THEORETICAL CONSIDERATIONS REGARDING ASSESSMENT OF HEMP AND IEMI UPSET OF DIGITAL SYSTEMS

I. Kohlberg[(1)], R. Boling[(2)], R. Gardner[(3)], and C. Ropiak[(4)]

[(1)] Institute for Defense Analyses, 4850 Mark Center Drive, Alexandria VA 22311 USA, ikohlber@ida.org
[(2)]As above, but E-mail RBoling@ida.org
[(3)] Consultant, 6152 Manchester Park Circle, Alexandria, VA 22310 USA, Robert.L.Gardner@verizon.net
[(4)]Envisioneering Inc., 4485 Danube Drive, King George, VA 22485, CRopiak@earthlink.net

ABSTRACT
This paper discusses the major analytical techniques and processes for assessing the response and upset of complex digital systems to the high-altitude electromagnetic pulse (HEMP) and to wideband pulsed Intentional Electromagnetic Interference (IEMI). We focus on electronic or communication information systems in a building containing computer network(s) with power cables and interconnecting data cables. External power and data cables enter the interior region that contains the system as well. The digital systems are considered to have a unit subsystem of a pair of electronic systems that store and process information connected by some communications channel such as a data bus.

INTRODUCTION
In this paper, we address the question: "Is it possible to render *approximate yet meaningful* assessments of failure and/or upset of digital communication systems caused by Intentional Electromagnetic Interference (IEMI) and the Electromagnetic Pulse generated by a single High Altitude Nuclear Detonations (HEMP)?" We demonstrate that such assessments are possible by showing how traditional assessments are used in conjunction with new approaches that include the role of bit errors in digital communication systems **[1]**. The connection between HEMP and pulsed IEMI is established by functionally equating HEMP with the first pulse in a low PRF IEMI pulse train.

INTERIOR ELECTROMAGNETIC FIELDS
Tesche has summarized the three ways an electromagnetic wave can penetrate through the external shield into a system **[2]**: (1) "hard-wire penetration formed by wires, cables, or other conductors", (2) "aperture penetrations through holes or other openings in the shield", and (3) "field diffusion through the shield material". Assessing the penetration of electromagnetic waves through windows, unintentional apertures, and walls is tractable because there are typically but a few apertures such as windows in a room or building, and electromagnetic propagation theory through apertures is known, as is the propagation of electromagnetic waves through walls **[3,4]**. Using the principal of stationary phase, and the minimum phase theory **[4],** we can get fairly good estimates of a wave after it passes through a wall from the measured attenuation as a function of frequency. Other methods for estimating the interior electromagnetic field are ray theory and diffraction theory. Although computationally intensive, these topics are well treated theoretically and numerically in the cited references.

APERTURES
Two canonical aperture problems are: (1) the case where the aperture is located in a perfectly conducting surface**,** and (2) the case where the aperture is located in a perfectly absorbing surface. In both cases the aperture is modeled by the rectangle with sides "a" and "b". The distance beyond which the far-field approximation applies from the center of the aperture is approximately $r^{(D)} \geq (2ab/\lambda)$, where λ is the wavelength.

PROPAGATION THROUGH WALLS
The time dependent electric field passing through a wall of thickness, *L*, is **[3]**

$$E^{(t)}(L,t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} E_{inc}(z=0,\omega)\exp\big(-\alpha(\omega)L\big)\exp\big(-j\beta(\omega)L\big)\exp(j\omega t)d\omega\,, \qquad (1)$$

where *z* is the direction of propagation, $\alpha(\omega)$ and $\beta(\omega)$ are material dependent functions, and $E_{inc}(z=0,\omega)$ is the Fourier transform of the incident field at $z = 0$.

MULTIPLE SCATTERING AND DIFFRACTION

The multiple scattering model is shown in **Figure 1**. We have shown **[3]** that multiple scattering can increase the rms value by the following multiple scattering enhancement factor: $F = (1-q^{n+1})/(1-q)$. Here q is an average reflection coefficient and n is the number of reflections. The foregoing formula can be used to bound the effect of multiple scattering.

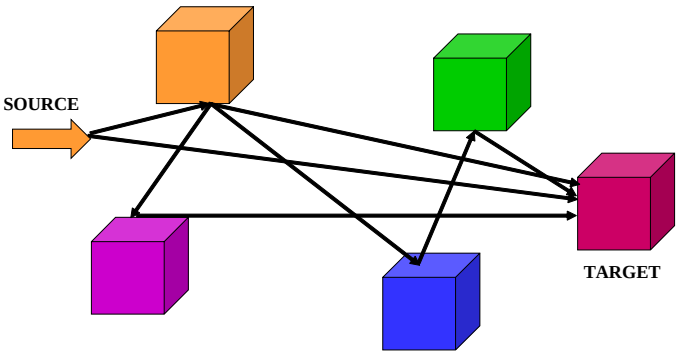

Figure 1. Multiple Scattering

The multiple scattering model just presented is based on geometric optics (ray theory). However, scattering is only one way that unwanted signals may be reinforced at equipment surfaces. Diffraction can also play a role, as shown in **Figure 2**. The equations that describe the fields are actually useful because they permit estimates to be made on the kinds of surfaces typical of rooms in office buildings. For example a typical diffraction field is of the form

