

Industrial automation applications across all segments—from factory, machine, and process automation to energy generation, distribution, and transportation—require an increasing amount of safety-enabled equipment. This white paper explores a case study on industrial system on a chip (SoC)—a drive on a chip—to explain how engineers can save up to 18 months of design time in achieving product certification according to IEC 61508. Having prequalified devices such as Altera® FPGAs means the designer benefits from the flexibility of FPGAs without having to worry about whether these FPGAs can be easily used for safety applications.

Altera's Safety Integrity Level 3 (SIL3) Functional Safety Data Package, which includes a certificate for Altera tools, IP, and device data from TÜV Rheinland, shortens and simplifies development of safe applications according to IEC 61508 while efficiently addressing the needs for low-cost and highly integrated embedded systems. The prequalified design flow and tools, as well as prequalified embedded system and diagnostic intellectual property (IP), reduce certification risks in safety-critical industrial applications, such as servo and inverter drives, safe I/O and PLCs, and automation controllers.

Introduction

Industrial automation, transportation, smart grid, and many other industries require machinery and products to be safe and certified for functional safety. Flexibility and the incremental cost for safety can be a significant decision factor when developing machinery that must be compliant to worldwide safety standards. If companies plan to ship their products into countries that require a certificate to prove compliance with the local safety regulations—such as the new machine builder directive (2006/42/EG), which represents a must-meet requirement for products exported to Europe—then they must adopt a safety-oriented approach throughout the whole design process to be competitive. Another reason to implement safety in applications comes from the factory operator who requires safe operation of machinery to improve productivity, such as maintenance work that can be executed while part of the machine is still in operation, or significantly shortened ramp-down and ramp-up times.

Safety imposes new processes to the development of machinery as well as an increase in complexity for the electronics in these applications. The increased complexity typically results in a significantly higher hardware cost. The more complex design and development processes increase the time to market for a new application, as well.



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.



When a company decides to develop a safe product, it must consider safety as a core system functionality. Historically, safety has been added to the system by additional functionality such as redundant controller or communication modules combined with circuitry to monitor the system. These added-on safety components, introduced as an afterthought into the system concepts, incur significantly higher costs and are less flexible and scalable than designing a safe application, optimized for safety and cost competitiveness, right from the start.

Design challenges for developing a safe application include:

- Adopting a “safe” design methodology and safety concepts
- Accounting for additional project effort (time and technology), resulting in longer time to market and higher cost of ownership
- Project management, gathering of data for all system components, and documenting the project according to the needs of the safety specification

This white paper will show how a project can be successful in both meeting the objectives of providing a safety solution and meeting the cost and time-to-market targets. The key to success is the adoption of validated design methodologies, qualified tools and devices as part of the product, and considering safety right from the start of the product development.

Designing a Safe Drive

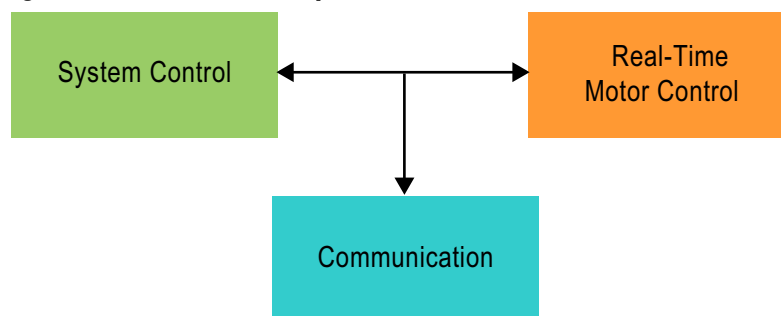
Without having safety in mind, the typical design steps to develop an application are as shown in [Figure 1](#).

