Single Event Effect Hardware Trojans with Remote Activation

Paul A. Quintana; John McCollum; William A. Hill

Microsemi Corporation, San Jose California 95134

Paul.Quintana@Microsemi.com; John.Mccallum@Microsemi.com; Bill.Hill@Microsemi.com

Abstract: *With the semiconductor value-chain residing primarily offshore, access to Trusted leading-edge Integrated Circuits (IC) are an increasing challenge for US Department of Defense acquisitions. Many studies have investigated methods of securing the global semiconductor supply chain using a variety of methods including, controlled manufacturing, device reverse engineering and various fingerprinting technologies. In each case, the goal is to maintain IC integrity, confidentiality, reliability and availability as the product transitions through the global supply chain to the end user. Maintaining these Trust characteristics throughout the supply chain includes eliminating the malicious injection hardware and/or software Trojans. One class of Trojan, which has not received much attention, is a Single Event Effect (SEE)-triggered hardware Trojan. While Single Event Latch-up (SEL) circuit testing is routinely performed on space qualified semiconductors the use of SEE sensitive circuits may represents a latent and remotely -triggered hardware Trojan which would be extremely difficult to detect.*

This paper examines and presents a brief overview of Single Event Effects in ICs and introduces a potential means of remotely activating a SEE Trojan in both space and terrestrial environments.

Keywords: FPGA; ASIC; Trust; Anti-Tamper; Anti-Counterfeiting; Supply Chain Risk Management; DoDI 5200; DMEA; TAPO; Cyber Security; Hardware; Trojan; Charged Particle Beam, Directed Energy

Single Event Effects and Integrated Circuits

Natural radiation effects are generally considered to occur in a space, i.e. exo-atmoshperic, operational environment. This has led to considerable semiconductor reliability modeling and testing for space qualified semiconductor products. In general, Commercial Off the Shelf (COTS) semiconductors are not modeled or tested with extensive radiation effects in mind [1]. However, by understanding the Single Event Effects (SEE) mechanisms and circuit effects, an SEE-triggered Trojan can be developed. Such a Trojan would be very difficult to detect and may be introduced during foundry Front End of Line (FEOL) processing.

There are numerous types of SEE trigger modes that can be exploited for this type of Trojan. Simply, radiation effects can be viewed as cumulative radiation effect and Single Event Effects (SEE). For the purposes of a kill-switch type Trojan we are limiting this discussion to SEE triggers. The SEE triggered Trojans considered are shown in Table 1-1.

Table 0-1 Single Event Effect Modes

Mode	Acronym	Description	Devices Affected
Single Event Upset	SEU	Corruption of the information stored in a memory element	Memories, latches in logic devices
Multiple Bit Upset	MBU	Several memory elements corrupted by a single strike	Memories, latches in logic devices
Single Event Functional Interrupt	SEFI	Corruption of a data path leading to loss of normal operation	Complex devices with built-in cpu/state machine or control sections
Single Hard Error	SHE	Unalterable change of state in a memory element	Memories, latches in logic devices
Single Event Transient	SET	Impulse response of certain amplitude and duration	Analog and Mixed Signal circuits
Single Event Disturb	SED	Momentary corruption of the information stored in a bit	Combinational logic, latches in logic devices
Single Event Latch-up	SEL	High-current conditions	CMOS, BiCMOS devices
Single Event Snapback	SESB	High-current conditions	N-channel MOSFET, SOI devices
Single Event Burnout	SEB	Destructive burnout due to high-current conditions	BJT, N-channel Power MOSFET
Single Event Gate Rupture	SEGR	Rupture of gate dielectric due to high electrical field conditions	Power MOSFETs, Non-volatile NMOS structures, VLSIs, linear devices

A taxonomy of Trojan types is shown in Figure 1-1 for reference.

