eg. $Z_0 = 50\,\Omega$, $Z_L = (25 - j50)\,\Omega$, $l = ?$, $d = ?$

$$\tilde{z}_L = \frac{Z_L}{Z_0} = \frac{25 - j50}{50} = 0.5 - j1 \qquad (A)$$

To find $\tilde{y}_L$ rotate by 0.25λ on constant Γ circle

(B)

$\rightsquigarrow \tilde{y}_L = 0.4 + j0.8$ (Position 0.115λ on WTG)

To achieve matching we need d: real part of $\tilde{y}_{in}$ is

→ two intersection points with real = 1 circle

C: $\tilde{y}_d = 1 + j1.58$ (θ 0.178λ on WTG)

Distance between B and C $\rightsquigarrow 0.178 - 0.115 = 0.063\lambda$

$$\tilde{y}_{in} = \tilde{y}_s + \tilde{y}_d \equiv 1 + j0 = \tilde{y}_s + 1 + j1.58$$

$$\Rightarrow \tilde{y}_s = -j1.58$$

Normalized admittance of SC is $-j\infty$ (point E)

$\angle 0.25\lambda$ on WTG

An input normalized admittance of $-j1.58$ is at F

($\angle 0.34\lambda$ on WTG)

$$l_1 = 0.34 - 0.25 = 0.09\lambda$$

Point D: $\tilde{y}_d = 1 - j1.58$ Distance between B-D is

$d_2 = 0.322 - 0.115\lambda = 0.207\lambda$

Stub $\tilde{y}_s = +j1.58$ at G ($l_2 = (0.25 + 0.16)\lambda = 0.41\lambda$)

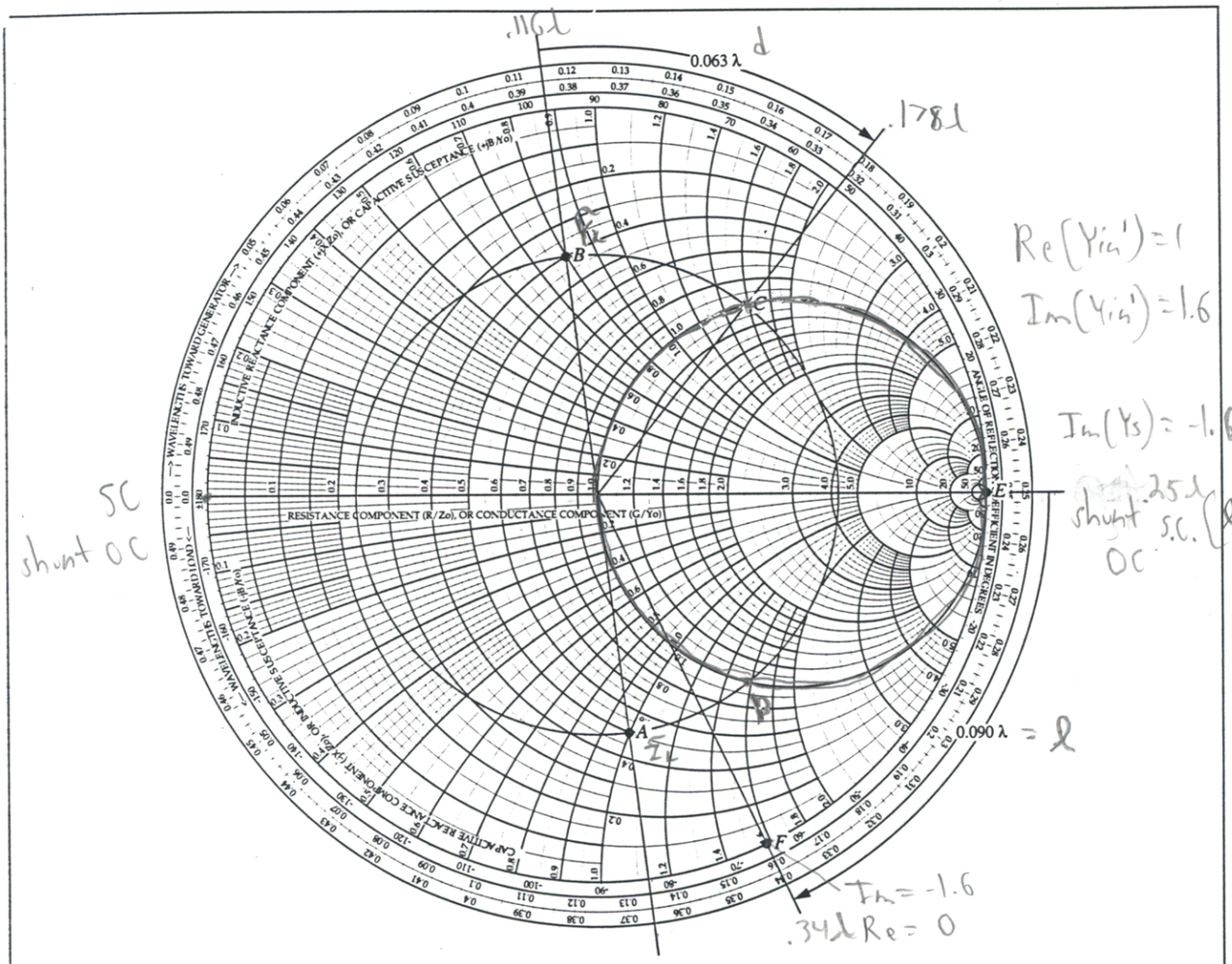

Figure 2-30: Solution for point C of Example 2-12. Point A is the normalized load with $z_L = 0.5 - j1$; point B is $y_L = 0.4 + j0.8$. Point C is the intersection of the SWR circle with the $g_L = 1$ circle. The distance from B to C is $d_1 = 0.063\lambda$. The length of the shorted stub (E to F) is $l_1 = 0.09\lambda$.

The normalized admittance of a short circuit is $-j\infty$ and is located at point E on the Smith chart, whose position is 0.25λ on the WTG scale. An input normalized admittance of $-j1.58$ is located at point F and is at position 0.34λ on the WTG scale. Hence,

$$l_1 = (0.34 - 0.25)\lambda = 0.09\lambda.$$

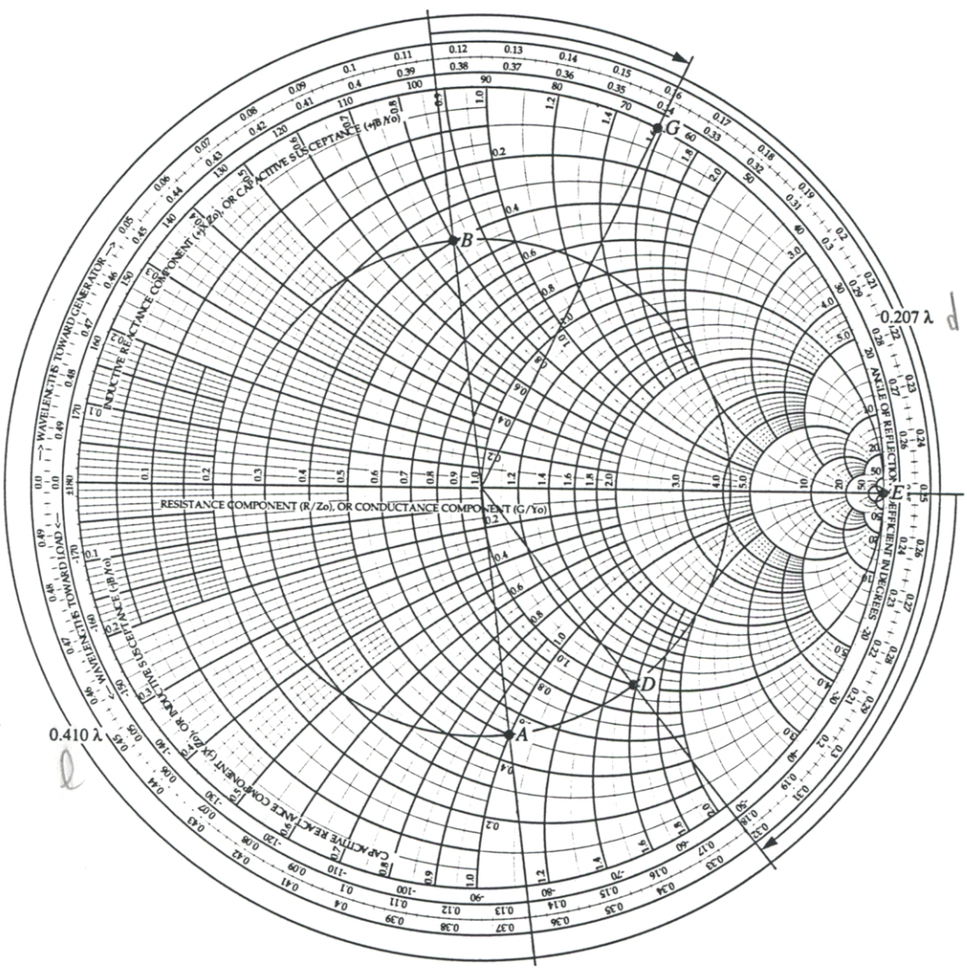

Figure 2-31: Solution for point D of Example 2-12. Point D is the second point of intersection of the SWR circle and the $y_L = 1$ circle. The distance B to D gives $d_2 = 0.207\lambda$, and the distance E to G gives $l_2 = 0.410\lambda$.

Solution for Point D (Fig. 2-31): At point D,

$$y_d = 1 - j1.58,$$

and the distance between points B and D is

$$d_2 = (0.322 - 0.115)\lambda = 0.207\lambda.$$

The needed normalized input admittance of the stub is $y_s = +j1.58$, which is located at point G at position

13. Intentional Electromagnetic Interference

R. L. Gardner[1], M. W. Wik[2], D. C. Stoudt[3]

[1]Vice-Chairman, URSI Commission E
Spectral Synthesis Lab, 6152 Manchester Park Circle, Alexandria, VA 22310 USA
Tel: (703) 924-9370; Fax: (703) 313-4179; E-mail: GardnerR@aol.com

[2]Chief Engineer, Strategic Specialist
Defence Materiel Administration
SE 115 88 Stockholm, Sweden

[3]Joint Program Office for Special Technical Countermeasures
Naval Surface Warfare Center, Code B20, Bldg. 1470
17320 Dahlgren Road, Dahlgren, VA 22448 USA

1. Abstract

Intentional electromagnetic interference (IEMI) is an extension of the work by the well-known electromagnetic compatibility (EMC) and electromagnetic interference (EMI) communities. Additional threats have recently surfaced that suggest that various individuals and groups can build devices to intentionally cause electronic systems to fail. The field levels that can be used by these people are much higher than the commonly used EMC standards, so that additional research and hardening is required to prevent electronic failures in the infrastructure supporting our society. There are a number of different people who threaten that infrastructure, varying from the person who violates the call to turn off his computer on the airplane, to the state-sponsored weaponeer. Community response also varies with the threat. URSI's role is to encourage research in this important area.

2. Introduction

Much of the work of URSI Commission E concerns the effects of electromagnetic noise and interference on various electronic systems. That work spans all types of noise, including that from improper frequency management, natural noise, and on to high-power electromagnetic sources. In this paper, we introduce a new cause for noise and interference in electronic devices: intentional electromagnetic interference (IEMI). Our society depends so much on sensitive, complex electronics that problems with that infrastructure can cause very serious

problems with the function of society. That dependence opens up a possible vulnerability to the use of electromagnetic interference to degrade the function of the electronic infrastructure.

