



Safety in drives

Functional safety in machinery, especially in AC drives

MIKKO RISTOLAINEN – Safety is paramount to manufacturing and should be every company's highest priority. This objective may sometimes appear to be in conflict with the goal to be as productive as possible. Thanks to improved control and monitoring concepts however, these goals can now be complementary rather than conflicting. Whereas safety was previously often assured through separate external equipment, integration is permitting safety, control and monitoring to increasingly go hand-in hand using common data and functions and thus create combined functionality that would previously have been unthinkable. One area where this is happening is in AC drives. Offerings from safe stopping to more elaborate monitoring functions are being introduced and are heralding new opportunities in machine safety.



Safety is important. National laws in the European Union require machines to meet essential health and safety requirements. This means that all new machinery must meet the same legal requirements when supplied within the EU. Fulfilling these requirements is the responsibility of machine manufacturers or importers.

Behind the harmonization of the national requirements is the Machinery Directive 2006/42/EC (which replaced the old directive 98/37/EC on 29.12.2009). It aims to ensure that machinery is safe and is designed and constructed so that it can be used, configured and maintained throughout all phases of its life to cause minimal risk to people and the environment.

According to the requirements, manufacturers (or their representatives) must perform and document risk assessments and take the results into account in machine design. Any risks must be reduced to an acceptable level through design changes or by applying appropriate safeguarding techniques. After all risk reduction measures have been applied, any residual risks must be documented. One way to carry out the risk reduction process and to ensure conformance with the requirements is to apply suitable har-

monized standards under the Machinery Directive.

When machines are designed and implemented according to relevant harmonized standards, it is presumed that the machinery complies with essential health and safety requirements and generally

Configurable safety systems today can be used to realize numerous standard safety functions for drives according to EN 61800-5-2.

does not require certification by a third party. Manufacturers can self-declare the conformity to the Directive via documentation and attach the CE marking to the machine as a sign of conformance to the set requirements.

The harmonized standards also provide a guideline for determining the machine's scope of application and its operating limits, potential hazards, as well as the

means to assess and evaluate the identified risks. Standards will assist in deciding whether risk reduction is required and outline a strategic approach to reducing the risks to an acceptable level.

The most effective way to reduce or eliminate risks is to design them away. But when risk reduction by design is not possible or feasible, safeguarding with static guards or by functional safety may be the answer. As a bonus, functional safety can often be used to achieve higher machine productivity, uptime and less abrupt behavior of the safety system, while at the same time meeting the legal requirements. Machines can be stopped quickly and safely – or even better – operated at a reduced speed during specific times to reduce risk.

In industries where people work in close proximity to machines, functional safety technology can be utilized to ensure their safety while keeping the processes running. When safety systems are designed into work processes, safety is part of the process, people are kept safe and high productivity is maintained.

Updated standards for updated technology

Due to developments in technology and in the field of standards, requirements to



The installation cost for an advanced safety system with an integrated system is usually lower than if the same functionality is achieved with external safety components, especially when several safety functions are implemented.

implement safety-related control systems have been updated. Previously, it was relatively easy to design safety systems according to the standard EN 954-1 (Safety of Machinery – Safety-related Parts of Control Systems – Part 1: General Principles for Design), which provided straightforward design rules for achieving a certain safety level (safety category). This standard is based on a cause-effect approach and the emphasis is on the use of proven components and methods.

The EN 954-1 is a relatively simple standard mainly for mechanical and electromechanical systems. It does not cover complex or software-configurable safety-related electrical control systems, which have become the standard approach in functional safety. The deterministic design oriented approach of EN 954-1 has been replaced by concepts such as failure probability and lifecycle thinking. They thus aim to cover the entire life of the machine from the first concepts to decommissioning.

The transition period for EN 954-1 ends December 2011, when it will become obsolete. Although the EN 954-1 still provides the presumption of conformity with the Machinery Directive until the end of 2011, it is no longer state of the art.

The modern harmonized standards under the Machinery Directive are EN 62061:2005 (Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems), and EN ISO 13849-1:2008 (Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design) for various types of safety related systems (including for example hydraulics and pneumatics). Both these standards are based on the umbrella standard IEC 61508-1...7 (Functional safety of electrical/electronic/programmable electronic safety-related systems), which defines the overall requirements and processes for designing safety related electrical / electronic control systems.

Support makes the difference

Implementing a machine safety system from start to finish following the new standards can be a complicated undertaking. Which standard should be used? Which steps should be taken? How should the necessary calculations be performed and designs validated? And so on. As a result, business for safety consulting services is booming. Furthermore, component suppliers need to provide customers with support to help them get through their safety design processes. It has been forecasted that companies providing safety design support and knowledge in addition to components will

increasingly be in a better position to get business. Such support may well become a standard requirement in selling safety products, with safety component suppliers being required to offer safety consultation along with their safety products.

