Concepts in networked machine safety

Ming Ng, Factory Automation, Siemens Industry Automation, Norcross, GA USA

Have you been a part of, or noticed all the big changes around us recently, be it the housing market or the industrial environment? Taking the same path is the implementation of networked safety systems, which is a change both culturally and in practice. Over the last decade the machine automation industry has been inundated with information about changing standards, new product developments and new possibilities. This white paper demystifies the different approaches and shows how safety related control functions using Safety PLCs and networks, can be combined to provide numerous cost-savings and increased productivity benefits to the users.

Let us start with one of the key considerations for the system and that is safety. The objective of safety systems is to keep potential hazards for both people and the environment as low as possible by using suitable technical equipment, without restricting more than absolutely necessary, industrial production, the use of machines and operator interaction. The protection of man and environment has to be put on an equal footing in all countries by applying rules and regulations that have been internationally harmonized. From the perspective of the object to be protected, safety cannot be segregated. The causes of danger and also the technical measures to avoid them can vary widely. This is the reason that a differentiation is made between various types of safety, e.g. by specifying the particular cause of a hazard. For instance, the term “electrical safety” is used if protection has to be provided against electrical hazards and the term “functional safety” is used for machine safeguarding.

In terms of market and motivation, why is safety necessary? The prime reason being that safety is for the protection of people, which is a social responsibility; secondly the existing machine safety standards necessitate innovations for reducing cost pressures and maintaining productivity. But due to globalization there is an added market demand and stringent competition, hence only maintaining productivity is not sufficient and therefore productivity needs to be increased and this can only be done with innovative engineered solutions on a network, that must include safety.

What is important to know is that the control system of a machine, which is operated and used in the US, must fulfill US requirements, even if the machine manufacturer (i.e. the OEM) is based in Europe. Following this, in the United States, the Occupational Safety and Health Act (OSHA) from 1970 regulates the requirements for employers to ensure safe working conditions. The core requirements of the OSH Act are administered through the Occupational Safety and Health Administration (also known as OSHA). OSHA deploys regional inspectors to check whether workplaces comply with the valid rules and regulations. The rules and regulations of OSHA - relevant for safety at work - are defined in OSHA 29 CFR 1910.xxx ("OSHA Regulations (29 CFR) PART 1910 Occupational Safety and Health") (CFR: Code of Federal Regulations).

OSHA has many regulations related to specific machine types, but for others, OSHA relies on National Consensus Standards. These National Consensus Standards, such as the ANSI B11
series, NFPA79 and others, are developed and are more up to date, specifically for machine safety applications. They reflect the state-of-the-art for safely implementing specific machines in the relevant machine applications. In conjunction with specific applications, OSHA specifies that all electrical equipment used to protect employees must be certified for the intended application by a Nationally Recognized Testing Laboratory (NRTL) authorized by OSHA.

The first consensus standards to adapt to the changes seen in the industrial markets was the American National Standards Institute and Robotic Industries Association ANSI/RIA 15.06, 1999 which introduced the “risk analysis” requirement for hazard identification in the robotics industry. NFPA 79 electrical standard for industrial machinery was the second major standard to change. Its 2002 revision (done to harmonize NFPA-79 with its European counterpart, IEC-60204) states that “hardware and software-based systems listed for such use” could now be used in safety applications. The compelling event was that, this NFPA 79, 2002 change was significant because it eliminated the exclusive requirement for hardwired connections of sensors and actuators to electromechanical (safety) relays. Furthermore, the NFPA79 2007 provides an exception that allows safety rated drives “listed” for such use to be used as the final switching element in an EStop application.

For designing safety into a machine, the machine safety standards require a Risk Assessment to be done on the machine. Risk assessment is a sequence of steps that allows hazards, which are caused by machines, to be systematically investigated. Where necessary, the risk assessment phase is followed by risk reduction. Using this process, hazards, as far as possible, can be eliminated and the appropriate protective measures can be applied. After the risks have been estimated, a risk evaluation is made as part of an iterative process to achieve safety. In this case, a decision has to be made whether it is necessary to reduce a risk. If a risk is to be further reduced, suitable protective measures must be selected and applied. The risk assessment should then be repeated.

