



Another EMC resource
from EMC Standards

Electromagnetic Compatibility for Functional Safety

Helping you solve your EMC problems



Electromagnetic Compatibility for Functional **Safety**



Guidance by the Institution of Engineering and
Technology Working Group on EMC for Functional Safety

IET 2008 Guide on EMC for Functional Safety

Contents	Page
0. Step 0: Introduction, management and planning	7
0.1 Overview	7
0.2 What this process applies to.....	8
0.2.1 'Electrotechnology for Functional Safety' (EFS).....	8
0.2.2 'Creator'	8
0.3 Why a process is needed for EMC for Functional Safety.....	8
0.4 Creators and safety assessors: learning curves and opportunities.....	10
0.5 IEC 61508 and IEC/TS 61000-1-2	10
0.6 Complexity, and how it affects safety engineering	10
0.7 Shortcomings in conventional EMI immunity tests	12
0.7.1 Faults and misuse are not addressed	12
0.7.2 Real EM environments not tested	12
0.7.3 EMI 'risk assessment' not done	13
0.7.4 Physical environment not considered	13
0.7.5 Only a representative sample is tested	13
0.7.6 Emergent behaviour	13
0.7.7 Shortcomings in the 'performance criteria'	14
0.8 This process applies to the whole 'lifecycle'	14
0.9 Graphical overviews of the EMC for Functional Safety Process.....	15
0.10 The management, planning and documentation of the process	18
0.10.1 Management issues.....	18
0.10.2 Planning issues.....	19
0.10.3 Estimate the 'anticipated lifecycle' of the EFS	20
0.10.4 Appropriate effort	21
0.10.5 Documentation.....	21
0.11 Design techniques for EMC for Functional Safety.....	22
0.12 Verification and validation techniques for EMC for Functional Safety.....	22
0.13 Operation, maintenance, repair, refurbishment, upgrade and modification	23
0.14 Iterations caused by later stages in the project.....	23
0.15 Overall conclusions on the above.....	23
0.16 List of contributors to this Guide	24
1. Step 1: Determine Intersystem EM and Physical Phenomena	25
1.1 Introduction: Step 1 in the EMC for Functional Safety Process	25
1.2 Assessing locations, routes and paths	26
1.3 Assessing the EM environment over the anticipated lifecycle	27
1.3.1 How to do an EM assessment	27
1.3.2 A check list of initial questions	27
1.3.3 Consideration of future technology trends, and future changes in the environment	28

1.3.4	Mobile and portable EFS	28
1.3.5	What EM issues should be taken into account?	28
1.3.6	Comparing the EM threats with the electronic technologies employed by the EFS	33
1.3.7	In-depth investigation of aspects of the environment	33
1.3.8	Taking uncertainties into account	35
1.3.9	Writing a quantified EM environment specification for the lifecycle.....	35
1.4	Assessing the physical environment over the anticipated lifecycle.....	35
1.4.1	How to do a physical assessment.....	35
1.4.2	What physical issues should be considered?	36
1.4.3	Taking uncertainties into account	37
1.4.4	Writing a quantified physical environment specification for the lifecycle	37
1.5	Also determine effects of emissions on other EFS.....	38
1.6	Iterations	38
1.7	Overview of types of EM phenomena	38
1.8	Some foreseeable future technology trends.....	39
1.8.1	Developments in Integrated Circuits (ICs)	39
1.8.2	Developments in power semiconductors	39
1.8.3	Increased use of wireless communications, for voice and data	39
1.8.4	Developments in hard disc drive technology.....	41
1.8.5	Systems are becoming more distributed.....	41
1.9	Some tools for assessing the EM environment.....	41
1.9.1	Examples of field strengths vs distances for various RF transmitters	41
1.9.2	Estimating the low frequency radiated fields emitted by long conductors	42
1.9.3	Estimating how radiated fields vary with distance.....	44
1.9.4	A list of the current standards in the IEC 61000-2-x series	46
2.	Step 2: Determine Intrasystem EM and Physical Phenomena	48
2.1	Introduction	48
2.2	Choosing the locations, routes and paths	48
2.3	Assessing the EM environment over the anticipated lifecycle	49
2.4	Assessing the physical environment over the anticipated lifecycle.....	50
2.5	Iterations	50
3.	Step 3: Specify EM/physical phenomena vs functional performance	53
3.1	Introduction	53
3.2	EMC Safety Requirements	53
3.3	Accounting for uncertainties	54
3.4	Two types of risk assessment are required	54
3.5	Hazard analysis and risk assessments are 'live' documents	55
3.6	Emissions specifications are also needed.....	55
3.7	Some hazard analysis and risk assessment methods	56
3.7.1	Some standardised methods	56
3.7.2	Some well-established but non-standardised methods.....	57
3.8	Iterations	59
4.	Step 4: Study and design the EFS	60

4.1	Introduction	60
4.1.1	General principles	60
4.1.2	How this Step fits into the process	61
4.2	Designing to achieve the EMC safety requirements	61
4.2.1	Appropriate methods of Risk Assessment	61
4.2.2	Common but incorrect assumptions in Risk Assessment	62
4.2.3	How to include EMI and intermittencies in the Risk Assessment	63
4.2.4	Iterations	64
4.3	Some design and development measures and techniques to be considered	65
4.3.1	Designing EFS architecture	65
4.3.2	Avoiding unsuitable components; and mechanical, hardware and software design techniques	65
4.3.3	Choosing suitable components, and mechanical, hardware and software techniques	65
4.3.4	'Hardening' communications	66
4.3.5	Using optical links instead of conductors	67
4.3.6	Using wireless links instead of conductors	67
4.3.7	Analysis and testing techniques that guide design	68
4.3.8	Determining the 'natural' susceptibilities of hardware, software and firmware	69
4.3.9	Design techniques for bonding, wiring, cabling and PCBs	69
4.3.10	Using computer-aided design tools to optimise EM performance	70
4.3.11	EM mitigation techniques	70
4.3.12	Physical mitigation techniques	72
4.3.13	'Layering' or 'nesting' EM/physical mitigation	73
4.3.14	Fault mitigation	75
4.3.15	Mitigation of problems caused by foreseeable use (misuse)	76
4.3.16	Don't rely on the user	76
4.3.17	Using checklists based upon case studies and experience obtained in similar applications	77
4.3.18	Taking the power distribution system into account	77
4.3.19	EMI mitigation for multiple redundant channels	77
4.3.20	Techniques for sensing the EM/physical environment	78
4.3.21	Issues with fail-safe methods	78
4.3.22	'Hardening' integrated circuits (ICs)	79
4.3.23	'Hardening' digital and analogue circuits and PCBs	79
4.3.24	'Hardening' software and firmware	79
4.3.25	Systems, installations and power quality	79
4.4	Realisation measures and techniques to be considered	80
4.4.1	Procure materials, components and products according to their EM/physical specification	80
4.4.2	Take all necessary actions to avoid counterfeits	80
4.4.3	Assemble according to the design	81
4.4.4	Control of suppliers and subcontractors, their suppliers and subcontractors, etc.	81
4.5	Installation and commissioning measures and techniques	82
4.5.1	Any constraints on the physical positioning of the items of equipment that comprise the EFS ..	83
4.5.2	Constraints on cabling	83
4.5.3	The methods of terminating any cable shields (screens)	83
4.5.4	Constraints on connectors and glands, and their assembly	83
4.5.5	The electrical power supply requirements (power quality)	84
4.5.6	Any additional shielding (screening) required	84
4.5.7	Any additional filtering required	84
4.5.8	Any additional overvoltage and/or overcurrent protection required	84
4.5.9	Any additional power conditioning required	85
4.5.10	Any additional electrostatic discharge protection requirements	85
4.5.11	Any additional physical protection required	85

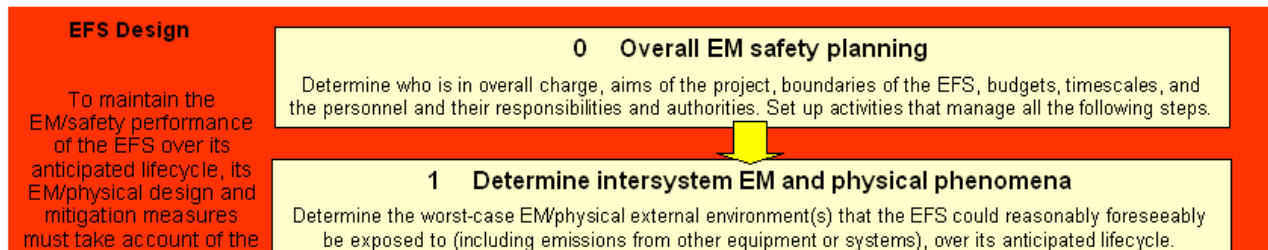
4.5.12	Any RF Reference requirements	85
4.5.13	Protection against corrosion	86
4.5.14	The procedures, materials and expertise to be used	86
4.6	Operation, maintenance, repair, refurbishment, etc.	87
4.6.1	Comprehensive Instructions	87
4.6.2	Maintenance, repair, refurbishment procedures and planning of mitigation measures	88
4.6.3	Maintain EM/physical characteristics despite repairs, refurbishment, etc.	88
4.6.4	Constraints on the EM/physical environments	89
4.6.5	Disassembly/reassembly techniques to preserve EM characteristics	89
4.6.6	Periodic testing (proof testing) of critical components	89
4.6.7	Periodic replacement of critical components	90
4.6.8	Verification of the absence of corrosion	90
4.7	Modifications and upgrades to hardware and software	90
4.7.1	Assessing the effect of proposed modifications and upgrades	91
4.7.2	Maintaining acceptable EM and physical characteristics	91
4.8	The relationship between the EFS, its constituent parts, and mitigation measures	91
5.	Step 5: Create EM and physical verification/ validation plans	94
5.1	Introduction	94
5.2	Planning for Verification, and for Validation	95
5.2.1	Planning the verification activities throughout a project	95
5.2.2	Planning the validation of the EFS	95
5.2.3	Iterations	95
5.3	Some examples of suitable techniques	96
5.4	EM immunity test methods for functional safety	97
5.5	Testing for physical environment, wear, ageing and lifecycle	98
5.6	Testing radiated EM immunity in reverberation chambers	99
5.7	Testing transients, surges, ESD	100
5.8	Test levels and uncertainty	100
5.9	Testing simultaneous phenomena	102
5.10	Testing emissions	102
5.11	Testing faults and misuse	103
5.12	Testing safe shutdowns, alarms and the like	103
5.13	Verification during operation	103
5.14	Conclusions	103
6.	Step 6: Selecting standard products and/or specifying custom hardware or software items	104
6.1	Overview	104
6.2	'Simple' and 'Complex' EFSs	105
6.2.1	What is the difference?	105
6.2.2	Simple EFS	105
6.2.3	Complex EFS with one level of subcontracting	106
6.2.4	Complex EFS with two or more levels of subcontracting	106
6.2.5	Simple EFS that is complicated in practice	106
6.3	The Step 6 activities for a Simple EFS	107

6.3.1	Overview.....	107
6.3.2	Iterating product specifications and mitigation	108
6.3.3	CE marking should not be taken as evidence of EM performance	108
6.3.4	Deficiencies in product EM/physical specifications	109
6.3.5	How to overcome the lack of useful product data	110
6.4	The Step 6 activities for a Complex EFS.....	111
6.4.1	Overview.....	112
6.4.2	Step 6a: Specify EM/physical phenomena vs functional performance for each custom-engineered item of hardware and/or software.....	112
6.4.3	Step 6b: Study and design each item of hardware and/or software.....	113
6.4.4	Step 6c: Create EM and physical verification/validation plans for each item of hardware and/or software	113
6.4.5	Step 6d: Select the commercially-available standard products to be used for each item	114
6.4.6	Step 6e: Assemble and check each item of hardware and/or software	115
6.4.7	Step 6f: Verify and finally validate each item of hardware and/or software	115
6.5	Iteration of all previous Steps	115
7.	Step 7: Assemble, install, commission and verify the EFS	118
7.1	Introduction	118
7.2	Verification during assembly, installation and commissioning	118
7.3	Following the EFS designers' instructions.....	118
7.4	Quality Control.....	119
7.5	Iterating the specifications (Steps 1, 2 and 3)	120
7.6	Iterating the design and verification (Steps 4 and 5).....	120
7.7	Realisation (assembly, installation, commissioning, verification, etc.) of EM/physical mitigation measures not incorporated in the EFS.....	124
7.8	QC Documentation	125
8.	Step 8: Validating the EFS	126
8.1	Introduction to Validation	126
8.2	Authority and responsibility.....	126
8.3	Remedial work.....	126
8.4	Iterating the earlier steps	127
8.5	Validating EM/physical mitigation measures that are not incorporated in the EFS.....	130
8.6	Documenting the validation	130
9.	Step 9: Maintain the EM and physical performance characteristics of the EFS over its lifecycle.....	131
9.1	Introduction	131
9.2	The activities required during operation, maintenance, repair, refurbishment, etc.	131
9.3	The activities required when modified or upgraded	132
9.4	The activities required during dismantling and disposal.....	132
9.5	Documentation	133
10.	References	134

11.	Annex A: Glossary of terms and abbreviations.....	139
12.	Annex B: Overview of electromagnetic phenomena, and how they can interfere	148
12.1	Overview of EM phenomena	148
12.2	The “Source – Victim/receptor Model”	153
12.3	Overview of how EMI can occur	154
12.3.1	Interference with analogue devices and circuits	154
12.3.2	Interference with digital devices, circuits and software	155
12.3.3	Interference with power semiconductors	155
12.3.4	Interference with signals	155
12.3.5	Interference with electromechanical devices	155
13.	Checklists.....	157
13.0	Checklist for Step 0: Management and planning.....	158
13.1	Checklist for Step 1: Determining Intersystem EM and Physical Phenomena.....	160
13.2	Checklist for Step 2: Determining Intrasystem EM and Physical Phenomena.....	161
13.3	Checklist for Step 3: Specify electromagnetic and physical phenomena vs the functional performance required to achieve the desired levels of safety risks or risk-reductions.....	162
13.4	Checklist for Step 4: The study and design of the EFS.....	163
13.5	Checklist for Step 5: Creation of EM and physical verification/validation plans.....	168
13.6	Checklist for Step 6: Selection of standard products and/or specifying custom hardware or software items.....	169
13.7	Checklist for Step 7: Realisation of the EFS (assembly, system integration, installation, commissioning, etc.) and the verification that occurs throughout this process	171
13.8	Checklist for Step 8: Validating the EFS	172
13.9	Checklist for Step 9: Maintaining the EM and physical performance characteristics of the EFS over its lifecycle	173

0. Step 0: Introduction, management and planning

*Determine who is in overall charge, aims of the project, boundaries of the EFS, budgets, timescales, and the personnel and their responsibilities and authorities.
Set up activities that manage all the following steps.*



0.1 Overview

The 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.

Where errors or malfunctions in electronics technologies could have implications for functional safety, appropriate EMC engineering is required to control safety risks, and to control the associated financial risks for manufacturers and service providers. Unfortunately, over past decades the disciplines of functional safety engineering, and EMC engineering, have developed separately, partly because it was mandated by certain international standards committees, but also for other reasons not discussed here [6].

In general, safety engineers do not have a detailed knowledge of EMC, and EMC engineers do not have a detailed knowledge of functional safety.

Also, at the time of writing in 2008, there are no published EMC standards that are appropriate for achieving functional safety, and there are no safety standards that include appropriate EMC requirements for functional safety (mostly, they have no EMC requirements at all).

The above was discussed in the 2000 IET Guide on this subject [3], and the aim of this 2008 IET Guide is to provide management and technical tools that enable the use of electronic technologies in applications where they could have an impact on functional safety – controlling the risks due to EMI for customers and third-parties, and thereby reducing financial risks to manufacturers and service providers.

Financial risks mostly arise due to product liability legislation, but also due to safety regulations that can cause unsafe products to be banned from large markets such as the European Union (EU) and/or undergo recall. Many companies are aware that legal claims that go against them could be very costly indeed, and could also ruin their brand reputation. For this reason, they have for decades employed legal experts to either win cases for them, or settle out of court with binding non-disclosure agreements. In this way the true cost of poor engineering has generally been hidden from the public, governments, and other companies.

It might be argued that the above process will also cope with inadequate EMC in the future, but the rapid growth in the use of increasingly-sophisticated electronic technologies means that at some point the costs of doing EMC engineering adequately will be less than the legal costs resulting from continuing not to do it.

That point may already have been reached, because of the general financial improvements that are available from EMC engineering. As [22] shows, appropriate EMC engineering techniques have for some time been available to help reduce the costs and timescales in design and development, reduce unit manufacturing and warranty costs, whilst also helping to maximise market share.

This Guide is based upon the principles of the current draft of the 2nd Edition of IEC TS 61000-1-2 [4], applying modern functional safety engineering techniques to the control of EMI.

Although the subject of this Guide is how to do practical EMC engineering for functional safety reasons, the methods described can be used to reduce risks in high-reliability, mission-critical and legal metrology applications, as well as generally improving financial performance and market share. This Guide will also help military suppliers comply with Annex H of Def Stan 59-411 Part 1 [91].

The term 'EMI' is often used colloquially: to denote electromagnetic (EM) phenomena, EM disturbances, or the degradation of functional performance caused by an EM disturbance. Since this document is intended to be read by people who may not be skilled in EMC, this is how 'EMI' is used throughout this document. EMC experts will be able to understand what is actually meant by the context.

0.2 What this process applies to

0.2.1 'Electrotechnology for Functional Safety' (EFS)

The EMC for Functional Safety process described in this IET Guide can be applied to any electrical, electronic or programmable electronic entity that provides a function having a direct impact on safety.

To avoid confusion with the many different terms used in electrical and electronic engineering (for example: device, apparatus, system, safety system, installation, etc.) a new acronym: 'EFS' has been created for this Guide.

EFS is defined as: "Any entity employing electrical and/or electronic technologies that provides one or more functions having a direct impact on safety" – with the intention of covering the entire range of constructional possibilities.

Note that an EFS is not a component, part, element, subsystem or subset of the entity that is providing the function having a direct impact on safety.

The designer, creator, purchaser, operator, maintainer, etc., of the EFS is responsible for ensuring that all of the components (etc.) that go to construct it have appropriate performance taking into account the characteristics of the EFS (see Complexity in 0.6). This may mean specifying custom-engineered units, and/or modifying standard products, and/or applying EM or physical mitigation measures to devices, products, systems or installations.

Only the designer of the EFS has the necessary knowledge of the application, and the overall control of the design, to competently ensure the achievement of the desired levels of safety risks (or risk-reductions).

0.2.2 'Creator'

The definition of 'creator' as employed in this document includes the role undertaken by: manufacturer, system integrator, installer, supplier, etc. – for example, the entity (or entities) who fulfils the 'realisation' stage in the 61508 lifecycle (see 0.5). Basically, this means the organisation that hands the finished EFS over to its end user.

0.3 Why a process is needed for EMC for Functional Safety

Electronic and programmable electronic devices are increasingly being used in applications where reliable functionality is necessary to achieve sufficiently low functional safety risks. The main reason for this is their increasing functionality and decreasing cost, both achieved through continual shrinking of the silicon dies used to make integrated circuits (ICs). This increasing use of modern electronic technologies is causing higher levels of electromagnetic interference (EMI) in the environment.

All electronic devices have always suffered from inaccuracy or malfunction, even permanent damage, due to EMI in their operational environments. Silicon die shrinking – and its consequent lower operating voltages – reduces the immunity of ICs to EMI. The result of worsening EMI and reducing immunity is decreasing functional reliability, with potentially serious consequences for functional safety.

EMI is controlled in the EU by the electromagnetic compatibility (EMC) Directive (89/336/EEC replaced by 2004/108/EC [31] on 20th July 2007) – which specifically does not address any safety matters. Safety Directives generally deal with EMI issues very poorly, if at all [1] [2]. As a consequence, the effects of EMI on functional safety risks are largely unconsidered at present, as shown by Figure 0.1.

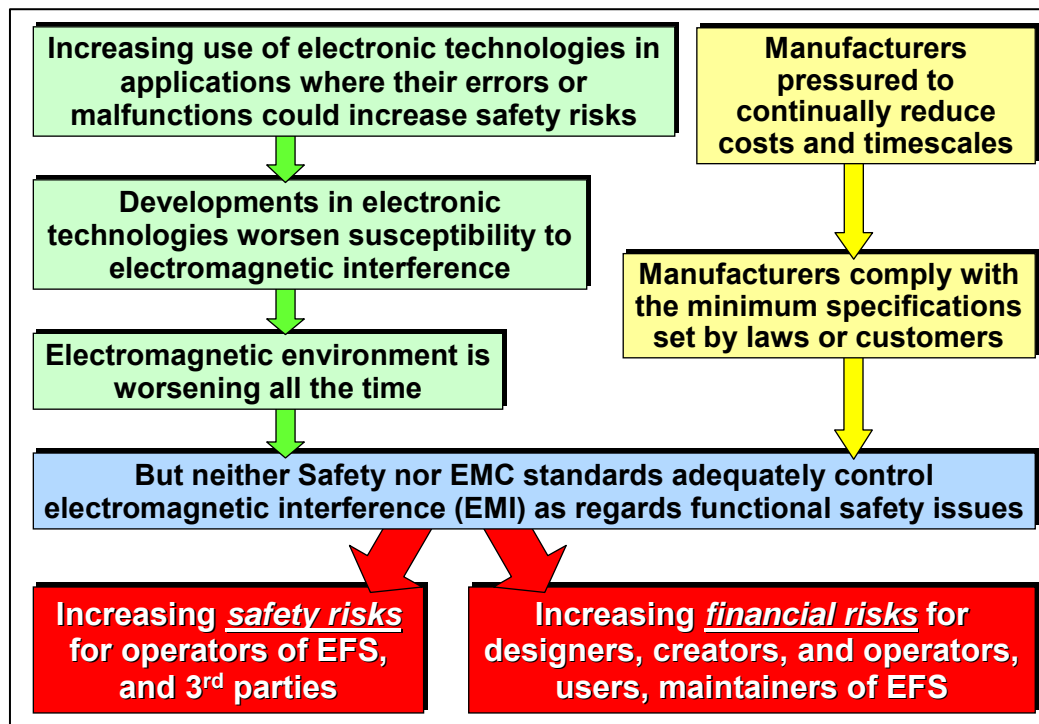


FIGURE 0.1 Increasing risks due to EMI

The IEE published a guide in 2000 [3] recommending an ‘EMI hazards analysis and risk assessment’ approach, and since then has run a number of successful training courses on this issue. Only IEC 61000-1-2 [4] employs a similar approach, but it is just a ‘Technical Specification’ and not (yet) a full IEC standard.

A very few IEC safety standards (and the EU’s Automotive EMC Directives) include EMI immunity requirements, but these rely solely on conventional EMI immunity testing, shown below to be incapable of demonstrating that risks are low enough. The EMC standard for medical device safety has recently been amended [5] to state that it is not a safety standard. EMC standards and regulations have developed over decades in a way that is considered by some to be unequal to modern requirements [6] and is demonstrably unsuitable for safety engineering purposes (see 0.10.7).

The safety of electrical/electronic equipment is generally verified by:

- Inspecting the design against a number of safety design criteria, well-proven to provide a sufficient level of lifecycle protection, including the effects of the physical environment and foreseeable use/misuse
- Testing samples of the finished design using worst-case combinations of physical environment phenomena, and by simulating each foreseeable fault in turn
- Safety testing of every item manufactured
- Regular safety inspections and tests during the period of use

But conventional immunity testing methods ignore design, and simply test one or two new samples in a benign physical environment. This is quite different from the approach taken for all other safety issues, including software (Part 3 of [7]), and is inadequate for a number of reasons, which are described in section 0.7.

What is needed instead, the basis for this Guide to a process for controlling EMI for reasons of functional safety, is discussed in sections 0.8 through 0.15.

But before we can discuss shortcomings and solutions, there are some basic issues to address first, in sections 0.4 through 0.7, and graphical overviews of the process described by this Guide in section 0.9.

0.4 Creators and safety assessors: learning curves and opportunities

It is recognised that adopting the approach to EFS risk assessment, design, verification and validation described in this Guide will create a significant learning curve for many (if not all) EFS creators. But the alternative is a future of unacceptable levels of deaths and injuries, and unacceptable financial risks and losses by both creators and their customers and users, as described in section 0.1.

So the process described by this Guide should be clearly seen for what it really is – a methodology for improving cost-effectiveness and reducing financial risks over the medium and longer term. In fact it is much more than that, it is also a methodology for ensuring customer and investor confidence, and for government bodies and other non-profit organisations it provides similar benefits in the political sphere.

Owners, directors and senior managers might also regard it as a method for reducing their personal liability under the UK's Corporate Manslaughter Act, or similar legislation in other jurisdictions, that aims to ensure that one or more senior responsible individuals are personally held accountable when their company's actions, or inactions, are proven to have caused safety accidents, regardless of the complexity of the organisation.

In addition, functional safety assessors (e.g. those already qualified to assess to IEC 61508 [7] or its 'daughter' standards such as IEC 61511 or IEC 62061) will generally need to develop the necessary skills to assess EMC for Functional Safety engineering practices and their verification and validation.

Perhaps some EMC testing laboratories will also develop the necessary skills to assess the EMC for Functional Safety of an EFS design. Some of them will certainly want to expand their markets by offering customised EMC tests for EFS, and maybe offer assistance in developing individual EMC for Functional Safety test plans.

0.5 IEC 61508 and IEC/TS 61000-1-2

IEC 61508 [7] covers the "Functional safety of electrical, electronic and programmable electronic safety-related systems" and is used by the HSE (Health and Safety Executive, UK) as an example of good engineering practice for complex EFS. It has also been adopted as an EN standard (EN 61508) but is not 'notified' or listed under any EU Directives.

There are some sector-specific standards that have been developed from IEC 61508, for example IEC 61511 [23] and IEC 62061 [24].

IEC 61508 is a large document with seven parts, and has specific requirements for software and firmware in its Part 3. However, it has no specific requirements for how to deal with EMI. The requirements in 61508 Part 3 are the result of decades of work by hundreds of experts in academia, institutions and industry – but although IEC 61508 requires EMI to be taken into account for functional safety reasons, no-one has yet applied the same levels of effort or thought to the issue of EMI as has been applied to software. This is despite the fact that EMI is arguably just as complex (if not more) than software, and can be just as serious an issue for safety.

IEC 61000-1-2 [4] is intended to become the IEC's 'basic standard' on EMC for Functional Safety, at the moment it is not a full IEC standard, but an IEC Technical Specification currently in its draft 2nd Edition. The EMC for Functional Safety Process described in this IET Guide is based upon the approach taken by the draft 2nd Edition of IEC/TS 61000-1-2, February 2008, and could be used as practical guidance by anyone wishing to comply with IEC/TS 61000-1-2.

0.6 Complexity, and how it affects safety engineering

There are many names used for various types of electrical and electronic equipment, including: device, module, subassembly, ESA (electronic subassembly) plug-in unit, line replacement unit, assembly,

apparatus, item, unit, product, equipment, COTS (commercial off the shelf equipment), MOTS (military off the shelf equipment), subsystem, system, installation (either fixed or mobile), etc., etc. – and they all mean different things to different people in different industries.

Any of the above can be important for safety purposes. IEC 61508 [7] has a requirement to identify ‘safety functions’. Many different components (discretes, boards, modules, products, systems, etc....) might have to work together to perform a safety function.

It is very important to realise that a safety function is *only ever a function that is performed by the EFS as a whole*.

None of the items (modules, products, etc....) incorporated *within* an EFS – that play a part in its achievement of its safety function(s) – can ever be described as providing a safety function in themselves.

The reason for this important distinction is the phenomenon of ‘emergence’, in which the characteristics of an entity can differ (and often do) from the characteristics of the entities that have been used to construct it – often in ways that are surprising and therefore very hard to predict. ‘Emergence’ is a general topic in philosophy and science, and it is very relevant in engineering wherever components items (modules, subassemblies, products, etc., etc....) are combined to create a more complex entity (equipment, system, installation, etc., etc....).

An EFS can therefore never be created ‘Lego™-brick’ fashion by simply combining together items (subassemblies, products, systems, etc....) that are claimed by their manufacturers to provide functions in a safe or reliable manner. For example, due to emergence it is possible for two very reliable items to become very unreliable when interconnected to operate as a system.

Example: Consider a system constructed by connecting a speed sensor to the appropriate input of a microprocessor to create a speed measurement system, part of a closed-loop speed control system. If the speed sensor is a simple analogue type it simply exposes a coil to the magnetic field from a magnet attached to a rotating shaft – and produces pulses of voltage at a certain rate depending on the speed of rotation. The input to the microprocessor has a comparator with a threshold that converts the analogue pulses into rectangular digital signals that the microprocessor can handle. The peak voltage from the analogue sensor depends upon the speed, and at low speeds can be very low – but the designer has set the comparator threshold so that, at any speed within the range to be controlled, the signal is digitised correctly.

EMI always occurs in real life, and adds noise to the sensor signal. At medium and high speeds the peak voltage from the sensor is so much higher than the threshold that (in this example) the noise has a negligible effect on the digitisation of the signal and hence upon the accuracy of the speed measurement and the safety risks of the speed control system. However, when the speed is very low, the peak sensor voltage is only a little higher than the threshold, and the same amount of EMI-induced noise can have a much larger effect on the accuracy of speed measurement, possibly with safety implications for the speed control system.

When the speed is lower than that which was intended to be controlled, the peak sensor voltage could be below the threshold entirely, but the added noise due to EMI could exceed the threshold and be digitised, resulting in gross errors in the measurement and hence in the speed control.

The unreliability of the overall speed control system could therefore be very high indeed at low speeds, in environments that had significant levels of EMI. This is something that could easily have been overlooked when the sensor and microprocessor were designed and tested individually. When each was individually tested with levels of EMI corresponding to their intended operating environment, following the usual EMC test standards, with (say) the simulated speed set to mid-range so as to be able to detect errors in either direction, each might prove to be perfectly immune.

Since each component of the system passes its own set of tests, when they are combined to create the speed control system many designers would simply check its functional performance in a normal laboratory environment. EMC tests would not be applied, because each component passed when tested on their own. But when operated in a real-life application with higher levels of EMI than in the laboratory, unreliability could be very high at the lower speeds and safety risks might arise as a result.

The reader of this Guide needs to be particularly alert to this very important issue, because very many system designers are simply ‘Lego™-brick’ system integrators who assume that if each component (subassembly, module, etc....) of their system meets its individual safety and EMC specifications, then whatever system (installation, etc....) they construct from these components will also be safe enough. *Nothing could be further from the truth.*

Appropriate competence [86] is required throughout the lifecycle for the EFS to achieve the desired levels of risk (or risk-reductions), taking into account all reasonably foreseeable interactions that result in emergent characteristics.

EMC for Functional Safety is just one aspect of the necessary knowledge and competencies required by personnel who are associated with EFS, which is why the IET produced its professional guide on this issue in 2000 and has now produced this additional professional guide.

0.7 Shortcomings in conventional EMI immunity tests

These descriptions are very brief; much more detail is available from the references and from the contributors to this Guide. This guide provides risk-based approaches for dealing with the issues below.

0.7.1 Faults and misuse are not addressed

An EFS must meet its requirements for safety, or risk reduction, taking into account reasonably foreseeable faults and misuse. These can significantly affect the interaction of the EFS with its 'everyday' EM environment. For example:

- Dry joints or short circuits (e.g. in a filter)
- Intermittent contacts in connectors
- Incorrect/out-of-tolerance electronic components
- Incorrect, loose or missing fixings associated with shielding or radio-frequency bonding
- Damaged or missing conductive gaskets
- Failure of a surge protection device
- Shielding doors or cover left open
- Installation using incorrect type of cable

Safety tests simulate foreseeable faults and misuse to check safety is maintained, but conventional EMC tests do not. This is sufficient in itself to show that conventional EMC testing is inadequate for functional safety purposes.

0.7.2 Real EM environments not tested

Standardised immunity tests appear to be primarily designed to be repeatable and use affordable test instrumentation, rather than simulate real-life EM environments. For example: real-life environments include simultaneous EMI threats – such as: radiated fields from two or more radio channels; a radiated field plus a fast transient burst on the mains supply or an electrostatic discharge to a keyboard; etc., but conventional tests only apply one EMI threat at a time. [8] shows that units that pass conventional immunity tests can readily fail when tested with simultaneous threats, even at lower levels.

The immunity of electrical, electromechanical, electronic or programmable electronic technologies depends strongly on the waveshapes of transient threats (surges, spikes, etc.), but the waveforms used in conventional transient/surge tests are greatly simplified versions of waveshapes that represent only a very tiny fraction of all the possible waveshapes.

Modulating an interfering signal at the rate of an electronic process associated with a circuit can significantly reduce its immunity [9] [10]. EM environments include a huge range of modulation frequencies, and types of modulation but conventional immunity tests simply modulate with a 1kHz sinewave (plus 0.5Hz pulse modulation for some medical devices).

Example: Analogue cellphone systems were widespread in the late 1980's, but in the 1990's they were replaced by digital cellphone 'GSM' systems. The digital cellphones operated at the same carrier frequencies (around 900MHz) as the analogue systems, and the handsets had the same (or less) transmitter power. But whereas analogue cellphones generally did not interfere with hearing aids, as soon as GSM was rolled-out, complaints of very loud interference from hearing aid users began to be made. The only real difference, and what caused the interference, was the change to digital modulation of the radio frequency (RF) carrier.

Since then both the IEC and FCC have published immunity standards for hearing aids, intended to make it possible for a hearing aid wearer to be able to use their aid when a GSM cellphone is in use

at least 2 metres away. What someone with hearing difficulties is supposed to do if they want to use a cellphone, 18 years after GSM was rolled out and significant hearing aid problems surfaced, is not yet addressed by the relevant authorities.

The anechoic chambers used for conventional radiated immunity tests are unlike most real-life EM environments, and there are concerns about the uncertainty in the test method itself [11] [12]. Other failures to cover the typical modern EM environment could be listed.

0.7.3 EMI ‘risk assessment’ not done

Conventional immunity tests do not address low-probability EMI threats, even though they could be significant where safety integrity levels (SILs, see [7]) are high [14]. For example, they do not cover the much higher field strengths and/or frequencies caused by the close proximity of cellphones, despite this being a reasonably foreseeable occurrence. Also, they only apply surges of up to $\pm 2\text{kV}$ to mains power inputs, even though it is known that $\pm 6\text{kV}$, or more, generally occurs several times each year in Europe [13].

For the types of EMI threats that are covered, by the conventional tests, the levels are generally based upon the two-sigma point (sigma being the standard deviation) – meaning that 95% of the events should fall below the tested level. But it might be unacceptable for a given EFS to become unsafe once in every 20 EMI events – especially where very low levels of safety risk, or high levels of risk-reduction, are required.

0.7.4 Physical environment not considered

Safety is required over the whole lifecycle, but conventional immunity tests never address the effects of the physical environment [15]. Extremes of temperature, supply voltage, shock, vibration, loading, condensation, icing, physical forces, etc. can reduce EMI immunity by degrading filtering, shielding and other EMI suppression measures. For example, [16] reports on tests on an EMI filter that showed that under reasonably foreseeable real-life conditions of ambient temperature and load current, its suppression could degrade by 20dB (i.e. to one-tenth) of that measured during conventional EMI immunity tests.

Ageing also degrades EMI immunity, and can be caused by condensation, liquid spills and spray, mould growth, sand, dust, cleaning (e.g. wire-brushing, solvents) and maintenance – plus wear and tear caused by multiple operations of controls, opening and closing of doors and access panels, temperature cycling, etc. For example, a common ageing problem is corrosion at metal joints, which degrades EMI filtering and shielding [17].

0.7.5 Only a representative sample is tested

Even if a particular product design had once passed its EMC tests, in isolation this proves nothing at all about the EMC performance of the unit actually supplied to the customer.

Where manufacturers’ QC systems do not check or control EMC characteristics in serial manufacture, the EMC characteristics of their products can vary unpredictably, due to the sensitivity of electronic and programmable electronic technologies to variations in devices (e.g. semiconductor ‘die-shrinks’ applied to discrete transistors and ICs) and to supposedly ‘small’ changes in manufacture (e.g. altered cable routes; modified fixing methods; software ‘bug fixes’; substitute components; changes in painting or plating methods, etc.).

0.7.6 Emergent behaviour

It can be difficult to test the EMI immunity of some EFS, so immunity tests on individual items or sub-assemblies are often considered adequate instead. The following example shows that this can increase safety risks.

Example: Conventional immunity testing permits a DC power supply unit to exhibit any amount of momentary degradation during transient tests, as long as it self-recovers afterwards. In some cases DC outputs collapse to 0V during the transient, but this is considered acceptable behaviour. But where a DC power supply powers a safety-related microprocessor, such a collapse could cause the microprocessor to crash, (hopefully) followed by a reboot. During this upset – and maybe afterwards too – functional safety will be compromised.

Many other simple examples could be given, and more complex interactions are possible. So even where all of the components incorporated into an EFS passed immunity tests that really did simulate their worst-case

real-life EM environments, it does not mean that the EFS constructed using them would also be immune enough [14].

0.7.7 Shortcomings in the ‘performance criteria’

The IEC/EN product and generic immunity standards applied under the EMC Directive specify the performance criteria to be achieved during and/or after the tests. The basic immunity tests in the IEC 61000-4 series that they call up are acknowledged at the highest levels in the IEC and CENELEC to represent economic/technical compromises that the committees who created them thought appropriate. However, it is also acknowledged that safety was not considered in the economic assessment, and the result is that the technical compromises that were made may not be appropriate where EMI could result in increased functional safety risks.

The product and generic immunity standards use the following performance criteria, listed as A to D:

- A** Normal performance within limits specified by the manufacturer, requestor or purchaser;
- B** Temporary loss of function or degradation of performance which ceases after the disturbance ceases, and from which the equipment under test recovers its normal performance, without operator intervention;
- C** Temporary loss of function or degradation of performance, the correction of which requires operator intervention;
- D** Loss of function or degradation of performance which is not recoverable, owing to damage to hardware or software, or loss of data.

Manufacturers generally claim that their products comply with the immunity tests without informing their customers exactly what this means in terms of performance (except for criterion A).

The EFS designer needs to know exactly how performance degrades due to EMI, so performance criteria B, C and D are no use because they do not require the manufacturer to state what the degradation is. The only performance criterion for which actual performance is specified is A, but it would generally be over-engineering to require that all EFS (or items of equipment intended for use in EFS) always maintained performance criterion A.

A manufacturer might decide that a certain temporary degradation of performance is acceptable for most applications, but without knowing the specific application for his product he has no way of knowing this for certain. The example in 0.7.6 above is a case in point.

0.8 This process applies to the whole ‘lifecycle’

Of course, no one knows what the duration of the actual lifecycle of an EFS will be, so it is necessary to anticipate what is the reasonably foreseeable worst-case lifecycle, to use in the risk analysis process to help ensure that the safety risks to users, third parties and the environment (and financial risks to creators) are kept below the chosen limits.

So, throughout this document (and in fact this whole process) the word ‘lifecycle’ should be taken to mean the anticipated worst-case lifecycle.

A lifecycle consists of the following stages:

- Concept, research, design and development
- Manufacture, storage and transport (shipping)
- Installation and commissioning
- Operation
- Maintenance, repair and refurbishment
- Modification and upgrading
- Decommissioning
- Disposal

Most designers (and safety standards) focus on the safety of users during the ‘Operation’ stage, but Health & Safety at Work regulations in Europe and most/all developed nations also make it unacceptable to expose workers to excessive safety risks. For example, it is not acceptable for interference to cause an industrial

robot to malfunction causing safety risks during its testing, commissioning, maintenance or repair, when it is operated with certain panels open, thereby degrading its EM shielding.

Such possibilities might be dealt with by the management and training of the personnel who will carry out those operations, rather than (solely) by the design of the EFS, but they must all be taken into account to achieve appropriate levels of safety risk during all lifecycle stages.

Depending on the design and application, some of the above lifecycle stages may have no implications for EMC for Functional Safety.

0.9 Graphical overviews of the EMC for Functional Safety Process

Figure 0.2 shows a graphical overview of the process recommended by this Guide, for a 'Simple' EFS (see 6.2) where one creator (who may or may not be the designer) manufactures the entire EFS employing volume-manufactured standard products as appropriate.

Figure 0.3 is a graphical overview for a 'Complex' EFS (see 6.2) that includes one or more custom items that are not designed or manufactured by the creator of the EFS, which also incorporates volume-manufactured standard products as appropriate.

This IET Guide includes text that greatly expands upon each of the Steps in the processes shown in Figures 0.2 and 0.3. It also includes checklists that can be used to help manage this process, at section 13 of this Guide.

Figure 0.4 on a subsequent page shows how the Steps in this process relate to the lifecycle as it is described in IEC 61508.

Figures 0.2 and 0.3 are available as high-quality laminated wall-charts from Nutwood UK Ltd, email pam@nutwood.eu.com for details.

Please note that for the sake of creating readable overview charts, only the major iterative loops are shown. The text describing the various Steps includes other iterative loops that may be necessary, but are not shown on Figures 0.2, 0.3 or 0.4 below.

Also please note that nothing in this Guide is intended to limit the freedom of the EFS designer, manufacture or operator to perform actions that will reduce safety risks (or increase risk-reductions). No guidance document like this can ever be totally prescriptive, so just because a desirable activity is not mentioned in this Guide – it does not mean that it should not be done.

Where this Guide recommends a certain activity, which is not in fact employed on a given EFS, it is recommended that the project documentation shows that it was considered and gives defensible reasons for why the activity was not necessary, or appropriate. This could be the case for a very simple EFS, and also for an EFS for which the safety risks are inherently low (or the level of risk-reduction required is very low) so that – for example – the EFS would not even qualify for consideration as a safety-related system under IEC 61508, yet nevertheless its correct functioning does have *some* impact on safety.

However, where this Guide recommends that a thing should *not* be done, it is almost always the case that it should not be done – but it is not impossible that there may arise circumstances where that thing might after all be necessary. Such a situation would require expert assessment, and thorough documentation to justify it.

Overview of the EMC for Functional Safety process for a 'Simple' EFS

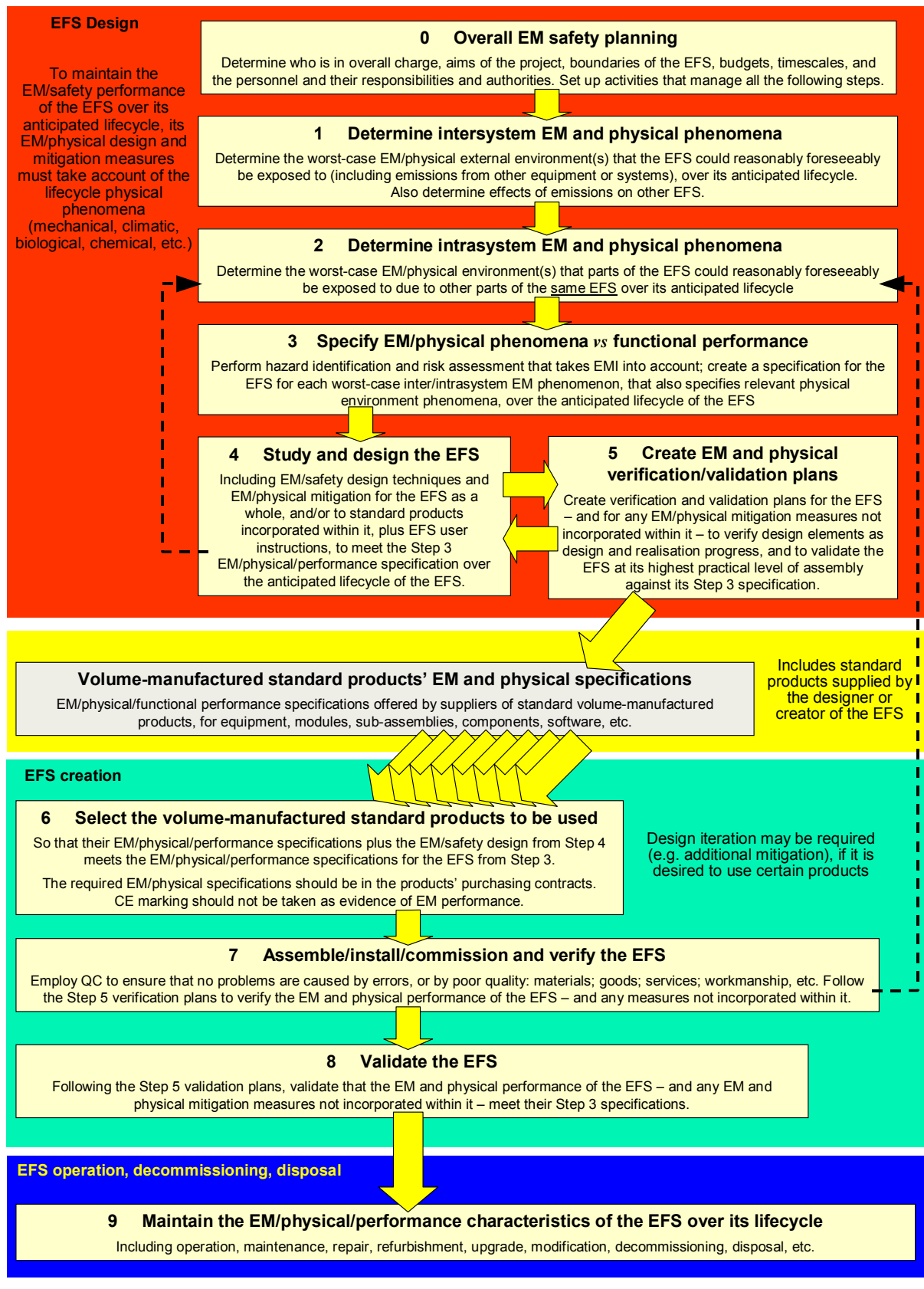


Figure 0.2 Overview of the EMC for Functional Safety process for a 'Simple' EFS

Overview of the EMC for Functional Safety process for a 'Complex' EFS

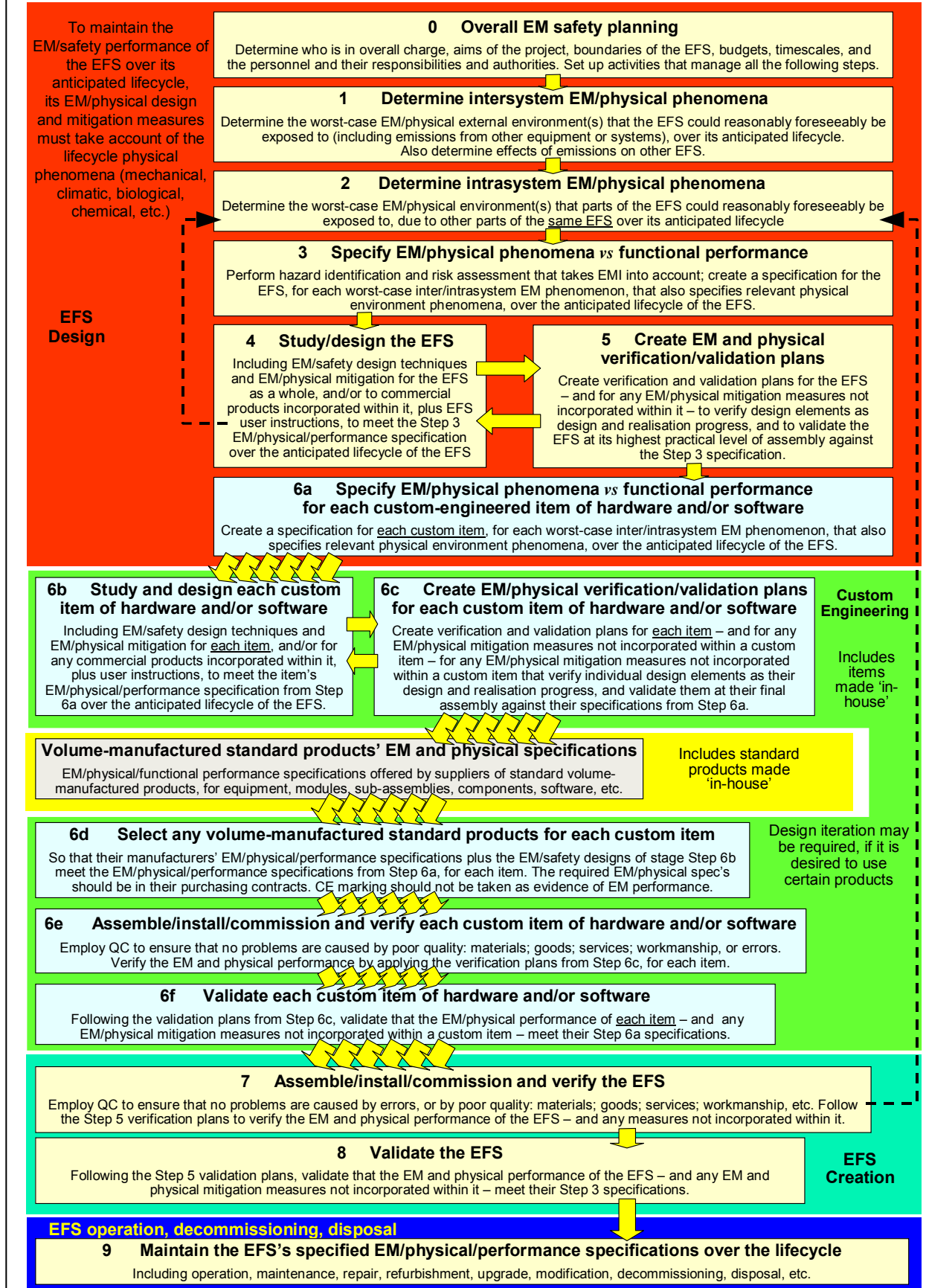


Figure 0.3 Overview of the EMC for Functional Safety process for a 'Complex' EFS

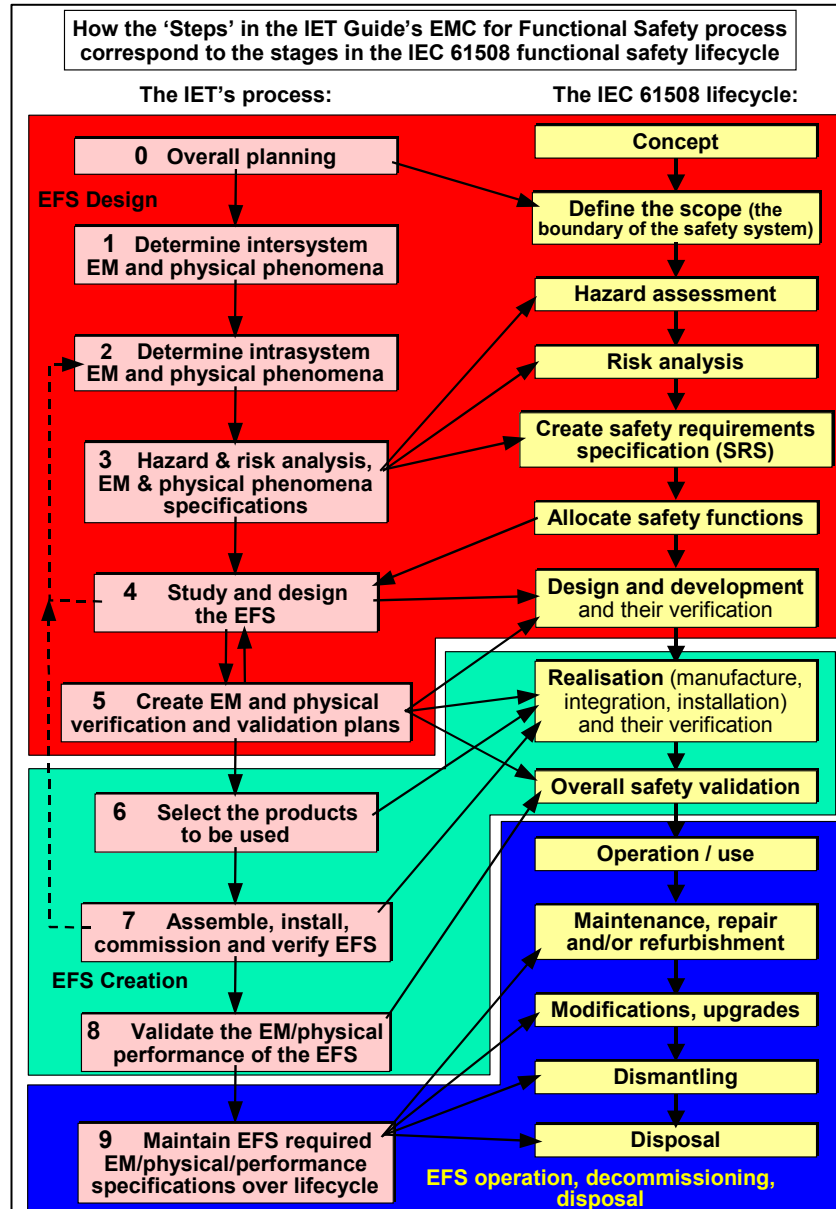


Figure 0.4 Comparison of IET EMC for Functional Safety 'Steps' with IEC 61508 lifecycle stages

0.10 The management, planning and documentation of the process

0.10.1 Management issues

An organisation with responsibility for any of the activities within the scope of this document, should appoint one or more persons to take overall responsibility for:

- The EFS, or for all relevant activities,
- Coordinating the EMC-related activities,
- The interfaces between those activities and other activities carried out by other organisations,
- Carrying out all the requirements of this section
- Ensuring that EMC is sufficient and demonstrated in accordance with the objectives and requirements of this document

NOTE: Responsibility for EMC-specific functional safety activities may be delegated to other persons, particularly those with relevant expertise, and different persons could be responsible for different activities and requirements. However, the responsibility for coordination, and for overall EMC for Functional Safety, should reside in one or a small number of persons with sufficient management authority.

For those activities for which the organisation is responsible, the policy and strategy for achieving EMC for Functional Safety should be specified, together with the means for evaluating their achievement, and the means by which they are communicated within the organisation. This should include appropriate arrangements for competency management [86].

All persons, departments and organisations responsible for carrying out EMC-specific functional safety activities should be identified, and their responsibilities should be fully and clearly communicated to them. Where appropriate, other persons, departments and organisations who could influence the safety-related performance achieved by the EFS should be made aware of these responsibilities.

Procedures should be specified for defining what information is to be communicated, between what parties, and how communication will take place. (See 0.10.5 for documentation.)

Procedures should be specified for ensuring that reported EMC-related hazardous situations are analysed for their relevance to EFS or activities for which the organisation is responsible, and that recommendations are made to minimise the probability of a repeat occurrence.

Procedures should be specified for ensuring prompt follow-up and satisfactory resolution of recommendations relating to EMC of EFS, including those arising from verification, validation and incident reporting and analysis. Organisations should maintain a system to initiate changes as a result of EMC-related defects being detected in the EFS for which they are responsible and, if they are unable to make the changes themselves, to inform users of the need for modification in the event of the defect affecting safety.

Those individuals who have responsibility for one or more of the activities within the scope of this document, should, in respect of those activities for which they have responsibility, specify all management and technical activities that are necessary to ensure the achievement and demonstration of EMC for Functional Safety of the EFS. This includes the selected measures, techniques and tests used to meet the requirements of this document. The amount of work that they specify to be done should be proportional to the benefits it will bring, see 0.10.4.

Procedures should be specified for ensuring that all persons involved in any activity within the scope of this document should have the appropriate training, technical knowledge, experience and qualifications relevant to the specific duties that they have to perform.

The procedures specified as a result of the requirements of this clause should be implemented and monitored.

Suppliers providing products or services to an organisation having overall responsibility for one or more activities within the scope of this document, should deliver products or services as specified by that organisation and should have an appropriate quality management system.

0.10.2 Planning issues

EMC safety planning (EMC safety control) should be carried out taking into account functional safety considerations. It is a strategy to ensure that the EFS has the necessary EM and physical characteristics (or performance) with respect to other devices, equipment, systems, installations, etc., in its vicinity and with respect to the outside world environment, to achieve at least its specified levels of safety risks (or risk-reductions).

The aim of EMC safety planning is to provide the EFS with EM performance that achieves acceptable safety risks (or risk-reductions) over its lifecycle, at acceptable cost, by meeting target requirements during all stages of project implementation. This means considering, investigating and assessing all the EMC issues which might arise during the project schedule that could have an impact on functional safety.

As stated in 0.10.1, all these activities and steps should be described in appropriate plans. The depth and extent of the EMC safety planning depends on the complexity of the EFS and the level of risk (or risk-reduction) required (see 0.10.4).

NOTE: In many cases EMC planning will be performed already due to requirements other than safety. In such cases the EMC planning might be able to be extended to cover EMC for functional safety.

During EM design management, one or more identified persons shall be responsible for creation and execution of the EMC safety plans, and they should have the necessary authority and budget to ensure it is carried out.

The plan will identify:

- i) What is being managed (the boundaries of the EFS).
- ii) The specification of the EFS.
- iii) The purpose and functions of the EFS.
- iv) The location(s) where the EFS is intended to be installed and/or operated.
- v) The specification of the electromagnetic and physical environment(s) over the anticipated lifecycle.
- vi) The specification of the electromagnetic and physical requirements for the EFS, to achieve the levels of safety risks (or risk reductions) considered to be acceptable over the anticipated lifecycle of the EFS.
- vii) The name of the person who has overall responsibility for the plan, and responsibility for ensuring that the final electromagnetic and physical characteristics of the EFS are good enough for the required functional safety over its anticipated lifecycle.
- viii) The names of any other people who also take some part of the responsibility for the final electromagnetic and physical characteristics of the EFS being good enough for its anticipated lifecycle.
- ix) Identification of all standards, specifications, design guides, quality control (QC) procedures, and in-company design guides and checklists that are to be used to guide the design, testing and QC to its eventual outcome.
- x) Any training, third party expert assistance, or third-party testing services when required by the above personnel to be able to discharge their responsibilities correctly.
- xi) Any publications, computer-aided tools or test equipment required by the above personnel to be able to discharge their responsibilities correctly.
- xii) A procedure for maintaining lifecycle electromagnetic and physical performance during maintenance, repair and refurbishment of the EFS (whether these are to be carried out by the creator, or not).
- xiii) A list of the documentation that will be produced by the above personnel (see 0.10.5):
Firstly: for in-company use to demonstrate that they have discharged their responsibilities correctly.
Secondly: to provide to customers, to ensure they are correctly advised on all of the electromagnetic and physical issues and on the resulting functional behaviour of the EFS when exposed to all of the electromagnetic and physical phenomena that could occur in its environment over its lifecycle.
Thirdly: to provide to customers, to inform them of any restrictions concerning future changes to the electromagnetic and physical environment(s) of the EFS over its anticipated lifecycle.
- xiv) Fixed points in the project programme where progress is reviewed by senior personnel and/or independent experts and changes to the programme of the project made as a result – as necessary.
- xv) The timescale for the above activities carried out by the above personnel.

0.10.3 Estimate the 'anticipated lifecycle' of the EFS

This is required so that an EFS can be designed to maintain adequate EM characteristics for the achievement of adequately low risks, or sufficiently high risk-reduction, over its anticipated lifecycle.

A 'lifecycle' includes everything that follows after the final manufacture of EFS, including periods of storage, transport, non-operation or maintenance, as well as operation. Some EFS might be required to be 'mothballed' for several years, maybe after several years of use, and expected to function safely again when put back into service. Some EFS might have very long lifecycles.

The lifecycle includes 'second-hand' use, and use following refurbishments, modifications or upgrades.

For some EFS (e.g. in nuclear power plants), a 'lifecycle' might also need to include the dismantling and disposal of the installation of which they are a part.

0.10.4 Appropriate effort

The amount of effort and cost involved in following the process described in this Guide should be proportional to the benefits that may be realised by its full implementation. 'Benefits' generally include a number of considerations, such as the benefits to the users and third parties of lower safety risks, and benefits to the creator of lower exposure to product liability claims.

It is not possible to provide appropriate guidance on acceptable levels of safety risks. Most countries have mandatory legal requirements for the protection of consumers and/or people at work, but they can differ between each other. And different applications expose companies to different levels of financial risk – for example, the UK public expect very much lower rates of death and injury per mile travelled by rail or air, than per mile travelled by car.

As mentioned earlier, an organisation might use the process described in this Guide (or its references), to minimise financial risks, and even to improve financial performance and market share. Consideration of such issues might also influence the amount of effort and cost that is put into the work described here.

A review of legal case histories, especially in the area of product liability, could also help establish an appropriate level of effort. Remember that this Guide has a two-fold aim: to help achieve appropriate levels of functional safety risks for users and third parties, whilst also improving company financial performance and competitiveness by 'working smarter', by using appropriate EMC techniques to help employ advanced electronic technologies cost-effectively.

Where more effort is required, it would be expected that this would involve a proportionally greater depth of analyses, more detailed and comprehensive assessments, more accurate calculations and/or simulations and/or tests and measurements, more thorough verification, and greater confidence in validation.

It would also result in a proportional increase in the amount of design documentation (see 0.10.5) and greater efforts to ensure its preservation, and more detailed and comprehensive instructions on operation, maintenance, repair, refurbishment, upgrade, modification, dismantling and disposal.

For example, the creators of nuclear power stations would generally be expected to put in more work on EMC for Functional Safety than the creators of domestic appliances.

0.10.5 Documentation

Appropriate documentation should be produced *during* the creation of the management plan, and *during* its execution.

Once the plan has been created and documented, the remainder of the documentation will generally be created during the process of its implementation.

The amount, quality and detail of the documentation will be commensurate with the levels of safety risk (or risk reduction) to be achieved (see 0.10.4).

It is *not* recommended that the EMC for Functional Safety engineering is documented *after* the EFS has been supplied. This is because the act of documenting something often reveals issues that need to be taken into account during the project, and as such it is an important tool in ensuring good cost-effective safety engineering. Also, appropriate documentation is required for the achievement of effective communication between the different people, teams, departments, etc., during the project. Without this documentation, time and/or cost will probably be wasted and/or the EFS will probably not be as safe as it should be.

'Peer review' and 'expert review' are powerful and low-cost verification techniques for use during a project, to ensure that work is progressing correctly. However, they can only be used if the documentation up to the stage of the review is complete. Also, in most organisations, prioritisation of work ensures that once a project has been delivered and paid for, any incomplete documentation will never be completed. Don't be tempted to think that the people who worked on a project will ever have enough 'spare time' to complete the documentation after the EFS has been supplied.

This Guide does not suggest any specific formats, contents or storage media, except to recommend that the documentation is sufficiently detailed and its storage sufficiently reliable to enable an assessor to determine, many years later, whether the plan and its execution resulted in the desired levels of safety risk.

Generally speaking (see 0.10.4), the lower the levels of acceptable safety risks or the higher the amount of risk reduction, the greater the degree of documentation required.

The documentation must be held safe and secure, and actions taken as necessary to ensure it remains readable at least for the whole lifecycle of the EFS, in case it is required by official safety inspectors. This is also necessary so that it is available to help guide designers and others if/when the EFS is repaired, refurbished, modified or upgraded in some way in the future (see Step 9). Note that ensuring readability in the case of stored data can require that the data is periodically losslessly converted to new formats or new media, or alternatively that the means of reading it (e.g. certain computer applications) are reliably maintained over the required period.

It may be a good idea to maintain documents secure and readable for some years even after the eventual disposal of the EFS, to help provide a defence against the possibility of certain types of legal proceedings.

The User Instructions are an important document for EMC for Functional Safety, and these should be provided to the user in a mutually agreed format (e.g. a printed book, or a CD-ROM) and language(s) (different parts of a user's organisation might use different languages. For example, an operator might be from an ethnic minority, or visually impaired, so certain instructions that are relevant for EMC for Functional Safety (e.g. do not operate the machine with the control cabinet door open) might need to be a suitable language, or Braille).

Some product liability lawyers in the UK recommend that all documents relating to safety or reliability (where financial loss is a major concern) are stored for a minimum of 25 years after the supply of an EFS, so as to be available if needed to help make a case for the defence.

It should be noted that the typical approach in European product liability law, is that if the defendant cannot show the court a document that proves that a certain thing was done, then the court assumes it was not done. The onus is on the creator to show they used appropriate safety engineering.

NOTE: This is in marked contrast to the way product liability law is done in some other countries (or parts of them) where the onus is on the plaintiff to show that the creator did not use appropriate safety engineering.

A reference structure should be defined for all EFS project documents that includes version control.

0.11 Design techniques for EMC for Functional Safety

There are many design techniques that can be applied to reduce the safety risks due to EMI, and these are described in detail in Step 4 of the process described in this Guide. Figures 0.2, 0.3 and 0.4 in section 0.9 show how Step 4 fits into the process, and a brief overview of appropriate techniques is given below.

As discussed in 0.10.4, the lower the level of safety risks required, and/or the higher the risk-reduction required – the more difficult are the design and development tasks, and the more effort and skill (and often cost) is required.

Step 4 describes in detail, a number of measures and techniques that can be applied during the design process, to address every stage in the lifecycle of an EFS, including:

- Design and development
- Realisation (manufacture, integration, etc.)
- Installation and commissioning
- Operation, maintenance, repair, refurbishment
- Modifications and upgrades to hardware and software

0.12 Verification and validation techniques for EMC for Functional Safety

There are many different verification and validation techniques that can be applied to reduce the safety risks due to EMI, and these are described in detail in Step 5 of the process described in this Guide. Figures 0.2, 0.3 and 0.4 in section 0.9 show how Step 5 fits into the process, and a brief overview of appropriate

techniques is given below. As discussed in 0.10.4, the lower the level of safety risks required, and/or the higher the risk-reduction required – the more difficult are the verification and validation tasks, and the more effort and skill (and often cost) is required.

