Safety-Related ASIC-Design in Terms of the Standard IEC 61508

Ali Hayek and Josef Börcsök
Chair of Computer Architecture and System Programming
University of Kassel
Kassel, Germany
ali.hayek@uni-kassel.de

***Abstract*—Due to the continuing development of semiconductor structures, it can be allowed nowadays to integrate more robust and high-efficient systems into a very small area of silicon. In such system-on-chip all individual components of a target system can be integrated into a single silicon die at lowest level, which in turn contributes in saving the substantial space and reduces power consumption and production costs. With the consideration of the miniaturization of safety-related systems into system-on-chips, where usually complete redundant architectures along with memory and interfaces are integrated into small silicon structures, many advantages can be taken into account. These advantages extend to all levels of the development cycle. In the present paper, the advantages of the miniaturization of integrated 1oo2D-safety architecture (one out of two with diagnosis) and its safety-aware implementation in terms of the safety standard IEC 61508 are presented.**

Keywords—Safety-related systems;Integrated Circuits; IEC 61508; on-chip redundancy

I. INTRODUCTION

Nowadays embedded System-on-Chip applications are increasingly used in several industrial control processes. Due to the development of silicon structures and thanks to the rapid development of the IP-Core market (Intellectual Property), Application Specific Integrated Circuits (ASICs) are increasingly used in several industrial applications compared to a decade ago. In this regard, one can integrate his own chip functionality concluding whole communication microcontroller units and other digital and analogue components can be today shortly integrated in such circuits. Latter makes from ASICs an interesting platform for realizing safety-related architectures, since those consist of complex redundant components which need to be implemented following stringent procedures and need to offer their functionality under specific conditions. Due to their flexibility of programming and reconfiguring at run-time, Field Programmable Gate Arrays (FPGAs) provide a popular platform for safety-related systems. Thus, the susceptibility of SRAM-based FPGAs to external effects increases with the ongoing miniaturization of silicon structures, such as the susceptibility to single-event upsets (SEUs). For this reason, the usage of SRAM-Based FPGAs in safety critical fields require the adoption of very specific reliability and fault tolerance techniques, in order to protect their functionality against such transient effects. In recent research work [1] a survey of using those FPGAs in safety-related systems was presented. In this paper, the disadvantages of using FPGAs such as the mentioned susceptibility to soft errors and the increasing part costs are solved by targeting ASICs as a platform for integrated safety-related systems. As against SRAM-based FPGAs, the functionality of systems implemented on ASICs is programmed only on time during the design and so permanent and immune to soft errors.

At a glance, this paper deals with the use of ASIC-based system-on-chips in safety-related systems conforming to established safety standards. In our opinion, there are two important points for dealing with this: the safety of the ASIC implementation itself and the safety properties of the hardware description code used to perform the functionality which is translated to the ASIC hardware.

In this paper, we first introduce the safety standards which are relevant for this work. Especially the standard IEC 61508 and its second edition (IEC 61508 Ed. 2) are explained in detail. In addition, the standard DO-254 from the field of aviation is introduced briefly, since it is widely used in the United States of America and has parallels to the standard IEC 61508. Afterwards, the safety-related 1oo2D-architecture is introduced. The heart of this research work is divided in two parts. First, a technical evaluation of using integrated architectures against discrete system solution, which is nowadays conform to the state of the art, is given. Second, an analysis of the use of ASICs according to the standard IEC 61508 second edition is introduced. Latter is divided into two main aspects: modeling and coding methodologies on software and physical measures on hardware. On the one hand, the implementation of standard techniques and measures on ASIC platform is motivated and discussed. This includes techniques for increasing the reliability of such systems like on-chip redundancy and safety-aware placement and routing. On the other hand, the coding methodologies of ASIC programming languages such as VHDL are discussed. In this context, we study the possibility of the use of these languages for realizing safety properties. Coding and verification measures are discussed in this section. Finally, the proposed techniques will be evaluated on ASIC using an example of the 1oo2D-architecture.

