

What is AS61508 and how is it different from AS4024?

Just as Australian industry comes to grips with safety standard AS4024, a newer, more complex, international and now also an Australian standard is gaining wider usage.

For almost a decade, Australian industry has been applying the basic principles of Australian Standard AS4024 Safeguarding of Machinery. Those same principles: hazard identification, risk assessment and control, are reflected in the regulations of both New Zealand and Australian states and territories. Unfortunately, while awareness has grown dramatically since AS4024 was published in 1996, there is still a long way to go before there is widespread understanding of the obligations assigned by the standard.

Recently, however, the process sector of Australian industry has begun to adopt AS61508 Functional safety of electrical/electronic/programmable electronic safety related systems, the Australian version of IEC 61508. The standard, published in 1999, covers the design of Electrical/electronic/programmable electronic Safety Related Systems. It addresses the life cycle of safety-instrumented systems, risk assessment methods, change procedures for safety-instrumented systems and provides performance requirements, called Safety Integrity Levels (SIL).

On the surface, AS61508 and AS4024 have quite a bit in common. Both start with a hazard identification or analysis process, both assess the level of risk involved and both assign a "safety integrity level" or "category" to define various levels of safety performance, but that is where the similarities end.

Perhaps the biggest difference between the two standards is the measurement of risk and consequences. AS4024 uses a simple decision tree to determine which category of safety control is required. AS61508 on the other hand, asks for a quantitative measure of the overall failure rate of the safety system. The mean time between failures needs to be ascertained for each element of the system and then a cumulative probability calculated.

Theoretically, it makes sense but, in practice, the data is often very difficult to source. How can an engineer say, for example, how long a particular photo-eye will or should operate before it fails? What about the solenoids on the gates, the light curtain and the deadman controls? Without good historical data, assumptions have to be made and when you are choosing between 103 hours or 104 hours, it makes a real difference to the rating of your system.

This lack of data proved a problem for The European Commission (EC) project, STSARCES (Standards for Safety-Related Complex Electronic Systems), which attempted to assess a machine according to IEC61508, the international standard reflected in AS61508. The report concluded:

"This assessment has not proven to be an appropriate way of demonstrating the effectiveness of IEC 61508... If the methodology has not been used by the manufacturer, subsequent assessment using IEC 61508 will inevitably be difficult because of missing

information. However, if IEC 61508 had been followed from the outset, the relevant information would have been available, facilitating the assessment."

What it means for Australian industry? AS61508 is here to stay and while compliance with the more manageable AS4024 will be sufficient in most cases, it makes sense to be familiar with at least the basics of AS61508.

The categories used by AS61508 are SILs (safety integrity level), which are based on the "probability of plant failure on demand" and the consequences of failure. Probability of plant failure on demand means how often the plant is required to operate and the reliability of the system. As with AS4024, the more serious the consequences of failure, the higher the SIL, and with an increased SIL ranking comes more stringent safety system requirements.

The standard's key criteria for rating safety systems are strength, diagnostics capability, common cause strength and redundancy.

To test strength of safety hardware, an engineer must consider all the factors that could affect the operation of the system, such as radio frequency interference or even heat.

Software rated to AS61508 (equivalent to SIL 3) for example, would include a process to check the reasonableness of data and data tables, filtering of communication messages, program flow control checking, online memory allocation testing and minimisation of real time influences by avoiding multitasking.

Diagnostic capability is measured by coverage factors, which represent the percentage of failures that will be detected. Detection rates of 60%, 90% and 99% are designated respectively as low, medium and high coverage.

Safety systems should also be designed for high immunity to common stressors. Typically, this might include isolated backplane and I/O, plus built-in diversity of processors and operating modes.

Redundancy is the final factor determining SIL ratings. Simply, the greater the redundancy and monitoring, the higher the level of safety becomes. Dual redundancy can mean, for example, that a system with a probability to fail with serious consequences once every 50 years can achieve a probability of failure of only once every 2500 years.

Despite the complexity of the detail, the basic tenets of AS61508 are simple. First, follow the safety lifecycle outlined in the standard and identify SIL requirements. When designing a safety system, look for rugged high-strength design, both in terms of hardware and software. Ensure the system has good common cause strength and the ability to tolerate and detect single failures and do not overlook the impact of field devices in SIL analysis.