The verification and validation techniques that can be used include:

- Demonstrations
- Checklists
- Inspections
- Reviews and Assessments
- Independent reviews
- Audits
- Non-standardised checks and tests
- Individual and/or integrated hardware tests
- Validated computer modelling
- Testing

0.13 Operation, maintenance, repair, refurbishment, upgrade and modification

Procedures need to be in place, and enforced, to ensure that the required EM performance is not degraded any more than was anticipated by the design, over the entire lifecycle. In some cases, systems will be designed so that they do not require special activities by their operators, repairers etc. But in other cases certain specified activities may be required.

However, remembering that safe design takes foreseeable use/misuse and faults into account, the design should ensure that any activities by operators, repairers, etc., that could excessively degrade EM performance would result in safe operation (e.g. by limiting certain operational functions, such as slowing the speed of operation of a machine) or safe shutdown.

The lower the level of safety risks required, and/or the higher the risk-reduction required – the more effort and skill (and often cost) is required during these stages in the lifecycle of an EFS.

0.14 Iterations caused by later stages in the project

When the management structure and plans are first created, the EFS is not yet specified or designed in any detail. During the remainder of the EFS lifecycle, represented by Steps 1 through 9 of this Guide, detailed specifications, design, realisation (assembly, integration, installation, commissioning, etc.), verification, validation, operation, maintenance, etc., will all occur as shown by Figures 0.2 and 0.3, and it is possible for these later stages to require changes to the management and planning.

The management of the EFS project over its entire lifecycle must encourage the consideration of such changes, and also encourage the modification of its management structure and plans as necessary to at least achieve the required specifications for the safety risks (or risk-reductions) achieved by the EFS over its lifecycle.

0.15 Overall conclusions on the above

EMI-related functional safety cannot be verified, at any reasonable cost or timescale, solely by EM immunity testing. To reduce the safety risks caused by EMI to acceptable levels over the lifecycle, or to achieve desired levels of risk-reduction over the lifecycle, methods similar to those already employed for all other safety issues should be employed – the application of well-proven and well-understood EM and physical environment assessment, design and assembly techniques, plus a range of different verification and validation techniques, appropriate QC measures in manufacture, and appropriate measures by the user during the operational life and disposal.

This requires a management process like the one described in this Guide. Section 0.9 includes several graphical overviews of this process – each numbered box in these graphics is associated with a

correspondingly-numbered Step, with its own section in this Guide (Steps 0 to 9 are associated with sections 0 to 9).

0.16 List of contributors to this Guide

Reproduced by permission of contributory author: -

Keith Armstrong, Cherry Clough Consultants, keith.armstrong@cherryclough.com, chair

Claire Ashman, RFI-Global Ltd, claire.ashman@rfi-global.com

Graham Barber, The IET, gbarber@theiet.org

John Cryer, Health & Safety Executive

Jon Duerr, Consultant

Richard Hoad, QinetiQ, rhoad@qinetiq.com

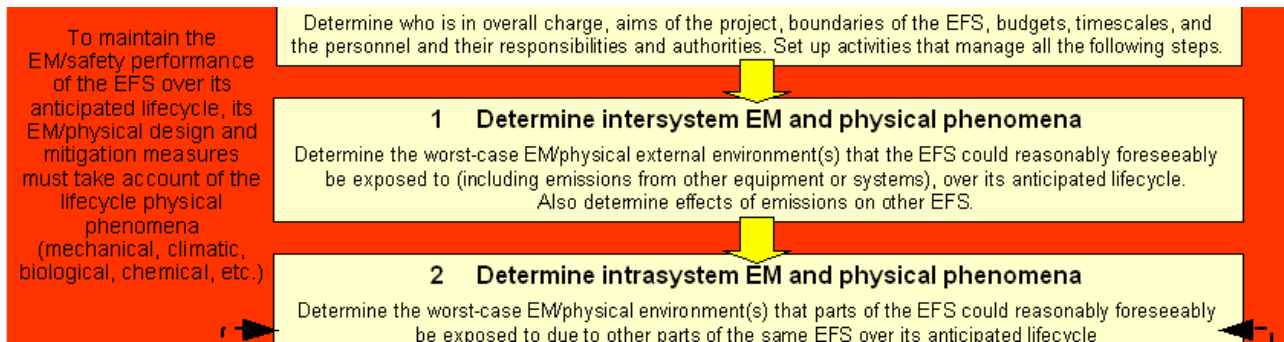
David Imeson, Compliance Europe Ltd, dave.imeson@gmail.com, liaison with BSI GEL/210/12/1

Peter Kerry, CISPR, peter.kerry@cispr.co.uk

Ken Webb, TUV Product Service Ltd, kwebb@tuvps.co.uk

1. Step 1: Determine Intersystem EM and Physical Phenomena

Determine the worst-case EM/physical external environment(s) that the EFS could reasonably foreseeably be exposed to (including emissions from other equipment or systems), over its anticipated lifecycle. Also determine effects of emissions on other EFS.



1.1 Introduction: Step 1 in the EMC for Functional Safety Process

An EFS may need to maintain certain minimum levels of electromagnetic (EM) immunity despite at least one fault, such as the wear-out of a surge protection device by the surges it is exposed to over time. Another example is a broken filter ground connection, which could be caused by poor assembly; shock, vibration, or corrosion over the lifecycle; or wilful damage.

It is not generally appreciated that the EM performance of electrical/electronic equipment that is measured by the normal immunity tests, can have very poor correlation with that equipment's functional behaviour in real life, see [25] [26] [27] [28] and [29]. For example, in real life it is common for two or more EM disturbances to occur simultaneously (e.g. radiated disturbances at more than one frequency; an electrostatic discharge or fast transient burst whilst a continuous radiated disturbance is present). But all standard EMC immunity tests apply one disturbance at a time, and [30] shows they can lead to a very optimistic view of an equipment's real-life immunity.

It is well known in the EMC community that the physical environment can degrade an equipment's immunity performance over a lifecycle, for example by corrosion, shock and vibration, bending forces, temperature extremes or cycling, wear and tear and many other lifecycle physical influences. Some of these issues are discussed in [19] [32] [33] and the last paragraph of [35].

Despite this, immunity is verified by applying standard test methods (e.g. the IEC 61000-4 series, DEF STAN 59-411, MIL-STD-461F, the EU's Automotive EMC Directive 2004/104/EC, etc.) to samples of *new* equipment in a *benign* physical environment. The effects of lifecycle physical environments on immunity are rarely tested.

EFS designers need to know enough about their equipment's 'environment' (EM; physical; climatic; wear and tear; etc. over the anticipated lifecycle) and foreseeable faults and misuse, to select appropriately rated components, and to design circuits, software, filtering, shielding and overvoltage protection. They need this information to be able to achieve the reliability required for operational functions that could have an impact on safety over the entire lifecycle.

For example, engineers need enough information to be able to design:

- EFS and its EM/physical mitigation techniques to cope with the foreseeable range of EM disturbances over the anticipated lifecycle of the EFS, including low-probability events (how low depends on the safety requirements of the EFS) and simultaneous EM disturbances.
- Feedback circuits – so that they do not become unstable due to temperature variations affecting component parameters (e.g. gain-bandwidth product, phase margin, etc.).

- Filters – so that vibration and corrosion will not cause their ground bonds to degrade; and that variations in supply voltage, load current and temperature do not degrade their attenuation too much [32].
- Shield joints and gaskets – so they will continue to perform as required despite twisting of the frame due to mounting on non-flat surfaces; and will withstand wear and tear, corrosion, mould growth or other lifecycle influences [17].
- Surge protection that will withstand the foreseeable overvoltages and overcurrents for the lifecycle of the EFS, or at least for the period between maintenance activities.
- EFS and its EM/physical mitigation techniques so that they will not be unacceptably degraded by lifecycle activities such as: maintenance; repair; refurbishment; modification; upgrade; decommissioning, etc.
- ...etc.

They also need this information to create a test plan for both EMC and HALT (Highly Accelerated Life Testing) that will verify/validate the design; and to design the routine EMC testing and physical stress screening required in volume manufacture.

The EM/physical environments that exist without the EFS in place, are called *intersystem* environments, and are the subject of this Step. Step 2 addresses the *intrasystem* environments – the effects internal to the EFS itself.

The combination of the reasonably foreseeable worst-case intersystem and reasonably foreseeable worst-case intrasystem environments should be captured in the environmental specifications that are the output of Steps 1 and 2 to the rest of the EMC for Functional Safety process.

As with all safety engineering undertakings, the time, effort and skill required by this step depends upon the level of safety risk (or risk-reductions) considered acceptable for the EFS. Lower levels of risks require greater confidence in design and verification – hence more work. Quantifying safety risks (for example using the ‘SIL’ metrics of IEC 61508 [7]) and quantifying everything to do with the EM and physical environments wherever possible, helps demonstrate that the work done was appropriate to achieving the appropriate level of safety risk. Also see 0.10.4.

Where the statistical distribution of an EM or physical ‘threat’ is not known, the ‘reasonably foreseeable worst-case’ value that could possibly occur during the lifecycle should be determined with sufficient accuracy, and the design based on this.

1.2 Assessing locations, routes and paths

The EMC for Functional Safety process is shown in Figures 0.2 and 0.3 as a linear series of steps with a few iterative loops between Steps 7 and 2, but it is not really that simple.

The assessment of an EM or physical environment depends upon the location of the EFS concerned. Just a small movement can make a great deal of difference, for instance moving an electronic control unit from the engine compartment of a motor car to its passenger compartment makes a huge difference to its physical environment, and locating an electronic control and its cables a metre or two further away from where a high-power variable-speed motor drive and its cables are located can make a big difference to its EM environment.

So, during the assessment of the EM and physical environments discussed in Steps 1 and 2 of this Guide, it might be noticed that the location of the EFS and/or its cables could be changed to ease its various environmental threats and achieve a cost-effective outcome for a given level of safety risk.

In the case of wireless communications the various path attenuations will need to be taken into account, and different locations might prove necessary.

The decision might be made there and then to change the location, and report the environments obtaining at the new location. Where such decisions cannot be made during this Step, the environmental assessors should notice whether such changes could give real benefits, and present the EM and physical specifications for suitable alternative locations.

Reducing EM and physical environment specifications by segregation (i.e. moving the location of an item of equipment, or a cable or antenna further away from the highest levels of EM or physical threats, and/or powering an item of equipment from a different electrical supply) is often the most cost-effective way to

reduce the threat levels in the environment, and ease the design and its verification for a given level of safety risk. So the instructions given to the environmental assessors, and the budgets and timescales they are allowed, should take the possibility of alternative locations into account.

1.3 Assessing the EM environment over the anticipated lifecycle

1.3.1 How to do an EM assessment

Not much has been written about how to assess an EM environment over a lifecycle, especially where low-probability EM disturbances are concerned. [36] provides some useful information but is aimed at helping comply with the EMC Directive so may need to be extended in some areas (e.g. High-Power ElectroMagnetics, HPEM, see IEC 61000-2-13 in 1.9.4) to be useful for functional safety.

Assessing a lifecycle EM environment is all about determining what 'EM threats' are present that might interfere with an EFS. It requires appropriate expertise and experience, EM survey equipment, a local collection of documents/library on EM environments and standards, and Internet access. 1.7 gives an overview of the types of EM phenomena that can occur, and Annex B provides more detail.

'Brainstorming' techniques (see Step 3) are generally necessary to help discover many of the possibilities discussed in this Guide, because they depend on the application.

EM environments can be very different, even within a single building. For example, a video camera for a hospital will experience very different, sometimes very powerful EM threats if used in an operating theatre; near X-Ray, CAT Scan or MRI equipment; in a physiotherapy department, life-support ward, or in a public area.

For custom-designed equipment, it is always best to agree the specifications for the operational EM environment with the customer in a written contract. Then, if the customer alters the EM environment and a safety incident occurs with the custom equipment, the blame can be apportioned.

An overall procedure for assessing a lifecycle EM environment includes the following:

- A check list of initial questions (see 1.3.2)
- Consideration of future technology trends and future changes in the EM environment (see 1.3.3)
- The range of EM environments that could be experienced (see 1.3.4)
- The EM issues that should be taken into account (see 1.3.5)
- Comparison of the foreseeable EM threats with the technologies used by the EFS, to decide where in-depth investigation of the EM environment is required (depends on the criticality of the safety application) (see 1.3.6)
- In-depth investigation of aspects of the environment (see 1.3.7)
- Taking uncertainties into account (see 1.3.8)
- Writing a quantified engineering specification for the lifecycle EM environment (see 1.3.9)

1.3.2 A check list of initial questions

An EM environment assessment begins with initial questions about the foreseeable location(s) of the items of equipment, cables, transducers, antennas, etc., that constitute the EFS concerned, and the quality of its AC or DC power supplies. There are also a number of simple questions about the types of equipment or industrial processes (e.g. arc welding) that will be used nearby, including in nearby buildings. A special concern is other equipment interconnected by cables to the EFS in question, for example by shared AC or DC power supplies, data, signal or control cables.

Another special concern is the proximity to any equipment that uses radio frequencies (RF). Any radio, TV or radar transmitters could be significant threats, as could diathermic processors such as those used in medicine and cosmetic surgery (e.g. electrosurgery, depilators, wart removal) and those covered by CISPR 11 and used to treat materials (e.g. plastic welders, microwave dryers, induction heating of metal, etc.).

Military and civilian avionics designers are used to dealing with significant RF threats from broadcast transmitters and radar systems, but these threats can just as easily affect other types of EFS if they are close enough to the transmitting antennas [39].

Personal mobile radio transmitters (e.g. cellphones, walkie-talkies, etc.) have low transmitted powers, but if held just inches away their radiated field strengths can be very high, so they can be significant threats to other electronics equipment.

1.3.3 Consideration of future technology trends, and future changes in the environment

Past years have seen sudden increases in the EM threats at 27MHz (Citizens Band), VHF and UHF (vehicle mobile e.g. taxis, and walkie-talkies). More recently, increases in EM threats have occurred around 900MHz, 1.8GHz (Europe) and 1.9GHz (USA) due to cellphones and GPRS datacomm's; and below 100MHz due to variable-speed motor controls and other switched-mode power converters. These have all caused significant EMI upsets, and some are still causing problems.

An increase in EM threats is now occurring at frequencies above 1GHz, and not just at the 2.45 and 5GHz frequencies used by IEEE 802.11. It is important to try to foresee future technology trends, to reduce the risk of unpleasant surprises.

Possible future developments near the location of the EFS should also be considered. For example, is it foreseeable that high-power RF equipment (transmitters, diathermy, etc.) might be employed nearby, or that a mobile radio communication system might be installed? What about the consequences of the possible roll-outs of PLT (power line telecommunications, also known as broadband over power lines, BPL), UWB (ultra-wideband wireless communications), the planned exploitation of millimetre waves up to 300GHz, etc.

Also see 1.8 – Technology Trends.

1.3.4 Mobile and portable EFS

Some types of EFS can be moved from place to place during their lifecycle, and thereby exposed to different EM environments at each place and/or during their journey. Examples include:

- Demonstration equipment
- Production equipment (e.g. machine tools used in one factory, then moved to another)
- Portable equipment (e.g. certain household appliances, portable tools, etc.)
- Vehicles, trains, vessels, aircraft and spacecraft
- Equipment mounted on – or transported by – vehicles, vessels, aircraft and spacecraft
- Personal medical and other equipment (e.g. medical monitors, pacemakers, drug delivery, wireless communications and navigation devices, portable computing devices, etc.)

1.3.5 What EM issues should be taken into account?

Figure 1.1 provides an overview of the EM issues that may be relevant. Subsequent sections describe each in more detail. Annex B also includes useful information on EM phenomena and the EMI problems they can cause.

'Brainstorming' techniques (see Step 3) are often required to determine the type and likelihood of many of these EM threats. [39] includes 500 examples of interference, showing their very wide range.

It is important to realise that infrequent, transient or low-probability EM events may leave insufficient evidence after the fact, thus making their identification difficult or even impossible. They may be falsely attributed to human errors or negligence, software/firmware malfunctions, physical disturbances, etc.

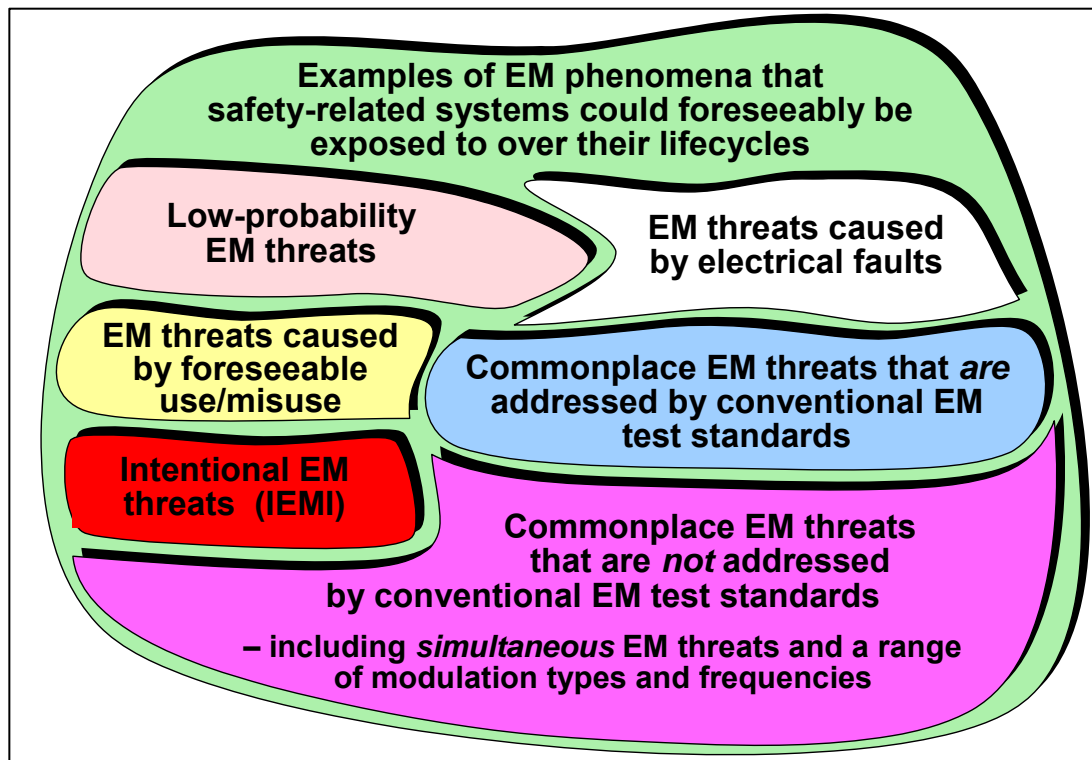


Figure 1.1 Issues to be considered in the assessment of a lifecycle EM environment

1.3.5.1 EM threats from electrical faults

The EM threats from foreseeable electrical faults should be assessed, including the effects of their ground-fault currents and their 'ground-lift' effects; transient overvoltages and noise bursts due to the opening of fuses or circuit-breakers; proximity of arcs and sparks; etc.

Earth faults occur often enough (e.g. due to insulation failure) for safety standards to make it mandatory to use overcurrent protection devices (such as fuses, circuit breakers, etc.). The EM disturbances associated with an earth fault in equipment connected to the same mains distribution network include a sudden large increase in the magnetic field at the powerline frequency (and its harmonic distortion frequencies), due to fault currents that can exceed 1kA. This is in addition to the 'earth lift' voltage at the powerline frequency (and its harmonic distortion frequencies) due to the fault currents travelling in the impedance of the protective earthing system.

These two EM disturbances last for as long as it takes the overcurrent device to open and 'clear' the fault, which can be several seconds. The earth fault ends with a surge overvoltage due to the 'flyback' of energy stored in the inductance of the supply circuit (high, because of the high fault currents) with a corresponding burst of broadband noise emissions as the fuse element or contact breaker opens. The noise burst can last for several seconds if the fuse or breaker rating is inadequate. These EM threats occur at the same time as any continuous EM threats in the environment, such as proximity to radio transmitters or diathermy equipment.

1.3.5.2 Low-probability EM threats

Low-probability EM disturbances include, for example:

- The EM effects of lightning, which can be quantified in all respects using the risk-based methods described in detail in IEC 62305 [40]
- The very close proximity of hand-portable and vehicle-mobile radio transmitters, including those on cars, trains, ships, boats, and aircraft (fixed or rotary wing)
- The proximity of illegal radio transmitters (e.g. 1kW Citizens Band transmitters on some juggernauts)
- Exposure to powerful radars, for example military weapons systems or weather radars, airport or harbour radars; and close proximity to mobile radars such as those mounted on cars (intelligent cruise control), ships, boats, and aircraft (fixed or rotary wing)

1.3.5.3 Intentional EMI (IEMI), High-Power Electromagnetic Environments (HPEM)

EM threats to EFS are not confined to legal activities. IEMI might be a possibility, even though such activities are generally illegal in any country. Certain types of EFS, used in certain applications, might be exposed to IEMI and so this should be taken into account when following this Guide.

Many types of EFS are exposed to HPEM due to lightning strike (or nearby strikes) and some must also continue to provide some level of safety risk when exposed to EM pulses from nuclear explosions (NEMP), the HPEM environments that can occur in certain scientific or industrial sites, or HPEM events that are not generally considered to be part of most environments (see [37]).

1.3.5.4 Commonplace EM disturbances: simultaneous EM threats

These include simultaneous EM disturbances, and a range of modulation types and frequencies.

Commonplace *simultaneous* EM disturbances include:

- Two or more RF fields or conducted voltages/currents at different frequencies
- A radiated RF field or conducted voltage/current plus a transient event such as a fast transient or surge on the mains lead; electrostatic discharge to the enclosure; supply dip or dropout, etc.
- A distorted mains supply waveform, plus a transient event
- A distorted mains supply waveform plus one or more RF fields or conducted voltage/currents
- ...etc.

Simultaneous disturbances with different frequencies can cause EMI through intermodulation (IM), which (like demodulation) occurs naturally in all non-linear devices such as semiconductors. Figure 1.2 shows a very simple example of two RF fields at different frequencies, which can cause EMI by:

- Direct interference from each frequency independently
- Demodulation of the amplitude envelopes of either frequency, or both mixed together
- Intermodulation, in which new frequencies are created

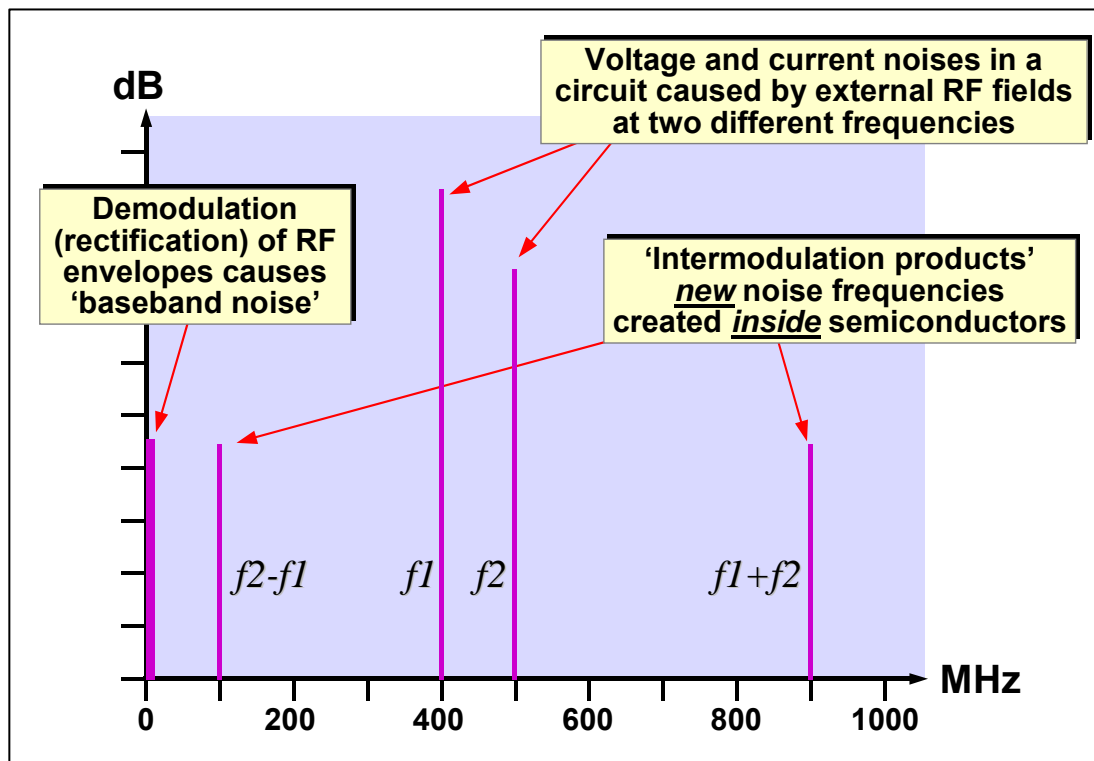


Figure 1.2 Example of RF noises in a circuit, showing demodulation and intermodulation

It is important to note that both demodulation and IM occur *inside* the electronic devices, in the circuits within the items of equipment comprising the EFS. Figure 1.2 shows the 'first-order' IM products in a very simple situation (two original frequencies). If there are more simultaneous frequencies – and especially if the levels

are high enough for the second and even the third-order IM products to be significant – the number of new frequencies created by IM can be very high.

Example: Imagine that conventional (single frequency) testing over the range 10kHz - 18GHz discovers that an item of equipment is only susceptible over the range 50 - 200MHz. The designers add shielding and filtering that is effective over the range 50 - 200MHz, to make the equipment pass the tests.

No shielding and filtering was added over 200MHz - 10GHz (for example), because the normal immunity tests revealed no problems in that range. But if the operational EM environment suffers from simultaneous frequencies in the range 200MHz - 10GHz, these can enter an equipment's circuits and be intermodulated in its semiconductors – creating internal noises in the range 50 - 200MHz and causing interference.

The above example uses simple numbers to illustrate the point that because of intermodulation, conventional RF immunity testing cannot on its own demonstrate that an item of equipment will exhibit a sufficiently low susceptibility to its real-life EM environment. Also, note that a large expansion in the use of the radio spectrum above 2.5GHz is now occurring; so considering the spectrum to 10GHz is generally necessary (to at least 18GHz where military equipment is implicated).

1.3.5.5 Commonplace EM disturbances: A wide range of modulation types and frequencies

A very wide range of 'digital' modulations are now being used in radio and televisions broadcasting (so-called 'digital' broadcasting) and most other kinds of wireless communications. For example, one test recently created to simulate exposure to the TETRA cell-based radiocommunication system recently 'rolled-out' in the UK and operating around 400MHz, uses a modulation consisting of an 18kHz square wave modulation with a depth of greater than 98%, pulsed on and off at 17Hz with a 50% duty cycle.

Some types of equipment might be much more vulnerable to the demodulation of this waveform (see Figure 1.2) than to a 1kHz sinewave, if the 17Hz or 18kHz components, or their harmonics, happen to coincide with frequencies employed in the equipment. Certain industry sectors already test with such modulations, e.g. UK emergency services [48].

Other types of modulation, of which there are very many, might affect other types of equipment.

Above 900MHz, almost all RF transmissions are 'digitally' modulated (e.g. cellphones, Wi-Fi, etc.), or else are pulsed (e.g. radars). And it must not be forgotten that some RF transmitters, including all portable or mobile transmitters, do not operate continuously. 'Keying' a transmitter (turning it on) creates a 'step DC' modulation that can interfere with some types of equipment in ways that that continuous modulations cannot.

It is instructive to consider the frequency spectrum associated with pulsed modulation. Figure 1.3 gives the example of a repetitive pulse, typical of a digital clock waveform.

Increasing the pulse width will result in shifting the 'knee' point f_1 up in frequency, increasing the bandwidth of the signal, increasing the power spectral density and therefore the energy density. Decreasing the pulse risetime will result in shifting the knee point f_2 up in frequency, increasing the bandwidth of the signal and to a lesser extent the energy density.

The frequency range used by common RF communications ranges from 150kHz to 2.5GHz at the time of writing, with higher frequencies limited to fixed microwave links (fixed and satellite). Microwave links use highly-directional dish antennas for point-to-point communications, and can generally be ignored except when there is a possibility that an EFS could find itself interrupting a beam (which can happen, see No. 61 in [39]). Medium term use of the radio spectrum up to 300GHz is now being planned by national, and international, regulators, for commercial, military and domestic applications with particular note that the latter will typically comprise ubiquitous low-power data services.

There are many 'industrial, scientific and medical' users of the RF spectrum, sometimes using very high RF powers for materials processing in a wide range of industries; for 'electro-surgery' and medical scanners; scientific experiments, over the frequency range DC to 100GHz. It must not be forgotten that there are fixed radars at airports, space launch facilities and harbours; and mobile radars on vehicles, vessels air/spacecraft of all types. Military 'search' radars used for aiming weapons systems and other high-power radars can generate very high levels of pulsed fields, for example up to 44kV/m (peak) for a spacecraft launch pad over 4-11GHz, and between 20 and 200V/m (peak) for satellites in orbit at 1000 nautical miles height, over the frequency range 10kHz to 40GHz.

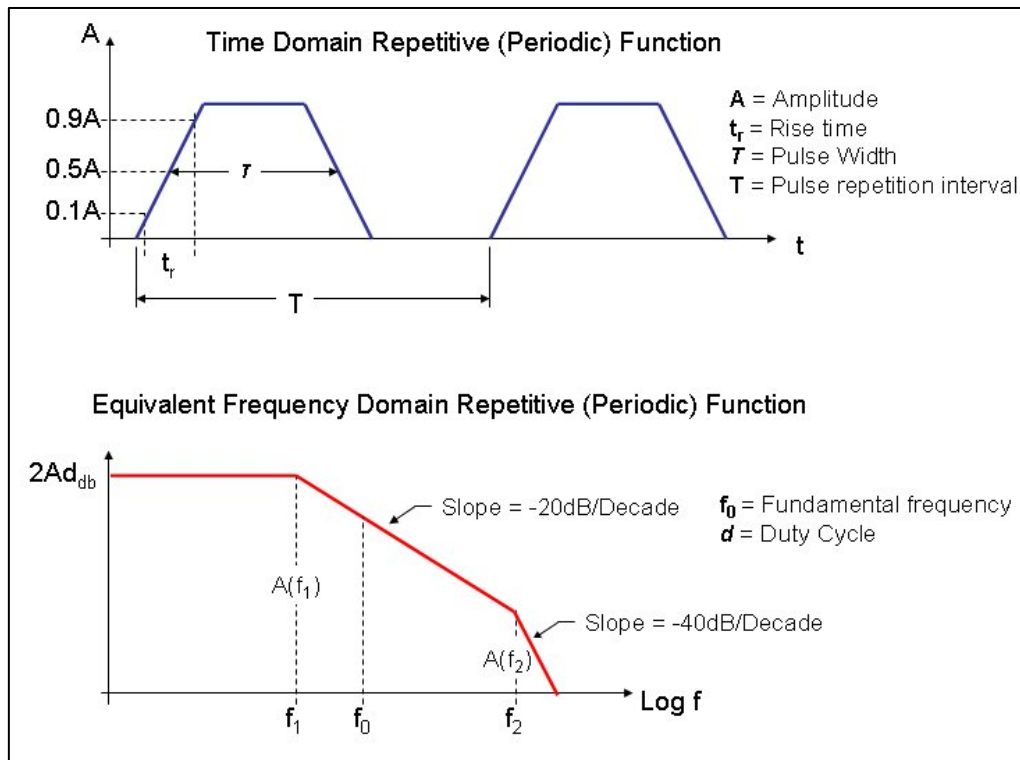


Figure 1.3 Example of a repetitive rectangular waveform

1.3.5.6 EM disturbances caused by foreseeable use/misuse, and ageing

For example: bored security guards poking their walkie-talkie antennas into apertures in computers; holding a walkie-talkie antenna closer to a cable bundle to improve transmission in an oil rig; allowing cellphones to lie around on a control desk amongst the cables to mice and keyboards, etc.

Equipment might be operated with its covers removed or doors open, removing shielding that was limiting its emissions. Ageing usually is associated with oxidative and galvanic corrosion at joints, also leading to degraded shielding and increased emissions. Equipment that has been misused or damaged can also have much higher levels of emissions than its relevant emissions standards would suggest, because of degradations to its shielding and/or filtering, or because of overloads. For example, audio amplifiers driven into clipping can cause significant levels of RF noise to be emitted.

Equipment in actual operation has been discovered that emits about 3Vrms of noise, spread over the range 150kHz to 5MHz, onto its mains cable. This level is roughly 60dB more than the limits in the relevant emissions standard. Such problems seem to occur because the X and Y capacitors in the mains filters have finally succumbed to high levels of surges, although the increase in emissions is surprisingly large. These types of capacitors are designed to fail open-circuit, so as not to cause electric shock or fire hazards, and normal mains voltages in Europe are routinely exposed to surge voltages of 6kV (or higher, according to EN 50160 [13]), whilst the surge levels tested by immunity test standards listed under the EU's EMC Directive are no more than 2kV, so failure of X and Y capacitors, resulting in increased levels of emissions, is not unusual. British Telecom (BT) has reported that they are having significant numbers of such problems, with domestic appliances interfering with their broadband Internet systems.

All these examples have been taken from actual experience. Many more examples will be found in [39]. 'Brainstorming' techniques (see Step 3) are always required to help discover these threats.

1.3.5.7 Multiport CM disturbances

Traditional immunity testing applies EM disturbances to only one 'port' at a time. A 'port' is defined as the enclosure itself, or a point of entry/exit of a conductor (e.g. a cable) to/from the enclosure. The enclosure port is tested with radiated fields above some frequency, often 80MHz, and with electrostatic discharge (ESD). The conductor ports are tested by injecting conducted EM disturbances into the conductors directly, using specially-designed injection devices for radio frequencies below some frequency (typically 400MHz), plus transients and surges.

Conducted RF tests are intended to simulate the coupling of radiated fields into cables, because it can be difficult (or very costly) to achieve good uniformity of the radiated fields, or high enough field strengths, in practical test chambers of the types specified by the standards.

In real life, when a radiated EM field ‘illuminates’ an EFS, all of the cables associated with an item of equipment within it will pick up RF voltages and fields at the same time – but with phase differences between them, depending on the frequency and the time differences caused by the finite velocity of wave propagation. Experiments that injected RF energies into all conductor ports simultaneously, with phase shifts to match what would be expected in real life, have shown that the immunity of the tested electronic units can be significantly worse than when one port is tested at a time in the traditional manner.

Since traditional testing does not simulate the simultaneous (actually, phase-shifted) application of EM disturbances to all ports that can be expected to occur in real life, its test results are incapable – on their own – of demonstrating that EM performance is adequate for achieving acceptably low safety risks.

1.3.6 Comparing the EM threats with the electronic technologies employed by the EFS

Following on from the initial assessment, the possible EM threat phenomena and their levels are identified and quantified using appropriate standards, other resources and experience, including whatever emissions test data is available for nearby equipment, or equipment on the same power network. The aim is to decide whether an in-depth investigation of the EM environment is required.

Simple calculations and computer simulations are often used at this stage to get at least order-of-magnitude estimations of all foreseeable EM threats. It is important to understand that EM test standards measure emissions data in the far-field. But if the emitting equipment will be located close enough for its near-field emissions to be significant, its radiated threat cannot be calculated from its far-field test results.

The proposed technologies, construction techniques, and operational modes that will be employed by the EFS are then assessed with regard to the potential impact on them of each foreseeable EM threat. This process usually allows some threats to quickly be assessed as negligible, taking into account the safety requirements of the final application.

The remaining threats should be investigated in more depth to see if they really are credible as a cause of increased safety risks (or decreased risk-reductions), in which case they will require appropriate design measures and verification (by appropriately designed tests).

The degree of rigour applied to this comparison, and to any subsequent in-depth investigation, depends on the criticality of the safety application, see 0.10.4.

1.3.7 In-depth investigation of aspects of the environment

In-depth investigations often involve instrumented site surveys. These are a very powerful tool but are most suitable for continuous or common threats, such as a nearby broadcast transmitter, road or railway line; or where foreseeable threats can be repeated at will (e.g. proximity of personal or mobile transmitters, microwave cookers, ground faults, fuse-opening, operation of HV circuit breakers, switching of reactive loads, etc). In some highly critical cases it may even be desirable to initiate cloud-to-ground lightning using rocket or laser lightning initiation methods, and measure the effects of the resulting strikes at the EFS’s intended location.

Site surveys should try to capture the reasonably foreseeable worst-case threats, as well as trying to get an idea of their statistical variations. Spectrum analysers with a range of suitable antennas are often used to fully measure threats in terms of their frequencies, amplitudes, modulations, and statistical variations. With some sites, surveys may need to continue for some time to capture the full range of activities. Automated site survey instruments are available for wide a variety of RF and power quality phenomena, and are often used in these situations.

As well as frequency and level, it is also important to determine the modulation types and frequency ranges, for each radiated or conducted RF frequency threat. Simply knowing the purpose of the RF signal (e.g. broadcast FM radio) is often enough to be able to specify its modulation scheme and range of possible modulation frequencies.

Where short-lived EM phenomena occur, for example from vehicles travelling at speed, the sweep times of spectrum analysers make it very difficult to capture the full spectrum of their possible emissions. [41] describes a measuring technique that can overcome this problem.

During a site survey, mobile radio communications devices that will be used on the site (personal and vehicle mobile, voice and data) can be brought close to the measuring antennas to simulate their foreseeable closest proximity to the equipment concerned. Where this distance is closer than the calibration distance for the antenna, and especially when it is within the antenna's near-field region, care is required not to make erroneous measurements. Data obtained in this way can help specify the real-life EM environment for the increasingly difficult problem of portable wireless devices.

A problem with site surveys is that it can be difficult to obtain reliable data on uncontrolled transient and other low-probability disturbances, because they can require a large number of measuring stations, and/or a very long measuring period. So for low-probability EM threats the usual approach is to do some research instead.

Research into EM environments usually begins with standards. The IEC 61000-2-x series generally addresses the household, commercial or industrial environments (see 1.9.4 and note its caveats), but electronic equipment can find itself in other environments such as outdoors, marine, land mobile, air mobile, space, etc., and there are standards and other documents that provide information on the EM threats in such situations.

Characteristics of mains supplies can be found in some IEC 61000-2 series standards, and also in [13]. The telecom's industry places great emphasis on reliability, especially for 'central office' (telephone exchange) equipment. Also, some telecom's equipment is located outdoors and very exposed to lightning. So telecom's EMC standards can contain useful information, for example [42], [43].

[19] and [18] are very useful for high-power EM (HPEM) environments, such as near radio transmitters or radar systems. Military authorities have field strength maps covering most of the world, but it may be hard to obtain them unless you are a member of that country's military or an allied nation. The national authorities in charge of civil aviation keep records of the radars in use (frequencies, power levels, and pulse characteristics) in their countries and should also be a good source of information on mobile radars (e.g. on ships). They may also be able to help with field strength maps.

Automotive and roadside EM environments have characteristic EM features. The UK's Motor Industry Research Association [45] surveys the EM environment of the UK's roads every few years and publishes a report. Some EMC consultancies specialise in railway EMC and should be able to provide data on railway and traction EM environments.

Lightning protection standards, lightning incidence ('isokeraunic') maps and knowledge of a site's lightning protection system help determine the threats from lightning and their statistical probabilities, see Chapter 9 of [46]. There is a natural tendency to focus on the highest peak voltages and currents during transient/surge events, but [47] shows it is possible for lightning events to have relatively low voltages and currents but continue for long enough to burn out simple designs of overvoltage protection – which then fail to protect their equipment.

'Ground lift' voltages from remote ground faults, and 'power cross' caused by mechanical damage to bundles of cables that include signals and mains power, are often just a few tens or hundred volts, but can damage equipment because simple types of overvoltage protection might fail to trigger, or be burnt out by the long duration currents. So the likelihood of such events needs to be considered too.

Information on HPEM and IEMI is now starting to appear in standards such as IEC 61000-1-5 [34], and in papers such as [37] and [38].

The Records of the IEEE International EMC Symposia are very good sources of information on real-world EM environments, and are all available on CD-ROM and on-line to facilitate searching [44]. Other regular international Symposia at which papers on EM environments are often published include Zurich, Rome, EMC-Europe and Wroclaw.

[36] includes some simple and very crude calculations that can help assess EM phenomena, and these are reproduced in 1.9. Computer simulation of aspects of the EM environment is increasingly possible, e.g. for the fields created by HV power lines or by nearby transmitting antennas. Some consulting companies offer bureau services in this area.

Also see Annex B.

1.3.8 Taking uncertainties into account

There are often uncertainties associated with the assessment of the EM environment(s). In some cases the maximum levels that are assessed cannot be exceeded for some fundamental reason associated with its physics, but in others they may have been assessed by computer simulations or measurements, which inevitably include some uncertainty.

Taking the example of an environmental assessment based upon a very long term and thorough programme of measurements – the measuring transducers, instruments and their interconnecting cables all suffer from measurement uncertainty, even though they are fully calibrated at the recommended intervals. There will also be a quantifiable uncertainty due to the way the measurements were made.

Ignoring the uncertainty in the assessment could lead to safety risks being higher than considered acceptable. So the specifications that are output from Step 1 should include a statement of the uncertainty associated with each specified reasonably foreseeable worst-case parameter.

To avoid specifying very high levels in Step 3 of our EMC for Functional Safety process – which could lead to over-design and unnecessarily high costs – it is important when assessing the reasonably foreseeable worst-case EM environment to use assessment techniques that achieve low levels of uncertainty.

1.3.9 Writing a quantified EM environment specification for the lifecycle

Once all the EM environment information has been acquired, a specification can be written for the EM environment in which the EFS will operate over its anticipated lifecycle. This should be used by engineers to help design its circuits, software and EMI mitigation measures, and to be used to help plan the design verification (EMC testing) and serial-manufacture testing regimes.

The reasonably foreseeable worst-case EM environment specifications that are the outputs of this step should be based – as far as practicable – on existing standards (such as the DEF STAN 59-411 or IEC 61000-2 series), modified where necessary. The use of existing standards makes it easier to actually verify the design by testing, in Steps 5 and 8, since test laboratories will already have the equipment and expertise necessary to apply much of the test methods.

Each parameter specified should be followed by a statement about the uncertainty associated with it.

Where multiple EM threats occur simultaneously [30] it is most important that the specification makes this clear.

The combination of the reasonably foreseeable worst-case intersystem (Step 1) and reasonably foreseeable worst-case intrasystem (Step 2) environments should be captured in the EM environmental specifications that are employed by the rest of the EMC for Functional Safety process.

Consider possible simultaneity between reasonably foreseeable EM and physical environments, some combinations may result in unacceptable safety risks, and include significant possibilities in the specification.

1.4 Assessing the physical environment over the anticipated lifecycle

1.4.1 How to do a physical assessment

Physical and climatic environments have generally been better characterised than EM environments. IEC 60721 is a series of standards that classify dynamic, climatic and environmental conditions to help the designer apply the IEC 60068-2 tests. IEC 60721 covers a range of conditions, including:

- Transport, storage, installation and use
- Extreme (short-term) conditions during transport, storage, installation, and use
- Solar radiation, temperature and humidity
- Stationary use at weather-protected locations
- Portable and non-stationary use

It is impossible to specify mandatory requirements for worldwide use, but the IEC 60721 series establishes principles and methodologies to determine alternative tests. Issues such as 'safety margin', 'acceleration factors', etc. are left to the designer's judgment.

There are also well-established military standards covering a wide range of physical and climatic environments, and some very well-established institutions devoted to reliability that may be able to provide additional data. Civilian EFS might use military standards and sources to fill in any gaps in the coverage of the IEC standards.

Where information is not available from published sources: calculations, computer simulations, instrumented site surveys and research amongst books, articles and papers should fill the knowledge gaps.

The assessment of the physical environment over the lifecycle should include the reasonably foreseeable worst-case physical 'threats' because they could be sufficient to degrade the EM performance permanently, possibly making the EFS vulnerable to normal EM threat levels.

However, physical threats that cause *temporary* degradation of EM performance might be acceptable; depending on how bad the degradation is and how often it occurs. A degradation that still leaves the EFS immune to normal EM threats might be acceptable if the extreme EM threats that are possible are very unlikely to occur at the same time. A quantitative analysis based on real-life statistics is always required for such assessments.

1.4.2 What physical issues should be considered?

Designing and testing an EFS to achieve adequate EM immunity to its anticipated EM environment over its lifecycle, requires knowledge of the *physical* environment the EFS will have to withstand over its lifecycle.

The lifecycle EM environment affects what performance is required from the EMI mitigation measures – whereas the lifecycle physical environment affects how those measures should be implemented in practice.

For example, it is necessary to know the vibration environment to decide whether vibration-proof fixings are required for a filter, so that its RF attenuation is more likely to be maintained over the EFS's life. Knowledge of the climate and possibilities for condensation, liquid splashes and spills etc, is necessary to be able to choose cost-effective conductive gasket materials and metal plating, so that corrosion does not reduce shielding effectiveness over the years.

Where electrical bonding is required, the build-up of grease, dirt, sealants, etc.; wearing away of plated surfaces by abrasive cleaning; painting and other 'improvements', have in the past increased contact resistances and degraded EM performance. These issues could also cause problems for new EFS unless it is designed accordingly.

EMI suppression techniques that will last the lifetime of (for example) a fire alarm system may not be physically robust enough for an automotive braking system; whereas applying the automotive system's EMI suppression techniques to the fire alarm might add too much cost without appreciably improving functional safety.

So the physical environment of the EFS needs to be specified, over its whole lifecycle – so that sufficiently reliable EMC mitigation measures can be designed at a reasonable cost.

The physical environment to be assessed should include the reasonably foreseeable worst-cases over the whole lifecycle, including (but not limited to) the following, as far as they could affect the items of equipment, cables, connectors, antennas, sensors, actuators, etc., comprising the EFS:

- Mechanical forces, such as bending and twisting forces, such as are caused, for example, by non-flat mounting (e.g. floor or wall); stacking other equipment on top; sitting or standing on top, vehicles driving over (especially cables) or collisions, etc.
- Shock, vibration, etc.
- Climatic parameters such as temperature extremes and cycling, air pressure extremes and cycling, humidity extremes, condensation, icing, etc.
- Pollution, such as conductive or dielectric dusts; liquid splashes and spills such as: fuels, beverages, inks, toner, coolants, lubricants, human or animal body fluids, etc.
- Corrosive atmospheres, e.g. sulphuric acid from batteries, petrol, hydraulic fluid, ethanol, salt spray, etc.

- Biological effects, such as contamination (e.g. mould/fungus growth) or attack by insects or animals (e.g. rodents eating insulation and shorting-out conductors), human and animal bodily fluids, etc.
- Wear and tear; misalignment; etc., over the whole lifecycle, including the effects of repetitive operations, maintenance and cleaning regimes, including the use of non-approved maintenance and cleaning materials and methods, etc.
- Exposure to solar and other radiation, etc.

A number of good examples showing how the physical environment, and well-meaning human activities such as cleaning and painting, can significantly degrade EM performance, are given in the appendices to [19].

Just as for the EM environment, foreseeable use and misuse should be taken into account. It is not unusual for EFS to be subjected by its users or others to physical abuse that its designers never imagined.

Also, just as for the EM environment assessment, physical stresses often occur simultaneously, for example:

- High levels of both temperature and humidity, plus mould growth in some environments
- Cold temperatures plus condensation
- Extremes of temperature, plus mechanical forces, shocks and vibrations
- Extreme temperature cycling combined with extreme air pressure cycling (e.g. aircraft equipment mounted on a wing)

'Brainstorming' techniques (see Step 3) are often required to determine the type and likelihood of many of these physical threats.

1.4.3 Taking uncertainties into account

Just as for the assessment of the EM environment, see 1.3, the uncertainties inherent in the assessment of the reasonably foreseeable worst-case physical environment(s) needs to be part of the specification that is the output from this Step.

To avoid specifying very high levels in Step 3 of our EMC for Functional Safety process – which could lead to over-design and unnecessarily high costs – it is important when assessing the physical environment to use techniques that achieve low levels of uncertainty.

1.4.4 Writing a quantified physical environment specification for the lifecycle

Once all the physical environment information has been acquired, a specification can be written for the worst-case physical environment(s) reasonably foreseeably expected to experienced by the EFS over its lifecycle. This should be used by engineers to help design the EFS's circuits, software and EMI mitigation measures, and to be used to help plan the design verification (EMC testing) and serial-manufacture testing regimes.

The reasonably foreseeable worst-case physical environment specifications that are the output from this step should be based – as far as practicable – on existing standards (such as the IEC 60068 series), modified where necessary. The use of existing standards makes it easier to actually verify the design by testing, in Steps 5 and 8, since test laboratories will already have much of the equipment and expertise necessary to apply the test methods.

Where multiple physical threats can occur simultaneously it is most important that the specification makes this clear.

Each parameter specified should be followed by a statement about the uncertainty associated with it.

The combination of the reasonably foreseeable worst-case intersystem (Step 1) and reasonably foreseeable worst-case intrasystem (Step 2) environments should be captured in the environmental specifications that are employed by the rest of the EMC for Functional Safety process.

Consider possible simultaneity between reasonably foreseeable EM and physical environments, some combinations may result in unacceptable safety risks, and include significant possibilities in the specification.

1.5 Also determine effects of emissions on other EFS

The EM and physical environments are not only about what EM/physical phenomena might exist that could threaten an EFS, they are also concerned with the impact that radiated EM and physical emissions from a new or modified EFS could have on another EFS that is nearby, or the impact that its conducted emissions could have on EFS that connect to its power or other cables or share the same mechanical structure.

Many of the EM and physical threat issues discussed in this document apply equally well to emissions, and installing a new EFS, or modifying an existing EFS, could have an impact on safety risks (or risk-reductions) associated with another EFS that is nearby or interconnected by conductors.

So where there is an EFS, the EM performance of other EFS that are nearby or interconnected – can be important for safety reasons. The management, design, and maintenance of the EFS should therefore extend to its EM and physical emissions.

1.6 Iterations

The EM and physical environments of an EFS (or parts of it) can change between the date of the initial assessments and it actually being operated, and they can also change during its life.

It should be part of the EMC for Functional Safety process to determine whether the environments have changed, and what (if any) actions are required. If the EM or physical environments have become more difficult in some way, the effects must be followed through the whole series of steps in this process, so that the EFS always achieves its levels of safety risks (or risk reductions) in its actual operating environment(s) over its anticipated lifecycle.

The EFS designer(s) must provide instructions to the EFS creator, and also to its owner/user/operator, describing how to deal with the possibilities of changes in the EM or physical environments, during the lifecycle stages that are under their control, see Step 4.

1.7 Overview of types of EM phenomena

Conducted low frequency phenomena	Harmonics, interharmonics Signalling voltages Voltage fluctuations Voltage dips and interruptions Voltage unbalance Power frequency variations Induced low frequency voltages DC. in AC networks
Radiated low frequency field phenomena	Magnetic fields ^a Electrical fields
Conducted high frequency phenomena	Directly coupled or induced continuous voltages or currents Unidirectional transients ^b Oscillatory transients ^b
Radiated high frequency field phenomena	Magnetic fields Electrical fields Electromagnetic fields – continuous waves – transients ^c
Electrostatic discharge phenomena (ESD)	Human and machine
Intentional EMI ^d	
High altitude electromagnetic pulse (HEMP) ^d	
^a Continuous or transients. ^b Single or repetitive (bursts). ^c Single or repetitive. ^d To be considered in case of special conditions.	

Table 1 – Overview of types of electromagnetic phenomena
(Source: IEC DTS 61000-1-2 2nd Edition [4])

See Annex B for more information on EM phenomena and how they can interfere.

1.8 Some foreseeable future technology trends

Electronic technology trends are generally in the direction of worsening EMI, creating more likelihood of functional safety issues due to interference. Some examples of these trends follow.

1.8.1 Developments in Integrated Circuits (ICs)

There are three main trends in IC developments, from the point of view of this Guide:

- Faster (higher frequency of operation) ICs, i.e. higher clock speeds; hence increased noise levels due to wider bandwidth (for both noise emissions, and noise pick-up from the environment)
- Lower power supply voltages for ICs; hence lower noise thresholds, hence greater likelihood of EMI
- Higher gate density ICs, achieved by using smaller feature sizes for the semiconductors, hence fewer electrons to represent a stored data bit and greater likelihood of EMI

These three trends are all caused by the drive to make ICs more capable and less costly, and one-third of the USA's GDP depends on this process continuing.

As ICs become more powerful and less costly, they are used more widely, often displacing other technologies that are much less likely to cause or suffer EMI. Also, the low cost and powerful processing capabilities are creating thousands of new types of application, that were never before possible – such as electronic stability control (ESC) of motor vehicles.

1.8.2 Developments in power semiconductors

These are enabling the rapid growth of two main classes of applications: switch-mode power conversion, and wireless communications.

Climate change is another driver for the increased use of switch-mode power conversion, because of the higher efficiencies it can achieve where power needs to be controlled. For example, during the next few years all domestic appliances will use variable-speed motors instead of fixed speed motors that are switched on and off, to achieve better 'energy ratings'. The variable speed motors will all be driven by switch-mode power converters, which will emit significant amounts of conducted noise onto the domestic mains electricity supplies, and radiated noise to the domestic environment.

1.8.3 Increased use of wireless communications, for voice and data

Wireless transmitters generate radiated EM emissions directly. Although the signals they emit into the air are intentional, they are *unwanted* noise emissions as far as receivers that want to use a different wireless communication are concerned, and for all other electronic technologies that are not themselves radio receivers. Developments in semiconductors are allowing more radiated power and/or higher frequencies to be transmitted more cheaply.

Wireless communications were once mostly the province of governments, military, sailors, emergency services, and radio and television broadcasters. But developments in power semiconductors (see the bullet point above) have 'democratised' the use of wireless technologies so that individuals these days might be using three or more radio transmitters without ever realising it (e.g. a cellphone with a Bluetooth headset, whilst accessing the Internet via Wi-Fi).

In 1990 it was not common for a person to own a cellphone that was the size of a house brick and had a short battery life. By 2000 nearly everyone in the developed world had a cellphone, including most of the children, and by 2005 it was clear that developing and third-world countries would never contemplate building a wired telephone infrastructure, they are all going directly to cellphone systems.

Cellphone companies now have markets for their products measured in billions, but this is dwarfed by the possibilities now being realised for what is called machine-to-machine wireless communications, which has the aim of eventually replacing all signal, control and data cables so that the only cables that equipment needs will be for power. The attractions are obvious, but it all results in a more crowded radio spectrum.

The traditional way of utilising the radio spectrum divided it up into individual, narrow channels, each assigned to individual transmitters (such as a particular radio station), placed severe limitations on the amount of communication that could occur. Digital modulation techniques, originally developed for the military, enabled the early cellphone systems to pack their millions of subscribers into a band of spectrum

that would previously have only handled a few hundred channels, and since then numerous more exotic digital radio modulation schemes have increased the 'packing density' of the airwaves. For example, in the USA and Europe a band of spectrum that used to handle a few 'analogue' television broadcasters, is being replaced with 'digital TV' that transmits hundreds of stations.

The increased power handling, higher efficiency and lower cost of the power transistors has enabled wireless transmitters to go mobile, and operate for hours or even days from batteries. The radio transmissions are not very powerful, often less than 1 watt, but being mobile they can be very close to an EFS and subject it to much higher radio field strengths than the 100kW broadcast transmitters providing the radio and television services.

A decade or two ago, if one erected an antenna anywhere and connected it to a spectrum analyser, one saw a few strong signals and a number of small ones, each occupying a narrow slice of spectrum, and all the rest was background noise. The same test now shows large blocks of frequencies filled with digital modulations for cellphones and digital TV and radio (e.g. Digital Radio Mondiale, which will eventually replace 'analogue' radio broadcasting). Spectrum usage has increased considerably.

The next phase of this process is well under way, and is called software-defined-radio, in which transmitters and receivers will actively look for spare bits of spectrum and use them, even if only for a few tens of milliseconds before having to 'hop' to a new frequency that is currently unused.

The radio licensing authorities are very keen to encourage the increasing use of the airwaves, because by selling more transmitting licences they earn more money for their governments. So there are some revolutionary new licensing schemes being seriously discussed at the international meetings where the regulators gather to discuss policy (after all, one country must not adopt schemes that interfere with others).

Any given band in the radio spectrum of the near-future will easily contain a hundred times as much radiated energy as was usual in 1990, and up to much higher frequencies. There are now firm plans lodged with the European Telecommunications Institute (ETSI) to exploit the radio spectrum all the way up to 300GHz, and the development of domestic products that employ the 60GHz band (mostly intended for the real-time wireless distribution of video) are very well advanced at the time of writing.

Also, a recent development has been UWB (Ultra Wide Band) wireless technology, that uses so-called time-domain radio techniques and as a result transmits over very wide frequency ranges all at the same time, for example from 1MHz to 10GHz. UWB is not only useful for wireless communications, there are many plans to use it for non-contact measurement and monitoring (e.g. of the heart rates of everyone in a room).

Complaints by radio astronomers and a concern not to degrade the Global Positioning Satellite (GPS) system has resulted in UWB being confined to frequencies above 3GHz or so. Most UWB devices are very low power, but in a decade or two any typical domestic, commercial or industrial environment is likely to contain transmissions by hundreds of such devices simultaneously.

Other modern developments in wireless technologies coming to fruition, thanks to the continuing developments in power semiconductors and ICs, include Radio Frequency Identification (RFID) in which little transponders called 'RFID tags' are affixed to whatever it is wished to monitor, and quite powerful transmit/receive stations called 'readers' placed at strategic locations to 'read' the tags that come within range.

Early versions of RFID were first used to prevent theft of on high-value goods from high-street stores, and was known as Electronic Article anti-Theft Surveillance (EATS), which did little more than detect the presence of a tag where it should not be. Now, the tags contain ICs containing pertinent data, which can be read by a 'reader'. So it will soon be possible to wheel a trolley of goods out of a supermarket, almost without slowing on your way to the car park, and have your credit card automatically deducted with the value of the goods in the trolley as you pass through the reader at the store door. The trolleys also will have readers in them, so, as you put goods in the trolley their value, and the value of the total 'basket' of goods, will appear on a screen on the trolley.

A further development of RFID allows the data carried by the tags to be modified by the reader's associated transmitter. So RFID can be used to track a component part through an industrial process, keeping a record of what it has undergone and its vital statistics as they change from one process to the next. Or track a patient through a hospital and record all their treatments and drugs and vital signs. It is possible to imagine readers being everywhere, so that almost everything is tracked at all times.

Whilst this explosion in wireless technologies is very welcome for many reasons, it means that we and our EFS will be increasingly be bathed in radiation, to levels that were never imagined in the 1990s. The International Committee on Non-Ionising Radiation, ICNIRP, has recently realised that all their estimates of

the human health hazards from wireless energy, and all their measurement techniques, have been based on there being one or two significant sources of radio energy, each of considerable power, but that in the future people will be exposed to dozens, maybe hundreds of simultaneous low-power sources, and they have no idea how to deal with that [50].

Just as people will be exposed to unforeseen multiplicity of radio energy sources, so will the EFS. Just as the authorities responsible for protecting human health are finding themselves unable to respond anything like quickly enough to these new unknowns, the EMC standards authorities are likewise unable to respond with emissions and immunity test standards and/or test limits and/or levels that correspond to the brave new wireless world that is being created as you read these words.

1.8.4 Developments in hard disc drive technology

Developments in 'hard disc drive' data storage media are achieved by the shrinking of the size of magnetic domains. As data storage capacity grows, and file sizes increase due to the addition of graphics, videos, etc., data transfer rates must continually increase, requiring electronics that operate at ever-higher speeds, with ever-weaker signals from the magnetic domains, hence more susceptibility to EMI.

1.8.5 Systems are becoming more distributed

In the past discrete 'boxes' have identified the 'boundary' of a 'system'. However, in the future the function performed by an original piece of equipment may be distributed in several boxes throughout a system.

For example, modular avionics may mean that a specific function such as landing gear control may be disassociated with a particular Line Replaceable Unit (LRU) or 'box' and be comprised of separate control cards within racks physically distributed around the aircraft, see Figure 1.4. This presents new challenges especially where compliance testing is relied upon since a distributed network is more difficult to test.

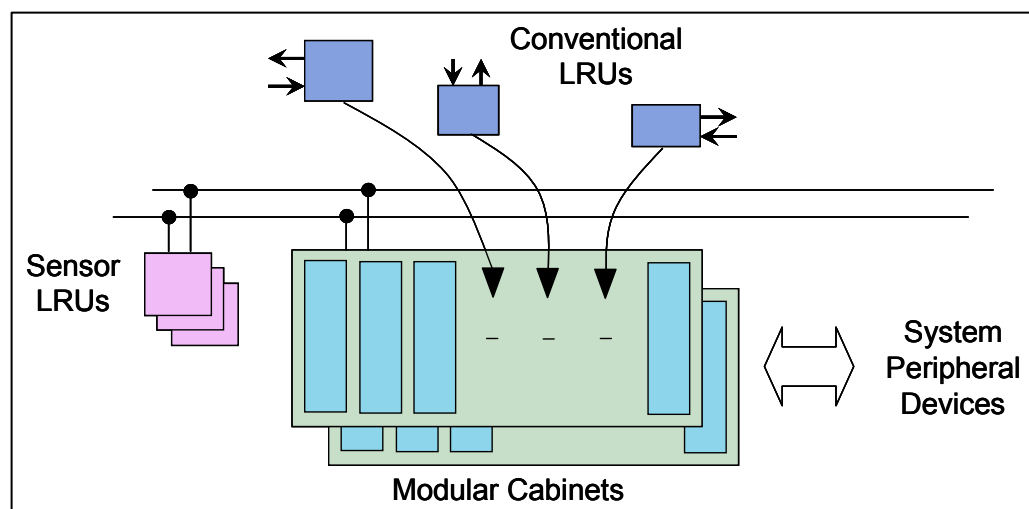


Figure 1.4 Impact of modularisation on avionics

1.9 Some tools for assessing the EM environment

1.9.1 Examples of field strengths *vs* distances for various RF transmitters

The distances given in Table 2 below assume free-space radiation (e.g. an omnidirectional antenna) and the relationship $E = \sqrt{(30P)/d}$ Volts/metre between effective radiated power (P) and field strength (E), at a distance of d metres from the transmitting antenna.

This is a crude estimate but at least it indicates the order of magnitude. Most real antennas have some gain in some preferential directions, increasing the field strength in those directions. For a cellphone antenna the gain might be between 1 and 2dB, and for dipole it might be 2.4dB.

Remember that actual radiated threats can be *at least* doubled by reflections from metal structures and the apparatus itself. At frequencies at which resonances (standing waves) can exist within metal structures, the

electric or magnetic field strengths can be amplified by as much as 10 or 100 times (20 or 40dB), possibly even more.

Total emitted RF power, and type of radio transmitter	Proximity (d) in metres for 3 V/m	Proximity (d) in metres for 10 V/m	Proximity (d) in metres for 30 V/m	Proximity (d) in metres for 100V/m
0.8W typical (2W maximum) hand-held GSM cellphone, and 1W leakage from domestic microwave ovens	1.6 (2.5)	0.5 (0.8)	0.16 (0.25)	0.05 (0.08)
4W private mobile radio (hand-held) (e.g. typical VHF or UHF walkie-talkies)	3.6	1.1	0.36	0.11
10W emergency services walkie-talkies, and CB radio	5.0	1.6	0.5	0.16
20W car mobile cellphone, also aircraft, helicopter, and marine VHF radio-communications	8	2.5	0.8	0.25
100W land mobile (taxis, emergency services, amateur); paging, cellphone, private mobile radio base stations	18	5.4	1.8	0.54
1.0 kW DME on aircraft and at airfields; 1.5kW land mobile transmitters (e.g. some illegal CBs on trucks)	70	21	7	2.10
25kW marine radars (both fixed and ship-borne)	290	89	29	8.50
100kW long wave, medium wave, and FM radio broadcast	580	170	58	17
300kW VLF/ELF communications, navigation aids	1,000	300	100	30
5MW UHF TV broadcast transmitters	4,000	1200	400	120
	V/m peak	V/m peak	V/m peak	V/m peak
100MW(peak) ship harbour radars	18,000	5,500	1,800	550
1GW(peak) air traffic control and weather radars	60,000	17,000	6,000	1,700
10GW(peak) some military radars	180,000	55,000	18,000	5,500

Table 2 – Estimating the radiated fields from intentional radio transmitters

A note on attenuation of field strength by buildings:

The attenuation of a double-brick wall in the UK may be assumed to be one-third (10dB) on average, but can be zero at some (unpredictable) frequencies that can vary depending on the weather. The attenuation of a typical steel-framed building can be much greater than this below about 10MHz, depending on position within the building and the size of the apertures created by the steel frame.

A note on radars:

Average threats from radars may be as much as 30 times less than the peak values given above: this depends on the type of and the radar pulse characteristics. Radar fields are line-of-sight, and the very high powers of ground-based radars may be considerably attenuated by geographical features such as hills or the curvature of the earth. Fixed radars are normally aligned so as not to include people or buildings in their main beam.

Conducted disturbances:

A rule-of-thumb for conducted interference currents above 150kHz due to mobile and fixed radio transmitters is to assume a cable characteristic impedance of 150Ω. Then the conducted currents = (V/m) divided by 150. E.g. a 30V/m field gives rise to 200mA of current.

