Progress In Developing Predictive Models For Erroneous Software Behavior Of Embedded Digital Logic Due To Electromagnetic Interference

M. Vitkovsky[1], T. Antonsen Jr. [2], S. Hemmady[1]
[1] Department of Electrical and Computer Engineering, University of New Mexico, Albuquerque NM, USA
[2] Department of Electrical and Computer Engineering, University of Maryland, College Park, MD, USA

Abstract— Predicting the behavior of digital electronic and embedded systems subjected to extreme electromagnetic interference is a growing concern for military and civilian systems operating in ever denser ambient electromagnetic environments. While the interaction of the electromagnetic stimulus with the system circuitry occurs at the physical level, the manifestation of this effect is often perceived as an erroneous behavior in the software state of the system. In this research effort, we are developing Markov state vector machine models (SVM) for describing the software state of a microcontroller-based digital electronic system when subjected to an external EMI-induced glitch. We describe our ongoing work in developing predictive models for erroneous software behavior through experimental data. Such a predictive capability will help EMI/EMC engineers develop quick assessment tools for modeling the behavior of higher complexity digital electronic and embedded systems exposed to extreme electromagnetic environments.

Keywords-Electromagnetic Interference, Radio Frequency Upset, Glitch, Software Effects, Microcontrollers, Markov Chains

I. INTRODUCTION

While the interaction of radiated extreme electromagnetic interference (EMI) with digital electronic systems occurs at the physical level, by way of inducing spurious voltage or current transients within printed circuit boards (PCB) and embedded semiconductor circuits, the manifestation of this interaction is often observed at the software level through an erroneous functional response of the entire system. In this body of research, we focus on developing a predictive model for software upset in a digital electronic system by treating the underlying hardware circuitry as a black box and utilizing a State Vector Machine and Markov Chain formalism to represent its perturbed functional response due to the injection of EMI pulses.

II. MOTIVATION

The Embedded Microprocessor Benchmark Consortium (EEMBC) has surveyed and categorized software scripts to reside within 6 categories. [Auto/Cons/Off/Net/Sec/Tele]. Independent of hardware architecture, software instructions within each script can be further categorized into 3 classes (ALU+Bit Operations; Branching (Program Flow) Operations; Data Flow Operations). We can leverage this body of work as a starting point for developing a predictive model for software glitches due to injected EMI pulses.

III. EXPERIMANTAL SETUP

Our experimental setup comprises of a custom PCB that contains a generic ATMEL 8-bit microcontroller (Figure 1). Specific connectors are presented which allow for injection of EMI pulses into the clock and/or power supply planes of the microcontroller. We have configured our experimental setup so as to implement an On-Chip Debugging (OCD) routine right after the injection of the EMI pulse. In this manner, we extract the contents of all the internal registers using the boundary scan technique. We compare the state of these internal registers with and without the injection of EMI pulses by repeating the process several times (~1000) to generate an ensemble of perturbed register values, which varies depending on the nature of the EMI pulses (amplitude, frequency, pulse width).

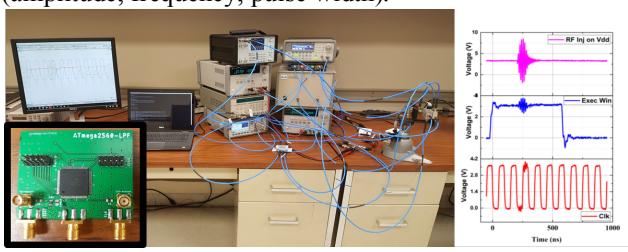

Figure 1: Experimental setup at UNM with sample trace of injected EMI on microcontroller power plane

IV. RESULTS

In our talk, we will present the statistical nature of how the injected EMI pulses perturbs the *program flow* or *data flow* of the set of instructions being executed by the microcontroller. We will characterize these perturbations as a function of EMI pulse parameters and instruction classes. We will then describe the probabilistic SVM and Markov Chain models we are developing that describes functional upset of software execution in the presence of injected EMI pulses. Developing such predictive models will help EMI/EMC engineers devise protection schemes for digital systems subjected to extreme EM environments.