WP461 (v1.0) April 9, 2015

Xilinx Reduces Risk and Increases Efficiency for IEC61508 and ISO26262 Certified Safety Applications

By: Ed Hallett, Giulio Corradi, Steven McNeil

Integrated safe/non-safe functionality is possible in a single device. Offering today's best-in-class tools and techniques, Xilinx makes IEC/ISO safety certification readily achievable.

ABSTRACT

This white paper introduces key dependability aspects for industrial and automotive customers who are designing and developing programmable electronic equipment for safety applications using Xilinx® FPGA and SoC devices. The main focus of this white paper is to explain how to create solutions with highly integrated, high-performance certifiable systems that target IEC 61508 / ISO 26262 norms. The goal is to achieve reduced risk, improved compliance, decreased certification time, and lower system cost.

The designer is guided through:

- The key dependable attributes of a safety design
- How to use Xilinx technologies and methodologies to solve fundamental challenges relating to the design of safety systems

Definition, partitioning, and verification procedures, carefully developed by Xilinx over the past decade, are described in detail. Employing these proven tools and processes results in safety block design elements that are certifiable as Functionally Safe.

This white paper shows how Xilinx quality and reliability data, published regularly for decades, is the cornerstone of the quantification of a safety design, including FIT rates and upset mitigation. Applying the All Programmable nature of Xilinx devices allows creation of architectures and functions tailored to meet dependability goals and requirements.

With the Xilinx development tool chain and Isolation Design Flow (IDF) methodology, designs benefit from the implementation of diverse channels and channel redundancy, the reduction of common cause failures, and mitigation of random errors, resulting in unmatched system security and dependability.

Introduction

Business Context

In today's economic environment, manufacturers are under immense pressure to contribute value by cutting costs and improving productivity wherever possible. As a consequence of cutting costs indiscriminately over the past few years, incidents such as the Gulf of Mexico oil spill and other large-scale accidents have impacted businesses and their customers, shareholders, and employees in many ways. Effective safety strategies that reduce the risks of such adverse events have become essential. Many surveys have indicated that 70% of the safety accidents were caused by human factors such as fatigue, overloading, distraction, excesses of overconfidence, and so on. Investing in more intelligent automation can reduce the human impact, improve safe decision-making, augment early detection of potential undesired events, decrease downtime, and improve productivity. Better, more intelligent automation can deliver dependability.

Dependability is defined as *the ability to deliver services that can justifiably be trusted*. Ordinary citizens everywhere are concerned about the reliability of their cars, the availability and safety of the water supply, the maintainability of their homes, the safety of their medications, and the security of their lives. All such concerns influence each other, and they have to be managed carefully.

From a business standpoint, product manufacturers are understandably concerned about:

- The reliability of their products, to avoid returns in the warranty period
- The availability of energy and materials to sustain their operations
- The maintainability of their machinery
- The safety of their plants and personnel
- The security of their facilities and IT infrastructure

All these concerns must be managed carefully and consistently.

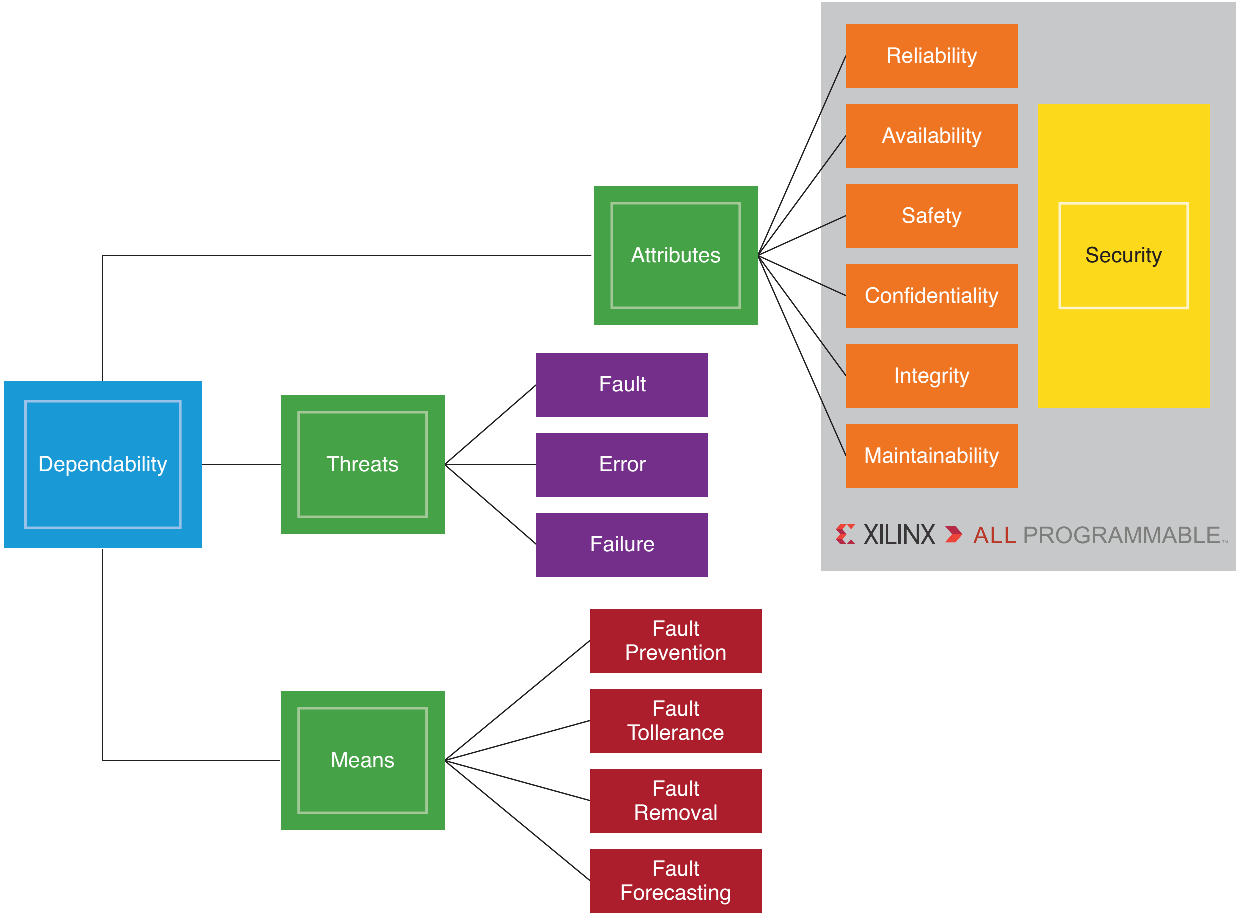
Many business executives and managers recognize the need to invest in technology and solutions for improving and managing dependability; safety, security, and availability must be made top priorities if superior dependability is to be achieved and maintained. Best-in-class companies understand the importance of investing in the latest dependability technology so that certified compliance with applicable regulations and standards can be achieved with as little complication and disruption as possible.

Even more important, however, is the ability to identify critical problems *before their occurrence* to avoid the unscheduled downtime that can result from equipment failure, operator error, or improper security intervention. Obviously, unforeseen downtime episodes can trigger significant financial losses, so investing in dependable technology is a wise choice. Organizations must learn and understand the reasons for asset downtime to improve overall productivity and dependability.

The System Challenge

Xilinx recognized more than fifteen years ago that dependability is an important asset for its customers, and has worked to deliver solutions that help in designing more dependable systems. Xilinx efforts on behalf of systems dependability are focused on reliability, safety, security, maintainability, and high-availability architectures. The approach of designing more dependable systems is also supported by processes and tools certified by regulatory authorities. Xilinx's certifications provide immediate customer benefits because they reduce the time to achieve realization and certification of a customer's systems.

Xilinx's objectives are to provide the tools and capabilities necessary to protect dependable systems. The attributes, threats, and means of solving the challenges are illustrated in Figure 1.



WP461_01_110514

Figure 1: **Dependability Attributes, Threats, and Means**

Dependability is formed by a set of attributes, affected by threats that can be mitigated using means to successfully manage dependable systems. This white paper starts with labeling dependability attributes, threats, and means, because such definitions allow the design team to share these important common terms when designing the final system.

First, the *attributes* of dependability:

- **Reliability** is
  - the continuity of a system's error-free service, or
  - the likelihood that the system can complete a specified mission within a specified period.
- **Availability** refers to the system's operational availability for use at any time during a specified period.
- **Maintainability** is defined by how swiftly a system can be accessed, inspected, and repaired.
- **Safety** denotes how well a system is protected against the possibility of unintended actions or responses that could damage the user and/or the environment.
- **Security** refers to a system's immunity to data disclosure or loss as a result of the unlawful electronic penetration of the system's protections and defenses.
- **Integrity** denotes the certainty that a system cannot be improperly altered.
- **Confidentiality** is the effectiveness of a system's protections against unauthorized disclosure of information.

Then, the *threats* to dependability:

- **Error** refers to a discrepancy between a computed, observed, or measured value and the true, specified, or theoretically correct value or condition. An error can be random or systematic. An error is basically any system state that causes failure.
- **Fault** is defined as an abnormal condition that might cause a reduction in or loss of capability of a functional unit to perform a required function. Fault is the cause of a system failure.
- **Failure** is the termination of a system's or functional unit's ability to perform a required function. (A failure in a subsystem can create a fault in a higher-layer system.)

Designing to satisfy these dependability attributes is achieved by properly avoiding or mitigating errors, faults, and failures such that unwanted outcomes are minimized. There are four *means* that can be identified to prevent threats to dependability:

- **Fault Prevention** defines how to avoid and prevent fault introduction or fault occurrence.
- **Fault Tolerance** is how to provide services that fulfill their specifications in the presence of faults.
- **Fault Removal** defines how to reduce the presence of faults, in terms of both the number and the seriousness of faults.
- **Fault Forecasting** is the ability to estimate the creation and the consequences of faults.

Proper processes must be created to avoid design errors by applying the proper tools for managing the attributes and their means along the whole product life cycle. This is accomplished first by using specific methods to qualify and quantify the threats, and second by deploying suitable architectures and techniques that implement the corrective means within the product itself.

Functional Safety

IEC 61508 and ISO 26262 are the two major standards that rule the certification of functional safety equipment. The two standards define a specific safety life cycle for the whole design process. To achieve a product certification, it is required that specific design details, the safety management system of the manufacturer, and the competencies of those professionals involved in the product creation are assessed. Xilinx personnel have the required IEC 61508 and ISO 26262 training necessary for a safety program.