A note on industrial RF processing equipment (e.g. ISM equipment covered by CISPR11) These can be very powerful indeed (e.g. MW) and do not use omnidirectional antennas. Their field strength 'contour maps' can only be determined by a site survey.

1.9.2 Estimating the low frequency radiated fields emitted by long conductors

At frequencies from DC (0Hz) to 100kHz it is possible to crudely estimate the strengths of the electric and magnetic fields emitted by voltages and currents in conductors, using the simple formulae below. Measurements of electric and magnetic fields at these low frequencies are easy to do, for fields of

magnitudes down to 0.1V/m, or 0.1A/m, using low-cost handheld instruments, so the main use for these rules-of-thumb will be where the apparatus concerned does not yet exist.

These rules-of-thumb will mostly be used for estimating high levels of magnetic fields from conductors carrying high levels of DC and AC power, such as motor drives, electromagnetic stirrers, etc., especially to determine whether CRT type monitors in the vicinity will give stable images.

These rules assume free-space radiation, but actual fields strengths will be modified by the proximity of cables, cable trays ducts and conduits, equipment and cabinets, structural steelwork, etc., and may be higher or lower than those estimated from these simple formulae.

Where safety-related issues are concerned it will be important to perform more exact assessments, or to perform measurements, even on partially constructed apparatus or apparatus of a similar type. If these rules are to be used in the initial stages of a project on safety-related issues their results should be multiplied by at least 10 to provide a suitable margin for uncertainty until a more accurate assessment or measurement can be made.

These rules-of-thumb all assume that the length of the conductors is much greater than the distance (d) at which the field strength is to be estimated. When the cable length equals d, a rule of thumb would be to divide the field by two, with further reductions as the cables become even shorter.

1.9.2.1 Estimating electric field emissions at low frequencies (DC-100kHz)

Electric field strength is given the symbol E and measured in Volts/metre (V/m).

EMC test equipment is usually calibrated in dB μ V/m, where 0dB μ V/m = 1 μ V/m, since EMC was traditionally concerned with interference to radio receivers which were intended to pick up radio signals with merely a few μ V/m field strength.

Personnel hazard measuring instruments for non-ionising radiation are usually calibrated in kV/m, since it is long-term exposure to such magnitudes of electric fields that may cause health problems.

Electric fields are difficult to calculate for real-life situations because free-space conditions are never found and the proximity of other conductors, metalwork, and ground have a profound effect. A very crude rule of thumb for the electric field between a long single conductor and anything else is to divide their voltage difference (Vdiff) by their spacing (s) in metres: $E = V_{diff} \div s$

E.g. A long cable carrying 1kV is 1 metre from an opto-isolator device which may be assumed to be at earth potential. The resulting electric field experienced by the opto-isolator is 1kV/m. (At 2m distance the field would be reduced to 500V/m.)

Where there are multiple long cables running in free space, the electric field at any point is the vector sum of all their individual contributions. In most cases cables are run parallel to each other, so the vector addition is merely a straight addition of the fields.

E.g. for +1kV on a long cable 1m away from an 'earthy' optical sensor, with a second long cable run in parallel with 100mm spacing from the first cable and 1.1m from the optical sensor: when the second cable carries an equal and opposite voltage of -1kV the resulting field strength at the optical sensor is very approximately (1,000) + (-909) = 91V/m.

If instead of 100mm the cable spacing was reduced to 10mm, the resulting field strength at the optical sensor would be roughly (1,000) + (-990) = 10V/m.

The presence of large masses of earthed metalwork nearby is likely to reduce the size of electric fields. If this mass of earthed metalwork is between the conductor with the high voltage and the sensitive part, it may reduce the electric field dramatically by acting as a shield. (If the mass of metalwork is not earthed its shielding effect could be much less.)

1.9.2.2 Estimating magnetic field emissions at low frequencies (DC-100kHz)

Magnetic fields are measured in Amps/metre (A/m), Tesla (T), or Gauss (G).

Conversion factors between these three units in free air are:

1A/m \approx 1.25 μ T
1A/m \approx 12.5mG
1T = 10kG \approx 800kA/m
1G = 100 μ T \approx 80A/m

EMC test equipment is usually calibrated in dB μ A/m, where 0dB μ A/m = 1 μ A/m, since EMC was traditionally concerned with interference to radio receivers which were intended to pick up radio signals with merely a few μ A/m field strength.

Personnel hazard measuring instruments for non-ionising radiation are usually calibrated in kAmps/metre, kGauss, or Tesla, since it is long-term exposure to these magnitudes of magnetic fields that may cause health problems.

In the special case of a long single conductor in free space, the magnetic field strength it produces at a nearby point may be calculated from Amps \div ($2\pi d$), in A/m, where d is the perpendicular line-of-site distance from the point concerned to the centre of the conductor (in metres).

E.g. For 100A in a long cable that is 1m away (the shortest distance at right angles to cable run) the field strength according to this formula is 16A/m (approx. 20 μ T).

Where there are two or more long cables similarly running in free space, the magnetic field at a point is the vector sum of all their individual contributions.

E.g. For +100 A in a long cable 1m away with its -100A return current in a parallel cable 1.1m away (e.g. a cable spacing of 100mm when the point of interest and the two cables all lie in a plane): the field strength at the point of interest is (16) + (-14.5) = 1.5A/m.

If instead the cable spacing is 10mm (i.e. the send/return cables are almost side-by-side, since d is measured to the centre of the conductor) the resulting field strength is (16) + (-15.8) = 0.2A/m.

1.9.2.3 Notes on running conductors close together

The above examples show the great reduction in electric and magnetic fields which can be achieved by running send and return conductors carrying equal and opposite voltages and currents, as close together as possible. Twisting send/return conductors together is even better (although easier for small-signal cables than for power).

For three-phase (or three-phase and neutral) power conductors the voltages and currents (and hence their fields) are all at 120° to each other, and running them together in a single cable or bundle (with a twist if possible) helps reduce electric and magnetic fields in exactly the same way.

Where very heavy currents are concerned, the mechanical stresses caused by running cables with opposing currents close to each other may damage the insulation in the cables in a relatively short period of time, leading to fire or shock hazards. Busbars that use solid insulation may be a better solution in such cases.

As well as considerably reducing the emitted electric and magnetic fields, running send/return or three-phase power conductors closely together also helps to reduce their pickup of interference from their environment, so this technique is important for immunity as well as for emissions.

1.9.2.4 Notes on frequencies higher than 100kHz

At higher frequencies the wavelengths become comparable with typical cable lengths in industrial situations, making the above rules-of-thumb useless.

Where intentional radio transmitters are involved, the table in section 1.9.1 gives useful guidance on field strengths, but for other high-frequency signals it is impossible to use the above rules-of-thumb and measurements are the only option.

Crude measurements may be done with simple low-cost test gear, but if the apparatus concerned is of recent manufacture, its manufacturer should already have emission test results.

1.9.3 Estimating how radiated fields vary with distance

Where the field strength at one distance from the emitter is known (e.g. from manufacturer's test results, or from a calculation) the rules-of-thumb below allow the field strength at other distances (d) to be crudely estimated.

These simple rules work over a very wide frequency range, at least to 1GHz, providing the distances concerned are not too near to the emitter (less than $\lambda/6$, where λ is the wavelength, see 1.9.3.3).

These rules assume free-space radiation, but actual field strengths will be modified by the proximity of cables, cable trays ducts and conduits, equipment and cabinets, structural steelwork, etc. Consequently an

'engineering margin' of at least 100% is recommended over and above the levels calculated using these rules to allow for these real-world effects, but it should be realised that such effects can sometimes cause field strengths to be 10 times (+1,000%) or reduced to negligible values, especially at frequencies above 10MHz.

Where safety-critical functions are concerned it will be important to initially either measure the actual field, or allow for the level to be at least 10 times higher than these calculations give and then measure the actual field as soon as it becomes possible to do so.

1.9.3.1 Electric field strength

Electric field strength tends to be proportional to $1/d$

E.g. An ISM apparatus is known to emit 135dB μ V/m (= 5.6V/m) at 84MHz at 3m radial distance from a part of its structure.

At 1m radially from the same part of its structure it may be expected to have a field strength of the order of 145dB μ V/m (= 16.8V/m).

At 30m radial distance from that part it may be expected to have a field strength of the order of 115dB μ V/m (= 0.56V/m).

1.9.3.2 Magnetic field strength

For single conductors, magnetic field strength tends to be proportional to $1/d$

E.g. A long single cable is known to emit a magnetic field strength of 16A/m at a distance of 1m (perpendicular to the run of the cable).

The field strength at 100mm distance may be expected to be of the order of 160A/m.

The field strength at 10m distance may be expected to be of the order of 1.6A/m (which is still too high for a CRT type computer monitor to be sure of meeting the Health and Safety "VDU Directive").

Where a number of conductors run very close together in parallel and carry currents that balance out (e.g. send and return currents to a DC motor, three-phase or three-phase-plus-neutral power), at distances (d) which are very much larger than the separation between the individual conductors the resulting magnetic field strength tends to be proportional to $\{(Amps) \times (separation)\} \div d^2$

E.g. A pair of DC drive cables (send/return) have a spacing of 10mm, and are known to create a magnetic field of 0.2A/m at a distance of 1m.

At a distance of 2m their magnetic field may be expected to be of the order of 0.05A/m.

For transformers, solenoids, and the coils of induction heaters, the magnetic field strength tends to be proportional to $Amps \div d^3$.

E.g. An 800kW 1.1kHz steel billet induction heating coil is known to produce 100A/m at 1m distance from the side of its coil.

At 100mm distance it may be expected to create a field of the order of 100kA/m, getting close to the levels at which health hazards may occur.

At 10m distance it may be expected to create a field of roughly 0.1A/m, quite low enough to be confident about fitting a CRT type of monitor at this distance and achieving good image stability.

Mixtures: in the real world coils and transformers are connected to other devices and to cables, and the rate of change of magnetic field strength with distance will be a mixture of all three of the above approximations.

E.g. In the above example of the steel billet induction heater, although the 1.1kHz magnetic field emitted by the coil has diminished to roughly 0.1A/m at a distance of 10m, the 11kV 3 ϕ 50 Hz power cables to its power electronics cabinet would be likely to be carrying around 100A each.

If these long cables had a spacing of 100mm from each other in the same plane as the computer monitor, and were 5m away from it on average, their magnetic field would be of the order of 0.06A/m, still a negligible amount.

However, if the power to the electronics cabinet was supplied at 1.1kV 3 ϕ 50Hz and their three 1000A supply cables were each spaced apart by 500mm: at 5m distance their resulting 50Hz magnetic field would be of the order of 3A/m, which could be expected to have a significant effect on the image stability on a normal CRT-type VDU.

1.9.3.3 The relationship between electric and magnetic fields at higher frequencies

All fields are emitted as either electric or magnetic fields, but after travelling a distance equivalent to roughly one-sixth of their wavelength they all turn into electromagnetic fields.

Electromagnetic fields consist of both electric and magnetic fields in a ratio that depends on the characteristic impedance of the medium they are travelling in. For air, the characteristic impedance is 377Ω , so it is possible to measure either the electric or magnetic component and calculate the other by dividing or multiplying by 377.

The wavelength (λ) of a frequency (f) is given by $\lambda = v/f$, where v is the velocity of propagation (the speed of light) in the medium the wave is travelling in.

In air, $v = 3.10^8$ metres/sec (approximately), so the wavelength of a 30MHz EM wave in air can be assumed to be 10m. So at more than about 1.5m from an emitter, whether it initially emits electric or magnetic fields, the result will be an electromagnetic wave with its electrical (E) and magnetic (H) field components in the ratio $E/H = 377\Omega$ (just like $V/I=R$, Ohms law).

Below 30MHz, most test methods measure the magnetic component of electromagnetic fields with a loop antenna. Above 30MHz most test methods use an electric-field antenna. However, the results from each type of antenna can easily be converted into E or H fields as required.

In PVC-insulated cables the velocity of propagation is less than in air, and is often as low as 2.10^8 metres/sec (depending on the cable type). This means that all frequencies have shorter wavelengths when they are conducted in a cable, compared with being radiated through the air.

Earlier, the frequency range of the simple formulae was limited to 100kHz, since the wavelength (in air) at this frequency is 3,000m. One-sixth of this λ is 500m, a large enough distance to enable us to ignore the effects of wavelength even in a large building.

1.9.4 A list of the current standards in the IEC 61000-2-x series

The raw data in these standards may be useful in helping to assess an electromagnetic environment without using a site survey, or when site surveys would take too long (e.g. to determine the likely number of mains voltage dropouts expected over a year).

When using these, beware of any assumptions in them about 'average' or 'typical' environments or sites – this indicates that either the measurements have been 'smoothed' by averaging, losing the worst-case data required by this Guide for an EM assessment, or that it is not actual data but an assessment by an expert. Unfortunately for this Guide, the expert's assessment will not be relevant where safety issues are concerned.

IEC 61000-2-1	Description of the environment. Electromagnetic environment for low frequency conducted disturbances and signalling in public power supply systems. (Low voltage power systems, i.e. up to 1kV rms)
IEC 61000-2-2	Compatibility levels for low frequency conducted disturbances and signalling in public power supply systems.
IEC 61000-2-3	Description of the environment. Radiated and non-network related conducted phenomena.
IEC 61000-2-4	Compatibility levels in industrial plants for low frequency conducted disturbances.
IEC 61000-2-5	Classification of electromagnetic environments. This was written to assist with regulatory EMC compliance rather than safety, it therefore makes certain assumptions about what constitute 'average' or 'typical' exposure to EM phenomena. It does not address <i>all</i> of the significant EM phenomena that <i>could</i> occur at a specific location, and neither does it specify their worst-case EM threat levels. As a result, it is of interest but not as useful as some of the other publications in the 61000-2 series.
IEC 61000-2-6	Guide to the assessment of the emissions levels in the power supply of industrial plants as regards low-frequency conducted disturbances.
IEC 61000-2-7	Low frequency magnetic fields in various environments.
IEC 61000-2-8	Voltage dips, short interruptions and statistical measurements.

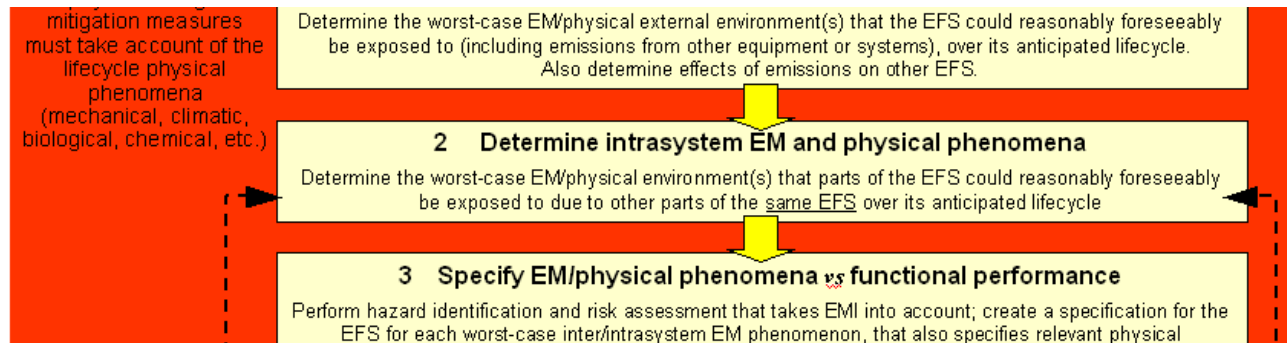
IEC 61000-2-9	Description of the HEMP environment – Radiated disturbance. (HEMP = High altitude electromagnetic pulse from nuclear explosions, also relevant to lightning exposure)
IEC 61000-2-10	Description of the HEMP environment – Conducted disturbance.
IEC 61000-2-11	Classification of HEMP environments.
IEC 61000-2-12	Compatibility levels for low frequency conducted disturbances and signalling in public medium voltage power supply systems.
IEC 61000-2-13	Electromagnetic compatibility (EMC) – Part 2-13: Environment – High-power electromagnetic (HPEM) environments – Radiated and conducted.

New standards are being added all the time, as well as existing standards being modified.

Always check for the latest situation, for example by visiting the BSI Standards website www.bsi-global.com, or the IEC website www.iec.ch, and looking in their lists of current standards. IEC standards can easily be purchased from their webstore at <http://webstore.iec.ch>, with a credit card.

2. Step 2: Determine Intrasystem EM and Physical Phenomena

Determine the worst-case EM/physical environment(s) that parts of the EFS could reasonably foreseeably be exposed to due to other parts of the same EFS over its anticipated lifecycle



2.1 Introduction

Step 1 described how to assess the EM and physical environments obtaining in the location(s) occupied by the EFS over its anticipated lifecycle.

But each item of electrical/electronic equipment creates its own EM and physical disturbances, and so has an effect on its local EM/physical environments.

Emissions from the EFS could interfere with another EFS, causing excessive safety risks, especially where they are near to each other, or share any power or data cables or earthing systems. (This is one of the reasons why Step 1 included the requirement to consider future technologies and trends in the assessment of the environment.)

Where the EFS is comprised of several items of equipment, the emissions from one or more of them might interfere with one or more of the other parts of itself. This is known as intrasystem interference, and is the subject of this step.

The combination of the worst-case intersystem and worst-case intrasystem environments should be captured in the environmental specifications that are the output of Steps 1 and 2 to the rest of the EMC for Functional Safety process.

As with all safety engineering undertakings, the time, effort and skill required by this Step depends upon the level of safety risk considered acceptable, or the risk reductions required, for the EFS. Lower levels of risks or greater risk-reductions require greater confidence in design and verification – hence more work. Quantifying safety risks (for example using the ‘SIL’ metrics of IEC 61508) and quantifying everything to do with the EM and physical environments wherever possible, helps demonstrate that the work done was appropriate to achieving the appropriate level of safety risk.

Where the statistical distribution of an EM or physical ‘threat’ is not known, the maximum ‘worst-case’ value that could possibly occur during the lifecycle should be determined with sufficient accuracy, and the design based on this.

2.2 Choosing the locations, routes and paths

As discussed in Step 1, the EMC for Functional Safety process is shown by Figures 0.2 and 0.3 as a linear series of steps with a few iterative loops between Steps 2 and 7, but it is not really that simple.

Reducing EM and physical environment specifications by segregation (i.e. moving the location of an item of equipment further away from an equipment that is causing high threat levels, and/or powering it from a different electrical supply) is often the most cost-effective way to reduce intrasystem interference (EM or physical), easing the design and its verification for a given level of safety risk or risk-reduction.

So the brief given to the intrasystem environment assessors, and the budgets and timescales they are allowed, should take the possibility of segregation into account.

2.3 Assessing the EM environment over the anticipated lifecycle

This assessment should be undertaken in the same way as for the intersystem EM environment described in Step 1 (see 1.3).

The difference is that in Step 2 we are only concerned with other parts of the same EFS, which are under our control, so gathering data on the EM threats is made much easier.

Many of the emissions from items of equipment will generally be known, as part of the process of achieving compliance with the EMC Directive, although these will not cover the whole frequency range. Where a component part of the EFS is purchased complete, it is strongly recommended to obtain all of its emissions test reports as part of the purchasing contract, otherwise it may be necessary to test it at additional cost.

Where a supplier's EMC quality control does not consider the EMC implications of all changes to the build state of the unit they are supplying, and/or where they do not do regular sample-based EMC testing – then EMC test results for an earlier unit are meaningless, so the unit should be tested for emissions again.

Where a supplier cannot provide the necessary information, it will be necessary to assess how the emissions performance of a unit will increase over time as its shielding, filtering and surge suppression degrade due to the EM and physical environments. This could entail subjecting an example of the unit of the EFS (or maybe just its shielding enclosure and filters) to highly-accelerated life tests (HALT) and then testing its emissions to see how badly they have degraded.

The emissions tests associated with compliance with the EMC Directive only cover a subset of emissions, but it is necessary to know the full spectrum of emissions from DC to the highest frequency of concern, as magnetic and electric fields, conducted voltages and currents, transients and continuous.

Where suppliers cannot or will not provide the necessary EM data, it may be necessary to determine it by inspection, calculation, simulation, and/or measurement at additional cost.

For example, EMC Directive emissions standards ignore emissions at most frequencies below 150kHz, yet radiated fields and conducted noise at audio frequencies can interfere with many types of devices and circuits.

If a unit does not consume power that varies significantly at audio frequencies, inspection of its circuits and simple calculations will probably show that its radiated and/or conducted emissions will be negligible at such frequencies. If in doubt, or where very low levels of safety risks are acceptable – whether significant emissions exist – can be quickly checked with calibrated close-field probes and current clamps, and then measured accurately if the checks indicate high levels.

However, the audio frequency emissions of a high-power variable-speed motor drive or high-power audio-frequency amplifier will almost certainly be very high, and so will require accurate 'calibrated' simulation and/or measurement.

A common management tool for intrasystem interference control is a matrix chart, sometimes known as a 'gap analysis' table, for an example, see [51]. A gap analysis lists all the items of equipment and their cables in a system along both axes, one axis being labelled 'emissions' and one labelled 'immunity'. The rows and columns of the matrix are then used to assess the potential for each item of equipment to interfere with every other item in the system. This step provides the emissions data for the gap analysis.

(Of course, to perform a gap analysis also requires that the immunity of each item of equipment to all these emissions phenomena is known, and how it degrades with physical threats over the lifecycle. This is not the subject of this step, but when negotiating with suppliers for the EMC data they will provide, it is as well to take this requirement into account at the same time.)

Where multiple EM threats occur simultaneously [30] it is most important that the specification makes this clear.

2.4 Assessing the physical environment over the anticipated lifecycle

This assessment should be undertaken in the same way as for the intersystem physical environment described in Step 1 (see 1.4).

The difference is that in Step 2 we are only concerned with other parts of the same EFS, which is under our control, so gathering data on the physical threats is made much easier.

Just as described in 2.3, we need to know what physical phenomena can be created ('emitted') by each item of equipment within the EFS, over the whole range of possible phenomena, over the lifecycle.

For example, if a machine that – when old or badly maintained – could leak fluids onto another part of the EFS, causing it to corrode, it is important to know this so as to design the EFS accordingly (e.g. by moving the potentially corroded item away from the path of the leak). Also, if a part of an EFS could suffer from high vibration or high temperatures, or emit high levels of ionising radiation that could upset microprocessors or their memories, it is important to know this too for the safe design of the EFS.

As for intrasystem EM phenomena, the compatibility between different items of equipment can be assessed by a 'gap analysis' using a matrix chart, so the 'emissions' of – and 'immunity' to – the various physical phenomena are needed to be known to complete this analysis.

Where suppliers cannot or will not provide the necessary data, it must nevertheless be assessed by inspection, calculation, simulation, or measurement.

Where multiple physical threats can occur simultaneously it is most important that the specification makes this clear. (Unlike the EM testing community, physical environment test engineers are very well used to applying simultaneous threats.)

2.5 Iterations

The intrasystem interference possibilities cannot be fully known until the EFS is installed and operational.

Figures 0.2 and 0.3 try to show this with two dotted arrows, one from Step 4 and one from Step 7, both of them leading back to Step 2. These are meant to show that some intrasystem interference possibilities might remain unknown until the design of the EFS is complete, and sometimes it is discovered during assembly, installation commissioning, etc., that the design must be altered, for example by moving an item of equipment or rerouting a cable, with consequences for intrasystem interference.

Of course, for a Complex EFS, the work on the custom-engineered items to be incorporated in the EFS might result in the need to re-assess the intrasystem interference possibilities for the complete EFS.

For both Simple and Complex types of EFS, to use certain models of standard volume-manufactured products might require modifications to the design of the EFS, or of custom-engineered items, and these might also affect the intrasystem interference possibilities.

EFS Validation (Step 8) might reveal modifications that need to be made, in order to comply with the EMC safety specification from Step 3, and these might also affect the Step 2 intrasystem assessments.

Figure 2.1 and 2.2 try to show all these iterations as bold dotted lines.

The EFS designer(s) must provide instructions to the EFS creator, and also to its owner/user/operator, describing how to deal with the possibilities of changes in the EM or physical environments due to intrasystem issues, and the resulting iterations, during the lifecycle stages under their control, see Step 4.

Overview of the EMC for Functional Safety process for a 'Simple' EFS

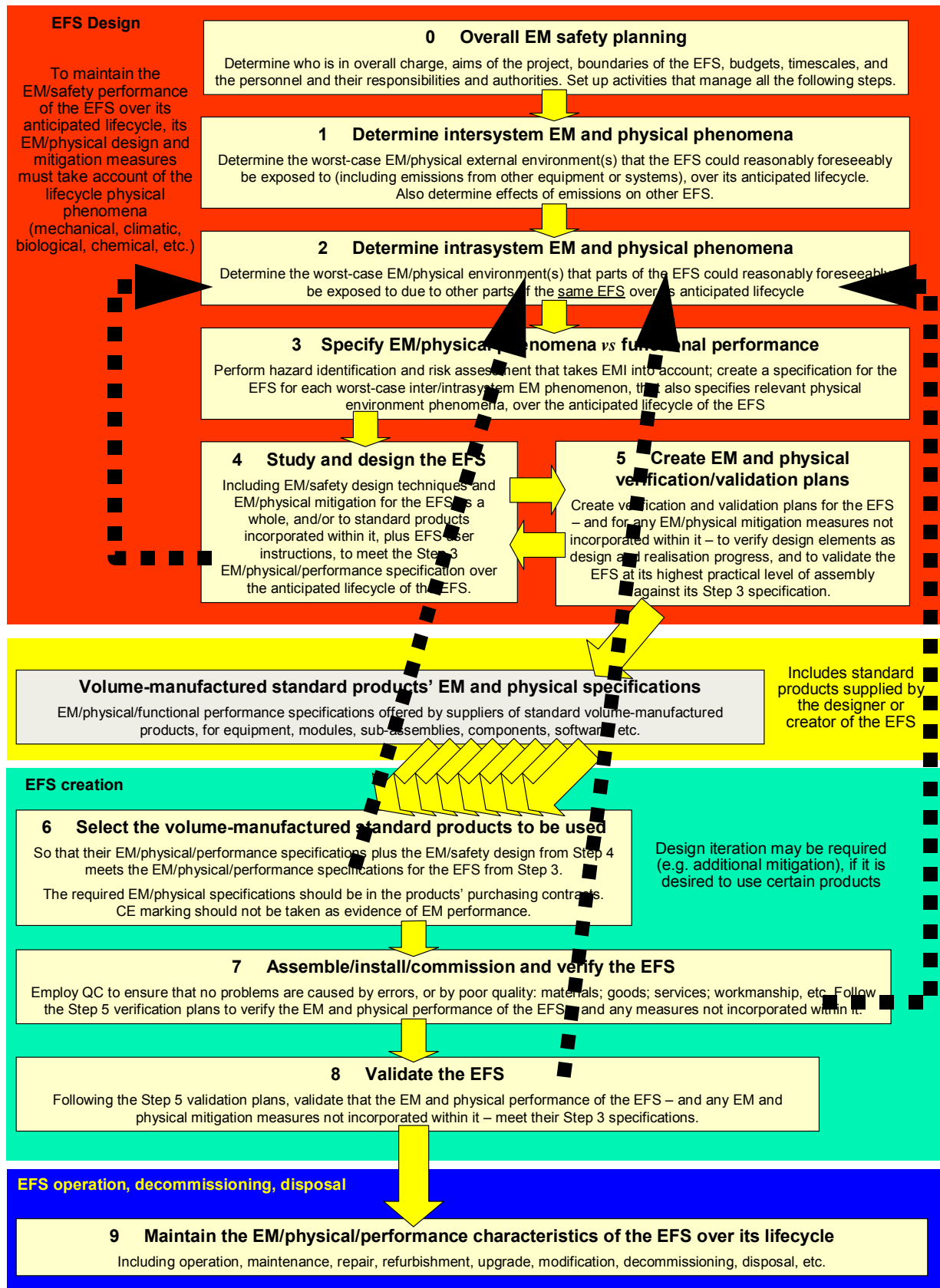


Figure 2.1 Iterative loops associated with determining intrasystem interference possibilities, for a Simple EFS

Overview of the EMC for Functional Safety process for a 'Complex' EFS

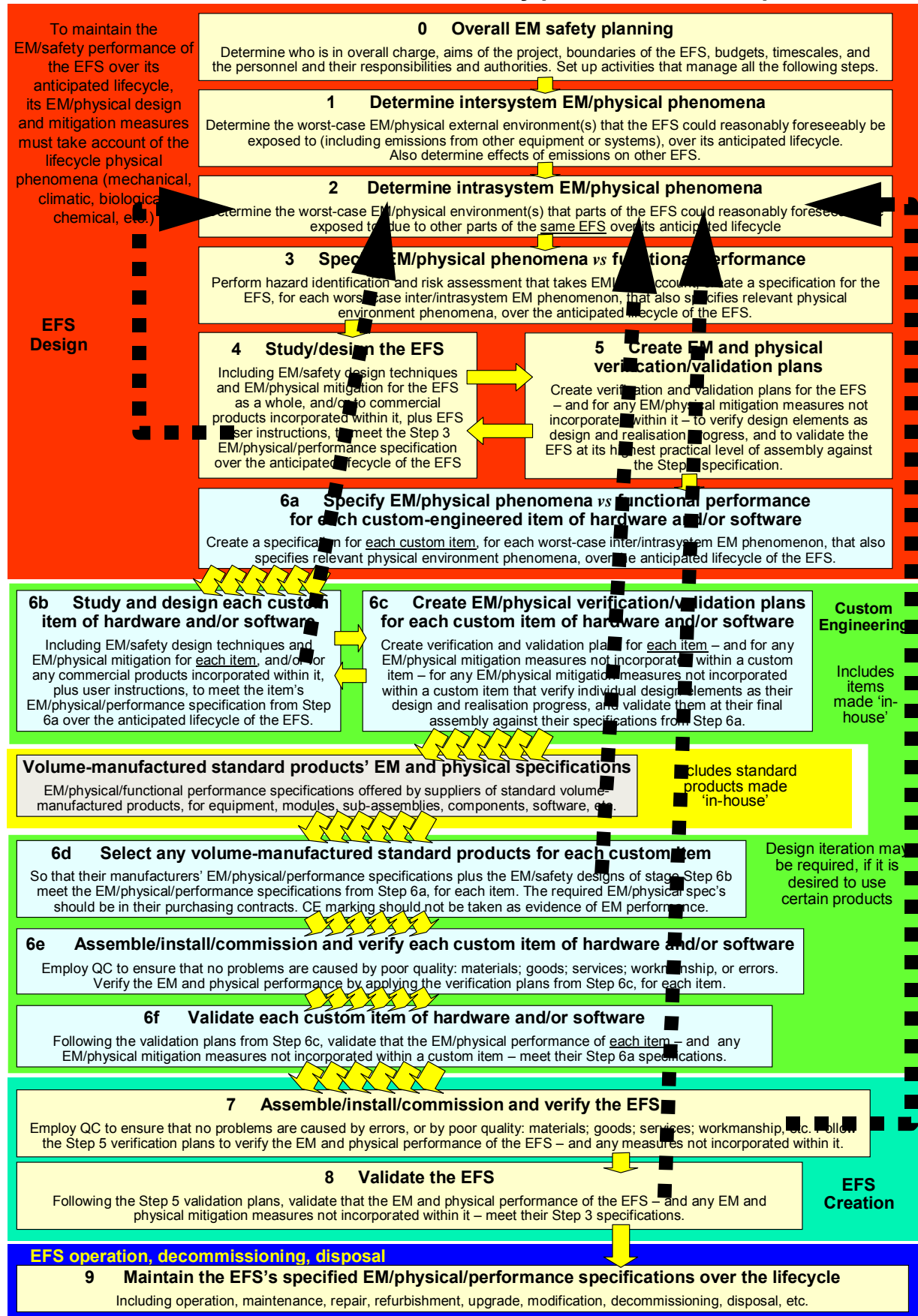
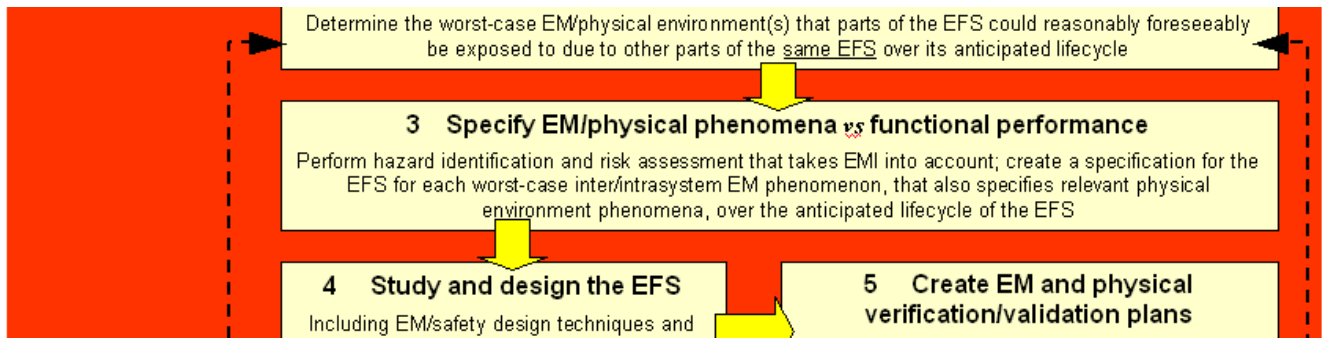


Figure 2.2 Iterative loops associated with determining intrasystem interference possibilities, for a Complex EFS

3. Step 3: Specify EM/physical phenomena vs functional performance

Perform hazard identification and risk assessment that takes EMI into account; create a specification for the EFS for each worst-case inter/intrasystem EM phenomenon, that also specifies relevant physical environment phenomena, over the anticipated lifecycle of the EFS



3.1 Introduction

No EMC or safety standard can ever specify exactly what is required for a given EFS, because to be adopted as international it must inevitably adopt a general approach and strike a balance between under-engineering and over-engineering, often called a technical/economic compromise. Competent engineers should carefully assess each EFS with respect to its operational situations.

This Step in the EMC for Functional Safety process creates an 'EMC safety specification' that helps a given EFS achieve acceptable levels of safety risks, or risk-reductions. It is also part of a process that helps ensure the amount of safety engineering is just right, so that under- and over-engineering is avoided.

Steps 1 and 2 assessed the worst-case EM and physical environments over the anticipated lifecycle. The outputs from these Steps are specifications for the worst-case EM and physical environments. Where appropriate, it can help to base these specifications on existing standards (such as the DEF STAN 59-411, MIL STD 461F, IEC 61000-4 or IEC 60721 series), competently modified as necessary. Doing this can make it easier to verify and validate the design by testing, in Steps 7 and 8, because test laboratories and equipment hire companies (and many manufacturers) will already have much of the equipment and expertise necessary to apply those test methods.

This Step is concerned with creating the EMC safety specification for the EFS, which will include both EM and physical specifications, and upon which Steps 4 and higher depend.

Where an EFS creator subcontracts part of the design, the subcontracted item requires an Item Requirement Specification (IRS) that helps to ensure that the overall EFS complies with its EMC safety specifications, see 6.2 and 6.4.

3.2 EMC Safety Requirements

Appropriate hazard identification and risk analyses should be performed for all types of EFS. These analyses should include consideration of EMC as a possible source of risk. Risk-reduction measures should be applied where necessary.

Appropriate EMC safety requirements should then be identified and recorded, for each EFS.

Where necessary, these EMC safety requirements could include information relating to:

- The electromagnetic, physical and climatic environments
- EMC performance requirements
- Arrangements for ensuring adequate EMC performance over the lifecycle

In the case of EFS that are safety-related systems as defined by IEC 61508 [7] these EMC safety requirements should be expressed as part of the Safety Requirement Specification (SRS). There are equivalent provisions in sector-specific implementations of IEC 61508. The EMC safety requirements should be a sufficient basis for handling EMC functional safety issues throughout the following stages of the EFS's lifecycle.

It is not the purpose of this Guide to provide in-depth understanding of how to do hazard analysis and risk assessment. Some hazard identification and risk assessment methods are listed in 3.7, and some pointers on how to apply them in connection with this EMC for Functional Safety process are given in 4.2. Annex B provides an overview of EM phenomena and how they can interfere with electrical, electronic and programmable electronic equipment.

3.3 Accounting for uncertainties

The EM and physical threat specifications will need to be higher than the actual environmental threats by a 'margin' that takes care of the various uncertainties in assessing the environments. This margin is known as the 'expanded uncertainty'. In general, the lower the level of safety risk, or the higher the amount of risk-reduction required, the greater the margin that is required to have sufficient confidence that the EMC safety requirement specification actually covers the real-life EM and physical environments over the lifecycle.

For example, MIL-STD-464 [19] employs a 6dB margin above the environmental specification for safety-critical and mission-critical equipment, and a 16.5dB margin for ordnance (missiles, bombs, etc.).

Note that we are not trying to achieve a given level of safety risk, or amount of risk-reduction, by simply testing with EM or physical phenomena at a higher level, because this approach does not work. Whatever level of safety risk, or amount of risk-reduction, is required for an EFS, the EM and physical environments it has to function in over its lifecycle are the same, and testing at higher levels than can occur in the environment is irrelevant.

What we are doing here is allowing for the uncertainty in our environmental assessments, to help us achieve the level of risk, or risk-reduction, required in real-life operation.

Steps 1 and 2 should have assessed the uncertainty when assessing their EM and physical environments (see 1.3.8 and 1.4.3). In some cases they may have specified maximum levels that cannot be exceeded for some fundamental reason, but in others they may have specified levels based on measurements, which include some uncertainties.

So when setting the EM and physical specifications to be used as the basis for the design and its verification, the specified levels should be increased by the appropriate 'margin' for each environment specified by the EMC safety requirements.

There are standard methods for adding together various types of uncertainty, taking their type of statistical distribution into account, for example [52]. Taking the example of an environment specification, EM or physical, based upon a very long term and thorough programme of measurements: the measuring transducers, instruments and their interconnecting cables all suffer from measurement uncertainty, even though they are fully calibrated at the recommended intervals. There will also be a quantifiable uncertainty due to the way the measurements were made.

Assuming that the statistical distribution of the total measurement uncertainty has a symmetrical distribution, the result is that the actual maximum value in the environment is likely to be 50% higher than the measured value (it is also likely to be 50% lower).

Assuming a 'Normal' (Gaussian) distribution – increasing a level by one standard deviation (σ) improves the confidence that the specification reached/exceeded the *actual* value of the environment to 68%. Increasing by three standard deviations (3σ) improves it to 99.7%, and four standard deviations (4σ) achieves 99.99%.

To avoid specifying very high levels, with their attendant risks of over-design and unnecessarily high costs, it is important to use techniques that achieve low levels of uncertainty, when assessing the environment during Steps 1 and 2.

3.4 Two types of risk assessment are required

During the initial stages of a project, before anything has yet been designed, it is necessary to determine the 'EMC Safety Requirements' described in 3.2 to guide the rest of the stages. But since the hardware and

software of the EFS will not yet have been designed, detailed risk assessments like FMEA, Fault Tree, etc. cannot yet be applied. An **'Initial Risk Assessment'** is required.

The hazards that could be created by the EFS are determined, and (once the EM/physical environment(s) have been assessed, see Steps 1 and 2) an overall risk assessment establishes the likelihood (probability) of the hazards occurring due to EMI. Those probabilities are compared with what is considered to be acceptable, and decisions made about EMI-related risk levels and risk reduction, creating the 'EMC Safety Requirements' discussed in 3.2.

These EMC Safety Requirements will eventually be used for the final validation of the EFS, in Step 8, once it has been designed, developed, and realised (including manufacture, integration, installation, commissioning, etc., as appropriate to the type of EFS).

Some of the methods mentioned in 3.7 will be found to be useful in the process of creating the Initial Risk Assessment.

During actual design/development/realisation stages (Steps 4 to 7 in this Guide, see Figures 0.2 and 0.3), a great deal of very detailed information will become available on all of the mechanics, hardware and software. Other techniques, such as some of those listed in 3.7, *should be applied to this data as it becomes available*, to guide the design, development and realisation stages (and their on-going verification) *in real-time*, to help achieve the overall goals of the Initial Risk Assessment.

In this way, the Initial Risk Assessment will accumulate more depth of analysis, eventually producing, at the end of the project, the **'Final Risk Assessment'**.

It is important to understand, as 3.5 makes clear, that risk assessment is an embedded and essential part of the design, development and realisation processes. Risk assessment is an iterative process that helps determine whether a particular aspect that is being worked on at a given time, will (or will not) help achieve the goals of the Initial Risk Assessment. It is not something one does at the end of a project, just to complete the documentation.

For example, where the risk assessment shows that the design of a particular piece of hardware or software will not achieve the levels of risk, or risk-reduction required, then steps should be taken to modify its design so that it will. For reasons of cost-effectiveness, it is very important that such design iterations take place while the design is unrealised (i.e. not yet manufactured).

The Final Risk Assessment becomes a very important part of the safety documentation of a project, and of course can only be available when the project has been completed. But the process of *creating* it, during the actual design, development and realisation activities, is the important thing that enables the achievement of the desired levels of risk (or risk-reductions) whilst also achieving cost and time savings, or at least not adding significantly to the costs or timescales.

3.5 Hazard analysis and risk assessments are 'live' documents

A hazard analysis and risk assessment is a 'live' document that should guide the project throughout its conception, design, development, manufacture, installation, operation, modification, etc. – indeed throughout its entire lifecycle (see Figure 0.4) – as the design, marketing and customer expectations change, obsolete components are replaced, improved manufacturing techniques adopted, etc.

Correspondingly, it is necessary to revisit the hazard and risk analysis during the lifecycle, whenever changes or modifications are proposed.

3.6 Emissions specifications are also needed

EMC for Functional Safety is not only about immunity to the EM and physical environments. Emissions from new equipment, systems, etc., could interfere with existing EFS and increase their safety risks.

The emissions specifications for the new EFS depend on the EMC for Functional Safety characteristics of the existing EFSs, according to what is covered by the steps in the EMC for Functional Safety process described in this Guide. Where appropriate data doesn't exist for the existing EFS, on-site immunity tests may be required to establish the emissions limits for the new EFS.

3.7 Some hazard analysis and risk assessment methods

3.7.1 Some standardised methods

These are methods for which IEC standards exist, but it is not an exhaustive list. There are also appropriate standards produced by other standards bodies, both international and national, but these are not listed here.

IEC 60300-3-9 is a guide to the risk assessment of technological systems.

Here is a brief summary of some standardised risk assessment methods, mostly taken from IEC 61508 Part 7 Annex B and C [7]. See IEC 60300-3-1, IEC 60300-2-9, and IEC 61508 Part 7 [7] for more information on these methods, and further useful references.

Failure modes and effects analysis (FMEA) (IEC 61508-7, clause B.6.6.1)

A widely used method that analyses a system design by examining all possible sources of failure of a system's components, then determines their effects on the system's functional safety. Sometimes called 'Hardware FMEA' – see below for 'Functional FMEA', this is a 'bottom-up' (consequence) method.

Reference standard: IEC 60812:1985, Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA).

Failure modes, effects and criticality analysis (FMECA) (IEC 61508-7, clause B.6.6.4)

Analyses the criticality of components that could result in injury, damage or system degradation through single-point failures, in order to determine which components might need special attention and necessary control measures during design or operation.

It is vital not to confuse the Criticality value with Safety Risk. Risk is assessed for harmful outcomes, with all causes taken together: Criticality is only relevant to individual failure modes.

Sometimes called 'Hardware FMECA' – see below for 'Functional FMECA', this is a 'bottom-up' method.

Reference standards: Design Analysis Procedure for Failure Modes, Effects and Criticality Analysis (FMECA). Aerospace Recommended Practice (ARP) 926, Society of Automotive Engineers (SAE), USA, 15 September 1967.

IEC 60812:1985, Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA).

Event tree analysis (IEC 61508-7, clause B.6.6.3)

Models, in a diagrammatic form, the sequence of events that can develop in a system after an initiating event, and thereby indicate how serious consequences can occur. A bottom-up method. Reference: IEC 60300-1, Table 2

Fault tree analysis (FTA) (IEC 61508-7, clause B.6.6.5)

Helps to analyse events, or combinations of events, that will lead to a hazard or serious consequence. A top-down method, that uses graphical techniques. Reference: IEC 61025:1990, Fault tree analysis (FTA).

Fault insertion testing (IEC 61508-7, clause B.6.10)

Introduces or simulates faults in the system hardware and documents the response – a qualitative method of assessing dependability. This is a 'bottom-up' method that uses a multidisciplinary team. Reference standard: IEC 61069-5:1994, Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 5: Assessment of system dependability.

Hazard and Operability Study (HAZOP) (IEC 615408-7, clause C.6.2)

A systematic study of deviations from design intent, that can be applied at equipment, system & plant levels. Documented record can help to demonstrate that good safety practice has been applied. Reference standard: IEC 61882:2001, Hazard and operability studies (HAZOP studies) – Application guide

Markov models (IEC 61508-7, clause C.6.4)

Evaluates the reliability, safety or availability of a system based on its failure states. Suitable for modelling multiple systems in which the level of redundancy varies with time due to component failure and repair. A 'bottom-up' method. Reference standard: IEC 61165:1995, Application of Markov techniques.

NOTE: See clause B.1 of IEC 61508-6 for a brief comparison between this technique and reliability block diagrams, in the context of analysing hardware safety integrity.

Reliability block diagrams (IEC 61508-7, clause C.6.5)

Diagrammatically models the set of events that must take place, and conditions that must be fulfilled, for a successful operation of a system or a task. A 'top-down' method. Reference standard: IEC 61078:1991, Analysis techniques for dependability – Reliability block diagram method.

NOTE: See clause B.1 of IEC 61508-6 for a brief comparison between this technique and Markov Modelling, in the context of analysing hardware safety integrity.

3.7.2 Some well-established but non-standardised methods

Here is a brief summary of some *non-standardised* risk assessment methods, which are nevertheless considered good safety engineering practice, mostly taken from IEC 61508 Part 7 Annex B and C.

See IEC 60300-3-1, IEC 60300-2-9, and IEC 61508 Part 7 for more information on some of these methods, and further useful references. Textbooks and/or Web searches may be required for some of the other methods.

Functional FMEA, and Functional FMECA

These methods are similar to 'Hardware FMEA' and 'Hardware FMECA', but analyse systems or processes instead. They start from a functional description of the system – which can be available at the Concept stage – even before there are any ideas of how the functionality could be achieved in hardware.

It is vital not to confuse the Criticality value with Safety Risk. Risk is assessed for harmful outcomes, with all causes taken together: Criticality is only relevant to individual failure modes.

Cause consequence diagrams (IEC 61508-7, clause B.6.6.2)

Models, in a diagrammatic form, the sequence of events that can develop in a system as a consequence of combinations of basic events. Can be considered a combination of the Fault-Tree and Event Tree methods, so combines deductive (top-down) and inductive (bottom-up) methods.

Reference: The Cause Consequence Diagram Method as a Basis for Quantitative Accident Analysis. B. S. Nielsen, Riso-M-1374, 1971.

Ishikawa diagrams (also known as fishbone diagrams)

A technique for trying to determine the causes of a particular event or hazard. Often called a brainstorming method, which is incorrect unless appropriate steps are taken to prevent peer pressure, and the other attributes of real brainstorming methods are also applied.

Common cause failure analysis (IEC 61508-7, clause C.6.3)

Determines potential failures in multiple systems or multiple subsystems which would undermine the benefits of redundancy, because of the appearance of the same failures in the multiple parts at the same time. A bottom-up method.

Monte-Carlo simulation (IEC 61508-7, clause C.6.6)

Simulates real world phenomena in software using random numbers. A general principle is to restate and reformulate the problem so that the results obtained are as accurate as possible rather than tackling the problem as initially stated. A bottom-up method.

Time Petri Nets (IEC 61508-7, clause B.2.3.3)

Models relevant aspects of the system behaviour and to assess and possibly improve safety and operational requirements through analysis and re-design. A bottom-up method.

Worst-case analysis and Worst case testing (IEC 61508-7, clauses B.6.7 and B.6.9)

Worst-case analysis uses unfavourable combinations of environmental conditions and component tolerances to predict the effects of environmental and other extremes. Worst-case testing tests the cases specified during worst-case analysis. A bottom-up method.

Expanded functional testing (IEC 61508-7, clause B.6.8)

Analyses the behaviour of the safety-related system in the event of rare or unspecified inputs to try to reveal failures during the specification and design and development phases. A bottom-up method.

DELPHI

A 'brainstorming' technique that can help foresee hazards. No references at present. SWIFT and HAZOP are also brainstorming techniques.

Structured What-If Method (SWIFT)

A brainstorming-based method similar to HAZOP, using prompts to explore the behaviour of a system and identify hazards. It addresses systems and procedures at a high level, and hence is often applicable to novel problems in different fields.

It considers deviations from normal operations identified by brainstorming, with questions beginning "What if...?" or "How could...".

The brainstorming is supported by checklists to help avoid overlooking hazards, and is sometimes extended into a DELPHI analysis. There is no single standard approach to SWIFT – one of its strengths is that it is flexible, and can be modified to suit each individual application. Its success relies upon the experience of the personnel involved. No references known at present.

Incident Reviews

One of the best ways of identifying possible Hazards is to look at previous accidents and incidents. These might be for the system itself or for similar systems used elsewhere. Often, data reporting systems are sketchy and this makes them imperfect for estimating rates of occurrence. But they are still very valuable for the purpose of identifying that a particular Hazard is possible.

Task Analysis and Hierarchical Task Analysis (HTA)

There are several types of Task Analysis methods. They work out not only the obvious jobs defined in the operator and maintainer procedures, but also the undocumented practices. The most common technique is Hierarchical Task Analysis (HTA) but there are several others.

Human Reliability Analysis (HRA)

After Task Analysis, a technique such as Human Reliability Analysis (HRA) is usually used to determine...

- What can go wrong in performing the task
- What are the consequences of each mistake
- How likely each mistake is to occur

There are several models, which are used to estimate the error probability and these take account of factors such as...

- Complexity of the action
- Level of training
- Level of experience
- Anxiety factor
- Time available to conduct the action
- Environmental conditions
- Usability of the Man/Machine Interface (MMI)

Don't think that human error is always reduced or eliminated by computer control or automation. This merely puts the human interface further back in the process. Automated or computerised systems are only as good as the people who specify design, make, test and install them.

PHA (Preliminary Hazard Analysis)

A bottom-up method.

Fault Simulation for Control Systems

A bottom-up method.

MOSAR (Method Organised for a Systematic Analysis of Risks)

Guide on EMC for Functional Safety

Function Analysis and Hazard & Consequences Analysis

Hazardous Scenario Analysis (HAZSCAN)

Master Logic Diagram

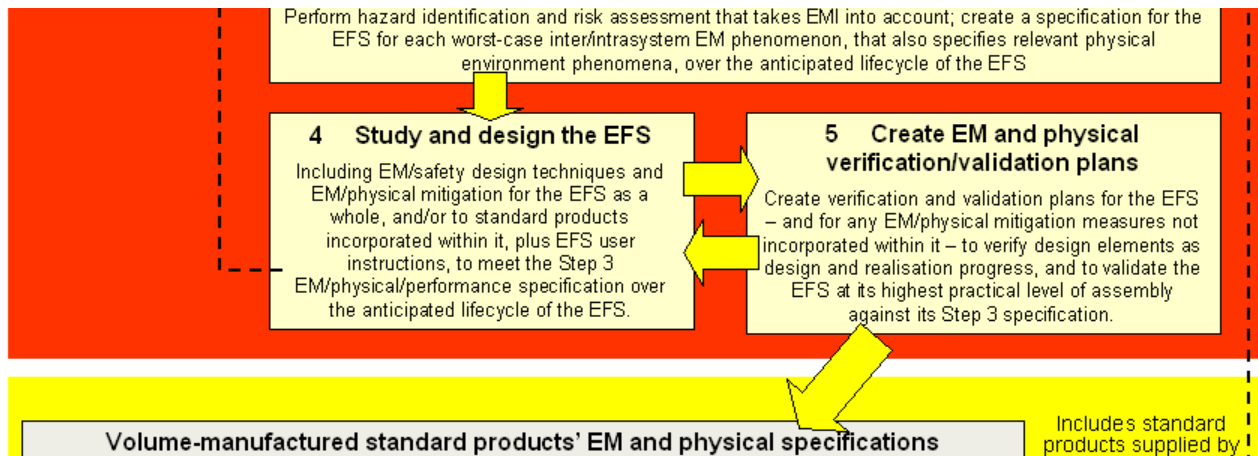
3.8 Iterations

As has been described in 1.6 and 2.5, the EM and physical environment specifications can (and often do) change during a project, and this means that Steps 1-3 are iterative, and the EMC Safety Specifications resulting from Step 3 will often change during the life of a project.

The management of the EFS project should facilitate this process, so that the EFS always achieves its safety risks (or risk-reductions) in the EM and physical environments that actually occur during the operation, decommissioning and disposal stages of its lifecycle.

4. Step 4: Study and design the EFS

Including EM/safety design techniques and EM/physical mitigation for the EFS as a whole, and/or to standard products incorporated within it, plus EFS user instructions, to meet the Step 3 EM/physical/performance specification over the anticipated lifecycle of the EFS.



4.1 Introduction

4.1.1 General principles

It is important to ensure that EFS do not become unsafe as a result of EMI due to their EM environment (including EMI they create themselves).

It is also important to ensure that the EM emissions from a new EFS (or part of it) does not cause safety risks by interfering with existing EFSs.

Accordingly, it is the responsibility of the EFS designer (which may be a team of people) to apply appropriate EM/physical measures throughout the lifecycle of the EFS.

Where it is not within the authority of the designer to apply a certain measure (e.g. repair of an EFS after it has been sold to another company), the designer should provide appropriate and clear instructions on what should be done, and by whom, with clear warnings about the potential consequences for safety risks (or risk-reductions) of failing to follow them.

In most cases, mass-produced electrical, electronic or programmable electronic products and other devices and interconnections that are often used to assemble an EFS, cannot be expected to have EM emissions and/or immunity characteristics that are adequate for all of the possible EM environments that an EFS might experience. Therefore, it is important to recognise that EM measures applied at the level of the equipment, system and/or installation are often an effective way to achieve the required EM characteristics and hence safety.

The aim of this section of the Guide is to provide an overview of some of the measures and techniques that are available for the achievement of functional safety with regard to EMI. It cannot tell you how to design an EFS, because each EFS and its application and EM/physical environment is so different. Instead, it discusses the major design issues and some techniques by which they may be addressed.

Whilst this Step describes many design techniques, it is not comprehensive and there are other techniques that could be equally effective. The following is just a list of some techniques that have been found useful in the past, and there is no obligation to use all or any of them. Some of these techniques might not be suitable for some types of EFS.

How the EFS designer ensures that the desired levels of safety risks (or risk-reductions) are achieved over the anticipated lifecycle is entirely up to him or her.

4.1.2 How this Step fits into the process

Step 3 in this EMC for Functional Safety process (see Figures 0.2 and 0.3) produced a specification of EFS functions versus parameters for the reasonably foreseeable worst-case EM and physical phenomena that EFS could experience, which it called the EMC safety requirements.

Sometimes two or more EM and/or physical phenomena could occur at once, although it is generally (but not always!) unlikely that they will all be at their worst-case levels when they do.

Step 3 also produced the hazard analysis and risk assessment – a ‘live’ document that will guide the project throughout its conception, design, development, manufacture, installation, operation, modification, etc. – over its entire lifecycle (see Figure 0.4), as the design, marketing and customer expectations change.

This Step 4 is concerned with designing EFS to achieve the required levels of safety risk, or risk reduction, given the inputs from Step 3.

For a ‘Complex’ EFS (see 0.9 and 6.2) the process described in Figure 0.3 applies, and each custom-engineered item will require an Item Requirement Specification (IRS) derived from the EMC safety specification of the EFS and the actual design of the EFS. IRSs are described in 6.4.2.

Figures 0.2 and 0.3 show Steps 4 and 5 as interacting with each other (arrows in both directions). It can be possible to avoid lengthy and expensive verification and validation programmes by doing the design in a different way, and employing certain verification and validation techniques can sometimes allow design to proceed faster, or lower-cost parts to be used.

4.2 Designing to achieve the EMC safety requirements

4.2.1 Appropriate methods of Risk Assessment

As described in 3.4, An ‘Initial Risk Assessment’ is performed during the early stages of a project, to determine the ‘EMC Safety Requirements’ (see 3.2) that guide the rest of the project and will eventually be used for the final validation of the EFS, in Step 8, once it has been designed, developed, and realised.

During the actual design/development/realisation stages covered by Steps 4 to 7 of the process described by this Guide, a great deal of very detailed information will become available on all of the mechanics, hardware and software. Detailed Risk Assessment techniques, such as some of those listed in 3.7, should be applied to this information *as it becomes available*, to guide the design, development and realisation stages (and their on-going verification) *in real-time*, to help achieve the overall goals of the Initial Risk Assessment.

Eventually, when Step 8 is complete, these detailed Risk Assessment activities will produce the ‘Final Risk Assessment’.

No standard hazard assessment and risk analysis methods have yet been developed for use with EM disturbances. So it will be necessary to choose which methods to use, and to adapt them accordingly (see 4.2.2 and 4.2.3). Where there is a defined customer, they should be asked if they prefer certain methods to be employed.

There is no standard, correct and formal way to analyse system safety: there is always the need for human judgement. What is required is an ordered approach to consider and document safety during design. The assessment should be systematic but there is no guarantee that the analysis will be 100% effective and complete, so there is always the need for competency and expertise to improve the ‘coverage’ of the analysis as far as is possible.

‘Inductive’ methods (sometimes called ‘consequence’ or ‘bottom-up’ methods), such as Failure Modes and Effects Analysis (FMEA) or Event Tree Analysis (ETA), are described in section 5.4 of IEC 60300-3-1. They generally start with a low-level error or failure, for example in a resistor or capacitor, and try to determine whether it could lead to a hazardous situation.

‘Deductive’ methods (sometimes called ‘causal’ or ‘top-down’ methods), such as HAZOP or Fault Tree Analysis are described in section 5.3 of IEC 60300-3-1. They start with the hazardous situations and try to determine what could have caused them.

‘Brainstorming’ techniques identify all kinds of possibilities, then determine whether they could increase any risks. If the result is undesirable, the causes of the originally brainstormed possibilities are then determined to see what could cause them and help identify the risk level. Examples of established brainstorming

methods exist. Although they may not be directly applicable to some applications, their *approaches* may still have some value.

As a result, it is usually recommended to employ at least one inductive and one deductive method to improve the accuracy of the hazard and risk assessment. For this reason FMEA and HAZOP-like techniques are often used together on projects. Another common pairing is Fault-Tree Analysis (FTA) with Event Tree Analysis (ETA). 'Brainstorming' is always recommended, to help identify faults and foresee use/misuse that would otherwise be overlooked.

Some safety engineers call hazard analysis 'hazard identification' instead, and some treat it as a separate technique to risk assessment. But it is beyond the scope of this Guide to go into this level of detail.

No foreseeable hazards are to be excluded from an analysis. The risk associated with each *possible* hazard is quantified and compared with the acceptable risk level. If the risk is low enough this then allows us to ignore the associated hazard.

The hazards assessment and risk analysis is an iterative process that should start early in a project, to guide initial design choices, and be kept up to date throughout a project as the design or marketing changes.

New hazards or risks might arise as the design or marketing changes during a project, and these should be identified and their risks assessed.

All foreseeable hazards should have their risks analysed at every iteration of the hazard/risk assessment, even where the hazards were considered negligible at the previous iteration, because changes to the design or marketing might increase their risks.

It is important to use a modern, 'open' method to identify possible hazards, but a safety study should consider hazards identified by any means: previous incidents; checklists; design reviews; task analysis; etc. Whatever techniques are used, good hazard identification depends on experience and imagination. Unfortunately, many manufacturers apply hazard analysis and risk assessment methods in a 'rote' or mechanical way, just to put a tick in a management procedure box, a practice that functional safety experts warn against [53] [54].

4.2.2 Common but incorrect assumptions in Risk Assessment

It is often incorrectly assumed that only single faults (and any other faults that arise as a direct result of the original fault) need to be considered, because the possibility of multiple independent faults is too remote. In fact, how many independent faults must be considered depends entirely upon the level of safety risk, or degree of risk reduction that is required, plus the probabilities of each failure occurring.

For example, if there were ten independent faults that could each cause a particular hazard to occur, and if each had a probability of occurring once in every 100 years, then we would expect the hazard to occur once every 10 years on average. This may be too often to be acceptable for a particular EFS.

Another example: in a particular design four independent faults would have to occur before a hazard could occur. If each fault was random and could occur once in every year, then we would expect the hazard to occur on average once every four years, which may be unacceptably soon for a given EFS.

So, we cannot simply assume that we only have to consider 'single-fault safety'; each hazard must be assessed on the probability arising from all the possible faults that could contribute to creating it.

Another common and often incorrect assumption is that failures occur at random (as in the above two examples). In fact many of the faults in electronic and programmable technologies are reliably triggered by certain EM and/or physical events, or sometimes simply by unanticipated combinations of perfectly correct inputs. These are called 'systematic' faults, and the only way to prevent them is by careful design and appropriate verification and validation techniques (not necessarily based on testing).

For example, a reliable ground bond is necessary for the correct operation of a particular electronic steering power assistance system, which replaces the more common hydraulic power steering system. The driver's operation of the steering wheel sends electronic signals to a microprocessor, which in turn operates electrical motors that provide assistance to the driver as they turn the wheels of the vehicle.

In power-assisted steering systems in vehicles, the power-assist function provides more torque to the mechanical steering system than the driver.

If the electrical power assist system malfunctions in a mode that simply ceases to provide any power assistance, this is often thought to be 'fail-safe' but it is not, because the driver may not react to this totally unexpected situation in time (assume at least three seconds), and also because the driver may not be strong enough to steer the vehicle adequately without the power assistance (e.g. elderly people). But programmable electronics can malfunction in unexpected ways, which could result in the steering assistance trying to steer the vehicle in random directions despite the intentions of the driver, clearly increasing safety risks very considerably.

In this example the ground bond uses a copper crimp tag that is bolted with a steel screw to the steel chassis (ground) of the vehicle. This construction might be expected to have a particular reliability, based on mechanical considerations taking component parameters and their tolerances, manufacturing tolerances (e.g. assembly torque), and the vibration environment into account.

If a manufacturer tested a new type of vehicle with such a ground bond by driving it for hundreds of thousands of miles in a wide range of climatic conditions over a period of a few months, he might conclude that the reliability of the ground bond was perfectly adequate given the anticipated mileage over the expected lifetime of the vehicle, and the number of vehicles expected to be manufactured (which of course relates to the number of people exposed to the hazard).

But the design of the ground bond is such that galvanic corrosion can be expected to occur due to its dissimilar metals, and after a few years it can be assumed that most of them will have become high-impedance. The original assumptions of ground bond reliability and their 'proving' by road testing will be wrong, probably by at least two orders of magnitude, depending on the amounts of salt used to prevent icing on the roads.

In fact, this is not a real-life example – we expect established motor manufacturers to know about galvanic corrosion by now – after decades of experience with it, but this sort of issue – where an environmental threat is not recognised and so not designed for, can make a mockery of any hazard and risk assessment, no matter how thorough it was in other areas.

Yet another incorrect assumption is that failures or faults are permanent, when in fact they can be as temporary as an intermittent connection or transient EMI event, or momentary change in some parameter, that causes a delayed, degraded, distorted or false signal. The terms 'failure' and 'fault' need to be extended to include all undesirable events, and should not be assumed to mean (for example) simply all-or-nothing events such as permanent short-circuits or open-circuits.

Some EM/physical events can cause what is known as common-cause or common-mode failures. For example overheating and/or overvoltages on the electrical power supply can cause two or more ICs to malfunction at the same time. Electrical transients, high temperatures, and ionising radiation can all conspire to cause ICs and other semiconductors to 'latch-up', in which state *all* of their inputs and outputs can assume fixed and undesirable levels, and correct operation can only be recovered by cycling the power to the device (assuming the device has not been overheated by unrestricted power supply current during its latch-up).

Reasonably foreseeable use/misuse is another very important issue that must be taken fully into account during brainstorming. Safety design should *never* assume that someone would never do anything because it would be 'too stupid' (or that they would not be able to successfully sue the manufacturer if they did, and suffered an accident as a result!).

4.2.3 How to include EMI and intermittencies in the Risk Assessment

As traditionally practiced, the techniques described in 4.2.1 are of limited effectiveness for the EM issues that this Guide is concerned with. Taking 4.2.2 fully into account will go some way towards making them more effective, but to be useful for EMI the techniques must fully take into account the EM/physical environment specifications resulting from Steps 1 and 2, plus the fact that in inadequately designed and/or protected hardware, software (including firmware) and interconnections, EMI can cause:

- Degraded, distorted or false signals to appear at each inadequately protected port of one component of an EFS. Depending on the type of EMI they can appear individually, to just one port at a given time, but similar or widely different degraded, distorted or false signals can also appear at two or more, or all of the component's ports at the same time.
- Similar or different degraded, distorted or false signals to appear at one or more inadequately protected ports of two or more *different* components of an EFS at the same time. This is a very important consideration where redundancy is used to improve reliability of safety-related electronic technologies.

- In addition to an almost infinite variety of degraded, distorted, or false signals, EMI can cause two types of failure modes in inadequately protected EFS:
 - a) 'Latch-up' of semiconductor hardware devices (transistors, ICs, etc.)
 - b) 'looping' or 'crashing' of software and firmware in programmable devices.

