

Developing Functional Safety Systems with TÜV-Qualified FPGAs

This white paper discusses how market trends, the need for increased productivity, and new legislation have accelerated the use of safety systems in industrial machinery. This TÜV-qualified FPGA design methodology is changing the paradigms of safety designs and will greatly reduce development effort, system complexity, and time to market. This allows FPGA users to design their own customized safety controllers and provides a significant competitive advantage over traditional microcontroller or ASIC-based designs.

Introduction

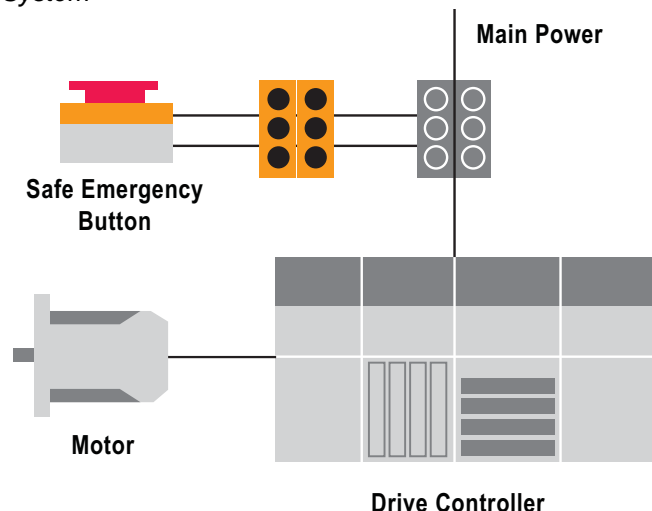
The basic motivation of deploying functional safety systems is to ensure safe operation as well as safe behavior in cases of failure. Examples of functional safety systems include train brakes, proximity sensors for hazardous areas around machines such as fast-moving robots, and distributed control systems in process automation equipment such as those used in petrochemical plants.

The International Electrotechnical Commission’s standard, IEC 61508: “Functional safety of electrical/electronic/programmable electronic safety-related systems,” is understood as the standard for designing safety systems for electrical, electronic, and programmable electronic (E/E/PE) equipment. This standard was developed in the mid-1980s and has been revised several times to cover the technical advances in various industries. In addition, derivative standards have been developed for specific markets and applications that prescribe the particular requirements on functional safety systems in these industry applications. Example applications include process automation (IEC 61511), machine automation (IEC 62061), transportation (railway EN 50128), medical (IEC 62304), automotive (ISO 26262), power generation, distribution, and transportation.

Local Safety Systems

In the past, functional safety was ensured by dedicated safety installations. For example, safe-stop buttons and mechanical switches were used to indicate an open door, guarding against the potentially unsafe access of a person to a hazardous area, such as a bottling machine or metal press. As shown in [Figure 1](#), such installations were connected to a power cut-off mechanism to stop the machine in the case of an unsafe circumstance. These types of safety critical devices rely on the machine being fail-safe and human operators to supervise the machine and hit the stop button in an unsafe situation. Because this type of implementation is only applied to a single discrete part of a machine, such as the main motor drive, it is often known as a “local” safety system. In such systems, only a small percentage of automation devices are actually secured by a safety measure.

Figure 1. Local Safety System



In recent years, market demands for higher productivity have led to the development of much larger and more complex machines that require less human supervision. This results in much higher levels of potential damage to both machine and humans, should there be a failure. This increased risk combined with changes to international safety legislation have accelerated the demand for the use of functional safety in machinery.

Increasing Productivity of Manufacturing Processes

In order to deliver higher and more efficient output, manufacturing processes are becoming ever more complex, with machine size, speed, and performance constantly growing. Larger, faster, and more complex machines are inherently more dangerous, so relying on a simple power off to protect operators, the machine itself, and its surroundings is no longer good enough. In fact, suddenly powering down a large, complex, high-speed machine can be more dangerous than the initial triggering condition. In addition, a sudden power off can also result in significant commercial repercussions. For example, an uncontrolled stop can damage the machine and the product it is processing, as well as the cost of the delay caused by the time taken to repair the machine, restart the production, and dispose of any damaged product.

