# 8 Reasons to Use FPGAs in IEC 61508 Functional Safety Applications

WP-01203-1.0 White Paper

FPGA, ASIC, and CPLD technologies play an important role in today's functional safety product development. Because FPGAs are increasingly replacing electronic components typically used for industrial applications, international standards like the IEC 61508 have to support these evolving technology trends if they want to keep their relevance. The inclusion of guidelines within the IEC 61508 gave FPGA vendors guidance on the requirements, gave assessors guidance how to certify FPGA-based designs, and also gave customers guidance how to use FPGAs within their safety applications. The following article will give developers eight simple reasons why FPGAs should be chosen in their IEC 61508 safety project versus standard microcontrollers or DSPs.

## Reason 1: Flexibility, FPGAs Provide Flexible Safety Solutions

Typically a customer already has a system in production and has a "new" requirement to make the successor product comply with a certain Safety Integrity Level (SIL.) Safety designs can be approached from two different directions: bolt-on safety option boards to the existing design or design your next-generation product from scratch.

- Using an option card increases the cost significantly and also needs to interface to the existing board in a flexible way, which presents challenges. Usually standard controllers can only solve this by replicating the first channel as well as by adding some arbitration logic.
- Creating the design from scratch will change the initial product significantly whilst still ensuring backwards compatibility in most cases. The concept of using "redundant channels" is often the industry standard answer to meet many safety requirements. While this may well be a viable approach, it may not be the most efficient solution as it requires duplication of channels. This duplication introduces an additional failure category—common cause failures—failures which are caused by common parts in both channels such as a common supply voltage or a common clock and so on.

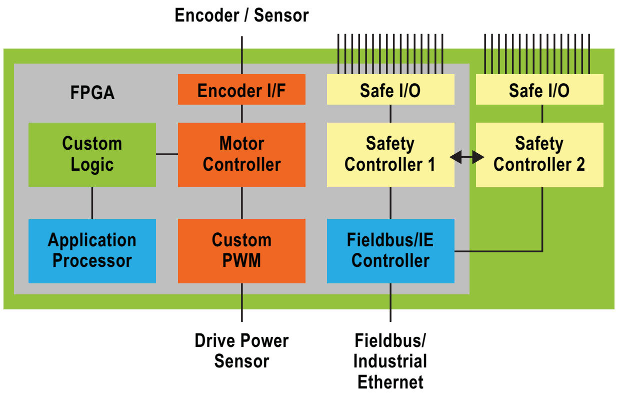
The flexibility of FPGAs provide you with many architectural and implementation options. For a new design you can take the dual-channel approach and add the arbiter functionality as implemented in many safety architectures available today. You also have the possibility to implement a more intelligent architecture including fault robust circuitry, which reduces the likelihood of common cause failures (since there is no second channel in this case). You could also interface to an existing non-safety product in a flexible way, using as many I/O interfaces or other functionality you may need to implement a "bolt-on" solution. You are not restricted to a given set of functionality defined within a standard device and have the freedom to implement the optimal level of functionality to achieve certification while minimizing cost.

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

# Reason 2: Integration

Figure 1 illustrates a typical industrial controller application. It integrates standard ("non-safe") and safety functions with very few board components using FPGA devices, such as the Altera® Cyclone® IV FPGA, and a soft processor core, such as the Nios® II processor. In this example, all three embedded controllers are Nios II soft-core processors, each with an individual custom peripheral set. With such a safety-focused architecture for a SIL3 certified application, you can reduce the total cost of ownership, design footprint, and power consumption while meeting the global requirements for functional safety.

**Figure 1. A Typical SIL3 Industrial "Safe" System**



The processors in the above example could also be implemented using the integrated dual-core ARM® Cortex™-A9 processors on Altera's SoC devices. Very high-performance digital signal processing (DSP) requirements can be met with custom logic implemented in the FPGA fabric, accelerating or offloading the application processor in the system.

# Reason 3: Product Range

The typical approach of microcontroller or DSP manufacturers is to develop a specific product range designed to meet the requirements of the IEC 61508. These products will have the necessary qualification, certification of a safety element out of context, and documentation needed to ease certification of your end solution. However, because those architectures are designed to match a multitude of applications, they can have their disadvantages too. The parts may be over-specified for the specific safety requirement needs, which makes them expensive. A second issue could be that they are missing functionality you might need for your specific implementation. The latter scenario typically exists if your safety requirements have not fallen under the initial requirement capture of the mainstream application for which the microcontroller or DSP has been designed. You either have to "swallow" the superset of functionality by accepting a more expensive solution where you only need a subset of functionality or you have to work around by adding additional logic outside of the microcontroller of choice.

