Integrated Machine Safety Comes of Age

Lowering costs, decreasing downtime, and speeding time to market

In the 1970s, machine builders began to change the way they wired machines, replacing relays with automatic sequencers – known today as PLC (programmable logic controllers). However, regulators excluded PLCs from playing a role in machine safety. Little attention was paid to safety by end users. Machine builders addressed safety as an afterthought.

Today, however, machine builders and end users are enjoying the benefits of new machine guarding technologies endorsed by international safety standards. From the most sophisticated manufacturing operation, to the simplest relay based system, machine manufacturers and end users now have economical and effective choices to enhance machine safety.

The latest options include integrated, networked safety systems utilizing reliable safety PLC technology. Designed and built according to IEC guidelines and tested by nationally recognized testing laboratories, such as TUV and UL, Siemens SIMATIC safety PLCs, buses, I/O, and other components are replacing traditional hardwiring on machines. No longer is it necessary to attach steel cables to operators' wrists to keep hands out of machines pinch points, for example. Safety is now automatic.

The most important benefit of integrated, automated machine safety is enhanced operator protection. According to one study, machine related injuries are among the most common in the workplace. The fatality rate from machine related accidents were second only to motor-vehicle-related accidents and recorded higher fatality rates than homicides, falls, and electrocutions according to the National Institute for Occupational Safety and Health (NIOSH).

In addition to protecting machine operators, machine builders and end users alike are realizing other benefits to enhancing machine safety, including:

- Lower cost of controls
- Speed time to market
- Decrease machine downtime
- Reduced litigation

Incorporating safety into machine designs begins by understanding recent changes in international safety standards and regulations. Then, it is simply a matter of applying the appropriate safety options to meet these requirements. Finally, as these options are considered, it is important not to overlook calculating total lifecycle costs into the decision making process.

Safety Standards Drive Changes

Recent developments to machine safety are changes in standards from the National Fire Protection Agency (NFPA). In the fall of 2002, NFPA 79 was republished providing application guidance for failsafe, or safety rated, PLCs and safety rated busses to be used in functional safety applications.

It also established requirements for a risk analysis to be performed on all machinery and described e-stops as a part of the safety design. All safety rated devices could thus be installed on a safety rated bus.

The code text changes appear as:

Original NFPA 79 1997 --Where a Category 0 stop is used for the emergency stop function, it shall have only hardwired electromechanical components. In addition, its operation shall not depend on electronic logic (hardware or software).

New NFPA 79 2002 -- Wording allows PLC Use in Safety-Related Functions:

11.3.4 Use in Safety-Related Functions. Software and firmware-based controllers to be used in safety-related functions shall be listed for such use.

Annex to NFPA 79 2002, A.11.3.4 IEC 61508 -- Provides requirements for the design of software and firmware based controllers for use in control systems performing safety-related functions.

These changes allow manufacturers to develop powerful new solutions that replace hardwired relays with PLC safety circuits with built-in safety functionality. This built-in safety greatly reduces cost, requires less time to implement, and increases machine uptime.

In 2004, ANSI B11 TR4-2004 was approved. It provides application guidance for safety rated hardware and software based devices in functional safety applications. These and other standards reference IEC 61508, 62061, 60204-1, and EN 954-1, many requiring a formalized risk analysis to establish risk reduction methodologies.

The risk analysis reference formalizes what has been a requirement all along, but wasn’t an absolute standard. It was once assumed that people would follow due diligence and engineering principles to provide a safe workplace, as required by OSHA.

