



BSI Standards Publication

Medical electrical equipment

Part 4-6: Guidance and interpretation — Voluntary guidance to help achieve basic safety and essential performance with regard to the possible effects of electromagnetic disturbances

National foreword

This Published Document is the UK implementation of IEC TS 60601-4-6:2024.

The UK participation in its preparation was entrusted to Technical Committee CH/62/1, Common aspects of Electrical Equipment used in Medical Practice.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 31499 1

ICS 11.040.01; 33.100.20

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 April 2024.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

TECHNICAL SPECIFICATION



**Medical electrical equipment –
Part 4-6: Guidance and interpretation – Voluntary guidance to help achieve
basic safety and essential performance with regard to the possible effects of
electromagnetic disturbances**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 11.040.01; 33.100.20

ISBN 978-2-8322-8809-2

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	8
2 Normative references	8
3 Terms, definitions and abbreviated terms	8
3.1 Terms and definitions.....	8
3.2 Abbreviated terms.....	9
4 How to use this document.....	9
5 General	10
5.1 Mitigation of effects caused by EM DISTURBANCES	10
5.2 Implementing well-proven techniques and measures for mitigating the effects that can be caused by EM DISTURBANCES	10
5.2.1 General principles	10
5.2.2 Choosing design techniques and measures from Annex A	10
5.3 Documenting the well-proven techniques and measures used for mitigating the effects that can be caused by EM DISTURBANCES	13
5.3.1 ME EQUIPMENT or ME SYSTEM.....	13
5.3.2 Non-ME EQUIPMENT	14
Annex A (informative) Detailed guidance on the techniques and measures for mitigating the effects that can be caused by EM DISTURBANCES	15
A.1 Techniques and measures that might be helpful in project management, planning and specification.....	15
A.1.1 Techniques and measures for project management and planning	15
A.1.2 Techniques and measures for use when creating a design specification	15
A.1.3 Specifying EMC test standards to help ensure availability.....	16
A.1.4 Protecting against high impact, unusual and malicious EM DISTURBANCES	19
A.2 Techniques and measures that might be helpful in system design.....	20
A.2.1 General	20
A.2.2 Separating system parts necessary for achieving BASIC SAFETY or ESSENTIAL PERFORMANCE from system parts that are not important for BASIC SAFETY or ESSENTIAL PERFORMANCE	20
A.2.3 Recording how the design specifications are achieved through design choices	21
A.2.4 Co-design electromagnetically diverse hardware/software in redundant channels	21
A.2.5 System integration, installation, and commissioning	24
A.2.6 Fault detection and event data recording for later diagnosis	25
A.2.7 Improving mitigation of the effects that can be caused by EM DISTURBANCES in communication links	26
A.2.8 Synchronization and resynchronization techniques	28
A.2.9 Protection from persistent interference by monitoring retry counts	28
A.2.10 Independent detection of EM DISTURBANCES and/or EMI.....	29
A.2.11 Protection of systems from tampering via communication links to external systems	30
A.2.12 Robust, high-specification electromagnetic mitigation	31
A.2.13 Techniques and measures to prevent RISKS being increased by virtualization of memory and PROCESS resources (e.g. a "digital twin")	31
A.2.14 Usability Engineering (Human Factors).....	32
A.3 Techniques and measures that might be helpful in operational design	32

A.3.1	General	32
A.3.2	Developing appropriate operation and maintenance instructions	33
A.3.3	Designing appropriate maintenance techniques	33
A.3.4	Limiting the possibilities for operation and hence mis-operation	34
A.3.5	Protecting against operation errors	34
A.3.6	Protecting against hardware or software modifications or manipulations	35
A.3.7	Defensive programming techniques	35
A.3.8	Limited use of interrupts	38
A.3.9	Limited use of memory address pointer variables	39
A.3.10	Avoiding recursion	39
A.3.11	Error detection and correction for invariable memory	40
A.3.12	Error detection and correction techniques in redundant designs	41
A.3.13	Time-based error detection/correction in buses and interfaces	42
A.3.14	Error detection and correction for variable memory	43
A.3.15	Error detecting/correcting coding for ROM, RAM, buses, and interfaces	45
A.3.16	Error detection and correction for logic and data processing	45
A.3.17	Error detection and correction for electrical and electromechanical components	47
A.3.18	Caution when using hardware or software libraries	48
A.3.19	Error detection and correction for electronic components	48
A.3.20	Error detection/correction by monitoring program sequence (i.e. watchdogs)	51
A.3.21	Error detection and correction using multi-channel input/output interfaces	53
A.3.22	Using test patterns: static and dynamic	53
A.3.23	Using fiber-optic cables for signals and data communications	54
A.3.24	Techniques and measures for AC and DC power supplies/power converters	54
A.3.25	Monitoring of ventilation, cooling, and heating	56
A.3.26	Careful use of wireless (radio) data communications	57
A.3.27	Good electromagnetic engineering at every level of design	58
A.3.28	Design to comply with EMC test specifications as set out in A.1.3 and A.1.4	58
A.3.29	De-rating of hardware components, where appropriate	59
A.3.30	Improve robustness of interrupts	59
A.4	Techniques and measures that might be helpful in implementation, integration, installation, and commissioning	60
A.4.1	Providing information on constraints and additional measures	60
A.4.2	Procuring materials, components, and products	61
A.4.3	Assemble/integrate according to the design for adequate mitigation of the effects that can be caused by EM DISTURBANCES	62
A.4.4	Install/commission according to the design for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES	62
A.5	Techniques and measures that might be helpful in VERIFICATION and validation (including testing)	62
A.5.1	Applying VERIFICATION and/or validation techniques and measures	62
A.5.2	VERIFICATION testing to the EMC test plan from A.1.3 and A.1.4	64
A.5.3	Using non-standardized ad hoc checks or tests	65
A.5.4	Verifying correct installation and commissioning	66
A.5.5	EMC tests before and after accelerated life tests	67

A.6	Techniques and measures that might be helpful in operation, maintenance, repair, overhaul, refurbishment, and upgrade	67
A.6.1	Assessment of changes in the ELECTROMAGNETIC ENVIRONMENT	67
A.6.2	Assessment of continuing correct installation	68
A.6.3	Maintaining adequate mitigation of the effects that can be caused by EM DISTURBANCES, despite modifications or changes	69
A.6.4	Batch (lot) traceability	70
A.6.5	Component changes, new supplier, dual / alternate source	70
A.7	Techniques and measures that might be helpful in decommissioning	71
A.8	Integrating third-party items into ME EQUIPMENT or ME SYSTEMS	71
A.8.1	The general iterative approach	71
A.8.2	Suppliers' certifications and electromagnetic assessments	73
A.8.3	Custom-manufactured component parts	73
Annex B (informative) Checklist of techniques and measures recommended for helping to achieve adequate mitigation of the effects that can be caused by EM DISTURBANCES		75
Bibliography		89
Index of defined terms		126
Figure 1 – General principles for achieving mitigation of effects that can be caused by EM DISTURBANCES		13
Figure A.1 – Choosing standard volume-manufactured subsystems and component parts		73
Table B.1 – Checklist of techniques and measures recommended for adequate mitigation of the effects that can be caused by EM DISTURBANCES throughout the EXPECTED SERVICE LIFE		76

INTERNATIONAL ELECTROTECHNICAL COMMISSION

MEDICAL ELECTRICAL EQUIPMENT –

Part 4-6: Guidance and interpretation – Voluntary guidance to help achieve basic safety and essential performance with regard to the possible effects of electromagnetic disturbances

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://patents.iec.ch>. IEC shall not be held responsible for identifying any or all such patent rights.

IEC TS 60601-4-6 has been prepared by subcommittee 62A: Common aspects of medical equipment, software, and systems, of IEC technical committee 62: Medical equipment, software, and systems. It is a Technical Specification.

The text of this Technical Specification is based on the following documents:

Draft	Report on voting
62A/1538/DTS	62A/1589/RVDTS

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this Technical Specification is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

In this document, the following print types are used:

- recommendations and definitions: roman type.
- *test instructions: italic type.*
- informative material appearing outside of tables, such as notes, examples and references: in smaller type. Normative text of tables is also in a smaller type.
- TERMS DEFINED IN CLAUSE 3 OF THIS TECHNICAL SPECIFICATION OR AS NOTED: SMALL CAPITALS.

In referring to the structure of this document, the term

- "clause" means one of the numbered divisions within the table of contents, inclusive of all subdivisions (e.g. Clause 1 includes 1.1, 1.2, etc.);
- "subclause" means a numbered subdivision of a clause (e.g. 1.1, 1.2 and 1.3.1 are all subclauses of Clause 1).

References to clauses within this document are preceded by the term "Clause" followed by the clause number. References to subclauses within this document are by number only.

In this document, the conjunctive "or" is used as an "inclusive or" so a statement is true if any combination of the conditions is true.

The verbal forms used in this document conform to usage described in Clause 7 of the ISO/IEC Directives, Part 2. For the purposes of this document, the auxiliary verb:

- "shall" means that compliance with a requirement or a test is mandatory for compliance with this document;
- "should" means that compliance with a requirement or a test is recommended but is not mandatory for compliance with this document.

A list of all parts of the IEC 60601 series, published under the general title *Medical electrical equipment*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

In 2017 it was decided to remove Annex F of IEC 60601-1-2:2014 [1]¹ into a separate document and provide guidance to help achieve basic safety and essential performance with regard to the possible effects of ELECTROMAGNETIC DISTURBANCE by a technical specification under the IEC 60601 series of standards.

This IEC document provides voluntary guidance on the assessment and application of techniques and measures that can help reduce the risks associated with the interfering effects of ELECTROMAGNETIC DISTURBANCES on medical equipment and medical systems.

¹ Numbers in square brackets refer to the Bibliography.

MEDICAL ELECTRICAL EQUIPMENT –

Part 4-6: Guidance and interpretation – Voluntary guidance to help achieve basic safety and essential performance with regard to the possible effects of electromagnetic disturbances

1 Scope

This document provides practical methods to help achieve BASIC SAFETY and ESSENTIAL PERFORMANCE with regard to the possible effects of EM DISTURBANCES throughout the EXPECTED SERVICE LIFE of ME EQUIPMENT or an ME SYSTEM.

These practical methods attempt to address all of the different types of errors, malfunctions or failures that can be caused by EM DISTURBANCES in ME EQUIPMENT or ME SYSTEMS.

