NATO STANDARD

AEP-41

Volume 4

NATO IMPLEMENTATION OF UNIFIED PROTECTION AGAINST ELECTROMAGNETIC ENVIRONMENTAL EFFECTS (UE^3)

Edition A, Version 1

SUSCEPTIBILITY OF PLATFORMS, SYSTEMS & EQUIPMENT TO E^3

OCTOBER 2014

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED ENGINEERING PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

13 October 2014

1. The enclosed Allied Engineering Publication AEP-41 Edition A NATO IMPLEMENTATION OF UNIFIED PROTECTION AGAINST ELECTROMAGNETIC ENVIRONMENTAL EFFECTS (UE^3), Volume 4 on SUSCEPTIBILITY OF PLATFORMS, SYSTEMS AND EQUIPMENT TO E3 which has been approved by the nations in the NAAG/JCBRND-CDG, is promulgated herewith. The recommendation of nations to use this publication is recorded in STANREC 4567 Edition 1.

2. AEP-41 is effective upon receipt.

3. No part of this publication may be reproduced, stored in a retrieval system, used commercially, adapted, or transmitted in any form or by any means, electronic, mechanical, photo-copying, recording or otherwise, without the prior permission of the publisher. With the exception of commercial sales, this does not apply to member nations and Partnership for Peace countries, or NATO commands and bodies.

4. This publication shall be handled in accordance with C-M(2002)60.

Edvardas MAŽEIKIS
Major General, LTUAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

AEP- 41, NATO IMPLEMENTATION OF UNIFIED PROTECTION AGAINST ELECTROMAGNETIC ENVIRONMENTAL EFFECTS (UE^3)

AEP - 41 VOLUME IV

SUSCEPTIBILITY OF PLATFORMS, SYSTEMS AND EQUIPMENT TO E^3

1.0 TABLE OF CONTENTS

AEP 41, VOLUME IV

UNIFIED ELECTROMAGNETIC ENVIRONMENTAL EFFECTS (UE^3) PHILOSOPHY AND METHODOLOGY

2.0 AEP-41, EXECUTIVE SUMMARY

There is a general consensus for an unified approach to the protection and hardening of all NATO military platforms, systems and equipments (hardware) against Electromagnetic Environmental Effects (E^3) caused by the plethora of Electromagnetic Environments (EMEs) that these platforms, systems and equipments are subjected to during their deployment life. These E^3 can adversely impact the operational capability of this military hardware resulting in their inability to accomplish their mission or even putting the crew’s safety at risk. The EMEs are generated by natural, operational and hostile sources. Additionally, today’s complex military operational environment is characterized by: multi-national operations, increasingly crowded EM spectrum coupled with a reduction of bandwidth allocated for exclusive military use, military hardware whose mission performance is dependent on electronics, and hardware that is increasingly dependent on more energy sensitive Non-Developmental Items (NDIs) and Commercial-Off-The-Shelf (COTS) electronic components. Traditional hardening against the total battlespace EMEs has been accomplished by considering each EME individually and serially. The Conference of National Armaments Directors (CNAD) recognized the need for a Unified E^3 (UE^3) protection policy, and directed the development of an Allied Engineering Publication (AEP) 41 and an associated Standardization Agreement (STANAG) 4567 to describe and define this policy. The proposed UE^3 protection approach can be applied to all six Operational Categories (OCs) of NATO military hardware. These six OCs are:

OC1 Land Mobile Systems
OC2 Static Land Systems
OC3 Space Systems
OC4 Sea Platforms
OC5 Air Platforms
OC6 Command, Control and Information Systems

The CNAD approved the following seven AEP-41 volumes to detail the different functional areas required to achieve, produce and sustain affordable UE^3 protection and survivability:

a) Volume I, Unified Electromagnetic Environmental Effects (UE^3) Protection, Philosophy and Methodology
b) Volume II, Electromagnetic (EM) Environments (EMEs), E^3, and Operational Categories (OCs)
c) Volume III, Electromagnetic Coupling
d) Volume IV, Susceptibility of Platforms, Systems and Equipment to E^3
e) Volume V, Unified Hardening and Protection Against E^3
f) Volume VI, Testing and Validation of E^3 Protection

g) Volume VII, Hardness and Sustainment Assurance, and Surveillance Test

The basic philosophy is to provide a User-controlled, performance-based approach to developing cost effective, verifiable, producible, maintainable and sustainable UE^3 protection for NATO military hardware. The methodology for implementing UE^3 protection to all types of military hardware is based on use of an EM barrier protection concept that is applicable to linear cases. In addition, this methodology is inherently accommodating and flexible for future growth and changes, and for sustaining EM hardness against degradations resulting from usage, age, maintenance and repairs, changes and additions, and ambient environments. This AEP uses extensively the UE^3 Protection Philosophy and Methodology documented in QSTAG 1051.

2.1 INTRODUCTION FOR AEP 41

2.1.1 Balanced E^3 Protection. This AEP describes an approach for achieving adequate, affordable and balanced UE^3 protection and survivability in the battlespace for all classes of NATO military platforms, systems, and equipments (all three defined as hardware) of the six operational categories. Balance is achieved between several factors. First, the protection design is balanced for unified coverage of the EME stresses encountered during hardware operations. Second, a balance is achieved between the protection provided and hardware cost and operational impact. Third, the User can balance the level of protection against risk of operational degradation in the presence battlespace EMEs. The philosophy embodied in AEP-41 does not mandate design solutions; but instead, provides a performance-based methodology that allows the User the flexibility for deriving the final UE^3 protection design to meet performance requirements.

2.1.2 E^3 Protection Needs. Adequate E^3 protection of electronic/electrical military hardware is essential since such hardware must operate during and after exposure to increasingly severe, complex and changing EMEs that can potentially impact crew safety as well as degrade or even destroy mission essential performance capabilities. Potential battlespace EMEs are listed in Table 1. Meeting the E^3 protection requirement has become more difficult due to the post-cold war policy of deploying NATO coalition forces (even combined with UN forces) consisting of military hardware hardened to different E^3 levels into many different areas each with its own set of EME threats. This disparity in E^3 hardening, combined with different national policies on E^3 survivability sustainment, has resulted in deployment of NATO hardware with widely varying E^3 survivability/vulnerability levels. Thus, the deployed force has EM Compatibility (EMC) problems. In addition, most of the hardware was developed in the cold war. Post-cold war policy of most NATO countries is to extent the operational life of their deployed hardware by a factor of two or more. This lifetime extension combined with rapidly advancing technology and increasing obsolescence has become the reason for multiple modernization cycles (was one, now eight-to-ten) and the increasing use of COTS/NDIs and advanced technologies both of which tend to have lower energy upset and damage thresholds. These new impacting factors are in addition to the traditional ones (worsen by the longer deployment lifespan) that can degrade E^3 survivability such as ambient environments, corrosion, aging, usage, and repeated maintenance and repairs. Thus, the combination of these new and old factors has greatly increased the difficulty of sustaining E^3 survivable hardware.

Table 1. Characteristics of Battlespace EMEs.

Externally Generated Electromagnetic Environments			
Environment	**Type**	**Waveform**	**Propagation ***
Near Strike Lightning (NSL)	Natural	Pulse	Radiated and Conducted
Direct Strike Lightning (DSL)	Natural	Pulse	Conducted
High Altitude Electromagnetic Pulse (HEMP) E1, E2, E3	Hostile	Pulse	Radiated and Conducted
Source Region EMP (SREMP)	Hostile	Pulse	Radiated and Conducted
Non-Nuclear EMP (N^2 EMP)	Hostile	Pulse	Radiated
Electromagnetic Emissions	Electronic Operation	Pulse, Continuous Wave (CW) and Modulated CW	Radiated and Conducted
High Intensity Radiated Field (HIRF)	Electronic Operation	CW Pulsed, CW and Modulated CW	Radiated
Electronic Counter Measures (ECM)	Hostile	CW and Modulated CW	Radiated
High Power Microwave (HPM)	Hostile	CW Pulsed, CW and Modulated CW, single or multiple Bursts of CW	Radiated
Ultra-Wideband (UWB)	Hostile	Pulse, single or multiple	Radiated and Conducted

Internally Generated Electromagnetic Environments			
Enviroment	**Type**	**Waveform**	**Propagation ***
Electromagnetic Emissions	Electronic Operation	Pulse, CW and Modulated CW	Radiated and Conducted
Electrostatic Discharge (ESD)	Natural	Pulse	Radiated and Conducted
SGEMP - Internal (Box and Cable)	Hostile	Pulse	Radiated and Conducted

*Propagation is the method by which energy arrives to the victim from the source

2.1.3. Methodology. The method of achieving UE^3 protection and survivability is through the use of EM barrier(s) plus special protective measures to protect Mission and Safety Critical Electronics (MSCEs). An EM protection barrier consists of two elements: one or more EM shields, and the necessary electrical and mechanical penetrations through the shield(s). To maintain the barrier effectiveness, penetration protection devices must be provided for all penetrations in the EM shield. Figure 1 illustrates the EM barrier protection concept applied to a multi-element system. (Note that this concept can be effectively applied to military hardware that has effectively no shield e.g., modern aircraft (OC5).) This protection concept is familiar to digital, circuit, integration and system designers; and, does not require the development of new design practices. The illustrated example employs multiple closed metallic EM barrier topologies to reduce the externally and internally generated EME stresses (conducted and radiated) to residual stress levels consistent with acceptable operation of the protected MSCEs. Choosing the acceptable operational levels and, in turn, the EM barrier performance requirements involves a process of balancing the externally and internally generated EME stresses, the MSCEs immunities, and the margin selected to control risk. The engineering trade studies necessary to achieve this balance are through the allocation process, illustrated in Figure 2, which is usually iterative and serves basically as a risk management tool. If the EM barrier concept is properly designed and implemented into military hardware, UE^3 protection and survivability can be achieved that is affordable and producible as well as verifiable, maintainable and sustainable throughout the hardware's operational life. Additionally, an integral and essential part of this methodology is testing, which is conducted throughout all four of the acquisition life-cycle phases to insure that the EM protection design is: adequate and complete during concept and engineering development, properly implemented during production, and properly maintained and sustained during deployment. Furthermore, the EM barrier protection concept facilitates unified testing by focusing on the barrier rather than individual E^3. Since this methodology can create benign internal EME stresses to which the MSCEs must survive, the EM barrier facilitates Diminishing Manufacturing Sources and Material Shortages (DMSMS) and technology insertions, especially COTS/NDIs, and upgrades/enhancements.

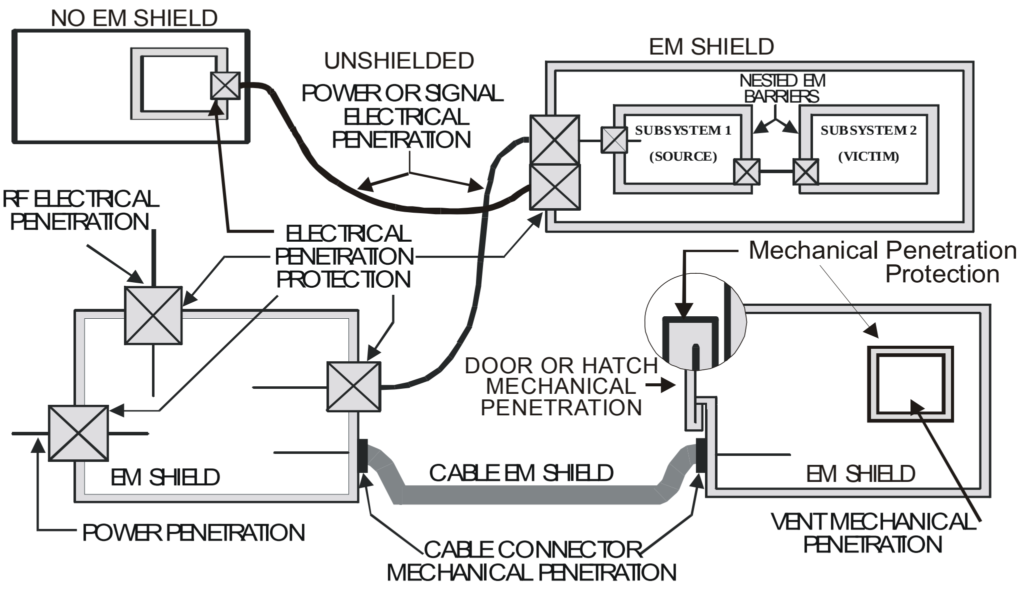
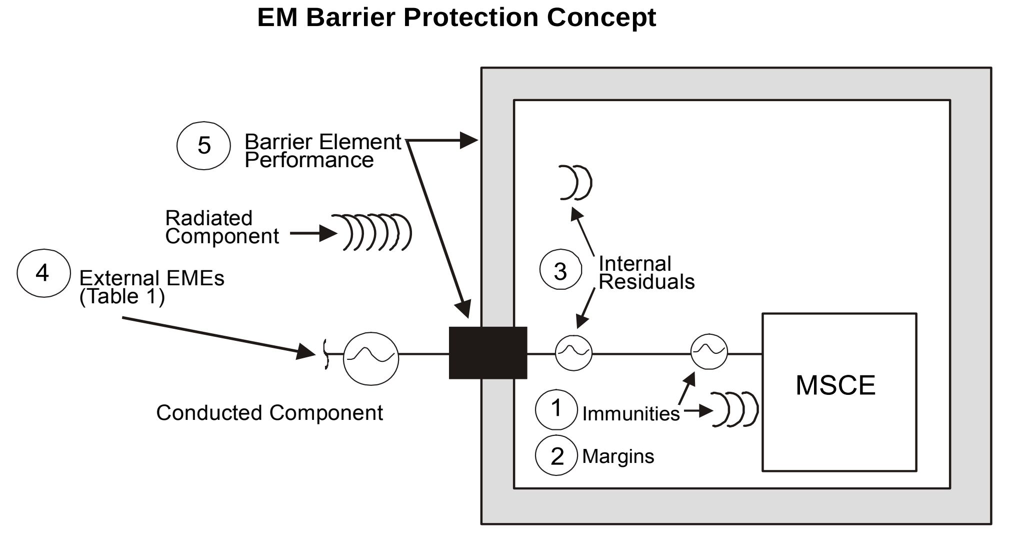


Figure 1. Multiple Barrier Topology Design



ALLOCATION EQUATIONS (db)

③ Internal Residuals = ① Immunity (MSCE) − ② Margin EQUATION 1

⑤ Barrier Performance Requirement = ④ External EME Stress − ③ Internal Residuals EQUATION 2

Figure 2. EM Barrier Protection Concept Keyed to Allocation Equations.