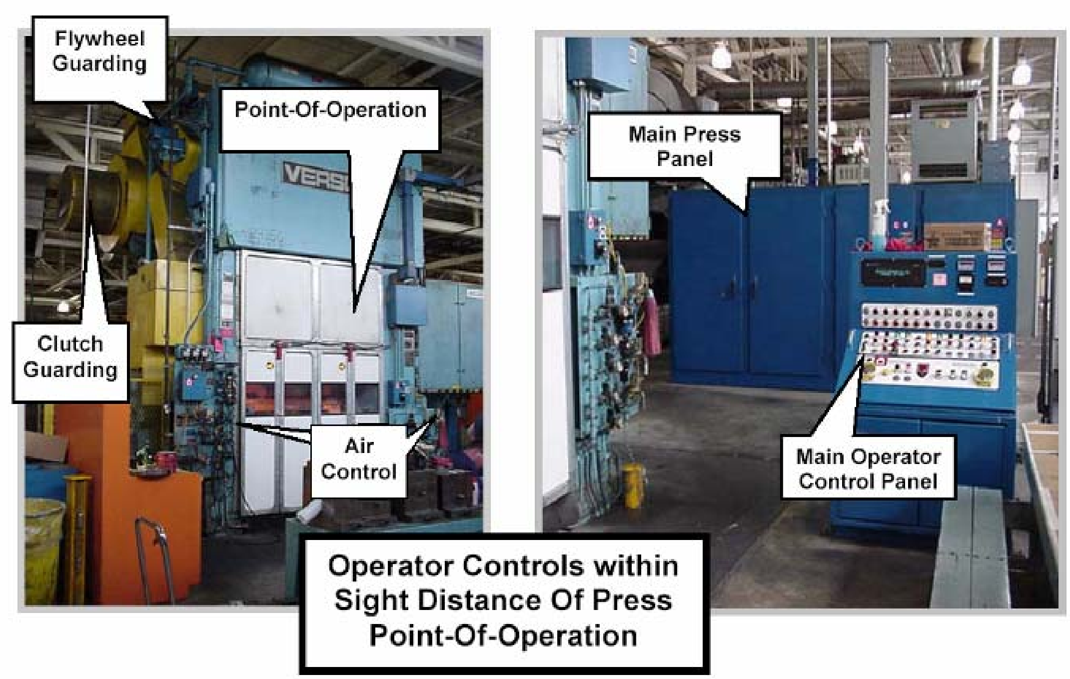
Now, a formal process must be followed to evaluate risk potentials throughout all modes and operations of a given machine. This process identifies all risk levels that could injure the operator, maintenance personnel, or even individuals walking past a machine. The person conducting the risk assessment must be trained and understand how machinery operation and production is affected by applicable codes and standards.

<u>The four most important factors taken into account during a risk assessment are:</u>

- Severity of foreseeable injuries
- Probability of occurrence
- Frequency of exposure to hazard
- A list of actions required to meet applicable standards (showing appropriate actions to ensure personnel safety)

By evaluating the machine and the environment around it for safety, a risk assessment lets a manufacturer know what needs to be changed to meet applicable codes. It also significantly lowers the risk to machine operators. If an injury occurs, OSHA will ask what the employer has done to make the area safe. A risk assessment shows the employer has taken steps to understand and correct any associated standard violations.

Looking beyond the factory doors and into the global marketplace, OEMs and machine builders familiar with the risk assessment regulations are expanding sales internationally. All machines shipped to Europe are required to provide complete risk assessment documentation



Risk assessments review all mechanical and electrical components of the machine

Safety Solution Options

The right safety strategy can provide a competitive advantage for the machine builder and manufacturer. The recent changes in safety standards mentioned above have opened the door to new solutions that would not have been permitted under the old rules. Choosing the right option can result in a quicker time-to-market with higher product throughput, and a lower total cost of ownership for safety systems, improving both overall equipment effectiveness (OEE), and return on assets (ROA).

Here are four safety options to consider:

Dedicated Safety Relays—The mainstay of safety circuits for decades, dedicated safety relays continue to be used even today. However, while dedicated safety relays may help meet machine safety standards, the overall costs may outweigh the benefits. These relays significantly limit the ability to monitor and troubleshoot machines. For example, a single machine might incorporate 20 emergency-stop buttons—any one of which must shut it down. Traditionally, e-stops are wired in series to decrease the cost of wiring. The challenge comes when a fault occurs and the operator needs to detect the problem. Using this conventional wiring method, many manufacturers often spend 10-20 minutes diagnosing the problem on the machine.