The purpose of this document is to provide recommendations for the techniques and measures used in the design, VERIFICATION, and validation of systems, hardware, software, and firmware used in ME EQUIPMENT or ME SYSTEMS to help achieve BASIC SAFETY and ESSENTIAL PERFORMANCE with regard to the EM DISTURBANCES that could occur throughout the EXPECTED SERVICE LIFE.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60601-1, *Medical electrical equipment – Part 1: General requirements for basic safety and essential performance*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60601-1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- IEC Electropedia: available at <https://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>

3.1.1

COMPETENCE

training, technical knowledge, experience, and qualifications relevant to the specific duties to be performed

3.2 Abbreviated terms

AC	alternating current
ANSI	American National Standards Institute
CE	Conformité Européen (European Conformity)
CISPR	Comité Internationale Speciale des Perturbations Radioélectriques (International Special Committee on Radio Interference)
DC	direct current
EDR	event data recorder
EMI	electromagnetic interference
EMP	electromagnetic pulse
ESD	ELECTROSTATIC DISCHARGE
HEMP	high-altitude electromagnetic pulse
I/O	input/output
IEC	International Electrotechnical Commission
IEMI	intentional electromagnetic interference
ISM	industrial, scientific, and medical
ISO	International Organization for Standardization
JTAG	Joint Test Action Group
NEMP	nuclear electromagnetic pulse
PCB	printed circuit board
PDS	pre-defined state
RF	radio frequency

4 How to use this document

This document makes it possible to create a structured justification to demonstrate adequate mitigation of the effects that can be caused by EM DISTURBANCES for each of the BASIC SAFETY or ESSENTIAL PERFORMANCE issues associated with ME EQUIPMENT or an ME SYSTEM.

Clause 4 describes the use of this document in detail. It is recommended to create a structured justification for each of the BASIC SAFETY or ESSENTIAL PERFORMANCE issues, by completing the cells in the right-hand-most column of the example checklist in Table B.1, plus providing all the documents referenced in those cells.

In general, it is expected that most ME EQUIPMENT or ME SYSTEMS could have several BASIC SAFETY or ESSENTIAL PERFORMANCE issues, each one of which is recommended to be associated with its own, completed, Table B.1 checklist.

In some circumstances two or more different issues for BASIC SAFETY or ESSENTIAL PERFORMANCE might be able to be addressed by a single Table B.1 checklist.

Note that IEC 60601-1, along with ISO 14971 and ISO TR 24971, provides a well-proven PROCESS for assessing RISKS and by how much they need reduction to be acceptable RISKS, and prescribes well-proven techniques and measures for reducing each of those RISKS.

This document relies on a HAZARD analysis and RISK ASSESSMENT PROCESS as specified in IEC 60601-1 and ISO 14971 having been completed. This document assumes the correct application of the requirements of IEC 60601-1-2:2014 and IEC 60601-1-2:2014/AMD1:2020, and of the requirements in any relevant "particular" standards in the ISO/IEC 60601-2-XX and IEC 80601-2-XX series. This document provides a list of possible techniques and measures that can be used to mitigate the effects that can be caused by EM DISTURBANCES.

5 General

5.1 Mitigation of effects caused by EM DISTURBANCES

There are many well-proven techniques and measures for mitigating the effects that can be caused by EM DISTURBANCES, including in:

- a) project management, planning and specification;
- b) system design (both hardware and software);
- c) operational design (both hardware and software);
- d) implementation, integration, installation and commissioning;
- e) VERIFICATION and validation of both hardware and software;
- f) operation, maintenance, repair, refurbishment and upgrade, and
- g) decommissioning.

5.2 Implementing well-proven techniques and measures for mitigating the effects that can be caused by EM DISTURBANCES

5.2.1 General principles

Appropriate techniques and measures for mitigating the effects that can be caused by EM DISTURBANCES are recommended to be identified and applied as necessary throughout the EXPECTED SERVICE LIFE.

The aim of this subclause is to give an informative overview of a range of techniques and measures available for mitigating the effects that can be caused by EM DISTURBANCES. For more detailed information on these techniques and measures, see Annex A.

Figure 1 shows the general principles of this approach.

It will often be the case that some of the techniques and measures listed in Annex A will have already been used by the MANUFACTURER in a given type of ME EQUIPMENT or ME SYSTEM to control RISKS caused by errors, malfunctions and failures that are not directly associated with EM DISTURBANCES. In this case, it is recommended to modify these techniques and measures to help achieve adequate mitigation of the effects that can be caused by EM DISTURBANCES, as described in their entries in Annex A.

However, even where this is done, it is recommended that as appropriate, additional techniques and measures specified in Annex A are used to achieve sufficient mitigation of the effects that can be caused by EM DISTURBANCES, to help achieve the MANUFACTURER's aims for the BASIC SAFETY and ESSENTIAL PERFORMANCE of the ME EQUIPMENT or ME SYSTEM throughout the EXPECTED SERVICE LIFE.

This is especially so because it is in the nature of EM DISTURBANCES to create a wide range of possible errors, malfunctions, or failures in several locations all at once or in some critical time sequence (see A.1.2).

5.2.2 Choosing design techniques and measures from Annex A

It is recommended to follow the techniques and measures with the following considerations:

- a) It has been generally found to be impractical to perform anything more than a general assessment of the EM DISTURBANCES that could possibly occur throughout the EXPECTED SERVICE LIFE. A MANUFACTURER's specification for the maximum ELECTROMAGNETIC ENVIRONMENT of their equipment is generally composed of assessments of EM DISTURBANCES and levels.

- b) These assessments are good enough for determining which of the many published EMC EMISSIONS and IMMUNITY standards to apply for the achievement of functionality with adequate uptime, but cannot determine what EM DISTURBANCES, and combinations of them, could foreseeably occur during the EXPECTED SERVICE LIFE.
- c) It is necessary to maintain adequate mitigation of the effects that can be caused by EM DISTURBANCES in the operational environment despite all foreseeable faults, misuse, ageing, component tolerances, assembly errors, physical and climatic conditions, etc., that could occur throughout the EXPECTED SERVICE LIFE.

It is recommended that the MANUFACTURER selects an adequate combination of techniques and measures that, together, help achieve adequate mitigation of the effects that can be caused by EM DISTURBANCES. It is recommended that their selection is documented with the reasons for the selections made and for rejecting those that are not used. These decisions are usually documented in the RISK MANAGEMENT FILE.

Table B.1 provides a basic checklist that can be applied for this purpose. It identifies a number of techniques and measures that can be used at appropriate stages of the EXPECTED SERVICE LIFE. However, Table B.1 is not necessarily exhaustive and it is applicable to use additional techniques and measures to give adequate assurance that the effects that can be caused by EM DISTURBANCES will not cause failure to achieve BASIC SAFETY and ESSENTIAL PERFORMANCE of the ME EQUIPMENT or ME SYSTEM throughout the EXPECTED SERVICE LIFE.

No techniques and measures with regard to EM DISTURBANCES, such as those described in this document, can be assumed to guarantee complete protection against every possible type of EM DISTURBANCE, combination of EM DISTURBANCES, fault or misuse that could result in EMI.

The exact combination of techniques and measures that a MANUFACTURER might select for a particular ME EQUIPMENT or ME SYSTEM depends on many factors specific to the medical application in question. Except where stated otherwise, the techniques and measures specified in Annex A are appropriate for both "continuous" and "on-demand" functions.

Depending on the nature of the project, different techniques and measures might be used in its various stages, for example:

- a) if a project does not involve any software design, then no software design techniques and measures would be selected for any of the project's stages; likewise,
- b) if there is no circuit design, then circuit design techniques and measures would not be needed.
- c) If ME EQUIPMENT or an ME SYSTEM does not need to maintain its functionality or be safe after a nuclear explosion that created EMP (such as HEMP or NEMP), then the techniques and measures described in this document that are intended to provide protection against EMP, HEMP or NEMP, need not be applied.

Knowledge of the extent to which robust conventional ELECTROMAGNETIC COMPATIBILITY (EMC) management techniques (such as high-specification electromagnetic mitigation including shielding, filtering, and transient suppression) are able to prevent EM DISTURBANCES from affecting the BASIC SAFETY and ESSENTIAL PERFORMANCE during the EXPECTED SERVICE LIFE can be used during the selection and application of the techniques and measures, where this is justified.

Each technique or measure described in this document is described in more detail in Annex A, based on its relevance to the stage of the project, under the headings: Aim; Description; Identification; Mitigation, and Effectiveness.

Aim	The overall purpose of the technique or measure.
Description	Broadly how the technique or measure achieves its aim.
Identification	The effectiveness of the technique or measure in revealing the presence of an error or malfunction that could be caused by EM DISTURBANCES
Mitigation	The behaviour of the system function in response to the detected errors or malfunctions that could have been caused by EM DISTURBANCES.

"Effectiveness" specifies the value of each technique or measure for mitigating the effects that can be caused by EM DISTURBANCES, using the attributes:

- Not Effective (NE);
- Effective (E);
- Highly Effective (HE).

In this document, the "effectiveness" of a technique or measure listed in Table B.1 as NE, E, or HE (see above) is graded by the RISK level resulting from the application of the PROCESS described in Annex C of ISO TR 24971:2020 [3] by the MANUFACTURER of the ME EQUIPMENT or ME SYSTEM.

Three RISK levels are used in this document, taken from C.4 of ISO TR 24971:2020 [3]:

- 1 = Insignificant or negligible risk
- 2 = Investigate further RISK reduction
- 3 = Unacceptable risk

It is recommended that if a technique or measure rated as HE for the relevant ME EQUIPMENT or ME SYSTEM is not used, a detailed technical explanation of why it was not used is documented. For example, the technique or measure might not actually be relevant for the design being implemented, or it might be that an alternative technique or measure is used instead that provides the same benefits regarding mitigation of the effects of EM DISTURBANCES for the design issue concerned.

Where a technique or measure applies to a technology that is not relevant to the ME EQUIPMENT or ME SYSTEM concerned, and the effectiveness is shown in Table B.1 as being HE, it is recommended that a justification for why that technique or measure was not applied is documented.

The "effectiveness" levels (E, HE) listed in Table B.1 are generic starting points, and it is recommended that the MANUFACTURER makes an informed application consistent with expectations of the medical application.

It is important to understand that ME EQUIPMENT and ME SYSTEMS cannot be said to achieve BASIC SAFETY and ESSENTIAL PERFORMANCE with regard to EM DISTURBANCES simply on the basis of the system parts from which they are composed.

Other techniques and measures not listed in Table B.1 might also be able to assist in demonstrating that the effects that can be caused by EM DISTURBANCES, have been sufficiently mitigated to achieve BASIC SAFETY and ESSENTIAL PERFORMANCE throughout the EXPECTED SERVICE LIFE, and space has been allowed in that table for them to be written in.