Many different types of people have motives and opportunity to profit from the vulnerability of the infrastructure. They include careless people, criminals, terrorists and state-sponsored weaponeers. We differentiate among these categories according to the resources they can allocate to this problem, and according to the advantage they may seek to gain. Careless people gain a few minutes of extra work time while operating their electronic equipment in locations and times where it might be dangerous to others. For example, they might operate the equipment during the landing of an aircraft. Criminals might use electromagnetic interference to defeat electronics use by law-enforcement agencies. Terrorists are motivated to interfere with the basic infrastructure, in ways that cause fear and notoriety for the terrorist organization. Applying the techniques of high-power electromagnetics to attack the banking or securities industry would cause fear and notoriety. Sensitive electronics might include medical equipment or other life-saving devices or equipment. Finally, state-sponsored weaponeers are trying to defeat particular military targets. While the weaponeers form the upper end of the spectrum of those who use IEMI, they are really beyond the scope of this document.

We can use simple calculations to bound what the various organizations might do with electromagnetic weapons. Limits on reasonable antenna-aperture area and air breakdown show that certain applications are not feasible for any but the state-sponsored weaponeer. Decay of fields as $1/r^2$ is another limiting factor. The inherent variability of the lethality of high-power microwave weapons is another limit that works in the favor of the electromagnetic terrorist or IEMI practitioner, and against the state-sponsored weaponeer.

We, in the EMC community, would like to debate this issue in private, so that we do not encourage terrorists or others to use IEMI. Unfortunately, that path is no longer open. There has been significant public debate on the problem of electromagnetic terrorism in the public press and there is likely to be more. A number of articles on electromagnetic terrorism have appeared since the 1991 cover article in *EMC Technology* [*White*, *1991*], which described a drive-by truck-mounted high-power microwave weapon. More recently, the Joint Economic Committee of the US Congress held hearings on this problem. The testimony clearly encouraged research and development in this area. There have also been a number of newspaper and magazine articles on electromagnetic terrorism, including one in the *New York Review of Books* [*Scarry*, *1998*] that asserted that the TWA 800 crash was caused by a high-powered radio-frequency transmission.

There are a number of communities that play a role in assuring that the civilian (and military, for that matter) infrastructures are safe from electromagnetic noise and interference. URSI's role is advisory, in that we suggest particular areas of

electromagnetic research that are particularly fruitful or important to the member nations of URSI. The electromagnetic compatibility (EMC) community has a number of different organizations that do set standards. In Europe, in certain circumstances, these standards have the force of law. At this time, the EMC standards for immunity are set, along with emission standards, at low-level interference levels. If these levels really were the failure levels of banks and airplanes, society would be very much at risk from IEMI. Fortunately, critical electronic equipment is built to withstand higher levels than the few-volt-per-meter level of EMC. The EMC community does have a responsibility to deal with this problem, and to set reasonable standards. The US Department of Defense Office for Emergency Preparedness Policy has assigned the Joint Program Office for Special Technology Countermeasures (JPO-STC) the job of providing technical support in radio-frequency weapon technologies and their infrastructure implications.

3. Those who practice IEMI

Many of us travel, and we encounter those who stretch the rules about turning off electronic devices before landing an aircraft. It is not clear exactly why electronic equipment is more of a hazard below 10,000 ft than above. It is likely that the rule was established because of the consequences of an error, rather than the likelihood of a problem. Regardless of the reason, the people who continue operating computers or other equipment potentially interfere with the navigation and communication instruments of an aircraft. At low levels and in bad weather, proper functioning of these instruments is critical to the safe operation of an aircraft in flight. These people are only marginally in our collection of threats. Their threat is real, but their intent is not hostile.

The criminal element represents a much more serious threat. Examples of criminal and related terrorist behavior, using microwave weapons, drove *Loborev* [*1996*] to coin the phrase "Electromagnetic Terrorism," and to begin the debate about EM terrorism at the AMEREM '96 conference, in Albuquerque, New Mexico. His presentation materials show a number of threats. The ones associated with criminal elements included the detonation of explosives with radio-frequency transmissions, and jamming police radio-communication nets. The other two were more traditional high-power microwave threats, and are related to the defeat of alarm systems and locks. The execution of highly technical operations, such as these, requires skilled manpower and investment in test apparatus. Russian panelists have reported that unpaid Russian scientists in high-power electromagnetics are finding employment with the Russian Mafia. Thus, the criminals have skilled manpower and equipment from projects abandoned by the Russian government.

Electromagnetic terrorists represent a more serious threat to the infrastructure than the other two groups. These people have money and motive to attack important, sensitive electronics, which often control the infrastructure. The canonical problem cited for EM terrorists is the truck-mounted high-power-microwave (HPM) system

that is used on a banking system. That system was described in *Rosenberg* [*1997*], and the story was amplified in the testimony before the Joint Economic Committee [*Saxton, 1998*].

Despite the resources available to the EM terrorist, he will probably have to deploy his transmitters very close to his target. The close approach will cause risk to the venture, and complicate the overall logistics. The covert nature of EM terrorism works to his advantage, since he can try one day, and if he fails or succeeds, he can repeat the attack the next day. The target will probably not identify the problem as EM terrorism, right away. Normal failures and reboots occur too often in computer systems in normal operation for EM terrorism to be the immediate cause of failure.

The EM terrorist must also choose electromagnetic means as his choice of attack. Normally, the terrorist wants to call attention to his actions and to cause fear in his targets. EM terrorism may be too esoteric for his tastes. It is covert, and the cause of the computer failure is not obvious. The effects of his work may be severe. Computer systems control the financial base, aircraft, trains, electric power systems, logistic systems, and other critical parts of the infrastructure.

The state-sponsored weaponeer defines the upper end of the scale. He has more money and talent to devote to the development of RF weapons. A number of countries gave talks at the EUROEM '98 symposium on various aspects of HPM weapons development, including source development, effects testing, test facilities, and coupling-code development. Those countries included the United States, the United Kingdom, France, Germany, Russia, Israel, and Ukraine. While these countries and others like them are likely to develop weapons that can be used against the infrastructure, it is unlikely that civilian organizations such as URSI can do very much about it, so we will concentrate in this paper on threats that are appropriate to the EM terrorist and below.

4. What can these people and organizations do?

An electromagnetic terrorist first requires a source, or radio-frequency transmitter. That source must be effective, to a reasonable range, against equipment important to the target country. In his design, the terrorist must consider all of the transfer functions indicated in Figure 1 [*Baum, 1992*].

Each of the boxes of Figure 1 represents a change in the HPM signal generated in the source. Transition to the antenna attenuates and distorts the signal. The antenna directs the signal and narrows its focus. Distance is one of the major limiting factors for high-power microwave devices, and is chiefly $1/r^2$. As the intervening attenuation block indicates, however, there may be additional layers, such as building walls that may further attenuate the signal. System surfaces accept varying frequencies with strongly varying degrees of efficiency, so the terrorist must

match the source to the target geometry. The signal is further attenuated as it penetrates to the sensitive circuit element. Finally, there must be sufficient signal strength remaining to affect the device of interest.

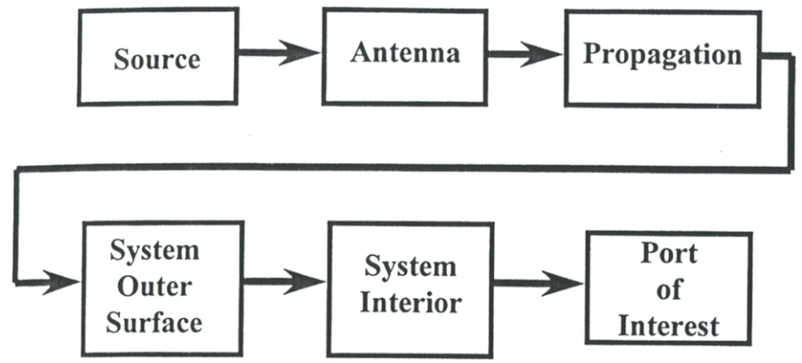

Figure 1. Transfer functions in HPM.

To get an idea of the requirements for such a terrorist weapon, we can consider some of the limitations. First, antenna-aperture sizes are limited, for practical reasons, to, say, about 1 m^2. That aperture could, in principle, be driven at up to air breakdown, which is about 10^6 W/cm^2. That allows a total power of about 10 gigawatts to be transmitted, if the terrorist can build an HPM source that big. Commercially available sources are limited to a few megawatts. Assuming a 1 GHz narrowband source, the relationship between the power density and range is shown in Figure 2. The megawatt-level source is about three orders of magnitude less, and generally ineffective for the example susceptibility levels cited below.

While this plot is just a simple $1/r^2$ plot, it demonstrates how little range some weapon concepts might have for required power levels. If one requires 10 W/cm^2 at the surface of a system to achieve lethality, then our hypothetical source configuration has a range of less than a kilometer. If 1 kW/cm^2 is required, then the range is only about 30 m, easily within rock-throwing distance.

The attenuation of walls and other parts of a structure make up an important part of the propagation attenuation. A simple wall may attenuate a signal by 10 dB. A more complex building, with metal cables and structural members, may attenuate the signal many tens of dB. These attenuators lower the curve in Figure 2 significantly.

We could dismiss the potential terrorist weapon if it were not for the uncertainty in the susceptibilities of electronic devices. There are variations of a factor of a thousand or more between failure levels of the same electronic systems. The issue of variability is covered in *Gardner and Jones* [*1995*], which notes that

there are potentially many orders of magnitude uncertainty in the actual failure level of an electronic system. When one attempts to predict the lethality level of an unknown system, this variation is particularly severe, because the system is untested and its exact design is unknown. It is this window of vulnerability that makes the terrorist particularly dangerous, even in situations where the state-sponsored weaponeer is ineffective.

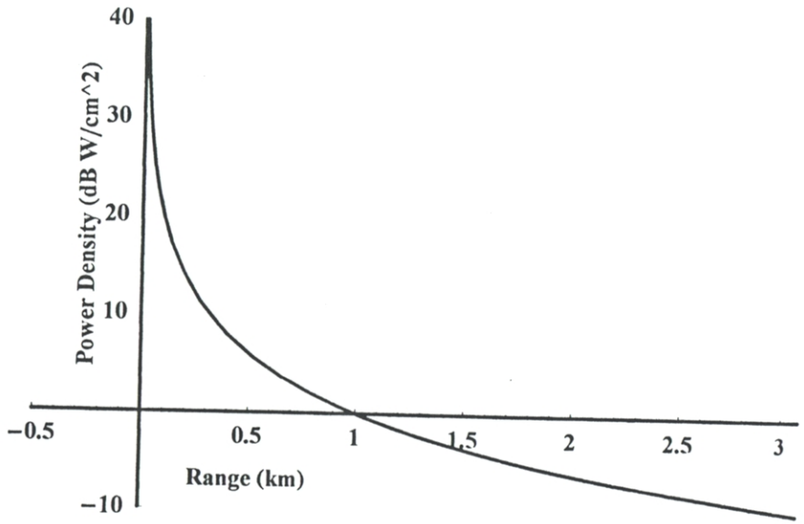

Figure 2. Fields for a 1 m aperture versus distance.

The list of systems that are potential victims is endless, just like the list for more-traditional terrorism. Civilian aircraft depend heavily on electronic devices for navigation and other safety-of-flight issues. Hospitals depend on radio links for patient monitoring. Almost all of us depend on electronics for our communications. The security of our financial institutions depends on electronics. These systems must be evaluated, to assure that the proper hardening techniques and design practices have been considered.

5. What can we do?

The threat from EM terrorism, based on available technology, involves a number of different sources and situations, which must be defined. Physical limits, depending on available technology and reasonable scenarios of applications, must also be studied. Transfer functions from source to ports of interest can be calculated,

just as for any EM problem. Susceptibility levels can be calculated and tested. Based on these studies, we can recommend protection devices, installation and mitigation guidelines with a reasonable cost/benefit ratio. How well a network can resist damage depends on its structure. Redundancy and diverse routing to improve reliability and availability can manage the risk of attack. Selected portions of a system can be protected. It is essential to establish verification that protection is effective, that incidents can be detected, monitored, and that warnings can be released.

