

This white paper describes the successful steps in achieving certification for an FPGA implementation of an application certified for functional safety. Safety is a critical system requirement in developing machinery that must comply with worldwide established standards such as the IEC 61508 basic functional safety standard. Altera's pre-qualified Functional Safety Data Package shortens development and certification time and reduces certification risks in safety-critical industrial applications.

Introduction

Many application developers have concerns about incorporating functional safety. Project managers and members of the validation team are confronted with a new and unknown field of safety certification. The concerns are typically caused by the fact that a certifying body, external auditor, gets involved with the project team. Authority over process and quality no longer lies only within the company's responsibility; it is supervised externally.

Safety projects require an increased amount of process and documentation. Fortunately, not all process steps have to be re-invented or created from scratch. By using prequalified tools or applying predefined techniques and measures, it becomes much easier to achieve safety certification. Documentation plays an important role, and international standards require a stricter level of following defined rules in a project. Therefore, it helps to rely on an already-qualified set of documents, processes, and methods.

To simplify and speed up the certification process, Altera worked with TÜV Rheinland and obtained qualification for Altera® FPGA devices, IP, the FPGA design flow, and development tools. This qualification means that Altera tools, methodologies, and devices are sufficiently free of systematic errors and can be used in safety-critical applications.

How to Start

The main intent of functional safety is to prevent the risk of injury or death as a result of random, systematic, or common-cause failures in safety-relevant systems. So-called random failures are caused by a malfunction of the safety system's parts or components in contrast to systematic failures that are a result of a wrong or inadequate specification of a safety function. A common cause failure is the simultaneous malfunction of several parts of the safety device caused by a single reason, like a single power rail powering multiple components on a board. Typically the goal for product development is to get a low probability of failures during operation, or in other words, to achieve a high level of quality and reliability. Functional safety defines qualitative measures for this quality and reliability and makes it even harder for the product definition and development to achieve them.



101 Innovation Drive
San Jose, CA 95134
www.altera.com

© 2011 Altera Corporation. All rights reserved. ALTERA, ARRIA, CYCLONE, HARDCOPY, MAX, MEGACORE, NIOS, QUARTUS and STRATIX words and logos are trademarks of Altera Corporation and registered in the U.S. Patent and Trademark Office and in other countries. All other words and logos identified as trademarks or service marks are the property of their respective holders as described at www.altera.com/common/legal.html. Altera warrants performance of its semiconductor products to current specifications in accordance with Altera's standard warranty, but reserves the right to make changes to any products and services at any time without notice. Altera assumes no responsibility or liability arising out of the application or use of any information, product, or service described herein except as expressly agreed to in writing by Altera. Altera customers are advised to obtain the latest version of device specifications before relying on any published information and before placing orders for products or services.



The first question to investigate before starting a safety project within your organization or company is: Which procedures are already established and available and can be reused to build the foundation for a functional safety project? Many companies apply management tools to achieve a high level of process quality, and by that, high product quality and reliability. For example, the ISO 9000 family of international standards (ISO 9000 ff.) defines the means and measures for quality management (QM) systems that are typically summarized in a QM manual. This manual provides a description of the applied methods for the daily workflow. As compliance to this quality standard is usually audited by an external certification body, it is ensured that these processes follow worldwide recognized requirements.

One of the eight pillars of ISO 9000 ff. is the description, implementation of, and compliance to company-specific procedures. The standard requires a process-oriented approach within a certified organization. Maintaining well-defined processes helps in repeatedly achieving high-quality results. The procedures are typically traceable and continuously improved.

Quality Management System

An organization's QM systems can help start a safety-relevant project because responsibilities within the company are already clearly defined, and the procedures for handling documents are very well understood. Documents are reviewed and contain all the relevant information to assure process and product quality.