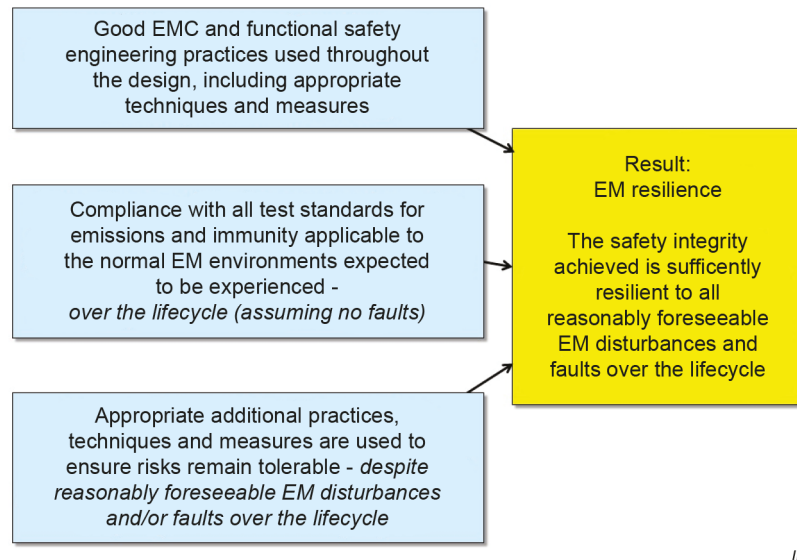


Figure 1 – General principles for achieving mitigation of effects that can be caused by EM DISTURBANCES

Table B.1 summarizes the techniques and measures recommended for helping to achieve sufficient mitigation of the effects that can be caused by EM DISTURBANCES throughout the EXPECTED SERVICE LIFE. It also provides a useful checklist that is recommended for use in demonstrating the application of the guidance in this document.

See Annex A for detailed information on the techniques and measures summarized in Table B.1.

5.3 Documenting the well-proven techniques and measures used for mitigating the effects that can be caused by EM DISTURBANCES

5.3.1 ME EQUIPMENT or ME SYSTEM

It is recommended that the safety documentation of ME EQUIPMENT or an ME SYSTEM includes all of the evidence that helps ensure that it maintains BASIC SAFETY and ESSENTIAL PERFORMANCE over the EXPECTED SERVICE LIFE.

Prior to the ME EQUIPMENT or ME SYSTEM being put into use, it is recommended that a structured justification is included in the safety documentation demonstrating that reasonable assurance of BASIC SAFETY and ESSENTIAL PERFORMANCE with regard to EM DISTURBANCES has been achieved. This justification could be assessed as part of RISK ASSESSMENT activities; alternatively, other appropriate structured assessment approaches could be used.

This structured justification could help to assess the extent of compliance with the applicable safety standards and the adequacy of the range of activities, techniques and measures that have been used to achieve BASIC SAFETY and ESSENTIAL PERFORMANCE about EM DISTURBANCES, including VERIFICATION and validation activities.

It is recommended that supporting information is made available for this justification. This usually includes ELECTROMAGNETIC ENVIRONMENT specifications, EMC test results and certifications, and material demonstrating the range and suitability of the techniques and measures used to help assure BASIC SAFETY and ESSENTIAL PERFORMANCE with regard to EM DISTURBANCES.

It is also recommended that information used to support claims made as to the BASIC SAFETY and ESSENTIAL PERFORMANCE with regard to EM DISTURBANCES of ME EQUIPMENT or an ME SYSTEM is made available to system integrators and end users and retained in order to support system review activities throughout the EXPECTED SERVICE LIFE of the ME EQUIPMENT or ME SYSTEM.

Independent assessment of the justification that BASIC SAFETY and ESSENTIAL PERFORMANCE have been achieved with regard to EM DISTURBANCES can be undertaken where considered appropriate.

It is recommended to demonstrate that the guidance in this document has been followed by adding text and hyperlinked references to relevant design, VERIFICATION, or validation documents, into the cells in the right-hand-most columns of the example checklist of Table B.1.

As discussed in 5.2.2, if a technique or measure in the checklist in Table B.1 is categorized as HE for the ESSENTIAL PERFORMANCE in question but has not been applied, then it is recommended that the right-hand-most column in Table B.1 states (or provides a link to a document that states) the reasons why not, and what was done instead.

5.3.2 Non-ME EQUIPMENT

In the case of a non-ME EQUIPMENT used in an ME SYSTEM, it is recommended that information is obtained or developed to determine the potential impact on the BASIC SAFETY and ESSENTIAL PERFORMANCE of the ME SYSTEM, and this information made available to system integrators and end users.

It is recommended that such information includes the environmental specifications with which the non-ME EQUIPMENT complies, the techniques and measures that have been applied in the design of the non-ME EQUIPMENT to mitigate the effects that can be caused by EM DISTURBANCES, and guidance on installation and maintenance.

It is also recommended that such information also includes details of the non-ME EQUIPMENT'S behavior, where appropriate, in the case of degradation; for example, "pre-defined operational states" (PDSs) that the equipment can assume in response to errors or failures due to intolerable EM DISTURBANCES, as well as guidance on the application of the non-ME EQUIPMENT.

It is recommended that information used to support a non-ME EQUIPMENT claims with regard to EM DISTURBANCES is made available to system integrators and end users, and the MANUFACTURER recommends that they retain it in order to support review activities throughout the EXPECTED SERVICE LIFE of the ME SYSTEM. Such information might use one or more copies of the checklist in Annex B, broadly as discussed in 5.3.1, to help to provide a structured justification demonstrating that reasonable assurance of BASIC SAFETY and ESSENTIAL PERFORMANCE have been achieved with regard to EM DISTURBANCES.

Annex A (informative)

Detailed guidance on the techniques and measures for mitigating the effects that can be caused by EM DISTURBANCES

A.1 Techniques and measures that might be helpful in project management, planning and specification

A.1.1 Techniques and measures for project management and planning

Aim: To help avoid failures in the management, planning, selection, design, implementation, commissioning, VERIFICATION, and maintenance of measures for avoiding and controlling dangerous failures due to EM DISTURBANCES and EMI.

This applies to an ME SYSTEM, ME EQUIPMENT, and to the components thereof.

Description: It is recommended that the PROCESSES for the management, planning, selection, design, implementation, commissioning, modification, VERIFICATION, and maintenance of each function explicitly include measures for mitigating the effects that can be caused by EM DISTURBANCES and be documented.

It is recommended that a competent person has overall responsibility for managing the mitigation of the effects that can be caused by EM DISTURBANCES on the ME EQUIPMENT or ME SYSTEM. It is also recommended that appropriate COMPETENCE is made available throughout the EXPECTED SERVICE LIFE.

Identification: By assessment of the design for conformance with this document.

Mitigation: By using the techniques and measures such as, for example, those described in this document (or equivalent techniques and measures as documented).

A.1.2 Techniques and measures for use when creating a design specification

Aim: To help ensure that the design specification includes all reasonably foreseeable EM DISTURBANCES and their EMI effects are taken into account in the specification of the system and its subsystems and component parts.

Description: Specify and use appropriate techniques and measures to help ensure that the ME EQUIPMENT or ME SYSTEM will achieve BASIC SAFETY and ESSENTIAL PERFORMANCE despite any EM DISTURBANCES throughout the EXPECTED SERVICE LIFE.

Amongst other issues, take the following into account:

- a) non-operation when operation is required;
- b) operation when no operation is required; and
- c) unintended or inaccurate operations.

It is recommended that the specifications for techniques and measures for MITIGATING the effects that can be caused by EM DISTURBANCES are complete, free from errors and contradictions, and easy to verify.

It is recommended that the design specifications with regard to EM DISTURBANCES and their EMI effects are specified using a variety of semi-formal and formal modelling techniques, for example those listed in the bibliography under "VERIFICATION/validation and other techniques (not specifically related to EM DISTURBANCES), a preliminary HAZARDS analysis as a semi-quantitative technique to be used in the initial design PROCESS, and Taguchi's "Design of Experiments" (see [771]).

Whichever techniques are chosen, take into account the potential effects of EM DISTURBANCES on the hardware and software. Typically, this might include consideration of the possibility of corruption of data and program memory content, corruption of data in transit on internal or external serial or parallel buses and their consequent effects on the safe operation of the ME SYSTEM.

Put more simply: EM DISTURBANCES (including intentional EMI (IEMI)) can contribute to the probability of a HAZARD occurring and its effects either eliminated, mitigated, or accommodated using appropriate techniques and measures such as, for example, those described in this document.

It is recommended that this activity takes fully into account the fact that EM DISTURBANCES and EMI can cause an effectively infinite variety of:

- a) any of noisy, degraded, distorted, false, delayed, re-prioritized, overvoltage, etc. controls/signals/data, both intermittently and continuously;
- b) any of under/over voltages, noises, dropouts, and interruptions, lasting from less than one microsecond to many seconds, minutes, even permanent, in one or any number of AC or DC power supplies, both intermittently and continuously;
- c) any of waveform distortions, frequency perturbations in any number of AC power supplies, plus phase and voltage imbalances in multi-phase supplies;
- d) one or more combinations of any of the above, occurring in any number of signal paths or power supplies, simultaneously or in any critical time relationship.

It is recommended that the design specification states the selection of techniques and measures to be used for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES to the ME EQUIPMENT or ME SYSTEM or its subsystems or component parts to help achieve BASIC SAFETY and ESSENTIAL PERFORMANCE in its expected operational environments over its EXPECTED SERVICE LIFE.

References: See the list in the bibliography under "VERIFICATION/validation and other techniques (not specifically related to EM DISTURBANCES)".

A.1.3 Specifying EMC test standards to help ensure availability

Aim: To help ensure adequate availability of the ME EQUIPMENT or ME SYSTEM and all of its systems that help achieve BASIC SAFETY or ESSENTIAL PERFORMANCE throughout the EXPECTED SERVICE LIFE, so that BASIC SAFETY and ESSENTIAL PERFORMANCE are maintained taking into account availability, throughput rate, production rate, and other financial and mission-critical needs.

Description:

- a) To help ensure that both intentional and unintentional ELECTROMAGNETIC EMISSIONS, throughout the expected service life, do not exceed levels that are likely to affect other equipment.
- b) To help ensure that the reasonably foreseeable normal operational ELECTROMAGNETIC ENVIRONMENT does not cause sufficient EMI to activate any safe failure modes, ensuring adequate availability of the ME EQUIPMENT or ME SYSTEM throughout the expected service life.

EMISSIONS and IMMUNITY tests are selected from the IEC (including CISPR) series of EMC EMISSIONS and IMMUNITY test methods considered appropriate for both the intended application and the expected ELECTROMAGNETIC ENVIRONMENT(S) throughout the EXPECTED SERVICE LIFE (see the bibliography under “IEC, ISO, IEEE, and CISPR standardized EMC test methods”). It is recommended that the assessment of the expected ELECTROMAGNETIC ENVIRONMENT includes both inter-system and intra-system electromagnetic energy coupling paths.

