Reliability Considerations for Automotive FPGAs

White Paper

September 2003

Table of Contents

Abstract 5
Introduction 5
Failure Mechanisms 6
  Temperature 6
  Effects of Neutrons on Programmable Logic 7
  Security and Tamper Resistance 11
  Time Dependent Dialectric Breakdown (TDDB) 12
Conclusion 14
Bibliography 15

Abstract

With the increasing deployment of electronics in automobiles, the need for high reliability components is essential to ensure the proper function of the systems in today's vehicles. While there has been substantial progress made in this area, there are still many engineering trade-offs that are poorly understood, which should be factored into the selection process for advanced digital circuits. Modern automotive systems require reliable, cost-effective, flexible solutions to deploy the complex arrangements of equipment consumer's demand. Programmable logic and especially Field Programmable Gate Arrays (FPGAs) are increasingly being used by the automotive industry. When selecting an FPGA it is important to evaluate the total cost of ownership for each of the various programmable architectures and to identify suppliers with inherently reliable core technology, rather than those who just up-screen or requalify commercial products designed for less demanding applications.

Introduction

In the last 25 years, automobiles have evolved from purely mechanical machines into highly integrated electro-mechanical systems. Initiatives in the market place today to improve safety, enhance emissions, and deploy intelligent drive-by-wire systems suggest that many, if not all, functions in tomorrow's automobile will be controlled by electrical systems. Additional customer demand for advanced entertainment, passenger comfort, information, and telematic applications make it is easy to understand how today's dreams will become tomorrows standard features.

Designers face the challenge of continually adding these complex electronics to each successive model year while still maintaining the industry’s high standards for quality and reliability. These developers have traditionally relied on Microcontrollers, custom ASICs, and bulky wiring harnesses to implement and control these systems and expand the capabilities of each automotive generation. The automotive industry is faced with new design challenges as these traditional solutions are reaching their technical limits as well as creating increased reliability concerns as complexity grows exponentially.   To solve these problems, many designers are turning to programmable logic for their next generation designs.

Increasingly, the automotive electronics development community is turning to FPGAs as a flexible, low-cost solution for control functions, bridging an interface between components or simply as glue logic for a variety of customized systems. Gartner Dataquest analysts have identified FPGAs as the fastest growing semiconductor segment for the automotive industry, with over 70% CAGR through 2007. As standard products, programmable logic devices also avoid obsolescence problems that plague most specialize custom circuits. Nonvolatile FPGAs are also ideal for integrating multiple functions into a single-chip solution to reduce board space, overall system cost, and improve system reliability.

As a technology decision maker evaluating FPGAs for the automotive industry, there are several trade-offs that must be weighed when choosing a supplier. It is best to invest the effort up front in the selection process rather than facing the far greater cost of undoing a wrong decision. Failures in FPGAs can be caused by a number of different mechanisms, through environmental and electrical conditions are considered the cause of most semiconductor failures. For example, operating temperature is of fundamental importance when evaluating an FPGA as it will accelerate almost all degradation and failure processes. In addition, as the industry’s understanding of failures evolves, engineers will have to consider a device’s immunity to neutron induced errors, the inherent level of tamper resistance for an FPGA, as well as dielectric breakdown in advanced process technologies.

Failure Mechanisms

Semiconductor technology continues to evolve at an aggressive rate. The main elements of this evolution focus on continual miniaturization and higher integration. In order to fuel this continued innovation, the process's technology and silicon platforms are becoming increasingly advanced and complex. Simultaneously, the failure modes could also be said to include more complex factors. As miniaturization of the wafer process advances, the design and process margins are tending to shrink, introducing new threats from unfamiliar failure modes.

Automotive manufacturers and suppliers have to contend with the unique problem of improving automotive electronic reliability while meeting the stringent demands of low-cost, high-volume production. As many designers are increasingly turning to FPGAs for highly integrated next generation products, there are a number of potential failure mechanisms impacting overall device reliability that need to be understood. While some are similar to ASICs, others are unique to specific FPGAs types or specific FPGA technology.

This paper focuses on the fundamental importance of technology selection and its relationship to overall system reliability. This general introduction emphasizes cause and cure, rather than statistical reliability, as a recognition of the guaranteed performance required in automotive applications.

This paper addresses the following topics:

1. Temperature as a primary stress factor in semiconductor failure
2. Neutron Induced Soft and Firm Errors
3. Tamper Resistance in Automotive FPGAs
4. Time Dependent Dialectric Breakdown (TDDB)

Temperature

As plastic encapsulated semiconductor devices, the reliability problems most frequently encountered by FPGAs are typically due to one of four root causes: the packaging technology, assembly technology, environmental overstress, or ESD. These failure mechanisms are all accelerated by exposure to high temperatures. As a result, automotive designers can significantly limit vulnerability to a wide variety of failures by using an FPGA's technology that provides extended temperature coverage. Today, many suppliers already employ proactive design and qualification methodologies to model and simulate environmental stress, but certain FPGA architectures, such as antifuse, are inherently superior in their tolerance to extended temperature exposures. Antifuse automotive FPGAs from Actel offer coverage to the industry's highest junction temperature (+150°C) and ensure designers extra margin in high- reliability systems.