Imagine a machine that prints newspapers. In order to be efficient, these machines process paper at very high speeds. The sheer speed of the machine poses a hazard, thus it is important to protect operators from the moving parts of this machine when it is operating. Should a person enter or be exposed to a hazardous zone of the printing machine, a safety sensor will detect the dangerous condition and send the machine into a safe state. In a small machine, where everything works from one large motor, a power cut-off to the main drive (safe stop) and a passive brake stops the machine as quickly as possible. However, in the case of heavy machinery, this may not be quick enough and resetting the production will take a significant amount of time and effort. Hundreds of meters of half-printed newspaper must be removed from the machine before starting the printing process again. There may be additional issues caused by the sudden power-down, such as tearing of the paper, jamming of the machine, and resetting of ink feeds and roller alignment. So while a safe stop delivers a minimally acceptable level of safety, it causes a significant commercial impact.

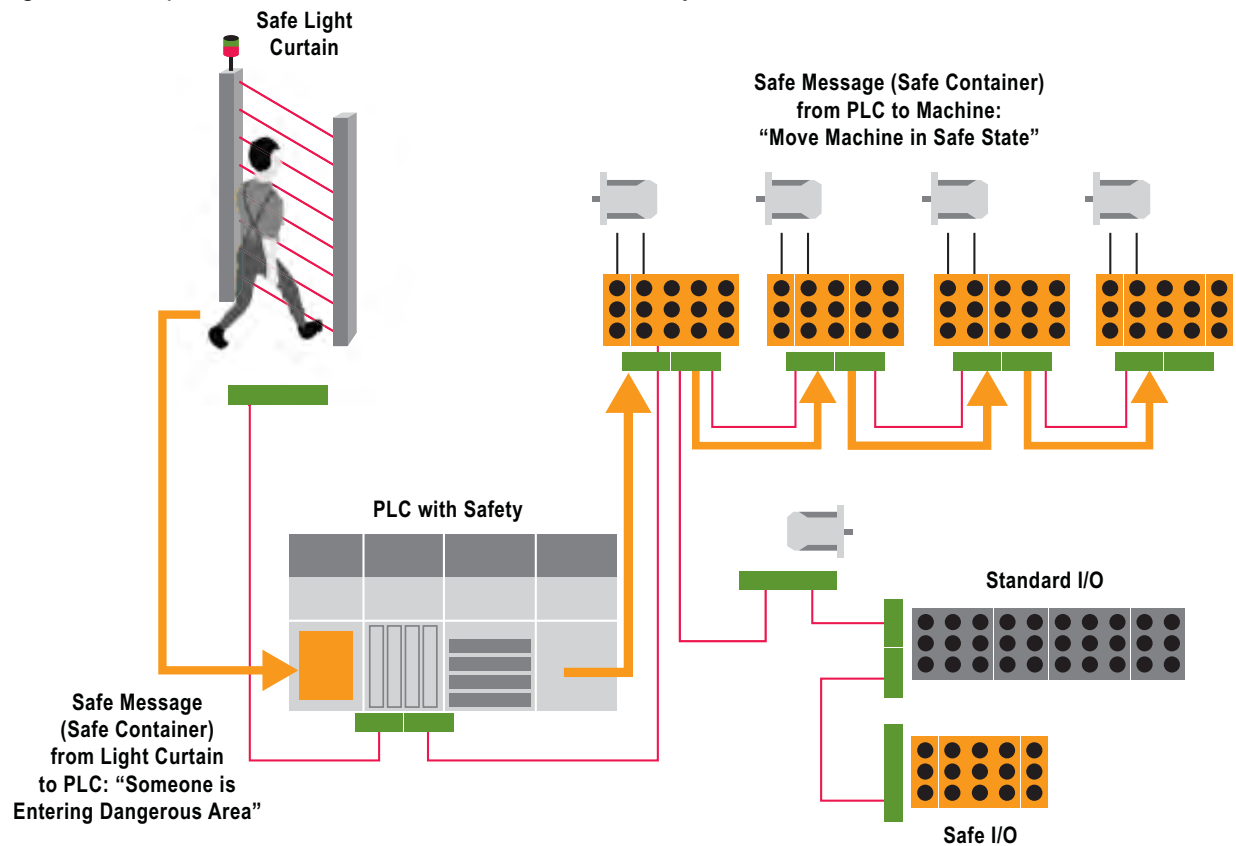
Modern systems are much larger and more flexible, which dictates the use of many networked and highly coordinated drives rather than everything being geared off one motor. Having multiple drives means that a simple power-off is not sufficient to put the machine into a safe state efficiently. Instead, safety systems are distributed throughout the machine, with each drive responsible for its own safe shutdown while communicating with the other parts of the machine to follow the same process. The safety critical drives and sensors are networked and connected to a safety controller that senses the dangerous situation and initiates a coordinated shutdown of the machine to a safe state. This controlled shutdown delivers rapid protection against the unsafe condition while reducing the impact on the rest of the machine and the product.