However, other types of EMC tests can be more appropriate than IEC or CISPR, especially for automotive, rail, aerospace, military, etc., applications and environments for which specific EMC test standards have been developed (see the bibliography under “Automotive industry EMC test standards” to “ITE, telecommunications and wireless industry EMC test standards”). Where appropriate EMC test standards are unavailable, it can be applicable for the MANUFACTURER to specify their own test methods and acceptance criteria.

To correspond to the predicted ELECTROMAGNETIC ENVIRONMENT and the application, it can be applicable to modify the test standards. For example an EMISSIONS limit can be reduced over a certain frequency range because of the close proximity of certain sensitive equipment or can be extended by some gigahertz to help protect certain wireless communications.

EXAMPLE 1: ME EQUIPMENT or an ME EQUIPMENT located near an airport or harbor can be tested for radiated IMMUNITY using the IEC 61000-4-3 method modified to simulate the nearby radar levels, frequencies, modulations, pulse repetition rates, etc., in addition to the tests specified in the relevant test standard (e.g. IEC 60601-1-2).

EXAMPLE 2: Most ME EQUIPMENT and ME SYSTEMS will be exposed to close-proximity transmitting PORTABLE electronic devices (T-PEDs), radio-frequency identification (RFID) readers, and/or machine-to-machine (M2M) transmitters, and wireless-data-enabled laptops, tablets, PDAs, e-book readers and the like. Consequently, their IMMUNITY can be tested accordingly, probably requiring the application of test standards such as [224] and/or [317], in addition to the other EMC IMMUNITY tests that have been selected.

EXAMPLE 3: Proximity to high-power electrical installations can expose ME EQUIPMENT or ME SYSTEMS to large magnetic fields, high-amplitude conducted noise at frequencies from DC to at least 10 kHz, and/or high-energy radiated and conducted transients requiring appropriate testing in addition to the other EMC IMMUNITY tests that have been selected.

Also, an IMMUNITY TEST LEVEL can be increased over a certain frequency range, or extended to higher frequencies, because of the close proximity of certain "noisy" equipment (for example, radio-frequency materials processing equipment operating with high RF power in an ISM band, a radio-communications transmitter, or a SPECIAL ENVIRONMENT.).

It can also be useful to modify standard testing to help confirm that specific aspects of the equipment's performance are adequately tested, for example, by extending test frequencies to help confirm that the performance of the system clock is adequately tested. The tables of recommended tests in IEC 61000-1-2 and IEC 61000-6-7 can assist with identifying far-field IMMUNITY tests. Near-field IMMUNITY testing (for an example, see [317]) can also be appropriate for situations where PORTABLE radio transmitters (such as mobile phones, cellphones, Wi-Fi, Bluetooth, etc.) could be in very close proximity to the equipment.

IMMUNITY levels can be increased to account for test measurement uncertainty. Testing at the specified limit only provides a 50 % confidence interval that the IMMUNITY level has been applied as there is equal probability that the IMMUNITY level applied is plus or minus the specified limit. Safety standards such as IEC 60601-1-2 do not mandate a particular confidence level for electromagnetic measures, but for EMC tests a minimum 95 % confidence interval is recommended. Further guidance is in [10].

See Clause 5 and [11] to [14] for discussions of the fact that no practicable IMMUNITY testing plan can, on its own, demonstrate sufficient confidence that EM DISTURBANCES will not cause unacceptable degradation of BASIC SAFETY or ESSENTIAL PERFORMANCE throughout the EXPECTED SERVICE LIFE.

Other appropriate techniques and measures such as, for example, those described in this document, are also needed to help achieve BASIC SAFETY or ESSENTIAL PERFORMANCE with regard to EM DISTURBANCES.

Identification: Make certain to devise a test plan by persons competent in applying the selected EMC tests and carry out VERIFICATION and validation testing according to this plan, as described in A.5.

It is recommended that VERIFICATION tests (see A.5) are applied to all relevant components of ME EQUIPMENT and ME SYSTEMS, ideally by the MANUFACTURER, during the integration phase.

It is recommended that validation tests (see A.5) are applied to the complete ME EQUIPMENT or ME SYSTEM, functioning in its final configuration in its intended application and environment.

It is recommended that, where this is not practicable, the standard tests are applied at the highest practicable level of assembly of the ME EQUIPMENT or ME SYSTEM or its subsystems, and the likely limitations and consequences of the partial testing documented. In addition, it is recommended that in situ EMC testing is carried out where practicable, for example, by using the methodology described in [600].

It is recommended that the IMMUNITY tests show that the tested items, equipment, or systems are unaffected at the applied test levels (i.e. their good electromagnetic design, plus filtering, shielding, etc. offers adequate protection against the EM DISTURBANCES).

The point of complying with IMMUNITY test standards is to maintain the intended availability of the ME EQUIPMENT or ME SYSTEM. To that end, it is recommended that components and subsystems intended for incorporation into ME EQUIPMENT or an ME SYSTEM not fail during these tests – unless they fail to a PDS and this situation is adequately documented.

For the same reason, it is recommended that functions that help achieve BASIC SAFETY or ESSENTIAL PERFORMANCE are not triggered during these tests – unless this is adequately addressed in the documentation.

It is recommended that functions that help achieve BASIC SAFETY or ESSENTIAL PERFORMANCE are never inhibited from operating as a result of these tests, which can require certain techniques and measures to be used, such as – for example – some of those described in this document.

It is recommended that the results of the testing according to the plan are documented and assessed against the relevant design specification. It is also recommended that any unexpected or anomalous behaviour is investigated, the underlying causes corrected, and the work involved documented.

It is recommended that the tests are carried out in a manner that provides sufficient confidence that compliance with them will be maintained throughout the EXPECTED SERVICE LIFE.

EXAMPLE 4: Some MANUFACTURERS take equipment that complies with its specified EMC EMISSIONS and IMMUNITY test standards, artificially age it using well-established acceleration techniques, then retest the aged units to check that they still comply with those EMC test standards.

Mitigation: By competently modifying the design using good electromagnetic engineering practices (see A.3.27) until the test specifications are met in a way that indicates their maintenance throughout the EXPECTED SERVICE LIFE.

NOTE 1 Compliance with EMC regulations applicable in the country of application is generally a starting point for this specification exercise, but is almost never sufficient, because complying with the conventional EMC test standards alone is generally insufficient for achieving sufficient mitigation of the effects that can be caused by EM DISTURBANCES (see Clause 4 and [11] to [14]).

NOTE 2 Manufacturers are not necessarily precluded from doing these tests themselves or constrained to using certain types of third-party test laboratories.

The degree of accuracy, confidence, test accreditation and independence needed for these tests is – like most BASIC SAFETY or ESSENTIAL PERFORMANCE issues – generally dependent on the RISK level, and therefore determined by the MANUFACTURER.

References: The bibliography under “Assessing the ELECTROMAGNETIC ENVIRONMENT, and detecting threats” includes some references on assessing ELECTROMAGNETIC ENVIRONMENTS and some relevant standards from different industries and application areas.

A.1.4 Protecting against high impact, unusual and malicious EM DISTURBANCES

Aim: To help achieve BASIC SAFETY and ESSENTIAL PERFORMANCE where the occurrence of high impact, unusual and malicious EM DISTURBANCES could reasonably be foreseen and cause temporary disturbance and/or permanent damage to hardware (electronic components, interconnections, etc.).

Description: Examples of unusual EM DISTURBANCES include: very near proximity lightning stroke, unusual ELECTROSTATIC DISCHARGE (ESD) events and transients, such as corona due to a nearby power fault or high-voltage switching event. Examples of malicious EM DISTURBANCES include HEMP, IEMI and jamming of wireless channels (see [661] [38] [659] [660] and [662]).

Identification: By specifying appropriate environments, selecting appropriate techniques and measures for helping to achieve sufficient mitigation of the effects that can be caused by EM DISTURBANCES and performing appropriate tests, using (for example) the relevant documents and standards listed in the bibliography.

Make certain to devise a test plan by persons competent in applying the selected EMC tests and carry out VERIFICATION and validation testing according to this plan, as described in A.5.

VERIFICATION tests (see A.5) are applied to all component parts and subsystems to be incorporated in the ME EQUIPMENT or ME SYSTEM, ideally by their MANUFACTURERS, during the integration phase.

It is recommended that validation tests (see A.5) are applied to the complete ME EQUIPMENT or ME SYSTEM in its final configuration in its intended application, running a typical application program. Where this is not practicable, it is recommended that the standard tests are applied at the highest practicable level of assembly of the ME EQUIPMENT or ME SYSTEM or its subsystems and the likely limitations and consequences of the partial testing documented. Some of these tests might involve in situ testing with EM DISTURBANCES.

Mitigation: Where it is considered necessary to cope with the occurrence of one or more such high-impact EM DISTURBANCES throughout the EXPECTED SERVICE LIFE, it is recommended that appropriate mitigation be applied, for example, as described in documents listed under “Good EMC engineering for systems and installation” or “Good EMC engineering for individual items of equipment”, to pass the relevant tests.

Alternatively, appropriate techniques and measures could be applied to detect inhibition or false operation of the functions that help achieve BASIC SAFETY or ESSENTIAL PERFORMANCE and cause it to default to a redundant or backup function that provides at least a minimal level of BASIC SAFETY or ESSENTIAL PERFORMANCE. To aid fault attribution and diagnostics, it is recommended that the fault detection is correlated to independent EMI event detection and monitoring (see A.2.10).

The redundant or backup function that provides at least a minimal level of BASIC SAFETY or ESSENTIAL PERFORMANCE could be normally completely disengaged from all power and signals, so that it is more likely to survive these powerful electromagnetic events and minimize common-cause failures.

A redundant or backup function that provides at least a minimal level of BASIC SAFETY or ESSENTIAL PERFORMANCE that uses low-technology electronics (i.e. does not use programmable electronics) is more likely to survive such powerful electromagnetic events, with a non-electrical backup system likely to be the most rugged. A non-electrical backup system is one based on mechanical, hydraulic and/or pneumatic technologies alone (i.e., with no electrical or electronic control).

NOTE The military and defence sectors have their own sets of standards for these high-power EM DISTURBANCES. See the relevant references in the bibliography for examples.

A.2 Techniques and measures that might be helpful in system design

A.2.1 General

This subclause describes various techniques and measures to help achieve and maintain adequate mitigation of the effects that can be caused by EM DISTURBANCES to ME EQUIPMENT and ME SYSTEMS.