Evolution of functional safety solutions in AC drives

Evolution in electronic control systems has also affected the safety technology used with AC drives. Traditionally, automation systems involving drives have typically used electromechanical safety relays. These relays monitor various safety input devices such as limit switches and emergency stop buttons, and operate contactors to safely cut off power to the power drive system when given parameters are exceeded.

Electronics is increasingly used in modern safety systems for AC drive applications. The trend has been so strong, that a new standard for functional safety requirements for drive systems, EN (IEC) 61800-5-2:2007 (Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional), was harmonized in 2008. This standard sets requirements for design principles of safety-related drive systems, as well as defining a number of standardized safety functions for drives. These definitions help in harmonizing the marketing terminology used to market safety functions.

The contactors to safely stop the motor movement in emergency or start-up prevention situations can now be eliminated thanks to a new feature integrated into the drive's power section. The safe torque off (STO) feature simply disables drive output modulation and safely eliminates the drive's capability to make the motor produce torque.

Processes can become more productive when STO is used to safely stop the motor without disconnecting the power supply or the drive's DC circuit. The drive can quickly be re-started without having to recharge the DC circuits or re-establish control parameters.

When additional functionality is needed, STO benefits can be complemented by combining the function with more advanced monitoring functions. External offerings include, for example, time-delay relays or so called configurable safety systems. These are typically intermediate between PLCs and solid state safety relays. Configurable safety systems today can be used to realize numerous standard safety functions for drives according to EN 61800-5-2. Typical functions include different safe stopping functions (EN 60204-1 stop categories 0, 1, 2), safely-limited speed (SLS), safe direction

External safety components are usually wired and configured to operate together with the drive. The development of an application usually requires wiring and configuration of the two devices individually so that they can work together. This can potentially result in a considerable effort in designing, installing and commissioning the system. There is thus a need for clear instructions from the drive supplier to support this configuration.

If safe communication is used, the system often has two separate fieldbusses, one for safety communication to the safety device and the regular fieldbus to the drive for control purposes. On the other hand, configurable safety systems, often with an abundance of extra inputs and outputs, can provide additional control functionality for other generic machine systems outside the actual safety realm.

Moving beyond the use of external components, the next logical step in drive-based safety is to integrate the safety functionality into the drive. This yields a number of advantages: Wiring is reduced, drive inputs and outputs are freed, space is saved, and the configuration can be performed through a single connection with one set of tools. Because

integrated safety functions are drive-specific, the commissioning process is basically concerned with setting parameter values and behavior options. The actual programming of the basic functionality is no longer required, an improve-

ment over the external systems which require the functional logic to be block programmed. Furthermore, a single fieldbus connection can be used for both regular and safety communication. The overall safety functionality can be optimized when safety and control parts of the drive share status information over a bus connection. And of course the system looks much cleaner without all the separate units and all the wiring.

Developing drive-integrated safety is a challenging process for drive manufacturers. However, the installation cost for

an advanced integrated safety system is usually lower than if the same functionality is achieved with external safety components, especially when several safety functions are implemented.

Seeing through the hype

Integrated safety systems are frequently promoted in trade magazines, trade fairs and research articles. Safety features thus often become a product differentiator, with safety being promoted as a "must-have" feature.

Functional safety features can help boost performance and usability of machines while meeting the safety regulations. But it also takes time to really understand the opportunities that safety functions offer and their implications and to ensure that these match the real needs of the application.

Many machine builders are currently developing plans and specifications for their future machinery. However, because the modern functional safety offering is not always fully understood, there is a risk of buyers following the marketing hype and products being selected that do not actually meet their needs. Instead products are selected because they offer the most safety features or the highest safety rating, "just in case it is needed". It is therefore important for buyers to clearly understand and define their safety needs in advance and select products that meet those needs.

Even though tools, techniques and regulations have evolved, the main purpose of safety is still to protect people and the environment. The more information a buyer has on safety, the better he or she will be able to differentiate marketing hype from real advantages, and so prevent the wrong purchasing decisions. ABB advises its customers to be informed and to be prepared and is ready to offer support and advice.

Mikko Ristolainen

ABB Drives
Helsinki Finland
mikko.ristolainen@fi.abb.com

The contactors to safely stop the motor movement in emergency situations can now be eliminated thanks to a new feature integrated into the drive's power section.

(SDI), safe operating stop (standstill) (SOS), safe (mechanical) brake control (SBC) and so on, some 17 functions in total.

Such configurable systems become feasible alternatives when several safety functions are implemented in the same system. For single safety functions, dedicated single purpose components such as time delay relays or two hand control relays remain the more feasible approach.