In the second section of this paper an overview about the relevant functional safety standards is given. Afterwards the targeted safety-related on-chip 1oo2D-architecture and its advantages are introduced. In section IV the software methodologies for safety-related on-chip systems are discussed. Section V presents hardware-based measures for the physical implementation of safety-related systems-on-chip. Section VI outlines the paper with a short conclusion and future prospects.

 ISBN: 978-1-61208-268-4

II. FUNCTIONAL SAFETY STANDARDS

Norms and standards for safety-related systems are not new; MIL-STD-882 from the US Department of Defense (DoD) developed in 1963, is the first standard in this area. This standard is derived from the military area. The idea was to improve the safety of weapons and to keep the risk of undesired accidental damage to people and the environment in an acceptable range. In 1998, a new paradigm was been developed with the standard IEC 61508 which has been associated with a new definition of the term “functional safety”. The main innovation is that in the context of functional safety only the safety features of a system are considered. The other non-safety-related functions are in accordance with the standard IEC 61508 only a part of quality management. In the following sections the standard IEC 61508 is primarily introduced, as the safety standard applied in Europe. Furthermore, a short insight into the standard DO-254 is given. Latter is irrelevant for the current research work but could be applicable in future considerations.

A. IEC 61508

The standard IEC 61508 [2] is a standard in the area of safety technology, which was developed by the International Electrotechnical Commission (IEC), an international standards organization, and first released in 1998. It is titled "Functional safety of electrical / electronic / programmable electronic systems" (E / E / PES). The standard is also known as basic safety standard, because it is application independent, but it addresses all safety functions of a system. It is regarded as basis for further application-specific standards. The standard IEC 61508 is limited on electrical and electronic programmable electronic safety-related systems. In this context, it defines four safety-integrity-level, so-called SIL. This applies: the higher the SIL, the safer the E / E / PES. The specification of SIL provides developers, producers and customers a clear and unequivocal basis for negotiating basic aspects of safety integrity.

The standard IEC 61508 is seen as a basis for further standards. In this regard, the standard gives sufficient flexibility for technical respectively technological innovations. The standard is also kept consciously abstract and flexible in regard to the methods to cover the requirements on hardware and software, while the requirement is clearly defined, it leaves ample room for researchers and developers to apply own implementation ideas and makes them free of the need to comply with stringent rules. In the context of in this research work considered ASICs, it gives for example a note on the requirements for using ASICs in safety-related applications. Furthermore, innovations find their way into new drafts of the standard. While using on-chip redundancy (OCR) was in the first standard version still unconsidered, it was contained in the following draft standards, and could thereby be taken into consideration by developers and certification bodies in terms of the standard. The main changes in the second edition of the standard are presented briefly in the next section.

B. IEC 61508 Ed. 2

Generally, the standard IEC 61508 is divided into 7 parts and provides a guide for developing safety-related systems. The specific implementation of the requirements is flexible. In the present work, the requirements for the development of safety-related systems based on ASICs conforming to the second edition of the standard IEC 61508 [3] are mainly considered. In the following the main novel features in the second edition are described briefly. In the next sections the applicable features for ASICs are argued in detail:

- New requirements for Application Specific Integrated Circuits (ASICs)
- Clear definition of Systematic Integrity Compliance Route (Route 1_S, Route 2_S and Route 3_S)
- Clear definition of Hardware Integrity Compliance Route (Route 1_H and Route 2_H)
- New definition of Proven-in-Use terms

C. DO-254

The standard DO-254 [4] is performed under the title "Design Assurance Guidance for Airborne Electronic Hardware" and is a standard for the development of complex electronic hardware systems in the aviation field. It was developed in April 2000 by the RTCA (Radio Technical Commission for Aeronautics) and EUROCAE (European Organization for Civil Aviation Equipment) and is today carried as a standard for the development of complex electronic hardware in the aviation field, of both by the American aviation authority FFA, as well as the European Aviation Safety Agency EASA demanded. The DO-254 is, like IEC 61508, a safety standard, which is also application independent, but specifically refers only to the hardware development.

Like in IEC 61508, it includes no binding guidelines for the direct implementation, but it lists conception guidelines for the intended certification of the whole development process. Outside the norm there are further standards, such as DO-178B [5], which deals exclusively with the software development in the aviation field. The standard specifies a complete documentation during development and takes into account the life cycle of the product. A consistent and binding implementation of the product life cycle from concept to decommissioning, as specified in IEC 61508, however is not requested.

