AFRL-RD-PS-
TP-2020-0005

AFRL-RD-PS-
TP-2020-0005

INTENTIONAL ELECTROMAGNETIC IRRADIATION ON A MICROCONTROLLER: REVIEW OF UPSET VARIATION WITH RESPECT TO CHIP INSTANCE

Daniel Guillette, Timothy Clarke

1 MARCH 2019

Technical Paper

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

AIR FORCE RESEARCH LABORATORY
Directed Energy Directorate
3550 Aberdeen Ave SE
AIR FORCE MATERIEL COMMAND
KIRTLAND AIR FORCE BASE, NM 87117-5776

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

Qualified requestors may obtain copies of this report from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RD-PS-TP-2020-0005 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

GUILLETTE.DANIEL.S.1404763179 Digitally signed by GUILLETTE.DANIEL.S.1404763179 Date: 2021.02.17 11:40:18 -07'00'

Daniel Guillette
Effects Dep. Tech. Advisor.
AFRL/RDHEE

HAZEL.ASHLEY.R.1106465211 Digitally signed by HAZEL.ASHLEY.R.1106465211 Date: 2021.02.19 08:55:32 -07'00'

MAJ ASHLEY HAZEL
Branch Chief
AFRL/RDHE

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Service Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01-03-2019	Technical Paper	Sept 2018 - March 2019

4. TITLE AND SUBTITLE
Intentional ElectroMagnetic Irradiation on a Microcontroller: Review of Upset Variation with Respect to Chip Instance

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Daniel Guillette, Timothy Clarke

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
D0CL

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)

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

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-RD-PS-TP-2020-0005

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. Release # AFMC-2019-0359.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
In the area of electromagnetic effects on electronics the most challenging technical problem is to understand and model the process of upset for digital systems. AFRL has chosen to study microcontrollers to act as a model for more complex systems due to their relative simplicity, ease of programming and control. Using a state-of-the-art automated testing system called SALVO, pulsed RF signals were direct-injected into the clock-line pin of a microcontroller (MCU) using careful timing. The MCU is programmed in assembly language to execute a simple binary count from 0-7, and the output of the MCU is monitored to establish whether the count has deviated beyond the nominal state, meaning an upset has occurred. A batch of 0851 architecture Atmel microcontrollers were subjected to IEMI testing to determine the variability in injected power required to induce upset.10 identical Atmel Microcontrollers were exposed to a fixed frequency EM pulse injected on the clock input at two distinct pulse durations; each time starting at a low pulse power level and increasing the power in 1 dB increments up to 20 W. The overall results reveal that the batch of MCU chips, with the expectation of M02, had extremely similar PoE values across the power range and pulse durations tested.

15. SUBJECT TERMS
Intentional Electromagnetic Irradiation, microcontrollers, upset , Effects, direct injection

16. SECURITY CLASSIFICATION OF: a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
Unclassified	Unclassified	Unclassified	SAR	17	Daniel Guillette
					19b. TELEPHONE NUMBER *(Include area code)* 505-846-0697

Reset

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18
Adobe Professional 7.0

1.0 Introduction / Experiment Purpose:

In the area of electromagnetic effects on electronics the most challenging technical problem is to understand and model the process of upset for digital systems. This is largely due to the ever increasing complexity of modern devices and their designers' aims to obfuscate software operations to improve security and/or simplify user interactions. AFRL has chosen to study microcontrollers to act as a model for more complex systems due to their relative simplicity, ease of programming and control.

Using a state-of-the-art automated testing system called SALVO, pulsed RF signals were direct-injected into the clock-line pin of a microcontroller (MCU) using careful timing. The MCU is programmed in assembly language to execute a simple binary count from 0-7, and the output of the MCU is monitored to establish whether the count has deviated beyond the nominal state, meaning an upset has occurred. Since the timing of the MCU program is well understood, an RF pulse can be injected at specific instructions and locations relative to the rise and fall of the clock signal. A batch of 0851 architecture Atmel microcontrollers were subjected to IEMI testing to determine the variability in injected power required to induce upset (referred to herein as the upset threshold.) Additionally, preliminary tests were conducted to investigate the dependence of upset threshold on pulse width by subjecting the MCU to pulses having a duration of either 25 ns or 50 ns.

2.0 Experiment, Background & Set-up

2.1 Experiment Description

This experiment is a series of direct injection single pulse electromagnetic exposure tests. The purpose of the tests is to explore the susceptibility of a 10 chip batch of Atmel AT89LP2052-20PU MCUs to pulsed EM injected on their clock input pins. Each of the 10 individual MCUs were loaded with a basic counting program written in the Assembly programing language. The instructions comprising the Assembly counting program can be viewed in Table A1 along with the corresponding time location for each instruction.

The experiment varies two aspects of the pulsed EM signal, its power level, and pulse width. The experiment was set-up to allow careful control of the timing within the experiment. For instance, the EM pulse can be delivered nearly anywhere along the clock cycle window sent to the microcontroller. Moreover, the number of clock cycles sent to the MCU and the timing of the reset pulse can also be carefully controlled.

25 shots were performed per chip at 2 unique pulse durations (25 and 50 ns) and 9 different power levels (approximately 300 mW to about 2.0 W.) Table 1 displays test sequences in the following way: Column 1 is the sequence number. Column 2 is the pulse injection location (notice it doesn't change) Column 3 is the pulse duration. Column 4 is the frequency (this too is constant). Column 5 is the desired number of shots per sequence (constant.) And finally, columns 6 and 7 which define the starting and ending power levels, which are defined in a dB scale relative to a 20 W source, where 0 dB would produce the entire 20 W. A set of measured output wattages for select power levels can be viewed in Table 2. An A_sec time of 20.060 µs was chosen because in initial tests it produced a varied upset response making it an ideal clock signal time location for further investigation.

Approved for Public Release; Distribution Unlimited.

Table 1: Testing criteria for each chip.

Seq #	A_sec	AB_sec	freq_Hz	#	dBm-i	dBm-f
1	2.0060E-05	2.50E-08	1.00E+08	25	-23	-23
2	2.0060E-05	2.50E-08	1.00E+08	25	-22	-22
3	2.0060E-05	2.50E-08	1.00E+08	25	-21	-21
4	2.0060E-05	2.50E-08	1.00E+08	25	-20	-20
5	2.0060E-05	2.50E-08	1.00E+08	25	-19	-19
6	2.0060E-05	2.50E-08	1.00E+08	25	-18	-18
7	2.0060E-05	2.50E-08	1.00E+08	25	-17	-17
8	2.0060E-05	2.50E-08	1.00E+08	25	-16	-16
9	2.0060E-05	2.50E-08	1.00E+08	25	-15	-15
10	2.0060E-05	5.00E-08	1.00E+08	25	-23	-23
11	2.0060E-05	5.00E-08	1.00E+08	25	-22	-22
12	2.0060E-05	5.00E-08	1.00E+08	25	-21	-21
13	2.0060E-05	5.00E-08	1.00E+08	25	-20	-20
14	2.0060E-05	5.00E-08	1.00E+08	25	-19	-19
15	2.0060E-05	5.00E-08	1.00E+08	25	-18	-18
16	2.0060E-05	5.00E-08	1.00E+08	25	-17	-17
17	2.0060E-05	5.00E-08	1.00E+08	25	-16	-16
18	2.0060E-05	5.00E-08	1.00E+08	25	-15	-15