$$E(r,t) = \frac{\exp(j\frac{\pi}{4})}{\pi^{1/2}} \int_{-\infty}^{+\infty} E_{inc}(\omega)[\exp(j\omega(t-(r/c))]Q(\omega))d\omega, \qquad (2)$$

where $E_{inc}(\omega)$ is the incident field and $Q(\omega)$ is geometry dependent.

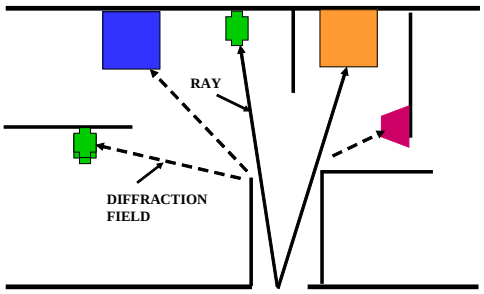

Figure 2. Diffraction

The frequency dependence of a diffracted signal could be quite different from the incident wave, which may be composed of signals that undergo multiple diffraction events. The key points are: diffraction can affect equipment not predicted by geometric optics; frequency content of diffracted fields may be different from the primary signal and become compounded with successive diffractions; time stretching of a signal could be long.

INTERFERING FIELD AND BIT ERRORS

We use a data bus model as an example for this discussion. Bit errors are caused by unwanted electromagnetic fields that get picked up by the bus. The error voltage at the input to the processor is $V_e(t)$. A critical question is: "Under what conditions can a single unwanted pulse, having the capability to cause bit errors, lead to upset or system error?" Let the duration of $V_e(t)$ be T_d, and start at $t = 0$.

We now connect $V_e(t)$ to the probability of bit error, P_e. We assume that the bits are either a 0 or 1, and that the system voltage is +*A* for the 1 and –*A* for the 0. The duration of the i^{th} bit extends from time t_i to $t_i + T_b$, where T_b is the duration of a bit. We note that there are two probabilities of bit errors: $P(0|1)$, the probability of a 0 being detected, given that a 1 was transmitted, and $P(1|0)$, the probability of a 1 being detected, given that a 1 was sent.

The communication systems that we are considering are assumed to be tolerant to bit errors defined by the following criteria:

$$P_{\max}^{\Delta T}(0|1) \geq P_i(0|1); \quad P_{\max}^{\Delta T}(1|0) \geq P_i(1|0); \quad t_i \leq t \leq t_i + \Delta T \qquad (3)$$

The terms in the foregoing equation have the following meanings: the P_i terms are the bit error probabilities due to the unwanted voltage $V_e(t)$ in the time interval $t_i \leq t \leq t_i + \Delta T$, and the $P_{\max}^{\Delta T}$ terms are the maximum probabilities of bit error that the system can tolerate in time $\Delta T >> T_b$.

Fundamentally, we recognize that the system in question is capable of tolerating bit error probabilities less than or equal to the $P_{\max}^{\Delta T}$ values for times less than or equal to ΔT. The maximum number of bits that could be affected in a single pulse lasting T_d seconds is $N_d = (T_d / T_b)$. Communication systems that are designed to withstand electrical surges such as lightning are example of systems that satisfy equation (3).

Determining whether or not a particular digital communication system is affected by a single pulse boils down to whether the P_i terms satisfy the conditions of equation (3). This is a problem in statistical decision theory. The decision as to whether the i^{th} bit is a 1 or 0 is a functional, $\Theta(X_i(t))$, of the signal

$$X_i(t) = \pm A + V_e(t); \quad (i-1)T_b < t \leq iT_b \qquad (4)$$

We need to know the mathematical operations embedded in the functional $\Theta(X_i(t))$ in order to calculate the P_i terms. If all the P_i's satisfy equation (3) for $T_d \leq \Delta T$, we assert, subject to the usual statistical conditions, that the system is tolerant to the pulse. For all other conditions a more detailed account of the probabilities of bit error and their consequences for all bits in time T_d is required.

MITIGATION OF BIT ERRORS

We ask "*Are coding techniques available that provide almost error-free communication in the presence of unwanted signals such as HEMP*"? The answer is YES, we can encode signals that will completely mitigate the effects of unwanted electromagnetic signals on a wide class of waveforms and communication networks. Error mitigation strategies concede the ability of interference to cause errors in the transmitted bit stream. Message coding minimizes the result of such bit errors, or even makes them irrelevant to the success of the data transfer. However, this immunity comes with a cost in transmission bandwidth and/or time, and in transceiver complexity, and an increase in background noise due to the increased bandwidth.

