Automated and Adaptive RF Effects Testing

***Everett G. Farr*[1], *Leland H. Bowen*[2], *W. Scott Bigelow*[3], *Robert L. Gardner*[4], *Peter Finlay*[5]**

[1]Farr Fields, LC, 1801 Count Fleet St SE, Albuquerque, NM, 87123, USA, efarr@Farr-Research.com

[2]Farr Fields, LC., lhbowen@Farr-Research.com

[3]Farr Fields, LC., Scott.Bigelow@Farr-Research.com

[4]6152 Manchester Park Circle, Alexandria, VA 22310, USA, Robert.L.Gardner@verizon.net

[5]Air Force Research Laboratory/RDHA, Bldg. 323, Kirtland AFB, NM, 87117-5776, USA, peter.finlay@kirtland.af.mil

Abstract

Testing electronics for vulnerability to radio frequency (RF) radiation is time-consuming, due to the large number of source variables of interest, including center frequency, pulse width, pulse repetition frequency, number of pulses, and bandwidth. One must intelligently select the source parameters most likely to expose the greatest vulnerability. We do so here using standard techniques from minimization theory. Within a space of two or more variables, we search for the combination that upsets the system at the lowest power or field level. We investigated the vulnerability of media converters to pulsed RF fields, by pinging a remote computer.

1. Introduction

The vulnerability of electronics to radio frequency (RF) fields has been well documented, for example in [1, 2]. This has led to a major effort to test electronics to find the minimum field or power at which an effect is observed. However, such testing is time-consuming, due to the large number of source variables of interest. One typically searches for the minimum electric field that causes upset, as a function of center frequency, pulse width, pulse repetition frequency, number of pulses, and bandwidth. It is impossible to test all combinations of all the variables, so one must intelligently select the source parameters most likely to expose the greatest vulnerability.

To select source parameters, we propose using standard techniques from minimization theory. Within a space of two or more variables, we search for the combination that upsets the system at the lowest power or field level. We begin by measuring the vulnerability levels on a coarse grid; and then fit a surface to the measured data. We then find the minimum of the surface, and measure the vulnerability at the minimum. With the new data, the process repeats itself iteratively until it converges.

Ideally, the entire process can be automated. The source variables can all be controlled electronically. In addition, one can determine automatically whether the test object has been upset, and send a reset command if necessary. This leads to a completely automated system that intelligently selects the test parameters, monitors the status of the device, and converges on a minimum upset threshold. During this first implementation, some manual operations were required; however, these can be automated at a later date.

In this project, we investigated the vulnerability of media converters (MCs) to pulsed RF fields. MCs are network devices that convert signal on Cat 5 Ethernet cable to optical fiber, and are known to be vulnerable. We tested these devices by pinging a remote computer, and observing the field levels at which the pings failed to return. We searched a space of source variables, and converged on a minimum upset threshold. Most of the operations were carried out automatically.

2. Experimental Setup

The MC we tested was the IMC model TP-TX/FX-MM850-ST, operating at 850 nm. This was selected because of its low cost and easy availability. A photo of this MC is shown in Figure 1. When configured for testing, the

978-1-4244-6051-9/11/$26.00 ©2011 IEEE

MC requires connections for two optical cables, an Ethernet cable, and a power cable. The two optical cables are necessary in order to communicate in both directions.

Figure 1. The IMC model TP-TX/FX-MM850-ST media converter.

We tested the MCs in the configuration shown in Figure 2. The main computer, running LabVIEW code, pings a remote computer through four MCs, two lengths of fiber optic cable, and three lengths of Cat 5 network cable. The computer controls the parameters of the synthesizer, which drives the amplifier that feeds into the TEM cell. Software running on the main computer then pings the remote computer, listens for the return signal, and detects a failure to respond.

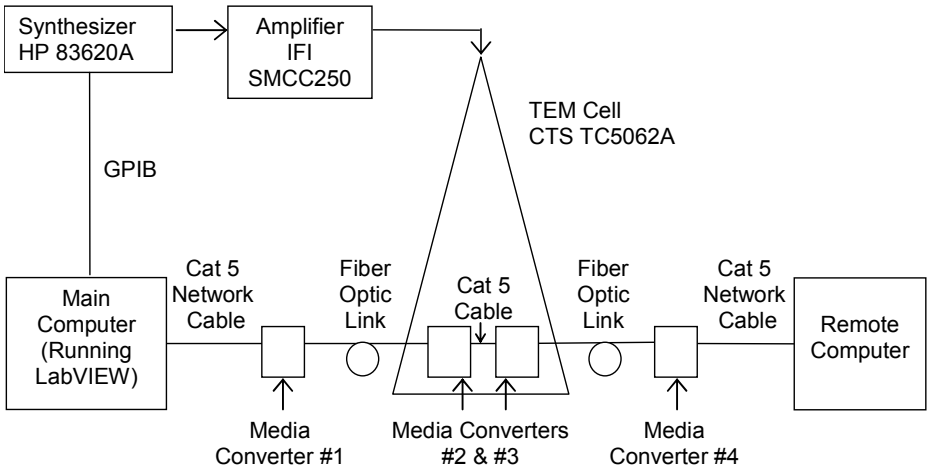

Figure 2. Experimental setup to test degradation of MCs with exposure to RF.

