WP412 (v1.1) October 16, 2013

The Xilinx Isolation Design Flow for Fault-Tolerant Systems

By: John D. Corbett

The ability to control system failure modes through fault-tolerant design requires an implementation methodology that ensures fault propagation can be controlled. Xilinx® Isolation Design Flow (IDF) provides fault containment at the FPGA module level, enabling single-chip fault tolerance by various techniques including:

- Modular redundancy
- Watchdog alarms
- Segregation by safety level
- Isolation of test logic for safe removal

IDF, pioneered for government cryptographic systems, is also appropriate for avionics, safety-related electronics, industrial robotics, critical infrastructure, financial systems, and other high assurance, high availability, and high reliability systems. The IDF is part of a spectrum of reliability technologies that when appropriately combined provide unmatched reliability, performance, and cost effectiveness.

More Automation and More at Stake

Modern life increasingly depends on automated systems. When systems fail, lives and fortunes can be at risk. The threats include natural disasters, human error, and intentional attacks as well as simple hardware failures. In all cases, attention to failure modes across the life cycle of the system can allow the user to avoid or mitigate disasters [Ref 1] [Ref 2] [Ref 3].

Massive Increase in Device Capacity

As Gordon Moore observed over half a century ago, computing capacity has been increasing at an exponential rate [Ref 4]. Xilinx offers the largest integrated circuits (IC) in history, with almost seven billion transistors in its largest device [Ref 5]. Increased device capacity and increasing power/performance requirements generate pressure to combine more features in fewer devices. When features formerly implemented in multiple devices are combined within a single FPGA device, it is no longer obvious that the features can be implemented independently.

FPGA Reliability

Xilinx has a long-standing practice of publishing quality testing data, including single-event upsets (SEU) upset rate measurements [Ref 6]. Despite the spectacular increases in Xilinx device capacity, Xilinx has decreased overall device hardware error rates through extensive research and careful design. This trend for Xilinx device reliability is projected to continue for the foreseeable future. However, low intrinsic error rates are not always sufficient for applications requiring fault-tolerance. Xilinx offers a spectrum of hard and soft options to increase system reliability, including the IDF.

Redundancy for Increased Reliability

If system failure can be made contingent on multiple independent subsystem failures, reliability can be improved by many orders of magnitude. For example, a system composed of two redundant subsystems in parallel has a probability of failure equal to the product of the probabilities of each of the subsystems failing. If the subsystems both had probability of failure of 10^{-9}, then the system has a probability of failure of $10^{-9} \times 10^{-9} = 10^{-18}$, many orders of magnitude lower than the subsystem failure rate [Ref 7].

This calculation assumes the failure probabilities are independent, that is to say, the subsystems do not have a single point of failure or common failure mode. This isolation or independence is the purpose of the IDF.

However, the independence provided by IDF does not cover design defects. Identical redundant defective designs can fail in identical ways, so techniques to ensure correctness and diverse implementations must be carefully considered [Ref 8].

The Isolation Design Flow

Without a painstaking analysis of the Xilinx FPGA architecture and the way modules are implemented in the FPGA, it is impossible to say whether redundant modules are independent or not with respect to single points of failure. Xilinx has performed this analysis. As a result, Xilinx was the first FPGA manufacturer to obtain public acknowledgement by the National Security Agency of the United States that Xilinx devices are approved for use in Type 1 Cryptographic Systems [Ref 9]. The IDF enables Xilinx devices to be used in critical applications, the failure of which could cause exceptionally grave damage to national security. Xilinx has had three generations of FPGAs approved since 2007 (Virtex®-4, Virtex-5, and Spartan®-6 devices). Support for the 7 series FPGAs and Zynq®-7000 AP SoCs is now available [Ref 10] [Ref 11].

Xilinx has achieved TÜD SÜD certification for the "FPGA Programming Tool Chain of the ISE Design Suite" as a "Software Tool for Safety Related Development" certificate number Z10 13 04 84605 001. This certification means a significant reduction in risk, schedule, and cost for customers building IEC 61508- or ISO 26262-certified equipment. The IDF is an integral part of the Xilinx safety concept.

The IDF and related materials were subjected to an independent verification and validation (IV&V) over a period of several years. The IV&V encompassed comprehensive review, analysis, and testing performed by an objective third party to confirm that the requirements are correctly defined and to confirm that the system correctly implements the requirements. This analysis covered all aspects of the Xilinx FPGA solution related to reliability and security, running the gamut from process technology, to circuit design, to tool implementation, to development flow.