Figure 1. Typical Design Steps



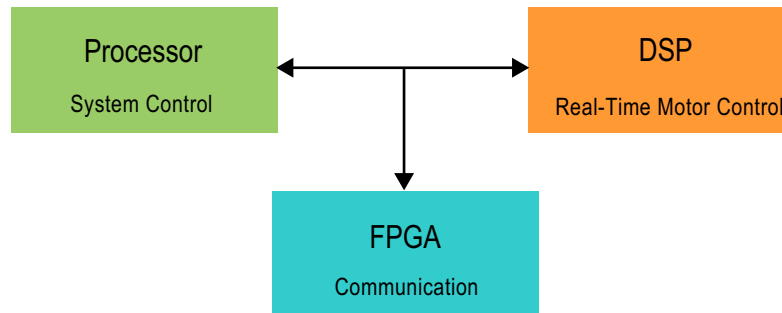
Based on market requirements and the companies’ vision to be successful in the market, the first step is to develop the architecture of the product, as shown in [Figure 2](#). For a typical motor control application, such as a drive, the partitioning step separates the system into system control, communication, and real-time motor control functions. For example, the architect selects a software implementation for the control part and for the real-time portion of the system, and decides to use a hardware/software approach for the communications portion to support real-time Industrial Ethernet communication protocols.

Figure 2. Architecture Development



The next step is the component selection (Figure 3). The decision may lead to an implementation where the control software runs on a standard application processor, the real-time motor control portion will get implemented on a digital signal processing (DSP), and the communication within the system will be realized with an FPGA-based approach. An FPGA allows flexibility in the system to realize various different Industrial Ethernet standards like Ethernet/IP, EtherCat, PROFINET, or SERCOS III in the same device interchangeably. This flexibility for the communication part of the architecture allows that a standard hardware platform can be customized for the specific protocol needs of the end customer very easily.

Figure 3. Component Selection



After the partition has been decided and the components are selected, the design teams will work on the development of their part of the application independently. Then, they will integrate the components to a full system, test the system functionality, and release the product.

Adding Safety

If the design is developed with functional safety as part of the product requirements, it is required to add additional phases to the project, as shown in yellow in Figure 4. 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. The IEC 61508 specification covers the whole safety life cycle, from developing the application to decommissioning. This white paper focuses on the first phases of the safety life cycle, from project start up to achieving certification. Following the procedures and processes in the safety standards is required to simplify the communication with the assessor to ensure that objectives, concepts, procedures, and solutions are understood clearly and meet the requirements for safety.

Figure 4. Design Steps with Safety Steps Added



Project Startup and Risk Analysis

In the project startup 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.

Architecture Development

Following this step, the architecture for the application is developed to meet the functional requirements, as well as the safety requirements. The safety requirements are refined and the specific functions to be realized during operation and maintenance work are documented, together with the identification of strategies that must be followed to validate that the safety measures meet the requirements.

Safety Requirements Specification

For a safe drive, the scope might include several aspects such as identifying whether the drive parameters are in the allowed range, or if a safety I/O signals a critical event. The most basic safety feature for drives is "safe torque off" (STO), in which the motor is disconnected from the power supply in a safe way. The procedure might also include communicating to the overall automation system that a safety event occurred and certain measures must be taken within a certain time window, such as a sequential shut down of a whole application following a series of steps over a predetermined period of time.

Validation, Verification Plan

The development of the validation plan might include methods of controlled failure insertion to test the system and additional monitors that observe the system to compare the current parameter to a range of predetermined, allowed values.

Component Selection, and Component, IP, and Tools Qualification

The component selection step takes place in a typical project, but with the additional need to ensure that the components and IP functions allocated and selected are suitable for use in a safe application. For the selection, it is important to consider the residual error probability, which is used as a basis to calculate the total failure probability (FIT) of a product and finally the achievable SIL. Partially, this can be achieved through gathering the required device and design tool data and information to ensure that products are used broadly by a wide range of users such that they are sufficiently free of systematic errors or proven in use (for IP, for example). It can also be achieved through access to reports that provide error rates and reliability information for semiconductor products like processors or FPGAs. However, it is often difficult to get access to reliability reports for components and semiconductor products that provide the necessary information, especially for related design tools and IP used for the application.

Application Design Implementation

Complex system functions like communication protocols, memory interface IP used in the FPGA or processor IP embedded in the FPGA, such as the Altera Nios® II embedded processor—typically used to run the software stack for industrial Ethernet protocols in drive applications—need to be analyzed, tested, and qualified for safety applications as well.

