Another EMC resource
from EMC Standards

Overview of Ts & Ms for EMC for FS

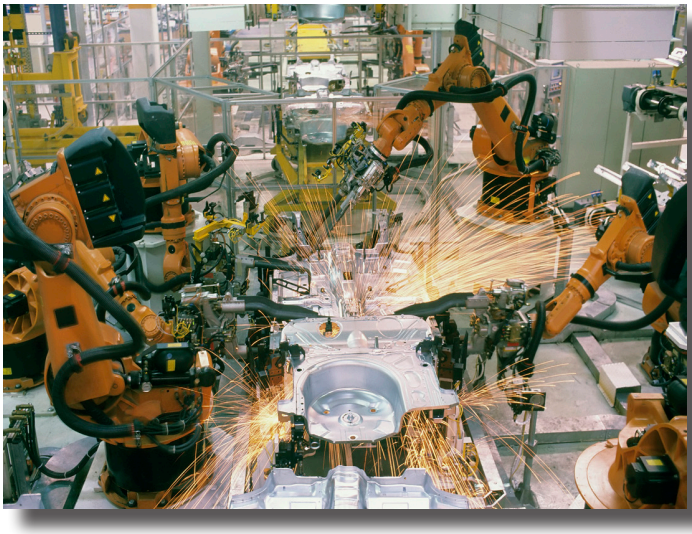
Helping you solve your EMC problems

9 Bracken View, Brocton, Stafford ST17 0TF T:+44 (0) 1785 660247 E:info@emcstandards.co.uk

Guidance

The Institution of Engineering and Technology

Overview of techniques and measures related to **EMC** for **Functional Safety**



www.**theiet.org**/factfiles

About This Guidance

The Institution of Engineering and Technology acts as a voice for the engineering and technology professions by providing independent, reliable and factual information to the public and policy makers.

For more Briefings, Position Statements and Factfiles on engineering and technology topics please visit http://www.theiet.org/factfiles.

The Institution of Engineering and Technology

The Institution of Engineering and Technology (IET) is a global organisation, with over 150,000 members representing a vast range of engineering and technology fields. Our primary aims are to provide a global knowledge network promoting the exchange of ideas and enhance the positive role of science, engineering and technology between business, academia, governments and professional bodies; and to address challenges that face society in the future.

As engineering and technology become increasingly interdisciplinary, global and inclusive, the Institution of Engineering and Technology reflects that progression and welcomes involvement from, and communication between, all sectors of science, engineering and technology.

For more information please visit http://www.theiet.org

The Institution of Engineering and Technology is registered as a Charity in England & Wales (no 211014) and Scotland (no SC038698).

Disclaimer

Cover images (clockwise from top left)

- Oil refinery
- Maglev train
- Nuclear power plant
- Robotic assembly line

Enquiries to:

policy@theiet.org

Contents

1 Introduction

1.1 The aim of this guide

The aim of this guide is to provide a non-exhaustive range of techniques and measures that can address the interfering effects of the electromagnetic (EM) disturbances that a safety-related system could experience over its complete lifecycle.

When competently selected and applied, a set of such techniques and measures will provide part of the evidence required for functional safety arguments and for compliance with IEC 61508.

Specifically, this guide deals with achieving adequate resilience to **EM interference (EMI)** in any electrical and electronic hardware and software in a safety-related system, or in any of its constituent parts, which could increase functional safety risks by more than is tolerable, see **Figure 1**.

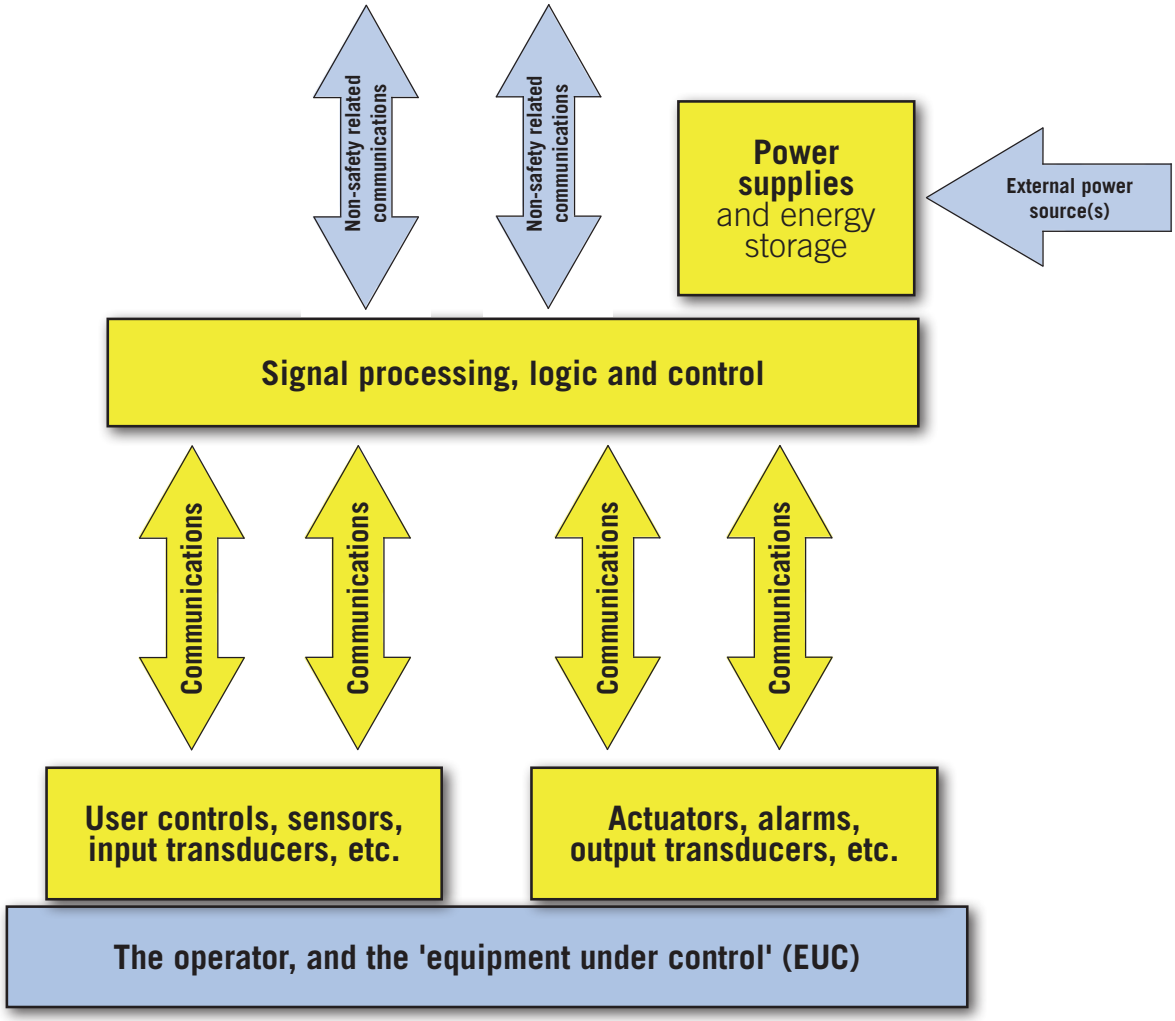


Figure 1: This guide may be applied to complete safety-related systems, and to any/all parts of them (shown in the yellow boxes)

This guide supplements the information on dealing with EMI given in IEC 61508 and other standards or specifications containing EMC requirements for functional safety, such as IEC TS 61000-1-2 [2], IEC 61326-3-1 [3], IEC 61326-3-2 [4] and IEC 61000-6-7 [5]. It also supplements the information in the IET's 2008 Guide on EMC for Functional Safety [6].

This subject of this guide is called **'EMC for Functional Safety'**, which is also referred to as **'Risk Management of EMC'**.

Note that EMC for Functional Safety is only concerned with the possible functional safety consequences of EMI, and not with any effects of EMI on non-safety-related functionality.

1.2 The intended audience for this guide

- Managers of projects that require functional safety engineering.
- Practitioners of EMC design engineering.
- Practitioners of Functional Safety engineering in design and/or design assessment.
- Persons involved in the creation of standards, guides, textbooks, education and/or training courses on functional safety engineering.

1.3 The background to EMC for Functional Safety

All electronics and electro-mechanical technologies can suffer errors, malfunctions or failures due to EM disturbances, so it is necessary for effective measures to be taken to improve the EMI resilience of safety-related systems over their lifecycles.

There is a rapidly increasing use of wireless communications, including within and between systems which may operate unpredictably in close-proximity to safety-related systems or parts of them.

There is also an increasing use of high-speed and/or high-power switching devices and programmable electronics in general in many sectors e.g. industrial, transport, consumer, information technology and communications, etc.

The EM disturbances increasingly being emitted by these technologies are making the EM environment progressively worse, in terms of their noise levels, spectral density and bandwidth.

In practice, the magnitude and distribution of possible sources of EM disturbances are rarely known with confidence and in some cases cannot be predicted at all. As a result, the EMI they cause in electronics or electro-mechanical technologies may cause an unacceptable dangerous failure rate to occur during the lifecycle of a safety-related system that uses them.

Errors, malfunctions and failures caused by EMI are often transitory, leaving no tangible evidence of their occurrence, making fault identification and evidence gathering extremely difficult. To aid fault identification special techniques and measures may be used.

Functional safety requirements must be met over the complete lifecycle, taking into account all reasonably foreseeable, worst-case:

i. errors, malfunctions and faults (whether static or intermittent);
ii. environmental conditions (shock, vibration, humidity, condensation, temperature, EM disturbances, etc.);
iii. wear, corrosion and aging;
iv. component tolerances and variability, construction and installation errors, etc.;
v. use and misuse (whether intentional or not);
vi. combinations of any/all i) - v) above.

The combination of these factors and the high level of EMC design confidence required for the achievement of functional safety over the lifecycle make EMC testing impractically difficult, lengthy and costly as the sole means of verifying or validating the EMI resilience of a design.

1.4 The purpose of this guide

This guide has been developed specifically to help overcome the following difficulties that have been found when attempting to apply the existing standards and guides on EMC for Functional Safety:

a. It has been generally found to be impractical to perform anything more than a general assessment of the EM disturbances that could possibly occur over a complete lifecycle.
   These assessments are good enough for determining which of the many published EMC emissions and immunity standards for functionality should be applied, but cannot determine what EM disturbances could occur over the lifecycle.
b. The traditional approach to dealing with the problems created by a) is to use EM mitigation techniques and measures (shielding, filtering, surge protection, etc.) that have:
   - a sufficiently high specification that they can be expected to protect what they enclose from any/all possible EM disturbances; and
   - are sufficiently rugged that they can be expected not to suffer significant degradation in their protection over the complete lifecycle; and
   - both of these characteristics achieved with the degree of confidence that is necessary for the achievement of functional safety.

As the use of electronic technologies in functional safety engineering expands rapidly into more sectors (e.g. aircraft, motor vehicles, portable or implanted medical devices, etc.), this traditional approach is found to be impractically large, heavy and costly. This is especially the case for safety-related systems that are manufactured in high volumes.

Indeed, many improvements in safety have only been made possible by the ever-increasing processing power of modern electronics, ever-

reducing size and weight, power consumption and cost, and this trend is accelerating in all areas of human life.

These issues make it increasingly desirable that functional safety is achieved by employing an appropriate set of EMC techniques and measures, such as (but not limited to) those described in this guide.

> **Note:** There is no reason why the traditional method described in (b) should not be applied in combination with EMC techniques and measures such as those described in this guide. For example, a complete safety-related system might be constructed from items of equipment supplied by third-parties (whether custom-designed, batch- or volume-manufactured) one or more of which use method (b) above, with the remainder using EMC techniques and measures such as those described in this guide.

1.5 The approach taken by this guide

The approach of this guide is illustrated in **Figure 2**.