In addition to applying structural measures, risk reduction for a machine can also be realized using safety-relevant control functions. Specific requirements must be observed when implementing these control functions, graduated according to the magnitude of the risk. These are defined in EN ISO 13849-1 and, for electrical control systems, especially with programmable electronics, in IEC 61508. The requirements placed on safety relevant parts of control systems are classified into categories, according to the level of risk and the necessary risk reduction. For this purpose, EN 954-1 - that has been valid up until now - defines “Categories” and describes a technique to select the suitable category to design the safety-related parts of a control system. With the new standard EN ISO 13849-1 a risk diagram has been introduced; instead of categories, where hierarchically graduated Performance Levels (PL) are defined.

EN 62061 uses the “Safety Integrity Level” (SIL) to classify risks. This is a quantified measure for the safety-related performance of a safety function. The necessary SIL is determined according to the principle of risk assessment according to EN ISO 14121. It is always important - independent of which standard is applied - that all parts of the control of the machine that are involved in implementing these safety-related functions clearly fulfilled the safety requirements. Safety is a relative term in our technical environment. Unfortunately, it is not possible to implement the so-called “zero risk guarantee” where nothing can happen under any circumstance. The residual risk is defined as: Risk that remains after the protective measures have been implemented. In this case, protective measures represent all of the measures to reduced risk.

The measure for the level of achieved functional safety is the probability of the occurrence of dangerous failures, the fault tolerance and the quality that should be guaranteed by avoiding systematic faults. Various terminology is used to express this in the standards. In IEC 61508: “Safety Integrity Level” (SIL), in EN 954: “Categories” and EN ISO 13849-1 “Performance Level” (PL). In the area of machine safety, EN ISO 13849 (derived from EN 954) and IEC 62061 specifically address the requirements placed on safety-related control systems and therefore concentrate on functional safety. In the basis safety standard IEC 61508, IEC addresses the functional safety of electrical, electronic and programmable electronic systems, independent of any specific application area.

In order to achieve the functional safety of a machine or plant, the safety-relevant parts of the protective and control systems must function correctly and must respond in the event of a fault in such a way that the system remains in a safe state or is brought into a safe state. To achieve this, specifically qualified technology is required, which fulfills the requirements described in the relevant standards. The requirements to achieve functional safety are based on the following basic goals: Avoiding systematic faults, Controlling systematic faults, Controlling random faults or failures. Safety networks fully comply with the mentioned requirements of the machine safety standards.

When we speak of networking, what is the first thought that comes to our minds? Ethernet is emerging as the de facto network for the plant floor communications, replacing field buses in the factory while also providing a link to front office systems. The ubiquitous network has enough speed for manufacturing environments, and it’s been enhanced with real time capabilities for the most demanding applications. Using Ethernet throughout an enterprise solution greatly simplifies installation and maintenance while opening the door to many advances in communication technology. Compatible wireless technologies can be installed easily, and safety networks can also communicate over a single cable. All these benefits can be gained at lower costs than those of proprietary field buses.

So how did this all start, Ethernet first saw usage on the factory floor as a backbone for linking various industrial networks together. Typically, it was only used to connect a manufacturing process to the business environment to gather quality data and manage recipes. But that’s changed dramatically in recent years. Ethernet now reaches down to the machine level, where it handles I/O and other jobs once only possible with a range of deterministic field bus protocols.

Ethernet is also displacing field buses at the system level, linking automation equipment together in a single common network, even when equipment is from a variety of vendors. Instead of spending unnecessary hours figuring out how two pieces of equipment can coexist on one network, Ethernet makes it simple to plug them into a common switch, and allow multiple protocols to coexist on the same
These benefits come without impacting the existing links between manufacturing processes and the Manufacturing Execution System (MES) tools used to manage the complete plant. As a result, it is possible to have one network infrastructure from the I/O level all the way to the MES.

There are many reasons to choose Ethernet throughout the networking hierarchy. One of the key driving factors in many organizations is the desire to create compatible networks throughout the entire facility. Automating operations is a critical factor for success in lean manufacturing environments. Linking the management systems that bring in orders to the manufacturing equipment that fulfills those orders makes it simpler to streamline operations. Instead of passing and translating information from one level to the next over several different types of networks and field buses, Ethernet makes it possible for the management system to send information directly to the individual pieces of manufacturing equipment over a single network. This is made possible because Ethernet supports multiple protocols such as TCP/IP, HTTP, SNMP, OPC and real time I/O at the same time on the same wire. That’s far more efficient than dedicating a field bus for each protocol. Ethernet truly opens communication possibilities.

