System Design and Assessment Notes

Note 38

29 November 2008

A Model for Transient Upset

Carl E. Baum
University of New Mexico
Department of Electrical and Computer Engineering
Albuquerque New Mexico 87131

Abstract

Pulsed electromagnetic environments can upset digital circuits causing disruption and failure to accomplish mission. If the circuits are vulnerable only certain time windows, then one needs to know the probability that the environment causes upset, for both single and multiple exposures, provided that the environment is strong enough for upset.

`

This work was sponsored in part by the Air Force Office of Scientific Research.

1. Introduction

Intentional electromagnetic interference (IEMI) can take various forms from various types of EM weapons [3-5]. Suppose one is trying to upset the electronics (e.g., a computer), and one knows that the environment he is producing is strong enough to produce an upset, provided the exposure occurs in some time-window, Δt. For simplicity, let the temporal duration of the environment (or at least the relevant part) be short compared to Δt. Then one would like to know the probability that one can produce an upset with some number N of environmental pulses, spaced in time somewhat larger than Δt.

One can consider that there are some number M of possible upset modes that the environment can upset. The probability of system upset may depend on one or more upsets in various combinations. This complicates the matter considerably.

2. Single Upset Mode

The simplest case (used at the HPE 201 short course) has an upset mode where the environment must appear in a time window of width t_1 (susceptibility window) at a random time as far as the attacker knows. Suppose this time window recurs at an average time spacing t_1. Then the probability of effect (system failure) from a single pulse is

$$P_1 = \Delta_1 = \frac{t_1}{T_1} \tag{2.1}$$

which may typically be small compared to unity. This is the probability that one pulse cases upset.

Well, what happens after N such pulses? Two susceptibility windows are assumed not to overlap. Otherwise they occur at random times with respect to each other. For one pulse nonupset has probability $1-\Delta_1$. After two pulses this is $\left[1-\Delta_1\right]^2$. After N pulses nonupset has probability $\left[1-\Delta_1\right]^N$, or a probability of at least one upset as

$$P_N = 1 - \left[1-\Delta_1\right]^N = 1-\left[1-P_1\right]^N \tag{2.2}$$

If Δ_1 is sufficiently small we have

$$\begin{aligned} P_1 &= \Delta_1 \simeq 1-e^{-\Delta_1} = 1-e^{-P_1} \\ P_N &\simeq 1-e^{-N\Delta_1} = 1-e^{-NP_1} \end{aligned} \tag{2.3}$$

Turning this around, we have

$$\begin{aligned} N &= \frac{\ell n\left(1-P_N\right)}{\ell n\left(1-P_1\right)} \qquad \text{(for small } \Delta_1 = P_1\text{)} \\ &\simeq \frac{\ell n\left(1-P_N\right)}{P_1} \qquad \text{(for small } P_1\text{)} \end{aligned} \tag{2.4}$$

If we want a particular probability of upset we can solve for N given Δ_1.

As an example, we might have

$$\begin{aligned} \Delta_1 &= 0.01 \quad , \quad P_N = 0.9 \\ N &\simeq 229 \end{aligned} \tag{2.5}$$

This shows the necessity for many pulses (repetitive pulsing).

3. Dual Upset Mode

Suppose that there are two upset modes, and that the environment is sufficiently large to cause each of these to upset. These two failure modes may exist in two different circuits with vulnerability time windows t_1 and t_2, which we assume to occur each with random average time spacings T_1 and T_2, respectively. Then we have

$$\Delta_n = \frac{t_n}{T_n} \text{ (both small)} \tag{3.1}$$

Now suppose that upsetting either circuit is sufficient to cause system upset. Then a single pulse causes an upset with probability

$$P_1 = \Delta_1 + \Delta_2 \tag{3.2}$$

After N such pulses we replace Δ_1 by $\Delta_1 + \Delta_2$ in the formulas in Section 2 as

$$
\begin{aligned}
P_N &= 1\left[1-\Delta_1 - \Delta_2\right]^N = 1 - \left[1 - P_1\right]^N \\
&\simeq 1 - e^{-NP_1} \\
N &= \frac{\ell n\left(1-P_N\right)}{\ell n\left(1-P_N\right)} \\
&\simeq -\frac{\ell n\left(1-P_N\right)}{P_1}
\end{aligned}
\tag{3.3}
$$

As an example we might have

$$
\begin{aligned}
&\Delta_1 = 0.005\,,\ \Delta_2 = 0.02\,,\ P_1 = 0.025\,,\ P_N = 0.9 \\
&N \simeq 92
\end{aligned}
\tag{3.4}
$$

As one might expect the more such vulnerable circuits there are, the fewer pulses that are required for system upset.