The following list describes a set of attributes that should be included in each document or can be obtained by a corresponding document list to guarantee clear document identification and relevance based on the International Electrotechnical Commission's IEC 61508:2010-1 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems standard, clause 5 and annex A:

- Document author (with description of the function within the project)
- Document version number
- Document date
- Document history
- Reference documents
- File location within a dedicated storage system
- Unambiguous and standardized document naming
- Clear assignment to certain project steps

To avoid errors and missing or wrong product features, all the documents are reviewed and the reviews are documented in a review report. In addition, all specified requirements have to be traceable throughout the entire project to ensure that all requirements will be implemented, tested, and validated. Companies even need to document later modifications of requirements in order to understand the changes months or years later.

Similar to functional safety projects, ISO 9000 ff. requires internal audits on a regular basis to ensure compliance to QM system and to identify improvements. All these measures help guarantee a high level of quality not only in standard projects, but also in safety-relevant projects. They are a critical prerequisite of all safety-relevant work.

Project Preparation

As quality standards are usually state-of-the-art, they constitute a base to start a safety project. The following topics summarize the main features of a QM system:

- Definition of responsibilities within a company or project team
- Description of available and applied processes
- Management and handling of process-accompanying documents
- Clear and repeatable procedures

These aspects are described in more detail in clause 6 of IEC 61508:2010-1.

Safety is not just about writing high-quality C- or (V) HDL-code and assembling printed circuit boards. Safety is an overall design philosophy applied to all phases a product undergoes during its lifetime. The following sections will focus on additional aspects associated with functional safety.

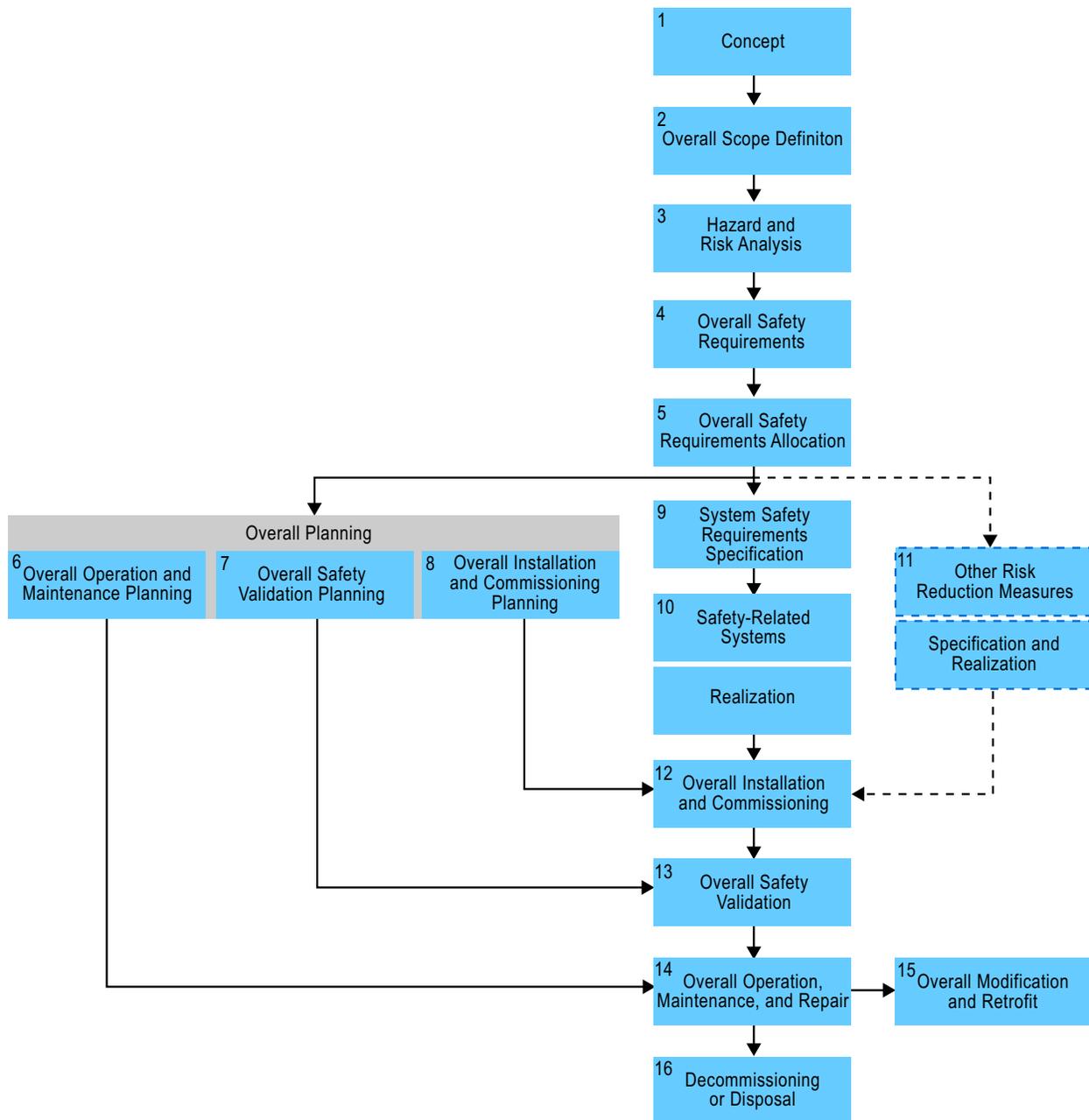
Functional Safety According to IEC 61508:2010

