Evaluation of FPGA Design Tools for Safety Systems with On-Chip Redundancy Referring to the Standard IEC 61508

Emil Gracic, Ali Hayek, Josef Börcsök
Chair for Computer Architecture and System Programming
University of Kassel
Kassel, Germany
e-mail: emil.gracic@uni-kassel.de, ali.hayek@uni-kassel.de

Abstract—**Internet of Things and Industry 4.0 lead to great possibilities of technical innovations but also to great risks and hazards. Not only the data has to be secured, but also the processing systems have to be more reliable and safe. From this perspective, implementation of safety related systems based on separated chip dies should belong to the past. ASIC developers have already designed diverse redundant system architecture on a single chip die. In last four years major FPGA manufacturers, Xilinx and Intel Altera, have been trying to establish a concept for implementing of redundant systems on a common FPGA. This study evaluates such concepts and conducts a comparative analysis with the requirements of international safety standard IEC 61508. Respectively, it argues with empirical results and discusses why the statements about reaching a SIL3 on FPGA platform are recently controversial. To resolve this kind of limitation, this research work proposes new conceptual modifications of current FPGA structure.**

Keywords-safety; FPGA; redundant; IEC 61508

I. INTRODUCTION

The Internet of Things (IoT) has been permanently growing. Consequently, it forces development of new technologies and conceptual solutions in order to manufacture this hyper-connected network defined as "an infrastructure of interconnected objects, people, systems, and information resources together with intelligent services to allow them to process the information of the physical and the virtual world and react" [1]. However, it cannot be assumed that only data becomes subject to manipulation as described in many studies [2] [3] [4]. In particular, all parts of this network have to be considerable maintained – sensor, actor and processing systems. We have to observe a data from various perspectives, from its genesis across transfer till the processing. According to the criticality of application field the requirements on processing systems differ significantly. In this context, system development must undergo a standardization process in order to achieve a certificate and confident level of safety and reliability. In medicine branch one has to follow the requirements of the international standard IEC 60601, in process industry IEC 61511, in automobile sector ISO26262 etc. All these standards have been derived from the general standard IEC 61508, which regulates functional safety implementation of electrical, electronic and programmable electronic systems [5]. The last edition from 2010 defines requirements for On-Chip redundant (OCR) solutions. In ASIC world, many respectable OCR-systems occurred in last few years such as Hercules TMS570 from Texas Instruments dedicated to automotive systems [6], or HiCore1 from HIMA [7] dedicated to process industry.

The primary objective of this study is to analyze and to evaluate the capabilities for implementing of Safety Integrity Level 3 (SIL) categorized systems on a FPGA platform. It offers important insights into design concepts of leading FPGA manufacturers – Xilinx and Intel Altera, for creating OCR architectures and provides a review of some controversial statements about certified SIL3 solutions. An investigation of new models for future FPGA structure will be also proposed in order to bring the FPGA on the same state of art as the current ASICs and to be respectable competitor for safety IoT applications.

In the next section basic principles of norm related implementation of On-Chip redundancy will be highlighted. Section III presents concepts of leading FPGA manufacturers Xilinx and Intel Altera for isolation of separated system components on a single FPGA chip. Focus of this work – analysis and evaluation of those concepts with proposal of methodologies for reaching confidence for higher safety integrity levels will be outlined thereafter. Finally, chapter VI summarizes this work.

II. BACKGROUND

As aforementioned International Electrotechnical Commission (IEC) 61508 is a general standard with the scope to define a whole safety lifecycle for functional safety implementation of electrical, electronic and programmable electronic (E/E/PE) devices. Other industry standards as ISO 26262 for automotive or IEC 60601 for medicine are its derivatives. To categorize a confidence of implemented safety one has to determine a SIL of complete system architecture. SIL is defined as "probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time" and considers two aspects [5]:

- Systematic integrity, which is related to methods of systematic failure avoidance and proven in use evidence of related system components and development tools.
- Hardware integrity, which is related to quantifying of random faults and architectural characteristics of

978-1-5386-3322-9/17/$31.00 ©2017 IEEE

the system especially to requirements for On-Chip redundancy defined in Annex E of the second norm part.

In the past, architectural constraints affected designing of redundant systems based on two separated chip dies. Introduction of the OCR principles made the development of redundant systems on a common chip die feasible.

Considering architectural characteristics based on diverse redundancy concepts and a Safe Failure Fraction (SFF) – parameter, which describes diagnostic capabilities of related system [8], SIL can be categorized as given in Table I.

