IEC TS 60601-4-6

Edition 1.0 2024-04

TECHNICAL SPECIFICATION

colour inside

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

IEC TS 60601-4-6:2024-04(en)

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

IEC TS 60601-4-6

Edition 1.0 2024-04

TECHNICAL SPECIFICATION

colour inside

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

CONTENTS

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 European (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 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.

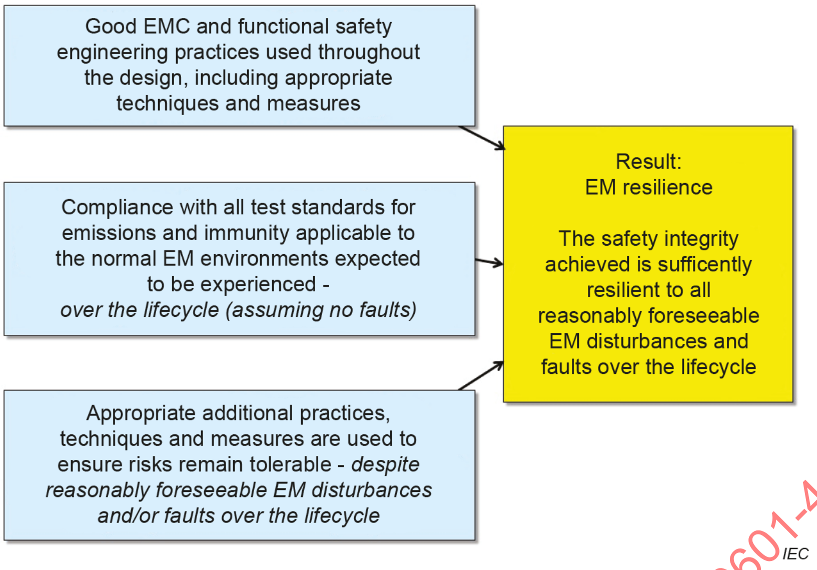
Good EMC and functional safety engineering practices used throughout the design, including appropriate techniques and measures
Compliance with all test standards for emissions and immunity applicable to the normal EM environments expected to be experienced - over the lifecycle (assuming no faults)
Appropriate additional practices, techniques and measures are used to ensure risks remain tolerable - despite reasonably foreseeable EM disturbances and/or faults over the lifecycle
Result: EM resilience
The safety integrity achieved is sufficently resilient to all reasonably foreseeable EM disturbances and faults over the lifecycle
IEC

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 ±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.

Mitigations:

a) Use scaled integers and fixed-point arithmetic where possible.

b) Extend the normal fixed word lengths when applicable by double precision. Round and truncate before output.

c) Use floating point only where fixed-word-arithmetic is inadequate.

d) Minimize the number of clock cycles taken to perform the arithmetic functions.

e) Range and clip results from both fixed- and floating-point calculations.

f) Use the overflow, divide-by-zero, and various error states for failure management and diagnostics.

g) Interweave a diagnostics routine within the application to compare sample fixed and floating-point calculations. Invoke failure management when differences are detected.

h) Use on-chip floating point implementations rather than external co-processors. External co-processors can be subject to temporary or permanent corruption that might not at the same time corrupt the CPU, and such errors might not be detectable.

i) Use integrated circuit IMMUNITY test techniques (robotized near field IMMUNITY test-bench, special GTEM cells, etc.) to check EM IMMUNITY of critical arithmetic computations at CPU / floating-point component level.

j) Seek evidence of validation / certification from MANUFACTURER.

A.3.8 Limited use of interrupts

Aim: To reduce the likelihood that EM DISTURBANCES will affect the execution of the software.

Description: EM DISTURBANCES can increase the likelihood that spurious interrupts are generated, possibly at such high rates that the timing of the software execution can be affected.

Interrupts can arrive asynchronously and, of course, interrupt the flow of the main program and possibly other interrupt routines that might be running at the time.

Interrupts are therefore prone to causing errors, and the determinism of the program's behaviour becomes very difficult to predict. For example, can it be guaranteed that an interrupt routine will never cause a loop that freezes the whole system?

It is recommended that the use of interrupts is restricted, but they can be used if they simplify the program to give an overall advantage for BASIC SAFETY and ESSENTIAL PERFORMANCE.

For example, it is understood that some very critical nuclear and military software is designed without any interrupts at all, in order to improve the determinism of the program's behaviour.

Identification: At compile time a static analysis program can be used to flag up any use of interrupts.

Mitigation: It is recommended that the use of interrupt routines be limited and, when used, their effect on system timing and the sharing of computing resources is documented.

It is recommended that software handling of interrupts is inhibited during critical parts (for example, time critical, critical-to-data changes) of the executed functions.

If interrupts are used, then it is recommended that parts not interruptible have a specified maximum computation time, so that the maximum time for which an interrupt is inhibited can be calculated.

Also see A.2.2.

References: [123], [125], [144] and [145].

A.3.9 Limited use of memory address pointer variables

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

Description: A pointer is a variable with a value that is an address of data in memory.

If the pointer variable is corrupted by EMI, then the impact on the behaviour of the program is likely to be unpredictable. For example, the corrupted pointer can either be pointing at some data, the program subroutine stack, the heap, or even the program itself, and consequently any write operation will corrupt the system.

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

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

If the hardware or run-tiME EQUIPMENT architecture allows memory address ranges to have protected access, then this feature can be used to ensure that only the intended memory partitions are accessible in each context. This would also make available the means for detecting an access violation. However, it would not detect data content corruption within accessible address ranges.

Partitioned ranges of memory and/or a memory management unit can be used to detect violations and provide some measure of protection (see A.3.11.4).

References: [113] to [115].

NOTE The importance 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. Be aware that the executable code might call addresses indirectly even if the source code is free from pointers.

A.3.10 Avoiding recursion

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

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

It is more susceptible to the effects of EMI-induced corruption as the nested chain of calls is held as a linked list of pointers on the stack, in effect potentially a very large list of pointers that increases susceptibility to EM DISTURBANCES. The deeper the level of recursion used the more susceptible the implementation. In general, the use of recursion can be replaced by an equivalent loop structure; this avoids extensive use of pointers and the possibility of running out of memory used to accommodate the pointer linkages for implementing recursion.

It is recommended that recursion is only used with the greatest caution – and comprehensive justification documented – in any software that helps achieve BASIC SAFETY or ESSENTIAL PERFORMANCE.

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

Mitigation: Programming guidelines would normally prohibit the use of recursion unless its use is fully analysed for resource usage and is clearly justified in the documentation. This would involve a rigorous argument for, or proof of, the maximum depth of recursion that would be experienced during operation, and the amount of memory that would be needed to support this at runtime.

Every algorithm that can be expressed using recursion also has an equivalent using an iterative looping construct. In general, it is recommended that the latter be the preferred solution for helping achieve BASIC SAFETY and ESSENTIAL PERFORMANCE.

A.3.11 Error detection and correction for invariable memory

A.3.11.1 General

Overall aim: To help detect information modifications in the invariable memory (i.e. ROM, or program memory).

Overall mitigation: It is recommended that techniques and measures are applied accordingly, bearing in mind all the possible susceptibilities of the system to the variety of EM DISTURBANCES described in A.1.

Some other suitable techniques and measures are described in A.3, and alternative or additional techniques can be used if technical justifications for them are documented.

A.3.11.2 Signature of a word or block of data

Aim: To detect single and multi-bit corruption within a block of data. Various checking techniques are available, such as cyclic redundancy checks (CRC), secure hash algorithm (SHA), and Hamming codes (for correction as well as detection).

Description: This PROCEDURE calculates a signature using an error-checking technique. The extended signature is stored, recalculated, and compared as in the single-word case. A failure is indicated if there is a difference between the stored and recalculated signatures.

Identification/Mitigation: When an error is detected, apply a response specified by the documentation. It is recommended that the error detection and/or correction method used is appropriate for the achievement of ESSENTIAL PERFORMANCE.

Where the safety documentation 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 the designer of the ME EQUIPMENT or ME SYSTEM.

References: [108] to [112] inclusive, [131] for Hamming codes and CRC, [132] for SHA.

A.3.11.3 Block replication with inversion (e.g. dual redundant ROM with comparison)

Aim: To help detect bit failures.

This is a powerful technique, and it is recommended that it is used wherever practicable.

Description: The address space is duplicated in two memories, and it is recommended that they are physically separate. The data is stored inversely in one of the two memories and inverted again to be compared with the other copy. The inversion of the data in one memory makes this technique much more effective against the common-cause errors, malfunctions or failures including the typical effects of EMI.

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

Mitigation: Repeat the memory read as many times as applicable without unacceptably degrading the ESSENTIAL PERFORMANCE.

If the failure clears, continue operation as usual. In any case, if a log is available, it is recommended that the fault be recorded (see A.2.6). If during the time available the failure does not disappear, apply an appropriate response, which is documented.

Where the safety documentation for a subsystem or component part includes a PDS, it can provide sufficient detail to allow its correct use by the designers of ME EQUIPMENT or an ME SYSTEM.

NOTE The use of electromagnetically diverse memories improves the effectiveness of this technique for adequate mitigation of the effects that can be caused by EM DISTURBANCES (see A.2.4).

A.3.11.4 Memory boundary protection

Aim: To prevent incorrect areas from being overwritten in specified types of memory.

Description: Runtime plausibility checking of use of a memory segmented into partitions. This is important as EMI-induced corruption of the program counter, stack pointer, heap pointer or any pointer in a program could cause data to be written to a wrong memory address, resulting in corruption of data or execution of the storing program instructions.

Statically defined and protected address ranges are used for the following:

a) program;

b) stack;

c) statically allocated variables;

d) heap (dynamically allocated variables);

e) inputs; and

f) outputs.

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

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

Mitigation: Upon detection, apply an appropriate response that is documented.

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

References: [113] to [115].

A.3.12 Error detection and correction techniques in redundant designs

Aim: To help achieve adequate mitigation of the effects that can be caused by EM DISTURBANCES by comparing the results of multiple redundant channels in hardware or software.

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

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

Similarly, to increase the effectiveness of this technique against the common-cause errors, malfunctions, or failures typical of EMI, electromagnetically diverse encoding of data and or programs can be used (see A.2.4).

When multiple channels are implemented on physically separate processors, mitigation of the effects that can be caused by EM DISTURBANCES will be enhanced if the power supplies are isolated and the interconnections are properly protected against EM DISTURBANCES.

Identification: The result of comparing the sets of signals will facilitate the acceptance of safety in the current context.

The comparator or voter (the circuit used to compare channels and detect errors) is a potential single point of failure and so can be designed to have considerably greater resistance to EM DISTURBANCES for this technique to be effective. This can be achieved by, for example, the strong use of self-testing to verify correct operation, switching to a redundant comparator or voter (ideally one using diverse technology; see A.2.10), if applicable. An alternative possibility is the use of rugged, lifetime-reliable, high-specification electromagnetic mitigation, which can be achievable with small size and low weight on a printed circuit board (see [69]).

Mitigation: Upon detection of an anomaly, apply an appropriate response that is documented.

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

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

A.3.13 Time-based error detection/correction in buses and interfaces

Aim: To assist in the detection of transient failures in bus and/or interface communication.

Description: The information is transferred several times in sequence.

The repetition is effective only against transient failures.

Identification: Each instance of the information is stored as it is received and then the instances are compared to see if they are consistent.

Often, sequence numbers or time stamps are incorporated into the data so that it becomes possible to check that data has arrived in the correct order and that none have been lost in transit.

To improve the effectiveness of this technique it is often combined with the use of error-checking codes to protect the sequence numbers or time codes (see A.3.12 and A.3.14).

Mitigation: Apply an appropriate response that is documented.

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

NOTE Needs at least one complete repetition in one cycle time of the PROCESS.

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

A.3.14 Error detection and correction for variable memory

A.3.14.1 General

Overall aim: To assist in the detection of failures during addressing, writing, storing, and reading data in memory.

A.3.14.2 Memory testing

Aim: To provide memory testing before operation and/or during operation to help detect errors specific to memory systems.

Description: It is crucial that read/write memory devices function correctly in order for any computer-based system to work reliably. The content of memory devices can be corrupted by EM DISTURBANCES and the devices themselves might even be physically damaged by severe EM DISTURBANCES.

It is therefore necessary to efficiently test the memory before operation and during operation to confirm that it is functioning normally. It is also necessary to design the testing in such a way that the known causes of error are tested as separately as possible.

This becomes more and more important as products and systems increase their use and size of memory. It is important that memory tests do not corrupt the running of the system itself, for example, the content of memory stacks, heaps, and configuration data.

However, even well-designed memory systems are naturally susceptible to EMI, in particular when they rely on the storage of electrical charge to represent digital values as charge can be altered by EM DISTURBANCES (and by ionizing radiation).

The purpose of the memory test is to confirm that the memory device is fully functional, so this kind of test usually writes a set of data to each individual address in the device and verify its correct value by reading the data back. In cases where such a test would destroy the data in the memory precautions can be taken, such as copying it, or specific techniques are used to conserve the memory content in situ.

The tests used usually are designed to efficiently identify the likely kinds of faults that the memory device being tested is likely to suffer from, or have induced by, EM DISTURBANCES and/or ionizing radiation.

Catastrophic internal failure of devices sometimes occurs and can be detected by appropriate means, but most memory failures are caused by wiring problems, including crosstalk on the data, address, and control line busses. Often these problems are difficult to detect and isolate as the memory affected might not actually be used for extended periods of time. When it is used and causes mal-operation of the system it can be very difficult to diagnose and isolate the originating cause.

A memory test strategy that takes account of at least the following points is recommended:

a) detection of missing memory chips;

b) detection of incompletely inserted or connected memory devices;

c) testing the memory data bus, preferably one bit at a time to aid fault isolation;

d) testing the memory address bus, primarily to detect that address bus faults are not causing overlapping memory locations to be addressed;

e) testing the function of the memory device itself;

f) if dynamic memories are being tested then signal integrity tests for DDR memory signal lines would also need to be tested;

g) testing of systems using "memory caching" techniques needs special consideration, such as provision for the safe flushing of cache memory, which might otherwise temporarily mask a fault that has developed after the saved data has been cached.

h) testing of memory currently in use by the system (its stacks, heaps, and state variables) needs great care in order for the testing not to corrupt the system itself. This is of particular concern for operational systems when memory tests are periodically scheduled as background activities to check on-going system integrity.

Detection: The memory test can be run:

a) during the initialization of the system and after any reset of the system; i.e. before operational use of the system starts; and/or

b) during the real-time operation of the system.

Mitigation: Analysis and diagnosis of the memory test result data can be used to identify specific kinds of common faults in the memory system efficiently.

It is recommended that future designs, or modifications to the existing design, take the resulting information into account to keep pace with the changes in memory technology, in particular its susceptibility to EM DISTURBANCES as memory cell sizes continue to be reduced, compounded by the worsening of the ELECTROMAGNETIC ENVIRONMENT.

NOTE Also apply other techniques and measures as appropriate for testing memories and achieving the aims of this subclause.

References: [133] to [136].

A.3.14.3 One-bit redundancy

Aim: To detect some changes in the content of a memory location, bus, or I/O register.

Description: Every data word is extended by a single bit, often called the parity bit, based on the binary value of the data.

Identification: The parity bit of the data word is set when it is stored, and then checked each time it is read.

If an invalid parity value is detected it indicates that the content has been corrupted. A failure action can then be activated.

If the parity value is correct then there might have been no error, however, there might have been multiple bit changes to the content resulting in the same parity value.

Mitigation: Upon detection, apply an appropriate response as documented.

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

References: [107].

A.3.14.4 Block replication with inversion to detect all bit failures

The techniques and measures in A.3.11.3 for invariable memory also apply here.

A.3.14.5 Memory boundary protection

The techniques and measures in A.3.11.4 for invariable memory also apply here.

A.3.15 Error detecting/correcting coding for ROM, RAM, buses, and interfaces

Aim: To help detect and/or correct one, or more, bit failures in a word.

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

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

Mitigation: If a difference is found, corrective action can be taken (or a failure indication produced) as specified and documented.

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

Correction of the data can be used to maintain the correct operation of the function. It is recommended that the strength of the technique used is justified and this justification is documented.

References: [110] to [112]

A.3.16 Error detection and correction for logic and data processing

A.3.16.1 General

Overall aim: To assist in the recognition of any failures that could lead to incorrect results in processing units.

Overall description: All the techniques and measures listed in this subclause are concerned with detecting failures in the processing units and soft failures (bit flips) in memories and registers, and are therefore useful for detecting damage caused by lightning (or other) surges and ELECTROSTATIC DISCHARGES, as well as soft failures such as those caused by ionizing radiation etc.

A.3.16.2 Self-test supported by hardware (one-channel)

Description: Additional special hardware supports self-test functions, for example, it monitors the output of a certain bit pattern, often referred to as a "signature". It is a form of watchdog that relies on data content rather than time.

Identification: Used for detecting disruption of program execution.

Coverage depends on the extent of the software functions generating the bit pattern signature.

Mitigation: Corrective action can be taken, or a failure indication produced, as documented.

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

The additional hardware could, for example, drive ME EQUIPMENT or an ME SYSTEM to a safe state, and/or restart it (if it is safe to do so).

It is usual for the additional hardware to be low technology (i.e. not programmable or electromechanical), or even mechanical, pneumatic, or hydraulic because they are not affected at all by EM DISTURBANCES.