Due to economic pressure, automotive electronics are designed and produced using the same material, packaging, and assembly techniques that are employed in commercial applications. This forces many semiconductor suppliers to qualify what is essentially a commercial platform for a much more challenging environment. Thus, it can be a tremendous advantage to use an FPGA supplier who has a history of providing 'mission critical' products and are already engaged in rigorous screening to ensure high performance and reliability in extreme environmental conditions. The specification of harsh environments for under-the-hood automotive electronics calls for a temperature range of -40°C to +125°C ambient well beyond the standard commercial and industrial temperature ranges as defined by most vendors.[1] FPGA suppliers who manufacture devices for high reliability applications, ranging from commercial aviation to military systems, are much more likely to deliver reliable and secure performance in extraordinary environments.

1. *R. Constapel, J. Freytag, P. Hille, V. Lauer and W. Wondrak, 2000, "High Temperature Electronics for Automotive Applications," CIPS 2000, 20.-21.6.2000, Bremen.*

Temperature is the single dominant stress factor affecting the reliability of electronic devices. With the potential to create failures at the device, package, and board level, it is critical to allow for margin at each level of the automotive system (Table 1). FPGA suppliers that characterize products over extended military temperature ranges, like Actel, are able to better characterize thermal expansion coefficients to help avoid thermal stress. Cyclic temperature changes will lead to low-cycle-fatigue of the soldered joints, and after a limited number of cycles, a surface crack will be initiated which is subsequently growing until completely separated.[2] Ensuring your automotive FPGA is covered by the industry's highest junction temperature is another way to help minimize the risk of almost all degradation and failure processes. (Table 2).

Table 1: Temperature is a Potential Source of Failure at all levels of the Automotive System[3]

Failure SIte	Stress Factor
Device Level Oxide Passivation System Metallization	Voltage Current Density Temperature
Package Level Molding material Die attach Bonds	Humidity Current Temperature Chip size ΔT Vibration
Board Level Substrate Solder Joint Bond Connector	Humidity Current Temperature ΔT Vibration

Table 2: The leading supplier of Automotive FPGAs and their Recommended Operating Conditions

Supplier	Product Family	Specified Automotive Temperature Range	Maximum Junction Temperature
Actel	SX-A, eX, MX	-40°C to +125°C (Ambient)	+150°C
Altera	Cyclone, ACEX 1K	-40°C to +125°C(Junction)	+125°C
Xilinx	Spartan XI, II, IIE	-40°C to +125°C(Junction)	+125°C

Effects of Neutrons on Programmable Logic

Semiconductor industry concern regarding neutron-induced errors is growing rapidly. The progression in semiconductor manufacturing processes to ever-smaller geometries is creating new issues and exacerbating other known problems, including neutron-induced upsets. Already, a well-known phenomenon at higher altitudes, incidents of neutron-induced errors are increasing in frequency and at much lower altitudes. These effects, which were once primarily observed at high atmospheric levels, are now becoming significant even at ground level as process geometries shrink and memory elements hold less charge, making them more susceptible to stray neutrons.

Neutron Sources

Neutrons are created when high-energy particles from deep space and our sun (galactic cosmic rays and solar rays) collide with atoms of nitrogen and oxygen in the earth's upper atmosphere. The collisions result in the destruction of the

2. *"Design guidelines for reliable surface mount technology printed board Assemblies," 1996, IPC-D-279, IPC.*
3. *Boos, A., R. Constapel and W. Wondrak, DaimerChrysler AG, Research and Technology, J. Wilde University of Freiburgn, Inst. For Microsystem Technology "Design for Reliability in Automotive Electronics Part I: Semiconductor Devices."*

nitrogen and oxygen atoms and the production of a variety of other high-energy particles. Most of these particles are charged and recombine quickly. However, a significant portion of the product of atmospheric collisions are neutrons. These neutrons are emitted from the collisions at very high rates and tend not to recombine with other particles, since they are not charged. They travel at high speed until they collide with atmospheric gases, objects on the earth's surface, or objects traveling through the atmosphere.

Figure 1 illustrates the relationship between altitude and neutron flux. Neutron flux is shown at a variety of altitudes and latitudes. It is interesting to note that the flux density is more than three times higher in Denver than it is in New York. Both cities are on approximately the same latitude, but Denver is located at a much higher altitude.