This configuration, which tests two MCs concurrently, was chosen in order to limit RF leakage from the TEM cell. The penetrations of the TEM cell were either fiber optic cables or filtered DC power cables, both of which could be configured to maintain the integrity of the RF shield. Previously, we tested a configuration with a single MC in the TEM cell; however, the metallic Cat 5 cable that penetrated the wall of the TEM cell caused excessive RF leakage. Attempts to limit this leakage by filtering the Cat 5 cable at the wall of the TEM cell resulted in loss of network signal.

It is necessary to relate the power out of the amplifier to the field in the TEM cell. To do so, we observe that power at the input is converted to voltage as

$$P_p = \frac{V_p^{\,2}}{2 \times 50\ \Omega}, \qquad V_p = \sqrt{P_p \times 100\ \Omega} \tag{1}$$

where P_p is the peak power, and V_p is the peak voltage in the sine wave on the 50-Ω feed line. The peak field in the TEM cell is related to the voltage at the input as $E_p = V_p/h$, where $h = 0.22$ m., the plate separation in the test volume. Finally, the average power is $P_{avg} = P_p \times DF$, where DF is the duty factor, $DF = PW \times PRF$, and PRF is the pulse repetition frequency. The duty factor is the fraction of time the square pulse of CW energy is turned on.

The software consists of two pieces of code, a threshold detector and a minimization routine. The threshold detector determines automatically the minimum field level required for upset for a given set of source parameters. It sets the frequency, pulse width (PW), and pulse repetition frequency (PRF) of the synthesizer. The power level is initially set to a low value, and is gradually incremented. At each increment, the remote computer is pinged 20 times. When the

power is high enough to yield 3 failures out of 20 pings, it is considered an upset condition, and that level is the upset threshold. This entire procedure is carried out in code that was written in LabVIEW.

The minimization routine guides the selection of parameters to test, in order to iterate to find a minimum upset threshold. We choose two variables over which to search, pulse width, and either duty factor or frequency. The procedure begins by taking data at nine points in the data space, the minimum, center, and maximum of each variable. A surface is fitted to this initial set of data using the "fminsearch" function in MATLAB, which then finds the minimum of the surface. This minimum is then used as the next point to test. The new results are added to the previous data, a new surface is fitted to the data, and a new minimum is found. The process repeats until the result converges.

3. Experimental Data

A key goal was to locate a minimum in the middle of a vulnerability test space. In a number of early experiments we found minima at less interesting locations—either at a corner or edge of the test space. However, finding a minimum in the middle of the test space demonstrates the usefulness of our minimization algorithm. We do so here.

We tested the vulnerability of two media converters in our TEM cell, using the configuration shown earlier in Figure 4. We tested with a pulse width (*PW)* of 10 µs, with frequency (*f*) ranging over 700-900 MHz, and duty factor (*DF*) ranging over 0.1-10%. The original nine points in the space are shown in Figure 3. Data are plotted in terms of peak power units. We have left the power units arbitrary intentionally. We then iterated three more times to find the minimum, and the result is shown in Figure 4. The minimum converges to a frequency (*f*) of 805.1 MHz, and duty factor (*DF*) of 7.8%, where we found a peak power (P_p) of 0.010, based on the curve fit. We then measured a point very close to the minimum, at f = 800 MHz and DF = 8%, where we found P_p = 0.018.

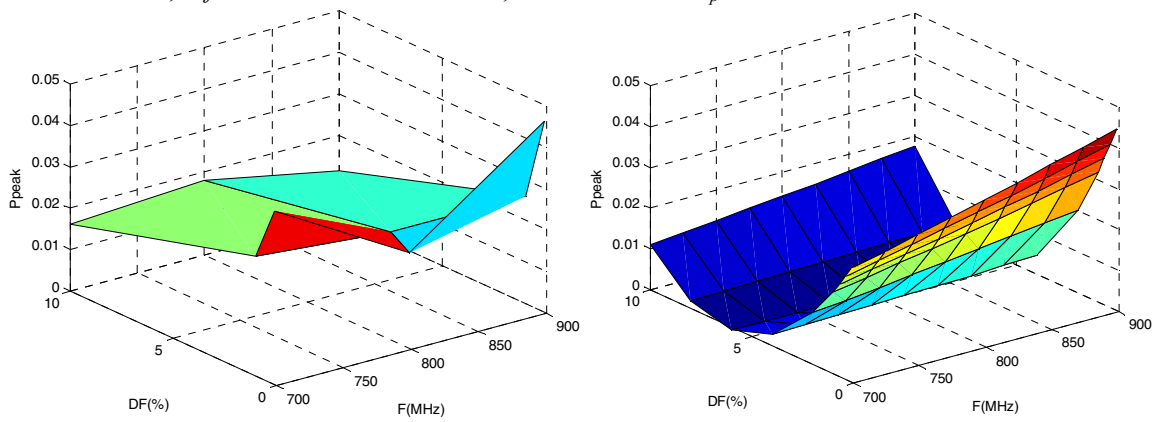

Figure 3. The original 9 points in the MC vulnerability test, left, surface fit, right,