Safety/Diagnostic Functions

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), are required. It is 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 or monitoring system clocks to ensure they are driving the design within the specified system parameters (or failed due to failure of external components) and that power supplies are operational.

Integration and Test

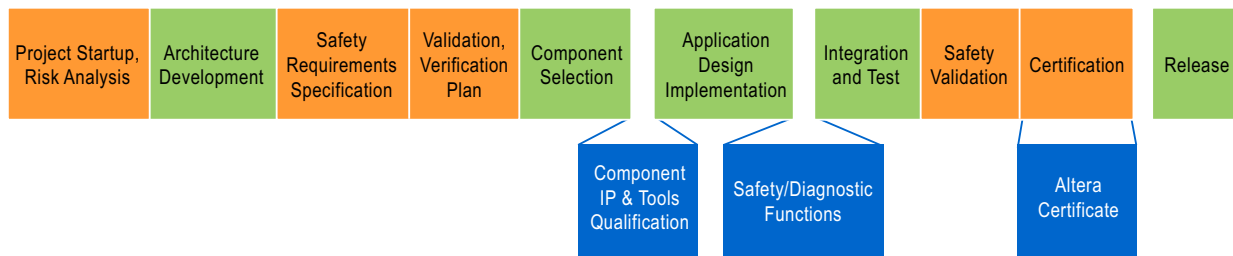
After development of the individual components, they are integrated to a safe drive implementation and tested for delivering the expected system functionality as well as providing the safety functionality that has been specified. The safety validation must ensure that the desired safety features are in effect and remain in effect during operation, for example to ensure that an external impact on the design has no negative effect on the safety function such as accidentally disabling it without being noticed by the system.

Safety Validation, Certification, and Release

Throughout the entire process, close cooperation with the assessor is required to ensure that the measures taken during the development process are reasonable and provide the right level of safe functionality. Finally, the assessor certifies the product for functional safety and it can be released into the market.

Adding Prequalified Safety

There are certain steps where semiconductor vendors like Altera can help with the process and reduce the effort for the development of safe applications. 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 [Figure 5](#).

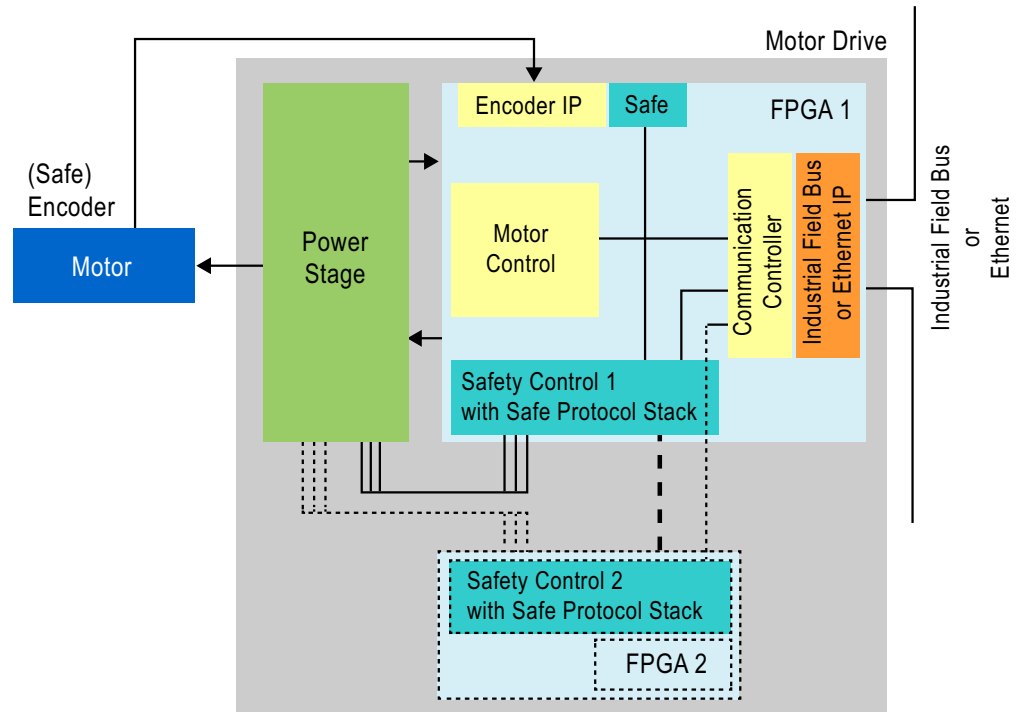
Figure 5. Design Steps with Prequalified Safety Steps

