# THE EASY PATH TO FUNCTIONAL SAFETY COMPLIANCE

*Functional safety has an unfair reputation as being difficult, obscure and only doable by experts. This short article intends to show the practitioner that it is not hard to achieve functional safety. It needs attention to a few important principles; the main driver is the need to demonstrate duty of care in managing risks.*

*By Mirek Generowicz, I&E Systems Pty Ltd, FS Expert (TÜV Rheinland #183/12)*

'Duty of care' applies to everybody that has some degree of influence in health and safety.

If you are a manager or a team leader it applies especially to you. It has meaning not only in health and safety legislation (statute law) but also in common law (in contract or in tort, which is the law of 'wrongs' or damages). We can be prosecuted for not fulfilling our statutory duty of care and punished with fines or imprisonment. Under common law we can be sued if we have failed to meet a contractual duty of care or if we have caused damage or harm.

Duty of care requires us to be able to show that we have taken 'reasonable' steps to prevent harm. Wherever there are well established standards or work practices that can be applied to prevent harm then we are obliged to consider them and to apply them appropriately. If we can't demonstrate that we have taken reasonable care then we may be found negligent.

No matter which standards or practices we choose to apply and no matter how we choose to interpret them, we need evidence to show that we have met our duty of care. This includes meeting a standard of 'reasonableness'.

Functional safety (as defined in the next section) contributes to the fulfilment of a duty of care. It is an area in which many companies struggle to achieve and demonstrate compliance.

Many companies leave it to the experts to worry about compliance. If we have technical experts that we can rely on, it may be possible to achieve partial compliance in an ad-hoc way – without formal systems and without setting clear expectations. But without formal evidence it is difficult to demonstrate clearly that we have fulfilled our duty of care.

The requirements for evidence are not particularly complicated or difficult. If we are responsible for some area of functional safety the easiest way to achieve and to demonstrate compliance is to make sure that the evidentiary requirements are clear to everyone concerned.

## FUNCTIONAL SAFETY AS A SPECIFIC EXAMPLE

This article examines functional safety as a specific example of using evidence to show a duty of care has been met. The same principles apply equally to any other form of technology based risk reduction, such as the application of electrical equipment in hazardous areas, the application of pressure relief valves or the use of certified plant such as boilers and pressure vessels.

Functional safety refers to the use of instrumented systems to implement safety functions that achieve a defined level of risk reduction. Safety functions are each designed to detect a particular hazard and to execute some specific action to achieve or maintain a safe state.

Functional safety always starts with a clear definition of the hazard and how much risk reduction is required. It ends in being able to demonstrate that the required risk reduction is actually achieved.

There are 2 main standards that we refer to in achieving functional safety:

IEC 61511 'Functional Safety – Safety instrumented systems for the process industry sector'

IEC 61508 'Functional Safety of electrical/electronic/programmable electronic safety-related systems'.

IEC 61508 is a more general standard that can be applied in any industry. IEC 61511 is simpler and easier to understand but it only applies to process industries – not manufacturing industries. It is typically applied for chemical processes, oil and gas production and refining, pulp and paper, and (non-nuclear) power generation.

## ASSESSING RISK REDUCTION

To gauge the risk reduction that a safety function actually achieves we need to assess the likelihood of that safety function failing.

For instance, for a safety function to reduce the risk of a hazardous event by a factor of 10 we need to show that the chance of the function failing when it is needed will be less than 10%.

There are two different ways in which functions can fail. They can fail either due to some random hardware failure or they can fail because of a systematic failure.

## RANDOM FAILURES

All equipment is subject to some level of random failure. There is no way of preventing all random failures from occurring. They are caused by a variety of degradation mechanisms. They occur at completely random times but at rates which can be predicted and measured. Failure rates can be expressed as failures per hour or as the mean time between failures. Estimating the failure rates of all of the hardware components in a safety function allows us to predict the probability that the function will fail when it is needed. We can improve the design if necessary to limit failure rates to below a given target.

Engineers and technologists usually find it easy to understand failure rate measurements and calculations. Accurate and reliable data may be hard to find but the data only needs to be accurate within an order of magnitude. Risk reduction is not a precise scientific exercise.

It is usually not too difficult to obtain enough failure rate data to make a reasonable prediction of a function's probability of failure and to provide evidence that sufficient risk reduction that can be achieved.

## SYSTEMATIC FAILURES

'Systematic' refers to things that are well organised according to some system, process or plan.

Systematic failures can be harder to deal with than random failures because they cannot be modelled using probability theory.

It is important to appreciate the difference between 'systematic' and 'systemic'. 'Systemic' refers to something that affects a whole system. For instance, systemic corruption affects a whole organisation from top to bottom, whereas systematic corruption is just very well organised.

Systematic failures have definite causes. Systematic failures are usually the result of human failings in specification, design, manufacture, software, installation, testing, operation or maintenance. They occur due to a lack of planning, organisation and management. A significant proportion of systematic failures can be traced to human behaviour. Although we cannot calculate the probability of systematic failures, we can reduce their likelihood by addressing their causes.

Out of all of the major accident events around the world over the past 30 or 40 years at least 95% were caused by multiple systematic failures. Incidents such as the Macondo well explosion have been shown to have multiple causes. The ultimate disaster is always caused by the failure of many protective mechanisms, practices or procedures, one after another.

It is hard to identify any major accident events that have been caused solely by random hardware failures. We can often identify 10 or more distinct failures contributing to each major accident event.

Similarly, closer to home, motor vehicle fatalities are never caused by the failure of a single mechanical component. Fatalities are always caused by the failure of several independent layers of protection, one after another. All accidental fatalities can be prevented if we have sufficient layers of protection in place.