III. INTEGRATED 1OO2D-ARCHITECTURE

The standard IEC 61508 gives a basis for realization of qualitative and quantitative analysis in areas of reliability and safety. Particularly, architectural measures were introduced, which are necessary to provide a desired safety or reliability such as the introduction of hardware fault tolerance, system redundancy and implementation of diagnostic and monitoring elements. Considering the use of hardware redundancy and hardware fault tolerance, MooN-system-architectures (M out of N) are usually targeted. The name describes the system architecture and the possible degradation behavior by fault

 ISBN: 978-1-61208-268-4

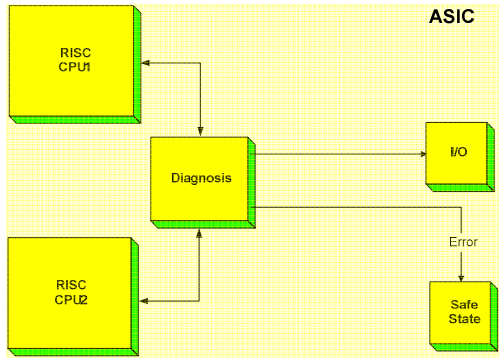

Figure 1. 1oo2D-Architecture

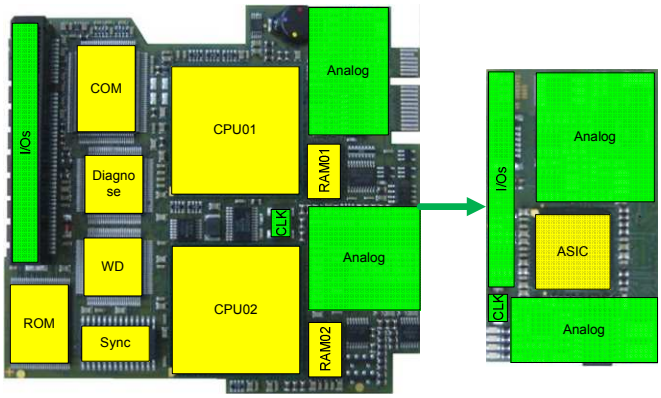

Figure 2. Integrated 1oo2D-Architecture

behavior. By this is meant that M out of N channels of a safety-related system are sufficient to transfer the system into a safe state. The lowest form of this redundancy is the present 1oo2-architecture. This represents a safety-architecture with hardware fault tolerance HFT = 1. In the following, the 1oo2-architecture and its advantages are discussed.

A. 1oo2D-Architecture

The 1oo2-safety-architecture (one out of two) is one of several system architectures which are described in the standard IEC 61508. This kind of architecture is composed of two parallel channels. If both channels of the system have a failure, the system loses the safety function. Additionally the 1oo2D-architecture is a 1oo2-architecture with integrated diagnostic units. Details of 1oo2D-architecture are explained in the following.

As mentioned above, a 1oo2D-architecture describes a complete system or a subsystem, consisting of two channels (main and redundant channel) with the same function. In case of failure, only one of the two channels is required to transfer the system into a safe state. A diagnostic unit compares continuously the results of both channels. If there is an inequality, this points to a faulty channel. The diagnostic unit signalizes this to the two channels and the faultless channel transfers the complete system to a safe state. The complete system remains therein until the fault is corrected and both channels are functioning again. If both channels fail independently of each other or by a fault with a common cause, the complete 1oo2D (sub-) system is not able to trigger the safe state. For such cases, external diagnostic measures such as watchdog, temperature and voltage monitoring are used to transfer the system into a safe state.

In Fig.1 below the block diagram of general 1oo2D-architecture on ASIC is given.

B. Advantages of the inetgrated 1oo2D-Architecture

Besides the 1oo2-architecture other architectures, such as 1oo3-, 2oo3- or 2oo4-architectures are used. Comparing the parameters for calculating the average probability of failure on demand (PFD) or per hour (PFH) the 1oo2-architecture arise very good values under consideration of minimal redundancy. The 1oo2-architecture has without any doubt their eligibility for systems that can be transformed to a safe state as needed.