A.3.16.3 Coded processing (one-channel)

Description: Processing unit designed with special failure-recognition or failure-correction circuit techniques.

Typically, a detection mechanism, such as a watchdog timer, can be used to detect a malfunction affecting the safety of the system. In response the system can be reset to a known state, often referred to as a "restore point", and the continuation of operation of the system attempted.

Identification: Good design practice maintains the independence of the detection of safety or operational malfunction from the main processing system.

For example, a watchdog timer that is implemented by a separate piece of hardware in such a way as to be itself electromagnetically resilient, otherwise false system resets and restores would be triggered.

Mitigation: The system-level implications of resetting to each reachable restore point before continuation, at any time during system operation, is useful to consider.

When used, it is recommended that the benefits to mitigation of the effects that can be caused by EM DISTURBANCES are assessed for the particular implementation, and the analysis documented.

Where a 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], [122] and [124].

A.3.16.4 Reciprocal comparison by software

Description: Two or more electromagnetically diverse processing units exchange data (results, intermediate results, and test data) and cross-check at specified "restore points" from which system operation could be continued in the event of a discrepancy. Detected differences indicate a failure.

Identification: Coverage of data discrepancies is high, and detection can be fast.

Excellent against hard failures and can be good against soft and transient failures too.

Mitigation: If the diagnostic test interval is short compared to the PROCESS safety time, a restart might be possible while keeping the PROCESS running. If the failed unit can be identified, continued operation with the healthy unit might be possible. Otherwise, restoration of the function to a safe state will offer desirable protection.

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

NOTE It is applicable that hardware and/or software diversity (see A.2.4) is used to greatly improve coverage of the common-cause errors, malfunctions, and failures typical of EMI.

A.3.16.5 Self-test by software during operation

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

Identification: Can detect some failures but coverage is low. The self-test can also be affected by the failure.

Mitigation: Additional monitoring circuitry is useful to achieve a safe state on failure.

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

References: [124] and A.3.14.2.

A.3.17 Error detection and correction for electrical and electromechanical components

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

Description: Electrical and electromechanical components are generally less susceptible to EMI-induced failure than electronic components as their operating signal levels are usually much higher, but they are never totally immune.

Direct failures due to gross overload causing contact welding or coil burnout are possible in some applications.

EMI to circuits that control electromechanical devices can cause failures due to:

a) chatter (unintended repeated operation causing early wear-out);
b) generation of additional EM DISTURBANCES via arcing or sparking at electrical contacts; or
c) paralysis (device physically stuck).

Identification: Electromechanical components can be monitored as part of loop, for example, by relay contact monitoring, by actuator position monitoring, or by the effects on the ME EQUIPMENT or ME SYSTEM (on-line monitoring). It is recommended that care is taken that such monitoring will detect chatter (especially in relays) or partial operation in actuators.

The use of electromagnetically diverse technologies (see A.2.4) is recommended when performing parallel functions to help deal with the common-cause effects of EM DISTURBANCES.

Mitigation: It is recommended that burn-out or paralysis failures are designed to achieve a safe state.

Where a 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.

Multi-channel systems might be able to tolerate a single-channel failure, but it is useful to consider the likelihood of common mode failures.

Examples are suppression of arcing and proper termination of inductive loads to avoid induced spikes.

A.3.18 Caution when using hardware or software libraries

Aim: To confirm that the techniques and measures for adequate mitigation of the effects that can be caused by EM DISTURBANCES are applied and verified throughout the whole software design and implementation of ME EQUIPMENT or an ME SYSTEM.

Description: Software development relies more and more on "standard" components encapsulated in libraries, for example, a TCP-IP stack, a matrix multiplication package etc. They are the software equivalent of COTS hardware. The overall software is as strong as its weakest part and so it is essential for ME EQUIPMENT or an ME SYSTEM that any library software used has been designed to the appropriate guidelines, such as (for example) those described in this document.

Identification: Auditing the source code of all library code will help to confirm that the techniques and measures for adequate mitigation of the effects that can be caused by EM DISTURBANCES have been competently and adequately applied.

Mitigation: It is recommended that any hardware or software components or modules copied from any library is checked against the guidance in this document before being incorporated into an operational system.

NOTE Hardware specification is now often implemented algorithmically (for example, IEEE Verilog, IEEE Standard 1364-2005) [70] for FPGAs.

A.3.19 Error detection and correction for electronic components

A.3.19.1 General

Overall aim: To help control failures in solid-state active and passive components.

A.3.19.2 Tests by redundant hardware

Aim: To use additional hardware to monitor the operation of functions that help achieve BASIC SAFETY or ESSENTIAL PERFORMANCE.

Description: Redundant hardware can be used to provide diagnostic testing for functions that help achieve BASIC SAFETY or ESSENTIAL PERFORMANCE.

Identification: Good for detecting failed states but might be poor at detecting transient failures.

Coverage depends on the rate of test compared to the PROCESS periodicity.

Mitigation: Effectiveness depends on diagnostic coverage and diagnostic test interval compared to the PROCESS periodicity. If/when used, it is recommended that the benefits for adequate mitigation of the effects that can be caused by EM DISTURBANCES are assessed for the particular implementation and the analysis documented.

Where a safety document for a subsystem or component part of ME EQUIPMENT or an ME SYSTEM includes a PDS, it can provide sufficient detail to allow its correct use by designers to help ensure BASIC SAFETY and ESSENTIAL PERFORMANCE.

A.3.19.3 Using dynamic signalling techniques

Aim: To help detect static failures by dynamic signal communications and processing.

Description: A forced change of otherwise static signals helps to detect static failures.

For example, alternating voltage signals are less vulnerable to stuck-at faults than static (direct voltage) signals.

Identification/mitigation: Good at detecting failed states, but poor at detecting transient failures. If/when used, it is recommended that the benefits for adequate mitigation of the effects that can be caused by EM DISTURBANCES are assessed for the particular implementation, and the analysis documented.

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

A.3.19.4 Caution with use of test access and real-time trace PORTS, and boundary-scan

Aim: To help prevent any added test/diagnostics, especially real-time trace PORTS and boundary-scan (such as JTAG) from making the system more susceptible to EM DISTURBANCES.

NOTE JTAG refers to the Joint Test Action Group; IEEE Standard 1149.1-1990, Standard Test Access Port and Boundary-Scan Architecture [71].

Description: The added interconnections can make susceptibility worse, especially boundary scan (which adds logic between the I/O buffers and the integrated circuits core logic to allow testing the core logic, creating a possible path for EM DISTURBANCES right into the "heart" of any electronics).

On some processors the real-time trace PORT can be a real problem if it is not removed from the PCB for release into production. Indeed, the large number of signals, fast and sensitive signals connected directly to the core, high density connectors and a large surface taken on the PCB, can increase the radiated EMISSIONS and / or degrade the IMMUNITY to EM DISTURBANCES.

If test access PORTS and their connections can be designed to be electromagnetically resilient then the system will be made more susceptible instead of less. Using a low-profile PCB-surface-mounted connector for the JTAG access PORT, and ensuring that no cable is ever left attached to it, is very helpful in helping to achieve adequate mitigation of the effects that can be caused by EM DISTURBANCES.

Identification/Mitigation: Where used, it is recommended that their effectiveness against EM DISTURBANCES is determined taking into account the particular design features, and this analysis documented.

It is also recommended that real-time trace PORTS are kept only in the development and debugging phase of functional prototypes; and that pre-production and production versions remove this feature.

References: [137] to [138]

A.3.19.5 Monitored redundancy

Aim: To compare the behaviour of two or more channels in a multi-channel system, to help detect errors and/or to correct them.

Description: The function is executed by at least two electromagnetically diverse hardware channels (see A.2.4). The outputs of these channels are monitored and if the output states differ a suitable action is initiated to maintain the BASIC SAFETY and ESSENTIAL PERFORMANCE.

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

Mitigation: As specified in the documentation, apply an appropriate response that maintains BASIC SAFETY and ESSENTIAL PERFORMANCE.

For a subsystem or component part: transition to a PDS as recorded in the safety document, can provide sufficient detail to allow its correct use by a safety system's designer.

However, with three or more channels and a voting function, error correction (isolation of the faulty channel and continued operation) can be practicable (see A.2.4).

A.3.19.6 Hardware with automatic self-test

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

Description: The hardware tests itself repeatedly at suitable intervals.

Identification: Will only detect failed states, not the transient failures that might have caused them.

Mitigation: As specified in the documentation, apply an appropriate response that maintains BASIC SAFETY and ESSENTIAL PERFORMANCE.

For a subsystem or component part: transition to a PDS as recorded in the safety document, can provide sufficient detail on it to allow its correct use by a safety system's designer.

However, by using redundant electromagnetically diverse-technology channels (see A.2.4) it might be practicable to continue safe operation by switching from a failed channel to one that is still operating correctly.

A.3.19.7 Analogue signal monitoring

Aim: To improve confidence in signals and controls.

Description: Analogue signals are used in preference to digital on/off states.

Trip or safe states are represented by analogue signal levels, which can be continuously monitored for credibility (for example, by using window comparators for amplitude ranges; high-pass, band-pass and low-pass filters for frequency ranges, etc.).

Identification: Can be effective against EMI, especially if unusual signals are detected, logged, and investigated.

Mitigation: As specified in the documentation, apply an appropriate response that maintains BASIC SAFETY and ESSENTIAL PERFORMANCE.

For a subsystem or component part: transition to a PDS as recorded in the safety document, can provide sufficient detail on it to allow its correct use by a safety system's designer.

However, by using redundant electromagnetically diverse-technology channels (see A.2.3) it might be practicable to continue safe operation by switching from a failed channel to one that is still operating correctly.

Signals can also be "smoothed" in hardware and/or software up to the maximum permitted for the accuracy and responsiveness needed.

Information on signal anomalies from event logs might be able to be used to improve long term mitigation of the effects that can be caused by EM DISTURBANCES, and future designs.

A.3.19.8 "Data assurance" (content credibility checking)

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

Description: The notion of data can include individual data values and also collections of data items, such as lists, arrays, records, and sets. The credibility checking can include range checking, and consistency of values between related data, such as by using the technique known as "median filtering".

There are several aspects to consider such as static (compile time) data typing, static range checking and dynamic (at runtime) value range checking, both on assignment and during the evaluation of arithmetic expressions.

Identification: Various checking schemes can be used to enable detection of corruption, for example, checksums or CRCs.

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

Mitigation: As specified in the documentation, apply an appropriate response that maintains BASIC SAFETY and ESSENTIAL PERFORMANCE.

For a subsystem or component part, transition to a PDS as recorded in the safety document, can provide sufficient detail on it to allow its correct use by a safety system's designer.

However, by using redundant electromagnetically diverse-technology channels (see A.2.3) it might be practicable to continue safe operation by switching from a failed channel to one that is still operating correctly.

Reference: [139]

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

A.3.20 Error detection/correction by monitoring program sequence (i.e. watchdogs)

A.3.20.1 General

Overall aim: To help detect a defective program sequence or timing and either take appropriate actions to maintain the ESSENTIAL PERFORMANCE; or restart the correct sequence if this is appropriate for maintaining the ESSENTIAL PERFORMANCE.

Overall description: A defective program sequence exists if the individual component parts of a program (for example software modules, subprograms, or commands) are processed in the wrong sequence or period of time, or if the clock of the processor is faulty.

Overall mitigation: As specified in the documentation, apply an appropriate response that maintains BASIC SAFETY and ESSENTIAL PERFORMANCE.

For a subsystem or component part, transition to a PDS as recorded in the safety document, can provide sufficient detail on it to allow its correct use by a safety system's designer.

However, by using redundant electromagnetically diverse-technology channels (see A.2.3) it might be practicable to continue safe operation by switching from a failed channel to one that is still operating correctly.

A.3.20.2 Watchdog with separate time base without time-window

Description: External timing elements with a separate time base (for example, watchdog timers) are periodically triggered to monitor the computer's behaviour and the plausibility of the program sequence. It is important that there is a clear design justification for the placement of triggering points in the program.

The watchdog is not triggered at a fixed period, but a maximum interval is specified.

It is recommended that the watchdog(s) be designed using appropriate techniques and measures for adequate mitigation of the effects that can be caused by EM DISTURBANCES such as, for example, those that follow the guidance in this document.

Identification: When the program fails to trigger any watchdog, a failure is indicated.

There could be several watchdogs, each monitoring different points in the program's execution sequence.

A.3.20.3 Watchdog with separate time base and time-window

Description: Timing elements physically separate from the computer, with a separate time base (watchdog timers), are periodically triggered to monitor the computer's behaviour and the plausibility of the program sequence.

It is important that there is a clear design justification for the placement of triggering points in the program.

It is useful to specify lower and upper limits for the watchdog.

This technique is preferred over A.3.20.2.

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

A.3.20.4 Logical monitoring of program sequence

Description: The correct sequence of the individual program sections is monitored using software (for example, counting PROCEDURE, key PROCEDURE) or using external monitoring facilities.

It is important that there is a clear design justification for the placement of triggering points in the program.

This technique is preferred over A.3.20.2 above.

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

A.3.20.5 Combination of temporal and logical monitoring of program sequences

Description: A temporal facility (such as a watchdog timer with a time-window) monitoring the program sequence is retriggered only if the sequence of the program sections is also executed correctly.

This technique is preferred over any of the three techniques in A.3.20.2, A.3.20.3 or A.3.20.4 above. It is also preferred over the application of both A.3.20.3 and A.3.20.4 at the same time but independently.

Identification: If the temporal facility monitoring the program sequence is not retriggered, a failure is indicated.

A.3.21 Error detection and correction using multi-channel input/output interfaces

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

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

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

The comparator (the circuit used to compare channels and detect errors) is a weak point and so it is applicable to be designed to have considerably greater mitigation of the effects that can be caused by EM DISTURBANCES for this technique to be effective (for example, very frequent dynamic testing). The technology used for the comparator can be justified in the documentation.

Mitigation: If a signal corruption is detected by the communicating partner(s), retransmission of the input or output data is requested. If the failure clears, continue operation as usual.

However, if during the time available the failure does not disappear, apply an appropriate response as specified in the documentation.

As specified in the documentation, apply an appropriate response that maintains BASIC SAFETY and ESSENTIAL PERFORMANCE.

For a subsystem or component part, transition to a PDS as recorded in the safety document, can provide sufficient detail to allow its correct use by a safety system's designer.

However, by using redundant electromagnetically diverse-technology channels (see A.2.3) it might be practicable to continue safe operation by switching from a failed channel to one that is still operating correctly.

Reference: [115]

A.3.22 Using test patterns: static and dynamic

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

Description: This is a dataflow-independent cyclical test of input and output units. It uses a specified test pattern to compare observations with the corresponding expected values.

The test pattern information, the test pattern reception, and test pattern evaluation need to all be independent of each other. It is recommended that the test pattern not interfere with the correct operation of the function.

Useful for helping achieve adequate mitigation of the effects that can be caused by EM DISTURBANCES by detecting damage caused by over-voltages from lightning, ELECTROSTATIC DISCHARGES, or other sources.

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

Mitigation: Repeat the test pattern as many times as there is time for, without unacceptably degrading ESSENTIAL PERFORMANCE.

If during the time available the failure clears, log in the EDR (if one is available) and continue operation as usual.

If during the time available the failure does not clear, log in the EDR (if one is available) and apply an appropriate response as specified in the documentation.

As specified in the documentation, apply an appropriate response that maintains BASIC SAFETY and ESSENTIAL PERFORMANCE.

However, by using redundant, electromagnetically diverse channels (see A.2.4) it might be practicable to continue safe operation by switching from a failed channel to one that is still operating correctly.

A.3.23 Using fiber-optic cables for signals and data communications

Aim: To avoid the effects of EM DISTURBANCES on communications media by using metal-free fiber-optic cables which do not conduct electricity.

Description: Optical fibers in themselves (see the note below) are unaffected by all EM DISTURBANCES (although they need protection from the thermal effects of lightning strikes, if exposed to them) and with suitable environmental protection can be used in all applications, including the most arduous.

Fiber-optic cables and their electronic interfaces (transmitters and receivers) are available in a wide range of types (and costs) to carry analogue signals from DC up to several gigahertz and data at up to hundreds of gigabaud.

Where electrical power needs are under 5 W, it is also practicable to carry AC or DC power over ordinary fiber-optics, converting the optical power into electrical power by using a photovoltaic cell instead of a signal/data receiver.

Mitigation: Optical fiber transmitters and receivers themselves *are* affected by EM DISTURBANCES, and so need to use the good electromagnetic design techniques described in A.3.27.

However, they are very small, making it much easier and less costly to achieve sufficient confidence in communications than when using metal cables.

Metal-free optical fibers are a good choice for at least one of the channels when designing an electromagnetically diverse multi-channel redundant communication link (see A.2.4).

NOTE Certain types of optical cables use metal foils as moisture barriers, metal wires as drawstrings, and/or metal armor. These all conduct electricity and can also worsen the thermal effects of lightning if the optical cable is struck by lightning.

A.3.24 Techniques and measures for AC and DC power supplies/power converters

A.3.24.1 General

Overall aim: To help detect or tolerate failures caused by degradations or defects in any of the electrical power supplies.

Overall description:

Degradations and defects in both DC and AC supplies:

Under voltages, over-voltages, sags, swells, and interruptions lasting from less than one microsecond to many hours, days, even months in some cases. AC ripple and noises with any frequency range and level.

