REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
01-09-2011

2. REPORT TYPE
Technical Paper

3. DATES COVERED *(From - To)*
Oct 2010-Sept 2011

4. TITLE AND SUBTITLE

Predictive Modeling of High-Power Electromagnetic Effects on Electronics (POSTPRINT)

5a. CONTRACT NUMBER
In House

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Timothy Clarke, Aaron Taylor, Nicholas Estep, Susumu Yakura, David Brumit

David Dietz, Sameer Hemmady, James Duffey

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
D04X

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory
3550 Aberdeen Avenue SE
Kirtland AFB, NM 87117-5776

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory
3550 Aberdeen Avenue SE
Kirtland AFB, NM 87117-5776

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RDHE

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-RD-PS-TP-2013-0006

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES
377ABW-2011-0820; 6/8/2011
International Conference on Electromagnetics and Advanced Applications Conference (ICEAA 2011)
Presented on 07/03/2011
Government Purpose Rights

14. ABSTRACT
The ability to understand and predict the effects on electronic systems that might result from an intentional EMI attack is of great importance in defending critical electronic systems against such a threat. In this paper we focus on predicting the response of a microcontroller to a high-power electromagnetic waveform. We will describe our approach and present results from experimental investigations as well as modeling of the response of different microcontrollers to direct injection of an RF signal into clock and signal lines. In addition, we will discuss how these results may be extended to the case of free-field illumination. Finally, we will describe how our results shed light on the broader problem of predicting the response of a general digital system to a high-power electromagnetic waveform.

15. SUBJECT TERMS
EMI, electromagnetic effects

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
					Timothy Clarke
a. REPORT	b. ABSTRACT	c. THIS PAGE	SAR	4	19b. TELEPHONE NUMBER *(include area code)*
UNCLASS	UNCLASS	UNCLASS			505-846-9107

Predictive Modeling of High-Power Electromagnetic Effects on Electronics

Timothy Clarke[1] Aaron Taylor[1] Nicholas Estep[1] Susumu Yakura[1]
David Brumit[1] David Dietz[2] Sameer Hemmady[3] James Duffey[4]

Abstract **– The ability to understand and predict the effects on electronic systems that might result from an intentional EMI attack is of great importance in defending critical electronic systems against such a threat. In this paper we focus on predicting the response of a microcontroller to a high-power electromagnetic waveform. We will describe our approach and present results from experimental investigations as well as modeling of the response of different microcontrollers to direct injection of an RF signal into clock and signal lines. In addition, we will discuss how these results may be extended to the case of free-field illumination. Finally, we will describe how our results shed light on the broader problem of predicting the response of a general digital system to a high-power electromagnetic waveform.**

1 INTRODUCTION

The question of how digital electronic systems are affected by incident radio-frequency (RF) energy is crucial to predicting the survivability of such systems in an extreme RF environment, or in the event of an IEMI attack. It is well known that high power electromagnetic (HPEM) pulses at sufficiently high field levels can cause physical damage to electronics. This effect can be explained in terms of the energy deposited on a circuit trace or component, resulting in destructive thermal effects. At lower field levels, where no actual physical damage is caused, an HPEM pulse can still cause data corruption resulting in the system locking up or rebooting itself, an effect we will refer to generically as upset.

Understanding and predicting upset is much more difficult than damage, since it involves not only characterizing the RF propagation to the system and entry into the interior by penetration through seams and coupling to external cables, but also describing the complex mode structure that is established in cavities as well as how the resulting electromagnetic fields couple to wires, circuit traces and components. In addition, it involves characterizing the rectification that occurs as the RF pulse interacts with nonlinear circuit elements, and how the rectified signal interferes with data flow within a single integrated circuit (IC), and, finally, understanding how a large number of such IC-level effects may combine to determine the behavior of the digital system as a whole. Some parts of this problem are relatively well-understood, while significant gaps in our understanding still remain for other portions such as those associated with the circuit response.

This paper addresses what is probably the most critical gap in our understanding of effects on digital electronics: predicting the response of a particular IC or collection of ICs to an RF pulse with a specified waveform. The work described here focuses on a microcontroller: this represents an ideal target for our investigation of RF effects, since it is intermediate in complexity between a single transistor or gate and a full digital system such as a PC. In section 2 we introduce our approach, while in section 3 we describe our experimental procedure. In section 4 we show the results of our experiments on two microcontrollers. Finally, in section 5 we discuss our conclusions.

