AEP-41
Volume 1
(Edition 1)

ALLIED
ENGINEERING
PUBLICATION

AEP 41

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

Volume 1

February 2004

AEP-41
Volume 1
Edition 1

BLANK PAGE

AEP-41
Volume 1
(Edition 1)

NORTH ATLANTIC TREATY ORGANISATION

NATO STANDARDIZATION AGENCY

NATO LETTER OF PROMULGATION

February 2004

1. AEP-41, Volume 1 (Edition 1) – UNIFIED ELECTROMAGNETIC ENVIRONMENTAL EFFECTS (UE^3) PROTECTION, PHILOSOPHY AND METHODOLOGY is a NATO/PFP UNCLASSIFIED publication. The agreement of nations to use this publication is recorded in STANAG 4567.

2. AEP-41, Volume 1 (Edition 1) is effective upon receipt.

J. MAJ
Brigadier General, PLAR
Director NSA

BLANK PAGE

AEP-41
Volume 1
(Edition 1)

NATIONAL RESERVATIONS

Nation	Specific Reservations

BLANK PAGE

AEP-41
Volume 1
(Edition 1)

AMENDMENTS

No.	Reference/Date of amendment	Date entered	Signature

BLANK PAGE

TABLE OF CONTENTS

BLANK PAGE

AEP-41
Volume 1
(Edition 1)

AEP 41, VOLUME I

UNIFIED ELECTROMAGNETIC ENVIRONMENTAL EFFECTS (UE^3) PROTECTION, 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
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, 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
Precipitation- Static (P-Static)	Natural	Pulse	Conducted
Electrostatic Discharge (ESD)	Natural	Pulse	Radiated and Conducted
System Generated EMP (SGEMP) External	Hostile	Pulse	Radiated and Conducted
Dispersed EMP (DEMP)	Hostile	Pulse	Radiated and Conducted

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

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

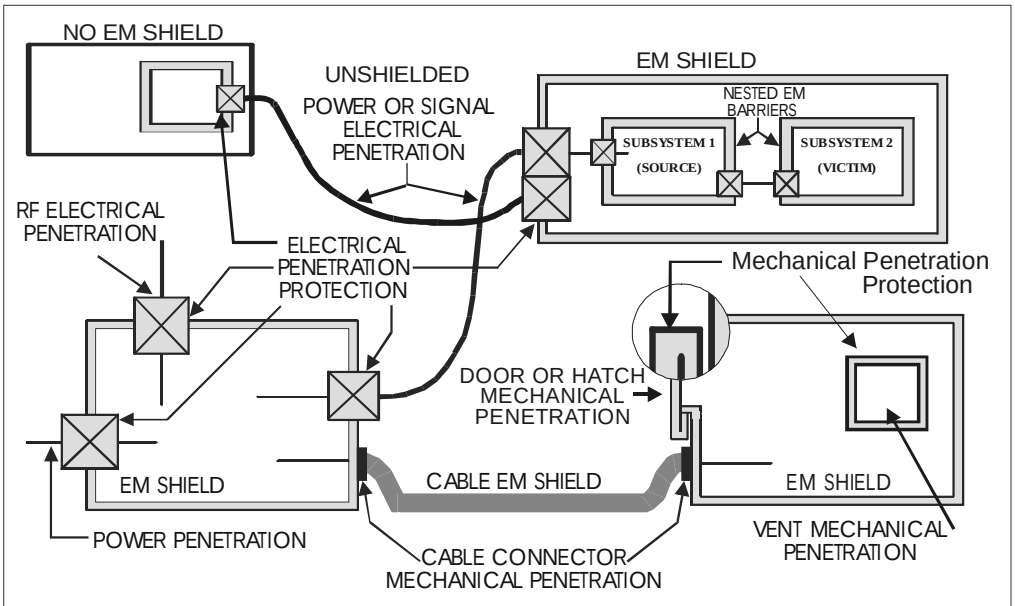


Figure 1. Multiple Barrier Topology Design

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 Fig 2, which is usually iterative and serves basically as a risk management tool. If the

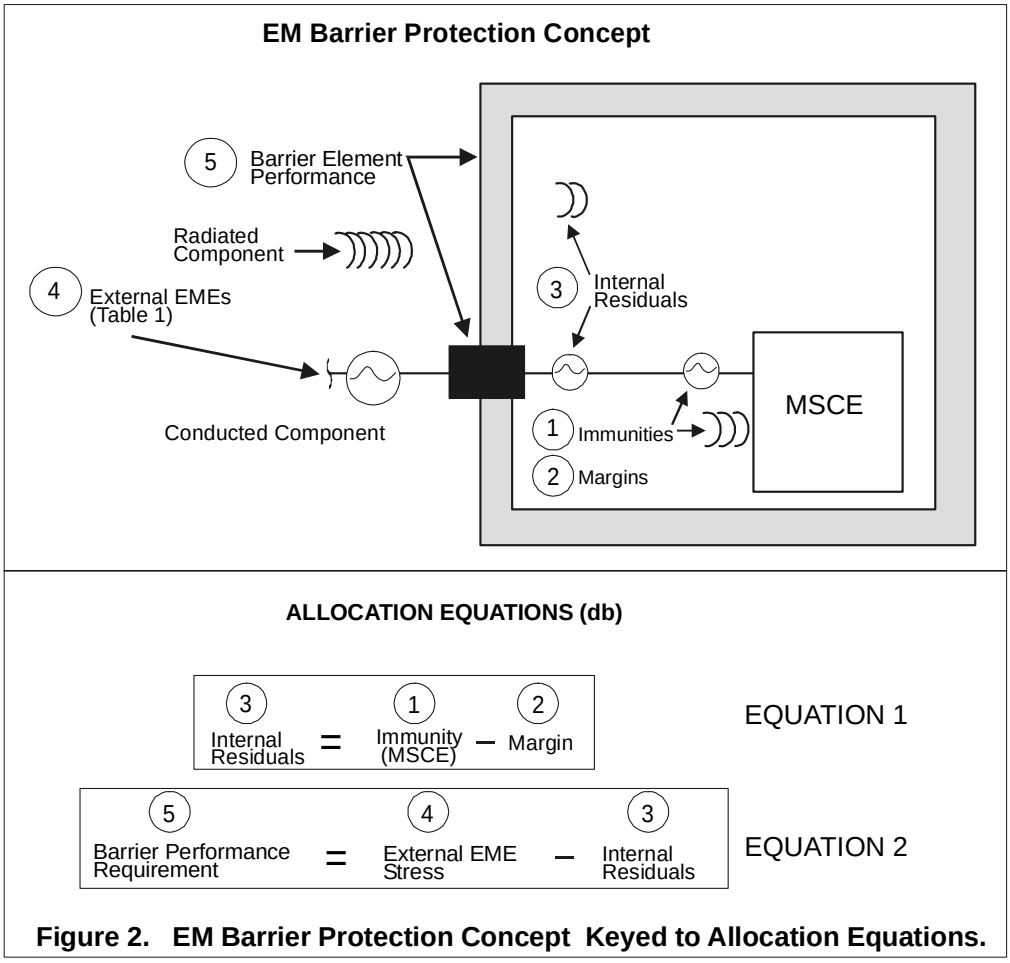


Figure 2. EM Barrier Protection Concept Keyed to Allocation Equations.

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.

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 todays 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 be electromagnetically compatible as well as survivable to a myriad of changing EMEs in the battlespace; and, this compatibility 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 Section 4 of Volume 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 Volumes 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 Volume I, 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 I, EXECUTIVE SUMMARY

This volume provides the philosophy and details of the methodology for achieving UE^3 protection in the battlespace for all six operational classes of military hardware. The hardening methodology traditionally followed is to consider each EME individually and often serially. The methodology proposed in this AEP is one of unifying EM standards and hardening procedures to simplify EM design and testing, and reduce costs. The basic philosophy is an approach to developing, verifying and implementing balanced UE^3 protection so that E^3 survivability can be achieved that is affordable and can be produced and then maintained and sustained throughout the operational life of military hardware. Balance is achieved between: UE^3 protection design and UE^3 coverage of the EME stresses encountered during operational deployment; unified protection provided, and costs and operational impacts; and level of UE^3 protection and risks of operational degradation. The methodology for implementing this philosophy is performance based, and is dependent on use of an EM barrier protection concept, which uses EM barriers to enclose MSCE unit(s) having inadequate immunity levels, and special protective measures for any MSCE unit(s) requiring additional protection beyond what the barrier provides. Such a barrier typically consists of two essential elements: one or more electromagnetic shields (to include nested shields) and conducted penetrations through the shield(s). The shield (including mechanical penetrations) is called an enclosure port. The conducted penetrations are called penetration ports. Thus, by organizing and controlling the interaction of the EMEs with the hardware, the EM barrier can control the potential impact of these EMEs on the hardware's MSCEs and, ultimately, its mission performance. E^3 survivability is achieved by proper application of the EM barrier combined with alternate methods and special protective measures. A principle advantage of the EM barrier protection concept is that a single barrier can potentially provide the capability for balanced, unified E^3 protection from multiple EMEs. Requirements or allocations for protective features must be tested and validated during engineering development and checked for compliance during production and deployment as shown in Table 2.

Table 2. Typical Life-cycle UE^3 Testing

TEST TYPE	OBJECTIVE	TEST OBJECT	PASS/FAIL CRITERIA
ENGINEERING DEVELOPMENT			
Immunity, EM Emissions, Protective Devices, Shielding Effectiveness	Acquire engineering data to support the UE^3 Protection Design. Establish EM emission levels, immunity levels, shielding effectiveness levels, residual levels, and special protective levels.	Bread- and brass-board, MSCE devices and components, prototype CCAs, equipments, and subsystem, materials, and port protective devices	Data and information does/does-not support UE^3 Protection Design
ACCEPTANCE ***EQUIPMENT IMMUNITY***			
EM Emissions	Confirm radiated and conducted emissions are within specified limits	Operating assembled MSCEs	Lower-bound emissions < allocations
Radiated Immunity	Confirm radiated MSCEs immunities meet performance objectives	Operating assembled MSCEs	Lower-bound radiated immunities ≥ allocations
Conducted Immunity	Confirm conducted MSCEs immunities meet performance objectives	Operating assembled MSCEs	Lower-bound conducted immunities ≥ allocations
ACCEPTANCE ***BARRIER PERFORMANCE***			
Shielding Effectiveness	Confirm EM shielding effectiveness meet performance requirements	Electromagnetic shield with all penetration protective devices installed	Measured shielding effectiveness ≥ performance requirements
Penetration Protection Devices	Confirm penetration protective devices meet performance requirements	Installed conducted penetration protective devices in barrier with test loads	Measured residual stresses ≤ allocations
DESIGN VALIDATION			
Illumination and/or Injection	Confirm production configuration hardware meets UE^3 survivability requirements by threat level EME illuminations or low- level illuminations plus injections	Final configuration and operating hardware	Acceptable system operation and residual stresses ≤ allocations Production design is E^3 survivable
PRODUCTION COMPLIANCE – HARDNESS ASSURANCE			
Visual Inspections and Measurements	Confirm workmanship and presence of all port devices/techniques and special protection measures. Confirm bonds and grounds meet specifications.	Production hardware Production samples of port penetration devices and special protective measures.	Bonds/Grounds ≤ limits. Port devices/techniques and special protective measures are present and their residual stresses ≤ allocations.
Illumination and/or Injection, Emissions, Immunity, Protective Devices,	Confirm production hardware modified by engineering changes can meet existing or new E^3 survivability criteria. Confirm engineering changes meet performance requirements.	Production hardware and production samples of engineering changes.	Hardware is E^3 survivable Engineering change residual stresses ≤ allocations

Shielding Effectiveness			
DEPLOYMENT COMPLIANCE – SUSTAINMENT ASSURANCE			
Visual Inspections and Measurements	Confirm deployed hardware is being properly maintained and repaired, and effects of ambient environments, age, and usage has not degraded E^3 survivability	Maintained and repaired deployed hardware.	Hardware is E^3 survivable Acceptable system operation and residual stresses ≤ allocations
Illuminations, Injections, EM Emissions, Immunity, Protective Devices, Shielding Effectiveness	Confirm deployed hardware modified by engineering changes meets existing or new E^3 survivability criteria. Confirm engineering changes meet performance requirements.,	Deployed hardware with engineering changes. Samples of engineering changes.	Hardware is E^3 survivable. Engineering change residual stresses ≤ allocations
SURVEILLANCE TEST – PRODUCTION			
Illuminations, Injections, shielding effectiveness, Immunity	Re-confirm E^3 survivability and assess adequacy of HA Program by performing periodic tests on randomly selected production hardware and hardware elements/items.	Production Hardware and/or selective elements of that hardware.	Production hardware is E^3 survivable. Hardware elements/items meet performance requirements. HA Program is/is-not adequate.
SURVEILLANCE TEST – DEPLOYMENT			
Illuminations, Injections, shielding effectiveness, Immunity	Re-confirm E^3 survivability and assess adequacy of SA Program by performing periodic tests on randomly selected deployed hardware and hardware elements/items.	Maintained as-is deployed hardware	Deployed hardware is E^3 survivability. Hardware elements/items meet performance requirements. SA Program is/is-not adequate.

3.1 Introduction to AEP 41, Volume I

3.1.1 Philosophy. The philosophy is to provide a User-controlled approach to achieving and verifying, and then producing, maintaining and sustaining affordable balanced UE^3 protection and survivability in all six operational categories of NATO military hardware. To be successful, this philosophy must be applied early in the hardware design phase and be made available to design engineers of all levels of assembly in order to be affordable, producible, maintainable and sustainable, and flexible for future upgrades and modernizations. This UE^3 protection philosophy provides a systematic approach for balancing the cost and quality of the EM barrier protection concept against the risk of unacceptable mission degradation and/or failure.

3.1.2 Methodology. The methodology based on use of an EM protection barrier is illustrated in Figures 1 and 2. The actual geometry/topology of the EM barrier can take

many forms some of which are shown in Figure 3. Note that the options range from no barrier to a complete barrier. Topological decomposition subdivides a problem into a set of volumes (or localized area) through which the EM energy propagates and surfaces through which it penetrates. The purpose of the barrier (where the prime level of unification occurs) is to reduce the externally and internally generated EMEs (conducted and radiated) to residual and stress levels (i.e. voltage and current) consistent with acceptable operation of the protected MSCEs. Shield penetrations (electrical and mechanical) must be controlled through the effective use of penetration protection devices, components and/or mechanical design. Conducted penetration ports are usually controlled with filters for Continuous Wave (CW) EMEs (out-of-band stresses) and nonlinear protection devices for pulsed and multi-pulsed EMEs (in-band stresses). Mechanical penetrations are usually controlled using gaskets, grids, finger stock, and/or waveguides. Choosing the acceptable operational level and, in turn, the barrier performance requirements, involves a process of balancing the internal residuals from the externally and internally generated EME stresses, the MSCE immunities, and the margin selected to control risk. The engineering trade studies necessary to achieve this balance are called the allocation process, (see Figure 2), which is usually iterative and serves basically as a risk management tool. The allocation approach assigns performance requirements to both the enclosed and penetration ports. The approach can then be used to unify the barrier performance requirements to define a single performance requirement for each port that addresses all applicable immunities and EMEs e.g. single immunity and EME, multiple immunities and single EME, and multiple immunities and EMEs.

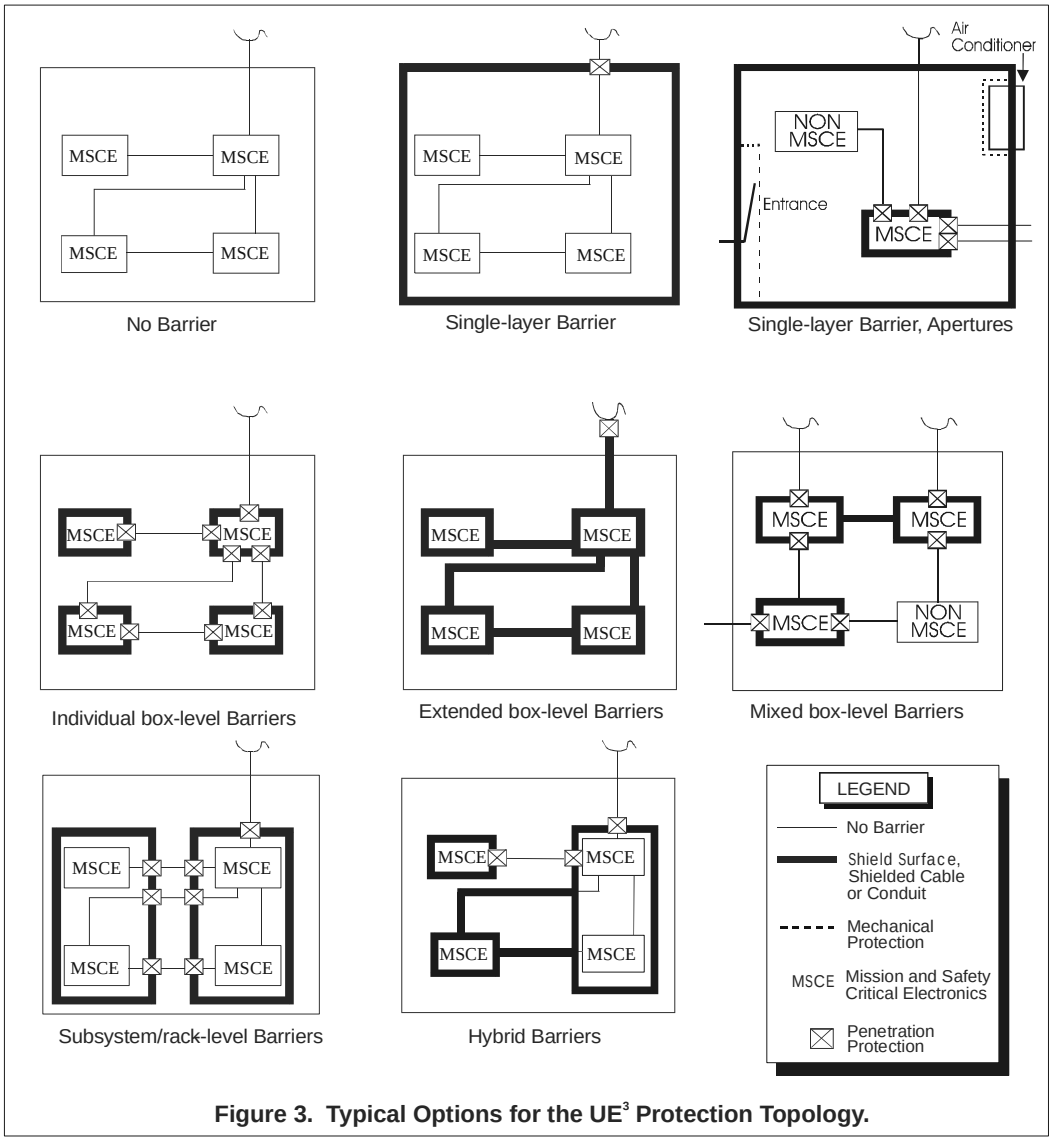


Figure 3. Typical Options for the UE^3 Protection Topology.