A. IEC 61508 Requirements for On-Chip Redundancy

The requirements for implementing of OCR on common semi-conductor substrate are defined in Annex E of the second norm part. Those, which are crucially important, can be summarized as:

- Separate physical blocks for each channel (part of redundant architecture) or monitoring element with its own separated inputs and outputs.
- Interconnections between the separated blocks must have sufficient distances between each other in order to avoid shorts and cross talk.
- Separate power supply for each channel in order to avoid Common Cause Failures (CCF).
- Temperature analysis, monitoring and handling.
- Complete Common Cause Analysis (CCA) has to be performed.

B. Beta Factor β_{ic}

Furthermore, a vulnerability of an OCR system to CCF has been determined as β_{ic} factor. It has a quantitative nature and it should be estimated according to the measures, which either increase the basic value of β_{ic} or decrease it. The basic beta factor is set on 33 % and has to be reduced on minimally 25 % or even less. Outlined, increasing measures can be formulated as:

- Interconnections between separate blocks.
- Internal monitoring units.

While decreasing measures refer to:

- Diversity in functionality and failure controlling.
- Decoupling of physical blocks and separate power supply.
- Diverse test and diagnostic structures.
- Methods for thermal monitoring and handling.

III. State of Art

Major FPGA manufacturers – Xilinx and Intel Altera have been trying recently to establish a conceptual solution in form of an adopted design flow for creating OCR systems. The concepts are presented in details later on. Moreover, it can be concluded that the Altera model was more automated in the early stage than those from Xilinx. On the contrary, Xilinx model provided a deeper insight into decoupling and separating structures. Consequently, it was appropriate for the detailed analysis and evaluation.

TABLE I. SIL Categorization [5]

Safe Failure Fraction	Hardware Fault Tolerance (Redundancy)		
	0	*1*	*2*
< 60%	Not allowed	SIL1	SIL2
60 % - < 90%	SIL1	SIL2	SIL3
90% - < 99%	SIL2	SIL3	SIL4
≥ 99%	SIL3	SIL4	SIL4

However, with the latest Xilinx tools version it can be argued that the significant differences in automatization level and design methodology are not present.

A. Xilinx Isolation Design Flow IDF

In 2013, Xilinx certified its tools for system development in functional safety area. Standard design flow existing in ISE and Vivado tools has been modified and adopted to achieve the goal of isolating the safety related/critical components on a common FPGA chip. As a result, new design concept - Isolation Design Flow was published [9] [10]. The main characteristics are:

- Each safety related component owns its separate partition.
- Each separate partition is isolated due to a block of unused logic called "fence".
- Each separate partition occupies one or more I/O banks and do not share it with other partitions.

Fig. 1 shows adoption of standard design flow for the isolation objectives. An Isolation Verification Tool (IVT) [11] has been introduced to check whether the all isolation rules defined in [10] are fulfilled.

IVT verifies floorplan constraints and the netlist of the complete system [10]. Interconnections between the isolated components are conducted by using different Look-Up-Tables (LUT). This principle is called "Trusted Routing".

B. Altera's Functional Safety Separation Flow

Altera's design flow takes into consideration almost all aspects as Xilinx IDF – separated partitions for safety related components and separated I/O register banks. Interconnections between the separated partitions are also realized via different LUTs. Comparing to IDF fence building it is worth mentioning that Altera does not publish details on the way the separation area has been created. In particular, it consists of unused FPGA elements but the details are hidden. Fig. 2 describes Altera's separation concept referring to [12].

First, one has to define safety related components and to preserve partitions for them. The crucial step is the integration of those components based on creating of LogicLock regions, which serve as physical location and separation. Further details can be found in [12].

IV. Analysis

The proposed concepts of Xilinx and Intel Altera for implementing of OCR systems on a common FPGA are very similar to each other as presented in previous chapter.

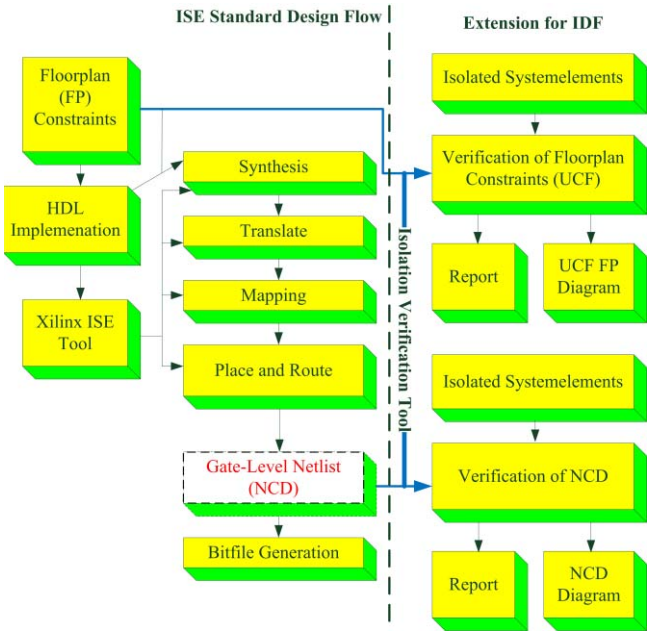

Figure 1. Comparison between standard and isolation design flow of Xilinx development tools

