Chapter 6

EMC and Functional Safety

Note: this chapter is intended only as an overview of issues relating to functional safety. It makes reference to a number of source documents. In no way is it comprehensive or definitive, and you are strongly recommended to consult the most up-to-date documents if you are actively involved in working with safety-related systems.

The rest of this book deals with EMC as it relates to control of emissions into the environment and control of immunity from environmental disturbances. The latter of these is normally concerned with maintaining a specific level of performance: the general performance criteria (see section 10.3) quoted in immunity standards refer to an "acceptable degradation of performance" as being set by the equipment manufacturer for a pass/fail criterion for such tests. Such standards explicitly exempt safety considerations.

But there are many applications where the continued safe operation of a system depends on correct performance of electronic apparatus. Transport and industrial process control are two examples where many functions cannot be allowed "acceptable degradation": quite the opposite, it is necessary to take measures to guard against any fault condition degrading the electronics and creating an unsafe situation. This has led to the development of many techniques of design and analysis which collectively allow a product to be certified to a "Safety Integrity Level" (SIL), and designers of high-integrity systems are by now familiar with these techniques.

But until recently, the effects of EMI have hardly featured in such analysis. Quite incorrectly, it has been assumed that compliance with EMC Directive standards was sufficient for EMC-related safety. Somewhat belatedly, this lack is now being addressed. What is the consequence of the EMC dimension for functional safety design?

6.1 Design for functional safety

6.1.1 IEC 61508

The most general of the functional safety specifications that have been developed is IEC/EN 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems* [175]. Other specific sectors – process industry, nuclear industry, railways, automotive, military – also have their own standards. IEC 61508 defines four SILs based on hardware and systematic safety integrity, SIL 1 being the least dependable and 4 being the most. The quantification of these levels are listed below in Table 6.1.

Table 6.1 Probabilities of failure versus SIL

SIL	Probability of failure on demand (low demand operation)	Probability of failure per hour (continuous operation)
1	10^{-1}–10^{-2}	10^{-5}–10^{-6}
2	10^{-2}–10^{-3}	10^{-6}–10^{-7}
3	10^{-3}–10^{-4}	10^{-7}–10^{-8}
4	10^{-4}–10^{-5}	10^{-8}–10^{-9}

The assignment of a particular SIL depends on an analysis of the maximum probability of dangerous failure, along with an assessment of the development process applied to the equipment. For any given system, “dangerous failure” must be carefully defined through a set of requirements whose integrity is verified during the system development. Risk analysis must identify hazards created by a system, and the risks mitigated until an acceptable “probability of dangerous failure” within a stated time period is achieved, whether by electronic or other means. Using equipment certified to a particular SIL is one part of the technique by which system developers can show that the system incorporating such devices can itself meet its own required SIL. But note that you can’t create a safety-related system with a given SIL, just by using components having the same SIL.

Quantifying the probability of failure is not the only requirement to achieve a particular SIL. It is also necessary to quantify the “Safe Failure Fraction” (SFF); this gives a comparison between the probability that a fault will revert to a safe condition, or whether it will result in a dangerous condition.

6.1.2 The basket of techniques

IEC 61508 in its various parts refers to a range of “Techniques and Measures” which can be used to demonstrate compliance with its demands. These are to be applied across the whole system life-cycle:

- development of the overall safety requirements (concept, scope, definition, hazard and risk analysis)
- allocation and specification of the safety requirements for the electrical/electronic/programmable (E/E/PE) safety-related systems
- design of safety-related hardware and software
- installation, commissioning and safety validation of safety-related systems
- operation, maintenance, repair, modification and retrofit, decommissioning and disposal of safety-related systems

Part 2 of the standard specifies how to design and manufacture E/E/PE hardware, while Part 3 does the same for the software that will form part of the system. The design techniques and measures address, amongst other things:

- hardware safety integrity architectural constraints
- quantifying the effect of random hardware failures
- avoidance and control of systematic faults
- system behaviour on detection of a fault
- data communications

- software architecture, languages, support tools, code implementation, module and integration verification and validation

The design techniques are embedded in an overall framework which encompasses the lifecycle from specification through to decommissioning. Although the focus is very much on the effect of failures, there is no explicit guidance or mention of failures due to EMI, and it is this omission which other documents have been drafted to address.