Also, many operators using machines that rely on this configuration often bypass the safety relays with short pieces of wire so that opening the cage door or breaking the beam on the light curtain will not shut down the machine. They claim this action increases efficiency while minimizing downtime because a maintenance person can get to the machine much more quickly and work on it even if it is still running. Despite the perceived advantages of this bypass process, this “jumpering” produces a dangerous condition and a major safety violation. Newer solutions cannot be jumpered in this manner, and therefore provide an extra level of safety.

Networked Safety Relays--These devices can significantly lower the cost of single- and multi-zone applications by allowing one device to be wired to the entire safety circuit -- networking to each individual device. This configuration significantly lowers the cost of wiring, allows individual safety incidents to be monitored, and permits fast troubleshooting. It is also a very good solution for safety systems with relatively low complexity (controlling two or three safety zones, for example).

However, networked safety relays may not be the best solution for highly complex systems where minimizing control programming is required.

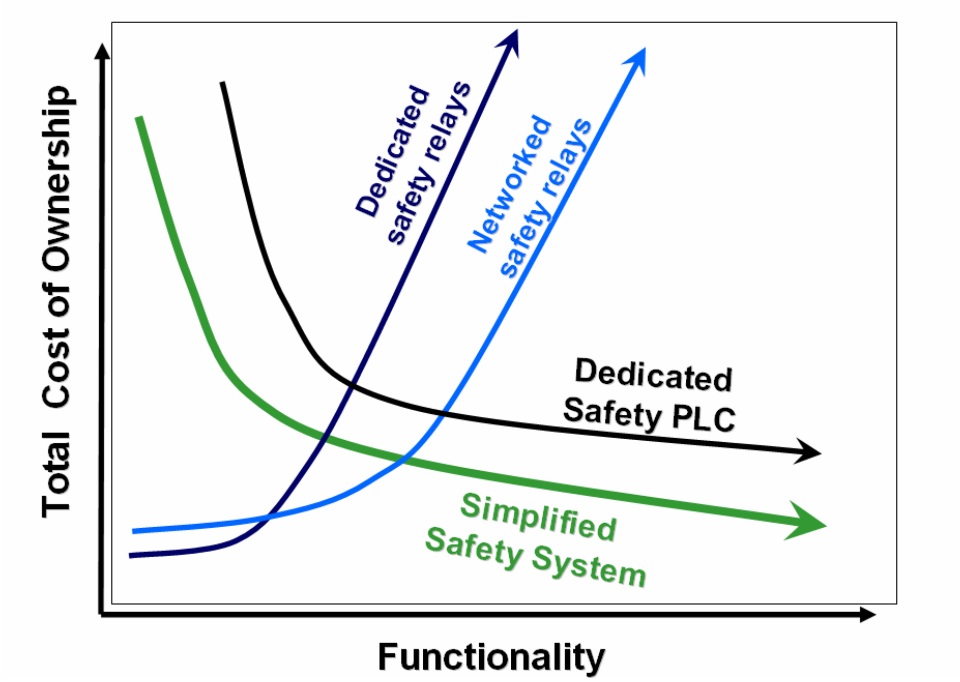
Dedicated Safety PLC—When a PLC is already in place and controlling a machine, a safety PLC may be added to the system. This solution can add greater monitoring capabilities to the system if the safety PLC is networked to the control PLC and it allows use of the existing PLC program. Challenges with this solution, however, are two fold: The added safety PLC is a new expense to the system and introduces another programming language to learn, implement, troubleshoot, and maintain.

Integrated, Simplified Safety System—Combining the functionality of a control system and a safety system into one PLC allows manufacturers to greatly reduce life cycle costs on a machine.

Siemens SIMATIC S7 PLC, for example, combines integrated control and safety into one controller. Implemented in more than 10,000 applications, manufacturers have saved millions in overall costs. This type of integrated safety system allows all data to flow to the HMI (human machine interface) for fast and easy troubleshooting. This approach simplifies machine control and safety system coordination -- from design, to installation, to troubleshooting.

