Sidebar

Functional Safety Unmasked

The 10 minute guide to IEC 61508

The functional safety management discipline ensures that software and electronic systems tasked with protecting life and property reliably perform their missions. International standard IEC 61508 provides a set of development life cycle activities for achieving this by identifying hazardous situations that could occur, evaluating the risk that a hazard could cause an accident and reducing that risk by building high integrity safety functions and operational procedures into safety-related systems.

Les Chambers • Chambers & Associates Pty Ltd • www.chambers.com.au

What is a Safety-related System?

A system is "safety-related" if its failure can cause harm to life and property. Examples are road traffic signalling and office building smoke extraction systems.

Why is Functional Safety Necessary?

The consequences of system failure have become more serious as we increasingly trust software and electronic systems to protect us from harm. At the same time these systems have become infinitely more complex with the introduction of computer software and electronic hardware.

Software can be both a benefit and a hazard. It is highly adaptable to any situation but can be hazardous because: 1) its inherent complexity makes software development an error prone activity; 2) its invisibility makes managing zero defect code development impossible; and 3) its lack of testability makes it difficult to find and fix all defects that might cause dangerous failures.

Making it Safe with IEC 61508

Released in 1998, IEC 61508 provides a framework for embedding a functional safety program in a systems engineering project (refer Figure 1). Functional safety activities are carried out in parallel with normal system development, operation and maintenance tasks. They commence with a hazard analysis of the target system in the concept phase and extend to assuring its safe decommissioning and disposal. The core activities of a functional safety program are as follows:

Identifying Hazards

A hazard is any situation that could cause harm. Examples are, heavy rain on a highway and failure of traffic signals. The former is a function of a system's environment and the latter comes about through dangerous failure of the system itself.

Hazards are analysed by identifying their causes and the possible negative consequences that might ensue. For example, the dangerous failure of a traffic signal could be caused by a logic error in the traffic signalling controller's software program. The consequence could be conflicting traffic flows simultaneously receiving green signals.

Assessing Risks

A safety risk is expressed in terms of the severity of a hazardous event and its likely frequency. For example, a traffic signalling controller displaying conflicting green signals might cause the death of a motorist. Looking at past experience and/or analysing the existing design of the target traffic signalling controller, a hazard analysis team estimates the frequency of this type of failure. It then estimates the number of "opposing green" incidents that might have to occur before a motorist is killed. From this the fatalities per year are estimated given that no additional safety features are added to the existing system.

The next step is to determine if this risk is tolerable. Setting risk tolerability limits is an emotional task. Most of us accept that no human activity is without risk however we find it difficult to quantify what we will tolerate. Some industry sectors have quantified maximum tolerable risk against a background of what the community accepts as the normal risks of every day life. For example, in Australia the risk of a road traffic fatality is 1 in 10,000/yr averaged over the population. Adopting the principle that the deployment of a new system should introduce negligible risk we might set the tolerable

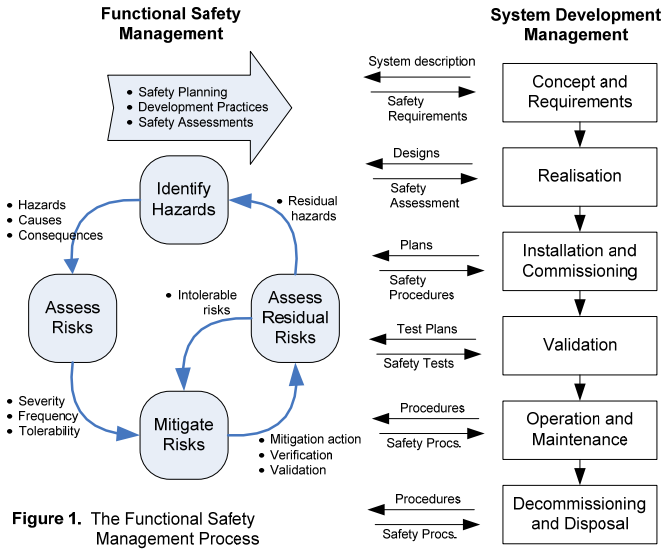

Figure 1. The Functional Safety Management Process

risk of fatality due to a traffic signalling system failure at 1 in 1,000,000/yr, two orders of magnitude less than the actual background risk.

Mitigating Risks

If a safety risk is intolerable you can take one or more of the following mitigation actions:

- Add safety functions to the system
- Employ other technologies
- Change the environment to make it inherently safer
- Introduce manual safety procedures.

In the case of the traffic signal, an independent conflict monitor could be added to the signalling controller to detect conflicting greens and "protect" it from dangerous failure by forcing the signals to flashing yellow. Alternatively an overpass could be constructed to eliminate dangerous conflicts in traffic flow.

