Xilinx All Programmable Functional Safety Design Flow Solution

PB015 July 9, 2014 **Product Brief**

Introduction

Xilinx provides a comprehensive and TUV SUD certified functional safety design flow solution to our customers to simplify and accelerate functional safety certifications according to IEC 61508, ISO 26262, DO-254/DO-178.

Over the last decades Xilinx FPGAs have been and are being used in a wide variety of industries and applications. The success is based on to their inherent value of:

- Configurability and increased performance.
- Integration of complex and complete systems into a single device.
- Reliability and long life time.

The unique value proposition of Xilinx FPGAs and All Programmable (AP) SoCs help you to drive innovations in:

- Industrial
- Automotive
- Medical
- Aerospace and Defence

In all these markets, reliability and safety is a key requirement, and designers are concerned about developing their products to meet established standards defining the minimum safety and reliability requirements. Xilinx FPGA and AP SoC are used at the heart of products that comply with functional safety requirements, and designers are concerned with questions like:

"How can I leverage the benefits of FPGA and at the same time, meet the functional safety requirements imposed by established standards?"

Safety Standards

The safety standards that are established worldwide are: ·

- Industrial - IEC 61508, (IEC62061/ISO13489)
- Automotive - ISO 26262
- Medical - IEC 60601
- Process Industry - IEC 61511
- Aerospace and Defense - DO-254/ D0178b

The fundamental safety standards immediately relevant to FPGA designs are IEC 61508, ISO 26262, and DO-254/DO178b.

Xilinx Certified Safety Design Flow Solution

Xilinx provides a certified and comprehensive functional safety design flow solution for FPGA and AP SoC which includes:

- Certificate and Reports.
- FPGA design and verification tools and methodologies.
- IP and devices.

This solution helps to shorten the certification process by many months.

The solution delivers essential project documentation and guidelines, along with Functional Safety system IP.

© Copyright 2013-2014 Xilinx, Inc. Xilinx, the Xilinx logo, Artix, ISE, Kintex, Spartan, Virtex, Vivado, Zynq, and other designated brands included herein are trademarks of Xilinx in the United States and other countries. AMBA, AMBA Designer, ARM, ARM1176JZ-S, CoreSight, Cortex, and PrimeCell are trademarks of ARM in the EU and other countries.All other trademarks are the property of their respective owners.

Xilinx's unique and certified functional safety design methodologies allow you to integrate safety with general applications in the same device. Xilinx Isolation Design Flow (IDF) and Isolation Verification Tools (IVT) provide a certified methodology to separate areas on the FPGA. Designs can be placed into these areas and physically isolated. The areas can be changed at any time without impacting other isolated locations, proven by the IVT tools (*impact analysis*). For more information, see http://www.xilinx.com/applications/isolation-design-flow/index.htm.

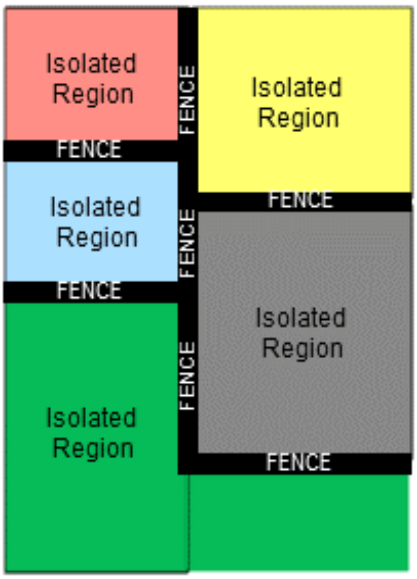

Figure 1: **Isolation Design Flow**

The solution includes:

- Certification for ISE® Design Suite 14.7 tools.
- Safety manual, *Elements for the Safety Guidelines IEC 61508 and ISO 26262* (UG990).
- SEM IP (diagnostic IP).
- IDF/IVT methodology.
- Comprehensive training for Xilinx products and Xilinx functional safety design flow solutions.



ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

CERTIFICATE

No. Z10 14 06 84605 002

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 for FPGA software development in safety-related applications 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, 2014-06-17

(Guido Neumann)

584192

Page 1 of 1

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

TÜV®

A1 / 04.11

Figure 2: **Certification**

Qualified Tools

Table 1-1: **ISE Design Suite Qualified Tools**

Tool/Feature	ISE Design Suite			Applicable Document (Doc ID) for v14.7
	Logic Edition	Embedded Edition	DSP Edition	
PlanAhead™	✓	✓	✓	UG632 UG685
ISE Simulator (ISim)	✓	✓	✓	UG626
XST Synthesis	✓	✓	✓	UG687 UG628 UG658
Power Optimization	✓	✓	✓	UG733 UG786 UG440

Table 1-1: **ISE Design Suite Qualified Tools *(Cont'd)***

Tool/Feature	ISE Design Suite			Applicable Document (Doc ID) for v14.7
	Logic Edition	Embedded Edition	DSP Edition	
Partial Reconfiguration(1)	✓	✓	✓	UG702 UG743 WP374
Design Preservation(2)	✓	✓	✓	UG748 WP362
CORE Generator™	✓	✓	✓	CORE Generator Help
iMPACT	✓	✓	✓	iMPACT Help
Additional Flow				
Isolation Design Flow	✓	✓	✓	UG747 UG633 UG676
Diagnostic Tools				
SEM (Soft Error Mitigation)	✓	✓	✓	PG036
ChipScope™ Pro and the ChipScope Pro Serial I/O Toolkit	✓	✓	✓	UG029
Xilinx SEU FIT-Rate Calculator(3)	✓	✓	✓	Release Version 1.2g 10-10-2011

Notes:

1. This feature is used for Isolation Design Flow.
2. This feature is used for Isolation Design Flow and to preserve safe or non-safe designs against changes.
3. Xilinx SEU FIT-Rate Calculator is a spreadsheet included in the safety package, and is not part of the ISE tool download.

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.

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

References

For more information on the markets served by Xilinx, use the links below:

1. http://www.xilinx.com/applications/industrial/index.htm
2. http://www.xilinx.com/applications/automotive/index.htm
3. http://www.xilinx.com/applications/aerospace-and-defense/avionics/index.htm
4. http://www.xilinx.com/applications/medical/index.htm
5. http://www.xilinx.com/support/documentation/white_papers/wp461-functional-safety.pdf

Revision History

The following table shows the revision history for this document:

Date	Version	Description of Revisions
07/09/2014	1.1	Updated Figure 2, Certification.
07/31/2013	1.0	Initial Xilinx release.

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.xilinx.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.

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.