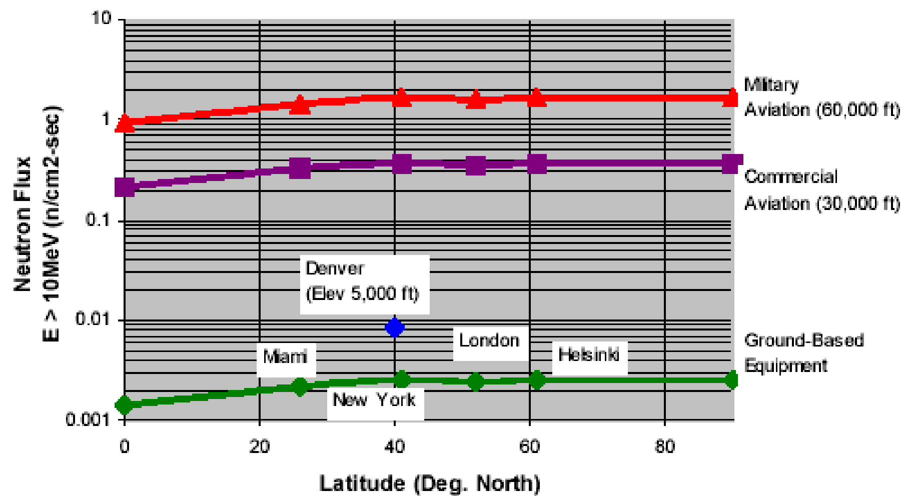


Figure 1: Neutron Flux as a function of Altitude and Latitude[4]

What Happens When Neutrons Strike Integrated Circuits?

Many neutrons striking an integrated circuit will pass through without interacting with the circuit, but some neutrons will pass close enough to a silicon or dopant atom to disturb the atom. The result of this interaction is the creation of secondary particles, which in turn create a trail of electron-hole pairs up to several tens of microns in length. Figure 2 on page 9 illustrates this interaction. If this occurs near the junction of a reverse-biased device in a memory cell or flip-flop, then a voltage spike can occur, resulting in the memory cell or flip-flop changing state. This change of state is frequently referred to as a single-event upset, (SEU) because it is caused by a single neutron interacting with the crystal lattice of the integrated circuit. Significant attention has been focused on how to mitigate against data corruption as a result of these SEUs, with techniques such as error detection and correction codes (EDAC) and triple-module redundancy (TMR) being used to detect and overcome SEU induced soft errors in memory devices. It is not possible to shield against high energy neutrons, so designers must either account for their effects or use neutron resistant technology.

4. *"Measurement and Reporting of Alpha Particles and Terrestrial Cosmic Ray Induced Soft Errors in Semiconductor Devices," 2001, JEDEC Standard JESD89.*

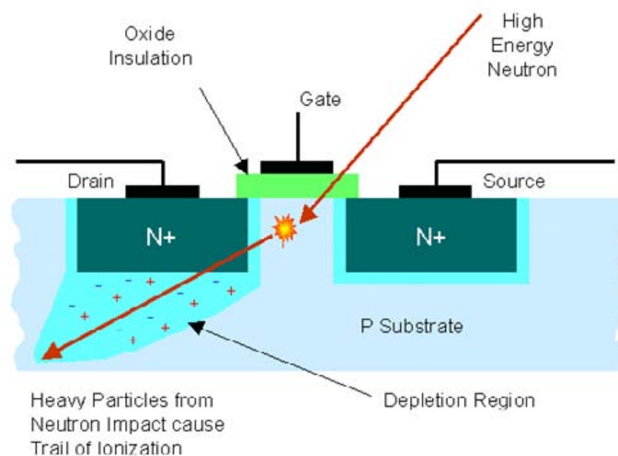


Figure 2: Interaction of a High-Energy Neutron and a Silicon Integrated Circuit

Consequences of Neutron-Induced, Single-Event Upsets

The SEUs caused by neutrons inside integrated circuits can occur in any type of memory cells. SRAM-based FPGAs use internal memory elements to hold the configuration state (or personality) of the FPGA. These memory elements pose a more serious reliability threat. When the contents of a memory device are changed without damaging the device, it is called a "soft error." In such a case, the device can successfully be rewritten with correct data. When an SRAM-based FPGA memory cell is corrupted, it is called a "firm error." These errors are called "firm" because they are not easily detected or corrected and are not transient in nature. Once a firm error occurs in an FPGA, the device must at a minimum be reloaded with its original configuration. In some cases, the power must first be recycled to clear the fault, and then the device must be reconfigured. The consequences of a neutron-induced SEU in one of these configuration cells could be severe. If a neutron causes a configuration bit to upset and change state, it could change the entire functionality of the device. Such a change could result in significant data corruption, the forwarding of spurious signals into other circuits in the system. In certain extreme cases, a firm error can become a "hard errror" and cause the destruction of the device itself or the system containing the device (a neutron induced firm error that misroutes a signal creating an internal short is one common example of this type of problem).