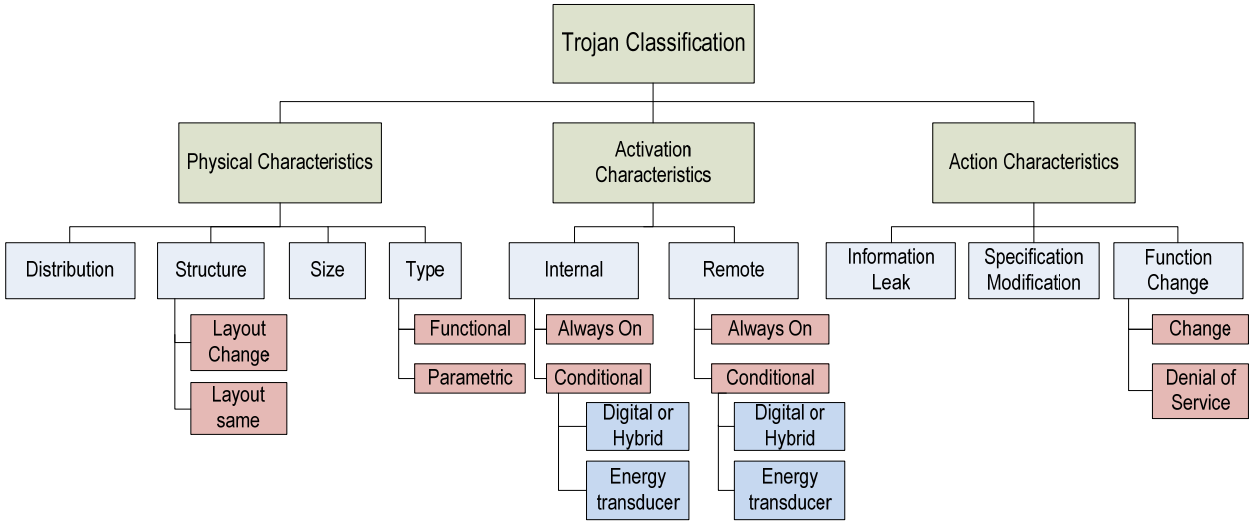

Figure 1-1 Hardware Trojan Taxonomy Characteristics (Source: Wang et.al. [4])

Enabling a Kill Switch

CMOS logic devices such as FPGA's are designed and tested for the mitigation of SEU/MEU types of effects. However, testing for other SEEs is typically limited to characterization or lot testing for space qualified applications. Wide bandgap semiconductor technology such as GaN power amplifiers can also be sensitive to SEE making this type of Trojan a potentially broad-ranging semiconductor threat [2].

The design of SEE-sensitive circuits as well as tuning sensitivity to SEE events is needed for this HW Trojan. With this type of trigger mechanism one can then create an SEE sensitive hardware (HW) Trojan trigged by a directed energy weapon such as a charged particle beam. A simple result would be rendering a denial of service attack against weapons system electronics. This approach is very similar to the approach taken by the Reagan-era Strategic Defense Initiative (SDI) [3]. However, the inclusion of a SEE HW Trojan would enhance sensitivity and therefore greatly extending the range of such directed energy weapons. This range extension would result in making directed energy weapons useful for not only exo-atmospheric environments, but also for ground based and endo-atmospheric use.

SEE-introduced Trojans in ICs

A CMOS flip-flop can be upset by a fairly low mass particle such as a Proton, Alpha Particle or a Neutron.

A flip-flop triggered Trojan, Figure 1-2, could then be implemented as a register that is reset at power-on and has no circuitry to set the state to the on-state or trigger condition. This can be easily achieved by making the cross-coupled devices asymmetric by capacitance load, device sizing, or a different transistor threshold voltage (Vt). Once triggered by an SEE the Trojan enable signal would be connected to a critical logic path through a simple gate, thereby corrupting, or co-opting the function of the device and performing a simple denial of service attack on the target IC.