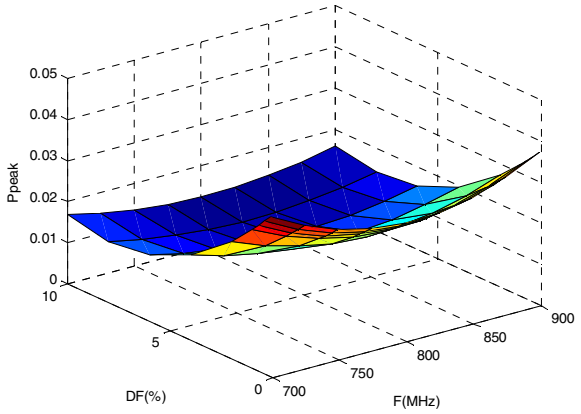

Figure 4. Surface fits of the data after adding 3 more points close to the minimum.

Thus, we observed P_p = 0.010 in the curve fit, and we measured P_p = 0.018 very nearby. This is a little less accurate than we would like to see, but it is still very good. We should be able to improve the fit of the surface to the

data by giving greater weight to data that is closer to the minimum. This is appropriate, since it is that portion of the surface in which we are most interested. We can do so, for example, by fitting to the inverse square or inverse cube of the vulnerability function.

4. Future Work and Conclusions

We outline here a number of areas that would benefit from further work, if there were interest. First, it would be necessary to fully integrate the software into a single unit. Currently, the software exists in two separate programs, which leads to manual operations. These programs have to be integrated in order to realize a fully automated system.

Second, we would add an automatic power characterization to each measurement, using a directional coupler and oscilloscope. This would involve making the software talk to the oscilloscope, downloading the voltage waveform, and converting the measured voltage to peak power. Ideally, one would prefer having an amplifier whose power is described by its dial settings, however, that seems to be difficult to realize in practice.

Third, we would investigate a number of variations on our minimization algorithm. For example, we would investigate alternative surface functions to fit to our data. In this paper, we used a function of the form

$$z = (a\,x^2 + b\,x + c)(d\,y^2 + e\,y + f) \tag{4}$$

where x and y are the two variables over which we are minimizing, and $a,\ \ ,f$ are the unknown coefficients that are chosen to give the best-fit surface to the measured data. However, many other functional forms are possible.

Fourth we would investigate methods of giving greater weight to the function value near its minimum. The current method simply implements a least-mean-square fit to the measured data. However, the data close to the minima are of greater interest, so it is more important to reduce the fitting error in that region. To emphasize the minima, one might fit a surface not to the data itself, but to its inverse square or inverse cube. By this method, errors near the minima carry more weight, and therefore are reduced in the fitted function.

Fifth, note that in this project we searched a two-dimensional space for the minimum upset threshold. However, this technique should apply equally well to searches in higher order spaces, and this should be examined.

Finally, we would test a variety of other devices, which might include cell phones, iPods, and/or network routers. The idea here would be to incorporate alternative upset modes and reset mechanisms into the programming. One could detect an upset by listening (electronically) for the music on a telephone or iPod to stop. One could also detect when a screen goes dark with a photodetector. One could reboot a system after upset by electronically toggling a power switch. One could use a servomotor to twist a knob on a source.

In conclusion, we have automated the testing of media converters for vulnerability to RF effects. Our testing involved pinging a remote computer, and listening electronically for missing return signals. To do this, we used software written in LabVIEW and MATLAB. The most important result is that we have successfully observed a minimum in the middle of a test space. This is the first nontrivial use of the minimization algorithm, so it is a significant milestone.

5. Acknowledgments

We wish to thank the Air Force Research Laboratory for funding this work as a Small Business Innovative Research project.

6. References

1. D. Nitsch, F. Sabath, H.-U. Schmidt, and C. Braun, Comparison of the HPM and UWB Susceptibility of Modern Microprocessor Boards, System Design and Assessment Note 36, July 2002.

2. M. Camp, D. Nitsch, F. Sabath, J.-L. ter Haseborg, H. Garbe, Susceptibility of Some Electronic Equipment to HPEM Threats, System Design and Assessment Note 37, February, 2004.