FPGAs offer a different path to successful safety certification. Because the safety system developer is implementing the safety functionality to meet their specific needs, they can implement only the blocks that are essential to achieve certification for their specific end system. This results in a more efficient design, which only consumes the resources needed for a given SIL within the FPGA fabric. In addition, the designer can choose a device from the standard product range without being restricted to selecting from a limited set of safety-certified products as shown in Figure 2. Using standard products with high confidence in use also present the added advantage of significantly reducing the risk of obsolescence – a critical factor in total cost of ownership of any safety solution.

**Figure 2. 28 nm Portfolio Provides a Range of Safety-Qualified Products**

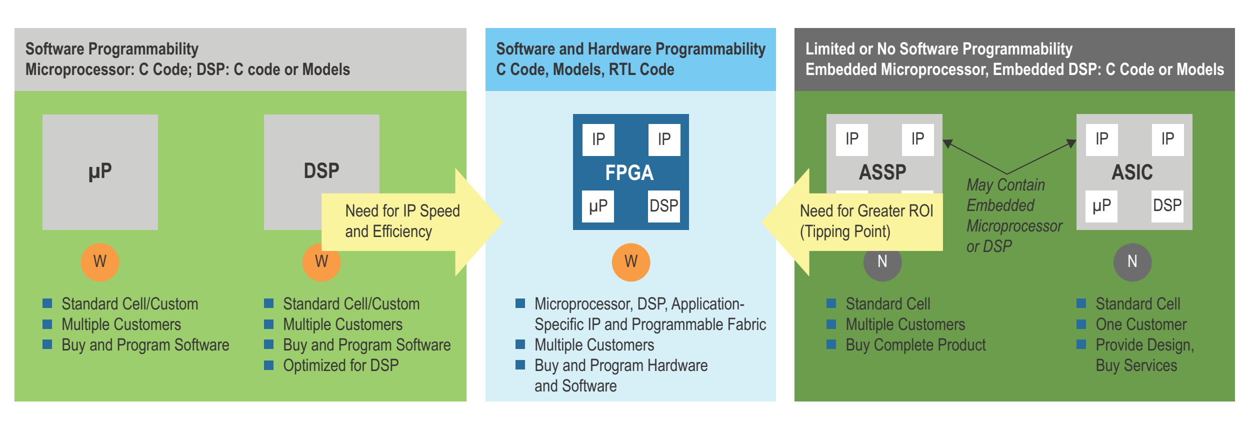
Cyclone Series
Arria Series
Stratix Series
TÜVRheinland
ZERTIFIKAT
CERTIFICATE
QUARTUS II
IP

## Reason 4: Performance

When it comes to safety, decisions on an event must be taken quickly to prevent harm or injury to human life. In many cases, fast calculation loop cycles and low latencies of safety-critical systems (hardware and software) are needed and exceed the performance needed in the system for “normal” operation mode. Advanced control algorithms need to be implemented in order to realize intelligent system control that exceed the “emergency stop” or “safe torque off” functionality of basic safety concepts. Examples of intelligent actions on a safety event would be switching down the operating speed of a machine or limit the movement of a robot to a restricted area, so it prevents harm to human life. Switching off a complete system is not always needed and in many cases not even possible. Considering an “emergency stop” of a complete production line with all the relevant interlinked systems cannot be achieved. Those systems cannot be stopped independently so you either stop the whole machine or production line or, as an alternative, bring it to a safe mode.

Besides system response in the case of a safety event, safety is also present in “normal” operation mode and also, in most cases, at system start-up. System start-up diagnostics usually do not demand a higher performance range since pre-operation tests will only lengthen the start-up time of a machine and are in most cases not time-critical. However, system diagnostic tests whilst in operation mode demand higher performance compared to the system without this functionality. Utilizing FPGAs will give you enough performance as well as flexibility to add those additional performance requirements. You could use hardened processor cores, soft-core processors, and dedicated logic to fulfill timing or latency requirements and pre-diagnostics, as well as runtime-diagnostics, without impacting the initial functionality of a system (see Figure 3).