Special detectors can warn about EM attacks. Detection and monitoring of incidents, release of warnings, repair, and restoration must be well managed. Efforts must be made to track origins of attacks, so those further incidents can be stopped. It is vital that personnel be trained for emergency situations. Most infrastructure systems work very well for long periods of time without many incidents. This is unfortunate, insofar as it makes people less alert to events preceding failure, when they happen. Resources for restoration and repair should be allocated, including back-up systems. Quality of protection and insertion of alternative systems, such as backup systems for software and power, must be routinely checked.

Since hardening is, in the end, an economic decision, business practice and the needs of the customer are important. It is not sensible to demand that all commercial electronics be hardened to levels that might be reached by a determined EM terrorist, but for high-value targets, that kind of performance is feasible. High-value targets include both electronics of military significance, and similar systems supporting the civilian economy. Important electronic installations include banks, electric power stations, pipelines, and other installations supporting the normal functioning of civilian economy. It is unlikely that complex systems can be completely protected against EM terrorism. However, just as a given level of reliability can be attained for a given effort and cost in design and engineering, so is the degree of hardening achievable dependent on the amount one is willing to spend on the hardening process.

The most important thing that we can do to stop EM terrorism is to make manufacturers of electronic systems, and their regulating and standards groups, aware of the problem. All manufacturers want to make products that sell and are free from liability expense. The products therefore must operate through their intended environment. That environment may or may not include EM terrorism. It is the purpose of this paper to encourage design engineers to make an informed choice.

Education of design engineers can take many forms. Most product designers are aware of the requirements of the electromagnetic-compatibility community. That community already causes additional expense. There are additional requirements for EM terrorism. EMC levels are now at the few-volts-per-meter level. Manufacturers resist higher levels, because of the limits to trade and the design and manufacturing expense. While the levels for EM terrorism are higher, the variability and complexity of EM vulnerability complicates the matter. The following statement

was made during an assembly of high-power-microwave test engineers, at the EUROEM '98 conference, in Tel Aviv, in June 1998:

> It is very difficult to use HPM to damage electronic equipment that has been properly designed using EMC/EMI standard practices, like integral shields and filters.

That statement suggests that following EMC guidelines will provide some protection. That protection may not be sufficient to prevent damage from all EM sources, but it will help. High-value targets will require substantial work and expense to assure hardness.

Education and debate within technical societies will encourage the use of commercial hardening practices. US EMC standards are voluntary at this time, while European Community standards eventually can have the force of law. The European Community sees the effects of EMC more frequently, because of its higher population density. American standards will probably continue to be voluntary, but we, in the EMC community, can encourage their use and demonstrate correct engineering practice.

Testing is the heart of any electromagnetic-vulnerability problem. We must determine the threat, and design sources to mimic the threat. We must develop techniques of failure prediction. And, we must show that our hypotheses are correct, through effective test conduct and publication.

Threat determination is most difficult, because we have only a little anecdotal evidence that this threat is real: just the argument that being prudent is reasonable. We can monitor selected facilities to find out if electromagnetic threats appear. Recall that the terrorist can continue returning until he achieves a failure, unless he is detected. The most urgent spot to conduct monitoring is aboard airplanes. We do know that the busy, careless people exist and are a threat. We are reminded of that every time we descend through 10,000 feet and are told to turn our computers off.

6. The public debate

6.1 Loborev's original address

General Loborev gave a Plenary Lecture to the AMEREM conference in May, 1996 [*Loborev, 1996*]. That lecture formed the basis of our present discussions on electromagnetic terrorism, and led to the public discussion of this important topic. In part of his talk on EM terrorism, he discussed radio-controlled explosive devices, the use of EMP radiators for disabling alarm systems, pulsed sources for opening locks, and the use of EM devices for suppressing radio communication. These uses are all closely associated with criminal activity, and the Russian Mafia is suspected of using these tactics. Professor Loborev also discussed the potential use of

electromagnetic waves for "reduction of the efficiency of professional activity" in people.

6.2 Recent Congressional testimony

On 17 June 1998, the US Joint Economic Committee heard testimony from Lt. Gen. Robert Schweitzer about radio-frequency weapons and their effects on electronics. Since these methods and weapons could be effective against their civilian counterparts, the Committee sought testimony on the potential effects of electromagnetic weapons against the infrastructure [*Saxton, 1997*]. Four scientists testified on the issue of electromagnetic threats to the infrastructure: James O'Bryon (Department of Defense), Dr. David Schriner (Electronic Warfare Associates), Dr. Ira Merritt (Missile Defense Space Technical Center) and Dr. Alan Kehs (US Army Research Laboratories).

6.2.1 Mr. James F. O'Bryon's statement. Mr. O'Bryon is Director of the Live Fire Range. His testimony was concerned with the role of the Live Fire Range in testing for RF weapons. He described a number of facilities in the live-fire arena, and suggested their use for testing the effects of RF weapons.

6.2.2 Mr. David Schriner's testimony. Mr. Schriner spent most of his time describing some of the advantages of a "Transient Electromagnetic Device." That device is known in the literature as a wideband or transient microwave transmitter. He supported the effectiveness of the device by reminding the Committee of the various announcements we hear on airplanes, not to use electronic devices while the aircraft is in flight. Mr. Schriner also built a simple transient electromagnetic device in his garage for about $500. He said that the device was effective, but did not demonstrate it.

6.2.3 Dr. Ira Merritt's testimony. Dr. Merritt discussed the proliferation of a number of different types of Russian radio-frequency weapons worldwide. For example, he discussed the recent Swedish exploitation of portable Russian RF weapons. Dr. Merritt described both electrically driven and explosively driven devices. His comments on susceptibility were less precise. He did conclude that much of the required risk mitigation could be accomplished through the development of low-cost, broadly-applicable mitigation techniques, similar, but not identical, to those used in the EMC community.

6.2.4 Dr. Alan Kehs' testimony. Dr Kehs provided only a general outline because of classification issues. However, he did say that "the growing US dependence on sophisticated electronics for warfighting and domestic infrastructure makes us potentially vulnerable to electronic attack" [*Saxton, 1997*].

6.3 Recent articles in the popular press

6.3.1 ***New York Times.*** *Rosenberg [1997]* considered a scenario in which an EM terrorist team attacks a government office building full of computer equipment. In his scenario, a terrorist group uses a van full of electronic equipment to cause significant damage to a building housing government electronics. He asserts that damage may be severe. This article, and others like it, grew from the above-cited testimony before the Joint Economics Committee hearing. That particular scenario was not used in the testimony, but it provides a clear statement of the situation that we all fear in electromagnetic terrorism.

6.3.2 ***The New York Review of Books.*** Elizabeth *Scarry [1998]* describes an even-more-serious scenario, in which she suggests that a possible cause of the TWA 800 disaster was electronic interference. While we do not believe that EMI was the cause of the TWA 800 explosion, Dr. Scarry's summary of the potential for disaster caused by electromagnetic interference is effective and scientific. Clearly, damage or interference with electronic communications or navigation gear on aircraft could cause a very serious accident.

6.4 Panel discussions

So far, there has not been sufficient information available at the various scientific symposia to support a complete session on electromagnetic terrorism. However, there have been meetings and panel discussions within the various scientific societies.

6.4.1 Electromagnetic Compatibility, Zurich, 1997. The meetings in Zurich were primarily organizational. URSI Commission E held an informal discussion on electromagnetic terrorism, and decided to form a subcommittee on Electromagnetic Terrorism under the existing URSI Committee on EMP and Other Matters, led by Dr. Manuel Wik. Dr. Heinz Wipf was asked to chair the subcommittee.

6.4.2 North American Radio Science Meeting. URSI Commission E held a Panel Discussion on Electromagnetic Terrorism in Montreal, during July, 1997. The panel discussion generated a lot of interest, and the standing-room-only audience overflowed into the hallway. Several members of the panel suggested scenarios in which electromagnetic terrorism could be a serious problem. One of those included the use of surplus radar equipment to threaten low-flying aircraft. There was little agreement on the vulnerability of such an aircraft, despite extensive testing for EMC/EMI purposes. It was, of course, not the purpose of the workshop to determine the hardness of the aircraft, but to determine the importance of the research topic. There was also considerable uncertainty in the vulnerability of ground equipment, particularly since the configuration of the equipment was ill-defined. Most of the audience supported additional research into electromagnetic terrorism and appropriate protection techniques. There was uniform support for work to establish appropriate levels for this threat. A minority expressed the fear that even discussion

of the topic would encourage the use of electromagnetic means to disrupt electronics critical to the infrastructure. We have found that the discussion is already in the public domain, and believe it should continue, with the aim of encouraging research and implementation of appropriate protection techniques.

7. Roles for future research

During the various workshops, there was some discussion about the role of URSI in this debate about protection from EM terrorists. URSI is, by its nature, a public, international, organization, so all of its technical meetings are open to anyone willing to register for the conference. The details of electromagnetic interaction of particular systems are not public, however, and specific vulnerabilities, should not be made public. There is still room for technical debate about the methods that should be used to protect the public from the damage that can be done to the infrastructure by EM terrorists. That brings us to the roles of the various organizations in this debate.

7.1 The role of URSI

URSI's home page describes the role of URSI in the following way:

> The object of the International Union of Radio Science (Union Radio-Scientifique Internationale) is to stimulate and to coordinate, on an international basis, studies in the field of radio, telecommunication and electronic sciences, and, within these fields....

We are now considering the issues, and members of Commission E will likely frame a resolution for consideration by the URSI Council at the next General Assembly. If the Council approves the resolution, it will be distributed. The formulation of standards of protection belongs to other parts of the electromagnetic compatibility community, however.

7.2 The electromagnetic compatibility community

The IEEE Web site describes the role of the Electromagnetic Compatibility Society with the words

> The IEEE EMC Society strives for the enhancement of electromagnetic compatibility through the generation of engineering standards, measurement techniques and test procedures, measuring instruments, equipment and systems characteristics, improved techniques and components, education in EMC and studies of the origins of interference.

The IEEE EMC Society, like some other organizations, is in the business of recommending standards for EMC, and that is where the real work of electromagnetic terrorism belongs. Businesses and governments will have to make the hard decisions associated with application of some of the more difficult and expensive standards, but the EMC community must provide reasonable data for these bodies to make those decisions. All parties responsible for electronics critical to the infrastructure should be encouraged to look at the problem.

8. Conclusions

The public should be protected from the extensive damage that could be done to vital computers in the infrastructure, or to other electronic communications or navigation equipment. To protect the public, the threat must first be defined. It must be assumed that terrorists do not have the resources of a major national power, and so will use available technology. It is then appropriate for us to survey the available surplus equipment sold by governments or by private companies. There are also physical limits on what can be done in microwave-source technology, such as those suggested in Section 4.

After the threat is defined, we must work to protect the electronic equipment used in vital equipment. Electromagnetic compatibility is the discipline that is designed to provide that protection to the public, and to insure that the protective measures work. It is only necessary to include the potential threat from intentional microwave sources in the EMC specifications, as well as those threats from unintentional sources. Some of the intentional sources may be severe and require extensive hardening. At that point, the EMC community must outline the risks and the economic trades to the public, and to the owners of the electronic equipment.

9. References

C. E. Baum [1992], "Maximization of Electromagnetic Response at a Distance," *IEEE Transactions on EMC*, **EMC-34**, 3, pp. 148-153.

R. L. Gardner and C. W. Jones [1995], "System Lethality, Perspective on High Power Microwaves," *System Design and Assessment Notes, Note 34,* EMP Note Series, Kirtland AFB, NM.

V. M. Loborev [1996], "The Modern Research Problems," Plenary Lecture, AMEREM Conference, Albuquerque, NM, May 1996.

E. Rosenberg [1997], "New Face of Terrorism: Radio-Frequency Weapons," *New York Times*, 23 June 1997.

J. Saxton [1998], Record of the "Joint Economic Hearing Radio Frequency Weapons and Proliferation: Potential Impact on the Economy," US House of Representatives.