6.1.3 Other standards

IEC 61508 and its sub-parts are stated to be basic safety publications. It was originally developed in the context of industrial process control by IEC committee TC65: *Industrial-process measurement, control and automation*. While it can be used as a stand-alone document, it is also intended to be referenced in other sector- or application-specific standards, and there are several such standards in existence: IEC 61511 for Safety Instrumented Systems, IEC 61513 for Nuclear Power Plant Control Systems, IEC 62061 for Machinery, and the EN 50126/50128/50129 series for Railways. The avionics sector uses RTCA DO-254, the automotive industry uses ISO 26262 and the UK MoD has DEF STAN 00-56.

The medical electronics industry has gone its own way for safety risk management and the principles have been documented in the existing standard IEC 60601-1, which covers general requirements for basic safety and performance of medical electrical equipment. This has a collateral standard (IEC 60601-1-2, see section 4.6.3) for EMC which, at edition 4, has been updated to incorporate EMC-related risk management principles.

6.2 Interference effects on safety

Other parts of this book consider the types of interference disturbance that can occur, and how to design to mitigate their effect. In the context of assuring functional safety, you have to take a series of measures to ensure that the variety of disturbances could not result in safety-related failures. This means, to begin with, that the intended environment should be assessed for reasonably foreseeable disturbances, such as, for instance, cell phones in close proximity. Expected disturbances could cause:

- degraded, distorted, delayed, intermittent or false data values or signals
- these effects simultaneously on several signal or data channels
- waveform distortion, over- or undervoltages or dropouts, phase imbalance, frequency changes and interharmonics on AC power supplies, and similar relevant effects on DC supplies
- these effects simultaneously on different supplies
- direct effects on the function of both analogue signals and digital processing within equipment enclosures

So this requires that relevant tests at appropriate levels don’t cause safety-related degradation, and design and through-life maintenance ensure that this assurance is maintained throughout the life cycle. But also, design techniques should ensure that any unexpected or extreme combinations of electromagnetic disturbances cannot cause unacceptable safety risks. Section 6.3 considers these techniques further.

6.2.1 The relevance of EMC tests

Testing against the phenomena which cause these disturbances is covered in Chapter 8 of this book. But the typical commercial test levels, quite explicitly, do not cover all likely maximum levels of every phenomena to be found in every environment; nor do the test methods explicitly require exact replication of the installation conditions of a real system, and neither are they performed under the various other environmental conditions to be expected during operation. None of these would be practical in a compliance context. Also, testing one example of a product or system at the start of its lifecycle says nothing about the performance of other examples of the same system, throughout their lifetime. In addition, completely testing the correctness of all the possible states of a digital machine is to all intents and purposes impossible, which is one reason why the approach taken in IEC 61508 does not rely on testing alone. So although testing against immunity pass/fail criteria has a part to play in analysing functional safety under EMI, it is by no means sufficient in itself.

In order to use EMC immunity test results effectively, more information is needed than just a "pass" against a single applied test level. This tells you nothing about the EUT's response to levels which *do* overstress it. Instead, what you have to do is to raise the stress levels high enough to provoke a fault response from the unit, note this response and then show that the design of the unit is such that the fault can be recovered safely. Or, if an unsafe state is encountered, that it will occur only under stress conditions which are unlikely enough to the extent needed to achieve the required SIL.

This over-testing approach is much more common in military and aerospace standard methods than commercial. For instance, DEF STAN 59-411 test DCS02 (Conducted Susceptibility on Control, Signal and Power Lines 50kHz–400MHz) says

> In addition this test will provide an amplitude/frequency malfunction signature for the system which, when compared with the levels of current on the looms (or cables) caused by adjacent or nearby transmitting sources measured during system acceptance trials, will assist in the establishment of adequate safety margins.