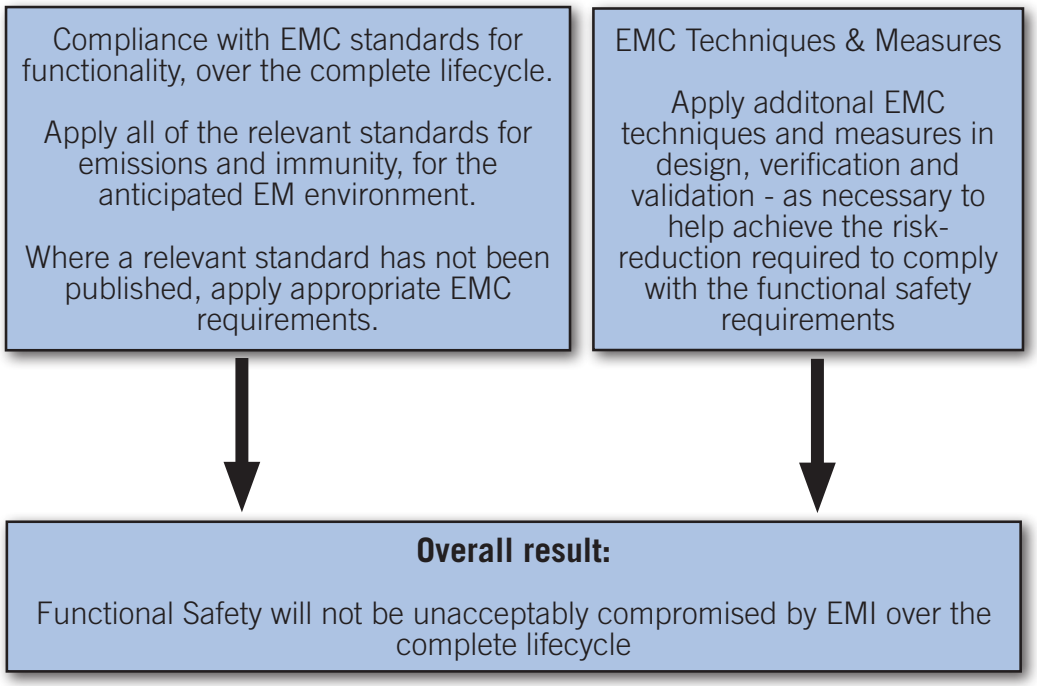


Figure 2: Overview of this guide's approach for achieving EMC for Functional Safety

The approach taken by this guide builds on the existing expertise of the EMC and Functional Safety engineering communities, as follows:

i. **Compliance with EMC standards for functionality**

Normal EMC design/testing expertise for non-safety-related functionality (e.g. to comply with the EMC Directive [7], other EMC regulations or customer EMC specifications) for equipment or systems when first supplied to their end-user, has been well-established worldwide for over two decades.

The EMC emissions and immunity standards that are used have been developed over the years (and are still developing) for the purpose of ensuring adequate availability of equipment/system functionality, with different standards being developed to suit the wide variety of generalised EM environments (e.g. domestic, commercial, light industrial, heavy industrial, military, road vehicles, railways, etc.)

This guidance builds on the above experience, expertise, and installed base of EMC testing facilities, by recommending that the equipment or systems comply with those same EMC standards throughout their anticipated lifecycles.

ii. **The use of EMC techniques and measures**

Current functional safety expertise to comply with IEC 61508 and related standards is well-established worldwide, generally using techniques and measures that are already well understood and widely used.

These techniques and measures have been developed to detect and/or correct errors, malfunctions and faults in any of the items

shown in **Figure 1** (user controls, sensors, input transducers, signal/data communications, etc.).

Because EMI may cause errors, malfunctions or faults, the techniques and measures that have been widely used to achieve compliance with IEC 61508 and related standards are also potentially effective at preventing EMI from causing dangerous failures.

This guidance builds on this experience and expertise by recommending:
- well-established functional safety techniques and measures that are known to be especially effective against EMI;
- modifications to certain techniques and measures to make them more effective against EMI;
- a set of EMC engineering techniques and measures for all stages in design and during the lifecycle.

To improve the EMI resilience this guide recommends a number of techniques and measures.

No single EMC technique can be relied upon on its own. The functional safety designer chooses a set that ensures that, regardless of the EM disturbance that causes the error, malfunction or failure, the overall functional safety specifications are met. The lower the level of acceptable functional safety risk, the greater is the amount of work and documentation, and the higher is the competence required in choosing EMC techniques and measures.

Compliance with EMC test standards cannot ensure protection against the unknown, unpredictable, unlikely or extreme EM disturbances, or combinations of disturbances, which could possibly occur during the complete lifecycle, nor can it ensure protection against the consequences of failures in EM mitigation and other EMI-related problems caused by faults, misuse, unanticipated physical or climatic conditions, aging, etc.

The competent application of a set of EMC techniques and measures should provide sufficient confidence that functional safety over the lifecycle will not be compromised by EMI, however caused.

1.6 Choosing EMC techniques and measures

This guide describes a range of EMC-related techniques and measures that are considered to be useful, where relevant, for all stages in any functional safety project:
- Management;
- Specification;
- System design;
- Operational design;
- Implementation;
- Verification and validation;
- Maintenance, refurbishment, upgrade, disposal.

All projects contain these stages, whether they concern the creation of equipment for use in all or part of a safety-related system (usually standard products manufactured in volume) or the integration or creation of a unique safety-related system.

Depending on the nature of the project, different EMC techniques and measures might be used in its various stages.

For example: If a project did not involve any software design, then no software design techniques and measures would be selected for any of the project's stages. If there is no circuit design required, then circuit design techniques and measures are not needed.

It is important to be aware that at each phase of the lifecycle of a safety-related system, a nominated person bears overall responsibility for the achievement of functional safety. This includes EMI and everything else that could have an effect on it, even for systems comprised entirely of hardware and software items supplied by others.

This guide does not suggest any rigid correlation between the techniques and measures, or combinations of them, and the safety integrity levels (SILs) specified in IEC 61508. Instead, as is usual when complying with IEC 61508 and related standards, suitably competent persons apply the techniques and measures as part of the overall process of achieving functional safety.

Competent functional safety designers perform risk assessments and select the techniques and measures to achieve the overall functional safety specifications relevant to their part of an overall design.

Also as in the usual IEC 61508 type of approach, a competent independent assessor must be satisfied that the design approach and implementation will meet the functional safety specifications.

No EMC techniques and measures, such as those described in this guide, should be assumed to guarantee 100% protection against every

possible type of EM disturbance, combination of EM disturbances, faults or misuse that could result in EMI.

It is the functional safety designer's responsibility to choose techniques and measures that will achieve sufficient coverage of all the ways in which EMI could occur in the hardware and software, to be able to demonstrate sufficient EMI resilience to meet the functional safety specifications over the lifecycle.

2 Definitions and abbreviations

'EMC'	electromagnetic compatibility: the discipline of controlling the emissions of EM disturbances to limit the EMI they cause; and controlling EM immunity/susceptibility so that any EMI that occurs is at or below tolerable levels for the application concerned.
'EUC'	the equipment under control: equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities, including the EUC's control systems (IEC 61508-4, definition 3.2.1, modified).
'Functional safety'	that part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the safety-related systems and other risk reduction measures (IEC 61508-4, definition 3.1.12).
'Lifecycle'	a period of time that starts at the concept phase of a project and finishes when all of the safety-related systems and other risk reduction measures are no longer available for use (IEC 61508-4, definition 3.7.1, modified).
'Safety'	freedom from unacceptable risk (ISO/IEC Guide 51:1999, definition 3.1).
'Safety-related system'	(IEC 61508-4, definition 3.4.1) the designated system that both: ■ implements the required safety functions necessary to achieve or maintain a safe state for the EUC; and ■ is intended to achieve, on its own or with other safety-related systems and other risk reduction measures, the necessary safety integrity for the required safety functions.
'SIL'	safety integrity level, a discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest. The target failure measures for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1 (IEC 61508-4, definition 3.5.8).

3 The techniques and measures

3.1 Overview

Much of this guidance is drawn from techniques and measures in IEC 61508, since many of them are effective against the effects caused by EMI. The particular relevance of each technique or measure to EMI is highlighted, and further techniques and measures not included in IEC 61508 are also given.

The guidance is provided in Sections 5 through 10, with their references in Section 11. Section 12 shows the relationship between the techniques and measures listed here, and those listed in [1].

3.2 Guidance based on classification

Each technique or measure is classified based on its relevance to detection, mitigation and importance for use relating to EMI.

An adequate combination of techniques and measures is selected, that together achieve the required risk reduction commensurate with functional safety regarding EMI.

Detection is concerned with the effectiveness of the technique or measure to reveal the presence of an error or malfunction that could be caused by EMI.

Mitigation is concerned with the behaviour of the safety function in response to the detected errors or malfunctions that could have been caused by EMI.

Importance incorporates the necessity and or desirability of the Detection and/or Mitigation technique or measure with the following attributes:

None: the technique or measure has no recommendation for or against being used in the context of EMC for Functional Safety.

Not Recommended (NR): the technique or measure is not relevant or useful in the context of EMC for Functional Safety.

Recommended (R): the technique or measure is recommended for use in the context of EMC for Functional Safety

Highly Recommended (HR): the technique or measure is highly recommended for use in the context of EMC for Functional Safety.

It should be borne in mind that just because a particular effect of EMI can be detected does not mean that its effects can always be corrected; however the knowledge of its occurrence may be valuable in itself, for the process of verification and diagnostic use for development and maintenance.

Where possible, the techniques and measures covered by this document are assigned as being appropriate to continuous or on-demand safety functions.

4 Project management

Aim: To avoid failures in the management, planning, selection, design, implementation, commissioning and verification of measures for avoiding and controlling failures due to EMI.

Description: The processes for the management, planning, selection, design, implementation, commissioning, modification and verification of each safety function should explicitly include EM resilience measures. A competent person should have the overall responsibility for managing the EMI resilience of the system. Appropriate expertise should be made available at all lifecycle stages.

Detection: By independent assessment of the design against the guidance in this document, see Clause 8 of [8] for guidance on the appropriate level of independence.

Importance: HR for all safety integrity levels (SILs).

5 Specification

5.1 Safety-related system design requirements specification

Aim: To produce a specification for EM resilience measures which is, as far as possible, complete, free from errors, contradictions and is simple to verify.

Description: The system design requirements specification (SDRS) should state the selection of techniques and measures to be used for achieving adequate EMI resilience for the intended system and its expected operational environment.

To comply with the SDRS, functional safety designers and independent safety assessors should take fully into account the fact that EMI can cause an effectively infinite variety of:

- Any/all kinds of noisy, degraded, distorted, false, delayed, re-prioritised, overvoltage, etc. signals/data, both intermittently and continuously;
- Any/all kinds of under/overvoltages, noises, dropouts and interruptions, lasting from less than one microsecond to many seconds, minutes, even permanent, in one or any number of AC or DC power supplies, both intermittently and continuously;
- Any/all kinds of waveform distortions, frequency perturbations in any number of AC power supplies, plus phase and voltage imbalances in multi-phase supplies;
- One or more combinations of the above occurring in one, more or all, signal paths in any time relationship.

Designers and assessors should also take fully into account the fact that any combination of the above effects of EMI can occur simultaneously, or in any other critical time relationship.

Note: This document acknowledges that in many cases the EM environment is unquantified or even unquantifiable; therefore it is not possible to state requirements numerically (e.g. in terms of interference levels and rejection ratios).

Importance: HR for all SILs.

6 System design

This section describes various techniques and measures, however, more detailed techniques are listed in Sections 8.1 (for hardware) and 8.2 (for software).

6.1 Separation of safety-related system safety functions from non-safety functions

Aim: To separate the safety-related part of the system from non-safety related parts such that the EMI generated in the non-safety related parts, or consequences of EMI events in the non-safety related parts, do not affect the safety-related part.

Description: In the specification, it should be decided whether a complete or partial separation of the safety related systems and non-safety-related systems is possible. Clear specifications should be written for the interfacing of the two parts. Possible remaining routes for interference which could create coupling between the safety-related part and the non safety-related parts should be identified and documented, such that appropriate techniques and measures can be implemented to address them.

Importance: HR for all SILs.

Note: This technique concerns the physical separation of hardware and the connections made between hardware elements (i.e. their interfaces).

6.2 Safety-related system design and development

Aim: To produce a stable design of the safety-related system in conformance with the specification.

Description: This is where the design choices - and justifications - for the EMC techniques and measures used to comply with the SDRS, are documented. These will typically include EMI filtering, separation, segregation, grounding and shielding, sufficient at least to meet normal requirements for EM immunity, together with a selection of the techniques and measures described in this document and elsewhere. See also 8.1.3.

The justification should show how the design choices fulfil the requirements described in the SDRS.

Note: It is generally impractical to demonstrate/verify/validate that a set of EMI mitigation techniques and measures is sufficient for any particular safety integrity level (SIL).

Importance: HR for all SILs.

6.3 Diverse hardware (redundancy)

Aim: To detect systematic failures during operation of the equipment under control (EUC), using multiple diverse channels. These use diverse components and circuit designs that have different modes and rates of failure due to electromagnetic disturbances.

Description: Different types of components are used for the multiple diverse channels of a safety related system that uses redundant hardware. This reduces the probability of systematic common cause errors or failures when the safety-related system experiences electromagnetic disturbances, and increases the probability of detecting such errors and failures, surviving them and maintaining availability.

- There are several types of diversity, for example: different physical principles, such as sensing diverse but related physical parameters, such as temperature and pressure.
- Different digital architectures, such as using diverse processors or diverse algorithms to determine check values in each channel.
- Different methods of physical realisation, such as using shielded cables, wireless or fibre-optic for communications.
- Spatial separation, such as having a separation of at least one-tenth of the wavelength of the disturbing EMI, e.g. 1m for 30MHz and above in air, 300mm for 100MHz and above in air, etc.
- Different circuit design principles, such as operating on a signal whose value is represented as a voltage, a current, a frequency or a mark-space ratio.
- Functional diversity, 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 EMI and may be able to be used to great benefit in some situations.
- Inversion of data/signals.