Neutron-induced errors have significant implications for critical automotive applications that are based around an SRAM FPGA. With worldwide automotive fleets running into the hundreds of millions, the widespread deployment of FPGA technology with increasing susceptibility to these events, could ultimately create the need for a new quality system to evaluate automobiles for their immunity to neutron-induced errors. (this is already the case with several vendors of communication’s equipment). Even the existing detection techniques, which rely on reading back the configuration of the FPGA at regular intervals, may let corrupt data enter the system for a significant period of time. The read-back circuits that enable detection of a corrupted configuration are themselves subject to single-event upsets or damage.[5] Additionally, schemes to detect and correct FPGA firm errors add extra complexity to the system design and significantly increase board space and bill-of-materials cost.

Neutron-induced firm errors can contribute significantly to the overall system failure in time (FIT) rate for ground-based equipment. Difficult to diagnose and detect, soft and firm errors could create maintenance and service issues with the potential to escalate to larger warranty concerns. Of the three main FPGA technologies, antifuse, Flash and SRAM, only antifuse and Flash are immune to the effects of neutron-induced soft and firm errors.

5. *Alfke, P., P. Dyreklev, K. Johansson, and M. Ohlsson, 1998, "Neutron Single Event Upsets in SRAM-based FPGAs," NSREC.*

Frequency of Neutron Induced Failures

Data has been published on the susceptibility to upsets of large SRAM-based FPGAs. The most recent data available covers devices with 0.22μ processing. It is expected that devices with finer processing are subject to significantly higher levels of upsets. Soft and firm error failure rates are typically expressed in FITs. A FIT is a single failure in 1 billion (1E9) hours. Hence, a system that experiences one failure in 13,158 hours has a failure rate of 1E9 / 13,158 = 76,000 FITs.[6, 7, 8, 9]

Example: Automotive System with 0.22μ SRAM-Based FPGAs

This example analyzes an in-the-cab ground-based system. Neutron flux densities were calculated for Denver at an elevation of 5,000 feet using SpaceRad 4.5 (a widely used radiation effects prediction software program).

Working from the published radiation data on 0.22μ SRAM-based FPGAs, we have a predicted upset rate of 1.05E-4 upsets per 1M-gate FPGA per day.

If a vendor deploys a 1M gate SRAM-based FPGA in an occupant sensor/airbag control module, we can multiply 1.054E-4 upsets per 1M gate device per day to model 4.38E-06 upsets per system per day, or 4,375 FITs.

This means if the same vendor uses the 1M gate SRAM-based FPGA safety system in 500,000 vehicles, we can multiply the number of upsets (1.05E-4) by the number of vehicles/systems on the road to arrive at a total of 52.5 upsets per day for the population. This translates to an upset every 27.4 minutes, or 2,187,500,000 FITs. Since these are firm errors, they will persist until the SRAM FPGA is reloaded (normally by cycling the power or forcing a reconfiguration). See Table 3 for more information.

Table 3: Upsets per day, 1M gate SRAM-FPGA at 90°N[10, 11, 12, 13]

Process Technology	0 ft. Altitude
0.22μ	3.16E-05
0.18μ	5.02E-05
0.15μ	7.97E-05
0.13μ	1.26E-04

** Projected based on measured 0.22m, 0ft Altitude result*

Using the same system as example 1, it is also possible to calculate the upset rate if the system uses 0.13μ FPGAs. As a point of reference, A 1M-gate 0.13μ SRAM-based FPGA would be subject to 4.19E-4 upsets per day in this environment. This means to scale a component from 0.22μ to 0.13μ increases the components susceptibility to Neutron-induced errors by a factor of four. New sub 100nm geometry devices promise to make the situation worse still. For further reading on this topic, please refer to the reading list in the appendix of this document. JEDEC has also now published a specification covering radiation effects on integrated circuits.[14]

6. *Fuller, E., et al, 1999, "Radiation Test Results of the Virtex FPGA and ZBT SRAM for Space-Based Reconfigurable Computing," MAPLD, Baltimore MD.*
7. *Fuller, E., et al, 2000, "Radiation Characterization, and SEU Mitigation, of the Virtex FPGA for Space-Based Reconfigurable Computing," MAPLD, Baltimore MD*
8. *Mattsson, S. and F. Sturesson 2001, "Radiation Pre-Evaluation of Xilinx FPGA XQVR300," ESA D-P REP-1091-SE.*
9. *Mattsson, S. and F. Sturesson, 2001, "Radiation Evaluation of Power-Up Behavior of Xilinx FPGA XQVR300," ESA D-P REP-1092-SE.*
10. *Fuller, E., et al, "Radiation Test Results of the Virtex FPGA and ZBT SRAM for Space-Based Reconfigurable Computing."*
11. *Fuller, E., et al, "Radiation Characterization, and SEU Mitigation, of the Virtex FPGA for Space-Based Reconfigurable Computing."*
12. *Mattsson, S. and F. Sturesson, "Radiation Pre-Evaluation of Xilinx FPGA XQVR300."*
13. *Mattsson, S. and F. Sturesson, "Radiation Evaluation of Power-Up Behavior of Xilinx FPGA XQVR30.,"*
14. *"Measurement and Reporting of Alpha Particles and Terrestrial Cosmic Ray Induced Soft Errors in Semiconductor Devices." 2001. JEDEC Standard JESD89.*

Actel offers a variety of Flash and antifuse-based FPGAs, which are functionally immune to firm errors. Their unique characteristics have led to their widespread adoption in hostile environments and make them eminently suitable for applications where reliability is a primary design concern.