For example, the printing press can stop the part of the line with the issue, cleanly shut down all printing functions, and deal with the paper in the machine in an appropriate manner (such as immediately cutting the paper and dumping the spoiled material into a bin). This delivers quicker, safer stops, faster recovery times, and less damage to product in the machine.

This networked approach, illustrated in [Figure 2](#), is driving two major trends in industrial markets:

- The number of safety-critical devices per machine is increasing by orders of magnitude. Safety monitoring must handle a larger number of nodes spread over the entire system and respond to safety issues in a controlled manner that minimizes the safety risk and the commercial impact of the shutdown.
- A fast communication media is needed to connect the safety devices in order to execute safety operations and coordinate the safety process between the safety devices over the entire machine. Due to the requirements for increasing speed and low costs, this bus communication media is migrating from fieldbuses to Industrial Ethernet standards.

Figure 2. Complex Fieldbus-Networked Coordinated Safety Machine



New International Safety Legislation for Machinery

In recent years, regulatory bodies have placed an increasing focus on safety and, as a consequence, are now demanding higher levels of safety in industrial machines and environments. The motivation is not only to protect people from being injured by machines. By following safety standards, plant owners, machine builders, and component manufacturers can rest assured that they are not likely to be sued in a court of law (except in cases of gross negligence). This legal coverage is provided by the demonstration of the safe design of a system and subsequent safety approval from trusted certification bodies, such as TÜV. These approvals indemnify machine builders and plant owners from legal action in specific failure cases.

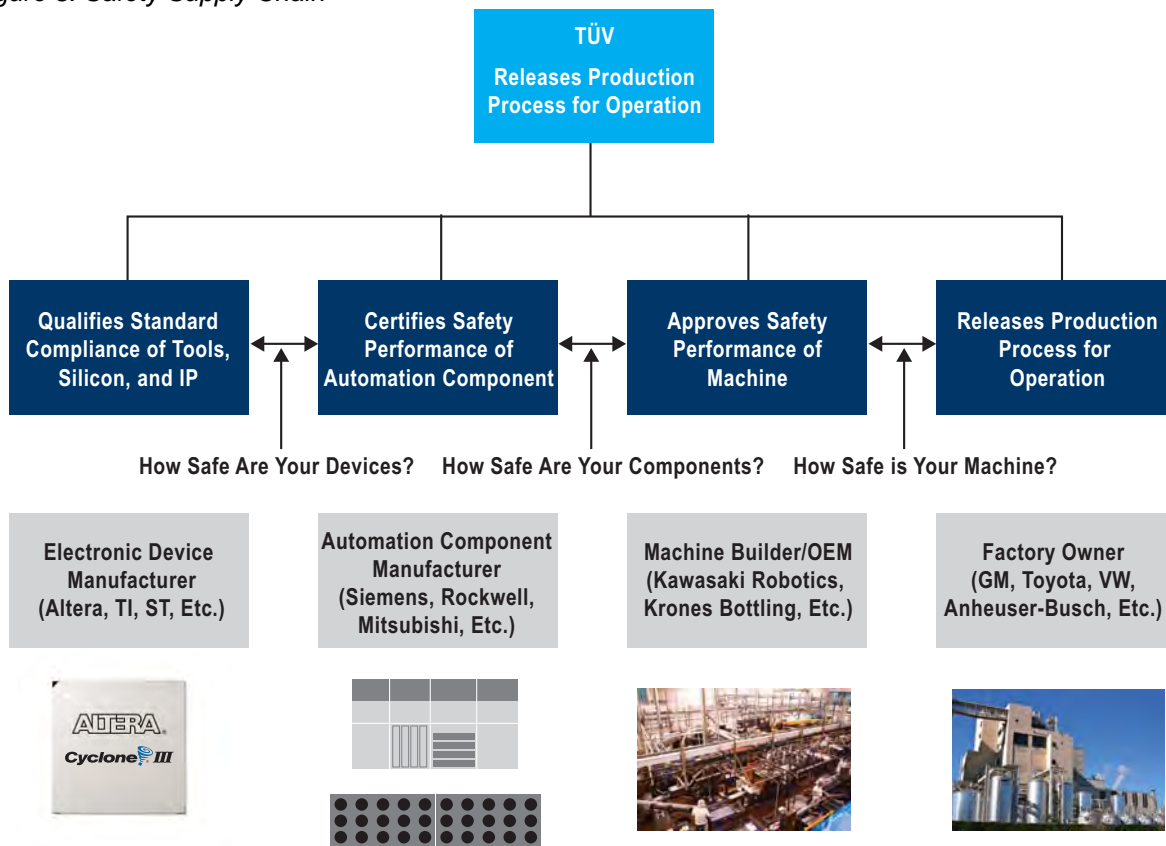
Old safety standards, such as European Standard EN 954-1, apply a deterministic failure evaluation of machinery, which involves evaluating a potential failure or dangerous situation by measuring how well the machine prevents persons from being injured. New machine standards add an evaluation of the quantitative and qualitative probability of failure of certain components of a machine. This requires a calculation of probability for specific dangerous scenarios to be included in the safety concept and evaluation of the machine.