In addition to using the EM barrier, alternate methods such as mitigation, timely re-supply, operational protection, functional protection, etc, should be considered in the design and engineering evaluation process to achieve E^3 survivability and for potential cost reduction. Mitigation is often employed in E^3 survivability whereas timely supply is not due to the theater-wide HEMP threat. Functional protection can be used along with the EM barrier protection in achieving E^3 survivability by addressing upset anomalies through the use of component/software protocols that are fault tolerant and/or circumvention/resets circuits. Operational protection can also assist in achieving E^3 survivability by providing the crew procedures to follow when anomalous response occurs. Both operational and functional protections are valuable in surviving upset, thereby, leaving the EM barrier to protect against damage.

The proposed methodology simplifies and reduces developmental and verification testing by facilitating unified testing to multiple EMEs to confirm hardware performance, thereby, minimizing test costs and hardware requirements. Table 2 shows typical tests performed during the various acquisition phases.

The methodology includes, as an integral part, the designed-in accommodation for HA and SA by focusing on the protective elements [shield(s) and protective devices(s)] and their ability to continue to meets their protection allocations. In addition, this methodology minimizes sensitivity to changes in EME specifications, accommodates reductions in MSCE immunity levels, and simplifies retrofits (if required). Finally, this methodology, by reducing the source generated EMEs to a relatively benign residual EME on the MSCEs, accommodates the incorporation of COTS/NDIs in the design as well as later insertions due to (DMSMS) solutions, technology advances, upgrades and modernization programs such as Modernization-Through-Spares (MTS). Table 3 in Section 4.2 outlines the proposed systematic approach for achieving UE^3 protection.

3.2 Scope for AEP 41, Volume I

3.2.1 Philosophy and Methodology

The scope presents a philosophy and methodology for achieving unified E^3 protection and hardening against battlespace and peace time EMEs such that NATO platforms, systems and equipments will be UE^3 survivable. The methodology employed is based on an EM barrier protection concept whose focus is to ensure that protective features: meets protection allocations in a manner that is cost effective while in concert with other system requirements, can accommodate the use of COTS/NDIs, and, most importantly, can be produced, maintained and sustained throughout the hardware's life-cycle. Various options for achieving adequate and affordable UE^3 protection/hardening will be considered such as: multi-barrier designs and use of nested barriers for victims and sources within the primary EM shield (Figure 1), various barrier topologies (Figure 3), alternate Methods (Figure 4), and special protective methods (Figures 5 and 6). Details will be provided in Para. 4.2.3.4 on how to determine the EM barrier performance requirements for: single EME and single immunity, single EME and multiple immunities, and multiple EMEs and multiple immunities. Unification of the various types of E^3 tests illustrated in Table 2 that must be performed during the last three phases of the hardware's life-cycle are discussed as well as how the tests should be tailored to the operational requirement of the hardware. Finally, a discussion is provided on preserving the integrity of the verified UE^3 protection design and verified level of E^3 survivability during production and deployment. Included are discussions on potential impacts due to: insertions and/or additions of more energy sensitive MSCEs, addition of new MSCEs and equipments to enhance capabilities, and debilitating effects from age, corrosion, usage, imperfect maintenance, and repeated exposure to EM and ambient environments.

3.2.2 Risks

There are risks with an E^3 protection concept, as well as the implementation, production, and sustainment of that concept during the life-cycle. These risks are driven primarily by: funding and time limitations, inadequate EM protection design, late insertion and development of the UE^3 protection design, no implementation of a well thought-out HA/SA program, and inadequate testing. Consequently, there is risk in all four life-cycle phases. To minimize and manage risks, a hardening approach must be developed during the design concept phase, implemented and validated during the engineering phase, and preserved during the production and deployment phase. Therefore, a thorough life-cycle program must be defined and implemented during the concept/design phase and fully developed during the engineering development phase. The life-cycle program, HA and SA, will manage and preserve the E^3 survivability design. The database of the life-cycle program must be updated with pertinent data, results, and information throughout the remainder of the acquisition phases. The life-cycle program itself will experience changes due to corrective action for inadequacies, improvements due to new knowledge, and updates for engineering, modernization, EME, and other changes. Thus, the implementation of early-in-design E^3 survivability based on the UE^3 protection concept followed by a well designed HA and SA program is the best tool for risk management.

4.0 UNIFIED ELECTROMAGNETIC ENVIRONMENTAL EFFECTS PROTECTION

4.1 Overview

4.1.1 General

Presented is an affordable approach to achieve UE^3 protection, based upon the EM barrier protection concept, that is practical; yet, achieves E^3 survivability in the battlespace for all classes of NATO platforms, systems and equipments of the six operational categories. Adequate E^3 protection of electronic/electrical material is essential since these military 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 destroy mission essential capabilities. In addition, the hardware must remain E^3 survivable for much longer periods of deployment (>50 years for many) while accommodating multiple upgrades and modernizations. The hardware must remain survivable against the traditional degradation impacts from ambient environments, aging, usage, and repeated maintenance and repairs. Today's hardware must also remain survivable against new factors such as integration of COTS/NDIs, and DMS-solution and technology insertions. (See AEP-50 and Vol. II of this AEP)

4.1.2 Electromagnetic Environments (EMEs)

Three general types of EMEs that military hardware must be survivable to are discussed in detail in Volume II and briefly below:

Naturally Occurring EMEs: Electrostatic discharge (ESD) and lightning are the two types of naturally occurring EMEs specified for most military hardware. Precipitation static (P-Static) applies primarily to OC5 platforms and briefly to the launch phase of OC3 systems. ESD by personnel applies to MSCEs of all six OCs of military hardware due to personnel involvement. ESD by helicopter applies to OC1, OC4, OC5 and OC6 due to landing of vertical lift aircraft, in-flight refueling, and systems operated or transported externally by vertical lift aircraft. Both NSL and DSL environments can affect all six OCs of military equipment. Except for regions of the poles, lightning is prevalent over all portions of the earth.

Electronics Operation Generated EMEs: Whenever electrical or electronic circuits operate, EM fields and/or currents are produced. These EM fields and currents can, in turn, affect or interfere with operational performance of victim MSCEs by a process called EM Interference (EMI). The EMEs due to electronic operation can be generated outside and/or inside the victim's hardware (See Table 1). The EMEs generated outside the victim's hardware are due to the operation of neighboring or remotely located hardware, or even remote or external units of the victim's hardware. Included in this category of externally generated EMEs is High Intensity Radiated Field (HIRF) generated by radars or other high-power emitters. When military hardware operates sufficiently close to HIRF emitters, the victim's electronic circuits and operations can be affected. Survivability to these external EMEs is normally addressed under control of EMI characteristics for equipments or inter-system EM Compatibility (EMC) for systems and platforms. Harmful levels of EMEs can also be generated internal to the hardware by the operation of electrical or electronic circuits within the hardware. These EME sources can cause neighboring electronic MSCE units or hardware to functionally upset or to be damaged. Survivability to these internal EMEs is normally addressed under control of EMI characteristics of equipments or intra-system EMC for systems and platforms.

Hostile EMEs:

Hostile EMEs are generated by an adversary for the specific purpose of degrading the performance of the victim's MSCEs. Hostile EMEs considered in this AEP are of two types: nuclear and non-nuclear generated. Nuclear weapon generated EME includes: High-Altitude Electromagnetic Pulse (HEMP), System Generated EMP (SGEMP), and Dispersed EMP (DEMP) for exo-atmospheric burst; and Source-Region EMP (SREMP) for endo-atmospheric burst. The HEMP has early, intermediate, and late time components. However, for most terrestrial hardware only the early time HEMP component requirement is considered. SGEMP results from the weapon's prompt gammas interacting directly with a system (OC-1, OC-2 and OC-6), and prompt gammas and X-rays interacting directly with a system's surface (OC3). In particular, the two internal components of SGEMP (box internal EMP (IEMP) and cable IEMP) are of great concern to space systems (AEP-50). DEMP is an unique case of HEMP where the radiated signal misses the earth and propagates through the ionosphere to a distant line-of-sight satellite (OC3

system, AEP-50). Although DEMP<SGEMP in magnitude, DEMP should be considered for satellite hardening because its frequency spectrum and pulse (similar to a swept CW waveform) may be considerably different than those of a SGEMP. This is due to the HEMP that traverses the ionosphere (a dispersive medium) to the satellite is "stretched out". SREMP formerly called low-altitude EMP (AEP-4) is a complex environment consisting of a deposition region of high air conductivity (both electronic and ionic) that decreases away from the burst point, and a localized EMP (sometimes referred to as endo-atmospheric EMP) with considerable horizontal magnetic and vertical electric field components. In addition, SREMP has a gamma pulse component that can directly interact with a system releasing Compton electrons, which, in turn, produces a complex EME that includes external and internal fields and currents induced on surfaces and within cables. Since hardware or hardware elements must be within the deposition region to be at risk, SREMP is normally considered for certain OC1 systems (AEP-20), OC2 systems (SHAPE 1460-3), and OC6 systems (AEP-19 and -20).

Non-nuclear weapon generated hostile EME includes High-Power Microwave (HPM), Non-Nuclear EMP (N^2EMP), and Ultra-Wideband (UWB). High power emitters consisting of RF generators, pulse forming networks, and directional antennas typically produce these hostile EMEs In addition, there are other types of hostile EMEs that will not be considered in this AEP such as Electronic Warfare and laser.

Any of these EMEs may interrupt, obstruct, or otherwise degrade or limit the effective performance of MSCEs or electrical equipment. As such, any of these EMEs may cause EMI that results in EM Compatibility (EMC) problems within the system or platform, or at the system or platform level [ANSI C63.14-1992]. Partial or complete loss of mission capability may result from these EMEs. A list of the EMEs is shown in Table 1.

4.1.3 Electromagnetic Environmental Effects (E^3) Survivability

4.1.3.1 UE^3 Protection. In general, the military hardware performance degradations are due to either functional upset or permanent damage of MSCEs caused by EME induced stresses. The purpose of the EM protection barrier is to provide a tool for control of the EMEs so that their resulting residuals are levels that enable the hardware's operational requirements to be met; and, furthermore, UE^3 survivability achieved to be preserved throughout production and deployment. The actual EM barrier geometry can take many forms some of which are illustrated in Figure 3. Note that these topology options range from: no barrier, assuming the allocation burden is placed entirely upon the MSCE's immunities; to a single-layer integral barrier where the allocation burden is placed entirely on the barrier; to subsystem/rack level barriers that can be tailored for controlling EME stresses in different regions of the hardware; to box level barriers that protect the individual MSCE units; to hybrid barriers that utilize the EME stress control features of both subsystem/rack and box level barriers.

4.1.3.2 Alternate and Special Protective Methods.

4.1.3.2.1 Alternate Methods. In combination with the UE^3 barrier, alternative methods may be desired in achieving E^3 survivability and reducing cost. Evaluation and selection of methods to be combined with the UE^3 barrier must occur in the design phase in order to be cost and design effective. The concept of using combination of methods to achieve E^3 survivability is shown in Figure 4.

4.1.3.2.2 Special Protective Methods. There are cases where special protective measures are required because adequate UE^3 protection cannot be achieved with the EM barrier alone. All volumes discuss these cases as they pertain to the volume's subject. Three major cases are provided.

a. The first case involves additional shielding, equipment-level protection, and/or unique penetration protection devices to achieve adequate E^3 survivability. Typical cases involve MSCEs that are: outside the EM barrier, within the EM barrier but still experience unacceptable responses (measured during subsequent verification testing), or within the EM barrier but still need additional supplementary isolation due to regular protection device interference with hardware's operation. Special protection measures should only be used for exceptional cases and not as a substitute for the EM barrier if all performance requirements can be met by the barrier.

b. A second case involves SREMP, which can affect hardware that are within or have conductive elements within the deposition or source region of a surface or near-surface endo-atmospheric nuclear event. As illustrated in Figure 5, SREMP occurs when the armored protected system (OC1) is within the deposition region and survives the other nuclear environments such as airblast, thermal radiation and initial nuclear radiation. Strong peak vertical electric fields (10s of kV/m) and horizontal magnetic fields (100s of A/m) are generated and can interact with the armored system producing currents and voltages on cables. These electric and magnetic fields are not perpendicular to one another in the traditional way due to the air conductivity being alter by interactions of Compton electrons (initially released from the gamma photon interaction with air molecules) with air molecules producing secondary electrons. In turn, these secondary electrons cause the air to become conductive producing effects in addition to the EMP-type EMEs. Both the environments and effects on hardware are difficult to predict. SREMP also has a large-in-magnitude peak gamma dose component in the deposition region that can interact with the conductive materials of armored systems or static hardened systems producing external SGEMP as well as internal SGEMP (box IEMP and cable IEMP). Thus, an armored command and control vehicle (OC1) can be affected by the SREMP generated SGEMP as well as the burst generated EMP. Illustrated in Figure 5 is a non-armored sheltered-based mobile command and control (C^2) unit (OC6) consisting of the C^2 systems outside the deposition region but are interconnected with long signal cables that go through the deposition region. The C^2 systems are unaffected directly but are affected indirectly due to induced currents and voltages into the interconnecting cables. Also shown in Figure 5 is another hypothetical case of commercial power transmission lines passing through the outer portion of the deposition region. These conductive lines connect to one of the mobile C^2

systems located outside deposition region as well as a C^2 static site (OC2) causing upset or even damage to end-item MSCEs in both OC systems.

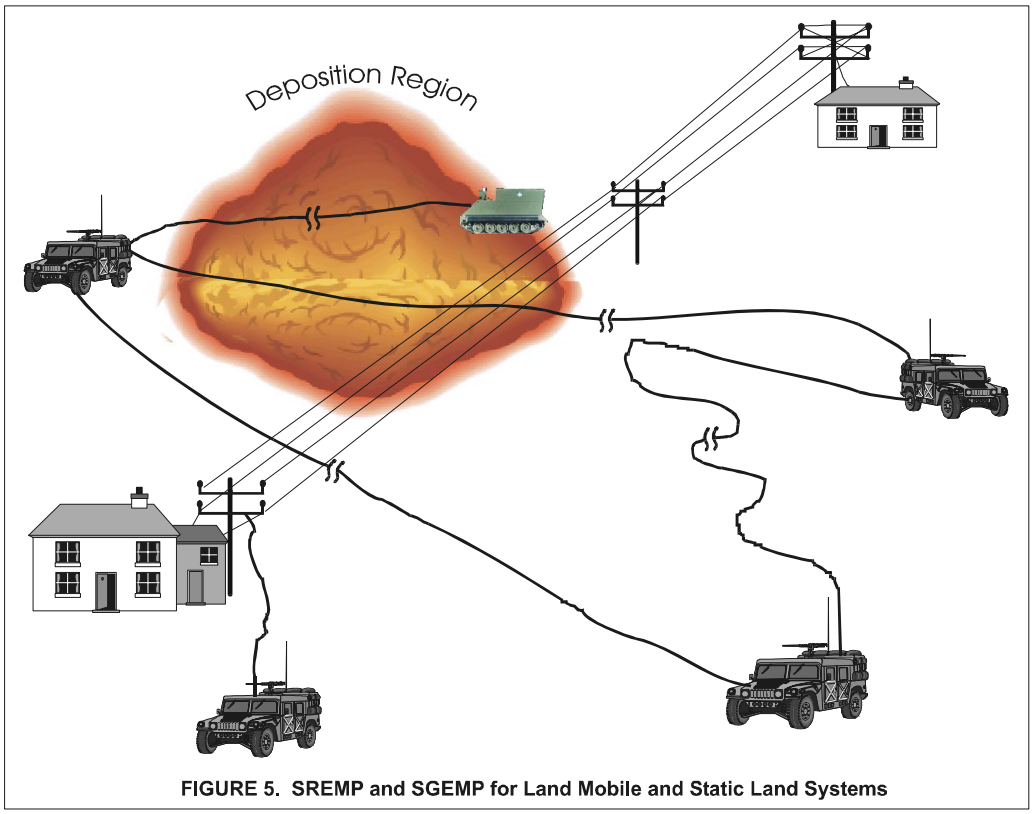


FIGURE 5. SREMP and SGEMP for Land Mobile and Static Land Systems

c. A third case requiring special protective methods, shown in Figure 6, is a scenario of an exo-atmospheric nuclear detonation affecting line-of-sight satellites. A nuclear detonation produces copious quantities of gammas and x- rays. These photons become the source of SGEMP for near line-of-sight satellites (OC3) as well as the EMP source region in the ionosphere that produces HEMP for terrestrial hardware (all OCs) and DEMP for a special cased of a distant line-of-sight satellite. The incident gammas and X-rays interact directly with the satellites' surface releasing Compton and photoelectric electrons that produces external and internal currents. External SGEMP can affect external equipments and enter into the interior via port-of-entries (POE). Diffusion through the satellites' skin can be usually be ignored because it is a lesser effect than those from POE penetrations or internal SGEMP. The penetrating energetic photons will create free electrons inside the satellite, which becomes the source of electric and magnetic fields. These fields become the source for two internal SGEMP components, internal fields or box IEMP and cable currents or cable IEMP. Of the three types of SGEMPs, typically the cable IEMP produces the largest internal open-circuit voltages and short-circuit currents. Although DEMP (~10 V/m) is usually not a problem if the satellite is hardened to survive SGEMP (box IEMP, ~100s V/m); DEMP should still be considered in the design because it has different coupling characteristics than SGEMP due to the EMP being stretched out as it traverses the ionosphere to the satellite. If no SGEMP hardening has been provided, then even the small DEMP environment can be a threat by causing spurious signals in the space system.