The genesis of this work is described in reference material [Ref 12]. Since then, the analysis techniques have been improved. The analysis strategy is tied to tessellation architecture of the FPGA. The basic architecture of the FPGA is a two-dimensional array of tens of thousands of tiles, but only tens of types of tiles. Analysis of the tile types is used to prove that the influence of a module can be geometrically bounded to the tiles the module occupies if the module is separated from other modules by a fence of unused tiles.

Xilinx has implemented routing constraints that guarantee a fence can be constructed to provide isolation between design modules. The Xilinx Isolation Verification Tool (IVT) is an independently implemented design rule checker that reports on the status of isolation requirements and visualizes the floorplan, both as specified and as implemented [Ref 13].

Figure 1 shows how isolation violations appear in the IVT output. The design floorplan is on the left and a magnified view of the area in the box is on the right. Every tile containing configuration information that violates isolation rules is marked with an '×'.

Logic elements associated with more than one isolation group are highlighted in orange. The design in Figure 1 was constructed intentionally to violate the design rules as a test case. Violations are also detailed in a textual report generated by IVT.

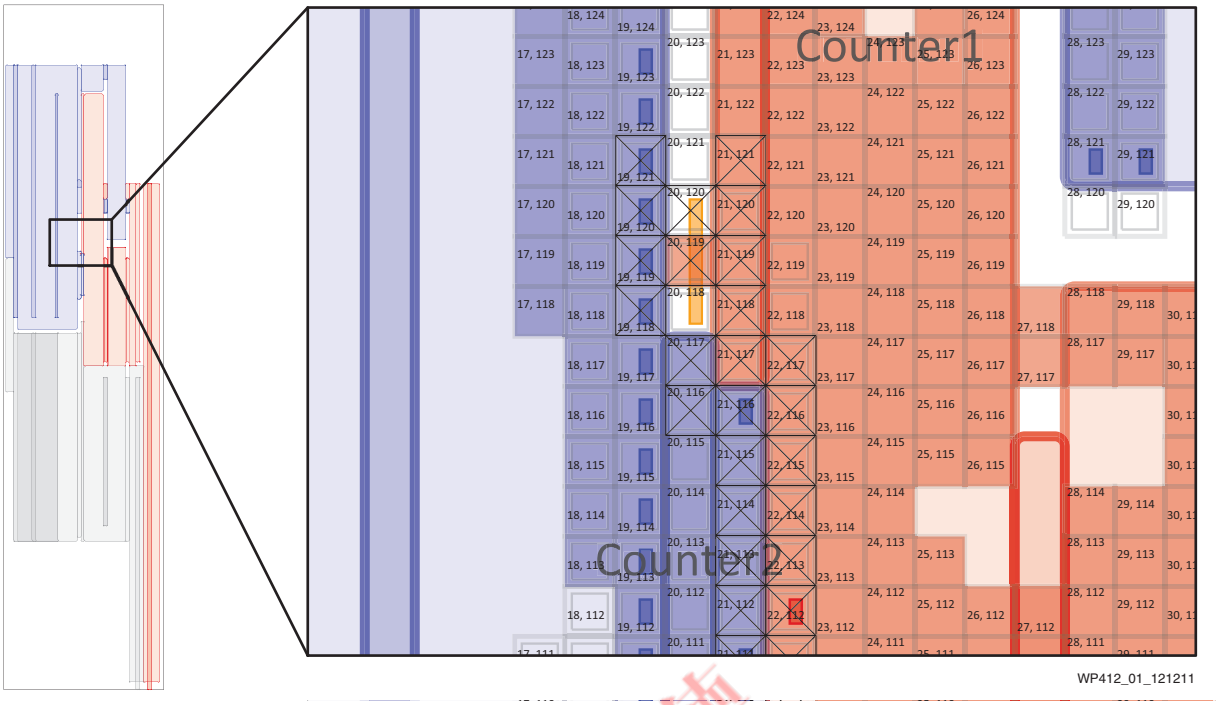

Figure 1: **Floorplan Detail Showing Isolation Violations**

Inherent Limitations in Reducing Device Counts

There are a few inherent disadvantages of combining redundant functions within a single device. For systems exposed to mechanical forces, such as avionics, it can be desirable to place redundant systems in physically separated zones of the aircraft. Redundancy within a single IC obviously cannot address this requirement.

Although it is unlikely for power to fail at the individual IC level, there is nothing that the internal programming of an individual device can do to mitigate this, whether through IDF or other design hardening techniques. System-level solutions such as heartbeat and watchdog functionality can be used to mitigate this risk if needed.

The programmable nature of the clock trees creates the possibility that a configuration memory upset could disable any branch of a clock tree, from the root down to a leaf. Clock failures fall into three qualitative categories: global, intermediate, and local. Global clocking failures are akin to power loss—any mitigation must involve a higher system level. Local failures are mitigated completely by the IDF. Intermediate failures can be mitigated with a combination of the IDF and careful design.