E. Scarry [1998], "The Fall of TWA 800: The Possibility of Electromagnetic Interference," *The New York Review of Books*, **XLV**, 6.

D. White [1991], "HERF and Electromagnetic Terrorism," *EMC Technology*, **10**, 1, p. 7.

14. Modeling Techniques for EMC Analysis

F. M. Tesche
EMC Consultant
9308 Stratford Way, Dallas, TX 75220 USA
Tel: +1 (214) 956-9378; Fax: +1 (214) 956-9379; E-mail: Fred@Tesche.com

1. Abstract

This paper provides a review of modeling concepts for analyzing problems in electromagnetic compatibility (EMC). The approach to be discussed here begins with first-principles considerations, including a system topological description, determination of appropriate material and geometrical parameters, and a statement of a formal model involving solutions of Maxwell's equations. As in most engineering problems, suitable approximations to the solution are required to make the problem tractable. To be avoided in this modeling approach are the "rules of thumb," which are often encountered in the EMC community.

2. Introduction

In today's increasingly complex electronic world, there are many new types of electrical systems that can produce unwanted electromagnetic interference, or EMI. Furthermore, these devices themselves may be adversely affected by emissions from another device, or from natural sources like lightning. Electromagnetic compatibility (EMC) is the study of such electrical interference, and the steps that can be taken to reduce or eliminate it from the environment.

EMC is the *science* of interference control, as opposed to a "rule-of-thumb" or "seat-of-the-pants" approach for interference mitigation. As such, it closely follows the steps of the scientific method: (1) observe a phenomenon, (2) formulate a hypothesis as to the cause, (3) test or experiment to validate the hypothesis, and (4) formulate and state the theory.

There are three basic goals of EMC activities. These are (1) to design an electrical system does not *interfere* with the operation of another system, (2) to insure that a system is not *susceptible* to electrical emissions from another system, and (3) to be sure that the system does not interfere with its own operation.

As illustrated in Figure 1, the EMC problem can be described by a source of electromagnetic interference, a coupling path along which electromagnetic energy travels, and a receptor, or victim, equipment that is affected by the interference [*Tesche et al., 1997*]. In the area of EMC analysis, one can develop models that describe the behavior of each of these items.

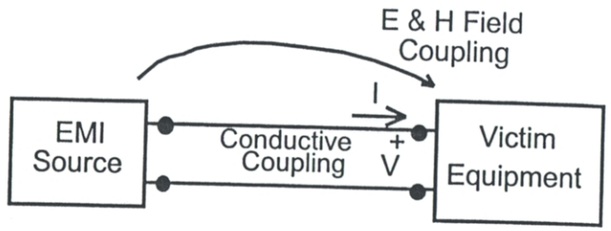

Figure 1. An illustration of the generic EMC problem.

Generally, electromagnetic interference can be categorized as being either conducted or radiated [*Paul, 1993*; *Keiser, 1979*]. Conducted interference, as illustrated in the top two diagrams of Figure 2, denotes interference that propagates along wires or other electrical conductors from the source to the victim circuit. Radiated interference, on the other hand, relates to the propagation of electromagnetic fields through free space from the source to the victim, as illustrated in drawings on the bottom row of the figure.

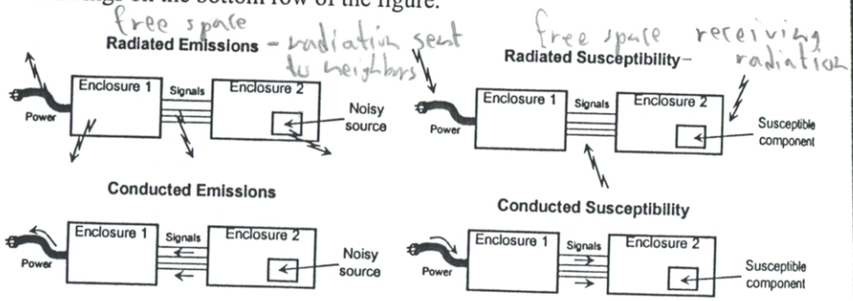

Figure 2. Four categories of electromagnetic interference encountered in EMC problems.

Electromagnetic interference may also be categorized by the terms *emission* or *susceptibility*. The term *emission* refers to the case when the electromagnetic interference is being produced internally within the device or component and escapes to the surroundings, possibly to upset nearby equipment. This is illustrated in the left column of Figure 2. The term *susceptibility* refers to an external electromagnetic environment disrupting, or otherwise affecting, a piece of equipment or a component, and is represented pictorially in the right column of the figure.

There are many different kinds of sources in the EMC area [*Tesche et al., 1997*; *Perez, 1995*; *Degauque and Hamelin 1993*; *Paul, 1992*]. Perhaps the most familiar are *natural* sources, such as lightning or electrostatic discharge (ESD). Triboelectric charging effects cause the well-known p-static interference on aircraft, and the disruption of radio communications by solar events is well known. Furthermore, very slow fluctuations of the Earth's magnetic field are known to cause significant disruptions in electrical power networks. The blackout of the Hydro Quebec power system in the late 1980s was a direct result of one such geomagnetic storm.

In addition to natural EMI sources, there are many man-made sources that cause disruptions within electrical systems [*Morgan, 1994*]. Such man-made sources include switching transients and harmonic generation on the electric power system, radiation from computer clock circuitry on printed circuit boards, harmonic radiation from switching power supplies, and noise from electric motors. Radio and radar transmissions have been known to adversely affect equipment in the vicinity of the transmitters. The areas of automotive and railroad noise are also of concern.

One infrequent, but potentially very serious, type of man-made electromagnetic interference is the nuclear electromagnetic pulse (NEMP) [*Lee, 1989*]. This occurs with the detonation of a nuclear bomb, and produces a large-amplitude, fast-rising transient electromagnetic field that may damage or upset electrical systems.

With such a wide diversity of EMI sources, many different types of signals are encountered in the EMC area. The signals might be narrowband (sometimes referred to as continuous-wave or CW signals). An example of this type of signal is found in a radio beacon transmitter. On the other hand, transient signals are often encountered. These signals may have very large amplitudes, such as those encountered with induced lightning currents or NEMP fields. Conversely, they may be very weak, such as radio signals received from a very distant transmitter or radiated from a micro-circuit. *Tesche et al.* [*1997*] provided several lists of EMI sources and their characteristics for reference.

2.1 Need for modeling

The need for electromagnetic interference control has been well-publicized [*Goedbloed, 1992*; *Chatterton and Houlden, 1991*]. Certainly, incidents involving loss of life and equipment illustrate a need for EMI control[†]. Regulations imposed by governments or by other standards organizations cause manufacturers to be more

[†]A notable example was the Forrestall incident in the 1960s, in which a ship-board radar illuminated an armed aircraft on the carrier deck, setting off a series of munitions explosions. This resulted in scores of servicemen injured or killed, and millions of dollars in equipment damage.

attuned to the problems of EMI, and to design their equipment such that it will meet the required specifications. In addition, manufacturers realize that developing a potentially dangerous product could cause liability problems, should a customer be injured or killed. In short, if a new product is put in the marketplace today, and it involves electrical technology, it *must* be designed and built with EMC in mind.

A key aspect in developing a correct and proper EMC design for a new system or product is *modeling*. Modeling is a useful tool for the analyst, as it a permits the *simulation* of system behavior. Instead of building a physical prototype of the system, an analyst can construct a mathematical version on the computer, and then study its responses for a wide variety of initial conditions, excitations, and configurations. This typically occurs in a much shorter period of time (and at a much lower cost) than the development of the prototype system. This process is often referred to as performing a "*numerical experiment*," because of the similarity of simulation and experimental processes.

2.2 Types of modeling

Modeling and imaging are fundamental to humans. Usually this is done to be able to represent *things or ideas* that cannot be seen or felt by one's senses. As time progressed and society became more complex, the modeling process has changed. In very early times, modeling was used to represent an abstract idea into something concrete–for example, human forms were used to represent the mythological Greek gods. More recently, physical and experimental phenomena have been represented by abstractions. The first such abstract models appeared when the link between mathematics, which itself has developed as an abstract science, and experimental observation of natural phenomena, was achieved.

The scientific method mentioned earlier is essentially a description of an early attempt to add rigor and traceability to modeling. The main features of this method are that *experimental observations* are used to *validate* the correctness of a cause-and-effect hypothesis. This approach offered a picture of reality that is *independent* of the observer–that is to say, every observer draws the same conclusion–and it forms the basis of classical physics.

As pointed out by *Johns* [*1979*], developer of the TLM method, there can be many ways of modeling a particular phenomenon. As pictured in Figure 3, a physician may have one specific view of the human being, and his model appears on the left. The Hollywood set designer has a different view, and consequently a different model is shown on the right. Both models are valid, of course: each one is correct for its own special purpose.

For models developed for EMC purposes, we shall be looking for a way to relate an *effect* to a *cause*, or equivalently, an *output* to an *input*. The numerical

implementation of such a model, while important, is only a secondary issue to the development of a modeling concept.

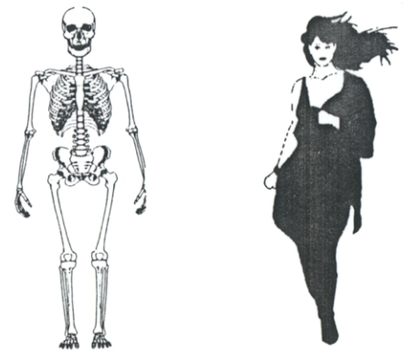

Figure 3. Two types of human models.

2.3 Development of models in electromagnetics

In the area of electromagnetics, models are based primarily on Maxwell's equations or on their simplifications. In addition to these equations, *boundary conditions* on the EM fields are necessary–and this relates to the subject of electromagnetic topology, which will be discussed shortly.

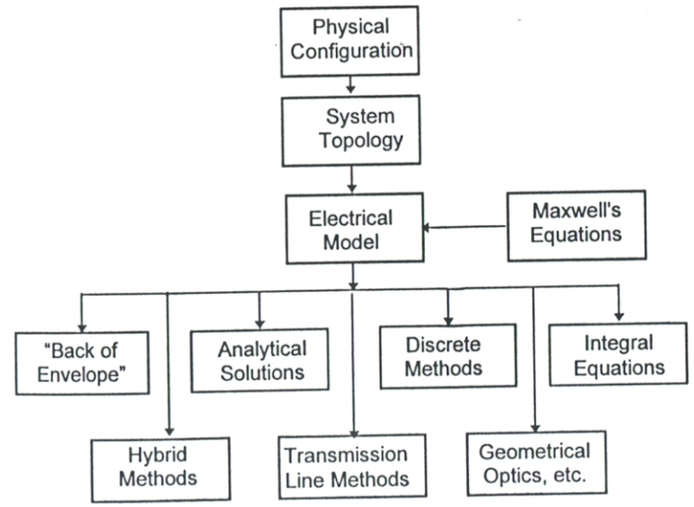

Figure 4. Model development in EMC.

From Maxwell's equations, many different approaches for a numerical solution are possible. Shown in Figure 4 is a flow chart of the analysis process. From a description of the *physical configuration* of a problem, its electrical configuration (system topology) may be defined. From this topology, and the use of Maxwell's equations, an electrical model evolves.

Depending on the nature of the problem, there are many types of solutions available. For example, in some cases a very simple, approximate, *back-of-the-envelope solution* may be adequate. Sometimes, the system topology may be so simple that an *analytical solution* is feasible. In most cases, however, the electrical model is sufficiently complicated that some type of numerical method must be used to obtain a solution. Such a solution could involve discrete methods, such as a finite-difference or a finite-element solution. Conversely, integral-equation techniques, transmission-line solutions, high-frequency solutions using the Geometrical Theory of Diffraction (GTD), or even combined or hybrid methods, are all possible.

