Functional Safety Solution Brief

INTRODUCTION

Xilinx's comprehensive functional safety design flow simplifies and accelerates safety certifications supporting IEC 61508 and ISO 26262. Together with Xilinx's unique SoC architecture, functionally safe implementations at the smallest size are possible.

Artificial Intelligence (AI) requires compliance to Safety standards to guarantee predictable behavior for autonomous decision-making. Xilinx SoCs have a rich history supporting the markets Industrial Automation, Automotive, Medical, Aerospace and Defense with safe products. Advantages are:

- High performance computing with acceleration in programmable logic
- On-chip heterogenous hardware redundancy with ARM Cortex A9/A53, Cortex R5 and MicroBlaze RISC softcore processors
- OTA Silicon - Updates are possible throughout the entire lifecycle
- Integration of complex and complete systems into a single device
- Long-term availability and extended temperature support

Xilinx products, designed with safety in mind, are developed to meet established standards for safety and reliability requirements. Xilinx co-operates with leading test institutes to assess Xilinx devices, design flows and tool architectures. Certificates are available for all parts of applicable design flows. Xilinx supports:

- Certifiable design flow to detect and avoid systematic failures
- Monitoring of the system at runtime to detect random failures
- Monitoring of the system at runtime to detect common cause failures
- Pre-defined consequent action on detected failures and transition into a safe state

ZYNQ® — PROVEN TECHNOLOGY

VIVADO® — CERTIFIED DESIGN FLOW

UltraFAST™ — COMPLETE SET OF IP AND TOOLS

Xilinx Complete Functional Safety Design Concept

XILINX INDUSTRIAL AND HEALTHCARE IOT SOLUTIONS STACK

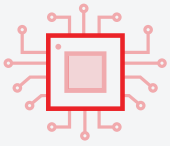
APPLICATION

EDGE AI

EMBEDDED SW
FOR MIXED CRITICALITY

ANY-TO ANY CONNECTIVITY
SMARTER CONTROL
EMBEDDED VISION

FUNCTIONAL SAFETY
& CYBERSECURITY



SILICON ARCHITECTURE

SAFETY STANDARDS

Leading test institutes assessed and certified Xilinx Design Tools against applicable standards:

- **Vivado (incl. SDK, HLS, SDSoC)** for Versions 2015.2, 2016.2 and 2017.3.1 by TÜV Süd
  - IEC 61508-3:2010
  - ISO 26262-8:2011
- **ISE** for Versions 14.2 and 14.7 by TÜV Süd
  - IEC 61508-3:2010
  - ISO 26262-8:2011
- **MicroBlaze Compiler (GNU Compiler)** for Versions 2015.2 and 2016.2 by SGS TÜV Saar
  - IEC 61508:2010 up to SIL4 class T3 tool
  - ISO 26262:2011 up to ASIL D, TCL1
- **Zynq UltraScale+ MPSoC** for Device Architecture and Safety Manual by Exida
  - IEC 61508:2010 part 1, 2 and 3 up to SIL 3 with HFT=1
  - ISO 26262:2011 parts 2,4,5,6,7,8,9 and 10 up to ASIL C

XILINX SAFETY DESIGN SOLUTION

Xilinx comprehensive functional safety design flow solution for FPGA and SoC includes:

Xilinx's certified toolflows and devices

- Certificates and related reports for development and validation toolflows and methods
- Safety Manuals
- Software Safety User Guides (only for SoCs)
- Zynq-7000 Safety Design Example with dedicated Safety Concept and assessment by TÜV Rheinland
- Reliability Reports (two updates per year) incl FIT rate calculator
- Triple Modular Redundancy and two core Lockstep with MicroBlaze Softcore RISC Processor
- Functional blocks to detect and correct errors in netlist (Single Event Upsets) and identification of "essential bits" in a device configuration
- Software test libraries (STLs) for Zynq Ultrascale+ MPSoC
- FMEDA tool and FMEDA calculation examples
- Application Notes and scripts to calculate base failure rates
- Built-in system monitors in Xilinx devices and related applications notes
- Isolation Design Flow for separation of safe and non-safe functions

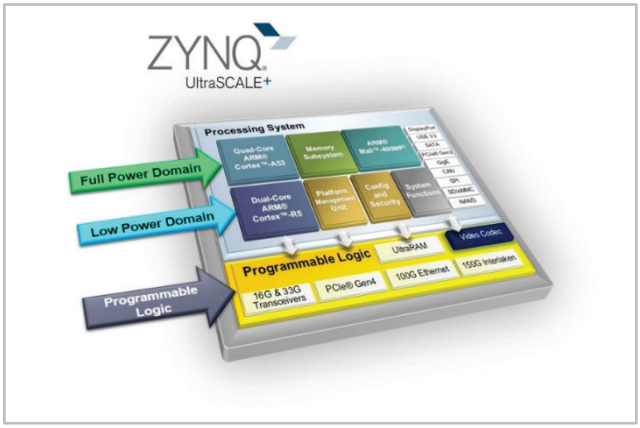
ANNUAL FUNCTIONAL SAFETY WORKING GROUP

Meet Xilinx's safety architects and systems engineers at the annual Functional Safety Working Group in late spring or early summer. Dates and places of the events are announced on the website for Xilinx Functional Safety (https://www.xilinx.com/products/technology/functional-safety.html, click on tab "Functional Safety Working Group" for event details).