Note 1: It should be borne in mind that functionally equivalent items of hardware from the same or alternative suppliers may not behave sufficiently differently when subjected to the same electromagnetic disturbances.

Note 2: It may be possible to suspend the operation of the safety function for a period of time until the channels agree once more, without degrading the safety integrity. This helps maintain availability by reducing the number of times the system fails to a safe state as the result of temporary or transient EMI, and so reduces the possibility that users will modify the system to compromise the correct operation of the safety function (an example of foreseeable misuse).

Extending the method to three or more channels requires a voting function that is sufficiently reliable and adequately resilient to EMI at the required level of safety. This voter must have a reliability (despite EMI) corresponding to the improvement in confidence that is the purpose of using the multiple channels. Various techniques may be used to do this, for example dynamic self-testing as described in this guide.

Where such voting is used it can be assumed, given sufficient confidence in the diverse behaviour of the channels as regards EMI, that the channels that meet the requirements of the voting function are operating correctly. Whilst the voting result is positive the system can maintain the correct operation of the EUC without any need to fail to a safe state.

In the absence of a safe state, the use of a sufficient number of redundant diverse-technology channels with a voting function is one of the most important methods for maintaining safety integrity.

Importance: R for SILs 1 and 2, HR for SIL 3 and 4.

6.4 Diverse software

Aim: To detect failures during operation of the EUC using diverse software components, reducing the likelihood that an EMI event will cause an incorrect output to be created.

Description: The first option for software diversity is to use two or more independent software components to implement the same safety function, where each component is designed and coded separately and uses different areas of memory for its data (and may use different algorithms where this is feasible).

Differences in the outputs of these components are detected by the software itself or by means of comparison or voting logic as for hardware redundancy. The rationale for the use of diverse software components is that a memory corruption or incorrect instruction execution caused by EMI may not affect both (all) of the diverse software components, or if it does then the effects of the EMI will in general be different allowing the comparison or voting logic to detect the error.

The second option for software diversity is to use a diverse monitor, a software component which checks the expected output of the main software against the actual output, to ensure safe (but not necessarily correct) behaviour.

The diverse monitor continually checks the output of the main software and prevents the system entering an unsafe state, either by means of a separate output or by bringing the main software back to a correct state.

A diverse monitor should be simpler than the main otherwise it is equivalent to a diverse implementation. It may be helpful to implement the diverse monitor on a separate computer to reduce the likelihood of the main software and the diverse software monitor being affected in the same way by the same EMI event. If a separate computer is not used then the diverse monitor must be capable of operating (and in particular recovering from EMI-induced errors) independently of the main software, for example in a different process or task using separate memory areas.

Diverse software of both kinds may be combined with hardware diversity (using different input channels and/or processors) to reduce further the likelihood of common cause errors due to EMI.

Note: EMI may cause software instructions or data to change, due to corruption of instruction address and/or data bus. Diverse software may also reveal implementation errors via the discrepancy of results during operation.

Importance: R for SIL 3, HR for SIL 4.

References: [113] [114] [115] and [116] describe methods of partitioning software on the same computer. Also see Annex F of [118].

6.5 System requirements and design specifications

Aim: To ensure that EMI and its effects are taken into account in the specification of the system and its software and that techniques and measures are incorporated to ensure that the system will achieve the anticipated safety integrity.

Description: The requirements and design specifications can be defined using a variety of semi-formal and formal modelling techniques. Whichever techniques are chosen the potential effects of EMI on the hardware, and consequently the software, need to be taken into account. Typically this might include consideration of corruption of data and program memory content, corruption of data in transit on internal or external serial or parallel buses and their consequent effects on the safe operation of the system.

Put more simply EMI must be considered as a hazard and its effects either eliminated, mitigated or accommodated using techniques and measures such as those described in this guide.

Importance: HR for all systems, especially for SIL 3 and 4.

6.6 Safety-related system integration

Aim: To ensure that EMC is considered when separately tested parts of the system are brought together to form the complete functional system.

Description: Most systems are constructed from a variety of functional modules and multiple commercially-sourced products. Each part needs to be designed and verified as being resilient to EMI, however further attention is needed when the individual parts of the system are housed and connected, including the shared power supplies and system interconnections that may create additional opportunities for EMI to occur.

Typical system issues might be the routing of cables (crosstalk), common cause failure due to EMI etc. The approach taken to avoid an increase in system wide EMI vulnerability due to system integration (physical, electrical and functional) should be documented in the safety case or an equivalent document.

Detection: By independent assessment of the design and realisation of the integration against relevant good EMC practices for systems and installations, see Good EMC engineering practices. Clause 8 of [8] provides guidance on the independence required according to the SIL. The use of event data recorders within the system may help to pinpoint the likely causes of malfunction, see Fault detection and event data recording for diagnosis. Data communication error counts may provide an indication of EMI influencing communications networks or systems.

Mitigation: By modification of the system.

Importance: HR for all SILs.

6.7 Fault detection and event data recording for diagnosis

Aim: Increase probability of localisation of malfunctions caused by EMI.

Description: Unless physical damage is caused by EMI, there is usually no evidence that it has occurred other than a transient malfunction of the system. In order to improve the possibility of establishing evidence that EMI has caused a malfunction an event data recorder (EDR) can be used.

Whenever an anomaly is detected (such as a data value out of range or a checksum failure or sequencing error) relevant data can be recorded. This data can then be analysed statistically in real time or at some later time to detect and diagnose trends due to sporadic failures and to propose remedial action.

Data captured by an EDR can only reflect the events and malfunctions it has been programmed to detect and record.

Detection: A routine can be called each time a malfunction is detected usually including at least the data itself and a time stamp code. It is necessary for the resolution of the data recorded and its sample rate to be adequate for meaningful subsequent analysis.

Mitigation: Analysis and diagnosis of the data can be used to look for co-related events and trends.

Importance: R for SIL 1 and 2, HR for SIL 3 and 4.

6.8 Improving the resilience of communication links

Aim/ Description: The resilience of the system can be improved by improving the EMI resilience of its communication links such as networks (e.g. CAN, Profibus, Ethernet…), backplanes (e.g. VME), printed circuit boards (earth planes) and even on-chip interconnect.

Detection/ Mitigation: Hardware and software techniques should be used, either individually or together, to improve the reliability of the link. Suitable hardware techniques are described in this guide, but others may be used. Suitable software techniques include, but are not limited to, 6.8.1, 6.8.2, 6.8.3.

Importance: HR for all SILs.

References: [100] [101] and [102].

6.8.1 Error detection on parallel or serial buses

Description: Redundant data is appended to the actual data using techniques outlined in Error detection and error correction. This enables error detection of data corruption using techniques such as parity or cyclic redundancy checking (CRC). Various retry schemes can be used to improve the reliability of the link at the expense of system performance.

6.8.2 Error detection and correction on serial or parallel buses

Description: This is a variation of the previous techniques, however the code is such that a level of error correction is possible in order to both detect corruption and also correct for it its effects. Various error correcting code (ECC) schemes can be used to improve the reliability of the link at the expense of reduced data rate.

6.8.3 Protection of a sequence

Description: When there is a stream of data packets on a data bus or communications link the packets may be duplicated, corrupted or lost during transmission possibly due to EMI.

Extra sequence codes can be appended to each packet to enable detection of lost or duplicated packets. Various techniques in this guide can be used at the packet level, for example even just a single bit can be alternated between packets to detect a single packet failure (omission or duplication) (for example, see [107]). More elaborate techniques are needed to detect multiple packet failures or corruption.

Detection: Depends on the technique used for marking the sequence of the packets.

6.9 System or function state synchronisation or re-synchronisation

Aim: To improve the availability of a function or system in the event of a detected EMI-induced corruption.

Description: The ability of a function or system to detect that it is running abnormally and then reset its own state, or the state of the system. For example, in some processor architectures EMI can cause a processing exception due to corrupt data or the incorrect execution of an instruction.

Detection: By any of the techniques in this guide.

Mitigation: A system design concept is needed for the credible and practical implementation of this technique. Different techniques may be needed to resynchronise continuous and non-continuous systems. The application must be able to tolerate safely the reset or resynchronisation.

The use of low level programming features may be necessary to implement state resynchronisation or to return the system to a safe state.

The use of built in exception handling within the language runtime package or operating system should only be relied on if the resulting response is deterministic and accommodated as part of the overall design.

Importance: HR for systems intended for continuous operation, for all SILs.

R for on-demand systems, for all SILs.

6.10 Protection of systems from persistent interference

Aim: To improve system resilience during persistent EMI.

Description: If a system is exposed to persistent EMI to which it is susceptible then the operation of the system may be severely affect or even halted. For example a communication link, even with a retry facility, may be so affected that no message traffic can successfully be received. Any defence mechanism relying on reactivation of a function or retransmission of a message might be so affected that there is effectively a 'denial of service', which may or may not be deliberate.

Detection: There are two main ways to detect this situation, described in 6.10.1 and 6.10.2.

6.10.1 Monitoring retry counts

Description: A task continually monitors the retry counter values and timestamps of functions, memory checkers, communication protocols and any other function which uses a retry or state recovery approach to improve its perceived short term reliability. This task itself would require a timeout in order to be effective, preferably based on an independent hardware watchdog timer.

Importance: HR for systems intended for continuous operation, for all SILs.

R for on-demand systems, for all SILs.

6.10.2 Independent detection of EM disturbance

Description: An independent detector or detectors can be used to detect EM disturbances.

Mitigation: This technique may be used in a variety of different ways, for example:

a. To help manage the external conducted and/or radiated EM environment over the lifecycle, for example by displaying or sounding a warning – or initiating other actions according to the safety case - if the equipment starts to experience levels of EM disturbance in excess of the level of immunity the equipment was designed to withstand.

   It could, for example, warn of the use of equipment using high RF power, such as a diathermic heater, in too-close proximity. This technique has been used in hospitals, to help enforce their 'no cellphones' policies by sounding a warning, and could be helpful in enforcing the walkie-talkie example in 7.4.

b. By detecting a failure of electrostatic control measures (e.g. humidity control, static floor re-treatments, etc.), that could expose equipment to higher levels of electrostatic discharge (ESD) than it was designed to be able to cope with.

   (The usual maximum ESD test level in immunity standards is ±8kV, but levels of ±25kV have been seen under reasonably foreseeable circumstances during reduced atmospheric humidity, and the automobile industry has tested to such levels for decades.)

c. By making sure that certain sensor or transducer readings were ignored, or certain circuits were reset, for the duration of an excessive disturbance. This is a well-established technique for preventing intentional interference with machines that can pay out money, for example gambling machines, change machines, automatic teller machines (ATMs), etc. (A typical tool used for such intentional EMI (IEMI) is the cattle prod, which generates impulses of around 35kV.)

   It has also been used with some very sensitive medical diagnostic instruments to warn when their results should be ignored because the EM environment was noisier than they were designed to cope with (sometimes at quite low levels, such as > 1V/m).

d. By recording data on the occurrence of certain types and/or levels of EM disturbances in an EDR (see 6.7) to help diagnose the causes of failures, after the fact.

e. By monitoring the internal EM environment of equipment that relies on external shielding and filtering and surge protection so that if any of them should degrade, and if that degradation permits higher-then-acceptable levels of EM disturbance to enter the equipment, then action in accordance with the safety case can be initiated. This could be helpful in enforcing Modification protection, so that, for example, if someone uses an incorrect type of shielded cable, or does not terminate it correctly, an alarm is sounded.

Importance: Importance: R for all SILs.

6.11 Protection of systems from tampering (e.g. wipe EMI log)

Aim: To conserve the integrity of the system.

Description: Many systems are connected to the internet and as such are vulnerable to hacking attacks, virus infestation, Trojan attacks, spoofing (imitation of identity), and denial of service attacks.

The offensive techniques can be used to access, change or delete electronic data recorder (EDR) records and to change programs to make them more vulnerable to EMI. If the EDR log media is physically removable then the records of its removal and replacement should be stored in non-volatile memory which is built permanently into the system. In the event of the EMI log being tampered with this record can be consulted.

Some EDR logs are built into the system and accessed interactively via a port. In this case it is necessary to restrict access to read-only so that the EDR data cannot be altered or deleted, thus destroying possible evidence.

EDR data may be encrypted to make tampering harder and alteration easier to detect.

Detection: Typically a firewall is used to prevent attack and thus enable protection of the EMI log.

For EDRs that are built in, the removal and replacement record can be consulted.

Mitigation: Use of a firewall.

Importance: R for all SILs

6.12 System support for EMI-induced malfunctions

Aim: To prevent EMI from degrading the safety integrity of the safety-related system.