Europe is already adopting this new methodology, and translated IEC 61508 into the new European Machinery Directive 2006/42/EG. All machines shipping to factories and plants in Europe were supposed to comply with this directive after December 29, 2009. However, this date has been pushed out to 2011, because most of machine builders were not yet prepared to deliver according to these guidelines. Japan, the United States, and Canada currently are preparing similar directives.

Functional Safety Certification

Machine builders and plant owners must follow internationally accepted safety standards. However, state-of-the-art machine and plant designs first need approval from certification bodies or trade associations that testify that these designs comply with their appropriate safety standards and legislations. To provide the certification body with a complete picture of the machine or plant with respect to safety, the owners or operators must have all available information and documentation for the components used to build the machine. Since the machine builders typically source automation components, such as sensors, drives, and PLCs, from automation component manufacturers, these components consequently must also be designed to the applicable standards, as demonstrated in Figure 3. This also means that the component suppliers must provide the relevant safety documentation (safety manuals) to the machine builders.

Figure 3. Safety Supply Chain



Automation component manufacturers are particularly affected when designing functional safety devices, because these devices are considered to be complex electrical and electronic devices. For these components, such as software, hardware, tools, mechanical parts, etc., safety has implications for the complete system design and across all stages of life, from concept to inception to decommissioning. Safety can only be assured by looking at all aspects of a system, including both hardware and software, through the “eyes” of the safety standards. As an example, software alone cannot provide safety assurance, as its correct operation is dependent on the system hardware. Similarly, hardware alone cannot satisfy the safety requirements. Therefore, an integrated approach to safety is essential.

In addition, functional safety designs are not guaranteed simply by a good design. The correct or incorrect behavior of any system is influenced by many factors, including failure rates, production, programming, and use.

The functional safety consideration of a system therefore covers all aspects of components, both software and hardware, that have high integrity, self-test mechanisms, and a fail-safe state. In the end, the designers will reach a

compound or average certainty level of failure probability (probability of a failure per hour of operation that introduces “danger”) for a design, which is categorized in the following safety integrity level (SIL) classes:

- SIL4: $\geq 10^9$ up to $<10^8$ (1 failure in a minimum of 110,000 years)
- SIL3: $\geq 10^8$ up to $<10^7$ (1 failure in a minimum of 11,000 years)
- SIL2: $\geq 10^7$ up to $<10^6$ (1 failure in a minimum of 1,100 years)
- SIL1: $\geq 10^6$ up to $<3 \times 10^6$ (1 failure in a minimum of 380 years)
- SIL1: $\geq 10^6$ up to $<10^5$ (1 failure in a minimum of 110 years)

It is assumed that SIL3 will become the standard requested by industrial machine builders. Consequently, system architects as well as hardware and software engineers will prove the integrity of a system, and will implement the system’s self test and define the fail-safe states to comply with this safety integrity level.