- **Functional safety** is a subset of safety, as shown in Figure 2. It is the part of overall safety that depends on active systems (e.g., temperature measurement, de-energizing sources of energy) or equipment operating according to its designed safety function.
- **Non-functional safety** is the safety achieved by measures reliant on passive systems (e.g., insulation on electrical conducting parts).

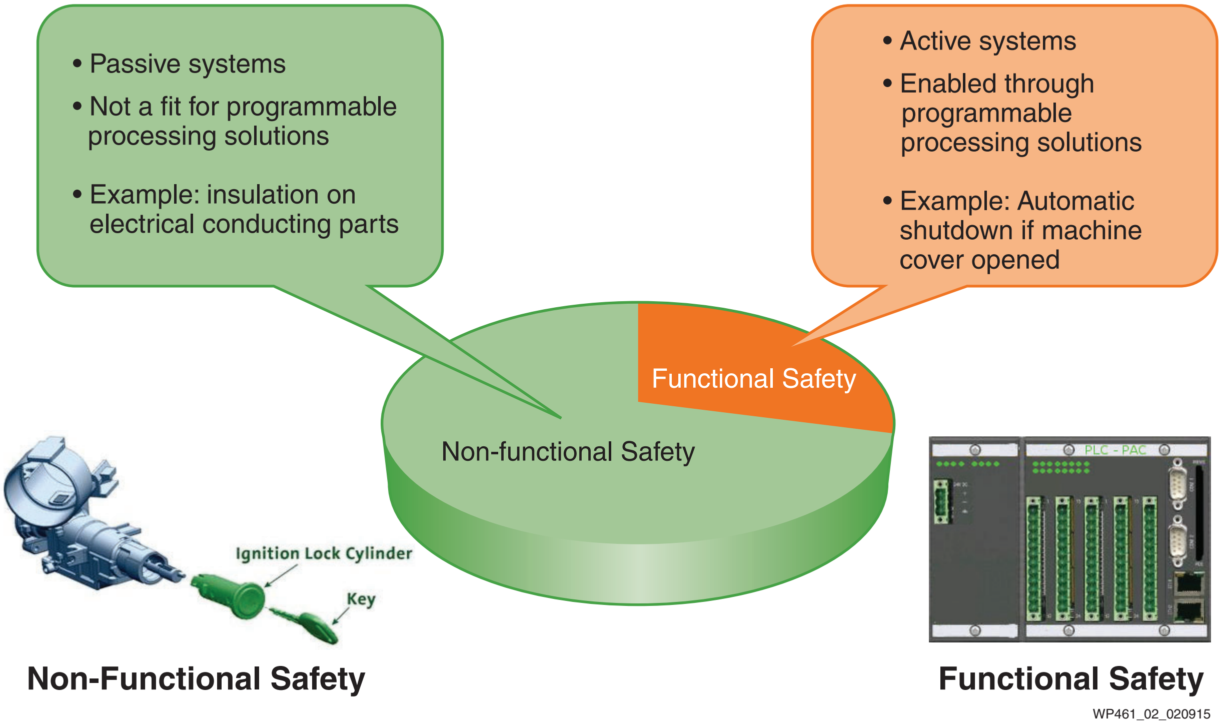

• Passive systems
• Not a fit for programmable processing solutions
• Example: insulation on electrical conducting parts
• Active systems
• Enabled through programmable processing solutions
• Example: Automatic shutdown if machine cover opened
Functional Safety
Non-functional Safety
Ignition Lock Cylinder
Key
PLC - PAC
Non-Functional Safety
Functional Safety
WP461_02_020915

Figure 2: **Functional Safety as a Subset of Overall Safety**

The basic concept for the development of programmable electronic safety equipment is summarized by the industry as:

A safety system is functionally safe if random, systematic, and common cause failures do not lead to a malfunction of the safety system resulting in injury or death of humans, spills to the environment, and/or loss of equipment or production.

Industrial Application Domain

Industrial, automotive, avionic, and communication systems are rapidly evolving toward greater integration. Figure 3 presents an example of typical industrial automation equipment and its integration trend.

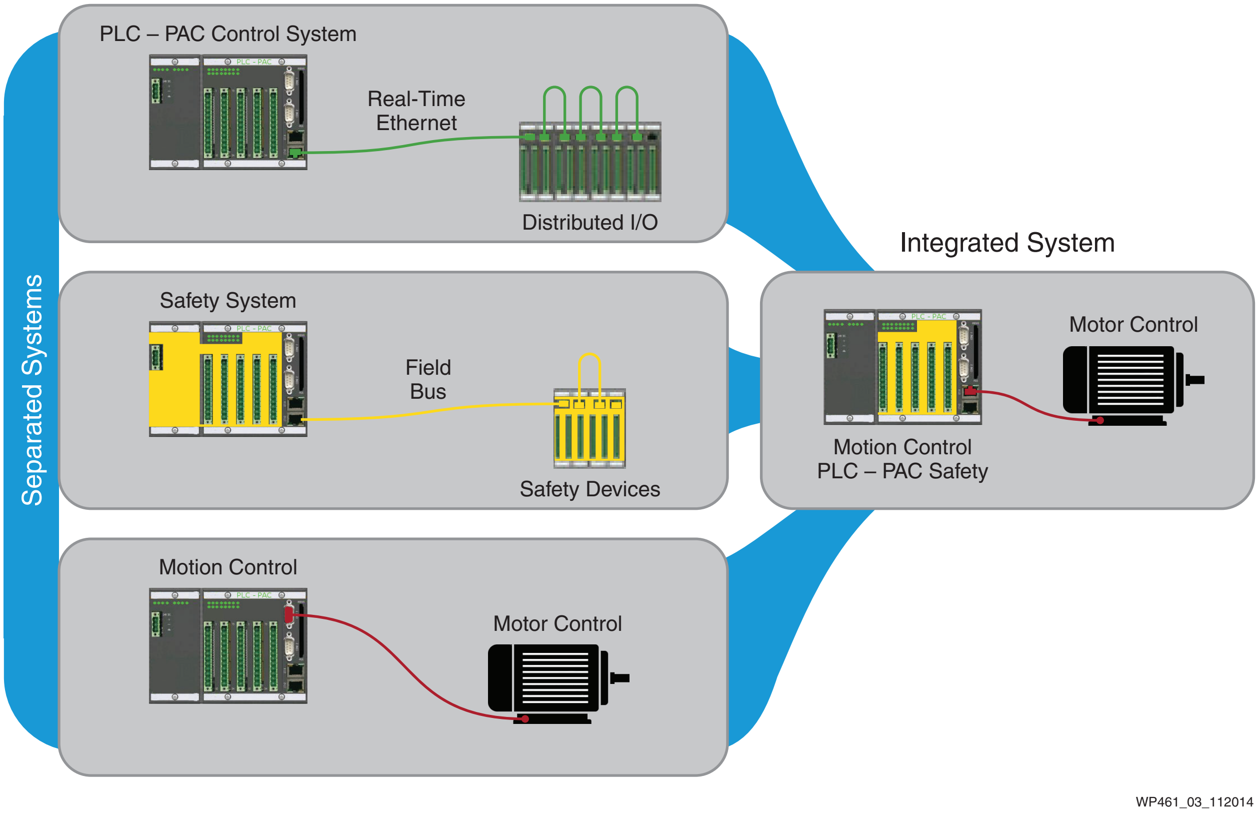


Figure 3: **Automation System Integration**

A traditional automation system comprises a combination of equipment such as a programmable logic controller (PLC) that sequences the process of activating local or distributed I/O. Motion controllers plan movements and trajectories of an ensemble of motor controllers, which in turn drive electrical motors that move automated parts. Safety controllers use safety input transducers and safety output actuators to supervise the full system for bringing the controlled process into a safe state if a violation occurs. Safety control systems also have communication networks—real-time Ethernet and field buses, as shown in Figure 3. These safety systems require security and confidentiality to avoid breaches resulting in safety risks or even plant shutdown.

The traditional configuration is very common, and is the result of afterthought. Initially, systems were designed for carrying functional aspects only (e.g., PAC plus motion plus motor controllers). Then other attributes were added (safety and security), making the system complex and full of traps, and its dependability was very difficult to assess. Such complexity defies the comprehension of all but a few experts, and sometimes even they possess an incomplete understanding of the system's potential behavior. Increased complexity of all types makes it difficult for designers to consider all potential system states, or for operators to handle all normal and abnormal situations and disturbances safely and effectively. In fact, leading experts on safety systems define complexity as intellectual unmanageability [Ref 1].

The modern approach to reducing complexity is to exploit the advantages of smaller silicon geometries and the availability of real estate into microelectronics to include the dependable means listed in Figure 1. To be effective, this approach must include design processes and product lifetimes for all the relevant dependable conditions. In Figure 3, this integration is depicted as the union of all three systems shown under the label of Integrated System.

Clearly, the integrated system must have enough performance to sustain the functions of the separate systems. An FPGA programmed with a soft processor IP core—or, preferably, an SoC like one of the Zynq®-7000 devices—provides sufficient performance to keep and enhance needed functionality while maintaining delivery of the required dependability attributes.

Fundamentally, integrating the separate functions into silicon allows greater decoupling, because the dependable functions are embedded at the lower system level. Thus, dependability can be managed at the source of the problem, not as an afterthought. This approach *decreases* complexity and therefore decreases system unmanageability.

The traditional architectures are *not* obsoleted by this approach. Integrated dependability management reduces risk and improves diagnostic capabilities, but at the system level, the proper dependability architecture must still be implemented. As an example, duplication (redundancy) at the equipment level is often appropriate (or mandated) if there are concerns that common faults affecting the integrated part could disable the full system.

Xilinx approaches this integration by providing certified means for every dependability attribute, thus making it possible to tailor the design appropriately. Figure 4 shows an example of how the tailored attributes enabled by Xilinx allow customers to make the appropriate assignments.