During this test, "at frequencies where the test sample is susceptible, the signal amplitude shall be reduced until a threshold of susceptibility is determined". It does of course require an adequate capability from the test house that is going to perform the tests, in order to find the susceptibilities. And in fact, companies who are interested in the reliability of their products will very often apply an over-stress compared to the specification level, precisely in order to find out what happens and how much margin exists. This then becomes vital data for the safety integrity assessment. Even so, testing a single product under benign environmental conditions can only take you so far, and it is essential also to apply good practice techniques in the design.

6.2.1.1 Extending the tests

There is nothing to stop you modifying the standardized immunity tests as discussed in Chapter 8 to provide greater coverage, as long as your chosen test house has the capability to do so. Significantly increasing the test levels as above, especially in order to find susceptibility thresholds, is one approach. Beyond this, you can consider:

- modulating CW disturbances with frequencies or wave shapes to which a design might be especially susceptible; this approach has been written into a number of RF immunity standards already, and could be more widely used;

- applying two or more disturbances at once (e.g. multiple frequencies during conducted or radiated tests to cause intermodulation in the EUT);
- applying different wave shapes on transient tests; and
- performing significantly larger numbers of transient tests to cover a greater proportion of the range of possible equipment states; this is, again, already written into some product specific test methods, particularly CISPR 24/35.

6.3 Techniques for assuring safety under EMI

IEC 61508 describes a number of fault-tolerant design techniques which can be used to demonstrate compliance with SIL requirements. While these were not explicitly aimed at dealing with EMI-induced faults, many of them are directly relevant. The IET's guidance on EMC and Functional Safety [215] expands on these techniques and has been published as an annex to IEC 61000-1-2. A précis of what it says is included here.

6.3.1 Hardware design

6.3.1.1 Heavy-duty protection

What might be called the "brute force" approach to dealing with EMI hazards is to enclose the safety-related equipment in a well-shielded enclosure with high performance filtering, galvanic isolation and/or shielded cables on all interfaces. This is intended to ensure that it can protect its contents from any electromagnetic disturbances over the lifecycle; to be sufficiently rugged that it doesn't suffer significant degradation in protection over the complete lifecycle, despite all foreseeable faults, misuse, ageing, component tolerances, assembly errors, and physical and climatic conditions that could occur; and that both of these characteristics are achieved with the degree of confidence that is necessary to achieve functional safety according to the SIL, by reducing impinging disturbances on the critical part of the system to a level which won't create failure modes.

This approach works, and is frequently employed in high performance military applications, but as may be deduced from the more extreme techniques described later in this book, it will often be found to be impractically large, heavy and costly. This is especially the case for high volume or weight- or size-sensitive products.

The technique can be optimised by careful identification and separation of the safety-related system parts from non-safety-related parts, at the early stages of preparation of the system architecture. Nevertheless you may prefer to achieve adequate EMI resilience by employing a more finessed set of design techniques and measures.

6.3.1.2 Light protection

The general high-integrity design principles described in IEC 61508 can in many cases be applied in the context of EMI resilience. Table 6.2, abstracted from [215], lists some of these techniques.

6.3.1.3 Hardware diversity

A common and useful technique in high-integrity design is to apply redundancy. This can be adapted for combatting EMI, but it's necessary to avoid exposing redundant