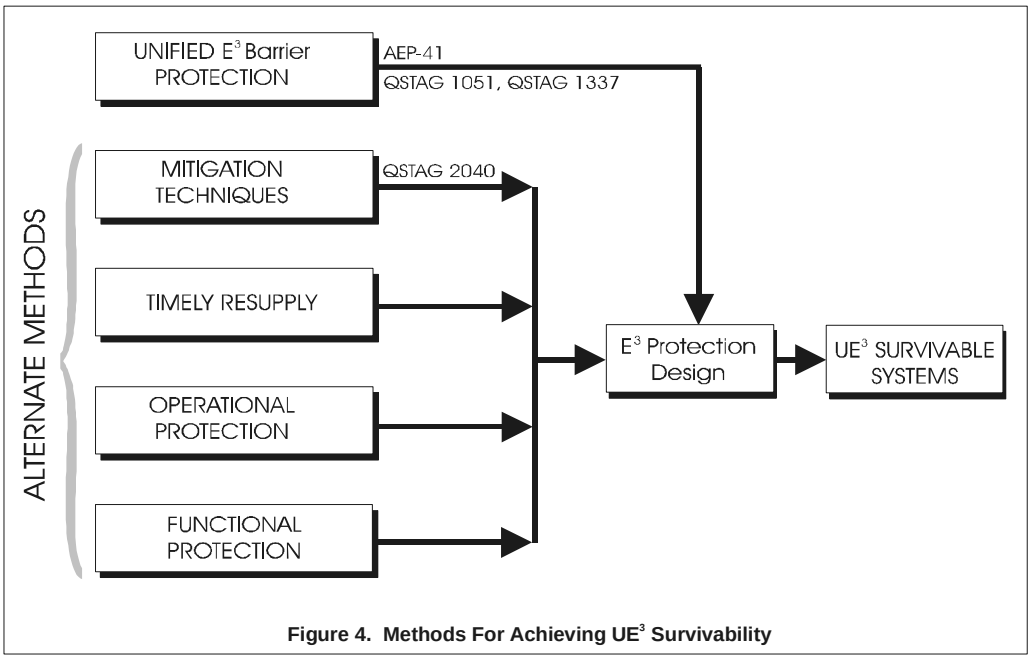


Figure 4. Methods For Achieving UE³ Survivability

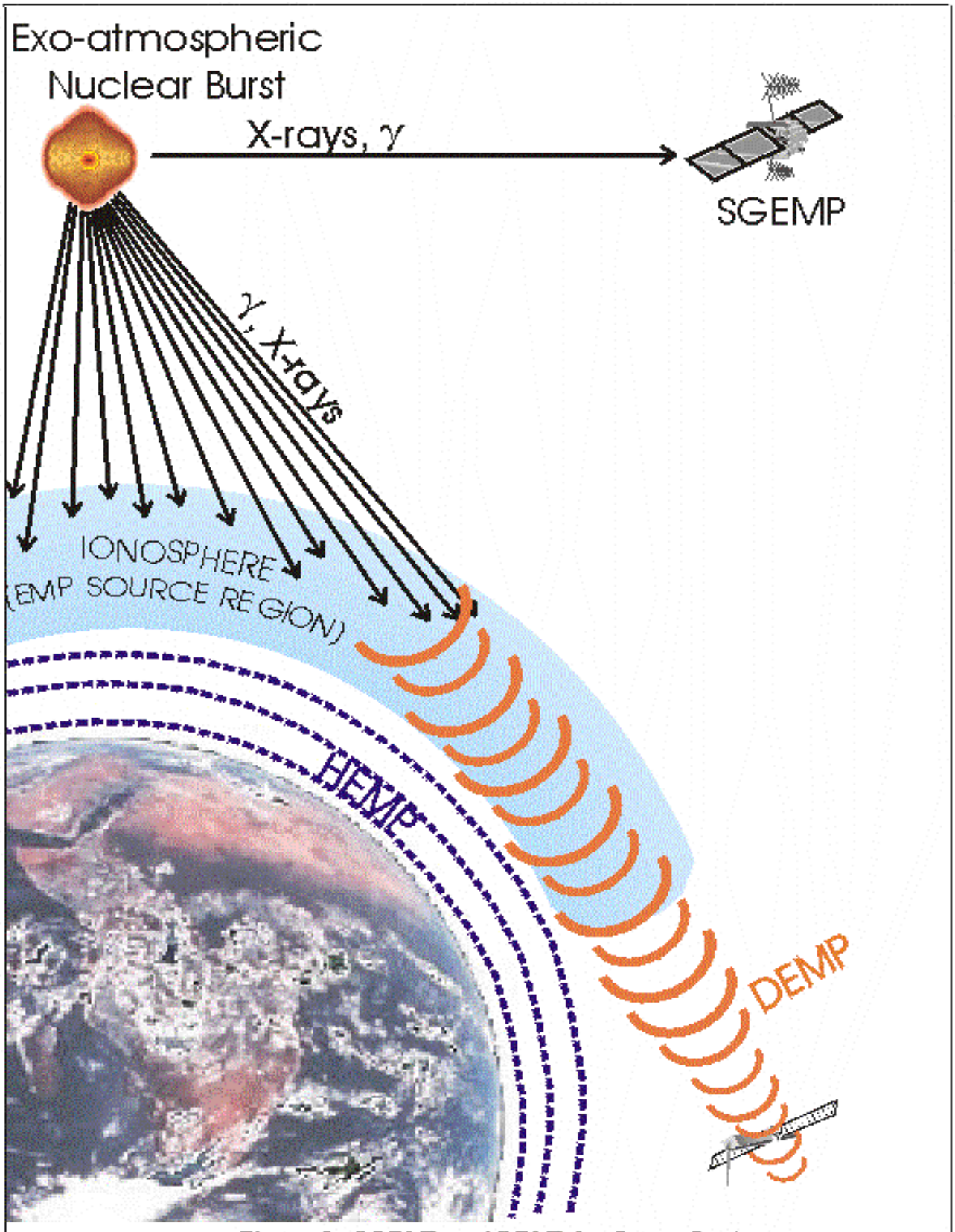


Figure 6. SGEMP and DEMP for Space Systems

4.1.4 Evolution of Electronics and COTS/NDI Usage

To achieve UE^3 survivability, adequate protection of all MSCEs must occur against both externally and internally generated EMEs. The MSCEs requiring protection are becoming increasingly more sophisticated, complex and sensitive to EMI. The increase in EMI sensitivities are due to: higher operating frequencies of digital electronics, smaller feature sizes, greater use of energy sensitive technologies, continued evolution to lower operating voltages for circuits and devices, increasing use of plastic encapsulated microcircuits (less inherent shielding), higher integration densities (both within packages and circuits), and increase use of COTS/NDIs. Consequently, the increasing use of these sophisticated electronics in the design, production, and, especially, in the deployment (maintenance/repairs/upgrades) of military hardware emphasizes the importance of applying an encompassing, versatile UE^3 protection scheme employing the EM barrier protection concept. It is especially important that this protection concept be incorporated early into hardware design in order to be affordable, achievable, and versatile to accommodate the many future changes involving MSCEs most of which will have lower immunity levels. In addition, this UE^3 protection scheme must be one that allows for COTS/NDIs to be used at all assembly levels in the initial design and the design as it matures as well as the design during production and deployment. Integration of COTS/NDI into the hardware throughout its life-cycle must be planned because such integration will occur to accommodate DMSMS solution and technology insertions, changes due to upgrades and modernizations, and changes due to maintenance and repair.–As an example, the MTS Program is a performance based concept that integrates state-of-the-art electronics into aging systems as part of maintenance for the explicit purpose to stabilize Mean Time Between Failure Rates (MTBFRs), improve readiness levels, increase the hardware's battlespace performance capabilities, and be proactive in regards to DMSMS issues.

4.1.5 Unified E^3 Protection Approach Overview

4.1.5.1 General

This section presents and overview of the procedures for achieving balanced E^3 hardening. Details follow in the paragraph 4.2

When applying the Unified Approach to E^3 protection, it might be possible to combine time or frequency EMEs together to reduce design, analysis and/or test costs. However, there are significant technical issues that must be considered. These are discussed in detail in Volume III.

4.1.5.2 Route to Adequate Protection

4.1.5.2.1 Development of E^3 Protection: Figure 7 is a flowchart showing the basic procedural steps to be followed in achieving EMC in a project. These steps occur during a hardware design concept and engineering development program (Phases 1 and 2).

4.1.5.2.2 Hardening Requirements: Figure 8 shows the steps in developing

effective hardening requirements in a program to ensure suitable in-built protection in the final hardware. These seven steps are the hardening activities required to achieve an EMC design (Figure 7) and are briefly discussed.

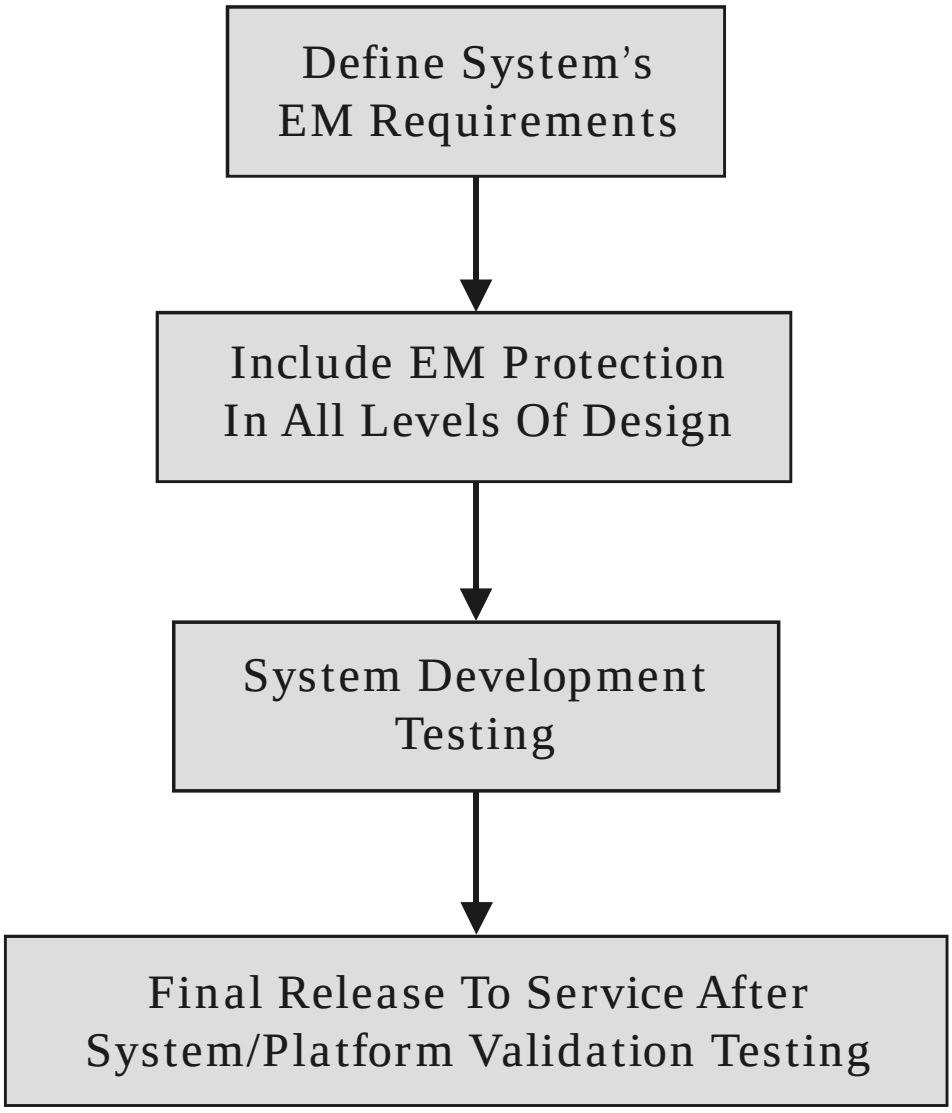


Figure 7. Procedural Steps to Achieve Electromagnetic Compatibility in a Project.

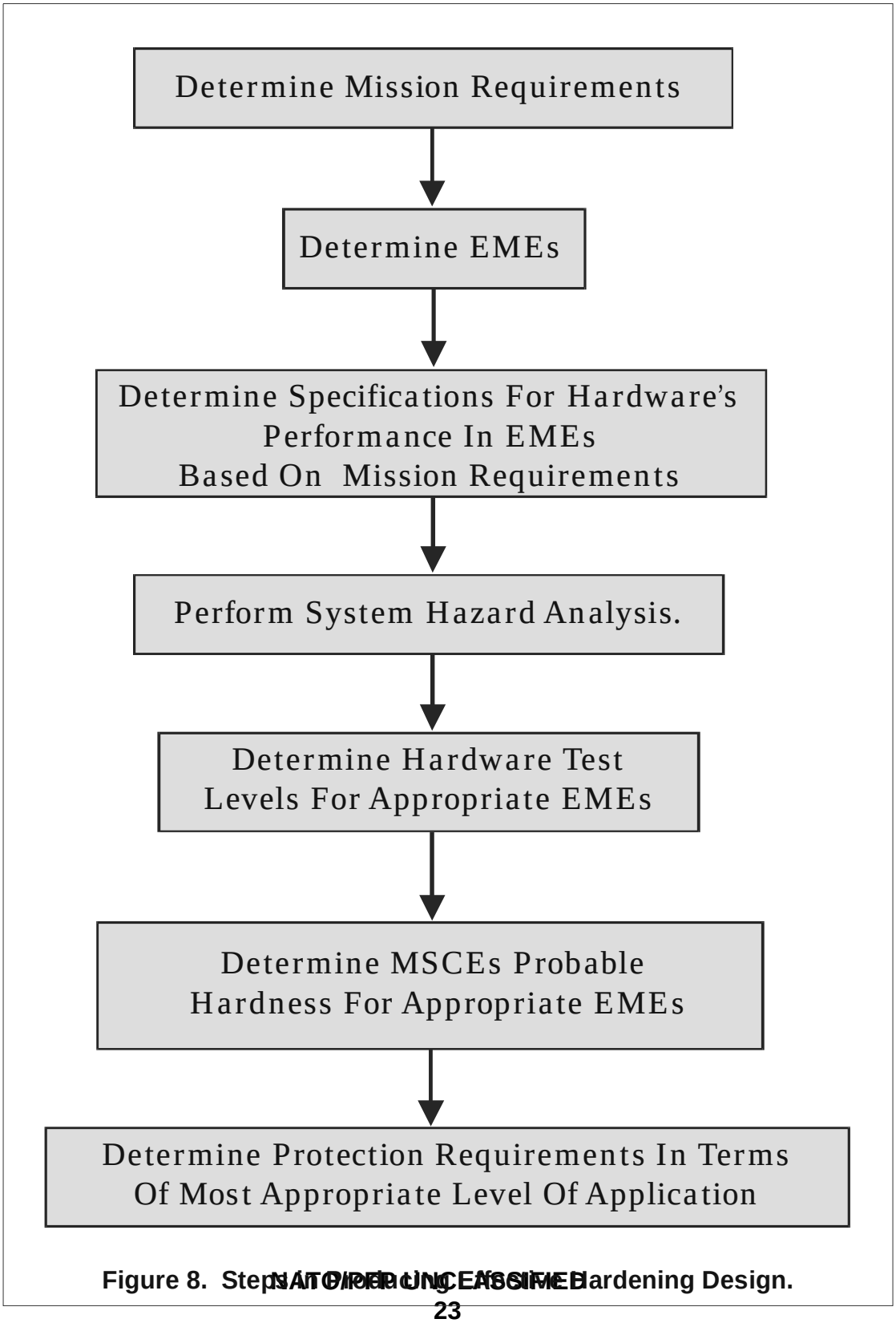


Figure 8. Steps In Performing EMP Hardening Design.

Step 1: Determine Mission Requirement

The mission requirements of the hardware are determined, and the various scenarios to be used is defined. These factors govern the EMEs that the hardware is likely to encounter during its entire deployment lifetime. For instance, the requirements on transport hardware may be very much lower then those for a front line combat hardware, although multi-role hardware will have to be designed to cover the worst case EME they may encounter.