Our model consists of pairs of two nodes in a data bus system that can transmit messages between themselves. These nodes accept information in the form of a stream of bits, transmit data, acknowledge receipt of messages, detect bit errors, take corrective action, and then send appropriate information in the form of a stream of bits to each other or other parts of the network. Messages are composed of words. A word is collection of bits. Bit errors can occur in any part of the word: synchronization bits, data bits, or parity check bit. Bits associated with coding and error-correction techniques do not add to the information content of a message, but are used to ensure its correctness.

Digital data communication is almost always executed in n-bit blocks of data. For generality, we consider a continuous stream of information bits translated into a series of symbols (blocks, or words) for transmission. Coding for error mitigation may be considered to be an algorithmic method to add redundant bits to a block to aid in detecting and correcting errors in digital communication. If every block code in a chosen set differs in three or more bits from every other coded block in the set, a single-bit error will not cause an incorrect block decision at the detector, because the disrupted block is still most like the "correct" block than any other. Formally, the measure of the bit-wise difference

between two coded blocks is known as the Hamming distance, d_H. It can be shown **[5]** that a coding scheme that produces blocks with a minimum difference, or distance, of $d_{H,\min}$ can correct up to q errors, where $q = (d_{H,\min} - 1)/2$. Further, it is known **[6]** that, for any positive integers m and q (where $m = n - k$, and n is the block size in bits, and k is the number of information bits in the block), a code exists that can correct q errors with $n = 2^m - 1, \quad k \geq n - mt$, and $d_{H,\min} \geq 2t + 1$

To go beyond the simple 1-bit error per word, we will consider two alternate approaches: a more complex block code, and a clever bit-interleaving technique. A subset of block codes (BCH) can tolerate up to 25 percent of erroneous bits (in any position in the block) without error. As may be expected with any error-correcting code, the effective information rate suffers.

The basic interleaving technique, developed to deal with fading communications channels, assembles a set of message words into a larger block for transmission. The interleaving arrangement for **r** words is shown in **Figure 3**. In this arrangement, a large "hit" only takes out a very few bits from each original word, and those words are individually encoded to withstand those few errors. The disassembly of the received bit stream is done on the receiving end prior to decoding.

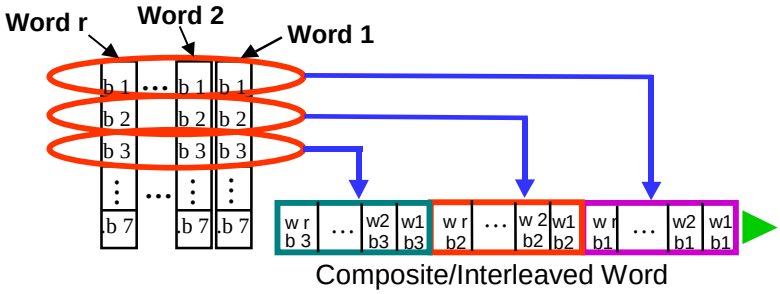

Figure 3. Composite interleaved word

These error mitigation techniques against unwanted signals will have the greatest impact when the information systems have a surplus of unused bandwidth, and may easily accommodate the higher bit rate required to maintain the same (un-encoded) information rate.

CONCLUSIONS AND RECOMMENDATIONS

An integrated system of analytical techniques and theoretical approaches is developed for assessing IEMP and HEMP effects that include role of bit errors in digital communication systems. To our knowledge this bit error feature has not been considered before. Previous approaches have stopped short of taking the last step of connecting the unwanted voltage signals to breakdown in communications.

REFERENCES

[1] I. Kohlberg and R. L. Gardner, "Functional and Communication Theory Models in Susceptibility Analysis", Conference Paper, IEEE-APS/URSI International Symposium, Columbus, Ohio, June 23-27, 2003

[2] F.M. Tesche, "Modeling Techniques for EMC Analysis," *Review of Radio Science 1996–1999*, Oxford Science Publications, Oxford University Press, 1999.

[3] P. Pauli and D. Moldari, Reduction and Shielding of RF and Microwaves, Printed by Druckerie Hugelschaffer GmbH, D-97360 Mainbernheim, Germany, May 2000

[4] A. Papoulis, The Fourier Integral and its Applications, Reissue 1987, McGraw-Hill, New York, 1987

[5] D.J. Torrieri, *Principles of Secure Communication Systems*, Norwood, MA: Artech House Publishers, p. 36, 1985.

[6] Edward Lee and David Messerschmitt, *Digital Communication*, Kluwer Academic Publishers, Boston p. 478, 1988