White Paper

Enabling Design Separation for High-Reliability and Information-Assurance Systems

Traditionally, system designs achieve reliability through redundancy, which leads to increased component count, logic size, system power, and cost. Altera's design separation feature meets these conflicting needs for low power, small size, and high functionality while maintaining high reliability and information assurance.

Introduction

FPGAs are an ubiquitous part of today's processing technology. Their use has grown from traditional glue logic interfaces of the past to the most advanced information-processing systems used by core Internet routers and high-performance computing systems. What remains common throughout this evolution is the desire to integrate more functionality in less space while decreasing power and cost.

High-reliability system design has experienced a similar need to reduce system size, power, and cost while maintaining expected reliability. Traditionally, these system designs have achieved reliability through redundancy. This redundancy manifests itself though increased component count, logic size, system power, and cost. These same reliability requirements and attributes are shared by other system design areas including: information assurance, avionics, and industrial safety systems.

Altera has developed a solution to meet these conflicting needs while maintaining the high reliability and information assurance these applications require. The design separation feature in Altera® Quartus® II design software and the Cyclone® III LS FPGAs provides designers an easy method of collapsing the established high-reliability redundant design methodologies into a single-chip FPGA-based architecture.

The Need for Fault Tolerance

The need for reliability engineering has been driven by the Department of Defense (DoD) since it studied the availability of Army and Navy equipment during World War II. For example, the mean time to failure (MTBF) of a bomber was found to be less than 20 hours, while the cost to repair the bomber was over ten times its original purchase price. Since then, the concept of total life-cycle cost in a system design has been used as a critical metric in design and system selection.

High-assurance cryptographic systems have a similar historical context. Failures in a cryptographic system affect the total life cycle of the system in terms of security for military systems and commerce for commercial systems. In this context, high-assurance cryptographic systems have similar design and analysis requirements as high-reliability systems.

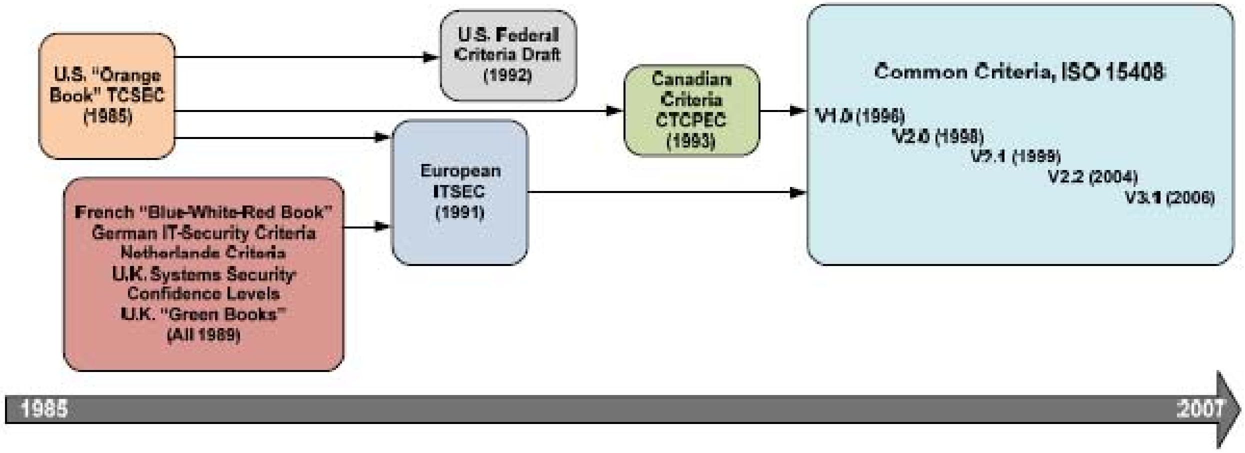
In each case, the designer's goal is to shrink the PCB size and number of components needed for a particular application. This has been the trend in the electronics industry for decades, first with system-on-chip (SoC) ASIC solutions and progressing to SoC FPGA solutions. The first step consolidated external digital logic into a single device. This paradigm progressed successfully until the cost and schedules of ASIC development exceeded market cost and time factors. With ASIC costs growing, system designers increasingly turn to FPGAs where performance and logic densities enable logic consolidation onto a reprogrammable chip. While the growth in SoC designs has been steady for many years, the design and complexity of FPGAs has precluded the integration of redundant designs. The analysis necessary to verify separate and independent datapaths was considered an intractable problem by many system and security analysts.

By working with certification authorities, Altera has eliminated the intractability of complex FPGA device analysis and ensured separate and independent datapaths. By seeking to design FPGA tools and data flows with this analysis in mind from the start, a designer can consolidate fail-safe logic designs into a single FPGA fabric. This allows the designer not only to meet the market goals of SoC, but also the requirements of high-reliability and high-assurance applications.