Table 6.2 Hardware design techniques

System design	Using diverse hardware (in redundant channels) to implement the same function	
	Using diverse software (in redundant channels) to implement the same function, and/or to implement the monitoring function.	
	Fault detection and event data recording for later diagnosis, to improve the localisation of malfunctions caused by electromagnetic disturbances	
	Improving the electromagnetic resilience of communication links, by:	Error detection, using redundant data to detect data corruption
		Error detection and correction, using sufficient redundant data code to achieve a level of error correction
		Adding redundant sequence codes to each data packet to enable detection of lost or duplicated packets
	System or function state synchronisation, or re-synchronisation	
	Protection from persistent interference by monitoring retry counts	
	Protection from persistent interference by independent detection of electromagnetic disturbances	
Operational design	Limiting the possibilities for operation, and therefore the possibilities for electromagnetic disturbances to cause failures	Limiting the number of possible operating modes
		Providing special operating modes (e.g. only selectable by key switches)
		Limiting the number of operating elements
	Protection against operator mistakes, for example by plausibility checks	
	Protection against hardware or software modifications or manipulations, for example by plausibility checks for the sensor signals; detection by the operating system, automatic start-up tests	
Implementation design	Protection against physically damaging electromagnetic disturbances, e.g. lightning, electromagnetic pulses and other high power disturbances, where these are to be expected over the lifecycle	
	Use optical fibre links for signals and data for intrinsic immunity to electromagnetic disturbances	
	DC power supplies / power converters	Detecting and controlling against faults such as overvoltages and undervoltages
		Detecting excessive radio frequency noise on DC power supplies
		Power hold-up, using sufficient energy storage (e.g. batteries) or back-up power supplies (e.g. generators or UPS)
	Monitoring of ventilation, cooling and heating to detect whether they have been influenced by electromagnetic disturbances	
	De-rating of hardware components, especially electromagnetic suppression or protection, to ensure they are operated at levels well below their specified maximum ratings even during worst-case environmental conditions	

hardware to common-cause disturbances which may have the same effect on different channels. Mechanisms for hardware diversity in redundant channels can include:

- Different physical principles, such as sensing different but related physical parameters, for example: temperature and pressure of a sealed vessel; the use of resistances and thermocouple voltages to measure temperature
- Different digital architectures, such as using processors with different internal structures or algorithms that use different techniques to solve the same equation
- Different methods of physical realisation, such as using shielded cables, wireless or fibre-optic for communications
- Spatial separation, so that a localised disturbance is unlikely to cause an upset in all of the redundant channels: i.e., different locations for items of equipment and different routing for cables
- Different circuit design principles, such as operating on a signal whose value is represented as a voltage, a current, a frequency, a mark-space ratio, or a digital code
- Functional diversity, i.e. the use of different approaches to achieve the same result, such as analogue, digital or optical electronic technologies. Mechanical, hydraulic and pneumatic technologies have the advantage of being immune to all electromagnetic disturbances
- Inversion of data or signals: for instance, one channel has an increasing analogue value while another has a reducing value, for the same variable
- Different offsets, encoding, amplitude ranges of data or signals
- Where different data channels are synchronised to the same clock, operating them on different clock phases. Ideally, operate redundant channels completely unsynchronised
- Provide different channels with power from different, independent sources.

6.3.1.4 Simultaneous disturbances

Remember that there is no rule which states that disturbances and faults will happen one at a time, even though the standard EMC tests are applied this way. Phenomena that could occur simultaneously are, for instance: high ambient temperature, vibration, a distorted voltage waveform from the AC supply, multiple RF fields, a corroded shielding gasket, the use of an incorrect cable, and an ESD event. These issues should be addressed by design, rather than by testing with simultaneous phenomena.

6.3.2 Software design

Techniques of high-integrity software design are well established and will naturally be used to develop a software product that is certifiable to a SIL. Later in this book some techniques are described (section 13.3.5) which can be employed in software for generally improved immunity. In fact, the techniques of hardware and software design are not necessarily best implemented separately: the most effective approach may be to use firmware in programmable logic rather than all software in microprocessor-based system and all hardware in hard-wired circuits. This requires hardware and software designers to work together on meeting the safety integrity requirements.

Software designers should be reminded that their virtual world can easily be affected by unexpected outside influences. This means that techniques of software diversity should take into account failures due to electromagnetic disturbances as well as other sources. The software risk analysis should take into account reset, latch-up and crashes, including:

- partial or full reset or corruption of programmable devices;
- hang-ups or crashes of software and firmware in programmable devices;
- latch-up of semiconductor hardware devices, so that they are tripped into an abnormal state.