Transients, "spikes" and surges lasting from less than one microsecond to hundreds of milliseconds.

Degradations and defects in AC supplies only:

Waveform distortions, frequency perturbations and, in multi-phase supplies, phase and/or voltage imbalances, all with any amplitudes and lasting from less than one second to many hours, days, even months in some cases. Includes incorrect phase rotation.

A.3.24.2 Detecting degradations and defects

Identification: Various devices and circuit techniques are readily available for detecting any/all defects in AC or DC power supplies. For detecting excessive RF noise, see A.3.24.4.

Mitigation: Upon detecting a degradation or defect in a power supply apply an appropriate response that is specified in the documentation and that maintains BASIC SAFETY and ESSENTIAL PERFORMANCE.

Can usefully be combined with mitigation in A.3.24.3 and/or A.3.24.5

A.3.24.3 Power hold-up

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

So e.g. electrolytic capacitors with liquid electrolytes might not be a good choice for some applications, especially those with high operating temperatures.

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

In the case of long sags, under voltages or interruptions, it is applicable to consider the energy storage requirements to be sufficient to continue correct (safe) operation whilst the ME EQUIPMENT or ME SYSTEM is put into a safe state, or some other action taken, as described in the documentation to maintain BASIC SAFETY and ESSENTIAL PERFORMANCE.

ME EQUIPMENT or ME SYSTEMS with high power consumption and/or needing a long time to be put into a safe state despite lack of power might use large battery banks (for example either directly or as part of a UPS) and/or rotating reserve power generators.

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

Mitigation: Improvement of the design, for example, by adding more energy storage of an appropriate type.

Before the energy storage becomes exhausted to the point where errors, malfunctions or failures could possibly occur, apply an appropriate response that is specified in the documentation and that maintains BASIC SAFETY and ESSENTIAL PERFORMANCE.

Can usefully be combined with A.3.24.5.

A.3.24.4 Detecting excessive RADIO FREQUENCY noise on power supplies

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

Description: Simple broadband RADIO FREQUENCY (RF) detectors can readily be created using ordinary circuit techniques (for example, a resistor, Schottky diode, capacitor, and operational amplifier) that will reliably detect frequencies up to tens of MHz, if they have sufficient amplitude. Some semiconductor MANUFACTURERS make single-chip RF detectors to detect up to many gigahertz.

It will generally be necessary to set the sensitivity of the detector so that it does not trigger on the normal systematic noises made by the equipment or system itself in any operating mode when operating correctly.

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

Mitigation: Apply an appropriate response that is specified in the documentation and that maintains BASIC SAFETY and ESSENTIAL PERFORMANCE.

A.3.24.5 Redundant electromagnetically diverse power supplies

Aim: To maintain BASIC SAFETY and ESSENTIAL PERFORMANCE despite any of the problems detected by A.3.24.2, A.3.24.3 and A.3.24.4, by providing alternative power supplies.

Description: Providing alternative power supplies to replace failed ones.

Identification: Problems with power supplies can be detected using the techniques and measures described in A.3.24.2, A.3.24.3 and A.3.24.4 above.

Mitigation: The availability of redundant electromagnetically diverse power supplies (see A.2.3) allows safe operation by switching from a failed power supply to one that is still operating correctly. It is useful to design the switch to be very electromagnetically robust as described in the documentation.

A.3.25 Monitoring of ventilation, cooling, and heating

Aim: To help confirm that ventilation, cooling, and heating systems are appropriately monitored to assist in the prevention of malfunctions caused by EM DISTURBANCES.

Description: Failures of the ventilation, cooling or heating can expose the ME EQUIPMENT or ME SYSTEM to environmental conditions that are outside is specified capabilities, possibly increasing the rate of dangerous failure to an unacceptable level. Such failures could be caused by EM DISTURBANCES.

Identification: Ventilation, cooling and heating systems are monitored for correct operation.

Mitigation: When a failure is detected, apply an appropriate response that is specified in the documentation and that maintains BASIC SAFETY and ESSENTIAL PERFORMANCE.

However, by using redundant electromagnetically diverse ventilation, cooling or heating systems (see A.2.3) it might be practicable to continue safe operation by switching from a failed one to one that is still operating correctly.

A.3.26 Careful use of wireless (radio) data communications

Aim: To help confirm that any wireless malfunction due to unwanted (in-band) and/or co-channel interference will not cause an unsafe failure, and that the introduction of a wireless function does not adversely impact upon the BASIC SAFETY or ESSENTIAL PERFORMANCE of ME EQUIPMENT or an ME SYSTEM.

Description: As many products now include an element of wireless functionality, it is conceivable that they will be used to contribute to the achievement of BASIC SAFETY and/or ESSENTIAL PERFORMANCE. A "heartbeat" signal is typically used in wireless design to confirm that there is continuous communication between the transmitter and receiver.

Identification: Selection of suitable frequencies that support continuous transmission is needed since many frequency allocations do not allow for this type of transmission. Reference [140] provides recommendations on suitable frequencies, power levels and modulation techniques for short-range wireless systems with implications for the safety of human life.

The introduction of a wireless function will change the ELECTROMAGNETIC ENVIRONMENT, so it is applicable to confirm the compatibility of the ME EQUIPMENT or ME SYSTEM to have sufficient IMMUNITY at the frequencies of wireless operation, plus techniques and measures such as (for example) those in this document, which help ensure that even if the IMMUNITY is insufficient for any reason, BASIC SAFETY and ESSENTIAL PERFORMANCE are maintained.

With regard to wireless coexistence: at this time there are limited consensus standards addressing the RISKS associated with inadequate wireless coexistence. Most current methods of evaluating wireless coexistence use test methods (in situ or special tests) that vary widely among device MANUFACTURERS. Moreover, current ELECTROMAGNETIC COMPATIBILITY (EMC) standards often do not specify requirements or test PROCEDURES to assess the performance of systems containing RF receivers in the presence of in-band interference.

Mitigation: Where the heartbeat signal is lost, a specified signal is generated and input to the system. If during the time available the heartbeat signal is re-established, log this in the EDR (if one is available) and continue operation as usual.

If during the time available the heartbeat signal is not re-established, log in the EDR (if one is available) and apply an appropriate response that is specified in the documentation and that maintains BASIC SAFETY and ESSENTIAL PERFORMANCE.

However, by using electromagnetically diverse redundant channels (see A.2.4) it might be practicable to continue safe operation by switching from the failed wireless link to another data communication link that is still operating correctly.

Successful coexistence among wireless devices is dependent on three main factors: time, frequency, and space. In terms of time, the probability of coexistence increases as the overall channel occupancy of the wireless channel decreases. In terms of frequency, the probability of coexistence increases as the frequency separation of channels increases between wireless networks. In terms of space, the probability of coexistence increases as the signal-to-noise ratio (SNR) increases.

To achieve a successful coexistence, it is necessary to at least control one of the three parameters, two it is even better, the three being the ideal.

The ANSI C63.27 standard [558] provides an evaluation PROCEDURE and supporting test methods for wireless coexistence and evaluation of key performance indicators (KPI). The standard will provide evaluation PROCEDURES, test methods and other guidance necessary for performing the evaluation. AAMI TIR 69-2017 [559] complements C63.27 [558] for RISK ASSESSMENT and management.

NOTE Also see A.6.

A.3.27 Good electromagnetic engineering at every level of design

Aim: To use accepted, good electromagnetic engineering practices at the time of system implementation so that a first line of defence against EM DISTURBANCES is provided.

Description: Well-proven and widely accepted good electromagnetic engineering design practices at the time of system implementation are applied at every level of design as appropriate, including (but not limited to) partitioning printed circuit boards (PCBs), units/modules/subassemblies/products, systems, installations, networks, etc. into different electromagnetic zones (see [24]), and also into lightning protection zones (usually the same as the electromagnetic zones) see [36], segregated by physical space and/or other electromagnetic mitigation techniques.

Identification: Design assessment by persons competent in the relevant electromagnetic design issues.

Mitigation: By competent correction of the design, as appropriate. Examples include:

a) electronic/electrical design appropriate for each electromagnetic zone;

b) selection of electronic, electromechanical, and electrical components appropriate for each electromagnetic zone;

c) communications design (within and between electromagnetic zones);

d) PCB design and layout (often incorporates several electromagnetic zones);

e) power converter design e.g. AC to DC, DC to DC, DC to AC, AC to AC (generally located at electromagnetic zone boundaries);

f) ENCLOSURE design for units/modules/subassemblies and products (could incorporate several electromagnetic zones);

g) mitigation techniques such as filtering, shielding, galvanic isolation, surge, and transient suppression, etc. (located at electromagnetic zone boundaries);

h) system design (generally incorporates several electromagnetic zones); and

i) installation and network design (always incorporating several electromagnetic zones).

References:

For circuits, units, modules, subassemblies, products, etc., see the bibliography under “Good EMC engineering for individual items of equipment”.

For cabinets, systems, installations, networks, etc., see the bibliography under “Good EMC engineering for systems and installations”.

The "Electromagnetic Zoning" technique [24] and guides based upon it: [21] to [23].

A.3.28 Design to comply with EMC test specifications as set out in A.1.3 and A.1.4

Aim: To help ensure that the ME EQUIPMENT or ME SYSTEM will comply with the EMC test specifications as set out in A.1.3 and, if relevant, A.1.4, during VERIFICATION and validation (see A.5.2) if/when they are tested.

Description: It is applicable to design the ME EQUIPMENT or ME SYSTEM to aim to comply with the EMC test specifications as set out in A.1.3 and, if relevant, A.1.4, when the VERIFICATION and validation tests (see A.5.2) are performed.

Identification: Achieved through regular assessment by personnel who are competent in the electromagnetic design of the relevant hardware and/or software, commensurate with the level of RISK.

Mitigation: Modification of the design, followed by re-assessment, until the appointed assessors are satisfied.

A.3.29 De-rating of hardware components, where appropriate

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

Description: Hardware components are operated at levels well below their specified maximum ratings or stress levels, so as to help ensure their correct function despite aging/degradation of performance.

As a rule, EMI suppression/protection components are especially conservatively RATED to survive repeated stress levels considerably higher than the worst anticipated, taking into account the full range of all reasonably foreseeable physical and climatic environments throughout the EXPECTED SERVICE LIFE (such as vibration, shock, humidity, extremes of ambient temperature (for example, when the air-conditioning has failed), etc.).

Identification: Achieved through independent assessment of the design by personnel who are competent (according to the RISK level) in the field reliability of the hardware components concerned.

Mitigation: By modification of the design, followed by re-assessment, until the appointed assessors are satisfied.

A.3.30 Improve robustness of interrupts

Aim: To help reduce the impact of CPU saturation and program execution lock-up due to EMI through interruptions.

Description: Interrupts are provided by circuits external to the processor running the software, and as such are liable to suffering sufficient coupling of EM DISTURBANCES to cause a false signal. Where an interrupt is not masked or otherwise disabled, such EMI will have an immediate effect on the software.

Because of its effect on software execution, a false signal (e.g. due to EMI) on an interrupt pin of a processor is very much more likely to impact reliability of functionality than similar false signals on most other types of processor inputs, all outputs, and power supply pins.

Identification: Whilst most of the advantages of using interrupts are associated with optimization of the hardware resources and achieving consistent response times, some benefits in robustness, and reliability, can also be attained by effective use of the internal interrupt mechanisms, which are sometimes called exceptions and traps.

EM DISTURBANCES can potentially increase the input data rate, which can saturate and lock-up the CPU, causing loss or corruption of data, inhibiting other part of system from executing failure modes, fallback operation, or the normal control operations. In effect, EM DISTURBANCES can potentially cause a "denial of service" to the interrupt servicing.

Mitigations:

a) Limit the use of interrupts only to what is necessary: reduce external interrupt inputs, reduce levels of interrupts, and reduce the rates of interrupts.

b) Provide electronic filtering (analogue and/or digital) to control slew-rate, de-bounce and reduce the bandwidth of potential interrupts.

c) Use edge or level triggering in conjunction with a level control at the beginning of interrupt routine to filter the unwanted / parasitic interrupts.

d) It is recommended that use memory protection and user / supervisor mechanism; interruption routines are executed only in privileged supervisor / system / kernel mode.

e) Control the use of the Enable and Disable interrupt instructions and use only matched pairs.

f) Disable interrupts during power-up initialization.

g) Disable and mask-out unused interrupt vectors. It is recommended that unused vectors point to an error handling routine or reset, as appropriate.

h) Use "atomic" Test-and-Set instructions or signalling mechanism, such as semaphores, to protect and mark as "in-use" any common resources.

i) Confirm that each interrupt and all interrupts together will not deadlock the system and inhibit the liveliness of the system.

j) Use an independent observation technique to detect and react to a lock-up.

k) Use a watchdog timer to free lock-up situations: the watchdog can never be "kicked" from an interrupt routine.

l) Confirm that calculations of CPU usage level and the specific impact of all the expected worst-case instances of all interrupt servicing can be met, with a safe margin of spare CPU capacity (typically of the order of 30 %).

A.4 Techniques and measures that might be helpful in implementation, integration, installation, and commissioning

A.4.1 Providing information on constraints and additional measures

Aim: To aid procurement, installation, and commissioning in accordance with the relevant design specification for adequate mitigation of the effects that can be caused by EM DISTURBANCES.

Description: It is recommended that the design specification for ME EQUIPMENT or an ME SYSTEM is based upon its operation in a specified ELECTROMAGNETIC ENVIRONMENT, or one that is less severe. The actual achievement of that specified ELECTROMAGNETIC ENVIRONMENT, or one that is less severe, might rely on certain constraints or additional measures being used during installation. Improvements to the lightning protection system of the site are a common example.

Identification: Achieved through the assessment of the intended operational site and its characteristics by personnel who are competent in the relevant site-related issues, commensurate with the RISK level.

Mitigation: By modification of the design, followed by re-assessment, until the appointed assessors are satisfied.

Measures include, but are not limited to, the provision of information on:

a) any constraints on the physical positioning of the items of equipment that comprise the ME EQUIPMENT or ME SYSTEM;

b) any constraints on types, lengths and routing of power, control, and signal interconnecting cables;

c) the methods to be used when terminating any cable screens (shields);

d) the types of connectors to be used and any special assembly needs;

e) the electrical power supply specifications (power quality);

f) any additional screening (shielding) that is needed, and how to install it;

g) any additional filtering that is needed, and how to install it;

h) any additional overvoltage and/or overcurrent protection that is needed, and how to install it (for example, by referencing the appropriate specifications in all applicable parts of IEC 62305);

i) any additional power conditioning that is needed (such as a reliable UPS);

j) any additional ELECTROSTATIC DISCHARGE protection needs (such as control of humidity);

k) any additional physical protection needs (for example, against the possibility of unusual physical and/or climatic conditions);

l) the earthing (grounding) and bonding needs of the installation;

m) the PROCEDUREs and materials to be used;

n) any protection against corrosion and its effects throughout the EXPECTED SERVICE LIFE; and

o) any OPERATOR/maintainer constraints, for example, the use of mobile phones or cellphones whilst performing commissioning or maintenance.

In addition: it is recommended that proper installation and commissioning, having regard to the constraints and additional measures listed above (and any others not listed above), is competently verified before the system is first operated (see A.5.4) and thereafter checked regularly throughout the EXPECTED SERVICE LIFE, depending on the specifications for maintaining BASIC SAFETY and ESSENTIAL PERFORMANCE (see A.6.2).

A.4.2 Procuring materials, components, and products

Aim: To help confirm that all materials, components and products are procured according to their specifications for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES, which will help to confirm that the ME EQUIPMENT or ME SYSTEM will comply with the EMC test specifications from A.1.3 and A.1.4, during VERIFICATION and validation (see A.5.2).

Description: Substandard or counterfeit materials, components and products are increasingly appearing in supply chains, especially when purchased on the "grey market" (an activity that this document does not recommend). Such components can threaten the adequate mitigation of the effects that can be caused by EM DISTURBANCES.

Identification: By regular quality audits on goods received during the project.

Audits are typically carried out by personnel who are competent in the relevant quality control issues for the types of goods concerned in each case, commensurate with the RISK level.

It is recommended that appropriate tests (see A.5.2 and, if appropriate, A.5.3) are applied to verify suppliers' claims of compliance with specifications, the rate of which depends on the acceptable quality level (AQL) chosen in each case.

Such tests are recommended in general to avoid substandard or counterfeit materials, components, and products from being incorporated in the ME EQUIPMENT or ME SYSTEM.

EXAMPLE 1 In the military avionics industry, it is not unknown to hear claims that suppliers' build quality slips by enough to cause failure to meet specifications after seven units have been manufactured. Detecting the failure and ensuring that the supplier corrects the problem is claimed to typically result in a further failure to meet specification, another seven units later.

EXAMPLE 2 The US Department of Defense has found counterfeit components in every weapons system; and in response has created a Regulation which all its suppliers now have to comply with, to try to prevent counterfeits from entering the military supply chain [9].

Mitigation: Replacement of the out-of-specification materials, components or products with in-specification materials, components or products that satisfy the appointed inspectors before they are assembled.

A.4.3 Assemble/integrate according to the design for adequate mitigation of the effects that can be caused by EM DISTURBANCES

Aim: To help confirm that the correct materials, components, and products are used in the correct ways so that the ME EQUIPMENT or ME SYSTEM is assembled and integrated according to their design specifications for helping to achieve adequate mitigation of the effects that can be caused by EM DISTURBANCES.