Description: During the operation of a system EMI may cause hardware malfunction in the form of corruption of data in memories and signals on data, address and control bus lines and interfaces. This in turn can cause software to malfunction and hence the system to malfunction, possibly presenting a system safety hazard.

Detection/ Mitigation: Techniques and measures should be applied accordingly bearing in mind the nature and severity of the anticipated EMI and the perceived susceptibility of the system to it.

Some techniques and measures are listed in section Implementation, or alternatives may be used if justification is provided in the safety case.

Importance: HR for all SILs.

Reference: [101] and [107].

7 Operational design

7.1 Operation and maintenance instructions

Aim: To develop procedures which help to avoid EMI-induced failures during the operation and maintenance of the safety-related system.

Description: This is where the operation and maintenance requirements - and their justifications - for the EMC techniques and methods used to comply with the SDRS are documented, also see Clause 7.6 of [119].

The operation instructions may include, for example:

- Restrictions on the use of potentially interfering equipment in the vicinity of the safety system (e.g. mobile phones, portable equipment, welding equipment etc.)
- Restrictions on the removal of access panels where these contribute to EMI protection.
- For portable safety-related equipment, restrictions on the type of EM environment in which the equipment is intended to be used.
- Restrictions in the way the safety-related equipment may be used, for example where the equipment is user-configurable, where this may affect EMI protection.
- Requirements for recording and reporting system upsets, system restarts, safe failures, trips to safe state etc., especially where the cause is not obvious and may be due to an EMI event. (Recording and assessing system trips is an important contributor to reliability growth in general, and it could be the only indication that the EM protection is not operating as intended.)

The maintenance instructions may include, for example:

- Inspection of EMI physical protection measures, such as access panel/door gaskets for deterioration or corrosion of mating surfaces.
- Recommendations on the inspection and maintenance intervals necessary to maintain EMI physical defences.
- Any lifetime restrictions due to the anticipated degradation of EMI physical protection measures e.g. due to corrosion
- Procedures to be followed to verify the continued effectiveness of physical protection measure after an unusual EMI event, such as a major power surge, nearby lightning strike, etc.

Detection: By independent assessment of the relevant documents against the guidance in this document, see Clause 8 of [8] for guidance on the appropriate level of independence.

Mitigation: By correction of the relevant documents.

Importance: HR for all SILs.

Note: Experience indicates that operation and maintenance instructions should only be expected to achieve a risk reduction factor of no more than 2.

7.2 Design for ease of EMC maintenance

The design should make it easy to monitor the condition/performance of, and replace if necessary, EMI mitigation items such as filters, surge suppressors, conductive gaskets, etc., which may have a limited operational life.

7.3 Limited operation possibilities

Aim: EMI can affect operator controls, creating the same effect as an unskilled or even malicious operator. This technique is to avoid operation in unwanted or unnecessary modes.

Description: This approach reduces the operation possibilities, and therefore the possibilities for EMI to cause failures, by limiting, for example:

- the operation within special operating modes, for example by key switches;
- the number of operating elements;
- the number of generally possible operating modes.

The hardware and/or software design techniques used for limiting the possibilities for operation should comply with the requirements of this document.

Detection: Competent independent assessment of the hardware and/or software design techniques used for limiting the possibilities for operation.

Mitigation: By modification of the design, using methods that comply with the requirements of this document.

Importance: HR for all SILs.

7.4 Protection against operator mistakes

Aim: To protect the system against operator mistakes.

Description: Wrong inputs (value, time, etc.) should be detected via plausibility checks, monitoring of the EUC, or other methods. To integrate these facilities into the design, it is necessary to state at a very early stage which inputs are possible and which are permissible.

An operator mistake should not result in dangerous failure. For example, using a walkie-talkie or cellphone closer than is permitted, or the failure to correctly close a shielding door, or to refit a shielding inspection panel, could prevent the attainment of a safe state (see Independent detection of EM disturbance). Such foreseeable misuse should never be permitted to compromise functional safety.

Detection: Competent independent assessment of the hardware and/or software design techniques used for the protection against operator mistakes.

Mitigation: By modification of the design, using methods that comply with the requirements of this document.

Importance: HR for all SILs.

7.5 Modification protection

Aim: To protect the safety-related system against hardware or software modifications or manipulations by technical means.

Description: Modifications or manipulations are detected automatically, for example by plausibility checks for the sensor signals, detection by the technical process, automatic start-up tests. If a modification is detected, appropriate action is taken in accordance with the safety case.

(6.10.2 describes one way of detecting modifications that could degrade EM mitigation.)

Dectection: Competent independent assessment of the hardware and/or software design techniques used for detecting modifications or manipulations.

Mitigation: By modification of the design, using methods that comply with the requirements of this document.

Importance: HR for all SILs.

Note: Modifications should be subject to a change control procedure and should not compromise functional safety.

8 Implementation

When the design is implemented the functionality may sometimes be realized either in hardware or software.

In the subsections below techniques and measures are classified as either hardware or software based, please bear in mind that some techniques and measures may have equivalent representations in either hardware or software.

8.1 Error avoidance

This section describes various detailed techniques and measures. Additional systematic techniques and measures are listed in Section System design.

8.1.1 Compliance with relevant EMC standards over the lifecycle

Aims:

i. To help ensure that EM emissions do not exceed levels which are likely to affect other equipment, over the lifecycle. This is achieved by applying the emissions tests considered appropriate for both the intended application and the expected EM environment(s).
ii. To help ensure that the reasonably foreseeable normal operating EM environment does not cause sufficient EMI to activate any safe failure modes, ensuring adequate availability over the lifecycle.
This is achieved by using the immunity tests considered appropriate for both the intended application and the expected EM environment(s).

Description: Tests selected from the IEC 61000-4 series of EMC immunity test methods should be used unless other tests are more appropriate. Where a customer contractual EMC immunity test is equivalent to a selected test, or exceeds its requirements, it should replace that selected test.

> **Example 1:** A safety-related system in an industrial plant located near to an airport or harbour might apply IEC 61000-6-4 and IEC 61000-6-2 (the generic standards for emissions and immunity for the heavy industrial environment) and also need to be tested for immunity to the various radars it will be exposed to by applying tests using the IEC 61000-4-3 method modified to simulate their levels, frequencies, modulations, pulse repetition rates, etc. – as well as to IEC 61000-6-2 (the generic immunity standard for the heavy industrial environment).
> **Example 2:** Most safety-related systems will be exposed to close-proximity mobile telephones, radio-frequency identification (RFID), and/or machine-to-machine (M2M) transmitters, and so their immunity should be tested accordingly, see [81], in addition to the other EMC immunity tests that have been selected.

See the introduction (and Section 0.7 in [6]) for a discussion of the fact that no practicable immunity testing plan can, on its own, demonstrate sufficient confidence that EMI will not cause unacceptable degradation of functional safety over the lifecycle.

Detection: A test plan should be devised by persons who are competent in applying the selected EMC tests, and testing should be carried out according to the plan.

The tests should preferably be applied to the complete safety-related system, in its final configuration in its intended application, running a typical application program.

Where this is not practicable the standard tests should be applied at the highest practicable level of assembly of the safety-related system or subsystems and the likely limitations and consequences of the partial testing documented. In addition, in-situ EMC testing should be carried out where practicable, using the methodology described in [53].

The immunity tests should show that the system is unaffected at the applied test levels (i.e. their good EMC design, plus filtering, shielding, etc. is adequately rejecting the interference).

The safety functions should not operate during these tests (unless this is adequately addressed in the safety case).
The results of the testing according to the plan should be documented and assessed against the SDRS. Unexpected or anomalous behaviour should be investigated and the underlying causes corrected.

The tests should be carried out in a manner that provides sufficient confidence that compliance with them will be maintained over the complete lifecycle.

> **For example:** Some manufacturers take equipment that complies with its usual EMC emissions and immunity test standards, artificially age it using well-established acceleration techniques, then retest the aged units to check that they still comply with those EMC standards.
> Another approach, sometimes used in large installations or costly military vehicles, is to inspect and/or test all of the EM mitigation measures at regular intervals during their lifecycles, refurbishing or replacing anything that is found to have degraded significantly or is close to its individual, planned, end-of-life.

Mitigation: By competently modifying the design using good engineering practices (see Good EMC engineering practices) until the test requirements are met in a manner that indicates they will be maintained over the lifecycle.

Importance: HR for all SILs (as described in the introduction, Section Introduction of this guide, see especially Figure 2).

References: [50] [51] [53] [54] and [57] to [81].

8.1.2 Protection against physically damaging EM disturbances

Aim: To achieve functional safety despite extreme EM disturbances that can cause permanent damage to hardware (electronic components, interconnections, etc.), where such protection is considered necessary (as it usually is for national infrastructure, for example).

Lightning, electromagnetic pulses and other high power disturbances are examples of the types of extreme EM disturbances considered (see [52] [83] [84] [85] and [86]).

Description: These are very powerful EM disturbances that could cause physical damage that might inhibit the operation of a safety function.

Detection: By performing appropriate tests, such as:
i. for high-power EM: [66] [71] [75] [80] [82] [87] [88] [89] [90] [91] [92] [93] and [98];
ii. for lightning: [60] [63] [64] [66] [71] [82] [94] [95] [96] and [97].

Mitigation: Where it is considered necessary to cope with the occurrence of one or more such extreme EM disturbances over the lifecycle, appropriate mitigation should be applied, as described in [22] [24] [41] [42] [43] [44] [45] and/or [46], to pass the relevant tests.

Alternatively, the safety-related system should default to a non-electrical backup system.

A 'non-electrical backup system' is one based on mechanical, hydraulic and/or pneumatic technologies alone (i.e. with no electrical or electronic control).

Importance: HR for all SILs where it is considered necessary to cope with the occurrence of one or more such extreme EM disturbances over the lifecycle.

Note: The military and defence sectors have their own sets of standards for these high-power EM disturbances, not covered in this guide.

8.1.3 Good EMC engineering practices

Aim: To use accepted EMC engineering practices to provide a first line of defence against EMI.

Description: Well-proven and widely-accepted EMC engineering design practices are applied at every level of design as appropriate, including (but not limited to):

- Partitioning printed circuit boards (PCBs), units/modules/subassemblies/products, systems, installations, networks, etc. into different electromagnetic zones (EM zones), and also into lightning protection zones (usually the same zones), segregated by physical space and/or other EM mitigation techniques.
- Circuit (schematic) design within each EM zone
- Choice of electronic, electromechanical and electrical components within each EM zone
- Communications design (within and between EM zones)
- PCB design and layout (often incorporates several EM zones)
- Power converter design e.g. AC-DC, DC-DC, DC-AC, AC-AC (generally located at EM zone boundaries)
- Enclosure design for units/modules/subassemblies and products (could incorporate several EM zones)
- EMI mitigation techniques such as filtering, shielding, galvanic isolation, surge and transient suppression, etc. (generally located at EM zone boundaries)
- System design (generally incorporates several EM zones)
- Installation and network design (always incorporate several EM zones)

Detection: By assessment of the design by persons competent in the relevant EMC design issues.

Mitigation: By competent correction of the design, where required.

Importance: HR for all SILs.

References:
i. For circuits, units, modules, subassemblies, products, etc. [10] [11] [12] [13] [14] [15] and [16].
ii. For cabinets, systems, installations, networks, etc. [20] to [40].
iii. The EM zone technique is described in [24] and in guides based upon it: [21] [22] and [23].

8.1.4 Use fibre-optic cables for signals and data

Aim: Avoid the effects of EMI by using communications media which are intrinsically immune.

Description: Optical fibres in themselves are unaffected by all EMI (although they require protection from the thermal effects of lightning strikes, if exposed to them) and with suitable environmental protection can be used in all applications, including the most arduous.

Optical fibres and their electronic interfaces (transmitters and receivers) are available in a wide range of types (and costs) to carry analogue signals from DC up to several GHz, and data at up to hundreds of gigabytes per second.

Optical fibre transmitters and receivers are affected by EMI, and so need to employ the design techniques of Good EMC engineering practices above - but they are very small, making it much easier and less costly than applying the necessary EMI protection techniques to metal cables carrying signals, data or control.

Importance: R for SIL 1 to 3, HR for SIL4.

8.1.5 Defensive programming

Aim: To produce programs in such a way that they will detect anomalous control flow, data flow or data values that may have been caused by EMI during their execution and to react in a predetermined and acceptable manner.

Description: Many techniques can be used during programming to detect and control the anomalies induced by EMI induced corruption, see the references.

Various techniques described in Sections Specification to Power hold-up in this guide can be used at the hardware level to implement an acceptable hardware/software solution.

Detection/ Mitigation: The principal defensive mechanisms are listed in 8.1.5.1 and 8.1.5.2.

References: [100] [101] [102] and [104].