INNOVATIVE DEVICE ARCHITECTURE FOR FUNCTIONAL SAFETY

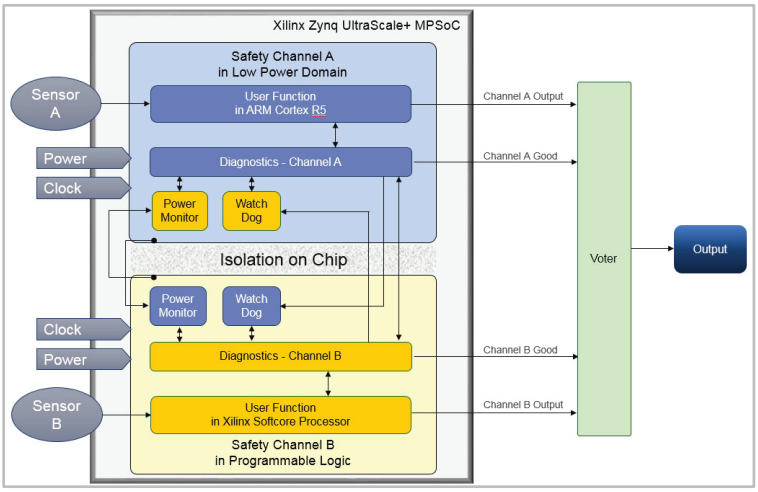
Xilinx Zynq UltraScale+ MPSoC is designed to be Functional Safety certifiable.
That results in a versatile System-on-Chip which fits ideally in modern Safety Concepts.

ESSENTIAL CHARACTERISTICS



Xilinx's Zynq UltraScale+ MPSoC Overview

- **Three separated chip domains** with independent power supply and clocks to achieve HFT≥1
  - Low Power Domain
  - Full Power Domain
  - Programmable Logic Domain
- **Low FIT**
  - Reliable and power-saving 16 nm FinFET technology
- **Protection for safety-critical elements**
  - Triple Modular Redundant Boot, Safety & Error Management processors
  - Lockstep for ARM Cortex R5
- **ECC** on all critical memories
- **Hardened Memory Protection Units and Periphery Protection Units**
- **Configuration and Security Unit** with triple modular redundancy
- **System monitors** for Common Cause Failure detection:
  - Voltage - Temperature - Clocks
- **Testable Architecture**
  - Logic BIST - Memory BIST - Error injection - Software Test Libraries



On-chip heterogenous hardware redundancy with Zynq UltraScale+ MPSoC

XILINX FUNCTIONAL SAFETY PACKAGE

Xilinx Functional Safety Package gives you access to the entire Safety documentation and all tools.
A web-based Functional Safety Lounge which is exclusive to subscribers provides access to latest information.

LICENSING AND ORDERING INFORMATION

The Xilinx All Programmable Functional Safety Design Flow Solution Safety package can be purchased under ordering code EM-DI-SAFETY-SITE, which gives full access to the functional safety solutions as well as real time updates for one year.

Extensions of an existing license are offered at 75% discount under order code EMR-DI-SAFETY-SITE.

For more detailed discussions about the Xilinx functional safety design flow solution, please contact your local Xilinx sales representative.

Xilinx's web-based Functional Safety Lounge

CONCLUSION

Zynq UltraScale+ MPSoC was designed with safety and security in mind and is the ideal architecture to support industrial IoT platforms and future generations of automotive, aviation, and AI-based systems.

With the innovative Xilinx Zynq UltraScale+ MPSoC architecture in combination with the recent IEC 61508 safety certification of the supporting Vivado Design Suite by TÜV Süd and the MicroBlaze™ compiler for additional soft processors by SGS-TÜV Saar, Xilinx now provides a complete ecosystem based on robust design flows that includes supporting documentation, assessment reports, and IP to minimize risks for customers.

Developers can retrieve tools and resources to support highly integrated safety-critical systems design by purchasing access to Xilinx's online Functional Safety Lounge. Privileges include access to the Safety Manual for Zynq UltraScale+ MPSoC, device and architecture updates, tool-flows and documentation including future reports and assessments. To learn more, visit https://www.xilinx.com/applications/industrial/functional-safety.html

Notice of 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 the Limited Warranties which can be viewed at http://www.xil-inx.com/warranty.htm; 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 Critical Applications: http://www.xilinx.com/warranty.htm#critapps.