The second edition (edition 2) of the international standard IEC 61508:2010 published in 2010 includes several modifications and enhancements which have led to a state-of-the-art standard that validates a reliable level of product quality for functional safety. The standard consists of seven parts:

- General requirements
- Requirements for electrical/electronic/programmable electronic safety-related systems
- Software requirements
- Definitions and abbreviations
- Examples of methods for the determination of safety integrity levels
- Guidelines on the application of IEC 61508-2 and IEC 61508-3
- Overview of techniques and measures

Figure 1 shows how IEC 61508:2010 with its seven parts is mapped into a more refined process that guides the user through the lifecycle of a safety application.

Figure 1. Safety Lifecycle According to IEC 61508-1:2010



Edition 2 of this international standard covers among other new topics FPGA, ASIC, and CPLD technologies. These components play an important role in today's product development. Because FPGAs are increasingly replacing electronic components typically used for industrial applications, standards like the IEC 61508 have to support these evolving technology trends if they want to keep their relevance. This is achieved through regular updates to the specification.

Product Safety Lifecycle

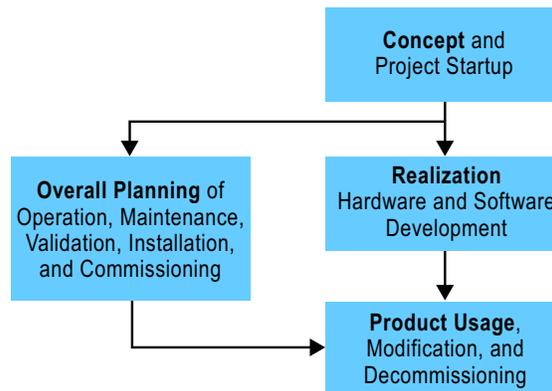
Safety as an overall philosophy and requirement includes the complete product lifecycle from its beginning to the very end when the product is retired. In other words, it has to be deeply embedded in planning the system. Safety must be included in the design methodology of safe equipment early on and cannot just be considered as an afterthought. This is in contrast to typically standardized development processes that tend to cover the design, implementation, and verification of a product only. Safety considerations do not end until the decommissioning of a product. IEC 61508:2010 describes the entire lifecycle of functional safety equipment, starting from first concept description and ending at the decommissioning of a product (Figure 1).

Project Phases

At first glance it seems that functional safety simply just introduces a significant amount of additional work at no value. If the concept and specification phase receives the required attention, then projects become much more predictable and achieve a higher level of quality. Investing in early phases of the project immediately brings an increase in productivity for the following work.

Referring to Figure 1, the functional safety lifecycle contains 16 cohering steps. As the process looks fairly complex, a segmentation into four main project phases helps structure the lifecycle model more clearly (Figure 2).