Altera invested almost two years to achieve qualification for their products. The required test and usage data for IP and design tools and device reliability data are summarized and formatted in a way that it can be presented for certification for functional safety. A TÜV-approved design methodology (V-Flow) was developed to address the specific needs of FPGA designs. Essential diagnostic functions were designed as FPGA IP and are provided as part of the functional safety package. Users of this functional safety package benefit from Altera's up-front investment with TÜV and can save a similar amount of time from their own project schedules.

Example of a Safe Drive

This example of a drive with a safe I/O uses Altera's qualified FPGA design tools, Quartus® II software version 9.0 SP2, and a suggested design methodology for the implementation of the application. In addition, a dual-FPGA implementation for the application, as shown in Figure 6, was used instead of external processors and DSP. The application is partitioned onto several Nios II soft processor cores. The first Nios II soft processor provides support for the communication stacks, the second handles the control of the system and the third Nios II processor is integrated into the motor control block. The motor control algorithm is partitioned so that its software portion runs on a Nios II processor and is accelerated by hardware blocks specifically developed for this applicator to accelerate the motor control loop. An external safety controller provides the redundancy required for a SIL3 application.

Figure 6. Dual-FPGA Implementation for a Safe Drive



This solution enables combining the safe controller with the field bus controller in a single FPGA, and uses Altera's SOPC Builder system integration tool to integrate the Nios II soft processors with the other IP blocks for communication, the encoder interfaces, and memory interfaces.

Safety in the Drive-on-a-Chip

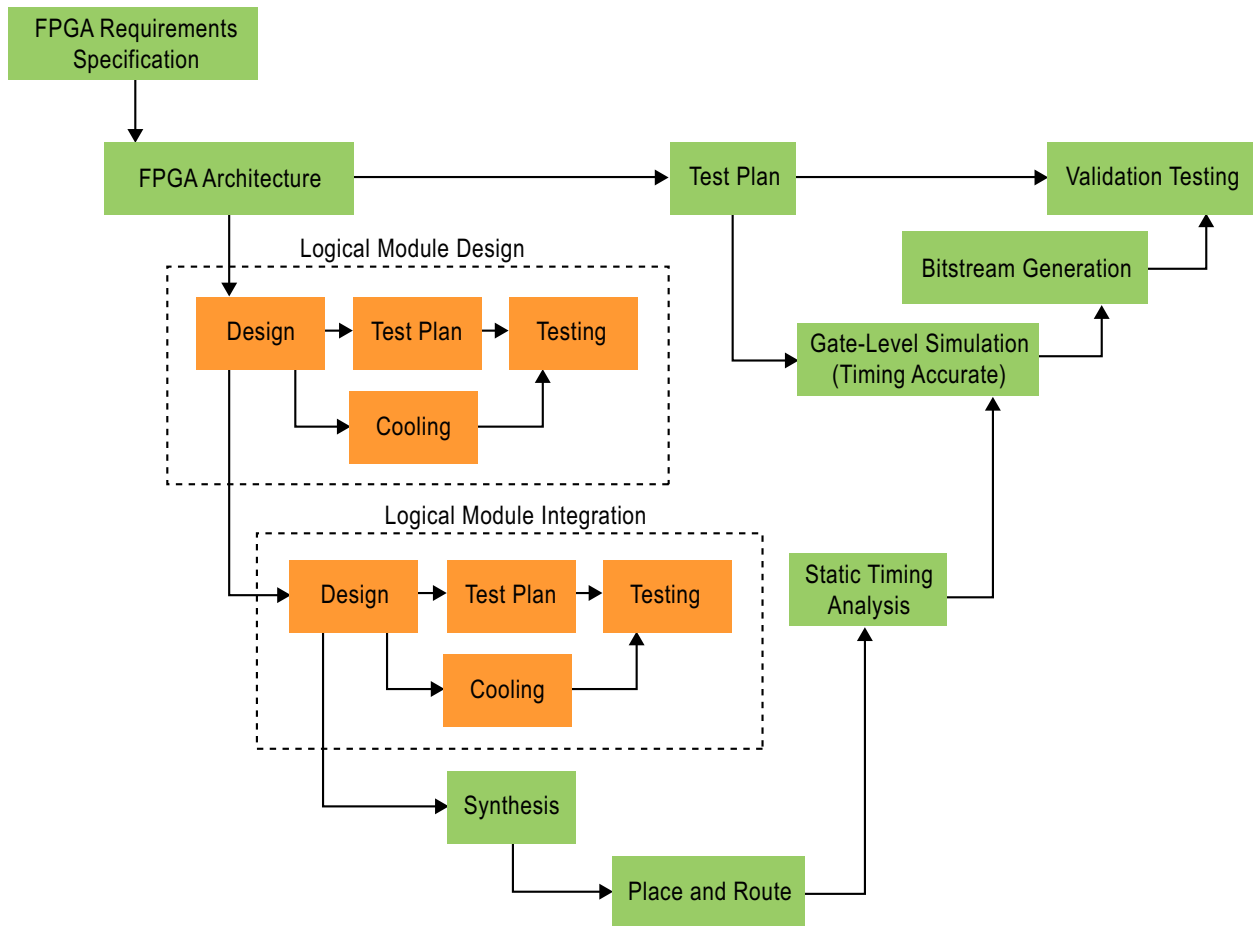
For low-level monitoring of critical but common diagnostic tasks in the FPGA, this example uses safety-qualified diagnostic IP blocks provided by Altera. These diagnostic IPs, designed to the IEC 61508 specification, perform common diagnostic functions such as the following:

