WiringMatters
Your insight into BS 7671 www.theiet.org/wm

Electromagnetic resilience: a new approach to EMI

In this article, electromagnetic specialist we first introduces the new(ish) engineering discipline of functional safety; then the very new engineering discipline of risk-managing electromagnetic interference (EMI) to help achieve functional safety.

Functional safety risks associated with the incorrect functioning of electronics

Functional safety is an increasingly important engineering issue that is very different from traditional product safety concerns, such as electric shock, fire, heat, etc.

Most of the safety standards we use don't specifically mention functional safety so, although required for legal compliance with product liability laws and EU safety directives, it is often overlooked, leaving people exposed to uncontrolled safety risks and manufacturers to uncontrolled financial risks. For example, if the electronics controlling a car, plane, train, radiation therapy machine, nuclear power plant, industrial machine/process, etc., malfunctions, the result can have serious safety consequences for people – and serious liability and reputational consequences for the manufacturers of said electronics.

Almost every aspect of our lives now relies on the correct functioning of electronics, usually microprocessors running software programs. Where electronic malfunctions could increase safety risks, we say that it presents functional safety risks.

Unfortunately, for at least the last 30 years it has been impossible to fully test even a modest microprocessor or software program, because:

- their complexity creates so many possible states that their system could get into that they can't all be tested in any reasonable timescale; and

- digital systems are discontinuous and non-linear, so testing any percentage of the states that a system could be in cannot predict anything about the untested states.

The result of the above is that all digital systems can malfunction despite any amount of testing.

Safety and product liability laws and regulations in the UK generally require the equipment, system or installation not to expose an ordinary user or a third party to a risk of death at a rate of greater than one in a million per year. This limit applies over the entire lifetime of the equipment, which could in some cases exceed 30 years.

Higher risks than this are generally permitted in cases where the manufacturer shows that the cost of further reducing the risk would significantly outweigh the value of the lives thereby saved (up to a maximum risk limit). These safety risk numbers come from a wide range of free guidance documents issued by the UK's Health and Safety Executive (HSE).

Standards for functional safety

The problem of not being able to thoroughly test digital systems was first recognised in the 1970s. So, by the 1980s, a huge international effort was underway to try to establish suitable functional safety engineering techniques – in system, hardware and software design, and in

its verification and validation – to ensure that safety risks could be demonstrated to be acceptably low despite the intractable problems with testing multiple system states.

The first international standard on functional safety, IEC 61508 *Functional safety of electrical/electronic/programmable electronic safety-related systems*, was published in 2000, and a number of application-related functional safety standards have since been based upon it, including:

- IEC 61511 *Safety instrumented systems for process industry* (in USA: ANSI/ISA S84)
- IEC 62061 *Safety of machinery*
- IEC 62278/EN 50126 *Railways – specification and demonstration of reliability, availability, maintainability and safety*
- IEC/EN 50128 *Software, railway control and protection*
- IEC/EN 50129 *Railway signalling*
- IEC 61513 *Nuclear power plant control systems*
- RTCA DO-178B *North American avionics software*
- RTCA DO-254 *North American avionics hardware*
- EUROCAE ED-12B *European flight safety systems*
- ISO 26262 *Automobile functional safety*
- DEF STAN 00-56 *Accident consequence* (UK military)

IEC 61508 and its family of functional safety standards deal with the impossibility of testing a sufficient proportion of a digital system's states by, first, determining the level of risk that is acceptable. This level is then used as the basis for the appropriate application of a range of well-proven techniques and measures (T&Ms) in the design, verification and validation of the systems. The hardware and software that comprise all these T&Ms are justified in detail in a 'Safety Case', alongside an independent assessment of all of the afore-mentioned items and, finally, any iteration necessary to satisfy the assessor.
Where a control system is complex it is normal to identify the functions that are only concerned with managing the functional safety risks, removing them into a separate safety-related system (SRS). This SRS is less complex and thus more amenable to using the above process to reduce safety risks to acceptable levels.

It is important to understand that the discipline of functional safety applies to the entire facility, including the management of its personnel (see Figure 1). The acceptable safety risk level is achieved by the combination of several risk-reduction methods, so the electronic systems do not have to shoulder the whole burden of managing the risk by themselves. However, IEC 61508 and the standards developed from it only provide requirements for the SRS itself.

A powerful technique in functional safety is to determine one or more 'safe states' that the equipment can be switched into by the SRS when it detects the potential for a hazard to occur. For example, opening a machine guard causes the machine's SRS to stop the machine quickly enough to avoid injury.

However, IEC 61508 also includes T&Ms suitable for applications in which all of the functional safety requirements have to be provided by electronic systems, and for electronic life-support systems that might have no safe states to be switched into, so must continually operate at least well enough to prevent death or serious injury.