Figure 2. Main Project Phases



Each of these project phases will be discussed in more detail in the following sections. This white paper mainly focuses on functional safety with FPGA applications, and as such, the readily available support from Altera for the different project phases is described together with the individual project phases.

V-Model

The V-Model (Figure 3) is commonly used in a huge variety of projects. It is a successor of the waterfall model (Figure 4) which defines a sequential design process. Compared to the waterfall model, the V-Model offers enhanced feedback and monitoring possibilities and separates the process of product specification from test, verification, validation, and integration. It describes a set of steps to be done during a project life cycle and begins with the decomposition of requirements and the clear definition of all necessary system specifications. In parallel each of these decomposition steps are accompanied by a corresponding verification step. The point of intersection of these two paths is the creation of hardware and software.

Figure 3. V-Model Simplified

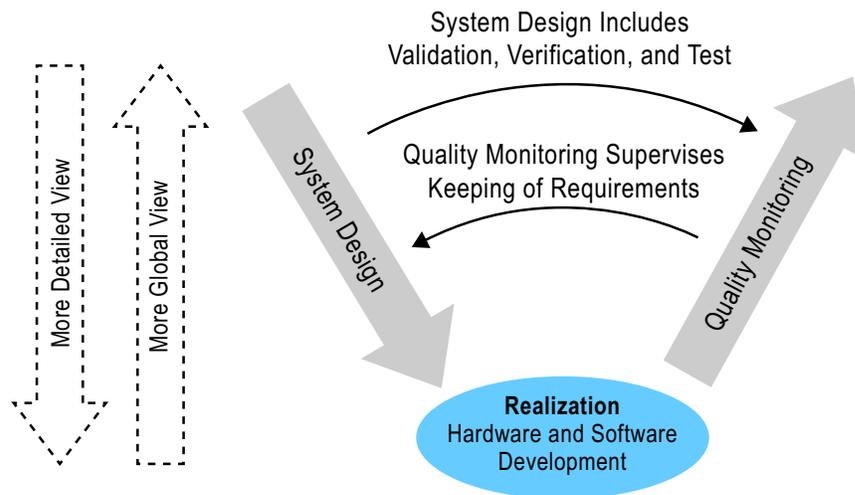
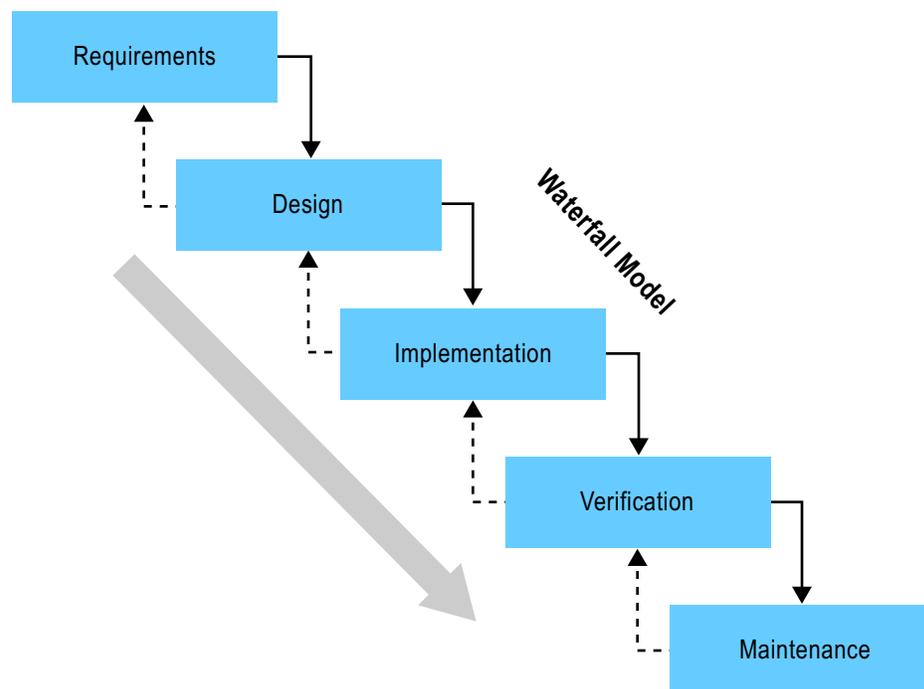


Figure 4. Waterfall Model



Two main aspects have to be considered when following the V-Model. It has to follow the IEC 61508:2010 lifecycle requirements, and each step of the V-Model requires particular documents to be attached as a precondition (input) as well as a result (output) after a successful completion of the step.

