC configuration has demonstrated that electronic components can provide an acceptable integrity level for safety systems.

In 1998, the first part of a seven-part international standard was published to define the requirements for programmable electronic systems used in the safety related parts of controls systems. This standard is known as IEC 61508, "Functional safety of electrical/electronic/programmable electronic safety-related systems". This seven part standard is driving the direction for future safety PLC developments.

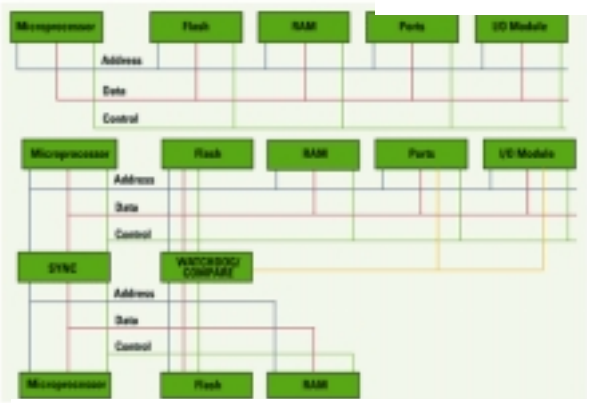
Basic Design Differences

There are three fundamental differences between a safety PLC and a standard PLC in terms of architecture, inputs, and outputs.

Architecture

Figure 2 shows a block diagram comparison of the two architectures. A PLC has one microprocessor which executes the program, a Flasuh area which stores the program, RAM for making calculations, ports for communications and I/O to detect and control the machine. In contrast, a safety PLC has redundant microprocessors, Flash and RAM that are continuously monitored by a watchdog circuit and a synchronous detection circuit.

Figure 2

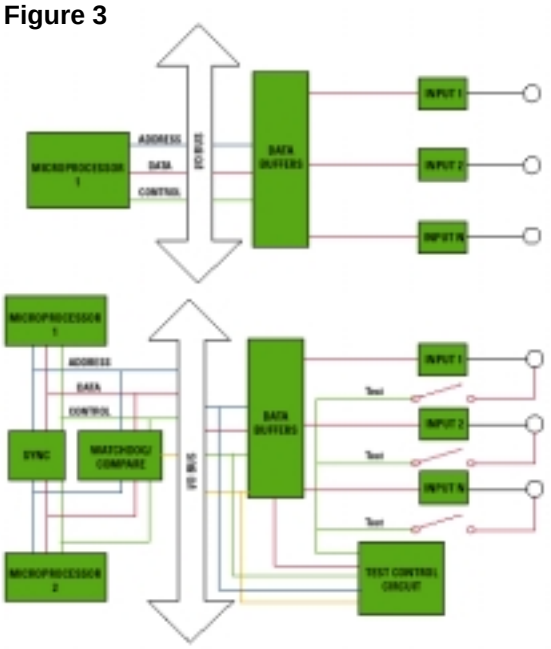


Architectural Comparisons

Inputs

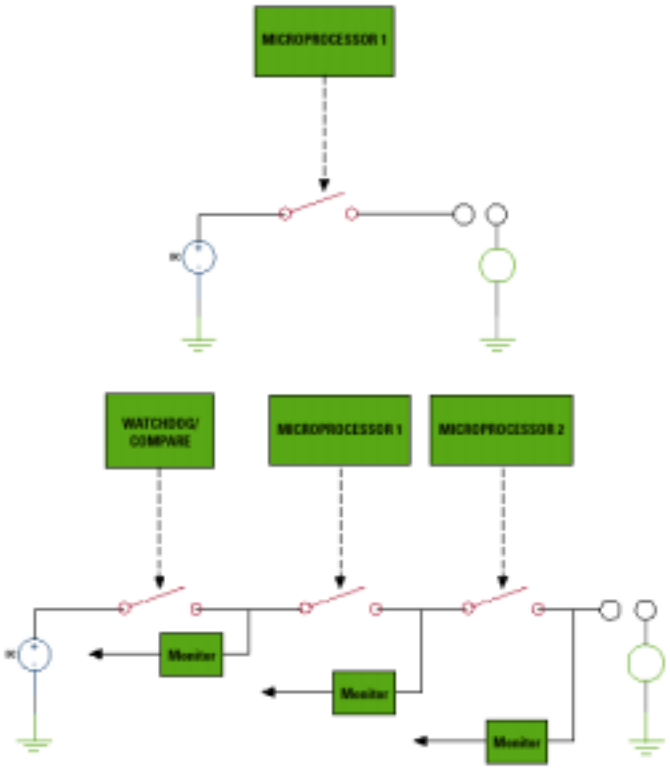
Figure 3 compares a PLC input to a safety PLC input. Standard PLC inputs provide no internal means for testing the functionality of the input circuitry. By contrast, Safety PLCs have an internal 'output' circuit associated with each input for the purpose of 'exercising' the input circuitry. Inputs are driven both high and low for very short cycles during runtime to verify their functionality.