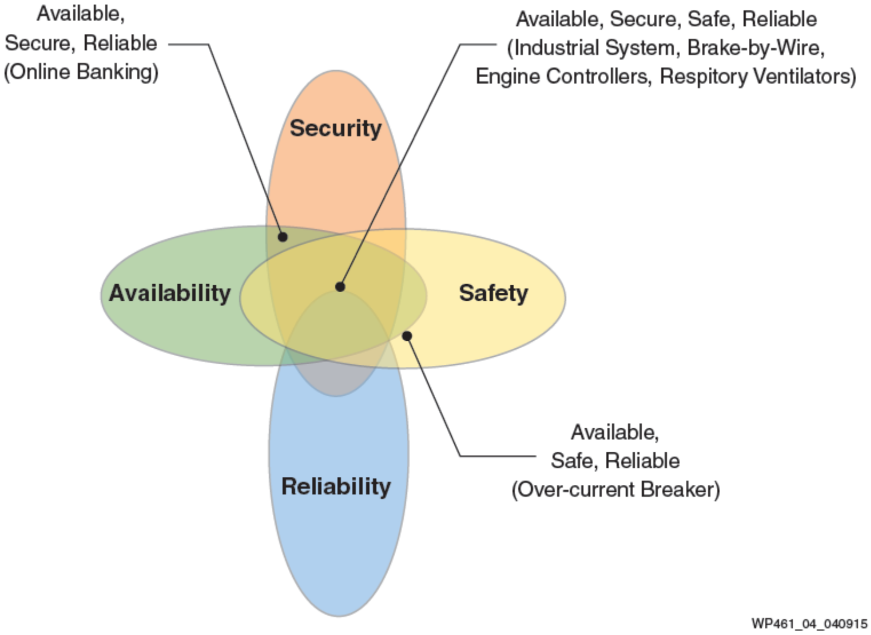


Figure 4: **Tailoring Dependability**

Reliable, high-availability, high-security systems that are *not* safety related, such as those typically found in online banking, stock exchange real-time data handling, and business-critical websites, can still make good use of Xilinx's security solutions and availability patterns. Manufacturing process targets like industrial systems, engine controllers, respiratory ventilators, brake-by-wire systems, and power systems fall into the center section, where secure, reliable, high-availability, and safety-critical systems overlap (Figure 4). The right bottom section of Figure 4 is for safe, reliable, high-availability systems that are *not* security-related, such as over-current interruption switches.

Synergistic Design and Functionality

Figure 4 also suggests a somewhat “deeper” interpretation: Attributes behave as a set of layers working together to fulfill dependability requirements. This is also called the layered approach. The layered approach helps in identifying and managing the required attributes such that every layer covers a specific dependability attribute, with the intersection of attributes determining the behavior of the whole system.

Implemented properly, layering can be extremely effective. However, proper implementation of layering alone is not a guarantee of success. For example, a properly implemented security attribute requirement might specify that, in case of a compromised password, the system must lock down every access portal to the system. While this action might be quite appropriate and justifiable in a banking application, it could actually be very dangerous in a different context—for example, in a chemical plant.

In a chemical plant, if the compromised password were followed by a second, highly unsafe command, immediate human intervention could be required to avoid unforeseen adverse consequences, such as a complete plant shutdown or even an explosion. With all inputs locked down, intervention by a human might prove impossible in the required time frame.

Xilinx's recommendation, therefore, is that all dependability attributes must be specified in a holistic, synergistic implementation, i.e., every subsystem must be aware of every other subsystem’s methods of operation and must predictably and safely work together within that context.

The importance of synergy in dependable systems is highlighted by the Swiss cheese model.

The Swiss Cheese Model

As in the previous chemical plant example, many well-known historical disasters, such as the recent Deepwater Horizon explosion and oil spill (2010), the Challenger Space Shuttle launch explosion (1986), and the partial nuclear meltdown at the Three-Mile Island power plant (1979), can all be described and analyzed using the Swiss cheese model.

Described originally in the book *Human Error* by James T. Reason, a researcher in cognitive psychology, the Swiss cheese model focuses on accident causation involving complex systems as the result of the confluence of multiple contributing factors. Taken individually, these factors would typically cause no serious problem to occur—but taken in confluence, they could result in a hazardous, even a catastrophic event.

In the Swiss cheese model, defenses against failure are modeled as a series of barriers, represented as slices of cheese. The holes in the slices represent the absence of synergy (i.e., weaknesses) in individual parts of the system. In the model, these holes are not static; rather, they are continually varying in size and position across the slices. The system produces a failure when a hole in each slice momentarily aligns with holes in all the other slices, permitting (in Reason's words) *"a trajectory of accident opportunity."* The coincidence of these momentarily aligned holes in the slices can then lead to an unforeseen failure scenario.

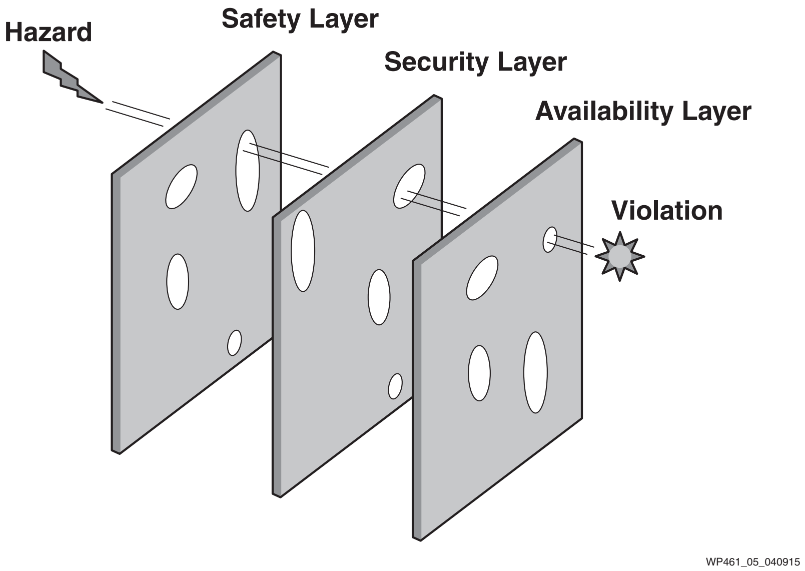


Figure 5: **Swiss Cheese Model**

Reason's important contribution in the dependability field is the idea that *the hole in the final layer of cheese* is what allows the ultimate accident to occur—but that the accident would be unlikely to have happened without a *series of previous failures* having lain dormant in the background.

Xilinx recognizes the effect of the Swiss cheese model, and recommends that customers follow a holistic approach in designing the architecture of dependable systems. Culture, organization, and process design must all be accounted for, providing inter-aware defensive layers that adequately mitigate against the inevitability of errors.

Xilinx Certified Processes

The Swiss cheese model in engineered systems is a reflection of the structure, management, procedures, and culture of the engineering organization that created, in effect, the process used for generating the final system. It is not merely a matter of having good processes, but of having certified processes that make the difference between (a) achieving dependability by knowing the facts, and (b) hoping to achieve dependability by relying on guesswork.

To give assurance to customers, Xilinx implements fully certified state-of-the-art processes that operate on all the elements coming together to sustain the whole Xilinx product life cycle [Ref 2]:

- Xilinx holds regularly scheduled internal quality audits of quality activities to confirm their effectiveness and adherence to defined procedures.

- Xilinx conducts true root-cause analysis to resolve problems, transforming them into opportunities for improvement. Together with subcontractors and suppliers, Xilinx employs the team-based Eight Discipline (8D) investigative approach, and then follows through with a data-driven approach to develop permanent and effective solutions.
- Xilinx is compliant with ISO 9001 Certification for quality management systems since 1995, and ISO 9001:2008 for the design, test, and deployment of custom embedded software and logic designs.
- Xilinx has been TL 9000 certified for telecommunications since 2004
- The Xilinx Quality Manual is structured around ISO 9001:2000, TL 9000, TS 16949, Military (QML), as well as other industry standards.
    - It applies to the design, manufacture, and testing of SoCs, FPGAs, CPLDs, and configuration devices.
- Xilinx Ireland (XIR) has been awarded the Authorized Economic Operator (AEO) certificate.
    - Currently, the US and EU are working together on mutual recognition of AEO.
- Xilinx has been in compliance with SoC STACK International, StackTrak - Supplier Certification Program for IC quality and reliability requirements, as well as AEC-Q100 Component and Device Qualification with full PPAP support for the automotive industry, since 2004.
- Xilinx complies with the Department of Defense MIL-PRF-38535 Custom Microcircuit Certification for Class Q and N.
- Xilinx has been ISO 14001:2004I certified, RoHS and Pb-free certified, and OHSAS 18001:2007 certified since 2008.
- Xilinx has proven compliance in Functional Safety [Ref 3]. (Registration required to access this page.)
    - IEC 61508 (TÜV SÜD Certification for ISE® Design Suite 14.2-14.7)
    - ISO 26262 (TÜV SÜD Certification for ISE Design Suite 14.2-14.7)
- To assure the highest level of satisfaction with Xilinx products, Xilinx has developed formal Return Material Authorization (RMA) procedures for components, software, boards, and cables.
- Xilinx has established and implemented a process focused on preventing quality issues at all manufacturing partners, with goals to obtain the highest product yields, quality, and reliability by using cause-and-effect analysis to minimize significant sources of variability.

Reliability

Xilinx has a long track record of published quality and reliability information [Ref 2]. With its Reliability Monitor Program, Xilinx ensures that product performance meets or exceeds reliability specifications dictated by internal programs as well as by international standards and individual customer requirements. Quality monitors take samples from finished goods. Program results are published in the quarterly UG116, *Device Reliability Report* [Ref 4]. Xilinx's focus on quality along with its zero-defect mindset and quality-focused culture is reflected in the PPM data along with the failure in time (FIT) rates and Single Event Upset (SEU) data detailed in the *Device Reliability Report*.

Upset Event Effects

All integrated circuits, programmable or otherwise, are susceptible to some degree to Single Event Effects (SEE). Some of these effects can be catastrophic (such as a Single Event Latch-up [SEL]), while others are recoverable, such as an upset to the data or, in the case of a programmable device, an upset to the configuration memory (an SEU). Since the beginning of the understanding of these phenomena, Xilinx has been actively pursuing methods to eliminate the effects, as well as methods to mitigate such events when they do happen. With each technology process node, Xilinx has driven down the inherent FIT rate due to SEUs (see Figure 6).

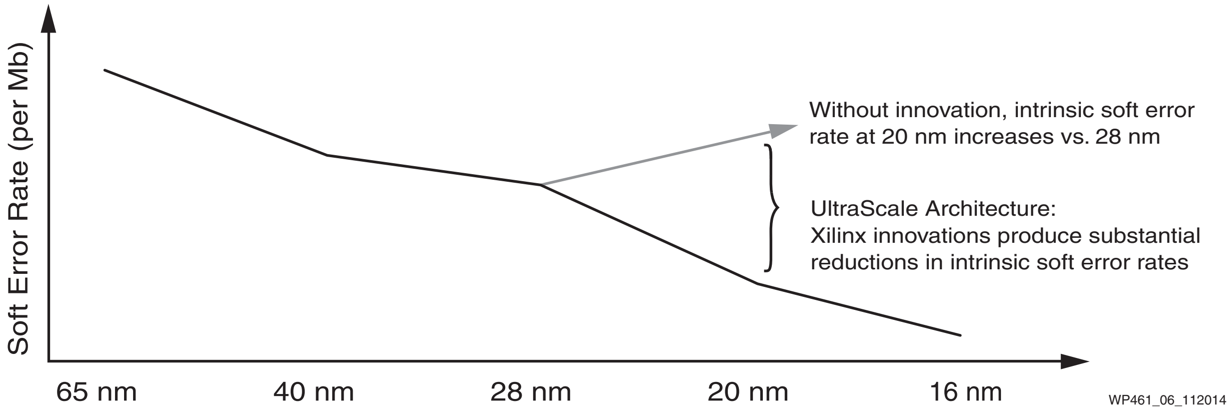


Figure 6: **Xilinx FPGA Soft Error Rate Trend**

However, silicon features alone cannot make a commercially safe device. Xilinx believes in a layered approach to addressing this issue, much like in the field of security (see Figure 7).