**Figure 3. Applications from Both Sides Are Converging to FPGA-Based Technology**

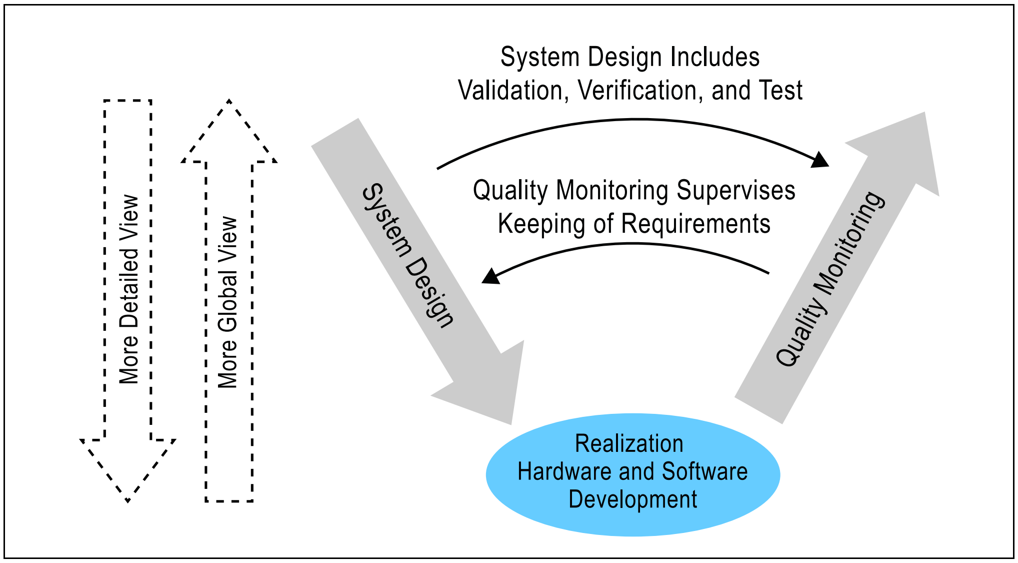

Software Programmability
Microprocessor: C Code; DSP: C code or Models
µP
DSP
W
W
Need for IP Speed and Efficiency
Standard Cell/Custom
Multiple Customers
Buy and Program Software
Standard Cell/Custom
Multiple Customers
Buy and Program Software
Optimized for DSP
Software and Hardware Programmability
C Code, Models, RTL Code
IP
IP
FPGA
µP
DSP
W
Microprocessor, DSP, Application-Specific IP and Programmable Fabric
Multiple Customers
Buy and Program Hardware and Software
Limited or No Software Programmability
Embedded Microprocessor, Embedded DSP: C Code or Models
IP
IP
ASSP
Need for Greater ROI (Tipping Point)
N
May Contain Embedded Microprocessor or DSP
IP
IP
ASIC
µP
DSP
N
Standard Cell
Multiple Customers
Buy Complete Product
Standard Cell
One Customer
Provide Design, Buy Services

# Reason 5: Tools and Methodology

When you design a safe product, you need to consider safety across all aspects of product development. Design challenges include adopting quality management standards, a "safe" design methodology, and safety concepts.