Information-Assurance Applications

Proliferating information-assurance equipment requires users to have a level of trust in the design and implementation of the cryptographic equipment. Guaranteeing a complex system design is trustworthy requires the establishment of design standards and system evaluation. Several security-design standards and evaluation bodies exist. While explaining the design requirements and evaluation criteria of each is beyond the scope of this paper, an overview of their evolution and complexity is shown in Figure 1.

Figure 1. Security Criteria Design and Analysis Evolution


U.S. "Orange Book" TCSEC (1985)
U.S. Federal Criteria Draft (1992)
Canadian Criteria CTCPEC (1993)
Common Criteria, ISO 15408
V1.0 (1996)
V2.0 (1998)
V2.1 (1999)
V2.2 (2004)
V3.1 (2006)
European ITSEC (1991)
French "Blue-White-Red Book"
German IT-Security Criteria
Netherlands Criteria
U.K. Systems Security Confidence Levels
U.K. "Green Books"
(All 1989)
1985
2007

Information technology (IT) systems have the most pronounced affect on information assurance. With an ever-increasing number of infrastructure-control systems as well as corporate and personal information accessible via the Internet, IT systems increasingly are relied on to protect sensitive information and systems from a global hacker community.

To provide information assurance on the Internet, a user must not only inspect data for virus protection, but also protect sensitive information using IPSec, HTTPS, and other applications. While the HTTPS cryptographic algorithm typically is implemented in software running on a computer platform, IPSec and Virtual Private Network (VPN) encryption applications typically require higher performance and rely more heavily on cryptographic hardware. The evaluation of network IT equipment is necessary to ensure trust in the overall system.

This trust must be proven by hardware analysis of each IT component, with information-assurance levels meeting the security requirements of either the Common Criteria or Federal Information Processing Standard (FIPS) 140-2 or 140-3. The complexity of such analysis is nontrivial, as can be seen in Figure 1. Due to such thorough evaluations, the design cycles on these systems can be significant.

Table 1. FIPS 140-2 Security Requirements Summary

#	Section	Security Level 1	Security Level 2	Security Level 3	Security Level 4
1	Cryptographic module specification	Specification of cryptographic module, cryptographic boundary, approved algorithms, and approved modes of operation Description of cryptographic module, including all hardware, software, and firmware components Statement of module security policy			
2	Cryptographic module ports and interfaces	Required and optional interfaces Specification of all interfaces and of all input and output datapaths		Data ports for unprotected critical security parameters logically separated from other data ports	
3	Roles, services, and authentication	Logical separation of required and optional roles and services	Role-based or identity-based operator authentication	Identity-based operator authentication	
4	Finite state model	Specification of finite state model Required states and optional states State transition diagram and specification of state transitions			
5	Physical security	Production-grade equipment	Locks or tamper evidence	Tamper detection and response for covers and doors	Taper detection and response envelope EFP and EFT
6	Operational environment	Single operator Executable code Approved integrity technique	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling	Referenced PPs plus trusted path evaluated at EAL4
7	Cryptographic key management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization			
		Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
8	EMI/EMC	7 CFR FCC Part 15, Subpart B, Class A (Business use) Applicable PCC requirements (for radio)		7 CFR FCC Part 15, Subpart B, Class B (Home use)	
9	Self tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests, conditional tests		Statistical RNG tests callable on demand	Statistical RNG tests performed at power-up
10	Design assurance	Configuration management (CM) Secure installation and generation Design and policy correspondence Guidance documents	CM system Secure distribution Functional specification	High-level language implementation	Formal model Detailed explanations (informal proofs) Preconditions and postconditions
-	Mitigation of other attacks	Specification of mitigation of attacks for which no testable requirements currently are available			

Commercial Cryptography

The financial industry is a driving force behind commercial cryptography and cryptographic equipment. The need for information assurance is pervasive, as the industry has grown from developing security for inter- and intra-bank electronic data interchange (EDI) transactions, to public automatic teller machines (ATMs), to high-performance cryptographic applications driving electronic commerce.

Similar to the military's need for information assurance, commercial electronic commerce needs commonly accepted standards for the design and evaluation of cryptographic hardware. The financial industry's need for cryptographic interoperability has been a key differentiator in this market. Commerce extends beyond national boundaries and so must the cryptographic equipment developed for this market. Complicating the commercial security picture is the classification of cryptography as a regulated technology under the International Traffic in Arms Regulations (ITAR). High-performance electronic-commerce cryptographic equipment is developed mainly by large server manufacturers, such as IBM and Sun, that can invest in the expertise and long design cycles necessary to create FIPS 140-2-certified cryptographic modules.