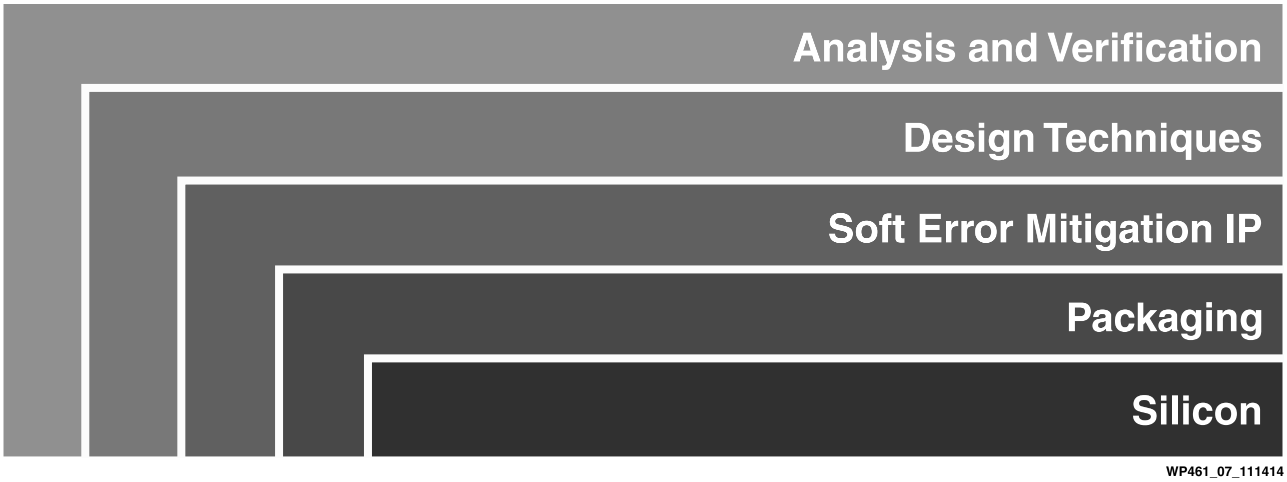


Figure 7: **Xilinx Multi-Level SEU Mitigation Solution**

First and foremost, this solution must start with the base silicon. From there, packaging materials must be addressed. Beyond that, Xilinx provides Soft Error Mitigation IP (SEM IP) along with various implementation methodologies allowing the user to create fail-safe and fault-tolerant designs. Additionally, Xilinx routinely measures its performance and strives to improve with each generation, both in silicon and in IP. Lastly, Xilinx offers tools to help the customer understand the impact of their specific operating environment so they are aware of what additional layers must be added to provide a truly safe context.

Public distribution of reliability data, including SEU FIT rate [Ref 4], is readily available. Additional information can be found at the Xilinx website Single Event Upsets page [Ref 5], in the Xilinx white paper *Considerations Surrounding Single-Event Effects in FPGAs, ASICs, and Processors* [Ref 6], and in the Xilinx white paper *Mitigating Single-Event Upsets* [Ref 7].

Mitigation of the Inherent Silicon FIT Rate

Silicon Features

As mentioned previously, the first necessary mitigation layer is to reduce the inherent FIT rate of the device. This starts at the core element of an FPGA/SoC: the configuration memory cell. Xilinx spends a significant amount of time researching best practices in SEU-resistant memory for configuration. Using proprietary design techniques for both design and layout, extensive simulations, test chip runs, and actual beam testing, Xilinx has continually reduced the FIT rate of its devices in each generation.

Packaging Technology

Beyond the silicon, Xilinx places strict control on materials used in the packaging of our devices. This reduces the SEUs from Alpha Radiation by orders of magnitude.

User Features

In addition to aggressive control of the actual design of the memory cell architecture, Xilinx has implemented a proprietary methodology for background detection and correction of SEUs. The FRAME_ECC primitive can be inserted into a user's design, allowing single-error correction and dual-error detection at a configuration frame level. With enhanced configuration frame interleaving, Xilinx has achieved unprecedented reduction in the impact of Multi-Bit Upsets (MBU), significantly reducing, if not practically negating, the effect of an MBU—all of this while having no impact on design performance.

However, in this category, Xilinx has not stopped at the configuration memory. Xilinx user memory array (block RAM) has a robust architecture and built-in error correction allowing for the correction of a single-bit error and the detection, not self-correction, of any double-bit error.

Software Mitigation, Classification, and Prediction

In line with the layered approach methodology, Xilinx provides SEM IP to aid in the classification and reduction of SEU and MBU effects [Ref 8]. The SEM IP builds upon the embedded silicon features of Xilinx devices but adds additional functionality such as error classification and error injection. Classification of errors and error location is fundamental to reduction to the overall device FIT. Xilinx devices are constructed around arrays of configuration frames (each with FRAME_ECC). This large memory array contains a myriad of bits but only a small number of them actually effect the operation of the users design. Depending on the design itself, an even smaller number affects the safety critical functions of the user IP. All these bits can be classified as the following:

- **Device Configuration Bits:** All the bits in the device configuration array
- **Essential Bits:** Those bits associated with the user design [Ref 9]
- **Prioritized Essential Bits:** Bits associated with user defined safety critical bits
- **Critical Bits:** Bits that cause a functional failure if they change state

The strength of the Xilinx solution is that identification of these bits is part of base Xilinx design software available to the user to customize to their needs [Ref 8].

As not all operating environments or applications need such a robust SEU solution, Xilinx offers the SEU FIT Rate Calculator [Ref 7], allowing the user to identify the projected FIT rate for the application in a given environment. More information can be found on the Xilinx Avionics page [Ref 10]. (*Registration required to access this page.*)

IEC 61508 Requirements for FPGAs

Covering all of the requirements of IEC 61508 is beyond the scope of this white paper; thus, only the main requirements for FPGAs are described, and the reader should get some familiarity with this norm. The safety life cycle must be considered for the methodology and hardware/software in order to address random faults and systematic errors. The life cycle must be managed by whomever implements the safety equipment. The IEC 61508 recommends several actions, and in particular clause 7.1.3.1 of IEC 61508-2 (Part 2) recommends the V-model for the safety life cycle, in which there is a corresponding verification and validation phase for every development phase.

Then, clause 7.4.4.2 sets six main requirements:

1. The architectural constraints on hardware safety integrity must be defined as an input requirement
2. The effect of random failures must be quantified for determining the reachable integrity level
3. Annex E of Part 2 should be used if the architecture targets on-chip redundancy
4. Systematic safety integrity (also called "systematic capability") must be met, following the prescriptions of Part 3 and using three possible routes labeled with the letter S (standing for "systematic safety" integrity)
    a. Route 1S: Prescriptions on Part 3 must be followed for the control of systematic faults
    b. Route 2S: Evidence must be shown that the equipment is proven in use
    c. Route 3S: Evidence must be shown that pre-existing software complies with Part 3 if it is desired that such software be trusted
5. Requirements must be defined for system behavior (i.e., executing the proper safety action) on detection of a fault.
6. Requirements must be defined for data communication processes to ensure the integrity of the exchanged information

Then, clause 7.4.4 of IEC 61508-2 sets the hardware safety integrity architectural constraints, referring to equations described in Annex C of its Part 2.

All six directives are simply too numerous to be fully described in this white paper; it suffices to know that they must all be fulfilled as a first priority.

Then, IEC 61508-2 establishes two possible routes for defining the hardware safety integrity level, one of which can be claimed for a safety function. Because Routes 1H and 2H are application-specific, IEC 61508-2 defers to the specific application standard to determine which of the two must be used:

1. Route 1H, based on hardware fault tolerance and safe failure fraction concepts

2. Route 2H, based on component reliability data from feedback from end users, increased confidence levels, and hardware fault tolerance for specified safety integrity levels

ISO 26262 gives similar requirements (sometimes less stringent) on how to achieve safety integrity.

It is easy to see that compliance with the Safety Standards is an involved process; over and above all this, it is also necessary to ensure the product can be supported for a lifetime that spans at least ten to fifteen years.

How Xilinx Solves Functional Safety Challenges

FPGAs are specifically addressed in the IEC 61508-2, and redundant design is the recommended path to achieve the required safety integrity level. Xilinx FPGAs and SoCs can reduce system costs by implementing a safety design with fewer components than other solutions by providing a higher level of integration, thus easing the creation of redundant designs. Xilinx products provide two approaches for implementing redundancy:

- A dual-chip solution can be used where the application standard disallows a single-chip solution, which is more costly.
- A single-chip solution can be used to implement the safety function if the application standard allows it, e.g., IEC 61508-2 Annex E allows up to SIL3. Xilinx FPGA and SoC capabilities make this option feasible. This solution is the best value for the customer, if not specifically excluded by other sector-specific norms.