8.1.5.1 Strong data typing

Detection: The programming language provides a means of assigning a data type to a data variable to define the range (or set) of values that it is intended to contain. Whenever values are assigned to the variable, either at compile time (constant values) or at runtime (constant or modified values) then a check is made that the new data value is within the range of values specified by the type of the variable.

This is valuable for EMI detection as the value of the original variable may have been corrupted by an EMI event. The program might well be correct but the result of an assignment might be 'out of range' and cause the program to malfunction. In any case all variables should be initialised explicitly to an acceptable value so that out of range errors are not caused by the arbitrary value in a memory when power is first applied.

Mitigation: If the language's run-time package supports range checking, then that can be used (bearing in mind the loss of performance and increased size of program). If there is no automatic run-time range checking, then explicit tests should be designed into the program.

Importance: R for SIL 1 and 2, HR for SIL 3 and 4.

References: [100] [102] and [104].

8.1.5.2 Sequence checking

Detection: Sequence checking is a powerful technique for ensuring that a stream of data packets is in the correct order and that there is no duplication and there are no omissions. Sequence checking can be used for data and also for program state e.g. using finite state machines or Petri nets. The program contains intermediate points where the expected state of the program, i.e. the values of data or status variables, are checked for credibility.

Mitigation: Various techniques described in this guide and others, can be used at the hardware level to implement an acceptable solution.

Transmission protocols at the packet level can be used to improve the effective quality and reliability of the link.

If the program is detected as being out of sequence then this fact can be logged and then, if appropriate, a recovery attempted so that processing can continue from a known valid state.

Importance: HR for systems intended for continuous operation and especially for SIL 3 and 4.

R for on-demand systems, for all SILs.

References: [102] [104] and [107].

8.1.6 Limited use of memory address pointer variables

Aim: Reduce impact of memory corruption due to EMI.

Description: A pointer is a variable with a value that is an address of data in memory. If the pointer variable is corrupted by EMI then the impact on the behaviour of the program is likely to be unpredictable. For example the corrupted pointer may either be pointing at some data, the program subroutine stack, the heap, or even the program itself, and consequently any write operation will corrupt the system.

Detection: At compile time a static analysis program may be used to flag up any use of pointers.

Mitigation: A set of programming guidelines would normally prohibit the explicit use of pointers, unless this is essential from an algorithmic viewpoint and its use can be clearly justified in the safety case.

When the program is being compiled a static analysis tool can be used to detect the use of pointers and raise an alert. If the processor architecture allows memory address ranges to have protected access then this feature can be used to ensure that only the intended memory partitions are accessible in each context. This also would make available the means for detecting an access violation, however it would not detect data content corruption within accessible address ranges.

Partitioned ranges of memory and/or a memory management unit can be used to detect violations and provide some measure of protection, see 8.2.1.3.

Importance: HR for systems intended for continuous operation, especially for SIL 3 and 4.

R for on-demand systems, for all SILs.

8.1.7 Avoid use of recursion

Aim: To reduce the impact of corruption of program execution due to EMI.

Description: Recursion is the act of a program calling or referencing a part of itself, either directly or indirectly.

It is more susceptible to the effects of EMI-induced corruption as the nested chain of calls is held as a linked list on the stack, in effect potentially a very large list of pointers which increases susceptibility to EMI. It should only be used with the greatest caution in safety-related software.

Detection: At compile time a static analysis program may be used to find instances of recursion in the program source text.

Mitigation: Programming guidelines would normally prohibit the use of recursion unless its use is clearly justified in the safety case. This would require a rigorous argument or proof regarding the maximum depth of recursion that would be experienced during operation, and the amount of memory that would be required to support this at runtime.

Every algorithm that can be expressed using recursion also has an equivalent using an iterative looping construct. In general the latter should be the preferred solution.

Importance: HR for all SILs.

8.2 Error detection and error correction

This section describes various detailed techniques and measures, additional systematic techniques and measures are in section System design. The following techniques are not exhaustive, other techniques and measures may be used provided evidence is produced in support.

Not all of the following techniques and measures need be used, but sufficient should be used appropriate to the system's complexity and application, taking into account the fact that EMI can cause a nearly infinite variety of noisy, degraded, distorted, delayed, altered-priority, etc., signals on one or more of the system's ports simultaneously, and under/over voltages, intermittency and noise on some or all power supplies.

8.2.1 Invariable memory (ROM)

Global objective: The detection of information modifications in the invariable memory (ROM, or program memory).

8.2.1.1 Signature of a word or block of data

Aim: To detect all one-bit failures and all multi-bit failures within a word of data, as well as a high proportion of all possible bit failures in a block, depending on the strength of the CRC (typically 8, 16 or 32 bit).

Description: This procedure calculates a signature using a cyclic redundancy check (CRC) algorithm. The extended signature is stored, recalculated and compared as in the single-word case. A failure is indicated if there is a difference between the stored and recalculated signatures.

Detection/ Mitigation: When an error is detected, apply a response defined by the safety case.

Importance R for SIL 1 and 2, HR for SIL 3 and 4.

Note: Modified checksums are insufficiently rigorous to be of any significant assistance against EMI.

References: [108] to [112]

8.2.1.2 Block replication (for example double (redundant) ROM with comparison)

Aim: To detect all bit failures.

Description: The address space is duplicated in two memories, which ideally should be physically separate. The data is stored inversely in one of the two memories and inverted again to be compared with the other copy.

The inversion of the data in one memory makes this technique much more effective against common-cause errors, malfunctions or failures including the typical effects of EMI.

Detection: The outputs are compared and a failure indication is produced if a difference is detected.

Mitigation: Repeat the memory read as many times as necessary without unacceptably degrading the safety integrity. If the failure clears, continue operation as usual, in any case the fault should be recorded if a log is available, see Fault detection and event data recording for diagnosis. If during the time available the failure does not disappear, apply an appropriate response defined by the safety case.

Importance: HR for all SILs, a powerful technique that should be used wherever practicable.

Note: The use of diverse types of memory can improve the effectiveness of this technique.

8.2.1.3 Memory boundary protection

Aim: Memory boundary protection, by preventing incorrect memory areas from being used.

Description: Runtime plausibility checking of use of a memory segmented into partitions. Statically defined and protected address ranges are used for the following:

- Program
- Stack
- Statically-allocated variables
- Heap (dynamically allocated variables)
- Inputs
- Outputs

Detection: This technique simply prevents incorrect memory areas from being used, for example, by the effects of interference on the address bus.

If the mechanism used to manage memory accesses can detect out of range addressing violations then they could be logged to support testing and diagnosis of system malfunction.

Mitigation: Upon detection, apply an appropriate response defined by the safety case.

Importance: R for SIL 1 and 2, HR for SIL 3 and 4.

References: [113] [114] [115] and [116].

8.2.2 Redundancy with duplication and/or diversity

Aim: To enhance resilience to EMI.

Description: The system may be replicated using one or more processors and/or buses. Each system independently determines the next action to be taken and their results are compared before the action is sanctioned. Various schemes can be used, for example 2 channels, 3 channels, one channel per processor or multiple channels per processor.

Hardware diversity (see 6.3) and/or software diversity (see 6.4) will improve resilience to the common-cause errors, malfunctions or failures typical of EMI.

Where duplicate or triplicate channels are used without hardware diversity, with or without software diversity, the effectiveness of this technique against common cause errors can be increased by ensuring that the channels are desynchronised, or if synchronous are kept out of step with one another. This makes it less likely that EMI will affect all the channels in the same way.

When multiple channels are implemented on physically separate processors the resilience will be enhanced if the power supplies are isolated and the interconnections are properly protected against EMI.

Detection: The result of comparing the sets of signals must be acceptable for safety in the current context.

The comparator (the circuit used to compare channels and detect errors) is a weak point and so must be designed to have considerably greater resilience to EMI for this technique to be effective.

Mitigation: Upon detection of an anomaly apply an appropriate response defined by the safety case.

Importance: HR for systems intended for continuous operation, especially for SIL 3 and 4.

R for all other systems for SIL 1, 2 and 3, HR for SIL 4.

Note: To increase the effectiveness of this technique against the common-cause errors, malfunctions or failures typical of EMI) diverse encoding of data and or programs may be used, see 6.4.

8.2.3 Transmission redundancy (time-based)

Aim: To detect transient failures in bus and/or interface communication.

Description: The information is transferred several times in sequence. The repetition is effective only against transient failures.

Detection: Each instance of the information is stored as it is received and then the instances are compared.

Mitigation: If the instances do not agree, upon detection, apply an appropriate response defined by the safety case.

Importance: R for SIL 1 and 2, HR for SIL 3 and 4.

Note: Requires at least one complete repetition in one cycle time of the process.

References: [100] [102] [104] [107] and [109]

8.2.4 Variable (RAM) memory ranges

Global objective: Detecting failures during addressing, writing, storing and reading.

8.2.4.1 Memory test patterns

Aim: To detect malfunctions in the storage and retrieval of data in memory.

Description: A number of different test patterns can be used to write data to memory and to read it back for checking. These tests are designed to verify that each memory cell is functional at the bit level and that the memory addressing is faithful.

Dectection: The technique is useful for detecting manufacturing faults, random failures, and damage caused by electrostatic discharges. In general it cannot detect soft errors caused by radiation-induced errors.

The appropriate pattern and technique depends on the characteristics of the memory technology. Typical examples of test patterns are known as checkerboard (march), walkpath, galpat, transparent galpat, and abraham.

Mitigation: The test pattern may be repeated as many times as necessary without unacceptably degrading the safety integrity. If the failure persists, apply an appropriate response defined by the safety case.

Importance: R for SIL 1 and 2, HR for SIL 3 and 4.

Note: If this technique is used as a background test during run time, it must not interfere with the operation of the safety function. It is essential that the memory content after each test is left identical to its content before that test.

8.2.4.2 One-bit redundancy

Aim: To detect 50% of all possible bit failures in a memory location, bus or I/O register.

Description: Every data word is extended by a single bit, the parity bit.

Detection: The parity of the data word is checked each time it is read. If invalid parity is detected then a failure action is activated.

Mitigation: Upon detection, apply an appropriate response defined by the safety case.

Importance: R for all SILs.

8.2.4.3 Double (redundant) RAM with comparison and read/write test

Aim: To detect all bit failures.

Description: The address space is duplicated in two memories, which ideally should be physically separate. The data is stored inversely in one of the two memories and inverted again to be compared with the other copy.

The inversion of the data in one memory makes this technique much more effective against common-cause errors, malfunctions or failures including the typical effects of EMI.

Detection: The outputs are compared and a failure indication is produced if a difference is detected.

Mitigation: Repeat the memory read as many times as necessary without unacceptably degrading the safety integrity. If the failure clears, continue operation as usual. If during the time available the failure does not disappear, apply an appropriate response defined by the safety case.

Importance: HR for all SILs.

Note 1: A powerful technique that should be used wherever practicable.

Note 2: The use of diverse memory devices (see Diverse hardware (redundancy)) can improve the effectiveness of this technique as regards EMI.

8.2.5 ROM, RAM, bus and interface monitoring with error-detection codes (EDC) or error-correction codes (ECC)

Aim: To detect one or more bit failures in a word.

Description: The memory, or the content of an interface data stream, is extended by one or more bits. Data code protection provides for dataflow-dependent failure detection, based on information redundancy (e.g. CRC or Hamming codes) and/or time redundancy.

Detection: Every time data is handled, either hardware or software can determine whether a corruption has taken place by checking the additional bits. The number of additional bits establishes the number of bit errors in the data word that can be detected.

Mitigation: If a difference is found, corrective action can be taken (or a failure indication produced). Correction of the data can be used to maintain the correct operation of the safety function.

Importance: R for SIL 1 and 2, HR for SIL 3 and 4.

Note: The strength of the technique used should be justified in the safety case.

References: [110] [111] and [112].

8.2.6 Logic and data processing units

Global objective: To recognise failures which lead to incorrect results in processing units.

All the techniques and measures listed in this clause are concerned with detecting failures in the processing units and soft failures (bit flips) in memories and registers, and so are useful for detecting damage caused by lightning (or other) surges and electrostatic discharges, and soft failures such as those caused by ionising radiation etc.

8.2.6.1 Self-test by software

Description: Standard processing unit hardware with additional software functions running self-tests.

Detection: Can detect some failures but coverage is low.

Self-test may also be affected by the failure.

Mitigation: May require additional monitoring circuitry to achieve a safe state on failure.

Importance: NR for all SILs.

8.2.6.2 Self-test supported by hardware (one-channel)

Description: Additional special hardware supports self-test functions, for example it monitors the output of a certain bit pattern. (This is essentially a sophisticated watchdog.)

Detection: Coverage depends on the extent of the software functions generating the bit pattern. Used for detecting disruption of program execution.

Mitigation: The additional hardware can drive the system to a safe state and/or restart if it is safe to do so.

Importance: HR for all SILs.

8.2.6.3 Coded processing (one-channel)

Description: Processing unit designed with special failure-recognising or failure-correcting circuit techniques.