To help confirm that good electromagnetic engineering practices are used (see A.3.26) as appropriate during assembly and integration.

To help confirm that the ME EQUIPMENT or ME SYSTEM will comply with the EMC test specifications as set out in A.1.3 and A.1.4, during VERIFICATION and validation (see A.5.2).

Identification: By regular quality audits and/or assessments by personnel who are competent in the assembly/integration activities concerned, commensurate with the level of RISK.

Mitigation: Replacement of incorrect materials, components, or products, and/or reworking of incorrect assembly or integration, as needed, to satisfy the appointed assessors.

A.4.4 Install/commission according to the design for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES

Aim: To help confirm that the correct installation and commissioning methods are used for the ME EQUIPMENT or ME SYSTEM according to their associated design specifications for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES.

To help confirm that good electromagnetic engineering practices are used (see A.3.25) as appropriate during installation and commissioning.

To help confirm that the ME EQUIPMENT or ME SYSTEM will comply with the EMC test specifications from A.1.3 and A.1.4 during VERIFICATION and validation (see A.5.2).

Description: The design of ME EQUIPMENT or an ME SYSTEM will have assumed or specified that its installation and commissioning will be performed in a certain way, to help achieve adequate mitigation of the effects that can be caused by EM DISTURBANCES. Consequently, it is important that installation and commissioning are performed as was assumed or specified by its designers.

Identification: By regular quality audits and/or assessments by personnel who are competent in the installation/commissioning activities concerned, commensurate with the level of RISK.

Mitigation: Reworking of incorrect installation or commissioning as needed to satisfy the appointed assessors.

A.5 Techniques and measures that might be helpful in VERIFICATION and validation (including testing)

A.5.1 Applying VERIFICATION and/or validation techniques and measures

Aim: To verify and/or validate as far as is practicable that the design techniques and measures that have been applied function according to the relevant design specification created as described in A.1.

Description: The VERIFICATION and validation of ME EQUIPMENT or an ME SYSTEM will have been specified by the designers as described in A.1, to help achieve adequate mitigation of the effects that can be caused by EM DISTURBANCES. Consequently, it is important that all VERIFICATION and validation activities are performed exactly as specified in A.1.

Identification: By performing a sufficient number of techniques listed below, or equivalent techniques described in the documentation, to enable different types of weaknesses or omissions in the design to be discovered.

The competency, measurement accuracy and measurement uncertainty needed for each VERIFICATION or validation technique is appropriate to be commensurate with the RISK level.

VERIFICATION applies these techniques to all components, sub-assemblies, etc. of the ME EQUIPMENT or ME SYSTEM.

Where the component or sub-assembly is a third-party item, its MANUFACTURER might have performed some or all of these techniques and documented their results in the item's safety documentation.

Validation applies these techniques at the highest practicable level of assembly of the ME EQUIPMENT or ME SYSTEM.

Failure prediction techniques can be helpful for quantitative RISK ASSESSMENT, when the RISK cannot be shown to be tolerable through other qualitative means.

Typical quantitative techniques include:

a) failure modes and effects analysis (FMEA);
b) failure modes, effects, and criticality analysis (FMECA);
c) cause-consequence diagrams;
d) event tree analysis (ETA);
e) fault tree analysis (FTA); and
f) fault tree models.

Examples of VERIFICATION and validation techniques include:

a) demonstrations, such as demonstrating that the BASIC SAFETY and ESSENTIAL PERFORMANCE have been achieved, using any appropriate methods.
b) checklists, to help confirm that design techniques and measures have been observed, applied, and implemented correctly.
c) inspections, to help confirm that the designs for assembly and installation have been correctly followed.
d) reviews and assessments, to help confirm compliance with the objectives of each phase of the EXPECTED SERVICE LIFE. These are usually performed by competent persons on each phase of the EXPECTED SERVICE LIFE and the various stages of the activities within each phase.
e) independent reviews and assessments. The degree of independence of the assessment being commensurate with the SEVERITY of RISK which has been determined by the MANUFACTURER, for example by applying Annex C in ISO TR 24971:2020 [3].
f) audits, which include VERIFICATION processes for specification, design, assembly, and installation.
g) "walk-throughs" of normal operation and plausibly abnormal operations (sometimes called "devil's advocacy").

h) individual and/or integrated hardware tests. Different parts of the final assembly or system are assembled step by step, with checks and tests applied to help confirm that they function correctly at each step.

i) validated computer modelling, simulation, etc.

j) the normal EMC tests applied in accordance with A.5.3 can be modified to provide greater coverage of the possible effects of EMI, as described in [651], [601] and [602]; also see A.5.4.

k) third party safety certification complying with the guidance in this document, at component, module, product or system level, examples: integrity of data, wireless standard, encryption, etc.

Mitigation: Changes are made to the design or operation to eliminate the weaknesses or omissions, and the relevant VERIFICATION or validation re-applied.

It is recommended that preceding phases of the EXPECTED SERVICE LIFE are reviewed if they can be affected by the changes. It is recommended that consideration be given as to whether similar weaknesses or omissions might be present in other, similar functions. If so, it is recommended that similar changes are made to those functions.

This PROCESS is repeated until the appointed assessors are satisfied. It is recommended that the decisions made and actions taken in this regard are described in detail in the documentation.

These quantitative techniques were not originally developed to deal with the effects of EMI, so they need to be competently modified to take into account the issues mentioned in A.1.2.

NOTE Because there can be multiple orthogonal (i.e. independent) effects acting on equipment, Taguchi's "Design of Experiments" approach [771] can help improve tests for robustness by quickly determining the worst cases to be tested.

References: See the list in the bibliography under “VERIFICATION/validation and other techniques (not specifically related to EM DISTURBANCES)”, especially [746].

A.5.2 VERIFICATION testing to the EMC test plan from A.1.3 and A.1.4

Aim: To help confirm that the ME EQUIPMENT or ME SYSTEM complies with the EMC test specifications from A.1.3 and, if appropriate, A.1.4.

Description: An EMC test plan that helps to achieve adequate mitigation of the effects that can be caused by EM DISTURBANCES, will have resulted from the activities described in A.1.3, and perhaps A.1.4 too. Consequently, it is important that these test plans are performed exactly as specified.

Identification: By performing tests in accordance with the EMC test plan(s) created by applying A.1.3 and (if appropriate) A.1.4, using competent test personnel using calibrated test equipment and facilities.

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

Care is typically taken over the order of tests, for example, performing EMISSIONS after IMMUNITY to reveal whether seals or protection have been "softened" during the IMMUNITY test.

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 level of RISK.

Mitigation: Modification of the ME EQUIPMENT or ME SYSTEM, followed by re-VERIFICATION and/or re-validation of the failed tests.

Depending on the tests which were failed, and the modifications needed to achieve passes to them, it is applicable to redo other EMC tests, possibly all of them.

This PROCESS is repeated until the appointed assessors are satisfied.

It is recommended that the decisions made and actions taken in this regard are described in detail in the documentation.

NOTE Complying with the conventional test standards alone is insufficient for adequate mitigation of the effects that can be caused by EM DISTURBANCES (see Clause 1 and References [11] to [14]).

A.5.3 Using non-standardized ad hoc checks or tests

Aim: To help confirm that the ME EQUIPMENT or ME SYSTEM or any component part or subsystem of it has adequate mitigation of the effects that can be caused by EM DISTURBANCES, appropriate to the level of RISK.

Description: Complying with the EMC tests specified by A.1.3 and (if appropriate) A.1.4 is necessary for maintaining sufficiently high levels of availability of the normal functions of the ME EQUIPMENT or ME SYSTEM so that OPERATORS or owners are not inclined to modify them in order to achieve productivity targets.

Of course, this is very important for adequate mitigation of the effects that can be caused by EM DISTURBANCES, but no affordable or practicable EMC test plan can possibly demonstrate that EM DISTURBANCES cannot unacceptably degrade the BASIC SAFETY or ESSENTIAL PERFORMANCE.

Using a suitable number of design techniques and measures is what makes it possible for BASIC SAFETY and ESSENTIAL PERFORMANCE not to be degraded by EM DISTURBANCES over the EXPECTED SERVICE LIFE. A.6.1 lists techniques and measures that can be used to verify or validate this.

Non-standardized or ad hoc checks or tests can be used in addition to the list in A.5.3 to achieve the necessary confidence in the design for adequate mitigation of the effects that can be caused by EM DISTURBANCES, according to the RISK level.

In many situations they can prove very useful in assessing the design for the mitigation of the effects that can be caused by EM DISTURBANCES.

Identification: By performing non-standardized or ad hoc checks or tests.

It is recommended that any non-standard ad hoc test methods are justified by recording the following in the documentation:

a) Rationale.
b) What measurements are needed? What is the purpose of measuring it? Why is a non-standard ad hoc test being proposed rather than a standards-based method?
c) A detailed explanation of the test method.
d) Including figures or photographs and its theoretical underpinning
e) A demonstration of validity of this non-standard ad hoc test.
f) (If it is not immediately obvious to an engineer competent in testing the issue concerned).

Examples of some non-standard ad hoc checks and tests include:

a) significantly increasing the test levels of standard IMMUNITY tests;

b) modulating continuous wave disturbances with frequencies, pulse shapes or patterns, or wave shapes to which a design might be especially susceptible (from inspection/investigation of the design);

c) applying two or more disturbances at once (for example, multiple frequencies during conducted or radiated tests to cause intermodulation in the tested design);

d) applying different wave shapes on transient tests (such as surge, ESD, etc.);

e) performing significantly larger numbers of transient tests to cover a greater proportion of the range of possible equipment states;

f) checks on earthing, grounding, and bonding by, for example, measurement with appropriate DC meters and/or visual inspections;

g) checking that temperature and humidity sensors are functioning correctly (to help prevent corrosion of shielding, overheating of filters, etc.);

h) checking the behaviour of shielding joints and gaskets during physical stress (for example, non-flat mounting surface), mechanical shocks, vibration, temperature changes, temperature extremes, condensation, icing, changes in air pressure (or water pressure for underwater equipment), etc., for example, by using battery-powered "comparison noise emitters" inside an ENCLOSURE, and close-field probes outside it, within an environmental test chamber.

i) quick checks of EMISSIONS and IMMUNITY performance for units that have undergone highly accelerated simulations of their likely exposure to mechanical, climatic, chemical, etc., environments and/or user interactions (for example, opening/closing doors, hatches, inspection panels, etc.) throughout their EXPECTED SERVICE LIFE.

Mitigation: Modification of the ME EQUIPMENT or ME SYSTEM, followed by re-VERIFICATION and/or re-validation of the failed checks or tests.

Depending on which checks or tests were failed, and the modifications needed to achieve passes to them, it is applicable to redo other checks or tests, or even standards-based testing.

This PROCESS is repeated until the appointed assessors are satisfied. It is recommended that the decisions made and actions taken in this regard are described in detail in the project documentation.

References: [600] to [604] in the bibliography under “Some ad-hoc test methods”.

NOTE A manufacturer is not precluded from doing these tests personally or constrained to use certain types of third-party test laboratories.

The degree of accuracy, confidence, and independence needed for these non-standard ad hoc checks and tests is – like most BASIC SAFETY or ESSENTIAL PERFORMANCE issues – generally dependent on the level of the RISK.

A.5.4 Verifying correct installation and commissioning

Aim: To help confirm proper installation and commissioning having regard to the constraints and additional measures listed as the result of applying A.4.1 and A.4.2, and any others not listed in those subclauses.

This is essential for "version control" of the finished as-built system, listing all the hardware and software parts that are used together as a "working set" to fulfil the BASIC SAFETY and ESSENTIAL PERFORMANCE objectives throughout the EXPECTED SERVICE LIFE.

Description: The designers of ME EQUIPMENT or an ME SYSTEM will have specified that its correct installation and commissioning will be verified in a certain way, to help confirm the achievement of sufficient mitigation of the effects that can be caused by EM DISTURBANCES. Consequently, it is important that the installation and commissioning are verified exactly as specified by its designers.

Identification: Inspection by competent personnel before the system is first operated and checked regularly throughout the EXPECTED SERVICE LIFE.

Mitigation: Modification of the ME EQUIPMENT or ME SYSTEM, followed by re-inspection, repeated until the appointed assessors are satisfied.

It is recommended that the decisions made and actions taken in this regard are described in detail in the documentation.

A.5.5 EMC tests before and after accelerated life tests

Aim: To help confirm that adequate mitigation of the effects that can be caused by EM DISTURBANCES is effective during and after accelerated life tests.

Description: Testing environments that simulate the reasonably foreseeable locations of use of ME EQUIPMENT or an ME SYSTEM are recommended to verify that adequate mitigation of the effects that can be caused by EM DISTURBANCES is maintained throughout the EXPECTED SERVICE LIFE.

Identification: When these tests are carried out, the mitigation of the effects that can be caused by EM DISTURBANCES can be evaluated both *before* and *after* the life tests; and some EMC tests might be able to be combined with the lifetime tests. Following the tests, it is necessary to evaluate whether the EMC performance has not been degraded, which can lead to an unacceptable RISK.

Mitigations:

a) Link to calculations of reliability on sensitive components whose characteristics can vary over time (e.g. capacitors).

b) Selection of components with appropriate electrical and thermal properties.

c) The tolerance of the components (e.g. value, voltage) can be chosen carefully taking into account aging.

d) It is recommended that particular attention is paid to the EMC seals of cabinets, racks, doors, connectors, and openings; because repeated handling can degrade their EMC performance over time.

e) The fixing points and electrical connection undergoing corrosion can be adapted and protected.

f) The life test profiles can take into account the environmental constraints of the intended or foreseeable environment (s).

A.6 Techniques and measures that might be helpful in operation, maintenance, repair, overhaul, refurbishment, and upgrade

A.6.1 Assessment of changes in the ELECTROMAGNETIC ENVIRONMENT

Aim: To discover new ELECTROMAGNETIC ENVIRONMENT conditions that were not taken into account in the original design.

To modify/upgrade as appropriate so that availability is maintained at a high level (as discussed in A.1.3).

Description: It is recommended that the design specification for ME EQUIPMENT or an ME SYSTEM is based upon their eventual operation in a specified ELECTROMAGNETIC ENVIRONMENT (or one that is less severe) throughout the EXPECTED SERVICE LIFE.

The achievement of that specified ELECTROMAGNETIC ENVIRONMENT, or one that is less severe, throughout the EXPECTED SERVICE LIFE is important for availability and needs the ELECTROMAGNETIC ENVIRONMENT to be managed, specifically in this case to identify and assess any changes in it. Ideally, proposed changes would be assessed before they were implemented, and modified if applicable, so as not to degrade the availability.

Identification: This is achieved by analysing the following, at least:

a) changes in the EMC test standards used in the specification (see A.1.3 and A.1.4).

b) changes in the standards listed in the bibliography under “Assessing the ELECTROMAGNETIC ENVIRONMENT, and detecting threats”.

c) results from independent detection of EM DISTURBANCES as described in A.2.9.

d) results recorded as described in A.2.6, and then analysed.

e) the assessment techniques described in A.1.3 and [650].

f) proposed changes in the ME EQUIPMENT or ME SYSTEM, or other equipment/systems that could affect inter-system or intra-system electromagnetic energy couplings into the ME EQUIPMENT or ME SYSTEM.

These proposed changes could be upgrades, repairs, overhauls, or any modifications for any reasons.

It might be useful to perform a "gap analysis", comparing the ELECTROMAGNETIC ENVIRONMENT that was the basis of the original design specification (see A.1), with the current ELECTROMAGNETIC ENVIRONMENT.

Mitigation: By re-applying the appropriate parts of the PROCESS recommended by this document, as appropriate to the changes in the ELECTROMAGNETIC ENVIRONMENT, for example in accordance with the approach taken by ISO 14971 in such circumstances.

This PROCESS is repeated until the appointed assessors are satisfied.

It is recommended that the decisions made and actions taken in this regard are described in detail in the documentation.

A.6.2 Assessment of continuing correct installation

Aim: To help confirm the maintenance of proper installation and commissioning having regard to the constraints and additional measures listed as the result of applying A.4.1, and any others not listed in that section.

Description: The design of ME EQUIPMENT or an ME SYSTEM will have assumed or specified that its installation be performed in a certain way, to help achieve adequate mitigation of the effects that can be caused by EM DISTURBANCES.

Because adequate mitigation of the effects that can be caused by EM DISTURBANCES is needed throughout the EXPECTED SERVICE LIFE, it is important that installation continues to have the same characteristics throughout the EXPECTED SERVICE LIFE as were assumed or specified by its designers for its initial installation.

Identification: Regular inspections by competent personnel throughout the EXPECTED SERVICE LIFE.

These inspections can include, for example: grounding/bonding; shielding effectiveness; filter insertion loss; the condition of surge protection components/devices and electromagnetic shielding gaskets; unapproved modifications (including cable/connector replacements and/or additions, software upgrades or other changes); etc.

EXAMPLE A common example is conductive gaskets used to seal apertures in shielding ENCLOSURES, and dissimilar metal bonds (such as earth/ground connections). These are often subject to corrosion that progresses over time until they no longer function well-enough to maintain adequate mitigation of the effects that can be caused by EM DISTURBANCES.

Another example is surge protection components and/or devices, which generally degrade as time progresses due to the surges they experience, until they can no longer provide adequate protection.