2.2 Scope for AEP-41

The general scope of this AEP is to document how affordable for all UE^3 survivability can be achieved, verified, produced and sustained for all six categories of NATO hardware using the EM barrier protection concept. This scope of work will be accomplished in the following seven volumes.

2.2.1. Volume I. This volume provides the philosophy and methodology for achieving affordable UE^3 protection and survivability through the use of the EM barrier protection concept. A discussion of how to apply the EM barrier protection methodology to achieve UE^3 survivability that is affordable, verifiable, producible and sustainable in today's and the future battlespace is provided.

2.2.2. Volume II. This volume provides the typical requirements for and defines and discusses the potential battlespace EMEs listed in Table 1 that military hardware must be protected against in order to be E^3 survivable in the battlespace. These EMEs interact with military hardware causing E^3, which are defined and discussed. Furthermore, military hardware (platforms, systems and equipments) of the six operational categories are discussed. 2.2.3. Volume III. This volume provides detailed discussion of E^3 coupling for the various classes of military platforms, systems and equipments defined in Vol. II. Understanding E^3 coupling is critical because the EM barrier is basically an E^3

management tool to insure that the resultant residual levels from the EME generated stresses are lower than the MSCE immunity levels by a realistic margin. (Margin depends on mission criticality of hardware and permissible risk; therefore, margin is usually 15-20 dB, which is adequate only if combined with a thorough life-cycle program.)

2.2.4. Volume IV. This volume discusses E^3 susceptibilities common to the six categories of NATO military hardware defined in Vol. II. How these E^3 susceptibilities occur, what they are, and how they affect these various hardware classes in the battlespace is discussed.

2.2.5. Volume V. This volume describes how to apply the EM barrier protection concept to achieve UE^3 protection and survivability against the E^3 susceptibilities described in Vol. IV resulting from the E^3 coupling described in Vol. III for the six operational categories of NATO hardware defined in Vol. II. Volume V also discusses why E^3 protection must be included early into the design of military hardware in order to be affordable, producible, sustainable as well as accommodating to insertions of DMSMS solutions and COTS/NDIs.

2.2.6 Volume VI. This volume discusses test and validation. A crucial part of achieving, producing and sustaining UE^3 survivability is a series of E^3 tests that must be performed during all phases of the hardware's life-cycle and tailored to the requirements of the hardware. The basic test types are: engineering development to support the design activities, acceptance (MSCE equipment immunity (both radiated and conducted) and barrier performance (shielding effectiveness and penetration protection devices)), final design validation, production compliance (under Hardness Assurance (HA)), deployment compliance (under Sustainment Assurance (SA)), and Surveillance Test (ST). Both HA and SA includes engineering-type tests and analysis, as necessary, to evaluate and validate that configuration, MSCE, and material changes do not degrade the E^3 survivability level of the hardware by increasing risk to unacceptable levels.

2.2.7 Volume VII. This volume discusses hardness and sustainment assurance, and surveillance test. The test and validation aspects of design, engineering development, and hardness assurance are presented in Vol. VI and will be briefly covered in Vol. VII for completeness. Consequently, Vol. VII focuses on sustainment assurance and surveillance test. The objective of a hardness and sustainment assurance program is to establish technical and management activities to ensure that UE^3 survivability achieved and verified during the Engineering Development Phase is not only produced, but, is also preserved throughout the hardware's Deployment Phase or its operational life. Also discussed are methods and guidelines on how to accommodate material changes, technology/DMSMS insertions and associated circuit additions, MSCEs upgrades and modernizations without degrading E^3 survivability to unacceptable risk levels during deployment. Finally, surveillance tests (and analysis) to periodically validate adequacy of both hardness and sustainment assurance programs are discussed.

2.3 Requirements

Military hardware of the six operational categories must not only be electromagnetically compatible within themselves, but must be electromagnetically compatible as well as survivable to a myriad of changing EMEs in the battlespace. This EMC (intra-system/platform and inter-system/platform) and survivability must be readily achievable and affordable as well as producible, maintainable and sustainable throughout the hardware's life-cycle. EMC, survivability, and EME requirements are provided in Sect. 4 of Vol. II.

The barrier performance requirements critical to achieving affordable, producible and sustainable UE^3 protection for NATO military hardware of the six operational categories are discussed in Section 4.0 of Vols. I, III and V. The E^3 performance objectives are established from the mission needs, E^3 protection criteria and concepts, and the selected E^3 survivability options (may require combinations of UE^3 barrier protection with alternate and/or special protective methods to achieve survivability). The performance objectives consist of: need to protect against specific EMEs, level of protection required, amount of allowable risk associated with the protection and, as needed, limits on hardware impacts related to E^3 protection. See Vol. 1, Figure 12 for illustration and Para. 4.2.2 for discussion. It is important that the E^3 performance objectives be clearly defined early in a program, since they drive performance specifications as well as all subsequent UE^3 protection design and engineering and acceptance test activities, affordability, producibility, sustainability, and flexibility of design.

3.0 AEP - 41, VOLUME IV, EXECUTIVE SUMMARY

3.1 INTRODUCTION TO VOLUME IV OF AEP-41

The importance of discussing susceptibility is to understand that different systems could experience catastrophic upset or damage that could cause the system not to meet its operational performance requirements. Figures 14 and 15 of Vol I illustrate the concept of UE^{3}P without having to establish the exact susceptibility levels for each of the six Operational Categories of NATO military systems. Rather UE^{3}P establishes acceptable internal residual signal strengths by looking at AECTP 500 (equipments, subsystems, systems and platforms) tests to keep signals at or below unacceptable upset or damage thresholds. The goal is adequate margins.

The EM barrier described in Volume I is a generic term covering all methods of EM protection. Usually the barrier consists of one or more electromagnetic shields and controlled mechanical and electrical penetrations through the shields. However, it also covers filters, lossy materials, circuits and software design measures. The required protection and hardening measures are based on the Unified Barrier Performance Requirements (UBPRs) (Vol. 1 Para 4.2.3.4.3) which must consider both linear and non-linear effects (see Vol. I, Section 4 and Vol. V, Section 4.3 and 4.4). The hardening and protection measures are required for susceptibilities that occur in all military equipments, subsystems, systems and platforms (developed, COTS or hybrid of both) from internal stresses produced by electronic/electrical operations and from external stresses produced by operational, hostile and natural EME sources (see Vol. II, Table1). These susceptibilities occur throughout the military hardware's life-cycle. Fortunately it is not necessary to determine, in general form, susceptibility or immunity (on each equipment) for a plethora of aggressive stresses generated by the set of EMEs.

3.2 SCOPE

3.2.1 Susceptibility. Susceptibility is an undesired reaction of hardware when subjected to an EME threat. This volume provides details of the susceptibilities that are one of the main features of the UE^{3}P process defined in Volumes I, II, III and V. Volume VI concerns validation testing of military hardware against battlespace and peacetime EMEs and Volume VII discusses life-cycle management.

Initial susceptibilities of MSCEs are estimated by the design engineer through modelling, experience and/or some laboratory test. However, susceptibility levels are usually determined by immunity tests (see Section 4.0 of this volume) as a function of all relevant stress parameters (e.g., frequency and time domain, radiated and conducted stress, and tolerated degradation of hardening and protection device/component). In this way, it is possible to determine whether susceptibilities exist within the standard and a check of the barrier protection adequacy.

3.2.2 Layout of Document. The Executive Summary of AEP - 41 is a part of all volumes and allows the reader to get a quick overview about the intention and the UE^{3}P methodology of this AEP. Thereafter, the special intentions of Vol IV are presented in Section 4.0, where the procedures and means are described for susceptibility. Shown in Section 4.0 is how susceptibilities are based on classical immunity tests and how susceptibilities can be inserted into the life-cycle phases of defence materiel. Finally, the summary and the conclusion are provided in the final two sections of this volume.

4.0 E^3 SUSCEPTIBILITIES OCCURRENCE, NATURE AND EFFECTS

PREAMBLE

Technological advances have to be taken into account when identifying the E^3 susceptibilities and how they affect the various hardware classes in the battle space. The start point for the analysis is the definition of the future battle space, on the basis of the NATO "Long Term Scientific Study 49 on Land Operations in the year 2020".

The future battle space will be variable in density, non linear and more dispersed. It will be cellular in nature, multi-directional and increasingly determined by what is above the battlefield in air and space. Force structures will need to change in order to exploit technology to the fullest. The following broad technology areas are deemed to be of special importance:

- High Power Electrical Technologies
- Directed Energy Weapons
- Computing Technologies
- Communications Technologies
- Electronic/Information Warfare Technologies

- Electronic Devices
- Biotechnologies
- Structural Materials Technologies
- Human Factors and Man-Machine Interfaces
- Precision Attack Technologies
- Automation and Robotics

The technologies areas mentioned above will be used for several applications, like Precision Attack, Sensing, Information fusion, Digitisation, Non-Lethal Weapons and Barriers, Robotics, Simulation and Synthetic Environments, Netcentric, Modular System. In this scenario, an increase in EMI sensitivities is expected due to: higher operating frequencies of digital electronics, smaller feature sizes, more energy sensitive technologies, continued evolution to lower operating voltages for circuits and devices, increasing use of plastic encapsulated microcircuits (less inherent shielding), higher densities (both within packages and circuits) and increase use of COTS/NDIs.

As an example, digital circuits have to coexist with analog circuits in more products than before. Unfortunately, analog circuits are usually susceptible to continuous conducted radio-frequency interference, while digital circuits exhibit high susceptibility to pulsed conducted interference. Thus, interference collected into complex ICs induces intermodulation, cross-modulation, rectification and other deleterious effects that cause upsets in the operation of the circuits.

Future COTS could actually be less susceptible to radiated fields. This point results from the reduction of the size of the components outweighed by their very large scale of integration capable to greatly reduce direct couplings. On the other hand, their fragility to the conducted interferences will be increased. This results from:

- their reduced size;
- the conservation of the coupling on the tracks of the mother boards and on the wires for the external bindings to the box which length will be maintained (ergonomics of the user work station).

In this way, signal integrity and EMC are closely related fields especially because there are some products that send signals between devices or systems on copper at hundreds of Megabits (or even Gigabits) per second. At these data rates, the distinction between the signal integrity and EMC is blurring.

The increasing use of these sophisticated electronics in the design, production and, especially in the maintenance/repairs/upgrades of military hardware emphasizes the importance of applying an encompassing, versatile UE^3 protection scheme like the EM barrier protection concept.

It is especially important that the UE^3 protection concept be incorporated early into hardware design in order to be affordable, achievable and accommodating to future changes involving MSCEs that may introduce lower immunity levels.

4.1 Introduction

4.1.1 General

This Volume discusses E^3 susceptibilities common to the six categories of NATO military hardware defined in Volume II.

Electromagnetic energy coupled into a system through deliberate antennas, via penetrations, or directly to internal circuit wiring due to apertures can degrade the system performance. The degree of degradation is a function of many factors related to the normal operating mode of the system, the mission of the system and the components utilized in the system.

The purposes of this chapter are to present the mechanisms which cause performance degradation, what the susceptibilities are and how they can affect the six categories of NATO military hardware defined in Volume II.

In order to understand the discussion that follows, it is necessary to clearly define the terminology that will be used in this and subsequent sections of this chapter.

The terminology to be defined here relates to the ability of a system to perform its mission in the presence of an EME.

Several definitions are included in Volume VI. In order to provide a well defined meanings to the terms used in this Volume, a list of some definitions are listed below [See reference 1].

4.1.2 Definitions

System - a combination of apparatuses and/or active components constituting a single functional unit and intended to be installed and operated to perform (a) specific task(s).

In the context of this document, a system may consist of several sub-systems which are each comprised of several equipments which, in turn, consist of several components. Figure 3 shows a typical system architecture.