During the operation of ME EQUIPMENT or an ME SYSTEM, EM DISTURBANCES might cause hardware malfunction in the form of corruption of data in memories, and corruption of signals on data, address and control bus lines and interfaces.

This in turn can cause software, and hence the system, to malfunction, possibly preventing the achievement of BASIC SAFETY or ESSENTIAL PERFORMANCE. It is recommended that techniques and measures be applied accordingly, bearing in mind all the possible susceptibilities of the system to the variety of EM DISTURBANCES described in A.1.

Some suitable techniques and measures are described in A.3 to A.8. Alternatives can be used if technical justifications are documented.

Where a technique or measure in this subclause applies to a technology that is not relevant to the ME EQUIPMENT or ME SYSTEM concerned, and the effectiveness as shown in Table B.1 as being HE, it is recommended that a justification for why that technique or measure was not applied is documented (see 5.3).

A.2.2 Separating system parts necessary for achieving BASIC SAFETY or ESSENTIAL PERFORMANCE from system parts that are not important for BASIC SAFETY or ESSENTIAL PERFORMANCE

Aim: To separate the system parts necessary for achieving BASIC SAFETY or ESSENTIAL PERFORMANCE from system parts that are not important for BASIC SAFETY or ESSENTIAL PERFORMANCE, so that the EM DISTURBANCES created by the system parts that are not important for BASIC SAFETY or ESSENTIAL PERFORMANCE, or the consequences of EMI occurring in them, do not affect the system parts that are necessary for achieving BASIC SAFETY or ESSENTIAL PERFORMANCE.

Description: In the specification, it is recommended that it is decided whether it is possible to create a complete or partial separation of the system parts necessary for achieving BASIC SAFETY or ESSENTIAL PERFORMANCE, from the system parts that are not important for BASIC SAFETY or ESSENTIAL PERFORMANCE.

Identification: It is recommended that clear specifications are written for the interfacing between the two different types of part.

Possible remaining routes for interference that could create coupling between the system parts necessary for achieving BASIC SAFETY or ESSENTIAL PERFORMANCE and the system parts that are not important for BASIC SAFETY or ESSENTIAL PERFORMANCE can be identified and documented, such that appropriate techniques and measures can be implemented to address them, such as those described in this document.

Mitigation: By applying the above interface specifications throughout all project stages, plus VERIFYING and validating that the specifications have been correctly applied at all project stages, and at the end.

Reference: [125]

NOTE This technique concerns the physical separation of hardware and the connections made between items of hardware (i.e. their communication, power, and physical interfaces).

A.2.3 Recording how the design specifications are achieved through design choices

Aim: To produce a stable design of the ME EQUIPMENT or ME SYSTEM, and any part of it, in conformance with its design specification (see A.1).

Description: This is where the design choices, mitigation strategies, techniques and their justifications, and the measures used to comply with the design specification, are documented.

These will typically include EMI filtering, separation, segregation, grounding and shielding, sufficient at least to meet normal test standards for ELECTROMAGNETIC IMMUNITY, together with a selection of techniques and measures such as (for example) those described in this document according to their effectiveness for the RISK level as determined by the MANUFACTURER. See also A.3.27.

Identification: The checklists in Annex A provide a non-exhaustive selection of techniques and measures that are likely to be applicable during the design PROCESS and for the practical implementation. Additional techniques can be used if they are documented.

Mitigation: It is recommended that a list of all the applicable techniques and measures is documented, and that this also records the justifications for not implementing any rated HE (see 5.3). It is recommended that the documentation shows that the parts of the design specification that relate to the RISK levels have been fulfilled.

NOTE 1 It is generally impractical to demonstrate/verify/validate that a set of electromagnetic mitigation techniques and measures alone is sufficient for any particular RISK levels.

NOTE 2 The RISK level can be used to determine the degree of COMPETENCE, amount of detail, amount of work, and amount of documentation involved.

A.2.4 Co-design electromagnetically diverse hardware/software in redundant channels

Aim: To detect and/or correct systematic failures using multiple electromagnetically diverse hardware channels and/or software components, to reduce the likelihood that the common-cause characteristics of EM DISTURBANCES will cause an incorrect output to be created.

Description: Electromagnetically diverse hardware and software designs have different modes and rates of failure due to EM DISTURBANCES.

Hardware and software diversity are often described as being different types of techniques and measures. However, these days some traditional hardware diversity techniques and measures might be more effectively accomplished in software, and some traditional software diversity techniques and measures might now be more effectively accomplished in hardware (for example, by using field-programmable gate arrays (FPGAs)) – so co-design is preferred.

It is recommended that hardware and software designers work together (i.e. co-design) to achieve the desired overall diversity in the most effective way in order to meet the design specification and RISK levels.

Identification / Mitigation for diverse hardware:

Where ME EQUIPMENT or an ME SYSTEM uses redundant hardware "channels" with comparison or voting on their outputs to detect and/or correct errors or faults, it is recommended that these channels be electromagnetically diverse.

This helps reduce the probability of systematic common cause errors or failures when the ME EQUIPMENT or ME SYSTEM experiences EM DISTURBANCES and helps to increase the probability of detecting such errors and failures, surviving them, and maintaining availability.

Methods for achieving electromagnetically diverse hardware channels include (but are not limited to):

- a) Different physical principles, such as sensing different but related physical parameters, for example, the temperature and pressure of a sealed vessel; using resistances and thermocouple voltages to measure temperature; etc.
- b) Different digital architectures, such as using processors and FPGAs with different internal structures.
- c) Algorithms that use different techniques to solve the same problem or calculate the same results.
- d) Different methods of physical realization, such as using shielded cables, wireless or fiber-optics for communications.
- e) Spatial separation, so that an EM DISTURBANCE or ionizing radiation track is likely to only affect one of the redundant channels.
- f) Locating each item of equipment in a different ELECTROMAGNETIC ENVIRONMENT.
- g) Routing cables such that each cable runs through a different ELECTROMAGNETIC ENVIRONMENT.
- h) Different circuit design principles, such as operating on a signal, the value of which is represented as either a voltage; current; frequency; mark-space ratio; digital code, etc.
- i) Functional diversity, i.e. the use of different approaches to achieve the same result, such as analogue, digital, or optical electronic technologies.
- j) Mechanical, hydraulic, and pneumatic technologies have the advantage of being immune to all EM DISTURBANCES and can be used to great benefit in some situations.
- k) Inversion of data or signals.
- l) Where different channels are synchronized to the same clock, operating them out of step with each other. Ideally, operating redundant channels non-synchronously.
- m) Where different communication channels, sensors, etc., use specific narrowband frequencies, ensure that each of them uses frequencies that are not harmonically related to the others. Examples include linear variable displacement transducers (LVDTs), strain gauges and other bridge measurements run on AC, Doppler sensors for velocity, metal detectors, solid-state gyroscopes, and any sensor, transducer or other type of circuit that uses phase-sensitive detection, phase-locked loops, or very narrow band-pass filters.
- n) Provide different channels with power from different, independent sources.

An example of using diversity in a multi-channel control system (many other ways are possible):

Two redundant, identical electronic sensors are mounted on the same printed circuit board, or in the same integrated circuit, and sense the same physical parameter (for example, the position, velocity, temperature, gas concentration, etc.). A comparator checks whether their outputs agree and switches the ME EQUIPMENT or ME SYSTEM into a safe state when they do not.

Because the sensors are so close together, they share the same ELECTROMAGNETIC ENVIRONMENT, which means that they experience the same EM DISTURBANCES at the same time.

A common effect of EM DISTURBANCES on electronic sensors is to cause a positive or negative "zero shift"; when this occurs, both of these sensors will give false high or low measurements at the same time.

If large enough, EM DISTURBANCES can cause zero-shifts in many types of sensors of as much as full scale deflection (FSD), but the comparator will be unable to detect any false high or low measurements, even up to $\pm$ FSD, because both sensors have the same (false) output at the same time. The ME EQUIPMENT or ME SYSTEM would not be switched into a safe state, even if the errors in the sensor signals resulted in unsafe operation (if, for example, the position were too far or not far enough; the velocity, temperature, or gas concentration were too high or too low; etc.).

However, introducing electromagnetic diversity by connecting one of the sensors so that it produces signals that are inverted with regard to the other, and restoring the correct polarity at its input to the comparator, makes it highly probable that the sensors' zero-shifts, due to EM DISTURBANCES, would in fact be detected by the comparator.

Identification / Mitigation for diverse software:

The first option for electromagnetic diversity of software is to use two or more independent software components to implement the same function, where each component is designed and coded separately and uses different partitions of memory for its data (and might use different algorithms where this is feasible). To avoid common conceptional errors it is reasonable to have the diverse software developed by different people.

Differences in the outputs of these components are detected by the software itself or by means of comparison or voting logic as for hardware redundancy.

The rationale for the use of electromagnetically diverse software components is that a memory corruption or incorrect instruction execution caused by EM DISTURBANCES might not affect both (all) of the diverse software components. If it does, then the effects of the EMI will, in general, be different, allowing the comparison or voting logic to detect the error.

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

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

An electromagnetically diverse monitor is usually simpler than achieving electromagnetically diverse main software. If not, it is equivalent to a redundant implementation.

It might be helpful to implement the electromagnetically diverse monitor on a separate computer to reduce the likelihood of the main software and the diverse software monitor being affected in the same way by the same EM DISTURBANCE.

If a separate computer is not used then it is applicable for the electromagnetically diverse monitor to be capable of operating (and, in particular, capable of recovering from EMI-induced errors) independently of the main software, for example, in a different PROCESS or task using separate memory areas.

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

Extending the method to three or more channels needs a voting function that is sufficiently reliable and adequately resistant to EM DISTURBANCES for the specified RISK level. This voter can have a reliability (despite EMI) that corresponds to the improvement in confidence that is the purpose of using the multiple channels. Various techniques can be used to do this, for example, dynamic self-testing as described in A.3.22.

Where such voting is used it can be assumed, given sufficient confidence in the electromagnetically diverse behaviour of the channels, that channels that meet the specifications for the voting function are operating correctly. Whilst the voting result is positive the system can maintain BASIC SAFETY and ESSENTIAL PERFORMANCE without any need to fail to a safe state.

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

NOTE 1 Bear in mind that functionally equivalent items of hardware from the same or alternative suppliers might not behave sufficiently differently when subjected to the same EM DISTURBANCE. In this case their internal hardware and/or software design are not sufficiently electromagnetically diverse.

NOTE 2 It can be possible to suspend operation for a period of time until the channels agree once more, without degrading ESSENTIAL PERFORMANCE. This helps to maintain availability by reducing the number of times the system fails to a safe state as the result of temporary or transient EMI, and so reduces the possibility that users will modify the system and unintentionally compromise BASIC SAFETY or ESSENTIAL PERFORMANCE (an example of foreseeable misuse).

