Word count: 2,974

Conference paper:
XVIII World Congress on Safety and Health at Work

For more information:
Andrea Hazard
Padilla Speer Beardsley
612-455-1733
Fax 612-455-1060
ahazard@psbpr.com

A Holistic Approach to Safety Automation

How technology, global standards and open systems help increase productivity and overall equipment effectiveness

By Dan Hornbeck
Manager Safety Business Development
Rockwell Automation

Every manufacturer aims to provide a safer workplace for its employees. In addition, they need to maintain productivity of the facility while protecting production equipment and the environment. Furthermore, depending on the corporate culture and location of each facility, a manufacturer must meet various social responsibility and legislative criteria.

What dictates the success of a safety program? First and foremost, corporate support. This support must start with top management's commitment to the program and continue through to each individual employee's adherence to the philosophy of "safety first."

Once corporate support is secured, an effective safety program encompasses several key factors, ranging from the proper use of eye and ear protection to the adoption of contemporary manufacturing strategies to the deployment of a well-designed and integrated safety automation system. This paper will focus on the latter.

The Historical View

Many of today's legacy manufacturing applications use dated technology and know-how. Some of these applications were developed with a blind eye toward safety – relying only

on the operator and maintenance technician to be alert to hazards. Others were deployed as an afterthought – in response to an accident or new industry standards. They used a "black box" approach to safety where the safety solution was completely separate from the automation system. Also contributing to this reactive and separate approach were the limitations of safety technology, which often required machines to come to a full stop and be in a "safe state" for repair, maintenance or anytime operator access was needed. Because this downtime due to a safety event decreased productivity, operators and maintenance personnel often bypassed safety systems, risking their own safety in the process. Still other systems were developed with an eye toward safety, but were improperly implemented and the equipment lacked required productivity – using a "trade off" mentality that resulted in neither being fully optimized.

Such risks are no longer needed or acceptable, thanks to progressive, enforced global standards, significant technological innovation, and risk management. When deployed properly using a holistic approach, today's safety automation systems allow the best of both worlds – a safer environment for employees, reduced environmental impact, better processes and optimized productivity.

The Impact of Standards

Though safety standards have continued to change throughout manufacturing history, the most recent wave of revisions improves the way machine safety systems will be designed. These are commonly referred to as functional safety standards.

Historically prescriptive in nature, safety standards provided guidance on how to structure control systems to help make sure safety requirements were met. These standards used redundancy, diversity and diagnostic principles, and created levels of safety system "structures" to help make sure the safety function would be performed. But a very important element was missing – time.

The new functional safety approach to global standards adds a time element – known as the Probability of Dangerous Failure, and its inverse, the Mean Time to Dangerous Failure – to build on the existing safety structure approach. This time element adds a confidence factor that the safety system is going to perform properly today and tomorrow.

Two important standards – ISO13849-1:2006 and IEC62061:2005 – apply the time element to safety systems for the machinery sector. ISO13849-1:2006 builds on the "categories" of safety structure, where as IEC62061 builds on the foundation of the structure, or what is called "Hardware Fault Tolerance." A third element, diagnostics, not new at all, is added to the picture to give the safety system designer more flexibility to achieve the safety requirements. Putting these three elements together yields a time-sensitive level of integrity in a safety system. IEC62061 uses the term "safety integrity level" (SIL). Only three SILs apply to machine systems: SIL1, SIL2 and SIL3. ISO13849-1:2006 uses the term "performance level" (PL), and then uses the alphabet, PLa through Ple.

Safety component suppliers share more of the responsibility of functional safety. Each component in the safety system must have an assigned probability of dangerous failure or mean time to dangerous failure. Currently, this type of information is often unavailable. In fact, many product design standards are being modified to define the criteria for dangerous failure, testing requirements, and statistical tools used to determine the time to dangerous failure. Once this is accomplished, many months of testing are required to confirm the achieved level.

The machine safety world continues to evolve. This change will provide flexibility to achieve safer designs. This will take some time to become widely implemented, but progress is in motion. Safety component suppliers now are working to help meet these requirements. And machine suppliers must become aware of functional safety and how to take advantage of its benefits.

Expanding the Technology Boundaries

A fundamental shift in two essential and related areas has helped make this new functional approach to safety possible. The first is major developments in safeguarding and control technologies – most notably the advent of new microprocessor-based technologies in lieu of electromechanical or hardwired control. The second is the evolution of global safety standards to allow these new electronic technologies to be incorporated into industrial safety systems.

Traditional hardwired safety systems can be difficult to troubleshoot, because they provide no indication of what went wrong. For example, in a scenario where multiple E-stops are daisy-chained together and hardwired into a safety relay, an "open circuit" between two of the E-stops will cause the relay to notify the controller resulting in a safe state. The maintenance crew then must investigate the reason for the open circuit – whether an E-stop was activated, or the circuit failed for some other reason. Without appropriate diagnostics, this process can take a lot of time, resulting in lost production.