The TÜV-qualified Functional Safety Data Package (FSDP) from Altera contains a detailed document to guide the user in drafting a process structure. It supplies a development FPGA V-Model that can be reused, and the internal FPGA development process can adapt easily to this model to comply with the safety requirements. This FPGA V-Model is approved according to IEC 61508:2010 and comes with a detailed description of the input and output documentation recommended for each step. Each of these FPGA V-Model steps contains a detailed description of the step itself, the verification methods to be applied, and the tools to be used. This detailed documentation reduces the time the project team has to invest in a safety-centric FPGA development process significantly, and if Altera's recommendation is adopted as is, then no time has to be invested in this critical project phase.

Configuration Management

A configuration management has to be installed to guarantee traceability and reproducibility for any kind of project. It defines a set of tools that are used within the project. Functional safety also requires that these tools be capable of fulfilling functional safety requirements and qualified for use in safety projects.

It is of great value if a tool vendor like Altera qualifies its tool chain for use in functional safety projects. IEC 61508-3:2010 highly recommends the use of certified tools for software design and development. If this certification is not available from the tool's vendor, it will be very difficult for the user to independently verify the tools needed for the project. Only a tool manufacturer has all the detailed information and knowledge necessary to perform a reliable tool qualification. Altera has already certified Quartus® II development software version 9.0 SP2 together with TÜV for use in safety-relevant projects. This certification includes a list of detailed recommendations on how to use the tool, tool flow, intellectual property (IP), and silicon data. In addition, the package includes certification checklists and references the detailed FPGA documentation.

Concept

Normally the draft specification of a functional safety concept is the most important part of the entire safety-relevant project. Having a well-defined concept determines the overall success of a project. The safety concept is also the very first step in the certification process as the certifying body should approve this concept before the project can progress to the next phase. Reviewing the concepts with the assessor at a later stage might require significant changes to the system's safety concepts, and implementation work may have to be revisited. Once the concept is approved, there are only very few possibilities to change, add, or remove safety-relevant features. This safety concept clearly defines the content of a project.

An example may illustrate this issue in more detail. The hardware fault tolerance (HFT) defines the minimum number of faults that can cause a complete drop through of the entire safety function. For example in a dual-channel architecture, a dangerous fault of one component does not destroy the entire safety function because the second channel still keeps the safety function working. In this case, the system has a HFT of one. The HFT has a significant influence on the achievable Safety Integrity Level 3 (SIL 3) of a safety product and is a major architecture decision.

A HFT of 1 can be realized, for example, by two different redundant channels that can move the equipment under control (EUC) into a safe state in case of emergency. If one channel fails, the system can still rely on the remaining second channel. This is a fundamental design decision and has to be described clearly and early on in the safety concept. Later on in a project, it cannot be as easily changed.

Besides normal project management aspects which are already part of the project plan, the following aspects have to be considered in the safety concept:

- Overall description of the system and its main parts
- System boundaries, usage, and mission profile
- Definition of the safety functions that will be implemented
- Interfaces to the system
- Analysis of risks that have to be reduced by safety functions
- Evaluation of the necessary SIL for risk reduction
- Additional standards that need to be followed depending on the range of use
- Description on how to achieve the required SIL
- Architecture principles

Depending on the kind of product, this list may not be complete yet. As each safety system is adapted to particular functional safety needs, it requires different topics to be described in the safety concept document. It is obvious that the safety concept requires a good level of accuracy and knowledge of all requirements, and an early involvement of the certifying body is required to identify gaps early.