While a complete description of techniques for mitigating risks associated with partial clock failures is beyond the scope of this document, solutions are likely to involve several ideas:

- Use of software features to estimate the number of memory cells used for clock tree configuration as compared to the total design
- Fault-injection via the SEM IP or accelerated SEU testing to characterize the actual failure modes resulting from configuration memory upsets
- Attention to the physical layout of clock trees versus the floorplan of isolated modules
- Use of redundant internal or external watchdog alarms

- Use of redundant clocks, e.g., an internal clock constructed from ring oscillators
- Use of diverse redundancy, e.g., time shifting redundant functions so that a partial clock failure affects the redundant functions differently
- Use of techniques to detect and correct configuration memory

Protecting Configuration Memory

The independence guaranteed by the IDF assumes errors in configuration memory are not permitted to accumulate over time. Configuration memory can be protected in several ways. Dedicated error checking for configuration memory and access to configuration memory from inside the design make it is possible to incorporate soft IP such as the Xilinx SEM IP [Ref 14] or the Xilinx Security Monitor IP [Ref 15] to monitor and react to configuration memory errors. It is possible to use either an internal or external configuration controller to rewrite configuration memory without stopping device operation. This capability for correcting configuration errors can also be used for fault-injection testing using the SEM IP. Some devices offer hardware error detection and correction [Ref 16] [Ref 17]. Soft error processing can be optimized by ignoring "Don't Care" configuration memory bits with the new "Essential Bits Mask" feature of the Xilinx configuration bitstream generation software BitGen. Dynamic Partial Reconfiguration can be used to replace a module without interrupting the functioning of other modules.

For devices intended to operate in high-radiation environments, the Xilinx TMRTool software automates the creation of triple-modular redundant designs [Ref 18].

Fault-Tolerant Design Considerations

IDF provides a transparent way to eliminate single points of failure between redundant modules within a single FPGA, however, fault-tolerant design must be considered at the system level. These considerations include:

- **Requirements:** Standards, traceability, and certification
- **Fault-tolerance:** Failure mode and effect analysis, module decomposition, floorplanning, fault containment, reduced functionality modes, redundant alarms, checkpointing, failover/failback, configuration scrubbing, memory error detection and correction, and built-in self-test
- **Security:** Confidentiality, integrity, availability, authentication, non-repudiation, and utility
- **Development methodology:** Tools and practices, tool settings for reliability, and documentation
- **Life cycle planning:** Ongoing testing, enhancement planning, repairs strategy, and supply chain risk management
- **Validation and verification:** Test automation, design for test, diagnostic logging, and formal verification

Applications

Although IDF was originally developed as part of the Xilinx Single Chip Cryptography flow, fundamentally, the requirements driving the technology are fault-tolerance requirements. Good cryptographic system design assumes any part can fail, but by design the failure will not be silent and will not compromise security. For such Information Assurance applications, security and safety are closely related.

For applications primarily concerned with safety, the same foundation is useful. Failure alarms can be used to initiate fail-safe modes. For example, if a fault is detected in a redundant function of the device, the system can switch to a secondary function until the primary function completes automated repair and reset procedures.

For DO-254, IEC 61508, ISO 10218-1, or other safety/security certifications, the Xilinx IDF provides a foundation for asserting that failure modes of functions within a device are statistically independent. Coupled with quantitative fault rate data provided in the Xilinx Device Reliability Report [Ref 6], designers can engineer to the required Design Assurance Level (DAL), Safety Integrity Level (SIL), or Evaluation Assurance Level (EAL). Xilinx has achieved TÜV SÜD certification for IEC 61508 and ISO 26262. Xilinx offers a DO-254 and DO-178 certifiable MicroBlaze soft processor with optional dual-lockstep capability using the IDF [Ref 19].

For mission-critical systems that are concerned with reliability, integrity, and availability such as stock exchanges, inter-bank funds transfers, and other systems subject to high financial risk, IDF can be used to construct fault-tolerant designs with FIT rates approaching the device hardware FIT rate.

For systems concerned with cost-effective reliability, faults can be monitored by isolated logging modules. Log data can be used to assess the actual cost of reliability mechanisms such as modular redundancy or error correcting codes. Reprogrammability makes it possible to improve reliability of fielded systems based on the analysis of actual system performance data.

For systems concerned with correctness, redundant computations can be performed by diverse means and compared.

For systems concerned with maximizing availability, independent monitoring functions can initiate fail-over, reset, and fail-back functions.