Detection/ Mitigation/ Importance: When used, the benefits to EMI resilience should be assessed for the particular implementation, and the analysis recorded in the safety case.

8.2.6.4 Reciprocal comparison by software

Description: Two processing units exchange data (results, intermediate results, and test data) and cross-check using software in each unit. Detected differences indicate a failure.

Detection: Coverage of data discrepancies is high and detection can be fast. Excellent against hard failures and can be good against soft and transient failures too.

Mitigation: If the diagnostic test interval is short compared to the process safety time, a restart may be possible while keeping the process running. If the failed unit can be identified, continued operation with the healthy unit may be possible. Otherwise, the safety function must achieve a safe state.

Importance: HR for all SILs.

Note: The use of hardware and/or software diversity can greatly improve coverage of common-cause errors, malfunctions and failures, for example those typical of EMI. See Diverse hardware (redundancy) and Diverse software for descriptions of hardware and software diversity, respectively.

8.2.7 Electrical and electromechanical components

Aim: To control failures in electromechanical components, such as relays, actuators, magnetic logic devices etc.

Description: Electromechanical components are generally less susceptible to EMI-induced failure than electronic components as the operating signal levels are usually much higher.

Direct failures due to gross overload causing contact welding or coil burnout are possible in some applications. More generally, EMI to circuits controlling electromechanical devices may cause failures due to chatter (unintended repeated operation causing wear out), paralysis (device stuck) or generation of EMI via arcing or sparking.

Detection: Electromechanical components may be monitored as part of loop, e.g. by relay contact monitoring, by actuator position monitoring, or by the effects on the EUC (on-line monitoring). Care should be taken that such monitoring will detect chatter (especially in relays) or partial operation in actuators.

The use of diverse technologies (see Diverse hardware (redundancy)) is recommended when performing parallel functions.

Mitigation: Burn-out or paralysis failures should be designed to achieve a safe state.

Multi-channel systems may be able to tolerate a single-channel failure but the likelihood of common mode failures must be considered. Examples are suppression of arcing and proper termination of inductive loads to avoid induced spikes.

Importance: HR for all SILs.

8.2.8 Electronic components

Global objective: To control failures in solid-state components.

8.2.8.1 Tests by redundant hardware

Aim: The use of additional hardware to monitor the operation of the safety function.

Description: Redundant hardware can be used to test safety functions (Diagnostic testing implemented by additional hardware.)

Detection: Good at detecting failed states but may be poor at detecting transient failures. Coverage depends on the rate of test compared to the process safety time.

Mitigation: Effectiveness depends on diagnostic coverage and diagnostic test interval compared to the process safety time. Importance: R for all SILs.

8.2.8.2 Dynamic principles

Aim: To detect static failures by dynamic signal processing.

Description: A forced change of otherwise static signals helps to detect static failures. For example, alternating voltage signals are less vulnerable to stuck-at faults than static (direct voltage) signals.

Detection/ Mitigation: Good at detecting failed states but poor at detecting transient failures.

Importance: R for all SILs.

8.2.8.3 Standard test access port and boundary-scan architecture

Aim: To control and observe what happens at each pin of an IC.

Description: A designed-in IC self-test technique. Additional logic between the I/O buffers and the core logic allows testing of the core logic.

Detection:/ Mitigation If available, its effectiveness against EMI should be determined taking into account the particular design features, and the analysis recorded in the safety case.

Importance: R for all SILs.

Note: Additional complexity within the IC may make it more susceptible to EMI.

8.2.8.4 Monitored redundancy

Aim: To compare the behaviour of two or more channels in a multi-channel system.

Description The safety function is executed by at least two hardware channels. The outputs of these channels are monitored and a safe condition is initiated if the output states differ.

Detection: Effective against static and transient failures, provided the monitoring system is not itself prone to EMI.

Mitigation: Transition to the safe state. With more than two channels and a voting function, isolation of the faulty channel and continued operation may be possible, see 6.3.

Importance: R for SIL 1 and 2, HR for SIL 3 and 4.

Note: Using hardware and/or software diversity (see Diverse hardware (redundancy), Diverse software and Redundancy with duplication and/or diversity) provides for better coverage of common-cause errors, malfunctions and failures typical of EMI.

8.2.8.5 Hardware with automatic self-test

Aim: To detect faults by periodic checking of the safety functions using automatic self-tests.

Description: The hardware self-tests repeatedly at suitable intervals.

Detection/ Mitigation: Will only detect failed states, not transient failures.

Importance: R for all SILs.

8.2.8.6 Analogue signal monitoring

Aim: To improve confidence in measured signals.

Description: Analogue signals are used in preference to digital on/off states. Trip or safe states are represented by analogue signal levels, which can be continuously monitored for credibility.

Detection: Can be effective against EMI, especially if unusual signal excursions are logged and investigated.

Mitigation: Information from logs of unusual signal excursions can be used to improve long term resilience to EMI.

Importance: HR for signals between devices, for all SILs.

8.2.8.7 Content credibility checking

Aim: To use known relationships within a dataset to detect corruption due to EMI.

Descripton/ Detection: The concept of data type can be extended to a collection of variables, typically a list, array or record structure. Various checking schemes can be used to enable detection of corruption, for example checksums or CRCs.

Various techniques described in this section can be used at the hardware level to implement an acceptable solution.

Mitigation: Upon detection of an anomaly apply an appropriate response defined by the safety case.

Importance: HR for systems intended for continuous operation, especially for SIL 3 and 4.

R for on-demand systems, for all SILs.

8.2.9 Temporal and logical program sequence monitoring

Global objective: To detect a defective program sequence. A defective program sequence exists if the individual elements of a program (for example software modules, subprograms or commands) are processed in the wrong sequence or period of time, or if the clock of the processor is faulty.

8.2.9.1 Watch-dog with separate time base without time-window

Aim: To monitor the behaviour and the plausibility of the program sequence, to detect divergence from intended program execution sequence and timing.

Description: External timing elements with a separate time base (for example watch-dog timers) are periodically triggered to monitor the computer's behaviour and the plausibility of the program sequence. It is important that the triggering points are correctly placed in the program.

The watch-dog is not triggered at a fixed period, but a maximum interval is specified.

The watch-dog(s) should use techniques or measures that comply with this guide.

Detection: When the program fails to trigger any watchdog (there could be several, monitoring different points in the program's execution sequence), a failure is indicated.

Mitigation: Upon detection, apply an appropriate response defined by the safety case.

Importance: If a time-window watchdog (8.2.9.2) cannot be used, R for SIL 1 & 2, NR for SIL 3 & 4.

8.2.9.2 Watch-dog with separate time base and time-window

Aim: To monitor the behaviour and the plausibility of the program sequence.

Description: Timing elements physically separate from the computer, with a separate time base (watch-dog timers), are periodically triggered to monitor the computer's behaviour and the plausibility of the program sequence. It is important that the triggering points are correctly placed in the program. Lower and upper time limits are given for the watch-dog.

Detection: If the program sequence takes a longer or shorter time than expected, a failure is indicated.

Mitigation: Upon detection, apply an appropriate response defined by the safety case.

Importance: HR for all SILs.

8.2.9.3 Logical monitoring of program sequence

Aim: To monitor the correct sequence of the individual program sections.

Description: The correct sequence of the individual program sections is monitored using software (counting procedure, key procedure) or using external monitoring facilities. It is important that the checking points are placed in the program correctly.

Detection: If the correct program sequence does not occur, a failure is indicated.

Mitigation: Upon detection, apply an appropriate response defined by the safety case.

Importance: R for SIL 1 and 2, HR for SIL 3 and 4.

8.2.9.4 Combination of temporal and logical monitoring of program sequences

Aim: To monitor the behaviour and the correct sequence of the individual program sections.

Description: A temporal facility (for example a watch-dog timer) monitoring the program sequence is retriggered only if the sequence of the program sections is also executed correctly.

Detection: If the temporal facility (for example a watch-dog timer) monitoring the program sequence is not retriggered as required, a failure is indicated.

Mitigation: Upon detection, apply an appropriate response defined by the safety case.

Importance: R for SIL 1 and 2, HR for SIL 3 and 4.

Note: This technique is preferred over 8.2.9.1, 8.2.9.2 and 8.2.9.3 above.

8.2.10 Multi-channel interface input or output with comparison

Aim: To detect random hardware failures (stuck-at failures), failures caused by external influences (e.g. EMI), timing failures, addressing failures, drift failures and transient failures (e.g. intermittency).

Desciption: This is a dataflow-dependent multiple-channel technique with independent inputs and/or outputs for the detection of random hardware failures and systematic errors.

To make this technique more effective against common-cause errors, malfunctions or failures, which are typical effects of EMI, diverse signals (e.g. encoding, inversion, modulation, amplitude range, offset, etc.) should be used.

Detection: Failure detection is carried out by comparing the signals with each other.

The comparator (the circuit used to compare channels and detect errors) is a weak point and so must be designed to have considerably greater resilience to EMI for this technique to be effective.

Mitigation: If a signal corruption is detected by the communicating partner(s), request retransmission of the input or output data. If the failure clears, continue operation as usual. If during the time available the failure does not disappear, apply an appropriate response defined by the safety case.

Importance: HR for all SILs.

Note: To increase the effectiveness of this technique against the common-cause errors, malfunctions or failures typical of EMI, hardware and software diversity (see 6.3 and 6.4 respectively) may be used.

Reference: [117]

8.3 Other / miscellaneous

8.3.1 Test patterns for interfaces and buses

Aim: To detect static failures (stuck-at failures) and cross-talk, particularly in input and output units (digital, analogue, serial or parallel), and to prevent the sending of inadmissible inputs or outputs to the process.

Description: This is a dataflow-independent cyclical test of input and output units. It uses a defined test pattern to compare observations with the corresponding expected values. The test pattern information, the test pattern reception, and test pattern evaluation must all be independent of each other. The test pattern should not interfere with the correct operation of the safety function.

Useful for increasing resilience to EMI by detecting damage caused by overvoltages from lightning, electrostatic discharges, and other sources.

Detection: When the observations do not correspond with the expected values for the test pattern, a failure is indicated.

Mitigation: Repeat the test pattern as many times as there is time for without unacceptably degrading the safety integrity. If the failure clears, continue operation as usual. If during the time available the failure does not clear, apply an appropriate response defined by the safety case.

Importance: HR for all SILs.

8.3.2 Power supply (i.e. power converter unit)

Global objective: To detect or tolerate failures caused by degradations or defects in any of the power supplies.

8.3.2.1 Detecting defects

Description Various techniques are available, such as overvoltage protection with safety shut-off, secondary voltage control, and power-down with safety shut-off.

Detection/ Mitigation: Upon detecting a degradation or other defect in a power supply, apply an appropriate response as defined by the safety case.

Importance: HR for all SILs.

8.3.2.2 Detecting excessive RF on power supplies

Aim: To detect the presence of excessive noise on power supplies, whether caused by failed/degraded decoupling capacitors, shielding, filtering, etc., or by EMI.

Description: Simple broadband RF detectors can be made with ordinary circuit techniques (resistor, Schottky diode, capacitor, op-amp) that will reliably detect frequencies up to tens of MHz. Some semiconductor manufacturers make single-chip RF detectors guaranteed to detect up to many GHz.

It will generally be necessary to set the sensitivity of the detector so that it does not trigger on the normal systematic noises made by the unit itself.

Detection: Excessive levels of RF on AC power lines or DC power rails cause the RF detector to trigger.

Mitigation: If during the time available the excessive noise does not disappear, apply an appropriate response as defined by the safety case.

Importance: R for SIL 1 and 2, HR for SIL 3 and 4.

8.3.3 Power hold-up

Aim: To maintain the power supply for long enough during and/or after any transient or short-term deficiencies in the electrical power supply (e.g. dips, dropouts interruptions, undervoltages, sags, etc.) to avoid a dangerous failure.

In the case of long sags, undervoltages or interruptions, the energy storage should be sufficient to continue correct (safe) operation whilst the EUC is put into a safe state or some other action taken to maintain the safety integrity according to the safety case.

Description: Sufficient energy is stored in capacitors, supercapacitors, batteries, etc., to ensure the above aims are met.

EUCs with high power requirements and/or requiring a long time to be put into a safe state despite lack of power for the safety-related system, might use large battery banks (e.g. either directly or as part of a UPS) and/or rotating reserve power generators.

Detection: Analysis and testing of the worst possible combinations of circumstances, including a continuous low and/or distorted supply voltage, components tolerances and the effects of ageing, to ensure that the above aims are reliably met.

Mitigation: Improvement of the design, e.g. by adding more energy storage.

Importance: HR for all SILs.

8.3.4 Monitoring of ventilation, cooling and heating

Aim: Failures of the ventilation, cooling or heating may expose the safety-related system to excessive environmental conditions, possibly increasing the rate of dangerous failure to an unacceptable level. Such failures could be caused by EMI.