Design and implementation are simplified by using the same programming language for control and safety circuits. Wiring is simplified by using safety networks to monitor and/or control each device on the safety circuit. Troubleshooting is often cut by 60-80% since each networked safety device communicates via the same HMI as the rest of the control system. These advantages significantly reduce downtime and the costs associated with failures.

An integrated safety system also makes it nearly impossible to bypass the safety circuit by jumpering out a safety device, including a door switch or light curtain.



Functionality and total cost of ownership are dramatically lowered with dedicated safety PLCs and simplified safety systems versus the use of dedicated or networked safety relays. Source: Siemens.

Integrated Safety Saves Life Cycle Costs

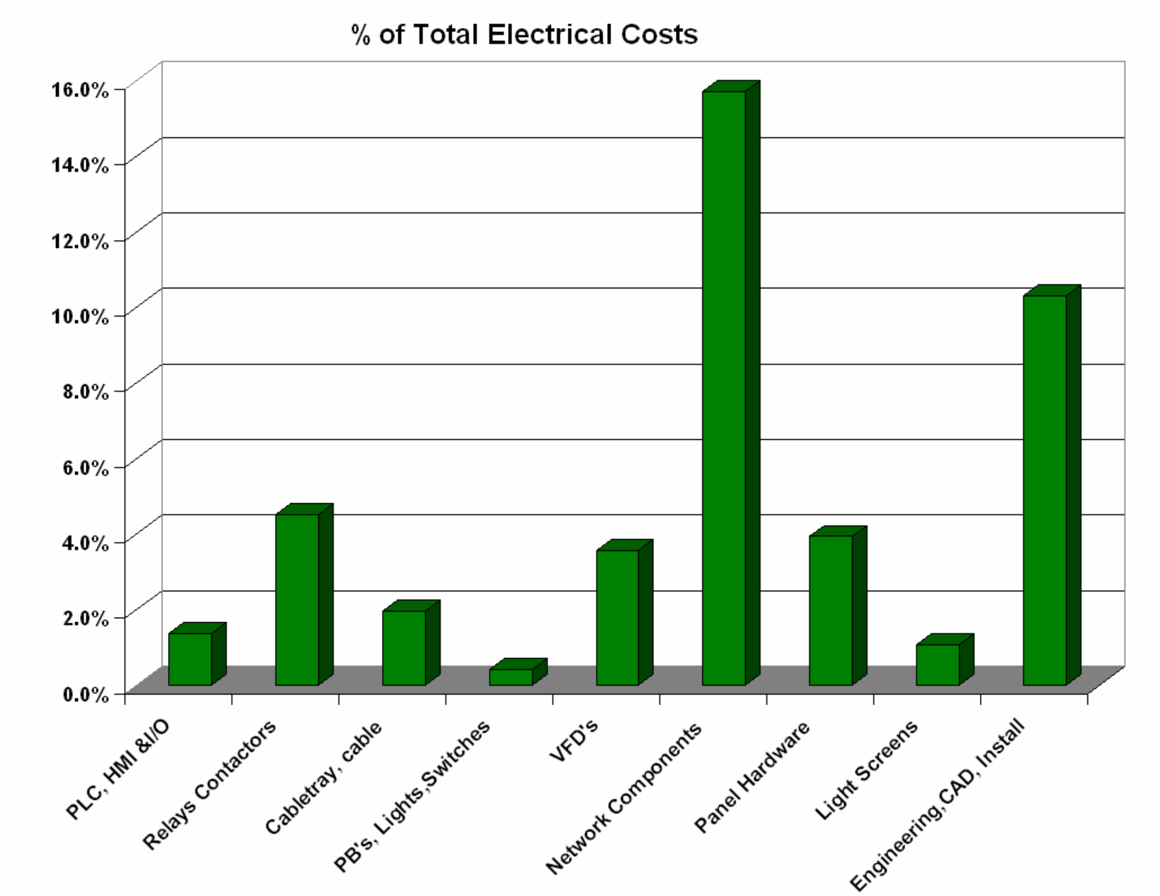
When considering the right safety option for the application, take into account the entire life cycle cost of the product or system, not just the purchase price.