Note that these surge protection components/devices and earth/ground bonds might be located remotely from the electronics of the ME EQUIPMENT or ME SYSTEM – for example, they might be installed as part of a site or vehicle's lightning and/or EMP protection system, and yet the adequate mitigation of the effects that can be caused by EM DISTURBANCES of the ME EQUIPMENT or ME SYSTEM can still rely on the protection they provide.

Mitigation: Modification of the ME EQUIPMENT or ME SYSTEM, followed by re-inspection, until the correct constraints and additional measures are once again satisfied.

Preventative maintenance also can be used wherever any aspect of the installation appears to be suffering from degradation of its electromagnetic characteristics at such a rate that they could become unacceptable before the next planned inspection.

Where the periodicity of the planned inspections is found to be inadequate to prevent certain electromagnetic characteristics from degrading by too much, it is recommended that the planning is changed to inspect at least those characteristics sufficiently often that their degradation is corrected before they have degraded to the point of unacceptability.

NOTE This activity is another essential for the "version control" of the as-built system (see A.5.4).

A.6.3 Maintaining adequate mitigation of the effects that can be caused by EM DISTURBANCES, despite modifications or changes

Aim: To help ensure that repairs, modifications, overhauls, upgrades, refurbishment, etc. do not unacceptably degrade the mitigation of the effects that can be caused by EM DISTURBANCES of the ME EQUIPMENT or ME SYSTEM.

Description: Repairs, modifications, overhauls, upgrades, refurbishments, etc. can cause significant degradations to the mitigation of the effects that can be caused by EM DISTURBANCES of a system. For example, even replacing a cable with a different one, even if supposedly of the same type, can cause unacceptable degradation of ELECTROMAGNETIC EMISSIONS and/or IMMUNITY.

It is recommended that such issues are foreseen and taken care of in the planning (see A.1.2), so that even if the ME EQUIPMENT or ME SYSTEM becomes unavailable as a result, it does not become unsafe.

This activity is another essential for the "version control" of the as-built system (see A.5.4).

Identification: By re-applying the parts of the PROCESS described in this document that are appropriate to the proposed changes to the ME EQUIPMENT or ME SYSTEM (for example in accordance with the approach taken by the applicable clauses of ISO 14971 in such circumstances).

Mitigation: Implement whatever the above PROCESS shows to be necessary – whether in specifications, system design, detailed techniques and measures, VERIFICATION/validation, etc. – to help ensure that the repairs, modifications, upgrades, refurbishment, etc. do not unacceptably degrade the mitigation of the effects that can be caused by EM DISTURBANCES of the ME EQUIPMENT or ME SYSTEM.

A.6.4 Batch (lot) traceability

Aim: to help analysis of the root cause of the problem caused by EM DISTURBANCES and containment by identifying product at RISK.

Description: Critical components for the achievement of adequate mitigation of the effects that can be caused by EM DISTURBANCES are identified, and it is recommended that their MANUFACTURERS / distributors provide traceability; this concerns the electronic components, printed circuit boards, power modules, displays, cables, specific electronic modules, etc.

Identification: If a concern does arise in volume production, it is essential to contain the situation by being able to identify the product at RISK efficiently.

ISO 9000:2015 [18] and other industry quality standards aim to be able to trace all materials through the production PROCESS.

Mitigation: It is recommended that the MANUFACTURER / distributor of the component codes (e.g. using barcodes, RFID tags, silicon fuses, embedded memories, DNA, etc.) all product such that the component parts can be tracked back to their respective delivery date. If properly designed, these codes can provide sufficient information to the MANUFACTURER to able to trace the parts through its system.

A.6.5 Component changes, new supplier, dual / alternate source

Aim: To preserve the design for the adequate mitigation of the effects that can be caused by EM DISTURBANCES, when replacing components due to changes in specifications or PROCESS, a reference change, a change of supplier, or obsolescence.

Description: Assess the EMC criticality of the component and if critical request samples and perform the following tests at component or assembly level:

a) High temperature and/or humidity functional tests
b) Low temperature and/or humidity functional tests
c) Ramps between temperature extremes
d) Vibrations
e) High supply voltages
f) Low supply voltages
g) ELECTROMAGNETIC EMISSION tests
h) ELECTROMAGNETIC IMMUNITY tests

Combine the tests if applicable.

Identification: These unit tests of characterization do not replace tests on the final product; they help to confirm that the new component conforms to equivalent, or better specifications, and help to confirm a sufficient level of confidence about the complete product before re-test if applicable.

See also Reference [731] on obsolescence management.

Mitigation: If a changed or new component, or the same component from a new supplier or alternate source fails to comply with all of the test specifications for a component that is critical for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES, ensure that component will not be purchased or used but an alternative sought that does comply with all of the test specifications.

Where an alternative is not available, it might be possible to redesign so that an available component can be used whilst still achieving the necessary mitigation of the effects that can be caused by EM DISTURBANCES. It is recommended that such redesign go back to the earliest stage in the overall project PROCESS to confirm that all necessary changes to any/all related aspects of the design; specifications; test plans; VERIFICATION and validation methods; maintenance; overhaul, and repair techniques, etc., are made to accommodate the component concerned to achieve the necessary mitigation of the effects that can be caused by EM DISTURBANCES, and to help confirm that it will be maintained throughout the EXPECTED SERVICE LIFE.

A.7 Techniques and measures that might be helpful in decommissioning

Aim: To help ensure the maintenance of adequate mitigation of the effects that can be caused by EM DISTURBANCES throughout any decommissioning, dismantling, or disposal PROCESSES.

Description: Since safety is expected to be maintained throughout the EXPECTED SERVICE LIFE, plus decommissioning, it is useful to ensure that dismantling and/or disposal does not cause unacceptable safety RISKS due to degradation of the mitigation of the effects that can be caused by EM DISTURBANCES, when ME EQUIPMENT or an ME SYSTEM is being degraded by the dismantling and/or disposal PROCESS even while those functions are still needed.

Where it is not practicable to remove all power supplies (of any type: electrical, pneumatic, hydraulic, etc.) from ME EQUIPMENT or an ME SYSTEM, or when the ME EQUIPMENT or ME SYSTEM itself contains significant amounts of stored energy (electrical, pneumatic, hydraulic, nuclear fissionable or explosive materials, etc.), BASIC SAFETY or ESSENTIAL PERFORMANCE could be considered to be maintained in full operation until safe disposal has been achieved.

EXAMPLE Certain types of batteries need controlled rates of charge and discharge if they are not to overheat and rupture, which would cause various kinds of safety HAZARDS. In smaller batteries (such as laptop computers) these charge control systems are built-into the battery, but they might be external items.

It can be applicable for a charge/discharge control system to remain in full working order at all times for reasons of BASIC SAFETY or ESSENTIAL PERFORMANCE, right up to the point of final disposal.

Identification: By re-applying the appropriate parts of the PROCESS described in this document to the proposed dismantling and/or disposal project (for example, in accordance with the approach taken by ISO 14971 in such circumstances.)

Mitigation: Implement whatever the above PROCESS shows to be necessary – whether in specifications, system design, detailed techniques and measures, VERIFICATION/validation, etc. – to help ensure that the dismantling and/or disposal project does not unacceptably degrade the necessary mitigation of the effects that can be caused by EM DISTURBANCES of each ME EQUIPMENT or ME SYSTEM concerned.

NOTE Dismantling and disposal might mean that the exposure of workers and/or the public to the foreseeable safety HAZARDS is different from the operational stage of its EXPECTED SERVICE LIFE, and this might affect its BASIC SAFETY or ESSENTIAL PERFORMANCE. Its specifications for BASIC SAFETY or ESSENTIAL PERFORMANCE during the decommissioning stage might be higher or lower than during operation, for example. A change in BASIC SAFETY or ESSENTIAL PERFORMANCE will (of course) influence the PROCESS described in this document.

A.8 Integrating third-party items into ME EQUIPMENT or ME SYSTEMS

A.8.1 The general iterative approach

Figure A.1 shows an example of the iterative PROCESS by which volume-manufactured commercially available standard products are chosen for incorporation into ME EQUIPMENT or an ME SYSTEM based upon the specifications for adequate mitigation of the effects that can be caused by EM DISTURBANCES of the ME EQUIPMENT or ME SYSTEM (see A.1).

As Figure A.1 shows, it can be necessary for the designer(s) to iterate the design of the electromagnetic mitigation measures, or even add new electromagnetic zones to create suitable ELECTROMAGNETIC ENVIRONMENTS for the chosen standard products.

In practice, this means that the detailed design of the ME EQUIPMENT or ME SYSTEM'S mitigation of the effects that can be caused by EM DISTURBANCES can be modified in order to achieve BASIC SAFETY or ESSENTIAL PERFORMANCE, due to the characteristics of the chosen standard products.

Always remember that designing and realizing any ME EQUIPMENT or ME SYSTEM is usually not a linear progression of steps – iteration (looping back to an earlier project stage) is often needed as the real characteristics become apparent during the design, integration, implementation, installation, VERIFICATION, and validation stages.

Figure A.1 shows:

Step 1: The specifications for the adequate mitigation of the effects that can be caused by EM DISTURBANCES for ME EQUIPMENT or an ME SYSTEM, are developed using the techniques and measures in A.1, comprising the list of EMC tests to be complied with plus a non-exhaustive list of appropriate techniques and measures to be used to achieve adequate mitigation of the effects that can be caused by EM DISTURBANCES.

Step 2: The specifications for the adequate mitigation of the effects that can be caused by EM DISTURBANCES for each of the subsystems or component parts to be used in the ME EQUIPMENT or ME SYSTEM are then developed from the specifications created in Step 1. These comprise a specification for the EMC tests to be complied with, plus a list of appropriate techniques and measures to be used to achieve adequate mitigation of the effects that can be caused by EM DISTURBANCES, taking into account any electromagnetic mitigation provided by the electromagnetic zone in which the subsystem or component part will be located.

Step 3: The specifications for the adequate mitigation of the effects that can be caused by EM DISTURBANCES of an individual subsystem or component part is compared with the information provided by commercial suppliers in their products' safety documentation. It is recommended that these include details of the EMC tests that were complied with, the techniques and measures used to help achieve adequate mitigation of the effects that can be caused by EM DISTURBANCES, and (where continual error-free performance is not confirmed) any PDSs.

Step 4: The standard volume-manufactured subsystems and component parts to be incorporated into the ME EQUIPMENT or ME SYSTEM are chosen from the list of commercial products whose safety documentation meets the necessary specifications and have acceptable PDSs.

It is good practice for the electromagnetic specifications to be included in the purchasing contract.

Also note that it is not recommended to place any reliance on CE Marking (European conformity marking) or MANUFACTURER's certificates/declarations of conformity.

Step 5: Where suitable commercially available products do not comply with the specifications, electromagnetic mitigation measures and/or techniques and measures for mitigation of the effects that can be caused by EM DISTURBANCES can be applied, or existing mitigation, techniques or measures modified, at any level of assembly and in any electromagnetic zone in order to change the specification for the adequate mitigation of the effects that can be caused by EM DISTURBANCES for the individual subsystem or component part in Step 2.

Step 6: Steps 2 to 4 are iterated for each subsystem and component part until compliance is achieved with the specifications for the adequate mitigation of the effects that can be caused by EM DISTURBANCES FOR the ME EQUIPMENT or ME SYSTEM in Step 1.

Step 7: The same process is repeated for every subsystem or component part of the ME EQUIPMENT or ME SYSTEM.

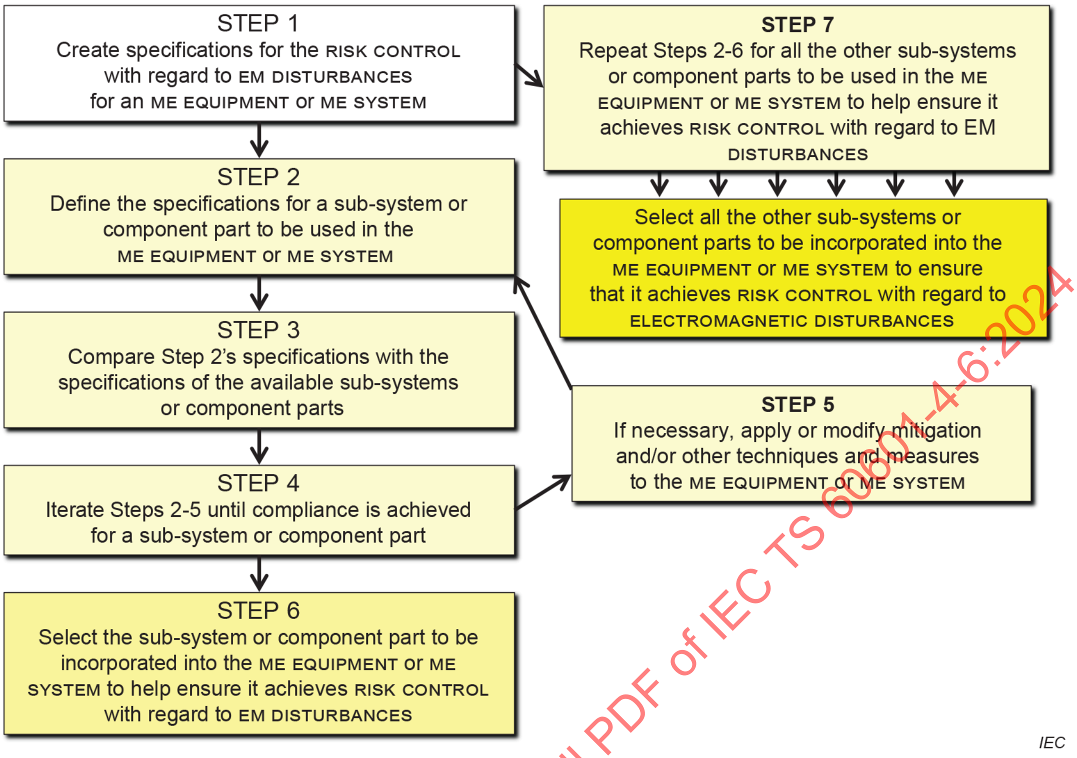
STEP 1
Create specifications for the RISK CONTROL with regard to EM DISTURBANCES for an ME EQUIPMENT or ME SYSTEM
STEP 2
Define the specifications for a sub-system or component part to be used in the ME EQUIPMENT or ME SYSTEM
STEP 3
Compare Step 2's specifications with the specifications of the available sub-systems or component parts
STEP 4
Iterate Steps 2-5 until compliance is achieved for a sub-system or component part
STEP 6
Select the sub-system or component part to be incorporated into the ME EQUIPMENT or ME SYSTEM to help ensure it achieves RISK CONTROL with regard to EM DISTURBANCES
STEP 7
Repeat Steps 2-6 for all the other sub-systems or component parts to be used in the ME EQUIPMENT or ME SYSTEM to help ensure it achieves RISK CONTROL with regard to EM DISTURBANCES
Select all the other sub-systems or component parts to be incorporated into the ME EQUIPMENT or ME SYSTEM to ensure that it achieves RISK CONTROL with regard to ELECTROMAGNETIC DISTURBANCES
STEP 5
If necessary, apply or modify mitigation and/or other techniques and measures to the ME EQUIPMENT or ME SYSTEM
IEC

Figure A.1 – Choosing standard volume-manufactured subsystems and component parts

A.8.2 Suppliers' certifications and electromagnetic assessments

Suppliers' markings, certifications, and declarations (including CE marking with regard to the EMC Directive) result from a "self-declaration" PROCESS. Accordingly, it is recommended that companies involved with integrating any electronic equipment or system take reasonable steps to check whether any markings, certificates or declarations issued by suppliers are reliably correct.

There are many independent assessment bodies that will validate and certify customer's products against their specifications. Using products whose EMC performance specifications are validated by independent assessment bodies is one way of achieving due diligence. Some suppliers are known to forge third-party assessment documents, so it is always a good idea to confirm them with the body purported to be the issuer.

Another way is to investigate suppliers' claims yourself, for example, by requesting test certificates or test reports; checking that they indicate the desired performance; and checking with the test laboratory to see how independent they are. Alternatively, you could perform simple checks, or even full tests, to verify suppliers' performance claims.

In general, the higher the RISK level, the more work is needed to achieve the assurance that purchased or free-issued subsystems or component parts have the electromagnetic characteristics their MANUFACTURERS claim.

A.8.3 Custom-manufactured component parts

In some cases, it could be a quite reasonable solution to pay a supplier of standard products to produce a custom-engineered version that meets the safety-system designers' electromagnetic specification and is provided with believable test results.

A product MANUFACTURER might even be persuaded to make a completely new type of product for use in a certain ME EQUIPMENT or ME SYSTEM.

This is typical of safety-critical electronics in automobiles (for example, anti-lock braking, engine management, etc.) where product volumes are high, justifying considerable investment in products that can be incorporated by the system integrator without having to create special electromagnetic zones for them by adding more electromagnetic mitigation.

The same "custom-designed component" approach might also be appropriate where the ME EQUIPMENT or ME SYSTEM is individually unique or only made in small quantities, and as such are not very price-sensitive.

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

It is recommended that as many copies of Table B.1 are completed as will cover each of the different issues concerned with helping to achieve the basic safety and/or essential performance of the ME EQUIPMENT or ME SYSTEM concerned, see Clause 4 and 5.2.2.