Description/ Detection: Ventilation, cooling and heating systems are monitored for correct operation.

Mitigation: When a failure is detected, an appropriate response can be made, according to the safety case, before the safety system is adversely affected.

Importance: HR for all SILs.

8.3.5 De-rating

Aim: To increase the reliability of hardware components, particularly those used for the suppression of EMI or protection against its effects.

Description: Hardware components are operated at levels well below their specified maximum ratings or stress levels.

EMI suppression/protection components should be especially conservatively rated to survive repeated stress levels considerably higher than the worst anticipated, taking into account the full range of all reasonably foreseeable physical and climatic environments over the lifecycle (e.g. vibration, extremes of ambient temperature for example when the air-conditioning has failed, etc.).

Detection: By independent assessment of the design, see Clause 8 of [8] for guidance on the degree of independence.

Mitigation: By modification of the design.

Importance: SIL 1, 2 and 3, HR for SIL 4.

9 Verification and validation

9.1 Safety-related system safety validation

Global objective: To validate as far as is practicable that the techniques and measures that have been applied function according to the design requirements specification.

Detection: By performing the tests listed below, at least, at the highest practicable level of assembly of the safety-related system.

Mitigation: By modifying the design so as to ensure that all the tests applied are passed. Failure prediction techniques such as the following may be helpful:

- Failure modes and effects analysis (FMEA).
- Failure modes, effects and criticality analysis (FMECA)
- Cause consequence diagrams.
- Event tree analysis (ETA).
- Fault tree analysis (FTA).
- Fault tree models.

Importance: HR for all SILs.

9.2 Examples of verification and/or validation methods

Aim: To achieve confidence in the EMC design.

Description: A wide variety of techniques are used, so that design issues that are not detected by one type of method might be detected by one or more different types of methods, for example:

a. Demonstrations such as demonstrating that the functional safety requirements have been correctly implemented, using any appropriate methods.
b. Checklists to ensure that design techniques and measures have been observed, applied and implemented correctly.
c. Inspections check that assembly and installation have correctly followed their designs.
d. Reviews and assessments these ensure compliance with the objectives of each phase of the lifecycle. Usually performed by experts, on each phase of the lifecycle and the various stages of the activities within each phase.
e. Independent reviews and assessments.
f. Audits which include verification processes for specification, design, assembly, installation.
g. 'Walk throughs' of normal operation, and plausibly abnormal operations (devil's advocacy).
h. Non-standardised 'ad hoc' checks and tests.
i. Individual and/or integrated hardware tests for different parts of the final assembly or system are assembled step-by-step, with checks and tests applied to ensure that they function correctly at each step.
j. Validated computer modelling, simulation, etc.
k. EMC tests for emissions and immunity, on individual parts of the safety-related system and on the whole system at its highest practicable level of assembly, as described in Compliance with relevant EMC standards over the lifecycle.
l. The normal EMC tests applied according to Compliance with relevant EMC standards over the lifecycle can be modified to provide greater coverage of the possible effects of EMI, as described in [54] [55] and [56].

Detection: Different verification/validation methods discover weaknesses or omissions in the design.

Mitigation: Changes are made to the design or operation to eliminate the weaknesses or omissions. Preceding lifecycle phases should be reviewed if they may be affected by the changes. Consideration should be given as to whether similar weaknesses or omissions may present in other, similar safety functions. If so, similar changes should be carried out to those safety functions.

Importance: HR for all SILs.

References: Section 5.3 in [6].

10 References

10.1 General references

[1] IEC 61508-7 Ed.2:2010, Functional safety of electrical/electronic/programmable electronic safety related systems - Part 7: Overview of techniques and measures, IEC Basic Safety Publication (2010), http://webstore.iec.ch

[2] IEC TS 61000-1-2 Ed.2:2008, Electromagnetic compatibility (EMC) - Part 1-2: Part 1-2: General - Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena, IEC Basic Safety Publication (2008), http://webstore.iec.ch

[3] IEC 61326 Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - General industrial applications, http://webstore.iec.ch

[4] IEC 61326 Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - Industrial applications with specified electromagnetic environment, http://webstore.iec.ch

[5] IEC 61000-6-7 (draft, 2013), Electromagnetic compatibility (EMC) - Part 6-7: Generic standards - Immunity requirements for systems, equipment and products intended to perform functions in a safety-related system (functional safety) in industrial environments, http://webstore.iec.ch

[6] Guide on EMC for Functional Safety, published by the IET in 2008,
PDF download: http://www.theiet.org/factfiles/emc/index.cfm
Colour-printed book: http://www.emcacademy.org/books.asp

[7] 2004/108/EC, the European Union's Directive on EMC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:390:0024:0037:en:PDF.
Note: does not cover any safety issues

[8] IEC 61508-1 Ed.2:2010, Functional safety of electrical/electronic/programmable electronic safety related systems - Part 1: General Requirements, IEC Basic Safety Publication (2010), http://webstore.iec.ch

10.2 Good EMC engineering for products

[10] EMC for Printed Circuit Boards - Basic and Advanced Design and Layout Techniques, Second Edition, Nutwood UK December 2010, ISBN 978-0-9555118-5-1, (the 2nd Edition is identical to the 1st Edition except for the book's format), http://www.emcacademy.org/books.asp

[11] EMC Design Techniques for Electronic Engineers, Keith Armstrong, Armstrong/Nutwood UK 2010, ISBN: 978-0-9555118-4-4, http://www.emcacademy.org/books.asp

[12] EMC for Product Designers, 4th Edition, Tim Williams, Newnes, December 2006, ISBN: 0-750-68170-5

[13] High Speed Digital Design: A Handbook Of Black Magic, Johnson, Howard and Graham, Martin, Prentice Hall, 1993, ISBN 0-13-39-5724-1

[14] Robust Electronic Design Reference Book, Volumes I and II, John R Barnes, Kluwer Academic Publishers, 2004, ISBN: 1-4020-7739-4

[15] Printed Circuit Board Design Techniques for EMC Compliance, Second Edition, A Handbook for Designers, M Montrose, IEEE Press 2000, ISBN 0-7803-5376-5, http://www.ieee.org/ieestore

[16] EMC and the Printed Circuit Board - Design, Theory and Layout Made Simple, M Montrose, IEEE Press 1998, ISBN 0-7803-4703-X, http://www.ieee.org/ieestore

10.3 Good EMC engineering for systems and installations

[20] IEC 61000-5-2 ed1.0, November 1997, "Electromagnetic compatibility (EMC) - Part 5: Installation and mitigation guidelines - Section 2: Earthing and cabling" , http://webstore.iec.ch

[21] Good EMC Engineering Practices in the Design and Construction of Industrial Cabinets (relevant for all types of electrical/electronic equipment), Keith Armstrong, REO (UK) Ltd., http://www.reo.co.uk/knowledgebase

[22] Good EMC Engineering Practices in the Design and Construction of Fixed Installation, Keith Armstrong, REO (UK) Ltd., http://www.reo.co.uk/knowledgebase

[23] EMC for Systems and Installations, Tim Williams and Keith Armstrong, Newnes 2000, ISBN 0-7506-4167-3, http://www.bh.com/newnes, RS Components Part No. 377-6463

[24] IEC/TR 61000-5-6, "Electromagnetic Compatibility (EMC) - Part 5: Installation and mitigation guidelines - Section 6: Mitigation of external influences", http://webstore.iec.ch

[25] Designing Electronic Systems for EMC, William G Duff, 2001, ISBN: 978-1-891121-42-5, Scitech Publishing, Inc., http://www.scitechpublishing.com

[26] Complying with IEC 61800-3 - Good EMC Engineering Practices in the Installation of Power Drive Systems, Keith Armstrong, REO (UK) Ltd., http://www.reo.co.uk/knowledgebase

[27] Mains Harmonics (problems and solutions) Keith Armstrong, REO (UK) Ltd., http://www.reo.co.uk/knowledgebase

[28] Power Quality (problems and solutions) Keith Armstrong, REO (UK) Ltd., http://www.reo.co.uk/knowledgebase

[29] Grounds for Grounding, Elya B Joffe and Kai-Sang Lock, IEEE Press, John Wiley & Sons, Inc., 2010, ISBN 978-04571-66008-8

[30] Protection of Electronics in High-Power Installations: Theory, Guidelines and Demonstrations, P C T van der Laan and A P J van Duerson (Eindhoven University of Technology), CIGRÉ Symposium, Lausanne, 1993, paper 600-08

[31] Reliable Protection of Electronics Against Lightning: Some Practical Examples, P C T van der Laan and A P J van Duerson (Eindhoven University), IEEE Trans. EMC, Vol 40, No 4, November 1998, pp 513-520

[32] Design Philosophy for Grounding, M A van Houten and P C T van der Laan (Eindhoven University of Technology), Proc. 5th Int. Conf. on EMC, York, UK, IERE Publication No. 71 (1986) p 267-272

[33] Protection of Cables by Open-Metal Conduits, S Kapora, E Laermans, A P J van Duerson, IEEE Trans. EMC, Vol. 52, No. 4, Nov. 2010, pp 1026 - 1033

[34] Analysis of Electromagnetic Shielding of Cables and Connectors (keeping currents/voltages where they belong), Lothar O. (Bud) Hoeft, PhD, IEEE, 2002, http://simbilder.com/ieee/34/EMag_Shielding_of_Cables_and_Connectors.pdf

[35] IEC 364-4-444:1996, Electrical Installations of Buildings - Part 4: Protection for safety - Chapter 44: Protection against overvoltages - Section 444: Protection against electromagnetic interference (EMI) in installations of buildings, http://webstore.iec.ch

[36] EN 50310, Application of equipotential bonding and earthing at premises with information technology equipment, http://shop.bsigroup.com/en

[37] ETSI EN 300 253:2002, Earthing and bonding of telecommunication equipment in telecommunication centres, http://www.etsi.org/deliver/etsi_en/300200_300299/300253/02.01.01_60/en_300253v020101p.pdf

[38] ITU-T Recommendation K.27 (1996), Bonding configurations and earthing within a telecommunications building, http://www.itu.int/rec/T-REC-K.27-199605-I

[39] ITU Recommendation K.35 (1996), Bonding configurations and earthing at remote electronic sites, http://www.itu.int/rec/T-REC-K.35-199605-I

[40] EN 50174-2, Information Technology - Cabling Installation Part 2: Installation planning and practice inside buildings, http://shop.bsigroup.com/en

[41] IEC/TR 61000-5-3, Installation and mitigation guidelines - HEMP protection concepts

[42] IEC/TS 61000-5-4, Installation and mitigation guidelines - Immunity to HEMP - Specifications for protective devices against HEMP radiated disturbance.

[43] IEC 61000-5-5, Installation and mitigation guidelines - Specification of protective devices for HEMP conducted disturbance.

[44] IEC 61000-5-8, HEMP protection measures for the distributed infrastructure

[45] IEC 61000-5-9, Installation and mitigation guidelines - System-level susceptibility assessments for HEMP and HPEM.

[46] ORNL/Sub/91-SG9131/1:1992, Recommended engineering practice to enhance the EMI/EMP immunity of electric power systems, Oak Ridge National Laboratory, USA.

10.4 Assessing the EM environment, and verification by testing

[50] EMC Testing (in seven parts), 'Do-It-Yourself' testing from lowest-cost to fully accredited, Keith Armstrong and Tim Williams, EMC & Compliance Journal, 2001-2002, from the 'Publications & Downloads' at http://www.cherryclough.com

[51] Assessing an EM Environment, Technical Guidance Note 47 from the EMC Test Laboratories Association, http://www.emctla.co.uk/technical-guidance-notes.aspx

[52] IEC 61000-2-11, Classification of HEMP environments

[53] On-Site (in-situ) EMC Testing, Technical Guidance Note 49 from the EMC Test Laboratories Association, http://www.emctla.co.uk/technical-guidance-notes.aspx

[54] Guides on 17 different EM phenomena and their EMC tests (including how to extend them to provide better 'coverage' of real-life EM disturbances), Keith Armstrong, REO (UK) Ltd., all free from http://www.reo.co.uk/knowledgebase

[55] W. Grommes and K. Armstrong, "Developing Immunity Testing to Cover Intermodulation", IEEE 2011 Int'l EMC Symp. Long Beach, CA, August 15-19, ISBN: 978-1-45770810-7

[56] K. Armstrong, "Testing for immunity to simultaneous disturbances and similar issues for risk managing EMC", IEEE 2012 Int'l EMC Symp. Pittsburgh, PA, USA, August 5-10 2012, ISBN: 978-1-4673-2059-7.