- **Design—**How much design time can be saved by implementing networked safety and control into one system? Mechanical, electrical, and programming issues are greatly simplified with a single PLC.
- **Wiring—**Installing an integrated system costs far less than hardwiring. By transporting safety and regular production data on a single network (such as ASI or Profibus), this architecture requires the use of only one cable instead of hundreds or thousands of wires.

According to the electrical project engineer for a packaging machine manufacturer, "A more complex, discrete wired machine can take six electricians more than 368 hours to wire and start up. Integrating distributed I/O and safety I/O eliminates manufacturing redundancy and reduces complexity. Two electricians can wire up that version of the system in just 96 hours."

In addition, manufacturers can now integrate electronic and programmable safety systems directly into servo drives, permitting axis movement at safe speeds while an operator is in the working envelope. This change reduces the number of cables and connections further, again reducing safety system complexity and lowering design, commissioning, and installation costs.

- **Production efficiencies.** If a manufacturer's downtime costs $10,000 an hour, it does not take long to justify a low-cost, integrated system that saves 30 minutes each time a safety circuit is activated.



Overall cost savings on a standard OEM machine

In a recent study, significant savings were found when new and old methods of safety and automation system implementation were compared. The study explored five key aspects of the overall costs; hardware design, software design, hardware costs, build and assembly, and field wiring. As can be seen in the chart above, savings were found in every major area delivering over 42% net savings for the automation and safety implementation on each machine built. Source: Siemens.

Conclusion

Unless the machine employs only one or two safety relays, a networked safety system utilizing a single PLC, will deliver far greater benefits than traditional, hardwired methods. Improved machine safety, reduced time to market, and lowered lifetime cost may be achieved by working with an experienced automation and safety advisor.

Siemens, for example, has implemented more than 10,000 safety PLCs and 360,000 safety network nodes worldwide. Siemens engineers understand the changes in international safety standards and regulations. They have the experience to apply the appropriate safety solution based on the application.

For more log on to http://automation.usa.siemens.com/automat/product/safe/auov.html

# # #

Safety Success Stories

Michelin Truck Wheels

Michelin manufacturers about 600,000 steel truck wheels per year in one facility. Each wheel consists of a "nave" that attaches to the truck hub and a "rim" that carries the tire. The company manufacturers each piece separately from steel coils. The piece is shaped, pressed, seamed, welded, tested, and painted. The plant includes three production lines for naves and one for rims. The company expects to double production levels over the next several years.

Michelin's corporate policy demands maximum safety at work, regardless of production levels. The company strives for fewer than five lost-time accidents per year in each of its factories. After a careful risk assessment, the company decided to implement a Safety Category 4 solution with a Siemens SIMATIC S7 controller to the line comprising three metal-forming systems.

Accomplishing the company's objectives meant establishing three protection areas—integrating 24 protective doors, 12 safety modules, and 30 motors into one factory-wide safety network. A conventional design—fixed wiring, safety controller, and a separate safety bus—would have presented considerable challenges for a project involving almost 60 safety relays. Siemens presented a viable alternative with its SIMATIC fail-safe PLCs. The head of electrical planning for the Michelin wheels division was particularly impressed by the solution's comprehensive fault diagnosis capabilities and flexibility.

The heart of the new safety design was built in parallel with the existing control without shutting the line down, an arrangement that saved both time and money. The safety network configuration used in Michelin's approach allows implementation of both standard and safety-oriented operations side-by-side. In this plant however, the processor carries only safety-related signals. If a fault occurs, the safety control switches the plant or plant module to a safe state. The safety devices connect to the CPU through a single bus (PROFIBUS) rather than through myriad individual wires. Near the protective equipment (protective doors, press safety modules) are small control boxes with fail-safe signal modules. These modules transmit local signals along the conventional bus cable to the switch-room command center where large contactors shut down primary power. The system guarantees communication via the PROFIsafe protocol profile developed by PROFIBUS International, which is designed to meet the most stringent safety requirements.