The main target of the present work is the integration of the 1oo2D-architecture on a single ASIC. In this case, the redundant processor channels as well as diagnosis units are integrated into a single chip. Fig. 2 shows an example for the difference between an integrated and a discrete 1oo2D-architecture.With reference to the architecture shown in Fig. 2, the following obvious advantages for the integrated 1oo2D-architecture:

- System size and costs: The integration of all digital components of 1oo2D-architecture on a single ASIC reduces the total count of the required resources. Thereby the system size is clearly reduced and also the system costs which are required for the system implementation.
- Power consumption and system performance: By integration the count of individual components and size of the off-chip communication are reduced. This leads to a clear reduction of the power consumption of the complete system. Otherwise, the system performance of the system can be increased by using modern semiconductor process technologies which allow higher system clock rates.
- Reliability and safety: By the integration of 1oo2D-architecture on ASIC the reliability and safety of the complete system increase. This is due to the fact that the count of component and all contiguous factors (such packages, routing lines, solder joints, etc.) decrease. The latter results to a lower failure rate of failure (λ) for the complete system, and thus to better values of the reliability and safety parameters MTTF and PFD.

The integration of diagnostic units on hardware and software level is a further important feature of the 1oo2D-architecture. All important components of the system are monitored by diagnostic units and forwarded to the watchdog, which is responsible for transferring the system to the safe state. On one hand diagnosis units are implemented on hardware level such as system comparator for monitoring the several states of the redundant channels, as well as diagnosis and test blocks for dedicated safety functions such as voltage, temperature and clock monitoring units. On the other hand, the implementation of diagnostic units on software level is performed. In this

 ISBN: 978-1-61208-268-4

context, an essential component of this diagnosis is the implementation of safe operating system. The latter includes in addition to his usual tasks as operating system, a cycle-based monitoring of the system on software level. This includes the integration of different test routines that are responsible for all safety functions. Software test routines like CPU-tests, memory-tests, synchronization-tests are performed at this level.

Summarized, the integrated safety 1oo2D-architecture offers an increased degree of system safety and system reliability on smallest area and allows the realization of SIL3 systems in different areas of embedded systems.

IV. SOFTWARE METHODOLOGIES

In regard to the requirements of hardware and software, the ASIC development cycle is double edged: On the one hand, ASICs are hardware devices. On the other hand the development of ASICs is mainly done by software coding. Concretely, the ASIC description is usually written in so-called hardware description languages (HDL). Such a description is similar in many respects to classic programming languages. Usual representatives are currently VHDL and Verilog. System-C is a target language to generate code for both hardware and software systems. In this work System-C is not considered, but pure hardware description languages. In this section, the methodologies according to the standard IEC 61508 Ed. 2 are presented, which arise on coding and verification level for design safe ASICs.

A. *Safety-related Design Cycle*

To develop safety-related systems on ASIC level, the standard IEC 61508 Ed. 2 recommends an approach based on the V-model shown in Fig. 3. This is due to the fact that ASIC system development is not only a hardware development, but also a software development. In this context, requirements of both Part 2 and Part 3 of the IEC 61508 are considered for the used HDL code. This is especially in view of avoiding systematic faults important and useful. For this, appendix C in Part 3 offers guidance for quantifying the systematic safety integrity. More general requirements for safety-related ASIC-design include:

- Clear, unambiguous, testable requirements;
- Traceable safety requirements specifications;
- Detailed specific hardware and software specifications, among others, Interfaces, Performance and response times;
- Requirements on systematic safety integrity:
  - Avoiding systematic faults according to IEC 61508 Part 2 and Part 3 (Route 1_S),
  - Using of proven-in-use elements (Route 2_S),
  - Only software: requirements of IEC 61508 Part 3 (Route 3_S);
- Requirements on hardware safety integrity: to determine Route 1_H or Route 2_H;
- Systematic safety integrity: systematic ability of the elements of the safety functions, architecture-related restriction of max. SIL.