The choice of which analysis method to use is often a difficult one. Usually, several different methods can be used for the same problem, and it is the skilled analyst that is able to determine the optimum method.

2.4 Model validation

Like the scientific method, modeling development relies on *independent experiments* or observations to validate the model. Such validation checks both the theoretical foundations of the model, and its numerical implementation.

Model validation may be done in several different ways. The first is by an *experimental check* of the model. This is accomplished by designing specific experiments to test the model, and then to compare the model results with measured data. Note that in doing this, the predictions must be made *independently* from the experiments.

It is possible to note cases in the past where experimental data were used to "tune" a model by optimizing its parameters so that the model provided the correct response for the experimental case. This is essentially the basis of operation of a neural network. Note that this approach is basically a curve-fit model, and is not based on Maxwell's equations or any other rigorous theory. This does not detract from the usefulness of this type of model, however, as long as it is validated properly.

Models may also be validated using non-experimental methods. For example, previously validated models may themselves be used to test a new model. In addition, the use of thought experiments is useful in examining the behavior of the following issues in a model:

- conservation of energy
- causality or turn-on time the response
- times of arrival of a waveform
- low-frequency or high-frequency asymptotic behavior of the spectral responses, and
- other known physical constraints of the solution, such as finite Q at system resonances, etc.

3. Representation of electrically complex systems

It goes without saying that the analysis of an electrically large system is very difficult. This is due to the complexity of the system and the many different ways the electromagnetic energy can interact with a system. Models abound for various types of radiating antennas, for aperture penetration, for waveguide propagation, etc. But how are these simple models to be combined into a more complex system model?

At lower frequencies, there can be inductive and *capacitive coupling* between wires or components. At the higher frequencies, direct electromagnetic radiation becomes important. Within the system, the propagation of electrical charge and current along conductors must be accounted for, as well as the *penetration* and *propagation* of electromagnetic energy through apertures and imperfectly conducting walls of the enclosure. Cavity-mode resonances are also important.

Early attempts at developing analysis model for complex systems were hampered by not having a structured way of decomposing the system into smaller parts. This led to models with errors frequently exceeding 30 to 40 dB [*Carter and Curtis, 1974*]. As a result, many people believed that modeling was not a useful tool for EMC purposes, and this led to the rule-of-thumb approach for EMC design.

3.1 Topological decomposition of systems

To begin the modeling process, the system can be thought of as consisting of several concentric layers of conducting surfaces, which shield the interior. This has been referred to as the *onion* concept of shielding [*Ricketts et al., 1976*]. This idea was refined by *Baum* [*1974*] and *Tesche* [*1978*], and later formalized in the literature [*Baum, 1986*].

Analysis using the electromagnetic topological concepts is straightforward. The system under consideration is first examined for the principal shielding surfaces or *electromagnetic barriers*. Usually these shields take the form of closed

conducting surfaces, much like in a Faraday cage. Imperfections in these shields are noted and categorized. From this information, a signal-flow diagram, which describes the flow of energy from the outside of the system to its interior, is constructed. Models are then developed for important elements of this signal path, and an analysis of the overall system is performed.

3.1.1 The topological diagram

The first step in model development is to determine the *topological diagram* of the system. This is a description of the principal shielding surfaces in the system and their interrelations. Real shields are not perfect, and external electromagnetic energy can penetrate by one or more of the following mechanisms:

- by hard-wire penetrations formed by wires, cables, or other conductors
- by aperture penetrations through holes or other openings in the shield, and
- by field diffusion through the shield material

As a simple example, consider the case of an aircraft excited by a distant cloud-to-cloud lightning discharge, as illustrated in Figure 5. The physical configuration of the aircraft, shown in the top of the figure, can be represented by the system-topology diagram on the bottom. The aircraft fuselage is represented by the barrier, or shield surface, S_1. The volume denoted as V_0 represents the space outside the aircraft, whereas the volume labeled as V_1 is the region just inside. Locations of aperture penetration, diffusive penetration, and the direct penetration of energy along an antenna cable, are shown schematically.

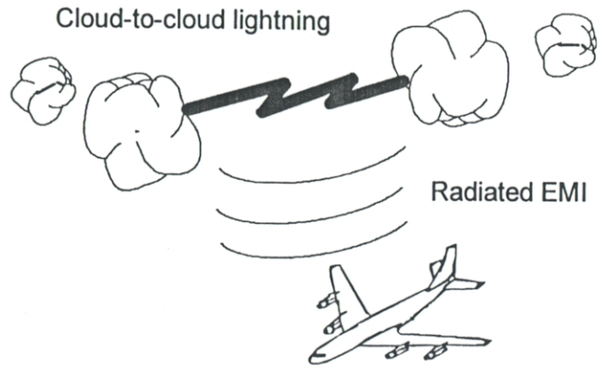

Figure 5a. An example of an aircraft and its EM topological diagram: physical configuration.

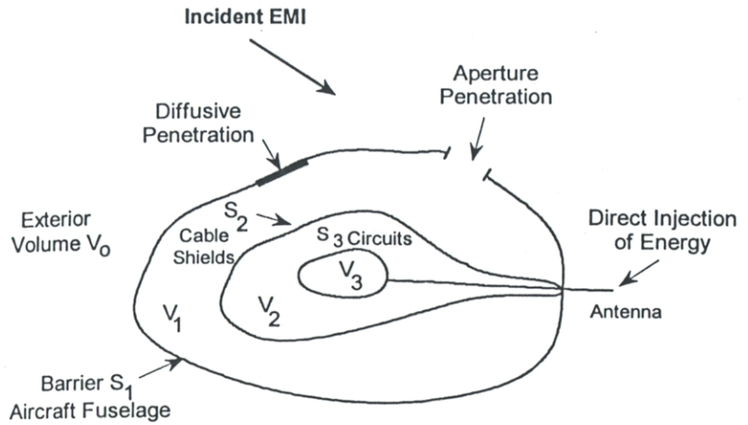

Figure 5b. An example of an aircraft and its EM topological diagram: EM shielding topology.

Additional shielded volumes within the main aircraft volume are also possible. These are the cable shields and equipment enclosures, and they form the *secondary* shielding surface S_2. Within this surface lies another, more highly protected region, volume V_2.

Notice that in constructing this topological shielding model, no attempt has been made to retain the original form of the aircraft. This is done deliberately, in an attempt to focus on the details of the inner connections of the shielding surfaces and volumes, rather than on the physical shape of the system.

3.1.2 The interaction sequence diagram

From the shielding-topology diagram, the interaction sequence diagram (ISD) can be developed. This diagram represents the paths that the external EM energy can take in passing from the outside to the inside of the system. Basically, this is a signal-flow diagram that is developed from the topological diagram and the penetrations. In most cases involving well-shielded systems, we make an assumption, commonly referred to as the *good shielding approximation*, which is that electromagnetic energy flows *only* from the outside to the inside of the system. The implication of this is that there is no mutual interaction between the equipment inside the shielded region and the sources on the exterior.

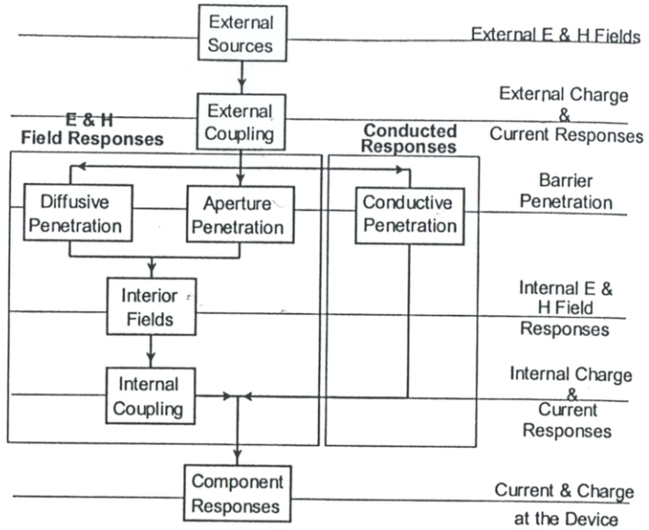

Figure 6. The interaction sequence diagram for a typical system.

Figure 6 illustrates a sample interaction sequence diagram for the case of the aircraft system with external electromagnetic sources. The source, shown at the top of the diagram, produces electromagnetic fields that propagate to the system, and induces external charges and currents on the system exterior. This process is referred to as *external coupling*.

On the conducting surface of the enclosure, the electromagnetic energy is able to penetrate through the surface, or barrier, by diffusive penetration or aperture penetration of the EM fields, as shown in the darkened box on the left in the figure. This process results in internal EM fields within the enclosure that subsequently couple to internal wires, inducing a voltage or current response.

A different interaction path for the EM energy is shown on the right-hand side of the figure. Here, externally-produced current and charge responses on conductors are able to penetrate the shield surface through a *conductive penetration*. Note that the responses now are thought of as currents and charges, as opposed to the EM fields considered in the previous penetrations. This interaction path also results in a voltage or current response induced on internal wires. The responses of both of these coupling paths ultimately provide a voltage or current response at a component, which is often the desired quantity in such an analysis.

From the interaction sequence diagram, a system electrical model can be developed. This is obtained by removing all of the unimportant features–or clutter–in the system that do not have significant impact on the electromagnetic response.

Of course, this step in the analysis requires significant judgment on the part of the analyst, since important parts of the system must not be discarded.

Using the electrical model, a circuit model is then developed. Usually, this is put into the form of an equivalent Thevenin or Norton circuit. In this way, the entire system-interaction model is represented by a single circuit, which then can be used to calculate the system response.

In many cases, the elements of such a circuit are not known analytically, and estimates for their values must be provided before a calculation can be performed. For example, per-unit-length inductance and capacitance values of a transmission line are necessary for such distributed circuits, and they must be calculated, estimated, or measured.

3.2 Example of system decomposition

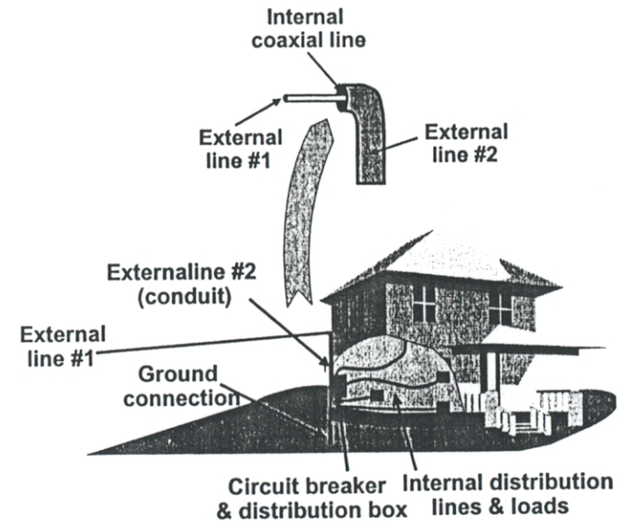

Figure 7. An illustration of a ground-based facility with an external line feeding an internal network.

At this point let us provide a concrete example of the topological concepts that have been discussed for modeling. Consider the case of a ground-based system, perhaps a communication facility. As shown in Figure 7, it is a shielded building, having a long electrical cable feeding power into the facility. This power line passes through a weather-head connection, and then enters into the shielded room. Inside the facility, the power cable fans out into several different internal lines, each going to various power loads in the building. For this system, we will assume that the

excitation is provided by a distant lightning strike to the overhead power line, and we are interested in determining the induced responses at the electrical loads within the facility.