Latch-up can cause some/all of a device's pins to assume uncontrolled static values at the same time. Latch-up is only recoverable by cycling the power (assuming the IC has not been damaged by the latch-up).

Software/firmware looping or crashing can be addressed with 'watch-dog' circuits that reset the device. Detection of looping may require very careful design or two or more watchdogs. In either case, operation of the watchdog will take from half to several seconds, maybe minutes in the case of a complex system that must be rebooted – and during that period the electronic technology is controlling the EFS incorrectly, and might even be outputting signals that increase safety risks.

NOTE: a 'port' is any interface between an electronic unit and other units or the world at large. A cable that enters or exits a unit is obviously a port, and most ports are associated with interconnections. But the enclosure of a unit is also a port and is exposed to a range of EM disturbances such as radiated EM near-fields and far-fields, electrostatic discharge (ESD), etc.

The EM characteristics of an EFS can degrade rapidly over time, if the equipment and interconnections that comprise an EFS are not designed to suit its physical environment, this issue should be taken into account in the risk assessment too.

Typical EMC and/or physical testing applies just one type of phenomenon at a time, but in real life many kinds of EM and physical events can (and do) occur simultaneously, creating combinations that can easily defeat simplistic design assumptions.

Intermittent contacts, and intermittent short-circuits and open-circuits, can also cause all three of the above types of events, and are significantly affected by the physical environment over the lifecycle.

All of the above can be totally prevented by the application of appropriate hardware EMI/physical protection measures, as discussed in 4.3 to 4.7 – but these might add cost, weight and size, or be unacceptable for other reasons. For example, most motor car manufacturers insist on using plastic-bodied connectors and loose bundles of unshielded wires, that can easily be assembled by relatively unskilled personnel, they will not accept shielded cables/connectors for anything but connections to radio antennas.

Where EMI/physical protection is partial or non-existent, the risk assessment process provides the information necessary to design the EFS so that it achieves adequately low safety risks or sufficiently high risk-reduction. The engineering techniques that can be used include those described in 4.3 to 4.7.

It can be difficult to adapt traditional inductive or deductive risk assessment methods to deal with the wide range of EM, physical and intermittency possibilities. This is the main reason why competent expertise should always be involved in such analyses, and also during brainstorming, to try to ensure that all reasonably foreseeable possibilities for EMI and intermittence to give rise to safety hazards have been thoroughly investigated and dealt with as appropriate.

4.2.4 Iterations

As has been described in 1.6, 2.5 and 3.8, the EM and physical environment specifications can (and often do) change during a project, and this means that Steps 1-3 are iterative, and the EMC Safety Specifications resulting from Step 3 will often change during the life of a project.

Changes in the EMC Safety Specifications mean redoing the hazard and risk assessment – unless it is the case that the amplitude of an environmental parameter has reduced (e.g. a worst-case RF field strength or vibration amplitude), in which case there is no need to redo the risk assessment unless there is hope that the changes will result in cost savings.

The management of the EFS project (see 0.10) should facilitate this process, so that the EFS always achieves its safety risks (or risk-reductions) in the EM and physical environments that actually occur during the operation, decommissioning and disposal stages of its lifecycle.

4.3 Some design and development measures and techniques to be considered

4.3.1 Designing EFS architecture

It is important to design the architecture of the EFS to adequately reduce the probability of dangerous failures due to EMI. Appropriate design measures and techniques may include: fail-safe design; the use of parallel redundant channels; etc. [59] [7].

Important elements or circuits with regard to safety may be duplicated and connected in parallel or series as appropriate to help ensure acceptable safety risks (or risk-reductions) are maintained in case of failure(s).

It is recommended that each parallel (or series) element in an EFS should be designed in a different technology (for both hardware and software, e.g. architecturally different microprocessors, software languages that do not share a common heritage, software teams that do not share a common background, etc.) to help avoid more than one of them failing at the same time due to any given EM disturbance (common-cause failures, see 4.2.2).

4.3.2 Avoiding unsuitable components; and mechanical, hardware and software design techniques

Some components, circuit designs, mechanical and software design techniques are generally known to be especially susceptible to certain EM disturbances, or can be shown by analysis to be especially susceptible. Some may have been found by experience to be especially susceptible in particular applications.

Three examples: ceramic integrated circuits (IC) with metal 'lids' are much more susceptible to E-fields if their lids are not 'grounded' to the IC's 0V; bipolar ICs tend to be more susceptible to EMI than Bi-FET and CMOS amplifiers; on-chip memory is less susceptible to EMI than when data is fetched over a data bus from a separate IC.

Components, and mechanical, hardware and software design techniques that are known to be especially susceptible to EM/physical threats, should be avoided wherever practical. Where they are used, they will generally add significantly to the difficulties, hence costs and timescales, of creating an EFS that achieves the required levels of safety risk, or risk-reduction.

4.3.3 Choosing suitable components, and mechanical, hardware and software techniques

Some components and products, circuit designs, mechanical and software design techniques, are generally known to be especially resistant (more immune) to certain EM disturbances or physical effects, or can be shown by analysis to be especially resistant. Some may have been found by experience to be especially resistant in particular applications.

Using components, circuit designs, mechanical and software techniques that are appropriately resistant, given the EM and physical specifications for the EFS and the planned use of any EM and/or physical mitigation measures (see 4.3.11, 4.3.12 and 4.8), ease the EM safety design of the EFS.

Electromagnetic test standards for individual ICs are now being developed and published, so it may soon be possible to select ICs on the basis of their manufacturer's published EM characteristics data. Where the EM characteristics of an IC or other semiconductor is not known, it is usually possible to choose between competing parts by operating them in an evaluation mode and applying simple EM tests (for example using close-field or other types of probes to measure relative emissions or inject RF fields or transients).

As far as digital circuits are concerned, software techniques can be used to help ensure safe operation, for example:

- Digital information coding
- Error detection algorithms
- Error correction algorithms

Error correction works in such a way that, in the presence of a transient perturbation, the EFS can resume normal operation as signal errors are detected and corrected. This should be done without increasing the risks beyond acceptable limits. Also see 4.3.4.

The reliable operation of the EFS can also be improved through judicious software design and the design of its structure. In particular it should be able to account for the occurrence of errors caused by the action of EM disturbances (unexpected program jump, or change in operating instructions, address codes, etc.). A number of references to designing software to resist EMI are given in [56] to [62].

The same approach should be taken for components, circuits, mechanics, software and products that are custom-designed for use in EFS, even if they are manufactured by the EFS creator.

4.3.4 'Hardening' communications

As has been mentioned: as well as preventing semiconductor devices from operating correctly (e.g. by shifts in their DC bias levels) many kinds of EMI can distort or even mimic real signals. 4.2.3 discussed some ways by which signal errors can be taken into account in risk assessments.

Signals are, of course, the 'lifeblood' of electronic circuits (and also of software, since real-life software operation requires real signals to be passed between devices in real hardware) – so their possible distortion and mimicry due to EMI is of the most vital importance.

All conductors couple (interact) with the EM fields in their environment, and antenna theory shows that the longer the conductor the higher is the maximum possible level of interference that can occur at a lower frequency. So, in general, we find that the longer the PCB trace, wire or cable, the greater the susceptibility of the signal.

Wireless (radio) communications couple (interact) with the EM fields in their environment, because they *are* EM fields (see 4.3.6).

These unwanted interactions are very important issues when communicating signals, data and control using conductors (especially long cables) or wireless techniques.

Perhaps the best approach is not to use conductors or wireless communications at all. Optical communications, because of the way they couple (interact) with the EM fields in their environment, are generally a better choice when EMI is to be avoided. Optical communications include free-space line-of-sight, and fibre-optic (see 4.3.5).

At the moment, optical communications cannot be used to replace all copper or wireless interconnections. Optical fibres can now be embedded within PCB substrates to connect optical transmitters and receivers mounted on the PCB, and can replace the longer and/or higher-data rate conductors on the PCB. Some companies are working towards integrating optical transmitters/receivers within silicon ICs, which will interface with such embedded optical fibres, but such devices are not yet available so there are still copper interconnections required for signals, data and control.

Where conductors are to be used for communication of signals, data or control, either as PCB traces, wires or cables of any length – appropriate digital communication protocols can be used to help distinguish good signals, data and control from distorted or false signals due to EMI.

Analogue signals cannot be protected by such protocols, and instead must rely on EM mitigation techniques such as shielding, filtering, galvanic isolation and surge protection (see later). Alternatively, they can be converted to digital signals with a suitable protocol, which is an especially powerful and cost-effective technique where analogue signals would otherwise have to travel over long cables or via a wireless (radio) communication link.

A communication link with an effective EMI-protecting protocol is sometimes called a 'hardened' link. EMI hardening protocols can also be combined with security protocols, to create communications links that are hardened against interference, and also against eavesdropping.

There are two basic types of EMI-hardening digital protocols:

- a) **Detection methods:** detect whether each data packet has been corrupted, and if so request it to be resent.
- b) **Correction methods:** detect whether each data packet has been corrupted, and if so reconstitute the correct data.

Detection methods require a two-way communication link, and when the EM environment is benign they achieve the highest possible data rate. When the EM environment is harsh, no usable data at all might be communicated – the data rate might fall to zero.

Correction methods only require a one-way communication link, and each data packet is made larger by the addition of data that is used for reconstruction of the data should it become corrupted en route. When the EM environment is harsh, as long as the signal is received, it is possible for some types of protocol to reconstruct it, so the data rate is unaffected by the EM environment. But the extra length of the data packets means that a given link will have a slower maximum data rate, and the receiver must be more complex and hence more costly.

Within each of the above two types of digital communication protocol there are numerous variations, each one suitable for different cost/benefit ratios for different EM environments and different applications. For example, reliably communicating between two different items of equipment over a long cable or wireless link will require a different protocol from a microprocessor reliably fetching data from memory ICs over an address/data bus on a PCB.

For example, if a two-way communications link is available, a detection-type protocol might be acceptable if the worst-case EM environment could only reduce the data rate below normally-acceptable levels for acceptable periods of time. Suitable applications are those in which a hazard takes a while to occur, and the periods of low data rate are short enough.

A 'backstop' for such a scheme, in the event that the assessment of the EM environment was inadequate, or the cable or wireless link is broken physically, is to provide the receivers with timers that apply a 'fail-safe' override when a period of low or zero data rate has existed for too long (application dependent). Many modern industrial field busses safety-rated according to IEC 61508 [59], appear to operate on this principle. Of course, 'fail-safe' schemes are difficult to apply to life-support EFS.

At the other extreme, the MIL-STD-1553 data bus is an example of a real-time bus that is designed to continue to communicate valid digital data (whether used as data, signals or control) in the harshest EM environments. Commercial versions are available, but it is not a low-cost solution.

All conductive interconnections can be affected by sufficient levels of EM and/or physical threats, whatever error detection or correction methods are used, so failure detection with automatic switching to a reserve interconnection that follows a different route, or else safe shut-down, might be required (also see 4.3.21).

4.3.5 Using optical links instead of conductors

As discussed in 4.3.4, all interconnections are weak points. Optical communications are generally preferred to conductors or wireless links (see 4.3.6) for communicating signal, data and control in all applications, including on PCBs.

Providing their transmitters, receivers and optical paths are chosen/designed to survive the physical environments, optical communication links will have very much greater robustness to EM threats than conductors or wireless links carrying the same signals, data or control.

4.3.6 Using wireless links instead of conductors

Wireless links can be designed to be more reliable than conductors such as cables. All radio receivers are very frequency-selective and this helps reject a great deal of the noise caused by EMI. Short-range radio propagation paths are less susceptible to physical effects than cables.

However, wireless designs can be designed badly, for example it is important that even the worst-case levels of EMI do not drive receivers into clipping. One way to deal with this is to use receiver circuits that have a larger dynamic range, and this is commonly done in military receivers. Instead or as well, passive RF filtering may need to be applied between the passive antenna and the first active device in the receiver (including ESD protection devices).

Even very well designed receivers are very sensitive to EM threats in their RF 'channel', whereas poorly designed receivers can be susceptible over a much wider frequency range due to overload and intermodulation in their RF stages. Digital signals with error-correcting protocols can help make radio communications more robust, and spread-spectrum techniques can be designed to resist all but very broadband interference. MIL-STD-464 [19] describes how multiple transmitting/receiving antennas can be co-located, and identifies simulators that can help designers to avoid problems.

Frequency-agile wireless links, that detect and avoid strong interference frequencies, and communications protocols that do not mind multiple time-shifted reflections, are also ways by which wireless links can be made more resistant to EMI, although they will never be as robust as optical links.

4.3.7 Analysis and testing techniques that guide design

It helps achieve functional safety if the relevant EFS functions are constructed using components, circuits, products, mechanics and software that have been proven by testing to function as intended in the maximum foreseeable EM/physical environments as specified in Step 3.

Where this is not practical, the EFS can employ EM/physical mitigation (see 4.3.11 and 4.3.12), and some or all of the verification methods applied to the components or circuits that are thus protected might not need to be as severe as if they had to meet the overall specifications for the EFS.

Identifying the EM characteristics of items of equipment and/or their circuits or devices is an important technique that helps understand how EM mitigation measures (e.g. shielding, filtering, surge and ESD suppression, etc.) should be applied most easily and cost-effectively to achieve the required safety integrity in real life. An item of equipment (or a circuit or device) can be susceptible to its EM disturbances, such as demodulation, intermodulation between two or more signals, overvoltage, overcurrent or overdissipation.

There are a number of ways of performing the required analysis. Two methods are outlined below.

- a) Prior experience of identical items (or circuits) that use identical devices.
Note that a semiconductor that has had a mask-shrink or die shrink, or is packaged differently, is not an identical device as far as its EM characteristics are concerned. The experience should be based on measurements and documentation.
- b) Subjecting unprotected items (or circuits or devices) to EMC tests designed to fully determine their natural emissions and susceptibilities.
These emission and immunity tests can use any appropriate method and need not follow IEC standards, as long as the results can be meaningfully interpreted from the point of view of the EM characteristics of the finished equipment.
During these tests, the equipment (and/or circuits) should be free from all EM mitigation measures. That is, they should not use any shielding, filtering, surge or ESD protection, automatic shutdown, etc. 4.3.8 explores this technique in more detail.

NOTE: b) is generally preferred whenever there is existing hardware that can be tested, since it is very rare that two designs are truly identical in both hardware and software.

Similar techniques can be applied to determine the natural susceptibilities to physical stresses, to aid the physical design and mitigation of the EFS so that adequate EM characteristics are maintained over the anticipated lifecycle.

Electromagnetic measures required for the achievement of adequate functional safety should be evaluated using EM testing and highly accelerated life testing (HALT), to demonstrate that individual EM design aspects (e.g. circuit design, shielded enclosure design, filter design, design of surge transient or ESD protection, etc.) should reliably achieve the necessary EM characteristics over their reasonably foreseeable lifecycle.

Such tests should be carried out as early in a project as possible, to reduce technical risks and save time and cost. Some of them will not need to have a functioning unit available, for example the shielding effectiveness of a PCB-mounted shield, enclosure, cable or connector can be tested in isolation.

The EM/HALT testing should be based upon the EM and physical requirements specifications of the EFS, and can use any appropriate technique, so need not be limited to IEC standard methods, as long as the results can be meaningfully interpreted from the point of view of the EM characteristics of the finished equipment over its reasonably foreseeable lifecycle.

Comparison (relative) measurements of EM measurands, often based on un-calibrated close-field probes and similar measuring devices, during or else before-and-after HALT, might be all that is required in some instances.

NOTE 1 – HALT testing on individual elements of an EFS are recommended where that element is required to perform functions with a high level of integrity (high reliability). Adding EM tests to these HALT tests need not add a lot of extra cost or time if they are designed appropriately.

NOTE 2 – The HALT Test Plan should be designed by HALT experts, based on the physical environment specification of the EFS.

NOTE 3 – Other methods of assessing physical degradation could be used instead of HALT.

Where suitable data exists or can be calculated for a particular EM design aspect – and when it is fully documented in the project's records (not referenced, because references may become unavailable) – the above combined EM and physical testing may not be necessary. Alternatives to the above testing include:

- Manufacturer's data
For example, good gasket manufacturers perform a variety of tests on their products simulating a variety of lifecycle physical exposures.
Manufacturer's data can only be used where their parts are applied fully in accordance with the manufacturer's application instructions.
- Data from previous projects

This could be from design tests, or from documented experience of identical designs in identical physical environments.

4.3.8 Determining the 'natural' susceptibilities of hardware, software and firmware

Any EM phenomena at any frequency can interfere with hardware or software if its level is high enough – but all hardware and software is especially vulnerable (maybe as much as 40dB or more) at certain frequencies, related to resonances in its structures, circuits or loads; or to the rates at which certain electrical operations occur, such as a digital system's clock frequency and its harmonics [10]. The vulnerable frequencies of an EFS are its major limiting factors for immunity, so knowing what they are helps the EM design.

We can determine the natural frequencies at which hardware and software are especially susceptible by analysing, simulating, or testing an EFS (or parts of it) *with any EM mitigation measures removed*.

When the especially susceptible frequencies are known, we need to decide whether they could occur – with significant levels – over the lifecycle of the EFS. Direct interference, demodulation, and intermodulation should all be taken into account (see Figure 1.2).

For example, if a circuit is especially susceptible to 1MHz, it might seem that using shielding and filtering effective around 1MHz will easily protect against this frequency. But if a potentially interfering signal at 2.450 GHz present in the environment is modulated at 1MHz, or if it is present at the same time as another signal at 2.451 GHz, each will easily pass through the 1MHz mitigation measures – and then either demodulate or intermodulate inside the circuit itself to create internal interference at 1MHz.

Analysis of especially susceptible frequencies, and of how the environment can cause them to appear in the circuits, helps cost-effective design by revealing which areas need the most design effort, and what design activities are needed.

4.3.9 Design techniques for bonding, wiring, cabling and PCBs

RF References, wiring, cabling and PCBs can all be designed to optimise their EM characteristics.

Bonding helps provide an electrical homogeneity in metallic structures to reduce potential differences between items of equipment, and to provide a path for common mode currents, at the frequencies that need to be controlled to achieve the required EM characteristics. The result is called the RF Reference. The impedance of bond straps should be low over a wide frequency range, and they should thus be as short as possible (direct metal-to-metal bonding is preferred to straps).

IEC 61000-5-2 [64] recommends the creation of a 'Meshed Common Bonding Network' or MESH-CBN, for the RF References in systems and installations, also see [65] to [68].

RF References should be protected against corrosion effects due to the physical environment(s). If the design of the EFS allows any part or joint in its RF Reference to corrode, the design should make it easy to remove and replace (see Clause 6 of IEC 61000-5-2 [64], and [65] to [68]) and the Maintenance Instructions (see 4.6.1) should specify the maintenance programme.

A proper wiring/cabling technique should avoid the induction of disturbing voltages or currents by external fields, and crosstalk between conductors, and should control the paths taken by common mode currents. The wiring/cabling scheme should be designed carefully. The interaction between wiring/cabling and EM disturbances should be minimised, for instance by using the following techniques:

- Cable screening (shielding)
- The use of double screening (shielding)
- Peripheral (360°) termination of cable screens (shields) to enclosure shields at both ends of a cable (inside equipotential zones only or with the addition of a parallel earthing conductor)
- The use of twisted wire pairs (with or without cable shielding)
- The separation of cables carrying signals of different levels and/or types (IEC 61000-5-2 recommends the use of five 'cable classes' and the minimum spacings between them)
- The shielding that may be able to be achieved by the use of metallic structures
- Providing a low-impedance path for a cable's common mode return current in close proximity to the cable, e.g. by using bonded metal conduit or ducting
- The use of fibre-optic, infra-red or radio links instead of conductive cables (fibre-optic links are now available that can transfer electrical power up to several Watts)

See [65] to [70], [72] for more details on the above techniques.

PCB layout plays an important role in the cost-effective mastery of EM characteristics, in the areas of emission as well as immunity. There are many EM design techniques that may be applied in their design, see [69] [70] [71], including these principal ones:

- The provision of an RF Reference that achieves a low impedance over the frequency range to be controlled.
- The provision of power distribution systems that have low impedance and low-Q resonances over the frequency range to be controlled.
- Separation (segregation) between switch-mode power converter, analogue and digital circuits. Inside each area thereby created, the circuits should be further separated to provide areas for sensitive and/or low-level circuits, and digital circuits be separated according to their working speed. In this manner, internal crosstalk is reduced.
- Localised shielding and/or filtering of components or areas of the PCB
- Suppression of conducted disturbances at the interfaces between a PCB assembly and other boards or cables, using shielding, filtering, overvoltage suppression and/or galvanic isolation techniques

Interactions between the PCB assembly and conducted and radiated EM disturbances are thus controlled to reduce intrasystem interference.

4.3.10 Using computer-aided design tools to optimise EM performance

Validated computer-aided design tools can help speed up the design/development process by allowing 'virtual' design iterations to improve EM characteristics before any hardware is made or tested.

They are not (yet) an alternative to testing actual hardware, but make it possible to deal with any major EM problems quickly and at low cost before the first hardware prototype. [71] includes a discussion on how to apply them to PCBs, and [68] includes a discussion on how to apply them to systems and installations.

NOTE: A validated computer simulator is one that has been shown, by comparison with real-life tests, to give suitably accurate results for a specific issue in design or assembly. All computer simulations are based on fundamental physics (e.g. Maxwell's Laws for electromagnetism) with certain assumptions and simplifications that allow them to analyse problems in a reasonable time. But the assumptions and simplifications only apply to certain types of problems, and are not suitable for other types. Validation ensures that the assumptions and simplifications in a given computer simulation allow accurate results for a given class of problems to be simulated.

4.3.11 EM mitigation techniques

EM mitigation measures include (but are not limited to):

- Shielding (screening)

- Filtering
- Surge and transient suppression
- Galvanic isolation
- Creation of (and connection to) an RF Reference

References [64] to [72] provide a great deal of detailed information on EM mitigation techniques (physical mitigation measures are discussed in 4.3.12). Because this wealth of information already exists, mitigation techniques will not be discussed here except to say that attention to the practical details of the way they are actually implemented in the EFS is very important indeed for the achievement of the desired mitigation performance.

Section 4.8 shows an overview of how EM (and physical) mitigation methods must be employed at the physical boundaries of specified 'EM Zones', to help achieve the desired results.

4.3.11.1 Shielding (screening)

Shielding is done with metallic barriers that are used to reduce the propagation of EM fields from one region to another. It can be used to substantially contain an EM field from a given source within a shielded volume, to reduce emissions. It can also be used to improve immunity by reducing the amount of external EM fields entering a volume and affecting its circuits. Shielding can be applied to cables, and/or to enclosures.

Shielding of cables and enclosures can be rendered partially or totally ineffective due to the presence of apertures, gaps, joints and other openings in the shield, or if the electrical continuity between the parts making up the shield is insufficient.

Enclosure shielding can be rendered partially, or even totally ineffective if any/all of the wires or cables entering or exiting the enclosure are not shielded and/or filtered to the appropriate degree. In either case the shields or filters should be correctly bonded to the enclosure shield at the point of penetration of the enclosure shield.

4.3.11.2 Filtering

Filtering uses specially designed circuits to reduce the propagation of conducted disturbances on wires and cables from one region to another. It can be used to substantially contain conducted EM disturbances from a given source to reduce emissions, and can also be used to improve immunity by reducing the amount of external conducted EM disturbances entering a circuit.

Filters can be used in power supply conductors (DC. and AC) and also on signal conductors. They are designed as a function of the current or the type of signal to be passed through the filter, and of the types and levels of EM disturbances that are to be suppressed.

4.3.11.3 Surge and Transient Suppression

Surge and transient suppression includes protection against overvoltages and overcurrents, and is used to prevent conducted transient or surge disturbances from causing interference or actual damage to circuits and devices. For protection from electrostatic discharge (ESD) transient overvoltage protection devices must operate in under 1ns but need only be rated for low total energies, whereas for protection from surges on the electrical power supply they may be able to operate as slowly as 100 ns to 1 ms but be rated for very large energies. In all cases, overvoltage protection devices require a 'ground' reference that has a low impedance, sufficient to absorb the required current without creating an appreciable rise in potential, over the appropriate frequency range.

Overcurrent protection is used to protect overvoltage protection devices (and hence the circuits and devices they protect) from damage due to electrical faults (e.g. in the electrical supply distribution network) that would cause them to exceed their power ratings.

4.3.11.4 Galvanic Isolation

Galvanic isolation is a solution to common mode surges, and (in some cases) to differential mode surges as well. For example, air or solid insulation that has a sufficient level of voltage withstand capability (dielectric strength) can prevent ESD from occurring to the protected item of equipment or device. One of the biggest problems with extreme events such as lightning, EMP, etc., is that the currents induced into the

'earth/ground' structure can, over a few metres, give rise to voltages that can damage drivers and receivers connected to cables. Optical and wireless communications (see 4.3.5 and 4.3.6) provide excellent galvanic isolation for voltages up to about 500kV/metre of space between transmitter and receiver. A number of other devices can provide galvanic isolation at up to one or two kV – for example isolating transformers, opto-couplers, opto-isolators, and other packaged isolators.

There are a large number of EM disturbances that affect power distribution systems, reducing their 'power quality', and for each type of disturbance there are mitigation techniques that can improve the power quality – from simple measures up to complete regeneration of the supply using a motor-generator set or charging a battery or super capacitor and using the stored energy to power a local inverter.

Several IEC standards or technical reports (e.g. the IEC 61000-5 series) give detailed guidance on how to apply certain mitigation measures. They might also be recommended in the relevant product standards.

Mitigation methods are generally used to create 'electromagnetic zones' (EM Zones), as described in 4.8 and Figures 4.2 and 4.3. These are volumes within an EFS that employ EM mitigation measures at their boundaries to provide different EM environments for the equipment and/or products located within them. For much more detail on practical methods of creating EM Zones for systems and installations, see [68], and for applying mitigation techniques to a cabinet to create an EM Zone within it, see [67].

The levels of protection (mitigation) required for an EM Zone depends upon the original assessment of the EM environment plus the EM characteristics (emissions and immunity) of the equipment intended to be located within it.

Items of equipment and their cables are then located within these EM Zones according to the degree of protection they need from each other; the degree to which the EM environment needs to be protected from them; or the degree to which they need to be protected from the EM environment over their lifecycle.

4.3.11.5 Creation of (and connection to) an RF Reference

An RF Reference is a conductive structure, usually a metal sheet or volume, or a mesh (grid) of conductors, that maintains a low impedance (generally much less than 1Ω) up to some defined frequency. A metal sheet has no significant limits on its upper frequency, at least up to 26GHz, but the upper frequency of a mesh structure is determined by the sizes and shapes of its meshes.

An RF Reference could be a two-dimensional structure such as a plane (e.g. in a PCB, a 0V plane layer is often used as an 'RF Reference Plane'), but it could also be any type of 3-dimensional shape. A special case is the inside of a conductive box, in which the box structure provides both shielding (see 4.3.11.1) and also an RF Reference for electronic circuits it encloses.

Having a low impedance, an RF Reference allows Differential Mode (DM) and Common Mode (CM) RF currents to flow in the paths that create the least EMI possible from the structures that are used. To take advantage of this, electronic units are generally connected directly to the RF Reference using connection methods that themselves have a low impedance at the frequencies concerned.

Filters (see 4.3.11.2) that employ 'grounded' capacitors require a low-impedance electrical connection to an RF Reference, and if either the connection method or the RF Reference does not have sufficiently low impedance at a given frequency, then the filter will be unable to provide its hoped-for attenuation at that frequency.

4.3.12 Physical mitigation techniques

The EFS should be designed so that its EM performance remains sufficient for its reasonably foreseeable worst-case EM environment(s) over its anticipated lifecycle – including multiple independent EM threats – despite all foreseeable physical stresses, strains, wear and ageing over that lifecycle.

Mechanical structures may need to be designed for foreseeable worst-case forces, shock and vibration with the aid of computer-aided finite element analysis.

Physical mitigation measures for equipment design include measures for the reduction of stresses due to mechanical; climatic; chemical; biological; etc. effects. They include (but are not limited to) the following techniques:

- Shock and vibration mountings (active or passive)
- Vibration-proof fixings for electrical contacts and other fixings

- Avoidance of resonance in physical structures
- Protective enclosures (e.g. splash-proofing, waterproofing)
- Conformal coatings and/or encapsulation
- Grease (conductive or not, as appropriate)
- Paint (conductive or not, as appropriate)
- Cable ties and other types of cable restraints
- Anti-condensation techniques (e.g. heaters, humidity control)
- Sealed enclosures (not easy!)
- Forced ventilation, air-conditioning, etc.
- Positively pressurised enclosures, using air or gasses (often nitrogen) with specified humidity and temperature
- Maintaining at least minimum levels of humidity to limit electrostatic discharge potentials

Physical mitigation methods are generally used to create 'Physical protection Zones', which are volumes within a structure that provide different levels of physical protection from the external ambient for the equipment and/or products located within them.

They are created by controlling the presence or variations in physical, climatic, chemical, biological, etc., parameters, based on the original assessment of the physical environment (see Steps 1 and 2).

Items of equipment and their cables are then located within these 'Physical Zones' according to the degree of protection they need from the physical environment of the EFS, to help ensure that their EM characteristics do not become excessively degraded at any point during their lifecycle.

For instance, in a motor vehicle mounting an electronic subassembly in the passenger cabin makes its EM design much easier, than if it is located in the engine bay where it is exposed to water and salt sprays from the roads, oil, brake fluid, etc., and more extreme temperatures and temperature cycling.

The principles embodied in the creation of 'Physical Zones' are exactly the same as for the EM Zones discussed in 4.3.11 – although of course it is physical (climatic, etc.) phenomena that are being controlled, not EM.

4.3.13 'Layering' or 'nesting' EM/physical mitigation

There are a number of design techniques, often called 'hardening', which can produce hardware and software/firmware that is *inherently* more immune to EM/physical phenomena. Alternatively, sufficient EM/physical characteristics can be achieved using EM/physical 'mitigation measures'.

EM mitigation measures are discussed in 4.3.11, and include filtering, shielding, surge suppression, galvanic isolation, etc. See [64] to [72] for more information on EMC design and mitigation techniques for hardware, and [56] to [62], [70] and [72] for more information on software EMC design techniques. Physical mitigation measures are also discussed in 4.3.12.

It can be easier, less costly, and more reliable, to use a number of 'layers' of inherent EM/physical performance and EM/physical mitigation measures, rather than relying on a single layer (such as a single EFS enclosure employing high-performance shielding and filtering), as shown in Figure 4.1 for the example of EM mitigation (a similar figure could have been drawn showing layered physical mitigation measures).

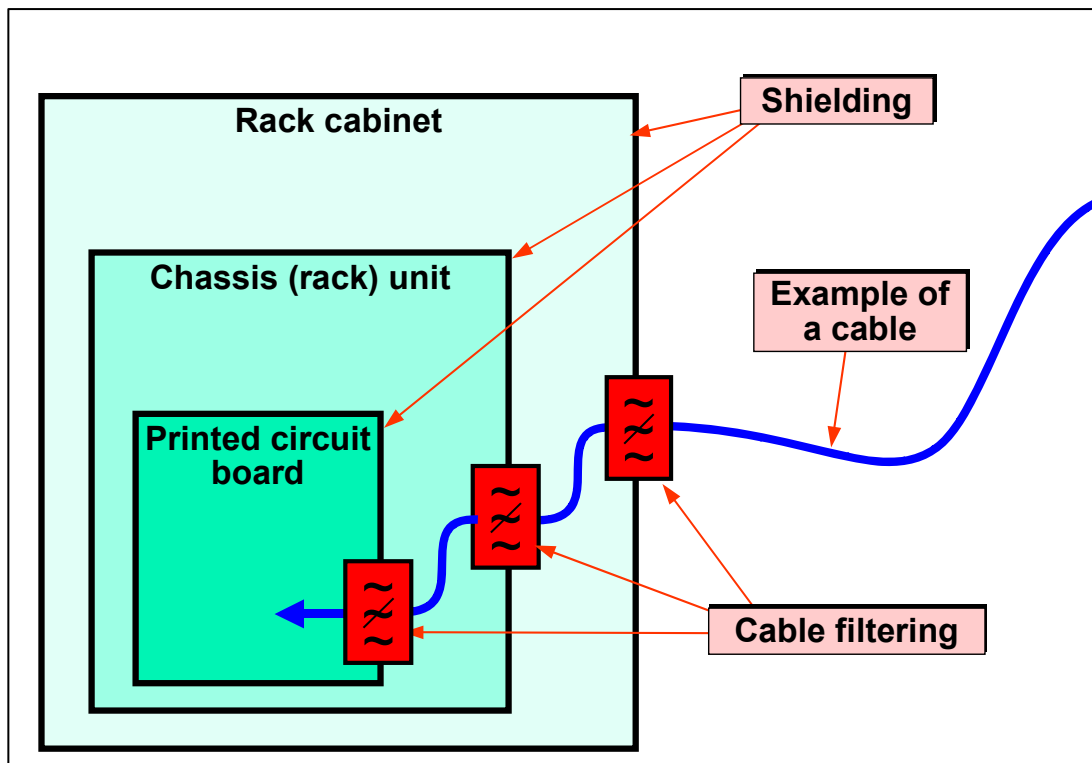


Figure 4.1 An example of a 'layered' or 'nested' design of EM mitigation

Another term for the 'layering' approach is 'nesting' – like Russian dolls, each layer of protection, once breached, reveals another protection layer 'nested' inside. In terms of EM Zones (see 4.8) the world outside the rack cabinet in Figure 4.1 is EM Zone 0, the interior of the rack cabinet is EM Zone 1, the interior of the Chassis Unit is EM Zone 2, and the Interior of the PCB is EM Zone 3.

It is recommended to design so that if one 'layer' (EM Zone boundary) should fail completely for some *unforeseen* reason (e.g. a fault or misuse, whether accidental or intentional) – the EFS will still have at least adequate EM/physical characteristics.

For example: assume that an enclosure requires a minimum of 40dB shielding effectiveness (SE) at 900MHz. A single shielded/filtered enclosure could easily achieve an SE of 80dB or more at 900MHz, and such enclosures are available from numerous suppliers. But cutting a single hole just 15mm in diameter (e.g. to add an indicator lamp) would reduce its SE to around 20dB at 900MHz.

However, if a three-layer design were used instead with each layer of shielding/filtering achieving 20dB at 900MHz – even completely destroying the outermost layer would still leave the overall design with an SE of 40dB. A three-20dB-layer design might cost less than a single 80dB protection layer, and is also more resistant to faulty assembly (e.g. EM gaskets missed out of one layer of shielding).

When using layers it is important to understand the possible interactions between the layers so that the overall result is the sum of its parts. For example, cascading certain types of mains filters can result in filtering effectiveness that is less than that of just one filter, although this can be avoided by the use of appropriate design techniques that are well known to filter experts.

Layers that can benefit from improvements in their inherent EM and/or physical performance, a process that is often called EM and/or physical 'hardening', include:

- Integrated circuits (ASIC, FPGA, custom, etc.) can be designed or chosen for good EM performance, see [73]
- Electrical and electronic circuits, interconnections, PCBs and software, can each be designed to have improved EM performance, see [69] to [72]

Layers where EM/physical mitigation measures (shielding; filtering; surge, transient, ESD protection, etc.) can be applied include:

- Individual ICs or transistors on a PCB, see [69] to [73]
- An area of a PCB, see [69] to [72]
- A complete PCB, see [69] to [72]
- Modules and sub-assemblies, see [69] to [72]

- Units (e.g. a rack mounting chassis unit), see [67], [69] to [72]
- The overall enclosure level (e.g. rack cabinets), see [67] to [72]
- Vehicles, rooms, entire buildings, see [65] [66] and [68]
- Entire sites (campuses) comprising numbers of buildings or other structures, or the sites where vehicles operate, see [65] [66] and [68]

4.3.14 Fault mitigation

The design of the EFS should ensure that acceptable safety risks (or risk-reductions) are achieved despite the degradation of EM characteristics caused by reasonably foreseeable faults that could occur over the anticipated lifecycle.

So the design should take into account what faults could foreseeably occur, and either reduce the incidence of the faults or use methods that limit their safety impact (for instance, a fault that could lead to an unacceptable degradation of EM characteristics could be detected and used to initiate a ‘fail-safe’ reaction), to the extent appropriate for the level of risk, or risk-reduction required.

It is very important to understand that EMI and physical stresses can cause ‘common-cause’ faults (which are *not* random faults) in identical elements – making many of IEC 61508 techniques ineffective (e.g. redundancy using identical elements operating in parallel).

A great deal of the safety engineering techniques that have been developed over past decades has assumed that faults occur at random, but this is not true of all faults, such as those due to physical and EMI effects, and if common-cause faults are not addressed the EFS will not achieve the desired levels of safety risk (or risk-reduction). Faults can include:

- Components open/short circuited, or their parameters altered (can seriously compromise filtering)
- Broken electrical bonds (e.g. shield joints and gaskets, filter grounding)
- Increased impedance of electrical bonds
- Loose, damaged or missing fixings or conductive gaskets (e.g. can seriously compromise EMI shielding)
- Failure of a transient/surge protection device (seriously compromising immunity to overvoltage transients)
- Latch-up in semiconductors (transistors, ICs, etc)
- Looping and crashing in programmable electronics such as microprocessors

The use of design techniques that protect against the effects of the foreseeable physical (mechanical, climatic, etc.) environment can reduce likelihood of most systematic hardware faults to low enough levels. HALT (highly accelerated life testing) can be used to help identify shortcomings in design, materials and components.

Random failures can still occur, and if they can lead to a safety risk IEC 61508 [7] specifies the design techniques for achieving the required safety level (e.g. duplication, triplication, etc.; automatic condition monitoring with safety shut-down; etc.). These techniques can also be used in the wider context of this Guide, to help EFS achieve the desired levels of risk, or of risk-reduction.

The likelihood of latch-up can be reduced by appropriate design of semiconductors themselves (see 4.3.22 and [73]), and also by appropriate mitigation measures (see 4.3.11). Mitigation measures to prevent latch-up include protection against over/under voltages (transient and continuous) on all pins, and/or temperature control and/or shielding against excessive radiation. If latch-up occurs, normal operation of the semiconductor can only be recovered from by removing all the voltages (power and signal) to the device, to allow the erroneous substrate currents to subside sufficiently, and then reapplying them. This will take some time, depending on the circuit design, limiting the use of this technique to EFS that does not have to have a fast response time.

Mitigation measures to prevent looping and crashing include techniques for software and firmware (see 4.3.24). Appropriate design of ‘watchdogs’ can detect looping and crashing (prevention of looping may require two or more watchdogs, and/or more sophisticated watchdogs) but it is important to understand that they take a finite time to detect the problem and reboot, which can be from half a second to several minutes depending on the EFS. During this period the EFS is not correctly controlling its functions, and indeed can be outputting random combinations of signals or controls that could significantly increase safety risks, or

compromise risk-reductions. So whether to rely on watchdogs for safety purposes depends upon their maximum 'detect and reboot' times and the time-constant of the functions being controlled.

For example, in an electronic steering system for a vehicle, the response of the EFS must not suffer errors or malfunctions lasting longer than about 10ms, so the hardware, software or firmware must be designed so that the likelihood of it suffering from latch-up, looping or crashing is low enough for it to be classed as negligible by the risk assessment (see 4.2).

But for the control of temperature in an induction furnace that is heating several tons of metal, latch-up, looping or crashing might be permitted providing the EFS reliably recovers from these states and brings the controlled functions back under control within acceptable parameters for safety within (say) a few tens of seconds.

The above has discussed EM design to cope with reasonably foreseeable faults and use/misuse to help achieve acceptable safety risks (or risk-reductions). A similar approach should be followed for the physical design of the EM elements that help maintain EM safety (see 4.3.12).

4.3.15 Mitigation of problems caused by foreseeable use (misuse)

Foreseeable actions during the operational phase can significantly affect immunity to the normal EM environment, and so 'foreseeable use' and 'foreseeable misuse' should be taken into account during the design of the EFS.

For example: if a shielding door could be opened at a time when its shielding was required for safety reasons, it could either be automatically locked shut during such periods, or electrically interlocked so that an alarm and/or 'fail-safe' reaction was initiated if it was opened, depending on the risk assessment.

NOTE: Relying on automatic locking might not be sufficient where safety is especially critical, because users have been known to employ crowbars and power tools to force their way into dangerous enclosures, when they did not understand the reason for their automatic locking.

Examples of foreseeable misuse include:

- Failure to follow the installation requirements could result in an unshielded cable being used where shielded was required, or shielded cable being used with incorrect shield termination, or incorrect cable routing leading to unanticipated levels of EM coupling
- Operating with shielded doors open (or not closed correctly), or with shielding panels removed (or not fixed correctly)
- Operating a mobile or portable radio transmitter too close to a cable or item of equipment

Because installation, commissioning and/or maintenance instructions might not be followed, it is best if the EFS creator performs these tasks. Users might open doors, covers or panels when they should not, or make unapproved modifications – so the designer needs to anticipate what could foreseeably happen, then design, guard and warn accordingly (in that order).

Sometimes users will need to be trained, maybe even pass an examination, before being appointed as a 'keyholder' and permitted to operate an EFS. In some applications users may need to pass an examination every year or so to remain a keyholder.

4.3.16 Don't rely on the user

It can sometimes be tempting to try to arrange for your customer to bear total responsibility for (and cost of) some EM mitigation measures, by adding them to the user manual. The assumption might be that it will be the customer's fault if a safety incident occurred because he did not read and fully implement the requirements in the manual.

But this approach might not provide a good legal defence – because everyone knows that no one reads manuals, and yet safety must still be achieved even considering reasonably foreseeable use or misuse (see 4.3.15).

So, when relying on mitigation at site-level for the safety of your EFS, always agree it in writing well beforehand with the customer, and maybe agree site verification requirements too so you can check that he has done it correctly. It is important to include an agreed legal disclaimer that has the effect of making the customer solely liable if the site improvements are not fully implemented before an EFS is operated.

Also, it is bad safety engineering practice in general, to rely on the user to detect and correct an error or malfunction in hardware, software or firmware. This should come out of the use of Task Analysis and Human Reliability Analysis in the risk assessment process (see 3.7), but anyway it should be realised that people are generally quite good (but never perfect!) at dealing with events that they have been trained for, and experience on a regular basis either in real life or in simulations. But people are very bad at dealing with the unexpected, such as a vehicle's electrically-assisted power steering that stops providing assistance, or decides to steer in a different direction to that which is required.

4.3.17 Using checklists based upon case studies and experience obtained in similar applications

Experienced personnel in organisations learn many things about the EM characteristics and their possible effects on the safety of the EFS they are associated with. They also learn about similar EFS manufactured or operated by other organisations through publications, conferences and similar events.

Technical guidance in international standards should, of necessity, be general, within the scope of the standard, but the knowledge gained by experienced personnel can modify the guidance in the relevant standards, or be additional to it.

It is important for the responsible people in organisations to actively seek out specialised safety information on their own and other EFS, and then to 'capture' this knowledge in checklists, so that when experienced personnel leave an organisation, their knowledge is not lost to that organisation. Using checklists in this way, the EM safety knowledge of the organisation is maintained and new or less experienced personnel can quickly become acquainted with what has found to be necessary to achieve adequate safety in new designs.

It is also important for such checklists to be kept up-to-date, and to be applied along with the relevant standards to the manufacture of all new EFS.

4.3.18 Taking the power distribution system into account

A number of different types of power distribution systems exist, for example TN-S, TN-C, TT, IT, etc. TN-C types, also known as PEN (Protective-Earth-Neutral) combine the functions of Neutral conductor and protective earth in one conductor, and are bad for EMC because they cause signal and data cables between items of equipment to experience high levels of noise at 50/60Hz and their harmonics. They also create strong magnetic fields throughout an installation at 50/60Hz and their harmonics, that make the images on VDUs and photo-multiplier tubes 'wobble', and can also interfere with sensitive electronic circuits.

So power distribution systems that use a single conductor for the neutral and the protective earth should not be used wherever signals, data, VDUs, photo-multipliers, or sensitive electronic or electrical equipment is used, such as equipment that complies with the product or generic immunity test standards used for compliance with the EMC Directive, which do not test at all for this kind of EM environment.

Where TN-C (PEN) systems are used, they can be converted to the EMC-friendly TN-S types by installing a suitable mains isolating transformer at the boundary of the area to be protected (see 4.8), and only supplying mains power to that zone from its TN-S output. The neutral of the new TN-S supply must only be connected to the Bonding Network (BN) for the area concerned (see 4.3.25). It is good installation practice to fit a link in the TNS neutral-BN connection, and before commissioning, during annual shutdown or when problems are suspected, isolate the power source, remove the link and check there is now no resistive path between the neutral and the BN. The equipment in the zone should be plugged in during this test, to discover if any of them is suffering a neutral-to-chassis insulation failure.

TN-C, PEN and similar distribution systems do not create interference problems where all of the electronics or other circuits are insensitive to the EM disturbances they create, or have been specially 'hardened' to operate reliably in an environment containing high levels of conducted electromagnetic disturbances, and high levels of magnetic fields, at the power line frequency, its harmonics, and its load currents.

All other types of AC power distribution have no EMC effects, as long as they do not prevent the use of the desired good EMC engineering practices or EM mitigation techniques.

4.3.19 EMI mitigation for multiple redundant channels

EMI can cause systematic ('common cause') failures, so, where IEC 61508 (for example) [7] requires multiple channels – with electronic voting on their results – to meet the required levels of risk, or risk-

reduction, it is necessary to use diverse (different) technologies, so that EMI does not cause all of the channels to fail in the same way at the same time, defeating the purpose of the voting circuit.

But using multiple diverse technology channels does not necessarily mean that each channel can be allowed to have a low EM performance – otherwise, during interference, it could happen that all of the digital channel outputs were at 0 or 1, and all the analogue channels could be at plus or minus full scale. In such situations the chances of defeating the voting circuit can be relatively high.

One way around this problem without increasing the immunity of the channels could be to send complex digital or analogue signals (such as a pulse train with specified timings) to the voting circuit instead of simple voltage levels. The complex signal should be designed so that a failed channel would be much less likely to create it, so that the voting circuit would not be so easily fooled.

Similar common-cause issues exist for some physical threats (e.g. overtemperature), with similar results.

4.3.20 Techniques for sensing the EM/physical environment

Interference sensors can be used inside or outside an EFS, to detect EM events that might cause hazards and initiate special protective measures or shut-down the EFS safely. For example:

- As already used to protect some military equipment from the pulses caused by nuclear explosions
- As already used by gaming machine manufacturers to protect from people trying to ‘break’ their gaming machines with interference (e.g. 30kV ESD from cattle prods)

A safety interlock on a door or panel can tell if it has been opened, and inhibit the EFS so as to protect from the possible safety consequences of degraded shielding (treating the shielded door like a machine guard that interlocks with an emergency stop function).

There are also wideband EM sensors [21] that can detect accidentally degraded shielding or filtering, or EM threats (whether foreseen or unforeseen), and initiate a safe shut-down. If these are used inside a shielded enclosure they could allow doors and panels to be opened without a safe shut-down occurring – unless EM threats occur at that time, at levels that could cause interference.

Sensing techniques (for example, accelerometers) can also be used for the physical environment, and used in a similar manner to the above, so that (for example) a safe shut-down is initiated if an extreme physical threat is detected, or if (for example) excessive degradation of a physical mitigation measure (e.g. a shock absorber, sealed enclosure, etc.) is detected.

There are many uncertainties associated with such techniques, and in many cases it would not be wise to rely upon them alone. However, in combination with other design techniques they can help to achieve the desired levels of risk (or risk-reductions) cost-effectively, and they can help protect against unforeseen aspects of the EM environment, for instance future developments (see 1.3.3).

4.3.21 Issues with fail-safe methods

Fail-safe reactions (such as safe shut-down) have been mentioned a number of times in the above design techniques. But the user or operator will become very frustrated if a protection function in an EFS initiates a safe shut-down every time the EM environment gets a little noisier than usual. It is not unusual for people to modify such EFS, so that they can reduce costly downtime.

Because it is reasonably foreseeable that people will modify or disable an EFS that causes excessive downtime, this counts as foreseeable misuse and an EFS creator could be held to be liable if they did not take such foreseeable human activities into account during design.

And of course there are some applications where fail-safe methods cannot be used, such as life-support EFS, where the EFS must continue to operate according to its design intent – although in some circumstances it may be possible to allow a certain amount of degradation of performance.

For example, implanted pacemakers are designed to fail-safe to provide a basic heart stimulus rather than stop working at all. The basic pacing waveform used makes the implantee feel very ill, and maybe even lose consciousness, but will keep them alive. However, if the implantee is driving a vehicle at speed at the time the fail-safe operation occurs, it might not be considered to have been fail-safe after the resulting traffic accident.

4.3.22 'Hardening' integrated circuits (ICs)

ICs can be designed to have improved immunity to EM and physical threats (including ionising radiation). Physical hardening techniques have been well established for decades, for example for the manufacture of MIL-qualified or radiation-hardened devices.

EM hardening techniques are less well known and documented, but [73] is recommended.

4.3.23 'Hardening' digital and analogue circuits and PCBs

There are a number of design techniques that can be applied to digital and analogue circuit design, the PCBs that carry the devices themselves, and the signal communications via cables, wireless, or whatever, and they are described in considerable detail in [69] to [72].

The EM immunity of electronic designs based upon counters and state-machines, and of programmable electronic technologies that employ software or firmware, depends strongly on the digital activity in the circuit from nanosecond-to-nanosecond. The operation of the digital hardware devices causes a variety of types of electrical noise, which degrade the noise thresholds. When certain digital operations are performed, for a period of typically between a few hundred picoseconds and a few tens of nanoseconds, the noise threshold can be significantly degraded, so a transient EM event occurring at just that time can cause an error or malfunction, whereas it might not be capable of doing that the rest of the time.

In the case of software or firmware, the especially susceptible states might depend on inputs and algorithms. It should be part of their design to ensure that the numbers of digital signal transitions occurring simultaneously are never so large as to significantly degrade the noise threshold. It may be possible to choose ICs that have built-in output-transition delays measured in picoseconds, so that none of their outputs change state at *exactly* the same time (e.g. some types of FPGAs).

Another way of dealing with this problem in digital circuits is to use computer simulation to determine when the most susceptible circuit periods occur, and whether they are very much more susceptible than during typical operation. If they are significantly more susceptible, design changes might be able to reduce them to more typical levels, or at least reduce their rate of occurrence.

Such simulation will require the extraction of 'stray' couplings, 'ground bounce' and 'power bounce' caused by PCB traces, connectors, cabling, maybe even by the packaging of the ICs themselves, and including them all in circuit simulations (e.g. using SPICE). Computer-aided design tools that can achieve this with good accuracy exist – they are not yet very low-cost but even so they could be very cost-effective.

Similar variations in electrical activity in some analogue circuits can also result in degraded EM immunity at certain times, especially where an analogue signal is being 'digitised' by a comparator. Unless the analogue signal has peak values that are either much lower or much higher than the comparator's threshold – *and* the comparator is designed with a level of hysteresis that exceeds the highest levels of signal noise – EMI could cause multiple threshold-crossings, resulting in a false signal out of the comparator.

One solution to the analogue comparator problem is to use an A/D converter instead, followed by a processor running software or firmware that 'cleans up' the signal using a variety of techniques, such as median filtering, a number of averaging techniques, window comparison using signal-derived thresholds, etc.

4.3.24 'Hardening' software and firmware

Software, firmware, and data communications protocols can be hardened to improve their immunity to EM threats.

Some issues concerning the use of 'watchdogs' are briefly discussed in 4.3.3 and 4.3.14, for much more information on these and other techniques see Chapter 37 of Part I of [72], Chapter 12 of [70] and [56] to [62].

4.3.25 Systems, installations and power quality

A number of design techniques exist for helping to achieve the desired EM/physical characteristics of EFS in systems and installations, including:

- Cable segregation and routing, see [64] to [68]
- Provision of paths for the return of common mode currents, see [64] to [68]

- ‘Mesh’ bonding of the earth/ground structure, see [64] to [68]
- EM mitigation (filtering, shielding, surge protection, galvanic isolation, etc.), see [64] to [68]
- Improving the quality of AC mains power, see [74] and [75]
- Lightning protection, see [65] [68] and [40]

These also help in the application of the usual EM mitigation techniques (filtering, shielding, transient/surge suppression, galvanic isolation, etc.), see 4.3.11.

4.4 Realisation measures and techniques to be considered

The word ‘realisation’ in the title includes the concepts of assembly, manufacture, implementation, integration, etc.

Section 4.5 addresses the lifecycle phase of installation and commissioning, and Section 4.6 addresses issues concerning the operational phases of the lifecycle.

4.4.1 Procure materials, components and products according to their EM/physical specification

A QC procedure should be in place that (amongst other things) ensures that the designer specifies all the necessary EM and physical parameters for purchasing the materials, components, products, equipment, etc., that are required to construct the EFS, plus the methods that are to be used in its assembly and production test.

The QC procedures should ensure that the other departments in the company comply with these specifications to help ensure that at the end of the manufacturing/integration process, the result is what was originally designed.

Design or component changes that suppliers make to their products can be important for EM characteristics and/or resistance to the lifecycle physical environment. This is especially true for the suppliers of electronic units or sub-assemblies, but can also be true for suppliers of items such as pieces of metalwork that are often assumed to be insignificant. Semiconductor suppliers might substitute die-shrunk versions of their product in the same packaging with the same part numbers, and since these can have very different emissions and immunity characteristics from the original units, this possibility should be actively controlled by the QC procedures.

Ideally, a QC system should control all relevant issues of the build-states of the components and products supplied by others, but this is often very hard to do, so instead most manufacturers rely on sample-based EM and physical inspections and tests. These inspections and tests are best applied upon delivery, before accepting a new batch of goods (before any value has been added). The EM and physical checks or tests do not need to follow IEC or ISO test standards, and relative comparison tests are preferred because they can be quick and easy to design, construct, and apply. They should check or test all of the significant parameters.

In serial manufacture, full EM and physical tests could be required whenever a supplier or subcontractor introduces a significant design change to their components or products.

4.4.2 Take all necessary actions to avoid counterfeits

All standard volume-manufactured electrical and electronic hardware, software and firmware are subject to counterfeiting. The counterfeit parts generally have inferior (or no) performance, or are not as reliable as the genuine items. For many years now, counterfeit parts have been known to even be delivered mixed in with *bona fide* parts from authorised distributors and original manufacturers.

Counterfeiting is now estimated to account for about 15% of global trade, and is known to be at least partly run by internationally organised crime.

Where the correct EM/physical performance and/or reliability of parts are important for the achievement of the specifications for safety risks or risk-reductions – the correct provenance and EM/physical characteristics of these parts must be actively managed.

It is no longer at all acceptable to ignore counterfeiting as a source of risk. Several trade associations are active in this area, so their expertise and databases should be employed, and whatever other activities are necessary should be undertaken commensurate with the level of risk (or of risk-reduction) required, see 0.10.4.

4.4.3 Assemble according to the design

The EFS should be assembled according to its design, using the correct materials, components and products according to their EM/physical specifications. This requires a QC system that controls every aspect of the build state, to help achieve the EM/physical characteristics of the EFS and maintain them over its reasonably foreseeable lifecycle.

All of the following issues (and more) can be very important, so should be actively controlled by the QC system:

- A single 'form, fit and function' replacement device, component or other part
- A wire or cable routed differently
- IC and semiconductor mask-shrinks (die-shrinks)
- 'Latest generation' power semiconductors
- Changes in painting method or supplier. For example: a new painting method or painter creates an overspray of non-conductive paint onto areas where metal-to-metal or metal-to-conductive-gasket electrical contact is required
- Metal parts supplied with non-conductive finishes. For example: non-conductive passivation coatings can sometimes be applied despite not being required by the drawing, resulting in EM problems for chassis-bonding, shielding and filtering. This often occurs when changing metalwork suppliers, but has even occurred despite using the same metal supplier.
- Metal fixings supplied with non-conductive finishes. For example: Metal screws that always used to be conductively-coated, are instead supplied with a non-conductive finish resulting in EM problems due to higher impedances in chassis-bonding, shielding and filter grounding.
- Changes in a plating method. For example: Over time can result in poor chassis bonding or EMC gasket characteristics due to oxidation and/or galvanic corrosion.
- Use of a different kind of 'shake proof washer'. For example: Where the shake proof washer was providing useful protection against the effects of vibration, changing to a different type can compromise that aspect of resistance to the lifecycle physical environment.
- Almost any design or component changes made by electronic unit or sub-assembly suppliers – the build-state of their goods should also be controlled.

The QC system should ensure that no changes in any aspect of build-state can occur — however insignificant they may seem — unless they have been checked and approved by the person responsible for the EM safety performance of the EFS.

Similar considerations apply to controlling the design to withstand the foreseeable physical environment.

The person responsible might want to do some quick EMC/physical checks, or even full retesting, before he/she feels confident in authorising the proposed change or deviation.

In serial manufacture, full EM and physical tests should be applied on a sampled basis, every few months or every few thousand items manufactured, or whenever a significant design change is introduced. More frequent sample-based 'checks' of EM and physical characteristics can be used to reduce the frequency of full tests.

4.4.4 Control of suppliers and subcontractors, their suppliers and subcontractors, etc.

A chain is only as strong as its weakest link, and modern systems integration and similar manufacturing activities often involve very lengthy supply chains. For an EFS to achieve the desired levels of risk or risk-reduction requires the whole supply chain to be controlled commensurately with the levels of safety risk or risk-reduction to be achieved.

Some EFS creators seem to assume that as long as they purchase goods or services ‘in good faith’ – if safety incidents occur with their EFS that can be traced back to parts or services provided by others, and that the design or manufacture of the EFS itself was not at fault – then any legal claims can be passed down the supply chain until they rest with the supplier of the defective part or service.

But according to case law, this is not the case in the UK, and probably not the case in most developed countries. UK law holds that it is the responsibility of the final integrator – the organisation that makes the EFS available to the owner and/or end-user – to ensure that all of the parts and services they use are fit for the purpose required by the EFS.

‘Buying in good faith’ is no defence at all, and being aware of this and acting appropriately is an important part of reducing financial risk.

All of the concerns in 4.4.1 – 4.4.3 above apply to *any* parts supplied or work done by suppliers and/or subcontractors. Where the EM/physical performance of something designed/manufactured by a subcontractor has an implication for the safety risks or risk-reduction achieved by the EFS over its operational lifecycle, the subcontractor should be applying the same level of control over their implementation and integration as the EFS creator.

Similar requirements apply to those companies who supply or subcontract to the EFS creator’s suppliers or subcontractors.

Some EFS creators find it difficult to achieve the necessary degree of control over suppliers and subcontractors of parts, hardware or software, so to reduce their risks they use:

- Sample-based EMC/physical verification upon delivery (appropriate checks and tests can be quick and easy to do if designed correctly)
- Sample-based EMC/physical verification in serial manufacture (generally frequent quick checks, with full tests every few months)
- EMC/physical verification as appropriate whenever there is any change in the design, including the use of alternative components

Verification can use one or more of the techniques described in Step 5, as appropriate, although ‘checking’ and ‘testing’ of the required specifications are commonly employed, going into a level of detail and accuracy commensurate with the levels of safety risk or risk-reduction required, see 0.10.4.

4.5 Installation and commissioning measures and techniques

To ensure the correct installation and commissioning of the EFS on its operational site, to achieve the desired EM safety performance, the EFS designer should take the issues described below into account in the design and its documentation.

This process will result in certain design features and/or instructions for the installer and commissioner, to overcome the problems identified that could have a negative impact on the achievement of acceptable safety risks (or risk-reductions) for the EFS over its lifecycle.

In the case of safety-related systems according to IEC 61508 [7], for example those in railway trains or power generating plants, it will almost certainly be the case that the people doing the installation and commissioning are at least knowledgeable about safety and/or EMC, and appropriately-written installation and commissioning instructions will be implemented by suitably-skilled people, even if they have to be subcontracted or trained especially for this.

In such situations, it is often the *combination* of the activities carried out by the installers, with the features of the EFS, which results in the desired levels of safety risk or risk-reduction. Installer activities could include, for example: choosing suitable types of cables; routing cables in ‘classes’ according to the signals or power they carry; fitting appropriate filters; providing electrical power that meets minimum specifications, etc.

However, at the other extreme, some types of EFS might be purchased directly by consumers who are not at all knowledgeable about safety and/or EMC, and who cannot be relied upon to carry out any special activities at all. Examples include domestic appliances, certain types of medical appliances, vehicles such as motorcars, motorcycles, boats, etc.; sports, entertainment and leisure equipment, etc.

Such EFS might be installed, commissioned and operated by people who are children, aged, disadvantaged or disabled (e.g. partially sighted, blind, deaf, weak, ill, missing limbs, intellectually challenged, etc.). Nevertheless, such EFS should be safe enough, or achieve the desired levels of risk-reduction. The issues

below should be taken into account, but the resulting design solutions will likely be very different from those applied to industrial EFS.

4.5.1 Any constraints on the physical positioning of the items of equipment that comprise the EFS

Step 1 should have identified areas within and outside the intended location(s) of the EFS where the EFS would be exposed to especially high levels of EMI, see 1.2, or where elements of the EFS could interfere with other EFSs. Step 2 should also have identified elements of EFS that could interfere with other elements of the same EFS, if they were located inappropriately, see 2.2.

Information on the EM protection measures resulting from the above analysis should be carried forward into the installation phase of the work, for example to ensure that the necessary minimum distances to prevent interference are achieved.

Similar issues apply to the physical environment (e.g. not placing electronics in areas of very high temperature, prone to flooding, or other significant physical effects), see 1.2 and 2.2.

4.5.2 Constraints on cabling

The installation might require various constraints on cable types, and/or on the lengths and routing of power, control and signal interconnecting cables.

The EM characteristics of different cable types vary very widely, so it is important to specify the types of cables to be used during installation in every case. A manufacturer's part number for a cable type can help, and is often taken as a guide to the cable characteristics required. In some cases it may be that only a specified manufacturer's cable type is permitted to be used for certain purposes in the installation of the EFS, and where this is so it should be made very clear in the installation instructions.

Cables may need to be separated to prevent intrasystem and intersystem interference. IEC 61000-5-2 [64] provides the essential guidance on good EM engineering practices for this issue, based upon the routing segregation of at least 5 'classes' of cable depending upon the types of signals they carry and their propensity for creating EM emissions or suffering from EM interference.

Common mode currents are the main cause of problems with conducted and radiated EM emissions and immunity, and crosstalk between cables. Designing the installation to provide appropriate paths for common mode currents, so that they are well controlled, is a good technique for improving emissions and immunity.

IEC 61000-5-2 [64] provides guidance on this, and [65] to [68] provide practical interpretations.

4.5.3 The methods of terminating any cable shields (screens)

Where cables are shielded types, the method used for terminating cable shields in connectors and glands can have a huge effect on the EM performance of cables, and on how it varies over the lifecycle.

[69] to [72] provide guidance on this as regards PCBs, circuits and equipment products. IEC 61000-5-2 [64] is the relevant IEC publication providing guidance on this issue as regards systems and installations, and [65] to [68] provide practical interpretations.

4.5.4 Constraints on connectors and glands, and their assembly

The installation might require various EM and/or physical constraints on the types of connectors and/or glands to be used, and might also require special assembly requirements for them.

The EM characteristics of different types of cable connectors and glands vary very widely, so it is important to specify the types to be used in every case. A manufacturer's part number for the connector or gland can also help, and is often taken to be a guide to the characteristics required. In some cases it may be that only a specified manufacturer's part number should be used for certain purposes in the installation of the EFS, and where this is the case it should be made very clear in the installation instructions.

The method used for terminating cable shields in connectors and glands can have a huge effect on the EM performance of cables, and on how it varies over the lifecycle, see [64] to [72].

4.5.5 The electrical power supply requirements (power quality)

Electrical power distribution or generation suffers from a large number of possible conducted EM disturbances (RF currents and voltages, surge overvoltages and overcurrents, fast transient bursts, etc.) often at the highest levels of any of the cables associated with an EFS.

There are also a number of power quality EM issues such as waveform distortion (harmonics and interharmonics), dips, dropouts, short and long interruptions, voltage sags, swells, flicker, etc., that afflict power distribution networks and generated supplies. These are also classified as EM disturbances, even though they may occur over timescales of seconds.

The EM characteristics of the electrical power supply can be very important indeed for the achievement of EM safety, so it is important that they are assessed very early in a project (see Steps 1 and 2) to help create the EM specification of the EFS (see Step 3). For the same reason it is very important that the specifications for the electrical power supply are applied to the installation, so that the installer can ensure that they are achieved (for instance, by taking the power from a suitable point of common connection in the distribution network, or providing an appropriate generator or uninterruptible power supply, (UPS)). [74] and [75] provide a great deal of information on Power Quality and techniques for improving it.

It is also important to specify the EM requirements for the electrical power supply so that the owner of the EFS can ensure they are maintained despite future changes to the site over the anticipated lifecycle of the EFS (see 4.6.4).

4.5.6 Any additional shielding (screening) required

The EM mitigation measures required by the EFS might require shielding to be applied during its installation (for example, the provision of a screened room). Where such requirements exist, they should be clearly specified in the Installation Instructions.

Such additional shielding can be specified either by a description of the exact build state to be achieved (requires detailed assembly drawings) or by specification of the EM characteristics (attenuation versus frequency range, for each type of radiated disturbance) that it is to achieve, plus the test methods that should be used to verify it.

For more information on shielding, from PCBs to whole buildings, see [64] to [72].