2 APPROACH

Our approach is motivated by an earlier German study into the immunity of digital electronics to transient pulses ([1], [2]). This work investigated how a burst of 50ns electrical transient pulses affected a simple 8-bit 80C51 microcontroller, while it performed a single assembler instruction repeatedly. For this specific model of microcontroller, characteristic of early 8051 designs, a single assembler instruction is built up from 24 micro-instructions, associated with rising or falling edges of consecutive clock pulses. By controlling the timing of the incident pulses precisely to make them coincide with specific micro-instructions, they were able to develop an empirical susceptibility probability for each, and hence predict the susceptibility for the entire assembler instruction by aggregating these probabilities.

Our work adopts a similar approach, but in our case we are interested in exploring the effect of RF pulses on the microcontroller, rather than transient spikes. In addition, our objective is not simply to build an

[1] AFRL/RDHE, 3550 Aberdeen Avenue SE, Kirtland AFB, NM 87117, USA, email: clarketj@ieee.org, tel: +1 505 846 9107
[2] Department of Electrical and Computer Engineering, University of New Mexico, Albuquerque, NM 87131, USA
[3] TechFlow, Inc., 2155 Louisiana Blvd. NE, Suite 3200, Albuquerque, NM 87110, USA
[4] Science Applications International Corporation, 2109 Air Park Road, S.E., Albuquerque, NM 87106, USA

empirical model describing the probability of upset for specific instructions, but rather to develop a basic understanding of how an RF pulse interacts with the microcontroller to cause an upset. Our approach is to expose the microcontroller to RF pulses with carefully controlled onset times and durations, while making use of software implemented in assembly language to exercise various functional areas and hence various physical regions of the microcontroller, with the aim of developing fundamental insight into the upset mechanism. Our ultimate goal is to build predictive models for the probability of upset as a function of the RF waveform parameters. As a starting point, we have developed an initial probabilistic model to describe the effect of the RF signal on the operation of the microcontroller, with the intent of refining this model as we collect more experimental data.

3 EXPERIMENTAL PROCEDURE

Our experimental approach was to mount the microcontroller on an evaluation board, both for ease of programming and to provide convenient connections for RF injection. We made use of an HP8116A pulse/function generator (figure 1) to generate an external clock signal for the microcontroller and to trigger a DG535 digital delay pulse generator. The pulse generator was configured to generate a specific number of square wave pulses, with a logic low at 0 volts and logic high at 5 volts, at a repetition frequency of 1 MHz.

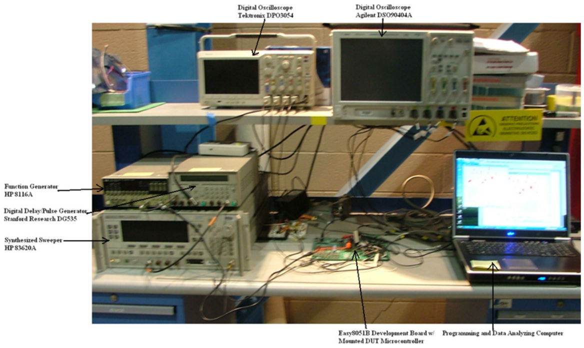

Figure 1: Experimental setup for microcontroller susceptibility investigation

The DG535 was used to trigger the oscilloscope for data collection, and to control the initiation time and duration of the RF pulse. The RF waveform itself was generated by an HP83620A Synthesized Sweeper as a CW signal with a frequency of 50 MHz and with a user-specified amplitude. The RF output signal was directly coupled into the microcontroller XTAL1 signal line, along with the external clock signal from the function generator. The microcontroller was programmed in assembly language to execute a simple binary counter, and we monitored the output of this counter to establish whether an upset had occurred.

Our set of experiments was designed to explore the susceptibility of the microcontroller as a function of the duration of the RF pulse and its onset time relative to the clock pulse. The nine combinations of onset time and duration (jointly referred to as test locations) are shown in figure 2. These locations include the leading and trailing edges of the clock pulse, as well as the logic high and logic low portions. Note that these test locations are not all mutually exclusive: for example, location 1 can be built up in various ways as a combination of other locations.