Xilinx Software and Implementation Methodologies

Qualified Tools

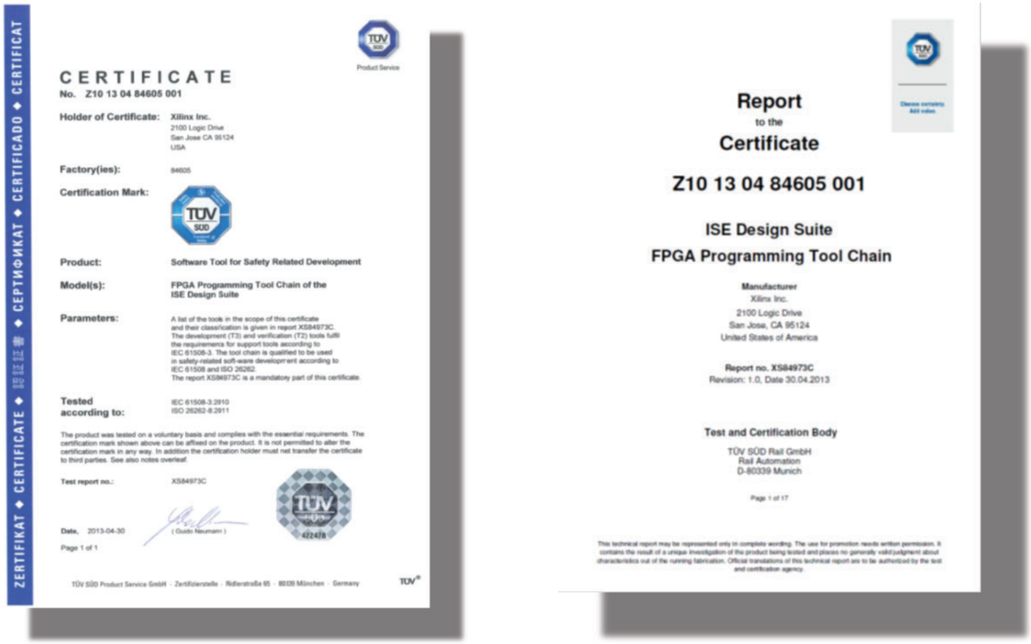
Implementers must use certified development tools to make sure they are able to cover the systemic “Requirements for FPGAs” listed at point 4 of IEC 61508-2. Xilinx certified its tool chain, creating a Functional Safety Package that allows FPGA users to implement safety designs following proper methodology and procedures. The safety manual *Elements for Safety Guidelines, IEC 61508 and ISO 26262* (available in the Functional Safety Package Lounge [Ref 3]) covers the Xilinx ISE FPGA programming tool chain, versions 14.2–14.7. It is used to develop safety-related FPGA application designs according to IEC 61508 Edition 2 and ISO 26262. It also covers the requirements for SIL1 to SIL3, or ASIL-A to ASIL-D.

The qualified tool chain describes a design methodology and flow based on Xilinx tools for safe FPGA designs. It guides the user toward the application of the design flow using partitioning and/or isolation of several functional building blocks needed to achieve the required level of redundancy with no interference. This allows synthesizing a final bitstream for the FPGA that fulfills a specified SIL or ASIL. It also provides guidance for verification and testing of the implementation (e.g., timing, temperature, power consumption, violation of design rules, and isolation violations) according to the V-model recommended by IEC 61508 Edition 2.

ISE Design Tool Suite 14.2 through 14.7 FPGA Programming Tool Chain

Xilinx currently has TÜV SÜD Certification for the ISE Design Suite 14.2 FPGA Programming Tool Chain [Ref 3] and for ISE Design Suite 14.7 (Figure 8) for the following safety standards:

- IEC 61508 Edition 2.0 2010-04
- ISO 26262 First Edition 2011-11-15



ZERTIFIKAT ◆ CERTIFICATE ◆ ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

CERTIFICATE
No. Z10 13 04 84605 001

Holder of Certificate:	Xilinx Inc. 2100 Logic Drive San Jose CA 95124 USA
Factory(ies):	84605
Certification Mark:	
Product:	Software Tool for Safety Related Development
Model(s):	FPGA Programming Tool Chain of the ISE Design Suite
Parameters:	A list of the tools in the scope of this certificate and their classification is given in report XS84973C. The development (T3) and verification (T2) tools fulfil the requirements for support tools according to IEC 61508-3. The tool chain is qualified to be used in safety-related soft-ware development according to IEC 61508 and ISO 26262. The report XS84973C is a mandatory part of this certificate.
Tested according to:	IEC 61508-3:2010 ISO 26262-8:2011

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: XS84973C

Date, 2013-04-30

(Guido Neumann)

Page 1 of 1

472478

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany

Choose certainty. Add value.

Report
to the
Certificate

Z10 13 04 84605 001

ISE Design Suite
FPGA Programming Tool Chain

Manufacturer
Xilinx Inc.
2100 Logic Drive
San Jose, CA 95124
United States of America

Report no. XS84973C
Revision: 1.0, Date 30.04.2013

Test and Certification Body
TÜV SÜD Rail GmbH
Rail Automation
D-80339 Munich

Page 1 of 17

This technical report may be represented only in complete wording. The use for promotion needs written permission. It contains the result of a unique investigation of the product being tested and places no generally valid judgment about characteristics out of the running fabrication. Official translations of this technical report are to be authorized by the test and certification agency.

WP461_08_110514

Figure 8: **TÜV SÜD Certification for the ISE Design Suite FPGA Programming Tool Chain**

Isolation Design Flow (IDF)

Xilinx Isolation Design Flow (IDF) [Ref 11] is the software methodology that allows for logically and physically isolating one logical function from another. It is a two-stage design consisting of:

- **Isolation**: The physical and logical isolation of functional blocks using the ISE PlanAhead™ floor-planning tool.
- **Isolation verification:** A software application called the Isolation Verification Tool (IVT), which verifies the physical isolation of the functional blocks as well as the proper isolation of routed connections among blocks.

This two-stage design flow is approved by TÜV SÜD for IEC 61508 and ISO 26262.

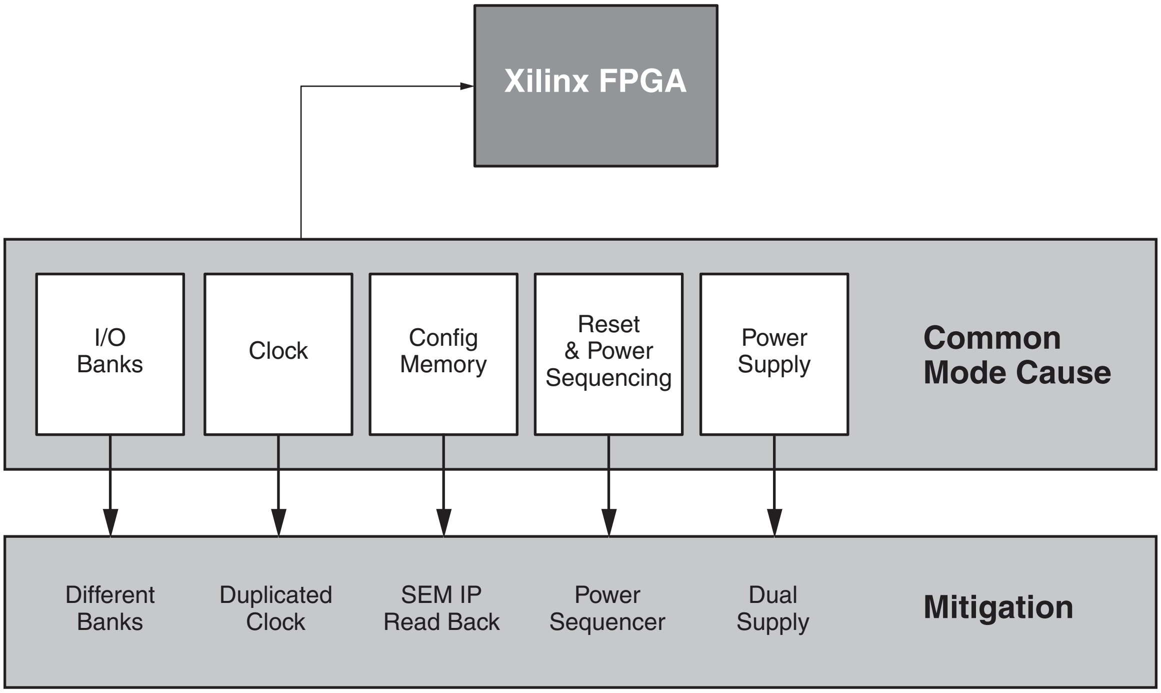
The IDF allows for multiple physically isolated, independent functions to be implemented within a single FPGA, utilizing a fence of unused device components between each function. Each isolated function is separated by this fence, generating isolated regions within the device. The flow uses early floorplanning, modular design, modular synthesis, and adherence to a set of guidelines and considerations to guarantee isolation between desired functions.

After a design is implemented, the IVT must be used to verify that the design rules for isolation (fencing between isolated modules) have been successfully implemented. The isolation blocks can also be considered as a structure that separates and decouples physical blocks as is defined in Table E.2 of the IEC 61508-2 standard.

Common Cause Failure Mitigation

Common causes are concerns for any safety application because they can seriously affect even the most carefully engineered design. The IEC61508-2 Annex E specifically addresses the most common FPGA causes using the Beta factor approach, requiring the fulfillment of several mitigation mechanisms.

Figure 9 shows typical Common Mode causes that might affect a safety system and the mitigation schemes Xilinx uses to address them. SEM IP refers to Xilinx Soft Error Mitigation IP [Ref 8].



WP461_09_040715

Figure 9: **Common Mode Causes in an FPGA and Xilinx Mitigation Schemes**

Multiple common cause failures are possible in safety systems, and these must be addressed. Some of these are highlighted in Table 1, along with the mitigation schemes used in Xilinx FPGAs/SoCs.

Table 1: **Common Cause Failures and Xilinx Mitigation for Zynq-7000 AP SoC**

Common Mode Cause	Xilinx Mitigation (Zynq-7000 AP SoC)
Power supply: Noise, disturbance propagation, PS switch-on (latch-up, etc.), excessive current draw	Separate and independent power supplies (PL and PS) and power sequencing (see IEC 61508-2, Table E.1)
Lack of diversity: One failure takes down the whole system	Multiple possible redundancy schemes: Multiple safety channels with diagnostics (PL and PS)
Safety and non-safety channel separation	On-chip redundancy using isolation design flow (see IEC 61508-2, Annex E, Table E.2)
Upgrades to functional blocks	Design preservation for functional upgrades (preserve QoR for unchanged blocks)

The Zynq-7000 AP SoC Answer to IEC 61508

Power supplies represent one common-mode concern; the availability of different power planes allows the realization of independent redundant circuitry.

Voltage Domains for PS and PL

IEC 61508-2, Annex E (excerpt from E.1) states:

> *e) Appropriate measures shall be taken to avoid dangerous failure caused by faults of power supply including common cause failures.*
>
> *NOTE 5: Faults of the power supply include, but are not limited to:*
>
> - *noise*
> - *disturbance propagation over the power supply lines*
> - *non-simultaneous power supply switch-on that could cause effects such as latch-up or high inrush current*
> - *excessive current draw resulting from short circuit*

The Zynq-7000 AP SoC addresses these power supply concerns by incorporating a separate and independent power supply for the PS and the PL, as seen in Figure 10.