Table 2: 20W Amplifier Measured Wattages

dB	-23	-22	-21	-20	-19	-18	-17	-16	-15
mW	278	350	440	550	710	890	1120	1400	1770

2.2 Experiment Set-up

To perform our experimental work we make use of a state-of-the-art automated testing system. The system – named SALVO – is built to take in a set of user defined parameters and automatically initialize and execute a series of shots, as well as to diagnose the effects and record the results. Our experimental approach is to mount the microcontroller (MCU) on a simple test board that provides convenient connections for RF injection. We use an SRS DG345 function generator to generate an external clock signal for the MCU while a DG645 digital delay pulse generator controls the triggering and timing for the experiment. The function generator is 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 1MHz. The DG645 is used to trigger the oscilloscope for data collection, and to control the initiation time and duration of the RF pulse. The RF waveform itself is generated by an HP83620A Synthesized Sweeper as a continuous wave (CW) signal with a frequency of 100 MHz and a user-specified amplitude. The RF output signal is directly coupled into the microcontroller XTAL1 signal line, along with the external clock signal from the function generator. The microcontroller is programmed in assembly language to execute a simple binary counter, and we monitor the output of this counter to establish whether an upset has occurred. Figure 2.1 shows a diagram of the equipment used in the setup as well as the flow of all relevant signals. Figure 2.2 is a photograph of the complete experimental setup, while Figure 2.3 shows an expanded view of the microcontroller mounted on the test board.

Approved for Public Release; Distribution Unlimited.

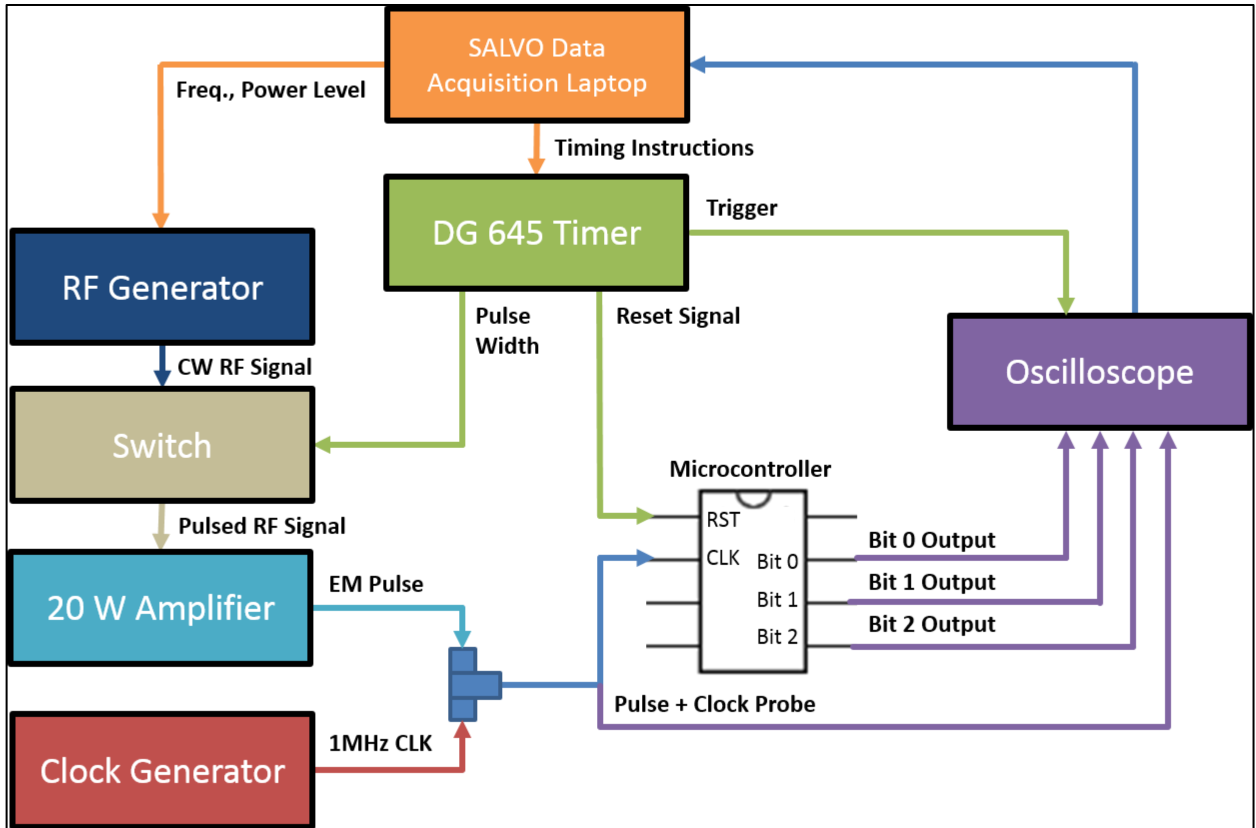

Figure 2.1: Experiment Flow Diagram.

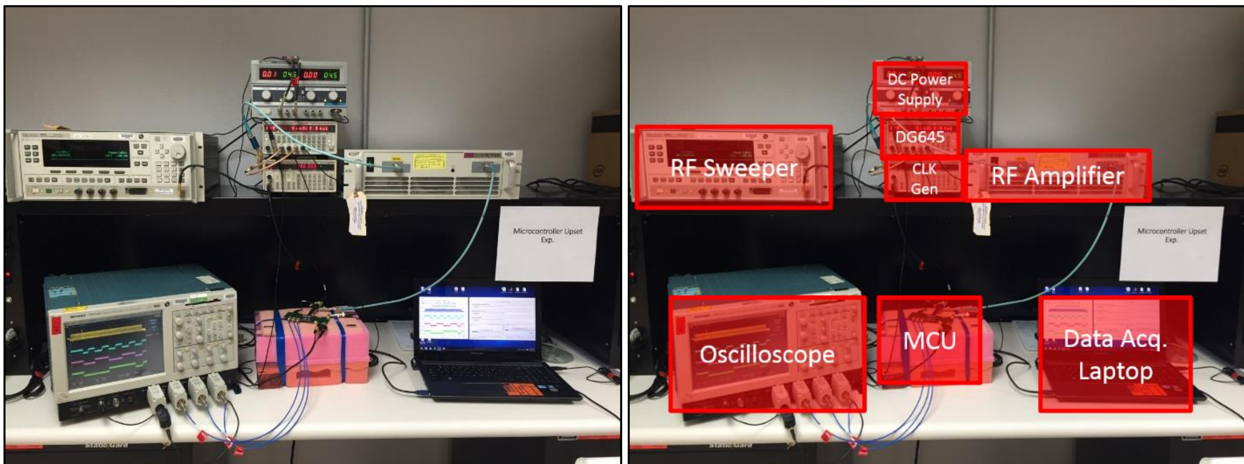

Figure 2.2: Experimental setup unlabeled (left), labelled (right)

Approved for Public Release; Distribution Unlimited.