Security and Tamper Resistance

As FPGAs continue to grow in capability while decreasing in price, they are being used for even more complex and valuable designs within the automotive industry. This trend raises questions about embedded design security, a subject that is coming under increased scrutiny to prevent infringements, counterfeit products, and of greatest concern, tampering. It is important to recognize that vehicle security and reliability begins at the component level. The challenge of risk mitigation from recalls and warranty claims becomes increasingly complex as more and more programmable logic devices become introduced into mainstream automotive electronics. It is critical to understand the benefits and potential risks of all programmable architectures to defend systems against unauthorized hacks, modifications, and tampering.

For example, if a hacker is able to compromise an FPGA-based satellite radio console receiver and disable the user authentication mechanism, unethical users could then access the service for free. The impact this would have to the company's subscription-based revenue model would be severe. One only has to look on a website such as Ebay to purchase a variety of hacked fee-for service consoles. There were over 200 separate listings for cable television descramblers alone at the time this paper was authored. In the Internet age, once a system's security has been defeated, it is not difficult to disseminate malicious or criminal technology for mass consumption. For instance, it is not difficult to imagine the threat of a similar scenario involving an automotive antitheft or security system. How is it possible to ensure that proprietary designs are not compromised? The most effective safeguard is to use secure antifuse or Flash FPGAs from Actel to ensure that sensitive automotive fee-for service and security systems are not compromised.

In high-volume technology markets like the automotive industry, it is understood that the competition will engage in market research and reverse engineering as a means of improving on a competitor's product while avoiding the original design effort.[15] Now the advent of programmable logic in automotive systems means that many new PLD-based systems that previously utilized ASIC technology are now attracting the attention of a new generation of hackers.[16] Beyond the scope of invasion attacks for competitive analysis, this new breed of hackers work to "tune" a variety of automotive products to enhance performance and in the process also often defeat regional or national safety and environmental standards. These unauthorized services are offered through a variety of channels that are difficult if not impossible to control or enforce. Many tuners recalibrate the stock settings in a variety of on-board system components to modify fuel delivery, spark timing, and other control function to increase performance.[17] Often these changes will create a vehicle that operates out of conformance with the manufacturers specifications and warranty guidelines, but savvy tuners could offer the option to reset the factory settings and bring a damaged and overstressed vehicle back into compliance with the manufacturers warranty for the possibility of illegitimate claims. Abating system-reliability concerns from tampering, and preventing your competitors from reverse engineering your valuable Intellectual Property starts with your technology selection. When evaluating FPGAs for your next automotive application, it is critical to understand the strengths and liabilities associated with each competing technology.

---

15. *Shankar, Nitin K., "Can Reverse Engineering Answer Your Design and Prototyping Needs?", India, Brown and Sharp, [online] http://www.brownandsharpe.com/mfg/mfg7/mfg7ar10.html.*
16. *Dipert, Brian, 2000, "Cunning Circuits Confound Crooks," EDN [online] http://www.e-insite.net/ednmag/contents/images/21df2.pdf.*
17. *Bell, A. Graham, 1988, "Modern Engine Tuning" Haynes Publishing; 2nd edition.*

Solutions range from very secure nonvolatile Flash and antifuse architectures to nonsecure SRAM products. Experts agree that antifuse is the most secure technology available. A number of factors complicate attempts to compromise an antifuse FPGA. In order to determine the state of any given fuse, the microscopic size (they cannot be seen optically but require a scanning electron microscope) and the sheer number of the antifuses make it essentially impossible to locate each fuse and identify its programming state. For example Actel's new 2 million gate AX2000 antifuse FPGA contains approximately 53 million antifuses with only 2-5% programmed in an average design. Invasive probing to evaluate each fuse would most likely result in the destruction of the very programmed states needed to trace the design. This means that once you program an antifuse FPGA, no one can read back the contents of your design, or change any of the programming states to "tune" or otherwise change your vital engine control systems.

Certain types of Flash technologies are also extremely secure and definitely more secure than SRAM-based FPGAs. Once a Flash FPGA is programmed, the configuration contents do not need to be reloaded each time power is applied to the system. This differs from SRAM FPGAs that require the additional overhead and expense of extra configuration devices, and special power design considerations to allow for in-rush current spikes and high configuration current draw. As no physical change actually occurs at the silicon level with Flash, it is also virtually impossible to determine the state of a device through intrusive probing surveys. Some suppliers have also taken steps to employ additional protection schemes involving an access key. Actel's new ProASIC^{PLUS} family uses keys that range from 79 bits to 263 bits in length. Once the key is used to secure the Actel ProASIC^{PLUS} device the contents cannot be read without first unlocking the device. Furthermore, the time taken to exhaustively test all key combinations would run into the billions of years.