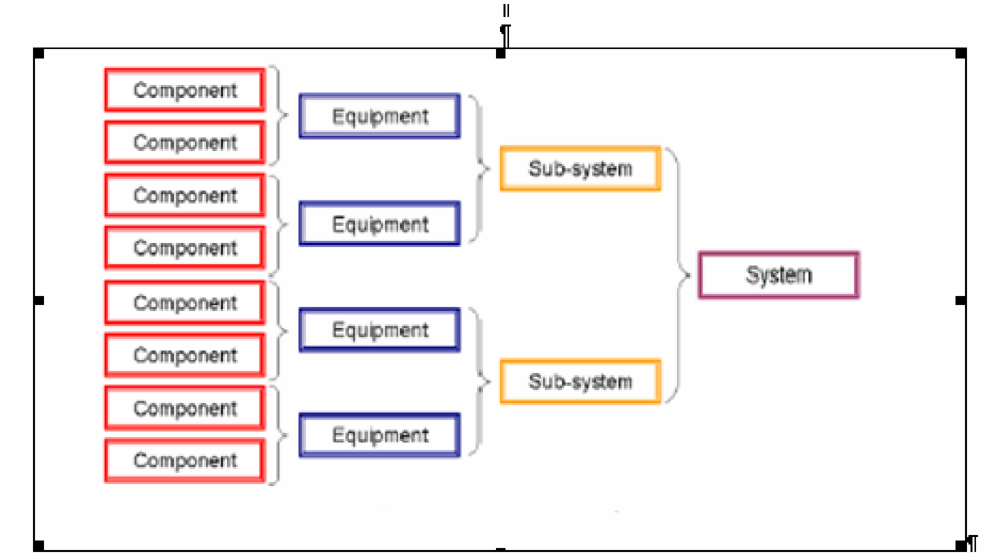


Figure 3: Example System Architecture

For example, a vehicle (system) may consist of an engine management unit (sub-system) which consists of circuit boards (equipment) and integrated circuits (component).

A system can also be considered to be a set of supplied equipments located within a defined physical boundary that are interconnected in order to perform a defined function.

The defined physical boundary may be: the outer hull (for systems located on military platforms - land vehicles, aircraft and ships); the outer building wall (for systems located within buildings).

The interconnection may be either: wireline (using either metallic or optical cables) or wireless and is made for the purpose of either exchanging information or receiving electrical power.

Any physical connection (i.e. wireline or wireless) with a supplied equipment that does not originate from within the System's defined physical boundary is an interface. Interfaces may be permanent (in the case of buildings, where a permanent connection with wireline power and telecommunications infrastructure can be expected) or temporary (in the case of military platforms, where the inherent mobility of the platform prevents permanent wireline interfacing).

Individual supplied equipments may themselves be individual systems (i.e. sub-systems, or sub-sub-systems et. al.) that should themselves have been subject to the methods container within this document.

Installation - a combination of apparatuses, components and systems assembled and/or erected (individually) in a given area. For physical reasons (e.g. long distances between individual items) it is in many cases not possible to test an installation as a unit.

Equipment - this term is not limited and includes modules, devices, apparatuses, sub-systems, complete systems and installations.

E/E/PE Equipment - equipment that employs electrical, electronic, or programmable electronic technologies.

Coupling - the transfer of electromagnetic energy from source to victim.

Front Door Coupling - the coupling of EM energy to equipment via antennas and/or sensors.

Back Door Coupling - the coupling of EM energy to equipment via connecting cables or apertures (not via antennas or sensors).

Immunity - the ability of a device equipment or system to perform without degradation in the presence of an electromagnetic disturbance (IEC 50(161):1990 and others).

Susceptibility - the inability of a device, equipment or system to perform without degradation in the presence of an electromagnetic disturbance (IEC 50(161):1990 and others). Susceptibility is often characterized as a lack of immunity. The threshold of susceptibility is the level of interference at which the test article begins to show a degradation in performance. This is often frequency dependent.

Susceptibility Degradation Criteria - a delineation of the essential safety and performance characteristics for an equipment under test (EUT) and the allowed degradation of these characteristics during susceptibility testing.

Susceptibility Level - the electromagnetic noise environment in which a device or equipment can operate satisfactorily.

Susceptibility Margin - difference between the threshold of susceptibility for a device or equipment and the environmental levels to which it is exposed.

Cable Coupling Regime - the cable coupling regime refers to the frequency range where cable coupling dominates. This is typically between 500 kHz and 400 MHz.

Degradation - performance degradation is the deterioration of some feature of a system in response to an undesired EME.

Aperture Coupling Regime - the aperture coupling regime refers to the frequency range where aperture coupling dominates. This is typically between 200 MHz to 18 GHz.

Pulsed Current Injection (PCI) - the use of current injection methods to assess for immunity or susceptibility with a pulsed waveform as opposed to more traditional continuous wave (CW) signals.

Surface Current Injection (SCI) - the injection of current directly on to the surface of an equipment box of system skin.

High-Level Illumination (HLI) - the use of high level (>100V/m) signals to assess for immunity or susceptibility.

Low Level Continuous Wave (LLCW) - the use of low level signals (typically <1V/m) to characterise the coupling of an external electromagnetic environment to an internally induced current, voltage or field (magnetic or electric).

Norm - a mathematical function used to describe a parameter of a waveform, several norms can be used to describe the ‘uniqueness’ of a waveform.

Margin - usually expressed in dB this is the amount added to a result to improve confidence or to allow for uncertainties.

4.2 Component and System Degradation

4.2.1 Types of Degradation in Electronic Systems.

EME coupled energy may affect an electronic system performance temporarily or permanently. Temporary effects are those which disappear along with or shortly after the disappearance of EME. For example, transient circuit disturbances resulting from EMP may be interpreted by the circuit as signals. Information errors may be introduced when such disturbances appear in the form of noise, deteriorating the signal-to-noise ratio for the circuit.

Most EMP-induced transients in electrical circuits are regarded as sources of temporary effects, although transients can lead to "latch-up" of a circuit or a semiconductor, thus requiring a reset before normal operating function can be restored. For example, flip-flops may be triggered by transients, counters can change count, memory can be altered due to driving current or direct magnetic field effect resulting from the transients, etc. Transients, as signals, may also be amplified in electronic circuits and the amplified signals may be interpreted as control signals by the circuits. Such control signals in turn may result in a system malfunction by providing controls where they are not needed or by altering the degree of control [See reference 2].

Because of numerous variables are involved in the prediction of susceptibilities due to EME transients, (magnitude of the "true" or "false" voltage level, switching time of the active semiconductors, circuit inductances and capacitances, magnitude of bias voltage in circuits, schematic of the circuit and its physical layout, etc.), it is difficult to present a comprehensive analysis or a methodology for the prediction of susceptibilities due to EME transients. Some generalization, however could be attempted regarding the response of digital circuits due to EME transients. First, the most sensitive lead on a digital circuit is usually the input lead, although the ground lead or dc-power lead could be as sensitive or more sensitive in some cases. Secondly, one can anticipate that at low frequencies, the threshold of the circuit can be related to its normal operating levels, or logic voltage levels.

4.2.2 Permanent Effects.

Permanent effects, in turn, have lingering consequences. Circuit latchup or burnout of components (damage or failure) are examples of permanent effects. Malfunctions due to both temporary and permanent effects could be of concern and they are referred to as EME susceptibilities.

The latchup is distinguished from the circuit upset discussed earlier, since in latchup the circuit is not automatically restored and the power into the circuit has to be removed for the restoration of the circuit. A latchup due to an EME-induced transient can occur when the transients flowing through the circuit cause a relay or switch to latch-up. A latchup can also occur within the semiconductor. For example, the Negative charge-Positive charge-Negative charge- Positive charge (N-P-N-P) or silicon-control-rectifier can be latched into conductance by an EMP-induced transient and the power into the circuit has to be removed to unlatch.

The possibility of a latchup of a circuit will depend on the type of circuit under consideration, and certainly many circuits do not latchup. The susceptibility due to latching, therefore, may not exist in many cases. For cases where the possibility of latch-up exists, one has to trace the path of the EME-induced transient and determine the threshold signal for the latch-up either by an examination of the circuit or by a circuit analysis.

In addition to latchup, an electronic system can be affected almost permanently by EME coupled energy, particularly when such energy causes components burnout. There are various system components which could be susceptible to burnout in an EME environment, the most sensitive of which are the semiconductors. EME-induced burnout can, of course, occur also for other circuit components, such as resistors, capacitors, inductors, transformers, relay coils, vacuum tubes, etc.

At the component level, susceptibility is usually determined empirically and may be expressed in terms of a threshold. For equipments, subsystems and systems, certain coupling modes and component thresholds are implicit in the determination of the susceptibility characteristics. A knowledge of susceptibility permits a determination of the performance degradation for various conditions of exposure.

The reduced capability of a component, equipment, subsystem or system is termed degradation of performance. The degradation may be determined by jointly considering the susceptibility and the environment (stimulus) or more directly by experimental methods.

In some cases, some performance degradation can be tolerable. When the performance degradation exceeds the limits of satisfactory performance due to a stress, the system/component is considered vulnerable to that stress.

There are two types of degradation. They are:

1. Functional damage and
2. Operational upset.

Functional damage refers to permanent damage due to an EME, while operational upset refers to temporary impairment due to an EME.

For example, if a system becomes permanently damaged due to a large electrical transient, it is said to have suffered functional damage, whereas the temporary impairment of a system’s operation due to a smaller electrical transient is known as operational upset.

There are likely to be a variety of failure criteria. These may be broadly classed into three categories:

1. Catastrophic failure refers to a device which could not be expected to operate satisfactorily in any circuit
2. Parametric failure refers to a device where parameter degradation has proceeded to a point where the circuit, although it continues to operate, will do so at reduced efficiency or lowered performance and
3. State failure refers to an undesired change of state of a circuit.

To define failure, therefore, it is necessary to consider the allowable degradation of performance of a component, circuit, equipment, subsystem and system. When this allowable degradation has been exceeded, failure has occurred.

4.2.2.1 General Damage and Upset Considerations

In order to assess EME effects on a system, it is necessary to determine if the system will properly respond once the stimulus conditions have been damped out. These predictions require a knowledge of the threshold levels at which component fail (damage) and the threshold levels at which circuits temporarily malfunction (upset).

The assessment problem is further complicated since for a component to fail or a circuit to upset, sufficient energy must reach the sensitive component or circuit. This energy collection and transfer problem is highly dependant on the system physical and electrical characteristics which determine the total available energy at the sensitive component, and the waveshape and fundamental frequency of the induced voltage and current at the sensitive component.

4.2.2.2 Component Failure

A number of damage mechanisms have been observed for electronic components subjected to EME threats. Some of these are:

- Dielectric breakdown
- Thermal effects and
- Interconnection failures.

The voltage at which dielectric breakdown occurs is a function of the material and the thickness of the material. Breakdown can occur in all types of insulating layers if the voltage stress is high enough and applied for a sufficient time. In the case of insulators, this generally occurs as surface breakdown. In the case of electronic components, it may occur as surface breakdown or internal breakdown.

Thermal effects result from the dissipation of energy in the component due to excessive current flow. This is a major cause of semiconductor junction failure and resistor burnout. Thermal effects may also be responsible for such failures as spot welding of relay contacts, and detonation of electro-explosive devices employing bridge wires.

Interconnection type failures result from the induced electrical transients increasing the temperature sufficiently to cause melting of metal surface connections, beam leads on integrated circuits and the wire in wirewound resistors.

Semiconductor Device Failure

The initial understanding of semiconductor device failure is best obtained by considering a single p-n junction. Subsequent extrapolation phenomena to multijunction devices are relatively straightforward.

The principal failure mechanisms for a single p-n junction are, for reverse voltages, surface breakdown around the junction, dielectric breakdown and internal breakdown through the junction within the body of the device, whereas for forward voltages the internal breakdown is in the body of the device.

The destruction mechanism of a surface breakdown is a leakage path around the junction, thus nullifying the junction action. The junction itself is not necessarily destroyed and re-etching the surface can return the junction to normal operation.

The problem of theoretically predicting surface breakdown is difficult since it depends upon many parameters such as geometrical design, doping levels near the surface, lattice discontinuities on the surface and general surface conditions.

Junction failure due to dielectric breakdown is a result of a large avalanche current which forms a path for an arc discharge to occur. This can result in a puncture through the junction with an actual pinhole being formed, resulting in a junction short.

Most semiconductor dielectric layers are thick enough to withstand severe electrical transients. Thin layers, such as those found in fast switching devices can breakdown at dc voltages ranging from 30 to 200 Volts. Dielectrics can withstand higher transients and ac voltages, but if the transient persists long enough for avalanching to occur, dielectrics can still be damaged.

In internal body breakdown, the destruction mechanism apparently results from changes in the junction parameters due to localized high temperatures within the junction area. These temperatures can be of such magnitude that alloying, or diffusion of the impurity atoms occurs to such an extent that the junction is either totally destroyed or its properties drastically changed. The current may be sufficiently high and localized to cause melting at hot spots within the junction. Such action can result in a resistive path(s) across the junction which develops after resolidification of the melted spots at the junction. The primary effect on device operating characteristics is manifested as a decrease in diode breakdown voltage and an increased leakage current, while in transistors decreased gain and increased junction leakage currents are observed.

The major cause of semiconductor failure occurs under reverse bias conditions. This failure mechanism is termed "secondary breakdown". The voltage-current curve for a p-n junction indicates that for low reverse voltages the device conducts only a very small current. As the reverse voltage increases, breakdown occurs with a resulting increase in current flow.

Many different microscopic mechanisms may contribute to semiconductor failure. However, most of these mechanisms have been found to be linked primarily to the junction temperature. Therefore, in most cases, the treatment of the problem can be reduced to a thermal analysis. The worst case as far as achieving high temperatures in the junction is when one considers that all of the power dissipation in the device occurs in the junction. This corresponds to the situation where a high voltage pulse of reverse polarity is applied to a junction with a high reverse voltage breakdown. When the avalanche breakdown occurs, almost all of the applied voltage is dropped across the junction and only a small percentage is dropped across the bulk material (except for a very short pulse).

Wunsch and Bell developed a theoretical model for the junction failure due to the temperature rise, for one-dimensional heat flow corresponding to a plane junction in an infinite medium [See reference 3].