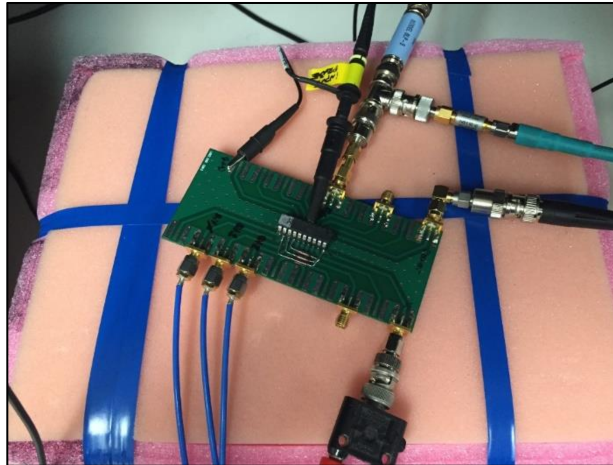

Figure 2.3: Close-up of test board with microcontroller and cables

This automated testing and data acquisition setup is controlled using an in-house developed instrument control program called SALVO, which takes in user inputs for the RF injection delay (from the start of the microcontroller operation), the RF pulse duration, the RF frequency, and the number of repetitions. Moreover, this system is designed to be able to supply two different pulses of same amplitude at any time specified along the operation window. SALVO automatically varies the RF pulse amplitudes and relevant timing parameters. An example of a user input file to the data acquisition system is shown below in Figure 2.4.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
1					Pulse 1								Pulse 2								
2	Sequence #	# Shots	Frequency Hz	Power	A Ref	A Time	B Ref	B Time	C Ref	C Time	D Ref	D Time	E Ref	E Time	F Ref	F Time	G Ref	G Time	H Ref	H Time	Notes
3	1	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	0.0000E+00	E	0.0000E+00	T0	0.0000E+00	G	9.5000E-05	AB Pulse 1
4	2	100	1.00E+08	-20	T0	0.0000E+00	A	0.0000E+00	T0	9.3000E-05	C	2.0000E-06	T0	1.5050E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	EF Pulse 2
5	3	100	1.00E+08	-20	T0	0.0000E+00	A	0.0000E+00	T0	9.3000E-05	C	2.0000E-06	T0	1.5100E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	EF Pulse 2
6	4	100	1.00E+08	-20	T0	0.0000E+00	A	0.0000E+00	T0	9.3000E-05	C	2.0000E-06	T0	1.5150E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	EF Pulse 2
7	5	100	1.00E+08	-20	T0	0.0000E+00	A	0.0000E+00	T0	9.3000E-05	C	2.0000E-06	T0	1.5200E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	EF Pulse 3
8	6	100	1.00E+08	-20	T0	0.0000E+00	A	0.0000E+00	T0	9.3000E-05	C	2.0000E-06	T0	1.5250E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	EF Pulse 4
9	7	100	1.00E+08	-20	T0	0.0000E+00	A	0.0000E+00	T0	9.3000E-05	C	2.0000E-06	T0	1.5300E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	EF Pulse 5
10	8	100	1.00E+08	-20	T0	0.0000E+00	A	0.0000E+00	T0	9.3000E-05	C	2.0000E-06	T0	1.5350E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	EF Pulse 6
11	9	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	1.5050E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	Pulse1&2
12	10	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	1.5100E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	Pulse1&2
13	11	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	1.5150E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	Pulse1&2
14	12	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	1.5200E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	Pulse1&2
15	13	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	1.5250E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	Pulse1&2
16	14	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	1.5300E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	Pulse1&2
17	15	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	1.5350E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	Pulse1&2
18	16	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	1.5400E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	Pulse1&2
19	17	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	1.5450E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	Pulse1&2
20	18	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	1.5500E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	Pulse1&2
21	19	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	1.5550E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	Pulse1&2
22	20	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	1.5600E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	Pulse1&2
23	21	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	1.5650E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	Pulse1&2
24	22	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	1.5700E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	Pulse1&2
25	23	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	1.5750E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	Pulse1&2
26	24	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	1.5800E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	Pulse1&2
27	25	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	1.5850E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	Pulse1&2
28	26	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	1.5900E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	Pulse1&2
29	27	100	1.00E+08	-20	T0	1.5000E-05	A	1.0000E-07	T0	9.3000E-05	C	2.0000E-06	T0	1.5950E-05	E	1.0000E-07	T0	0.0000E+00	G	9.5000E-05	Pulse1&2

Figure 2.4: SALVO experiment set-up file

SALVO reads all of the columns of the user defined experiment setup file and distributes the relevant information, such as Frequency, Power, # Shots or pulse timing parameters to the correct instruments via GPIB. Once all the equipment is initialized, SALVO tells the DG645 to activate. This activation signal is designated as the time t_0,

Approved for Public Release; Distribution Unlimited.

and all other timing commands are set relative to this. The DG645 then sends signals to reset the MCU, cue the oscilloscope to record, and toggle the switch. Resetting the MCU ensures that the MCU's commands take place at the same time relative to t_0. When the switch is toggled on, the Continuous Wave (CF) Radio Frequency (RF) signal is passed to the amplifier for the duration of the user set pulse width, which results in the RF pulse. The RF pulse continues onward through a bias tee and onto the clock signal line. The MCU output bit values are recorded by the oscilloscope and are then passed back to SALVO program, which saves them to a data archive on the computer.

The oscilloscope connected to the MCU, monitors the real-time state of bits 0, 1, & 2. During normal operation, the MCU will toggle the output lines between a logical HI (~5V) and a logical LOW (~0V) such that the MCU will count upwards from zero in steps of one until the MCU is reset. An example of normal operation captured by the oscilloscope can be observed in Figure 4.

The instructions programmed into the MCU are executed in sequential order, at a rate defined by the external clock. The clock frequency used in this experiment is 1 MHz; therefore, the period of this clock is 1 µs. If a consistent clock frequency is provided to the MCU, the exact time for which a specific instruction is performed can be determined. Furthermore, this ensures that the counting program instructions take place at the same relative timing location with respect to the start of the program and t_0.

2.3 Nominal Microcontroller Operation

The MCU outputs connected to the Oscilloscope monitor the real-time state of Bits 0, 1, & 2. During normal operation the MCU will toggle the output lines between a logical HI (~5V) and a logical LOW (~0V) such that the MCU will count upwards from zero in steps of one until the MCU is reset. An example of normal operation captured by the oscilloscope can be observed in Figure 2.5.

As the clock (CLK) ticks along each HI and LOW cycle, the Assembly commands programmed into the microcontroller are executed in sequential order at the rate of the input CLK. The CLK frequency used in this experiment is 1 MHz; therefore, the period of this clock is 1 µs. If a consistent clock frequency is provided to the MCU, the exact time to which an Assembly operation is performed can be determined – these values can be found at the end of this report in Table A1. Furthermore, this means that the counting program instructions take place at the same relative timing location with respect to the start of the program and t_0. The first instruction that changes the bit values takes places at the rising edge of the 16th clock signal, changing the output bits to 000. At the 21st rising edge of the clock signal, Bit 0 is changed to one, altering the overall count to 001.

Approved for Public Release; Distribution Unlimited.

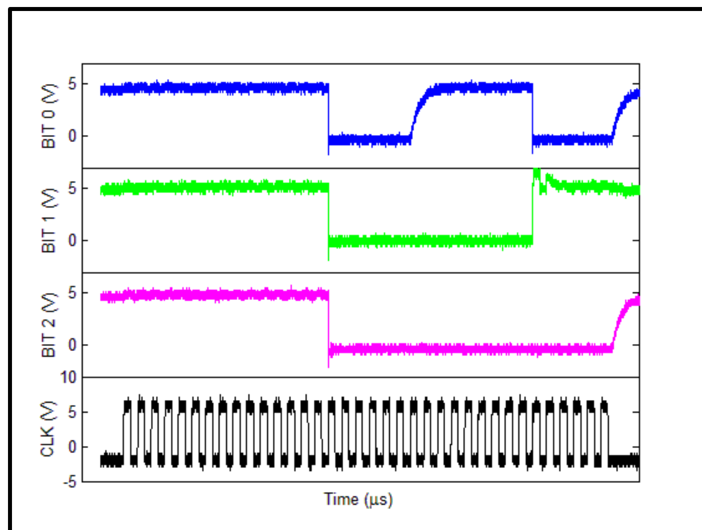

Figure 2.5: Normal MCU Operation when performing Assembly counting program.