SRAM-based products are the least secure of all technologies. Since SRAM-based FPGAs are volatile, they must be initialized (or configured) at each power on cycle. The bitstream used to initialize an SRAM FPGA is typically loaded from an on-board configuration device. This bitstream can be intercepted in route at the circuit board level and replicated or altered. This configuration data can be read from the configuration device and manipulated or copied, or the on-board PROM can be replicated. This security back-door is discussed in Internet news groups regularly, which detail the ease with which one can simply read back the internal configuration bitstream through a chip's JTAG or proprietary programming interface.[18] There have been some advanced solutions, utilizing preconfigured FPGAs with a battery back-up, but this approach requires additional board space for batteries and PROM memories, power, reduced reliability (battery life), and can add significantly to overall system complexity and cost, not to mention significant impact to overall system reliability.

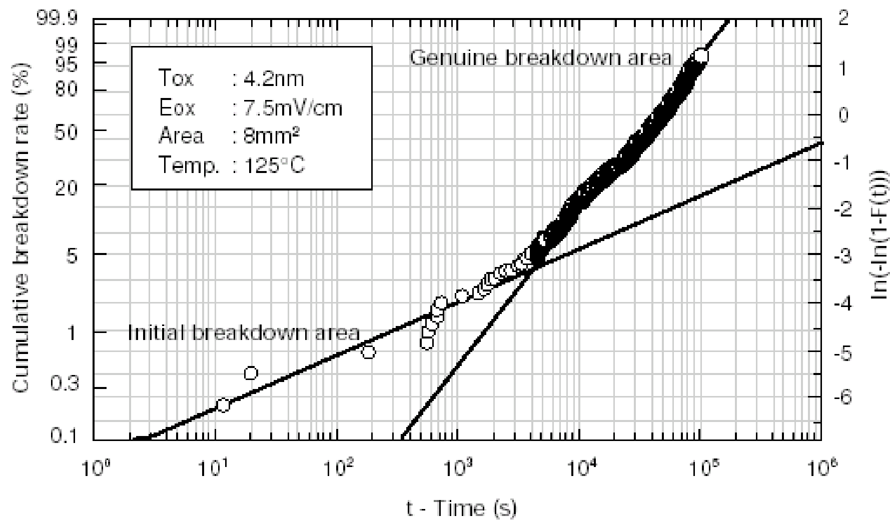
Time Dependent Dialectric Breakdown (TDDB)

Even at normal voltages, continuously applying stress to the gate oxide film of an FPGA will eventually produce insulating film breakdown. This breakdown of the insulating film over time is called time-dependent dielectric breakdown (TDDB). While this phenomenon is generally well understood and modeled for a variety of oxide film densities and process variables, the progression in manufacturing to ever deeper sub-micron technologies like 90nm is increasing the risk of failures in the field. These failures pose a particularly significant threat to automotive systems that employ silicon vendors attempting to leverage using the latest semiconductor process technology.

When defining and expressing the boundaries of semiconductor oxide films, differences in reliability are generally determined by accelerated TDDB evaluation using high voltage stress testing. This makes it possible to evaluate new processes and quickly detect significant manufacturing and process problems. In addition, many high reliability vendors also predict oxide film life from accelerated TDDB data, and then work to optimize screening and test flows to eliminate defective silicon. These methodologies are especially effective for predicting and identifying genuine breakdown areas when all samples rapidly collapse and cease to function after a long period of time. Unfortunately, these methods are

18. Algotronics, "Secure Configuration of Field Programmable Gate Arrays."

much less effective in modeling initial breakdown when failure modes are much more sporadic, especially when bringing up a new process. The problem is this initial breakdown produces the serious result of failure in a short time after the device has entered the market (Figure 3), which could have catastrophic results and implications for safety critical automotive systems, as well as added liability from warranty claims.



Note the sporadic failure modes of the initial breakdown area.

Figure 3: TDDB evaluation results for a 4.2 nm Oxide Film at Constant Voltage[19]

Differences in reliability can be clearly understood for genuine breakdown events. The challenge becomes identifying initial breakdown phenomenon for oxide films, which show no difference at the initial withstand voltage in testing. Any initial testing and qualification from TDDB data only demonstrates the genuine breakdown life limit of the oxide film. While genuine breakdown data may be an important factor in understanding overall component reliability, it provides minimal assurance in determining the product life of an FPGA. This problem is further compounded by the genuine breakdown rates of new, smaller, more cost-effective process geometries. There is increased speculation that time to genuine breakdown and the subsequent device failure may be significantly reducing product life cycles at 90nm to a point that components will be unable to sustain many commercial OEM product life cycle requirements. Should these theories prove true as mainstream FPGA manufacturers move to 90nm fabs, designers of automotive products with stringent quality and extended support models will need to carefully evaluate technology selections that leverage next generation process technologies. An ideal FPGA solution for automotive applications leverages a well-understood technology platform that is not likely to experience unanticipated early dielectric breakdown.