Figure 3



Input Circuit Comparison

Figure 4



Output Circuit Comparison

Outputs

Figure 4 compares the digital output circuitry of a PLC to a safety PLC. The PLC has one output switching device, whereas a safety PLC digital output logic circuit contains a test point after each of two safety switches located behind the output driver and a third test point downstream of the output driver. Each of the two safety switches is controlled by a unique microprocessor. If a failure is detected at either of the two safety switches due to switch or microprocessor failure, or at the test point downstream from the output driver, the operating system of a safety PLC will automatically acknowledge system failure. At that time, a safety PLC will default to a known state on its own, facilitating an orderly equipment shutdown.

Certification

Several safety validation bodies are driving the design parameters behind safety controllers. TÜV from Germany, Factory Mutual (FM) from the United States, and Health and Safety Executive (HSE) from the United Kingdom each test for adherence to the stringent standards safety PLCs must meet. For example, TÜV typically tests products against IEC 61508, a standard that defines Safety Integrity Levels (SILs) 1 through 4. Safety PLCs are suited for applications at SIL 2 and SIL 3 where they can be certified for use in most common safety applications. SIL 4 addresses applications beyond standard industrial safety; it defines controller requirements for nuclear reactors, flight system (fly-by-wire) control, or any number of applications whose failure would be catastrophic.

International and European standards finding their way into OSHA and ANSI standards in the United States are IEC 61508 and EN 954-1. IEC 61508 provides an exacting definition for functional safety in programmable electronic systems. EN 954-1 outlines the requirements for the safety-critical parts of control systems in machinery.

Application-specific standards for robotic devices are provided by ANSI-RIA15.06. Control requirements for mechanical stamping presses and other machines are defined in the ANSI-B11 series of standards.

Although there are some differences between the standards supported by each of the primary validation bodies, each takes a total system approach. Specifications for entire safety control systems take software, hardware, and operating systems into consideration. Some of these standards take the additional step of providing guidelines for specific applications.

When to Utilize Safety PLCs

The redundancy and self-checking features of safety PLCs come with a price tag. Safety PLCs cost approximately 25% to 30% more than their standard PLC counterparts. However, they do provide a significant savings when compared to the total cost of dual cross-wired PLCs. Likewise, this cost differential, when compared with safety relay-based systems, is offset by reduced wiring costs and panel space as well as improved flexibility.

Developers should be aware that specific control architectures based on standard PLCs have been certified by safety governing bodies for use in specific applications. In specific instances, it may prove more cost effective to use the certified package versus taking a new control architecture through the certification process. Also, end users need to evaluate the additional training, stocking and maintenance costs incurred by implementing a new system as opposed to the cost of creating a safety system using the standard hardware and software with which they are familiar.

Scope

This article highlights some of the fundamental differences between PLCs and safety PLCs. Other differences which aren't elaborated upon in this article include the use of power supplies designed specifically for use in safety control systems and redundant backplane circuitry between the controller and I/O modules.

Conclusion

While safety PLCs, standard PLCs and safety relays all have their niche, final selection of the appropriate control system will be determined by a variety of factors. Engineers developing safety systems should evaluate each control approach in an effort to determine the appropriate solution for their specific application. Whatever control architecture is chosen when implementing safety systems, it is important to work with a control supplier that can supply and support multiple approaches.

The GuardPLC™ controller is a new safety rated PLC from Rockwell Automation. It is designed to meet the requirements of this standard.

Special thanks to Frank Watkins and Steve Dukich for their expertise and assistance with this white paper.

www.rockwellautomation.com

Corporate Headquarters
Rockwell Automation, 777 East Wisconsin Avenue, Suite 1400, Milwaukee, WI, 53202-5302 USA, Tel: (1) 414.212.5200, Fax: (1) 414.212.5201

Headquarters for Allen-Bradley Products, Rockwell Software Products and Global Manufacturing Solutions
Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe: Rockwell Automation SA/NV, Vorstlaan/Boulevard du Souverain 36-BP 3A/B, 1170 Brussels, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, 27/F Citicorp Centre, 18 Whitfield Road, Causeway Bay, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Headquarters for Dodge and Reliance Electric Products
Americas: Rockwell Automation, 6040 Ponders Court, Greenville, SC 29615-4617 USA, Tel: (1) 864.297.4800, Fax: (1) 864.281.2433

Publication SAFETY-WP002A-EN-E — March 2002