At any given time, the counting value of the MCU can be determined by inspecting the instantaneous value of the output lines (Bits 0, 1, & 2). These bits, when ordered correctly, describe a decimal number using the binary counting method. For example:

If,

Bit 0 = 0
Bit 1 = 1
Bit 2 = 1

Then, according to the binary counting method,

*[Bit 2]*4 + [Bit 1]*2 + [Bit 0]*1 = Decimal value*
*[1]*4 + [1]*2 + [0]*1*
4 + 2 + 0,

equals six.

2.4 Upset Response

Over the years, the term upset has been used to define a broad range of observed and unobserved responses following (immediately, delayed, or otherwise) an asset's exposure to HPEM. Therefore, to determine the upset threshold of a particular asset, the criteria for upset must be clearly defined. Throughout this experiment, the MCU displayed three different responses when the pulsed RF energy was present:

Response 1: *No effect.* In this case, the output count values match the expected values, at their corresponding times, which suggest that the MCU and program are performing nominally. Figure 2.6 shows an example of the RF pulse being injected on the CLK (around 20 µs mark) and the Bit count values toggling correctly. For example the count changes properly from 000 to 001 at around the 25 µs mark.

Approved for Public Release; Distribution Unlimited.

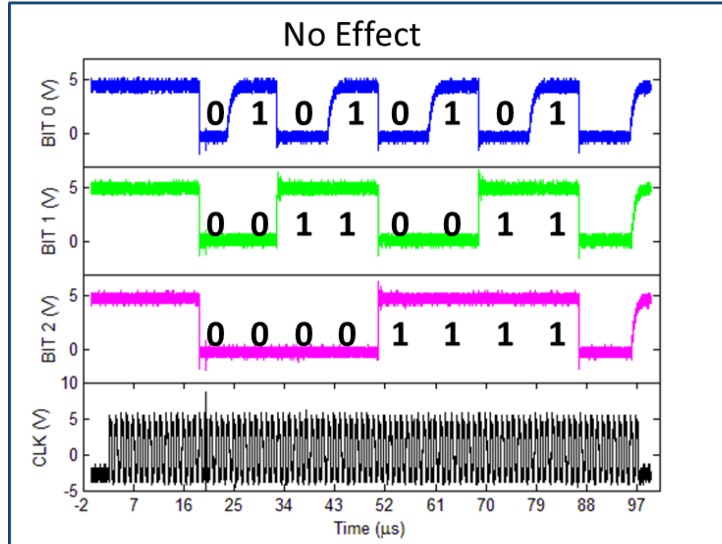

Figure 2.6: No effect example.

Response 2: *Compromised response with recovery.* In this case, the output count values do not match their expected values (red marked values) at one or more instances, but the output eventually resumes counting appearing to have self-corrected (orange marked values). Although the MCU may self-correct, the output count values are not observed at the expected times. Therefore, the system was compromised by the HPEM. Figure 3 provides an example of this response. According to Figure 2 at approximately 25 µs the expected count value is 001. However, Figure 3 doesn't produce the count value of 001 until around the 40 µs mark. After that point though, the counting program appears to count normally.

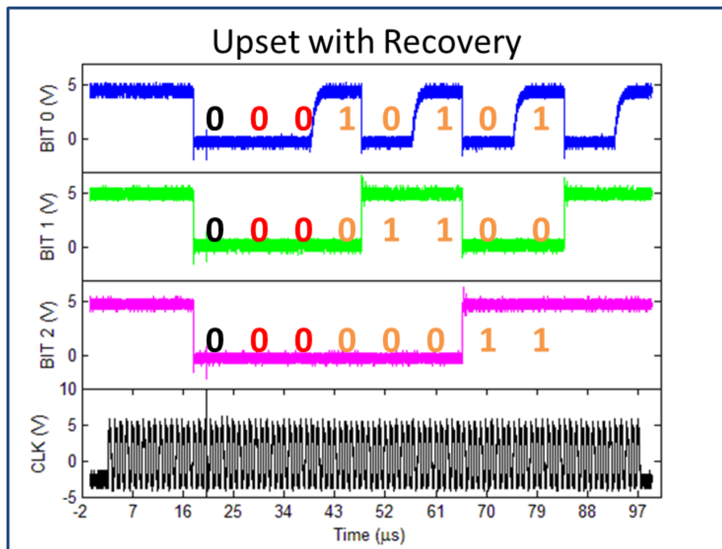

Figure 3: Upset with count recovery example.

Response 3: *Compromised response with no recovery.* In this case, all bit values are set to zero for the duration of the shot interval. This means that the system requires external support in order to restore normal operation. An example of this response can be viewed in Figure 4.

Approved for Public Release; Distribution Unlimited.

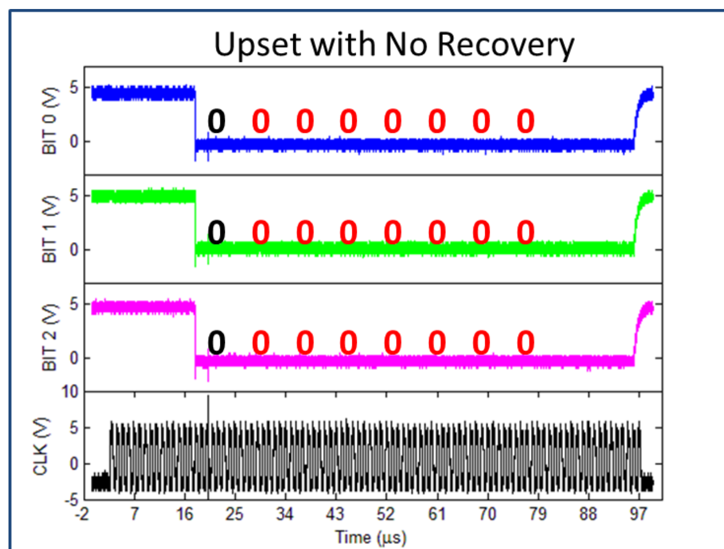

Figure 4: Upset without count recovery example.

When processing the datasets for this report, data-points resembling Response 2 or 3 were categorized as upset data. Although, there is a clear difference between Response 2 and Response 3, both suggest that the pulsed EM compromised the output bit stream. Future studies may desire to explore the nuanced difference between these two responses, but at this time they are considered to be representative of system upset and therefore the same.

2.5 Upset Threshold Calculation via Probability of Effect

Once the data for the 18 sequences and 10 chips was collected each shot was processed to determine if the bit count matched the expected bit count, if yes, the data was marked 0 (no upset); if no, then the data was marked 1 (upset). The probability of effect (PoE) was then calculated by dividing the number of shots per sequence by the number of upsets recorded in that sequence.

$$\textit{Probability of Effect} = \textit{Number of upsets} \,/\, \textit{Total number of shots} \qquad \text{(EQN.1)}$$

For example, if a sequence had a total of 25 shots and 12 of those shots were marked as upset, then the probability of effect for this sequence would be 12/25 or 0.48. The upset threshold is typically designated as a corresponding power level at which the probability of effect is approximately 50%.

3.0 Results:

3.1 Upset Response using a 25 ns Pulse Width:

Figure 5 displays the calculated PoE value for each of the 10 MCUs at a pulse duration of 25ns as a function of injected pulse power. For the most part, the 10 MCU chips, labeled M02 through M11, have similar PoE at a given power level. The overall trend suggests that the PoE increases from essentially 0 to 1 as the injected power level increases from about 0.6 to 1.4W.