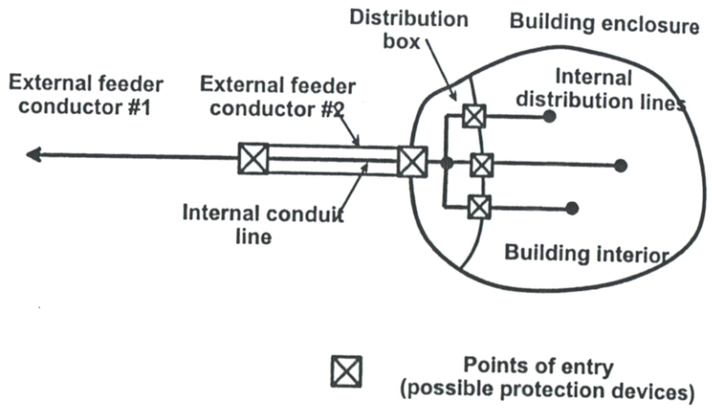

Figure 8. A topological diagram for the ground-based system.

The topological diagram for this system is shown in Figure 8. As mentioned earlier, the topological diagram consists of several shielding surfaces, or barriers, that attenuate the external electromagnetic stress. Shown in this diagram is the principal building enclosure and its internal volume, the power-distribution box, and the shielded feeder section of the external power connection. Locations on the power system where protection devices, like surge arrestors or filters, may be found are illustrated in the diagram.

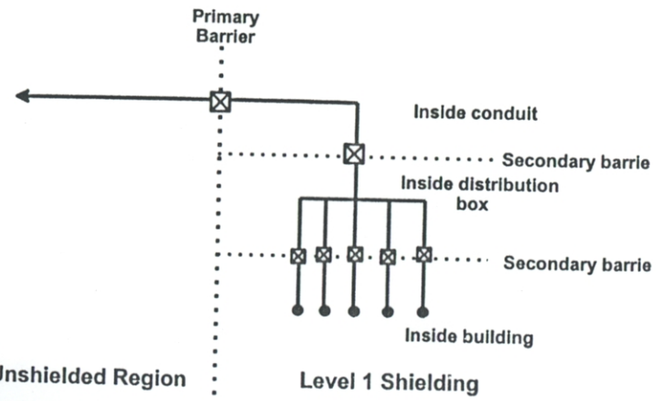

Figure 9. The interaction sequence diagram for the ground-based system.

The next step in the process of developing a model for this system is to define the interaction sequence diagram. The path along which the external electromagnetic energy propagates into the system is illustrated in Figure 9. The dotted lines signify the locations of the electromagnetic barriers or shields, with the solid lines representing the signal paths. A box with a cross through it indicates locations where there may be attenuation of the signals. Such attenuation can arise either from deliberately installed protection devices, or from naturally occurring attenuation due to signal splitting within the distribution box, etc.

From the interaction sequence diagram, one can develop a more detailed electrical-system model for calculating the propagation and penetration of energy within the facility. As shown in Figure 10, the above-ground power line is represented by a long electrical conductor at height h_1 over the earth. The lightning excitation is assumed to be provided by a voltage source located along this line.

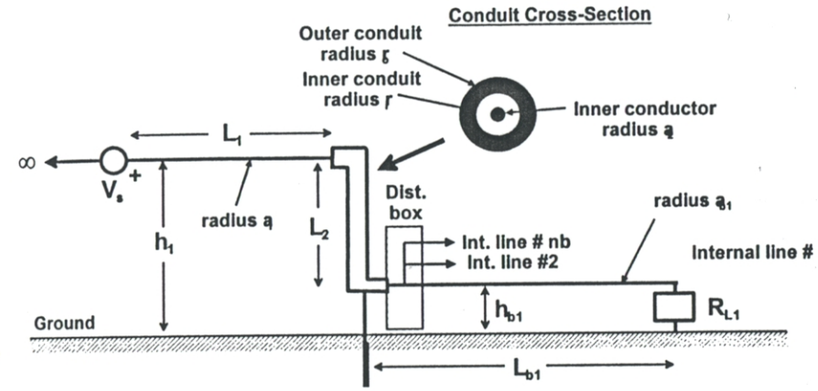

Figure 10. The system model for the ground-based system.

The power line entering into the weather-head is modeled as a coaxial transmission line, with its external shield connected to the ground. Inside the distribution box within the facility, the internal power lines spread out, each one being represented as a single transmission line over the reference conductor. Each of the loads on the power system is denoted by the resistors R_{L1}. The induced voltage or current at these loads will be the desired responses.

From the previous electrical model of the system, a distributed circuit is formed. This circuit, as shown in Figure 11, consists of an interconnection of transmission lines, with appropriate sources, loads, and distributed parameters. Using standard transmission-line models [*Tesche et al., 1997*], responses within the system can be easily estimated.

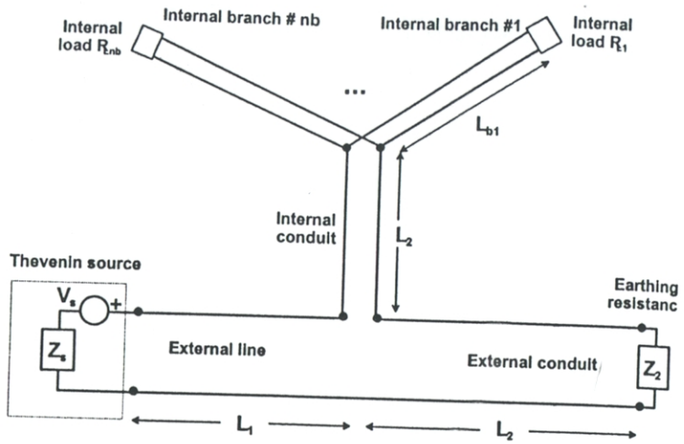

Figure 11. The distributed-circuit representation of the system model.

4. Use of EMC models and their results

Once an EMC model has been developed, it is important to use it in a productive manner. Unfortunately, in many instances models are not used in the most efficient manner. These deficiencies need to be addressed.

Frequently, a model will be developed for the calculation of a *single* response within a system, and only a very limited number of calculations performed. The result may be one or two transient waveforms, or one or two spectral densities. Left unanswered are the following questions:

- How typical is a calculated response?
- What are the maximum and minimum values of the response?
- If parameters defining the system change slightly, how much does the response change?
- How accurate is the response?

These questions can be answered by using the models in a different way. For example, a sensitivity analysis to understand the impact of small changes in system parameters can be performed using the concepts of *response elasticities* and *waveform deviations*. Furthermore, *statistical representations* of system responses, using probability distributions and cumulative probability functions, can be very useful.

To conduct a sensitivity analysis, a suitable scalar response (or observable) must be identified. For a transient waveform, it is convenient to describe such observables by one or more signal norms [*Baum, 1979*]. Possible norms include the

energy contained in a response, the peak values (both positive and negative) of the response, and the maximum rate of rise of the waveform.

Once a response is defined, its partial derivatives with respect to changes of all of the system parameters may be calculated. In most cases, the model is so complicated that these derivatives can not be determined analytically. They must be found numerically. As will be discussed in the next section, these partial derivatives are used in calculating the elasticities and waveform deviations.

4.1 Response elasticities

As mentioned earlier, often we are interested in estimating the change in a response of the system due to a change in one of the system parameters. This is because, in most cases of complex systems, parameters are not known accurately, and we wish to assess the degree of error caused by this uncertainty.

One possible way of representing a change in a response is to define the elasticity of the response with respect to a particular parameter. This quantity is commonly used in financial modeling, and is the normalized partial derivative of the response [*Thomas, 1968*]. For a particular response norm, denoted by E, the elasticity, $\mathcal{E}_i$, for a change in a system parameter, x_i, is given as

$$\mathcal{E}(E)_i = \frac{\partial E / \partial x_i}{E / x_i}. \qquad (1)$$

Elasticities provide a convenient way for characterizing the relative importance of the parameters in determining the overall response. A zero value of $\mathcal{E}_i$ for a parameter x_i indicates that the parameter plays a negligible role in determining the total response, and its value is not very important. A large value of $\mathcal{E}_i$, however, signifies that x_i is a significant variable and suggests that its value must be known accurately.

4.2 Waveform deviations

In addition to the elasticities, waveform deviations also may be calculated to illustrate the effects of small changes in system parameters when transient responses are considered. A waveform deviation is a normalized difference between two transient responses. Consider a particular parameter, x_i, undergoing a change Δx_i. Letting the partial derivative of the response, v, be a function of time, the corresponding change in the voltage waveform $\Delta v(t)$ is given by the expression

$$\Delta v(t) = \frac{\partial v(t)}{\partial x_i} \Delta x_i . \qquad (2)$$

This expression amounts to a time-dependent, difference waveform. The amplitudes of these waveform deviations illustrate the relative importance of the variations of each parameter within the system. In addition, these waveform deviations provide information about the time of arrival of the effects from these parameters. It gives information as to the electrical distance of the effect of the parameter.

4.3 Statistical descriptors

Statistical representations of responses are also useful in understanding *global* system behavior. As mentioned earlier, in most system problems there is imperfect knowledge of the exact values of parameters. Furthermore, the system configuration may change or be extremely complex. In these cases, it is useful to quantify the range of possible system responses, as has been discussed by several different authors. *Morgan and Tesche [1978]* have examined the responses of multiconductor cables with random twists using statistical methods, and the behavior of an ensemble of randomly oriented dipoles has also been treated [*Graham and Mo, 1978*]. In some cases, analytical representations of the statistics of a response are possible, for example, as in the case of the cavity, as described by *Lehman [1993]*. In more complex cases, however, a Monte Carlo procedure may be developed to simulate the overall system-wide effect of parameter uncertainties. Such a procedure, however, does not seem to have been widely used in system-level EM studies.

The statistical response of an observable within a system can be represented in several different ways. The probability density function, $P(x)$, represents the probability of encountering a particular response with a value between x and dx. The cumulative probability distribution (CPD) is the integral of the probability density function. As a result, it represents the probability of obtaining a response that is less than, or equal to, the value x. Finally, the complementary cumulative probability distribution represents the probability of obtaining a response that is greater than the value x.

4.4 Examples of system responses

As an example of calculated responses, let us consider the previous case of the ground-based system, shown in Figure 7. This is a shielded facility with an entering power line, which is excited by a lightning strike to the line. The induced voltage or current at an internal load will be the desired response. The electrical model for this system has been described in Figure 11, and has been developed using topological-modeling methods.

In this example for the behavior of the electrical model, it will be necessary to make choices for the various parameters describing the system. These are:

- External Line #1: $L_1 = 10\,\text{m}$; $h_1 = 3\,\text{m}$; $a_1 = 0.01\,\text{m}$
- External Line #2 (coax): $L_2 = 2.5\,\text{m}$; $h_2 = 2.5\,\text{m}$; $r_o = 0.05\,\text{m}$; $r_i = 0.04\,\text{m}$; $a_2 = 0.01\,\text{m}$

Only one internal line is assumed in this example, and it has the following parameters:

- Internal Line #1: $L_{B1} = 20\,\text{m}$; $h_{B1} = 0.5\,\text{m}$; $a_{B1} = 0.01\,\text{m}$; $R_{L1} = 50\,\Omega$

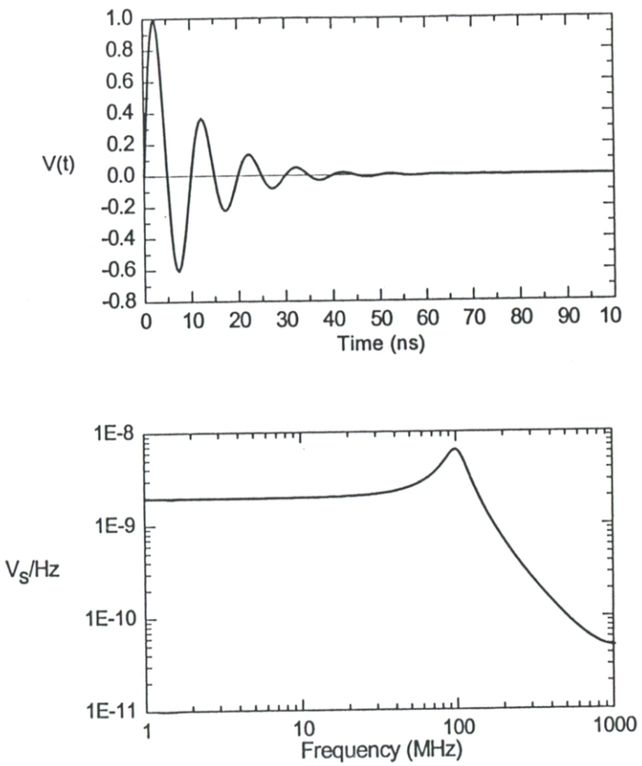

Figure 12. The assumed excitation voltage for the sample ground-based system: (a - top) The transient response; (b - bottom) The spectral magnitude

For simplicity, we will assume that the lightning excitation is represented by a damped sinusoidal waveform of the form

$$V_s(t) = V_o \Gamma\left[e^{-\alpha t}\sin(2\pi f_o t)\right], \tag{3}$$

with assumed parameters $V_o = 1\,\text{V}$, $\alpha = 0.1\ \text{ns}^{-1}$, $f_o = 100\,\text{MHz}$, and Γ is chosen so that the peak value of $V_s(t)$ is equal to V_o. This waveform is not typical of a lightning-induced surge; it has been selected only to illustrate sample system responses. A plot of the time-dependent source voltage is illustrated in Figure 12a.