Step 2: Determine EMEs

The various EMEs are defined in detail in Volume II of this AEP and listed in Table 1. All EME threats are continuously updated due to a better understanding of the EME threat as in the case of lightning, new EME transmitters coming on-line, new threat scenarios, or insertion of more E^3 sensitive MSCE devices or units. EME threat projections are critical in defining the built-in design features, design flexibility, and margins.

The "my threat is larger than your threat" syndrome that tends to be prevalent when various groups are competing for funds must not be allowed to color the judgment of the program manager. All EME threats should initially be given equal consideration in a procurement program. An EME threat, which may be worst case for one system, may not be for another, and changes in constructional material can impact on which EME threat can cause the biggest problems. For instance, the use of carbon fiber composite in airframes increases the lightning protection required due to the composite's poorer electrical and thermal conductivity properties.

Step 3: Determine Hardware Specification

It is important to tailor the requirements to those needed to ensure that the required hardware performance is met. Sometimes, equipments may be used on several platforms/systems; therefore, platform/system specifications applied to such equipments must be encompassing.

Over-specifying will involve cost penalties. A degree of degradation may be permissible. It may not be necessary for all the equipment to work all the time. An example of this may be lightning strike where on some aircraft programs, only flight critical equipments are protected, not mission critical equipment, as the probability of a strike is low and the resultant attrition would be acceptable. Another example involves many ground and naval systems/platforms when operational recovery can occur within a specified timeframe due to crew intervention (without hardware replacement or repairs); thus, preventing the need for hardening to a more expensive and difficult requirement of operate-through.

Under specifying may mean the platform/system fails to meet its mission requirements in all areas of the EME battlespace. In addition, the platform/system will unlikely be able to accommodate future electronic insertions or EME threat changes without

expensive re-designs to achieve adequate hardening. Also, one would anticipate later increase in susceptibilities due to normal E^3 protection degradation that occurs during deployment.

Step 4: Perform System Hazard Analysis: i.e. Determine Hardware Criticality and Upset Criteria

The functional criticality of the various hardware equipments must be defined. This will define the severity of the requirements to be put on the supplier of the hardware. The performance requirements of the hardware can then be defined in terms of allowable upset. An example of this is in the civil aircraft environment where there is an "everyday" and a Level I "emergency" environment with different performance requirements for the systems. Another example may be armored or mobile missile systems where upsets are allowed so long as crew intervention can restore system functionality within a specified period, say 5 minutes, and without changing components.

Step 5: Determine Hardware Test Levels

Now that the EME and required performance has been defined, the test specifications complete with levels can be defined. This can be assisted by the use of data from previous hardware tests such as the transfer functions defining the relationship between the external threat fields and the stresses at the internal MSCEs. These will provide a reasonable assessment of the internal environment the systems designer must protect against and provide test levels for the military hardware compliance specifications/standards. It must be remembered that the limits provided in military EMI/EMC standards such as AECTP 500 series are for guidance and need to be tailored for particular applications.

Where possible, the defined internal environments and test procedures can be integrated together to reduce test costs and aid in the design stages.

Step 6: Determine MSCEs Probable Hardness

In today's environment, usage and later insertions of COTS/NDIs must be planned and designed for. As no or minimal control can be applied to their individual E^3 hardness, an assessment of their E^3 hardness or immunity levels will aid in defining extra design measures which need to be taken to protect these COTS/NDIs when installed, and prevent possible compromise of the hardware performance. However, the EM barrier protection concept to include good margins and planned flexibility in the design will enable future COTS/NDIs insertions and additions to occur without major impacts such as major re-designs and/or hardening efforts/costs. A discussion on COTS/NDIs vulnerabilities can be found in Volume IV "Susceptibility of Platforms, Systems and Equipments to E^3"

Step 7: Determine Protection Requirements

The required protection of the hardware is usually defined in terms of various required performance characteristics of the various "barriers". These performance characteristics are dependent on the EME threat and the type of "barrier" being specified. EME threat unification can ease the definition of the requirements but extreme care is required when attempting to unify the requirements for time and frequency domain threats. Often, only partial unification of protection requirements is practical. Figure 9 illustrates examples of the various protection methods available to the designer. Some of the protection procedures revolve around the use of protective devices such as metal oxide varistors (MOVs), transorbs, surge arrestors, filters or system skin design. Others revolve around more esoteric methods, such as system and software architecture. The latter group is harder to characterize in terms of protection requirements. Protection methodology is discussed in detail in Volume V: "Unified Hardening and Protection Against E^3".

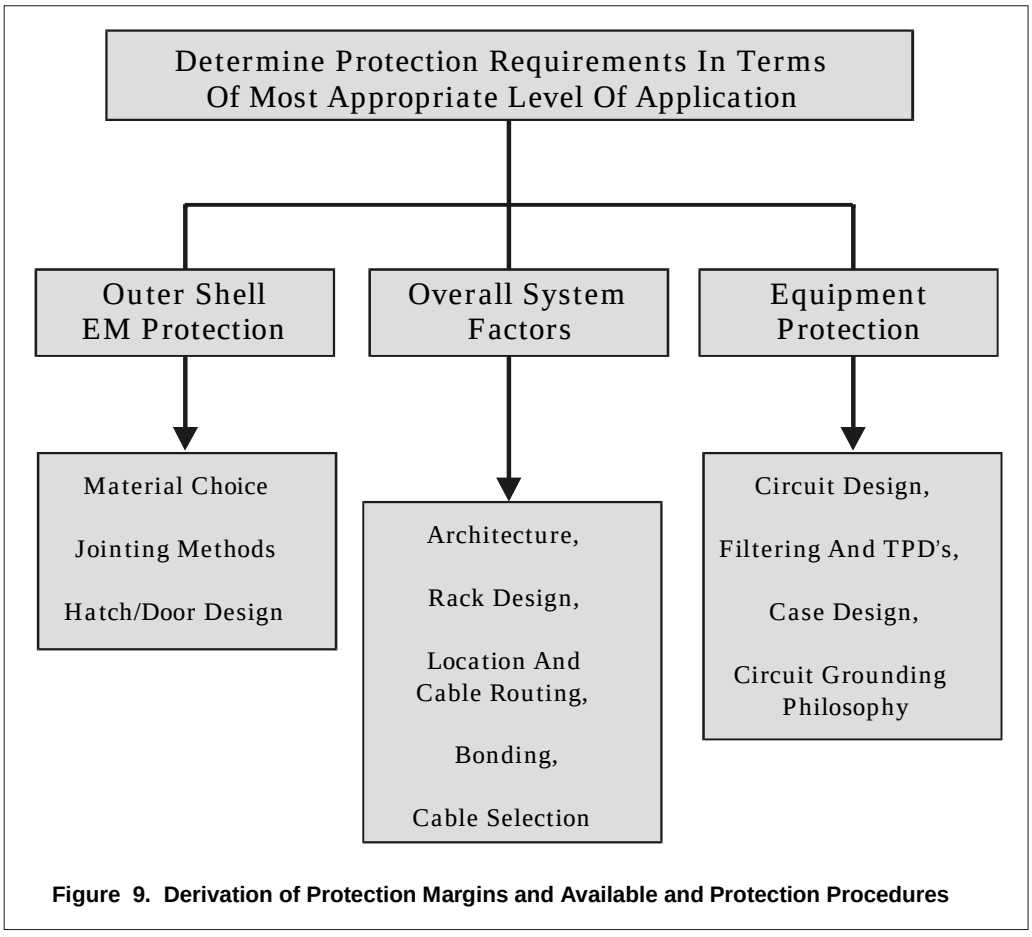


Figure 9. Derivation of Protection Margins and Available and Protection Procedures

4.1.5.2.3 Testing and Validation of UE^3 Protection The final two stages of Figure 7 are tests and evaluations, which are essential and must be performed in order to ensure adequacy and that the protection design meets hardware specifications and compliance requirements. Testing is both a critical and an integral part of the UE^3 protection concept. Tests are designed to aid in the allocation process by determining MSCE unit immunity levels and the determination of the ability of the protection features to meet their protection allocations rather than simulating individual EMEs. These tests aid in developing the detailed design (Phase 1), demonstrating final compliance (Phase 2), and demonstrating adequate E^3 protection is entering production (Phase 3). Commercial test standard should be used when appropriate. First principle analyses are often used in the allocation process. Table 2 provides a summary of the E^3 test protocol guidelines for testing during a system's life-cycle. The test methods are discussed in detail in Volume VI: "Testing and Validation of E^3 Protection"

4.1.5.2.4 Stress Transfer Function (STF). The stress transfer function relating the external environment to the internal environment is an engineering tool that can be used in evaluations of internal stresses seen by the MSCE equipments. This STF describes the performance of the "barriers" surrounding the equipment. The MSCEs may be located within a single compartment or distributed internally and externally to the system/platform. These "barriers" may be represented by Figure 10 and include such items as:

- Outer, Internal and Cable Shields
- Antennas
- Penetration Protection Devices

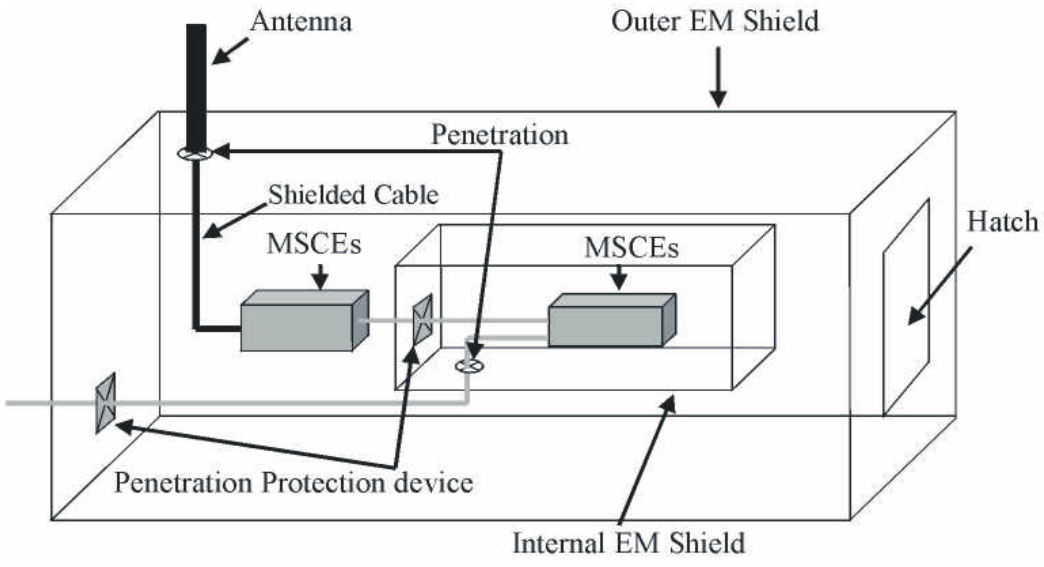


Figure 10. Illustration of a Simplified "Barrier Topology"

The STFs describing the effect of such barriers are usually defined in three primary ways:

- Relationship of the internal field surrounding the equipment to the external stress.
- Relationship of the induced equipment cable bundle or wire currents to the external stress.
- Relationship of the induced pin voltages to the external stress.

The STF of the barrier may not be linear in time, frequency or amplitude of the applied EME threat, depending on the elements contributing to the barrier. Even when dealing with the hardware's skin, non-linearities due to the material composition can arise. The various coupling definitions are detailed in Volume III of this AEP.

4.2 Life-Cycle Application of the UE^3 Protection Philosophy and Methodology

4.2.1 General

Whereas the preceding Para. 4.1.5 provided an UE^3 protection approach overview this section provides a detailed discussion of how to apply the UE^3 protection concept to the four basic acquisition phases of all six OCs of military hardware. Figure 11 illustrates the four fundamental phases of a life-cycle program along with the corresponding technical activities supporting the UE^3 protection design and survivability requirement.

The UE^3 protection concept described in this AEP must be initiated in Phase 1, Concept Definition, and developed and integrated into the hardware's design during Phase 2, Engineering Development. Otherwise, this protection concept as well as any other concept will: become expensive to implement and costly to produce and maintain/sustain; likely to have inadequate margins, and likely to have inadequate flexibility to accommodate future insertions of COTS/NDIs and changes due to upgrades and modernization programs.

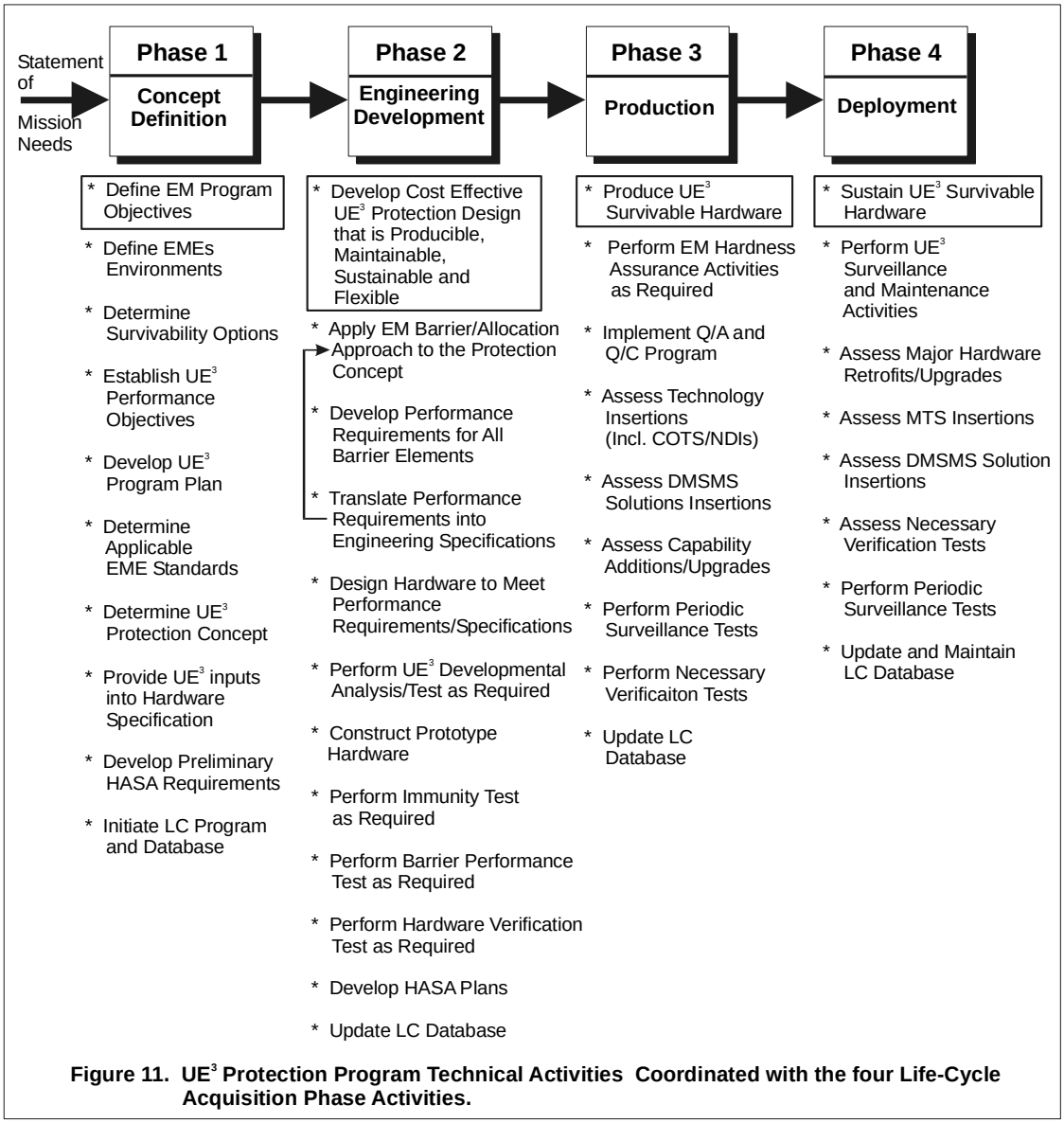


Figure 11. UE^3 Protection Program Technical Activities Coordinated with the four Life-Cycle Acquisition Phase Activities.

4.2.2 Phase 1: Concept Definition

4.2.2.1 General

The basic objective of this phase is to develop a hardware UE^3 protection concept based upon the EM barrier that will meet the mission requirements and EM program objectives. The seven basic steps of the concept definition phase are provided in Table 3. Illustrated in Figure 12 is the interrelationship between the five defining elements of the Concept Definition Phase that are used in developing the performance objectives.

Note that the EM performance objectives are used in developing the hardware specifications and the UE^3 protection concept.