19. Realize Inc., Editor K. Taniguchi, "Silicon Thermal Oxide Films and Their Boundaries," pp.235-240.

Conclusion

FPGAs are achieving wide-scale acceptance as a design solution for next generation automotive electronics. The need for component reliability data is essential to ensure the proper function of the various systems in today's vehicles. While many elements of component reliability are well understood, there are some unique issues that should be factored into the selection process when selecting an FPGA. When designing for demanding automotive environments it is important to identify suppliers that support extended temperature coverage and support defined operating conditions that will ensure thermal problems are eliminated as a source of potential failures. Ensuring sufficient margin in this area can be further mitigated by focusing on suppliers who have demonstrated experience in delivering high reliability products for extraordinary environments like Actel automotive FPGAs with the industry’s highest junction temperature for automotive FPGAs (+150°C).

Technology decision makers must also anticipate sources of failure that will impact systems in the future. Neutron-induced errors can pose a significant reliability risk for many different types of electronic equipment. An upset to one cell in an SRAM FPGA could potentially result in the FPGA losing its configuration. When this occurs, it may cause the host system to malfunction. Neutron-induced firm errors have progressed from being a nuisance to being a significant problem. Future deep submicron manufacturing processes will create substantial challenges for designers of automotive electronics. For designers using SRAM-based FPGAs, it will become necessary to implement circuits to detect and correct configuration errors. This will add to system cost and complexity. Radiation testing data has shown that Actel's antifuse-based and Flash-based FPGAs are not subject to loss of configuration due to neutron-induced upsets. This makes them eminently suitable for all applications where reliability is a concern.

As the complexity of automotive electronics grows, and FPGA usage continues to increase, so the does value of the designs they hold. Intellectual property theft and FPGA tampering pose one of the largest economic threats to the automotive industry. SRAM FPGAs are typically considered susceptible to attacks requiring minimal expertise and equipment and consistently prove inadequate for providing effective design security. On the other hand, nonvolatile Flash and antifuse FPGAs from Actel are even more secure against attack than the ASIC technologies they often target to replace. There are often significant repercussions should a design be compromised and designers are recommended to select an FPGA that will have minimum impact on total system cost while providing higher levels of overall design security.

Early adopters of 90nm FPGA technologies must also anticipate reliability concerns associated with TDDB. The challenges associated with identifying initial breakdown phenomenon for oxide films introduces new potential sources of risk.   It is also important to remember that while genuine breakdown data may be an important factor in understanding overall component reliability, it provides minimal assurance in determining the product life of an FPGA. An ideal FPGA solution for automotive applications leverages a well understood technology platform that is not likely to experience un-anticipated early dielectric breakdown.

Choosing the FPGA for an application involves many trade-offs and an informed designer must evaluate, density, packaging, product features, initial cost, lifetime support cost, availability and reliability.

Bibliography

Alfke, P, P. Dyreklev, K. Johansson, and M. Ohlsson. 1998. "Neutron Single Event Upsets in SRAM-based FPGAs," NSREC.

Algotronics. "Secure Configuration of Field Programmable Gate Arrays."

Bell, A. Graham. 1988. "Modern Engine Tuning." Haynes Publishing; 2nd edition.

Boos, A, R. Constapel, and W. Wondrak. DaimerChrysler AG, Reserarch and Technology. J. Wilde University of Freiburgn. Inst. For Microsystem Technology "Design for Reliability in Automotive Electronics Part I: Semiconductor Devices."

Constapel, R, J. Freytag, P. Hille, V. Lauer and W. Wondrak. 2000."High Temperature Electronics for Automotive Applications." CIPS 2000, 20.-21.6.2000. Bremen.

"Design Guidelines for Reliable Surface Mount Technology Printed Board Assemblies." 1996. IPC-D-279, IPC.

Dipert, Brian. 2000. "Cunning Circuits Confound Crooks." *EDN* [online] http://www.e-insite.net/ednmag/contents/images/21df2.pdf.

Fuller, E. et al. 2000. "Radiation Characterization, and SEU Mitigation, of the Virtex FPGA for Space-Based Reconfigurable Computing," (MAPLD, Baltimore, MD).

Fuller, E. et al. 1999. "Radiation Test Results of the Virtex FPGA and ZBT SRAM for Space-Based Reconfigurable Computing." MAPLD, Baltimore MD.

Mattsson, S and F. Sturesson. 2001. "Radiation Pre-Evaluation of Xilinx FPGA XQVR300," ESA D-P REP-1091-SE.