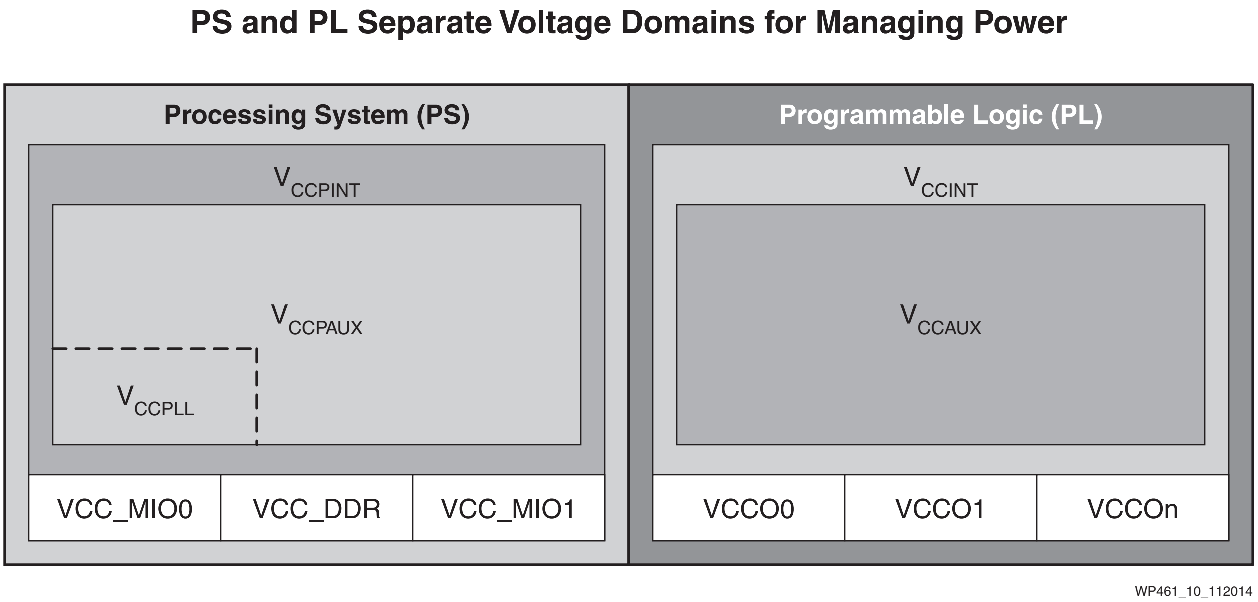


Figure 10: **Separate Power Supplies for the PS and PL**

Zynq-7000 AP SoC Redundancy Schemes

There are multiple methods for mitigating failures using redundancy. A redundant function is realized by duplicating an already existing function. Redundancy can increase the availability of a system and can increase the robustness of the system.

Redundancy can be implemented at different system levels, depending on the requirements to be met. Because safety-related functions might be very complex and expensive to fully duplicate, normally only a specific part of such a function is duplicated.

Numerous possible architectures are available with the Zynq-7000 devices. All schemes require isolation (the IDF) of the block to counter common-mode failures. See Figure 11 for four possible Zynq-7000 AP SoC architectures.

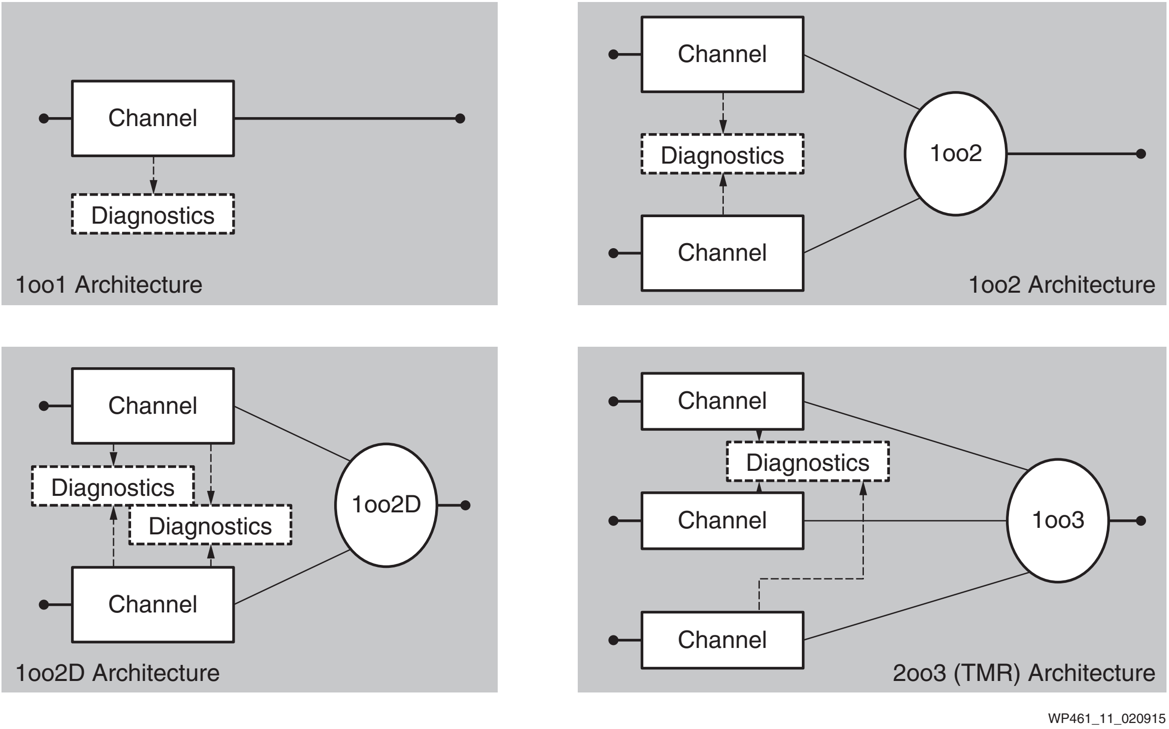
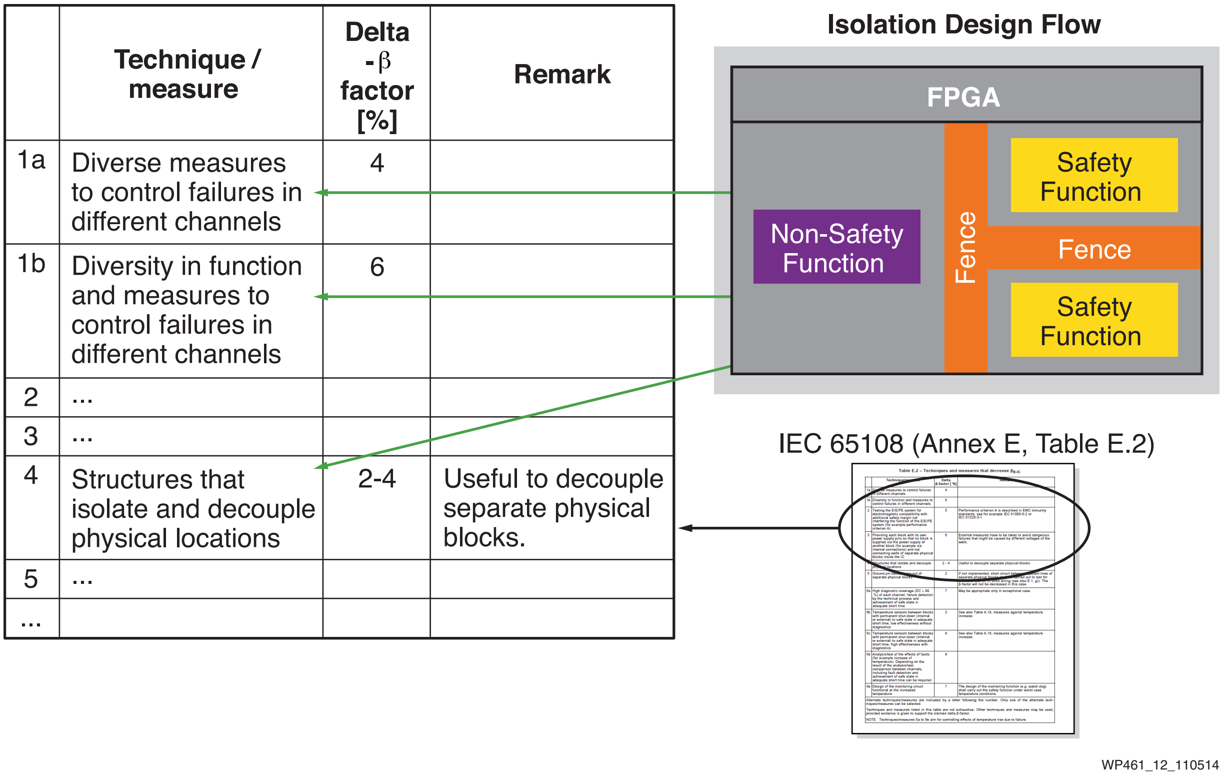


Figure 11: **Possible Zynq-7000 AP SoC Architecture Block Diagrams**

On-Chip Redundancy with Isolation Design Flow

It is widely understood that common-cause failures can have a negative impact on the safety and availability of redundant equipment. Use of the IDF [Ref 11] helps in several ways to decrease the susceptibility of redundant systems to common-cause failures. IEC 61508-2 (Annex E, Table E.2) highlights several techniques and measures that decrease the basic Beta-factor (susceptibility of the IC). Figure 12 shows a snippet of Table E.2 and highlights three of the techniques/measures where using the IDF can decrease β_{IC} significantly for on-chip redundant (OCR) systems. For instance, the "fence," or isolation region defined in the IDF, is a *"structure useful to decouple separate physical blocks"* (IEC 61508-2, Table E.2, item 4).



	Technique / measure	Delta -β factor [%]	Remark
1a	Diverse measures to control failures in different channels	4	
1b	Diversity in function and measures to control failures in different channels	6	
2	...		
3	...		
4	Structures that isolate and decouple physical locations	2-4	Useful to decouple separate physical blocks.
5	...		
...			

Figure 12: **On-Chip Redundancy and Separation Using the Isolation Design Flow**

Implementation Diversity

Diversity is a type of redundancy where different implementations are proposed to ensure the independence of common development errors in the redundant components.

Design diversity is a defense against common-mode or common-cause development errors in safety-critical systems. It is a system design concept that attempts to reduce the possibility of failure stemming from a common development error in one functional failure path, which can result in another functional failure path. This is accomplished by designing a functional failure path with sufficiently dissimilar characteristics to minimize the likelihood that the error manifests itself in another component. Any faults generated are successfully masked and ignored within the system.

Diversity can be performed in software or hardware. In hardware, the diversity is realized using a component or subsystem designed and delivered by different manufacturers with the same initial specifications.