[57] IEC 61000-4-2, immunity to personnel electrostatic discharge (ESD)

[58] IEC 61000-4-3, immunity to continuous radio-frequency radiation using an anechoic chamber

[59] IEC 61000-4-4, immunity to electrical fast transients and bursts (EFT/B)

[60] IEC 61000-4-5, immunity to surges

[61] IEC 61000-4-6, immunity to continuous conducted radio-frequency currents

[62] IEC 61000-4-8, immunity to power-frequency magnetic fields

[63] IEC 61000-4-9, immunity to pulsed magnetic fields

[64] IEC 61000-4-10, immunity to damped oscillatory magnetic fields

[65] IEC 61000-4-11, immunity to voltage dips, dropouts, short interruptions and voltage variations

[66] IEC 61000-4-12, immunity to ring wave surges

[67] IEC 61000-4-13, immunity to distorted AC supply waveforms up to 2kHz

[68] IEC 61000-4-14, immunity to AC supply voltage fluctuations

[69] IEC 61000-4-16, immunity to conducted common-mode disturbances DC-150kHz

[70] IEC 61000-4-17, immunity to voltage ripple on DC electrical power supplies

[71] IEC 61000-4-18, immunity to damped oscillatory surges

[72] IEC 61000-4-19 (draft), immunity to conducted differential mode disturbances 2-150kHz

[73] IEC 61000-4-20, immunity to continuous radio-frequency radiation using a TEM Cell

[74] IEC 61000-4-21, immunity to continuous RF radiation using a Reverberation Chamber

[75] IEC 61000-4-25, immunity to HEMP for equipment and systems

[76] IEC 61000-4-27, immunity to unbalance in three-phase AC power supplies

[77] IEC 61000-4-28, immunity to variations in AC power supply frequency

[78] IEC 61000-4-31, immunity to conducted broadband noise

[79] IEC 61000-4-34, immunity to supply voltage dips, dropouts and voltage variations for equipment consuming more than 16A per phase

[80] IEC 61000-4-36, immunity to Intentional EMI

[81] IEC 61000-4-XX (proposed), immunity to radiated fields in close proximity, 9kHz to 6GHz.
At the moment the closest to this standard is ISO 11452-9.2 "Road vehicles - Component test methods for electrical disturbances from narrowband radiated electromagnetic energy - Part 9: Portable transmitters".
This is based upon the Ford Motor Company's Test Method RI115 "RF Immunity to hand portable transmitters" in their EMC-CS-2009.1, "EMC Specification For Electrical/Electronic Components and Subsystems".
Many EMC test labs around the world are equipped for, and familiar with doing this test.

[82] C37.90.1-2002, IEEE Standard for Surge Withstand Capability (SWC) Tests for Relays and Relay Systems Associated with Electric Power Apparatus

[83] IEC/TR 61000-1-5, High power electromagnetic (HPEM) effects on civil systems

[84] IEC 61000-2-9, Description of HEMP environment - Radiated disturbance

[85] IEC 61000-2-10, Description of HEMP environment - Conducted disturbance

[86] IEC 61000-2-13, Highpower electromagnetic (HPEM) environments - Radiated and conducted

[87] IEC/TR 61000-4-32, Testing and measurement techniques - High-altitude electromagnetic pulse (HEMP) simulator compendium

[88] IEC 61000-4-33, Testing and measurement techniques - Measurement methods for high-power transient parameters

[89] IEC 61000-4-35, Testing and measurement techniques - HPEM simulator compendium

[90] IEC 61000-4-23, Test methods for protective devices for HEMP and other radiated disturbances

[91] IEC 61000-4-24, Test methods for protective devices for HEMP conducted disturbances

[92] IEC 61000-6-6, HEMP immunity for indoor equipment

[93] ITU-T K.78:2009, High altitude electromagnetic pulse immunity guide for telecommunication centres

[94] ITU-T Handbook, The Protection of Telecommunication Lines and Equipment Against Lightning Discharges, Chapters 1 to 5, http://www.itu.int/pub/T-HDB-EMC.3-1974-P1/en; Chapters 6 to 8, http://www.itu.int/pub/T-HDB-EMC.3-1978-P2/en; Chapters 9 and 10, http://www.itu.int/pub/T-HDB-EMC.3-1994-P3/ento

[95] IEC 62305, Protection against lightning; Part 1: General Principles, Part 2: Risk Management, Part 3: Physical damage to structures and life hazard, Part 4: Electrical and electronic systems within structures connected to telecommunications and signalling networks - Performance requirements and testing methods

[96] IEC 62561, Lightning protection system components (LPSC)

[97] RTCA DO-160, Environmental Conditions and Test Procedures for Airborne Equipment, Section 22: Lightning induced transient susceptibility, Section 23: Lightning direct effects

[98] IEC 61000-4-32, HEMP simulator compendium

10.5 Software design techniques and measures

[100] Software Engineering for Real Time Systems, J E Cooling, Pearson Education2003, ISBN 0201596202

[101] Dependability of Computer Systems, EWICS Technical Committee 7, Elsevier Applied Science1989 ISBN 1851663819

[102] Article on Defensive Programming, http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Defensive_programming.html

[103] Safety Critical Systems Handbook: A Straightforward Guide to Functional Safety, IEC 61508 (2010 Edition) and Related Standards, Including: Process IEC 61511, Machinery IEC 62061

[104] NASA Software Safety Guidebook - FMEA Info Centre

[105] National Conference on Nonlinear Systems & Dynamics, NCNSD-2003, N-Version programming method of Software Fault Tolerance: A Critical Review, Bharathi V, http://ncnsd.org/proceedings/proceeding03/html/pdf/173-176.pdf

[106] Formal Methods in Safety-Critical Standards, Jonathan Bowen, Oxford University Computing Laboratory, 11 Keble Road, Oxford OX1 3QD, UK. http://reference.kfupm.edu.sa/content/f/o/formal_methods_in_safety_critical_standa_100249.pdf

[107] Using Software Protocols to Mask CAN BUS Insecurities, B R Kirk, IEE Colloquium on the Electromagnetic Compatibility of Software, Thursday, Savoy Place, London, WC2R OBL, 12 November 1998, IEE document reference 98/471, available from the IET Library at Savoy Place, libdesk@theiet.org, or archives@theiet.org, telephone 020 7344 8407, fax: 020 7344 846.

[108] Profibus specification - Profisafe - Profile for Safety Technology, Version 1.30, June 2004, Profibus International

[109] IEC 61784-3 Ed.1 CDV, Digital data communications for measurement and control: Part 3: Profiles for functional safety communications in industrial networks (update!)

[110] Philip Koopman, 32-Bit Cyclic Redundancy Codes for Internet Applications, International Conference on Dependable Systems and Networks, 2002

[111] Cyclic redundancy check (CRC), http://en.wikipedia.org/wiki/Cyclic_redundancy_check
CRC is an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data. Blocks of data entering these systems get a short check value attached, based on the remainder of a polynomial division of their contents; on retrieval the calculation is repeated, and corrective action can be taken against presumed data corruption if the check values do not match.
CRCs are so called because the check (data verification) value is a redundancy (it expands the message without adding information) and the algorithm is based on cyclic codes. CRCs are popular because they are simple to implement in binary hardware, easy to analyse mathematically, and particularly good at detecting common errors caused by noise in transmission channels. Because the check value has a fixed length, the function that generates it is occasionally used as a hash function.
The CRC was invented by W. Wesley Peterson in 1961; the 32-bit polynomial used in the CRC function of Ethernet and many other standards is the work of several researchers and was published during 1975.

[112] Error Correction: http://www.wikipedia.org/wiki/Error_correction

[113] The avionics standard based on the concept of partitioning the processor time, memory ranges and I/O access: http://en.wikipedia.org/wiki/ARINC_653.

[114] An operating system that supports partitioning: http://www.ghs.com/products/safety_critical/arinc653.html

[115] Another operating system that supports partitioning: http://www.windriver.com/products/platforms/safety_critical_arinc_653/

[116] A paper describing the concepts of partitioning operating systems: http://air.di.fc.ul.pt/air-ii/downloads/27th-DASC-Paper.pdf

[117] Reliable/redundant array of independent/inexpensive nodes (RAIN): http://en.wikipedia.org/wiki/Reliable_array_of_independent_nodes
RAIN is an architectural approach to computing and network-attached computer storage (or NAS), that combines commodity or low-cost computing hardware with management software to address the reliability and availability shortcomings of non-redundant NAS systems.

[118] IEC 61503-3, Annex F

[119] IEC 61508-2 Ed.2:2010, Functional safety of electrical/electronic/programmable electronic safety related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety related systems, IEC Basic Safety Publication (2010), http://webstore.iec.ch

11 Some functional safety standards related to IEC 61508

IEC 61511	Safety Instrumented Systems for the Process Industry Sector (in USA: ANSI/ISA S84)
IEC 62061	Safety of Machinery
IEC 62278 / EN 50126	Railways - Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) 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
SO 26262	Automobile Functional Safety
IEC 62304	Medical Device Software
IEC/EN 50402	Fixed Gas Detection Systems
DEF STAN 00-56	Accident Consequence (UK military)

12 Comparisons with IEC 61508-7

This table shows the relationship between the Techniques and Measures listed above with those in [1]. Additional Techniques or measures are indicated by an X in the tight-hand column.

Section number in this guide	Equivalent in Annex A	Equivalent in Annex B	Equivalent in Annex C	No equivalent in IEC 61508-7
4.1		B.1		
4.1.1		B.1.1		
4.1.2		B.1.2		
5.1		B.2		
6.1		B.1.3		
6.2		B.3		
6.3		B.1.4		
6.4			C.3.4, C.3.5	
6.5			C.2	
6.6		B.5		
6.7			C.6	
6.8			C.7	
6.8.1			C.7.1	
6.8.2			C.7.2	
6.8.3			C.7.3	
6.9			C.8	
6.10			C.9	
6.10.1			C.9.1	
6.10.2			C.9.2	
6.11			C.10	
6-12				X
7.1		B.4.1		
7.2		B.4.3		
7.3		B.4.4		
7.4		B.4.6		
7.5		B.4.8		
8.1.1				X
8.1.2				X
8.1.3	A.11			
8.1.4				X
8.1.5			C.3	
8.1.5.1			C.3.1	
8.1.5.2			C.3.2	
8.1.6			C.4	
8.1.7			C.5	
8.2.1	A.4			
8.2.1.1	A.4.3, A.4.4 and A.7.6			
8.2.1.2	A.4.5			
8.2.1.3				X
8.2.2	A.7.3		C.3.4	
8.2.3	A.7.5			
8.2.4	A.5			
8.2.4.1	A.5.1			
8.2.4.2	A.5.2			
8.2.4.3	A.5.3			
8.2.4.4	A.5.4			
8.2.4.5	A.5.5, A.7.1			
8.2.4.6	A.5.7			
8.2.5	A.4.1, A.5.6 and A.6.2			
8.2.6	A.3			
8.2.6.1	A.3.1			
8.2.6.2	A.3.2			
8.2.6.3	A.3.3			
8.2.6.4	A.3.4			
8.2.6.5	A.3.5			
8.2.6.5	A.3.5			
8.2.7	A.1			

Section number in this guide	Equivalent in Annex A	Equivalent in Annex B	Equivalent in Annex C	No equivalent in IEC 61508-7
8.2.7.1	A.1.1, 2, 3 and 4			
8.2.7.2	A.1.5			
8.2.8	A.2			
8.2.8.1	A.2.1			
8.2.8.2	A.2.2			
8.2.8.3	A.2.3			
8.2.8.4	A.2.5			
8.2.8.5	A.2.6			
8.2.8.6	A.2.7			
8.2.8.7			C.3.3	
8.2.9	A.9			
8.2.9.1	A.9.1			
8.2.9.2	A.9.2			
8.2.9.3	A.9.3			
8.2.9.4	A.9.4			
8.2.10	A.6.3, A.6.4, and A.11.4			
8.3.1	A.6.1 and A.7.4			
8.3.2.1	A.8			
8.3.2.2				X
8.3.2.3				X
8.3.3	A.10			
8.3.4	A.2.8			
9.1		B.6		
9.2				X

Guidance

The Institution of Engineering and Technology

The use of use of ever-more sophisticated electronic technologies (including wireless, computer and power conversion technologies) is now commonplace, and increasing in every sphere of human activity, including those where errors or malfunctions in the technology can have implications for functional safety. Activities affected include, but are not limited to:

- Commerce
- Industry
- Banking
- Defence
- Medicine & healthcare
- Government
- Security
- Energy & energy efficiency
- Entertainment & leisure
- Agriculture
- Transport (vehicles and infrastructure for road, rail, marine, air, etc.)

All electronic technologies are vulnerable to errors or malfunctions caused by electromagnetic interference (EMI), and increasingly sophisticated technologies tend to be more susceptible. As well as natural sources of EMI, such as lightning, all electrical and electronic technologies are sources of EMI, and as electronic technologies become more sophisticated they tend to emit EMI at higher levels and/or higher frequencies.

The consequence of all this, is that without appropriate electromagnetic compatibility (EMC) engineering (the discipline concerned with controlling EMI) there will be uncontrolled consequences for people in general, and uncontrolled financial risks for manufacturers and service providers who employ electronic technologies.