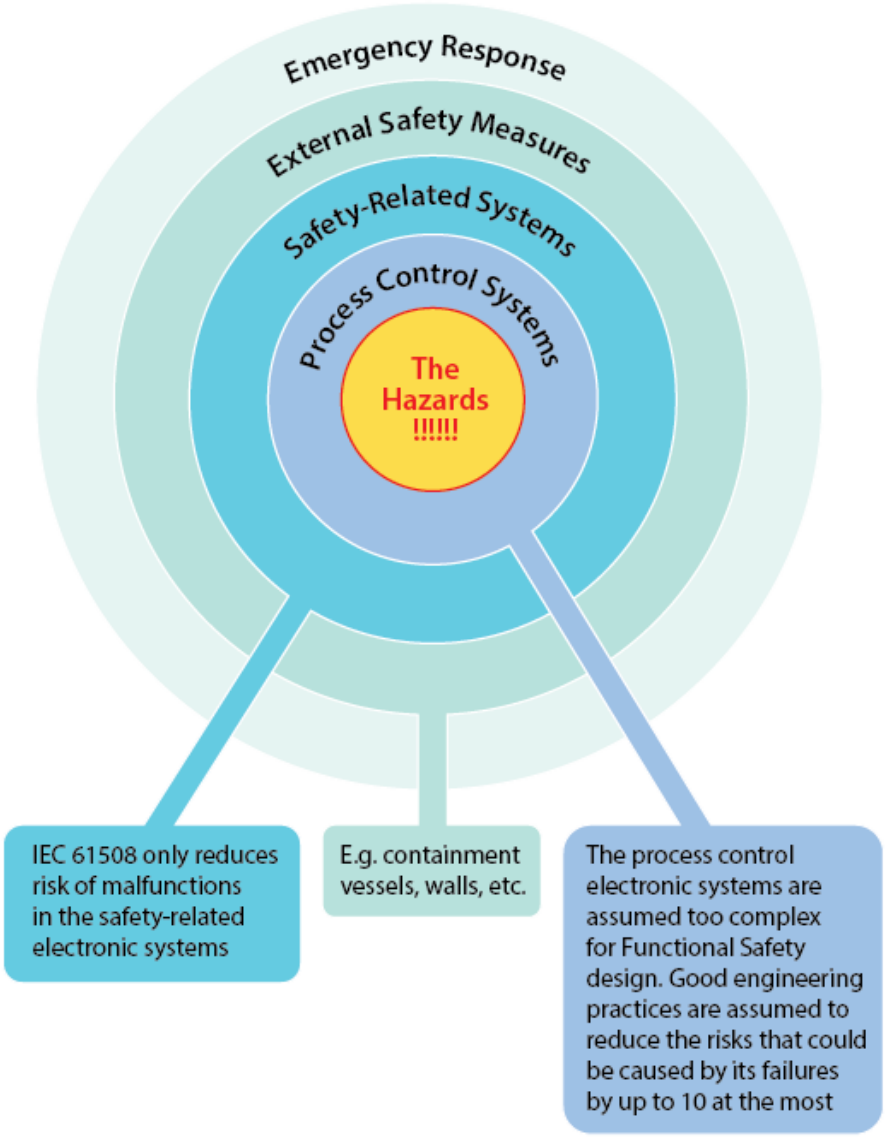

Figure 1: Example of the functional safety of an industrial processing plant

Managing functional safety risks due to electromagnetic interference (EMI)

All electronics can suffer from errors, malfunctions and/or failures due to electromagnetic interference (EMI), so EMI must be taken into account when complying with functional safety.

When applying IEC 61508 or its family of functional safety standards, it is typical to allocate one-tenth of the acceptable risk level to EMI. So, for example, if a digital system must maintain a risk of less than one death per million per year over its complete lifecycle, then the risk of EMI causing it to suffer an error, malfunction or failure that could lead to a death must be less than one in 10 million per year.

Electromagnetic compatibility (EMC) is traditionally assured by laboratory testing and, where functional safety risks are concerned, it is traditional to apply the standardized immunity tests at higher levels. However, although this approach has been recognized as inadequate since 2004, it is still generally relied upon. The result is that people are being exposed to uncontrolled functional safety risks and manufacturers exposed to uncontrolled financial risks, due to EMI.

Immunity testing is inadequate on its own because, as previously discussed, it is physically impossible to test all possible states of a digital system.

Further, because functional safety risks must be low enough over the whole lifecycle, proving that EMI will not cause excessive functional safety risks must also take into account the effects of the following on equipment's electromagnetic characteristics:

- corrosion, aging, wear, contamination, etc.
- electrical faults (for example, a broken filter ground wire).
- foreseeable use/misuse (for example, leaving a shielding door open, replacing a shielded cable with a less-well-shielded type).
- mechanical stresses and strains that alter the impedances of electrical bonds, EMC gaskets, etc., degrading the performance of shielding and filtering.
- the very wide range of variations in the characteristics of real-life EMI when compared with very simplified EMC laboratory tests.
- different types of EMI occurring simultaneously or in some critical time sequence.
- reasonably foreseeable combinations of all of the above independent variables.