Conclusion

The Xilinx Isolation Design Flow (IDF) is a technology appropriate for fault-tolerant systems, including high assurance, high availability, and high reliability systems. The IDF provides increased guarantees over the intrinsic device reliability that the failure modes of redundant modules within a single device can be made statistically independent through floorplanning and routing constraints, thus eliminating virtually all single points of failure within the device and providing control over the FPGA failure modes. When combined with configuration memory monitoring, the IDF flow enables designers to drive down the failure rate due to Single Event Effects and localized defects below the intrinsic device failure rate. When combined with fault-tolerant systems architecture, even the most demanding reliability targets can be achieved with Xilinx technology.

More Resources

1. *Avionics/DO-254*, http://www.xilinx.com/applications/aerospace-and-defense/avionics/
2. WP365, *Solving Today's Design Security Concerns*
3. *Secure Solutions*, http://www.xilinx.com/applications/aerospace-and-defense/secure-solutions/index.htm
4. *Single Event Upsets*, http://www.xilinx.com/products/quality/single-event-upsets.htm

References

1. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* The White House. [Online] 2009. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
2. Stouffer, Keith; Falco, Joe; and Kent, Karen. *Guide to Industrial Control Systems (ICS) Security.* Computer Security Division, NIST. 2011. http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.
3. *Security Requirements for Cryptographic Modules.* Computer Security Division Computer Security Resource Center. [Online] Revised DRAFT 09/11/09, September 11, 2009. http://csrc.nist.gov/publications/drafts/fips140-3/revised-draft-fips140-3_PDF-zip_document-annexA-to-annexG.zip.
4. Moore, Gordon E. *Cramming More Components into Integrated Circuits.* Electronics, 1965.
5. Merrit, Rick. *Upcoming Xilinx FPGA shows 3-D IC progress*. EE Times. [Online] September 8, 2011. http://www.eetimes.com/electronics-news/4219726/Upcoming-Xilinx-FPGA-shows-3-D-IC-progress.
6. UG116, *Device Reliability Report.*
7. Von Neumann, J. *Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components*, Automata Studies, ed. C. Shannon, pp. 43–98. Princeton University Press, 1956.
8. Lübek, Lennart, et al. *Ariane 5 Flight 501 Failure Report.* [Online] July 19, 1996. http://esamultimedia.esa.int/docs/esa-x-1819eng.pdf.
9. *NSA Approved Defense-Grade Spartan®-6Q FPGA in Production for Highest Level Cryptographic Capabilities Strengthens Xilinx Secure Leadership.* Xilinx, Inc. website. [Online] August 31, 2011. http://investor.xilinx.com/phoenix.zhtml?c=212763&p=irol-newsArticle&ID=1601746&highlight=.
10. XAPP1085, *7 Series Isolation Design Flow Lab Using ISE Design Suite 14.4.*
11. XAPP1086, *Developing Secure and Reliable Single FPGA Designs with Xilinx 7 Series FPGAs Using the Isolation Design Flow.*
12. McLean, Mark and Moore, Jason. *FPGA-Based Single Chip Cryptographic Solution (U).* Military Embedded Systems. [Online] 2007. http://www.mil-embedded.com/pdfs/NSA.Mar07.pdf.
13. XAPP1145, *Developing Secure Designs with the Spartan-6 Family Using the Isolation Design Flow.*
14. *Soft Error Mitigation (SEM) Core.* [Online] Xilinx, Inc. http://www.xilinx.com/products/intellectual-property/SEM.htm.

15. Peterson, Ed. *Developing Tamper Resistant Designs with Xilinx Virtex®-6 and 7 Series FPGAs.* [Online] 1.0, September 21, 2011. http://www.xilinx.com/support/documentation/application_notes/xapp1084_tamp_resist_dsgns.pdf.
16. Virtex-6 FPGA Family. [Online] Xilinx, Inc. [Cited: November 15, 2011.] http://www.xilinx.com/products/silicon-devices/fpga/virtex-6/index.htm.
17. 7 Series FPGAs. [Online] Xilinx, Inc. [Cited: November 15, 2011.] http://www.xilinx.com/innovation/7-series-fpgas.htm.
18. TMRTool. [Online] Xilinx, Inc. http://www.xilinx.com/ise/optional_prod/tmrtool.htm.
19. XAPP584, *Spartan-6 FPGA Dual-Lockstep MicroBlaze Processor with Isolation Design Flow.*

Revision History

The following table shows the revision history for this document:

Date	Version	Description of Revisions
01/30/12	1.0	Initial Xilinx release.
10/16/13	1.1	Updated FPGA Reliability, The Isolation Design Flow, Protecting Configuration Memory, Applications, and References.

Notice of Disclaimer