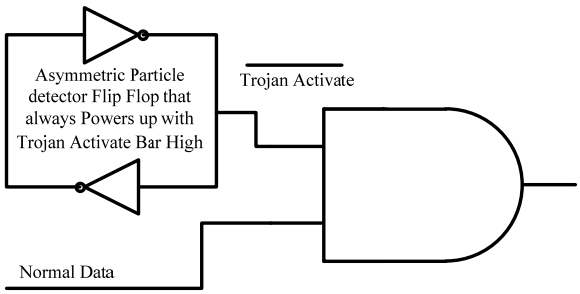

Figure 0-1 Simple Trigger Mechanism Example

The tailored SEE-sensitive register would be small so as to make it sensitive to a low LET (linear energy transfer) particles. Additionally, the SEE trigger would be unbalanced to favor being set by a specific low LET particle. This example is trivial but is unlikely to be caught by any amount of electrical testing. Additional trigger tuning may further allow selection of trigger type,

and only flip when a charged particle beam weapon is used and not radiation testing.

Increasing its target cross-sectional area can enhance trigger gain, but would require many cells. An ideal device would be an IC with many regular structures, which could hide multiple trigger gain elements, Figure 1-3. An FPGA with its regular structure and layout could allow a Trojan to be inserted in every Universal Logic Module (ULM) or Logic Element (LE). A large FPGA would have millions such structures. If the cross-section of each trigger cell was $0.25u^2$, then a 1 million LE FPGA would have a cross-section of 0.25 mm^2. An electronics system being targeted would likely have many FPGA's making for a very large target. Adjusting the ideal cross-section target area needed could then be accomplished by merely adjusting the number of trigger cells.

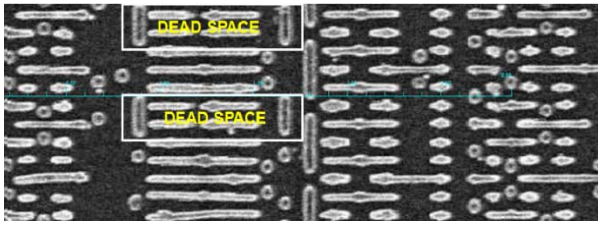

Figure 0-2 A 20nM FPGA Mux Showing a repeating dead space where a Trojan could be inserted

Third Party IP (3PIP) Insertion

The use of commodity third-party IP (3PIP), say a microcontroller, with a trigger cell could allow for broad deployment of the SEE-triggered Trojan. If the 3PIP Trojan is tuned such that it is in the background of the normal latch failure rate due to atmospheric neutrons, it could easily escape detection. Thus it could be possible to trigger a denial of service attack even if the logic is using triple mode redundancy (TMR) or Dice cell technology protections [5]. Few if any countermeasures would be available for protection.

Extending the Trojan complexity by incorporating conditional activation features, such as grounding the enable gate, configures the Trojan to pass particle beam testing during qualification. Once the IC became ubiquitous in defense applications a simple contact mask change in production would activate the Trojan. To prevent the introduction of the activated Trojan would require regular radiation testing in the production flow and/or the use Trusted IP only.

An even more complex problem would be the incorporation of the Trojan latch in concert with on-board microcontroller code. Such a particle beam weapon activated Trojan would only be triggered when code was run that would disable system protections or allow privilege elevation.

Directed Energy Triggering

The Trojan discussed requires the use of a charged particle beam within the Earth's atmosphere. The energy required to trigger the Trojan will be far less than the energy required to disable the target kinetically as in the SDI approach. These high-energy directed energy weapons have been studied and developed largely for the purpose remote sensing and kinetic effects.

In the case of atmospheric directed energy, there is a long list of experiments and research since the 1950's, if not earlier. Multi-pulse hole-boring and propagation through the atmosphere is feasible in all weather for defensive ranges where several kilometers are sufficient. Example accelerators, and a focusing system, have been developed at the Los Alamos and Sandia National Laboratories in the United States [6].