Integrated Circuit Failure

Integrated Circuit (ICs) employ large number of junctions on a single chip. Depending on the type of IC, it is possible that the state of the logic (digital logic circuit) voltage at one input will affect the burnout level when a pulse is applied to another input. This was investigated for several circuits and it was determined that the gates fail independently and the state of the logic voltage at the other inputs did not affect the burnout level. The input and output of an IC are more susceptible to transient damage than the positive battery lead. This is not an unexpected result since a transient entering via the positive battery lead would be distributed over a number of p-n junctions in the device.

Interconnection Failure Modes

The vulnerability of device leads, metallization patterns and lead bonds, for the most part, can be considered as a thermal problem. In this case, the problem reduces to that of considering heat dissipation due to system thermal conductivity up to its melting point, together with an assessment of the dynamic stress conditions produced at material discontinuities. In general, one would expect that at least the leads and metallization patterns should exhibit a fairly uniform current density throughout their material cross sections for relatively moderate pulsewidths as compared to the current constriction sites in semiconductor junctions which can be altered by defect and bias conditions.

For relatively short pulses, such a phenomenon as skin effect would, of course, alter the cross sectional current density in such a way as to produce a "peripheral current constriction" condition. These effects, though, are fairly well defined and can be considered in a rather straightforward manner. In general, it is observed that the vulnerability of the interconnection system usually occurs at current levels in excess of those required to cause significant junction damage in typical semiconductor devices at hundred nanosecond pulsewidths.

Resistor Failure

Resistive elements in the form of either lumped resistors or diffused resistors often are the terminating elements for long cables. Consequently, information on the way these devices fail and typical failure levels are important. Tests have been conducted on wire wound, metal film, carbon composites and diffused resistors.
Four types of failure have been found. These are:

1. Resistance value change: failure is defined as a change in value beyond normal tolerance. The importance of this change is dependent on the circuit function. This mode of failure can be due to thermal effects (energy dissipation) or voltage stress induced.
2. Internal breakdown: this breakdown occurred when the resistors under test opened but did not blow apart or no external evidence of arcing was present. This was due to thermal dissipation with the device.
3. Arc across resistor casing: this type of breakdown was exemplified by an arc across the external surface of the resistor. No damage to the resistor resulted from this failure.
4. Catastrophic breakdown: this type of breakdown occurs when an external arc starts across the resistor, but due to some defect in the ceramic casing, re-enters the core. The pulse energy is then dissipated in only a small fraction of the resistor and causes the casing to rupture (blow off) and the resistor to open.

Capacitor Failure

Tests on capacitors have been limited in types of studies and component sample size because they have been considered to be much harder than other electronics components such as semiconductors and thin film resistors. These limited studies have indicated that some capacitors types fail at levels as low as those seen for semiconductors. Therefore, consideration should be given to the failure levels of these components because if the semiconductors in the circuit are protected, the non- semiconductor components may determine the resulting EM vulnerability.

The basic failure mechanism in capacitors is internal (dielectric) breakdown. For ceramic type capacitors this breakdown is very abrupt. The amount of post breakdown degradation was related to the energy dissipated in the capacitor during breakdown.

In the case of low voltage tantalum electrolytics, the breakdown characteristics are quite different. The abrupt breakdown was not observed but the leakage resistance decreased progressively until breakdown occurred. As the leakage current increases, dissipation in the devices decreases and the sustained voltage decreases.

Inductive Elements Failure

Inductive elements can fail similar to capacitors and resistors whereby a temporary impairment such as an arc-over or saturation occurs such that the characteristics of the inductive elements are not impaired on a long-term basis. Similarly, a catastrophic failure can occur such as an arc-over and punch-through for the insulation similar to the capacitor insulation or semiconductor surface failure.

Studies to date on inductive elements per se have been quite limited owing to the relative hardness of these devices in comparison to the more susceptible semiconductors and passive thin-film resistor elements.

Cable and Connector Failure

Other very important system components that may be functionally damaged by induced transients are cables and connectors. This is particularly important for cables that are already electrically stressed such as transmitter output cables. The difference between the voltage applied to the cable by the transmitter and the voltage breakdown rating of the cable may be sufficiently small that the EM induced transients will cause breakdown of the insulation or air space in connectors.

The breakdown strength of cable insulation may be limited by the dielectric strength of small imperfections in the insulation. Within the body of the cable, breakdown starts from a small air pocket. At first, discharges take place in the pocket. This produces local heating. The insulation melts and carbonizes and ultimate failure occurs, either through mechanical effects or due to a short circuit produced by a carbonized track across the dielectric from one conductor to another. A mechanical effect that can occur is for distortion of the dielectric to occur resulting in the inner conductor becoming eccentric and touching the outer conductor.

4.2.2.3 Effects of Operational Upset

The effect of operational upset on system performance and mission is highly dependent on the system design and use. In some systems, loss of synchronization for as long as few milliseconds is of no great importance. On the other hand, loss of stored information in a computer may require re-boot of a very long computer program, thus delaying the operation of a specific system.

The trajectory control of a spacecraft or missile is an example where operational upset for a very short time may be of considerable significance.

Some functions performed by a computer may be impaired by relatively long periods of circuit upset. Others may be impaired by short periods of upset. For example, in a power station computer, functions as data logging, scan and alarm, performance calculations and trend recording may be relatively unaffected by operational upset. On the other hand, process control functions such as turbine start-up, boiler set point control, and combustor control may be affected to a much greater extent.

Large amounts of energy may be collected by power lines and cause circuits breakers to open. The time to re-energize the system may cause its function to be seriously impaired. Also, since a considerable amount of generator's load could be dropped, undesirable effects might occur in the generating and transmission system.

Upset is defined as, for example, the unintentional toggling, or change of state, of a digital device. For an individual device, upset is usually assumed to be produced by transients that are smaller than those required to produce component damage (this is certainly true for usual switching signals, but there may be some waveforms for which it is not true).

On the basis of this assumption, it may be asserted that less EME protection is required to prevent damage than to prevent upset. However, in a system containing many devices, it is not valid to conclude that upset occurs at a lower stress than damage. All elements are not exposed to the same stress; some elements can be stressed to the damage level before others are upset. If EME stresses exceed the dielectric strength, insulation may be damaged in exposed regions before circuits are upset in protected areas. If insulation breakdown causes power circuits to be connected to signal or control circuits, serious circuit damage can occur at stress levels that did not produce circuit upset. It is not unusual for system damage to occur before upset in system-level EME tests.

Digital electronics are used in modern systems because small and low-power circuits can control large systems: small-signal errors in either the processing or the control signals can propagate through the system to produce disastrous errors in the output.

In some cases, the consequence of logic upset is system damage. A dramatic example is an upset rocket guidance system that erroneously commands a manoeuvre that destroys the vehicle. Thus, in cases where upset occurs before direct electronic damage, the final result is sometimes serious system damage. And the distinction between upset and damage is blurred.

It is important to recognize that misdirected system energy, rather than energy extracted from the EME for a correct system functionality, is often the cause of EME-induced damage in systems.

Because the distinction between upset and damage is not clear at the system level, EME protection should be based on preventing both upset and damage.

4.2.3 MSCEs Susceptibilities to E^3

Two types of relevant coupling paths exist. The first is the penetration of radiated EM fields through space or shields and the second is the penetration of currents and voltages on a conductor or through protective devices, like filters or non linear elements.

The primary coupling process of the battlespace EMEs (see Table 1) is radiated coupling on the exterior equipment cables and/or conductive surfaces. Exceptions are DSL, P-Static and ESD. Examples for radiated coupling are described in Vol. III, Sections 4.3 to 4.6. There, the coupling to vertical or horizontal conductors, to Printed Circuit Boards (PCBs) and MSCE components, the coupling onto shields and to its interior cables, are discussed in detail. The result of radiated coupling is a current or voltage wave coupled onto a conducting material, like the shield of an enclosure or cable. These current or voltage waves serve as new EME sources for radiated stress or for conducted stress to equipment inside the enclosure and are the primary sources for the effects on MSCEs (see Figure. 2, Section 2.1.3).

The induced current and voltage waves on shields, cables, wires, or on PCBs are the direct carrier of the conducted stress to internal MSCEs. The measure of the coupling to conducted material and the measure of the stress to MSCEs, have to be related to waveform Norms of the external and internal EMEs. These waveform Norms lead to the relevant Stress Transfer Function (STF), (See Volume V).

The necessary UE^{3}P measures depend to a high degree on susceptibility or at least on immunity levels of MSCEs. Normally, susceptibility levels of MSCEs will be determined in the allocation process for military hardware, if the hardware is vulnerable against the considered recommended Battlespace EMEs. Of course, in this case, EM hardening is required. Otherwise, immunity levels will only be determined to avoid tests with unrealistic high stress amplitudes.

The known susceptibility levels usually cannot be applied directly for the Unified Stress Quantification (USQ) (See Volume V). The reason is that these levels are determined with respect to the existing standards and not to a unified EME. But, indirectly, important information for UE^{3}P can be extracted by comparing the stress of the applied existing standards with the stress of the unified EME. It is possible to compare the amplitudes, frequency band, pulse duration, pulse sequence or generally the waveform Norms. The best way to avoid redundancies in UE^{3}P should be to link susceptibility levels only to unified stress.

4.2.4 Classification of Effect

The terms immunity and susceptibility have subtly different definitions when used by commercial and military EMC communities. In the military community, equipment is only immune when no effects are observed up to the specified test level. If an affect is observed the equipment is said to be susceptible. It is only when this susceptibility has an impact on the mission of the equipment that it is deemed to be a vulnerability. In the commercial community, equipment can show effects during testing and still be ‘immune’ as long as there is deemed to be no degradation to the performance of the equipment.

Thus, a transient non-critical effect (such as screen interference on a computer monitor) would be deemed as a susceptibility in the military community. If this effect did not degrade the performance of the equipment, the commercial community would state that the equipment is immune.

Figure 4 shows a flowchart that explains the correct assignment of terminology according to IEC definitions for the HEMP [See reference 4]. High Power Electromagnetic (HPEM) environment includes: Direct Strike Lightning (DSL), HEMP, High Power Microwave (HPM) and Ultra-Wideband (UWB) (See Table 1 of Vol. I).

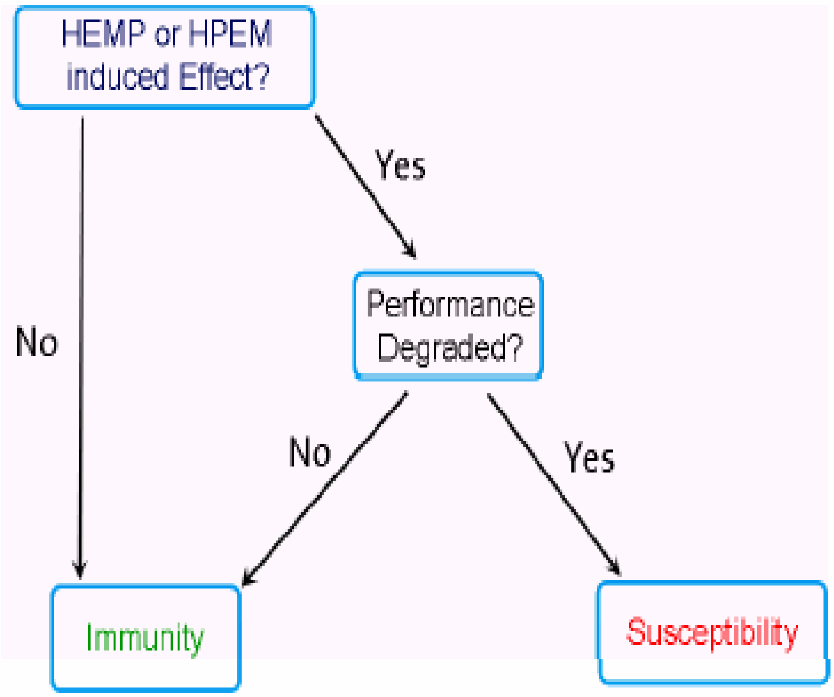


Figure 4: Classification of effect

Effects can be further categorised by:

1. Attributes of the physical interaction mechanism

2. The impact of the effect on the main (or critical) function of the system and

3. Duration and the need of human intervention, to recover normal operation.

Classification by attributes of the physical interaction mechanism contains less sufficient information to assess the effect with regard to operational value or the main function. For example, a bit flip that occurs only during the exposure to an UWB environment can be detected and corrected by channel coding. Even if the coding is not able to correct the bit flip, the system will be back to full operation after the environment has been removed.

Consequently, classification by attributes of the physical interaction mechanism is not in the scope of this document and is not considered further.

4.2.4.1. Classification by Criticality

For a practical assessment of EM induced effects it is necessary to classify the observed effects with regard to the operational impact, the functionality of the system and operational condition (e.g. critical periods of time, critical functions, minimum performance). Nitsch and Sabath [See reference 5] introduced a classification of effects by its criticality for the main function or mission. Table 2 provides the essential information on the functionality isolated from its duration and physical mechanism.

Table 2 Categorisation of effect by Criticality

Level	Effect	Description
U	Unknown	Unable to determine due to effects on another component or not observed.
N	no effect	No effect occurs or the system can fulfil its mission without disturbances.
I	interference	The appearing disturbance does not influence the main function or mission.
II	degradation	The appearing disturbance reduces the efficiency and capability of the system.
III	loss of main function (mission kill)	The appearing disturbance prevents the system from being able to fulfil its main function or mission.

As classification by criticality requires analysis of the observed effect and its impact on the function of the system with regard to a particular application, this classification scheme depends on the system's application and its operational conditions. As a result the assessment usually requires the assistance of a system specialist, who is familiar with the system under test.