Table 3. Outline of Unified E^3 Protection Methodology

1. Establish Mission Requirements
2. Establish E^3 Protection Criteria

    a. Specify all relevant EMEs in terms of levels and time histories
    b. Specify hardware's operational performance requirements for each EME
    c. Identify applicable EM standards (performance requirements oriented)

3. Delope UE^3 Protection Concept

    a. Determine existing immunities
    b. Define EM barrier configuration
        i. EM shield(s)
        ii. Mechanical penetrations
        iii. Electrical penetrations
        iv. Circuit design protection
    c. Evaluate special protective measures
        i. MSCE outside EM barrier
        ii. Supplementary isolation, special protective volumes
        iii. Enclosed MSCEs requiring additional protection
        iv. SGEMP protection
        v. SREMP protection
        vi. Use of absorbent materials
    d. Set mission and immunity requirements for sub-elements

4. Evaluate E^3 Survivability Options

    a. UE^3 barrier protection
    b. Mitigation techniques
    c. Timely re-supply
    d. Operational protection
    e. Functional protection

5. Establish EM Performance Objectives

    a. Protect against specific EMEs
    b. Level of protection required
    c. Amount of allowable risk associated with the protection
    d. Limits on hardware impacts related to E^3 protection
    e. Initiate baseline configuration

6. Initiate Life-cycle Program and Plan for Design Assurance, Hardness Assurance (HA), Sustainment Assurance (SA), and Surveillance Test

a. Design assurance for Concept Definition and Engineering Development
b. Hardness assurance for production
c. Sustainment assurance for deployment
d. Surveillance test for HA and SA

7. Initiate Life-cycle Database

4.2.2.2 Requirements

a. The mission requirements identify the overall mission critical performance functions that the hardware must be developed to meet. Included are the overall E^3 survivability requirements.

b. E^3 protection criteria includes current as well as future EME threats quantified in terms of levels and time histories, and the development of hardware operational requirements for each EME. These EMEs and operational requirements support decisions on E^3 survivability options and EM protection concepts. Applicable EME and E^3 standards including commercial standards that can be used to support the program should be identified. The standards should address MSCE equipment-level immunities, EM shielding effectiveness, EME specifications, and E^3 testing. Emphasis should be on performance requirements rather than design processes.

c. E^3 protection concept is based on an EM barrier concept in combination with special protection measures. The latter is particularly important for achieving E^3 hardening against hostile EMEs and systems with MSCEs outside the EM barrier(s).

d. The alternate methods illustrated in Figure 4 are evaluated for combining with the EM barrier to achieve E^3 survivability.

e. The hardware's EM performance objectives illustrated in Figure 12 should be developed in sufficient detail to support the barrier protection concept definition and subsequent engineering development technical activities. The hardware's EM performance objectives consists of the need to protect against specific EMEs, level of protection (immunity against upset, permanent damage, or both is required), amount of allowable risk associated with the protection, and limits on hardware impacts related to EME protection

g. The above requirements as well as references and margin guidelines are documented in the system specification document that becomes the guidelines for designing, testing, producing, and sustaining E^3 survivable hardware based upon the EM barrier protection concept combined with special protection methods.

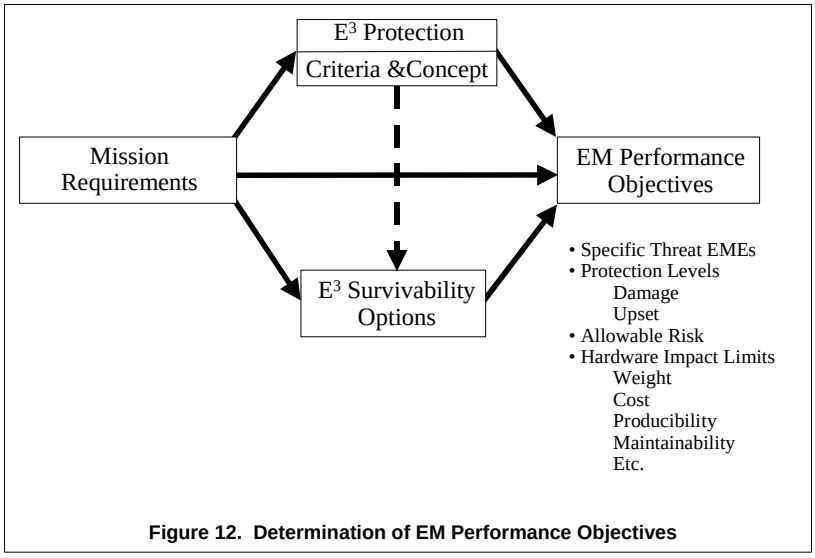


Figure 12. Determination of EM Performance Objectives

4.2.2.3 Unified E^3 Protection Concept

4.2.2.3.1 General. Based upon the above requirements, an UE^3 protection concept is defined using EM barrier(s) to provide MSCE protection against multiple EMEs. As illustrated in Figure 2, the EM barrier consists of two essential elements, an EM shield and electrical and mechanical penetrations through the shield. Variations in the physical geometry of the basic EM barrier may be necessary to accommodate physical constrains and/or to add special protective measures. Some of the possible topology geometries are shown in Figure 3. Alternate methods to be considered in combination with the EM barrier to achieve E^3 survivability and potential cost reductions are shown in Figure 4. Special protective measures to include those for SREMP and SGEMP are discussed in para.4.1.2. These alternate methods and special protective measures that complement or enable the EM barrier protection concept to provide balanced coverage against the threat EMEs are evaluated and included as appropriate into the UE^3 protection design. As a result of these evaluations and hardening selections, the EM performance objectives can be established to match the operational degradation risk or other constraints. Thus, the combination of physical configuration (EM barrier) and performance flexibility provides the User with a capability for balanced coverage for the EMEs optimized to confirm to specific system requirements.

4.2.2.3.2 EM Barrier Protection Concept. A very significant advantage of designing the EM barrier protection concept early into a hardware's acquisition cycle is the establishment of good protection allocations and margins to cover risks, uncertainties, and changes in EME specifications; and to allow later addition and integration of sophisticated electronics (likely COTS/NDIs), many having lower immunity levels. The EM barrier combined with reasonable margin provides design flexibility that will allow these integrations and additions (in most cases) to occur during deployment without major re-designs or hardening costs. This is significant because many future

electrical, electronic/ photonic changes and additions will occur to deployed hardware, especially since these hardware will be deployed longer (average was 20 years, now more than 50 in some cases), upgraded and modernized (policy) several times (3 to 10), and maintained and repaired many more times.

4.2.2.4 Life-Cycle Program

a. A life-cycle (LC) program and plan for the hardware is initiated during the Concept Design Phase. The program addresses preliminary design, hardness and sustainment assurance requirements. Fairly detail program objectives are established for the EM performance objectives, hardware specifications, and especially the E^3 barrier protection design. Management of the design as it develops is critical and is the primary objective of the life-cycle program during the Concept Definition Phase. Program objectives and procedures are established for both HA and SA. By the end of this phase, these objectives and procedures should be basically completed and documented. Program objectives and procedures are also established for the surveillance test (ST) segment. These objectives are documented in a HA, SA and ST program plan that will be finalized during the Engineering Development Phase as the design matures. This plan becomes the plan of execution for the life-cycle program. It will be updated and modified as required by the program development and changes.

b. A critical element of the life-cycle program is the database. This database is initiated during the Concept Definition Phase and updated throughout the hardware life-cycle. The database records the E^3 protection design as it matures, mission requirements, EM performance objectives, and technical configuration information, and hardware specifications. Pertinent data on the selected alternate methods, EM barrier concept definitions, threat EMEs, performance standards, critical design features, operational requirements, inherent and deliberate hardness, protection penetration devices and their characteristics, margins, immunity levels, standards employed, and legacy data are entered for Phase 2 and later use in the remaining two phases. Lessons learned are particularly important and should be included. Also pertinent information for special measures/techniques are included.

4.2.3 Phase 2: Engineering Development

4.2.3.1 General

a. The basic objective is to complete hardware development and the UE^3 protection design initiated during the Concept Design Phase. The second objective is to perform testing necessary to collect needed engineering data for the UE^3 design, demonstrate that all barrier elements meet performance allocations, assess shielding effectiveness, and demonstrate that the production-configuration system/platform being developed is compliant with all requirements.

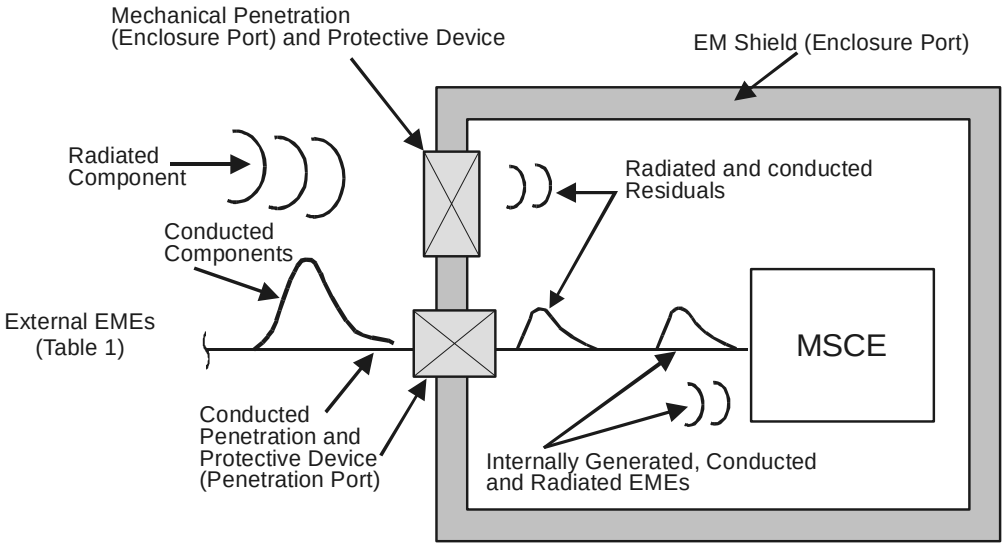


Figure 13. Externally and Internally Generated EMEs and their Interaction with the EM Barrier.

b. To accomplish the basic objective, detailed performance allocations are derived for each of the barrier elements to meet the performance requirements. The objective is to translate the hardware's EM barrier protection concept as illustrated in Figure 13 into a cost effective producible/maintainable/sustainable design, and one that can be verified and periodically checked by tests and analysis to demonstrate continued compliance with all requirements. (Details are in Volume VI.) Most of the technical activities for achieving UE^3 survivability occur during this phase.

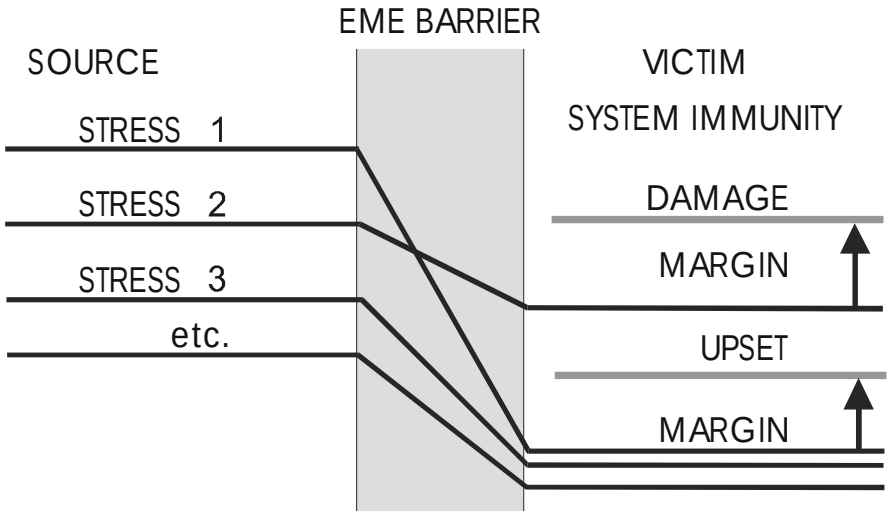


Figure 14. E^3 Allocations are Set to Attenuate Incident EM Stresses to a Level Consistent with MSCE Immunity Levels and Margins

4.2.3.2 E^3 Allocation Process Overview

a. The primary purpose of E^3 allocation is to assign performance requirements to all elements of the UE^3 protection. Included are performance requirements for MSCE equipment immunity, shielding effectiveness, penetration and special protective devices, and margin. The approach of deriving performance requirements that assures all external EME induced stresses are attenuated/reduced below the corresponding MSCE immunities by an amount (margin) chosen by the designer to cover risk is illustrated in Figure 14. The allocation process is a risk management tool that can function as an interactive engineering trade study with the objective of deriving performance requirements that are: balanced to cover all the EMEs, balanced between effectiveness and system performance/cost impact. Adjustments are made for risk acceptance. The output from the allocation process is used to develop design specifications for the protection design and to provide pass/fail criteria for the E^3 testing.

b. General guidelines for using the allocation process to derive the performance requirements inside an EM barrier are illustrated in Figure 15. Note that the lower bound of the immunities must be determined, as well as the upper bound of the internal residuals (from external EME stress) and internally generated EME stresses. The lower bound of the MSCE unit immunities are determined using standard test practices whereas the internal residuals are determined from the allocation process. The upper bound from internally generated EME stresses only become part of the allocation process if they are greater than the internal residuals. Otherwise, internally generated EME stresses are documented for later life-cycle evaluations.

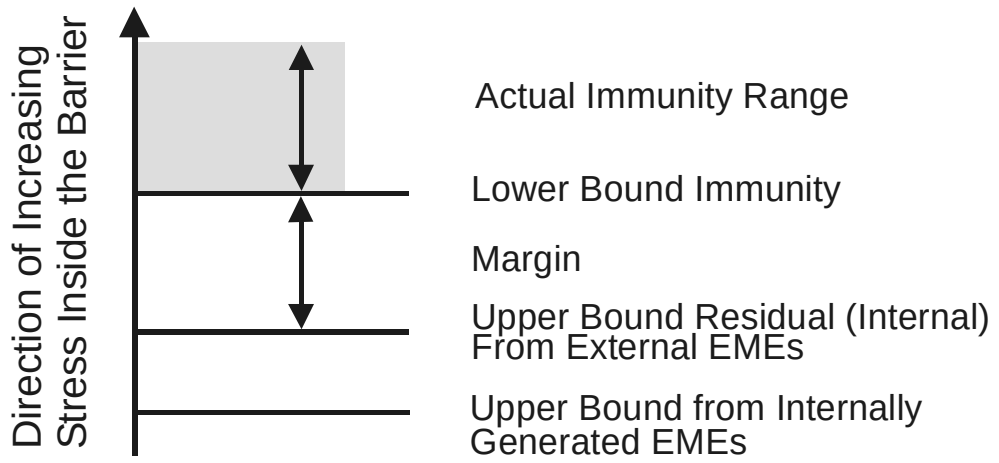


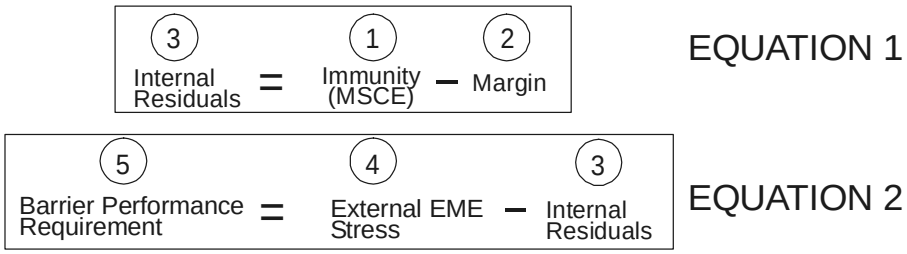
Figure 15. Guidelines for Allocating Stresses Inside the EME Barrier.

4.2.3.3 Unified E^3 Protection Allocation

4.2.3.3.1 Performance Requirements. Performance requirements for the shield are generally prescribed in terms of continuous wave attenuation for all frequencies important to the incident EMEs. An exception is a shield with aperatures where the location of the MSCEs relative to the aperature must be considered (See Vol. III). Performance requirements for the conducted penetrations are generally prescribed in terms of allowed residual transients on the transmission side of the protective devices when the protective devices are excited by conducted transients on the incident side. Therefore, performance requirements are derived for the shield and all conducted penetrations through the shield, and can be used to define formal performance specifications for each barrier component/element.

4.2.3.3.2 Allocation Process. The allocation process can be described by the two allocation equations extracted from Figure 2 and shown below. The two

equations consist of five logarithmic terms; which are discussed below. Application of these equations to each enclosure and penetration port will result in a unified performance requirement for each port.



ALLOCATION EQUATIONS (db)

a. MSCEs Immunity (1). MSCE immunity is the ability of the unit to perform without degradation in the presence of the EM disturbance [ANSI C63.14]. As illustrated in equation 1, MSCE immunity (1) is the difference between the internal residuals (3) and margin (2). MSCE lower immunity bound is the level of EM induced stresses that the MSCEs can tolerate while operating satisfactorily according to the hardware's operational requirements. Only the lower immunity bounds are required and can be obtained from standard test practices. MSCE immunity against both conducted and radiated EM residual stresses are required for the penetration and enclosure ports, respectively. The conducted residual stresses are EME induced transients on conductors attached to the MSCE unit, and will usually be different for the different class of penetration ports, e.g., power, data communications and antennas. The radiation residuals stresses are the residual radiated EME inside the barrier. Existing EM standards such as IEC-61000-4, CE Norms (EMC) for equipment, and the USA's MIL-STD 461E can be used to determine immunity bounds for equipment. The existing immunity standards may need to be augmented depending on the hardware's specific requirements.

b. Margin (2). As illustrated in equation 1, the difference between the MSCE's immunity (1) and the internal residual stresses (3) is the margin (2). Total margin allocation should be affordable; yet, it must be large enough to cover: immunity variations, test uncertainties, future use of MSCEs with lower immunities, deployment degradations, and risk. Margin is traditionally between 15 – 40 dB**,** depending on mission criticality of the hardware and the number of systems in the operational force. However, with longer deployment life spans (more maintenance and repairs), greater usage and dependency on COTS/NDIs, and many modernization cycles, the lower limits of the margin should be larger, perhaps 20 to 25 dB. In either case, the margin value is only adequate if a thorough HA/SA program is implemented.

c. Internal Residuals (3). As illustrated in equation 1, the internal residuals (3) are the differences between the MSCE's immunity level (1) and the margin (2). Both conducted and radiated internal residuals are important. The conducted internal residuals are the residuals allowed inside the barrier through penetration port protective

devices. They will be different for the different types of conductive penetration ports such as antenna, power and signal. The radiated internal residuals are the residuals from externally generated EMEs that penetrate the EM shield. In some cases (example ESD or local emitter like a microprocessor clock harmonics or power supplies), the internally generated EMEs may dominate the residuals resulting from external EME stresses. In these cases, the internally generated EMEs will replace the internal residuals and become part of the allocation process.

d. External EME Stress (4). As illustrated in Figure 13 and equation 2, the external EMEs stresses (4) incident to each enclosure and penetration port are reduced to the internal conducted and radiated residuals (3) by the EM barrier (5). In equation 2, external EME stress is the difference between performance requirements and internal residuals. The EMEs should be defined for all enclosures and penetration ports and can be derived from existing commercial or program specific standards.

e. Barrier Performance Requirements (5). As illustrated in Figure 2 and equation 2, the barrier performance requirements (5) are the differences between the external EME stresses (4) and the allowed internal residuals (3). Barrier performance requirements are required for each enclosure and penetration port, and for each EME and corresponding immunity (EME/immunity combination). The result for each EME/immunity combination can then be unified to provide unified coverage for all EMEs. Thus, the barrier performance requirements for multiple EMEs can be established.