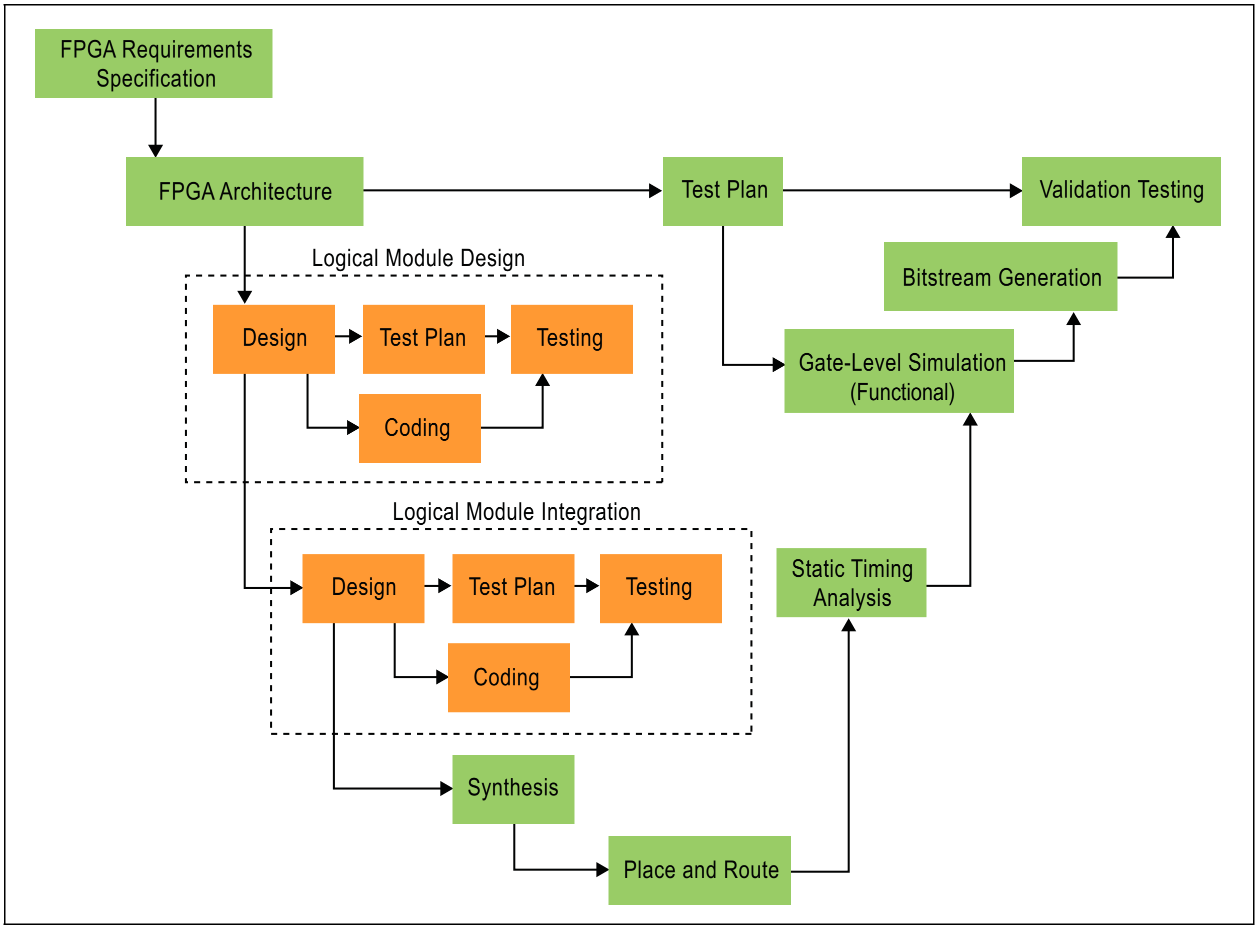
The V-Model is commonly used in a wide variety of projects (see Figure 4). It is a successor of the waterfall model, which defines a sequential design process. Compared to the waterfall model, the V-Model offers enhanced feedback and monitoring processes and separates the phases of product specification 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 4. Simplified V-Model**



Two main aspects have to be considered when following the V-Model. It has to follow the IEC 61508:2010 life cycle 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. Altera's TÜV-qualified Functional Safety Data Package (FSDP) contains a detailed document to guide the user in defining a process structure. It supplies a FPGA development V-Model that can be reused and to which existing FPGA development processes can be easily adapted to comply with the enhanced 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 significantly reduces the time the project team has to invest in a safety-centric FPGA development process, and if Altera's recommendation is adopted as is, then no time has to be invested in this critical project phase (see Figure 5).