4.5.7 Any additional filtering required

The EM mitigation measures required by the EFS might require filtering to be applied during its installation. Where such requirements exist, they should be clearly specified in the Installation Instructions.

Such additional filtering is generally specified in terms of the EM characteristics (attenuation versus frequency range) that it is to achieve, and the test methods that should be used to verify it. It is also possible to specify it by a description of the exact build state to be achieved (requires detailed schematics and assembly drawings).

For more information on filtering, from PCBs to whole buildings, see [64] to [72].

4.5.8 Any additional overvoltage and/or overcurrent protection required

The EM mitigation measures required by the EFS might require overvoltage and/or overcurrent protection to be applied during its installation (for example, the provision of a lightning protection system meeting certain performance specifications). Where such requirements exist, they should be clearly specified in the Installation Instructions.

Such additional protection is generally specified in terms of the EM characteristics (the attenuations achieved for various waveshapes of surges) that it is to achieve, and the test methods that should be used to verify it. It is also possible to specify it by a description of the exact build state to be achieved (requires detailed schematics and assembly drawings).

For more information on overvoltage/overcurrent protection, from PCBs to whole buildings, see [64] to [72].

4.5.9 Any additional power conditioning required

As discussed in Steps 1 and 2, part of the initial design process is to assess the foreseeable EM characteristics of the electrical power supply provided at the site, and design the EFS accordingly. As a result of this process, an EFS might require additional power conditioning to be installed during installation.

There are many kinds of power conditioning available, depending on the power supply characteristics to be controlled. Where such additional power conditioning requirements exist for the installation, they should be clearly specified in the Installation Instructions along with the methods to be used for verifying that the requirements have been successfully implemented.

For example, it is not uncommon for some sort of emergency power back-up to be required, for a few seconds or tens of seconds, to permit the EFS to shutdown safely in the event of an interruption in the power supply, or in the event of a serious degradation in power quality that could affect functional safety (e.g. a voltage sag of more than 10% below nominal).

In the case of life-support equipment, or where shutdown would cause significant risk to life, disruption or financial losses, power back-up could be required for minutes, hours, maybe even for days or weeks. Such requirements are commonly satisfied by the installation of appropriately-rated uninterruptible power supplies (UPSs). These typically use super capacitors, batteries, or fuel cells for their energy storage, with the super capacitor and battery types relying on switching to local power generation for long-term back-up.

For more information on power conditioning, see [74] and [75].

4.5.10 Any additional electrostatic discharge protection requirements

The levels of electrostatic discharge (ESD) that an EFS should be protected from can be reduced by a variety of techniques, including the use of electrically dissipative materials for floorings, furnishings and clothing to reduce furniture and personnel ESD. Appropriate electrical bonding and charge dissipation measures can reduce the levels of discharges from ESD caused by machinery. Other techniques for ESD control include maintaining the air to be above a specified minimum level of humidity (typically >25%); and blowing air that has been ionised by an AC source so that it is neutral overall but more conductive than normal air at that humidity.

Where such additional ESD reduction requirements exist for the installation, they should be clearly specified in the Installation Instructions, either in terms of their detailed construction requirements, or the performance to be achieved, and the test methods to be used to verify their effectiveness.

For more information on ESD suppression and protection, from PCBs to whole buildings, see [64] to [72].

4.5.11 Any additional physical protection required

As discussed in Steps 1 and 2, the reasonably foreseeable physical environment that an EFS has to endure over its anticipated lifecycle should be assessed early in a project, so the designer knows how to realise the EM characteristics so that they remain adequate over the lifecycle.

It may be that during the installation of the EFS, additional physical mitigation measures might need to be applied so that the EFS remains safe enough over its lifecycle. These might include roofs or enclosures to protect from rain and snow, air-conditioning or heaters to protect from condensation, anti-vibration floors or mountings, etc.

Where such additional physical protection requirements exist for the installation, they should be clearly specified in the Installation Instructions, either in terms of their detailed construction requirements, or the characteristics to be achieved, and the test methods to be used to verify that they are providing the required characteristics.

4.5.12 Any RF Reference requirements

The RF Reference should provide an equipotential network over a specified range of frequencies (for example: to handle surges, transients, and RF noise currents, etc.).

The frequency range should be identified and the RF Reference structure designed and constructed so that it provides a low enough impedance, given the frequencies and currents concerned, to achieve the degree of equipotentiality required.

For more information on creating RF References, from PCBs to whole sites, see [64] to [72].

4.5.13 Protection against corrosion

The materials used in the EFS and in its installation, and the physical environment in which the EFS will be operated, should be taken into account during design from the point of view of corrosion.

There are three basic types of corrosion:

- a) Oxidation
- b) Fretting
- c) Galvanic Corrosion

Fretting corrosion is a form of accelerated atmospheric oxidation that occurs at the interface of conducting materials undergoing slight, cyclic relative motion. In electrical contacts involving non-noble metals, fretting action can cause rapid increases in contact resistance, even creating open circuits in a matter of minutes in extreme cases [77].

Oxidation always occurs on the surfaces of metals that are exposed to gasses or liquids containing air (or at least oxygen), and metal oxides are either non-conducting or semi-conducting, both of which are bad for electrical contacts and RF-bonds. In the case of iron, most steels, and aluminium the oxides are very tough, and their thickness will almost always build up to such an extent that reliable electrical connections and RF-bonding cannot be ensured.

Galvanic corrosion is a different corrosion mechanism from oxidation or similar chemical conversion mechanisms described above. It arises because different metals have different positions in the electro-chemical series, so when connected by an electrically conductive liquid (called an electrolyte, for example ordinary water) they form an 'accidental battery' and a self-generated current flows in them. The most anodic of the metals gets eaten away by this current, eventually disappearing (or turning into non-conductive or semi-conductive corrosion products) altogether. If the choice of metals is poor for the environment, galvanic corrosion can completely destroy an electrical connection or RF-bond very quickly indeed, maybe in just a few weeks.

The installer/commissioner might need to employ certain parts or materials (e.g. this connection must be made with a tin-plated crimp terminal; after assembly this connection must be protected against exposure to liquids using grease to specification xxx, etc.) or techniques (e.g. do not locate this junction where it could be exposed to liquids).

For more information on preventing corrosion, see [68] and [78].

4.5.14 The procedures, materials and expertise to be used

The procedures, materials and expertise used should help ensure that the required EM characteristics, which could affect safety risks or risk-reductions are achieved, despite the effects of the physical environment over the reasonably foreseeable lifecycle.

The design of the EFS should consider whether specific procedures, materials and/or expertise are needed during installation and/or commissioning. Where this is the case, appropriate steps should be taken to ensure that the specific procedures, materials and/or expertise that are needed, are employed – by whoever does this work – and that they are provided with all of the information they need to carry out their activities correctly.

The QC system should ensure that the integration/installation of the EFS in its operational site follows all of the intentions of the EFS designers. In the case of an EFS in a vehicle, the vehicle is its operational site.

Where the consequences of errors, malfunctions, etc., in an EFS could be severe, it can often be financially least risky for all of the installation and commissioning to be done by the organisation that designed the EFS. The designers should still provide all the necessary information.

The designers should leave nothing to be decided by the people doing the installation/commissioning, unless this is unavoidable, in which case they should ensure that the people making those decisions have the necessary information, tools, procedures, materials, expertise, etc.

Verification and validation of correct installation should use one or more of the techniques described in Step 5 as appropriate, and will generally include actual inspections, checks and testing that ensure that the design

features relating to achieving functional safety over the lifecycle with regard to EMI are correctly implemented in the installed EFS.

The amount of verification and validation work, and the levels of detail and accuracy employed, should be commensurate with the levels of safety risk or risk-reduction required.

Inspections compare the assembly against its design documents. For example, checking whether the correct types of EMC gaskets have been fitted properly; the screens of screened cables terminated correctly in connectors; the correct types of cables used and routed correctly.

Checks of EM characteristics can be performed using simple tests using close-field probes and similar low-cost RF transducers, using ad-hoc methods as appropriate. Such checks are quick and low-cost techniques for discovering a range of assembly errors especially with regard to mitigation techniques such as shielding and filtering.

4.6 Operation, maintenance, repair, refurbishment, etc.

To ensure the correct operation, maintenance and repair of the EFS, to achieve the desired EM safety performance over its anticipated lifecycle, the EFS designer should take the issues described below into account in the design and its documentation.

This process will result in certain design features and/or instructions for the operator and maintainer, to overcome any problems identified by the below that could have a negative impact on the achievement of acceptable safety risks (or risk-reductions) by the EFS over its lifecycle.

In the case of safety-related systems according to IEC 61508, for example the safety systems operating in a railway train or power generating plant, it will almost certainly be the case that the people doing the operation and maintenance are at least knowledgeable about safety and/or EMC, and appropriately-written operation and maintenance instructions will be implemented by suitably-skilled people, even if they have to be subcontracted or trained especially for this.

In such situations, it is often the *combination* of the activities carried out by the operators and maintainers, with the features of the EFS, that results in the desired levels of safety risk or risk-reduction.

However, at the other extreme, some types of EFS might be purchased directly by consumers who are not at all knowledgeable about safety and/or EMC, and who cannot be relied upon to carry out any special activities at all. Examples include domestic appliances, certain types of medical appliances, vehicles such as motorcars, motorcycles, boats, etc.; sports, entertainment and leisure equipment, etc.

Such EFS might be operated and maintained by people who are disadvantaged or disabled (e.g. partially sighted, blind, deaf, weak, ill, missing limbs, intellectually challenged, etc.). Nevertheless, such EFS should be safe enough, or achieve the desired levels of risk-reduction. The issues below should be taken into account, but the resulting design solutions will likely be very different from those applied to industrial EFS.

4.6.1 Comprehensive Instructions

Comprehensive Instructions are required, that include any operating procedures necessary to maintain adequate EM characteristics for the EFS over its operational life. The purpose of these is to help achieve safety in real life, and also to help limit liability in the case of safety incident. These Instructions can have a variety of names, e.g.:

- Operational requirements in the User Manual, User Instructions, Operator Manual, etc.
- Maintenance requirements in the Maintenance Manual, Maintenance Instructions, etc.
- Repair requirements in the Repair Manual, Instructions for Repair, etc.

The maintenance and repair instructions might be sections in the User Manual, especially where the user/operator is expected to perform maintenance and/or repair too.

Whatever the instructions are called, they should clearly and unambiguously describe all that should be done by the owner and/or operator and/or maintainer and/or repairer/refurbisher so that the EFS remains as safe as its designers intended it to be – for its whole lifecycle.

Instructions should include requirements for the maintenance procedure to be logged and evidentially confirmed. They should also always include a legal disclaimer that makes the person who was supposed to carry out the instructions liable if they were not followed exactly.

They should clearly describe the EM and physical environment specifications of EFS, plus everything that the user should do, for all lifecycle stages, to ensure that the EFS maintains its EM and physical characteristics to help ensure adequate safety over its reasonably foreseeable lifecycle.

This should include the operating procedures necessary to preserve EMC characteristics and EM safety. It should also include the specifications for any planned maintenance necessary to preserve adequate EM characteristics over the reasonably foreseeable lifecycle, for example checking/replacement of transient suppressors, batteries, etc., before their characteristics degrades too much.

It may also be necessary to include specifications for cleaning materials, techniques and procedures that should be used to preserve EM characteristics over the anticipated lifecycle (e.g. do not paint specified bonding areas, do not use wire brushes on plated areas, etc.).

In the case of EFS intended to be used by consumers, repair and refurbishment instructions might be as simple as “return to manufacturer using the original packaging”, combined with warnings against attempting any repair oneself.

4.6.2 Maintenance, repair, refurbishment procedures and planning of mitigation measures

Overcurrent and overvoltage protection devices often have a limited effective life, which depends on the EM environment they are exposed to. Filter capacitors can go open-circuit due to overvoltage surges. Some types of physical mitigation measures can degrade over time.

Where failure of a mitigation measure could increase safety risks, planned maintenance should check and replace them as necessary before they fail.

Planned maintenance may also be required to check and repair cable shields and terminations, gaskets, filters, RF bonds, galvanic isolation, misuse, damage, unapproved modification, etc.

Cost-effective maintenance benefits from designing-in appropriate test features, to help maintain EM performance over the lifecycle (e.g. providing diagnostic test points at external connectors).

4.6.3 Maintain EM/physical characteristics despite repairs, refurbishment, etc.

Maintaining the desired EM and/or physical characteristics of an EFS after its realisation is made much easier if all of the elements of its design that are critical for the achievement of these characteristics are shown on the drawings, or identified in their part numbers. So it should be part of the design process to identify all of the ‘EMC/physical critical elements’, marking-up drawings and raising new part numbers accordingly.

Maintenance and repair should not alter any critical elements of the build state, even down to very tiny details, and should use exactly the same critical parts, assembly methods and processes, as the original. Some gaskets may need to be checked and replaced, and all of the fixings must be refitted with their correct torques.

Partial or full EM and/or physical testing may be required after the repair or refurbishment, to ensure that the EM/physical characteristics have not been compromised.

The general rule is – “Do not design it if it cannot be repaired” – and this is good advice for an EFS that is large, has a high-value, or is permanently installed. But some household appliances, consumer goods, high-volume or low-cost products are intended never to be maintained, and as a result their functional safety design can be more challenging – especially because large numbers of people could be exposed to their safety risks at any one time.

Each maintenance, repair or refurbishment activity may be specified as being carried out by the user, by the original creator, or by a specified third party. It is very important for the designer of the EFS to make quite clear to all involved what is required to be done, who is required to do it, and when.

Maintenance sometimes requires that certain installed components serving to ensure EM characteristics be removed or disassembled (e.g. doors, access panels, etc.). Those people performing the maintenance work should thus be warned of the risks linked to any malfunctions that may result from the lowering of the level of

immunity. Although this can be done in the manual, warning signs or panels should be posted on or near the equipment in question.

Resumption of normal operation of the EFS, either manually or automatically, should be done only in the absence of any foreseeable risk.

It is now increasingly practical for EFS to test itself, log faults, etc., and report its status via cellphone networks or the Internet, so that maintenance or repair visits only occur when necessary.

4.6.4 Constraints on the EM/physical environments

It may be necessary to control changes in the EM/physical environments, to prevent threats to the EFS from arising that were not included in its original design.

Restrictions should be applied on the operation of other equipment that might not achieve an adequate level of EM compatibility with respect to the equipment in an EFS. This can include constraints on proximity to other equipment, including mobile transmitting equipment (especially mobile phones, walkie-talkies, but possibly including other mobile radio transmitters including Wi-Fi, Bluetooth and the like).

NOTE: In some applications it is practical or necessary to control the external EM environment. For example, an airliner only travels in designated routes avoiding known areas of high field strength, and the captain has the authority to control the use of personal electronic devices used by staff and passengers.

However, it is generally impossible to control the future EM environment of EFS that is operated by consumers. A consumer might be warned not to use the EFS in close proximity to a radio transmitter, but how are they to know, for example, that a Wi-Fi enabled laptop PC employs a radio transmitter? They might be warned not to use the EFS in strong magnetic fields, but how are they to know where these might be found?

A User Manual should include descriptions of EM/physical environments to be avoided, written in layman's language, but of course it is foreseeable misuse for a user to ignore, or forget to follow such instructions. It is also foreseeable use/misuse for someone who cannot be expected to have an understanding of such EM/physical issues, to apply User Instructions incorrectly.

Depending on how the above issues are treated in the risk assessments, and on the levels of risk (or risk-reduction) required, it may be necessary for the EFS to be designed on the basis that it could in future be exposed to EM environments that did not exist when it was designed.

It is often possible for a designer to predict the future EM environment for, say, the next five years. EFS that must achieve acceptable safety risks (or risk-reductions) for a longer anticipated life should use appropriate design techniques (e.g. sensing the EM/physical environments, see 4.3.20) where the user cannot be expected to provide the necessary control.

4.6.5 Disassembly/reassembly techniques to preserve EM characteristics

The designer should provide the user with appropriate instructions to help ensure that disassembly and reassembly, for example for maintenance or repair, does not degrade the EM characteristics of EFS below what is necessary for the maintenance of acceptable safety risks.

In some cases, especially where risks must be low, or risk-reduction high, the instructions might need to include requirements for verification or validation of the EM characteristics of an EFS after reassembly, using techniques similar to those mentioned in 4.6.6 (Periodic testing).

4.6.6 Periodic testing (proof testing) of critical components

Some components can wear out or suffer from corrosion or ageing over their life. For example: transient suppressors are only rated for a given number of transients of given energies, and so should be considered to have a specified operational lifecycle in a given EM environment. Joints and gaskets in shielding can suffer degraded EM characteristics due to friction and corrosion.

Where the EM characteristics of such components are important for maintaining the desired EM characteristics of an EFS, the designer should provide the user with appropriate instructions on their periodic testing (proof testing) to help ensure that the necessary EM characteristics of the EFS are maintained over its anticipated lifecycle.

An alternative to proof testing might be to employ a planned maintenance regime, as briefly described in 4.6.2.

There are many types of proof testing that could be effective, for example: visual inspections (e.g. for gasket damage, broken wires, etc.); electrical checks/tests (e.g. contact resistance, clamping voltage, leakage current, etc.); tests of EM characteristics (e.g. shielding effectiveness, filter attenuation, etc.), etc.

The interval between the proof tests should be specified based upon the anticipated rate of degradation of the components, and should be much less than the time over which the degradation is expected to become unacceptable. The lower the level of risk, or the higher the level of risk-reduction achieved by EFS, the shorter should be the proof test interval, and the more searching and stringent should be the proof tests themselves.

Where a component is becoming too degraded, instructions should be provided for its correct repair/replacement (also see 4.6.2 and 4.6.7) so as to preserve the necessary EM/physical characteristics of its EFS over its anticipated lifecycle.

Periodic proof testing can be made less costly if the components are designed so they can easily be tested and replaced where necessary.

The Manuals should advise the user to maintain an authenticated log of the periodic testing carried out, so as to have a stronger legal evidential position if required.

It is now increasingly practical for an EFS to test itself, log faults, etc., and report its status via cellphone networks or the Internet, so that maintenance or repair visits only occur when necessary.

4.6.7 Periodic replacement of critical components

Some EM-characteristics related components have a limited life expectancy. Some will 'wear out' due to repetitive overvoltage/overcurrent transients or physical overstresses.

Such components may require planned maintenance regimes, which can be made less costly if the components are designed so they can easily be checked and replaced where necessary.

Examples include: surge protection devices; filters connected to AC supply or long cables; gaskets around doors; batteries for program memories, etc.

Also see 4.6.2.

4.6.8 Verification of the absence of corrosion

As explained in 4.5.13 there are three basic types of corrosion: oxidation; fretting, and galvanic corrosion.

The materials used in the EFS and in its installation, and the physical environment in which the EFS will be operated, should be taken into account during design from the point of view of the corrosion that could occur over the operational lifecycle.

Where considered necessary to maintain the EM performance of the EFS over its anticipated lifecycle, all parts or connections, joints, seams, etc. should be assessed for their likelihood of suffering corrosion over time, and Instructions provided on:

- Where to check for corrosion
- When to check parts or connections, joints, seams, etc.
- How to identify excessive corrosion
- How to deal with the corrosion
- How to confirm that the EM performance of the EFS has not been degraded by the above activities

4.7 Modifications and upgrades to hardware and software

The EM/physical characteristics necessary for the EFS to achieve acceptable safety risks (or risk-reductions) over its anticipated lifecycle should not be compromised by any modifications (including but not limited to additions, reductions, improvements or upgrades) to its hardware or software.

A software or firmware 'bug fix' is a modification, as are upgrades in hardware, software or firmware and variants produced for a specific customers or market segments.

Any modification to EFS hardware, software or firmware must be treated as if it was a new design, starting from the appropriate Step in the process described in this Guide.

For many modifications this will be a trivial process, but it is a process that should be gone through nevertheless.

This should not lead to a complacent frame of mind in which the 'letter' of the process is followed but not the 'spirit' – many unpleasant and/or costly incidents have been caused by modifications that had been assumed to be trivial, but with the wisdom of hindsight were revealed not to be.

4.7.1 Assessing the effect of proposed modifications and upgrades

The EM performance of the EFS should be maintained at the required levels over its anticipated lifecycle, despite modifications, upgrades, etc.

Before any modifications or upgrades are carried out, their effects on the EM characteristics of the EFS should be assessed. The EM immunity of the modified/upgraded EFS should be maintained at acceptable levels given its EM environment and level of risk, or risk-reduction.

The emissions of the modified/upgraded EFS may also need to be controlled (level, frequency, modulation, etc.) so as not to have a negative effect on their safety risks or risk-reductions of other EFS. Steps 1 and 2 provide the necessary data on this.

The purpose of this assessment is to foresee any areas where the modifications/upgrades might unacceptably degrade the required EM characteristics of EFS.

Where this assessment shows that unacceptable degradation could occur, it is then continued to determine the actions that should ensure that when the modification/upgrade is carried out on the actual EFS, the resulting EM characteristics are adequate for the achievement of acceptable safety risks (according to the level of risk, or risk-reduction).

The result of this assessment will be instructions that describe any necessary detailed changes to the design of the modification/upgrade, and any necessary instructions for the detailed implementation of the modification/upgrade. A modification or upgrade might require the modification, upgrade or addition of EM mitigation measures such as shielding, filtering, transient suppression, etc.

These instructions should be provided to the appropriate personnel, and might need to include requirements for verification or validation of the EM characteristics of the EFS after the modification or upgrade has been carried out. Depending on the level of risk, or risk-reduction, these might use techniques similar to those mentioned in 4.6.6 (Proof Testing).

4.7.2 Maintaining acceptable EM and physical characteristics

It is important to ensure that modifications and upgrades do not reduce the EM or physical characteristics below acceptable levels, for the EFS concerned, and for any other EFS that might be affected (for example by changes in the emissions of the modified EFS).

Modifications and upgrades (to mechanical structures, hardware or software) to the design and construction of an EFS can affect its achievement of the necessary EM and physical characteristics over the reasonably foreseeable lifecycle. So the procedures and techniques that are necessary here are the ones relating to design, see 4.2 and 4.3.

Each modification or upgrade activity may be specified as being carried out by the user, by the original creator, or by a specified third party. It is very important to make quite clear to all involved what is required to be done, who is required to do it, and when.

4.8 The relationship between the EFS, its constituent parts, and mitigation measures

An EFS could simply be a single item of equipment, or a system or installation of any scale comprising any number of items of equipment.

EFS are subject to the EM/physical environments at their users' locations, and possibly also to significant EM threats from parts of themselves.

For the purpose of this section, a product is an item of equipment that is commercially available on the market, from manufacturers or their agents, e.g. an industrial computer, motor drive, etc. It might or might not have been designed for use in anything that might have an impact on safety risks, on the other hand it is possible that it is an EFS in its own right.

In this section, an example EFS is used to illustrate certain aspects of the use of EM mitigation techniques. Similar illustrations could be created for aspects of the use of physical mitigation measures.

This example EFS is comprised of one or more items of equipment. And each item of equipment in this example is either a single product, or incorporates one or more products – or even a number of subsystems (each one comprising a number of products), as shown in Figure 4.2.

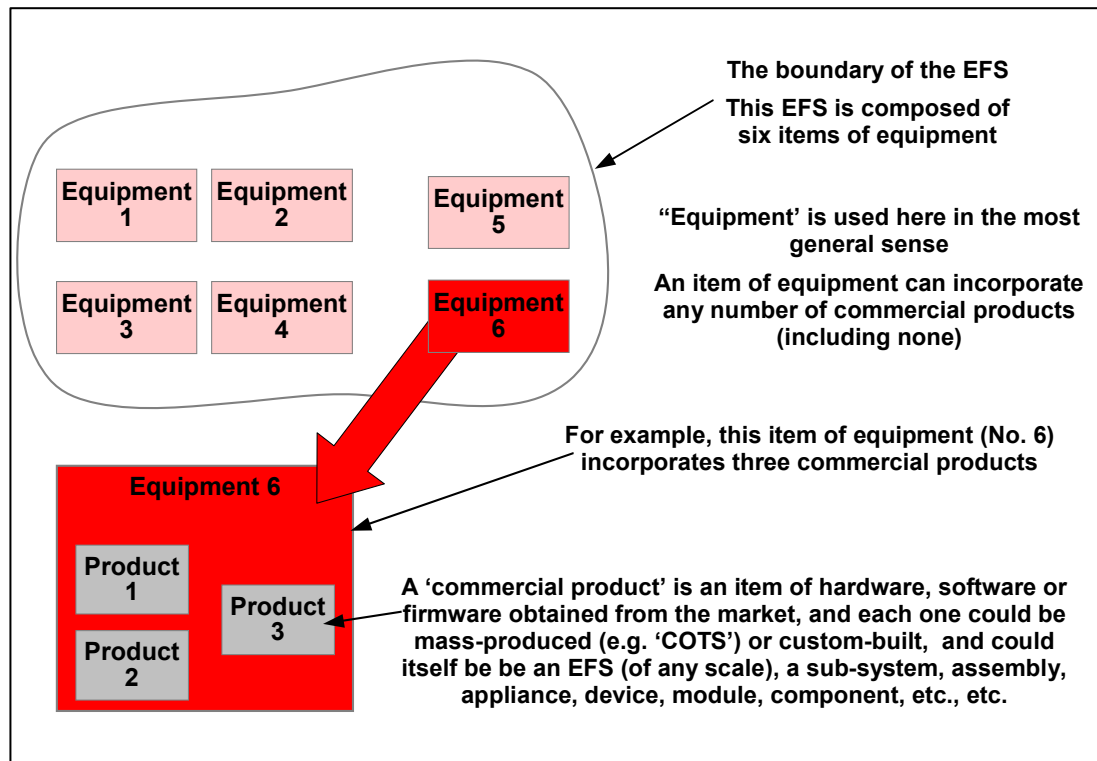


Figure 4.2 The example EFS consists of six items of equipment

Products purchased on the commercial market could, of course, be used by themselves to construct the EFS, without being incorporated into items of equipment, but this example EFS has all of its products installed within items of equipment.

In this discussion the terms EFS and product are very precisely defined – the first is the final goal of our EFS design project, the second is the parts we purchase commercially in order to construct it.

But the term equipment as used in this discussion is very general indeed and could be applied to any number of possible assemblies, sub-systems, systems, apparatus, appliances, etc., that form part of the EFS.

EM mitigation measures (such as grounding, shielding, filtering, galvanic isolation, overvoltage suppression, power quality improvements, etc.) can be applied at the following levels:

- The EFS itself
- A part of the EFS comprising one or more items of equipment (e.g. a segregated area with its own ground bonding network; a shielded room; etc.)
- An individual item of equipment (e.g. contained within a shielded/filtered cabinet)
- A part of an equipment (e.g. a shielded enclosure within an equipment)
- A product (e.g. by modifying it after purchase)

Employing typical IEC terminology (e.g. 61000-5-6 [63]) – we call the external EM environment ‘EM Zone 0’.

Each time we protect the EFS, or some part of it, by applying EM mitigation measures, we create a new EM Zone.

It is *very important indeed* that each set of EM mitigation measures are physically located at the boundaries of the EM Zone they create. The practical implications of this for assembly, construction, installation, etc., are described in detail in [66] to [69].

The first zones we create within EM Zone 0 are called EM Zone 1A, 1B, etc. Any zones nested within a Zone 1 are called EM Zone 2A, 2B, etc. Any zones nested within a Zone 2 are called EM Zone 3A, 3B, etc. – and so on.

One reason for using mitigation to create a new EM Zone, might be to protect one part of the EFS from the emissions from a different part of the same EFS. Figure 4.3 shows an example of this concept.

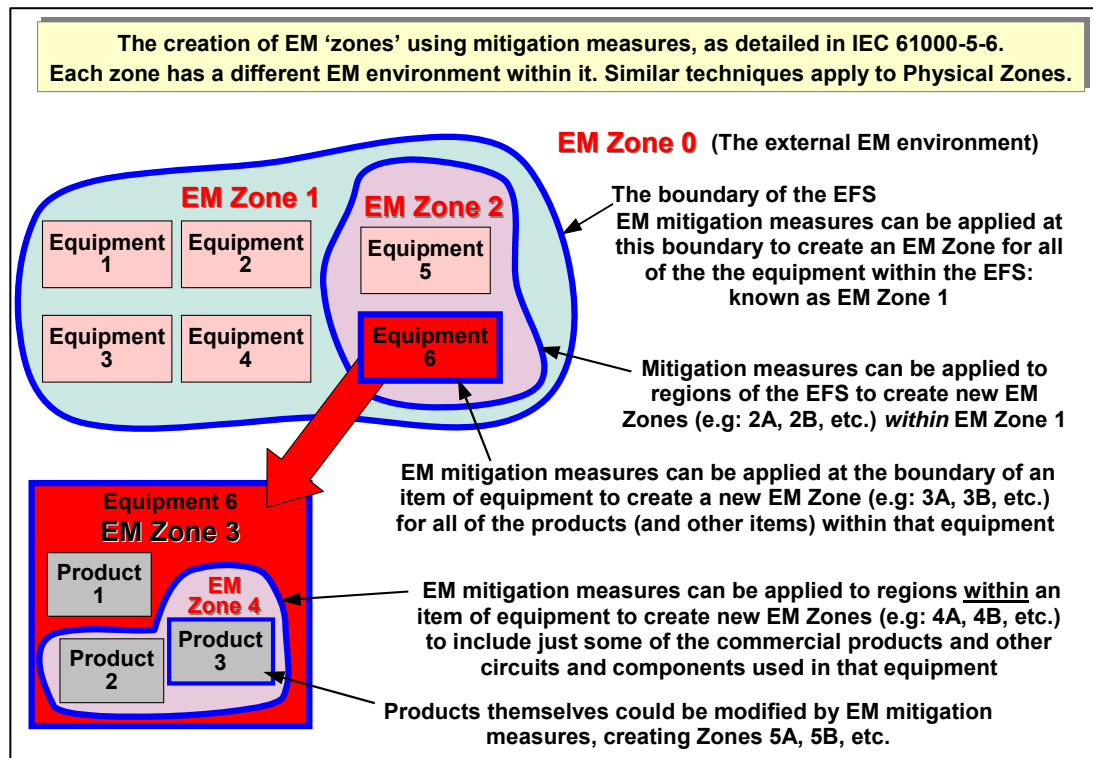


Figure 4.3 Relationships between EFS; 'equipment'; 'products' and EM mitigation

In the example of Figure 4.3 above, EM mitigation measures have been applied at the boundary of the EFS, making it all EM Zone 1.

Within the EFS, one area has had some additional EM mitigation measures applied, creating EM Zone 2. If there was more than one EM Zone at this level, we would number them 2A, 2B and so on.

Within EM Zone 2 is an item of equipment (No. 6) that has some additional EM mitigation measures applied to it (such as a shielded enclosure) and everything in this equipment is therefore in EM Zone 3.

All of the products comprising Equipment No. 6, in this example, are in EM Zone 3, so have three 'layers' of EM mitigation protecting them from the external EM environment. However, they only have one layer of EM mitigation protecting them from emissions from the equipment in Zone 2 (or protecting the equipment in EM Zone 2 from their emissions).

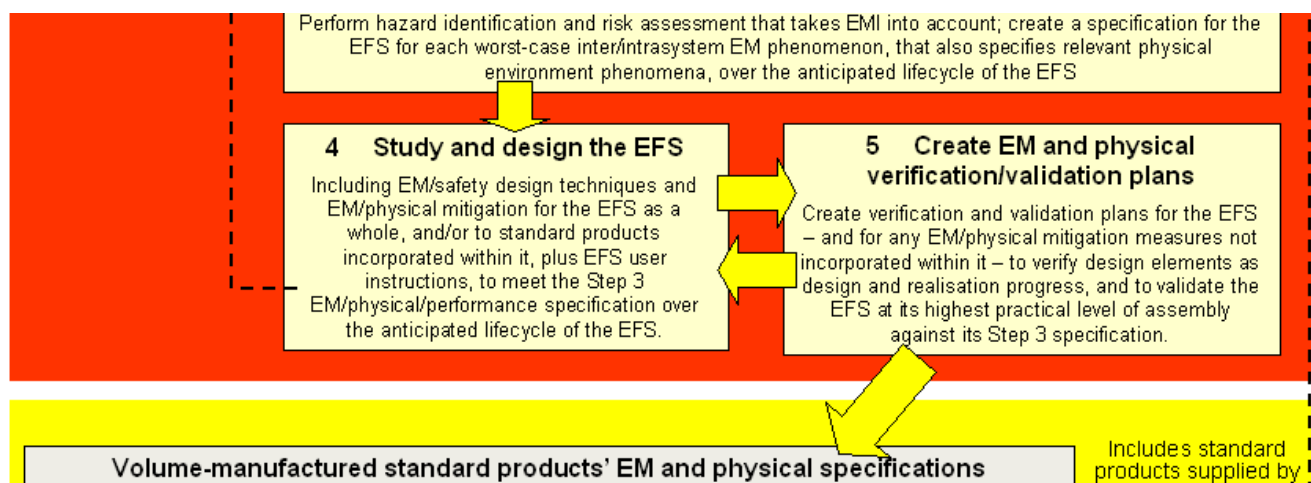
It is the job of the EFS designer(s) to determine the worst-case external EM environment, and the worst-case emissions from the various component parts of the EFS (see Steps 1 and 2 of our process).

The EFS designer(s) will then design the EM mitigation for each zone, and select the products to be purchased for use in that zone, with the ultimate goal of making the EFS safe enough despite its worst-case external EM environment (and also despite the EM threats it creates for itself).

For much more detail on practical methods of creating EM Zones for systems and installations, see [68], and for applying mitigation techniques to a cabinet to create an EM Zone within it, see [67].

5. Step 5: Create EM and physical verification/validation plans

Create verification and validation plans for the EFS – and for any EM/physical mitigation measures not incorporated within it – to verify design elements as design and realisation progress, and to validate the EFS at its highest practical level of assembly against its Step 3 specification.



5.1 Introduction

As was shown in Step 0 – the introduction to this EMC for Functional Safety process – EMC testing can never be sufficient *on its own* to demonstrate that risks are low enough, or that risk-reduction will be high enough, over the lifecycle of an EFS, taking its physical environment (including wear and ageing) into account. Test plans could be drawn up which would provide the necessary design confidence, but no-one (even governments) could afford their cost, or the very long time they would take.

No other safety engineering discipline, including software, ever relies totally upon testing a finished product. In fact it is very well recognised in safety engineering, and especially in functional safety engineering, that testing alone is insufficient. What they employ instead, and we now need to apply to EMC, is competent design engineering, plus a variety of verification and validation techniques, including some carefully-targeted testing.

Different designs of EFS may employ modified or different design techniques (see Step 4 of this Guide) and/or be used in different applications – no one design methodology is suitable for all types of EFS (to be time and cost-effective).

Where EFS designs and/or applications differ, verification and validation techniques may need to be adapted – and different techniques may need to be employed. The EMC testing employed may need to be adapted, or different tests applied. No one verification/validation plan or EMC test methodology is suitable for all designs of EFS (to be time and cost-effective).

Step 4 of our EMC for Functional Safety process (see Figures 0.2, 0.3 and 0.4) designed the EFS, using techniques as appropriate to its application, functions, and the EM/physical requirements of its EMC safety specification and risk assessment (from Step 3).

This Step 5 deals with planning the verification and validation of the EFS design, including its EMC testing, against the EM/physical requirements of its EMC safety specification (from Step 3). Most of the text and graphics in this Step deals with EMC testing issues, but that **does not mean** that testing is the most important verification and validation method of the several that must be applied. For example: Expert Review is often found to be the most powerful method for detecting design errors, and also one of the quickest and most cost-effective.

The planning of the validation and verification techniques needs to be performed by competent and knowledgeable personnel during the design phase (Step 4), because the two steps are interactive. It can be

possible to avoid lengthy and expensive verification and validation programmes by doing the design in a different way, and employing certain verification and validation techniques can sometimes allow design to proceed faster, or lower-cost parts to be used.

5.2 Planning for Verification, and for Validation

5.2.1 Planning the verification activities throughout a project

According to ISO 8402 (excluding its notes): **'Verification'** means "...confirmation by examination and provision of objective evidence that the requirements have been fulfilled."

In the context of this Guide, verification is the activity of demonstrating for each phase of the lifecycle, or for the various stages in the activities within each phase, that the deliverables meet, in all respects, the objectives and requirements set for that phase or stage within it.

So verification can be carried out as and when required, on various aspects of the design and realisation, as they progress. Each 'module' of the design (hardware or software) will be designed to meet specifications that are intended, eventually, to result in the EFS complying with the specification created by Step 3. These 'module' specifications should be verified as soon as there is a design to assess.

Some techniques suitable for use in verification are listed in 5.3.

As 5.3 shows, verification activities need not wait until something is assembled so that it can be tested, and for example peer-reviewing a design for an IC, circuit or software module before actually creating the item concerned, helps reduce the likelihood of requiring major design changes later in a project – and so help save time and cost.

For anything but the simplest EFS, having just a few verifications during a project runs the risk that a design iteration will have to redo a lot of work, and hence waste a lot of time and effort. For this reason, performing frequent verifications as the design and realisation progress is strongly recommended – because it provides many small 'course corrections' and so generally leads to a smoother, quicker, more cost-effective project.

Don't forget that the process of specifying the various 'modules' to be designed – the planning and specification of the detailed design activities – should also be verified using appropriate techniques at every opportunity. If the design planning or specifications are wrong, one or more aspects of the design will be incorrect but the error might not be discovered by verification techniques until the overall validation of the EFS itself (see 5.2.2).

5.2.2 Planning the validation of the EFS

According to ISO 8402 (excluding its notes): **'Validation'** means "...confirmation by examination and provision of objective evidence that the particular requirements for a specified intended use are fulfilled."

In the context of this Guide, validation is the activity of demonstrating that the EFS meets, in all respects, the EMC safety specification for that EFS.

So validation can be seen as a 'final verification' that the complete EFS meets the EMC safety specification that was developed for it (see 3.2).

Validation can occur before and/or after installation, the choice generally depending on the point at which ownership changes from the creator to the owner or end-user.

Some techniques suitable for use in validation are listed in 5.3.

5.2.3 Iterations

As has been described in 1.6, 2.5, 3.8 and 4.2.4, the EM and physical environment specifications can change during a project, making Steps 1-5 iterative, resulting in changes to the Step 3 EMC Safety Specifications, and changes to the Step 4 risk assessments and design of the EFS, during the life of the project.

These changes will often need corresponding changes in the verification and validation plans covered by Step 5. The management of the EFS project (see 0.10) should facilitate this process, so that the EFS always

achieves its safety risks (or risk-reductions) in the EM and physical environments that actually occur during the operation, decommissioning and disposal stages of its lifecycle.

5.3 Some examples of suitable techniques

Whilst this section describes a number of verification and validation techniques, it is not comprehensive and there are other techniques that could be equally effective. The following is just a list of some techniques that have been found useful in the past, and there is no obligation to use any or all of them. Some of the techniques might not be suitable for some types of EFS.

How the EFS designers choose to verify and validate that the desired levels of safety risks (or risk-reductions) will be achieved over the anticipated lifecycle of the EFS, is entirely up to them.

- a) **Demonstrations.** Such as demonstrating that the functional safety requirements have been correctly implemented.
- b) **Checklists.** For example, to ensure that EMC design measures have been observed, applied and implemented correctly.
- c) **Inspections.** For example, checking that the assembly and installation have followed the EMC requirements correctly.
- 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 (shown in Figure 0.4) and the various stages of the activities within each phase.
- e) **Independent reviews.** Companies and institutions (e.g. universities, training organisations) can have corporate cultures that include bad or non-ideal practices, or what we might call 'blind spots', but they generally cannot detect them in themselves.

So, independent reviews of EM and physical design are recommended, especially for EFS required to achieve very low safety risks, or very high risk-reductions. Even if the reviewers are not as expert as EFS designer(s), their different perspectives will help detect problems caused by cultural (institutional) issues.

- f) **Audits.** These include verification processes for specification, design, assembly, installation. Audits are a quality control (QC) activity and the designers should not carry them out themselves. Instead, people familiar with QC auditing, who are independent from the design process, should carry them out.
- g) **Non-standardised checks and tests.** Because EMC testing has become standardised, many people tend to think of EMC testing only in terms of the standard test methods, such as MIL-STD-461F, IEC 61000-4-x, etc. But there are very many non-standard EMC checks and tests that can (and often should) be done to improve confidence in safety integrity.

For example, a low-cost portable spectrum analyser and close-field probe can be used to check the correct assembly of shielded enclosures, shielded connectors, and filters. This is a qualitative technique, rather than a quantitative one, but nevertheless can be very useful in improving confidence. It can also be usefully applied during the operational stage of the lifecycle to check that shielding and filtering performance is being maintained.

Similar close-field probing techniques can check purchased devices (e.g. ICs) or equipment (e.g. power supplies, computers, etc.) to detect bad batches or errors in assembly, before they are incorporated into the EFS.

Many other EMC 'checking' methods can be designed and used to improve confidence without adding significant cost.

- h) **Individual and/or integrated hardware tests.** Different parts of the EFS are assembled step-by-step, with checks and tests applied to ensure that they function correctly at each step.
- i) **Validated computer modelling.** Computer-aided EMC design has made large strides in recent years, and is now routinely used in certain critical industries ([79]) to successfully reduce design and test timescales without sacrificing reliability.

All computer modelling is based on simplifications, so it is important to validate any predictions by appropriate testing. But once the model is shown to replicate the test results with sufficient fidelity, it can be used to quickly simulate the results of numerous similar tests that would be too costly or time-consuming to perform in real-life.

- j) **Testing** (e.g. factory acceptance test or on-site testing)

Most EMC engineers automatically think of EMC testing as the only way to prove adequate EM performance. But as described in Step 0, mentioned in 5.1 above, and described in detail in [80] [81] [82] and [83], an EMC test plan that could – on its own – give sufficient confidence in EM performance for safety reasons, will always be much too lengthy and much too costly.

EM immunity testing is supplementary to the other verification and validation measures. Clause 9.1 of [4] says: “In most cases there will be no simple or practicable way to verify by means of testing that EM immunity is achieved.” Despite this, appropriately designed testing is a powerful verification/validation technique, and some suitable techniques are discussed below.

5.4 EM immunity test methods for functional safety

EM measures required for the achievement of acceptable safety risks, or desired levels of risk-reductions, should be evaluated using EM testing and highly accelerated life testing, to demonstrate sufficient confidence that individual EM design aspects (e.g. circuit, shielding, filtering, surge transient or ESD suppression, etc.) will reliably achieve at least their minimum EM performance requirements over the anticipated lifecycle of the EFS.

Such tests should be carried out as early in a project as possible, to reduce technical risks and save time and cost. Some of them will not need to have a functioning unit available – for example the effectiveness of filters, and shielded enclosures, cables and connectors, can be tested in isolation.

It is also good practice to apply the immunity tests to the EFS, after installation and commissioning. For smaller systems this may be possible in a test laboratory, but larger systems may need to be tested on-site. On-site EMC test methods exist, such as [84], but some might prove too difficult, in which case they should be applied at the highest practicable level of EFS integration. Care should be taken to apply them so that they realistically simulate the way in which EM phenomena will affect the whole EFS. For example, when testing an EFS that uses redundant channels, all of the channels should be exposed to the EM environment simultaneously – testing one channel at a time proves nothing at all about the safety of the EFS.

All immunity tests should be based upon accepted test methodologies, such as the IEC 61000-4-x series, Def Stan 59-411 [91], MIL-STD-461F [76], etc., competently modified (where necessary) to better simulate the real-life EM environment where the EFS is to be operated, and/or to improve confidence that the test results are meaningful for its real-life safety risks (or risk-reductions).

For instance, the IEC’s basic test method for radiated RF immunity, IEC 61000-4-3, is limited in terms of – angle of incidence; frequency range; modulation type; modulation frequency; and numbers of simultaneous modulated frequencies – any/all of which could have a significant effect on the performance of electronic devices and software.

Real-life radiated RF environments are always more complex than those simulated by the unmodified IEC 61000-4-3 test method, and can cause very different and complex effects. Similar considerations apply to the other IEC 61000-4 series standards, see [80] [81] and [82], and this problem is recognised in [4].

Equipment is especially susceptible at the operating frequencies of its internal hardware and software processes, as described in 4.2 and [83]. But high-enough levels of interfering signals can overdrive devices, causing errors, malfunctions, maybe even damage, at any frequency.

A continuous RF test method currently used in some safety-critical industries uses unmodulated signals stepped in small increments over the range 0 to 30kHz, with a one-second pulse OFF then ON again at each step. Some test methods (e.g. IEC 61000-4-16) only test common mode, whereas differential mode tests may also be required to properly simulate the EM environment.

Above 30kHz, the test signal at each frequency step has an unmodulated period, followed by ‘chirp’ modulation at least over the range of ‘especially susceptible frequencies’ below 30kHz, then is pulsed OFF for one second then back ON again using an unmodulated CW signal.

Such ‘CW, chirp, plus OFF/ON’ tests must be slow enough to be sure of detecting any errors, malfunctions or damage given the response times of the functions being monitored. If necessary, time may be able to be saved by monitoring critical internal signals to avoid having to wait for long time-constants to respond. Special fibre-optic probes are available for such monitoring, but intelligent test design might avoid the need to use them.

If the ‘especially susceptible frequencies’ have previously been identified (see 4.3.8 and [83]), the testing time might be able to be reduced by modulating only at those frequencies, instead of a full chirp. Where exposure to pulsed sources is possible (e.g. radars, pulse weapons, etc.) their relevant frequency range

should be covered using appropriate pulse modulation waveforms, especially any waveforms with a frequency content that includes any of the 'especially susceptible frequencies'. At each tested RF frequency, a CW test with a one-second pulse off and then on again is usually required.

During immunity testing, all variations in functional performance should be recorded, and analysed afterwards to see if they had any relevance for safety.

5.5 Testing for physical environment, wear, ageing and lifecycle

The physical environment over the lifecycle of the EFS can degrade its EM performance. Shock and vibration, bending forces, temperature extremes or cycling, wear and tear and many other lifecycle mechanical, physical, climatic and biological influences can affect the RF stability of some types of circuits, and degrade the performance of EM mitigation measures such as shielding, filtering and transient suppression, for example by corrosion.

There are well-established test methods for most physical phenomena. In highly accelerated life tests ('HALT') life-testing experts apply one or more physical test methods to quickly discover likely end-of-life characteristics.

But some physical stresses might occur that are not covered by established standards, for example the use of abrasive cleaners, or the repetitive opening and closing of a door or inspection panel. It may be necessary to devise realistic tests for such physical lifecycle stresses.

To verify that the EM design is adequate requires EM testing during the application of the physical stresses such as static mechanical forces, shock, temperature extremes, condensation, etc. Appropriate close-field probing techniques can detect whether the EM performance of an EM mitigation measure has been unacceptably significantly degraded by the physical stress.

However, EM testing is only needed before and after highly accelerated life tests that simulate the accumulated effects of the physical environment, regular cleaning and maintenance, ageing and wear.

Where electronics are protected from the physical environment by an external means, such as an enclosure, physical tests can be carried out on the enclosure itself, as shown in Figure 5.1, maybe using close-field probing instead of the antenna shown.

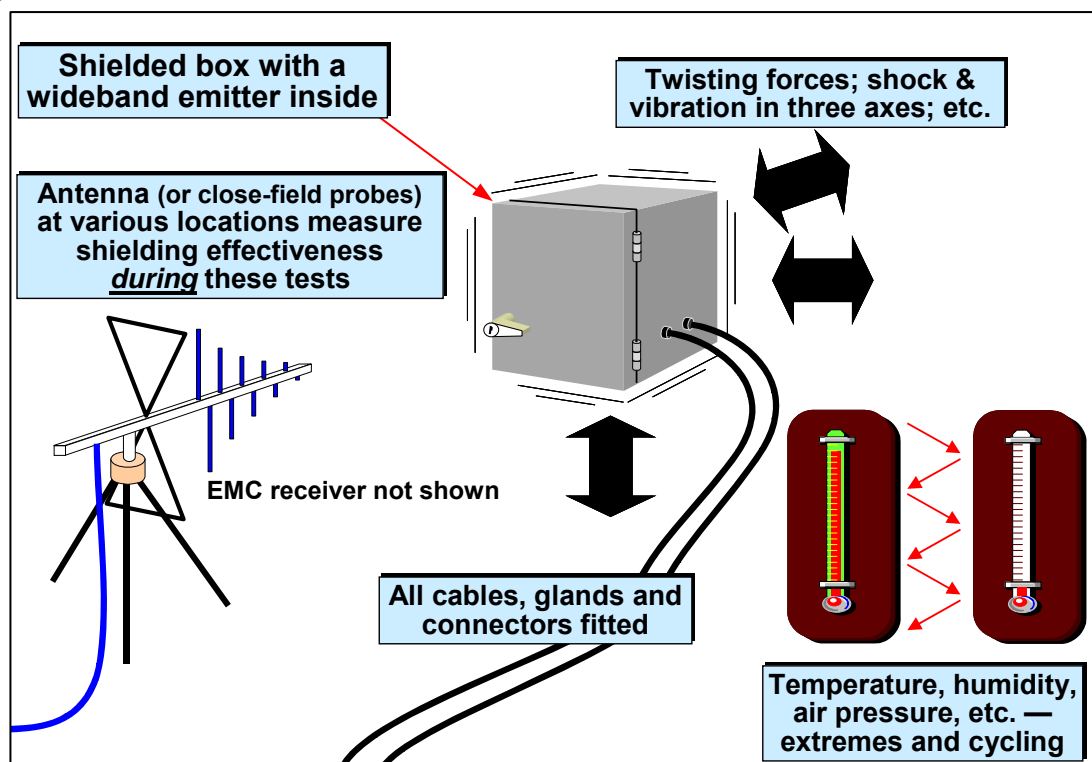


Figure 5.1 EM testing *during* physical stress testing

This has the advantage that the enclosure can be proved to be adequate as a parallel activity to the electronic and/or software or firmware design, helping to shorten timescales and reduce overall project costs.

Highly accelerated life test plans must be designed by accelerated life-testing experts, based on the physical environment specification of the EFS from Steps 1 and 2 [85]. Adding EM tests to such tests need not add significantly to the overall time or costs, if the tests are designed appropriately.

Where suitable data exists or can be calculated for a particular EM design aspect, and when it is fully documented in the project's records, combined EM and physical testing may not be necessary. For example, tests such as those depicted by Figure 5.1 might not be needed where an enclosure manufacturer has already applied appropriate physical and highly accelerated life tests and measured their effect on EM performance (having first checked that the manufacturer's claims can be relied upon).

5.6 Testing radiated EM immunity in reverberation chambers

Anechoic testing is unlike most real-life radiated EM environments, so Reverberation Chamber methods have been developed to give more confidence [11] [87] [88]. Unlike anechoic chambers, their results can be correlated mathematically with the reflectivity of the operational EM environment. An example of a reverberation chamber is shown in Figure 5.2. Stirred-Mode test methods are an alternative way of using Reverberation chambers.

Reverberation chambers and their RF power amplifiers cost a great deal less than anechoic chambers, and thorough testing can take less time than in anechoic chambers because there is no need to test with many angles, and with vertical and horizontal antenna polarizations.

A reverberation chamber test method currently used for some safety-critical avionic systems rotates the chamber's 'stirrer' or 'paddlewheel' over a full revolution using between 20 and 120 angular steps.

At each step, radio fields are generated in the chamber, comparable in frequency range and magnitude with the foreseeable worst-case EM environment(s). The frequency range is covered in small steps (e.g. 0.1%). At each step the field is modulated with the appropriate 'CW, chirp plus OFF/ON pulse' (see 5.4), or other modulations (see 4.3.8), at a rate that is slow enough to be sure to detect any errors or malfunctions in the functions being monitored.

Where the EFS is too large, or the frequencies too low, or when testing on-site with no transmitting license, conducted coupling test techniques may be able to replace radiated methods. But conducted testing is not a true alternative to radiated testing – so it may be more realistic to use striplines, TEM cells, Helmholtz coils, or other test methods.

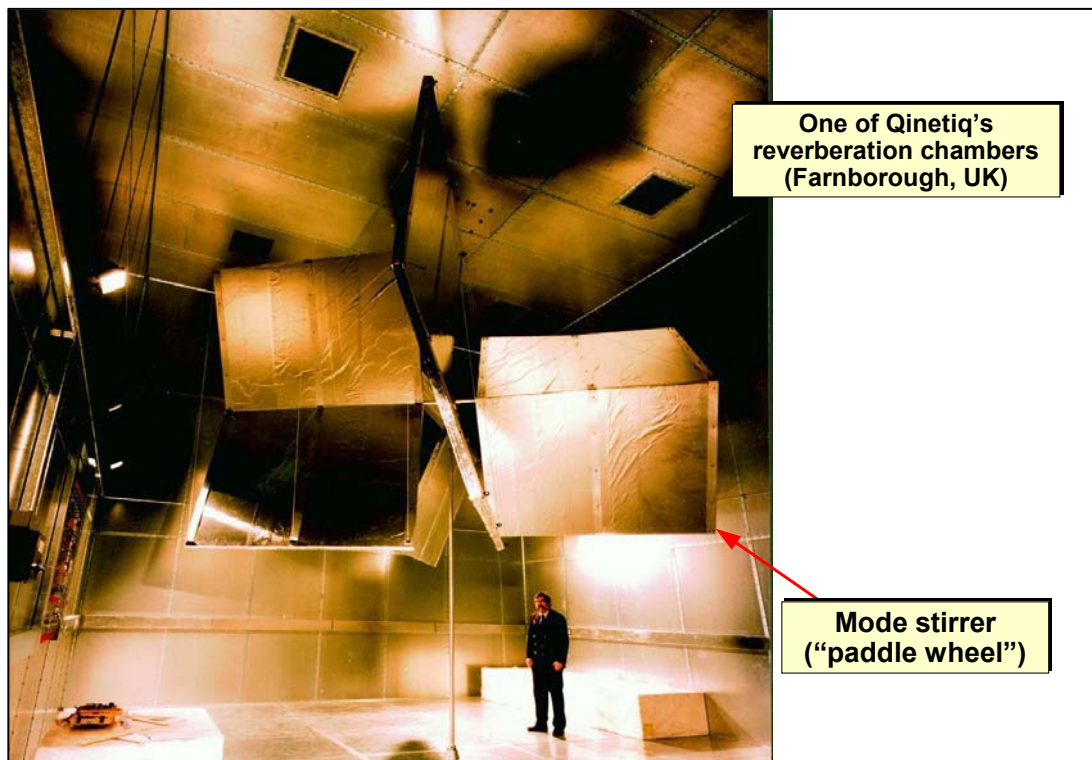


Figure 5.2 Example of a reverberation chamber

5.7 Testing transients, surges, ESD

The EM immunity of electronic designs based upon counters and state-machines, and of programmable electronic technologies that employ software or firmware, depends strongly on the digital activity in the circuit from nanosecond-to-nanosecond. The operation of the digital hardware devices causes a variety of types of electrical noise, which degrade the noise thresholds. When certain digital operations are performed, for a period of typically between a few hundred picoseconds and a few tens of nanoseconds, the noise threshold can be significantly degraded, so a transient EM event occurring at just that time can cause an error or malfunction, whereas it might not be capable of doing that the rest of the time.

In the case of software or firmware, the especially susceptible states might depend on inputs and algorithms. It should be part of their design to ensure that the numbers of digital signal transitions occurring simultaneously are never so large as to significantly degrade the noise threshold.

Similar variations in electrical activity in some analogue circuits can also result in degraded EM immunity at certain times.

For example, a common speed sensor interface uses a coil to pick up pulses of voltage from a magnet attached to a rotating shaft. The transducer output is connected to a comparator to 'square its signal up' to create a regular train of rectangular pulses to feed into a counter or microprocessor. Normally, the output from the transducer is well above the comparator's threshold and any reasonably foreseeable noise due to EMI has a negligible effect. But at low speeds the peak output voltage from the transducer may only be a little higher than the comparator threshold, and EMI at typical levels could cause multiple threshold-crossings, resulting in an incorrect speed signal.

Continuous EMI tests discover these especially susceptible situations – providing the EFS is exercised over the full range of inputs and operations so that they will all occur often enough to be detected. But when testing with transients, such as fast transient bursts, surges, and electrostatic discharge (ESD), it is very difficult to ensure that the peak of the transient occurs during the periods when the circuits are especially susceptible to EMI. Extended testing periods might enable this problem to be dealt with.

Another way of dealing with this testing problem is to use computer simulation to determine when the most susceptible circuit periods occur, and whether they are very much more susceptible than during typical operation. If they are significantly more susceptible, design changes might be able to reduce them to more typical levels.

Such simulation will require the extraction of 'stray' couplings, 'ground bounce' and 'power bounce' caused by PCB traces, connectors, cabling, maybe even by the packaging of the ICs themselves, and including them all in a circuit simulations (e.g. using SPICE). Computer-aided design tools that can achieve this with good accuracy exist – they are not yet very low-cost but even so they could be very cost-effective.

Another technique is to synchronise the timing of the transient to the circuit clock, or to some circuit state (like a state-driven trigger on a digital oscilloscope), then vary the relative timing of the transients so that over the period of the test they 'hit' on every mode of circuit operation.

Clearly, these two techniques can be combined to save testing time, so that transient testing is synchronised to the circuit clock and only performed during periods when the circuit is especially susceptible.

A third technique is simply to perform the transient, surge or ESD test as usual, but repeat it many more times than would be normal, to increase the confidence in the test. The lower the risk levels to be achieved, or the higher the risk-reductions, the more confidence is required in the validity of the testing and so the longer the tests will be. Exactly how long the tests should be performed, for a given level of confidence, is hard to quantify without some knowledge of the rate of occurrence of these especially vulnerable periods, or how to induce them.

5.8 Test levels and uncertainty

The design of the EFS is related to the desired levels of safety risks, or risk-reductions (from Step 3) and the EM and physical environments (from Steps 1 and 2). Confidence in the design is achieved by the validation and verifications techniques employed, as explained in 5.1.

To achieve a given level of confidence in EM and/or physical immunity testing, the EM and physical threat specifications will need to be higher than the environmental threats by a 'test margin' that takes care of the various uncertainties. There are uncertainties in:

- a) Specifications of the lifecycle EM and physical threats

- b) The stresses actually applied during immunity tests
- c) The 'natural' variations in the EM and physical characteristics of individually manufactured EFS of the same design (e.g. due to component tolerances, variations in assembly and installation, etc.)

For example, MIL-STD-464 adds a 6dB test margin for safety-critical and mission-critical equipment, and a 16.5dB margin for ordnance.

Figure 5.3 shows that when an immunity test is performed exactly at the specified threat level, for example a test at 10V/m to simulate an RF field in the operational environment of up to 10V/m, there is only a 50% chance that the test was actually carried out at or above the desired level.

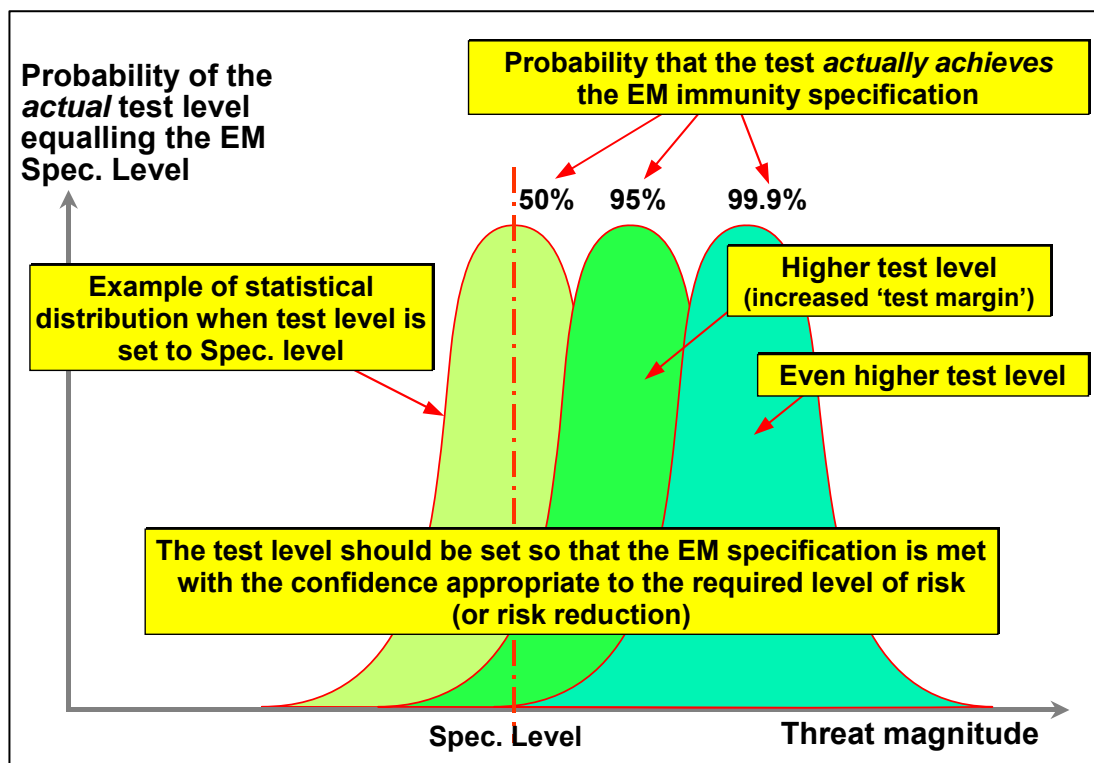


Figure 5.3 Uncertainty, statistics, and test margins

There are standard methods for adding together various types of uncertainty, taking their type of statistical distribution into account, for example [89]. Assuming a Normal (Gaussian) distribution (for example) in Figure 5.3 – increasing the test level by a test margin of one standard deviation improves the confidence that the test level reached/exceeded the specification to 68%. A test margin of three standard deviations improves it to 99.7%; and four standard deviations achieves 99.99%.

When applying IEC 61508 and its derived standards, the level of confidence achieved by the testing should generally be *at least* the same order of magnitude as the required SIL. For example, SIL 3 represents a probability of dangerous failure of a safety function 'on demand' or 'in a year' of between 0.01% and 0.1%, which is comparable with the 99.99% confidence given by testing above the specified test level by a test margin of four standard deviations. The same considerations apply when aiming for an acceptable level of risk, or desired level of risk-reduction.

To avoid testing at very high levels, with its attendant risks of over-design and unnecessarily high costs, it is important to use test methods and quality control that achieve low standard deviations.

Where the EFS employs 'EM Zones' protected by EM mitigation measures (e.g. filtering, shielding, transient suppression, etc.), see 4.8, some or all of the EMC tests applied to the equipment in the protected zones may not need to be as severe as the overall EM specification of the EFS.

Example: If the worst-case lifecycle radiated RF threat, plus the test margin to achieve sufficient test confidence, required a test level of 1000V/m, employing an enclosure that can be relied upon to achieve at least 40dB attenuation (over the anticipated lifecycle, despite the worst-case physical environment) would require the equipment housed within it to be tested at only 10V/m.

The effectiveness of the mitigation measures also needs to be verified, but for techniques such as filtering or shielding over their linear regions there is usually no need to test at the worst-case levels plus the test margin – their effectiveness in dB can be measured using low test levels.

Where a purchased enclosure is provided with all pertinent EM performance data, it may not be necessary to test the effectiveness of its EM mitigation at all. In such cases it is always necessary to ensure that the manufacturers' data can be relied upon, taking into account whether the measurement methods used to obtain the enclosure data are relevant for the EM environment.

For example, shielding data may only be given for 'plane waves', which are EM 'far-fields', whereas the EM environment might suffer from magnetic near-fields, which would generally be attenuated far less than plane waves, at a given frequency. Where supplier's data is incomplete, or suspect, the enclosure could be tested by the EFS designer(s), using methods that better simulate the real-life worst-case EM environment that is anticipated.

Where it seems impossible to avoid RF testing at very high levels, reverberation chamber methods (such as those described in [90], or recommended for civil aircraft by [18]) can be much more cost-effective than 'traditional' anechoic chamber tests. Where 'EM Zoning' is employed, methods of using low-level RF tests to predict the outcomes of high-level tests, to avoid the cost of high-level tests, can be used (see IEC 61000-4-23 for example). Testing with high levels of surges and transients often requires finding or making suitable test equipment.

Because of the complexity and non-linearity of modern electronic technologies, including software, firmware and systems, passing an immunity test at the highest level does not always ensure that the test would also be passed at a lower, more commonplace level. Confidence can be improved by repeating all types of immunity tests using a range of levels up to the highest.

5.9 Testing simultaneous phenomena

Simultaneous phenomena are a feature of real-life EM environments (e.g. transmissions on multiple radio channels; continuous RF fields plus mains transients or ESD, etc.) as discussed in 1.3. They are also a feature of real physical environments (e.g. temperature plus vibration; temperature plus humidity, etc.). As discussed in [85], these issues should have been captured in the specification used to control the design and formulate the validation/verification plans.

Testing with multiple simultaneous RF threats is already applied to some military aircraft [79], and to some digital TV receivers [92], and multiple-signal RF generators are commercially available. So testing using simulated real-life RF environments is an option that should be considered.

Testing that applies different types of phenomena simultaneously is not uncommon in physical/climatic testing, and is normal in highly-accelerated life testing, but is (almost) unknown in EMC testing. Appropriate analysis techniques can generally be used to achieve sufficient confidence in safety performance despite simultaneous EM phenomena, without the need to test more than one phenomenon at a time.