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

Overview: techniques and measures helpful for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES, applied to: …………………………………………………………………………………………	Effectiveness *vs* RISK level from Annex C, ISO/TR 24971:2020			References in this document	Deemed by the MANUFACTURER to be applicable? Yes/No Add comments, links, etc.	Row No.
	RISK level					
	1	2	3			
Techniques and measures that might be helpful in project management, planning and specification				**4 and A.1**		1
Establishment of a RISK MANAGEMENT PROCESS It is recommended that a RISK MANAGEMENT PROCESS is established for the ME EQUIPMENT or ME SYSTEM, in accordance with the latest version(s) of the most relevant standard(s), for example ISO/TR 24971, IEC 60601-1. It is recommended that a competent person has overall responsibility for managing the RISKS of the project, by using the RISK MANAGEMENT PROCESS, throughout the EXPECTED SERVICE LIFE.	HE	HE	HE	4		2
Project management and planning It is recommended that the PROCESSES for the management, planning, selection, design, implementation, commissioning, modification VERIFICATION and maintenance of each part that is relevant for the achievement of BASIC SAFETY or ESSENTIAL PERFORMANCE explicitly include adequate mitigation of the effects that can be caused by EM DISTURBANCES on the ME EQUIPMENT or ME SYSTEM and be documented. It is recommended that a competent person has overall responsibility for managing the achievement of adequate mitigation of the effects that can be caused by EM DISTURBANCES on the ME EQUIPMENT or ME SYSTEM, and that appropriate competency is made available throughout the EXPECTED SERVICE LIFE.	HE	HE	HE	A.1.1		3
Creating a design specification To help ensure that all reasonably foreseeable EM DISTURBANCES and their effects are taken into account in the design specification for the ME EQUIPMENT or ME SYSTEM and its subsystems and system parts. It is recommended to specify appropriate techniques and measures to ensure that the ME EQUIPMENT or ME SYSTEM remains safe, 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) un-intended or inaccurate operations. It is recommended that the specification for the techniques and measures for adequate mitigation of the effects that can be caused by EM DISTURBANCES strives to be complete, free from errors and contradictions, and easy to verify.	HE	HE	HE	A.1.2		4
Specifying EMC test standards to help ensure the availability of the ME EQUIPMENT or ME SYSTEM To help ensure the availability of the ME EQUIPMENT or ME SYSTEM throughout its EXPECTED SERVICE LIFE, so that it continues to maintain BASIC SAFETY and ESSENTIAL PERFORMANCE taking into account availability, throughput rate, production rate, and all other functional needs.	HE	HE	HE	A.1.3		5

Overview: techniques and measures helpful for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES, applied to:	Effectiveness *vs* RISK level from Annex C, ISO/TR 24971:2020			References in this document	Deemed by the MANUFACTURER to be applicable? Yes/No Add comments, links, etc.	Row No.
	RISK level					
	1	2	3			
Protecting against high impact, unusual and malicious EMI To help achieve and maintain BASIC SAFETY and ESSENTIAL PERFORMANCE where high impact, unusual and malicious EM DISTURBANCES could reasonably foreseeably occur and cause temporary disturbance and/or permanent damage to hardware (electronic components, interconnections, etc.).	HE	HE	HE	A.1.4		6
						7
Please describe here any other technique or measure used in project management and planning if applicable: (Please add more rows like this if there are additional techniques or measures to be included.)	-	-	-			8
Techniques and measures that might be helpful in system design				**A.2**		9
Separating system parts important for BASIC SAFETY **or** ESSENTIAL PERFORMANCE **from system parts that are not important for** BASIC SAFETY **or** ESSENTIAL PERFORMANCE	HE	HE	HE	A.2.2		10
Recording how the design specification is achieved through design choices	HE	HE	HE	A.2.3		11
Co-design of electromagnetically diverse hardware and software in multiple redundant channels 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. Hardware and software designers work together (i.e. co-design) to achieve the necessary overall diversity in the most effective way in order to meet the design specification (from A.1.2).	E	E	HE	A.2.4		12
System integration, installation, and commissioning To ensure that adequate mitigation of the effects that can be caused by EM DISTURBANCES is correctly considered when separately tested system parts are brought together to form the complete functional ME EQUIPMENT or ME SYSTEM.	HE	HE	HE	A.2.5		13
Fault detection and event data recording for later diagnosis To increase the probability of localising malfunctions caused by EM DISTURBANCES.	E	E	HE	A.2.6		14

Overview: techniques and measures helpful for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES, applied **to: ....**		**Effectiveness *vs* RISK level from Annex C, ISO/TR 24971:2020**			**References in this document**	**Deemed by the MANUFACTURER to be applicable? Yes/No** **Add comments, links, etc.**	**Row No.**
		RISK level					
		1	**2**	**3**			
Improving the mitigation of the effects that can be caused by EM DISTURBANCES of communication links, by using hardware and/or software techniques to improve the reliability of the links	**Error detection** Redundant data is appended to the actual data using error detection coding (EDC) techniques such as parity or cyclic redundancy checking (CRC) (see A.3.11, A.3.12, and A.3.14), or suitable equivalent EDC techniques, to detect data corruption. Upon detection of data corruption, appropriate action is taken to maintain safety, as described in the documentation. For example, various retry schemes could be used to improve the reliability of the link (at the expense of overall system performance).	HE	HE	HE	A.2.7.2		15
	Error correction A variation of error detection using code such that a level of error correction is possible in order to both detect corruption and correct for its effects. Various error correcting code (ECC) schemes (see A.3.11, A.3.12, and A.3.14) can be used to improve the reliability of the link at the expense of reduced data rate. Whenever error correction occurs, it is recommended that this is logged to aid later diagnosis. See A.2.5.	HE	HE	HE	A.2.7.3		16
	Protection of a sequence Extra sequence codes can be appended to each packet to enable detection of delayed, lost, or duplicated packets. Various techniques and measures listed in this table can be used at the packet level, e.g. just a single bit can be alternated between packets to detect a single packet failure (omission or duplication). More elaborate techniques can detect multiple packet failures or corruption.	HE	HE	HE	A.2.7.4		17
	Wireless mesh networks Creates multiple geographically diverse wireless data communication links to improve the redundancy of data communications	E	E	HE	A.2.7.5		18
Synchronisation and re-synchronisation techniques	Synchronous system functions intended for continuous operation.	HE	HE	HE	A.2.8		19
	Synchronous system functions intended to operate on demand.	E	E	E			20
	Any kind of synchronous system that has no safe state.	HE	HE	HE			21

Overview: techniques and measures helpful for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES, applied to: …………………………………………………………………………………………		Effectiveness *vs* RISK level from Annex C, ISO/TR 24971:2020			References in this document	Deemed by the MANUFACTURER to be applicable? Yes/No Add comments, links, etc.	Row No.
		RISK level					
		1	2	3			
Protection from persistent interference by monitoring retry counts	Systems intended for continuous operation.	HE	HE	HE	A.2.9		22
	On-demand systems.	E	E	E			23
Independent detection of EM DISTURBANCES and/or EMI		E	E	HE	A.2.10		24
Protection of systems from tampering via communication links to external systems To maintain the BASIC SAFETY and ESSENTIAL PERFORMANCE of ME EQUIPMENT or ME SYSTEMS, subsystems or system parts that have external communication links, especially with the Internet, at least for adequate mitigation of the effects that can be caused by EM DISTURBANCES.		E	E	E	A.2.11		25
Robust, high-specification electromagnetic mitigation. Especially useful when degradation or interruption of functionality is not desired.		E	E	E	A.2.12		26
Techniques and measures to prevent Virtualization of memory and PROCESS **resources from causing unacceptable** RISKS		E	E	HE	A.2.13		27
Usability engineering		E	E	HE	A.2.14		28
Please describe here any other technique or measure used in system design if applicable: (Please add more rows like this if there are additional techniques or measures to be included.)		-	-	-			29
Techniques and measures that might be helpful in operational design In the subclauses below, techniques and measures are classified as hardware or software based, but some of them might have equivalent representations in either hardware or software, which might be more effective in some useful manner.					**A.3**		30
Developing appropriate operation and maintenance instructions For PROCEDURES that help to avoid EMI-induced failures during the operation and maintenance of ME EQUIPMENT or an ME SYSTEM, or of a subsystem or system part.		HE	HE	HE	A.3.2		31
Designing appropriate maintenance techniques 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.		HE	HE	HE	A.3.3		32
Limiting the possibilities for operation and hence for mis-operation. To help avoid EM DISTURBANCES causing failures by affecting OPERATOR controls.		HE	HE	HE	A.3.4		33
Protecting against OPERATOR **errors, mistakes, and other foreseeable misuse**		HE	HE	HE	A.3.5		34

Overview: techniques and measures helpful for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES, applied **to: ……………………………………………………………………………………**			**Effectiveness *vs* RISK level from Annex C, ISO/TR 24971:2020**			**References in this document**	**Deemed by the MANUFACTURER to be applicable? Yes/No** **Add comments, links, etc.**	**Row No.**
			RISK level					
			1	**2**	**3**			
Protecting against hardware/software modifications or manipulations Using any technical means			HE	HE	HE	A.3.6		35
Defensive programming techniques To design software programs to detect anomalous control flow, data flow, or data values, which might have been caused by EM DISTURBANCES during their execution, and to react in a predetermined and acceptable manner.	**Range checking in hardware and in software** Range checking the values of all variables (not just I/Os), sometimes called strong data typing. A number of bands are specified for the value of each variable. A typical 3-band example is: a) normal operation; b) warning zone; and c) out of range.		E	E	HE	A.3.7.2		36
	Sequence checking	Safety functions intended for continuous operation	HE	HE	HE	A.3.7.3		37
		Safety functions intended for on-demand operation	E	E	E			38
	Correct rounding and resolution in all calculations		HE	HE	HE	A.3.7.4		39
	Floating point unit and real number arithmetic Help avoid corruption of arithmetic processing operations		HE	HE	HE	A.3.7.5		40
Limited use of interrupts To help reduce the impact of corruption due to EM DISTURBANCES upon program execution			E	HE	HE	A.3.8		41
Limited use of memory address pointer variables to reduce impact of memory corruption	System functions intended for continuous operation		HE	HE	HE	A.3.9		42
	System functions intended for on-demand operation		E	E	E			43
	Any/all systems with no safe state		HE	HE	HE			44
Avoiding recursion To help reduce the impact of corruption due to EM DISTURBANCES on program execution			HE	HE	HE	A.3.10		45
Error detection and correction for invariable memory (i.e. ROM or program memory)	**Signature of a word or block of data** To detect single and multi-bit corruption within a block of data. Various checking techniques are available, such as Cyclic Redundancy Checks (CRC), Secure Hash Algorithm (SHA), and Hamming Codes (for correction as well as detection).		E	E	HE	A.3.11.2		46
	Block replication with inversion to detect all bit failures Plus the use of electromagnetically diverse memories to improve effectiveness.		HE E	HE E	HE HE	A.3.11.3 A.2.4		47
	Memory boundary protection To prevent incorrect areas being overwritten in the following types of memory: program; stack; statically allocated variables; heap (dynamically allocated variables); inputs, and outputs		E	E	HE	A.3.11.4		48

Overview: techniques and measures helpful for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES, applied to: …………………………………………………………		Effectiveness *vs* RISK level from Annex C, ISO/TR 24971:2020			References in this document	Deemed by the MANUFACTURER to be applicable? Yes/No Add comments, links, etc.	Row No.
		RISK level					
		1	2	3			
Error detection and error correction techniques in redundant designs	System functions intended for continuous operation	HE	HE	HE	A.3.12		49
	System functions intended for on-demand operation	E	E	HE			50
Time-based error detection/correction in buses and interfaces to detect transient failures Combine with error checking codes to protect the sequence numbers or time codes.		E E	E E	HE HE	A.3.13 A.3.12 and A.3.14		51
Error detection and error correction for variable memory (e.g. RAM). Detecting failures during addressing, writing, storing, and reading data in memory.	**Memory testing** Before and/or during operation to detect memory-system-specific errors.	E	E	HE	A.3.14.2		52
	One-bit redundancy To detect some changes in the content of a memory location, bus, or I/O register.	E	E	E	A.3.14.3		53
	Block replication with inversion to detect all bit failures Using diverse types of memory can improve the effectiveness of this technique.	HE E	HE E	HE HE	A.3.14.4 A.2.4		54
	Memory boundary protection	E	E	HE	A.3.14.5		55
Error detection/correction in ROM, RAM, buses, and interfaces Detects/corrects one or more bit failures in a word.		E	E	HE	A.3.15		56
Error detection for logic and data processing units	**Self-test supported by hardware (one-channel)**	HE	HE	HE	A.3.16.2		57
	Coded processing (one-channel)	E	E	E	A.3.16.3		58
	Reciprocal comparison by software Two or more electromagnetically diverse processing units (see A.2.3) exchange data (results, intermediate results, and test data) and cross-check at specified "restore points" from which system operation could be continued in the event of a fault.	HE	HE	HE	A.3.16.4		59
	Self-test by software during operation	E	E	HE	A.3.16.5		60
Error detection and error correction for electrical and electromechanical components To help control failures in components such as relays, actuators, magnetic logic devices etc. Diverse hardware and/or software improves resistance to the common-cause effects of EMI.		HE E	HE HE	HE HE	A.3.17 A.2.4		61

Overview: techniques and measures helpful for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES, applied to:			**Effectiveness *vs* RISK level from Annex C, ISO/TR 24971:2020**			**References in this document**	**Deemed by the MANUFACTURER to be applicable? Yes/No** **Add comments, links, etc.**	**Row No.**
			RISK level					
			1	**2**	**3**			
Caution when using hardware or software libraries To ensure that the techniques and measures for adequate mitigation of the effects that can be caused by EM DISTURBANCES are applied and verified throughout the whole software design and implementation of ME EQUIPMENT or an ME SYSTEM.			HE	HE	HE	A.3.18		62
Error detection and correction for electronic components	**Testing by redundant hardware** To monitor the operation of the relevant function.		E	E	E	A.3.19.2		63
	Using dynamic signalling techniques To detect static failures in communications and processing.		E	E	E	A.3.19.3		64
	Caution with use of test access PORTS **and boundary-scan** To prevent any tests/diagnostics from making the ME EQUIPMENT or ME SYSTEM more susceptible to EM DISTURBANCES.		E	E	E	A.3.19.4		65
	Monitored redundancy Compares the behaviour of two or more electromagnetically diverse channels (see A.2.3).		E	E	HE	A.3.19.5		66
	Hardware with automatic self-test To detect faults by periodic checking of the functions using automatic self-tests.		E	E	E	A.3.19.6		67
	Analogue signal monitoring To improve confidence in signals and controls.		HE	HE	HE	A.3.19.7		68
	"Data assurance" (content credibility checking) Uses known relationships within a dataset to detect corruption due to EMI.	System functions for continuous operation.	HE	HE	HE	A.3.19.8		69
		System functions for on-demand operation.	E	E	E			70

Overview: techniques and measures helpful for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES, applied to:		Effectiveness *vs* RISK level from Annex C, ISO/TR 24971:2020			References in this document	Deemed by the MANUFACTURER to be applicable? Yes/No Add comments, links, etc.	Row No.
		RISK level					
		1	2	3			
Error detection and correction by monitoring program sequence (i.e. "watchdogs")	**Watchdog (temporal monitoring) with separate time base without time-window** ***– only to be used if A.3.20.3 or A.3.20.4 below cannot be used.***	E	E	***NE***	A.3.20.2		71
	Watchdog (temporal monitoring) with separate time base and time-window Periodically triggered to monitor the computer's behaviour and the plausibility of the program sequence, with both lower and upper time limits set; preferred over A.3.20.2.	HE	HE	HE	A.3.20.3		72
	Logical monitoring of program sequence Monitoring of individual program sections using software (e.g. counting PROCEDURE, key PROCEDURE) or using external monitoring facilities; preferred over A.3.20.2.	E	E	HE	A.3.20.4		73
	Combination of temporal and logical monitoring of program sequences Combining both temporal (with time window) and logical monitoring to retrigger a temporal facility (e.g. an external watchdog) only if the sequence of the program sections is executed correctly. Preferred over either A.3.20.3 or A.3.20.4 above. Also preferred over A.3.20.3 and A.3.20.4 used together but independently.	E	E	HE	A.3.20.5		74
Error detection and error correction by comparing multi-channel input/output interfaces **Using electromagnetically diverse hardware and/or software** To improve the effectiveness of this technique with regard to the common-cause effects typical of EM DISTURBANCES, permitting more confident error correction.		E E	E E	HE HE	A.3.21 A.2.4		75
Using test patterns: static and dynamic Using static and dynamic test patterns to detect static failures ("stuck-at" failures) and crosstalk, particularly in input and output units (digital, analogue, serial or parallel), and to prevent sending inadmissible inputs/outputs to the PROCESS **Using electromagnetically diverse channels** To permit more confident error correction.		HE HE	HE HE	HE HE	A.3.22 A.2.4		76
Use metal-free fibre-optic cables for signals and data They are intrinsically immune to EM DISTURBANCES.		E	E	E	A.3.23		77