Mechanical interlocks on the protective doors and additional control-program checks eliminate inadvertent production interruptions. A bus coupling provides a necessary link to the line control for proper coordination between safety equipment and production processes.
With old-style hard-wired safety relays, even minor modifications incurred significant costs, and larger changes often proved prohibitively expensive. Michelin found that merely connecting the protection devices via PROFIBUS drastically reduced that effort and its associated costs. Machine operators also appreciate the transparent enclosures and the easy-to-use touch-panel on the new safety equipment.

Opel

In a project that provided an effective safety system for a new robot welding line while also replacing an existing traditional safety system, Opel recently completed its first automation and safety installation in its body shop based on safety integration technology. Originally, potentially dangerous machines and conveyance systems were set in cages and behind light curtains with safety switches and emergency stops, but all were still controlled by relay connections. Any new functions the company installed had to meet current safety standards and provide adequate functionality. The system also had to provide detailed and reliable fault reporting, as well as offer expandability to meet future needs and maintain reasonable life-cycle costs.

While shopping for the new system, Opel compared a safety system with separate PLCs for control and safety relays with a true fail-safe PLC system. The nature and configuration of the Opel plant accentuated the advantages of the fail-safe approach. The assembly process comprises preparation cells in continuous operation, as well as a typical supply system that requires small, decentralized automation units. The system selected boasts greater flexibility, shorter cables, and the advantages of a network architecture, accurately reporting safety failures down to the last wire. The time saved during installation permitted additional time to conduct testing.

Opel was also looking for a comprehensive fault-reporting capability from its new safety system that would generate fault reports on the human-machine interface (HMI) panels using only the software supplied with the systems. Using this system, engineers found they could implement other forms of safety intelligence as well, such as by controlling “muting” (programmed and safe suppression of safety functions during routine production) using light curtains.

The fail-safe PLC controls all of the safety measures in the plant—including emergency stop chords, emergency stop buttons, light screens with or without muting functions, screens for lift apertures, classical safety cages with safety catches—and communicates with the ordinary control systems through PROFIBUS couplers.

Opel's team reports that the system start-up proceeded smoothly with no problems. In fact, it worked so well that they promptly forgot about it.

SEZ Group

Facing an average price erosion of 25 to 30% per year and shorter innovation cycles, the SEZ group—a leading supplier of wet-surface preparation equipment for the semiconductor-wafer manufacturing industry was looking for a way to reduce equipment costs to its customers while increasing productivity. The company chose to integrate Siemens' SIMATIC fail-safe controllers into its new 300 mm immersion tools to meet these goals.

As a result, SEZ avoided the expense and complications of implementing separate safety and system functions. The SIMATIC system can switch to or remain in a safe condition when a fault occurs. All communications between the central controller and the I/O are performed through the PROFIBUS DP and PROFIsafe profile, which form a single network system. The equipment's architecture requires safety technology only at relevant points in the system, further reducing costs and cutting down on configuration, programming, installation, and commissioning efforts.

SEZ engineered its systems so that each component exists as an independent module with autonomous electronic and mechanical functions and application software. With such a clear and logical architecture, the company claims that its systems are more flexible and easier to expand and maintain than its competitors' more centralized configurations. In addition, SEZ's system architecture allows the company to use the same components for multiple purposes in different systems without additional effort, shortening engineering and construction times considerably.

The integrated approach also provides customers with other important benefits—the system requires less space at a time when floor-space costs are rising or the space is not available, performs faster fault diagnostics, and requires the customer to stock fewer spare parts. By implementing this solution, SEZ reduced assembly time for its systems from 21 weeks to 12 weeks and reduced commissioning time by 30% (because the company no longer needs to assemble and test modules at customer sites).