4.2.4.2. Classification by Duration

Other than the criticality, the duration of an effect provides essential information on the susceptibility or vulnerability of a system under test. For example, degradation could be acceptable if the system recovers without human intervention some time after the environment has been removed. Classification based on the duration of the effect is shown in Table 3.

The main advantages of this method of classification are that effects are characterised (1)independent of the particular system and the main function or (2) by objective criteria.
However, the decision between category T and H does not support aspect (2) without restrictions. At this point the reliance on human intervention requires some explanation. In most cases a hang-up in a software or program (e.g. in the system software) can only be solved by a manually initiated reboot of the computer or a restart of the software. The situation becomes more complicated if the system software of an IT system (e.g. computer network or server) runs through an automatic reboot but the status of normal operation requires a manual start of application software (or data stream). Some test engineers tend to classify this situation as category "T" as the system itself recovers without human intervention. As the main function needs the manual start of software the situation can be

categorized as “H”. In reality, the decision depends on whether the test focuses on the main application (this will lead to H) or the basic system (T).

Table 3: Categorisation of effect duration

Cat.	Duration	Description
U	unknown	Unable to determine due to effects on another component or no effect is observed or no effect occurs.
E	during exposure only	Observed effect is present only during exposure to EME’s; system functionality is completely available after HPEM environment has vanished.
T	some (follow-up) time after exposure	Effect is present some time after EME has vanished, but system recovers without human intervention. Follow-up time is shorter or equal to typical reaction/operation cycle of the system.
H	Resistant until human intervention	Effect is present till human intervention (e.g. reset, restart of function). Due to the effect the system is not able to recover to normal operation within an acceptable period (e.g. typical reaction/operation cycle of the system). No replacement of hardware or reload of software is necessary.
P	permanent or until replacement of HW / SW	Effect is permanent; intervention of an operator or user does not recover normal operation. Effect has damaged Hardware (HW) to the point that it must be replaced or Software (SW) to the point that it must be reloaded.

4.2.4.3. Combination of Both Classification Schemes

When considering the operational efficiency or operational restrictions which are caused by the EM environment, criticality as well as the duration of the status (effect) can both be necessary information. As classification by criticality (Table 2) and classification by duration (Table 3) present the information as a function of one isolated criterion, both classifications can be combined. Combinations with practical relevance are listed in Table 4.

Table 4: Combination of Criticality Level and Duration Category

		Criticality Level				
		U	N	I	II	III
Duration Category	U	X	X			
	E			X	X	X
	T			X	X	X
	H			X	X	X
	P			X	X	X

4.3. Assessment Methodology

The aim of this document is also to provide information on methods and techniques available to assess the impact of E^3 on systems.

Specifically, a methodology for the assessment of systems to the effects of EME's is given. The techniques associated with this methodology will be presented along with examples of how the techniques can be applied to evaluate the susceptibility of electronic systems. This work is closely related to the evaluation of EMC system level susceptibility.

Until now, E^3 survivability or immunity demonstration of equipments, subsystems, and even systems/platforms has been usually accomplished by validation or qualification testing during the engineering development phase.

The purpose of this work is to provide information on available methods for the assessment of system-level susceptibility as a result of E^3.

4.3.1. Susceptibility/Vulnerability Assessment

Assessment of the susceptibility of a system must begin with:

1. As detailed technical description of the system as possible
2. Identification and estimate of the EME coupling to the system and
3. An evaluation of the effects of the coupled energy on critical elements of the system.

To perform this assessment requires adequate mathematical and experimental tools and system models for analysis which are sufficiently detailed to be consistent with the various uncertainties of the problem.

The description of the system may vary from design concepts to detailed technical characteristics depending on the phase of development of the system. If the system is in the conceptual design state, far less detailed information will be available than if the system is already operational.

A physical description of the system is essential to performing the coupling analysis. This must include the layout of the system (number of elements comprising the system, interconnection of these elements, etc.) and the physical size and shape of these system elements. In addition, any deliberate antennas must be identified. Characteristics of importance are size of the antenna (length, diameter, etc.) operating frequency, type (aperture, parabolic dish and feed, whip, dipole, long wire, etc.) and location (height above ground, supporting structure, etc.).

In the case of new system design, this information may have to be based on experience and the required performance characteristics. If options are available, each of these options should be described. Whenever possible, an attempt should be made to identify ports of entry for EME energy into the system. These include apertures, hatches, access ports, ventilation ducts and cable penetrations.

For existing systems, the problem of describing the system is simplified. In this case, detailed drawings and technical specifications are available. Further, an actual system installation is available for scrutiny to identify ports of entry in the form of apertures or penetrations. Often experimental data are available on the technical performance characteristics of the system.

Data may also be available on the EMI response aspects of the system which can provide excellent guidance to its EME susceptibility characteristics.

Detailed circuit characterization of the critical elements of the system, especially interface circuits, is also required to perform an in-depth susceptibility/vulnerability assessment.

Even if detailed circuit drawings and technical specifications are available of the system, the response characteristics and exact values of the circuit components are not adequately described. Often these component characteristics can only be obtained through a measurement program. In the case of systems which are in the conceptual design state, the component characteristics and values can be estimated based on data sheet information, by measurements on typical or generic type of components, or from existing data bases. The type of component data required includes frequency response characteristics and damage constants for both passive and active components. For example logic levels and noise margin must also be known for digital circuits to perform an upset assessment of the circuits.

4.3.2. Approaches to Susceptibility Assessment

There are several approaches for performing a susceptibility assessment. These approaches vary in the level of detail of either the analytical, experimental or combined evaluation. At the extremes are: a worst case analysis and a rigorous analysis.

A worst case analysis is generally employed to obtain a first cut estimate of the system susceptibility and vulnerability. It usually utilizes simplified geometric coupling structures, a simplified environment waveshape and a simplified electrical model of the terminal device impedance.

This type of quick look analysis is particularly useful to determine whether or not a potential EME problem exists. If a problem is apparent, this approach provides a high safety margin hardening criteria. Also, worst case waveform for laboratory tests can be identified prior to full scale tests. Early isolation of potential problems enables design changes in circuit layouts, system groupings, etc. and provides a framework for a more complete analytical approach as required.
The quick look stress comparison approach involves seven major steps:

1. Establishment of performance requirements. The first step is to determine the mission and performance requirements of the system and the significance of EME induced malfunctions.
2. Identification of susceptible components. The second step is to identify components susceptible to EME degradation. In many cases, the degradation threshold is specified in terms of the minimum stress required to cause a malfunction. This often must be determined empirically or using information on representative components.
3. Determination of representative EME collectors. The third step is done by actual visual inspection of the system, if available, or examination of the blue prints and system layout. For new systems, conceptual design must be used. Simplified geometric models of the coupling structures must be developed. Effective height and source impedance must be estimated.
4. Development of simplified EME waveforms. The fourth step can use representation ranging from waveform Norms to Standards or even tailored waveforms.
5. Development of simplified circuit impedance. The fifth step is to determine the stress transfer by matching the impedance between coupling sources and circuit under study.
6. Calculation of the worst case stress. The sixth step is to develop the maximum possible stress based on the worst case orientations of the typical EME collectors.
7. Comparison of the worst case stress and minimum degradation: As the final step in this worst case type of quick look analysis, the maximum possible collected stress is compared with the minimum stress required to degrade the various components. If the total stress available exceeds the minimum degradation stress, then a more detailed study, analysis and testing should be considered.

A detailed (rigorous) vulnerability assessment requires development of analytical models which define the response of the system. There are two generic approaches which can be applied: the circuit inherent hardness estimate and the circuit vulnerability estimate.

The circuit inherent hardness approach utilizes component failure data or circuit upset data and translates these device terminal voltages and/or currents to circuit terminal voltages and currents required to produce the response through the circuit transfer function. These failure terminal voltages and currents are then compared to the coupled voltages and currents to determine the margin of safety or protection requirements.

The circuit vulnerability estimate begins with the source (coupling estimate) in terms of open circuit voltage and equivalent source impedance as the driving function. These data are translated via the circuit transfer function to determine the device terminal voltages and currents which are then compared to the failure or upset thresholds.

The accuracy of either approach is dependent on how well the system can be modelled. The variables associated with the analysis are the coupled waveform, the complex impedance of the passive elements, the complex impedance of the active components, the active element response (damage or upset model), the complex source impedance and, if experimental techniques were utilized to measure these data, the waveform used.

As stated previously, simple geometric models are usually employed for determining coupling to the structure. Simple models can be used to obtain exterior skin currents, cable sheath currents and antenna currents.

The time domain response waveforms are usually of the form of damped sinusoids or a combination of damped sinusoids depending on the coupling elements resonances. Shielding estimates to obtain shield currents or unshielded wire currents on internal cables can also be performed using simple models. Terminal voltages and currents are determined utilizing the transfer impedance of the shielded cables. Computer codes are available to determine the source impedance for coaxial or multi-conductor cables.

Lumped parameter circuit models have been developed for simple antennas which are directly usable in circuit analysis codes to provide the terminal voltages and currents. For existing systems, these terminal voltages and currents can also be obtained experimentally.

To perform an analytical assessment, models of the passive elements in the circuit must be developed which characterize element response for normal and extreme signal levels. High signal response models are required which will predict failure as a function of electrical overstress amplitude and duration. These models will predict the effectiveness of the passive components in protecting the active devices.

Having developed correct models, a reasonably accurate assessment of system vulnerability can be obtained. The more accurate the model, the better the assessment. The most practical and cost effective approach is a combination of analysis and test methods. Care must be exercised in the combined approach since empirical component failure data are most often obtained using simplified driving waveforms, a square wave being the most common. As a result, there is not a direct correspondence to the actual or predicted waveforms. Conversion factors must be developed based on a convolution integral solution.

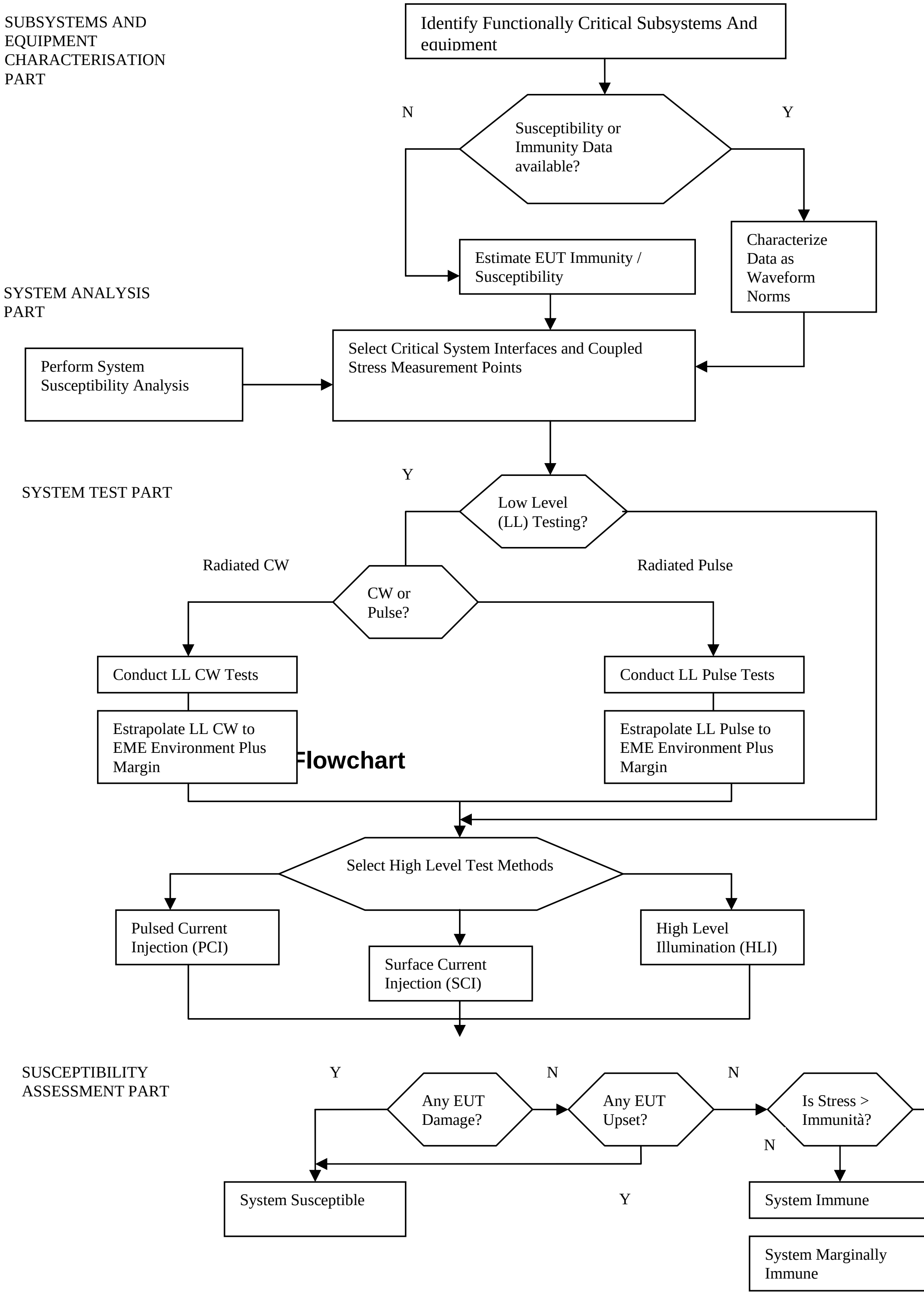
As a final consideration, the susceptibility assessment may be numeric, analytic or experimental or a combination of these techniques. The discrepancies associated with the different approaches induce the need to add a safety margin between the determined susceptibility levels (immunity or damage) and the constraints admitted inside the barrier boundaries.