However, it is possible to test with different types of EM phenomena at the same time, and some such tests might need to be employed in some cases, to improve confidence when very low risks, or very high levels of risk-reduction are required. Any such tests would need to be very carefully designed and planned, to achieve the desired confidence without disproportionate increases in timescales and costs.

5.10 Testing emissions

It is usually assumed that all that is needed for EMC for Functional Safety is to ensure that the EFS is immune enough. But it is possible for the emissions from an EFS to exceed the levels and/or frequencies assumed when the intrasystem effects were analysed (Step 2) to help create the EM safety specification in Step 3, see [85].

Also, as briefly mentioned in sections 1.5 and 3.6, the emissions from an EFS must not cause problems for other EFS in their vicinity, or sharing the same conductors (e.g. AC mains power, Ethernet, etc.).

So it is also important to employ verification and validation techniques like those discussed above, to ensure that the emissions from the EFS and/or its component parts are within their design limits, after assembly, installation and commissioning. It is also important to have sufficient confidence (given the acceptable level of risk, or desired level of risk-reduction required) that they will remain so over the anticipated lifecycle of the EFS in its physical environment.

5.11 Testing faults and misuse

The design of the EFS (Step 4) should have taken into account reasonably foreseeable faults, use and misuse, and the effects that these could have on EM performance and hence on the safety risks or risk-reductions achieved by the EFS [83].

To achieve sufficient confidence in the safety performance of the EFS, it may be necessary to devise verification methods to determine whether the design adequately deals with such events. For example, EM and/or physical checks and/or tests could be repeated whilst simulating the various faults, use or misuse.

Careful planning will be required to ensure that such tests add usefully to the confidence in the safety of the EFS, without disproportionate increases in timescales and costs.

5.12 Testing safe shutdowns, alarms and the like

Safety engineers often seem not to care whether an EFS fails, as long as it remains safe enough. But in real life an EFS that shuts down or alarms too frequently will cause annoyance and/or financial costs to its operators or owners, and is likely to be modified in an unapproved manner, for example by disabling certain safety shut-down or alarm functions.

Such modifications by the user are a reasonably foreseeable outcome of unduly sensitive shut-down or alarm functions, so if an accident resulted the EFS creator could possibly be found liable.

So where safety shut-down, alarm and similar protective functions are to be tested, they should be tested twice. One test is required to ensure that they do not operate when they should not; the second test is conducted with the safety faults simulated, to ensure that they will operate reliably enough when they should.

5.13 Verification during operation

The design of an EFS, and its verification and validation, are based on assessments of the worst-case EM and physical environments (from Steps 1 and 2) that often include assumptions that should be verified after the installation of the EFS. EM and physical mitigation measures can degrade over time, and certain assumptions will have been made in their design. EM and physical environments can also change unpredictably over the anticipated lifecycle.

The desired levels of safety risks (or risk-reductions) are required over the whole lifecycle of an EFS, so it can be necessary to verify the EM and physical environments, and/or performance of certain mitigation measures, regularly throughout its life.

Automatic or manual verification methods may be used, taking appropriate actions as required based on their results, to maintain the required levels of risk, or risk-reduction, over the lifecycle of the EFS, despite the EM and physical environments.

5.14 Conclusions

It should now be readily apparent that proving that the EM characteristics of an EFS will be adequate for safety, over its anticipated lifecycle, requires a very great deal more than simply asking a test laboratory to perform some standard EM tests on shiny new equipment.

Since no organisation can afford the time and cost of an EM test plan that – on its own – could give sufficient confidence for the levels of risk or risk-reduction required, it is necessary to use a wide range of design, validation and verification techniques to reduce the amount of standardised EM testing whilst achieving the required level of confidence in functional safety performance over the anticipated lifecycle.

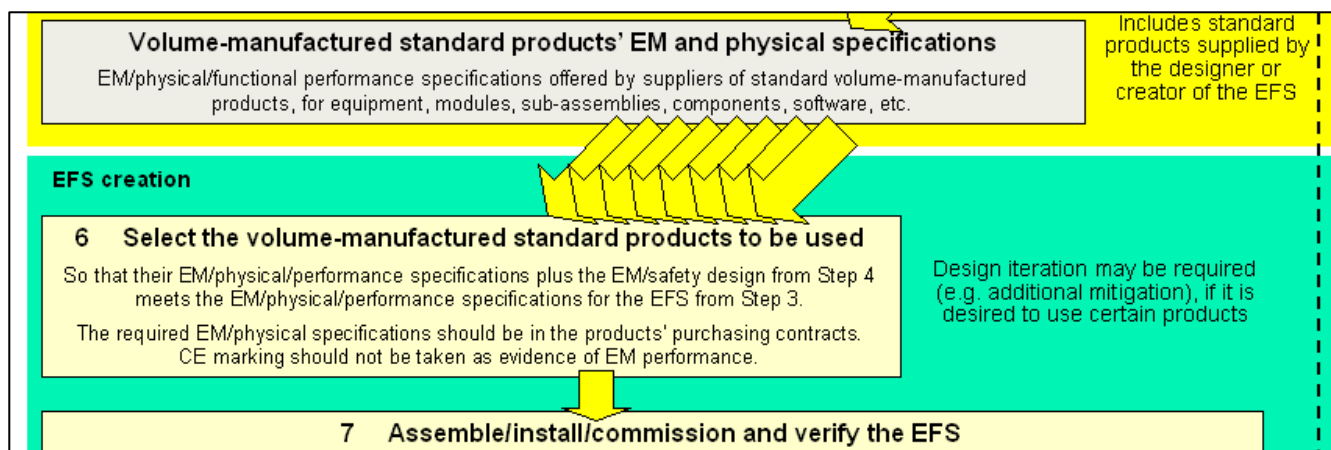
The planning of the verification and validation techniques needs to be performed by competent and knowledgeable personnel, in parallel with the design phase, using appropriate rigour as discussed in 0.10.4.

It can be possible to avoid lengthy test sequences, and hence achieve a more cost-effective and quicker project, by doing the design in a different way.

6. Step 6: Selecting standard products and/or specifying custom hardware or software items

So that their EM/physical/performance specifications plus the EM/safety design from Step 4 meets the EM/physical/performance specifications for the EFS from Step 3.

*The required EM/physical specifications should be in the products' purchasing contracts.
CE marking should not be taken as evidence of EM performance.*



6.1 Overview

This Step 6 only applies where the EFS designer(s) permits the EFS creator to have such freedom of choice.

In some EFS designs, especially simpler ones, some EFS designer(s) will completely specify everything about the EFS, including any standard volume-manufactured or custom-engineered items of hardware or software that are to be incorporated within it. The EFS creator then has no flexibility in this regard and Step 6 does not apply to that EFS.

NOTE: The remainder of this Section 6 of this Guide assumes that the EFS creator has been permitted by the EFS designer(s) to choose one or more standard volume-manufactured items of hardware or software, or specify one or more custom-engineered items of hardware or software, for incorporation within an EFS.

This Step of the process is concerned with selecting standard volume-manufactured items of hardware or software and/or specifying custom-engineered items of hardware or software, for incorporation into the EFS by the EFS creator (who may or may not be the same company as the EFS designer(s)).

The aim of this step is to ensure that – taking into account the EM/safety design of the EFS – the EM/physical/performance of any standard volume-manufactured or custom-engineered items of hardware or software incorporated into the EFS do not prevent it from meeting the EM safety specification of the EFS (see 3.2).

The required EM/physical performance specifications should be in the purchasing contracts for the standard products or custom items.

CE marking should not be taken as evidence of EM performance, see 6.3.3.

Remember that an EFS is never a component, part, subset, or a purchased standard product or custom-designed item that is incorporated into something else – it can only be the finished, complete entity that, when finally installed, is what provides the function that has a direct impact on safety risks or risk-reductions.

6.2 'Simple' and 'Complex' EFSs

6.2.1 What is the difference?

Two 'Overview of the EMC for Functional Safety Process' graphics were presented in Step 0: a 'Simple' EFS in Figure 0.2, and a 'Complex' EFS in Figure 0.3. Figure 6.1 shows the essential difference between a Simple and a Complex EFS, according to this Guide.

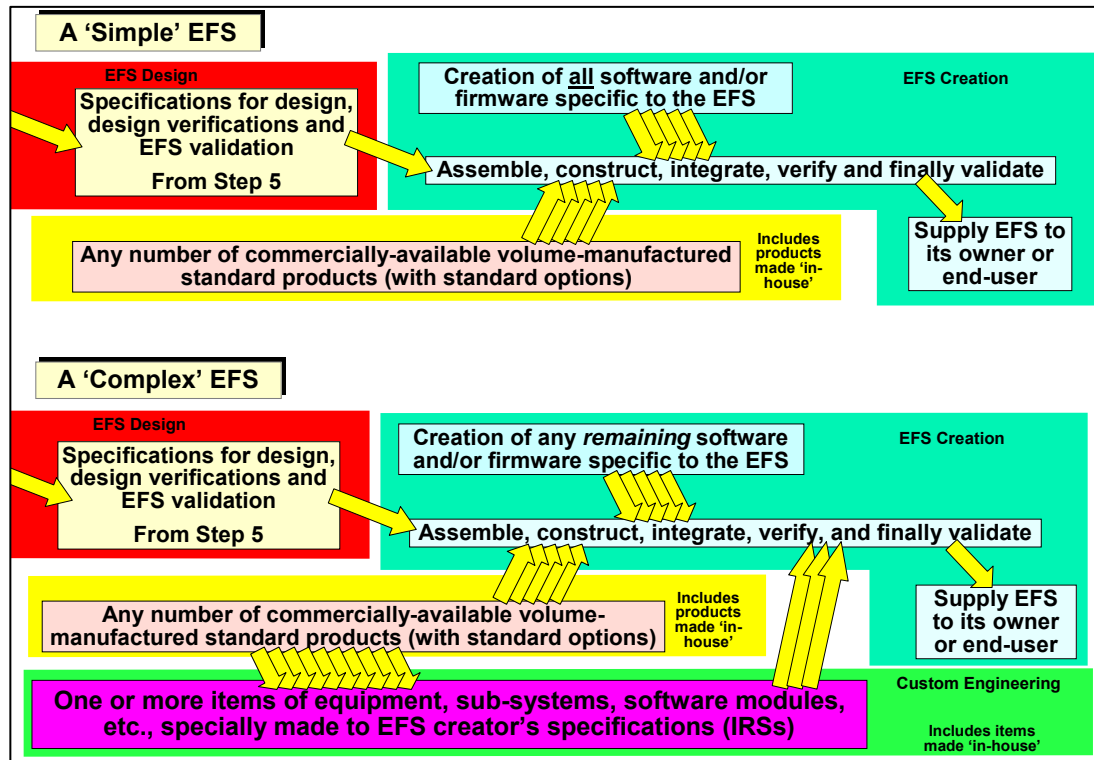


Figure 6.1 Comparison of 'Simple' and 'Complex' EFSs

6.2.2 Simple EFS

Figure 0.2 shows the process applicable to what this Guide calls a Simple EFS, and the upper half of Figure 6.1 also helps make it clear that a Simple EFS is one for which a single manufacturer (the EFS creator) is responsible for performing all of the realisation (assembly, construction, integration, etc.) of the EFS, and only purchases or otherwise obtains volume-manufactured standard products (i.e. parts, components, modules, units, etc.) to use in its realisation.

The volume-manufactured products employed are assumed by this Guide to be commercially available standard products that have not been custom-manufactured or customised to suit the EFS in any way (other than choosing from a list of standard options provided by their supplier).

An example of a Simple EFS might be an industrial system, comprising one or more interconnected cabinets, the cabinets containing standard industrial electrical/electronic products such as: relays; contactors; motor drives; programmable logic controllers fitted with a variety of standard input/output modules; DC power supplies; isolators/disconnectors; circuit-breakers; human-machine interfaces, etc. and for which any software or firmware programming was done by the EFS creator.

Another example might be an engine management unit for a motor car, comprising one or more interconnected modules containing PCBs on which are mounted standard electrical/electronic components such as: resistors, capacitors, inductors, power management ICs, microprocessor ICs, memory ICs, transistors, LEDs, relays, fuses, surge arrestors, etc., and for which any software or firmware programming was done by the EFS creator.

6.2.3 Complex EFS with one level of subcontracting

Figure 0.3 shows the process applicable to what this Guide calls a Complex EFS – one for which a single manufacturer (the EFS creator) is responsible for integrating a number of items (modules, equipment, sub-systems, etc.) to realise the EFS, where one or more of the items that are integrated were custom-designed and manufactured for use in that EFS by *other* manufacturers, each working to a specification provided by the EFS creator.

The remainder of the items being integrated by the EFS creator are volume-manufactured products assumed by this Guide to be commercially-available standard products that are not custom-manufactured or customised to suit the EFS in any way (other than choosing from a list of standard options provided by their supplier).

An example of a Complex EFS might be an industrial system identical to the example used for the Simple EFS above, but in which one or more units contained software or firmware programmes created by a third party – not by the EFS creator or his customer.

Another example of a Complex EFS might be an engine management unit for a motor car, comprising one or more interconnected modules that are designed and manufactured (including any software or firmware programming) to the EFS creator's specification, plus any number of interconnected modules that were manufactured entirely by the EFS creator.

Yet another example might be a railway signalling network, where the EFS creator is responsible for the provision of the whole signalling network, but some or all of the equipment and/or systems that comprise the network are manufactured by subcontractors to the EFS creator's specification, including some or all of the software programming.

We can regard this type of EFS as having one level of subcontracting. The EFS creator is the main contractor (and may or may not be the same company that designed it), and their suppliers of custom-engineered items of hardware or software are subcontractors.

6.2.4 Complex EFS with two or more levels of subcontracting

There are some types of EFS for which the EFS creator specifies and purchases custom-engineered items of hardware or software from other suppliers. But each of those items is itself like a Complex EFS, in that their manufacturers in turn specify and purchase custom-engineered items of hardware or software from other suppliers, and so on.

We can regard such types of EFS as having two or more levels of subcontracting. The EFS creator is the main contractor (and may or may not be the company that designed it), and the suppliers of custom-engineered items of hardware or software to their subcontractors are sub-subcontractors, and so on to sub-sub-subcontractors, etc.

Although this Guide only describes how to deal with Complex EFS with one level of subcontracting, the same techniques can be employed allowing any number of levels of subcontracting to be controlled from the point of view of EMC for Functional Safety.

A commonly observed cliché is: "A chain is only as strong as its weakest link" – and in the context of an EMC for Functional Safety process it is important to note that there is no level of assembly (or level of subcontracting) below which the possible effects of EMI over the lifecycle can be ignored.

For example: An EFS that is ensuring the flight safety of a 500-passenger aircraft, or preventing a nuclear power plant from melting down, will generally be a very Complex, highly-specified, highly-verified and validated electronic apparatus, but if a single low-cost electrical or electronic device in a critical path is upset by EMI, and this was not foreseen and dealt with by the EFS process, all the other work on EMC for Functional Safety could be valueless.

6.2.5 Simple EFS that is complicated in practice

Some types of EFS that this Guide calls Simple because the EFS creator is in control of all the design, realisation, verification and validation, can nevertheless be very complicated to design and manufacture because of the number of different items of equipment or sub-systems that must be incorporated to create the EFS.

An example might be a medical patient monitoring system for a hospital, comprising several different types of patient monitoring devices (e.g. video cameras, pulse detectors, temperature detectors,

liquid level detectors, etc.), all connected to 'bed stations', with all the 'bed stations' communicating with one or more management stations where nurses observe whether the patients in their care need assistance or not.

Another example might be a monitoring system for a nuclear processing site, comprising several different types of detection devices (e.g. video cameras, radiation detectors, temperature sensors, fluid leakage detectors, level detectors, etc.), all communicating with one or more management stations where personnel monitor automated processes to see if they need to intervene, sound alarms, etc.

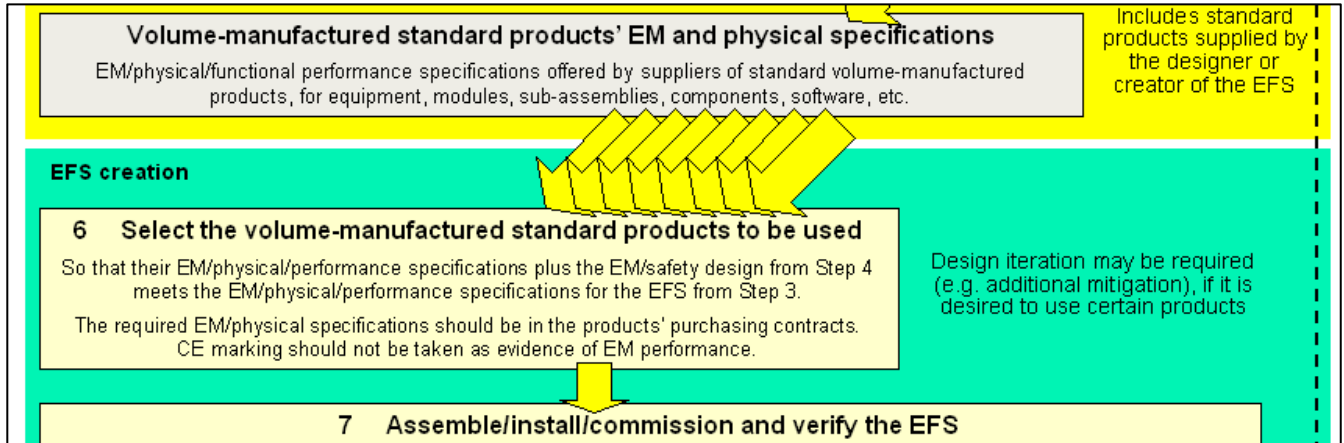
Even where the entire EFS is designed, realised, verified and validated by a single creator, different departments and/or teams could be concerned with different parts of the EFS.

In the above examples, the EFS are all distributed systems, and in most manufacturing companies it would be normal for different departments and/or teams to design and make the different types of cameras, sensors and other detectors; a different department or team to design and make the distributed communication system; and a different department or team to design and make the management station. There may even be a different department or team to write the software/firmware for some or all of the hardware departments or teams.

Controlling all these different specialist departments and/or teams can be almost as difficult as controlling subcontractors or other independent custom-engineering suppliers. So the approach described for the Complex EFS in 6.2.3 should be applied, treating the in-house departments and/or teams as if they were 'external' subcontractors or other independent suppliers.

The only difference should be in the negotiation of the 'purchase order' – but even then some companies operate their different departments as different profit centres, creating an 'internal market' that is very little different in practice from an external market, in which case even the purchase order negotiations will be similar.

6.3 The Step 6 activities for a Simple EFS



6.3.1 Overview

For a Simple EFS, the Step 6 activities are concerned only with the appropriate choice of standard volume-manufactured products (i.e. parts, components, modules, units, etc.) to use in its realisation.

But an EFS is not just items of equipment, it includes their interconnections. The design/selection of appropriate interconnections (for example: cables and connectors) and the use of appropriate good EMC engineering practices in their assembly and installation, are vital issues that should be controlled by this process.

Section 6.3.2 shows how to use EM mitigation to select products with appropriate EM specifications.

Section 6.3.4 discusses the problems created by working with the deficient product EM specifications that are presently offered.

Section 6.3.5 discusses how to deal with the problems of deficient product specifications.

These discussions and figures concern EM performance, but the same applies to physical performance.

6.3.2 Iterating product specifications and mitigation

Figure 6.2 shows an example of the iterative process by which volume-manufactured commercially-available standard products are chosen based upon the worst-case EM and physical environment the EFS might encounter.

As Figure 6.2 shows, it may be necessary for the EFS designer(s) to iterate the design of the EM mitigation measures (see 4.3.11), or even add new EM Zones (see 4.8) to create a suitably-low worst-case EM environment at the location of the chosen standard product.

What this means in practice, is that the design of the EFS might have to change – affecting the activities described in Steps 4 and 5 – as a result of Step 6.

The overall process diagram (Figure 0.2) does not show all these possible iterations, because they would make it too confusing. But it should always be remembered that designing and realising even a Simple EFS is not necessarily a linear progression of steps – indeed if shown on a Gantt or PERT project management chart it would be clear that for cost-effective project many of the tasks in Steps 4, 5, and 6 would be occurring concurrently, or at least overlapping considerably along the project time-line.

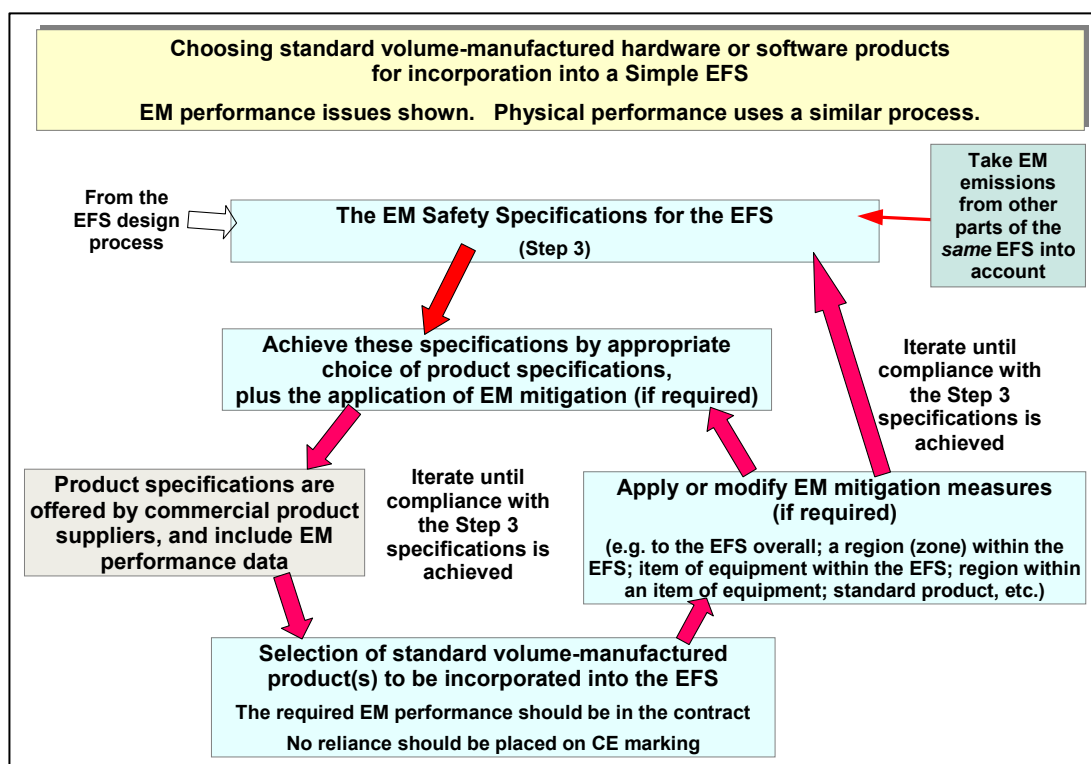


Figure 6.2 Choosing standard volume-manufactured products for a Simple EFS

Figure 6.4 shows an iterative loop stretching back from Step 6 to Step 3 (also see 3.8), but as 1.6 and 2.5 have shown the loop could also reach right back to Steps 1 and 2. The Step 2 iterations are shown in Figures 2.1 and 2.2.

6.3.3 CE marking should not be taken as evidence of EM performance

Don't forget that, as shown by the Step 6 task box in Figure 0.2, and the Step 6d task box in Figure 0.3, CE marking should not be taken as evidence of EM performance. This is because CE marking is a 'self-certification' process, in which the manufacturer does not have to involve anyone else at all – no EMC test laboratories, EMC Competent Bodies or Notified Bodies – and as a result his CE marking and Declaration of Conformity may not even be worth the paper it is written on.

The European Commission has acknowledged that for the countries where measurements have been made, between 25% and 50% of the products on the EU market do not comply with all of the Directives listed on their Declarations of Conformity [93], which is why it is planning a 'Market Surveillance' Directive that would force European Union Member States to at least do a minimum of enforcement of the CE marking scheme.

According to the UK case law used by Trading Standards Officers to enforce many laws, including the UK's EMC Regulations (which implement the European Union's EMC Directive, 2004/108/EC), accepting any document issued by a manufacturer regarding their own products, such as a marking, certificate or declaration, cannot be considered to be 'due diligence' for anyone other than a private individual or very small company that cannot afford to check properly.

No company involved with creating an EFS should accept any markings, certificates or declarations issued by their suppliers without taking adequate steps to check whether they are true or not.

There are many independent assessment bodies who will validate and certify customer's products and their declared performances. Using commercial products whose EMC performance specifications are validated by independent assessment bodies, is one way of achieving due diligence. Some suppliers are known to forge third-party assessment documents, so it is always a good idea to confirm them with the body purported to be the issuer.

Another way is to investigate suppliers' claims yourself, for example by requesting test certificates or test reports, and checking that they indicate the desired performance and checking with the test laboratory to see how independent they are. Yet another way is to perform simple checks or even full tests yourself to verify suppliers' performance claims.

The above due diligence techniques have been normal procedure for decades for retailers selling domestic appliances, such as electric kettles or electric blankets, to ensure that they really are as safe as their suppliers' claim. It has not often been applied to EMC performance because a lack of EMC performance has heretofore not been considered to be a cause of increased safety risks. But for EFS this is not the case, so these normal safety precautions should be applied to EMC performance too.

The lower the levels of risk (or the greater the amount of risk-reduction) to be achieved by an EFS – the more work would be required to achieve due diligence in ensuring that purchased or free-issued components of an EFS actually do have the EMC and physical performance that is claimed for them, see 0.10.4.

6.3.4 Deficiencies in product EM/physical specifications

The iterative process described in 6.3.2 and shown in Figure 6.2 seems straightforward enough, but the big problem faced by EFS designers in most industries is that volume-manufactured standard products *do not have EM specifications that are useful in this process*.

It is very tempting to imagine that a standard product that has complied with the EMC Directive by passing tests with (for example) radiated field strengths of 10V/m from 80 to 2700MHz using the latest version of the IEC 61000-4-3 test methodology, could be expected to *actually function as required* in radiated field strengths of up to 10V/m from 80 to 2700MHz.

However – even if the relevant test report had been seen (and could be believed) – section 0.10 of this Guide showed in some detail that there are at least a dozen reasons why such a test could not give an EFS designer sufficient confidence in EM performance for safety engineering reasons.

Continuing with the above example, there are ways of verifying and validating radiated RF immunity that would provide the EFS designer(s) with more confidence (maybe even sufficient confidence) and they are described in Step 5 of this Guide. Similar comments could be made about all of the EMC tests normally performed by volume-manufacturers, not just radiated RF immunity.

But at the time of writing, in most industries there are few (if any) suppliers of volume-manufactured standard products that employ appropriate EM design/verification/validation techniques that are *at all useful* for the EMC for Functional Safety process described in this Guide.

It is instructive to discuss one industry where this problem has been partly addressed – avionics. Military and civil aircraft EM test standards include a variety of EM threat levels depending on the physical location of the product concerned, that is: depending on its EM Zone (see 4.8). And their test standards benefit from a very exhaustive history of investigations into the worst-case EM environments in the various EM Zones in aircraft.

Unfortunately, even the avionics [18] and military [91] [76] EM test standards do not address all of the issues raised in section 0.7. For example, for radiated immunity testing they *require* testing with 1kHz square wave modulation, but only *recommend* testing with modulations that the equipment under test could be more susceptible to (see 4.3.8). However, some avionics manufacturers go further than the mandatory standards and employ methods like those described in 4.3.8 and 5.6, to have more confidence in the safety risks (or risk-reductions) achieved by their EFSs.

Similar comments apply to the physical performance specifications provided for volume-manufactured standard products.

6.3.5 How to overcome the lack of useful product data

There are a number of design/verification techniques that can be used in the absence of product data that could be useful in the process described in 6.3.1 and Figure 6.2, including....

- a) **Protective enclosures.** Enclose the product(s) that have deficient EM/physical specifications in an EM/physical protected enclosure that exposes the products to very benign EM/physical environments (e.g. $< 0.1\text{V/m}$ field strengths at any frequency).

The enclosure should reliably achieve the required EM/physical mitigation over the anticipated lifecycle of the EFS (proven in turn by appropriate accelerated life testing).

There should be a realistic assessment that the 'very benign' EM/physical environments achieved will actually result in the desired levels of safety risks or risk-reductions.

Such enclosures are readily available for protecting almost any standard products in almost any EM/physical environments, up to and including direct lightning strike. They are commonly used on warships to enable them to employ standard personal computers (what the Military call COTS – Commercial Off The Shelf equipment) and achieve reliable operation even under the most extreme operational situations.

Although suitable enclosures are costly and bulky, an advantage of this approach is that, if competently implemented, it might be possible to achieve sufficient confidence in EM verification for the parts of the EFS so protected without having to perform some (possibly all) EM testing on them – saving time and cost.

Where a complete EFS was so protected, it might be to achieve sufficient confidence in EM validation for the EFS without having to perform some (possibly all) EM testing.

- b) **Clever design.** Designers are clever people, and they can often find a way around a particular shortcoming in product data.

One solution might be to design the EFS so that the product concerned was less critical for the achievement of the desired safety risks or risk-reductions. (Ideally, the functional performance of the product would no longer have any impact on safety.)

Other approaches might employ one or more of the techniques briefly described in section 4.3, to reduce the sensitivity of the safety risks (or risk-reductions) to the functional performance of the product with deficient data.

(It is important to note here, that the use of two or more products of the same model in a parallel redundancy type of system architecture will not generally have any benefit for safety. If exposed to EMI that they are not sufficiently immune to – all of the parallel channels will fail in the same way at the same time.)

If the shortcoming in product data is identified early enough in the design/verification process, clever design solutions can be very cost-effective indeed, sometimes even free or with negative time/cost benefits.

However, if the project management does not discover such shortcomings until realisation of the EFS is well advanced, the same design solutions could be unaffordably expensive.

- c) **Additional product verification.** Assess the design/verification of the volume-manufactured standard product against the requirements of the EFS (taking into account any mitigation as shown in Figure 6.2). Where there are shortfalls in the data required for sufficient confidence, perform (or have the supplier perform) the necessary verifications to achieve the required confidence.

For example, in the case of the deficient radiated RF immunity data mentioned in 6.3.2, the especially susceptible frequencies could be determined (see 4.3.8) and additional tests done on sample products using modulation at those frequencies (see 5.6). To see how performance would be maintained over the lifecycle, the products could be put through appropriately-designed accelerated life tests (see 5.5) and its radiated RF immunity performance retested.

An important concern in this approach is design control and QC. As discussed in 4.4, there are numerous ways in which the EM/physical performance of volume-manufactured standard products can vary, and few manufacturers do sufficient production line EM/physical verification

(e.g. testing) to be sure that they are supplying products with similar EM/physical characteristics to the one that was originally tested for EM compliance.

Where an EFS creator is a good customer of a supplier, he may be able to persuade the supplier to undertake the design/verification/QC activities that he considers necessary. This sort of thing is commonplace in the personal computer, cellphone and automotive industries, because of their huge buying power.

But where an EFS creator is not such a big purchaser, they should institute the necessary QC activities at their own goods-in (goods receiving) departments.

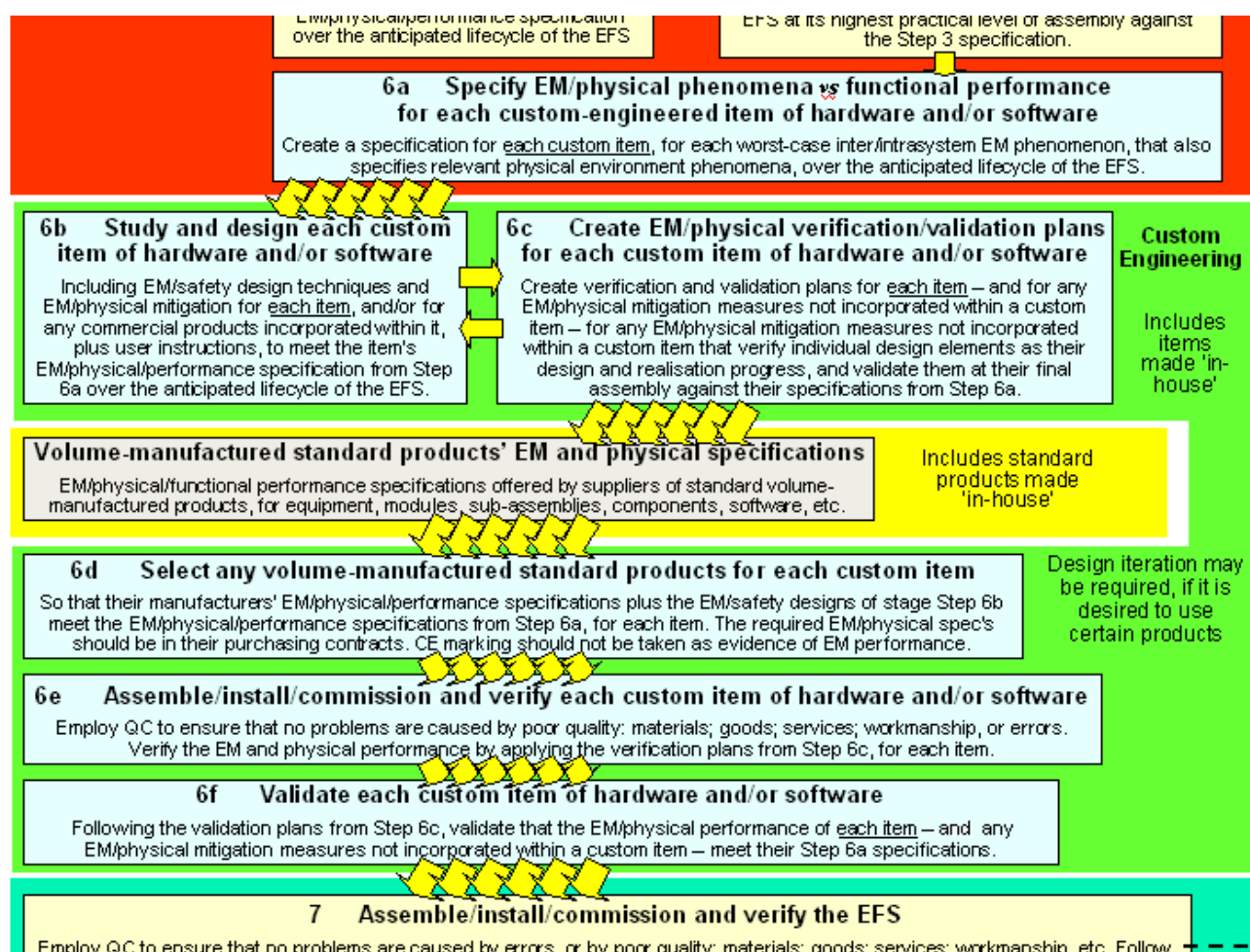
Many types of EFS intended for industrial control and similar applications are 'one-offs', and the quantities of products purchased is quite small and is anyway a single purchase. So as long as the additional product verification activities described above are satisfactory, there is no need for additional QC.

- d) **Use a custom product instead.** Convert the EFS from a 'Simple' type to a 'Complex' (see 6.2) by using a custom-designed product instead of a standard one.

In some cases it could be quite reasonable solution (or at least more cost-effective than the alternatives a-c above) to pay a supplier of standard products to produce a custom-engineered version that meets the EFS designer's EM/physical design/verification/validation specification and is provided with believable test results.

A product manufacturer might even be persuaded to make a completely new product for the EFS concerned. This is typical of EFS for motor vehicles (e.g. ABS) where product volumes are high. It may also be appropriate where the products are required in one-offs or small quantities, for example for a high-profile EFS that is not very price-sensitive, e.g. for safety in nuclear power or fuel rod reprocessing.

6.4 The Step 6 activities for a Complex EFS



6.4.1 Overview

For a Complex EFS, the Step 6 activities are concerned with the purchase of custom-manufactured items of hardware and software to use in its realisation – as well as with the appropriate choice of standard volume-manufactured products (i.e. parts, components, modules, units, etc.) as described in 6.3 and Figure 6.2.

An EFS is not just items of equipment, it includes their interconnections too. The design/selection of appropriate interconnections, such as cables and connectors, and the use of appropriate good EMC engineering practices in their assembly and installation, are issues that are just as important as the design, selection and realisation of items of equipment, and should also be controlled by this process.

The subsections below deal with the activities relating to the custom-engineered items of hardware and software.

Each design/realise/verify/validate project for an item of hardware and software should be treated as if the item concerned was a Simple EFS (see 6.2) in its own right. The only difference, is that instead of the EM/physical specifications for the item being derived from the ambient EM/physical environments as discussed in Steps 1, 2 and 3 – they are derived from the EM/physical environments obtaining in the part of the EFS where they are located.

Example: An anti-lock braking system (ABS) for a road vehicle is an EFS that must operate reliably over the vehicle's lifecycle, despite the EM and physical environments the vehicle is exposed to. But analysing the EM and physical environments (for example using the 'zonal' method in 4.8) shows that the wheel sensors are the most exposed to the external (ambient) EM/physical phenomena because of their very exposed locations on the wheel hubs.

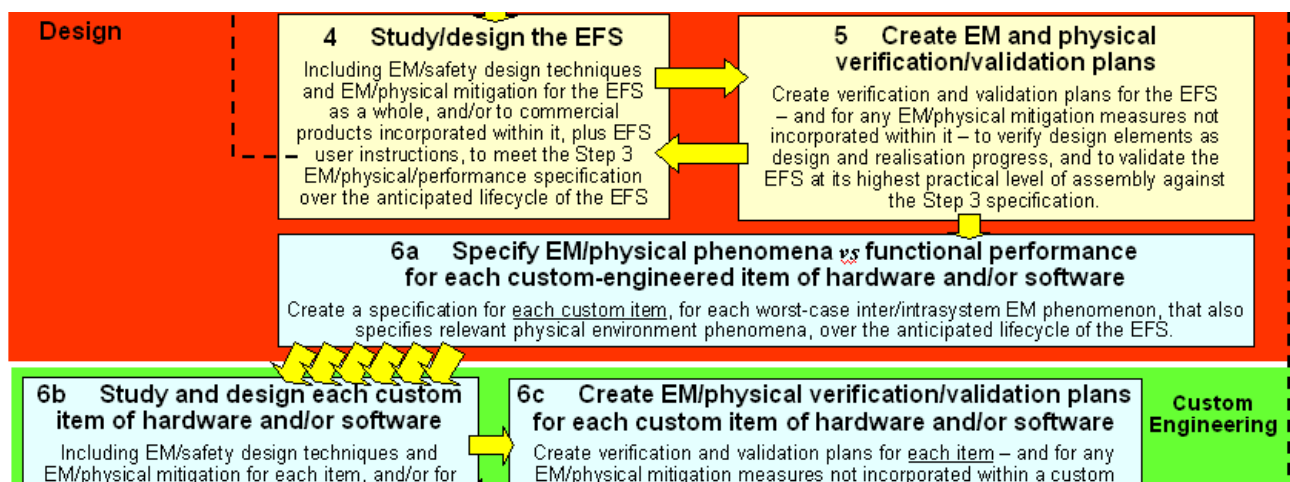
The hydraulic brake actuation unit is located inside the engine compartment, so is partially shielded from external EM threats over certain frequency ranges, and is also less exposed to shock, vibration, water, salt spray, etc., but is more exposed to near-field EM coupling from nearby cable harnesses and very high temperatures due to the nearby engine and its exhaust pipes.

But an electronic ABS control unit could be located inside the passenger compartment (e.g. within the dashboard assembly) and so benefit from an even more protected EM and physical environment. Appropriate design of the control unit's location, for example routing cables associated with other circuits and water/air pipes associated with the heater matrix far away, could ease the EM/physical environments even more.

So the Steps 6a through 6f shown in Figure 0.3 correspond to the Steps 3 through 8 of the Simple EFS process. For this reason, their descriptions below contain little detail, since the appropriate techniques are discussed in the text covering Steps 3 through 8.

The creator of a Complex EFS will often incorporate volume-manufactured standard products as well as the custom-engineered items discussed here – but this activity is not shown in Figure 0.3, to avoid making them appear overly complex. The Simple EFS process applies to the volume-manufactured standard products incorporated by an EFS creator (see 6.3).

6.4.2 Step 6a: Specify EM/physical phenomena *vs* functional performance for each custom-engineered item of hardware and/or software

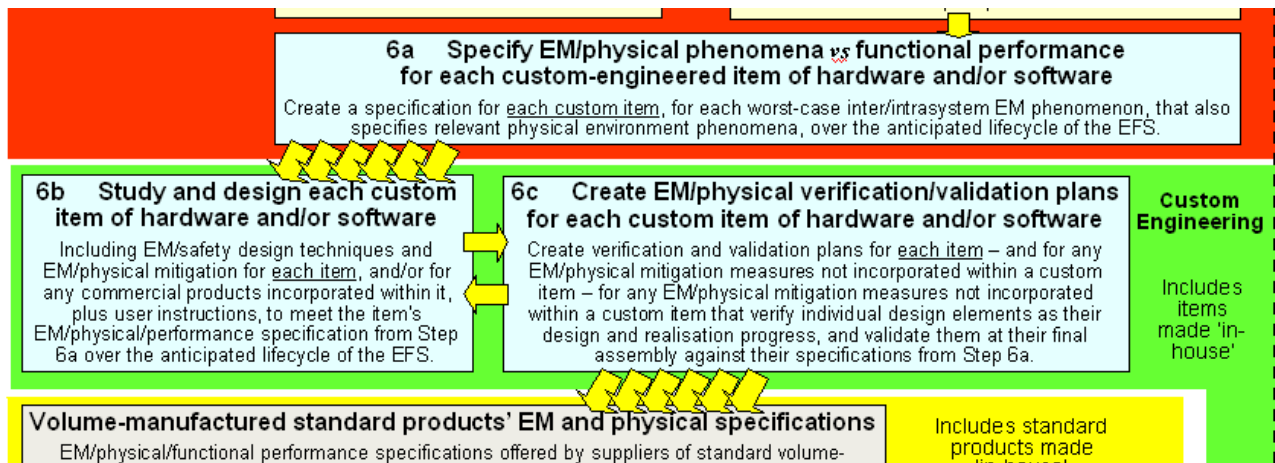


For each custom item of hardware, software or firmware, create a specification for the EM/physical phenomena *vs* functional performance, for each function that could foreseeably affect the performance of the EFS. The result is the Item Requirement Specification or IRS (see Figure 0.3).

As discussed in 6.4.1, the process of creating the IRS is identical to that described in Steps 1, 2 and 3 of this Guide – except that the EM/physical specifications for the item are derived from the EM/physical environments obtaining in the part of the EFS where they are located.

Where EM/physical mitigation has been employed in the design of the EFS (e.g. ‘zoning’ as described in section 4.8), the mitigation will reduce the threat levels in the EM/physical specifications.

6.4.3 Step 6b: Study and design each item of hardware and/or software



The design of each custom-engineered item of hardware or software should take into account EM/safety design techniques and EM/physical mitigation for the item as a whole, and/or for any standard products incorporated within it (plus their user instructions), so as to meet the item's EM/physical/performance specification from Step 6a over the anticipated lifecycle of the EFS.

As discussed in 6.4.1, this activity is effectively identical to that described in Step 4 of this Guide – except that the EM/physical specification comes from Step 6a instead of Step 3, and results in an IRS for each custom-engineered item.

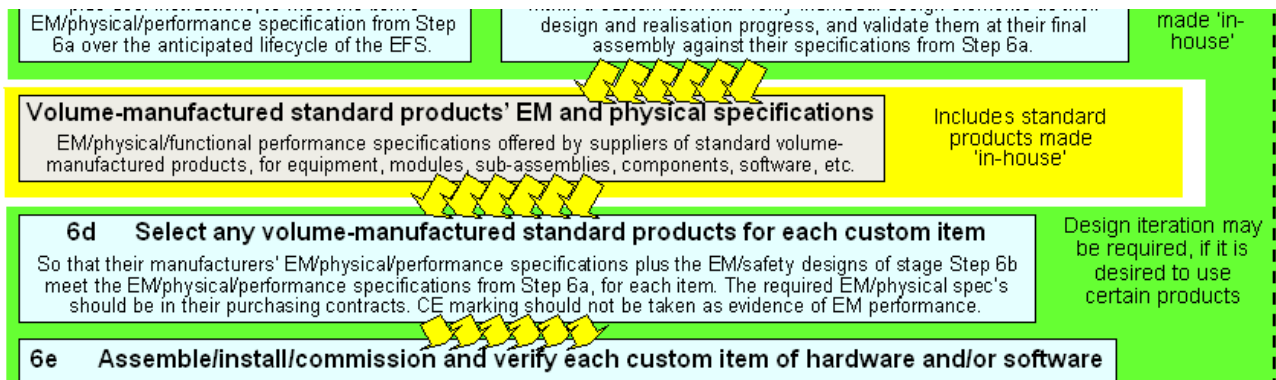
6.4.4 Step 6c: Create EM and physical verification/validation plans for each item of hardware and/or software

Create a verification and validation plan for the item, to verify individual design elements as the design and realisation progress, and to validate the item at its final assembly.

Also create a verification and validation plan for any EM/physical mitigation measures that are not incorporated into the item.

As discussed in 6.4.1, this activity is effectively identical to that described in Step 5 of this Guide – except that the EM/physical specification comes from Step 6a instead of Step 3, and results in an IRS for each custom-engineered item.

6.4.5 Step 6d: Select the commercially-available standard products to be used for each item



The EM/physical/performance specifications for any volume-manufactured standard products used to construct the item of hardware or software – plus any EM/physical/safety design/mitigation applied by the EFS – must meet each item's EM/physical/performance specifications from Step 6a.

The required EM/physical specifications should be in each products' purchasing contracts, and CE marking should not be taken as evidence of EM performance (see 6.3.3).

As discussed in 6.4.1, this activity is effectively identical to that described in Step 6 of this Guide for a Simple EFS, which is described in detail in 6.3 above. Of course, as mentioned earlier, the EM/physical specification for each item comes from Step 6a, instead of Step 3, and results in an IRS for each custom-engineered item.

Figure 6.3 shows the process, which should be compared with Figure 6.2.

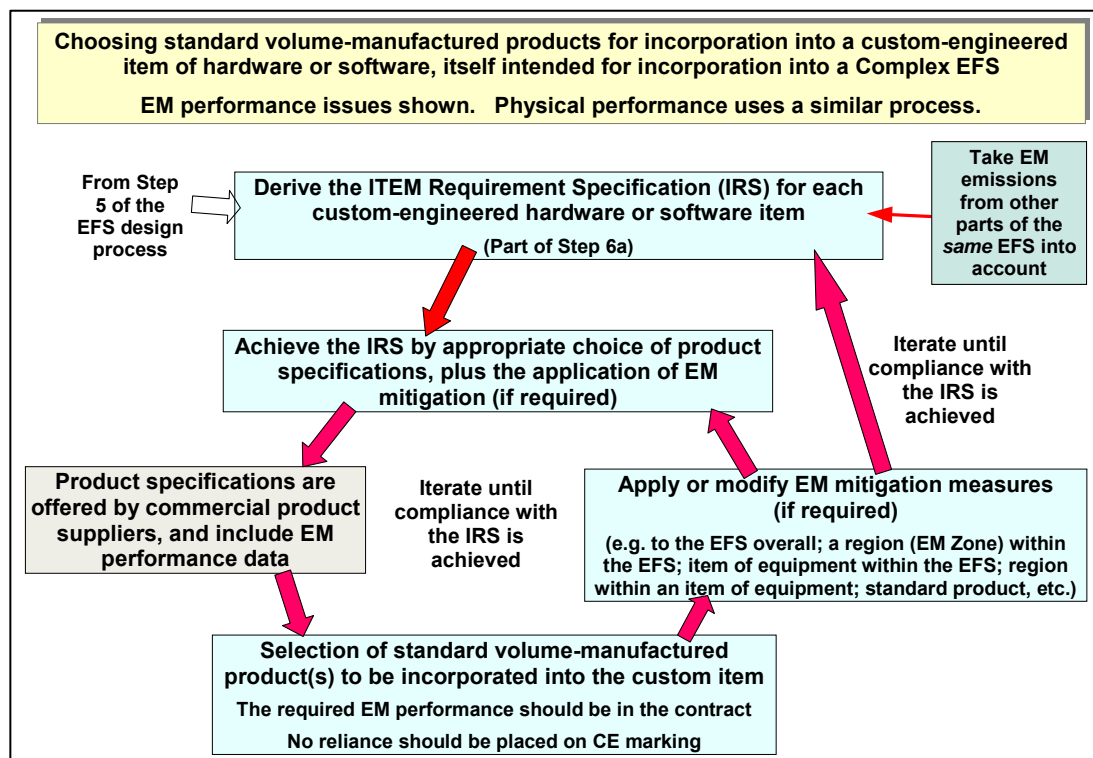


Figure 6.3 Choosing standard products for a custom-engineered item of hardware or software

Figure 6.5 shows an iterative loop stretching back from Step 6 to Step 3 (also see 3.8), but as 1.6 and 2.5 have shown these iterations can also involve Steps 1 and 2. The Step 2 iterations are shown in Figures 2.1 and 2.2.

6.4.6 Step 6e: Assemble and check each item of hardware and/or software

QC plus EM/physical checks ensure the original design was followed, and that no problems are caused by poor quality or errors in:

- Materials
- Goods
- Services
- Workmanship

As discussed in 6.4.1, this activity is effectively identical to that described in Step 7 of this Guide – except that the EM/physical specification for each item comes from Step 6a, instead of Step 3, and results in an IRS for each custom-engineered item.

6.4.7 Step 6f: Verify and finally validate each item of hardware and/or software



Verify and finally validate the EM/physical performance of each item against its verification/validation plans. Also verify the performance of any EM/physical mitigation measures that are not incorporated within the EFS itself.

As discussed in 6.4.1, this activity is effectively identical to that described in Step 8 of this Guide – except that the EM/physical specification for each item comes from Step 6a, instead of Step 3, and results in an IRS for each custom-engineered item.

6.5 Iteration of all previous Steps

Where Step 6 has been used, it is because the EFS designer permitted the EFS creator to choose at least one standard volume-manufactured item, or specify at least one custom-engineered item, for incorporation within the EFS.

This means that before Step 6 occurred, the EFS designer(s) will not have been able to finalise the Intrasystem specifications in Step 2, the EMC Safety specifications in Step 3, the study and design in Step 4 (including the hazard identification and risk assessment) as shown in figures 6.2 and 6.3, or the verification or validation plans in Step 5.

It is also possible for the choices made during Step 6 to affect the assumptions on which the management of the project was based (Step 0) and on which the intersystem EM and physical environments were based (Step 1). So it could happen that the activities of Step 6 could require changes to Steps 0 and 1. This is more likely to occur for large EFS such as geographically distributed networks, but such possibilities should always be assessed for any EFS for which Step 6 is permitted.

Where Step 6 is employed, the EFS creator should ensure that the necessary information is provided to the EFS designer(s) so that they can iterate all of the previous Steps, modifying them as necessary as a result of the activities of Step 6, so that they will provide the necessary confidence (see 0.10.4) that the EFS will at least achieve the safety risks (or risk-reductions) specified over its anticipated lifecycle.

See Figures 6.4 and 6.5.

Overview of the EMC for Functional Safety process for a 'Simple' EFS

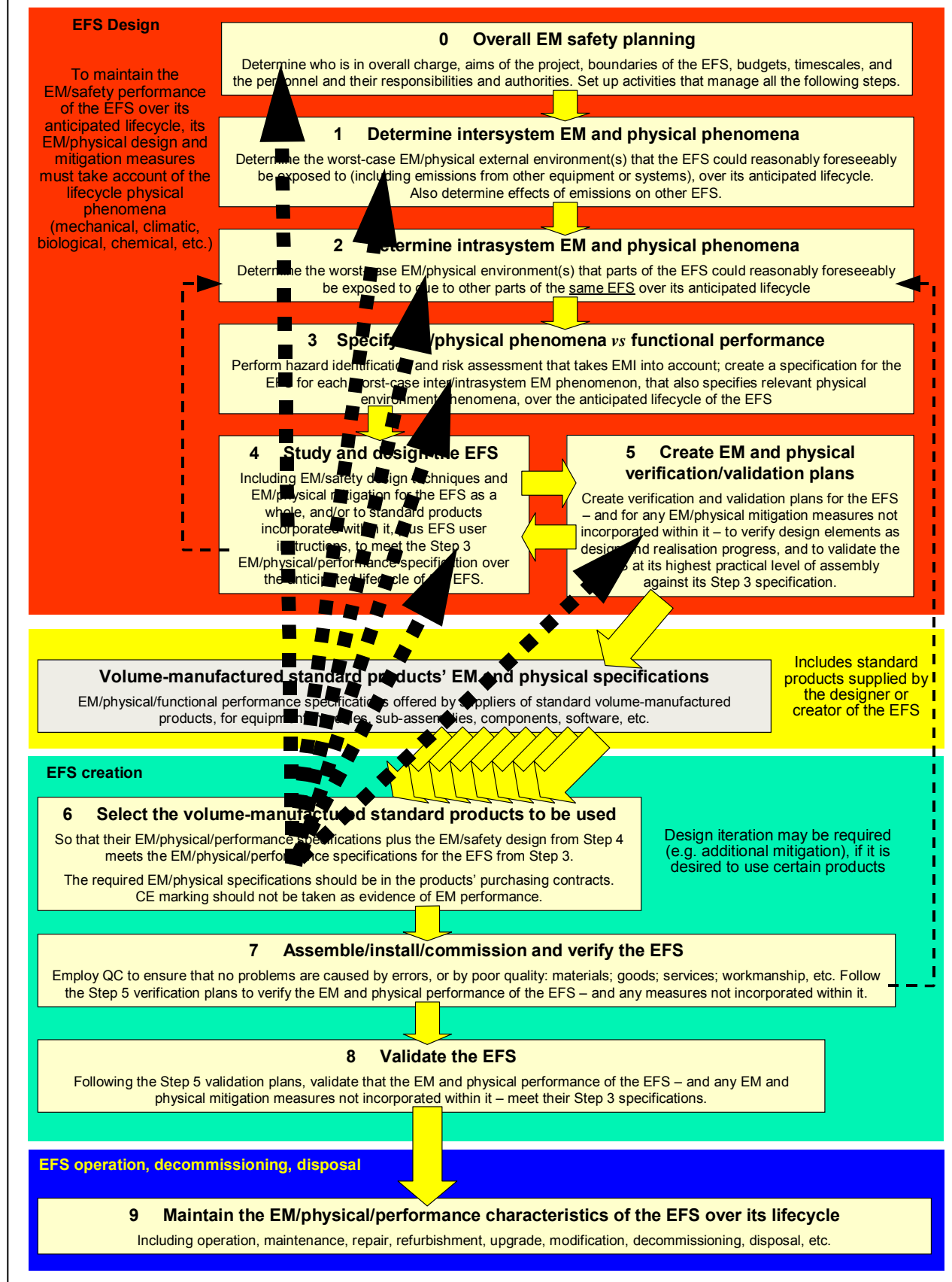


Figure 6.4 Iterating all previous Steps due to Step 6, for a Simple EFS

Overview of the EMC for Functional Safety process for a 'Complex' EFS

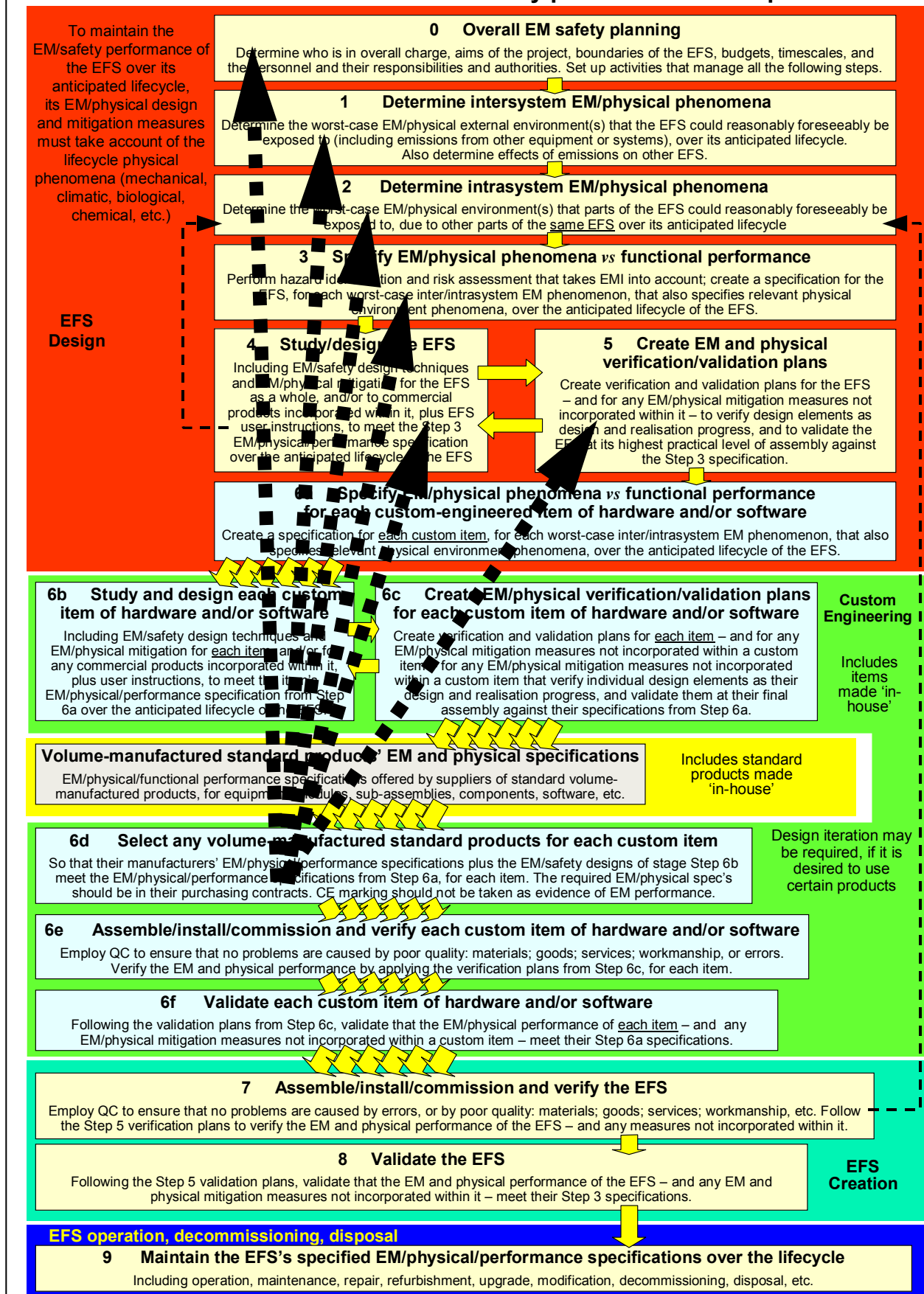
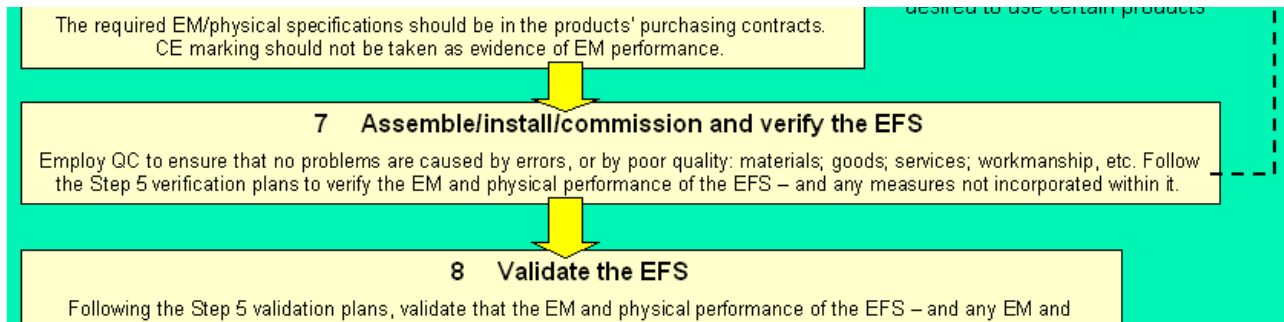


Figure 6.5 Iterating all previous Steps due to Step 6, for a Complex EFS

7. Step 7: Assemble, install, commission and verify the EFS

Employ QC to ensure that no problems are caused by errors, or by poor quality: materials; goods; services; workmanship, etc. Follow the Step 5 verification plans to verify the EM and physical performance of the EFS – and any measures not incorporated within it.



7.1 Introduction

A very wide variety of assembly, installation, commissioning and verification activities are possible in this Step. Some of them might take place on the manufacturer's site (or manufacturers' sites), and some on the operational site (including fixed locations, vehicles, vessels, etc.), depending on the type of EFS and the way it is designed.

These activities all fall within the lifecycle phase known as 'Realisation' in IEC 61508 [7], and include such 61508 concepts as 'manufacture' and 'integration'. They are all specified by the design and verification documents created during Steps 4 and 5, in order to meet the specifications created by Step 3, so that the EFS achieves the desired levels of safety risk, or risk-reduction, over its lifecycle.

7.2 Verification during assembly, installation and commissioning

Verification activities (see Step 5) are applied at all stages of assembly, installation and commissioning. For example, sub-systems might be individually verified as far as it is practical, using certain techniques, before they are integrated together to create the EFS, which is then verified using techniques that could be different.

The purpose of this is cost-effectiveness. Solving problems at the level of a complex system can be very time-consuming due to its complexity, and the cost per hour can be very high because it is a late stage in the project. Verifying everything as far as is practicable at the lowest level of assembly makes any problems easier to find, and the cost per hour is less. Also, solving problems earlier in the design process is much less costly than solving them later, and there are more degrees of design freedom available, often making the modifications easier.

7.3 Following the EFS designers' instructions

Step 4 will have created the design documents and associated specifications for materials and components. The EFS creator must therefore:

- Procure the materials, components, products and equipment according to their EM/physical specifications
- Take appropriate steps to avoid counterfeit parts
- Have controls in place to ensure all suppliers and subcontractors provide adequate compliance documentation (these controls should apply all the way down the supply chain)
- Realise the EFS (manufacture, assemble, integrate, install, etc.) according to the design

These activities must be undertaken, and documented, with the appropriate amount of effort, see 0.10.4.

Steps 4 and 5 will also have created a comprehensive set of instructions for assembly, installation, commissioning and verification activities required (see 4.6 and 5.2). These will include (but are not limited to) the following, where appropriate for the type of EFS and its design and application:

- Any constraints on the physical positioning of the items of equipment that comprise the EFS
- Constraints on cabling
- The methods of terminating any cable shields (screens)
- Constraints on connectors and glands, and their assembly
- The electrical power supply requirements (power quality)
- Any additional shielding (screening) required
- Any additional filtering required
- Any additional overvoltage and/or overcurrent protection required
- Any additional power conditioning required
- Any additional electrostatic discharge protection requirements
- Cooling/heating/humidity/temperature control
- Any additional shock or vibration damping
- Any additional physical protection required
- Any earthing (grounding) and bonding requirements
- Protection against corrosion
- The procedures, materials and expertise to be used

These instructions must also be followed by the EFS creator, and documented, with the appropriate amount of diligence, see 0.10.4.

7.4 Quality Control

Some EFS will be completely assembled by its creator, moved to its operational site and then installed (e.g. cabled), then commissioned.

Some EFS will only be partially assembled by its creator, moved to its operational site, and its final assembly will occur at the same time as its installation.

Some types of EFS will not be assembled at all, until it is installed on its operational site.

The designer of the EFS might be the same organisation that creates the EFS, or not.

The creator of the EFS might be the same organisation that operates the EFS, or not.

The assembly, installation, commissioning and verification that occurs might be carried out by the creator of the EFS, the end-user/operator of the EFS, or by one or more third parties such as professional installers, testers, etc. Third parties might be employed by the creator of the EFS or by its end-user/operator.

Regardless of who performs what assembly, installation, commissioning and verification activities, and where they do them, quality control (QC) activities must be applied to their work.

These QC activities must be designed so that they will ensure that the original design (see Step 4) was followed, and the relevant specifications met (see Step 3). They may include EM/physical checks or tests as appropriate. They must ensure that no deviations from the design or design intent are caused by poor quality, errors or inadequate expertise in:

- Materials
- Goods
- Services
- Workmanship
- Verification (e.g. inspections, tests, etc.)

Some or all of the QC activities might have been specified by the EFS designer during Steps 4 or 5.

A single person or organisation – which could be the creator, end-user/operator or a third party – must have the responsibility for ensuring that the necessary QC activities are employed, and to that end must have all necessary authority over the people actually performing the QC work.

This single person or organisation must also have the authority/responsibility for making decisions about whether the work that was subject to the QC activities was done correctly.

The people responsible for QC, their authority and contact details, must be made known to everyone involved in the assembly, installation, commissioning and verification activities.

Of course, there is a cost-risk balance to be struck, and where this differs from that adopted by the EFS designers it requires independent 'champions' to present both sides of the argument, and any compromise to be documented and available to safety assessors or inspectors (see 7.8).

Where safety risks must be very low, or risk-reductions very high (e.g. SIL4 systems according to IEC 61508) it may even be necessary for the person or team charged with implementing the validation, to be completely independent of the EFS creator.

7.5 Iterating the specifications (Steps 1, 2 and 3)

The EM and physical specifications to be met by the EFS over its lifecycle were specified by Step 3, taking into account the assessments from Step 1 (intersystem phenomena, caused by the ambient at the operational site(s) and from Step 2 (intrasystem phenomena, due to interactions between EFS component parts).