The frequency-domain spectrum of this sinusoid is broadband, as noted in Figure 12b, with a peak occurring at the carrier frequency of 100 MHz. This requires that we conduct an analysis that is also broadband, in order to adequately characterize the response of the system to this excitation.

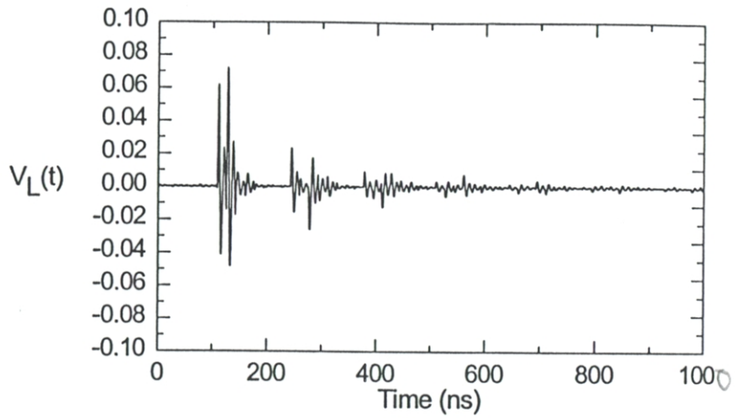

Figure 13. A plot of the transient load voltage response at the end of the internal line. reflections cause ringing.

Using the transmission-line network model, the transient load voltage can be computed. This is accomplished by calculating the response of the model at the many different frequencies contained in the excitation spectrum and then performing an inverse Fourier transform. The resulting load voltage at the end of the internal line is illustrated in Figure 13. This response has several interesting features, including

- a finite time delay of approximately 100 ns before the first response is seen
- oscillatory behavior of the voltage at a frequency characteristic of the excitation function
- multiple wave packets in the response due to ringing on the transmission-line network, and
- an eventual decay of the response due to losses in the system.

From this waveform, we may calculate the values of selected signal norms. The values of the maximum and minimum voltage norms, and the energy norm, are

$$V_{\max} = 0.072\,\text{V},\ V_{\min} = -0.048\,\text{V}, \text{ and Energy} = 0.87 \times 10^{-12}\ \text{Joules}.$$

The response spectrum is similar to the excitation; however, it has many system resonances, as illustrated in Figure 14. We see that the overall shape of the response is similar to that of the excitation. However, the effects of the different system resonances are clearly illustrated.

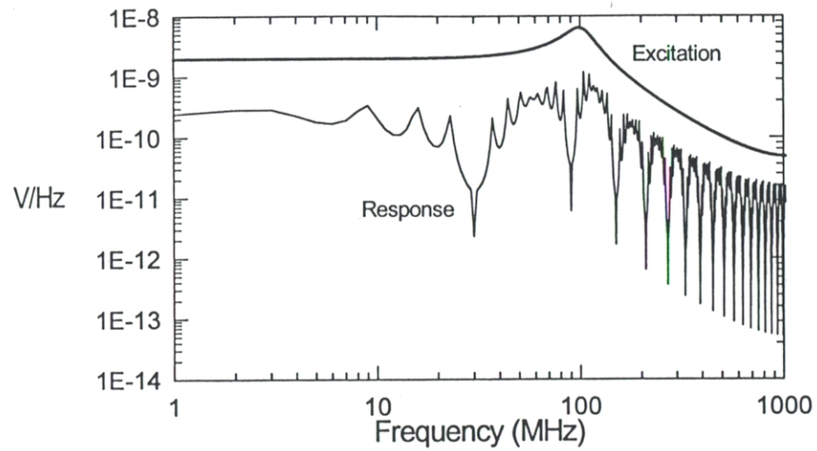

Figure 14. The spectral magnitudes of the excitation and voltage-response waveforms for the ground-based system example.

Using the definition discussed earlier, the elasticities for the minimum voltage, the maximum voltage, and the energy norms have been calculated. Figure 15 illustrates the relative values of these elasticities for each of the parameters describing the model. Along the x axis of this chart, the various system parameters are listed. For example, the first parameter is the length of the exterior power line, L_1. For each parameter, there are three columns, or bars, representing the elasticities for the three norms.

From this chart, we see that the lengths of the transmission lines in this problem, L_1, L_2, and L_{B1}, are the most important parameters in determining the normalized responses. The parameter h_2, which is the average height of the coaxial

weather-head line, is seen to be unimportant, because its elasticity is so small. This implies that in gathering data to represent such a system, the line lengths should be determined accurately, but considerable errors could be tolerated in some of the other parameters.

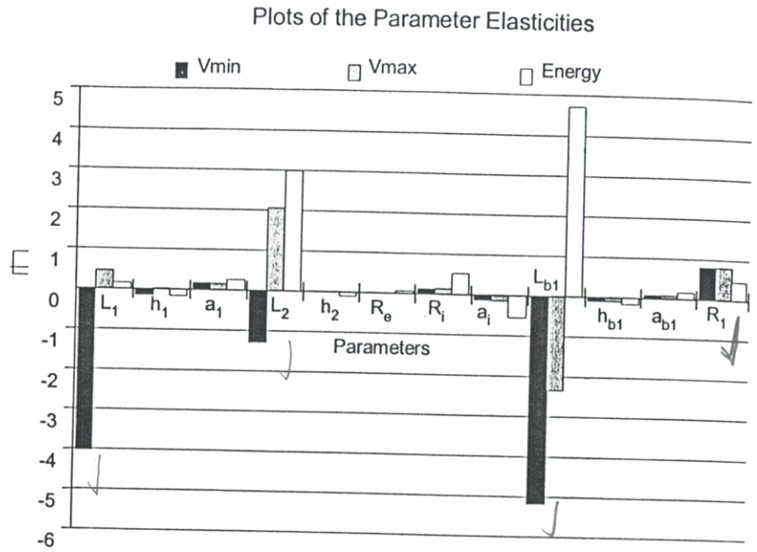

Figure 15. A plot of the calculated elasticities for the maximum and minimum voltage and energy norms.

Figure 16 illustrates the waveform deviations computed for the load voltage response, assuming a 1% change in the length of the external power line L_1, and a 1% change in the parameter h_2. Notice that the change in L_1 causes a much larger waveform deviation then does the corresponding change in h_2. This is consistent with the results from the elasticities in the previous figure.

To illustrate the statistical responses of this network, a Monte Carlo calculation using a computer-simulation program has been performed. For this calculation, a total of 2^{14} individual cases have been considered, each having random variations in the model parameters. Each parameter in the problem was assumed to be described by a Gaussian distribution, having a standard deviation of 10% of the nominal mean value of the parameter. Of course, in a real problem we expect that such standard deviations will be much smaller for the parameters, and that these deviations will not all have the same value.

These Monte Carlo simulations are relatively expensive in terms of computer time, due to the requirement that a large number of individual calculations be

performed. This particular simulation required a total of 6.8 hours on a 60 MHz Pentium computer. Figure 17 illustrates the calculated probability density function for the energy norm for the load response. Notice that this response is not smooth–a typical feature of a Monte Carlo simulation.

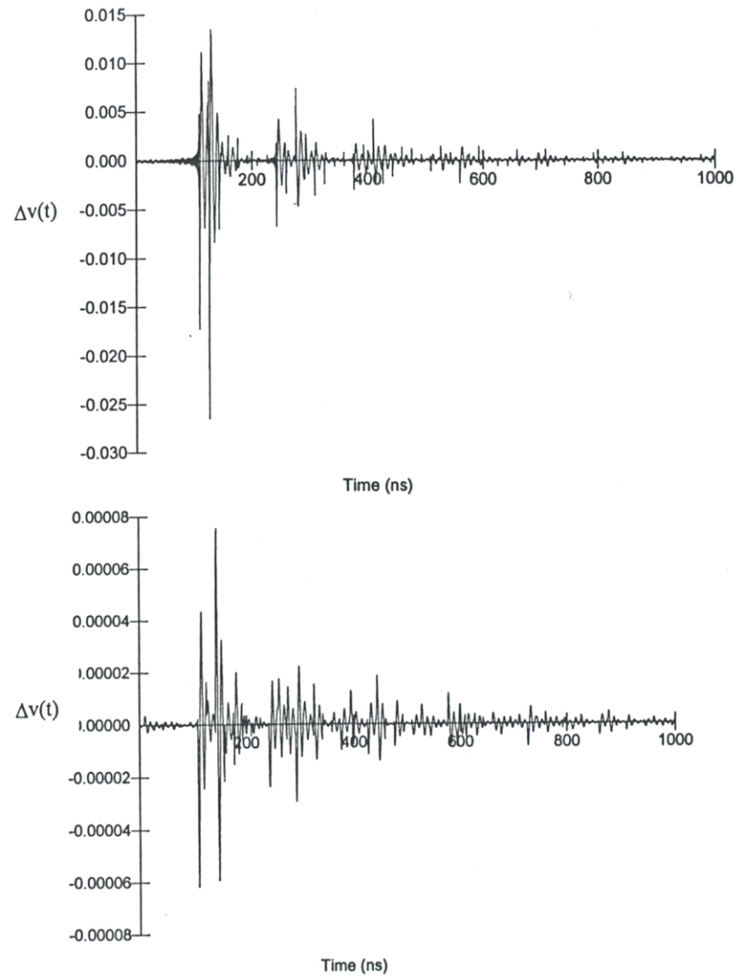

Figure 16. The waveform deviations of the voltage response for a 1% change of a model parameter: (a - top) For a 1% change in L_1; (b - bottom) For a 1% change in h_2.

The complementary cumulative probability distribution for the energy norm, as calculated from the previous probability density function, is presented in Figure 18. This curve represents the probability of the energy norm exceeding the

value specified along the x axis. Such curves are very useful for characterizing the global response of the system.