High Integrity

To assess integrity of a safety-related system, several parameters must be considered during the conceptual work and the design of an electronic/electrical device:

- Failure rate of the hardware—Failure-in-time (FIT) rates
- Safety failure fraction—How much does a specific software or hardware failure contribute to the overall system failure rate?
- Diagnostic coverage—How, and how effectively, can an error, such as a failing phase-locked loop (PLL) or flipped memory bit, be detected?
- Test time—How frequent should a test to be performed in order to guarantee system integrity?
- Common cause factor—Are there single elements in the systems, such as the power supply, that could cause a total system failure should they fail?

Self Tests

It is important to implement test capabilities into a system to detect systematic or stochastic failures. Typically, every component of an E/E/PE machine is analyzed with respect to its functions and to see how far a function failure influences its behavior. These self tests (or diagnostic tests) deliver a so-called diagnostic coverage, which again is a percentage of probability wherein a failure will be detected. However, this test mechanism must be itself tested to ensure that it actually detects the failure correctly. To reach a qualified diagnostic coverage of a safety system, it is mandatory to integrate the respective cyclic-running self tests, which should detect, for instance, stuck-at, data consistence, drift, and access failure. The fault models and the achievable diagnostic coverage are provided by the IEC 61508.

As an example, memory tests are needed in every E/E/PE machine that uses memory to execute a safety application. Potential failure points of a memory are corrupted memory cells (static failures) and bit flips (stochastic failures). Both failures must be detected with a certain efficiency. Thus the system architect must implement the correct test strategy, as well as the respective reactive measures in his safety concept.

Fail-Safe State

In case of failure or if safety-related information is corrupted, the system must change to a safe state. As already indicated, most of today’s industrial applications define the safe state as “power off” or “output signal off.” For future safety systems, the standards define more sophisticated states such as safe torque or safe limited speed, which require a safety control and/or safety application of a component.

Certifying the Safety Integrity of a System

IEC 61508 describes a methodology to design, deploy, operate, and decommission safety devices. Every company that follows this standard can testify to and document the fitness for safety of their designs or machines and sell the device as IEC 61508 compliant. However, machine builders and factory owners are used to relying on certifications from third-party certification bodies that state a neutral individual has reviewed the component’s development processes and confirms its compliance with safety concepts, the specifications meet the standards, and the correctness of its failure calculations.

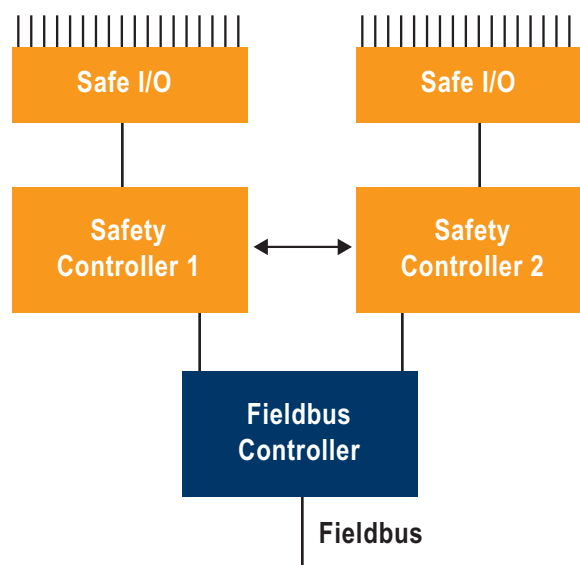
Germany’s TÜV (Technischer Überwachungsverein, or technical supervising association) has an over-100-year history in certifying complex industrial machinery and is the certification body for dozens of different industries and their respective standards and legislations. Today TÜV enjoys the highest reputation in certifying industrial appliances and is the number-one certification body for functional safety certifications. It is highly recommended that automation-component manufacturers work hand in hand with the certification body through the design and deployment of safety-critical designs. This ensures the highest acceptance of their devices by machine builder and plant owners worldwide.