Approved for Public Release; Distribution Unlimited.

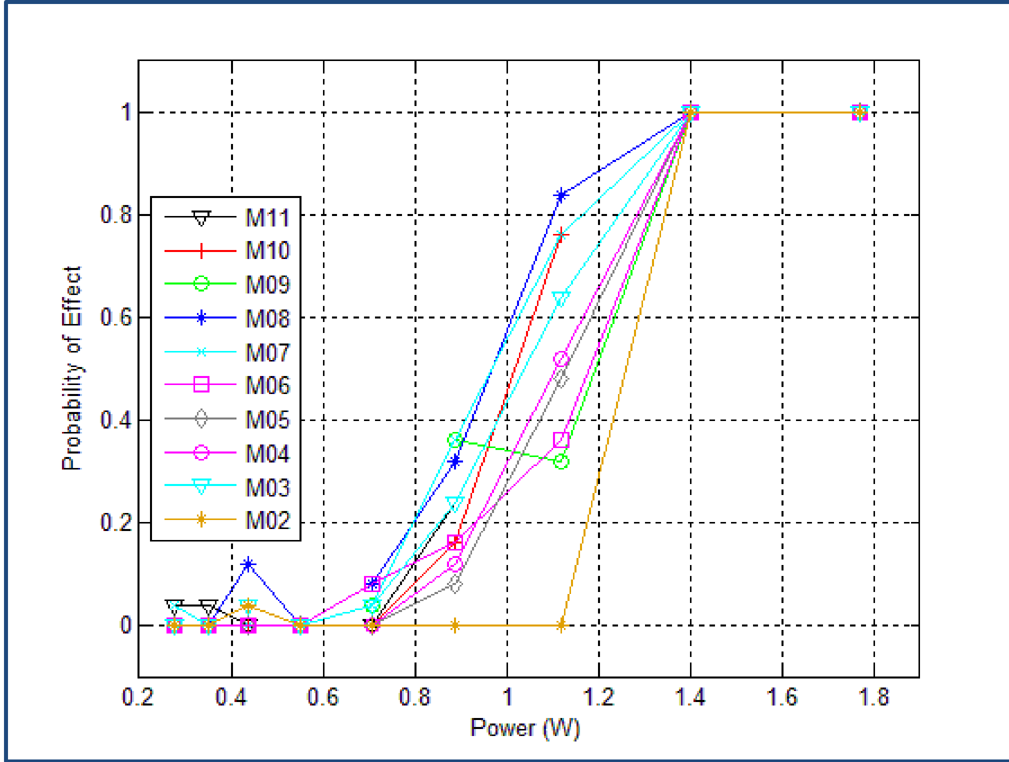

Figure 5: Probability of Effect results for MCU chips labeled M02-11 using a 25ns pulse duration.

Figure 6 presents the mean value and standard deviation of the data seen in Figure 5, which provides a clearer understanding of the overall dataset. The blue triangular markers depict the $Mean + \delta$ data, the red square markers describe the Mean, and the black circle markers describe the $Mean - \delta$ data. It can be seen in Figure 6 that, for a 50% PoE, the mean upset threshold is close to 1.1 W and the standard deviation is close to 100 mW.

The experimental data shown in Figure 5 and 6 generally resembles a sigmoid function, mathematically defined below:

$$f(x,a,c) = \frac{1}{1+e^{-a(x-c)}} \qquad \text{(Eqn. 2)}$$

where x defines the location along the curve, a defines the slope of the curve and c defines where the curve is centered on the x axis. Determining a set of correct values for a, x, and c can often be difficult. In this particular case, a brute force curve fitting method was implemented. The brute force method is characteristic of manually adjusting the values of x, a, and c until the curve matches the desired shape.

Approved for Public Release; Distribution Unlimited.

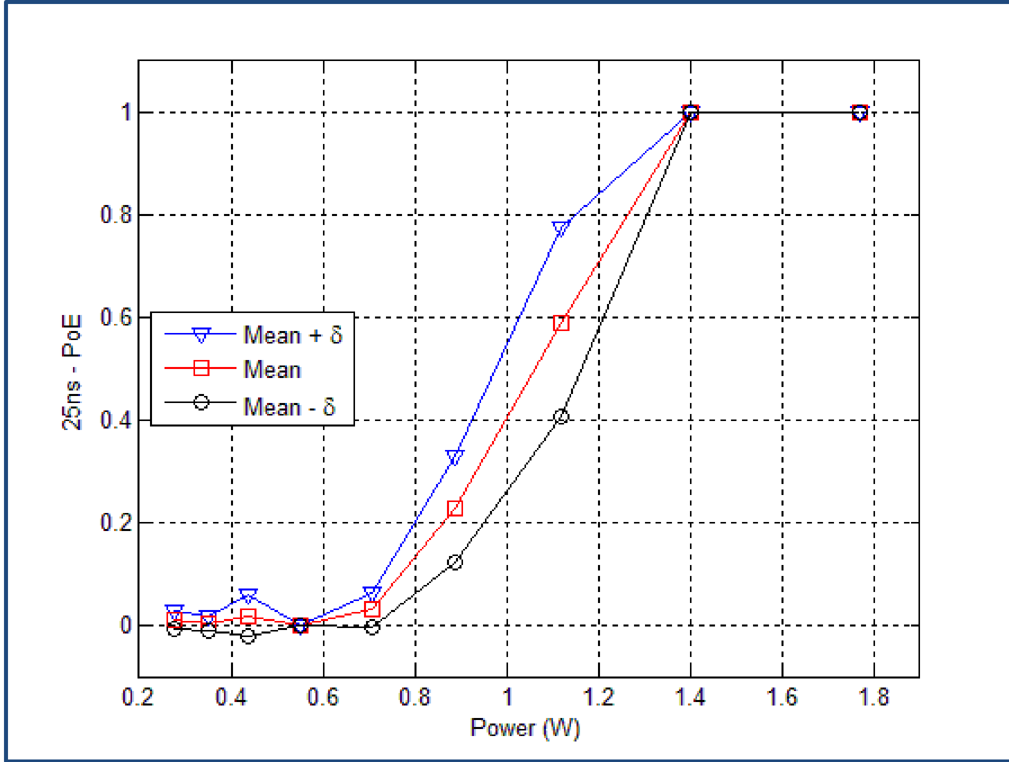

Figure 6: Mean and δ Probability of Effect results using a 25ns pulse duration.

Figure 7 presents the data points seen in Figure 6 as well as a fitted sigmoid curve for each data set. In general, the pink (top most) curve represents the blue, *Mean + δ* data. The green (middle most) curve represents the red Mean data and finally the orange (bottom most) curve represents the black *Mean - δ* data. Overall, the data fits extremely well with the sigmoid function. The values which ultimately define the curves found in Figures 7 and 10 can be found in Table 3, with *x* being a specified wattage.

Curve #	0	1	2	3	4	5
a	8.75	8.75	8.75	22	22	22
c	0.975	1.055	1.135	0.68	0.71	0.74

Table 3: Sigmoid curve variables

Now that the data has been fit to a curve, the corresponding power level for each curve at any given PoE level can be determined. Choosing the 0.5 PoE point provides the following three power levels: 0.99 W, 1.07 W, and 1.15 W. Therefore, the mean upset threshold for a 50% Probability of Effect is 1.07 W with a standard deviation of 80 mW.

