

How functional safety helps to save lives

In this article Ron Bell explains functional safety and looks ahead to the revision of the IEC 61508 standard that is due for publication in 2010.

On 11 December 2005, at a fuel depot in Buncefield, UK, an overfill switch designed to monitor fuel levels failed as workers pumped fuel into a tank. The fuel spilled over into a bund, vaporised, reached an ignition source, and exploded, resulting in a fire that took four days to extinguish. Twenty white cylindrical fuel tanks collapsed like marshmallows held over a campfire too long. Although there were no fatalities, homes were damaged and residents were evacuated.

A few months earlier on 23 March 2005, in the USA, a pipeline exploded at a BP petrochemical plant in Texas City, killing 14 people.

Not all failures are as spectacular or public as Buncefield or Texas City but they underscore the fact that systems fail, even with apparent safeguards in place. After accidents like these, safety experts pore over the chain of events and do a hazard analysis. IEC functional safety expert Ron Bell says a hazard analysis helps identify what went wrong. Most important, pinpointing the cause helps design control systems to lower the risk of other hazardous events. Bell's professional expertise lies in functional safety. He is principle of Ron Bell Consulting Ltd, a safety consulting firm, and a member of the IEC Advisory Committee On Safety (ACOS) with special responsibilities for functional safety.

Functional safety systems are active rather than passive. A seatbelt would not be a functional safety system; an airbag would. As the world market continues its shift towards globalisation, Asian markets expand, litigation costs rise and environmental awareness continues to grow, so does the need to establish good practice standards whether you are designing air bags for an automobile, a Ferris wheel, a train or a baby incubator. This has led to more countries adopting safety standards. The market for functional safety, which reached \$850million in 2007, is expected to grow by \$50million in 2008.

In the world of safety standards, such as the IEC 61508 (Functional safety of electrical, electronic and programmable electronic safety-related systems), 'good practice' has a specific meaning. The idea is to achieve functional safety for safety systems. To do this, it is necessary to consider every phase from initial concept through development of the safety requirements, design, construction and installation, to maintenance and modification. Bell calls this the 'safety lifecycle.' This lifecycle facilitates the building of safety systems to defined safety performance levels and lessens the risk of an accident. Every safety system requires safety functions to be performed and these are carried out through a chain of electronic and sometimes human links. The first step identifies what needs to be done by the safety system. This part of the IEC 61508 standard deals with the safety function. It identifies the starting risk, without safeguards, and identifies what is needed to achieve the target, tolerable risk.

It is the 'tolerable' part that gets difficult from a social point of view, says Bell, because it has to be acknowledged that systems will fail, and the challenge is to be able to maximise the benefit of computer-based technology while achieving tolerable risks for the plant under control. He explains: "The safety systems on petrochemical plants are increasingly computer-based and the failure modes are complex. It is only by adopting a systematic approach to all aspects of the design and application of such safety systems that sufficient confidence can be gained that the target tolerable risks have been achieved."

The price of safety

The answer to these questions determines how reliable the safety system needs to be, which brings us to the difficult part: what are citizens prepared to pay for safety? The irony here seems to be that saving lives means determining, at least theoretically, how many deaths you are willing to live with. In the UK, the determination of what constitutes a tolerable risk is approached through the concept of ALARP. The ALARP concept requires risks be made 'As Low As Reasonably Practicable.' Bell says: "In any assessment, to determine whether the risks have been reduced to achieve ALARP, additional measures to reduce risks can only be ruled out if the sacrifice involved, in terms of money, time and trouble, are grossly disproportionate to the benefits to be gained."

Once these safety and performance boundaries are agreed on, the design phase determines the safety levels of a particular function. Because these systems are built to a designed failure rate, functional safety experts like Bell describe safety in terms of integrity rather than reliability. These safety integrity levels (SILs) number 1 through 4, where 1 is the lowest and 4 is the highest.

This is where IEC 61508 comes in; the IEC Standard provides design parameters for each level. It is easiest to think of these systems as rings encircling a particular design, such as a petrochemical plant. The addition of each ring brings another layer of safety. One ring could represent an electronic alarm; another could represent a pressure relief system. Because of this multi-layer approach, not all safety systems would need to be designed to the rigour of SIL 3 or 4. The more systems you have, the lower each SIL needs to be. From a safety integrity point of view, putting these rings in place from the start is the best way to prevent accidents.

When Bell headed the Electrical and Control Systems Group in the UK's HSE (Health and Safety Executive), he and his staff analysed 37 incidents involving control system failures by lifecycle phase. The results, published in a book titled 'Out of Control: Why Systems Go Wrong and How to Prevent Failures' (HSE Books 2003), showed that more than 60 per cent of failures happened because there were inadequate specifications, meaning that failure was built into the systems before the service was up and running.

Bell states: "Identifying what the hazards are is actually very difficult because you need to identify what could go wrong before you can say 'this is how to prevent it.' So in a complex piece of machinery or a plant if you cannot identify what could go wrong then when it goes wrong there is nothing in place to stop it."

IEC 61508 - the complete package

But this is where IEC 61508 helps. The standard gives directions on the thoroughness needed in terms of design and confers special safeguards for design requirements in safety systems, according to Bell. This standard is different from other IEC standards because it includes both technical requirements and management specifications for competent, properly trained staff. People control computers; they turn switches on and off and monitor equipment. They make mistakes. "This standard is a complete package," says Bell.

There are plenty of places for things to go wrong when designing a safety system. If you have not identified key steps in the chain then you cannot put something in place to prevent them. If you have missed what the safety system is supposed to do then you cannot do anything about it when something goes wrong. You can also mistakenly design a safety system to a SIL 1 when it should have been a SIL 3, which increases the chances an accident will happen.

Plus, the economics of design always bring challenges. Everything cannot be designed to the best specifications because that is too costly. Bell says: "This is not a simple case of, 'how many people are you going to kill if we can only afford this.' It is necessary to understand the legal requirements of the country in which the equipment is being used and ensure that the tolerable risk is achieved according to those legal requirements."

Many plants and factories, though, were built decades ago. These 'legacy systems' pose unique challenges, especially in terms of personnel. Long-time staff may know a piece of equipment so well that they no longer need to look at documentation for daily operations and maintenance. They may also stop documenting anything. Over time, safeguards can be lost or not understood. For legacy systems IEC 61508 allows a gap analysis to be undertaken. Essentially, this allows you to check to see how far the old safety system falls short of current good practice as specified in IEC 61508. A judgement then needs to be made as to what action to take. In many instances the old safety system differs from a safety system that you would design today. Bell cautions: "The key issue is ensure that after the gap assessment is undertaken a considered plan of action is developed."

IEC 61508 is currently under revision, with the process due to be complete by early 2010. Bell comments: "The revision has been a challenge because we have to balance any technical changes with the improvements in functional safety that would result and the impact such changes would have on the current customer base. Most importantly we have to base the changes we make primarily on the comments we have received."

Further information on the IEC 61508 series of standards is available on the IEC website.

This article by Jeanne Erdmann was first published in the January 2008 edition of the IEC's E-TECH.

<http://www.iec.ch>