6.3.3 Installation and maintenance

The risk analysis should take into account the physical, climatic and use environments to which the safety related system could reasonably foreseeably be exposed over its lifecycle, since its ability to function as intended in the presence of EMI can be degraded by exposure to its physical and climatic environments and by the actions of operators and third parties. Extremes of temperature, supply voltage, shock, vibration, loading, physical forces, and so on can reduce immunity by degrading filtering, shielding and other EMI mitigation measures. For example, under reasonably foreseeable real-life conditions of ambient temperature and load current within the ratings of the components an EMI filter's attenuation could degrade by 20 dB – see for instance the discussion regarding voltage coefficient of capacitance (page 408).

Immunity degradation can be caused by ageing, moisture and contamination, as well as wear and tear caused by multiple operations of controls, opening and closing of doors and access panels, or temperature cycling. For example, a common ageing problem is corrosion at metal joints, which affects EMI shielding and can also degrade filtering and other earth connections.

Tests that simulate the reasonably foreseeable operational life of equipment, for example accelerated life tests are recommended to help verify that the design is adequate to maintain safety over its expected service life. Where you do such tests, it is also recommended that the EMC characteristics of the equipment or system are assessed before *and after* the tests, to verify that as a result of the tests they have not become degraded to the point where risks have risen to unacceptable levels.

Some examples of faults and use/misuse that can affect equipment functionality as required in the presence of EMI include:

- dry joints or short circuits;
- intermittent contacts in connectors;
- incorrect/out-of-tolerance electronic components;
- incorrect, loose or missing fasteners associated with shielding or RF bonds;
- damaged or missing conductive gaskets;
- failure of a surge protection device, for example by overstress;
- shielding doors or covers left open;
- installation or modification using an incorrect type of cable.

6.3.3.1 Installation and commissioning

Instructions for installation and commissioning should include:

- Any constraints on physical positioning of safety-related equipment;

- Any constraints on types, lengths, routing and screen termination of power, control and signal cables;
- The types of connectors to be used and any special assembly requirements;
- The electrical power supply requirements (power quality), and any additional power conditioning required (e.g. a UPS);
- Any additional shielding or filtering needed, and how it should be installed;
- Any additional overvoltage and/or overcurrent protection required, and how it should be installed (e.g. by referencing the appropriate lightning protection requirements in the IEC 62305 series);
- Any additional electrostatic discharge protection requirements, such as control of humidity or operator static precautions;
- Any additional physical protection required (e.g. against the possibility of extreme physical and/or climatic conditions);
- The earthing (grounding) and bonding requirements for the installation;
- The procedures and materials to be used; and
- Any protection that is required against corrosion over the lifecycle.

6.3.3.2 Through-life maintenance

Proper installation and commissioning, with regard to the constraints and additional measures, should be competently checked before the system is first operated, and regularly during its lifecycle, depending on the SIL requirement. Degraded EMC protection does not often show itself in the day-to-day functioning of a system; only when it is hit by an unexpected burst of interference is the absence realised. So regular checks of the protection components are needed, and the design of a system has to allow and even encourage this. A few examples can demonstrate what may be needed.

Checking the integrity of suppression devices

A transient voltage suppressor (see section 14.2.5) may fail open, short or degraded [146]. If it's failed open circuit then the equipment will carry on operating apparently as normal, but without protection. This is a state which should be detected and corrected. You can do this either by regular testing of interfaces with an external test set, or by continuous monitoring with a designed-in circuit (Figure 6.1). The first option adds operational complexity, the second adds design complexity. For these reasons it may be preferable to avoid the use of transient suppressors altogether and use other methods, such as stringent galvanic isolation, for transient protection.

Checking the integrity of earth bonds

Bonding is widely used in systems to maintain the electrical integrity of structural components, but it can deteriorate if not effectively maintained. DEF STAN 59-411 Part 4 [219] clause B.3 gives a comprehensive specification for checking earth bonding:

> This Standard is concerned with demonstrating the adequacy of earth bonds which occur at a great many points in the installation under test (IUT), e.g. between equipments, the secondary and primary mounting hardware and the platform. These bonds will be achieved by one or more of the following methods.
>
> a) The metallic hardware used to define the physical position of equipments within the IUT.
>
> b) Special earth braids and straps.