This prior research has been focused on using this directed energy to destroy or disable a threat directly. This assumption has direct implications on the energy levels required on-target as well as the lethality range of the charged particle beam (CPB). Typical lethality parameters used for this type of application may be:

- Particle Type: Electron, Proton or Muon
- Peak Power Output: 10^{12} Watts– 10^{14} Watts
- Particle Energy: 0. 5 GeV- 10 GeV
- Tracking Accuracy: 2 micro-radians – 25 micro-radians

These assumptions can relaxed greatly for charged particle Trojan triggering or maintained to gain additional lethality range. Requirements for beam control can also be relaxed as the cone of radiation is much larger than the beam radius [7]. In comparison High Energy Laser (HEL) weapons in the 30kWatt -60kWatt range have been demonstrated by Lockheed Martin with a range of about 1.6 km.

Conclusions

Single Event Effects occur as common part of semiconductor design. Circuit design techniques to test for and to mitigate SEE are known. However, SEE still

occur either through 3PIP or simply through unexpected design consequence.

The feasibility of an SEE hardware Trojan including tuning sensitivity to charged particles has been examined. We simplistically examined the requirements of charged particle defense system including; charged particle beam, Pointing and tracking, fire control system, beam propagation and target interaction to evaluate the practicality of an SEE-triggered Trojan. Further, the ability to insert an SEE Trojan into the semiconductor supply chain and escape detection was introduced.

If an enhanced sensitivity SEE Trojan should be introduced into an IC, one has the opportunity for broad ranging actions. By exploiting a SEE hardware Trojan it would be feasible to create small and hard-to-detect Trojans capable of remote triggering. The most likely consequence would be a denial of service attack. Using additional conditional triggers, enabling more sophisticated attacks would also be possible. Thus, reducing a targets knowledge of the attack or the mechanism used.

Coupling Single Event Effects with the maturing technology of charged particle beam directed-energy weapons creates a tactical version of the Strategy Defense Initiative. Potentially realizing what "The Hunt for the Kill Switch [8]" introduced.

References

[1] Sinclair, Doug and Dyer, Jonathan, "Radiation Effects and COTS Parts in SmallSats, 27th Annual AIAA/USU Conference on Small Satellites, 2013

[2] Fleetwood, Dan, Chen, J, Jiang R., and Schrimpf, R.D., "Hardness Assurance Issues for GaN/AlGaN HEMTs", Vanderbilt University, 2016

[3] M. Bundy, G. Keenan, R. McNamarah, and G. Smith, "The President's Choice: Star Wars or Arms Control," Foreign Affairs, Winter 1984/85, p. 264

[4] X. Wang, M. Tehranipoor, and J. Plusquellic, ''Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions,'' Proc. IEEE Int'l Workshop Hardware-Oriented Security and Trust (HOST 08), IEEE CS Press, 2008, pp. 15-19.

[5] T. D. Loveless, S. Jagannathan, T. Reece, J. Chetia, B. L. Bhuva, L. W. Massengill,S-J. Wen, R. Wong, D. Rennie, "Neutron- and Proton-Induced SEU Error Rates for D- and DICE-Flip/Flop designs at a 40 nm Technology Node", IEEE Trans. Nuclear Sci., 2011, Page(s):1008 - 1014

[6] M. G. Mazarakis, J. W. Poukey, S. L. Shope, C. A. Frost, P. J. Pankuch, B. N. Turman, J. J. Ramirez, and K. R. Prestwich, ""Smile" A New Version for the RADLAC II Linear Accelerator", Proc. Of the Linear Accelerator Conference, 1990

[7] Gsponer, Andre, "The Physics of high-intensity high-energy Particle Beam Propagation in open Air and outerspace Plasmas", Independent Scientific Research Institute, January 11, 2009

[8] S. Adee, "The Hunt for the Kill Switch", IEEE Spectrum, 1 May 2008.