Fundamental issues in a safety concept can be detected before the implementation starts. Altera's FSDP offers detailed information about the applications and safety functions that can be realized in an FPGA platform. This information contributes further to the simplification of the concept phase and speeds up the overall planning process.

Preparation of Quality Measures

In addition to the V-Model in [Figure 3](#) that highlights all specification and design steps, it is important to note that each of these steps requires a related method to ensure the overall quality. To extend this model toward functional safety, the international standard IEC 61508:2010 defines in more detail which techniques and measures should be applied to guarantee a successful implementation of a functional safety project.

Techniques and Measures

Parts 2, 3, and 7 of IEC 61508:2010 provide detailed lists of techniques and measures. Depending on the desired SIL, a certain set of methods has to be applied to a particular extent. From the beginning of the project on, it has to be determined and documented which techniques and measures will be used.

An example is table F.2 in part 2 of IEC 61508:2010. This table in combination with part 7 of the standard defines which technique or measures have to be applied if a certain SIL has to be realized. In the design phase a “script-based procedure” is recommended if SIL 2 is desired. The same method is highly recommended for SIL 3 applications because SIL 3 requires a higher level of applied techniques and measures compare to SIL 2. The Quartus II tool command language (Tcl) flow is the suggested tool for this purpose. Altera provides detailed information on how to fulfill the needs of IEC 61508:2010 with its list of techniques and measures that prevent the introduction of faults during design and development.

With Altera’s FSDP, the selection of measures and techniques is already done, well documented, and ready to be used by the development team. This helps in understanding the application of methods, especially when realizing the very first safety-related FPGA project. In addition, these methods are also clearly linked to tools that implement them.

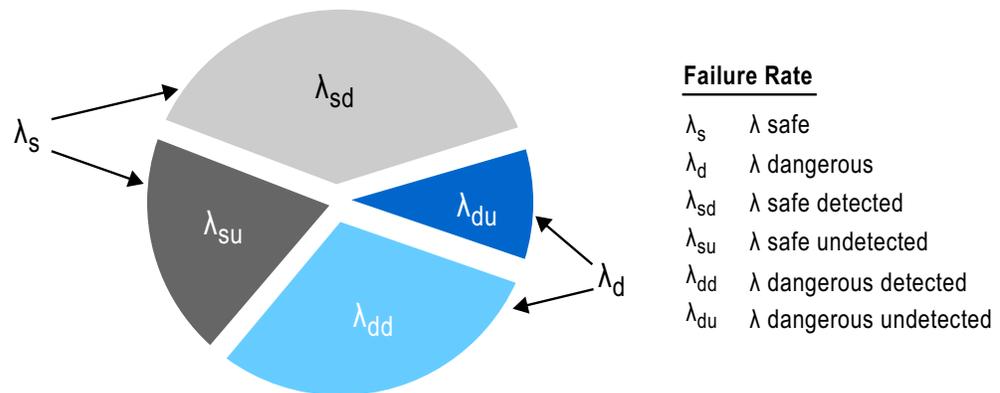
In order not to forget any of the required documents and design steps, Altera’s FSDP provides detailed checklists which help the development teams ensure that for all lifecycle phases the necessary input and output documents are available. In addition, a set of lifecycle actions are defined to verify that all phases are performed completely. As these checklists are already qualified by TÜV, no additional work is necessary to show how it will be guaranteed that the development V-Model of Altera’s FSDP is used correctly.

Safety Demand Modes

Safety functions are categorized into two classes: Low-demand mode of operation and high-demand mode of operation. Low-demand mode of operation refers to safety functions with a demand frequency of less than one time per year to set the EUC in a safe state. Therefore, the characteristic safety key value for this class of safety functions is called probability of dangerous failure on demand (PFD) and describes the risk that a safety function fails in the moment it is triggered.