Providing Flexibility with FPGAs

The networks used in industrial automation, such as process automation (i.e., petrochemical plants) or discrete automation (i.e., packaging machinery), are based on fieldbuses (low speed, less deterministic) or Industrial Ethernet (high speed, selectively highly deterministic). Today, around 20 different fieldbus standards and 20 Industrial Ethernet standards are used, with Profibus (fieldbus)/Profinet (Industrial Ethernet) developed by Siemens enjoying the highest market share worldwide of roughly 30%. DeviceNet/EtherNet/IP developed by Rockwell Automation, CC Link/CCLink IE by Mitsubishi, and emerging standards such as Ethercat (Beckhoff), Powerlink (B&R), and Sercos III (Bosch Rexroth) are also gaining significant market shares in specific geographies or subsegments of the industrial automation market.

The remarkable fact about these communication standards is that each of these are complemented by safety concepts that use the fieldbus/Industrial Ethernet as the communication media for the safety-related data between functional safety devices. Almost all fieldbus-oriented safety concepts foresee a dual-channel architecture for SIL3 systems, which means that a safety dual-processor system executes the safety application and is connected to a non-safe communication/networking subsystem, as shown in Figure 4.

Figure 4. Typical Discrete SIL3 Implementation with Three Microcontrollers



This networking subsystem typically implements one of the communication standards described in [Table 1](#).

Table 1. Communication Standards

Company	Fieldbus Standard	Industrial Ethernet Standard	Safety Extension	Notes
Siemens	Profibus (1)	Profinet (1)	Profisafe	
Rockwell	DeviceNet	EtherNet/IP (1)	CIP Safety	
Mitsubishi	CC-Link (1)	CC-Link IE (1)	CC-Link Safety	
Beckhoff	CANopen	EtherCAT (1)	Twinsafe	Supports various fieldbuses
B&R	CANopen and others	Powerlink (1)	Powerlink Safety	Supports various fieldbuses
Bosch Rexroth	SERCOS II (1)	SERCOS III (1)	CIP Safety	Supports various fieldbuses

Note:

(1) Requires proprietary MAC, Switch or HUB which are typically found in vendor-specific ASICs or are provided as FPGA IP.

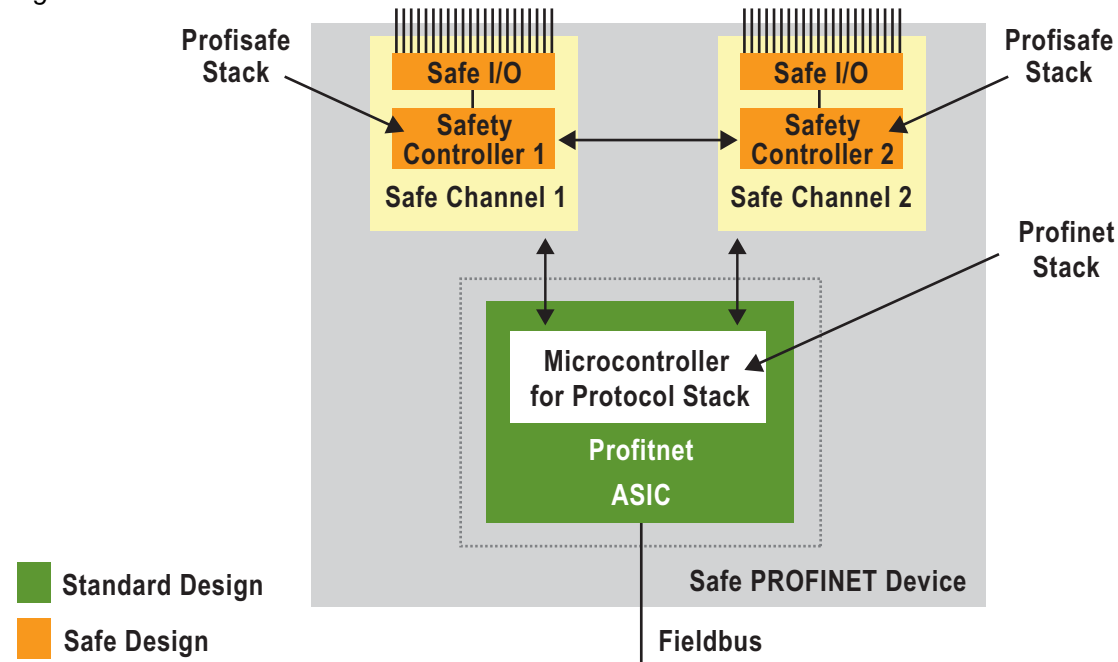


Please note that any fieldbuses not listed in [Table 1](#) do not show significant safety concepts and are therefore not discussed in this paper.