High-Reliability Applications

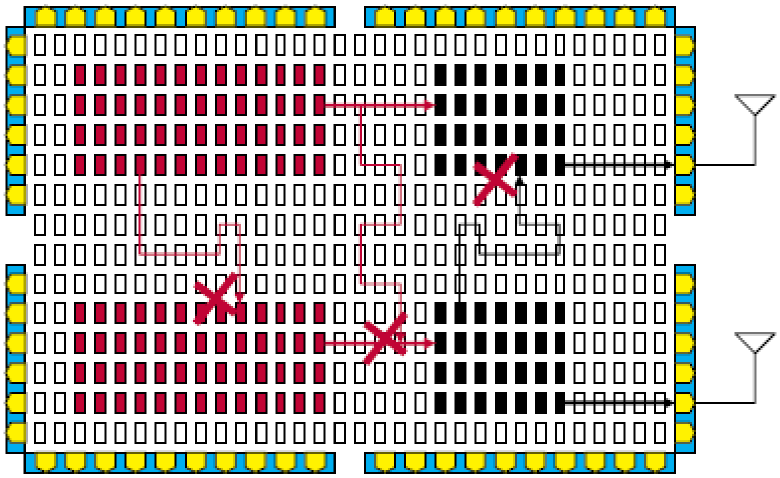
Industrial applications also take advantage of the design separation and independence available with Altera FPGAs. For example, increasing numbers of embedded control units (ECUs) are used in automobiles, with increasing complexity and functionality. Due to the competitive nature of the auto industry, ECU designers must maintain reliability while reducing size and cost. Having the ability to separate redundant logic within a single FPGA allows system designers to reduce the number of hardware components while maintaining fault isolation.

The Design Separation Solution

Information-assurance and high-reliability applications currently require at least two chips to ensure the logic remains separate and functions independently of the other. This ensures that a fault detected in one device does not affect the remainder of the design. In cases where design separation is critical—such as financial applications, where data must be encrypted—data must not be able to leak from one portion of the design to another in the event of an inadvertent path created by a fault. In cases where high reliability is critical— such as industrial systems where entire manufacturing lines may be shut down if one piece of equipment fails—redundant circuits continue to control the system in the event of one circuit failing, ensuring little to no downtime.

The design separation feature in the Quartus II design software allows designers to maintain the separation of critical functions within a single FPGA. This separation is created using the Altera's LogicLock™ feature, which allows designers to allocate design partitions to a specific section of the device. When the design separation flow is enabled, as shown in Figure 2, each secure partition has an automatic fence, or "keep out" region, associated with it. In this way, no other logic can be placed in the proximity, creating one level of increased fault tolerance.

Figure 2. Design Separation for High Reliability and Information Assurance



However, to ensure true separation, the routing also must be separated. Therefore, all routing is restricted to the LogicLock area of the design partition. This means that the fence region is void of all logic and routing, ensuring physical isolation from any other function in the device. This is effectively the same as using two physical devices to ensure separation.

Altera has designed, rigorously evaluated, and optimized the Cyclone III LS fabric architecture to ensure the separation results in an increased fault tolerance with the minimal fence size, enabling designers to use over 80 percent of the resources for their design. The design separation flow also enables specific banking rules that ensure the separation created in the fabric for critical design partitions extends to the I/Os. The Cyclone III LS packages also are designed to support such I/O separation.

Summary

There are many design requirement similarities between high-reliability and information-assurance systems. Both systems require design separation and independence, as each system requires redundancy to ensure proper design operation in the event of hardware faults. Traditionally, the implementation of redundancy increases system size, weight, power, and costs because this redundancy is implemented at the board level. To reduce these factors, low-power FPGA processes are used with a high-assurance design flow to meet stringent NSA FSDA requirements.

By ensuring design separation and independence, redundant logic can be transferred from the board level to a single FPGA device as part of a SoC design approach. Combining low power, high logic density, and design-separation features allows developers of high-reliability, high-assurance cryptographic and industrial systems to minimize design development and schedule risk by using reprogrammable logic, and to improve productivity by using a proven incremental-compile design flow.

Further Information

- Cyclone III FPGAs—Security:
  www.altera.com/products/devices/cyclone3/overview/security/cy3-security.html
- Webcast: "Partitioning FPGA Designs for Redundancy and Information Security":
  www.altera.com/education/webcasts/all/wc-2009-partitioning-fpga-redundancy.html
- Literature: Cyclone III Devices:
  www.altera.com/products/devices/cyclone3/literature/cy3-literature.jsp
- *AN 567: Quartus II Design Separation Flow:*
  www.altera.com/literature/an/an567.pdf
- *Protecting the FPGA Design From Common Threats*:
  www.altera.com/literature/wp/wp-01111-anti-tamper.pdf
- Quartus II Subscription Edition Software:
  www.altera.com/products/software/quartus-ii/subscription-edition/qts-se-index.html

Acknowledgments

- Paul Quintana, Sr. Technical Manager, Military Business Unit, Altera Corporation
- Juwayriyah Hussain, Sr. Product Marketing Engineer, Low-Cost Products, Altera Corporation

ALTERA®
101 Innovation Drive
San Jose, CA 95134
www.altera.com