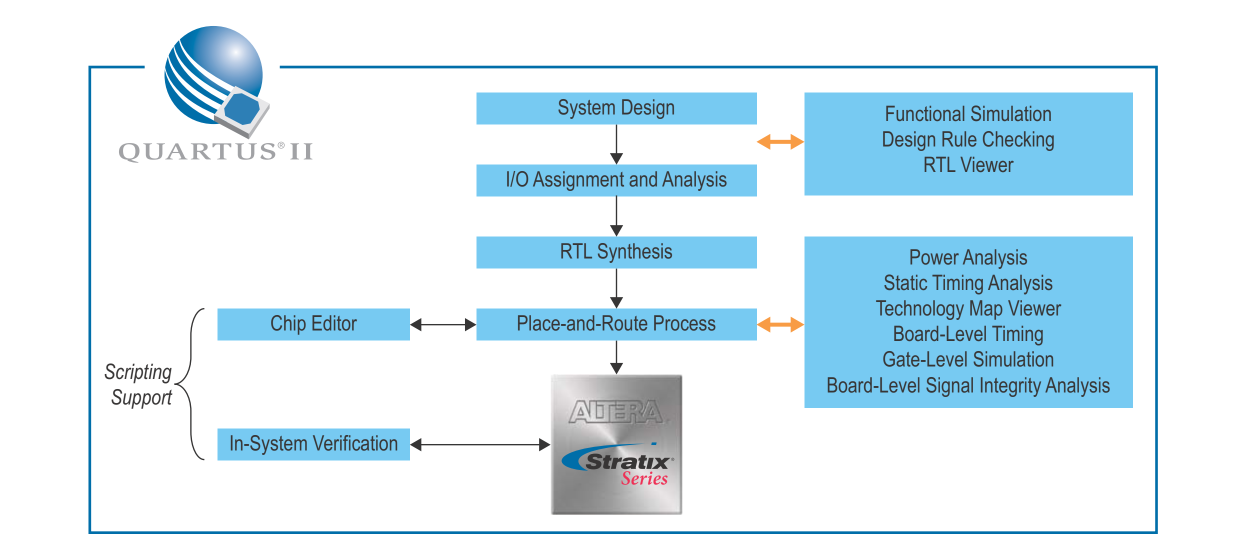
**Figure 5. Tool Flow**



The V-Flow and the documentation that comes along with it maps all steps in the design of a safe application for FPGAs to the IEC specification and its requirements. In addition, it explains which tools should be used for the specified design steps. Specific chapters in the IEC specification guide the users to follow the right development steps for the development of a safe application.

In addition, the pre-certified development toolchain for system design, synthesis, simulation, and analysis functions span the entire set of tools you need along the V-Flow for your safety design (see Figure 6).

**Figure 6. Certified Quartus II Environment Includes Necessary Steps for Functional Safety Development and Validation**



For example, the Altera Quartus® II software, shown in Figure 6, is a complete suite of tools for FPGA development. It contains all the necessary elements to take a user design into hardware—design entry, synthesis, place and route, simulation, static timing analysis, and so on. Since all these steps are available within the Quartus II design environment, users can be confident that they operate correctly together. The Quartus II design tool suite has been extensively reviewed by TUV Rheinland and qualified for use in the design of safety-related systems.

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 life cycle phases the necessary input and output documents are available. In addition, a set of life cycle 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.

# Reason 6: Certified Data

Having documentation available in the right format saves a significant amount of work for the documentation of the safety project. In the reliability report included in the FSDP, Altera provides an extensive analysis of the statistical information about the reliability of Altera FPGAs. All the necessary information to calculate failure-in-time (FIT) rates is part of the provided documentation, including a guideline that explains how to perform this calculation so that it can easily be presented to the assessor for certification. Since certification bodies have reviewed the provided data, the user has confidence that the right data is being used.

The safety data package also contains a silicon integration guide. References to relevant silicon data used in typical safety calculations and inclusion of information about specific IEC61508 compliance items. The basis for many of those figures is extensive quality and reliability work that was carried out on FPGA silicon products.

# Reason 7: Diagnostic IP

In addition to the implementation of the application, certain additional functionality must be added to the design. Basic parameter monitoring functions, such as clock and power, and complex functions, such as data monitors that ensure correct system operations by observing the output from a pulse-width modulation (PWM), may be required. It is often required to implement functions that automatically identify failures, and transition the system into a safe state. Basic functions include:

- Ensuring that memory content didn’t change due to external impact on the design
- Monitoring system clocks to ensure they are driving the design within the specified system parameters (or failed due to failure of external components)
- Power supplies are operational

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 a safety-qualified soft processor.

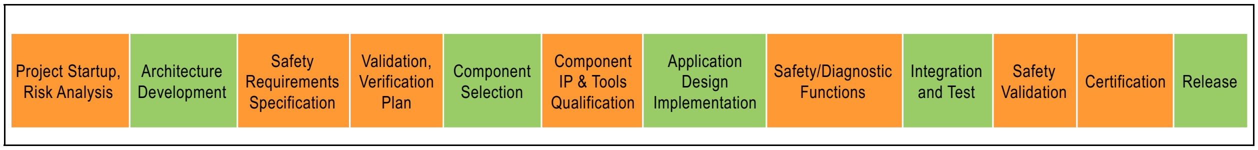
The most important aspect to consider for the reliability of a safety function is the fraction of failures, Safe Failure Fraction (SFF) that can be detected or do not lead into a dangerous state in relation to all possible failures. One of the best techniques to increase the safe failure fraction is to raise the 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.