There are multiple options for diverse safe channels in the Zynq-7000 family:

- Programmable Logic (PL) and Processing System (PS)
- PL and MicroBlaze™ processor and PS (APU)
- PL and PS (APU) and Dual-Lockstep MicroBlaze processor

See Figure 13 and Figure 14 for possible diversity options in a Zynq-7000 device.

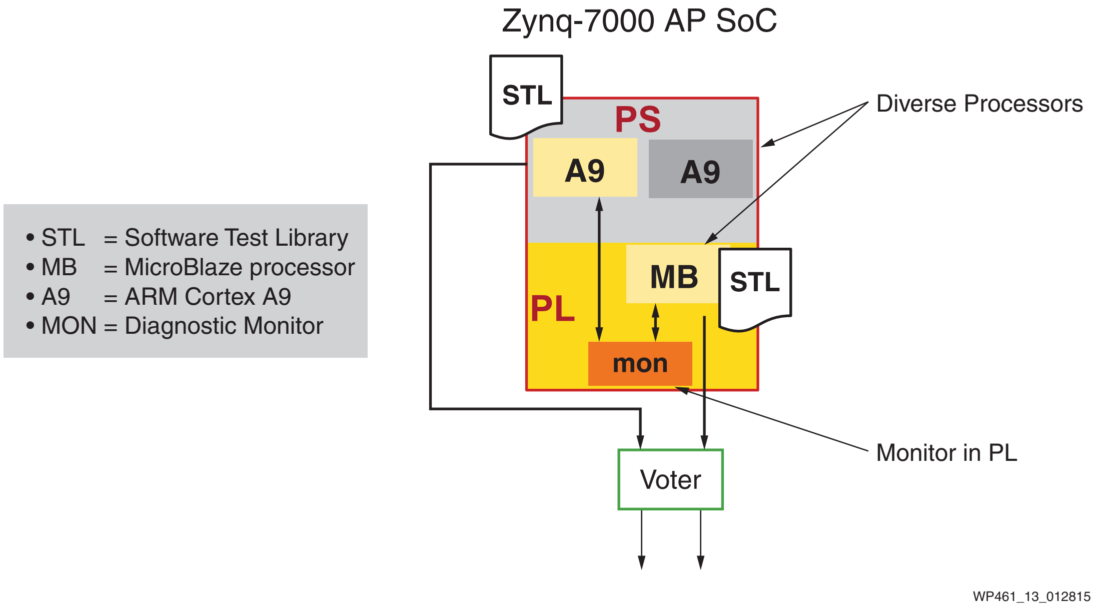


Figure 13: **Zynq-7000 SoC Diversity Options: Using a Single MicroBlaze IP Processor**

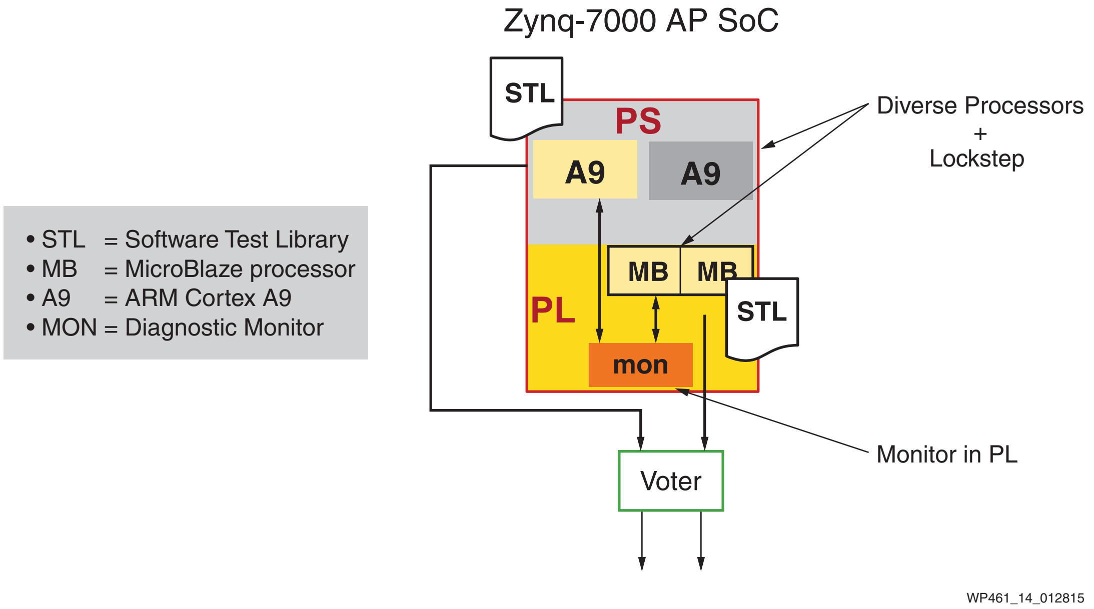


Figure 14: **Zynq-7000 SoC Diversity Options: Using Dual-Core Lockstep MicroBlaze IP Processors**

Lockstep Concept

In lockstep architecture, two processors, the master and the checker, execute the same code in strict synchronization. The master has access to the system memory and drives all system outputs. The checker continuously executes the instructions fetched by the master processor. The outputs produced by the checker, both addresses and data, feed the compare logic (monitor). The compare logic checks the consistency of the master and checker data, address, and control lines. Disagreement on the value of any pair of duplicated bus lines reveals a fault on either CPU (without identifying which CPU is at fault). The block diagram of a Dual-Lockstep MicroBlaze processor system [Ref 12][Ref 13] is shown in Figure 15.

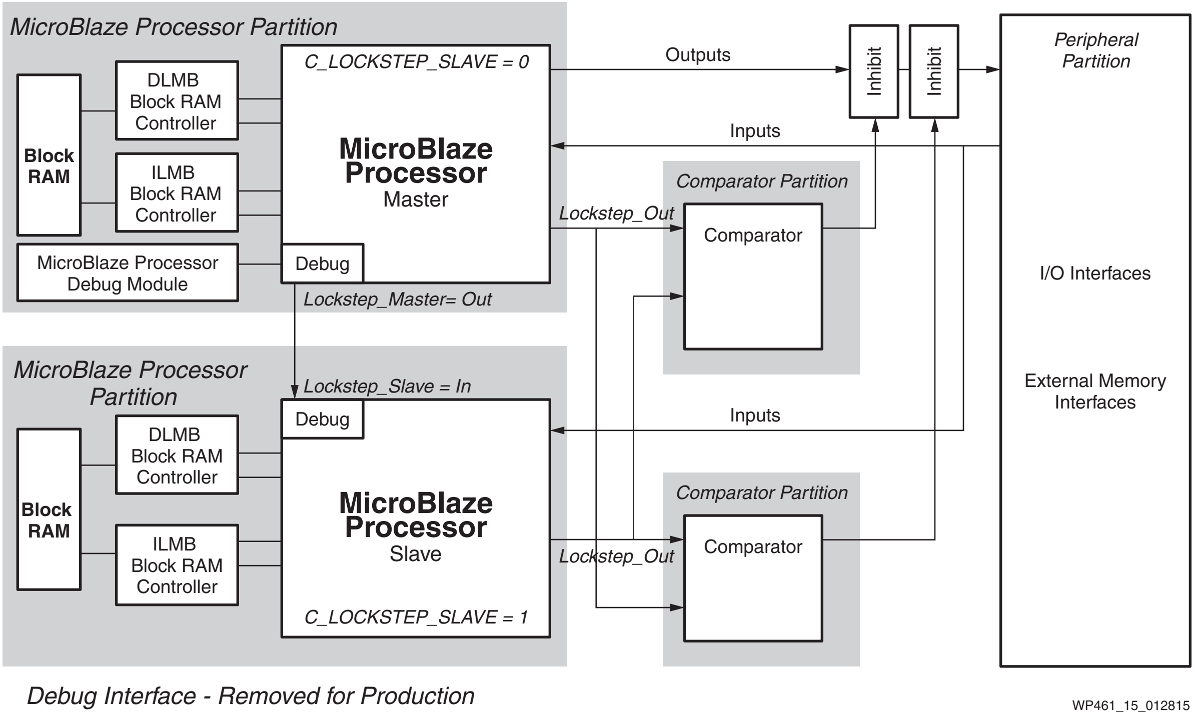

MicroBlaze Processor Partition
Block RAM
DLMB Block RAM Controller
ILMB Block RAM Controller
MicroBlaze Processor Debug Module
C_LOCKSTEP_SLAVE = 0
MicroBlaze Processor Master
Debug
Lockstep_Master= Out
Outputs
Inputs
Inhibit
Inhibit
Peripheral Partition
I/O Interfaces
External Memory Interfaces
Comparator Partition
Comparator
Lockstep_Out
MicroBlaze Processor Partition
Block RAM
DLMB Block RAM Controller
ILMB Block RAM Controller
Lockstep_Slave = In
Debug
MicroBlaze Processor Slave
C_LOCKSTEP_SLAVE = 1
Inputs
Comparator Partition
Comparator
Lockstep_Out
Debug Interface - Removed for Production
WP461_15_012815

Figure 15: **Xilinx Dual-Lockstep MicroBlaze Processor Block Diagram**

There are some limitations for a lockstep implementation. The monitor is not capable of detecting bus and memory errors. These errors are in fact a source of common-mode failure causing both CPUs to fail the same way. Bus and memory must be protected against faults with error detection (correction) techniques, such as parity bits (error-correcting codes).

The lockstep architecture can be employed as a fail-silent node providing the capability of detecting any 100% coverage single error (permanent or transient) occurring indifferently on the CPU, memory, or communication subsystem.

Redundant Dual-Lockstep Concept

A redundant dual-lockstep MicroBlaze [Ref 12][Ref 14] processor implementation can be employed to remedy some of these limitations. A high-level block diagram of a possible redundant Dual-Lockstep MicroBlaze processor system is shown in Figure 16.