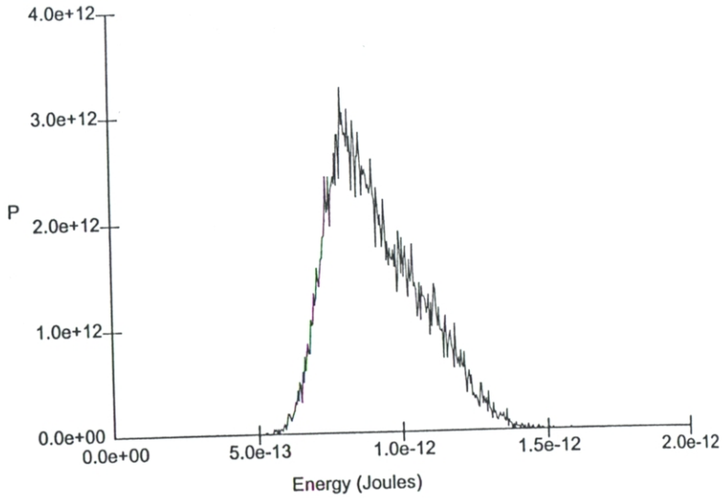

Figure 17. A plot of the PDF for the energy norm for the load response.

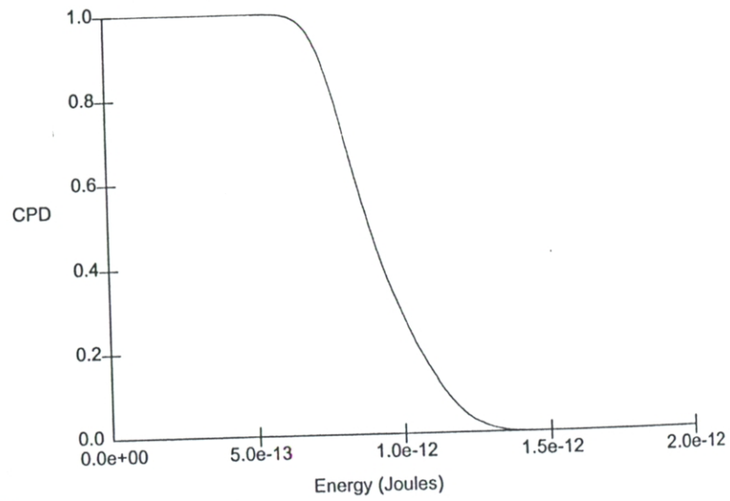

Figure 18. A plot of the complementary cumulative probability distribution for the energy norm for the load response.

5. Summary

This report has discussed the need for EMC modeling, and has provided an overview of the modeling process. We have introduced the concept of the electromagnetic topology, and have illustrated how it allows us to develop models of the system based on Maxwell's equations and appropriate simplifications. This results in a distributed-circuit representation of the system, for which a numerical simulation of the system response can be obtained.

Using this modeling approach, we have examined a sample ground-based system, and have illustrated typical responses that can be obtained from the models. We wish to stress that system-level models should be used in a way that permit the global understanding of the system behavior. That is to say, instead of calculating just one response at a single point, the models should be used to understand the importance of various system parameters (by using response elasticities), by computing response-waveform deviations, or by performing Monte Carlo simulations to develop a statistical view of the system behavior.

6. References

C. E. Baum [1986], "Electromagnetic Topology for the Analysis and Design of Complex Electromagnetic Systems," in I. E. Thompson, L. H. Luessem, Martinus Nijhoff, and Dordrecht (eds.), *Fast Electrical and Optical Measurements, Volume 1*, pp. 467-547.

C. E. Baum [1974], "How to Think About EMP Interaction," *Proceedings of the 1974 Spring FULMEN Meeting*, Kirtland AFB, New Mexico.

C. E. Baum [1979], "Norms and Eigenvector Norms," *AFWL Mathematics Notes*, Note 63, Kirtland AFB, New Mexico.

J. M. Carter and W. L. Curtis [1974], "Common Mode Model Development for Complex Cable Systems," Boeing Company report, AFWL-TR-74-60.

P. A. Chatterton and M. A. Houlden [1991], *EMC: Electromagnetic Theory to Practical Design*, New York, John Wiley and Sons.

P. Degauque and J. Hamelin (eds.) [1993], *Electromagnetic Compatibility*, Oxford, Oxford University Press (also in French).

J. J. Goedbloed [1992], *Electromagnetic Compatibility*, New York, Prentice Hall.

W. R. Graham and T. C. Mo [1978], "Probability Distribution of CW Induced currents on Randomly Oriented Subresonant Loops and Wires," *IEEE Transactions on Antennas and Propagation*, **AP-26**, 1, pp. 107-117.

In a perfect dielectric (e.g. free space) $\rightsquigarrow \sigma = 0 \rightarrow \delta_s = \infty$

in a perfect conductor ($\sigma = \infty$) $\rightarrow \delta_s = 0$

(Insulations have to be many skin depths thick!!)

when $\frac{\varepsilon''}{\varepsilon'} \ll 1$ ($< 10^{-2}$) $\rightsquigarrow$ low-loss dielectric

---

Low-loss dielectric ($\varepsilon''/\varepsilon' < 10^{-2}$)

$\alpha = \partial \simeq \frac{\omega \varepsilon''}{2} \sqrt{\frac{\mu}{\varepsilon'}} = \frac{\sigma}{2} \sqrt{\frac{\mu}{\varepsilon}}$ → not fxn. of freq. (Np/m) attenuation: $e^{-\alpha z}$ $e^{-\alpha \ell}$ Np

$\beta \simeq \omega \sqrt{\mu \varepsilon'} = \omega \sqrt{\mu \varepsilon}$ (rad/m) consider attenuation + crosstalk when placing chips on board.

$\eta_c \simeq \sqrt{\frac{\mu}{\varepsilon}}$ (Real) phase = 0 → low-loss dielectric

$u_p = \omega / \beta$ (m/sec)

$\lambda = 2\pi/\beta = u_p / f$ (m)

when $\frac{\varepsilon''}{\varepsilon'} \gg 1$ ($> 10^2$) $\rightsquigarrow$ good conductor

---

$\partial = \sqrt{\pi f \mu \sigma} \sim \sqrt{f}$ (Np/m) attenuation increases w/ freq.

$\beta = \sqrt{\pi f \mu \sigma}$ (rad/m)

$\eta_c = (1+j) \frac{\partial}{\sigma}$ (Ω) phase = 45° → good conductor (complex number $\angle 45°$)

$u_p = \sqrt{4\pi f / \mu \sigma} \sim \sqrt{f}$ (m/sec) faster frequency components of a signal travel at different velocities → dispersion

$\lambda = u_p / f \neq \frac{\omega}{\beta}$ (m)

when $\frac{\varepsilon''}{\varepsilon'} \in [10^{-2}, 10^2] \Rightarrow$ quasi-conductor

---

Use formulas of (4)

Power Density

Poynting Vector: $\bar{S} = \bar{E} \times \bar{H}$ (W/m^2)

Average Power Density: $\tilde{S}_{av} = \frac{1}{2} Re[\tilde{E} \times \tilde{H}^*]$ (W/m^2)

Lossless Medium: $\tilde{S}_{av} = \hat{z} \frac{|\tilde{E}|^2}{2\eta}$ (for $+\hat{z}$ propag. wave)

Lossy Medium: $\tilde{S}_{av} = \hat{z} \frac{|E_0|^2}{2|\eta_c|} e^{-2\alpha z}$ cosθ_n

$= \hat{z} \frac{|E|^2}{2\eta} (e^{-\alpha z})^2$

$(\eta_c = |\eta_c| e^{j\theta_n})$

$|E_0|^2$ = magnitude of $\tilde{E}(z)$ at $z=0$

At $z = \delta_s = 1/\alpha$ (δ_s: skin depth), $e^{-\alpha \frac{1}{\alpha}} = e^{-1} \Rightarrow$ attenuation of power $e^{-2} \approx 14\%$

Decibels

α [db] $= 20 \log\left(\frac{E_1}{E_{20}}\right) = 10 \log\left(\frac{P_1}{P_{20}}\right)$

$E_0, S_0 \xrightarrow{\ell} E, S$ ↓ ↓ ↑

$E = E_0 e^{-\alpha z} \rightarrow 20 \log e^{-\alpha z}$

$S = S_0 e^{-2\alpha z} \rightarrow 10 \log e^{-2\alpha z} = 20 \log e^{-\alpha z}$

Example

Seawater: $\varepsilon_r = 80$, $\mu_r = 1$, $\sigma = 4$ S/m, $f = 1$kHz

At $z=0$: $\bar{H}(0,t) = \hat{y}\, 100 \cos(2\pi \times 10^3 t + 15°)$ mA/m

and propagates $\rightarrow +\hat{z}$ $\bar{H}(z,t) = \hat{y}\, 100 e^{-\alpha z} \cos(2\pi f t - \beta z + 15°)$

$(\tilde{E} = -\eta_c \hat{u} \times \tilde{H}) \Rightarrow \tilde{E}(z) = \hat{x} E_{x0} e^{-\alpha z} e^{-j\beta z}$

$\tilde{H}(z) = \hat{y} \frac{E_{x0}}{\eta_c} e^{-\alpha z} e^{-j\beta z}$

$\omega = 2\pi \times 10^3 \Rightarrow \omega = 2\pi f \Rightarrow f = 10^3$ Hz $= 1$kHz

$\frac{\varepsilon''}{\varepsilon'} = \frac{\sigma}{\omega \varepsilon} = \frac{\sigma}{\omega \varepsilon_{r2} \varepsilon_0} = \frac{4}{2\pi \times 10^3 \times 80 \times 10^{-9}/36\pi} = 9 \times 10^5 > 10^2$

Use lower freq. so less attenuation. $\Rightarrow$ good conductor

$$\alpha = \sqrt{\pi f \mu \sigma} = \sqrt{\pi \cdot 10^3 \cdot 4\pi 10^{-7} \cdot 4} = 0.126 \text{ Np/m}$$

$$\beta = \sqrt{\pi f \mu \sigma} = 0.126 \text{ rad/m}$$

$$\eta_c = (1+j)\frac{\alpha}{\sigma} = 0.044 e^{j\pi/4} \quad (\Omega)$$

$$\bar{E}(z,t) = \mathrm{Re}\left[\hat{x}\, |E_{x0}| e^{j\phi_0} e^{-\alpha z} e^{-j\beta z} e^{j\omega t}\right]$$

$$= \hat{x}\, |E_{x0}| e^{-0.126 z} \cos(2\pi \times 10^3 t - 0.126 z + \phi_0) \quad (\text{V/m})$$

$$\bar{H}(z,t) = \mathrm{Re}\left[\hat{y}\, \frac{|E_{x0}| e^{j\phi_0}}{0.044 e^{j\pi/4}} e^{-\alpha z} e^{-j\beta z} e^{j\omega t}\right]$$

$$= \hat{y}\, 22.5\, |E_{x0}| e^{-0.126 z} \cos(2\pi \times 10^3 t - 0.126 z + \phi_0 - 45°) \quad \text{A/m}$$

At $z = 0 \Rightarrow \bar{H}(0,t) = \hat{y}\, 22.5\, |E_{x0}| \cos(\ldots)$

$$= \hat{y}\, 100 \cos(\ldots)$$

$$|E_{x0}| = 4.44 \text{ mV/m}$$

$$\phi_0 - 45° = 15° \Rightarrow \phi_0 = 60°$$

$$\bar{E}(z,t) = \hat{x}\, 4.44 e^{-0.126 z} \cos(2\pi 10^3 t - 0.126 z + 60°) \quad (\text{mV/m})$$

$$\bar{H}(z,t) = \hat{y}\, 100 e^{-0.126 z} \cos(2\pi 10^3 t - 0.126 z + 15°) \quad (\text{mA/m})$$

$$\eta_c = 0.044 \angle 45° \quad (\Omega)$$

$$\tilde{S}_{av}(z) = \hat{z}\, \frac{|E_0|^2}{2|\eta_c|} e^{-2\alpha z} \cos\theta_\eta =$$

$$= \hat{z}\, \frac{(4.44 \times 10^{-3})^2}{2 \times 0.044} e^{-0.252 z} \cos 45°$$

$$= \hat{z}\, 0.16 e^{-0.252 z} \quad (\text{mW/m}^2)$$