Using a single networking scheme also pays off when problems on the plant floor are diagnosed. For instance, it was traditionally difficult to notify the maintenance staff if a wire on an I/O device’s sensor broke. First, the automation controller would have to recognize that there was an issue on one of its I/O devices on the dedicated field bus. Then it would send an alarm to an HMI over another network to notify the machine operator. Next, the machine operator alerts the maintenance staff. They would then have to plug their programming device directly into the automation controller and its field bus to investigate the problem.

Using an Ethernet network greatly simplifies this scenario. When the I/O device recognizes the wire break, this information can be pushed directly onto the Ethernet network by the device itself. The diagnostic can then be read in multiple locations by a variety of devices. For example, the HMI can let the machine operator know that there is a broken wire. The MES can read the message and record the issue into its quality database. The maintenance staff can be informed via an SMS message sent directly from the automation system. The maintenance staff can even collect further diagnostics directly from the I/O device regardless of where the programmer is located in the plant. This sort of Ethernet connectivity extends plant network visibility, bringing many new possibilities for delivering real time information and keeping equipment running at peak performance.

Cost is yet another benefit of Ethernet. Having a compatible network throughout the enterprise helps keep expenses down. First, it eliminates the need for field bus gateways, devices or software that perform media translation. Beyond the obvious hardware cost of these gateways, there is also a cost for installation, commissioning, and maintenance. Furthermore, supporting multiple networks in a plant means that the engineering and maintenance staff must be trained on multiple networks and a number of specialists are needed to support each type of network. In either case this means additional expenses. With Ethernet throughout the plant, these costs are greatly reduced and in the case of additional gateways, completely eliminated.

Once a plant decides to standardize on Ethernet, a whole new world is available. New innovations in the Ethernet community provide constant improvements in automation technology. These advances save time and money during design, engineering, and commissioning. These new technologies have been enabled in large part by the addition of real-time Ethernet protocols. Protocols such as TCP/IP and OPC by themselves do not support real-time capabilities. There have been considerable innovations that provide automation-based protocols over Ethernet. Several protocols from different field bus organizations now provide real-time, automation-based solutions. These field bus organizations have transformed their real time device level network strategies of the past into protocols that runs on today’s Ethernet networks. As a result, it is possible to do much more on Ethernet today than in the past.

Adopting the versatile Ethernet network makes it possible to streamline communications, letting devices talk directly to each other. These devices can be as simple as an I/O module or as complex as a complete automation cell. Device to device communications are becoming increasingly common as engineers figure out how to utilize data without taking time for humans to review it. With Ethernet, it’s much simpler to communicate since Ethernet enables more comprehensive protocols. In the past, adding a camera to an automation controller was a difficult task because of the type of data that a camera transmits. With Ethernet based protocols, data easily passes between the camera and the controller. Equally important, it’s simpler to set up the communications between these devices. With existing field buses, systems must be hardwired to communicate, or programmers must figure out the various commands for each device, writing complex programs to tie them together. Using Ethernet opens the door to device to device communication protocols, which let users link pieces of equipment by simply mapping inputs and outputs via the engineering system. Complex programming to integrate machines and exchange data is replaced by this simple mapping of IO registers, allowing engineers to focus more time on their application and less time on solving integration issues.