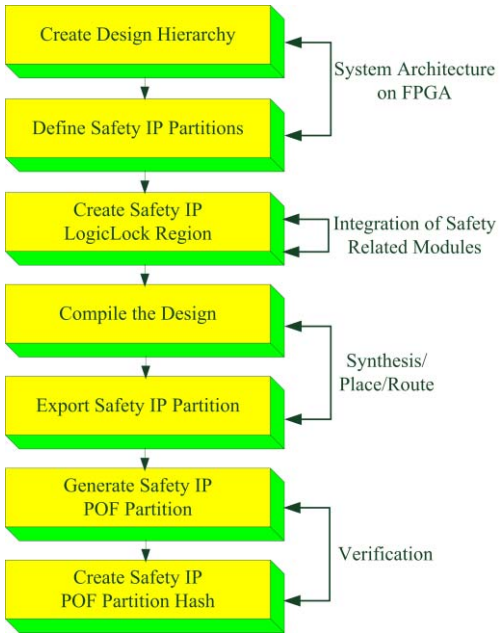

Figure 2. Altera's safety separation flow with Quartus II software

Considering general aspects of safety integrity both concepts will be disputed. To conduct deeper analysis of certified tools, Xilinx tools have been chosen, since they provide detailed access to design flow.

A. *Systematic Integrity*

As mentioned in the second section of this study, systematic integrity comprises two aspects – avoidance of systematic failures and evidence that the used development tools and system components are proven in use. The second one can be assumed as satisfied, since Xilinx and Altera received a certificate for development of safety related applications. Discussable is avoidance of systematic failures and management of common cause failures. Indeed, Xilinx references diverse sources of CCF in [13] but no concrete solution for its avoidance or mitigation has been presented recently. The study [14] examined such measures for Spartan 6 FPGA. They are not applicable for other FPGA types and require modifications respectively.

B. *Hardware Integrity*

Quantifying of random faults as a part of hardware integrity is considerably covered by reliability reports, which are periodically maintained by leading FPGA manufacturers. On the other side, architectural requirements related to OCR and hardware tolerance degree have to be reviewed. Separation or isolation, which is particularly noticed for building of OCR refers only to physical logic separation. Separation area will be built due to an amount of unused logic and other FPGA elements. As a consequence of a complex networking and cross linking of routing and multiplexing elements, it cannot be argued, that isolated, redundant components are interference free.

C. *Temperature Analysis*

Referenced reliability reports provide an insight into thermal influences from the packaging perspective. Some Xilinx devices are supplied with temperature sensor placed in its middle. They might be used only if the redundant components are placed and routed in a characteristic manner. This way free configurability of FPGA systems will be significantly restricted. Alternatively, ring-oscillators can be used for on-line thermal monitoring, as described in [15].

One essential benefit of the mentioned design flows is the division of safety related components into separated partitions. It affects spreading of routing and logic elements, so that the hotspots will be avoided or mitigated referring to [16].

A remarkable gap existing in analysis is the manner the isolated components of OCR behave in some extreme conditions, for example when it comes to uncontrolled warming up of one component. Consequently, it cannot be argued that they are interference free from thermal point of view.

D. *Inconsistency of Xilinx Tools*

By implementing safety related systems and conducting of general design methodology it is particularly required to determine fixed principles and to certify those by respectable and wide accepted certification authority. Xilinx reports in [13] the certification process of its tools.

From this perspective at least two conclusions are very critical:

- Assignment of global clock buffers (BUFG). As presented and argued in [14] the separation of clocking elements can lead to the mitigation of common failures caused by clocking resources.