In some cases it might not have been possible to accurately determine these specifications until the EFS was assembled, installed, commissioned or verified, see 1.6 and 2.5. This especially applies to Step 2 (intrasystem) EM and physical phenomena, because at the time of writing the specification the actual EM and physical characteristics of the standard volume-manufactured products or custom-engineered equipment might not have been completely known.

In some cases, the ways in which the component parts of the EFS might interact is not known until they are assembled. Even where it was possible to fully simulate the interactions, the simulation results might have been subject to considerable uncertainty, or needed verification, or an appropriate simulation might not have been done at all.

In all cases, appropriate verification activities are required to discover whether the specifications from Step 3 are adequate for the achievement of acceptably low safety risks, or the required levels of risk-reduction, of the EFS.

In all cases where the Step 3 specification requires modification as a result of the activities in Step 7 (see 3.8) the EFS creator must inform the EFS designers and supply them with all of the information they need to modify the specification in Step 3.

The EFS designer(s) then iterates the design (Step 4), and the verification/validation plans (Step 5) as appropriate, see 4.2.4 and 5.2.3, and Steps 6 and 7 then proceed as before based upon these new requirements.

As before, QC activities are applied as described above and it may be found that second and third iterations (or more) are required to ensure that the EFS achieves the desired levels of safety risk, or risk-reduction, over its lifecycle

The iterative loops from Step 7 back to Steps 1 and 2 were not shown in Figures 0.2 or 0.3, to avoid making them appear too complex and/or difficult to read, but they are shown in Figures 2.1 and 2.2, and also in Figures 7.1 and 7.2. The corresponding loops associated with custom-engineered items are shown in Figure 7.3.

7.6 Iterating the design and verification (Steps 4 and 5)

Assembly, installation, commissioning or verification might reveal that the design (from Step 4) or verification techniques (from Step 5) cannot comply with the specification (from Step 3). This might be because, for example:

- It proves impractical to implement an aspect of the design

- A purchased item (standard volume-manufactured product or custom-engineered equipment) is discovered to be inadequate or unsuitable
- Commissioning and/or verification reveals that certain specifications cannot be met
- Verification techniques cannot be applied as intended, or prove to be inadequate

In all cases where the design (Step 4) or verification (Step 5) cannot comply with the specification (Step 3), the EFS creator must inform the EFS designers and supply them with all of the information they need to modify the design so that the EFS achieves the desired levels of safety risk, or risk-reduction, over its lifecycle.

The EFS designers then iterate the specification, design and verification requirements (Steps 3, 4 and 5) as appropriate and Steps 6 and 7 proceed as before based upon these new requirements. As before, QC activities are applied as described above and it may be found that second and third iterations (or more) are required to ensure that the EFS achieves the desired levels of safety risk, or risk-reduction, over its lifecycle

The iterative loops from Step 7 back to Steps 4, 5 or 6 were not shown in Figures 0.2 or 0.3 to avoid making them appear too complex and/or difficult to read. They are shown in bold dotted arrows in Figures 7.1 (Simple EFS) and 7.2 (Complex EFS). Figure 7.3 shows the iterative loops associated with each custom-engineered item in a Complex EFS.

Overview of the EMC for Functional Safety process for a 'Simple' EFS

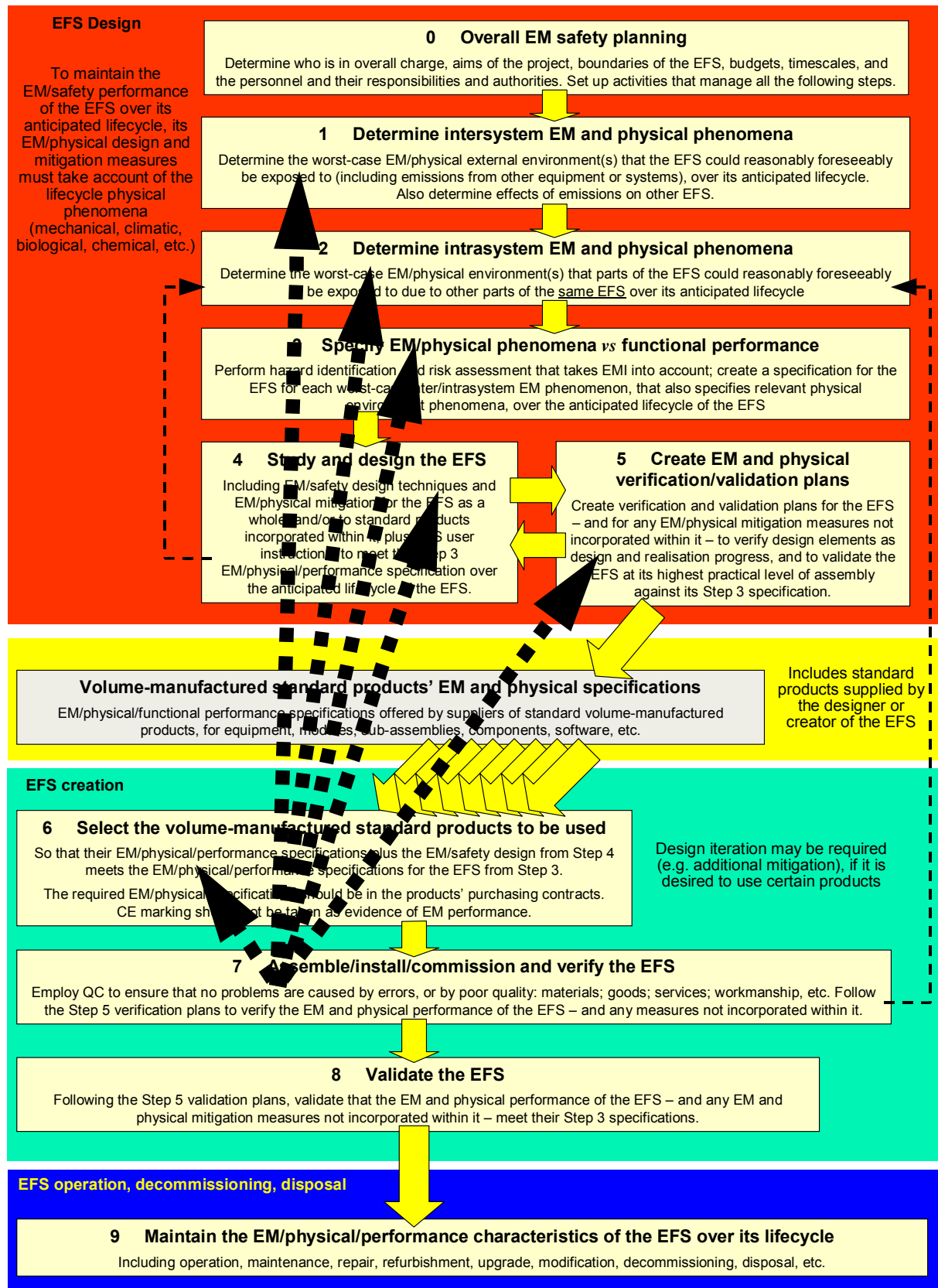


Figure 7.1 Iterative loops from Step 7, Simple EFS

Overview of the EMC for Functional Safety process for a 'Complex' EFS

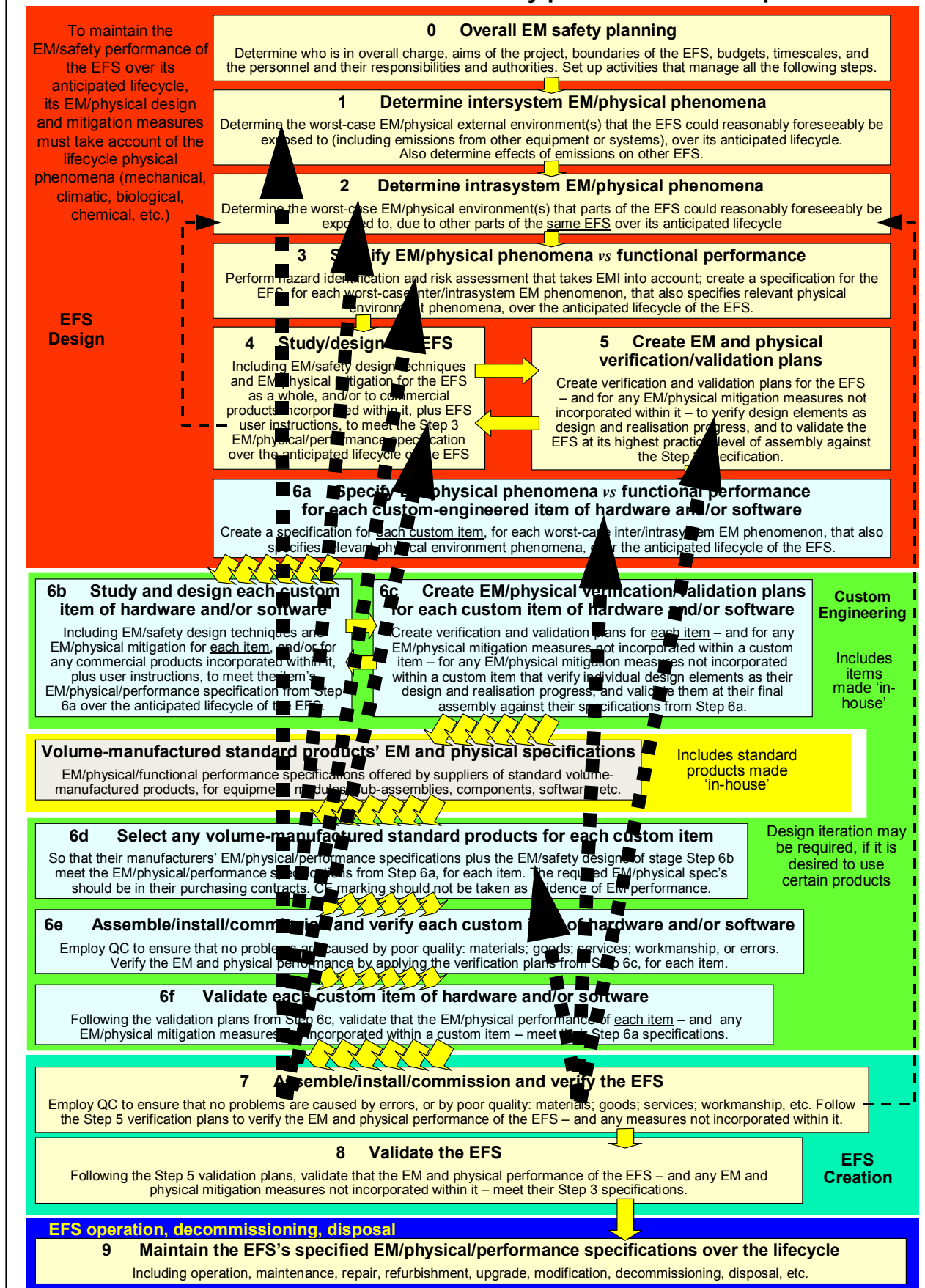


Figure 7.2 Iterative loops from Step 7, Complex EFS

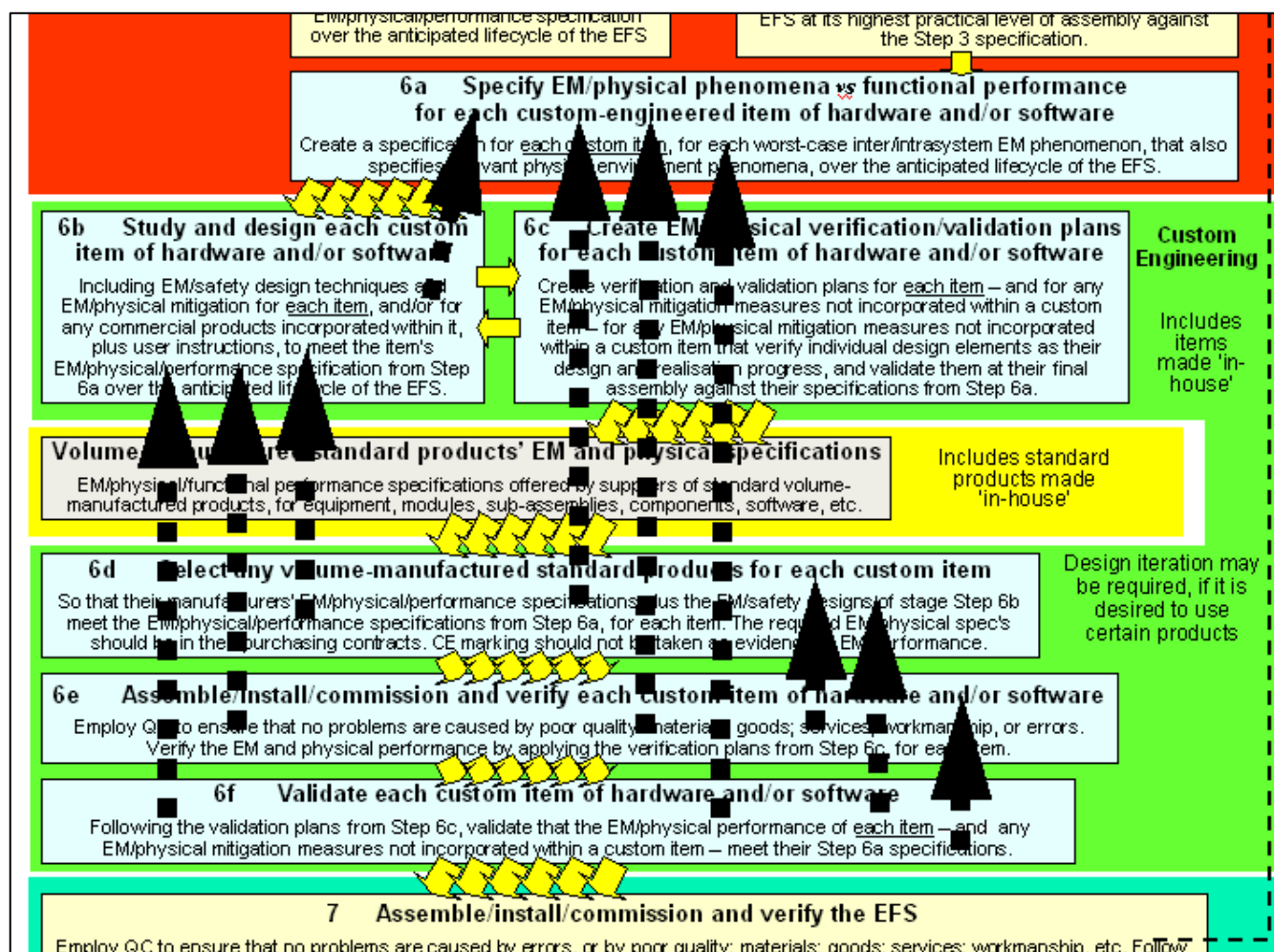


Figure 7.3 Iterative loops associated with custom-engineered items that are to be incorporated into a Complex EFS

7.7 Realisation (assembly, installation, commissioning, verification, etc.) of EM/physical mitigation measures not incorporated in the EFS

Some EFS are supplied with instructions to install additional EM and/or physical protection/mitigation measures that are not themselves part of the EFS.

For example: lightning and lightning surge protection systems, sprung floors for vibration and shock damping, earthquake protection, special protection against fire or flood, power quality improvement equipment such as uninterruptible power supplies, etc.

Since the EFS cannot achieve its required levels of safety risks (or risk-reductions) without these measures being in place and functioning effectively, it is necessary to follow the same procedures as described in 7.1 to 7.6 to realise (manufacture, assemble, integrate, install, etc.), commission and verify them.

These activities might be incorporated into certain of the EFS activities, or performed separately.

The issues discussed in 7.2, 7.3, 7.4, 7.5 and 7.6 apply equally to the verification of EM/physical mitigation measures that are not incorporated within the EFS itself, but which are necessary for it to achieve its specified levels of risk or risk-reduction over its anticipated lifecycle.

7.8 QC Documentation

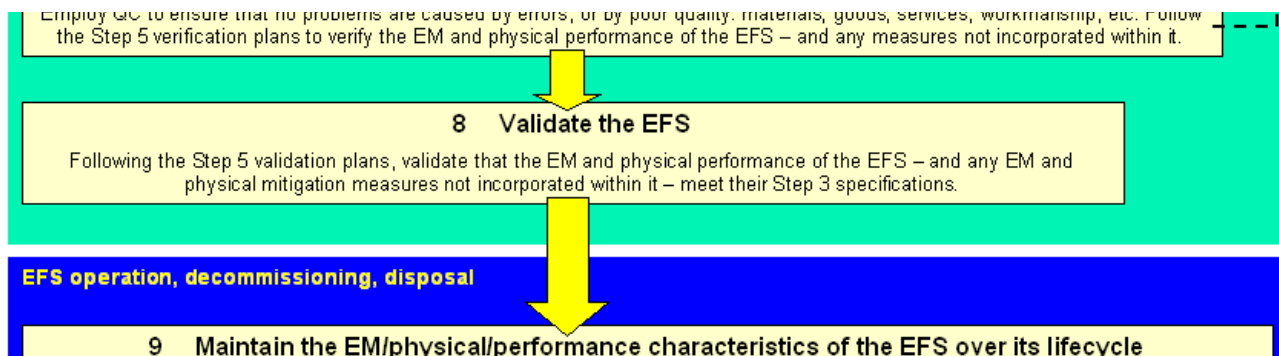
The QC activities and their results, the planned verification work (from Step 5) and any remedial work to ensure that the original design was followed, must all be documented in such a way as to allow the correct operation of the QC activities to be assessed later on, by other people who may even be independent.

Generally speaking, the lower the levels of acceptable safety risks or the higher the amount of risk-reduction, the greater the degree of QC documentation required, see 0.10.4.

As discussed in 0.10.5, QC documentation must be held safe, secure, and readable at least for the operational life of the EFS, in case it is required by official safety inspectors, and also so that it is available to help guide designers and others if/when the EFS is repaired, refurbished, modified or upgraded in some way in the future (see Step 9).

8. Step 8: Validating the EFS

Following the Step 5 validation plans, validate that the EM and physical performance of the EFS – and any EM and physical mitigation measures not incorporated within it – meet their Step 3 specifications.



8.1 Introduction to Validation

This is the Step in which the finished, fully functioning EFS is validated as complying with its Step 3 requirements for safety risks and/or risk-reductions over its lifecycle, by implementing the validation plans from Step 5.

Where the EFS is large, or is a distributed system, EMC testing of its final build stage might be impractical and/or there may be no standard test methods that are suitable. A wide variety of validation activities are available for use in this Step (see Step 5) depending on the type of EFS and the way it is designed, to support whatever testing is practical (and affordable) to achieve sufficient confidence in the safety risks or risk-reductions achieved by the EFS.

8.2 Authority and responsibility

The validation activities are specified by the EFS designers as part of Step 5, but carrying them out is the responsibility of the EFS creator in this Step 8. The EFS creator might subcontract some or all of the validation activities to one or more third parties, even to the end-user/operator, but **responsibility for the accuracy and completeness of the validation remains with the EFS creator.**

The EFS creator should ensure that the people carrying out this work have the appropriate competencies.

The name of the person tasked with being responsible for validation (or the head of the validation team), their authority and contact details, must be made known to everyone involved in the project, and they may be a third-party.

Although the EFS creator is responsible for all of Step 8, and for appointing the person or team responsible for validation, they cannot over-ride the authority of the person or team they have given charge of validation to. This is to prevent considerations such as cost or timescale over-riding safety considerations.

Of course, there is a balance to be struck, and where this differs from that adopted by the EFS designers it requires independent 'champions' to present both sides of the argument, and any compromise to be documented and available to safety assessors or inspectors (see 8.6).

Where safety risks must be very low, or risk-reductions very high (e.g. SIL4 systems according to IEC 61508) it may even be necessary for the person or team charged with implementing the validation, to be completely independent of the EFS creator.

8.3 Remedial work

To achieve validation, certain remedial work may be found to be necessary (e.g. broken or damaged equipment, incorrect assembly or installation, etc.). This should be carried out as necessary, repeating the necessary assembly, installation, commissioning and verification activities in Step 7 as appropriate.

Where the remedial work would change the design, section 8.4 applies instead.

8.4 Iterating the earlier steps

Validation of the EFS might reveal a lack of confidence that the EFS will achieve the desired levels of safety risk, or risk-reduction over its lifecycle. Concerns could arise with regard to any/all of the preceding steps:

- EM and physical assessments (Steps 1 and 2)
- Specifications (Step 3)
- Design (Step 4)
- Verification and validation planning (Step 5)
- Selection of standard volume-manufactured products or design of custom-engineered equipment (Step 6)
- Assembly, installation, commissioning and verification (Step 7)

In any/all such instances, the EFS creator must inform the EFS designers and supply them with all of the information they need to modify the relevant Steps, to ensure that the EFS achieves the desired levels of safety risk, or risk-reduction over its lifecycle.

The EFS designers then iterate the relevant Steps as appropriate, and the subsequent Steps in the process are repeated, including the Validation in this Step 8.

The possible iterative loops from Step 8 back to all previous Steps were not shown in Figures 0.2 or 0.3 in Step 0, to avoid making them appear too complex and/or difficult to read, but they are shown as bold dotted arrows in Figures 8.1 and 8.2.

Figure 7.3 shows the iterative loops that exist for each of the custom-engineered items to be incorporated in a Complex EFS.

Overview of the EMC for Functional Safety process for a 'Simple' EFS

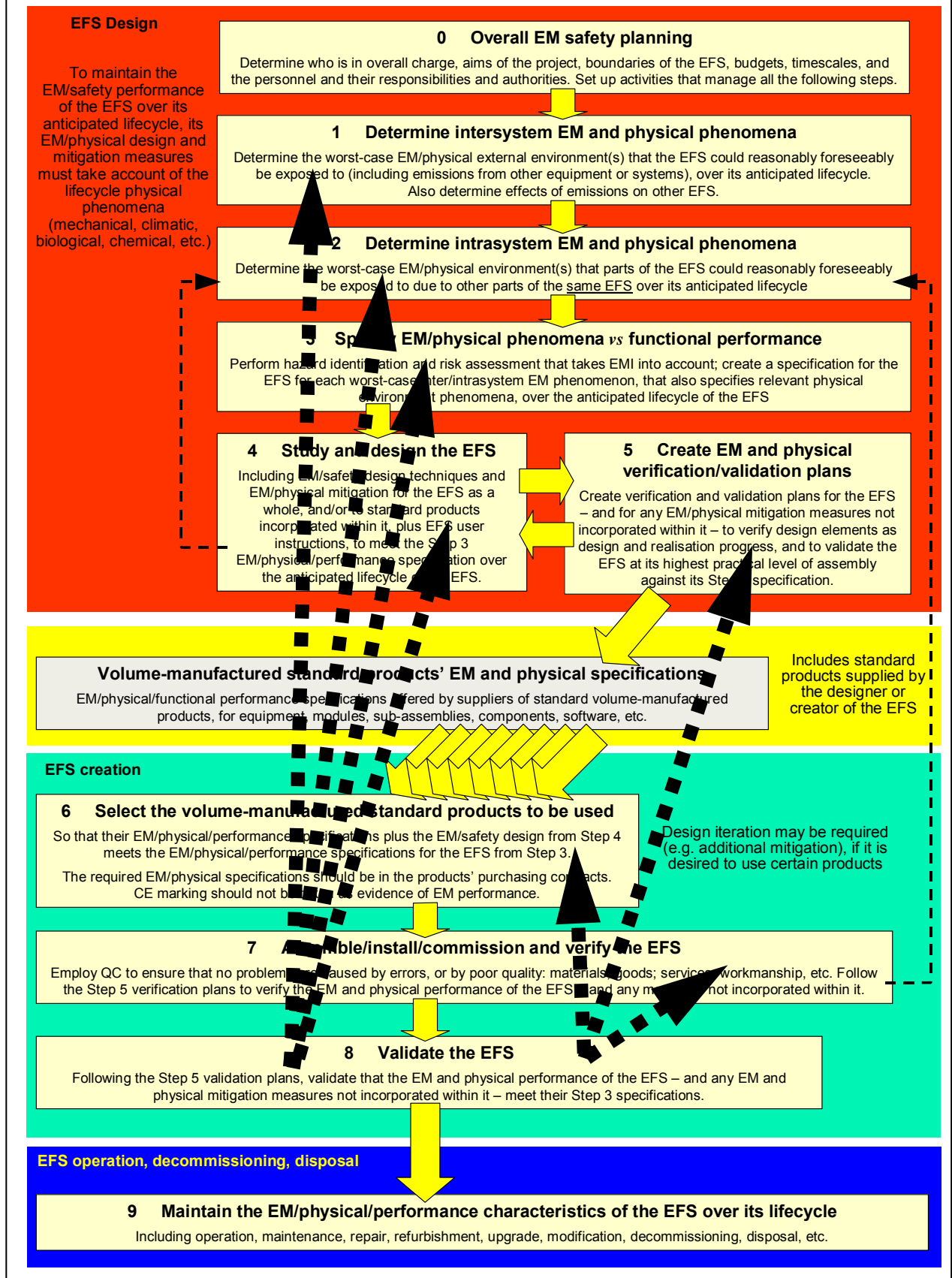


Figure 8.1 Iterative loops from Step 8, Simple EFS

Overview of the EMC for Functional Safety process for a 'Complex' EFS

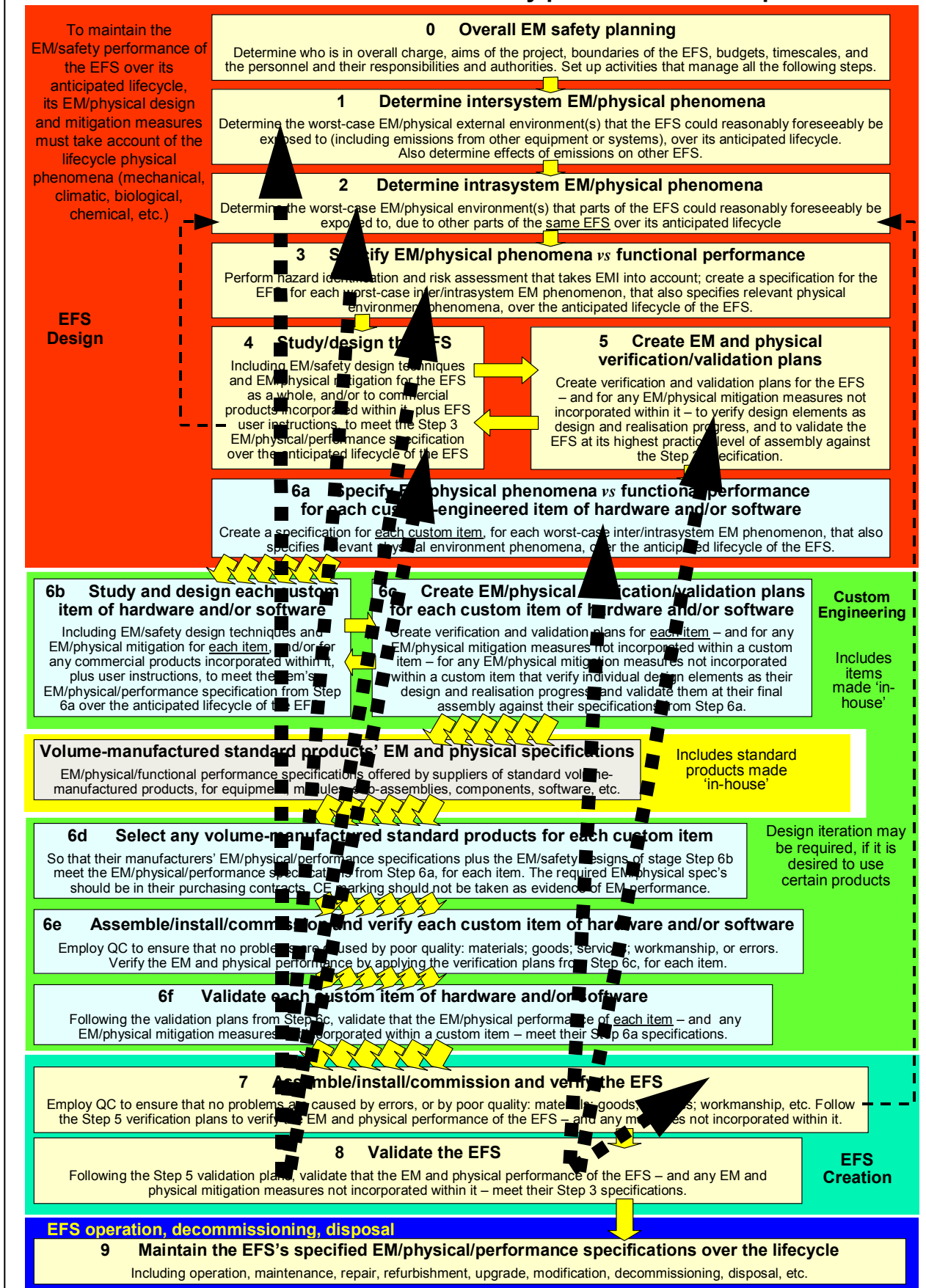


Figure 8.2 Iterative loops from Step 8, Complex EFS

8.5 Validating EM/physical mitigation measures that are not incorporated in the EFS

Some EFS are supplied with instructions to install additional EM and/or physical protection/mitigation measures that are not themselves part of the EFS.

Example: lightning and lightning surge protection systems, sprung floors for vibration and shock damping, earthquake protection, special protection against fire or flood, power quality improvement equipment such as uninterruptible power supplies, cooling/heating/air-conditioning, etc.

Since the EFS cannot achieve its required safety risks (or risk-reductions) without these measures being in place and functioning effectively, it is necessary to validate them.

Their validation might be incorporated into certain of the EFS validation activities, or performed separately.

The issues discussed in 8.2, 8.3 and 8.4 apply equally to the validation of EM/physical mitigation measures that are not incorporated in the EFS, but necessary for it to achieve its specified levels of risk or risk-reduction over its anticipated lifecycle.

8.6 Documenting the validation

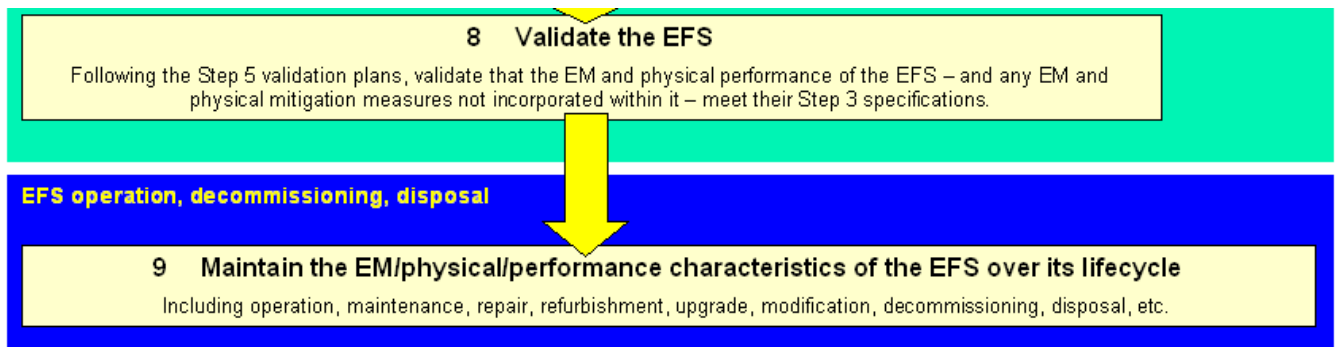
All of the planned validation activities (from Step 5) and their results, and any remedial work to ensure the original designs were followed, must all be documented in such a way as to allow the correct implementation of the activities to be assessed later on, by other people who may be independent.

Generally speaking, the lower the levels of acceptable safety risks or the higher the amount of risk-reduction, the greater the degree of validation documentation required, see 0.10.4.

As discussed in 0.10.5, validation documentation must be held safe, secure and readable for at least the operational life of the EFS, in case it is required by official safety inspectors, and also so that it is available to help guide designers and others if/when the EFS is repaired, refurbished, modified or upgraded in some way in the future (see Step 9).

9. Step 9: Maintain the EM and physical performance characteristics of the EFS over its lifecycle

Including operation, maintenance, repair, refurbishment, upgrade, modification, decommissioning, disposal, etc.



9.1 Introduction

The EFS must maintain its desired levels of safety risks and/or risk-reductions over its lifecycle, which of course includes operation, maintenance, repair, refurbishment, and modifications and upgrades to its mechanics, electrical and electronic hardware and software. It must also remain safe enough during dismantling and disposal.

The safety of everyone who could be exposed to risks from the EFS in any of its lifecycle phases must be controlled, by appropriate design and/or management procedures.

Example: Where an EFS is controlling a powerful robot, during certain lifecycle activities (other than operation) it may be acceptable to remove the power to its motors and actuators, so that if the EFS suffers interference (e.g. due to the door of a shielded enclosure being opened) the robot cannot make any unintended or erroneous movements. If the robot needs to be exercised with the shielded enclosure door open, it may be acceptable for the person in charge of that activity to clear the area of any radio transmitters, or clear the area reachable by the robot of any personnel, both of them being precautions that are not taken during normal operation.

Different types of personnel perform the various activities during these phases of the lifecycle. For example an operator will have a different set of skills, competencies and experiences than someone performing a repair or installing an upgrade, and will generally (but not always) be exposed to safety hazards for a shorter time. For this and other reasons the levels of safety risk or risk-reduction that are necessary for the EFS during various post-manufacture activities can be different from those that are necessary during operation.

Dismantling and disposal lifecycle phases often require no safety precautions, but the issue should always be addressed because sometimes they can.

Example: Nuclear power plants can take a long time to dismantle and dispose of, and certain types of EFS (e.g. cooling systems, safety interlocks, radiation alarms, etc.) need to remain operational and provide the required level of safety risks (or risk-reductions) during part or all of those phases.

9.2 The activities required during operation, maintenance, repair, refurbishment, etc.

Steps 4 and 5 will have created a comprehensive set of instructions for ensuring that the EM and physical performance characteristics of the EFS (and any related protection/mitigation measures, see 7.7) remain adequate for the achievement of the desired levels of safety risks, or risk-reductions, throughout the post-

manufacture lifecycle, including: operation; maintenance; repair and refurbishment (see 4.6). Depending on the EFS and its design and application, these can include (but are not limited to):

- Constraints on the EM and physical environments
- Disassembly/reassembly (and, where necessary, appropriate verification/validation) techniques to preserve EM and physical performance characteristics
- Periodic testing (proof testing) of critical or lifed components
- Periodic replacement of critical or lifed components
- Verification of the absence of corrosion, plus activities to prevent or limit corrosion, or recover from the effects of corrosion
- Verification of the absence of faults, damage and/or misuse, plus activities to recover from the effects of faults, damage or misuse
- Revalidation of some or all EM and/or physical performance characteristics as described in Step 8

All of these requirements can require a wide range of activities, from (for example) keeping apprised of nearby planning applications and developments that could, if unchallenged, place a wireless transmitter or basestation too close to the site of the EFS – through periodically inspecting the EFS for faults, damage and misuse and repairing any found – to performing a full set of validation activities.

All these activities must be performed as specified by the EFS designers, and their implementation and results, and any replacements, repairs, revalidation, etc. undertaken must be documented as described in 9.5.

Operational experience and the outcome of maintenance activities should be regularly reviewed with the aim of identifying necessary improvements to the operational and maintenance regimes. Such activities might identify areas where other changes are necessary. Where the safety performance of the EFS is more critical, more diligence and effort is generally required for these activities, see 0.10.4.

9.3 The activities required when modified or upgraded

The effects on the safety risks (or risk-reductions) of any modification or upgrade to an EFS cannot be determined in isolation from the EFS. A small change to software, maybe to add a useful feature, could (accidentally) have major implications for safety – so it could be a mistake to assume that a small change to an EFS would be a small project.

Steps 4 and 5 will have created a comprehensive set of instructions for ensuring that the EM and physical performance characteristics of the EFS (and any related protection/mitigation measures, see 7.7) remain adequate for the achievement of the desired levels of safety risks, or risk-reductions, throughout the post-manufacture lifecycle, including: modifications and upgrades to mechanics, hardware or software (see 4.7).

These activities will require returning to the appropriate Step in the process, and then going through the whole process described in this Guide from that point.

Depending on the type of EFS and the consequences of the modification or upgrade, the amount of work required to ensure that the EFS's desired safety risk levels (or risk-reductions) are maintained following the modification or upgrade could range from very little to very large. But it is important to understand that it is not possible to determine the amount of work required without considering the consequences of returning to the appropriate Step in the process and going through the whole process described in this Guide from that point.

All these activities must be performed as specified by the EFS designers, and documented as described in 9.5. Where the safety performance of the EFS is more critical, more diligence and effort is generally required for these activities, see 0.10.4.

9.4 The activities required during dismantling and disposal

As for 9.2 and 9.3 above, Steps 4 and 5 will have created a comprehensive set of instructions for ensuring that the EM and physical performance characteristics of the EFS (and any related protection/mitigation measures, see 7.7) remain adequate for the achievement of the desired levels of safety risks, or risk-reductions, during dismantling and disposal (see 4.7) – where any are required at all.

All these activities must be performed as specified by the EFS designers, and documented as described in section 9.5. Where the safety performance of the EFS is more critical, more diligence and effort is generally required for these activities, see 0.10.4.

9.5 Documentation

All of the activities that the EFS designers require to be carried out during the post-manufacture lifecycle stages of the EFS, to maintain its desired levels of safety risks and/or risk-reductions, must be undertaken at the required times and their implementation and results documented.

Generally speaking, the lower the levels of acceptable safety risks or the higher the amount of risk reduction, the greater the degree of documentation required, see 0.10.4.

As discussed in 0.10.5, this documentation must be held safe and be readable for the operational life of the EFS, in case it is required by official safety inspectors, and also so that it is available to help guide designers and others if/when the EFS is to be repaired, refurbished, modified or upgraded in the future.

10. References

- [1] "New Guidance on EMC-Related Functional Safety", Keith Armstrong, 2001 IEEE EMC International Symposium, Montreal, Aug. 13-17 2001. Proceedings: ISBN 0-7803-6569-0/01, pp. 774-779
- [2] "New Guidance on EMC and Safety for Machinery", Keith Armstrong, 2002 IEEE International EMC Symposium, Minneapolis, Aug. 19-23 2002. Proceedings: ISBN: 0-7803-7264-6, pp. 680-685
- [3] "Guidance document on EMC and Functional Safety", 2000 The IET: www.theiet.org/factfiles/emc/archive.cfm
- [4] IEC DTS 61000-1-2, 2008 (77/356/DTS), "Electromagnetic Compatibility (EMC) – Part 1-2: General – Methodology for the achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena."
- [5] Amendment 1 to IEC 60601-1-2 Ed2.0 (also Clause 6.2.1.1 in IEC 60601-1-2 Ed 3.0)
- [6] "Breaking All the Rules: Challenging the Engineering and Regulatory Precepts of Electromagnetic Compatibility", D A Townsend *et al*, 1995 IEEE International Symposium on EMC, Atlanta, ISBN: 0-7803-2573-7, pp 194-199
- [7] IEC 61508: "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems"
 - Part 1: General requirements
 - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
 - Part 3: Software requirements
 - Part 4: Definitions and abbreviations
 - Part 5: Examples of methods for the determination of safety integrity levels
 - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
 - Part 7: Overview of techniques and measures
- [8] "Combined Effects of Several, Simultaneous, EMI Couplings", Michel Mardiguian, 2000 IEEE International Symposium on EMC, Washington D.C., August 21-25 2000, ISBN 0-7803-5680-2, pp. 181-184
- [9] "Using Reinforcement Learning Methods for Effective EMC Immunity Testing of Computerised Equipment", Wendsche S. and Habiger E., Proc. Int. Symp. Electromagnetic Compatibility (ROMA'96), Rome, Italy, Sept 1996, pp.221-226
- [10] "The Dependence of the Immunity of Digital Equipment on the Hardware and Software Structure", Vick R. and Habiger E., Proc. Int. Symp. Electromagnetic Compatibility, Beijing, China, May 1997, pp 383-386
- [11] "Directivity of Equipment and its Effect on Testing in Mode-Stirred and Anechoic Chamber", Jansson, L., and M. Bäckström, IEEE Int. Symposium on EMC, Seattle, WA, August 1999
- [12] "Distribution of Responses for Limited Aspect Angle EME Tests of Equipment with Structured Directional Directivity", Freyer, G. J., The 2003 Reverberation Chamber, Anechoic Chamber and OATS Users Meeting, Austin, TX, April 2003
- [13] EN 50160, "Voltage characteristics of electricity supplied by public distribution systems", relevant to public mains electricity supplies in the European Union.
- [14] "Functional Safety and EMC", Simon J Brown and William A Radasky, a guide presented at the IEC Advisory Committee on Safety (ACOS) Workshop VII, Frankfurt am Main, Germany March 9/10 2004.
- [15] "The Case for Combining EMC and Environmental Testing", W H Parker, W Tustin and T Masone, ITEM 2002, pp 54-60, www.interferencetechnology.com
- [16] "EMC Performance of Drive Application Under Real Load Condition", F Beck and J Sroka, Schaffner Application Note, 11th March 1999
- [17] "Ageing of Shielding Joints, Shielding Performance and Corrosion", Lena Sjögren and Mats Bäckström, IEEE EMC Society Newsletter, Summer 2005, www.ieee.org/organizations/pubs/newsletters/emcs/summer05/practical.pdf

- [18] RTCA/DO-160F, Civil aerospace EMC standards, from www.rtca.org, include descriptions of civil aircraft EM environments.
- [19] MIL-STD-464, "Department of Defense Interface Standard – Electromagnetic Environmental Effects – Requirements for Systems"
- [20] "Specifying Lifetime Electromagnetic and Physical Environments – to Help Design and Test for EMC for Functional Safety", Keith Armstrong, 2005 IEEE International Symposium on EMC, Chicago, Aug 8-12, ISBN: 0-7803-9380-5, pp. 495-499
- [21] "The Application of Intentional Electromagnetic Interference (IEMI) detectors for safety and security", R. Hoad and A. Leaver, EMC Europe Workshop 2007, 14-15 June 2007, Paris, France
- [22] "Profit from EMC", Keith Armstrong, IEE Review, July 1994, EMC Supplement: pp S-24 and S-25
- [23] IEC 61511, "Functional safety. Safety instrumented systems for the process industry sector", in three parts
- [24] IEC 62061, "Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems"
- [25] "Why EMC Immunity Testing is Inadequate for Functional Safety", Keith Armstrong, 2004 IEEE EMC Symposium, Santa Clara, August 9-13 2004, ISBN 0-7803-8443-1, pp 145-149. Also published in Conformity, March 2005, pp 15-23, www.conformity.com
- [26] "EMC for Functional Safety", Keith Armstrong (a half-day paper) 2004 IEEE Symposium on Product Safety Engineering, Santa Clara, August 13-15 2004
- [27] "Functional Safety Requires Much More Than EMC Testing", Keith Armstrong, EMC-Europe 2004 (International Symposium on EMC), Eindhoven, The Netherlands, September 6-10 2004, ISBN: 90-6144-990-1, pp 348-353
- [28] "Characterization of Human Metal ESD Reference Discharge Event and Correlation of Generator Parameters to Failure Levels — Part I: Reference Event", and "Part II: Correlation of Generator Parameters to Failure Levels", by D Pommerenke *et al*, IEEE Transactions on EMC Vol. 46 No. 4 November 2004, pp 498-511
- [29] "Functional Safety and EMC", Simon J Brown and Bill Radasky, paper presented at the IEC Advisory Committee on Safety (ACOS) Workshop VII, Frankfurt am Main, Germany March 9/10 2004
- [30] "Combined Effects of Several, Simultaneous, EMI Couplings", Michel Mardiguian, 2000 IEEE International Symposium on EMC, Washington D.C., August 21-25, ISBN 0-7803-5680-2, pp. 181-184
- [31] European Union Directive 2004/108/EC (as amended) on Electromagnetic Compatibility (2nd Edition) in English: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l/_390/l/_39020041231en00240037.pdf
in any EU language: http://ec.europa.eu/enterprise/electr_equipment/emc/directiv/dir2004_108.htm
The Directive's official EU homepage includes a downloadable version of the current EMC Directive and its successor; a table of all the EN standards listed under the Directive; a guidance document on how to apply the Directive; lists of appointed EMC Competent Bodies; etc., all at: http://europa.eu.int/comm/enterprise/electr_equipment/emc/index.htm.
- [32] "EMC Performance of Drive Application Under Real Load Condition", F Beck and J Sroka, Schaffner EMV AG application note, 11th March 1999
- [33] "The Case for Combining EMC and Environmental Testing", W H Parker, W Tustin and T Masone, ITEM 2002, pp 54-60, www.rbitem.com
- [34] IEC/TR 61000-1-5, "Electromagnetic Compatibility (EMC) - Part 1-5: General - High Power Electromagnetic (HPEM) Effects on Civil Systems"
- [35] "Correlations Between EMI Statistics and EMC Market Surveillance in Finland", Jyri Rajamäki, 2004 IEEE International EMC Symposium, Santa Clara, August 9-13 2004, ISBN 0-7803-8443-1, pp 649-654
- [36] "Assessing an Electromagnetic Environment", a Technical Guidance Note (TGN) from the EMC Test Labs Association (EMCTLA), www.emctla.co.uk. Also available from the 'Publications & Downloads' page at www.cherryclough.com

- [37] "Special Issue on High Power Electromagnetics (HPEM) and Intentional Electromagnetic Interference (IEMI)", IEEE Transactions on Electromagnetic Compatibility, August 2004, Vol. 46, No. 3, ISSN 0018-98375, pp 314 - 445
- [38] "The New Cold War: Defending Against Criminal EMI", Compliance Engineering, May/June 2001, pp 12-19, www.ce-mag.com
- [39] "The First 500 'Banana Skins'", compiled by Keith Armstrong on behalf of the EMC Journal, Nutwood UK Ltd, October 2007, available for purchase from pam@nutwood.eu.com and accessible on-line at www.theemcjournal.com. This is a collection of reports and anecdotes on EMI, previously published as a regular column in the EMC Journal.
- [40] IEC 62305 "Protection Against Lightning" in four parts – Part 4 covers the protection of electrical, electronic and programmable electronic equipment against damage from various lightning-related phenomena. Note that BS EN 62305 replaces BS6651 in the UK in mid-2008
- [41] "Improved measurement of radiated emissions from moving rail vehicles in the frequency range 9kHz to 1GHz", A C Marvin et al, 2004 IEEE EMC Symposium, Santa Clara, August 9-13, ISBN 0-7803-8443-1, pp. 19-24
- [42] International Telecommunication Union (ITU) 'K' standards on EMC and 'resistibility', via: www.itu.org
- [43] Telcordia telecomm standards, e.g. GR-1089-CORE "Electromagnetic Compatibility and Electrical Safety – Generic Criteria for Network Telecommunication Equipment" are available from: <http://telecom-info.telcordia.com>. Its unhelpful titles may make it necessary to search by keywords
- [44] The IEEE EMC Society, www.ewh.ieee.org/soc/emcs/
- [45] MIRA, the Motor Industry Research Association, www.mira.co.uk
- [46] "EMC for Systems and Installations", Tim Williams and Keith Armstrong, Newnes 2000, ISBN 0-7506-4167-3
- [47] "Mitigating the Low Level Lightning Threat to Wayside Signal Systems", R A Perala, R MacMillan, EMC Europe 2004, Eindhoven, Sep 6-10, ISBN 90-6144-990-1, pp 510-51
- [48] Police Information Technology Organisation (PITO), Automotive & Equipment Section (AES), AUTOMOTIVE CONFORMANCE SPECIFICATION 5 (Issue 9), 'A specification relating to the electromagnetic compatibility (EMC) performance of vehicle mounted, electrically powered equipment, designed for use by the Police & Fire Services of England and Wales', August 2004
- [50] "ICNIRP Statement on EMF-Emitting New Technologies", G. Ziegelberger, published by the Health Physics Society, 94(4):376-392; 2008, 0017-9078/08/0, from: www.icnirp.de/PubEMF.htm
- [51] "Gap Analysis between Defence and Commercial Standards", Peter Dorey, TÜV Product Service, EMC Compliance Journal, Issue 73 November 2007
- [52] CISPR 16-4, "Specification for radio disturbance and immunity measuring apparatus and methods. Uncertainty in EMC measurements"
- [53] "The Reality of Risks", Erik Hollnagel, Safety Critical Systems Club Newsletter, Vol. 17, No. 2, January 2008, pp 20-22, www.safety-club.org.uk
- [54] "Are 'Safety Cases' Working?", Tim Kelly, Safety Critical Systems Club Newsletter, Vol. 17, No. 2, January 2008, pp 31-33, www.safety-club.org.uk
- [55] "Reducing Risks, Protecting People", Health and Safety Executive, 2001, www.hse.gov.uk/risk/theory/r2p2.pdf
- [56] IEC 61508-3: "Functional safety of electrical, electronic and programmable electronic safety-related systems – Software Requirements"
- [57] "Noise, EMC and Real-Time", MISRA Report 3, February 95. The Motor Industries Software Reliability Association (MISRA), www.misra.org.uk
- [58] "Electromagnetic Compatibility of Software", IEE Colloquium, Thursday 12th November 98, IEE Colloquium Digest: 98/471, sales@iee.org.uk
- [59] "EMC-Hardening Microprocessor-Based Systems" Dr D R Coulson, IEE Colloquium "Achieving Electromagnetic Compatibility: Accident or Design", 16th April 97, IEE Colloquium Digest: 97/110, sales@iee.org.uk

NOTE: The software techniques described in [60] [61] and [62] are equally valuable for 'hardening' software and firmware to all types of transients (the main causes of EMI for software and firmware) and many other EM threats

- [60] "Designing Electronic Equipment for ESD Immunity", John R Barnes, Printed Circuit Design, vol. 18 no. 7, July 2001, pp. 18-26, www.dbicorporation.com/esd-art1.htm
- [61] "Designing Electronic Equipment for ESD Immunity Part II", John R Barnes, Printed Circuit Design, Nov. 2001, www.dbicorporation.com/esd-art2.htm
- [62] "Designing Electronic Systems for ESD Immunity", John R Barnes, Conformity, Vol. 8 No. 1, February 2003, pp. 18-27, www.conformity.com/0302designing.pdf
- [63] IEC/TR 61000-5-6:2002, "Electromagnetic Compatibility (EMC) - Part 5-6: Installation and Mitigation Guidelines - Mitigation of External EM Influences"
- [64] IEC 61000-5-2:1997 "Electromagnetic Compatibility (EMC) – Part 5: Installation and Mitigation Guidelines – Section 2: Earthing and cabling"
- [65] "EMC for Systems and Installations" Tim Williams and Keith Armstrong, Newnes 2000, ISBN 0-7506-4167-3
- [66] "EMC for Systems and Installations" Keith Armstrong, EMC Compliance Journal, 1999, www.compliance-club.com/KeithArmstrong.aspx
- [67] "Good EMC Engineering Practices in the Design and Construction of Industrial Cabinets", Keith Armstrong, published by REO (UK) Ltd in 2007, available from www.reo.co.uk. These techniques are equally relevant wherever two or more electrical/electronic components/modules/units/etc. are assembled in one box to create an item of equipment
- [68] "Good EMC Engineering Practices for Fixed Installations – for compliance with the EU EMC Directive, the IEE Wiring Regulations, and the lightning protection standard BS EN 62305", Keith Armstrong, to be published by REO (UK) Ltd in late 2008, available from www.reo.co.uk/knowledgebase
- [69] "Design Techniques for EMC", Keith Armstrong, EMC Compliance Journal, 1999 and 2006-8 versions available from the EMC Journal's archives at www.compliance-club.com
- [70] "EMC for Product Designers, 4th Edition" Tim Williams, Newnes, 2007, ISBN 0-7506-8170-5
- [71] "EMC for Printed Circuit Boards – Basic and Advanced design and layout techniques", Keith Armstrong, Armstrong/Nutwood 2007, ISBN: 978-0-9555118-0-6 (spiral bound) and 978-0-9555118-1-3 (paperback). Visit www.cherryclough.com for a contents list. Purchase from pam@nutwood.eu.com
- [72] "Robust Electronic Design Reference Book, Volumes I and II", John R Barnes, Kluwer Academic Publishers, 2004, ISBN: 1-4020-7739-4
- [73] "Electromagnetic Compatibility of Integrated Circuits: Techniques for Low Emissions and Susceptibility", Etienne Sicard, Sonia Ben Dia and Mohamed Ramdani, Springer Science & Business Media 2006, ISBN: 0-387-26600-3 or 978-0387-26600-8, e-ISBN: 0-387-26601-1, orders-ny@springer-sbm.com, www.springer.com/0-387-26600-3
- [74] "Mains Harmonics", Keith Armstrong, published by REO (UK) Ltd in 2007, available from www.reo.co.uk/knowledgebase
- [75] "Power Quality", Keith Armstrong, published by REO (UK) Ltd in 2008, available from www.reo.co.uk/knowledgebase
- [76] Department of Defense, MIL-STD-461F, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment"
- [77] "Fretting Corrosion in Electrical Contacts", E M Bock and J H Whitley, Twentieth Annual Holm Seminar on Electrical Contacts, October 29-31, 1974. Available as Tyco White Paper www.tycoelectronics.com/documentation/whitepapers/pdf/p154-74.pdf
- [78] "The Design of Military Equipment Enclosures to Minimise the Effects of Corrosion", John Terry, EMC-UK 2005 Conference, Newbury, Oct 13-14, pp 85-88
- [79] Ian MacDiarmid of BAE Systems, EMCIA seminar, Whitehall, London, UK, 14 December 2006, www.emcia.org

- [80] "EMC for Functional Safety", (half-day paper), Keith Armstrong, 2004 IEEE International Symposium on Product Safety Engineering, Santa Clara, August 13-15
- [81] "Why EMC Immunity Testing is Inadequate for Functional Safety", Keith Armstrong, 2004 IEEE International Symposium on EMC, Santa Clara, August 9-13 2004, ISBN 0-7803-8443-1, pp. 145-149. Also: Conformity, March 2005, pp 15-23, http://www.conformity.com/artman/publish/printer_227.shtml
- [82] "Functional safety requires much more than EMC testing", Keith Armstrong, EMC-Europe 2004, Eindhoven, September 6-10 2004, ISBN: 90-6144-990-1, pp. 348-353
- [83] "Design and Mitigation Techniques for EMC for Functional Safety", Keith Armstrong, 2006 IEEE International Symposium on EMC, 14-18 August 2006, Portland Oregon, ISBN: 1-4244-0294-8
- [84] "Technical Guidance Note on On-site EMC Testing", EMC Test Labs Association, TGN 49, www.emctla.co.uk
- [85] "Specifying Lifetime Electromagnetic and Physical Environments – to Help Design and Test for EMC for Functional Safety", Keith Armstrong, 2005 IEEE International Symposium on EMC, Chicago, Aug 8-12, ISBN: 0-7803-9380-5, pp. 495-499
- [86] "Safety Competency and Commitment – Competency Guidance for Safety-related System Practitioners", The IET, 1999, www.theiet.org/publicaffairs/scc/index.cfm
- [87] "An Introduction to Reverberation Chambers for Radiated Emission/Immunity Testing", G J Freyer, and M O Hatfield, ITEM 1998, www.interferencetechnology.com
- [88] "Coupling to Devices in Electrically Large Cavities, or Why Classical EMC Evaluation Techniques are Becoming Obsolete", John Ladbury, IEEE International Symposium on EMC, Minneapolis, Aug 02, ISBN: 0-7803-7264-6
- [89] CISPR 16-4, "Specification for radio disturbance and immunity measuring apparatus and methods. Uncertainty in EMC measurements"
- [90] IEC 61000-4-21, "Electromagnetic compatibility (EMC) – Testing and Measurement Techniques – Reverberation chamber test methods"
- [91] Ministry of Defence, Defence Standard 59-411, "Electromagnetic Compatibility", generally known as 'Def Stan 59-411' and available from www.dstan.mod.uk
 - Part 1: Management and Planning. Provides advice on the selection and specification of EMC requirements for military equipment and systems, advice on Commercial Off The Shelf (COTS) equipment procurement and provides a list of Electromagnetic Environment Effects (E3) definitions and terms. It also describes the management responsibilities and the essential requirements for control and test plans, test reporting and records.
 - Part 2: The Electric, Magnetic and Electromagnetic Environment. Details methods of how to identify and quantify the Electromagnetic Environment present for a variety of Defence scenarios. Detailed descriptions of the environment for some particular scenarios are given.
 - Part 3: Test Methods and Limits for Equipment and Sub-Systems. Details appropriate test methods and limits to be specified and gives technical details of the tests and describes the minimum performance criteria for test equipment specific to this Standard.
 - Part 4: Platform and System Test and Trials. Provides requirements for electromagnetic compatibility test and trials of platforms and large systems for Air, Land or Sea service.
 - Part 5: Code of Practice for Tri-Service Design and Installation. Describes the recommended design practices to ensure EMC in equipment, systems and platforms for Air, Land and Sea service.
- [92] IEC 62002:2006, "Mobile and Portable DVB-T/H Radio Access. Interface Conformance Testing"
- [93] "The Future of Market Surveillance for Technical Products in Europe", Ivan Hendrixx, Conformity, April 1, 2007, www.conformity.com
- [94] "EMC – Electromagnetic Theory to Practical Design", P A Chatterton and M A Houlden, John Wiley & Sons, January 1992, ISBN-10: 047192878X, ISBN-13: 978-0471928782

11. Annex A: Glossary of terms and abbreviations

These descriptions are provided as an aid to understanding this Guide.

Formal definitions for many of the terms may be found in the IEC International Electrotechnical Vocabulary: www.iec.ch/webstore/custserv/mld.htm.

λ	Wavelength	(Greek symbol: Lambda)
Ω	Ohms	(Greek symbol: Omega)
μ	Micro, one part in a million, 10^{-6}	(Greek symbol: Mu)
μs	Microsecond.	
A	Amp, the standard unit of measuring electrical current.	
AC	'Alternating Current', a term used to denote electrical power or signals that are at a frequency other than 0Hz.	
A/m	Amps/metre, a unit of magnetic field (H-field) strength, usually used for RF fields.	
AF	Audio Frequency, typically considered to be the range 20Hz to 20kHz.	
AM	Amplitude Modulation (usually of a carrier wave).	
BCI	Bulk Current Injection, an EMC immunity test method.	
Bill of Materials	The list of parts and materials required to construct something (BOM).	
BN	See Bonding Network.	
BOM	Bill Of Materials.	
BOM cost	The overall cost of the parts and materials required to construct something.	
Bonding	Making electrical connections. In the context of EMC, the type of bonding is usually 'RF bonding', that achieves a low impedance over the frequency range that is to be controlled.	
Bonding Network	<p>The interconnected metalwork associated with an installation, usually consisting at least of structural metalwork, creating an RF Reference to which the chassis or enclosures of electrical/electronic items are (or may be) electrically connected to help control EM phenomena.</p> <p>In a building or fixed site, the Bonding Network is almost always connected to the lightning protection system's earth electrode structures, and is often called a protective (or safety) earthing structure, earthing/grounding network, or similar.</p>	
Brownout	USA term for a dip: a reduction of the supply voltage well below its normal tolerances, followed by a recovery to the original level. The voltage during the dip does not reduce to zero. Brownouts can last for seconds, minutes, or even hours. Also known in the USA as a sag (but note that in IEC EMC terminology, a sag is a slow reduction in supply voltage over a period of time).	
Bypass conductor	See Parallel Earth Conductor, PEC.	
Carrier Wave	An unmodulated radio wave, or the unmodulated basis of a radio wave.	
CB	Citizen's Band. A band of frequencies within the 27MHz ISM band, used for walkie-talkies and vehicle-mounted radio communications with few restrictions on use.	
CE marking	A form of mark that indicates that a product is claimed by its supplier to comply with all relevant EU Directives, such as the EMC Directive [31].	

CEN	Comité Européen de Normalisation, a European organisation that produces standards, including electrotechnical and EMC standards for some industries
CENELEC	Comité Européen de Normalisation Electrotechnique, a European organisation that produces electrotechnical and EMC standards
Choke	An inductor used specifically to suppress radio frequencies, usually based upon a soft-ferrite material that behaves lossily at RF
CISPR	Comité Internationale Speciale des Perturbations Radioélectriques, a branch of the IEC devoted to producing EMC test standards, usually (but not always) for emissions.
CM	Common Mode
CM choke	A choke used specifically to suppress CM voltages or currents, usually at radio frequencies.
CM current	Common Mode current.
CM voltage	Common Mode voltage.
Coax, Co-ax	A coaxial type of cable, in which a single inner conductor is surrounded by a concentric conductor that acts as its return and as a shield.
Common Mode	A term used to describe voltages and/or currents that apply identically to all the conductors (including return conductors and shields) associated with a cable, or with an item of equipment, with respect to some remote reference. CM voltages or currents are always unwanted noise, and are associated with many EMC issues.
Common Mode current	A current that flows identically in all of the conductors (including return conductors and shields) associated with a cable, cable bundle, or with an item of equipment. CM currents are measured with respect to a remote RF Reference, such as the metal floor of a shielded room in which the tests are being conducted.
Common Mode voltage	A voltage that applies identically to all the conductors (including return conductors and shields) associated with a cable, cable bundle, or with an item of equipment. CM voltages are measured with respect to a remote RF Reference, such as the metal floor of a shielded room in which the tests are being conducted.
CMR, CMRR	Common-Mode Rejection, Common-Mode Rejection Ratio. A measurement of the degree to which an electronic component (e.g. a CM choke) attenuates the CM component of a signal, compared with the attenuation of the DM component.
Conducted	When applied to emissions or immunity, this term refers to unwanted EM energy conducted from equipment via the power supply or data, signal or control conductors.
Conducted emissions	Energy transmitted as EM waves along a cable or other conductor. Most countries have mandatory limitations on conducted emissions into their electrical power supply networks, to help reduce interference with other electronic equipment. Because conducted EM waves are a cause of radiated EM waves, these limitations also help protect licensed users of the radio spectrum.
Conducted transients	Conducted emissions that are transient (short-term) in their nature, such as 'spikes', usually described in time-domain terms, for example as a waveform, rather than frequency-domain terms, e.g. as a spectrum.
Continuous disturbance	A disturbance which cannot be resolved into a succession of distinct events by measuring equipment. For transient disturbances, this term is typically applied to disturbances that occur more than 30 times a minute on average.
CRT	A type of VDU based upon a Cathode Ray Tube.

CW	Continuous Wave, also Carrier Wave.
DC	‘Direct Current’, a term used to denote an electrical power or signal voltage or current at 0Hz.
Differential Mode	The mode of conduction of voltages and/or currents associated with intentional (wanted) power, signals, data, etc. A DM voltage is created on a conductor with respect to a different one in the same cable or item of equipment. A DM current flows conductor and returns by a different one in the same cable or item of equipment.
DM	Differential Mode.
DM choke	A choke used specifically to suppress DM voltages or currents, usually at radio frequencies.
Dip	A momentary reduction in the voltage of an AC or DC electrical power supply, usually for a time-period of less than one second.
Disturbance	Unwanted EM energy, which could cause a problem to victim equipment, often called EM disturbances. Disturbances may be produced by either intentional or spurious sources, from equipment, or by natural causes (e.g. lightning, or electrostatic discharge).
Dropout	A sudden reduction of the electrical power supply voltage to zero for short period of time, usually less than 1 second, followed by a recovery to the original level.
DSP	Digital signal processing, or digital signal processor.
Earthing	Sometimes called grounding; this is an electrical safety engineering term, with no relevance for EMC. However, because RF References are often also developments of existing protective earthing structures, the action of connecting to an RF Reference is often (mistakenly) called ‘earthing’. This mistaken use of electrical safety engineering terms in EMC work often leads to confusion and wasted time and cost.
Earth electrode	A conductor embedded in the soil beneath a site or building, to try to make a low-impedance connection to the mass of the planet. Sometimes called a ground electrode.
E-field	Electric field, measured in Volts/metre, V/m
EFS	<p>An acronym coined especially for this Guide, that means: “<i>Any entity including electrical or electronic technologies that provides one or more functions having a direct impact on safety</i>”. This definition is intended to cover the entire range of constructional and application possibilities, and so is not limited to – for example – the “safety-related systems” covered by IEC 61508 [7].</p> <p>An EFS is never a component, part, element, subsystem or subset of the entity that is providing the function that has a direct impact on safety. An EFS is <i>always</i> the final, completed entity, however its construction might be described.</p>
Electromagnetic	All electrical and electronic phenomena (signals, data, power, etc.) and radio waves are electromagnetic in nature – their energy flows as both electric energy (e.g. that flows in the electric field between the plates of a capacitor due to fluctuating voltages) and magnetic energy (e.g. that flows in the magnetic field due to fluctuating currents).
Electromagnetic Compatibility	<p>The ability of equipment or a system to function satisfactorily in its electromagnetic environment:</p> <ul style="list-style-type: none"> – without introducing intolerable EM disturbances into that environment, and; – without suffering unacceptable degradation of performance due to the EM disturbances present in that environment,

– when used as intended.