High-demand mode of operation refers to safety functions used more than once a year or that are permanently used to set a EUC in a safe state as part of normal equipment operation. In this case, the safety key value is called average frequency of dangerous failure per hour (PFH) and describes the probability a safety function fails during one hour operating time. As an example, the PFH value has to be located within the range of $10^7/h$ and $10^8/h$ to achieve SIL 3.

In both cases (PFD, PFH), the remaining probability of failure for a safety-relevant product has to be calculated (Figure 5).

Figure 5. Different Types of Failure Rates

The hardware determines this probability value, and international standards provide detailed information on failure probabilities of electronic components and publish λ -values. With semiconductor devices like microcontrollers or FPGAs, the situation is more complex as the number of transistors and the internal structure of the chip has to be very well-known to support an overall calculation of the λ values.

This detailed information about the internal structure of a semiconductor device is usually difficult to retrieve. Altera offers its customers an annual reliability report with detailed information on the λ value in failure in time (FIT) of each type of available devices. Altera provides an application note that explains how the data in the reliability report has to be applied to the IEC 61508 certification. Providing this information as part of the qualified data package saves a significant amount of time and effort in the project documentation phase and later on during product certification.

Realization

The realization project phase covers hardware and software development as well as the diagnostic function.

Hardware and Software

To model and implement safety-relevant electronic systems, it is possible and desirable to combine self-developed Verilog HDL or VHDL modules with off-the-shelf, complex intellectual property (IP) functions like the Nios® II processor, which in the Altera case already has been qualified for use in safety-relevant designs. In cases where the processor is used together with the functional safety part of the system, all relevant requirements of the IEC 61508:2010 standard have to be applied. Part 2 of IEC 61508:2010 covers hardware aspects of functional safety and part 3 deals with software-related topics. Finally, part 7 provides an overview of the techniques and measures mentioned in part 2 and 3.

Software for functional safety demands a consideration of the entire software lifecycle as well. Part 3 of IEC 61508:2010 includes all steps of the software lifecycle in detail. It also outlines the requirements for the specification, validation, design, and development of software as well as software modifications and verification.

Altera provides additional benefit when using a Nios II processor by pointing out different items that are of relevance depending on the desired SIL. These items deal with topics such as the usage of interrupts, Quartus II software and the Nios Integrated Development Environment (IDE) versions, and variants of assembler, compiler, and linker tools.

Diagnostic Coverage

It is impossible to develop a safety-relevant product that is guaranteed to be 100% free of errors. The important point is to detect as many errors as possible and to move the EUC into a safe state in case of failures. Possible failures are subdivided in two classes. The first type of error does not cause a dangerous situation (λ_s) and the second type of error leads to a non-safe or dangerous state (λ_d). In addition, these failure rates are subclassified into detectable (λ_{sd} and λ_{dd}) or undetectable (λ_{su} and λ_{du}) failure classes as explained in [Figure 5](#). If it is possible to detect a failure, the EUC is brought into a safe state to mitigate the risk of the cause of failure. The most important aspect to consider for the reliability of a safety function is the fraction of failures that can be detected or do not lead into a dangerous state in relation to all possible failures.

IEC 61508-2:2010 defines the safe failure fraction (SFF) of a device with the following equation and the λ values of [Figure 5](#):

$$\text{SFF} = \frac{\sum \lambda_s + \sum \lambda_{dd}}{\sum \lambda_s + \sum \lambda_{dd} + \sum \lambda_{du}}$$

It is obvious that the SFF value will get a higher value with a reduced number of undetected dangerous failures (λ_{du}) in a safety-relevant design.

Part 2 of IEC 61508:2010 differentiates two types of elements that are used for safety systems. Elements are regarded as type A if, for example, the failure modes are defined well and the element behavior under fault conditions is entirely known. If a safety system is only built up out of type A elements, it is treated as a type A system. In other cases or if one element of a safety system does not fulfill type A requirements, the entire system is considered type B. Type B systems contain at least one component with unknown failure modes or an unpredictable failure behavior.