NOTE 3 EM DISTURBANCES can cause software instructions or data to change, due to corruption of instruction address and/or data bus.

References: Methods of partitioning software on the same computer: [113] to [115] and [122] to [125]. Common cause failures: [746]

A.2.5 System integration, installation, and commissioning

Aim: To help ensure that sufficient mitigation of the effects that can be caused by EM DISTURBANCES is correctly considered when parts of the system that have been separately tested are brought together to form the complete functional system.

Description: Most systems are constructed from a variety of functional modules and multiple commercially sourced products.

Each part can be designed and verified as being suitably resistant to EM DISTURBANCES (see A.8), however, further attention is needed when the individual parts of the system are housed and connected, including the shared power supplies and system interconnections that can create additional opportunities for EMI to occur or its effects to be propagated within the system.

Typical system-level EMI issues might occur through, for example, the inappropriate selection of cable types; cable segregation issues (such as crosstalk); unsuitable earthing/grounding structures; common cause failures due to EMI, etc.

It is recommended that the approach taken to avoid an increase in system-wide EM DISTURBANCE vulnerability due to system integration (physical, electrical, and functional) is documented.

Identification: By independent assessment of the design and realization of the integration against relevant good electromagnetic engineering practices for systems and installations (see A.3.27).

The use of event data recorders (e.g. non-volatile memory that stores events) within the system might help to pinpoint the likely causes of malfunction, (see A.2.6), and data communication error counts might provide an indication of EM DISTURBANCES influencing communications networks or systems.

Mitigation: By modification of the relevant design to the satisfaction of the appointed independent assessors.

A.2.6 Fault detection and event data recording for later diagnosis

Aim: To increase the probability of localizing malfunctions caused by EM DISTURBANCES.

Description: Unless physical damage is caused by EMI, there is usually no evidence that it has occurred, other than a transient malfunction of the system, which might not even be noticed at the time.

Physical damage caused by EM DISTURBANCES is also likely to be misdiagnosed unless EM DISTURBANCE detection is used to correlate events.

An event data recorder (EDR) can be used to enable the establishment of evidence that a malfunction, which could have been caused by EM DISTURBANCES, has occurred.

Whenever an anomaly is detected (such as an out-of-range data value, checksum failure, sequencing error, etc.) relevant data can be recorded. For example, electromagnetically diverse software might reveal implementation errors via the discrepancy of results during operation, so all such discrepancies are timestamped and logged in an EDR (when one is used).

This data can then be analysed statistically in real time or at some later time to detect and diagnose trends due to sporadic failures and to propose remedial action.

Data captured by an EDR can only reflect the events and malfunctions it has been designed and programmed to detect and record. Consequently, to be practically useful, It is recommended that an EDR stores information for the sort of event types adequate for diagnosing the system behaviour retrospectively.

To aid fault attribution and diagnostics, it is recommended that the fault detection is time-correlated to the independent EMI event detection (see A.2.10).

Identification: A routine can be called each time a malfunction is detected and usually records, at the very least, the data itself and a time stamp code.

It is necessary for the resolution of the data recorded and its sample rate to be adequate for meaningful subsequent analysis.

Depending on the type of event recorder used and its mode of operation, pre-event data settings might also be important.

Depending on the size of the system and the level of the RISK, the EDR might be physically separate (and able to be "arrested" by the relevant safety authorities) for example, for a train or plane.

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

It is recommended that future designs, or modifications to the existing design, take the resulting information into account to keep pace with the worsening of the ELECTROMAGNETIC ENVIRONMENT, and also to improve the techniques and measures used for helping to achieve sufficient mitigation of the effects that can be caused by EM DISTURBANCES.

NOTE 1 Also see the anti-tampering techniques and measures in A.2.11.

NOTE 2 It can be applicable to consider increasing the ELECTROMAGNETIC IMMUNITY of the EDR, by using the techniques and measures such as, for example, those detailed in this document, to help ensure that an electromagnetic event that affects the ME EQUIPMENT or ME SYSTEM does not also affect the data stored in the EDR.

A.2.7 Improving mitigation of the effects that can be caused by EM DISTURBANCES in communication links

A.2.7.1 General

Overall aim: To help confirm that communication links have sufficient mitigation of the effects that can be caused by EM DISTURBANCES, where their functional performance is necessary for helping achieve BASIC SAFETY or ESSENTIAL PERFORMANCE.

This applies to, but is not limited to, communications links such as networks (for example, CAN, Profibus, Ethernet, wireless links including wide/local area networks, etc.); backplanes (for example, VME); printed circuit boards and even on-chip interconnect,

Overall description: Communication links can be made more robust to improve mitigation of the effects that can be caused by EM DISTURBANCES, by applying suitable hardware and software techniques and measures.

Overall Identification/mitigation: It is recommended that hardware and software techniques and measures are used, individually or together, to improve the reliability of the communication links with regard to EM DISTURBANCES. Suitable hardware techniques exist, such as – for example – those described in this document. Suitable software techniques include, but are not limited to, those set out in A.2.7.2 to A.2.7.4.

Wireless links are especially susceptible to EM DISTURBANCES (see A.3.26).

References: [100] to [102].

A.2.7.2 Error detection on parallel or serial buses

Description: Redundant data is appended to the actual data using error detection coding (EDC) and error correction coding (ECC) techniques (for examples, see A.3.12 to A.3.14).

This enables the detection of data corruption using techniques such as parity or cyclic redundancy checking (CRC).

Once data corruption is detected, appropriate action can be taken to maintain the ESSENTIAL PERFORMANCE, as described in the documentation. For example, various retry schemes could be used to improve the reliability of the link (at the expense of the overall system performance).

Where the safety document for a subsystem or component part includes a PDS, it can provide sufficient detail on it to allow its correct use by a safety system's designer.

A.2.7.3 Error correction on serial or parallel buses

Description: This is a variation of the previous technique; however, the code is such that a level of error correction is possible in order to both detect corruption and also correct for its effects.

Various error correcting code (ECC) schemes (see A.3.12 to A.3.14) can be used to improve the reliability of the link at the expense of a reduced data rate.

Whenever error correction occurs, it is recommended that this is logged to aid later diagnosis (see A.2.5).

A.2.7.4 Protection of a sequence

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

Extra sequence codes can be appended to each packet to enable detection of delayed, lost, or duplicated packets.

Various techniques and measures in this document can be used at the packet level, for example, even just a single bit can be alternated between packets to detect a single packet failure (omission or duplication) (for example, see [107]).

More elaborate techniques are needed to detect multiple packet failures or corruption.

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

A.2.7.5 Wireless mesh data communications networks

Description: Creates multiple geographically diverse wireless data communication links to improve the redundancy of data communications. Wireless mesh networks are being made increasingly cost-effective by the creation of low-cost commercial products intended to be used in the "Internet of Things" (IoT).

Identification: A wireless mesh network (WMN) is a communications network made up of radio nodes organized in a mesh topology. It is also a form of wireless ad hoc network. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The mesh clients are often laptops, cell phones, sensors, and other wireless devices while the mesh routers forward traffic to and from the gateways which can, but need not, be connected to the Internet.

The coverage area of the radio nodes working as a single network is sometimes called a mesh cloud. Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network.

A mesh network is reliable and offers redundancy. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes, as long as the nodes have been programmed to automatically adapt to changes in the mesh. Wireless mesh networks can be programmed to self-form and self-heal.

Wireless mesh networks can be implemented with various wireless technologies including 802.11, 802.15, 802.16, cellular technologies and need not be restricted to any one technology or protocol. (From https://en.wikipedia.org/wiki/Wireless_mesh_network).

Mitigation: The geographically diverse redundant nature of an automatically adaptive mesh network helps to ensure that data communication is maintained despite EM DISTURBANCES, because they tend to occur at high enough levels to cause EMI only over relatively small areas.

Accordingly: the larger the size of the mesh network, and the more redundant paths exist in the network, the greater is the mitigation of the effects that can be caused in data communications with regard to the effects of EM DISTURBANCES.

It is common to create mesh networks using all the same wireless technologies and frequency bands, however, additional protection against degradation of data communications as the result of EM DISTURBANCES can be achieved by using different technologies and frequency bands in the network. See also A.3.26.

A.2.8 Synchronization and resynchronization techniques

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

Description: The ability of a synchronous function or system to detect that it is running abnormally and then reset its own state, or the state of the system, whilst maintaining its ESSENTIAL PERFORMANCE.

For example, in some processor architectures EM DISTURBANCES can cause a processing exception due to corrupt data or the incorrect execution of an instruction.

Identification: By any appropriate techniques and measures, such as (for example) those described in this document.

Mitigation: A clear and understandable system design concept is needed for the credible and practical implementation of this technique.

Different techniques might be needed to resynchronize continuous and non-continuous synchronous systems.

Such resets or resynchronizations are to be safely tolerated by the application.

The use of low-level programming features is useful to implement state resynchronization, or to return the system to a safe state.

It is recommended that the use of built-in exception handling (for example: https://en.wikipedia.org/wiki/Exception_handling) within the language runtime package or operating system is only be relied upon if the resulting response is deterministic and accommodated as part of the overall design.

It is also recommended that the use of an electromagnetically diverse monitor be considered (see A.2.4).

NOTE The effectiveness of this technique depends on whether the function is intended for: continuous operation; to operate "on demand"; or where any kind of system has no safe state.

A.2.9 Protection from persistent interference by monitoring retry counts

Aim: To help achieve adequate mitigation of the effects that can be caused by EM DISTURBANCES during persistent failures including those caused by EMI.

Description: If a system is exposed to persistent EM DISTURBANCES to which it is susceptible, causing it to suffer EMI, then the operation of the system might be severely affected or even halted.

For example, a communication link, even with a retry facility, might be so affected that no message traffic can successfully be communicated.

Any defence mechanism relying on reactivation of a function or retransmission of a message might be so affected that there is effectively a "denial of service" (DoS), which might or might not be deliberate.

Identification: A task that continually monitors the retry counter values and timestamps of functions, memory checkers, communication protocols, and any other function that uses a retry or state recovery approach, to improve its perceived short-term reliability.

This task itself would involve a check for "Liveness" [128], for example, a timeout in order to be effective, preferably based on an electromagnetically diverse independent hardware watchdog timer (see A.2.4 and A.3.20).

Mitigation: Possible approaches might be to switch to a backup system; to switch to document operation; or to provide information to OPERATORS or maintainers. It is recommended that many other possibilities for the end-use application are considered at the system design stage.

Reference [143] can also be of use in the case of near-continuous EMI.

NOTE The effectiveness of this technique depends on whether the function is intended for continuous or on-demand operation.