Overview: techniques and measures helpful for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES, applied to: …………………………………………………………………………………………		Effectiveness *vs* RISK level from Annex C, ISO/TR 24971:2020			References in this document	Deemed by the MANUFACTURER to be applicable? Yes/No Add comments, links, etc.	Row No.
		RISK level					
		1	2	3			
Techniques for AC and DC power supplies and power converters To detect or tolerate failures caused by degradations or defects in any of the electrical power supplies.	**Detecting degradations and defects** Various devices and circuit techniques are readily available for detecting any/all defects in AC or DC power supplies.	HE	HE	HE	A.3.24.2		78
	Using electromagnetically diverse hardware and/or software To improve the effectiveness of this technique with regard to the common-cause effects typical of EMI.	E	HE	HE	A.2.4		
	Power hold-up By using sufficient energy storage (e.g. batteries, supercapacitors, etc.) or back-up power supplies (e.g. generators) with appropriate action taken to maintain safety when the energy storage runs out.	HE	HE	HE	A.3.24.3		79
	Detecting excessive RADIO FREQUENCY noise on power supplies	E	E	E	A.3.24.4		80
	Redundant electromagnetically diverse power supplies Using redundant electromagnetically diverse power supplies to continue safe operation by switching from a failed power supply to one that is still operating correctly (e.g. a backup/reserve power supply).	E	E	HE	A.3.24.5		81
Monitoring of ventilation, cooling, and heating To detect whether they have been influenced by EM DISTURBANCES.		E	E	HE	A.3.25		82
Careful use of wireless (radio) data communications Ensuring that wireless (radio) data communications will not cause an unsafe failure and will not adversely impact the safety of the ME EQUIPMENT or ME SYSTEM.		HE	HE	HE	A.3.26		83
Good electromagnetic engineering practices used at every level of design To use accepted, good electromagnetic engineering practices at the time of system implementation in order to provide a first line of defence against EM DISTURBANCES.		HE	HE	HE	A.3.27		84
Design to comply with EMC test specifications from A.1.3 (and A.1.4 if appropriate) To help ensure that the ME EQUIPMENT or ME SYSTEM will comply with these EMC test specifications during VERIFICATION and validation.		HE	HE	HE	A.3.28		85
De-rating of hardware components, where appropriate To increase the reliability of hardware components, particularly those used for the suppression of EM DISTURBANCES or protection against their effects.		E	E	E	A.3.29		86
Improve robustness of interrupts To help reduce the impact of CPU saturation and program execution lock-up due to EM DISTURBANCES through interruptions.		E	HE	HE	A.3.30		87

Overview: techniques and measures helpful for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES, applied to:	Effectiveness *vs* RISK level from Annex C, ISO/TR 24971:2020			References in this document	Deemed by the MANUFACTURER to be applicable? Yes/No Add comments, links, etc.	Row No.
	RISK level					
	1	2	3			
						88
						89
						90
Please describe here any other technique or measure used in operational design, if applicable: (Please add more rows like this if there are additional techniques or measures to be included.)	-	-	-			91
Techniques and measures that might be helpful in implementation, integration, installation, and commissioning				**A.4**		92
Providing information on any constraints and/or additional measures recommended for installation and commissioning To aid installation and commissioning in accordance with the relevant design specification for adequate mitigation of the effects that can be caused by EM DISTURBANCES.	HE	HE	HE	A.4.1		93
Procure materials, components, and products According to their design specifications for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES.	HE	HE	HE	A.4.2		94
Assemble/integrate according to the design specifications Using the correct materials, components, and products according to their design specifications for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES.	HE	HE	HE	A.4.3		95
Install/commission according to the design for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES *Also* to ensure that good electromagnetic engineering practices are used as appropriate during installation and commissioning. *Also* to help ensure that the ME EQUIPMENT or ME SYSTEM will comply with the EMC test specifications from A.1.3 and (if appropriate) A.1.4 during VERIFICATION and validation.	HE	HE	HE	A.4.4		96
						97
						98
						99
Please describe here any other technique or measure used in implementation, integration, installation, and commissioning, if applicable: (Please add more rows like this if there are additional techniques or measures to be included.)						100

Overview: techniques and measures helpful for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES, applied **to: ....**	**Effectiveness *vs* RISK level from Annex C, ISO/TR 24971:2020**			**References in this document**	**Deemed by the MANUFACTURER to be applicable? Yes/No** **Add comments, links, etc.**	**Row No.**
	RISK level					
	1	**2**	**3**			
Techniques and measures that might be helpful in VERIFICATION and validation (including testing)				A.5		101
Applying VERIFICATION**, and validation techniques and measures** To verify and/or validate as far as is practicable that the design techniques and measures that have been applied function according to the relevant design specification (created by A.1). (Note that EMC testing is covered by A.5.3 and A.5.4)	HE	HE	HE	A.5.1		102
VERIFICATION **testing to the EMC test plan resulting from A.1.3 (and A.1.4 if appropriate)**	HE	HE	HE	A.5.2		103
Using non-standardised ad hoc checks or tests To help ensure that the ME EQUIPMENT or ME SYSTEM or any component part of it has sufficient adequate mitigation of the effects that can be caused by EM DISTURBANCES, taking into account the level of RISK being aimed for.	HE	HE	HE	A.5.3		104
Verifying correct installation and commissioning Having regard to the constraints and additional measures listed as the result of applying A.4.1 and A.4.2, and any others not listed in those subclauses.	HE	HE	HE	A.5.4		105
EMC tests before, during and after accelerated life tests To help ensure that the intended mitigation of the effects that can be caused by EM DISTURBANCES is effective both during and after accelerated life tests.	E	HE	HE	A.5.5		106
						107
						108
Please describe here any other technique or measure used for VERIFICATION and validation (including testing), if applicable: (Please add more rows like this if there are additional techniques or measures to be included.)	-	-	-			109
Techniques and measures that might be helpful in maintenance, refurbishment, repair, modification, upgrade, etc., throughout the EXPECTED SERVICE LIFE				**A.6**		110
Assessment of changes in the ELECTROMAGNETIC ENVIRONMENT And, if applicable, modify/upgrade so that the availability of the ME EQUIPMENT or ME SYSTEM is maintained at a high level (discussed in A.1.3).	HE	HE	HE	A.6.1		111
Assessment of continuing correct installation Having regard to the constraints and additional measures listed as the result of applying A.4.1, and any others not listed in that section.	HE	HE	HE	A.6.2		112

Overview: techniques and measures helpful for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES, applied **to: ………………………………………………………………………………………**	**Effectiveness *vs* RISK level from Annex C, ISO/TR 24971:2020**			**References in this document**	**Deemed by the MANUFACTURER to be applicable? Yes/No** **Add comments, links, etc.**	**Row No.**
	RISK level					
	1	**2**	**3**			
Maintaining adequate mitigation of the effects that can be caused by EM DISTURBANCES, **despite modifications or changes** Assessing proposed changes to the ME EQUIPMENT or ME SYSTEM to ensure that repairs, modifications, upgrades, refurbishment, etc. do not unacceptably degrade its achievement of adequate mitigation of the effects that can be caused by EM DISTURBANCES.	HE	HE	HE	A.6.3		113
Batch (lot) traceability To help ensure analysis of the root cause of any problems caused by EM DISTURBANCES OR EMI, and containment by identifying product at risk.	HE	HE	HE	A.6.4		114
Component changes, new supplier, dual / alternate source When replacing components due to changes in specifications or PROCESS, a reference change, a change of supplier, or obsolescence, to help ensure that these activities do not unacceptably degrade the mitigation of the effects that can be caused by EM DISTURBANCES, for the ME EQUIPMENT or ME SYSTEM.	HE	HE	HE	A.6.5		115
Please describe here any other technique or measure used for maintenance, refurbishment, repair, modification, upgrade, etc., throughout the EXPECTED SERVICE LIFE:	-	-	-			116
Please describe here any other technique or measure used for maintenance, refurbishment, repair, modification, upgrade, etc., throughout the EXPECTED SERVICE LIFE: (Please add more rows like this if there are additional techniques or measures to be included.)	-	-	-			117
Techniques and measures that might be helpful in decommissioning				**A.7**		118
To ensure – where appropriate – that decommissioning does not cause unacceptable degradation of the mitigation of the effects that can be caused by EM DISTURBANCES, for the ME EQUIPMENT or ME SYSTEM undergoing the decommissioning PROCESS.	HE	HE	HE	A.7		119
						120
Please describe here any other technique or measure used for decommissioning: (Please add more rows like this if there are additional techniques or measures to be included.)	-	-	-			121

Overview: techniques and measures helpful for achieving adequate mitigation of the effects that can be caused by EM DISTURBANCES, applied to: …………………………………………………………………………………………	Effectiveness *vs* RISK level from Annex C, ISO/TR 24971:2020			References in this document	Deemed by the MANUFACTURER to be applicable? Yes/No Add comments, links, etc.	Row No.
	RISK level					
	1	2	3			
Techniques and measures that might be helpful when integrating third-party system parts into ME EQUIPMENT **or an** ME SYSTEM				**A.8**		122
The general iterative approach As shown in Figure A.1 (see A.8.1)				A.8.1		123
Suppliers' certifications and electromagnetic performance specifications It is recommended that suppliers' markings, certifications, and declarations (including CE marking with regard to the EMC Directive [7]) are not taken as reliable evidence of electromagnetic performance.				A.8.2		124
Alternatively, use custom-manufactured component parts or subsystems And make producing reliable evidence of electromagnetic performance part of the contract specification.				A.8.3		125
						126
Please describe here any other technique or measure used for integrating third-party items into ME EQUIPMENT or an ME SYSTEM: (Please add more rows like this if there are additional techniques or measures to be included.)						127

Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this document. Reference to these resources is made for informational use only.

When using any of the standards listed in this Bibliography, it is recommended to use the most recently published edition or version, including all amendments.

NOTE These lists are not exhaustive as new standards and other documents (and new versions of existing material) are constantly being created.

General references

[1] IEC 60601-1-2:2014, *Medical electrical equipment – Part 1-2: General requirements for basic safety and essential performance – Collateral Standard: Electromagnetic disturbances – Requirements and tests*
IEC 60601-1-2:2014/AMD1:2020

[2] ISO 14971:2019, *Medical devices – Application of risk management to medical devices*

[3] ISO TR 24971:2020, *Medical devices – Guidance on the application of ISO 14971*

[4] Void

[5] IEC 61000-1-2, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

[6] ISO/IEC Directives, Part 2*, Principles and rules for the structure and drafting of ISO and IEC documents*

[7] 2014/30/EU, the European Union's Directive on EMC, 26 February 2014, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0030.

[8] IEC 61000-6-7, *Electromagnetic compatibility (EMC) – Part 6-7: Generic standards – Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations*

[9] Defense Acquisition Regulations System, Department of Defense. 48 CFR Parts 202, 231, 244, 246, and 252, RIN 0750–AH88, Defense Federal Acquisition Regulation Supplement: Detection and Avoidance of Counterfeit Electronic Parts (DFARS Case 2012–D055), published in the Federal Register / Vol. 79, No. 87 / Tuesday, May 6, 2014 / Rules and Regulations.

[10] CISPR 16-4-2:2011, *Specification for radio disturbance and immunity measuring apparatus and methods – Part 4-2: Uncertainties, statistics and limit modelling – Measurement instrumentation uncertainty*
CISPR 16-4-2:2011/AMD1:2014
CISPR 16-4-2:2011/AMD2:2018

[11] Armstrong, K., *Why EMC Immunity Testing is Inadequate for Functional Safety*, IEEE 2004 International Symposium on EMC, Santa Clara, CA, August 9-13, ISBN: 0-7803-8444-X

[12] Armstrong, K., *Why increasing immunity test levels is not sufficient for high-reliability and critical equipment*, IEEE 2009 International Symposium on EMC, Austin, TX, August 17-21, ISBN: 978-1-4244-4285-0

[13] Armstrong, K., *Testing for immunity to simultaneous disturbances and similar issues for risk managing EMC*, IEEE 2012 International Symposium on EMC, Pittsburgh, PA, August 5-10, ISBN: 978-1-4673-2059-7

[14] Armstrong, K., *Why Do We Need an IEEE EMC Standard on Managing Risks?*, 2016 IEEE Electromagnetic Compatibility Magazine – Volume 5 – Quarter 1, pages 81-84, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7477140

[15] IEC TR 62366-2, *Medical devices – Part 2: Guidance on the application of usability engineering to medical devices*

[16] IEC 60050 (all parts), *International Electrotechnical Vocabulary (IEV)*, available at https://www.electropedia.org

[17] ANSI C63.14:2014, *American National Standard Dictionary of Electromagnetic Compatibility (EMC) Including Electromagnetic Environmental Effects (E3)*

[18] ISO 9000:2015, *Quality management systems – Fundamentals and vocabulary*

[19] Void

Good EMC engineering for systems and installations

[20] IEC TR 61000-5-2, *Electromagnetic compatibility (EMC) – Part 5: Installation and mitigation guidelines – Section 2: Earthing and cabling*

[21] Armstrong, K., *Good EMC Engineering Practices in the Design and Construction of Industrial Cabinets* REO (UK) Ltd., https://www.emcstandards.co.uk/good-emc-engineering-practices-in-the-design-an1

[22] Armstrong, K., *Good EMC Engineering Practices in the Design and Construction of Fixed Installation*, REO (UK) Ltd., https://www.emcstandards.co.uk/good-emc-engineering-practices-for-fixed-instal2

[23] EMC for Systems and Installations, Tim Williams and Keith Armstrong, Newnes 2000, https://shop.elsevier.com/books/emc-for-systems-and-installations/williams/978-0-7506-4167-8

[24] IEC TR 61000-5-6, *Electromagnetic Compatibility (EMC) – Part 5-6: Installation and mitigation guidelines – Mitigation of external EM influences*

[25] Duff. W. G, *Designing Electronic Systems for EMC* , 2001, ISBN: 978-1-891121-42-5, Scitech Publishing, Inc., https://shop.theiet.org/des-electron-syst-emc

[26] Armstrong, K., *Complying with IEC 61800-3 – Good EMC Engineering Practices in the Installation of Power Drive Systems*, REO (UK) Ltd., https://www.emcstandards.co.uk/complying-with-iecen-61800-3-good-emc-engineeri

[27] Armstrong, K., *Mains Harmonics (problems and solutions)*, REO (UK) Ltd., https://www.emcstandards.co.uk/mains-harmonics-guide

[28] Armstrong, K., *Power Quality (problems and solutions)*, REO (UK) Ltd., https://www.emcstandards.co.uk/mains-power-quality-guide

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

[30] Van der Laan, P. C. T., and Van Duerson, A. P. J., *Protection of Electronics in High-Power Installations: Theory, Guidelines and Demonstrations*, CIGRÉ Symposium, Lausanne, 1993, paper 600-08

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

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

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

[34] Hoeft, L. O. (Bud), *Analysis of Electromagnetic Shielding of Cables and Connectors (keeping currents/voltages where they belong)*, IEEE, 2002, https://www.scribd.com/document/135325285/Electromagnetic-Shielding-of-Cables-and-Connectors

[35] IEC 60364-4-44:2007, *Low-voltage electrical installations – Part 4-44: Protection for safety – Protection against voltage disturbances and electromagnetic disturbances*

[36] IEC 62305 (all parts), *Protection against lightning*

[37] Mardiguian, Michel, *Combined Effects of Several, Simultaneous, EMI Couplings*, 2000 IEEE International Symposium on EMC, Washington D.C., August 21-25, 2000, ISBN 0-7803-5680-2, pp. 181-184

[38] IEC TR 61000-1-5, *Electromagnetic compatibility (EMC) – Part 1-5: General – High power electromagnetic (HPEM) effects on civil systems*

[39] Radasky, W. A., 2007 *Status of the Development of High-Power Electromagnetic (HPEM) Publications in the IEC,* 2007 International Symposium on Electromagnetic Compatibility, https://ieeexplore.ieee.org/document/4413418

[40] IEC TR 61000-5-3, *Electromagnetic compatibility (EMC) – Part 5-3: Installation and mitigation guidelines – HEMP protection concepts*

[41] IEC TS 61000-5-4, *Electromagnetic compatibility (EMC) – Part 5: Installation and mitigation guidelines – Section 4: Immunity to HEMP -Specifications for protective devices against HEMP radiated disturbance*

[42] IEC 61000-5-5, *Electromagnetic compatibility (EMC) – Part 5: Installation and mitigation guidelines – Section 5: Specification of protective devices for HEMP conducted disturbance*

[43] IEC TS 61000-5-8, *Electromagnetic compatibility (EMC) – Part 5-8: Installation and mitigation guidelines – HEMP protection methods for the distributed infrastructure*

[44] IEC TS 61000-5-9, *Electromagnetic compatibility (EMC) – Part 5-9: Installation and mitigation guidelines – System-level susceptibility assessments for HEMP and HPEM*

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

[46] IEC TR 61000-1-3, *Electromagnetic compatibility (EMC) – Part 1-3: General – The effects of high-altitude EMP (HEMP) on civil equipment and systems*

[47] Void

[48] Void

[49] Void

[50] Void

[51] Void

[52] Void

[53] Void

[54] Void

[55] Void

[56] Void

[57] Void

[58] Void

[59] Void

Good EMC engineering for individual items of equipment

[60] *EMC for Printed Circuit Boards – Basic and Advanced Design and Layout Techniques*, Second Edition, Nutwood UK December 2010, ISBN 978-0-9555118-5-1, https://www.emcstandards.co.uk/emc-for-printed-circuit-boards