It is important to note that the assessment methodology presented within this document is intended to assist in reducing the risk of detrimental impact of system exposure to E^3. This methodology can be applied during the design and development phases of a system.

According to the following flowchart, it is possible to define four different parts [See reference 1] in order to define the overall assessment methodology.

These four parts are:

1. Subsystems and Equipment Characterisation
2. System Analysis
3. System Test and
4. Susceptibility Assessment.



4.3.1 Subsystems and Equipment Characterisation

Characterisation of the system needs to be completed prior to any detailed evaluation or assessment. At this stage, it is essential that critical aspects of the system are identified such that the impact of any EME induced effect can be correctly assigned as either immunity or susceptibility during the susceptibility assessment phases. Also, areas of potential weakness may be identified based upon information about similar systems or technology types.

During this part it is useful to gather immunity and/or susceptibility information that may be relevant; this may be obtained from Electromagnetic Compatibility (EMC) test data. If waveforms associated with susceptibilities are available, waveform Norms that allow parameters of waveforms to be mathematically quantified should be computed for later use.

A typical system characterisation will breakdown the system into its components, sub-systems and equipments. Each of these sub-systems and equipments will then be assessed for coupling paths relevant to the frequency density of the illuminating EME's of interest.

This is conducted by translation of the frequency content of the illuminating environment into wavelength by using the simple expression given in the following equation:

$$c = f \lambda$$

where c = speed of light in a vacuum ($3 \times 10^{8}\ \mathrm{ms}^{-1}$), f is the frequency (in Hz) and λ is the wavelength (in m).

Depending on the type of coupling path, frequencies corresponding to a wavelength of $\lambda/2$ or $\lambda/4$ tend to dominate and this provides an indication of the ability of the illuminating EM environment to couple to the system being characterised.

Any protection added should be noted during this phase of the assessment and may negate the need for more extensive testing during the later stages. An effective shield at the frequencies of interest may reduce the illuminating EM environment to a level that is below the immunity requirements for commercial electronics thus demonstrating that further radiated testing of the commercial electronics is not required. In this case, a conducted test would still be required unless adequate filtering can be demonstrated to show that anticipated conducted currents and voltages would be attenuated to a level for which the electronics has been demonstrated to be immune. However, testing at the later stages is recommended to assure that the added protection is adequate.

The effective shield will be typically a result of the determination of the protection requirements in terms of the most appropriate level of application (See Vol. I, Chapter 4.1.5.2.2). For the EME "HEMP" the result could be the reduction of the amplitude of the incident electromagnetic filed strength by a factor of 10,000 or 80 dB. For example, this would reduce amplitude of 50 kV/m to 5 kV/m inside the enclosure. It is of course not necessarily immune against 5 V/m CW excitation using frequencies within the bandwidth fo HEMP. The difference of the immunity against pulsed and CW stress depends for example on the amplitude spectrum of the pulse related to the amplitudes and frequencies of CW, the quality factor of the unit under test or its sensitivity to energy effects. Therefore, the CW excitation will be typically the worst case test compared to pulse excitation. Thus, if an equipment or system is immune to 5 V/m CW., it is possible that it will be immune to larger peak amplitudes of transient (damped sinusoidal) signals. For interference the peak amplitude is likely to be the susceptibility driver, but for permanent damage, energy is a key susceptibility driver.

A further consideration here is that EMC tests are driven by the need to demonstrate continued operation in a particular EM environment i.e. they are required to demonstrate immunity in that environment.

Without the appropriate test information, it is generally not possible to make conclusions about susceptibility based on immunity data only. However, in the context of system level assessments, the immunity data plays an important role as it can be used to bound the data and provide an indication of the range from EM environments where continued functionality (immunity) can be expected. Without susceptibility information, this type of calculation will provide the system user with a range at which the system will continue to operate but does not provide information on the range at which effects can be expected, thus detailed susceptibility data is required in order to generate this information.

Knowledge of the shielding effectiveness of equipment, sub-system and system interfaces also provides important information as sub-system immunity of 5 V/m (CW) with system shielding of 26 dB means that the sub-system will continue to operate in an externally illuminating field of 100 V/m (CW).

4.3.2 System Analysis

The purpose of the system analysis is to identify critical subsystems and equipment, system configurations and operational modes that will be assessed through a combination of low-level and high-level tests to estimate a system's susceptibility to the EM environments. A key element in this process is selection of a set of measurement or test points at critical interface locations within the system that will be used later in the susceptibility assessment part to compare coupled stress waveform data (obtained in the system test part) to Equipment Under test (EUT) immunity or susceptibility waveform data at corresponding interfaces (obtained in the sub-systems and equipment characterisation part). During the test point selection process, emphasis should be placed on choosing test points at EUT interfaces that both a) are predicted to have the highest level stresses and b) are functionally critical to proper operation of the system.

4.3.3 System Test

This part describes EUT and/or system level testing that can be used to provide information on the system's overall protection against EM environment.

4.3.3.1 Low Level Tests

Low level (LL) tests can be conducted with either CW or pulsed illuminating fields.

Transfer function and attenuation data should be collected for those cable bundles and areas of interest identified by the system analysis. For HEMP and/or HPEM environments that dominate in the cable coupling regime (500 kHz to 400 MHz, depending on the length of cabling) convolution with cable bundle transfer functions will result in predicted currents as a result of the incidence of the environment of interest. For HEMP and/or HPEM environments that dominate in the aperture coupling regime (400 MHz to 18 GHz) convolution with attenuation data will result in predicted fields within the system enclosure. These data can then be compared with any available EMC test results to provide immunity, and possibly, susceptibility thresholds.

As these tests are conducted at low level, they will not adequately characterise the performance of non-linear protection such as transient protection devices. The performance of these devices should be carefully considered in the overall assessment.

4.3.3.2 High Level Tests

High level (HL) susceptibility tests should be conducted by an appropriate technique. This could include free-field (directional) methods, reverberation chamber methods or via direct injection methods. Reverberation chamber testing can be said to represent a worst case illumination from a polarisation and orientation perspective, due to the statistically isotropic environment of the chamber [See Volume VI for more details]. However, for the same reason, it essentially represents only an average case in terms of the stress on the EUT, compared with a plane wave having the same field strength. High level free field testing will identify susceptibility dependencies on polarisation, orientation and EM waveform parameters within the constraints of the facility used for the assessment [See Volume VI for details].

Consideration of the parameters of the EM waveform of interest and the likely upset parameters for the technology contained within the sub-system or EUT is necessary in order to utilise the optimum test parameters during the assessment.

During this part of the assessment, the EUT should be made to operate in a representative configuration. This must include careful location of cables used during the EUT’s deployed state. Any Radio Frequency (RF) link between a screened chamber and the outside world requires hard-wired replacement such that the EUT can be monitored for any induced susceptibility. It is important that the addition of any such link is suitably attached to the EUT, such that changes in the electromagnetic properties of the EUT are minimised. This is particularly the case when replacing RF links for hard-wired links as the RF link has inherent physical isolation but a hard-wired link introduces another path for coupling of RF to EUT. The impact of this is typically alleviated by the use of ferrite loaded cables to prevent the circulation of skin currents in the screen of the cable . Bulkhead connectors should also be used to prevent the transfer of any circulating current entering the inside of the EUT and re-radiating.

The result of this part of the assessment will be a set of frequencies at which the EUT has been affected allowing susceptibilities to be identified. A frequency density spectrum can be generated for all EM sources of interest. This can be compared against the frequency bands for susceptibilities to identify sources that could generate the same effect.
Where applicable, an accurate comparison of the effects of different modulation types at this stage is critical.

4.3.3.2.1 Pulsed Current Injection

This part of the assessment involves the injection of pulsed waveforms whilst the EUT or system is monitored for susceptibility. This can involve the injection of damped sinusoidal waveforms that are centred on a single frequency or complex transients that consist of many frequencies. For example, it is possible to obtain a predicted induced cable bundle current for an illuminating HEMP or other HPEM environments using the transfer functions. During this part of the assessment it is important to consider the impact of single port excitation when the HEMP or other HPEM environments may excite many ports simultaneously. In particular, multi-port excitation should be used on EUT where redundancy may be built in during practice. If multi-port excitation is used, the assessment must give due care to ensuring that all ports are excited within the cycle time of the EUT as failure to do this may result in an misleading test result.

The Pulsed Current Injection (PCI) methods described in IEC 61000-4-24 and IEC 61000-4-25 may be useful.

4.3.3.2.2 Surface Current Injection

Direct drive techniques may be used to inject currents onto either a return conductor built around the system under assessment or the system itself. The current flow in the return conductor or in the system exterior cross-couples to the cabling within the system. This method can be used at low level to measure transfer functions or at high levels to monitor for susceptibilities. One of the advantages of this technique is that it can be applied at lower frequencies than the LLCW methods. This technique can also be applied to system level.

4.3.3.2.3 High Level Illumination

This part of the assessment involves exposing the system to high power RF sources indicative of the types of technology that could be used as HPEM and/or HEMP. It is essential that the set-up used during the radiated susceptibility phase is used to ensure that the coupling paths to the system remain unchanged. Changes in the set-up could either remove or provide additional modes of ingress into the system that could potentially alter the electromagnetic properties of the system.

Selection of HEMP and/or HPEM waveform parameters should be based around the modulations used during the radiated susceptibility. The effect of variation in pulse length, pulse amplitude and pulse repetition frequency should be investigated during this stage. At this stage it is important to increase the level of the incident environment in stages up to the full level. Experience of HEMP qualification testing shows that the system can exhibit no effects at 10 kV/m and 50 kV/m but many effects at 30 kV/m. In these cases the protection devices did not operate at 30 kV/m but the environment contained enough energy to cause effects in some of the system’s equipments. At 50 kV/m protective devices operated and protected the system.

4.3.4 Susceptibility Assessment

The purpose of the susceptibility assessment part is to evaluate the test data including any observed effects such as EUT upset or damage that occurred during the testing to determine any degradation to normal system operational performance. Typically test simulators do not exactly reproduce the EM environments. Therefore the stress waveform data needs to be extrapolated to the actual EM environment of interest. Susceptibility assessments should be based on high-level test data since linear scaling of low-level test data cannot account for non-linearities in the systems' response such as unintentional arcing or firing of surge protectors. The assessment process involves comparisons of stress waveform data with the EUT immunity or susceptibility data at corresponding interfaces in the system.

A safety margin is frequently applied in these comparisons to account for uncertainties in the susceptibility assessment process. These uncertainties are due to limitations both in knowledge of system parameters and in testing including but not limited to inability to test all system configurations and operational modes, system orientations, component, equipment variation and angles of incidence.

For example, a factor of two margin (6dB in terms of electric field strength) applied to each critical interface (subsystem test level) means that the immunity or susceptibility data must exceed the measured extrapolated stress test data by a factor of two or greater. Higher safety margins are generally applied to systems and in particular for critical systems(e.g. nuclear reactors.) It is important to note that even though no observed effect may have occurred during the test, the system still fails the overall assessment if it fails to meet or exceed its stated safety margin requirements.

If any EUT is damaged or upset during the testing and this degrades the system functionality, then the system is deemed to be susceptible. An exception to this is if the susceptible EUT can be shown to be used in a redundant manner by the system. If this is the case, and if the susceptibility can be shown to be removed by the use of redundancy, then the system is ready for system test.

If no EUT damage or upsets occurred during the system testing, or if any damage or upsets observed do not degrade the function of the system, and the induced currents on the equipment meet the safety margin criteria, then the system is deemed to be immune. The extent of immunity depends on whether the test results exceed the required safety margin defined earlier in this section.

Finally, if the measured stress (e.g. induced current) at each interface in the system is less than the immunity level (e.g. the level achieved during testing with no effects observed) for the same interface then the system is deemed to be immune to the environment of interest. If the stress is greater than the immunity level, then the system is deemed to be marginally immune as immunity levels have been exceeded but effects have not been observed.

4.3.5 Experimental Methods List

The experimental methods for determining the susceptibility of equipment to E^3 are described in various standards. For example:

- AECTP 500 is the test part of the NATO E^3 standard. It is similar, for different points, to the French GAM-EG-13 (Fascicle 63, 64 and 65), the European EN 61000 series, Germany's VG 95373, and the American MIL-STD 461F.
- MIL-STD-461F is the American military standard for EMI. It includes test requirements and procedures, and applies to equipment and subsystems.
- MIL-STD 464A is the American military E^3 standard for systems (external RF EME and other EMEs, and E^3 for systems and platforms). VG 95370 is the German standard for system level testing.
- ADS-37A is the American standard for military and civil aircraft to include rotary aircraft.
- VG 96903 is the German military NEMP standard, MIL-STD 2169B is the American HEMP standard, AEP-4, Ed 4, Vol II is the NATO HEMP standard and AECTP 250, Leaflet 256 is the NEMP unclassified criteria of the NATO E^3 standard.
- IEC is the international organization that establishes civilian standards. Applicable standard is the 61000.series.

These standards describe the threat environments, and most provide methods, types of tests, and test levels. The designer determines the types of tests and in some countries, the test agency may modify the types of tests and test levels dependent on known inherent or deliberate hardening and mission requirements. See Volumes II and VI for additional information on standards and tests, respectively.

4.3.6 Tools for System–Level Susceptibility Assessment

One of the important tools available for system-level susceptibility assessments for EME threats is computational electromagnetics. Computational Electromagnetics (CEM) has evolved over the past decade to a point where predictions can be made for a wide class of problems. The available methods may be classified broadly into two categories: a) Differential Equation (DE) solution methods and b) Integral Equation (IE) methods.