4.2.3.4 Design for a Linear Application

4.2.3.4.1 Unified Barrier Performance Requirements (Single EME and Immunity)

a. General Approach.

A detailed design is developed from the general design (Phase 1) and must meet the barrier performance requirements/specifications. These barrier performance requirements are expressed in terms of attenuation as a function of frequency. Figure 16 illustrates the general approach to deriving barrier performance requirements that can then be unified to define a single performance requirement for each port that covers all applicable immunities and EMEs. The three basic steps in deriving the performance requirements are discussed below.

(1) EME/Immunity. Each EME/immunity combination is expressed as a magnitude that is frequency dependent (see Figure 16). Wideband transient immunities must first undergo a Fourier Transform. The magnitudes of narrowband immunities and EMEs can be used directly.

(2) Margin. The margin is expressed as a magnitude that is frequency dependent and is usually a constant function of frequency. Margin can be varied as a function of frequency or selected for each EME/immunity combination by the designer. For example, one margin can be chosen for NSL and a different one for EMP.

(3) Residual and Performance Requirements. For each immunity, the internal residual is calculated by either subtracting the margin from the immunity when each is expressed by db attenuation or by dividing the immunity by the margin when each is expressed as a magnitude at each frequency. This is performed for each frequency and results in an allowed internal residual for each MSCE immunity as a function of frequency. After the magnitude of each residual and EME has been expressed as a function of frequency, the performance requirement as a function of frequency for each EME/immunity combination can be determined for each enclosure and penetration port as illustrated in Figure 16. The performance requirement for each combination is the ratio of the EME to the allowed residual. Since the ratio is calculated as a function of frequency, it provides an attenuation requirement as a function of frequency for each EME/immunity combination for each port. When the quantities are expressed in logarithmic terms (e.g. dB as function of frequency), the ratio becomes a difference. (For data that are in the time domain, a Fourier transformation to the frequency domain must be performed prior to analysis.)

b. Enclosure Port Performance Requirements.

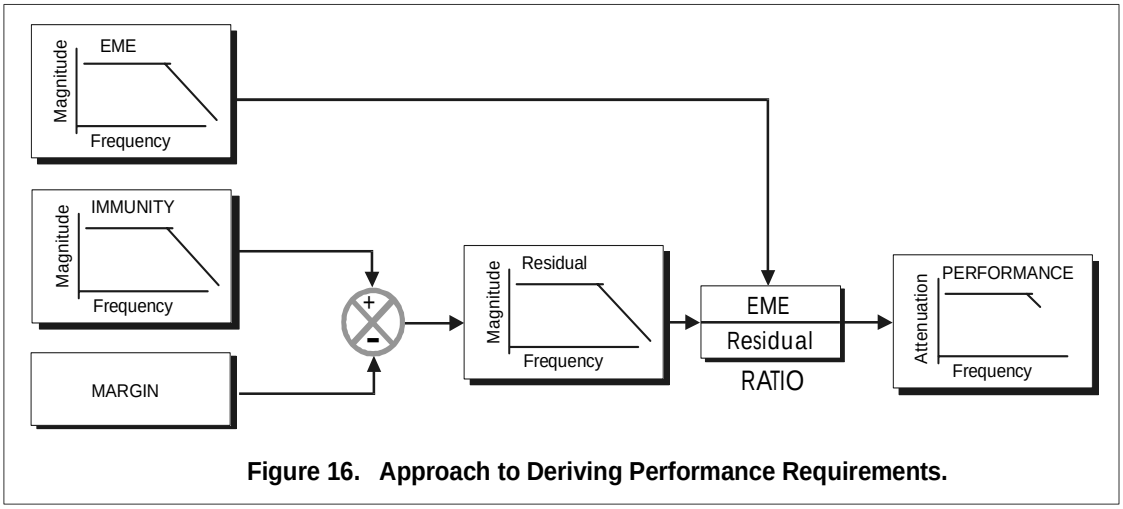


Figure 16. Approach to Deriving Performance Requirements.

Enclosure port performance requirements are obtained for the radiated component of the external EMEs using a direct application of the procedure illustrated in Figure 16 adapted to the radiated EME/immunity combinations and defined by allocation equation 2. Thus, performance requirements are determined for each radiated EME/immunity combination (both transient and narrowband), and provide the enclosure port attenuation as a function of frequency for each radiated EME/immunity combination. The EME/immunity combinations are then unified for each EME using the procedure described in Para. 4.2.3.4.2. The resulting EME specific protection requirements are then unified using the procedure described in Para. 4.2.3.4.3.

c. Penetration Port Performance Requirements.

(1) Penetration Port. Penetration port performance requirements are derived for the conducted component of the externally generated EMEs using the procedure shown in Figure 16 adapted to the conducted EME/immunity combinations. Figure 17a illustrates the use of Thevenin or Norton equivalent sources to represent the conducted penetrations. Each equivalent circuit is related to a single penetration port driven by a single conducted EME. The source term is a function of the coupling of each EME to the corresponding penetration. The impedance is a function of the physical configuration of the penetration. Procedures for deriving the equivalent sources from the externally generated EMEs and penetration port physical configurations are described in QSTAG 1051.

(2) Immunity Equivalent Source An equivalent source term for each immunity drives a calibration load (Figure 17b) and can obtained from military, commercial or tailored immunity standards. The value of the calibration load is a function of the penetration port category. For AC and DC power penetration ports, the calibration load should be 2 ohms. For signal/control and antenna penetration ports, the calibration load should be 16 and 50 ohms, respectively. The response through the calibration load is the resultant immunity. For wideband transient EMEs, this response must first undergo a Fourier transformation in order to provide a magnitude as a function of frequency. Narrowband responses can be used directly. Margin is then subtracted (assuming logarithmic quantities) from the calibration load immunity to provide the allowed residual as a function of frequency. This procedure is repeated for the equivalent source term from each military, commercial or customized immunity standard used.

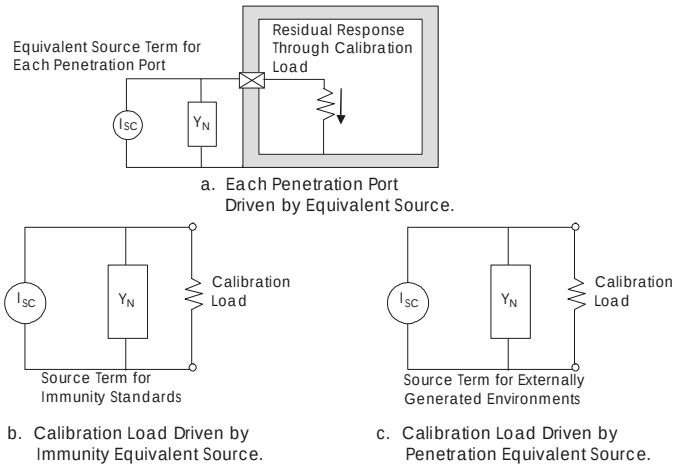


Figure 17. Use of Equivalent Sources for Deriving Penetration Port Performance Requirements

(3) Penetration Equivalent Source. The equivalent source term for each conducted EME for each penetration port is then applied to the same calibration load used to derive the residual response (Figure 17c). The response through the calibration load is the conducted EME response. A Fourier transform of the transient conducted EME (time domain) is required to provide the response as a function of frequency. The narrowband EME response can be used directly.

(4) Performance Requirements. The penetration port performance requirement for each EME/immunity combination is then derived by taking the ratio (subtracting if logarithmic quantities are used) of the calibration load EME response to the calibration load residual. This ratio, as a function of frequency, is the performance requirement as a function of frequency for each conducted EME/immunity combination. This provides penetration port attenuation as a function of frequency for each radiated EME/immunity combination. The EME/immunity combinations are then unified for each EME using the procedures of Para. 4.2.3.4.2. Resulting EME specific performance requirements are then unified using the procedures of Para. 4.2.3.4.3.

4.2.3.4.2 Barrier Performance Requirements (Single EME and Multiple Immunities)

a. Specific Performance Requirements (One MSCE). The first step in the unification process is to develop a unified performance requirement for each EME unified across all the immunities that apply for the EME. The following process is used when multiple immunities exist for a port with only one MSCE unit inside (enclosure ports) or connected (penetration ports) to it. For environment Y shown in Figure 18, N immunities are applied, resulting in N performance requirements (EME/immunity combinations as described in para. 4.2.3.4.1) as a function of frequency. The EME specific performance requirement for Environment Y (unified across all N immunities) is

the minimum magnitude (function of frequency) from all the individual immunity performance requirements. As shown in Figure 19, this process is repeated for all the separate EMEs (1 through X) for the MSCE unit being processed. The result is X performance requirements (one for each EME), each of which is unified to cover all the immunities that provide coverage for the corresponding individual EME.

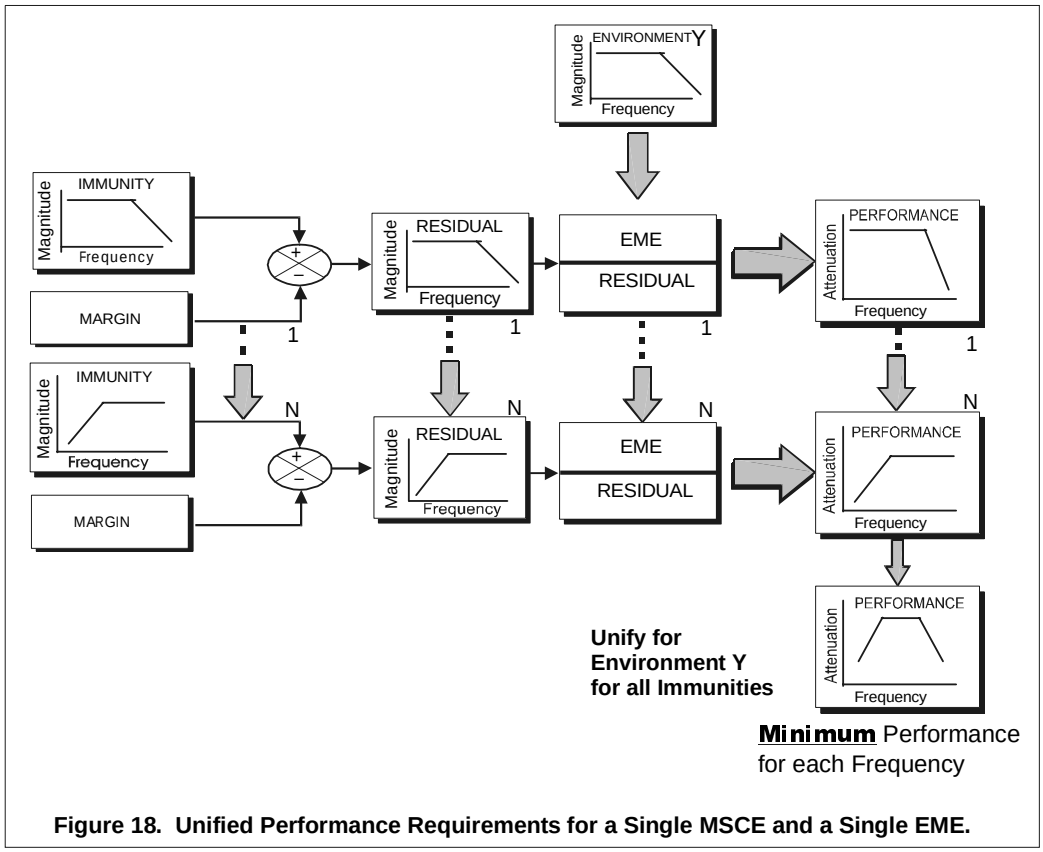


Figure 18. Unified Performance Requirements for a Single MSCE and a Single EME.

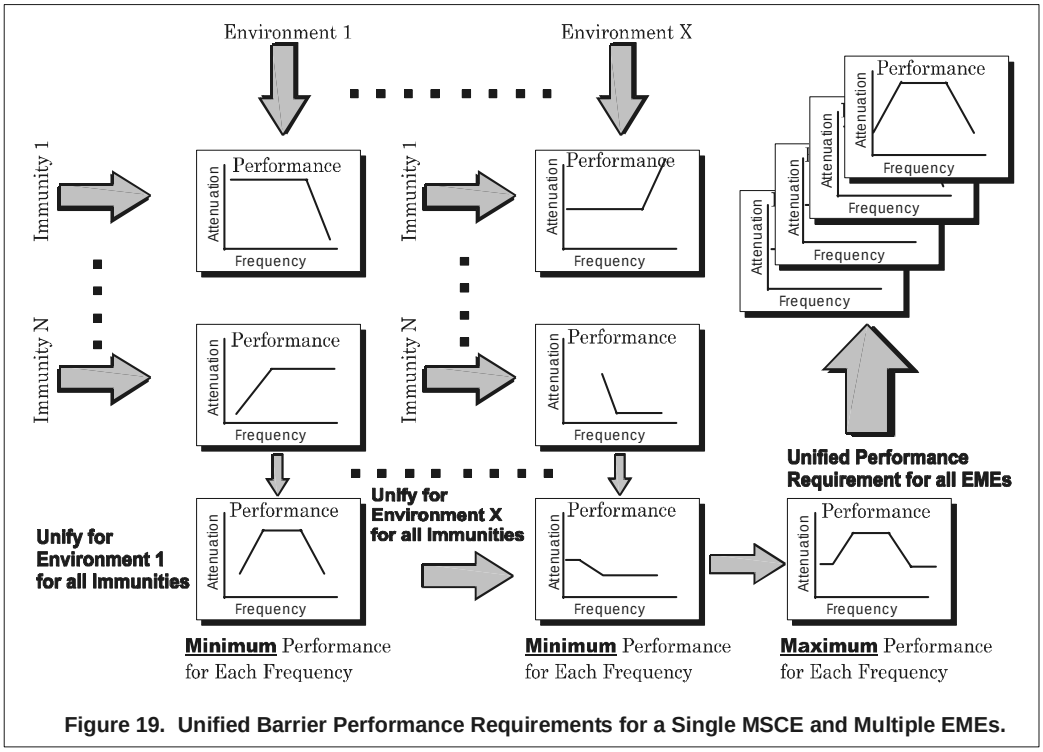


Figure 19. Unified Barrier Performance Requirements for a Single MSCE and Multiple EMEs.

b. Specific Performance Requirements (Multiple MSCEs). An additional step is required when there is more than one MSCE inside or connected to a port. If all of the MSCEs are developed with the exact same immunities, this step is not necessary. When there are W MSCE units inside an enclosure port or connected to a penetration port (or combination of both), the procedure shown in Figure 18 must be performed for each MSCE unit. This yields W MSCE/EME specific performance requirements that are then unified to a single EME specific performance requirement by selecting the maximum magnitude as a function of frequency from all the sets of W MSCE/EME specific performance requirements. This step is required to ensure that the MSCE unit with the lowest immunity level is fully protected.

4.2.3.4.3 Unified Barrier Performance Requirements (Multiple EMEs and Immunities)

a. General. Unification is the process of deriving a single performance requirement covering the EME/immunity combinations for each enclosure and penetration port. Therefore, a barrier that meets this single performance requirement can be used to provide coverage for all the battlespace EMEs.

b. Unified Performance Requirements for Ports. The procedure for developing unified performance requirements is shown in Figure 19. The unified performance requirements for each port are developed from the EME specific performance requirements that are developed from the individual EME/immunity combinations as previously described.

c. Unified Performance Requirements for EMEs. EME specific performance requirements unify over all the EMEs. Taking the maximum value at each frequency from the EME specific performance requirements derives the unified performance requirement covering all the EMEs. Installed enclosure and penetration port protective devices that meet these requirements will provide coverage for all battlespace EMEs considered. It is not necessary to provide individual protective devices.

4.2.3.4.4 Allocations for Internally Generated EMEs

Usually, the internally generated EMEs (both radiated and conducted) produce stresses that are less than the internal residuals produced by the externally generated EMEs. However, if the internally generated EME stresses are greater than the internal residuals (example is ESD radiated fields), they too can effectively be dealt with by the same allocation equations and barrier protection concept. Also, protection against these internally generated stresses may be achieved by alternate methods such as increasing separation distance between victim and source, controlling cavity Q and effective apertures, and providing higher immunity levels for special cases (SREMP and SGEMP).