If you introduce a protection system to reduce risk you are now "trusting" it to do its job. Safety integrity is a measure of that trust. Say for example, that to deliver an acceptably safe passage through an intersection, the dangerous failure rate of your traffic signalling controller cannot exceed 1 in 10,000 years (λ_p). But what if your estimated failure rate for the current controller is 1 in 10 years (λ_{np})? Clearly your conflict monitor must contribute the additional safety margin. Its required reliability can therefore be quantified as Average Probability of Failure on Demand (PFD_{avg}) = λ_p/λ_{np} = 1 in 1,000 or, in plain English, for every 1,000 dangerous failures of the controller the conflict monitor must work, as specified, 999 times.

Table 1. IEC 61508 Safety Integrity Levels (SILs) for low demand operation

SIL	Prob. Of Failure on Demand (PFD_{avg})	Safety Availability % ($(1 - PFD_{avg})*100$)
4	$\geq 10^{-5}$ to $< 10^{-4}$ (≥1 in 100,000 to < 1 in 10,000)	99.999 to 99.99
3	$\geq 10^{-4}$ to $< 10^{-3}$ (≥1 in 10,000 to < 1 in 1,000)	99.99 to 99.9
2	$\geq 10^{-3}$ to $< 10^{-2}$ (≥1 in 1,000 to < 1 in 100)	99.9 to 99.0
1	$\geq 10^{-2}$ to $< 10^{-1}$ (≥1 in 100 to < 1 in 10)	99.0 to 90.0

IEC 61508 classifies safety integrity in terms of 4 bands labelled 1 to 4 where 4 is the highest. Safety-related systems can then be characterised by a Safety Integrity Level (SIL). For example, railway authorities classify railway signalling as a SIL 4 application while road transportation authorities have classified variable message signs as SIL 1. In our example the conflict monitor, with a required PFD_{avg} of 1 in 1,000, would be classified as SIL 2 (refer to Table 1).

Assessing Residual Risks

Taking into account the risk reduction measures already in place, a risk assessment team determines if the safety risk has been reduced to a level that is as low as is reasonably practicable (ALARP). You have reached ALARP when further risk reduction is impracticable or its cost is grossly disproportionate to the improvement gained. If the risk is intolerable further risk reduction measures are introduced. For example, in road transportation risk might be further reduced by modifying the geometry of an intersection to improve driver visibility. If all else fails you may choose to refuse the risk and not engage in the risky activity at all.

Specifying Safety Requirements

Testable safety requirements are the most important outputs of a hazard analysis. A safety requirement describes the behaviour of a safety function and specifies its required reliability in a way that can be verified as the system is developed and validated before it is set to work.

Specifying Hardware and Software Reliability

Hardware reliability is commonly specified as a failure rate (e.g. failures per hour). Hardware systems can be built to this specification as manufacturers provide failure rate estimates for components such as integrated circuits, switches and indicators. In contrast software reliability cannot be specified as all software failures originate from human error which is notoriously unpredictable. This failure mode is referred to as "systematic failure", for example, failure to follow proper practice in system development and operation resulting in incorrect system requirements, design errors and coding errors in software programs. Systematic faults also extend to inadequate design review, incomplete testing and lack of competence in managers, developers and operators.

Question: How then, as a customer, can you determine that a developer has delivered software to a standard of reliability required by your target SIL?

Answer: IEC 61508 indicates various development practices that, if followed, will allow a developer to claim that the delivered system implements safety functions at the required SIL. For software, SIL 1 and 2 ratings are achievable by an ISO 9001 compliant organisation with the addition of enhanced review and testing. SIL 3 requires higher levels of validation while SIL 4 involves higher skill levels again, featuring "formal methods" in design.

Is Your Organisation Safety-aware?

If you're working for a functional safety-aware company you'll have regular contact with:

Management

- A senior manager responsible for functional safety
- A safety authority on each safety-related project
- Decision making from quantified facts (e.g. consolidated safety incident metrics)
- Procedures for design and operational hazard and risk analysis, functional safety assessment, safety function verification and validation, configuration management and safety audits
- Safe operating and maintenance procedures
- Safety meetings
- Trained staff capable of recognising hazards and following safe development processes.

Project Deliverables

- Project Safety Plans
- Documented quantitative risk tolerability criteria
- Preliminary Hazard Analysis Reports
- Operation and Support Hazard Analysis Reports
- Safety Requirements Specifications
- Hazard Logs covering the complete development life cycle including corrective action and closeout
- Design Safety Review Reports including analysis of all design changes
- Evidence of compliance with the development practices "highly recommended" by IEC 61508 for the target SIL
- Safety related test plans, procedures and test results
- Safety Cases providing reasoned arguments that systems, as delivered, are acceptably safe
- Records of incident analysis and corrective action
- Records of system failures.

Is Functional Safety Your Issue?

If you are responsible for buying or building a system that will be trusted to preserve human life and property, functional safety IS your issue. The functional safety discipline described by IEC 61508 reduces risk by systematically evaluating what could go wrong and building safety into trusted systems to ensure that it doesn't. IEC 61508 sets an internationally recognised standard for due diligence in the development of safety-related systems. Objective evidence of compliance with this standard is therefore a defence against claims of negligence. By embracing the standard we protect both system users and our professional reputations from harm.

Les Chambers is Managing Director of Chambers & Associates Pty Ltd, a systems engineering consulting company. Contact him at les@chambers.com.au.