Depending on the type of the safety system and its hardware fault tolerance, the SFF together with the PFD or PFH value have a significant influence on the SIL that can be achieved. FPGA designs are considered mainly type B as they are based on complex semiconductor devices. As a result of this, it is required that the SFF be in the range of 90% to 99% to achieve SIL 3 with a dual-channel architecture.

One of the best techniques to increase the safe failure fraction is to raise the amount of diagnostic coverage within the design. This can either be achieved through additional diagnostic software or redundant hardware with monitoring capability. A benefit of using FPGA technology is that diagnostic features can be implemented on a hardware level. This saves the effort of writing additional software code and is less time-consuming and impactful to the system performance than software-based diagnostics. FPGAs can easily provide resources and capabilities in the logic array such that no extra electrical components or devices are required.

Altera's FSDP comes with IP cores that provide fundamental diagnostic functions. A clock checker diagnostic IP core can be used for monitoring the frequency and presence of a clock signal against a stable reference clock. The single-event upset (SEU) diagnostic IP core offers the possibility to identify SEUs in the FPGA to alert the system. The SEU core also provides functionality to test the diagnostic IP and the system response to an alert through means of inserting errors. And a cyclic redundancy check (CRC) diagnostic IP core can be used to calculate and check CRC values across a communication link.

Dedicated software algorithms for the Nios II processor to run diagnostic functions on memory, registers, and other processor parts have to be implemented in the same way as for stand-alone microcontrollers.

Conclusion

More effort may be necessary compared to most standard projects for the first functional safety project. However, a high level of reusability in subsequent projects can be expected because of the detailed processes, measures, and techniques provided by the functional safety standards. A profound examination of existing tools, quality measures, and resources will bring additional benefits and simplification to establishing a new application development process for safety projects within the company. FPGAs offer design flexibility and are well supported in terms of functional safety through Altera's upfront investment in providing methods, qualified tools, and devices together with qualified IP and diagnostic IP.

As the V-Model is the key to the entire functional safety project, it is important to spend a good amount of time on this part of the project. Being able to reuse proven methodologies and a validated V-Model for FPGAs provided by Altera can help during this phase of the project.

The clear definition and understanding of the planned system and the reuse of pre-qualified technology will lead to a successful project very quickly.

Altera's FSDP helps project managers and development teams meet the requirements for a safety project and save a significant amount of project planning and development time. It offers significant benefits for developing safety-relevant applications up to SIL 3 designs that conform to the latest IEC 61508:2010 standard.

Further Information

- TÜV-Qualified FPGAs for Functional Safety Designs:
www.altera.com/end-markets/industrial/functional-safety/ind-functional-safety.html
- White Paper: *Developing Functional Safety Systems with TÜV-Qualified FPGAs*:
www.altera.com/literature/wp/wp-01123-functional-safety.pdf
- White Paper: *A Validated Methodology for Designing Safe Industrial Systems on a Chip*
www.altera.com/literature/wp/wp-01168-safe-industrial-soc.pdf
- Altera Design Software:
www.altera.com/products/software/sfw-index.jsp
- *Quartus II Handbook Version 9.0*:
www.altera.com/literature/hb/qts/archives/quartusii_handbook_9.0.pdf
- *Quartus II Software Device Support Release Notes*:
www.altera.com/literature/rn/rn_qts_90sp2_dev_support.pdf
- ISO 9000 ff.:
www.iso.org/iso/iso_9000_essentials
- Altera Reliability Report:
www.altera.com/literature/rr/rr.pdf
- Functional Safety and IEC 61508
www.iec.ch/functionalsafety/

Acknowledgements

- Roland Rauch, Functional Safety Engineer, Engineering Office, Rauch
- Christoph Fritsch, Senior Manager Strategic Marketing, Industrial and Automotive Business Unit, Altera Corporation
- Jason Chiang, Senior Technical Marketing Manager, Industrial and Automotive Business Unit, Altera Corporation
- Adam Titley, Design Engineer MTS, Embedded Solutions, Altera Corporation

Document Revision History

Table 1 shows the revision history for this document.

Table 1. Document Revision History

Date	Version	Changes
November 2011	1.0	Initial release.