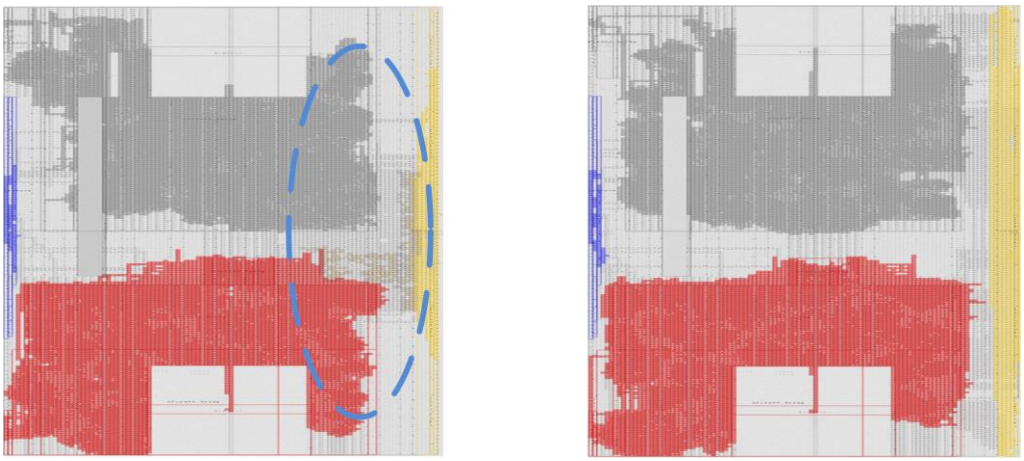

Figure 3. Inconsistency of IDF: left automated Trusted Routing, right manual forced Trusted Routing

By using Xilinx tool ISE 13.4 it is allowed different BUFGs to belong to different separated partitions. The higher versions do not allow such assignments. This effect was registered by system design with Spartan 6 and Artix 7 FPGAs.

- Remarkable difficulties with automated compiling process of complex system based on two softcore microcontrollers and two additional safety functions. Overall there are four separated components, which are building up the OCR. The use of interconnections based on Trusted Routing method as required in [10] causes with automated compilation process diverse isolation violations reported by IVT. Such violations can be eliminated only due to a manual and intuitive assignment of LUTs used for Trusted Routing. Fig. 3 depicts this issue. It was registered on Spartan 6 as well as on Artix 7.

E. Resource Overheads

Referred safety system based on four separated components has been longstanding designed and analyzed on Spartan 6 and Artix 7 platforms. It is worth mentioning that at least 40 % more resources per microcontroller partition were required for successful compilation. As result, 20 % of complete FPGA resources were dissipated. Translated in account of logic elements it considers 40 000 unused LUTs. This effect was observed with tools version 13.4 as well as with the version 14.7. Therefore, it is a systematic disadvantage.

V. EVALUATION

Xilinx concludes in [13] that its FPGAs are suitable for creating OCR systems and fulfilling the norm requirements up to SIL3, since the development tools have been certified. SIL3 is, as shown in Table I, achievable only by implementing redundant architecture. On the contrary, with single system solution one has to increase a diagnostic coverage over 99 %, which is nearly unrealizable. Furthermore, in the same study Xilinx forces a Zynq-7000 FPGA consists of two chip dies – one for programmable logic and another one for Cortex A9 based processing system in form of an ASIC chip [17]. Consequently, the demonstrated IDF may not be applicable.

On the other side, Intel Altera also argues the capability for achieving of SIL3 by implementing OCR system architecture. Altera's solution is based on NIOS II processors in lockstep mode (two processors are running in parallel and performing the same task) with diverse safety measures [18]. The solution is available as IP written in Verilog and can be implemented on a single FPGA by using safety separation flow. Controversially, in the same document Altera presents SafeFlex as SIL3 certified solution based on referred NIOS II lockstep system. SafeFlex [19] consists of two Cyclone V FPGAs and is not an OCR solution.

As already mentioned, since 2013 both manufacturers have been trying to establish a concept for implementing of redundant systems on a common FPGA chip. The background for observed contradictory lies in separation/isolation area. It consists of an account of unused logic and other elements. This area produces a static power, so that the isolated/separated components are not interference free from electrical and thermal point of view. The study [20] offers excellent analysis about methodology for creating interference free separation area on Spartan 3 FPGA. Summarized, all unused elements have to be connected to the ground.

Another relevant argument for discrepancy of proposed concepts is the effort for handling of common cause failures on a common chip. However, none manufacturer has presented any systematic approach for its avoidance or mitigation so far.