Although Maxwell's curl equations are usually first encountered in the Time Domain (TD*), i.e.,* with time as an explicit, independent variable, until recently, most electromagnetic instruction and research has taken place in the Frequency Domain (FD) where time-harmonic dependence is assumed. A principal reason for favouring the FD over the TD in the pre-computer era had been that a FD approach was generally more tractable analytically. Furthermore, the experimental hardware available for making measurements in past years was largely confined to the FD.

Time domain electromagnetics (EM) became more in vogue with the arrival of the digital computer, which has not only profoundly affected what can be accomplished numerically (or computationally), but also experimentally. Since the beginning of what has come to be called CEM in the early 1960s, there has been a steady growth in both TD and FD modelling. This growth, which began slowly at first, was primarily confined to Integral-Equation (IE) treatments, but has grown recently as TD differential-equation modelling has attracted wide attention.

We now review the essential elements of CEM environments:

Time Domain Differential Equation models, whose use has increased tremendously over the past several years due, primarily, to much larger and faster computers [See reference 6].
Time Domain Integral Equation models, although available for well over 30 years, have gained increased attention in the last decade. The recent advances in this area make these models very attractive for a large variety of applications [See reference 6].

Frequency Domain Integral Equation models which remain the most widely studied and used models, as they were the first to receive detailed development.

Frequency Domain Differential Equation models whose use has also increased considerably in recent years, especially for low frequency applications.

Computer codes available for Frequency Domain Integral Equation and Frequency Domain Differential Equation are:
- MEEP;
- MPDB;
- COMSOL FINITE ELEMENT SOLVER;
- SEMCAD.

These four choices mentioned above can actually be narrowed down to two broad choices, i.e. a) IE models and b) DE models, depending on the mathematical formulation. The well-known method of moments codes (e.g. NEC and CONCEPT) in general, involves IE modelling whereas the well-known finite element method (FEM) uses DE formulation.

A large number of circuit analysis computer codes are available and are sufficiently documented to allow their general usage. The better known codes are :

ECAP
NEDAP
SCEPTRE
CIRCUS and
NET-2…

PSPICE can be used as a linear operation code.

These codes provide a mathematical tool for predicting response of a circuit with a given set of components in given configuration and for use in circuit design. These circuit analyses enable the User to solve even several classes of non linear problems arising from:
- Non linear volt- ampere characteristics of semiconductor junction,
- Variation in active device gain with respect to operating point,
- Variation in device junction capacity with respect to current and voltage,
- Photocurrent variation with respect to junction voltage and operating current levels, and the variation in carrier life-time and gain.

Some of the features of various circuit analysis programs are :
- Basic circuit elements (for example resistors, capacitors),
- Switch (this allows applying linear analysis to nonlinear problems),
- Controlled current sources(this feature may be used to model transistor function),

- Components representation (for example diodes and transistor with power dissipation region),
- Damage prediction and possibility to continue with damaged model and
- Driving waveform (for example current or voltage sources of any time duration).

4.3.7. Numeric Methods- Introduction

Numeric tools can be used to obtain:

1. Constraint determination on equipment PCBs,
2. Determination of the E^3 Susceptibility (E^3Ss) and
3. Parametric determinations of the equipment protections.

There are different numeric tools that can be applied to treated problems.

Points 1 and 3 can be treated by solving Maxwell equations, or by solving transmission line equations. For the 3-dimensional methods, it is necessary to represent all details (e.g., cases, openings, cables/wires, cards). Points 1 and 2 can be treated by tools using methods based on the theory of circuits (PSPICE). In addition point 2 must be treated using databases containing E^3Ss of different components.

Equipment E^3S require the EM transfer function determination from point of entry to different components inside equipment.

For low frequency spectra, computations are applied essentially on lines conducting current (equipment feed through).

For high frequency spectra, computations start from the external equipment parts surrounded by ambient EM field (e.g. equipment apertures).

Knowledge of stresses on each component (for the first stage concerned) compared with corresponding strength or upset data gives information on damage or local upset.

Unfortunately, the equipment complexity and the component discrepancy results with large uncertainties (+ or -10dB), thus, reducing the safety margin.

4.3.7.1 Numeric Applications

The sequential application consists of dividing the system susceptibility assessment into several stages. Every stage is treated then by the most suitable numeric tool. The analysis of the results at the end of every stage is a decision point: is there adequate information to conclude or is it necessary to continue and refine the survey?

The simultaneous application consists of dividing the object into sub-domains. Every sub-domain is dealt with using the best numeric solution and the resulting information (I, V, E or Electric field, H or Magnetic field) are exchanged, with the progression of the calculations, between the different sub-domains. This technique requires the hybridization of the different numeric tools, but permits the results in only one calculation.

The choice of the most suitable method can be made while taking into account:

- Domain of survey (time and frequency) and
- Characteristic dimension (D) of the object in relation to the wavelength of the signal.

4.3.7.2 Choice of the Methods

4.3.7.2.1 Domain of Survey

Time domain:

Time domain codes are the favorite choice in the simulation of the EMEs of transients such as HEMP, Lightning, ESD Time domain. These codes use the available computer capacity more efficiently than frequency codes, especially for very short pulses like UWB. The calculation in the time domain covers typically a time window in the order of the incident pulsewidth. Additionally, these codes are able to deal with non-linearies.

Frequency Domain.

FD codes are the favorite choice to EMEs of CWs like Electromagnetic Emissions, HIRF and HPM. These codes are more accurate and efficient than time domain codes, especially for very long pulses compared to the time (1/frequency). The accuracy of FD codes can be based on a consistent solution of an infinite volume. These codes are useful even if the volume is much larger than the corresponding wavelengths. Unlike in FD codes, in TD codes the whole volume has to be made into finite elements. These discrete elements have a size commensurate with the distance an EM wave would travel that medium (e.g., 30 cm per nanosecond in air). Typically, FD codes treat linear problems; however, attempts have been made to introduce non-linear effects.

Most frequency domain codes work frequency by frequency. The time of calculation is therefore a linear function of the number of frequencies. These codes are therefore particularly interesting when the spectrum of the survey spectrum is narrowband.

Transferring time domain to the frequency domain is accomplished by the Fourier Transform. Some precautions must be taken to get correct transformations to preserve phase.

4.3.7.2.2 Characteristic Dimension

The second method is based on the characteristic dimension of the object in relation to the shortest wavelength of the signal. (For more details, see Vol. III.)

4.3.7.3 Statistical Electromagnetics

Although there is a plethora of computational EM tools available for application to the study of the interaction of electromagnetics with systems, the challenge of CEM tools is that not all of the boundary conditions can be known in advance. As a result, an alternative paradigm needs to be developed. Statistical electromagnetics provides such an alternative [See reference 1].

One of the challenges in treating problems pertaining to the coupling of EM with systems is the short-wavelength nature of the radiation. The coupling properties of systems (an enclosure) depend in great detail on its size and shape, the structure of the apertures that act to facilitate or inhibit routes for the electromagnetic energy, and on the frequency of the electromagnetic radiation. Furthermore, the nature of the modal patterns within the enclosure is extremely sensitive to subtle changes in frequency, the shape of the enclosure, and the orientation of the internal disturbances (which could be critical assets).

At present, even with the plethora of fast and powerful computers that utilize efficient 3-D CEM tools, addressing this problem is a great challenge. Two major issues arise: i) the large aspect-ratio problem, which is a consequence of the ratio of the largest-to-smallest dimensions in the problem. Most of the CEM tools apply Maxwell's equations after "meshing" the entire simulation region of the problem. For low frequencies (say 100 MHz and lower), these tools have proven to be reliable for calculating internal electromagnetic fields for large scale systems. However, when attempting to resolve higher frequencies (GHz and above), the entire simulation region will have to be "meshed" with increasingly fine resolution. As a result, the number of mesh-points that would be required render such an approach to be infeasible.

Statistical electromagnetics seeks to address the question, "Given an electromagnetic environment and an electronic system, what is the probability that the system's performance will be unacceptably degraded?" The proponents then construct stochastic models based on certain fundamental assumptions for the fields within complicated enclosures.

These predictions can then be validated with measurements performed in mode-stirred chambers (See Volume VI).

Reference 7 identifies several emerging fields that could be applicable to future EM coupling to system problems. For example, the coupling of high-frequency electromagnetic energy into complicated enclosures falls within a larger class of similar problems previously encountered by physicists in the fields of acoustics, mesoscopic transport, and nuclear physics. These seemingly disparate systems comprise short-wavelength waves (electromagnetic, acoustic, or quantum mechanical) that are trapped within an irregularly-shaped enclosure or "cavity," in the limit where the perimeter of the cavity is many wavelengths. This limit is termed the "Ray Limit." In this limit, the enclosure can be approximated as rays undergoing specular reflection off of the boundaries of the enclosure. The study of such wave-systems, in the short-wavelength or ray-limit, is widely termed "wave chaos" or "quantum chaos" (when referring to quantum-mechanical wave systems such as atomic nuclei or mesoscopc condensed-matter systems) [See reference 7].

4.3.8 Analytical Methods

Analytical methods play an important role in system-level HEMP and HPEM assessments, in particular the use of Fourier transforms are key in extracting frequency information from time domain waveforms. Additionally, the use of waveform norms enables the unique characterisation of a waveform and this technique can be useful during system-level assessments. For more details on this subject see Volume III and V.

4.3.8.1 Fourier Analysis

Fourier analysis is a method applied to time-domain waveforms to evaluate their frequency content. The method computes a frequency density spectrum which is referred to as the result of a Fourier transform. This frequency density spectrum can be used to identify the frequencies that contribute the largest amount of energy to the transient.

4.3.8.2 Waveform Norms

Waveform Norms are a method of uniquely characterising a waveform by computation on various properties. Strictly, a Norm is a mathematical description of a property of a waveform; waveform Norms are discussed in detail in IEC 61000-4-33, however, for the evaluation of system-level susceptibility, three properties are of key significance:

1. Maximum rate-of-rise – this Norm gives an indication of the maximum frequency within the waveform,
2. Peak – this Norm provides the peak level for direct comparison with immunity/susceptibility test results and
3. Action Integral – this Norm provides an indication of the energy contained within a waveform.

These three properties enable the evaluation of a waveform with respect to the primary susceptibility drivers, namely stress (maximum rate-of-rise and peak) and energy (action integral).

The use of the Waveform Norms can simplify the description of the EM stresses, the external and internal stress to the system, and simplify the determination of the envelopes of stresses. In addition, they compare the transient characteristics of the different stresses of different shapes. In susceptibility analysis, the retained waveform Norms correspond to the parameters capable of effecting the electronic circuits. Table 5 lists the five most significant waveform Norms.

Table 5. Typical Waveform Norms

Waveform Norm Name	Waveform Norm Description	Related Effect on Electronics
Peak Amplitude (N_1)	$N_1 = \left\| f(t) \right\|$	Toggling of digital circuits Dielectric breakdown Punch through
Peak Derivative (N_2)	$N_2 = \left\| \frac{df(t)}{dt} \right\|_{\mathrm{MAX}}$	Mutual coupling Reactive element response Toggling of digital circuits
Peak Impulse (N_3)	$N_3 = \left\| \int_0^t f(x)dx \right\|_{\mathrm{MAX}}$	Toggling of digital circuits Dielectric breakdown
Rectified Impulse (N_4)	$N_4 = \int_0^\infty \left\| f(x) \right\| dx$	Toggling of digital circuits Dielectric breakdown Analog circuit drift and latchup
Root Action Integral (N_5)	$N_5 = \left\{ \int_0^\infty \left(\left\| f(x) \right\| \right)^2 dx \right\}^{1/2}$	Thermal failure (junction burnout) Metalization melt

Table 5. Typical Waveform Norms

These Norms permit the construction of a synthetic signal from the different stresses. See Paragraphs 4.2.2.3, 4.2.2.4 and 4.2.2.5 of Vol. V and 4.9.3.1 of Vol. III for more discussion on waveform Norms. This method also permits the creation of a synthetic signal envelope or synthetic envelopes of the parameters for the different stresses. These envelopes can be reduced by merging the probability or frequency of appearance for threats with a well-balanced constraint like localized threats to one system and multiple systems, area of coverage, type of risk. See Para 5.2.2. of Vol. VI for discussion on synthesized waveforms.

4.4 Technical Limitations

This section discusses potential technical limitations of the techniques discussed within this document [See reference 1]. The purpose of this discussion is to highlight the potential deficiencies such that an appropriate margin can be considered and applied to the system.

These limitations are listed below:

Single Point Illumination

Many test techniques illuminate the test object from a single discrete location. However, the system may be exposed from a direction or directions by the threat environment which is different to that tested (see also discussion below on directivity).

Facility Limitations

It is generally not possible for a single test facility to provide all of the required test parameters. There also may be physical limitations of the facility such as the size of system which can be accommodated within the test volume or the availability of the correct power supplies.

Cumulative Effects

Susceptibility testing generally requires a step by step increase in the stress environment until the susceptibility threshold is found and recorded. However, some systems may be ‘weakened’ by repeated exposure to the stress environment.

Degradation/Aging

Consideration should be given to the life cycle of the system. It is well known that the system hardness can be reduced over the lifetime of the system due to issues such as corrosion, misuse and poor maintenance.

The impact of ageing and corrosion on the performance of shielding joints has been investigated in various studies. Corrosion is governed by materials, material combinations, atmospheric conditions etc. Effects of corrosion on the electrical performance are governed by amounts and properties of corrosion products formed, as well as by the design and mechanical properties of the joint. Avoiding unsuitable combinations of materials is thus not sufficient for ensuring continued shielding performance.