IP cores that provide fundamental diagnostic functions would be, for example, a clock checker diagnostic IP core that could be used for monitoring the frequency and presence of a clock signal against a stable reference clock. Another example is diagnostic IP, which would be able to detect single-event upsets (SEU) in an FPGA. In addition, fault insertion in order to check those SEU upsets would be beneficial. Another example of a diagnostic IP would be a cyclic redundancy check (CRC) IP core, which could be used to calculate and check CRC values across a communication link.

On top of that, designers could even utilize a separate small softcore processor that would be dedicated to exclusively run software algorithms to perform diagnostic functions on memory, registers, and other parts of the system.

If the design is developed with functional safety as part of the product requirements, the designer is required to add additional phases to the project, as shown in orange in Figure 7. To design a safe application with the goal to achieve functional safety certification, such as IEC 61508, the project complexity increases significantly to provide a clear and transparent project structure that matches the standard.

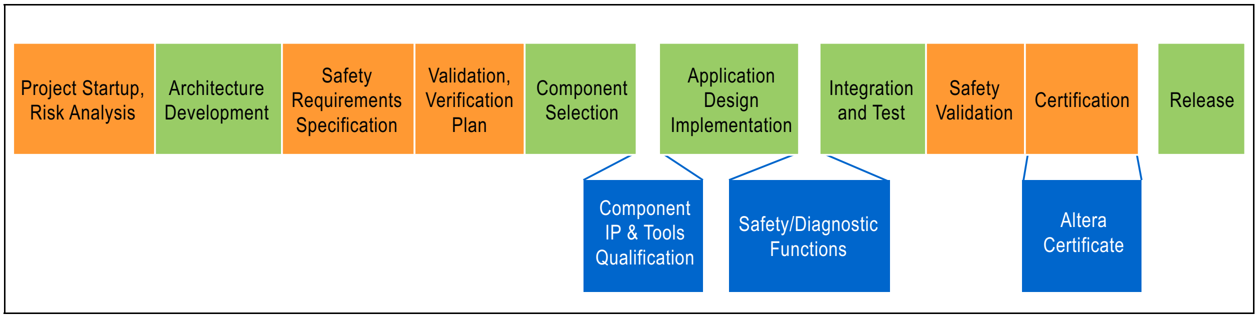
**Figure 7. Project Life Cycle Steps According to IEC 61508 Standard**


Project Startup, Risk Analysis
Architecture Development
Safety Requirements Specification
Validation, Verification Plan
Component Selection
Component IP & Tools Qualification
Application Design Implementation
Safety/Diagnostic Functions
Integration and Test
Safety Validation
Certification
Release

In the project start-up and risk analysis phase, the scope for safety in the project is identified based on the general requirements for the application. The desired and achievable SIL for the application is determined, formulated, and documented for the implementation stages, and acts as the basis for the risk analysis and assessment. The risk analysis provides the foundation for measures that must be taken later in the process to develop a safe application. It represents the understanding of the product's boundaries and is closely linked to the products scope definition. It provides the base for the required SIL, a detailed definition of the safety function, and the framework of the product documentation. This must happen on the component as well as on the system level.

There are certain steps where semiconductor vendors like Altera can help with the process and reduce the effort for the development of safe applications, as shown in Figure 8. For example, having immediate access to semiconductor data, IP, development flows, and design tools that are already qualified for functional safety can provide a significant acceleration of the overall product development process, as shown in the diagram below