Approved for Public Release; Distribution Unlimited.

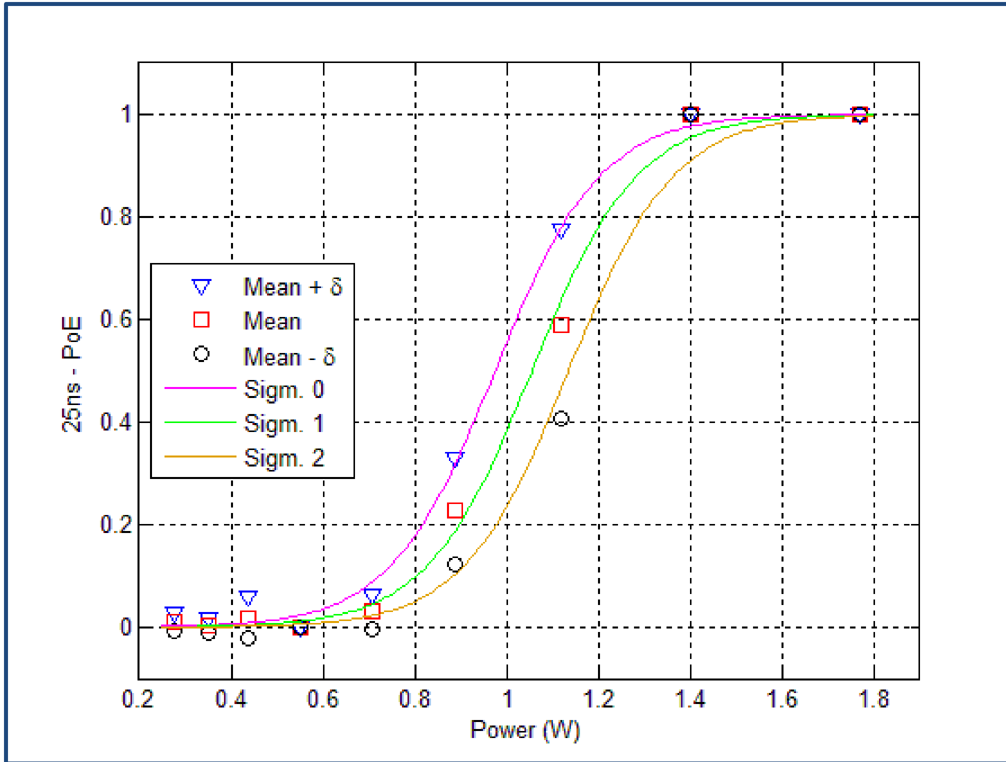

Figure 7: Sigmoid Probability of Effect curves overlaid on Figure 6 data points

3.2 Upset Response using a 50 ns Pulse Width:

Figure 8 displays the PoE value for each of the 10 MCUs at a pulse duration of 50 ns. Overall the chips have a similar PoE at nearly any given power level. M02 appears to be a clear outlier because it doesn't conform to the same trend, however the chip does eventually upset, which suggests it isn't broken.

Figure 9 presents the mean value and standard deviation of the data seen in Figure 8. The blue triangular markers depict the $Mean + \delta$ data, the red square markers describe the Mean data, and the black circle markers describe the $Mean - \delta$ data. Power levels below 0.4 W suggest that absolutely no effect will take place while power levels greater than 0.85 W suggest nearly absolute effects. In between those power levels, lie a similar sigmoid trend seen in the 25ns data set. The main observable difference, beyond the specific location of the transition region, is that the slope is much steeper. To get a clearer picture the sigmoidal response for each of the three mean curves was determined – again using a brute force method. Figure 10 presents the sigmoidal response along with the mean data sets from Figure 9.

Figure 10 presents the data points seen in Figure 6 as well as a fitted sigmoid curve for each data set. In general, the pink (top most) curve represents the blue, $Mean + \delta$ data. The green (middle most) curve represents the red Mean data and finally the orange (bottom most) curve represents the black $Mean - \delta$ data. Overall, the data fits extremely well with the sigmoid function. Inspecting the 0.5 PoE value of the three sigmoid curves, reveals the following three power levels: 0.68 W, 0.71 W, and 0.74 W. Therefore, the mean upset threshold for a 50% Probability of Effect is 0.71 W with a standard deviation of 30 mW.

Approved for Public Release; Distribution Unlimited.

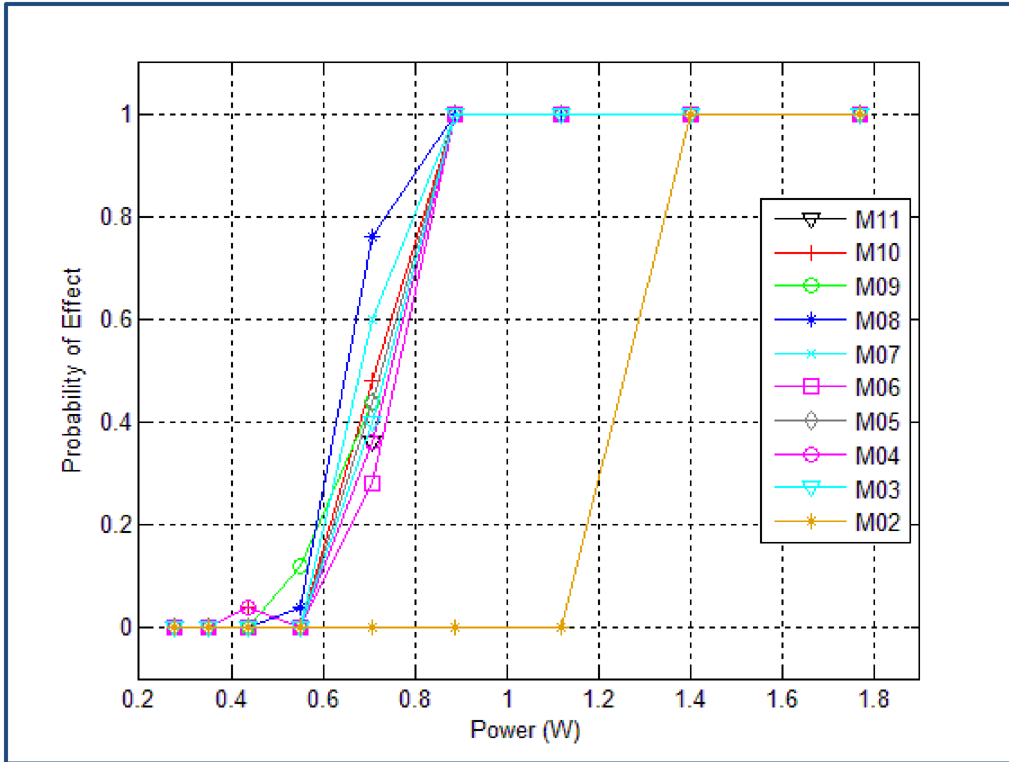

Figure 8: Probability of Effect results for MCU chips labeled M02-11 using a 50ns pulse duration.