Some results are reported from a test where different kinds of gaskets, materials and coatings were combined. The specimens were exposed for one year under a hood outdoors immediately north of Stockholm City Centre. The study shows that fingerstock gaskets offer good shielding performance, but are sensitive to corrosion. Performance of wire mesh gaskets varies depending on design. Wire mesh gaskets with an elastomer core did not show as good performance as fingerstock gaskets initially, but suffered virtually no effects from the one-year weather protected exposure. Other types of gaskets, likely to provide lower contact force, offer lower shielding effectiveness and, in many cases, suffer deterioration from exposure.

Results with and without chromate conversion coatings show that corrosion protection offered by a conversion coating is no guarantee for preserved shielding properties.

Non-Linearity

The low level techniques discussed in this document provide a transfer function for the system in a relatively benign environment. High level illumination may excite non-linearities within the system such as flashover, ‘rusty bolt effects’, saturation and activation of protective devices which may affect the transfer function.

Determination of shielding effectiveness is a vital part in the analysis of a systems capability to withstand EM threats. It is usually assumed that the shielding effectiveness, determined at low field levels, is valid also at threat levels. This assumption might be refuted by the presence of non-linear effects. These may result in generation of new frequency components in the spectrum of the transmitted pulse. Irradiation at threat levels may also result in damage of shielding joints. 31 corroded EMC joints from two groups of specimens, one subjected to laboratory exposures (IEC 62-2-28) and the other to a one year outdoor exposure immediately north of the Stockholm City Centre, were investigated. The specimens were exposed to radiation from a 3 GHz radar source. The pulse length was 1 µs and the maximum electric field strength about 50 kV/m. Non-linear effects were revealed by changes in the time domain shape and frequency analysis. Degradation was studied by comparing the transmission cross section of the specimens before and after irradiation. No major degradation could be detected after the HPM irradiation. Most of the objects showed none, or only a moderate, generation of harmonics.

Synergistic Effects

In some cases, cable bundles may be tested in isolation whereas in reality all cable bundles would be excited simultaneously. This can lead to a difference in the susceptibility level of the system.

Statistical Confidence

A one-only system would need a complete assessment whereas a production line approach requires re-measurement of transfer functions and susceptibility data at various stages to confirm that the overall system response to the HEMP or HPEM environment of interest is not impacted.

Directivity

Directivity is a property of the radiation, or receiving, pattern produced by an antenna. It is defined as the ratio of the power radiated (or received) in a given direction to the average of the power radiated (received) in all directions. A EUT subjected to a radiated susceptibility test can be regarded as a receiving antenna. The directivity reflects the angular dependence of its susceptibility, i.e. the EUT is most susceptible in the direction corresponding to the maximum directivity. Due to the random location of coupling paths, e.g. apertures on the skin, the maximum directivity at a given frequency is smaller than that of a deliberate antenna of the same size. Expression can be used to estimate the maximum directivity for a typical EUT.

The directivity of a EUT appears as a complex lobe pattern. The differences between peaks and nulls might be 20 dB or even larger. The width of the lobes decreases with increasing frequency. At a few GHz the width is typically of the order of 10 degrees or less for a EUT having a size of a couple of decimeters. This means that hundreds, or even thousands of angles of incidence may be needed in a plane wave susceptibility test in order to achieve an uncertainty of a couple of dB's. If the test is instead carried out in a reverberation chamber this problem disappears due to its statistically isotropic environment. On the other hand, since the available energy is spread out in an isotropic fashion thereby irradiating the EUT from many angles of incidence simultaneously most of the energy is wasted in directions for which the EUT is not susceptible. Therefore, a margin related to the maximum directivity of the EUT has to be added in order to simulate worst case plane wave irradiation. This margin is typically of the order of 10 – 15 dB. It should be noted that worst-case plane wave illumination may be difficult to perform.

5.0 Summary

The E^3S is an important part in the platform/system EM hardening work and more particularly in the unified approach to the protection and hardening to E^3.
AEP-41, Volume IV shows that EME coupled energy may affect an electronic system performance temporarily or permanently, and this can result in two types of degradation which are functional damage and operational upset.
Due to the above mentioned degradations, effects on a system can be categorised by Criticality, Duration and such a combination of Critically level and Duration Category.
In order to assist in reducing the risk of detrimental impact of system exposure to E^3, an overall assessment methodology, based on subsystems and equipment characterisation, system analysis, system test and susceptibility assessment has been shown.
Methods and techniques available to assess the impact of E^3 on systems have been shown, such as potential technical limitations of the techniques discussed within the document.

6.0 Conclusion

To assess the impact of an EM threat or any other stimuli on a system performance, the response of the system to the stimulus must be known. This response (in terms of degradation or upset), of a component, equipment package, discrete subsystem or system can be termed as susceptibility.
AEP-41, Volume IV describes methods and tools to perform an assessment methodology for reducing risk to the systems due to their susceptibilities to E^3. The E^3 susceptibility occurrence, nature and the effects have been investigated in order to apply the EM barrier protection concept to achieve UE^3 survivability against the E^3 susceptibilities described in this volume.
Due to technical limitations, in order to assure an adequate level of protection for system through the use of EM barrier(s) plus special protective measures, it is necessary to add a safety margin between the determined susceptibility levels and the internal residuals.
The data collected from the determination of system susceptibilities are fundamental in order to reach a comprehension about the problems related with the operational employment of the six Operational Categories of NATO military hardware.

7.0 Annex

7.1 System Level Assessment - HEMP

This annex provides an example of a system level assessment to an unclassified EMP environment. The assessment applies to a fictional building that contains a simple computer network [See reference 1].

The first stage of the methodology requires that critical aspects of the system are identified. In this case, the primary concern is the continued operation of the server computer that all other computers connect to. The server is located within an office with no specific EM protection employed. Thus, this assessment assesses the survivability of the server computer in a HEMP environment. During this phase, details on the immunity of the server computer would be obtained either from EMC measurements if available or by assuming immunity to standards such as IEC 61000-4-2 (ESD), 61000-4-3 (radiated immunity), 61000-4- 4 (EFT), 61000-4-5 (surge), 61000-4-6 (conducted immunity). This example addresses the three components of the HEMP waveform separately.

Early-time HEMP assessment

The initial measurement phase would include LLCW measurements on all the server PC connecting cables such as mouse lead, keyboard lead, power leads (both computer and monitor if applicable), monitor lead and network leads. Attenuation measurements would also be made in the area where the server computer is located. From this information, incident server computer field strengths can be predicted and compared to immunity levels. Also, currents can be predicted for comparison with immunity levels. This will results in an understanding of the protection required to ensure that the server computer remains unaffected by an incident HEMP.

By way of a simple example, if the attenuation measurement showed that the inherent protection afforded by the building was 20 dB over the frequency range of interest, the field strength incident upon the server computer would be 5000 V/m (with an external electric field strength of 50 kV/m). If the server computer is immune to 3 V/m, additional protection of 64.4 dB would be required to ensure that the field strength does not exceed the immunity level. The same analysis can be performed for the conducted aspects of the incident HEMP by considering the difference between conducted immunity levels and predicted currents as a result of an incident HEMP.

If further information on the immunity level of the server computer is required, high level testing could be conducted. This could be with the aid of free-field radiating simulators that simulate the early-time component of HEMP or by injecting the predicted current using damped sinusoidal injection (direct drive) methods. Both techniques could yield effects the threshold of which would determine the minimum level of protection required to ensure continued operation of the server computer.

Intermediate-time HEMP

For the intermediate-time HEMP, the main threat to a building with a simple computer network is the conducted environment produced by the coupling to long lines outside of the building. This should include both the power system and the communications system. To assess the levels of conducted environment, it is not necessary to consider whether the long lines are fully exposed in the air or whether they are below ground as this is not an important factor. If no lightning protection is found, then test level IC3 from IEC 61000-4-25 should be applied. The test level is 4 kV (common mode) using the ITU-T test from IEC 61000-4-5. This waveform rises in 10 microseconds and has a pulse width of 700 microseconds. The test should be performed at the point the communications cables enter the building (or at the main panel) or at the point where the power line reaches the power panel.

As described in IEC 61000-4-25, it is also necessary to test (or evaluate) at the lower voltage levels of 1 and 2 kV to ensure that non-linear effects are not important.

Late-time HEMP

The Late-time HEMP couples to long lines power lines outside of the building and can be a concern for both the medium voltage power lines and long communications cables (in the air or buried). If there is a building transformer that reduces the voltages from medium to low voltage before entering the building, tests or analyses should be performed for level LC3 (400 V, 25 A) from IEC 61000-4-25. The waveform to be used has a risetime of approximately 1 second and has a pulse width of 60 seconds. Some test generators producing these types of pulses have been made from car batteries.

In the case of the power system, an important test to perform at the equipment level is to inject high levels of harmonics into the power port. These harmonics are caused by the quasi-dc currents injected upstream by the late-time HEMP into transformers that are then driven into half-cycle saturation. IEC 61000-4-13 is recommended in IEC 61000-4-25 with levels of 5% of Vr (Voltage reference) for the 2nd harmonic and 8% of Vr for the 3rd harmonic.

For telecommunications cables entering the building, the threat level LC2 (400 V, 1.33 A) is recommended with the same 1-second rise and 60-second pulsewidth shape. The test or analysis should be performed for an external (to the building) injection or an injection into the main telecommunications panel inside the building.

7.2 List of National Points of Contact

Centro Interforze Studi per le Applicazioni Militari
Lt. Col. Engineer Massimo Agostinelli
Via della Bigattiera lato monte 10
56122 Pisa

Fax: +39050964332
Email: massimo.agostinelli@cisam.it

7.3 References

[1] 2nd Committee Draft IEC 61000-5-9 Ed.1.0 – Electromagnetic Compatibility (EMC) – Part 5-9: Testing and measurement techniques – System level susceptibility assessment for HEMP and HPEM.

[2] Rabindra N. Ghose, EMP Environment and System Hardness Design, ISBN 0-932263-16-X, 1984

[3] D.C. Wunsch and R.R. Bell, “Determination of Threshold Failure Levels of Semiconductor Diodes and Transistors Due to Pulse Voltages”, IEEE Transactions on Nuclear Science, Vol. NS-15, No. 6, Dec. 1968, pp 244-259

[4] IEC 61000-1-5 Ed. 2 – High power Electromagnetic (HPEM) Effects on Civil Systems.

[5] D. Nitsch and F. Sabath, Electromagnetic Effects on Systems and Components, Book of abstracts AMEREM 2006, July 2006.

[6] Sedasiva M. Rao, Time Domain Electromagnetics, Elsevier Publishers 1999.

[7] S.D. Hemmady, *A Wave-Chaotic Approach to Predicting and Measuring Electromagnetic Field Quantities in Complicated Enclosures,”* Ph.D. Dissertation University of Maryland (College Park, MD, 2006).

7.4 Acronyms

ac	alternating current
ADS	Aeronautical Design Standard
AECTP	Allied Environmental Conditions and Test Publication
AEP	Allied Engineering Publication
ANSI	American National Standards Institute
CEM	Computational ElectroMagnetics
CNAD	Conference of National Armaments Directors
COTS	Commercial Off The Shelf
CW	Continuous Wave
dB	decibel
dc	direct current
DE	Differential Equation
DEMP	disperse EMP
DMS	Diminishing Manufacturing Sources
DMSMS	Diminishing Manufacturing Sources & Material Shortages
DSL	Direct Strike Lightning
ECM	Electronic Counter Measures
EED	Electro-Explosive Device
EFT	Electrical Fast Transients
EID	Electrically Initiated Device
EM	Electromagnetic
EMC	ElectroMagnetic Compatibility
EME	ElectroMagnetic Environment
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
EN	European Norm
ESD	ElectroStatic Discharge
EUT	Equipment Under Test
E^3	Electromagnetic Environmental Effects
E^3S	Electromagnetic Environmental Effects Susceptibility
FD	Frequency Domain
FEM	Finite Element Method
HA	Hardness Assurance
HEMP	High-altitude ElectroMagnetic Pulse
HIRF	High intensity Radiated Field
HL	High Level
HLI	High Level Illumination
HPEM	High Power ElectroMagnetic
HPM	High-Power Microwave
HW	Hardware
ICs	Integrated Circuits
IE	Integral Equation
IEC	International Electro-technical Commission
IEMP	Internal EMP
IT	Information Technology
LL	Low Level
LLCW	Low Level CW
LRU	line replaceable unit
MHz	Megahertz
MIL-STD	Military Standard
MSCE	Mission and Safety Critical Electronics

MTS	Modernization-Through-Spares
µs	microsecond
NATO	North Atlantic Treaty Organization
NDI	Non Developmental Item
N^2EMP	Non Nuclear EMP
NSL	Near Strike Lightning
OP	Operational Categories
PARA.	Paragraph
PC	Personal Computer
PCB	Printed Circuit Board
PCI	Pulsed Current Injection
POE	Point Of Entry
P-STATIC	Precipitation STATIC
QA	Quality Assurance
QC	Quality Control
QSTAG	Quadripartite STANAG
RADHAZ	RADiation HAZard
RF	Radio Frequency
RS	Radiated Susceptibility
SA	Sustainment Assurance
SCI	Surface Current Injection
SGEMP	System Generated EMP
SREMP	Source Region EMP
ST	Surveillance Test
STANAG	STANdardization AGreement
STF	Stress Transfer Function
SW	Software
TD	Time Domain
UBPR	Unified Barrier Performance Requirement
UE^3	Unified Electromagnetic Environmental Effect
UE^3P	Unified Electromagnetic Environmental Effect Protection
USA	United States of America
USQ	Unified Stress Quantification
UWB	Ultra WideBand
V/m	Volts per meter
V_r	Voltage reference