4.2.3.5 Design for Non-Linear Application

The previous discussion applies to frequency domain cases involving linear barrier elements such as shields and filters. Non-linear elements such as TPDs cannot be specified by the EM barrier protection method; therefore, analysis must be performed in the time domain. Time behavior should be considered while matching transient immunities and transient EMEs so that important details of time behavior (upset or damage) are not lost. Also, transient behavior of resonant barriers must be treated by another approach. These cases are presented in Section 4.8 of Vol. III in greater detail.

Another approach to unification is through the use of waveform norms (IEC 61000-4-33). Table 4 shows five commonly used waveform norms for testing [Lubell]. Additional waveform norms can also be defined and may be required for certain analytical applications. These waveform norms provide a quantitative description of the important characteristics of a time domain waveform. These norms can be used to compare different transient stresses. Norm attributes of a waveform can be expressed as $N = \| f(t) \|$. Note that norms must be non-negative real numbers, and proportional to the waveform-scaling factors and obey the right-triangle rule. Selection of norms is based upon circuit being tested. Section 4.8 of Vol. III provides additional information.

Table 4. Typical Waveform Norms

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

These five waveform norms provide a description of the size of the waveform *f*(*t*).It should be noted that some physical phenomena, such as dielectric breakdown or semiconductor damage, are related to more than one norm. Both dielectric breakdown and semiconductor damage normally depend on a combination of signal amplitude and duration for example.

Waveform norms are useful for defining the properties of a substitute waveform that can then be used as a substitute for a specific threat waveform assuming it meets certain criteria. If hardware under test is not upset or damaged by the substitute waveform, then it is assumed that the hardware will also be immune to the original threat waveform. The substitute waveform is usually expressed in terms of waveform norms, N_1 to N_5, that meet or exceed the corresponding norms of the threat waveform. Note that in some applications, a subset of the five basic norms may be applied. For example, N_1, N_2 and N_5 together with the specification that the absolute value of the amplitude of the frequency spectrum of the substitute waveform exceed that of the threat waveform at all frequencies. It should be noted that selection of substitution waveforms would optimize the probability of damage but not upset. To maximize the probability of upset, additional norms are likely.

Norms can be used in the unification process by a combination waveform, which is similar to a substitute waveform except that it is used to replace multiple radiated or conducted threats. The combination process can be applied at various stages during the unification process specifically for the combination of threat waveforms, of residuals and of immunities. Section 4.9.3 of Volume II provides greater detail.

Another approach to unification proposed by Dion et al [ ] is to combine all of the stress and interactions along a given path. In this approach, a distinction is made between narrowband and wideband EM quantities (signals or interactions). Wideband quantities are described by a function corresponding to the magnitude of their spectrum whereas narrowband quantities are described by the peak magnitude and bandwidth at the center (resonance) frequency. Wideband and narrowband signals are combined separately to form two distinct composite signals, which may be further propagated or compared against the pre-defined failure thresholds. This approach combines all of the stresses and interactions along a given path. Section 4.8 of Vol. III provides additional details

4.2.3.5 Testing

4.2.3.5.1 Tests. A series of tests are performed whose purpose is to demonstrate that the EM barrier protection objectives have been met and the developed hardware is E^3 survivable, and that the hardware is electromagnetically compatible within itself and with its defined external EMEs such that its operational performance: requirements are met. The final determination of acceptable hardware performance should be based on test data with minimum reliance on first-principle analysis. During this phase, there are three basic types of tests performed engineering development, acceptance, and verification (See Table 3).

Engineering development testing begins during the concept/design phase and is continued into the engineering development phase. These tests are usually designed

and performed by the developing contractor for the purpose of acquiring needed information to evaluate the feasibility of design concepts, adequacy of barriers, radiated and conducted emission problems, hardening technologies/devices, or to assist in the allocation process.

Acceptance testing is performed to demonstrate that the mature design satisfies specified technical performance requirements that are generated through the allocation process. There are three basic types of acceptance tests: equipment level (immunity and emission), barrier performance (shielding effectiveness and current injection on conductive penetration devices), and performance tests on special protective devices. All of these tests are performed during the engineering development phase to verify the adequate of the design. In general there are existing standards that can be used for these tests.

Verification testing is performed to demonstrate that the proposed production hardware will perform its specified operational performance functions in the presence of the threat EMEs. These tests are usually performed after completion of the acceptance tests. During these tests, the system/platform must be demonstrated as being electromagnetically compatible within itself and with its defined external EMEs such that its operational performance requirements are met. Much of the hardware verification testing should include whole or full body illumination to threat-like external EMEs such as HIRF for inter-system EMC and RADHAZ, HEMP and NSL. See Table 3. If low-level illuminations are performed, they should be combined with pulse current injections. Verification test should be performed on production-like prototype hardware. If there are configuration differences between the tested system/hardware and production, the differences must be defined and evaluated. The test results must be adjusted for the validation assessment.

4.2.3.5.2 Unification of Tests. Emphasis should be placed on combining or unifying testing at every stage to reduce costs and hardware requirements. Since the barrier concept provides coverage for multiple environments, the number of protection devices and number of immunity tests are already reduced. Selecting the test frequencies to cover the unified performance requirements can consolidate conducted and radiated CW tests. Some consolidation for conducted and radiated transient test waveforms can be achieved using waveform substitution and/or combination algorithms, which, in turn, can reduce the number of separate tests. Also, co-location of all E^3 test facilities and expertise can greatly reduce test costs and time, training costs, number of test personnel, and logistic requirements. Sufficient numbers of samples must be provided to achieve test objectives, and to obtain an acceptable level of confidence. A minimum of three test samples is recommended. Test levels should include a final confidence test at 6 db or even higher. Response measurements are essential for later evaluations.

4.2.3.6 Life-Cycle (LC)

a. The preliminary HA/SA program definition initiated during Phase 1 is completed during this phase. Subsequent updates and additions will occur during Phase 3 and

especially Phase 4 to address insertions and additions, circuit and material changes and additions, enhancement and modernization programs, and new knowledge. A design assurance program is implemented to documented and manage the design configuration and DMSMS.

b. All pertinent data of the final version of the detailed design, baseline configuration, test data and results, analysis, margins, EME threats, and protection and survivability assessment are entered into the life-cycle database. Other significant information entered includes: operational requirements, performance requirements for each barrier element, MSCE immunities, shield effectiveness, EM protection designs and devices, and assessments. These data will be used for later engineering evaluations/decisions, and in managing and preserving the UE^3 survivability of the hardware during production and deployment

4.2.4 Phase 3 Production

4.2.4.1 General New factors affecting the E^3 survivability of hardware in production are occurring at an ever-increasing rate in today's world. Production units are designed with increasing amounts of non-conductive material and increasing number of COTS/NDIs, primarily at the piece-part and component level. During production, integration of COTS/NDIs into the design must be expected and planned for due to: production trends of producing fewer units annually but over a longer period of time, thus, exposing the hardware to more opportunities for MSCE replacements and additions; the military's decreasing market share with the result of having fewer military grade electronic devices available, thus, more insertions of COTS/NDIs; and, the electronics industry being driven by the rapid technological advances, thus, increasing the number of COTS/NDIs inserted into production units as a result of DMSMS, availability, capability, and costs. In general, the EM barrier protection design will facilitate these COTS/NDIs and more E^3 sensitive devices with realistic margins by creating a relatively benign internal EME (inside EM barrier). Notable exceptions are: replacing a metal packaged device with a plastic or ceramic one, and re-designs using lower operating voltage devices which tend to be more energy sensitive. In these cases, and those involving material replacements (conductive with non-conductive), additional shields and/or protective devices may be required. Evaluations (immunity and allocation), as a minimum, should be performed on all replacements and additions.

4.2.4.2 Quality Assurance and Control It is critical that a thorough Quality Assurance (Q/A) and Control (Q/C) program be in place to insure that each production unit has the UE^3 protection design intact so that the hardware's technical performance requirements and operational performance requirements are met. Perhaps the greatest cause of degraded survivability in fielded hardware is the result of poor Q/A and Q/C at the factory. As a minimum, the following verifications should be performed: the correct penetration port and special protection devices are in-place and are within specifications, integrity of the enclosure is intact, bonds and ground are within specifications, and the approved materials and devices are being used. These Q/A and Q/C programs are the basis of a pro-active Hardness Assurance (HA) program. All changes to the baseline configuration must be identified and then evaluated and tested (when needed), and approved before implementation.

4.2.4.3 Testing Early in production, if uncertainties exist in regards to UE^3 survivability compliance, selective port injection immunity tests, enclosure integrity tests, or even platform or system level verification test (if concerns are at the platform or system level) may be required. If required, production verification test may involve: full body illuminations for HEMP, NSL and HIRF below 500 MHz, spot illuminations at high HIRF frequencies (>500 MHz) on hardware in different configurations/orientations as determined from analysis or prototype test data (database); combined low-level illuminations and injections; and/or pulse current injections on selected conducted penetrations based on engineering analysis and/or data from Phase 2 testing. The test hardware cost, degree of uncertainty, margin level, and complexity, determines test magnitude and sample size. The current injection results from Phase 2 and 3 (early) can be used later as the basis for qualifying hardware changes/additions without performing platform or system level testing, or, at least, reducing the amount of platform or system level testing. Often times, mode stir chamber testing or low level CW system illuminations combined with limited current injection tests can be performed to evaluate the impact of the changes and overall hardware E^3 integrity. These techniques have been applied successfully in some cases to aircraft systems as well as tanks and permanent sites. Care must be exercised with mode-stir chambers since these tests will not determine EM entry points and aspect angels associated with specific susceptibilities, and system response below 80-100MHz.

To insure adequacy of the HA program and to check higher level-of-assembly impacts from multiple integration effects (insertions due to DMSMS, technology, enhancements, etc.), periodic surveillance tests are needed. This has become especially true for the much longer production cycles that, in turn, provide greater opportunities for the accumulation of small or below threshold effects due to many assembly changes and additions. The sum or integration of these effects can have impacts on survivability of the hardware. Normally surveillance tests are performed with a reduced set of methods and procedures (compared to the verification tests) that are based upon careful analysis of existing data and changes to the configurations.

4.2.4.4 Life-Cycle Database The life-cycle database initiated in Phase 1, updated in Phase 2, must be updated over the production period, as new pertinent information becomes available. Types of data include: system response test data, results, margins, hardware changes, assessments of the completed baseline system configuration, EME threat updates, operational requirements updates, modifications to the UE^3 barrier protection design, and EME test levels. This information is critical to the HA program and ensuring that E^3 survivable platforms and systems are being produced.

4.2.5 Phase 4: Deployment

4.2.5.1 General

The traditional concerns of degrading a hardware's E^3 survivability were: aging, usage, corrosion, poor maintenance, repeated maintenance and repairs, ambient

environments, storage, cable re-routing, bonds and grounds deterioration, non-approved configuration changes to the deployed hardware, and improperly installed retro-fits and upgrades. These were in addition to impacts on E^3 survivability due to EME threat changes and inherent susceptibilities due to poor production QA/QC and/or design. These concerns are still valid; however, now there are new and major factors impacting UE^3 survivability. The new ones are due to a much longer deployment life-span (also worsens the traditional problems), increasing rates of DMSMS, the need for multiple upgrades and modernization cycles in order to enhance the operational mission capabilities, and new EME threats. Of particular concern is the fact that most of the electronic changes and additions involving substitutions will be COTS/NDIs that are more sensitive to E^3, i.e., the electronics will have lower immunity threshold levels. Another factor is material changes. Some replacements may involve replacing conductive materials with non-conductive materials. These factors are discussed below and in Volumes VI and VII and briefly in the other volumes.

4.2.5.2 Traditional Factors

The traditional factors listed in the above paragraph are under the responsibilities of the hardware's Sustainment Assurance (SA) Program. Verification of the adequacy and effectiveness of the SA program is the responsibility of the Surveillance Test (ST) Program. Over previous decades, these two programs evolved to a level where E^3 survivability was being sustained effectively and at reasonable costs. Problems were reported in the logistic, maintenance, SA or ST; and corrective actions were identified, implemented and verified. Documentation was issued or changed, as necessary. Modifications to procedures and training of military operators and maintainers occurred, as required. Data on effects due to aging, usage, storage, ambient environments and SA maintenance and repairs were collected, stored, evaluated and used to improve the SA Programs and to predict maintenance's material requirements, actions, and needs. Periodic ST verified the adequacy of the SA program in preserving E^3 survivability and identified deficiencies for correction. The infrequent EME threat changes that occurred were evaluated relative to the E^3 survivability of the hardware, and hardening modifications were identified, verified and implemented. The SA Program was updated as necessary. Overall, the tools were known, updated as necessary, and available to preserve adequate E^3 survivability in deployed systems. Today and in the future, without modifications, these same tools can no longer be used to effectively preserve E^3 survivability because of much longer deployment periods and factors driven primarily by technology, DMSMS, growth of the commercial market, and decline of the military device availability.

4.2.5.3 Modern Factors

4.2.5.3.1 General.

New and major factors influencing E^3 survivability in the deployment phase have occurred in recent years. End of the Cold War has resulted in the development of fewer types of platforms and systems, and fewer numbers of units per platform or system being produced and deployed. The end of the Cold War has also resulted in fielded hardware being deployed much longer (50 to 400%) and with inadequate sustainment

budgets. Replacement MSCEs and material are usually COTS/NDIs and different technology with lower energy sensitivity thresholds. To keep these hardware and their mission critical functions current, planned upgrade and modernization cycles (typically five to seven years) are employed. In parallel, there are major DMSMS problems and tremendous technological advances in both electronics/photonics and materials. There will be continued integration of and increasing dependency on digital COTS/NDIs electronics. In general, these newer electronics are more energy sensitive, less reliable and rugged, and more susceptible to DMS. Also, many of the new materials are non-conductive.

4.2.5.3.2 Operational Status

To maximize operational effectiveness and readiness of hardware during these much longer deployed periods, improved and new procedures are required to address factors such as DMSMS issues, deliberate COTS/NDI and technology insertions (MTS), increasing dependency on electronics, multiple modernization cycles, and more frequently changing EME threats and platforms/systems configurations. To accomplish these objectives, additional features to the traditional SA Program are required. In regards to DMSMS, it has increased from 2 to 20 percent during the last 10 years and has become a major concern in sustaining E^3 survivability. This is discussed in Para.4.2.5.3.2 (a). To keep mission essential capabilities current, and the platform/system reliable, periodic and frequent upgrades and modernizations programs are required. This is discussed in Para. 4.2.5.3.2.b. To take advantage of state-of-the-art electronics, technology innovations, product availability, electronic variety, and lower costs, COTS/NDIs must be considered routinely. This is discussed in Para. 4.2.5.3.2.c. Finally, the MTS approach achieves its goals through investing in material replacements and additions, and especially through deliberate technology insertions of state-of-the-art electronic devices to include COTS/NDIs. This is discussed in Para. 4.2.5.3.2.d.

a. DMSMS. As hardware continues to become more and more dependent on electronics, especially digital COTS/NDI, the potential for DMS increases. The commercial market controls COTS which has a very high and increasing DMS rate due to performance, lower power consumption and reduced cost drivers. The traditional solution of simply performing multi-year or last chance buys of the same technology is no longer the automatic “best” solution. In fact, these buy solutions actually delay resolution of DMS to a later date and will likely have a negative impact on maintenance, sustainment and MTS goals. In part, to minimize future DMS, maintain an acceptable level of readiness and at an affordable cost, insure electronic device availability, and improve mission capability, newer technology must be inserted. Also, both DMS and MTS programs must address the problems caused by the total number of military grade part-types and manufacturers decreasing by more than 50% and 70%, respectively, during the past eight years. This decrease in state-of-the-art military grade devices and availability and variety of military grade electronic products, (especially acute for digital devices such as microprocessors and memories), has forced increased usage of and dependency on COTS even with its known problems.

b. Improved Capabilities. To accomplish the modernization objective of

keeping mission essential capabilities current, numerous modernization cycles are required and are planned for each platform and system, typically, every 5 to 7 years. Thus, hardware is likely to be modernized/upgraded 6 to 10 times during its deployment lifetime rather than once or twice as before. These modernization efforts will involve equipment(s) replacement and/or additions and extensive use of COTS/NDIs. Upgrades involving these equipments and material and/or cabling changes will require, as a minimum, UE^3 evaluation, and may require some additional penetration port protection and/or EMI filtering. The EM barrier concept's inherent EM protection features accommodate these upgrades. If properly planned, these cycles can effectively addresses DMSMS and availability issues while preserving E^3 survivability. More importantly, these cycles enable new and/or improved capabilities to be integrated into the hardware; thus, effectively extending the hardware's deployment life span with current capabilities.

c. COTS/NDIs. Additions and especially insertions of COTS/NDIs into hardware will occur at an increasing rate because of the need to use state-of-the-art electronics and materials. Many of the required electronic devices are no longer available as military grade products or have not been developed as military grade products. Consequently, the usage of COTS/NDIs is widespread and will continue to increase with time. Thus, the critical need for a good UE^3 protection design that reduces the EME generated stresses to benign internal residual levels and has conservative margins, is more important than ever. Such a design is inherently accommodating to insertions/additions and enables UE^3 survivability of deployed hardware to be maintained even after many upgrade/modernization cycle, and replacements and additions involving COTS/NDIs. However, each replacement and addition must be evaluated for E^3 integrity and margin adequacy. In some cases, additional penetration port protection will be required.

d. Modernization Through Spares. This is a relatively new concept being applied to U.S. military hardware and results from the fact that the life span of these deployed hardwares must be much longer while maintaining combat effectiveness and readiness. MTS must also be affordable. Thus, to accomplish these objectives without new and major funding requirements, better utilization of existing sustainment funds must occur. The mission essential capabilities of these older systems must be modernized in order to meet new battlespace demands, while achieving stabilized MTBFRs and repair costs (even improving them), and effectively addressing DMSMS. The key is the use of performance base requirements that encourages design innovations and leveraging off commercial practices and manufacturing processes that results in technology insertion of state-of-the-art products. The intended result also decreases DMSMS through the use of emerging and mature technologies rather than very mature and sunset technologies, and effectively expands the defense industrial base. MTS also minimize DMSMS by being pro-active rather than reactive. The MTS concept emphasizes the critical need for the UE^3 protection design to be one that has designed-in features such as EM protection barriers which provides the designer and integrator the closed EM topologies that will accommodate material and electronic device changes and additions.