The benefits of Ethernet’s seamless networking environment extend to wireless communications as well. For many companies, one of the biggest potential benefits of Ethernet is the ease of adding wireless communications. This simply wasn’t possible with past field network protocols. Wireless can be a real boon for industrial applications. Equipment can be moved without worrying about wiring. Distributed I/O connected to field devices such as sensors and motors can be installed in hard-to-reach spots. Temporary monitoring stations can be installed without the cost or danger of stringing wires around equipment. Expanding into wireless technology for automation is easily accomplished by implementing Wi-Fi technology that’s an extension of the wide-ranging 802.x Ethernet specifications and the automation protocols designed for them. A number of companies have been using Wi-Fi in harsh factory environments for years. Wi-Fi simplifies the transition to wireless, maintaining all the commands and protocols of conventional wired Ethernet networks. Employing Wi-Fi extends the compatibility that comes with using Ethernet throughout the enterprise network, bringing ease of maintenance along with compatibility. This trend to wireless communications is expanding rapidly because it brings a high level of freedom. Operators who often move equipment around once had to employ wiring trays that were difficult to setup and manage. Wireless links eliminate that complexity. Similarly, engineers can add sensors to monitor equipment in a matter of minutes.
Eliminating wires also facilitates the usage of autonomous vehicles that can deliver materials or components. Traditionally, these automatic guided vehicles (AGVs) communicated back to a central controller over a hardwired network using slip-ring technology. This technology, because of its mechanical nature, had many possibilities for failures, so maintenance costs were quite frequently very high. When these robotic vehicles can communicate over a wireless network, they can move freely and alter their routes to maximize efficiency since they are not physically tethered to a network cable.

Ethernet is only the wire. On top of the infrastructure we need an application protocol (“communication language”) which enables the devices to talk to each other. The answer for this, is PROFINET for plant-wide connectivity.

The closest real-world parallel comes from telecommunications. It is possible to pick up a phone in the US, dial an extension in France and be connected. However, just because the phone rings on the opposite end and someone answers doesn’t mean that both parties can communicate. A common language is needed for a conversation, which means a common application protocol for the process data is needed. PROFINET is this application protocol for the industrial world.

PROFINET satisfies the real-time determinism requirements of an industrial system while still allowing standard communication such as video to coexist over the same system. The standardized PROFINET protocol enables plant-wide interoperability.

PROFINET allows safety functionality to be utilized directly over an ETHERNET network. Since the PROFIsafe profile exists as part of the application layer, safety I/O can be utilized in conjunction with standard I/O. The safety related data is included in the process data information in the protocol. And it doesn’t matter is it a PROFIBUS or PROFINET protocol. This makes it so easy to implement safety on a network. Use the same configuration tools for standard and safety applications, mix and match standard modules and safety modules in one station.

What are the benefits of combining safety over a PROFINET network? PROFINET has the bandwidth to support protocols for safety signals and communications. Doing away with dedicated safety circuits and eliminating wiring provide a significant benefit in plants where expansion and equipment upgrades are common. When safety signals are sent over Ethernet, safety circuits can be handled in ladder logic that runs on automation controllers. Safety equipment like light curtains are typically linked to failsafe input cards that send alerts to automation controllers over PROFINET. Using PROFINET to carry these safety signals also makes it simpler to keep a plant up and running. Conventional safety relays shut down power to broad areas, regardless of the type of problem. With PROFINET connectivity to all equipment, it’s straightforward to program systems to shut down only equipment that’s related to the safety alert. The system can analyze the reason for a safety alert, then determine whether all equipment in the area of the alert should be shut down or whether sections of the system can continue running without danger. Since PROFINET and Wi-Fi are tightly integrated, these benefits extend to all equipment linked to the safety system even with a wireless connection.

Users have implemented Safety networks and are benefiting from the cost saving advantages: Here is an operational system that was designed for a Wireless Distributed Safety Control Network for Large Overhead Gantry Robot Systems. The main challenges the customer was facing were that they had never designed a similar architecture before. There was a laundry list of needs to be satisfied. It needed to be reliable, cost effective, compliant to RIA 15.06-1999, safety rated with flexible connectivity, expandable, and wireless with scalability. The objective of the project was to create a state of the art material handling solution, with local/global service and support that provided a one-year payback period.

Based on the safety wireless network design on PROFINET, the operation improvements achieved were that they could now implement one network for all applications: Distributed Safety, Vision, Motor Control over wireless, reduction of installation time by as much as 30%. A safety rated wireless network further minimized wiring, saving additional installation costs. It also provided faster troubleshooting & diagnostics allowing for a 2-day deployment time. Robust proven products, ease of expansion, modular architecture & scalability were the benefits that increased productivity on the plant floor.

Thus you can see with the changing trend in technologies, the safest way to move forward to realize additional cost savings, operator protection, resulting in increased productivity is the next best change that can be achieved with safety networks. Safety networks have been making original equipment manufacturers and their customers not only more safe, but more efficient.

So are you ready to make the change on your plant floor?