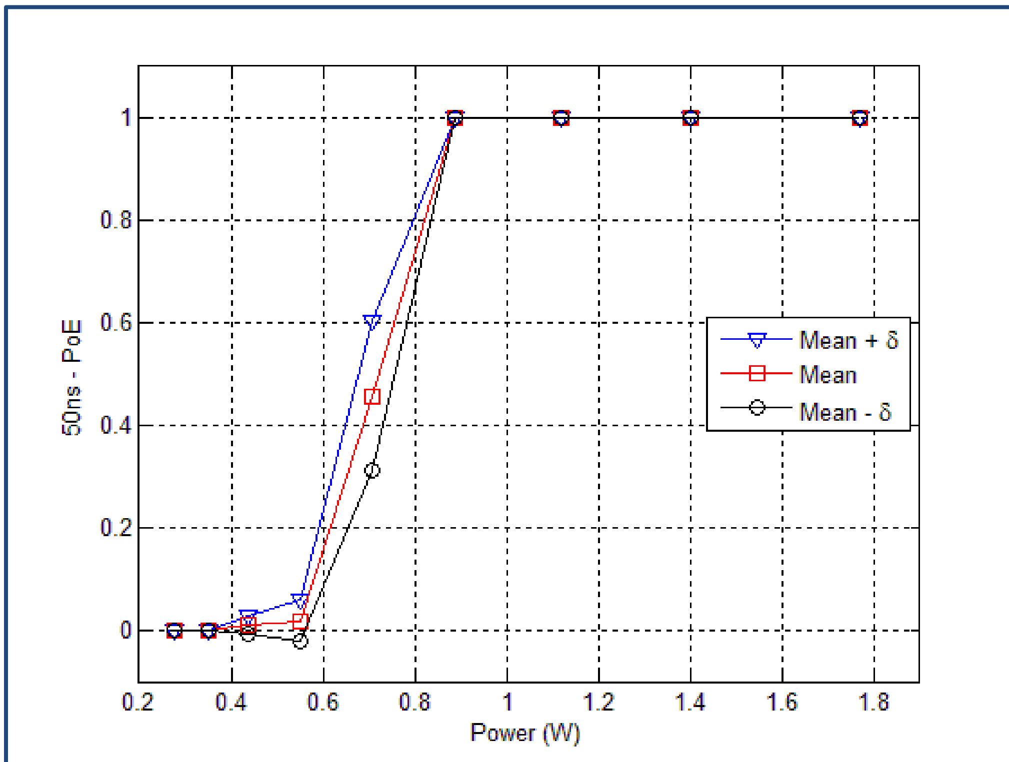

Figure 9: Mean and δ Probability of Effect results using a 50ns pulse duration.

Approved for Public Release; Distribution Unlimited.

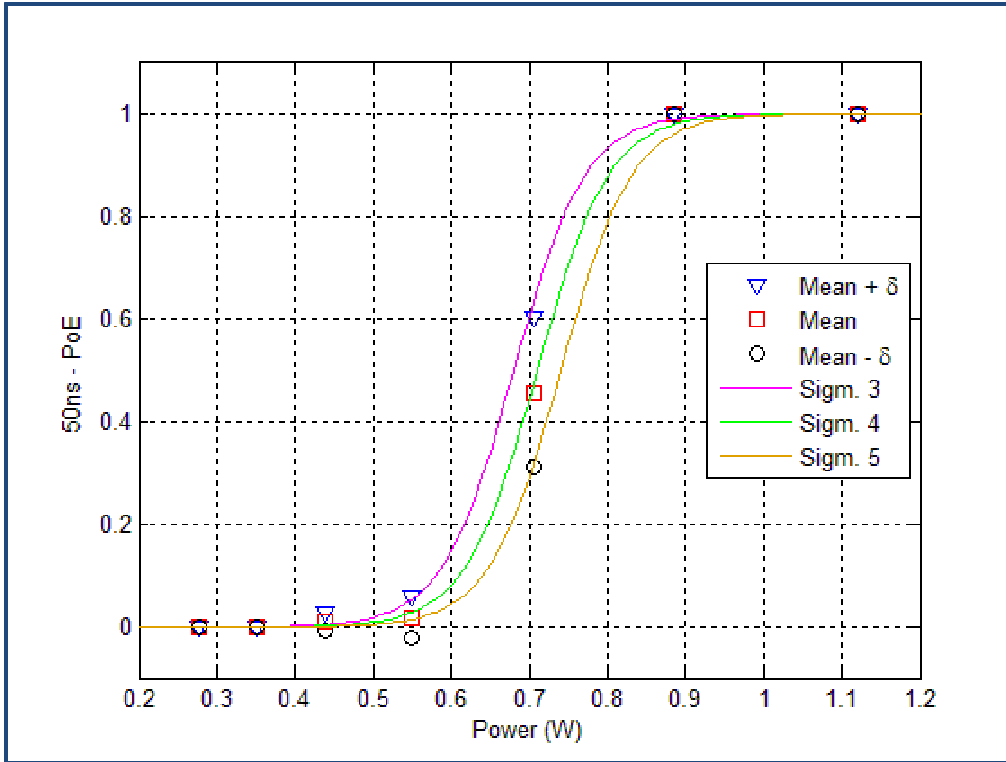

Figure 10: Sigmoid Probability of Effect curves overlaid on Figure 9 data points

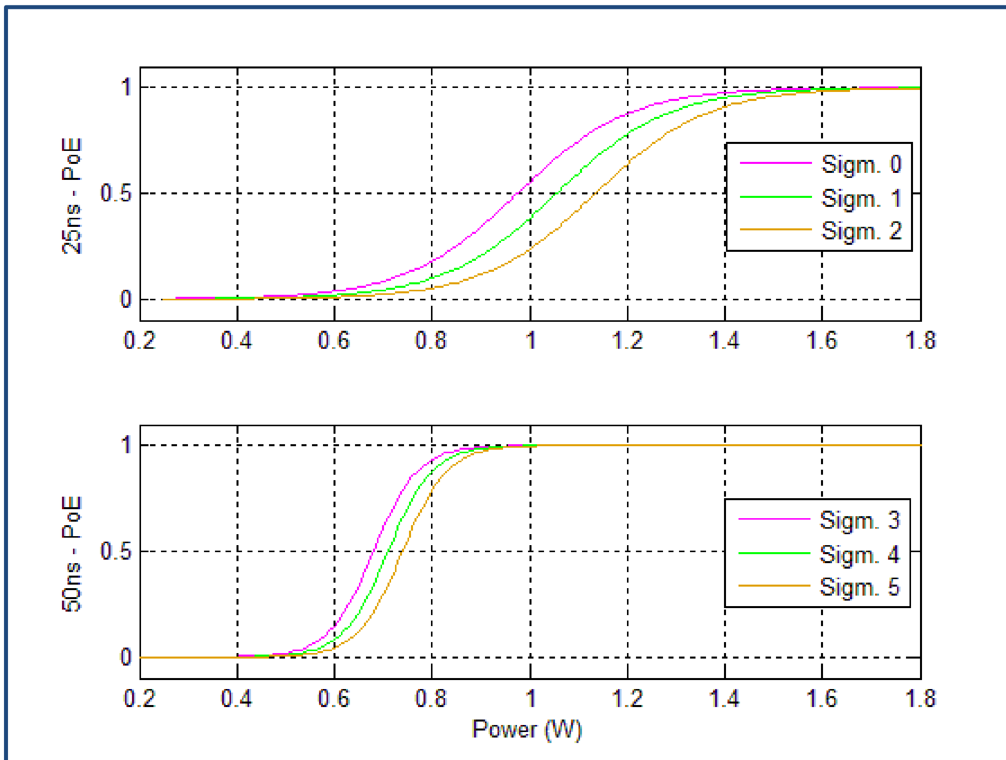

Figure 11: Comparative graph of Sigmoid Probability of Effect curves for 25 and 50 ns.

Approved for Public Release; Distribution Unlimited.