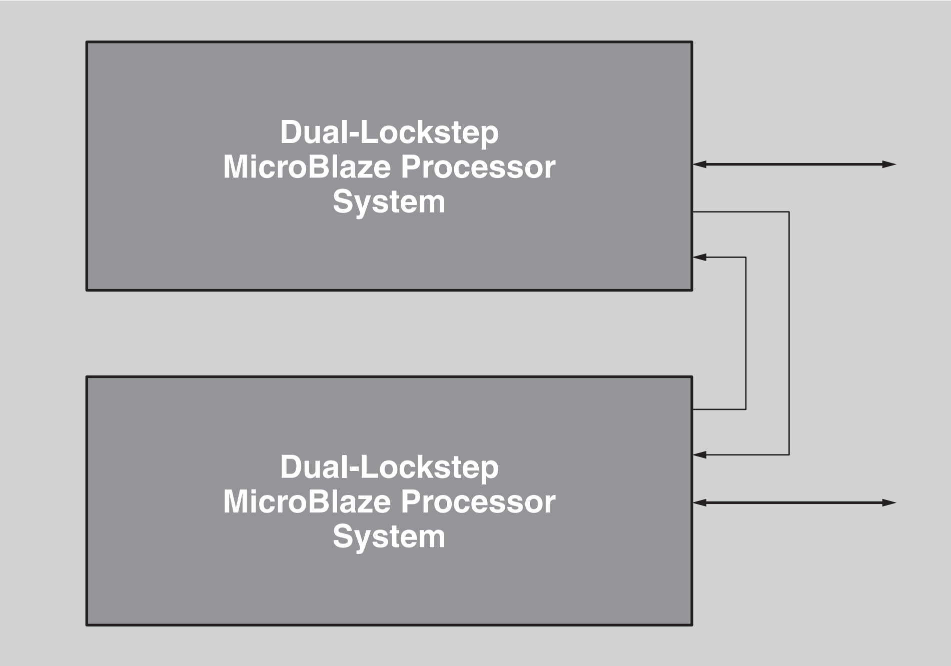

Dual-Lockstep MicroBlaze Processor System
Dual-Lockstep MicroBlaze Processor System
WP461_16_112114

Figure 16: **Redundant Dual-Lockstep MicroBlaze Block Diagram**

- In the dual-lockstep architecture, the two fail-silent channels share the same memory subsystem.
- The method for implementing a redundant dual-lockstep architecture also covers a triple-modular redundant (TMR) solution, as it has the same fault-tolerant properties.
- When fail-operational capability is required, the two channels can be arranged in lockstep mode
  - Provides masking capabilities of CPU's faults as in the TMR solution
  - Can be used as two completely parallel fail-silent channels providing double performance

System Security

Xilinx has been at the forefront of providing secure FPGA solutions for many generations of products dating back to the Virtex®-II Pro family. At each generation, threats have been analyzed as they evolve, and additional features added to counter them. Starting first with silicon features and then leading to a fully integrated security IP (Security Monitor), Xilinx has proven its leadership in providing secure solutions for FPGA/SoC developers. A high-level overview of Xilinx's secure solutions can be found on the Xilinx website[Ref 15].

Silicon Features

Xilinx takes a layered approach to security, with each layer building on the previous. This basic tenet creates a secure foundation upon which the developer can build. The first layer is, of course, the silicon itself. No platform can be secure if the base layer is not. This is tantamount to building a house on a sand foundation. Xilinx uses silicon security features such as AES256 encryption with a 256-bit HMAC authentication scheme, both to authenticate and to provide confidentiality of the FPGA load. Additionally, Xilinx offers RSA2048 to authenticate the Zynq-7000 AP SoC first-stage boot loader (FSBL) and provides the necessary code to extend this authentication to all follow-on device loads. Building upon this layer of security, Xilinx provides methods to “lock the door” of the FPGA/SoC by showing the user how to disable external interfaces such as the JTAG controller. In addition to this physical protection, Xilinx demonstrates how to use the System Monitor or XADC to monitor the device’s environmental voltage and temperature. All of this and more is openly documented in *Developing Tamper Resistant Designs with Xilinx Virtex-6 and 7 Series FPGAs* [Ref 16]. Building on all of these features, devices such as the Zynq-7000 AP SoC provide a secure platform from the moment power is applied.

Intellectual Property (IP)

For those users who do not wish to assemble their own custom security solution, but who operate in an environment where security is the first priority, Xilinx offers a secure solution in a single package. This solution is Security Monitor. It provides a solid layer of security wrapped up in a single IP core. Security Monitor includes not only use of the built-in secure features described in the previously cited Xilinx application note [Ref 16], but also adds a layer of security by monitoring device configuration memory to ensure nothing has changed since the initial configuration. This background monitoring of system health can detect and, if desired, correct any configuration memory change, either by an adversary or by a single-event upset (SEU). If an issue is detected, the user can correct it and return to a safe state—or, if desired, zero out the device contents, thus protecting the user’s IP. For more information on the full functionality of the Security Monitor IP core, refer to the *Security Monitor IP Product Brief* [Ref 17].

Conclusion

With the ability to closely integrate safe and non-safe functionality into a single device, Xilinx products deliver (among many other advantages) best-in-class quality, FIT, SEU handling, as well as unmatched tools and techniques (such as the IDF and IVT) to meet customers’ most stringent safety goals. Because the Xilinx safety technologies are certified standards-compliant, customers can count on a risk-free safety solution.

A high-level overview of Xilinx's functional safety solutions can be found in the Xilinx Product Brief *Xilinx All Programmable Functional Safety Design Flow Solution* [Ref 18].

Xilinx Deliverables for Functional Safety

Xilinx offers a broad range of deliverables for customers desiring to create functionally safe systems:

- A TÜV SÜD qualified safety data package [Ref 3]
  - Qualified tools (ISE 14.2 – 14.7) and methodology for safety designs with Xilinx FPGAs/SoCs
  - Safety Manual [Ref 3], Certificate and Test Report
    - V-Model, QM, and Reliability Data for devices
  - Isolation Design Flow (IDF) and Isolation Verification Flow (IVT) [Ref 11]
    - Integrates but separates safe and non-safe applications in one device
    - Reduces effort and risk of subsequent certifications
- SEU Mitigation IP [Ref 8]
  - Provides detection and correction of configuration upsets
- Tools for FIT Rate Analysis [Ref 7]
  - FIT rate calculator, essential and critical bit analysis – reduces FIT Rate consideration for safety applications
- Power Analysis tools [Ref 19]
- Xilinx and supply chain committed to quality and quality management
  - ISO9000 / QML / TL9000 / TS16949
- Secure Solutions [Ref 15]
  - Silicon security features
  - Security IP [Ref 17]
    - Security Monitor
  - Documentation [Ref 16]

Table 2 below highlights the applicable Functional Safety specs and safety integrity levels attainable with Xilinx FPGAs / SoCs.

Table 2: **Functional Safety Specifications and SIL / ASIL Attainable**

Functional Safety Specification	Safety Integrity Levels
IEC 61508 Edition 2.0 2010-04	SIL1 to SIL3
ISO 26262 First Edition 2011-11-15	ASIL-A to ASIL-D

References

1. "A New Accident Model for Engineering Safer Systems," Nancy Leveson, *Safety Science*, Vol. 42, No. 4, April 2004, pp. 237-270
2. Xilinx Annual Quality Report March 2013
3. Xilinx website Functional Safety Package landing page (*registration required to access page*)
4. Xilinx user guide UG116, *Device Reliability Report, Fourth Quarter 2013*
5. Xilinx website Single Event Upsets
6. Xilinx white paper WP402, *Considerations Surrounding Single Event Effects in FPGAs, ASICs, and Processors*
7. Xilinx white paper WP395, *Mitigating Single-Event Upsets*
8. Xilinx product guide PG036, *LogiCORE IP Soft Error Mitigation Controller v4.1*
9. Xilinx application note XAPP538, *Soft Error Mitigation Using Prioritized Essential Bits*
10. Xilinx website Avionics landing page (*registration required to access page*)
11. Xilinx website Isolation Design Flow (IDF)
12. Xilinx application note XAPP584, *Spartan-6 FPGA Dual-Lockstep MicroBlaze Processor with Isolation Design Flow*
13. Xilinx user guide UG081, *MicroBlaze Processor Reference Guide*, (EDK 14.7)
14. Logicircuit Inc. website, DO-254 MicroBlaze 1.00a
    http://logicircuit.com/products/do-254-microblaze-1-00a
15. Xilinx website Design Security Solutions
16. Xilinx application note XAPP1084, *Developing Tamper Resistant Designs with Xilinx Virtex-6 and 7 Series FPGAs*
17. Xilinx product brief CS1140_AD, *Security Monitor IP Core*
18. Xilinx product brief PB015, *Xilinx All Programmable Functional Safety Design Flow Solution*
19. Xilinx user guide UG440, *Xilinx Power Estimator*

Revision History

The following table shows the revision history for this document:

Date	Version	Description of Revisions
04/09/2015	1.0	Initial Xilinx release.

Disclaimer

The information disclosed to you hereunder (the “Materials”) is provided solely for the selection and use of Xilinx products. To the maximum extent permitted by applicable law: (1) Materials are made available “AS IS” and with all faults, Xilinx hereby DISCLAIMS ALL WARRANTIES AND CONDITIONS, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, OR FITNESS FOR ANY PARTICULAR PURPOSE; and (2) Xilinx shall not be liable (whether in contract or tort, including negligence, or under any other theory of liability) for any loss or damage of any kind or nature related to, arising under, or in connection with, the Materials (including your use of the Materials), including for any direct, indirect, special, incidental, or consequential loss or damage (including loss of data, profits, goodwill, or any type of loss or damage suffered as a result of any action brought by a third party) even if such damage or loss was reasonably foreseeable or Xilinx had been advised of the possibility of the same. Xilinx assumes no obligation to correct any errors contained in the Materials or to notify you of updates to the Materials or to product specifications. You may not reproduce, modify, distribute, or publicly display the Materials without prior written consent. Certain products are subject to the terms and conditions of Xilinx’s limited warranty, please refer to Xilinx’s Terms of Sale which can be viewed at http://www.xilinx.com/legal.htm#tos; IP cores may be subject to warranty and support terms contained in a license issued to you by Xilinx. Xilinx products are not designed or intended to be fail-safe or for use in any application requiring fail-safe performance; you assume sole risk and liability for use of Xilinx products in such critical applications, please refer to Xilinx’s Terms of Sale which can be viewed at http://www.xilinx.com/legal.htm#tos.

Automotive Applications Disclaimer

XILINX PRODUCTS ARE NOT DESIGNED OR INTENDED TO BE FAIL-SAFE, OR FOR USE IN ANY APPLICATION REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS APPLICATIONS RELATED TO: (I) THE DEPLOYMENT OF AIRBAGS, (II) CONTROL OF A VEHICLE, UNLESS THERE IS A FAIL-SAFE OR REDUNDANCY FEATURE (WHICH DOES NOT INCLUDE USE OF SOFTWARE IN THE XILINX DEVICE TO IMPLEMENT THE REDUNDANCY) AND A WARNING SIGNAL UPON FAILURE TO THE OPERATOR, OR (III) USES THAT COULD LEAD TO DEATH OR PERSONAL INJURY. CUSTOMER ASSUMES THE SOLE RISK AND LIABILITY OF ANY USE OF XILINX PRODUCTS IN SUCH APPLICATIONS.