A.2.10 Independent detection of EM DISTURBANCES and/or EMI

Aim: To help detect EM DISTURBANCES in the environment and/or EMI in the equipment.

Description: Independent detectors are used to sense the occurrence of certain types (ideally, all types) of EM DISTURBANCES, although perhaps only when they exceed certain levels. An example is described in [664], and [665] describes current experience of a deployed IEMI Detector. Several other types of detectors have been developed, usually by military/security organizations.

Identification: Where certain electromagnetic signals are necessary for safe operation, such as GPS signals, some means to detect their absence or "jamming" is useful for maintenance of ESSENTIAL PERFORMANCE. (Also see A.2.11, where the communication link is electromagnetically based).

An approach that relies on the internal resources of commercial off-the-shelf (COTS) devices operating system logs and other internal data and signals to provide valuable information about whether EMI is being experienced, is introduced in references [666] and [667]. An effective set of sensors has been identified for computers and smartphones and it has been shown that these observables were responsive to EM DISTURBANCES.

This definition of observables is empirical as it involves only resources that are accessible to users with simple or administrative rights in the operating system and which were not designed by the COTS MANUFACTURERS to be used for EMC testing, or for anything to do with BASIC SAFETY or ESSENTIAL PERFORMANCE.

Consequently, this approach could be improved by having CPU MANUFACTURERS and operating system editors provide more interfaces to gather low-level information about the health status of the system. This approach has the benefits of allowing the design of a real-time remote monitoring system for EM DISTURBANCES that cause EMI.

Mitigation: This technique can be used in many ways, for example:

- a) To help manage the external conducted and/or radiated ELECTROMAGNETIC ENVIRONMENT throughout the EXPECTED SERVICE LIFE, for example, by displaying or sounding a warning – or initiating other actions as documented – if the equipment starts to experience levels of EM DISTURBANCE in excess of the level of IMMUNITY it was designed to withstand.
- b) It could, for example, warn of the use of equipment using high RF power, such as a diathermic heater, in too-close proximity. This technique has been used in hospitals to help enforce their "no cellphones" policies by sounding a warning and could be helpful in enforcing the walkie-talkie example in A.3.5.
- c) By detecting a failure of electrostatic control measures (such as humidity control, static floor re-treatments, etc.) that could expose equipment to higher levels of ESD than it was designed to be able to cope with.

- d) (The usual maximum ESD test level in IMMUNITY standards is ± 8 kV, but levels of ± 25 kV or more have been seen during reduced atmospheric humidity and the automobile industry has tested to such levels for decades for this reason.
- e) By making sure that certain sensor or transducer readings were ignored, or certain circuits were reset, for the duration of an excessive disturbance.
- f) This is a well-established technique for preventing intentional interference with machines that can pay out money, for example gambling machines, change machines, automatic teller machines (ATMs), etc. (A typical tool used for such IEMI is the cattle prod, which generates impulses of around 35 kV.)
- g) It has also been used with some very sensitive medical diagnostic instruments to warn when to ignore their results because the ELECTROMAGNETIC ENVIRONMENT was noisier than they were designed to cope with (sometimes at quite low levels, such as >1 V/m).
- h) By recording data on the occurrence of certain types and/or levels of EM DISTURBANCES in an EDR (see A.2.5), ideally with time-of-event correlation to help attribute and diagnose the causes of failures, after the fact.
- i) By monitoring the internal ELECTROMAGNETIC ENVIRONMENT of equipment that relies on external shielding, filtering and/or surge protection so that if any of them degrade, and if that degradation permits higher-than-acceptable levels of EM DISTURBANCE to enter the equipment, then action in accordance with the documentation can be initiated.
- j) This could be helpful in enforcing A.6.2 so that, for example, if someone uses an incorrect type of shielded cable, or does not terminate it correctly, an alarm is sounded.

A.2.11 Protection of systems from tampering via communication links to external systems

Aim: To help maintain the BASIC SAFETY and ESSENTIAL PERFORMANCE of ME EQUIPMENT or ME SYSTEMS and/or of their subsystems or component parts that have external communication links, especially with the internet, at least with regard to adequate mitigation of the effects that can be caused by EM DISTURBANCES.

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

The offensive techniques can be used to access, change, or delete electronic data recorder (EDR) records and to change programs to make them more vulnerable to EMI.

Identification: Typically, a firewall is used to prevent attack, enable protection of the EMI log, and keep a record of the attacks it has detected, together with any consequent actions.

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

Remember that it is the system integrator who is responsible for protecting the system from this kind of threat (see A.1.4).

Mitigation: At least provide some protection of the EMI log by using a firewall to help prevent attacks from succeeding. Actually, detecting and subsequently attributing a malicious event is more likely to be effective in a broader context than just helping to achieve adequate mitigation of the effects that can be caused by EM DISTURBANCES.

If the EDR log media is physically removable, then it is recommended that the records of its removal and replacement are stored in a non-volatile memory that is built permanently into the system.

In the event of the EMI log being tampered with this record can be consulted.

Some EDR logs are built into the system and accessed interactively via a PORT. In this case it is necessary to restrict access to "read only" so that the EDR data cannot be altered or deleted, thus destroying possible evidence. EDR data can be encrypted to make tampering harder and alteration easier to detect.

A.2.12 Robust, high-specification electromagnetic mitigation

Aim: To provide a benign "internal ELECTROMAGNETIC ENVIRONMENT" by reliably attenuating the external ELECTROMAGNETIC ENVIRONMENT to a very high degree, throughout the EXPECTED SERVICE LIFE.

Description: A combination of high-specification electromagnetic mitigation including shielding, filtering, transient suppression, galvanic isolation, etc., traditionally taking the form of a mechanically rugged metal ENCLOSURE fitted with bulkhead-mounted cable connectors incorporating robust filtering, transient suppression and/or galvanic isolation.

This combination is designed so as to provide reliable attenuation of all EM DISTURBANCES, possibly even including direct lightning strike and electromagnetic pulse (EMP – see A.1.4), throughout the EXPECTED SERVICE LIFE by a suitable combination of initial design plus regular maintenance, repair, and refurbishment, which includes re-VERIFICATION of mitigation performance.

Electromagnetic detection techniques (see A.2.10) might be able to be used within an overall ENCLOSURE used for this purpose, in order to provide prior indication of certain failures or degradations in mitigation, perhaps enabling repair and refurbishment to take place when needed outside of the regular maintenance schedule. This approach can also be useful to help identify foreseeable misuse, such as doors or panels left open or not fitted properly, the use of incorrect types of cables/connectors, etc., or to identify EM DISTURBANCES that exceed those covered by the original design.

Robust, high-specification electromagnetic mitigation, when implemented correctly, can allow an electronic system to operate continuously throughout any/all external EM DISTURBANCES, so can be very useful when degradation or interruption of functionality is not desired.

Identification/mitigation: With appropriate design, this technique can be used to address any external (i.e. inter-system) EM DISTURBANCES throughout the EXPECTED SERVICE LIFE. However, it cannot deal with intra-system (internal) EM DISTURBANCES.

NOTE The extent to which robust conventional EMC mitigation techniques (for example, high-specification electromagnetic mitigation including shielding, filtering, transient suppression, galvanic isolation, etc.) can prevent EM DISTURBANCES from affecting BASIC SAFETY or ESSENTIAL PERFORMANCE throughout the EXPECTED SERVICE LIFE can be taken into account during the selection and application of the techniques and measures, where this is justified.

A.2.13 Techniques and measures to prevent RISKS being increased by virtualization of memory and PROCESS resources (e.g. a "digital twin")

Aim: To help confirm that virtualized systems do not prevent adequate mitigation of the effects that can be caused by EM DISTURBANCES.

Description: Virtualization is a technique for creating a virtual (rather than actual) version of something, including virtual computer hardware platforms, storage devices, and computer network resources. The virtualization is designed to provide a more idealized or convenient representation of the underlying physical computing resources, for example a virtual apparently contiguous memory address space composed from disjoint physical segments of memory.

Identification: For the system designer and programmer virtualization can be very convenient, particularly when attempting to support multiple programs on shared hardware, each apparently running on a different processor and with its own address space. However, the convenient illusion comes at a cost; consideration of this can be given during the design PROCESS in order to be aware of the potential for errors or malfunctions that could be caused by EM DISTURBANCES.

Virtualization almost always involves the low-level manipulation of computing resource. It makes systems more susceptible to EMI. For example, with memory virtualization, when data is read or written the virtual address will be translated by software or hardware at run time into the actual physical location of the memory. So, this mechanism itself needs protection from effects of corruption by EMI.

Similar situations arise for processor (instruction set) virtualization and network (private virtual network) virtualization.

Mitigation: In each case (memory, processor, and network) the mechanism used to translate between the virtual and physical can be subjected to a HAZARD and mitigation analysis, with appropriate mechanisms put in place to help understand the behavior of the system function in response to the detectable errors or malfunctions that could have been caused by EM DISTURBANCES.

Note that errors induced by corruption of the virtualization mechanisms can be extremely hard to detect and compensate for at the application software level, precisely because the virtualization is presumed to provide an ideal execution environment at that level and the virtualization mechanism is (intentionally) hidden from the application layer of the software.

A.2.14 Usability Engineering (Human Factors)

Aim: To use human resources and electronic resources wisely, to help minimize safety RISKS due to EMI.

Description: People are unaffected by a wide range of EM DISTURBANCES that can cause malfunctions (EMI) in electronics. So sometimes it makes good sense to use human resources instead of electronics.

Also, a human can recognize that electronics have malfunctioned even though no overt indication of the malfunction has been provided.

Identification: When using human resources, a number of issues can be managed to optimize the design for effectiveness – this is generally called Usability Engineering but is also known as Human Factors Engineering.

Like the topic of EM DISTURBANCES, the topic of usability engineering is briefly mentioned in ISO 14971, but little detail is provided. It is not within the scope of this document to discuss how to do usability engineering to help achieve adequate mitigation of the effects that can be caused by EM DISTURBANCES, but it is worth mentioning that [15] is a valuable resource and provides references to many other resources on this important issue.

Mitigation: By the appropriate use of usability engineering techniques and measures to help achieve adequate mitigation of the effects that can be caused by EM DISTURBANCES.

A.3 Techniques and measures that might be helpful in operational design

A.3.1 General

When the design is implemented, the functionality can be realized in hardware and/or software. In A.3.2 to A.3.29 techniques and measures are classified as either hardware or software based, but some techniques and measures can have equivalent representations in either hardware or software, which might be more effective.

NOTE Where a technique or measure in this subclause applies to a technology that is not relevant to the equipment or system concerned, and the importance as shown in Table B.1 as being HE, it is recommended that a justification for why that technique or measure was not applied be included in the documentation (see 5.3).