Generalizing this result we can define

$$
\Delta = \sum_{m=1}^{M} \Delta_M \tag{3.5}
$$

for M such venerability windows. Then we can replace Δ_1 by Δ in Section 2. Of course, we expect Δ to be larger than the Δ_n. However, for Δ near (or even greater than) 1.0, the foregoing formulas do not apply since the time windows for upset begin to overlap.

4. Simultaneous Upset Requirement

Suppose now, by our design of the computer logic, it takes two circuits to be simultaneously upset (within a time short compared to the T_n) to cause a system upset. Essentially a certain amount of redundancy is incorporated in the design. Then for a single pulse to trigger a system upset requires that the environment occur simultaneously in all the relevant circuits in the same time window.

For two such vulnerability windows then the probability of the simultaneous environmental stimulus is just

$$
P_1 = \Delta_1\Delta_2 \tag{4.1}
$$

For M such simultaneous upsets we have

$$P_1 = \prod_{m=1}^{M} \Delta_m \tag{4.2}$$

This formula can also be substituted in the formulae in Section 2.

As an example we might have

$$\begin{aligned} M &= 2\,,\ \Delta_1 = 0.0052\,,\ \Delta_2 = 0.02\,,\ P_1 = 10^{-4}\,,\ P_N = 0.9 \\ N &\simeq 2.3\left(10^4\right) \end{aligned} \tag{4.3}$$

or 23 kilopulses. As one increases M (the number of circuits required for simultaneous upset) N can become quite large.

This suggests a hardening technique based on redundancy. As long as the circuits can reset before the next environmental pulse arrives, increasing the number of such circuits greatly reduces the vulnerability.

5. Extension

One can envision much more complicated scenarios for system upset based on simultaneous upset of various circuits. For example, one might have groups of circuits. In each group it may take only one circuit upset, but require that every group be upset, for system upset. Then each group can be considered as a single circuit for computing probability of upset for that group. Then the formulae in Section 4 apply.

6. Concluding Remarks

The real problem can be even more complicated. Time windows can be long, and even overlap. Some windows may be time correlated to each other. Given a different model, a new probability can be computed.

Of course, different circuits may require different environmental levels, and even different polarizations, for maximum effect, to cause upset. So we need to have a sufficiently strong environment to allow for such differences. Even environmental waveforms are optimally different, in general, for each circuit vulnerability, due to the various resonant frequencies with which one may be concerned [1, 2].

Another hardening technique, circumvention, can also be used. Detecting an upset, the system can temporarily be shut down (cease computation) and then be reset (and restart computation).

As a final note, if the interfering environment is strong enough, permanent damage of some particular necessary component (subsystem, etc.) may occur, causing system failure. This can occur if there are insufficient shielding, filters, limiters, etc.

References

1. C. E. Baum, “Maximization of Electromagnetic Response at a Distance”, IEEE Trans. EMC, 1992, pp. 148-153; also Sensor and Simulation Note 312, October 1988.

2. C. E. Baum, “A Time-Domain View of Choice of Transient Waveforms for Enhanced Response of Electronic Systems”, Proc. ICEAA 01, Torino, Italy, pp. 181-184, also Interaction Note 560, September 2000.

3. W. D. Prather, C. E. Baum, R. J. Torres, F. Sabath, and D. Nitsch, “Survey of Worldwide High-Power Wideband Capabilities”, IEEE Trans. EMC, 2004, pp. 335-344.

4. C. D. Taylor and D. V. Giri, *High-Power Microwave Systems and Effects*, Taylor & Francis, 1994.

5. D. V. Giri, *High-Power Electromagnetic Radiators*, Harvard U. Press, 2004.