E-stop events can cause even more trouble than simply being difficult to diagnose. They usually occur when a machine is in full production, which potentially can lead to machine alignment issues, material waste, longer restart times and possibly even equipment damage over time. These factors contribute to increased downtime and costs, since the work in progress may need to be cleaned, removed, reset or scrapped, and equipment re-homed or re-initialized.

Consider, on the other hand, a scenario where the E-stops are wired into a safety I/O block that is connected via a safety capable network – such as DeviceNet or EtherNet/IP – to the integrated standard/safety programmable automation system. In this case, the diagnostic information is provided to the controller and human-machine interface (HMI) in a readily accessible format and the controller or an operator/maintenance employee can take appropriate action to remedy the situation. This diagnostic information might reveal

that the operator on the third shift keeps hitting the E-stop to perform certain tasks rather than pre-defined steps to put a system into a safe state, or it might reveal the existence of a serious electrical problem that needs to be remedied. Either way, the cause of the event is diagnosed quickly, allowing the maintenance team to rectify the problem and get production back online sooner.

The second major development in safety technology was driven by the same market dynamics that have led companies to integrate other control disciplines (sequential, motion, drive and process). The result is a new breed of safeguarding and safety control platforms where safety technology is integrated into standard automation products – such as programmable automation controllers, programmable safety relays, plus variable frequency and servo drives. In addition, high-integrity safety communications networks, which incorporate message redundancy, cross-checking and stringent timing, also are in place, allowing safety and standard messages and devices to exist on common media.

Historically, safety has been separated from standard control, whether safety was implemented with individual components, such as safety relays or safety contactors, or a dedicated safety controller was used, requiring different hardware and software. Many manufacturers still value this approach, where dedicated safety personnel are the only employees who know a plant's safety hardware and software. In other words, if people aren't familiar with the safety hardware or safety software, there is less risk of safety being compromised – a sound approach, but one that generally adds costs.

In contrast, the ability to implement safety control within an architecture that can perform the four primary control tasks delivers major benefits. For starters, hardware costs are minimized, because system components can be used by the standard and safety portions of the application. Software and support costs also are reduced, because the same software can be used, and personnel only have to learn and keep current with one networking architecture. Moreover, depending on the demands of the application, users

can deploy and distribute the hardware necessary to help meet the application demands, whether on an individual machine or within an entire facility.

Safety automation systems now can be completely integrated with the standard plant automation system – yielding a single platform to perform defined safety functions, meet safety standards, and efficiently operate the plant. In this scenario, both facets of the automation system are designed to accommodate all machine lifecycle tasks, including design, start-up, operation and maintenance. Moreover, this holistic approach can lead to opportunities for designing out hazards where possible, based on detailed risk assessments in the early stages of any project. It also can help speed maintenance processes.

For example, manufacturers historically required employees to remove all sources of energy from a machine in order to gain access to the machine to perform maintenance operations, a process known as lock-out/tag-out. This process was often time-consuming, which reduced the machine's overall availability for production and, because it was time consuming, was often bypassed by the plant maintenance personnel.

With changes to safety standards and the advent of new, more sophisticated safety control, manufacturers can create safety zones in the application that can be managed independently for various operational and maintenance scenarios. This design flexibility can help reduce the time required for plant personnel to restore the machine to working order after performing the necessary maintenance, thereby improving productivity. It also reduces the operator motivation to bypass the safety system, thereby improving plant safety.

As these examples illustrate, well-designed safety systems deliver production improvements that can justify their implementation. Moreover, as functional safety standards evolve to accommodate technology developments, the industry can take advantage of new tools, such as integrated safety systems to improve performance. A

holistic approach based on risk assessments and contemporary technology helps make sure the task of servicing and operating the machine becomes intricately tied into how safety is controlled. No longer is the safety system its own individual entity – it is a critical component of the entire plant automation and production system.

This also is where advances in networking and communication technologies are helping to make these connections.

Bridging Communication Gaps

Integrating safety control systems to operate with the standard control system is one sign of a future of flexible, effective safety solutions. Another is communication integration using open protocols.

Seamless communication in the past was near-impossible, because no single network was able to integrate safety and standard control systems, while also allowing the seamless transport of data across multiple plant floor physical networks. That has changed with the emergence of CIP Safety, a networking standard that allows safety-rated devices to be connected to the same communications network as standard control devices. CIP Safety is based on the Common Industrial Protocol (CIP) standard, an open application protocol for industrial networking that is independent of the physical network.

CIP Safety greatly improves the level of integration between standard and safety control functions, increasing the visibility of safety across the entire system. The combination of fast-responding, local safety cells and the inter-cell routing of safety data creates safety applications with faster response times. The additional flexibility also helps speed up system configuration, testing and commissioning.