Even if it was possible to test all the states of a digital system, taking the items in the above non-exhaustive list into account shows that attempting to prove functional safety compliance over the lifecycle by EMI immunity testing alone would result in an impractically large test plan.

Instead of attempting to rely on immunity testing, we need to use the IET's new 'electromagnetic resilience' approach. This builds on the existing expertise in the EMC testing and functional safety communities and is summarised in Figure 2.

IEC 61508 describes many T&Ms for use in design, verification and validation to reduce risks caused by errors, malfunctions, faults, etc. in hardware and software to the degree required to comply with functional safety, and functional safety designers and assessors have become very experienced in applying them.

These T&Ms operate on the digital data and other signals, or on the electrical power supplies, and were never intended to deal with EMI. However – because EMI can only affect data, signals and/or power supplies – many of IEC 61508's design T&Ms are very effective in dealing with the effects of EMI.

Accordingly, the IET's new *Code of Practice on Electromagnetic Resilience* (due to be published in early 2017) details which IEC 61508 T&Ms are good for dealing with EMI, and how to improve their benefits for electromagnetic resilience.

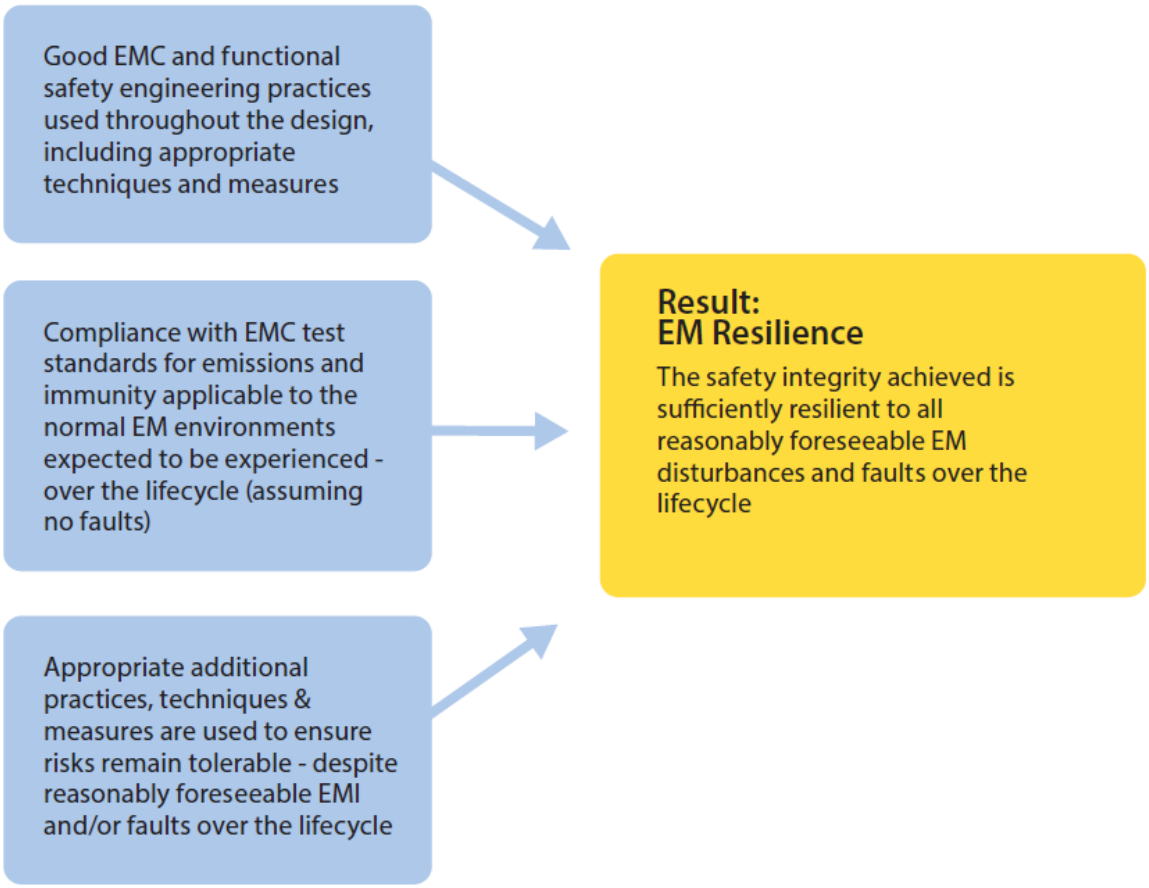

Figure 2 Overview of the IET's electromagnetic resilience approach

The IET's new *Code of Practice on Electromagnetic Resilience* is now available for pre-order.