4.2.5.3.3 Technology

To keep operational capabilities current, improve capabilities, and provide pro-active DMSMS solutions, state-of-the-art electronic devices are required. In general, these devices will be COTS/NDIs. Their usage creates a new problem, especially for digital applications. Due to market, (performance, power and cost factors), the technology path of digital devices (smaller feature size) is to lower operating voltages and higher integration densities. The lower operating-voltage device tends to be more susceptible to energy. As hardware become more dependent on electronics, COTS/NDIs, and performance-based solutions, insertion and utilization of these lower operating voltage devices becomes a necessity. Besides the difference in operating voltages, the newer digital devices are usually fabricated from CMOS technology, which, also tend to have lower energy susceptibility thresholds. Therefore, whenever these devices are inserted or utilized in an existing design, an E^3 assessment must be performed for impacts on the pertinent design margin and overall UE^3 survivability. The EM barrier protection concept facilitates and minimizes the impacts caused by the usage of these lower operating voltage and energy threshold devices.

4.2.6 Surveillance Test (ST)

4.2.6.1 Hardness Assurance. All deliberate changes to the hardware's configuration, E^3 protection enclosures and/or protection devices, MSCEs, as well as effects from maintenance, repairs, storage and operational usage must be assessed for impacts on the UE^3 survivability of the hardware. Also, changes in EME threats or operational requirements will require E^3 impact assessments. These assessments are accomplished under the HA Program. The proposed EM barrier protection design allows many of the assessments to be by analysis and/or lower level of assembly

testing. Since risk will increase as a function of change, periodic surveillance tests should be performed on completely assembled and operating production hardware. The results of the ST will be used to evaluate the adequacy of the HA Program.

4.2.6.2 Sustainment Assurance. To assess the effectiveness of the SA Program and insure adequate UE^3 survivability exists in fielded hardware, a pro-active surveillance test (ST) program is essential. Such a program requires periodic testing and assessments. These UE^3 survivability assessments require data from test programs such as system level CW, selective comparison test, cable shield effectiveness, measurements of immunity levels and port protection device integrity, bonds and grounds, and barrier effectiveness. The frequency and types of testing and the level of assembly at which test are conducted are, to a significant degree, dependent on the "goodness" of the original EM barrier protection design and the quantity of the HA/SA programs. Unification testing and evaluation is the goal, and when achieved, can reduce costs, hardware requirements, and time. The ST results will serve as an evaluation of the SA Program.

4.2.6.3 Life-Cycle Program

It is particularly important to keep the life-cycle database updated and current. The database must be maintained and updated for decades until the hardware is retired from the inventory. Over the life-time, there will be numerous changes, additions, and traditional effects. Without a current and complete database, there will be no cost effective method of insuring E^3 survivability. Therefore, the database must be current and accurate at all times to provide inputs to evaluations and determinations of what tests are required and at what assembly level.

5.0 SUMMARY

Proper design and implementation of the UE^3 protection concept in military hardware can result in life-cycle UE^3 survivability that is affordable, producible, maintainable and sustainable; and, with sufficient design margin, its inherent protection and flexibility can accommodate future EME threat changes, integration of COTS/NDIs, technology insertions, modernizations and upgrades. In order to achieve these goals at an affordable cost, the design must occur early in the design concept phase. Sufficient testing must be accomplished, especially in the engineering developmental phase to insure, with confidence, that the hardware's design is adequate with sufficient design margin. Testing and QA/QC (HA) are required during production to insure the validated UE^3 protection design is being properly produced and E^3 survivability is not being compromised by all of the changes that will occur to the initially validated configuration. A thorough and changeable SA program is required during deployment to insure that the hardware is UE^3 survivable even for an unexpected operational deployment. The SA program will require continuous EM protection adequacy assessments, which, in some cases, will require selective testing. A detailed life-cycle database must be initiated during Phase 1 and updated and maintained throughout the hardware's life-cycle. Different degrees of unification can occur in the barrier protection design against multiple EMEs and the testing against these EMEs. The overall benefits are affordable costs, and an inherently accommodating design concept that is relatively easy to

implement, verify and produce; while, at the same time, increasing in the probability of fielding E^3 survivable hardware whose E^3 survivability can be maintained and sustained during a very long deployment cycle that includes the MTS and modernization concepts.

6.0 CONCLUSIONS

AEP Volume 1 provides the philosophy and methodology for achieving UE^3 protection and life-cycle survivability of NATO military platforms, systems, and equipments in all six operational categories against hostile, natural, operational EME threats. The methodology is based on the unified EM barrier protection concept and usually requires a closed conductive EM topology to enclose all MSCEs. It is emphasized that the actual geometry of the EM barrier can take many forms. The EM barrier is defined as one or more EM shields plus protection controls at shield penetrations. The purpose of the EM barrier is to create a benign environment by reducing the externally and internally generated EMEs to residual levels lower than the corresponding radiated and conducted MSCE immunity levels by an acceptable margin. When these allocations are achieved, the MSCE units will be protected against both externally and internally generated EME stresses. The proposed methodology is easy to implement, affordable, producible, and sustainable. It also is very accommodating for performance based designs. However, it is emphasized that in order to be affordable and accomplish the overall objective of providing UE^3 life-cycle survivability, the EM barrier protection concept must be designed into the hardware in Phase1 and fully implemented and verified in Phase 2. Verification and testing will continue throughout production and deployment. The degree to which elements of the EM barrier treat multiple EME and immunity combinations is a measure of the degree of unification. Finally, the proposed EM barrier protection concept has inherent features that accommodates future technology insertions, upgrades and usage of more E^3 sensitive COTS/NDIs.

7.0 Appendix

7.1 References

1. NASA TR 32-1500
Final Report RF Voltage Breakdown in Coaxial Transmission Lines

2. ANSI C63.14
Standard Dictionary for Technologies of Electromagnetic Compatibility (EMC), Electromagnetic Pulse (EMP) and Electrostatic Discharge (ESD)

3. MIL-STD 461E
Requirements for the Control of Electromagnetic Interference Emissions and Susceptibility

4. MIL-STD 464, Department of Defense, USA, 18 Mar 1997
Electromagnetic Environmental Effects Requirements for Systems

5. QSTAG 1051, Quadripartite Standardization Agreement (QSTAG) Number 1051, Edition 1, U.S.A, U.K. Canada and Australia, 6 Oct 1998, A Unified Approach to Electromagnetic Protection

6. SAE ARP5412, Society of Automotive Engineers, Inc

7. DODI 6055.11, Department of Defense Instruction
Protection of DoD Personnel from Exposure to Radio Frequency Radiation and Military Exempt Lasers

8. MIL-STD 469, Department of Defense, USA,
Radar Engineering Design Requirements, Electromagnetic Compatibility

9. AEP-4, Allied Engineering Publication No. 4, NATO

10. NTIA, National Telecommunication and Information Agency
Manual of Regulations and Procedures for Federal Radio Frequency Management

11. AEP-41 Space and Nuclear Radiation Hardening Guidelines for Military Satellites

13. 3516 AE NATO Electromagnetic Interference and Test Methods for
Aircraft and Electronic Equipment

14. 3614 AE NATO Electromagnetic Compatibility (EMC) of Aircraft Systems

15. 3659 AE NATO Bonding and In-Flight Lightning Protection for Aircraft

16. 3856 AE NATO Protection of Aircraft, Crew and Subsystems In-Flight
Against The Effects of Electrostatic Discharge – AEP 29 and Electronic Equipment

17. 4435 NAV NATO Electromagnetic Compatibility Testing Procedures and Requirements for Naval Electrical and Electronic Equipment (Surface, Ship, Metallic Hull)

18. 3516 AE NATO Electromagnetic Interference and Test Methods for Aircraft And Electronic Equipment

19. AECTP 500 NATO Electrical/Electromagnetic Environmental Tests

20. QSTAG 1337 Quadripartite Standardization Agreement (QSTAG) Number 1337, Edition 1, U.S.A, U.K. Canada and Australia, Application of Unified E^3 for Command, Control and Communications Mobile Shelters

7.2 ACRONYMS

Abb	abbreviation
AC	alternating current
AEP	allied engineering publication
ANSI	American National Standards Institute
CNAD	Combined National Armaments Directors
COTS	commercial off the shelf
dB	decibel
DEMP	disperse EMP
DMS	diminishing manufacturing sources
DMSMS	diminishing manufacturing sources & material shortages
DSL	direct strike lightning
EED	electro-explosive device
EID	electrically initiated device
EM	electromagnetic
EMC	electromagnetic compatibility
EME	electromagnetic environment
EMI	electromagnetic interference
EMP	electromagnetic pulse
E^3	electromagnetic environmental effects
HA	hardness assurance
HEMP	high-altitude electromagnetic pulse
HIRF	high intensity radiated field
HPM	high power microwave
IEC	International Electro-technical Commission
LRU	line replaceable unit
QA	quality assurance
QC	quality control
QSTAG	quadripartite standardization agreement

MHz	megahertz
MIL-STD	military standard
MOV	metal oxide varistor
MSCE	mission and safety critical electronics
MTS	modernization-through-spares
NATO	North Atlantic Treaty Organization
NDI	none developmental item
NSL	near strike lightning
P	power
PARA.	paragraph
POE	point of entry
P-STATIC	precipitation static
RADHAZ	radiation hazard
RE	radiated emissions
RF	radio frequency
RS	radiated susceptibility
USA	United States of America
□**s**	microsecond
UWB	ultra wideband
V/M	volts per meter
VOL.	volume
SA	sustainment assurance
SGEMP	system generated EMP
SREMP	source region EMP
ST	surveillance test
STA	stress transfer function

7.3 Definitions

1. Arc Attachment. The point of contact of the lightning flash with the vehicle so that current can flow onto the vehicle from this point.

2. Charge Transfer. The integral of the current over its entire duration. $\int i^2$ dt. (coulombs).

3. Final Entry Point. The spot where the lightning flash channel last “enters” the vehicle (usually a trailing edge).

4. Initial Entry Point. The spot where lightning flash channel first “enters” the vehicle (usually an extremity).

5. Internal Environment. Includes the structural current and voltage changes with associated distribution and the aperture-coupled and diffused electromagnetic fields.

6. Lightning Flash. The total lightning events in which charge is transferred from

one charge center to another within a cloud, between clouds, or between a cloud and ground. The event can consist of one or more strokes plus intermediate or continuing currents. Typically, the duration of a flash is 2 seconds or less.

7. Lightning Strike. Any Attachment of the lightning flash to a vehicle or ground facility.

8. Lightning Stroke (Return Stroke). A lightning current surge that occurs just before the lightning leader makes contact with the ground or other region of opposite charge,

9. Multiple Burst. A randomly spaced series of bursts of short-duration, low-amplitude current pulses and arch pulse or pulses characterized by rapidly changing currents. These burst may result from lightning leader progression or branching and may be accompanied by or super imposed upon a stroke or continuing current. The multiple bursts appear to be most intense at time of initial leader attachment to a vehicle.

10. Multiple Stroke. Two or more lightning return strokes occurring during a single lightning flash.

11. Swept “Flash” (Or “Strike”) Points. Spots where the flash channel reattaches between the initial and final points, usually associated with the entry part of the flash channel.

12 Action Integral. A critical factor in the production of lightning damage related to the energy deposited or absorbed in a system. The actual energy deposited without knowledge of the resistance of the system.

13. Direct Effects. Any physical damage to an element’s structure due to the direct attachment of the lightning channel or the flow of current through the vehicle’s structures, either when vehicle is on the ground or in flight. This includes thermal and shock wave effects on the exterior skins, coatings, or other exposed components such as windshields, nozzles, umbilical, fuel and oxidizer lines, edges, control surfaces, and engines. Damage to electrical or avionics systems or individual equipment due to direct attachment of the lightning flash to an exposed part of such a system is also termed a direct effect.

14. Indirect Effects. Voltage and/or current transients produced in vehicle electrical wiring due to lightning currents in the elements that can upset an/or damage components within electrical /electronic systems. These transients occur due to one or more coupling mechanisms, i.e., changing magnetic or electric fields and structural voltage rises due to lightning currents in structural resistance. Thus, voltage induced in a sensor wire harness by changing magnetic fields accompanying lightning currents in unbiblical cable shields are also called indirect effects.

15. Multipaction. An RF effect that occurs strictly in a high vacuum where RF field

accelerates free electrons resulting in collisions with surfaces creating secondary electrons that are accelerated resulting in more electrons and ultimately a major discharge and possible equipment damage.

16. Compromising Emanations. Unintentional intelligence- bearing signals which, if interrupted and analyzed, disclose the national security information transmitted, received, handled, or otherwise processed by any classified information processing system.

17. EMC. Electromagnetic Compatibility. The capability of electrical and electronic systems, equipment and devices to operate in their intended electromagnetic environment within a defined margin of safety, and at design levels of performance. This must be achieved without suffering or causing unacceptable degradation as a result of electromagnetic interference.

18. EMH. Electromagnetic Hazards. This term describes the electromagnetic environment generated by all electromagnetic sources, both frequency and time domain.

19. E^3. Electromagnetic Environmental Effects. The impact of the electromagnetic environment upon the operational capability of platform electronic or electrical systems, equipment or devices. It encompasses all electromagnetic disciplines, including electromagnetic compatibility, electromagnetic interference, electromagnetic vulnerability, electromagnetic pulse, electronic countermeasures, hazards of electromagnetic radiation to ordnance and volatile materials, RF weapons and natural phenomena effects of lightning and p-static.

20. EME. Electromagnetic environment. The totality of electromagnetic phenomena existing at a given location.

21. EMI. Any electromagnetic disturbance, whether intentional or not which interrupts, obstructs or otherwise degrades or limits the effective performance of electronic or electrical equipment. This is normally used to describe the threat posed by the platform's own systems, mutually interfering with one another.

22. HIRF. High Intensity Radiated Fields. This term covers the inadvertent threat posed by ground based and airborne transmitters such as radar, radio and TV transmitters. This threat is the one threat that is known to have caused the loss and flight control disruption of military aircraft, primarily from ground based HF transmitters.

23. RFW. RF Weapons. This term covers the deliberate use of EM energy in an attempt to disrupt a platform's mission. The use of an exo-atmospheric nuclear burst to generate HEMP could be considered as the first RFW with a continent-wide or theater-wide effect. However, in the context of this report RFW is limited to non-nuclear EM weapon sources such as HPM, UWB and N^2EMP. RFW are currently being researched and although certain threat waveforms have been identified as being practical, new waveshapes may be used in the future.

24. Platform. A platform is a structure into which systems and equipments are to be installed (e.g., ship, aircraft, building, tank).

25. System. A set of equipment/modules interconnected to provide a function (e.g., avionic system on an aircraft, a truck, a missile).

26. Subsystem. A set of equipment/modules interconnected to provide a function, (e.g. radio, cabling and antenna; fire extinguish amplifier, cabling and sensors; anti-tank missile launcher and display).

27. Equipment. Normally a single electrical/electronic box, line replaceable unit or shop repairable unit. Can also be several modules that form the equipment are not located in the same box (e.g., radio, missile, flat-panel display).

28. Module. A subject of equipment which is reliant on the equipment for functionality (e.g., power supply, mother-board, hard disk drive).

29. Circuit. The means by which components are electrically connected together.

30. Component. Lowest assembly or integration level consisting of two or more piece-parts (e.g., hybrids, microprocessors, analog-to-digital converter).

31. Piece-part. The smallest element from which components, modules and equipments are built (e.g., integrated circuit, resistor, capacitor, transistor).

32. Hardware. A generic term for platform, system, subsystem and equipments

33. Aperture. An electromagnetic transparent opening

34. Upset. An impairment platform of system operation, either permanent or momentary (e.g., a change of digital or analog state) which may or may not require manual rest.)

35. Cable Bundle. A group of wires and/or cables bound or routed together that connect two pieces of equipments.

36. Electromagnetic Barrier. The topologically closed surface created to prevent or limit EMEs (radiated and conducted) from entering the enclosed space. The EM barrier consists of a shield and penetration port devices.

37. Electromagnetic Stress. A voltage, current, charge, or EME that acts on an equipment. If the EM stress exceeds the vulnerability threshold of the equipment, mission impacting damage or upset may occur.

38. Electromagnetic Shield. A continuous metallic housing (enclosure) that substantially reduces the coupling of electric and magnetic fields into the protective volume.

39. Penetration Protection Device. The protective measure used to prevent or limit EM energy from entering the protective volume at a POE or penetration port. Common penetration port or POE protection devices include waveguides below cutoff EM closure plates and metal grids for aperture POEs, and filters and linear/non-linear devices on penetrating conductors.

40. Penetration Port of Point-of-Entry. (POE). A location on the EM barrier where the shield is penetrated and EM energy may enter the protected volume.