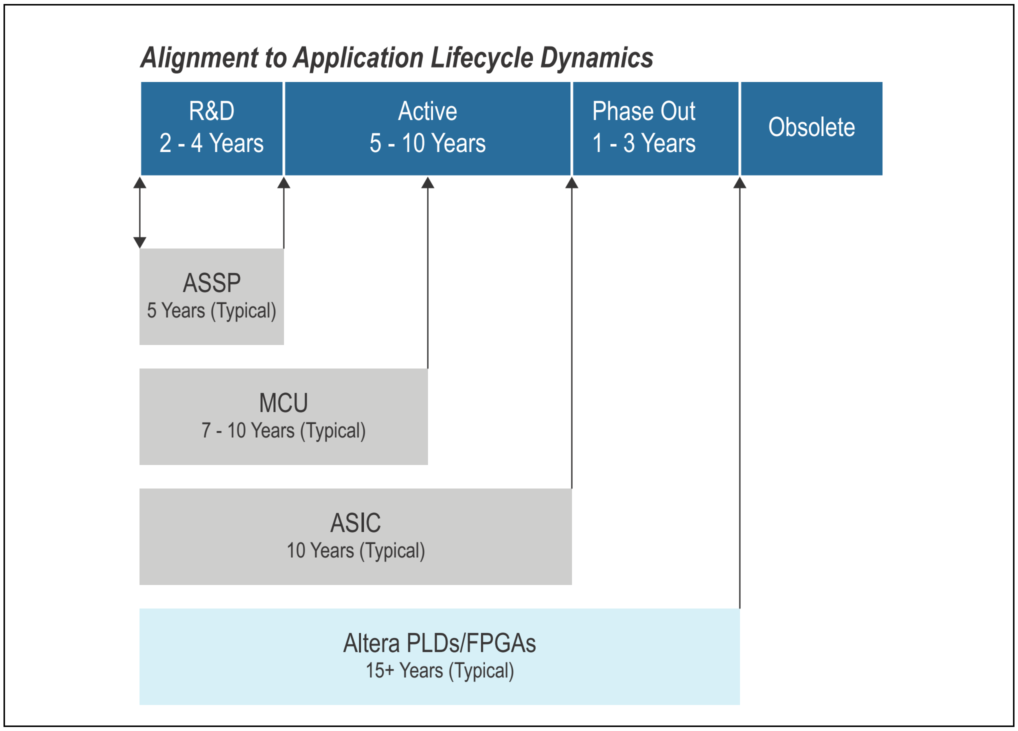
**Figure 8. Design Steps with Prequalified Safety Steps**


Project Startup, Risk Analysis
Architecture Development
Safety Requirements Specification
Validation, Verification Plan
Component Selection
Application Design Implementation
Integration and Test
Safety Validation
Certification
Release
Component IP & Tools Qualification
Safety/Diagnostic Functions
Altera Certificate

# Reason 8: Proven in Use, Reduced Obsolescence Risk

Coming back to the strategy, how do you approach functional safety product range within the company's product life cycle? The ideal scenario is to use the same product portfolio as you are using in non safety applications. By doing this, many essential requirements will be addressed. First, when using standard products, it assures that those products have been used many times in a wide variety of applications and have reached a market and product penetration, earning the "proven product" status. A second requirement for functional safety designs is that the parts have long-term availability with a low risk of being "end of lifed." Again, while allowing that all standard parts can be utilized for functional safety applications, the long-term availability is not only dependant on the number of customers using this specific product in a certain market segment in a dedicated safety application, but also depends on the number of customers using this part in any product and design, regardless of whether it is for a specific market, or if it is a safety or non-safety application. FPGAs have a proven track record to exceed the typical lifetime of ASICs, ASSPs as well as standard microcontrollers and DSPs by years, as shown in Figure 9.

**Figure 9. Typical Lifetime of Semiconductor Products**



# Conclusion

International legislation as well as the need for improved productivity is driving both the complexity and quantity of safety devices in almost all segments of industrial automation. As standards change and increase, standard microcontroller- and ASIC-based safety concepts cannot deliver the flexibility and simplification needed for complex safety systems to meet cost targets and get the number of design variations under control.

In contrast, FPGAs allow designers to implement safety designs in an extremely flexible and scalable fashion. The TÜV-qualified safety data package for Altera's tools, IP, and semiconductor devices simplifies and shortens the overall qualification and certification process. Finally, the long product lifetimes of FPGAs as well as the strong support for migration of application-specific functions and firmware reduce functional obsolescence risk for the safety design.

FPGA-based design methodology, facilitated by TÜV-qualified safety manuals, is changing the paradigm for safety designs and are greatly reducing development effort, system complexity, and time to market. This allows FPGA users to design their own customized safety systems and controllers and provides a significant competitive advantage over traditional microcontroller or ASIC-based designs.

## Further Information

- Solution sheet: *Qualified Functional Safety Data Package*
  www.altera.com/literature/po/ss-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
- White paper: *Reducing Steps to Achieve Safety Certification*
  www.altera.com/literature/wp/wp-01174-safety-certification.pdf

## Acknowledgements

- Wolfgang Kattermann, Market Development Manager – Industrial

## Document Revision History

Table 1 lists the revision history for this document.

**Table 1. Document Revision History**

| Date | Version | Changes |
|---|---|---|
| September 2013 | 1.0 | Initial release. |