4.0 Summary and Conclusions:

In summary, 10 identical Atmel Microcontrollers were exposed to a fixed frequency EM pulse injected on the clock input at two distinct pulse durations; each time starting at a low pulse power level and increasing the power in 1 dB increments up to 20 W. The overall results reveal that the batch of MCU chips, with the expectation of M02, had extremely similar PoE values across the power range and pulse durations tested.

Sigmoid curves were fit to the sample data for each pulse duration, which can be seen in summary in Figure 11. In general, the variation in power required to achieve a 0.5 PoE across the batch of chips is small. For the 25 ns pulse duration the standard deviation value is approximately 80 mW while the standard deviation value for the 50 ns pulse duration is only 30 mW, which suggests that the PoE variation response in this particular microcontroller is small at the power range and pulse durations tested here. Comparing the upset thresholds of the MCU for these two pulse durations, it is clear, that the upset threshold of the MCU when subjected to the 50 ns pulse is significantly less and has a smaller standard deviation than that the 25 ns pulse. It is also interesting to observe that the slope of the 50 ns sigmoid curve is far steeper than the 25ns pulse duration.

These experimental results establish a good baseline for further testing planned in FY 2016. This experiment established the individual and chip-to-chip variation of upset threshold for the chosen MCU and briefly explored its dependence on pulse duration at a given frequency. These efforts helped to establish the foundation for tests planned in 2016. Moreover, they developed and refined a unique test setup that controls the relative timing between the onset of the injected pulse and a specific point in the clock cycle. A significant amount of work went into refining the set-up in 2015, which was necessary to gain the above mentioned precision in timing. A description of the experiments intended for next year can be found in the next section.

5.0 Future Work:

This section describes Microcontroller Upset Task experiments which are slated to take place in FY16 and beyond.

1) **Expanded Pulse Duration**

   This experiment aims to pulse durations lower and higher than the 25 and 50 ns pulse durations explored in Experiment 24. Exploring PoE with respect to pulse duration, at a variety of power levels, could provide evidence towards a hypothesis that suggests upset may be tied to total energy delivery.

2) **Expanded Range Power Sweep**

   This experiment aims to expose MCU assets to a larger range of direct injected HPEM power levels. Experiment 24 only explored the range of -23 dB to -15 dB (300 mW to 1.8 W). Present in-house capabilities will accommodate tests up to 20Ws. Although it is clear that at high power levels the MCU chips will begin to physically break down, at this time, the exact range is not known for this asset. Moreover, Experiment 24 provided a clear conclusion that higher power levels beyond a couple δs do not appear to alter the more-or-less absolute PoE response. However, it is presently unclear if higher power levels promote different upset style responses similar to the clear difference between Response 2 and 3 as described earlier in this report.

3) **Injection Location Sweep**

Approved for Public Release; Distribution Unlimited.

This experiment aims to determine the PoE for a specific pulse duration as it is shifted along the input clock signal, see Diagram 2. Previous experiments have suggested that the PoE is different when the HPEM pulse is positioned during the high section of the clock cycle versus the LOW section of the clock cycle. Moreover, it is unclear if the LOW to HI, HI to LOW, edge of HI, edge of LO, etc. locations on the similar PoE value.

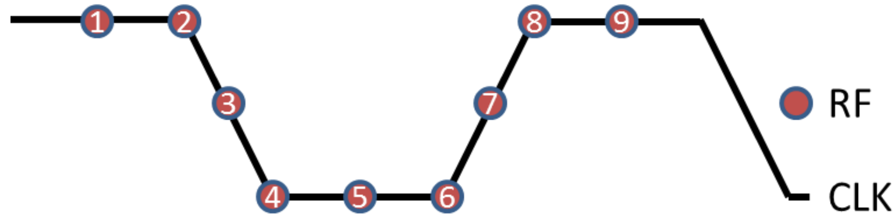

Diagram 2: Clock Signal and RF injection locations with respect to clock cycle.

4) PoE of a Single Pulse versus a Double Pulse

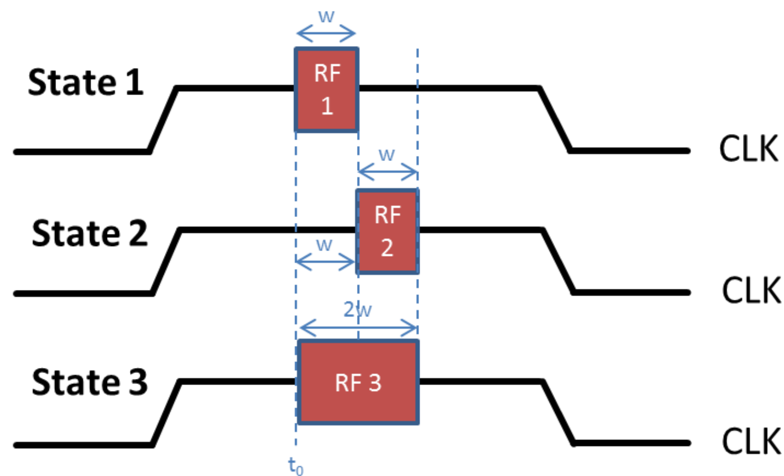

Diagram 3: RF Injection Locations and pulse width durations where w is the pulse duration and t_0 is the starting location of the testing region.

This experiment aims to determine and compare the PoE for three states, see Diagram 3, to determine if the PoE for the states is statistically Independent. The first state is a pulse of width *w* located at a time t_0 that is firmly within the middle part of either the HI or LOW region the clock cycle. The second state is a pulse of width *w* located at the position of $t_0 + w$. The last state is a pulse of width $2x$ located at the position of t_0. Following the successful collection of the PoE values for each state will allow usage of the statistical independence equation (EQN 3), where P_{e1} and P_{e2} are the PoE values for State 1 and State 2 respectively. If P_{e3} equals the right hand side of EQN. 3, then the system can be seen as independent.

$$P_{e1} + P_{e2} = 1 - (1 - P_{e1})(1 - P_{e2}) \qquad \text{(EQN.3)}$$

Approved for Public Release; Distribution Unlimited.

5) Instruction Dependence

This experiment aims to determine if the PoE for a consistent HPEM signal changes as it is injected during different Assembly operations. Experiment 24 chose to inject during the MOV command corresponding to the 17th rising edge of the 1MHz clock signal. However, it is unclear how similar that command's PoE with be to another command such as the ADD command or even to all other usages of the MOV command with in a single program.

6.0 Appendix:

Instruction	Time (us)
NOP	1 (1 cycle)
NOP	2 (1 cycle)
NOP	3 (1 cycle)
NOP	4 (1 cycle)
NOP	5 (1 cycle)
MOV SP,#080H	6, 7 (2 cycles)
MOV 0C2H,#001H	8, 9 (2 cycles)
MOV 0C3H,#001H	10, 11 (2 cycles)
MOV P1,#001H	12, 13 (2 cycles)
L0011:	
MOV A,P1	14, 15 (2 cycles)
ADD A,#001H	16, 17 (2 cycles)
MOV P1,A	18, 19 (2 cycles)
SJMP L0011	20, 21, 22 (3 cycles)

Table A1: Assembly counting program instructions and time locations.

Approved for Public Release; Distribution Unlimited.

DISTRIBUTION LIST

DTIC/OCP 8725 John J. Kingman Rd, Suite 0944 Ft Belvoir, VA 22060-6218	1 cy
AFRL/RVIL Kirtland AFB, NM 87117-5776	1 cy
Daniel Guillette Official Record Copy AFRL/RDHE	1 cy

Approved for Public Release; Distribution Unlimited.