Mattsson, S and F. Sturesson. 2001. "Radiation Evaluation of Power-Up Behavior of Xilinx FPGA XQVR300," ESA D-P REP-1092-SE.

"Measurement and Reporting of Alpha Particles and Terrestrial Cosmic Ray Induced Soft Errors in Semiconductor Devices." 2001. JEDEC Standard JESD89.

Realize Inc. Editor K. Taniguchi. "Silicon Thermal Oxide Films and Their Boundaries." pp.235-240

Shankar, Nitin K. "Can Reverse Engineering Answer Your Design and Prototyping Needs?" .India, Brown and Sharp. [online] http://www.brownandsharpe.com/mfg/mfg7/mfg7ar10.html.

For more information concerning neutron-induced firm errors, refer to the following documents:

Cronquist, Brian et al. 2000. Radiation-Hardened/High Reliability Programmable Logic Using Modified Commercial off the Shelf: RTSX32S. MAPLD, Baltimore, MD.

McCollum, John. 1999. Programmable Elements and Their Impact on FPGA Architecture, Performance, and Radiation Hardness. MAPLD, Baltimore, MD.

Speers, Ted et al. 1999. 0.25µ Flash Memory Based FPGA for Space Applications. MAPLD, Baltimore, MD.

Wang, J. J. et al. 2000. Radiation Effects on Flash Memory Based FPGA. MAPLD, Baltimore, MD.

Wang, J. J. et al. 2000. Radiation Tests and Results of a Rad-Tolerant Antifuse FPGA RT54SX. RADECS, Belgium.

Wang, J. J. et al. 2002. Single Event Effects of a Flash Based FPGA. SEE Symposium, Manhattan Beach CA.

Wang, J. J. et al. 2001. Single Event and Total Dose Effects on SEU Hardened Antifuse FPGA. MAPLD, Baltimore, MD.

Wang, J. J. et al. 1999. Total Dose and SEE of Metal-To-Metal Antifuse FPGA. MAPLD, Baltimore, MD.

For more information concerning design security in FPGAs, refer to the following documents:

Abraham, D.G., G.M. Dolan, G.P. Double, and J.V. Stevens. 1991. Transaction Security System. *IBM Systems Journal* vol. 30 no. 2 New York: International Machines Business Corporation: 206-229.

Anderson, Ross J. 2001. Security Engineering: A Guide to Building Dependable Distributed Systems. New York: John Wiley and Sons.

Blythe, S., B. Fraboni, S. Lall, H. Ahmed, U. de Riu. 1993. Layout Reconstruction of Complex Silicon Chips. *IEEE Journal of Solid-State Circuits* vol. 28 no. 2 (Feb. 1993): 138-145.

FBI Congressional Statement. 2000. Statement for the Record of Guadalupe Gonzalez Special Agent In Charge, Phoenix Field Division Federal Bureau of Investigation on Cybercrime. [online]. Washington, D.C.: FBI. [cited 12 August 2002] Available from World Wide Web: http://www.fbi.gov/congress/congress00/gonza042100.htm.

Federal Bureau of Investigation the Financial Institution Fraud Unit. 2002. Financial Institution Fraud. In About Intellectual Property Crimes [online]. Washington D.C.: FBI, [cited 12 August 2002] Available from World Wide Web: http://www.fbi.gov/hq/cid/fc/fifu/about/about_ipc.htm.

Actel Resource Center

As FPGAs continue to displace ASICs, designers face new challenges. Not all FPGA technologies are the same, and not all FPGA solutions offer true ASIC features. Actel's Resource Center provides designers with current and relevant information on a wide variety of FPGA related topics. The resource center targets New as well as experienced FPGA designers, ASIC designers and former ASIC designers and System architects. Topics covered include: Design Security, Soft/Firm Errors, Packaging, Power.

Details available at: http://www.actel.com/products/rescenter/index.html

For more information, call **1.888.99.ACTEL** or visit our website at **http://www.actel.com**

www.actel.com

Actel Corporation

2061 Stierlin Ct.
Mountain View, CA 94043-4655
USA
Tel: (650) 318-4200
Fax: (650) 318-4600

Actel Europe Ltd.

Dunlop House, Riverside Way
Camberley, Surrey GU15 3YL
United Kingdom
Tel: +44 (0)1276 401450
Fax: +44 (0)1276 401490

Actel Japan

EXOS Ebisu Bldg. 4F
1-24-14 Ebisu Shibuya-ku
Tokyo 150 Japan
Tel: +81 03-3445-7671
Fax: +81 03-3445-7668

Actel Hong Kong

39th Floor
One Pacific Place
88 Queensway
Admiralty, Hong Kong
Tel: 852-22735712

© 2003 Actel Corporation. All rights reserved. Actel and the Actel logo are trademarks of Actel Corporation. All other brand or product names are the property of their respective owners. 51700050-0/9.03