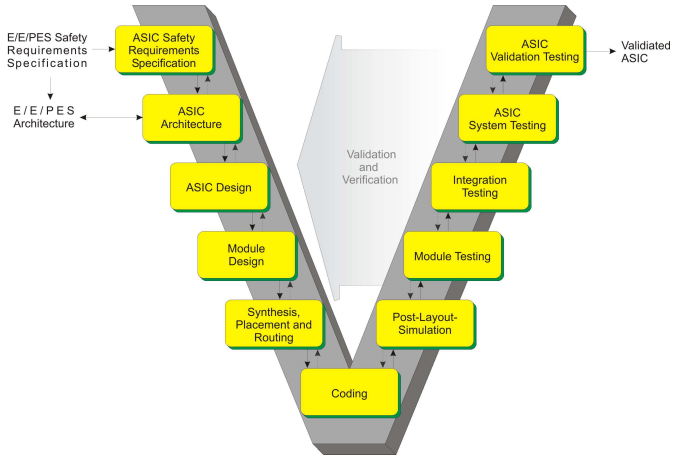

Figure 3. V Model for ASIC-development conforming to the safety standard IEC 61508

The three routes to avoid systematic errors mentioned above can be interpreted as described below.

For proven-in-use elements the residual number of systematic error is assumed to be small enough. Proven-in-use elements are defined as those elements which were used long enough used in similar projects. This primarily means that the field experience with the used elements should be conforming to the targeted SIL. Elements which are even already certified for the intended SIL can surely meet the requirements for systematic safety integrity following the route 2S. Route 1S refers to hardware; in our case to the hardware chip itself and its substrate, layout and manufacturing process, but also the HDL code. Although the latter also has software characteristics, it also applies for HDL code the requirements of Part 2 of the standard IEC 61508. Route 3S is reserved for the software running on the developed ASIC, e. g. safe operating system, driver software and application.

In any case, measures and methodologies for avoiding systematic faults, and thus for increasing systematic safety integrity are treated in Appendix F of Part 2 of the standard. The main part is represented in tabular form, wherein some measures and methodologies for respective SIL are recommended or not recommended. Considering an ASIC design as software, Part 3 of the standard introduces different requirements for software.

B. *Coding Methodologies*

Considering an ASIC design as software, Part 3 of the standard introduces different requirements for software that are applied in HDL code. The most important in our view are listed below:

- Modularity
- Other methods to reduce code complexity;
- Programming conforming to following aspects:
  - functionality,
  - exchange of information between elements,
  - timing behavior,
  - timing constraints,

 ISBN: 978-1-61208-268-4

  - concurrency,
  - data structures,
  - design-related assumptions and dependencies,
  - exception Handling (on HDL-level: Wiring of interrupt control lines),
  - pre-conditions, invariants, results / post-conditions,
  - comments;
- Ability to represent the design at multiple levels (structurally, functionally) - this is generally satisfied with HDL,
- Intelligibility.
- Testability (on verification and validation level).

In this context, the standard also requires the determination of suitable coding rules and naming conventions. But these are not specified, it is left to developers to define in advance useful guidelines.

Finally, for verification issues HDL tests are especially targeted. To illuminate this topic is beyond the scope of this document. For more information this and about requirements on HDL code in general, see our related work in [7].

V. HARDWARE METHODOLOGIES

After the software methodologies have been introduced in the last section, this section deals with the technical implementation of the safety-related systems on ASIC level. In this context, the term “on-chip Redundancy” is introduced in detail. Furthermore, the requirements and implementation methodologies of OCR on ASIC are presented. Furthermore, the handling with common cause failures is argued briefly. Finally an example for an ASIC-based 1oo2D-architecture is represented in the last section.

A. On-chip Redundancy

On-chip redundancy (OCR) is defined as a multiple (redundant) component implementation on a single chip. Hereby is generally not specified whether these components are active or passive redundant components. In Fig. 4 an example of a double on-chip redundancy is shown.