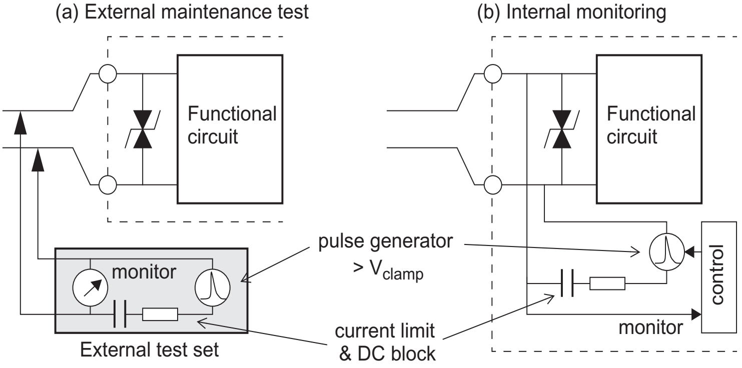

Figure 6.1 Testing transient suppressors

> c) The outer screens of cable assemblies used to interconnect equipments.
>
> The actual earth bond test is simple but it is of great importance to identify precisely what is measured and where. For this reason, a rather detailed description of some aspects of the IUT forms a general test requirement... It is the responsibility of equipment and installation designers to implement earth bonding measures by means which allow the testing of these measures on installed equipments without damage to protective finishes... Bonding measurements, with a general limit of 2 milliohms maximum, are recommended as follows:
>
> Screened Cable Assemblies: bond resistance between cable screen and connector back shell at each end of the cable, between the back shell and the body of the connector to which it is secured
>
> Equipment: bond resistance between connector body and equipment case in the near vicinity of the connector body. If the equipment is provided with an earth terminal measure the terminal-to-case bond resistance in the vicinity of the terminal. Measure the resistance between any detachable portion of the equipment case (e.g. the lid, cover or front panel) and the main body of the case. Bond resistance between the equipment earth terminal (for a braid) or relevant case region (for the mechanical method) to the mounting hardware, should be measured separately.
>
> Mounting Hardware: Identify the point(s) which should be in good contact with the equipment case and the point(s) which should make good contact with the Secondary Mounting Hardware, and measure the resistance between these points; similarly between Secondary and Primary Mounting Hardware, and between Primary Mounting Hardware and the primary installation earth.

Checking the integrity of screened cabling

Low-level signal interfaces may be heavily reliant on the integrity of screened cables to protect them from interference. A fairly extreme example of this occurs in the nuclear power industry [70]: neutron detectors in the reactor core are essential for the safe operation of the reactor, but their outputs are wideband pulses measured in microvolts. Interference on the cabling from the core to the control system could either cause unwarranted false pulses or could block the wanted signal, and the cable is very heavily screened to prevent this. Continued performance of the screening is crucial, and to assure this the system includes a coupling wire laid concurrently with each cable run (Figure 6.2). On a regular basis, the maintenance schedule requires that the wire is energised with a swept frequency signal (while the reactor is powered down, of course) and the crosstalk into the signal circuit is measured. Comparison with historical data

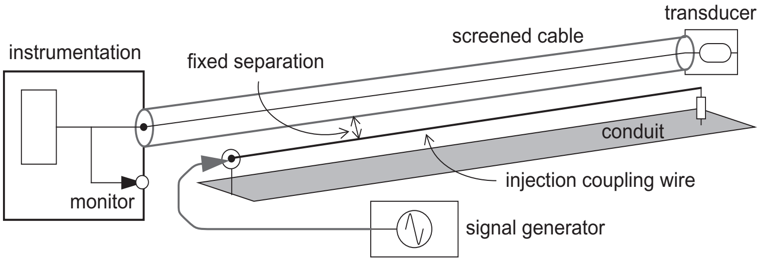

Figure 6.2 Screened cable injection testing

from previous tests shows that the cable screening has not (or, in the undesirable case, has) suffered degradation. Any such degradation will require remedial action.