[61] Armstrong, K., *EMC Design Techniques for Electronic Engineers,* Armstrong/Nutwood UK 2010, ISBN: 978-0-9555118-4-4, https://www.emcstandards.co.uk/emc-for-printed-circuit-boards

[62] Williams, Tim, *EMC for Product Designers, 5th Edition*, December 2006, ISBN: 978-0-08-101016-7, https://www.emcstandards.co.uk/emc-for-product-designers

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

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

[65] Montrose, M., *Printed Circuit Board Design Techniques for EMC Compliance, Second Edition, A Handbook for Designers*, IEEE Press 2000, ISBN 0-7803-5376-5, https://ieeexplore.ieee.org/book/5264372

[66] Montrose, M., *EMC and the Printed Circuit Board – Design, Theory and Layout Made Simple,*IEEE Press 1998, ISBN 0-7803-4703-X, https://ieeexplore.ieee.org/book/5237459

[67] Ott, Henry O., *Electromagnetic Compatibility Engineering*, John Wiley & Sons, 2009, ISBN: 978-0-470-18930-6

[68] Sjögren, Lena, and Bäckström, Mats, *Ageing of Shielding Joints, Shielding Performance and Corrosion,* IEEE EMC Society Newsletter, Summer 2005, https://ewh.ieee.org/soc/emcs/acstrial/newsletters/summer05/practical.pdf

[69] Degraeve, A., Pissoort, D., Armstrong, K., *Improving the shielding effectiveness of a board-level shield by bonding it with the waveguide-below-cutoff principle,* 10th International IEEE Workshop on the Electromagnetic Compatibility of Integrated Circuits (EMC Compo), Edinburgh, UK, 2015

[70] IEEE 1364-2005, *IEEE Standard for Verilog Hardware Description Language*

[71] IEEE 1149.1-2013, *IEEE Standard for Test Access Port and Boundary-Scan Architecture*

[72] Void

[73] Void

[74] Void

[75] Void

[76] Void

[77] Void

[78] Void

[79] Void

[80] Void

[81] Void

[82] Void

[83] Void

[84] Void

[85] Void

[86] Void

[87] Void

[88] Void

[89] Void

[90] Void

[91] Void

[92] Void

[93] Void

[94] Void

[95] Void

[96] Void

[97] Void

[98] Void

[99] Void

Software design techniques and measures

[100] Cooling, J. E., *Software Engineering for Real Time Equipment*, Pearson Education 2003, ISBN 0201596202

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

[102] *Defensive Programming*, https://www.cs.princeton.edu/techreports/2002/658.pdf

[103] Void

[104] *NASA Software Safety Guidebook, NASA-GB-8719.13, March 31, 2004*, https://s3vi.ndc.nasa.gov/ssri-kb/static/resources/nasa-gb-8719.13.pdf

[105] Bharathi V., *N-Version programming method of Software Fault Tolerance: A Critical Review,* National Conference on Nonlinear Systems & Dynamics, NCNSD-2003, https://www.semanticscholar.org/paper/N-Version-programming-method-of-Software-Fault-A-Bharathi/3af85a971e3872cfb94202f1a41e17a418b79681

[106] Bowen, Jonathan., *Formal Methods in Safety-Critical Standards*, Proceedings 1993 Software Engineering Standards Symposium, https://ieeexplore.ieee.org/document/263953

[107] Kirk B. E., *Using Software Protocols to Mask CAN BUS Insecurities*, IEE Colloquium on the Electromagnetic Compatibility of Software, Thursday, Savoy Place, London, WC2R OBL, 12 November 1998, IEE document reference 98/471, https://ieeexplore.ieee.org/document/744676

[108] Profisafe, https://www.profibus.com/download/profisafe

[109] IEC 61784-3, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

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

[111] Cyclic redundancy check (CRC), http://en.wikipedia.org/wiki/Cyclic_redundancy_check

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

[113] ARINC 653, http://en.wikipedia.org/wiki/ARINC_653

[114] ARINC 653, *An avionics standard for safe, partitioned systems*, Wind River Inc. IEEE-CS Seminar, 4 June 2008 https://docplayer.net/287772-Arinc-653-an-avionics-standard-for-safe-partitioned-systems.html

[115] *Reliable/redundant array of independent/inexpensive servers,* https://en.wikipedia.org/wiki/Redundant_Array_of_Inexpensive_Servers

[116] Void

[117] Void

[118] Void

[119] Void

[120] IEEE Standard 754-2008, *Floating-Point Arithmetic*, https://ieeexplore.ieee.org/document/4610935

[121] Hass, K.J., *Synthesizing optimal fixed-point arithmetic for embedded signal processing,* 53rd IEEE International Midwest Symposium on Circuits and Systems (MWSCAS), 1-4 Aug. 2010, Seattle, WA, pp 61 – 64, ISBN: 978-1-4244-7771-5

[122] Kaegi, Thomas, and Schagaev, Igor, *System Software Support of Hardware Efficiency,* https://www.researchgate.net/publication/257930590_System_Software_Support_For_Hardware_Efficiency

[123] RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification,* North American Avionics Software

[124] Susskraut, Martin, *et al, Safe Program Execution with Diversified Encoding*, Embedded World 2015, www.embedded-world.eu

[125] *Deos, a Time & Space Partitioned, Multi-core Enabled, RTOS Verified to DO-178C/ED-12C DAL A* https://www.ddci.com/products_deos_do_178c_arinc_653/

[126] Void

[127] Void

[128] *Liveness*, https://en.wikipedia.org/wiki/Liveness

[129] *ARIANE 5, Flight 501 Failure*, Report by the Inquiry Board, The Chairman of the Board: Prof. J. L. LIONS, http://sunnyday.mit.edu/accidents/Ariane5accidentreport.html

[130] *The Mars Climate Orbiter failure,* https://en.wikipedia.org/wiki/Mars_Climate_Orbiter

[131] Moon, Todd K., *Error Correction Coding: Mathematical Methods and Algorithms*, Wiley 2005, ISBN: 0-471-648-00-0.

[132] *Hash Functions*, CSRC.NIST.gov/groups/ST/toolkit/secure_hashing.html

[133] Barr, Michael, *Software-Based Memory Testing*, in Embedded Systems Programming, July 2000, pp. 28-40, https://barrgroup.com/embedded-systems/how-to/memory-test-suite-c

[134] *Data caching*, https://en.wikipedia.org/wiki/Cache

[135] *DDR2 Synchronous Dynamic Data Interface,* https://en.wikipedia.org/wiki/DDR2_SDRAM

[136] DDR3 Synchronous Dynamic Data Interface, https://en.wikipedia.org/wiki/DDR3_SDRAM

[137] Johnson, R., Christi, S., *JTAG101 – IEEE 1149 and Software Debug*, (Intel Corp.2009)

[138] IEEE 1149.6, *A Boundary-Scan Standard for Advanced Digital Networks*

[139] Arce, G. E., *Nonlinear Signal Processing: A Statistical Approach*, Wiley New Jersey November 2004, Print ISBN: 978-0-471-67624-9, Online ISBN: 978-0-471-69185-3

[140] CEPT ERC Rec 70-03, *ERC Recommendation 70-03 Relating to the use of Short Range Devices (SRD)*, https://docdb.cept.org/download/25c41779-cd6e/Rec7003e.pdf

[141] *Exception handling*, https://en.wikipedia.org/wiki/Exception_handling

[142] *IEEE Transactions on Dependable and Secure Computing (TDSC)*, www.computer.org/web/tdsc/about

[143] Dirik, C., Gole, A., Rodriguez, S., Wang, H., and Jacob, B., *The Embedded Reliable Processing System (TERPS) – A Robust Architecture that Achieves Forward Progress in Near-Continuous Electromagnetic Interference,* Technical Report UMD-SCA-2004-10-01, November 2004, https://user.eng.umd.edu/~blj/papers/UMD-SCA-2004-11-01.pdf

[144] Churchley, Andrew, *Microprocessor Based Protection Systems*, (1991-11-30), Springer. p.64. ISBN 9781851666119, https://link.springer.com/book/9781851666119

[145] VIPER microprocessor, https://en.wikipedia.org/wiki/VIPER_microprocessor

[146] Void

[147] Void

[148] Void

[149] Void

[150] Void

[151] Void

[152] Void

[153] Void

[154] Void

[155] Void

[156] Void

[157] Void

[158] Void

[159] Void

[160] Void

[161] Void

[162] Void

[163] Void

[164] Void

[165] Void

[166] Void

[167] Void

[168] Void

[169] Void

[170] Void

[171] Void

[172] Void

[173] Void

[174] Void

[175] Void

[176] Void

[177] Void

[178] Void

[179] Void

[180] Void

[181] Void

[182] Void

[183] Void

[184] Void

[185] Void

[186] Void

[187] Void

[188] Void

[189] Void

[190] Void

[191] Void

[192] Void

[193] Void

[194] Void

[195] Void

[196] Void

[197] Void

[198] Void

[199] Void

IEC, ISO, IEEE, and CISPR standardized EMC test methods

[200] IEC 61000-4-2, *Electromagnetic compatibility (EMC) – Part 4-2: Testing and measurement techniques – Electrostatic discharge immunity test*

[201] IEC 61000-4-3, *Electromagnetic compatibility (EMC) – Part 4-3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test*

[202] IEC 61000-4-4, *Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques – Electrical fast transient/burst immunity test*

[203] IEC 61000-4-5, *Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques – Surge immunity test*

[204] IEC 61000-4-6, *Electromagnetic compatibility (EMC) – Part 4-6: Testing and measurement techniques – Immunity to conducted disturbances, induced by radio-frequency fields*

[205] IEC 61000-4-8, *Electromagnetic compatibility (EMC) – Part 4-8: Testing and measurement techniques – Power frequency magnetic field immunity test*

[206] IEC 61000-4-9, *Electromagnetic compatibility (EMC) – Part 4-9: Testing and measurement techniques – Impulse magnetic field immunity test*

[207] IEC 61000-4-10, *Electromagnetic compatibility (EMC) – Part 4-10: Testing and measurement techniques – Damped oscillatory magnetic field immunity test*

[208] IEC 61000-4-11, *Electromagnetic compatibility (EMC) – Part 4-11: Testing and measurement techniques – Voltage dips, short interruptions and voltage variations immunity tests for equipment with input current up to 16 A per phase*

[209] IEC 61000-4-12, *Electromagnetic compatibility (EMC) – Part 4-12: Testing and measurement techniques – Ring wave immunity test*

[210] IEC 61000-4-13, *Electromagnetic compatibility (EMC) – Part 4-13: Testing and measurement techniques – Harmonics and interharmonics including mains signalling at a.c. power port, low frequency immunity tests*

[211] IEC 61000-4-14, *Electromagnetic compatibility (EMC) – Part 4-14: Testing and measurement techniques – Voltage fluctuation immunity test for equipment with input current not exceeding 16 A per phase*

[212] IEC 61000-4-16, *Electromagnetic compatibility (EMC) – Part 4-16: Testing and measurement techniques – Test for immunity to conducted, common mode disturbances in the frequency range 0 Hz to 150 kHz*

[213] IEC 61000-4-17, *Electromagnetic compatibility (EMC) – Part 4-17: Testing and measurement techniques – Ripple on d.c. input power port immunity test*

[214] IEC 61000-4-18, *Electromagnetic compatibility (EMC) – Part 4-18: Testing and measurement techniques – Damped oscillatory wave immunity test*

[215] IEC 61000-4-19, *Electromagnetic compatibility (EMC) – Part 4-19: Testing and measurement techniques – Test for immunity to conducted, differential mode disturbances and signalling in the frequency range 2 kHz to 150 kHz at a.c. power ports*

[216] IEC 61000-4-20, *Electromagnetic compatibility (EMC) – Part 4-20: Testing and measurement techniques – Emission and immunity testing in transverse electromagnetic (TEM) waveguides*

[217] IEC 61000-4-21, *Electromagnetic compatibility (EMC) – Part 4-21: Testing and measurement techniques – Reverberation chamber test methods*

[218] IEC 61000-4-25, *Electromagnetic compatibility (EMC) – Part 4-25: Testing and measurement techniques – HEMP immunity test methods for equipment and systems*

[219] IEC 61000-4-27, *Electromagnetic compatibility (EMC) – Part 4-27: Testing and measurement techniques – Unbalance, immunity test for equipment with input current not exceeding 16 A per phase*

[220] IEC 61000-4-28, *Electromagnetic compatibility (EMC) – Part 4-28: Testing and measurement techniques – Variation of power frequency, immunity test for equipment with input current not exceeding 16 A per phase*

[221] IEC 61000-4-31, *Electromagnetic compatibility (EMC) – Part 4-31: Testing and measurement techniques – AC mains ports broadband conducted disturbance immunity test*

[222] IEC 61000-4-34, *Electromagnetic compatibility (EMC) – Part 4-34: Testing and measurement techniques – Voltage dips, short interruptions and voltage variations immunity tests for equipment with mains current more than 16 A per phase*

[223] IEC 61000-4-36, *Electromagnetic compatibility (EMC) – Part 4-36: Testing and measurement techniques – IEMI immunity test methods for equipment and systems*

[224] IEC 61000-4-39, *Electromagnetic compatibility (EMC) – Part 4-39: Testing and measurement techniques – Radiated fields in close proximity – Immunity test*

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

[226] IEC 61000-6-1:2016, *Electromagnetic compatibility (EMC) – Part 6-1: Generic standards – Immunity standard for residential, commercial and light-industrial environments*

[227] IEC 61000-6-2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity standard for industrial environments*

[228] IEC 61000-6-3, *Electromagnetic compatibility (EMC) – Part 6-3: Generic standards – Emission standard for equipment in residential environments*

[229] IEC 61000-6-4, *Electromagnetic compatibility (EMC) – Part 6-4: Generic standards – Emission standard for industrial environments*

[230] IEC 61000-6-5, *Electromagnetic compatibility (EMC) – Part 6-5: Generic standards – Immunity for equipment used in power station and substation environment*

[231] IEC 61000-4-33, *Electromagnetic compatibility (EMC) – Part 4-33: Testing and measurement techniques – Measurement methods for high-power transient parameters*

[232] IEC 61000-4-35, *Electromagnetic compatibility (EMC) – Part 4-35: Testing and measurement techniques – HPEM simulator compendium*

[233] IEC 61000-4-23, *Electromagnetic compatibility (EMC) – Part 4-23: Testing and measurement techniques – Test methods for protective devices for HEMP and other radiated disturbances*

[234] IEC 61000-4-24, *Electromagnetic compatibility (EMC) – Part 4-24: Testing and measurement techniques – Test methods for protective devices for HEMP conducted disturbance*

[235] IEC 61000-6-6, *Electromagnetic compatibility (EMC) – Part 6-6: Generic standards – HEMP immunity for indoor equipment*

[236] IEC 62561 (all parts), *Lightning protection system components (LPSC)*

[237] IEC 61000-4-32, *Electromagnetic compatibility (EMC) – Part 4-32: Testing and measurement techniques – High-altitude electromagnetic pulse (HEMP) simulator compendium*

[238] CISPR 11, *Industrial, scientific and medical equipment – Radio-frequency disturbance characteristics – Limits and methods of measurement*

[239] CISPR 14-1, *Electromagnetic compatibility – Requirements for household appliances, electric tools and similar apparatus – Part 1: Emission*

[240] CISPR 14-2, *Electromagnetic compatibility – Requirements for household appliances, electric tools and similar apparatus – Part 2: Immunity – Product family standard*

[241] CISPR 15, *Limits and methods of measurement of radio disturbance characteristics of electrical lighting and similar equipment*

[242] CISPR 16 (all parts), *Specification for radio disturbance and immunity measuring apparatus and methods*

[243] CISPR 32, *Electromagnetic compatibility of multimedia equipment – Emission requirements*

[244] CISPR 35, *Electromagnetic compatibility of multimedia equipment – Immunity requirements*

[245] IEC TR 60601-4-2, *Medical electrical equipment – Part 4-2: Guidance and interpretation – Electromagnetic immunity: performance of medical electrical equipment and medical electrical systems*

[246] IEC 61000-4-22, *Electromagnetic compatibility (EMC) – Part 4-22: Testing and measurement techniques – Radiated emissions and immunity measurements in fully anechoic room (FARs)*

[247] ISO 14117, *Active implantable medical devices – Electromagnetic compatibility – EMC test protocols for implantable cardiac pacemakers, implantable cardioverter defibrillators and cardiac resynchronization devices*

[248] ISO 14708-3, *Implants for surgery – Active implantable medical devices – Part 3: Implantable neurostimulators*

[249] ISO 14708-4, *Implants for surgery – Active implantable medical devices – Part 4: Implantable infusion pump systems*

[250] ISO 14708-7, *Implants for surgery – Active implantable medical devices – Part 7: Particular requirements for cochlear and auditory brainstem implant systems*

[251] ISO TS 10974, *Assessment of the safety of magnetic resonance imaging for patients with an active implantable medical device*

[252] IEC 61000-4-30, *Electromagnetic compatibility (EMC) – Part 4-30: Testing and measurement techniques – Power quality measurement methods*

[253] Void

[254] Void

[255] Void

[256] Void

[257] Void

[258] Void

[259] Void

[260] Void

[261] Void

[262] Void

[263] Void

[264] Void

[265] Void

[266] Void

[267] Void

[268] Void

[269] Void

[270] Void

[271] Void

[272] Void

[273] Void

[274] Void

[275] Void