The question is 'how can we show that we are doing enough to minimise systematic failures?'

Systematic failures can never be completely eliminated, but they can all be either avoided or controlled to some extent through appropriate procedures and practices.

## TECHNIQUES AND MEASURES

In the functional safety standards IEC 61511 and IEC 61508 these procedures and practices are referred to as 'techniques and measures'. The standards describe many techniques and measures that may be applied to manage the risks of systematic failures. Most of these techniques and measures are already well understood and widely practised. The fundamental ideas are essentially the same as those commonly used in project management and quality management.

Exactly how much effort needs to be put into managing systematic failures depends on how much risk reduction is required. To achieve a risk reduction factor of 1,000 we would need 100 times more attention to detail in preventing mistakes than if we only needed to achieve a risk reduction of 10.

Imagine driving a car on icy or wet and slippery roads. It takes a lot more attention and care because the risk is significantly higher.

## CLEAR EXPECTATIONS AND AN AUDIT TRAIL

Success in management relies firstly in making sure that people know what is expected of them, secondly in making sure they have the information, tools, resources and competencies that they need and thirdly in 'closing the loop', making sure that people actually do what is expected.

Auditable evidence is essential for managing performance and to demonstrate that expectations are being met. Without evidence we cannot monitor performance and we cannot 'close the loop'.

That applies equally whether we are managing operations and maintenance, projects, quality or safety.

## EVIDENCE FOR FUNCTIONAL SAFETY

To demonstrate that we have achieved the risk reduction that we need from functional safety we need evidence to show how we manage both random hardware failures and systematic failures.

Evidence for the probability of random hardware failure can be demonstrated through gathering failure rate data and by documenting probability calculations in a report.

The other 95% of the evidence we need is to demonstrate how we reduce the risk of systematic failures. For that we need evidence of effective management.

## SAFETY LIFECYCLE

The functional safety standards talk about defining a 'safety lifecycle' in terms of lifecycle phases. The safety lifecycle is similar to a project lifecycle. The easiest way to understand and define a lifecycle is by identifying the key inputs to and outputs from each phase.

Defining a set of deliverables at the start of a project is a very natural way of giving project team members a clear understanding of what they are expected to do. At project handover the complete set of deliverables will make up the documentation 'dossier' (or database) for the project. The dossier has to be regularly updated with operations and maintenance records throughout the life of the plant.

Dossiers are essential for documenting compliance for electrical equipment in hazardous areas or for pressure safety valves. Similarly, safety instrumented systems need to have a dossier. To put it simply, the safety lifecycle plan outlines all of the deliverables that need to be kept in the 'functional safety dossier'.

The standards give clear guidelines on what should be kept in the dossier. Refer to IEC 61511-1 section 19.2.9 or to IEC 61508-1 section 5.

The dossier should always include documents describing plans for the management of functional safety.

## THE MANAGEMENT PLAN

Some people manage to achieve good results without any formal planning. If we have a task that we understand well and if we can rely on good people to help us then maybe we can get by without a plan. As soon as we start dealing with complex systems we need planning.

The old adage applies universally: Proper Prior Planning Prevents Poor Performance.

We know this to be especially true for project management, risk management and quality management.

To comply with the standards we need evidence of effective management planning for any safety systems project or for the operations and maintenance of a safety system.

Both IEC 61511 (sections 5, 6 and 7) and IEC 61508 (sections 6, 7 and 8) give similar requirements for management planning.

The management plan clearly defines all of the activities needed to achieve success and the records to be kept. It not only defines the evidence that will be kept in the safety lifecycle dossier, it defines the 'why, who, how, where and when'.

## SHOW ME THE EVIDENCE

Early in the 19th century the DuPont family established the rule that the managers at their explosives plants should reside on the plant grounds. That ensured a personal commitment to safety. To sleep easily at night any manager needs to be confident that safety is being achieved.

To establish that level of confidence it is not enough to plan and direct a team to achieve safety, managers need hard evidence that the plan is working in practice and that safety is being achieved.

The best way to assess the evidence is to conduct regular audits and then to review and assess the results. If there have been no audits or assessments the manager cannot have confidence that duty of care has been fulfilled and can been demonstrated.

The relevant standards set out very clear requirements for evidence and they provide a solid foundation for audit. These days most suppliers are certified to some sort of quality or safety standard such as IEC 61508, IEC 61511, ISO 9001, AS/NZS 4801 or OHSAS 18001.

A plant manager cannot simply assume that suppliers (and that includes EPC or EPCM contractors as well as systems suppliers) will achieve safety because they have certification. Certification on its own does not guarantee results.

Without audit and review there can be no confidence that the evidence exists, and that evidence might one day be needed in court.

Take the simple example of a document review or a 'check print'. I have seen many examples of documents or software that have been signed off as 'reviewed' or 'checked' but with no evidence of how it was checked and against what basis. If we don't keep a record of what we checked it is as if the work had not been checked at all.

Imagine picking up your car from a service mechanic. If the mechanic can't show you a completed checklist and explain what work has been done then what confidence do you have that all of the necessary maintenance has actually been done?

## THE BUCK STOPS AT THE TOP

In conclusion, if you are a manager or a team leader you have a duty of care in managing hazards in the workplace. You need to have hard evidence that demonstrates that you have taken reasonable steps to comply with appropriate standards.

IEC 61511 and IEC 61508 are the standards that apply when we use instrumented systems to achieve hazard risk reduction. Both standards require similar evidence.

The easy way to achieve functional safety is to make sure that you and your team know what evidence is needed. Start out with a plan so that everybody knows what they are supposed to be doing and what evidence they are supposed to be keeping.