Contrasting Application Specific Integrated Circuit (ASIC) solutions to FPGA a major assessed difference is that the separation area does not include any logic. Such a gap does not produce static power. Respectively, the isolated components are clearly interference free. FPGA manufacturer have to implement this aspect, if they want to be competitive to ASIC devices and much more to be available as safety related OCR systems. One possible way to implement this requirement is to adopt existing design

flows by algorithms, which would automatically connect all unused FPGA elements to the ground. According to [20], it implies a significant effort. Another approach might be investigation of a new FPGA type, dedicated for functional safety applications, which would consist of certain separation areas free from any logic. It has also to be considered that the account of interconnections should be predefined. Elements for temperature measuring and handling could be integrated without a remarkable effort on a new platform. This way, the set of requirements from IEC 61508 related to temperature aspects would be met.

VI. CONCLUSION

Existing design flows for OCR implementation on the FPGA do not comply with the requirements of safety standards, since the major manufacturers offer either two-die in one package solution or two-FPGA solution. The main argument is insufficient grade of decoupling between isolated components. Furthermore, aspects of systematic integrity referring to avoidance of common cause failures are not adequately covered.

In the area of IoT two-die or two-FPGA solutions should belong to the past. The structure of field programmable devices has to be adopted or even better conceptually modified in order to satisfy requirements of safety norms and to be respectable solution for safety IoT applications.

REFERENCES

[1] ISO/IEC 2015, “Internet of Things, Preliminary Report 2014,” Geneva London, 2015.

[2] T. Xu, J. B. Wendt and M. Potkonjak, “Security of IoT systems: Design challenges and opportunities,” 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Jose, CA, 2014, pp. 417-423.

[3] J. A. Oravec, “Emerging “cyber hygiene” practices for the Internet of Things (IoT): Professional issues in consulting clients and educating users on IoT privacy and security,” 2017 IEEE International Professional Communication Conference (ProComm), Madison, WI, USA, 2017, pp. 1-5.

[4] D. Minoli, K. Sohraby and B. Occhiogrosso, “IoT Security (IoTSec) Mechanisms for e-Health and Ambient Assisted Living Applications,” 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), Philadelphia, PA, 2017, pp. 13-18.

[5] International Electrotechnical Commission, IEC/EN 61508, “International standard 61508: Functional safety, safety related systems,” Second Edition, Geneva, 2010.

[6] Texas Instruments, “Safety Manual for Hercules™ TMS570LS20x/10x ARM Safety Critical Microcontrollers,” April 2012.

[7] HIMA Paul Hildebrandt GmbH, “Safety System-on-Chip: Shorter time to market, even for high safety levels”

[8] J. Börcsök, “Functional safety : basic principles of safety-related systems,” Hüthig, Heidelberg, 2007.

[9] G. Corradi, R. Girardey and J. Becker, "Xilinx tools facilitate development of FPGA applications for IEC61508," 2012 NASA/ESA Conference on Adaptive Hardware and Systems (AHS), Erlangen, 2012, pp. 54-61.

[10] J. D. Corbett, “The Xilinx Isolation Design Flow for Fault-Tolerant Systems,” Xilinx White Paper, October 2103.

[11] J. D. Corbett, “Isolation Verification Tool (IVT) Software User Manual,” Xilinx User Manual, December 2013.

[12] Intel Altera, “FPGA-based Safety Separation Design Flow for Rapid Functional Safety Certification,” Dec. 2015.

[13] E. Hallett, G. Corradi, S. McNeil, “Xilinx Reduces Risk and Increases Efficiency for IEC61508 and ISO26262 Certified Safety Applications”, Xilinx White Paper, April 2015.

[14] E. Gracic, A. Hayek and J. Börcsök, "Implementation of a fault-tolerant system using safety-related Xilinx tools conforming to the standard IEC 61508," 2016 International Conference on System Reliability and Science (ICSRS), Paris, 2016, pp. 78-83.

[15] M. Happe, A. Agne and C. Plessl, "Measuring and Predicting Temperature Distributions on FPGAs at Run-Time," 2011 International Conference on Reconfigurable Computing and FPGAs, Cancun, 2011, pp. 55-60.

[16] S. Velusamy, Wei Huang, J. Lach, M. Stan and K. Skadron, "Monitoring temperature in FPGA based SoCs," 2005 International Conference on Computer Design, 2005, pp. 634-637.

[17] Xilinx, “Zynq-7000 All Programmable SoC Data Sheet,” June 2017.

[18] Altera, R. May, “Safety design on FPGA’s using soft Lockstep Processors,” 2016.

[19] SafeFlex, https://www.newtec.de/web/en/defence/products/SafeFlex/SafeFlex.php

[20] R. Girardey, M. Hübner and J. Becker, "Safety Aware Place and Route for On-Chip Redundancy in Safety Critical Applications," 2010 IEEE Computer Society Annual Symposium on VLSI, Lixouri, Kefalonia, 2010, pp. 74-79.