Electromagnetic Disturbance	An EM phenomenon that, in a specified situation, can cause EMI. In this Guide the terms EM Disturbance and EM Interference are lumped together and both are called EM Interference, as more usual colloquially.
Electromagnetic environment	The totality of the continuous and transient electric, magnetic, and EM fields, conducted EM energy, and electrostatic discharges at a given location.
Electromagnetic field	As an EM wave propagates in three-dimensional space and time, the magnitudes of its electric and magnetic waves can be represented as varying fields within the volume through which it is passing or has passed. Electric field strengths are measured in Volts/metre (V/m) and Magnetic field strengths in Amps/metre (A/m).
Electromagnetic interference	EMI. The degradation in performance, malfunction or damage that is the result of inadequate immunity to EM Disturbances. In this Guide the terms EM Disturbance and EM Interference are lumped together and both called EM Interference, as more usual colloquially.
Electromagnetic Pulse	A powerful radiated transient EM disturbance, sometimes used as shorthand for NEMP.
Electromagnetic wave	All EM energy travels in the form of waves, whether it is associated with electrical power, signals, data or control. In a conducted EM wave, the magnitudes of the voltages and currents vary along the conductor. In a radiated EM wave the magnitudes, the magnitudes of the electric and magnetic fields vary with position in three-dimensional space.
Electrostatic discharge	A sudden transfer of electric charge from one body to another, usually because of the voltage breakdown of the air between them (a spark). The dissipation of the charge causes transient disturbing currents to flow, and the spark is a source of very wideband radiated emissions.
EM	Electromagnetic.
EM-field, EM field	Electromagnetic field.
EM wave	Electromagnetic wave.
EMC	Electromagnetic Compatibility.
EMC Directive	Legal instrument by which all member states in the European Union (EU) are obliged to enact national laws that have the same effect, to restrict the supply of electrical and electronic goods in the EU to those that meet certain minimum requirements for electromagnetic emissions and immunity. [31]
EMI	Electromagnetic interference, sometimes simply 'interference'.
EMP	Electromagnetic Pulse.
ESD	Electrostatic discharge.
ETSI	European Telecommunications Standards Institute, www.etsi.org .
EU	European Union.
European Union	A trade bloc based in the continent of Europe, http://europa.eu
Fast transient	Usually used to describe an impulse with a risetime of under 100ns on power or signal cables. Most likely to appear in the form of a burst of such transients, generally caused by sparking at electromechanical contacts, also called 'Fast Transient Burst' (FTB) and Electrical Fast Transient (EFT).
FCC	The USA's Federal Communications Commission, responsible for creating the USA's EMC regulations and setting standards for the protection of the EM environment, and also for enforcing those laws and standards, www.fcc.gov .
FDA	The USA's Food and Drug Administration, responsible for ensuring the safety of medical equipment, as well as drugs, www.fda.gov .

FET	Field Effect Transistor.
Field	See Electromagnetic Field.
Filter	A combination of capacitors, inductors, RF absorbers and/or resistors intended to reduce the amount of EM energy at certain frequencies from being conducted along a cable or wire.
Flicker	Rapid fluctuations in the mains supply voltage, perceivable by the eye as a flickering in the illumination provided by electric lamps and luminaires.
FR4	A common type of dielectric material used for making PCBs, consisting of a woven mat of glass-fibres set in epoxy cement.
Functional Safety	That part of the overall safety that depends on the correct functioning of the EFS.
G	Gauss.
Gauss	A unit of magnetic field strength, usually used for DC and low-frequency magnetic fields. $10\text{mG} = 1\mu\text{T}$.
GHz	Gigahertz, units of thousands of millions (10^9) cycles per second.
GPRS	General Packet Radio System, a GSM cellphone technology that uses several GSM radio channels simultaneously to achieve higher data rates for digital wireless communications.
GSM	Global System for Mobile communications (originally Groupe Spécial Mobile), the normal digital cellphone system, called GSM-850 and GSM-1900 in the USA, and GSM900, GSM1800 everywhere else, the numbers reflecting the frequency range of operation.
GW	Gigawatts, units of thousands of millions (10^9) of Watts.
Grounding	Sometimes called earthing, this is an electrical safety engineering term, with no relevance for EMC. However, because RF References are often also developments of existing protective grounding structures, the action of connecting to an RF Reference is often (mistakenly) called 'grounding'. This mistaken use of electrical safety engineering terms in EMC work often leads to confusion and wasted time and cost.
Harmonics	Frequencies which are integer multiples of the fundamental frequency. In AC mains electricity supplies they are caused by the power supplies of equipment drawing current in a non-sinusoidal manner, which distorts the waveform. All repetitive non-sinusoidal waveforms can be represented as the sum of a number of its harmonics, with various amplitudes and phases applied to each harmonic.
H-field	Magnetic field.
HEMP	High-altitude ElectroMagnetic Pulse. A powerful EM radiated transient caused by nuclear bombs exploded in the upper atmosphere, capable of destroying electronic devices over a radius of several hundred km.
Hertz	Cycles per second, a measure of frequency.
HF	High Frequency, generally between 3 and 30MHz.
HIRF	High Intensity Radiated Field – a general term that includes continuous EM disturbances near to powerful broadcasting transmitters of ISM equipment, and transient disturbances such as created by radar transmitters and EMP, NEMP and HEMP.
HV	High Voltage. (In general usage: anything above 1kV rms AC, or 1.5kV peak DC. According to IEC standards: anything above 33kV AC rms or 46kV DC.)
Hz	Hertz.

IC	Integrated Circuit, a type of semiconductor device that contains many transistors, arranged to provide certain electronic functions. The latest types of IC can contain several million individual transistors.
IEC	International Electrotechnical Commission. Creates standards for EMC emissions and immunity, and safety, amongst many other issues, www.iec.ch .
IEMI	Intentional EMI, used by bad people (unless it is we who are using it), see [37] [38] and [34].
I/O	Input/Output.
ITU	The International Telecommunications Union, www.itu.org .
Interference	Electromagnetic Interference.
Interharmonics	Frequency components (generally below 10kHz) that are not an integer multiple of the fundamental frequency of the AC power.
ISM	<p>A number of frequency bands set aside by international treaties for use by Industry, Medicine or Science. There are no licensed radiocommunications in these bands, so the EM disturbances created by ISM equipment or systems should cause no interference with licensed users of the radio spectrum.</p> <p>However, the levels of EM emissions permitted in the ISM bands by the relevant emissions standard (CISPR11) can be very high indeed, sufficient to cause health hazards to personnel, and to interfere with almost any kind of nearby electronic (possibly even electrical) devices, equipment and systems. Immunity to EM disturbances from nearby ISM equipment is not covered by any EMC standards in the IEC 61000-4 series, or listed under the EMC Directive.</p>
kHz	kilohertz, units of thousands (10^3) of Hz.
kW	kilowatts, units of thousands (10^3) of Watts.
LAN	Local Area Network (example: Ethernet).
LCD	Liquid Crystal Display, used for displaying text and/or graphics. If used as a computer monitor they can be called a VDU.
LEMP	Lightning electromagnetic pulse: EMP caused by lightning strokes (either cloud-to-ground, or cloud-to-cloud). One of the means by which thunderstorms worldwide cost billions in damaged electronic equipment every year.
LF	Low Frequency, generally considered to be anything less than RF, i.e. frequencies below 150kHz.
Lightning protection	Protection against the direct and/or indirect effects of lightning.
Lightning Protection System	A system consisting usually of a mixture of conductors, shields, filters and surge suppression devices that provides a building, site, vehicle or vessel against the direct and/or indirect effects of lightning.
LPS	Lightning Protection System.
MCC	Motor Control Contactor. A power relay with protection functions used to protect motors from (for example) undervoltages, overcurrents, three-phase unbalance, etc.
MDA	See MHRA.
MHRA	The UK's Medicines and Healthcare Products Regulatory Agency, now incorporates what used to be called the Medical Devices Agency (MDA), and responsible for the safety of medical devices, equipment and systems.
MHz	Megahertz, units of millions (10^6) of Hz.

Microwave	Typically, the frequency range above 1GHz.
Microsecond	10^{-6} seconds, one microsecond (μ s) is one-millionth of a second.
Millisecond	10^{-3} seconds. One millisecond (ms) is one-thousandth of a second.
ms	Millisecond.
MV	Medium Voltage (according to IEC standards: anything between 1kV rms AC or 1.5kV peak DC and 33kV AC rms or 46kV DC)
MW	Megawatts, units of millions (10^6) of Watts
Nanosecond	10^{-9} seconds. One nanosecond (ns) is one-thousand-millionth of a second.
ns	Nanosecond.
NEMP	EMP emitted by the explosion of a nuclear bomb, capable of destroying electronic devices over a radius from several km to several hundred km – depending on the height of the explosion above ground, also see HEMP.
Parallel Earth Conductor	<p>A bonding conductor that connects the chassis or ‘earths’ of two or more items of equipment, to encourage currents flowing in the ‘earth’, ‘ground’, metal structure or common-bonding-network of a building or site to flow in the low resistance of the PEC instead of in the signal or power cables it is connected in parallel with.</p> <p>‘Parallel earth conductor’ is the term used in IEC 61000-5-2 [64], which is why it is used in this Guide, but it is not a very good term because a PEC does not necessarily have anything to do with protective (safety) earthing or grounding. ‘Parallel bonding conductor’ would have been a better term, and some standards use the term ‘bypass conductor’ instead of PEC.</p>
PC	Personal Computer.
PCB	Printed Circuit Board.
PDA	Personal Digital Assistant, usually a small portable computer with a wireless link to the Internet.
PEC	Parallel Earth Conductor.
PLC	Programmable Logic Controller.
PFC	Power Factor Correction. With respect to the mains current consumed by an item of equipment, it can either mean the reduction in harmonic current consumption, for example to meet emissions standards for mains harmonics (true power factor); or it can mean the reduction in the phase angle between sine-wave voltage and current (displacement power factor). Be sure you know which meaning is relevant.
Picoseconds	10^{-12} seconds. One picosecond (ps) is one million-millionth of a second.
PM	Pulse Modulation (usually of an RF carrier wave).
Power Quality	A general term embracing a number of issues affecting the quality of the AC or DC electrical power supply, such as dips, dropouts, interruptions, sags, swells, harmonic waveform distortion, inter-harmonic waveform distortion, surges, spikes and transients. The standard for Power Quality measuring instruments is IEC 61000-4-30.
PQ	Power Quality.
Printed Circuit Board	A laminated structure with layers of etched foil conductors (usually copper) known as tracks or traces, interspersed with layers of dielectrics (often a glass-fibre matrix). Sometimes called a Printed Wiring Board (PWB). The traces are interconnected between layers by plated-through holes (PTH) known as via holes. Electronic components are mounted onto the PCB and soldered to the traces on the outermost layer(s). Components with long pins or leads may be connected directly to traces on inner layers by plated through holes.

ps	Picoseconds.
PWM	Pulse Width Modulation: the mark/space ratio of a rectangular waveform is modulated to convey information, or to control electrical power.
Radiated emissions	Energy transmitted as EM waves in the air or other dielectrics. Most countries have mandatory limitations on radiated emissions, to help protect licensed users of the radio spectrum from EMI.
Radiated transients	Radiated emissions that are transient (short-term) in their nature, such as 'spikes'. Usually described in time-domain terms, for example as a waveform rather than frequency-domain terms (e.g. as a spectrum).
Radio frequency	Frequencies generally considered to be between 150kHz and 300GHz.
RF	Radio Frequency.
RF Reference	A conductive structure, usually a continuous or meshed (gridded) metal sheet or volume, in installations usually a meshed structure made of interconnected conductors and metal structures, that maintains a low impedance (generally much less than 1Ω) up to some defined frequency.
RFI	Radio Frequency Interference: electromagnetic interference that occurs at radio frequencies. Sometimes used to specifically mean interference to radio services such as broadcast radio or cellphones.
RFID	Radio Frequency Identification. An active or passive radio frequency transponder device attached to an item exchanges data with a host computer, computer system, or other device. Generally used for logistics, stock control, transport charging, medical and identity purposes etc., etc.
RMS	Root Mean Square, the square root of the sum of the squares.
SA	Spectrum Analyser.
Sag	A temporary decrease in the voltage of the AC or DC electrical power supply, typically more than 5% but less than 100%, Also known as a brownout.
Screening	An alternative term for shielding.
Shielding	The use of conducting material to form a barrier to EM waves, so that they are reflected and/or absorbed. Also known as screening.
SI	Signal Integrity.
Signal Integrity	The functional quality of a signal, measured by a variety of means. Digital signals are often characterised by their rise and fall times, percentage overshoot and undershoot, ringing amplitude, frequency and duration, and noise margin. Analogue signals are often characterised by their distortion and signal-to-noise ratio (SNR).
SMD	Surface Mounted Device, a device that uses SMT.
SMPS	Switch Mode Power Supply. This type of power supply performs power conversion functions by using power-switching PWM technologies, usually at several tens or hundreds of kHz, maybe even MHz, to achieve high levels of energy efficiency. SMPS is usually the term used for AC-DC converters providing DC power to electronic devices from the AC mains supply. DC-DC converters use the same technologies, but are usually just called DC/DC converters.
SMPSU	Switch Mode Power Supply Unit.
SMT	Surface Mount Technology, a technology for attaching devices to PCBs by solder solely on the surface of the PCB.
SPD	Surge Protection Device.
Spectrum	A way of representing an electrical or electronic event in the frequency domain, usually as a graph of amplitude versus frequency. Fourier

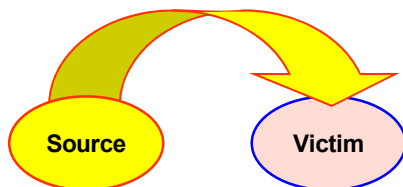
	transforms can be used to obtain spectrum data from a time-domain representation, such as a waveform.
Spike	An alternative, colloquial term for transient.
STP	Shielded Twisted Pair, a type of cable consisting of a send and a return conductor twisted together, with an overall shielding layer around them.
Surge	A type of transient voltage band/or current with a high energy content, typically produced by the current from a lightning strike coupling into long cables such as power supply or telecommunication cables. A surge is generally considered to have much longer risetimes and decay times, and much more energy associated with it, than a fast transient.
Surge protection device	A device for suppressing surges, typically by switching to a low-resistance state to shunt surge energy away from a protected circuit, such as an MOV, spark gap, TVS, SAD, etc. Sometimes called a surge arrester.
Swell	A temporary increase in the voltage of the AC or DC electrical power supply, typically more than 5% but less than 100%, for a period of time usually exceeding one second. The opposite of a sag.
T	Tesla
Tesla	A unit of magnetic field strength used for DC and low-frequency fields. Also, mT (milliTesla), μ T (MicroTesla) and nT (nanoTesla)
THD	Total Harmonic Distortion, one measure of the quality of an AC power or signal voltage or current, the ratio of the RMS value of its harmonic components, to that of its fundamental frequency.
Transient	A rapid change of the waveshape of voltage, current, or field, of very short duration followed by a return to steady state. Usually described in time-domain terms, for example as a waveform, rather than frequency-domain terms, for example as a spectrum.
TVI	Electromagnetic interference that specifically affects televisions, or the frequencies used for television broadcasting.
UTP	Unshielded Twisted Pair, a type of cable consisting of a send and a return conductor twisted together.
UHF	Ultra High Frequency, typically between 300MHz and 3GHz.
UWB	Ultra Wide Band (ultra-wideband), a radiocommunications technology that simultaneously transmits over a very wide range of frequencies, usually several GHz.
V	Volt, the standard unit of measuring electrical voltage (potential difference).
VDU	Visual Display Unit, generally a computer monitor.
VHF	Very High Frequency, typically between 30 and 300MHz.
VLSI	Very Large Scale Integration. A dense and complex IC, such as a memory, microprocessor or DSP device.
V/m	Volts/metre, the standard unit of electric field (E-field) strength.
W	Watts.
WAN	Wide Area Network.
Wi-Fi	A term for a specific commercial realisation of the IEEE 802.11 wireless datacommunication standard.

12. Annex B: Overview of electromagnetic phenomena, and how they can interfere

12.1 Overview of EM phenomena

There are three necessary contributors to every EMI event

- A source of EM phenomena (a possible EMI threat)
- An electrical, electronic or programmable device (a potential victim)
- And at least one EM coupling path between them



There are four types of EM coupling, and they can occur singly, or in any combination

- **1 Common impedances**
 - all metalwork and conductors have impedance (e.g. metal structures, chassis, cables, PCB tracks, etc.)...
 - so when carrying a current due to one electrical or electronic circuit they develop a voltage ('noise')...
 - ◆ that can interfere with *other* circuits that are connected to the same metalwork or conductors
 - one consequence is that there can never be a perfect 'earth' or 'ground'...
 - ◆ so 'safety earths' are ineffective for preventing EMI

Four types of EM coupling continued...

- **2 Electric (E) fields**
- **3 Magnetic (H) fields**
- **4 Electromagnetic (EM) fields**
 - these all radiate through the air (or through insulators such as plastic, wood, glass, etc.)...
 - and couple into *all* metalwork and conductors (e.g. metal structures, chassis, cables, PCB tracks, etc.)...
 - ◆ by inducing 'noise' currents and voltages into them...
 - which can then interfere with the electrical or electronic circuits connected to them

Four types of EM coupling continued...

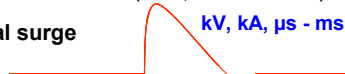
- The victim experiences the result as noise voltages and currents...
 - which can be either continuous or transient in nature...
 - and will occur as differential-mode (DM) noise and/or common-mode (CM) noise....
 - ◆ DM occurs between a signal or power conductor and its reference or return conductor
 - ◆ CM occurs on all conductors simultaneously

EM phenomena in long cables (including mains cables, because they are long)

■ Transient over-voltage surges

e.g. due to thunderstorms; reactive load switching such as large motors or capacitor banks; fault clearance (fuses, circuit-breakers)

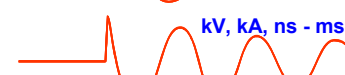
- example of unidirectional surge



- example of 'oscillatory wave'



- example of 'ring wave'

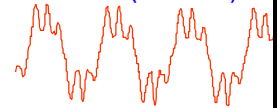


EM phenomena in long cables (inc. mains) continued...

■ Voltages at the frequency of the electrical power supply (and its harmonics)

10's of volts
(continuous)
kV (short-term)

- differential-mode (transverse) and common-mode (longitudinal), both continuous and transient

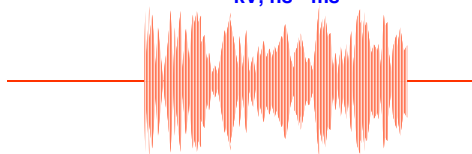


- caused by capacitive and inductive coupling ('crosstalk')
- caused by potential differences between different parts of the earthing system due to current leakages and faults in the power distribution
- caused by mains current flowing via insulation breakdown or spark aristor operation after an overvoltage event

EM phenomena in long cables (inc. mains) continued...

■ Fast transient overvoltage bursts

kV, ns - ms

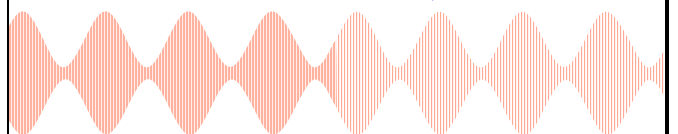


- caused by arcs and sparks
- e.g. switches, relays, contactors, commutator motors, poor connections, insulation breakdown, fault clearance (operation of fuses, circuit breakers, etc.)

EM phenomena in any cables (inc. mains)

■ Continuous radio frequency (RF) voltages and currents

V, kHz - GHz



- often many frequencies present at the same time
- usually modulated with different frequencies, using different modulation schemes (80% AM shown above)
- the longer the cable, the lower the frequency range

EM phenomena in any cables (inc. mains) continued...

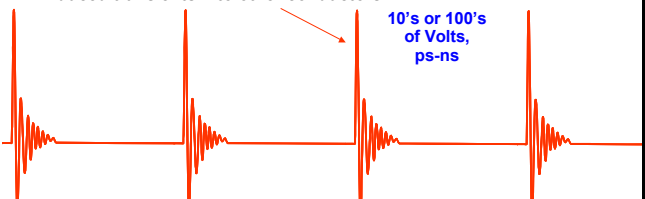
■ Very fast transients

usually caused by electrostatic discharges (not only from personnel)

- electrostatic discharges (ESD) directly into inadequately insulated conductors
- induced transients into other conductors

Personnel ESD
test waveform
30A
50ns or so

10's or 100's
of Volts,
ps-ns



EM phenomena associated with electrical power supplies

■ AC waveform distortion (this example is from Israel, in 2000)

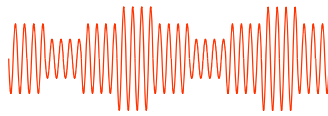
%, 50Hz - 2kHz



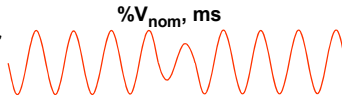
- the distortion can be *harmonic* (mostly caused by rectifiers and fluorescent lamps)
- and/or *interharmonic* (mostly caused by frequency-changing power converters)

EM phenomena in electrical power supplies continued...

- **Rapid fluctuations of the supply voltage** caused by load fluctuations



- **Voltage dips and flicker** from network control and fault-clearance

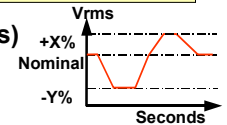


- **Dropouts / interruptions** from network protection and fault-clearance

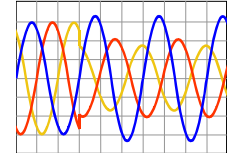


EM phenomena in electrical power supplies continued...

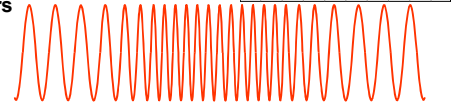
- **Slow variations (sags and swells)** caused by load variations



- **Three-phase voltage unbalance** caused by unbalanced loads, faults, etc.



- **Frequency variations** caused by significant load fluctuations on the generators



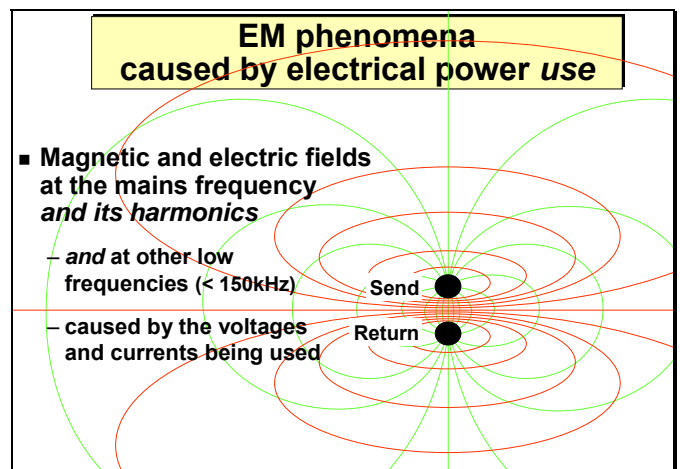
EM phenomena in electrical power supplies continued...

- **All the above mains-power-related phenomena can be much worse where the mains distribution system is of poor quality**
 - or when mobile or portable generators are used
- **And don't forget that electrical supply cables tend to be long**
 - so suffer from all of the EM phenomena in cables described earlier
 - ♦ sometimes with higher levels and/or lower source impedances (especially fast transient bursts and surges)

EM phenomena caused by electrical power use

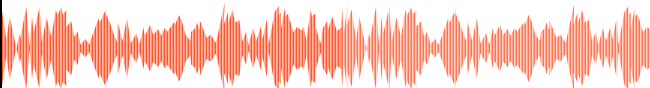
- **Magnetic and electric fields at the mains frequency and its harmonics**

- and at other low frequencies (< 150kHz)
- caused by the voltages and currents being used



EM phenomena caused by electrical power use continued...

- **Electric and magnetic fields at random frequencies 0 - 400GHz from all arcs and sparks**
 - from switches, relays, contactors, motor commutators, slip-rings, arc-welding, bad connections, insulation breakdown, fault clearance, etc.



EM fields from intentional radiators

- **Radio and TV broadcast transmitters, civilian and military radars (fixed and mobile)**

- ♦ aircraft spec's went from 1 to 6000 V/m over 15 years

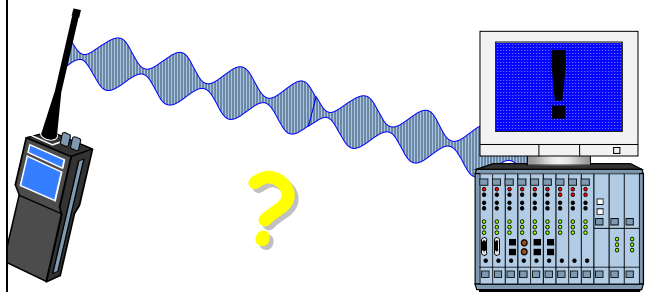
- **Plastics welders, induction furnaces, microwave ovens and dryers, etc.**

- **Cellphones, walkie-talkies, wireless LANs**

- ♦ even low-power cellphones have strong fields nearby



What distance from a 'hand-held' is equivalent to the immunity test levels under EMC and Medical Device Directives?



Typical type of transmitter or radiator	For 3V/m Domestic, commercial and light industrial generic, and most medical equipment	For 10V/m Industrial generic, and medical life support equipment
Cellphone in strong signal area, 'intrinsically safe' walkie-talkie RF power = 0.8 Watts	1.7 metres (5½ feet)	0.5 metres (1½ feet)
Cellphone in weak signal area and standby mode RF power = 2 Watts	2.5 metres (8 feet)	0.76 metres (2½ feet)
Walkie-talkie handset RF power = 4 watts (emergency services can be 10W)	3.7 metres (12 feet)	1.1 metres (3½ feet)
Vehicle mobile (e.g. taxicab), Electro-Surgery RF power = 100 Watts (some ES are 400W or more)	18 metres (59 feet)	5.5 metres (18 feet)

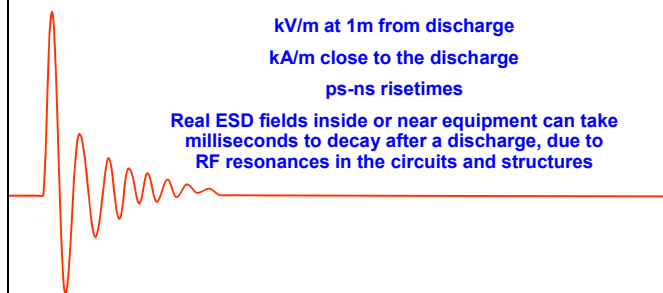
Multiply distances by $\sqrt{2}$ for one constructive reflection from a metal surface, by $\sqrt{3}$ for two reflections, etc.

EM fields caused by *unintentional* radiators

- **Everything** which uses electricity or electronics always 'leaks' and so emits some EM disturbances
 - the higher the rate of change of voltage or current, the worse the emissions tend to be
- Power and signals in devices, printed circuit board (PCB) traces, wires and cables leak EM waves
- Shielded enclosures leak EM waves from apertures, gaps and joints

Electric and magnetic fields from electrostatic discharges

– caused by personnel, furniture, and mechanical motion

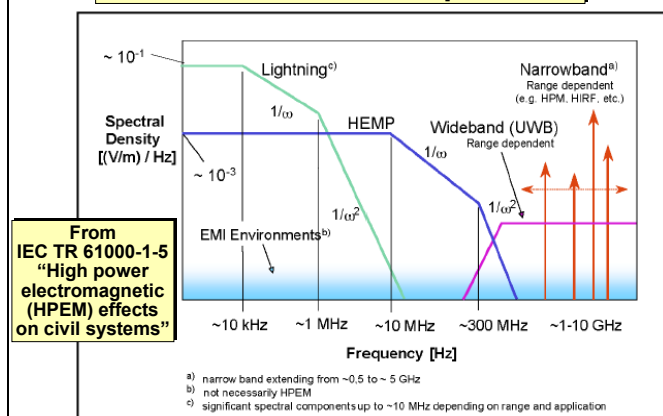


High Power Electromagnetic threats (HPEM)

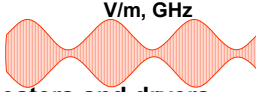
(including: Intentional EM interference: IEMI)

- Lightning
- Powerful radio and radar transmitters creating High Intensity Radiated Fields (HIRF) e.g. airports, harbours
- Nuclear electromagnetic pulse (EMP, NEMP, HEMP)
- A variety of powerful EM devices for military use
 - some of which can be purchased for private use, or constructed by a reasonably competent engineer
 - making IEMI a real possibility for some applications

Some HPEM examples



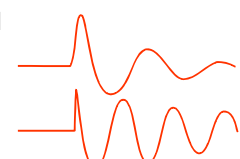
Most civilian immunity standards only test up to 1GHz, so don't cover...

- 1.8GHz GSM, GPRS, 2GHz 3G cellphones and datacomms 
- Microwave ovens, industrial heaters and dryers (usually 2.45 GHz, but can be 0.6 - 5GHz)
- Wireless LANs (1.8, 1.9, 2.45 and 5 GHz)
- Radars (airports and aircraft, harbours, ships, intelligent cruise control on cars) up to 77GHz
- IEMI above 1GHz
- Microwave communications (up to 60GHz) use narrow beams and low power – not usually a threat when off the beam's line

Most civilian immunity standards only test down to 150kHz so don't cover...

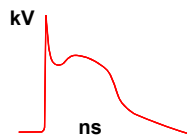
- Emissions from thyristor power control; motor drives (and other switch-mode or PWM power converters)
 - ♦ typically create strong disturbances 100Hz - 200kHz
- Electronic Article Surveillance (EAS) devices in shop doorways
 - ♦ can create very strong magnetic fields: 200Hz to 10MHz
- Mains supply emissions, including harmonics

Most civilian immunity standards only test with unidirectional surges to $\pm 2\text{kV}$, 100J

- Where surge protection not fitted, supply overvoltages will reach at least $\pm 6\text{kV}$, up to 300 times / year
 - ♦ depends on geography and whether the power lines are overhead or underground
- Superconducting magnet field collapse can create surges of up to 4 million Joules 
- Oscillatory surges can occur, and these cause more stress

Most civilian immunity standards test ESD with 0.7-1ns risetimes, up to $\pm 8\text{kV}$

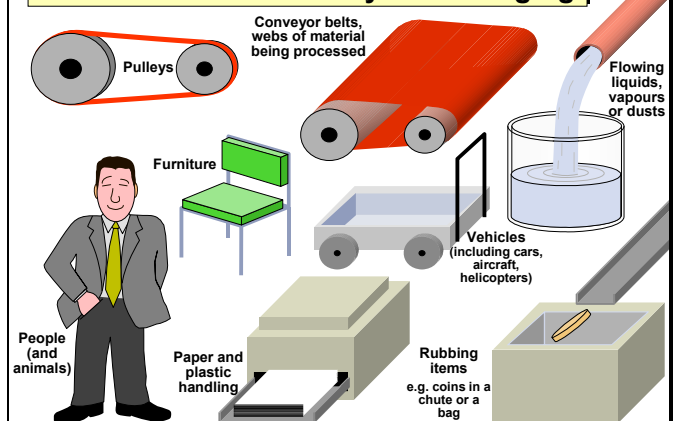
- But personnel ESD can be *much* faster than 0.7ns...
 - or can exceed $\pm 24\text{kV}$, when relative humidity falls below 25%
- ESD from processing machinery can be much faster, or have a much higher voltage, and can have also have much higher energy than personnel ESD
 - e.g. due to tribocharging



Some typical 'personnel ESD' potentials

Generation method	The electrostatic voltage generated (in kV)	
	10-20% Relative Humidity (RH)	65-90% Relative Humidity (RH)
Walking across carpet	35	1.5
Walking on vinyl floor	12	0.25
Worker moving at non-metal bench	6	0.1
Opening a vinyl envelope	7	0.6
Picking up a polyurethane bag	20	1.2
Sitting on a polyurethane foam padded chair	18	1.5

Some sources of ESD by tribocharging



12.2 The “Source – Victim/receptor Model”

At an engineering level all of the EM interference phenomena can be described via the simple source – victim/receptor model [94].

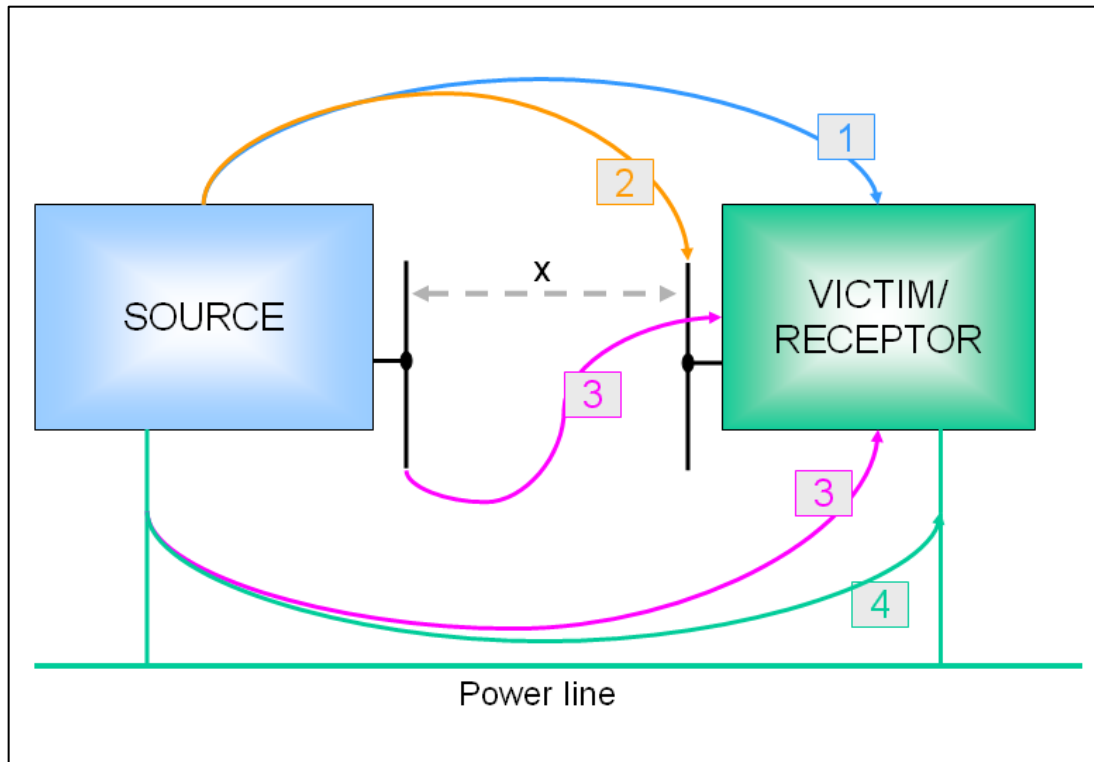


Figure B.1 The Source – Victim/Receptor model

It can be seen from the diagram that there are several paths from the source to the victim over which EM emissions and interference can propagate.

Path 1: Represents direct radiation from the source to the victim over the air. This is referred to as radiated interference. The emission propagates from the source via apertures, such as fan grille slots or via the system enclosure and enters the victim/receptor via apertures.

Path 2: Is also representative of radiated interference from the source. However in this instance the interference is ‘picked up’ by the victim cabling, such as antenna, power, signal or control cables (e.g. network or keyboard leads). The interference that propagates to the victim/receptor along the cable is termed conducted interference. It should be noted that incorrectly shielded wires, and metallic pipes or conduits can act as an antenna.

Another term used to describe interference coupling to non-antenna elements such as apertures, enclosures or cables is ‘back door’ coupling. This differentiates it from the coupling to actual antennas or electronic sensors, which is known as ‘front door’ coupling.

Path 3: Interference is radiated from an antenna or cables and couples to the victim/receptor via the aperture or enclosure.

Path 4: This represents a purely conducted disturbance where the emission from the source propagates to the victim through cabling. This cable could be the power line, as shown, or in practice any interconnecting cable (e.g. network connection) or conductor (e.g. a copper coolant pipe).

Path x: This path represents actual physical antennas and the source and receptors are specifically transmitting/receiving devices. This path is representative of normal radio communication (e.g. Wireless Local Area Networks (W-LAN), radio broadcast/reception). This distinction between intentional transmission/reception and unintentional transmission and unintentional reception is important.

12.3 Overview of how EMI can occur

Silicon chips (ICs) use extremely tiny feature sizes, which makes them very susceptible to overvoltages. They also operate at high speeds and low voltages (e.g. 1.2V), which makes them more susceptible to interference. But even large power semiconductors are not immune from interference, and neither are electromechanical devices (e.g. as used in 'hard-wired' safety systems).

This is a brief discussion on how EMI manifests in various types of electronic devices and circuits.

Figure B.2 provides an overview of how the three types of interference mechanism (direct, demodulation and intermodulation) can give rise to EMI in electronic devices and circuits.

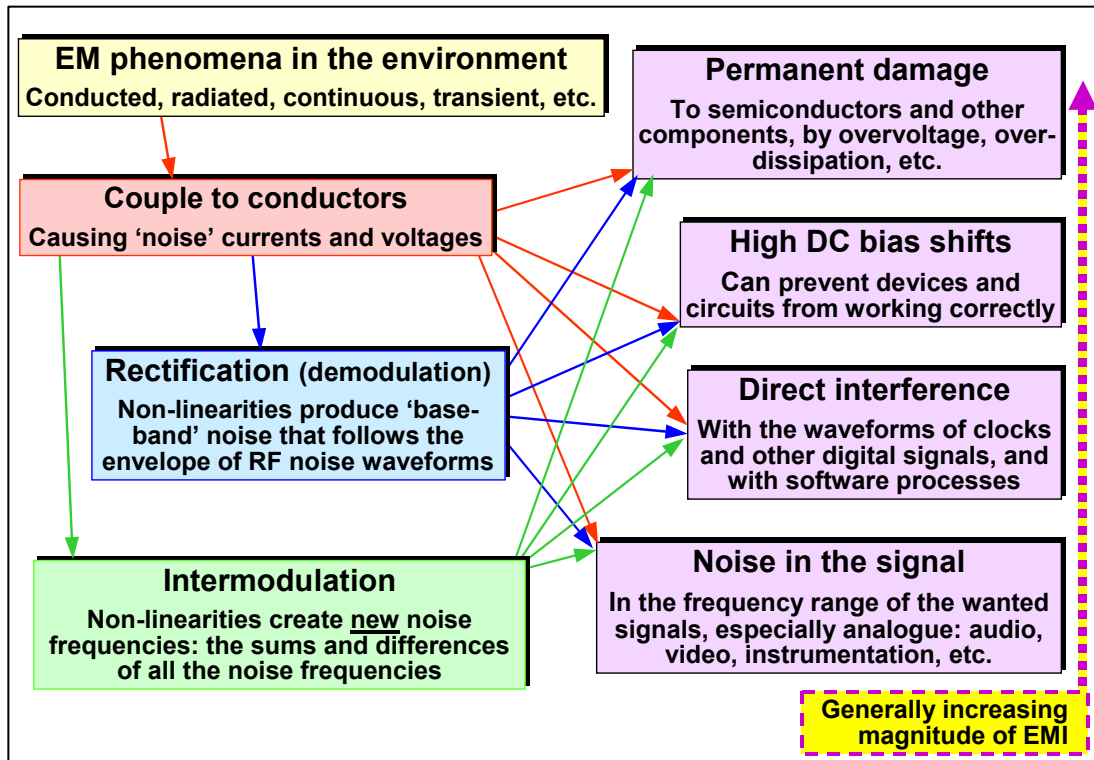


Figure B.2 The three interference mechanisms

12.3.1 Interference with analogue devices and circuits

Analogue circuits have no noise immunity as such, so circuits with higher signal/noise ratios (or which will be digitised with more bits) are more likely to suffer unacceptable errors due to EMI.

Errors usually increase in proportion to the square of the magnitude of the EM threat, so a 6V/m RF field can cause four times the error of 3V/m.

Full-scale errors are not unusual when measuring physical parameters, causing problems for measurement and control of:

- Physiological parameters
- Chemical reactions
- Temperature
- Pressure
- Weight, mass
- Flow, velocity, movement
- Level, angle
- etc....

EMI errors are most likely in low-level signals, e.g. millivolt-output transducers, a common problem for microphones, strain gauge sensors, and especially for temperature sensors.

Transient EMI produces transient errors, which many types of analogue circuits (those with no 'memory' of what has gone before) will recover from and continue as normal (assuming the transients are not so high as to cause actual damage). For example, an audio signal might click, or a needle twitch in a meter reading.

For such types of circuits, continuous EMI is often worse than even large transients, because even though the errors may be small they are continuous and cannot be ignored. For example a background whine in an audio signal, a zero error in a meter reading.

Analogue devices are easily destroyed by overvoltages from surges, fast transients, ESD and very high-power RF (mostly a military, security or IEMI issue).

12.3.2 Interference with digital devices, circuits and software

A well-designed digital circuit has a good 'noise margin' and completely ignores continuous EMI up to a certain level. Where continuous EMI is low enough, transient events will be the only problem.

When the magnitude of the EMI (continuous or transient) exceeds the noise margin, a variety of malfunctions can occur, for example:

- Errors in data received over communication links, leading to false data and false operations based on that data
- Errors in communications and control, for example false key-presses, possibly leading to uncommanded operations
- Incorrect software operation, for example:
 - continually repeating an inappropriate activity or series of activities ('looping')
 - changing operational mode (e.g. from crawl to full speed)
 - stopped operation (often called a 'freeze' or 'crash'), which can cause the control outputs to assume random combinations of states, including those which can have undesirable or unsafe results for whatever is being controlled

All digital devices can easily be destroyed by overvoltages from surges, fast transients, ESD and very high-power RF (mostly a military, security or IEMI issue) with powerful microprocessors and their memory chips being the most vulnerable.

Some programmers have been known to forget that all software runs on physical devices, and when those devices are crashed or destroyed by high levels of EMI, software techniques cannot work.

12.3.3 Interference with power semiconductors

Permanent damage can be caused by overvoltages, surges, fast transients, ESD, and also by overcurrents, so lightning effects can be significant for them.

Power semiconductors are generally unaffected by conducted and radiated RF, magnetic fields, etc., at levels that occur most of the time (excluding military, security or IEMI threats, such as NEMP), but they are ultimately controlled by digital ICs that can suffer from all of the problems listed earlier and can cause the control terminals of the power devices to be triggered at the wrong time – causing malfunctions and/or actuation of protective devices, and/or damage up to and including explosive disassembly.

12.3.4 Interference with signals

As well as preventing semiconductor devices from operating correctly (e.g. by shifts in their DC bias levels) many kinds of EMI can distort or even mimic real signals. Signals carried on wires or cables are generally more susceptible, the longer the wire or cable. These issues are included in the above analyses.

12.3.5 Interference with electromechanical devices

So-called 'hard-wired' circuits use electromechanical devices, which many designers seem to assume are totally immune to all EM threats. But dips and dropouts in their AC or DC supplies can cause relays, contactors and solenoids to 'drop out', individually – depending on type, age, and temperature. If they were held-in by a normally-open contact, or operated on a reduced 'hold-in' voltage – they may not pull back in again after the dip or dropout is over.

Shock and vibration can make switch contacts 'chatter', causing sparking, which can interfere with all kinds of electronic devices.

Overvoltages due to surges and fast transients can make open contacts spark-over, which is the same as closing them momentarily – applying power to circuits which should be off.

Overcurrents can 'weld' contacts together, so that they won't open when required. The design of most electromechanical switches allows them to change state mechanically, even when their contacts are welded and cannot change state, so they can be mechanically in an OFF position when one or more of their contacts is still in the ON position. This can be a significant problem for switches, relays and contactors that do not use positively-guided or forced contacts, or where feedback of actual contact position is not used.

An increasing number of electromechanical devices are employing electronic devices to add functionality, for example 'safety relays', MCCs (motor control contactors), self-protected motors, so can suffer from all the interference problems that electronic devices are prone to. The electronic content of any electromechanical device should always be asked about, and if it contains even one diode, transistor, hall sensor or IC – it should be treated as an electronic device.

13. Checklists

These checklists are provided as an aid to managing or assessing the work, when using this Guide. When completed, they become an important part of the final EFS documentation (see 0.10.5).

The numbers of each line correspond to the text above in which they are described.

Each checklist starts on a new page, to facilitate their copying and use.

A number of boxes are left blank for your own titles and information.

Many of the replies to the checklist questions will be references to documents that answer the requirement in detail, where there is not enough room on the form.

Sometimes, people just tick checklist boxes just for project management or assessment meetings, to give the impression that they are on schedule, when in fact they have not done the necessary work – or not done it with the thoroughness that is required given the safety risk levels (or risk reductions) to be achieved. This is not acceptable for the process covered by this Guide.

It is important for everyone to understand that the detailed work must actually be done, so that the *intent* of this Guide is followed. A checked-off checklist is not worth the paper it is printed on, if the actual work has not been done as well as is needed (see 0.10.4).

Therefore, managers and assessors should only 'tick' items on these checklists when they have satisfied themselves that the detailed work associated with the item, described in the text above, has *actually been performed* according to this Guide and good engineering practices, using the appropriate diligence (see 0.10.4).

13.0 Checklist for Step 0: Management and planning

Text ref.	Action			Comments
0.10.1	Name the responsible person(s)			
0.10.2	i) Describe the boundaries of the EFS			
	ii) Specify the EFS			
	iii) Specify the purpose and functions of the EFS			
	iv) Describe the location(s) where the EFS is intended to be installed and/or operated			
	v) Specify the electromagnetic and physical environment(s) over the anticipated lifecycle of the EFS			
	vi) Specify the electromagnetic and physical requirements for the EFS to achieve the desired levels of safety risks (or risk reductions) over the anticipated lifecycle			
	vii) Name the person who has overall responsibility for the plan and responsibility for the final electromagnetic and physical characteristics of the EFS over the anticipated lifecycle			
	viii) Name any other people who also take some part of the responsibility for the final electromagnetic and physical characteristics of the EFS being good enough for the anticipated lifecycle			
	ix) List all standards; specifications; design guides; quality control (QC) procedures; and in-company design guides and checklists to be used to guide the design testing and QC			
	x) List any training; third party expert assistance or third-party testing services required by the above personnel			
	xi) List any publications; computer-aided tools or test equipment required by the above personnel			
	xii) Identify the procedure that will maintain lifecycle electromagnetic and physical performance during maintenance repair and refurbishment of the EFS (carried out by the creator or not)			
	xiii) a) List the documentation produced by the above personnel for in-company use to demonstrate that they have discharged their responsibilities correctly			

	xiii) b) List the documentation produced for customers to ensure they are correctly advised on all of the electromagnetic and physical issues and on the resulting functional behaviour of the EFS when exposed to all of the electromagnetic and physical phenomena that could occur in its environment(s) over its lifecycle			
	xiii) c) List the documentation produced for customers to inform them of any restrictions concerning future changes to the electromagnetic and physical environment(s) of the EFS over its anticipated lifecycle.			
	xiv) Identify the fixed points in the project programme when progress will be reviewed by senior personnel and/or independent experts and changes to the programme of the project made if necessary; give the relevant details when they have occurred			
	xv) Give the timescales for the above activities carried out by the above personnel			
0.10.3	Give details of the anticipated lifecycle of the EFS			
0.10.4	Describe the amount of effort that is considered appropriate taking the level of safety risk (or risk-reduction) to be achieved by the EFS into account			
0.10.5	List the documentation that will be produced during the project and describe how it is to be stored (media; formats; ensuring security and readability etc.), and referenced			
0.14	Describe any changes to the above that occur during Steps 1 through 9.			

13.1 Checklist for Step 1: Determining Intersystem EM and Physical Phenomena

Text ref.	Action			Comments
1.2	Specify the location(s) of the items of equipment and the routes taken by their cables			
1.3	Assessing the EM environment over the anticipated lifecycle			
1.3.2	Give the questions and responses to a checklist of initial questions if used			
1.3.3	Describe the future technology trends and future changes in the environment that have been taken into account			
1.3.4	Describe how any mobility or portability of the EFS was taken into account			
1.3.5	Describe all other EM issues taken into account			
1.3.6	Give the assessment of how the EM and physical phenomena (threats) in the environment could affect the technologies employed by the EFS			
1.3.7	Describe any in-depth investigations into aspects of the environment			
1.3.8	Describe how measurement uncertainty was taken into account			
1.3.9	Give the quantified EM environment specification for the EFS anticipated lifecycle			
1.4	Assessing the physical environment over the anticipated lifecycle			
1.4.2	State the physical issues that were taken into account			
1.4.3	Describe how measurement uncertainty was taken into account			
1.4.4	Give the quantified physical environment specification for the EFS anticipated lifecycle			
1.5	State the possible effects of EFS emissions on other EFS			
1.6	Describe any iterative changes to the EM and physical intersystem specifications, for example resulting from design, assembly, validation, etc.			

13.2 Checklist for Step 2: Determining Intrasystem EM and Physical Phenomena

Text ref.	Action			Comments
2.2	To avoid duplication, see the response to checklist 1.2, that specifies the location(s) of the items of equipment and the routes taken by their cables			
2.3	Assessing the EM environment over the anticipated lifecycle			
	a) Give the questions and responses to a checklist of initial questions if used			
	b) Describe the future technology trends and future changes in the EFS that have been taken into account			
	c) Describe how any mobility or portability of the EFS was taken into account			
	d) Describe all other EM issues taken into account			
	e) Compare the EM phenomena assessment with the electronic technologies employed by the EFS			
	f) Describe any in-depth investigations into aspects of the intrasystem environment			
	g) Describe how measurement uncertainty was taken into account			
	h) Give the quantified EM intrasystem environment specification for the EFS anticipated lifecycle			
2.4	Assessing the physical environment over the anticipated lifecycle			
	a) State the physical issues that were taken into account			
	b) Describe how measurement uncertainty was taken into account			
	c) Give the quantified physical intrasystem environment specification for the EFS anticipated lifecycle			
2.5	Describe any iterative changes to the EM and physical intrasystem specifications, for example resulting from design, assembly, validation, etc.			

13.3 Checklist for Step 3: Specify electromagnetic and physical phenomena *vs* the functional performance required to achieve the desired levels of safety risks or risk-reductions

Text ref.	Action			Comments
3.2	State the EMC Safety Requirement Specifications			
3.3	Describe how EM and physical uncertainties were taken into account in the above specifications			
3.4	Two types of risk assessment are required			
	a) State the document reference for the initial risk assessment			
	b) State the document reference for the final risk assessment			
3.5	Describe the procedure by which the hazard analysis and risk assessments are kept 'live' throughout the EFS project			
3.6	Give the emissions specifications for the EFS			
3.8	Describe any iterative changes to the above specifications, for example resulting from design, realisation, verification, validation, etc. during the later stages of the EFS project.			

13.4 Checklist for Step 4: The study and design of the EFS

Text ref.	Action			Comments
4.2	Describe how the design was controlled to achieve the EMC safety specifications over the lifecycle			
4.2.1	a) List the standardised methods that were used in the hazard/risk assessments			
	b) List the non-standardised methods that were used in the hazard/risk assessments			
4.2.2	Describe how the common but incorrect assumptions in Risk Assessment were avoided			
4.2.3	Describe how EMI and intermittencies were taken into account in the Risk Assessment			
4.2.4	Describe any iterative changes to the risk assessments for example resulting from design assembly validation etc.			
–	Any other measures or techniques that were used to help meet the EMC safety requirements over the lifecycle			
4.3	List all the design and development measures and techniques that were used to help meet the EMC Safety specifications over the lifecycle, and provide all necessary references so that they may be assessed			
4.3.1	Design of EFS architecture			
4.3.2	Avoidance of unsuitable components; and avoidance of unsuitable mechanical electronic hardware software techniques			
4.3.3	Choice of suitable components; and choice of suitable mechanical electronic hardware and software techniques			
4.3.4	'Hardening' of communications			
4.3.5	Use of optical links instead of conductors			
4.3.6	Use of wireless links instead of conductors			
4.3.7	Use of analysis and testing techniques to guide design, including appropriate reliability and security			
	a) Prior experience			
	b) EM testing			
	c) HALT testing			
	4.3.8 Determination of the 'natural' susceptibilities of hardware software and firmware			
4.3.9	Use of appropriate design techniques for bonding, wiring, cabling and PCBs			
	a) Cable screening (shielding)			
	b) Cable double screening (shielding)			

	c) Peripheral (360°) termination of cable screens (shields) to enclosure shields at both ends of a cable (inside equipotential zones only or with the addition of a parallel earthing conductor)			
	d) Twisted wire pairs (with or without cable shielding)			
	e) Separation of cables carrying signals of different levels and/or types (IEC 61000-5-2 recommends the use of five 'cable classes' and the minimum spacings between them)			
	f) Shielding from metallic (or metallised) structures			
	g) Providing a low-impedance path for a cable's common-mode current in close proximity to the cable			
	h) Use of fibre-optic, infra-red or radio links instead of conductive cables			
	i) Provision of PCB 'ground' or 0V reference that has a low impedance over the frequency range to be controlled.			
	j) PCB power distribution systems that have low impedance and low-Q resonances over the frequency range to be controlled			
	k) Separation (segregation) on PCBs between switch-mode power converter, analogue and digital circuits			
	l) Use of localised shielding and/or filtering of components or areas of the PCB			
	m) Suppression of conducted disturbances at the interfaces between a PCB assembly and other boards or cables, using shielding, filtering, overvoltage suppression, galvanic isolation techniques, etc.			
4.3.10	Use of computer-aided design tools to optimise electromagnetic characteristics			
4.3.11	Use of EM mitigation techniques			
	a) Shielding			
	b) Filtering			
	c) Surge or transient suppression			
	d) Galvanic isolation			
	e) Creation of (and connection to) an RF Reference Plane			
	f) Any other electromagnetic mitigation techniques not already described			
4.3.12	Physical mitigation techniques			
	a) Shock and vibration mountings (active or passive)			
	b) Vibration-proof fixings for electrical contacts and other fixings			
	c) Avoidance of resonance in physical structures			
	d) Protective enclosures			

	e) Conformal coatings and/or encapsulation			
	f) Grease			
	g) Paint			
	h) Cable ties and other types of cable restraints			
	i) Anti-condensation techniques			
	j) Sealed enclosures			
	k) Forced ventilation, air-conditioning, etc.			
	l) Positively pressurised enclosures			
	m) Maintaining minimum levels of humidity to help control ESD			
	n) Any other physical mitigation techniques not already described			
4.3.13	'Layering' or 'nesting' techniques used for electromagnetic or physical mitigation			
4.3.14	Fault mitigation techniques			
4.3.15	Mitigation of problems caused by foreseeable use (misuse)			
4.3.16	Describe how the user is not relied upon to reduce the risk			
4.3.17	Use of checklists based upon case studies and experience obtained in similar applications			
4.3.18	Taking the electrical power supply distribution system into account			
4.3.19	The EM mitigation techniques used where there are multiple redundant channels to avoid common-cause failures			
4.3.20	Techniques for sensing or otherwise monitoring the EM/physical environment			
4.3.21	Safe use of fail-safe methods			
4.3.22	'Hardening' integrated circuits (ICs)			
4.3.23	'Hardening' digital and analogue circuits and PCBs			
4.3.24	'Hardening' software and firmware			
4.3.25	Systems installations and power quality			
	a) Cable segregation and routing			
	b) Provision of paths for the return of common-mode currents			
	c) 'Mesh' bonding of the earth/ground structure			
	d) EM mitigation (filtering shielding surge protection galvanic isolation reference plane bonding etc.)			
	e) Improving the quality of AC mains power			
	f) Lightning protection			
–	Any other measures or techniques that were used to help meet the EMC safety requirements over the lifecycle			

4.4	List all the realisation (assembly, construction, integration, manufacture, etc.) measures and techniques that were used to help meet the EMC Safety specifications over the lifecycle, and provide all necessary references so that they may be assessed			
4.4.1	Procuring materials components and products according to their EM/physical specification			
4.4.2	Avoiding counterfeit parts			
4.4.3	Assembly according to the design			
4.4.4	Control of suppliers and subcontractors and their suppliers and subcontractors etc.			
	a) Sample-based EMC/physical verification upon delivery			
	b) Sample-based EMC/physical verification in serial manufacture			
	c) EMC/physical verification as appropriate whenever there is any change in the design including the use of alternative components.			
–	Any other measures or techniques that were used to help meet the EMC safety requirements over the lifecycle			
4.5	List all the installation and commissioning measures and techniques that were used to help meet the EMC Safety specifications over the lifecycle, and provide all necessary references so that they may be assessed			
4.5.1	Any constraints on the physical positioning of the items of equipment that comprise the EFS			
4.5.2	Any constraints on cabling			
4.5.3	The methods of terminating any cable shields (screens)			
4.5.4	Constraints on connectors and glands and their assembly			
4.5.5	The electrical power supply requirements (power quality)			
4.5.6	Any additional shielding (screening) required			
4.5.7	Any additional filtering required			
4.5.8	Any additional overvoltage and/or overcurrent protection required			
4.5.9	Any additional power conditioning required			
4.5.10	Any additional electrostatic discharge protection requirements			
4.5.11	Any additional physical protection required			
4.5.12	Any earthing (grounding) and bonding requirements			
4.5.13	Protection against corrosion			
	a) Oxidation			
	b) Fretting			
	c) Galvanic Corrosion			

4.5.14	The procedures materials and expertise to be used			
–	Any other measures or techniques that were used to help meet the EMC safety requirements over the lifecycle			
4.6	List all the measures and techniques that were applied to issues such as operation, maintenance, repair, refurbishment, etc., to help meet the EMC Safety specifications over the lifecycle, and provide all necessary references so that they may be assessed			
4.6.1	Comprehensive Instructions			
	a) Operational requirements in the User Manual User Instructions Operator Manual etc.			
	b) Maintenance requirements in the Maintenance Manual Maintenance Instructions etc.			
	c) Repair requirements in the Repair Manual Instructions for Repair, etc.			
4.6.2	Maintenance, repair, refurbishment procedures and planning of mitigation measures			
4.6.3	Maintain EM/physical characteristics despite repairs refurbishment etc.			
4.6.4	Constraints on the EM environment			
4.6.5	Disassembly/reassembly techniques to preserve EM characteristics			
4.6.6	Periodic testing (proof testing) of critical components			
4.6.7	Periodic replacement of critical components			
4.6.8	Verification of the absence of corrosion			
	List any other operation, maintenance repair and refurbishment techniques that were used to help meet the safety requirements, and provide all necessary details.			
4.7	List all the measures and techniques that were applied to issues such as modifications and upgrades (to hardware and software) to help meet the EMC Safety specifications over the lifecycle, and provide all necessary references so that they may be assessed			
4.7.1	Assessing the effect of proposed modifications and upgrades			
4.7.2	Maintaining acceptable EM and physical characteristics			
–	Any other measures or techniques that were used to help meet the EMC safety requirements over the lifecycle			

13.5 Checklist for Step 5: Creation of EM and physical verification/validation plans

Text ref.	Action			Comments
5.2	Planning for Verification, and for Validation			
5.2.1	Provide the plan for the verification activities throughout the project			
5.2.2	Provide the plan for the validation of the EFS			
5.2.3	Describe any iterative changes that have been made to the EMC Safety specifications as a result of planning the verification or validation, and why.			
5.8	Describe how the test levels have taken measurement uncertainty into account and show how the 'expanded uncertainty' used is appropriate for the level of risk (or risk reduction) specified for the EFS.			
5.9	Describe how simultaneous phenomena have been dealt with in the verification and validation planning			
5.10	Describe the verification or validation techniques that have been applied to emissions from the RFS			
5.11	Describe how foreseeable faults and misuse have been dealt with in the verification and validation planning			
5.12	Describe how safe shutdowns, alarms, and the like have been dealt with in the verification and validation planning			
5.13	Describe how verification during operation has been dealt with in the verification and validation planning			
–	Any other verification measures or techniques that were used to help meet the EMC safety requirements over the lifecycle			

13.6 Checklist for Step 6: Selection of standard products and/or specifying custom hardware or software items

Text ref.	Action			Comments
6.1	State whether Step 6 was permitted by the design of the EFS			
6.3	The Step 6 activities (where permitted by the EFS design) for a Simple EFS			
6.3.2	Describe any cases where it was necessary to modify the design and/or verification of the EFS, for example by adding EM or physical mitigation, in order to use any standard volume-manufactured products incorporated within the EFS.			
6.3.3	Describe how sufficient confidence was achieved, appropriate for the level of risk (or risk reduction) specified for the EFS, in the EM and/or physical performance of any standard volume-manufactured products incorporated within the EFS. (Note that CE marking and/or manufacturers certificates or declarations should not, on their own, be considered to be evidence of performance.)			
6.3.4 and 6.3.5	How to overcome the lack of useful product data			
	a) Protective enclosures			
	b) Clever designs			
	c) Additional product verifications			
	d) Use of custom product(s) instead			
	e) Anything else?			
–	Any other measures or techniques that were used to help meet the EMC safety requirements over the lifecycle			
6.4	The Step 6 activities (where permitted by the EFS design) for a Complex EFS			
6.4.2	Step 6a: Give the specifications for the EM/physical phenomena vs functional performance for <u>each</u> custom-engineered item of hardware and/or software that is to be incorporated within the EFS. For each item, this requires a separate checklist in its own right, each with the structure of the Step 3 checklist given in 13.3.			
6.4.3	Step 6b: Study and design each custom-engineered item of hardware and/or software that is to be incorporated within the EFS. For each item, this requires a separate			

	checklist in its own right, each with the structure of the Step 4 checklist given in 13.4.			
6.4.4	<p>Step 6c: Create EM and physical verification/validation plans for each custom-engineered item of hardware and/or software that is to be incorporated within the EFS.</p> <p>For each item, this requires a separate checklist in its own right, each with the structure of the Step 5 checklist given in 13.5.</p>			
6.4.5	<p>Step 6d: Select the commercially-available standard products to be used for each custom-engineered item that is to be incorporated within the EFS.</p> <p>For each item, this requires a separate checklist in its own right, each with the structure of the Step 6 checklist given in 13.6.</p>			
6.4.6	<p>Step 6e: Assemble and check each custom-engineered item of hardware and/or software, that is to be incorporated within the EFS.</p> <p>For each item, this requires a separate checklist in its own right, each with the structure of the Step 7 checklist given in 13.7.</p>			
6.4.7	<p>Step 6f: Verify and finally validate each custom-engineered item of hardware and/or software, that is to be incorporated within the EFS.</p> <p>For each item, this requires a separate checklist in its own right, each with the structure of the Step 8 checklist given in 13.8.</p>			
6.5	Describe any iteration of any previous Step and how it was caused by the activities of Step 6.			
–	Any other measures or techniques that were used to help meet the EMC safety requirements over the lifecycle			

13.7 Checklist for Step 7: Realisation of the EFS (assembly, system integration, installation, commissioning, etc.) and the verification that occurs throughout this process

Text ref.	Action			Comments
7.3	Following the EFS designers' instructions			
	a) Describe how it was ensured that the materials, components, products and equipment were all procured according to their EM/physical specifications			
	b) Describe all the actions that were taken to avoid counterfeit parts and show how they are commensurate with the levels of risk (or risk-reduction) required for the lifecycle of the EFS			
	c) Describe the controls that are in place to ensure all suppliers and subcontractors provide adequate documentation. Note: These controls should apply to the entire supply chain.			
	d) Describe how it was ensured that the realisation of the EFS (manufacture, assembly, integration, installation, etc.) was fully in accordance with the EFS design.			
7.4	Describe the Quality Control regime that was used			
7.5	Describe how the specifications (from Steps 1, 2 and 3) were modified, if they were, as a result of the Step 7 activities			
7.6	Iteration: Describe how the design and verification requirements (from Steps 4 and 5) were modified, if at all, as a result of the Step 7 activities			
7.7	Describe the realisation (assembly, installation, commissioning and verification) of any EM/physical mitigation or other measures that are not incorporated within the EFS itself			
	i) As for the Step 7.3 checklist item			
	ii) As for the Step 7.4 checklist item			
	iii) As for the Step 7.5 checklist item			
	iv) As for the Step 7.6 checklist item			
–	Any other measures or techniques that were used to help meet the EMC safety requirements over the lifecycle			
7.8	List the documents that were created during Step 7			

13.8 Checklist for Step 8: Validating the EFS

Text ref.	Action			Comments
8.2	Describe the authorities and responsibilities of the people carrying out the validation, and show how these are appropriate to the EFS specifications for risk or risk-reduction.			
8.3 and 8.4	Describe any remedial work that was necessary to comply with the Step 5 validation requirements, and how it affected any of the earlier Steps			
8.5	Describe the validation of any EM/physical mitigation or other measures that are not incorporated within the EFS itself:			
	i) As for the Step 8.2 checklist item			
	ii) As for the Steps 8.3 and 8.4 checklist item			
–	Any other measures or techniques that were used to help meet the EMC safety requirements over the lifecycle			
8.6	List the documents that were created during Step 8			

13.9 Checklist for Step 9: Maintaining the EM and physical performance characteristics of the EFS over its lifecycle

Text ref.	Action			Comments
9.2	Describe the activities required during operation maintenance repair refurbishment etc.			
	a) Any constraints on the EM and physical environments			
	b) Any disassembly/reassembly (and, where necessary, appropriate verification/validation) techniques to preserve EM and physical performance characteristics			
	c) Any periodic testing (proof testing) of critical or lifed components			
	d) Any periodic replacement of critical or lifed components			
	e) Any verification of the absence of corrosion, plus activities to prevent or limit corrosion, or recover from the effects of corrosion			
	f) Any verification of the absence of faults, damage and/or misuse, plus activities to recover from the effects of faults, damage or misuse			
	g) Any revalidation of some or all EM and/or physical performance characteristics as described in Step 8			
	h) Anything else			
9.3	Describe the activities required when the EFS is modified or upgraded			
9.4	Describe the activities required during dismantling and disposal			
–	Any other measures or techniques that were used to help meet the EMC safety requirements over the lifecycle			
9.5	List the documents that are created during Step 9			



The 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.

Group on EMC for Functional Safety

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