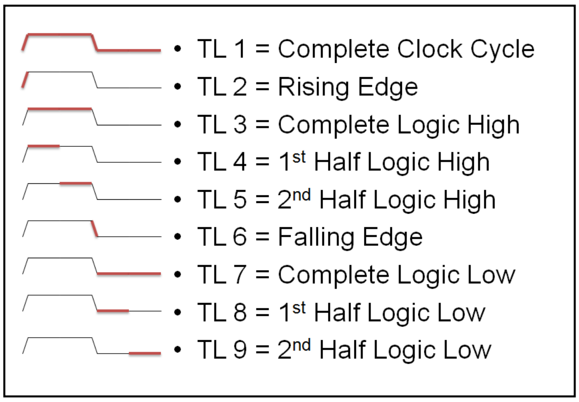

Figure 2: Locations of RF pulses relative to clock cycle

For each location, we performed the RF injection at a set of voltages ranging approximately from 0.5 to 5 volts, and recorded the response of the microcontroller. Specifically, we monitored the output of the counter, and documented whether or not the RF pulse resulted in an upset. At each voltage we repeated the experiment a specified number of times, and made use of a Bayesian approach to convert the binary data (effect/no effect) into a continuous probability of effect curve. We then summarized the curve for each location by the voltage associated with a 50% probability of upset, together with a 95% confidence interval (strictly a Bayesian credible interval).

4 RESULTS

We repeated the same set of experiments for two nominally identical LP2052 microcontrollers. Figure 3 shows our results, with the voltage corresponding to a 50% probability of upset identified for each microcontroller, together with the 95% confidence interval (vertical line). The ellipses are used to group together the results for the two microcontrollers for a specific test location. For two test locations the 50% points are displayed as zero voltage: these correspond to cases where the maximum RF voltage injected was insufficient to cause any upset.

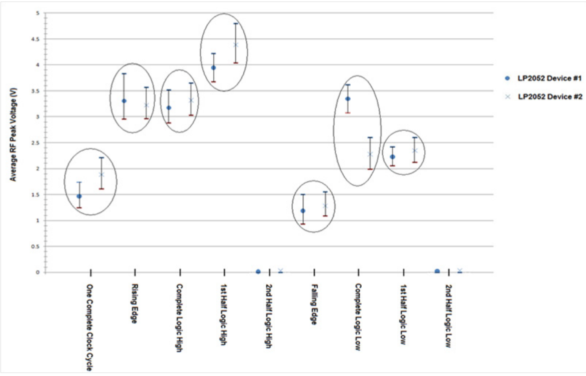

Figure 3: Results of experiments on two identical microcontrollers, showing voltage associated with a 50% probability of effect for the locations shown in figure 2.

5 CONCLUSIONS

The results shown in section 4 indicate that there are significant differences between the susceptibility levels for the various portions of the particular instruction being executed during this study. In particular, the lowest susceptibility level was associated with the trailing edge of the clock pulse, while the second half of the clock pulse was least susceptible, both for the logic high and the logic low states. Moreover, with one exception (test location 7) our results for the two instances of the same microcontroller are consistent, supporting the idea that the differences in susceptibility between locations are associated with fundamental aspects of the microcontroller functionality. Our initial analysis shows that these results are generally consistent with the model we have developed, but more analysis and additional experiments are required to fully characterize the behavior of the microcontroller, as well as to validate and refine our model. Future work will involve investigating the susceptibility of other instructions and other injection sites, as well as extending our approach to the case of free-field illumination.

Acknowledgments

The work described was supported in part by the Air Force Office of Scientific Research.

References

[1] R. Vick, “The influence of hardware and software structure on the immunity of digital equipment”, Tech. Univ. Dresden, Germany, Ph.D. dissertation, 1995.

[2] S. Wendsche, R. Vick and E. Habiger, “Modeling and testing of immunity of computerized equipment to fast electrical transients”, IEEE Trans. on Electromagnetic Compatibility, Vol. 41, No. 4, 1999.