

Industrial Microprocessor Design

Paper 1

Victoria Steele

Table of Contents

1. Problem Statement 2

2. Nomenclature 2

3. AssumptionS 2

4. Results and Analysis 3

4.1 Background on Single-Event Upsets 3

4.2 Requirements for Appliances Pertaining to Single-Event Upsets 3

4.3 Conclusion 3

5. References 3

# Problem Statement

*Address whether or not engineers should do anything in hardware or software in response to the likelihood of a singe-event upset occurring in consumer appliances using microcontrollers. Explain why or why not and what should be done.*

# Nomenclature

|  |  |
| --- | --- |
| Abbreviation | Definition |
| SEU | Single Event Upset |
| ROM | Read Only Memory |
| RAM | Random Access Memory |
| ECC | Error Checking and Correction |
| EDAC | Error Detection and Correction |
| SSC/DSD | Single Symbol Correction/Double Symbol Detection |

# 

# AssumptionS

* Knowledge of appliance controls does not need to be sited if information is inherent to developer.

# Results and Analysis

## Background on Single-Event Upsets

A single event upsets (SEUs) are characterized by the change of a transistor state which introduce system errors. These are referred to as soft memory errors as they corrupt the value held by the memory cell but do not damage the physical memory. It should be noted that and SEU can also cause hard memory errors which result in permanents damage to the memory [3]. The main causes of SEUs have been traced to alpha particle radiation in chip packaging material and atmospheric neutrons caused by cosmic rays [3][1]. Single Event Upsets have caused a variety of “glitches” including lockups in security cameras, routers, switches, avionic systems, and a myriad of others [2][4]. The likelihood of SEUs depends primarily on memory architecture and altitude, but the soft error rate for DRAM and SRAM are expected to rise as chip trends continue toward higher density, lower voltage, and increased frequency. There are a number of hardware and software prevention methods, which can be used to decrease the chances of serious issues caused by SEUs. Hardware solutions have largely solved alpha particle errors and include the elimination of particles sources from packaging materials and the addition of shielding [3]. The software solutions include Error Checking and Correction (ECC) algorithms and Error Detection and Correction (EDAC) algorithms, several of which were invented for communication reliability [1]. Specific methods include Single Symbol Correction/Double Symbol Detection (SSC/DSD), caching, scrubbing, and parity protection. It is worth noting that some can be quite costly to implement [3].

## Requirements for Appliances Pertaining to Single-Event Upsets

Appliance control boards, microprocessors, and harnesses are highly susceptible transient and intermittent faults caused by environmental conditions, EMI, ground loops, aging components, line variation, and noise [1]. All GE appliances undergo a rigorous reliability testing and review process before being introduced into the consumer’s home. Although the primary concern for appliance controls falls under the EMI category, the microcontroller is also required to perform UL 1998 periodic RAM and ROM checks for corrupted memory [3]. Additionally, the internal GE Appliance communication protocol uses parity as well as acknowledgement, retry, and error handling. Additionally, wireless modules are shielded and isolated to separate boards, analog and digital circuits are separated, and the watchdog timer is used with assert methods for logging system errors on reset. GE Appliances primarily uses products from Renesas, STM, Atmel, and Cypress. Atmel and Cypress have been used as the cap touch chips for several of the range products and are placed on a different board from the main controller such that primary machine control operations are independent from the cap touch operation in an effort to further protect the consumer. Lastly, appliances are equally as susceptible to cosmic ray disruptions as other microcontroller based applications, although the clock speeds are typically lower. That being said, micros are becoming progressing more powerful and less costly leading to a higher probability of future errors.

## Conclusion

Traditionally, radiation immune electronics have been used for space, aviation, and military applications; however, with the previously mentioned trends in digital electronics, the focus is shifting to include consumer products. For appliances, design is driven by cost. Board space, memory, and power consumption are precious commodities with very little room for complex algorithms, background tasks, or redundancy. When speaking of consumer safety, no corners should be cut; in all GE Appliance control systems, “heartbeat” signals are sent between boards to verify that no lockups have occurred, memory checks are completed in the background task, and the watchdog is running at all times. While safety is the primary driver for such things as the redundant micro, and RAM and ROM checks, Single Event Upsets are not typically an area of focus. Adding a second chip for ECC is not a practical solution for a board that is priced to the penny [3]. For example, considering the recently developed data flash driver, the startup algorithm is tolerant to almost all forms of errors except cosmic rays. The risk of adding more algorithmic complexity, stack usage, and RAM usage outweighed the benefit of protecting against an event with such a low probability of occurring. Therefore, when considering protective measures for in home appliances, a cost benefit analysis should be conducted for each problem. The algorithms and system architecture should be extensively reviewed, UL checks should be verified for each new implementation, and microcontroller lockups should be prevented through hardware and software redundancies. Lastly, home appliances have very small memory footprints, are at low altitudes, and are not considered high-risk applications.

# References

[1]Auburn University. "Auburn University Engineering." *Auburn University.* http://www.eng.auburn.edu/~agrawvd/TALKS/tutorial\_6pg.pdf (accessed October 18, 2014).

[2] NASA. "Space Math @ Nasa." *Space Math @ Nasa.* http://spacemath.gsfc.nasa.gov/engineering/3Page6.pdf (accessed October 18, 2014).

[3] Tezzaron Semiconductor. *Soft Errors in Electronic Memory - A White Paper.* Naperville, IL: Tezzaron Semiconductor, 2004.

[3] Underwriters Laboratory. *UL Standards .* 2014. http://ulstandardsinfonet.ul.com/scopes/scopes.asp?fn=1998.html (accessed October 18, 2014).

[4] VideogeniX. "Praeger Security International." *Praegure Security International.* 2006. http://psi.praeger.com/pdfs/whitepapers/SEUsandTheirEffectonElectronicDevices.pdf (accessed October 18, 2014).