- Cyclic redundancy check (CRC) calculation—This calculation is useful in many systems and is particularly useful for fieldbus applications.
- Derived clock checking—This core looks at the presence and frequency of clocks in the system.
- SEU check controller—This block works with the built-in soft error checking hardware in the device to monitor changes brought about by so-called soft errors.

Since the implementation of these hardware IP cores is in the FPGA logic area, the system processor is relieved of these tasks.

The design implementation follows the recommendations provided by Altera. In the area of qualified methods, Altera took the IEC spec and analyzed the FPGA design methods and related clauses. From this analysis, Altera produced a tool flow document. The central theme of this tool flow is the description of an Altera-developed FPGA V-Flow, shown in [Figure 7](#).

Figure 7. Tool Flow



The V-Flow and the documentation that comes along with it maps all steps in the design of a safe application for Altera FPGAs to the IEC specification and its requirements. In addition, it explains which Altera tools are used for the specified design steps. Specific chapters in the IEC specification are discussed and an explanation is provided to guide the Altera user to follow the right development steps for the development of a safe application.

Altera provides the industry's first TÜV-qualified Functional Safety Data Package that covers qualified development tools, qualified IP, and qualified silicon data for devices under a specific tool flow (e.g., Quartus II software version 9.0 SP2). The documentation and data that the assessor needs for certification are included and provided in a format that matches precisely the IEC 61508 specification format so they can easily be processed by the assessor. Having this 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 Functional Safety Data Package, 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.

Conclusion

By reusing a system concept for a drive that followed a pre-approved 2-chip implementation and following a qualified design methodology, a qualified design flow, tools and IP, a typical application development can be significantly accelerated. The certification is accelerated as reliability data for the components is immediately available and provided in a format that can be easily integrated into the overall documentation for the safety qualification. Designers can take advantage of flexible design integration using FPGAs for both safety and system design. As the safety aspect is considered as a key requirement for the application, it is integrated into the overall concept and can be realized by meeting cost and time-to-market targets.

Further Information

- TÜV-Qualified FPGAs for Functional Safety Designs:
www.altera.com/end-markets/industrial/functional-safety/ind-functional-safety.html

Acknowledgements

- Christoph Fritsch, Strategic Marketing, Industrial and Automotive Business Unit, Altera Corporation

Document Revision History

Table 1 shows the revision history for this document.

Table 1. Document Revision History

Date	Version	Changes
September 2011	1.0	Initial release.