A.3.2 Developing appropriate operation and maintenance instructions

Aim: To develop instructions for PROCEDURES that help to avoid EMI-induced failures during the operation and maintenance of ME EQUIPMENT or an ME SYSTEM, or a component or subsystem used within ME EQUIPMENT or an ME SYSTEM.

Description: This is where the operation and maintenance specifications – and their justifications – for the techniques and methods used to comply with the design specification for the adequate mitigation of the effects that can be caused by EM DISTURBANCES are documented.

The operation instructions might include, for example:

- a) restrictions on the use of potentially interfering equipment in the vicinity of the safety system (such as mobile phones, cellphones, welding equipment etc.)
- b) restrictions on the removal of access panels where these contribute to the mitigation of the effects that can be caused by EM DISTURBANCES.
- c) for PORTABLE ME EQUIPMENT or ME SYSTEMS, restrictions on the type of ELECTROMAGNETIC ENVIRONMENT in which they are intended to be used.
- d) restrictions in the use of the ME EQUIPMENT or ME SYSTEM, for example, where it is user-configurable, where this might affect the adequate mitigation of the effects that can be caused by EM DISTURBANCES.
- e) the recording and reporting of system upsets, system restarts, safe failures, trips to safe state etc., especially where the cause is not obvious and might be due to an EMI event. (Recording and assessing system trips is an important contributor to reliability growth in general, and in some instances might even provide the only indication that mitigation of the effects that can be caused by EM DISTURBANCES is not operating as intended.)
- f) monitoring the ELECTROMAGNETIC ENVIRONMENT and detecting/recording EMI events to enable correlation with faults.

The maintenance instructions might include, for example:

- a) monitoring/inspection of physical protection measures against EM DISTURBANCES, such as access panel/door gaskets for deterioration or corrosion of mating surfaces, shielding effectiveness, etc.
- b) recommendations on the inspection and maintenance intervals necessary to maintain physical defences against EM DISTURBANCES.
- c) any lifetime restrictions due to the anticipated degradation of physical protection measures against EM DISTURBANCES, such as those due to corrosion.
- d) PROCEDURES to be followed to verify the continued effectiveness of physical protection measures after an unusual EM DISTURBANCE event, such as a major power surge, nearby lightning strike, etc.

Identification: By independent assessment of the relevant documents against, for example, the guidance in this document.

Mitigation: By correction of the relevant documents.

NOTE Experience indicates that operation and maintenance instructions typically only achieve a RISK reduction factor of no more than two.

A.3.3 Designing appropriate maintenance techniques

Aim: To help achieve adequate mitigation of the effects that can be caused by EM DISTURBANCES throughout the EXPECTED SERVICE LIFE.

Description: To make it practical to monitor the condition/performance of, and replace, if applicable, electromagnetic mitigation items such as filters, surge suppressors, conductive gaskets, etc., which can have a limited operational life.

Identification: By independent assessment of how easy it is for the relevant people to monitor and replace electromagnetic mitigation items that can have a limited life.

Mitigation: By correction of the relevant documents.

NOTE Experience indicates that maintenance instructions typically only achieve a RISK reduction factor of no more than two.

A.3.4 Limiting the possibilities for operation and hence mis-operation

Aim: To help avoid EM DISTURBANCES causing failures by affecting OPERATOR controls.

Description: EM DISTURBANCES can affect OPERATOR controls, creating the same effect as an unskilled or even malicious OPERATOR. This technique helps to avoid operation in unwanted or unnecessary modes.

Identification: This approach helps reduce the operation possibilities, and therefore the possibilities for EM DISTURBANCES to cause failures, by limiting, for example:

- a) the number of generally possible operating modes;
- b) physically protected operation of special operating modes, for example, by using key switches that are lockable or have protected access;
- c) the number of operating elements;
- d) consistency checks specifically aimed at detecting operationally inconsistent or non-plausible operating modes.

It is recommended that the hardware and/or software design techniques and measures used for limiting the possibilities for operation comply with this document.

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

Mitigation: By modification of the design using appropriate techniques and measures such as, for example, those described in this document.

A.3.5 Protecting against operation errors

Aim: To help protect the system against OPERATOR errors, mistakes, and other foreseeable misuse.

Description: Incorrect OPERATOR inputs (value, time, etc.) are detected via plausibility checks, monitoring of the ME EQUIPMENT or ME SYSTEM, or other methods.

To integrate these facilities into the design, it is necessary to state at a very early stage which inputs are possible and which are permissible.

It is recommended that any mistake in operation does not result in a dangerous failure, and that any foreseeable use/misuse is not permitted to compromise BASIC SAFETY or ESSENTIAL PERFORMANCE.

Identification: Competent independent assessment of the hardware and/or software design techniques and measures used for the protection against OPERATOR mistakes.

For example, using a walkie-talkie or cellphone closer than is permitted, or the failure to correctly close a shielding door, or to refit a shielding inspection panel, could reduce availability and/or prevent the attainment of a safe state (see A.2.10).

Mitigation: By HAZARD analysis, modification of the design and logging of mal-operations, using appropriate techniques and measures such as, for example, those described in this document.

A.3.6 Protecting against hardware or software modifications or manipulations

Aim: To help protect ME EQUIPMENT or an ME SYSTEM against hardware or software modifications or manipulations by any technical means.

Description: Modifications or technical manipulations can be detected automatically, for example, by plausibility checks for the sensor signals, detection by the technical PROCESS, automatic start-up tests, etc.

If an un-approved modification or technical manipulation is detected, appropriate action is taken in accordance with the documentation.

(A.2.10 describes one way of detecting modifications that could degrade electromagnetic mitigation.)

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

Mitigation: By modification of the design, using techniques and measures such as – for example – those in this document.

NOTE Modifications are usually subjected to a documented change control PROCEDURE and they are not expected to compromise BASIC SAFETY or ESSENTIAL PERFORMANCE.

A.3.7 Defensive programming techniques

A.3.7.1 General

Overall aim: To design software programs in such a way that they will assist in the detection of anomalous control flow, data flow or data values that might have been caused by EM DISTURBANCES during their execution and to react in a predetermined and acceptable manner.

Overall description: Many techniques can be used during programming to help detect and control the anomalies induced by EMI-induced corruption; see the references.

A range of error detection and/or correction techniques and measures, such as (for example) those described in this document, can be used to implement an acceptable hardware/software solution.

To aid fault attribution and diagnostics, it is recommended that the fault detection is correlated with the independent EMI event detection (see A.2.10).

Overall identification/mitigation: The principal defensive mechanisms are listed below, in A.3.7.2 to A.3.7.4.

Where the safety document for a subsystem or component part includes a PDS, it is recommended that it provides sufficient detail on it to allow its correct use by a safety system's designer.

References: [100] to [102] and [104] and by prevention: [113] to [115].

A.3.7.2 Range checking in hardware and in software

Identification: Range checking of the values of all variables, for credibility.

This is achieved by specifying a number of bands for the value of each variable, the meaning of the bands being specific to the application.

A typical example of three bands is: normal operational values; warning zone values; and out of range values.

This applies to values anywhere in the processing chain, not just I/O "signals", whether they are analogue or digital. It also applies to algorithms implanted in hardware such as FPGAs.

This is valuable for EMI detection as the value of the original variable might have been corrupted by an EMI event.

A program might well be correct, but the result of an assignment might be "out of range" and cause the program to malfunction.

The programming language provides a means of assigning a data type to a data variable to specify the range (or set) of values that it is intended to contain.

Whenever values are assigned to the variable, either at compile time (constant values) or at runtime (constant or modified values) then a check is made that the new data value is within the range of values specified by the type of the variable.

Some standards and other publications call this this "strong data typing".

In any case, it is recommended that all variables are initialized explicitly to an acceptable value, before being used, so that out-of-range errors are not caused by the arbitrary value in memory when power is first applied.

Mitigation: If the language's run-time package supports range checking, then that can be used (bearing in mind the loss of performance and increased size of program). If there is no automatic run-time range checking, then it is recommended that explicit tests are designed into the program. This also applies to hardware, for example hardware specified algorithmically in languages such as Verilog, including in FPGAs.

Range checks can be implemented both at:

- a) "Compile time", using assertions about the value ranges that the software/logic is specified to handle. This is often referred to as "static analysis"; it has no runtime overhead.
- b) "Operation time" or "run time", using program checks during system operation to verify values before they are relied upon for decision-making. This is often referred to as "dynamic analysis". The run-time load can be taken into account in the system design.

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

A.3.7.3 Sequence checking

Identification: Sequence checking is a powerful technique for ensuring that a sequence of values or stream of data packets is in the correct order and that there is no duplication or omission.

Sequence checking can be used for data and also for program state, for example, using finite state machines or Petri nets.

The program contains intermediate points where the expected state of the program, i.e. the values of data or status variables, can be checked for credibility.

Mitigation: Various techniques and measures, such as (for example) those described in this document, can be used at the hardware level to implement an acceptable solution.

Communication protocols using sequencing can be used to improve the effective quality and reliability of the link, for example, packet sequencing.

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

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

NOTE The importance of this technique depends on whether the function is intended for continuous operation or on demand.

A.3.7.4 Correct rounding and resolution in all calculations

Description: The incorrect handling of rounding errors and resolution (fixed or floating point) has been the cause of many high-profile project failures, such as [129], and [130]. Where different parts of systems use different units of measurement contemplate examining the conversions between data used in all contexts.

The corruption of data by EM DISTURBANCES can cause invalid values of data to occur and software exception handling techniques, such as range checking, can be used to verify the plausibility of data before it is relied upon by a safety critical function.

References: [120], [121], [129] (an example of poor exception handling), [130] (an example of incompatible units), [141].

A.3.7.5 Floating point unit and real number arithmetic

Aim: To help avoid the corruption of arithmetic computation by EM DISTURBANCES.

Description: Floating point is an example of a class of instructions that take multiple CPU cycles, making them more vulnerable to suffering interference due to EM DISTURBANCES (i.e. they have a larger time-window for data corruption).

Identification: In most applications the fixed-point capability of processors gives adequate accuracy for real number arithmetic and use of either hardware or software floating point is not contemplated. However, as the complexity of the arithmetic computations increases rounding errors rapidly become significant.

Where response times are important for the achievement of BASIC SAFETY or essential performance, generalized software floating point routines are unlikely to offer a viable solution and the addition of a hardware floating point begins to look attractive. The hardware can be either a co-processor or on-chip.

There are a number of difficulties with verifying that programs using real-number arithmetic are free from overflow, divide-by-zero, or error accumulated from the effects of rounding. These difficulties can be reduced by using hardware floating point arithmetic with the necessary precision.