

Machine safety

EN ISO 13849-1 was harmonised to the Machinery Directive on 8 May 2007. Kevin Ives discusses the implications for machinery safety systems

Following the ISO 13849-1:2006 debacle, and now its harmonisation to the Machinery Directive, machinery safety standards are under the spotlight again.

ISO 13849-1 (Safety of machinery, Safety-related parts of control systems, Part 1: General principles for design) will replace EN 954-1:1997 (Safety of machinery, Safety-related parts of control systems, with Part 1: General principles for design).

The problem is that EN 954-1 is relatively simple, with an easy-to-follow (often criticised as too easy), qualitative risk graph that helps users establish safety categories for machines. But while EN ISO 13849-1 follows a similar process to define a performance level, the user then has to perform calculations covering diagnostic coverage, mean time to dangerous failure, architecture and common-cause, in order to validate the result.


For those that find themselves using both EN ISO 13849-1 and EN 62061 (electrical control systems only), it is also frustrating and possibly

confusing, because the terminology is different. For example, EN ISO 13849-1 performance level 'b' is roughly equivalent to a 'low' EN 62061 SIL 1; performance level 'c' is a 'high' SIL 1; performance level 'd' is SIL 2; and performance level 'e' is SIL3 under EN 62061.

One point in EN ISO 13849-1's favour, however, is its quantitative approach, which is more useful for complex machinery – and the standard also enables a safety-related control system to be validated. With EN 954-1, it was a case of designing the system and relying on the design being right, but the new standard forces engineers to validate that the control system really does do what is required.

Choosing the standard

The new standard was harmonised on 8 May 2007, but there is a transition period until 30 November 2009, during which machine builders can choose whether to work to EN 954-1 or EN ISO 13849-1. For a simple machine – typically one on which the safety system uses nothing more than safety relays – I would recommend using EN 954-1. However, for more complex machinery, or anything using a programmable safety controller, EN 62061 is better. Then complex non-electrical safety-related systems should be designed to EN ISO 13849-1.

In addition, pay attention to the Type C standards that relate to specific categories of machinery. They help to reveal the risks and indicate the minimum safety category (as per EN 954-1) that should be used. These 'three-letter' standards are being rewritten as international ISO standards with a five- or six-figure denotation. They will contain references to EN ISO 13849-1 and IEC 62061, rather than the old EN 954-1. 

Technical pointers

- For a simple machine – typically one on which the safety system uses nothing more than safety relays – use EN 954-1
- For more complex machinery, or anything using a programmable safety controller, EN 62061 is better
- Complex non-electrical safety systems should be designed to EN ISO 13849-1
- Pilz's PNOZsigma safety relays all now have plug-in, spring-loaded terminals, as well as built-in intelligence and LEDs for diagnostics
- The company's PNOZmulti controllers provide the bigger system logic in software

Relays and systems

There is no getting away from safety-related control equipment on machinery, but there is a problem when it becomes one of the main causes of downtime – and that's usually due to older technologies and/or poorly installed equipment.

Guard switches, for example, can be troublesome. On guards that are frequently opened for loading and unloading parts, or for routine maintenance, hinges can wear and the guard switch and actuator become misaligned. Tongue-operated mechanical switches can be problematic, but even if non-contact switches are used (for their better misalignment tolerance), problems may not become obvious until the switch fails to operate when the guard is closed – or vibration causes it to break the safety circuit while the machine is running.

One way to avoid such problems is to install the switch on a robust sliding bolt, so that it maintains the correct alignment. But there are more basic points: traditional control systems use banks of safety relays – even though every connection is a potential source of unreliability. Also, many still prefer screwed terminations, even though these are vulnerable to vibration, and alternative sprung cage clamp terminals, especially the plug-in types, are better and quicker to wire and replace.

It's worth noting that, if you move over to digital safety systems, you can transmit diagnostics to an HMI (human machine interface) or machine controller using plant fieldbuses, such as Profibus, DeviceNet, CANopen, CC-Link and Interbus.



Kevin Ives is with Pilz Automation Technology