Another level of integration that often is overlooked is the use of safety data in a plant wide information system. Because safety data is readily available, the information system can be tightly coupled with the safe automation strategy. This results in information, such

as diagnostic data, reasons for and frequency of safety events, statistical data for lean manufacturing improvements, production data, security access and more.

One reason safety networks traditionally were isolated on the control floor is because the safety devices and controllers needed to react at different speeds from their standard counterparts. Historically, using a single network to accommodate both safety and standard systems proved problematic, because the larger a network grew, the more the performance speed decreased. However, with CIP Safety, each node's network update rate can be set at a different speed. This allows each device to perform at a rate that is best optimized to its safety function, helping to efficiently allocate network bandwidth.

Bridging and routing is an important feature of CIP Safety because it allows seamless communication of both safety and standard data across multiple and potentially different physical networks. This feature removes the need for message path routing and data translation, allowing the data to flow openly between networks and devices with minimal effort on the part of the system engineer. This seamless communication allows manufacturers to perform monitoring and data collection of their standard and safety systems from any authorized location in a facility.

The protection measures within CIP Safety help elicit high integrity communications when safety and standard communications are mixed. This is what allows safety sensors to operate alongside variable-speed drives, standard sensors, safety controllers with standard PLCs and proximity switches. Users can realize a wide combination of safety and standard devices on the same network, and the integrity of the safety control loop will be maintained.

Perhaps the greatest advantage of CIP Safety is its ease of use features and reliability, including bridging and routing with no programming requirements. This means more efficient training, faster commissioning and improved diagnostics capabilities. CIP Safety capabilities on DeviceNet and EtherNet/IP are TÜV-approved with products available

today on both networks from multiple vendors. CIP safety on EtherNet/IP allows safety networks to be integrated into the same Ethernet architecture used by standard control devices, the Internet and the rest of the enterprise.

The future promises to be bright as more automation suppliers develop CIP Safety-compatible products that support integration among safety and standard controllers, devices and networks.

Effective Risk Management

Another bright spot and critical aspect of a holistic approach to safety is the increased support of proactive risk analysis on the part of manufacturers. A safety system's general objective is to help make people, processes and machines safer without decreasing productivity. Manufacturers that conduct risk assessments are several steps closer to achieving all the above – and in so doing, they help reduce risk and the costs associated with it.

The definition of formal risk assessment processes, which covers risk identification, risk quantification and risk mitigation, are included in many international and regional standards, including IEC61508, ISO13849 and ANSI/B155.1. Risk assessment processes defined within these standards typically take a life cycle approach in clarifying how to implement an effective process to identify machinery related risks, as well as quantify the level of risk in terms of severity, frequency of exposure and probability of avoidance. The result is a quantified level of risk that must be decreased via protective measures.

Risk assessments give manufacturers a process for 1) identifying specific hazards on a machine; 2) quantifying the risk these hazards present to employees; and 3) evaluating practices that can help mitigate the risk In addition, the process will specify the most appropriate safety circuit architecture required to mitigate the initial risk rating determined by the assessment team.

Once the risks are fully defined and understood, they must be designed out or mitigated to the greatest extent possible. Risk mitigation measures physically improve the machine to reduce the potential of personal injury, environmental or property damage. Risk mitigation can be accomplished through a variety of activities. One effective method is to use safeguarding equipment, such as light curtains, safety relays and cable pull switches to help reduce risk to employees.

Using a formal risk assessment process also provides the benefit of documenting any identified risks, the protective measures and safeguards implemented to mitigate them, and the residual risk remaining when these mitigation methods have been deployed. Illustrating due diligence and good engineering practices in providing a safe work environment, a company potentially can lower its risks of litigation in the event of an incident.

After implementing and documenting the process, it is important to provide the appropriate training and supervision. It is critical to make sure operators understand the safety measures, including proper use of personal protective equipment. Operators must be trained to effectively operate the machines and safely perform their work. This also includes clearly defining their tasks and processes, versus those tasks to be implemented by more specialized and trained maintenance personnel.

A comprehensive machine safety program can help improve plant-floor operations and productivity across the board. In order to facilitate the multifaceted lifecycle of machine safety, it is important to link risk analysis, risk mitigation and training/supervision together in evaluating the effectiveness of the machine safety program. It is important that all plant floor personnel benefit from the safety measures and training available to protect them.

Reaping the Benefits of a Holistic Approach to Safety

Today more than ever, progressive manufacturers are focusing on safety automation solutions that keep their people safe, their machines working, and their bottom lines robust. Thanks to the holistic approach to safety automation – which emphasizes global standards, innovative technologies, trained personnel and ongoing risk assessment, all working together – manufacturers have a best practice template to implement and achieve a high level of safety.

# # #