For the purposes of functional safety one usually considers channels; over the entire loop from sensors to control logic and actuators. In this regard, OCR could be used in order to implement redundant control logic or even the whole loop without using multiple chips. In case auf ASICs, the simplest example is a 1oo2-architecture described above; therefore a single ASIC could be used to implement two processors channels and its needed diagnosis components. Architecture-related requirements for ASICs in general with OCR are described in Appendix E in Part 2 of the standard IEC 61508. At a glance, it is noted that the requirements apply to purely digital ASICs with common substrate. Furthermore, there are currently no requirements for ASICs with a mixed design of digital and analog parts, so-called mixed-mode ASICs, or even purely analog ASICs. It is also noted that the standard in terms of OCR and in favor of safety is driving a more conservative

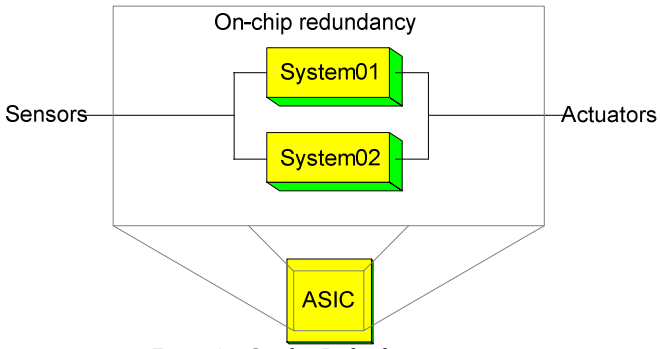

Figure 4. On-chip Redundancy

course. For this reason, the maximum SIL is limited to SIL 3. Nevertheless, the requirements on OCR are the following:

- Restriction to SIL 3,
- No systematic skills upgrading by combination,
- Consideration of random errors by temperature increasing,
- Physical channel separation by formation of blocks with "sufficient" distance to avoid short-circuits, for instance by electron migration and crosstalk
- Short circuits and crosstalk between adjacent lines of different blocks must not lead to failure of a safety function,
- Measures to avoid errors caused by faulty power supply, e.g. noise, crosstalk, high currents caused by short circuits, ...
- Connecting the substrate to ground, independent of the design process, for example n-well or p-well CMOS,

From practical view some of the requirements can be covered by concrete simulation runs for the target process technology design, such as temperature propagation at maximum clock frequency. Other requirements, such as avoiding cross talk, can be covered by applying concrete formal assessments for the routing. For other requirements, such as noise and the migration of soft errors, sufficient probability models or statistical experience results can be applied. For the minimum distance required between physical blocks experience values depending on the targeted process technology can be took into account. In any case, all these measures and methodologies have to be evaluated and fixed in agreements with the suitable certification authority, .e.g. TUV.

Finally, it is important to mention that fulfilling concrete measures to cover the above requirements depends heavily form the target application and the target process technology. In a failure mode and effects analysis (FMEA) and arrangement with the certification authority these aspects should be sufficiently considered.

 ISBN: 978-1-61208-268-4

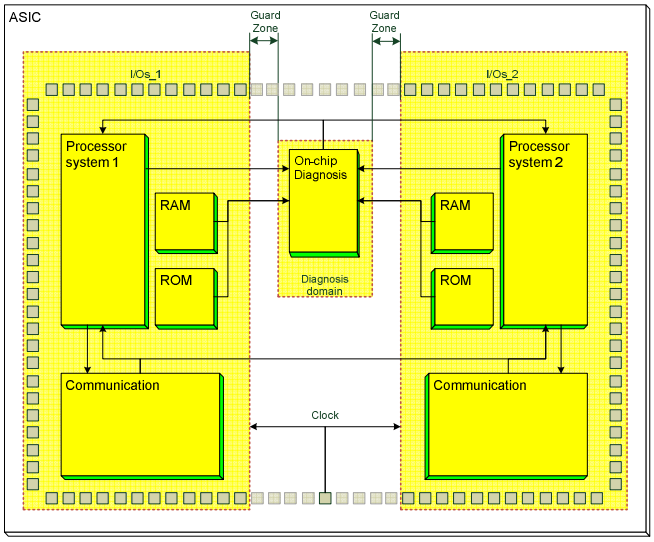

Figure 5. Safety-related ASIC Implementation

B. Commom-Cause Faults

In addition to the previously considered single-point failures, it is important to consider faults which have common cause, so-called common-cause faults. This is described in detail in the standard and be touched upon only briefly here. For ASICs with OCR a base-beta factor β_{IC} of 33% is assumed. By applying additional measures according to the tables given in the standard IEC 61508 this factor may increase or decrease. Thus the resulting beta coefficient is: $\beta_{ASIC} = \beta_{IC} + \Sigma$ modification. This shall not be higher than 25%. More information on this can be found in the standard. In this context, the following aspects are to be considered:

- Recognizing an uncontrollable faults - by diagnostic units, online tests, proof tests - needs to reach or holding the safe condition,
- For each channel and each singular executed monitoring component a diagnostic coverage (DC) of at least 60% should be achieved,
- Only diversely implemented (also differently designed) channels may monitor each other and thus improve as a watchdog the SFF and DC
- Homogeneous channels may only act as watchdogs for other channels if high SFF and DC has been already sufficiently reached,
- Tests regarding electromagnetic compatibility (EMC) with additional safety margin should neither impair the IC functionality neither destroy it
- Unsymmetrical wiring should be avoided as much as possible.

C. ASIC Implementation

This section describes the implementation of the measures presented in the previous sections illustrated by a case example. In the context of a recent research work, the implementation of a redundant 1oo2-architecture with on-chip diagnostic has been presented for FPGA implementation [6]. In Fig. 5 the block diagram of this architecture is shown. In this diagram the implemented measures according to section V A and B are mentioned. The physical separation and the establishment of guard zone are realized by using ASIC design tools. The width of the guard zone is weighted conforming to the guidelines of the standard IEC 61508 and depend on the used semiconductor process technology. Each channel is placed in a separated power domain and has its own power supply pins. The routing between the channels is effected by the use of special pre-routing blocks affected by the used design tools.

VI. CONCLUSION

Safety-related ASIC-design conforming to the safety standard IEC 61508 was introduced in this paper. First the target 1oo2D-architecture was presented. Afterwards, the advantages of the integration of this architecture on ASIC platform were motivated. Furthermore, software and hardware based methodologies for safety-related ASIC-design were presented. The key methodologies are on-chip redundancy and safety-related ASIC implementation. Particular attention was paid to the separation channel by power domains and guard zone. Finally, the determination of the beta factor for on-chip redundant design channels was briefly introduced. Techniques and measures to improve it were also presented and discussed in terms of the standard. In a future work the physical ASIC-implementation will be published.

REFERENCES

[1] A. Hayek and J. Boercsoek, “SRAM-Based FPGA Design Techniques for Safety Related Systems Conforming IEC 61508: a Survey and Analysis,” Second International Conference on Advances in Computional Tools for Engineering Applications (ACTEA), IEEE Conference Publications, Zouk Mosbeh, Lebanon, 2012, pp. 319–324

[2] International Electrotechnical Commission, IEC/EN 61508: International Standard 61508 Functional Safety: Safety-related Systems, Geneva; 2005

[3] International Electrotechnical Commission, IEC/EN 61508: International Standard 61508 Functional Safety: Safety related Systems: Second Edition, Geneva; 2010

[4] RTCA Inc., “DO-254: Design Assurance Guidance for Airborne Electronic Hardware,” Washington D.C., USA , 2000

[5] RTCA Inc., “DO-178: Software Considerations in Airborne Systems and Equipment Certification,” Washington D.C., USA , 1992

[6] J. Boercsoek, A. Hayek, B. Machmur and M. Umar, “Design and Implementation of an IP-based Safety-related Architecture on FPGA”, XXII International Symposium on Information, Communication and Automation Technologies (ICAT), Sarajevo, Bosnia and Herzegovina, IEEE Conference Publications, 2009, pp. 1–6

[7] A. Hayek, M. Schreiber and J. Boercsoek, “Basic VHDL tests conforming to IEC 61508”, Seventh International Conference on Networked Sensing Systems (INSS), Kassel, Germany, 2010, IEEE Conference Publications, 2010, pp. 41–44

 ISBN: 978-1-61208-268-4