Inflating System Complexity in Safety Designs

To supply automation components into a machine which uses Profinet, a manufacturer must implement Profinet as communication layer and Profisafe as safety layer. As illustrated in [Figure 5](#), this requires implementing a Profinet ASIC as communication controller plus two microcontrollers to execute the Profisafe stack in a SIL3 system.

Figure 5. SIL3 Profisafe Device



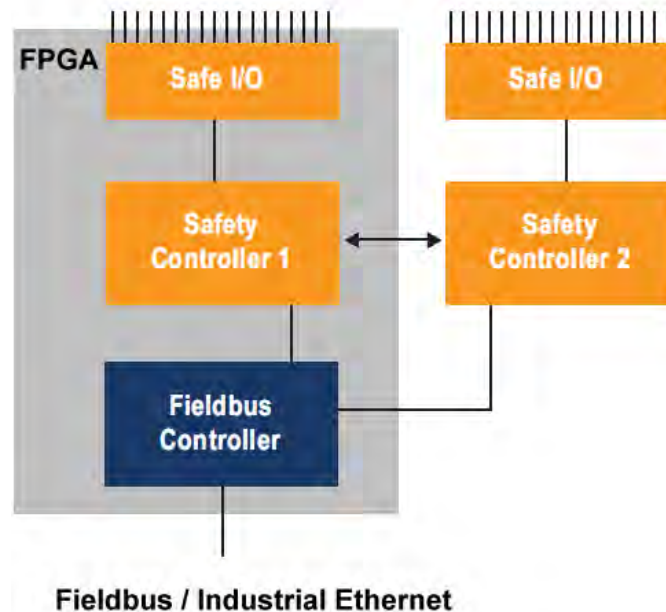
If the same company is next asked to deliver a machine with an EtherCAT network, the EtherCAT ASIC plus a specific architecture for Twinsafe must be implemented. Obviously, each additional network used introduces significant pain for the designers of automation components, because each design must be separately developed and certified according to the IEC 61508.

This pain point is where FPGAs provide two major advantages. Instead of using specific proprietary ASICs, the fieldbus and Industrial Ethernet IP are also available as FPGA IP. (In fact, some Industrial Ethernet protocols are only

available as FPGA IP, such as SERCOS III or Ethernet Powerlink.) FPGA designs have the advantage in that a lower number of device variants can be enabled with a specific communication standard by just loading the respective MAC IP and communication software on the FPGA. Thus, fewer variants or, in the case of Industrial Ethernet, a unique FPGA design can help to implement all of the above mentioned Industrial Ethernet IP (with the exception of Mitsubishi's CC technology which is only available as CC-link and CC Link IE ASICs).

Altera offers a flexible way to combine standard Industrial Ethernet IP as well as embedded safety controllers into one FPGA, as shown in [Figure 6](#). Consequently, the communication layer and one channel of the safety layer can be implemented in one FPGA. This not only offers scalability and reduces system complexity because the number of devices are reduced, but also provides multiple ways to route together safe and unsafe/standard controllers in a unique system design as required by the different safety standards.

Figure 6. Flexible Altera FPGA Simplifies Functional Safety Design



All of the IPs listed in [Table 1](#) (with the exception of CC-Link/IE) are available for Altera FPGAs, thereby guaranteeing a flexible and scalable integration of various fieldbus and Industrial Ethernet standards in combination with a safety controller.

Proving Fitness of Used Components and Tools

IEC 61508 provides a set of requirements which must be followed for the quantitative and qualitative evaluation of the failure probability of an electronic design, and implies that the tools and the electronic parts used for the design of a safety component must be rated. The core requirement is a verification and validation (V) flow which is applied to the overall design cycle. The design steps and tools used in the V-flow must be either certified—unrealistic because it is too expensive and too specific—or proven in use.

“Proven in use” also applies to semiconductor components used in the safety design. Typically, designers must provide a well-defined set of reliability and quality data as well as mathematic calculations to verify the fitness of these items in a safety design. While designers typically do not have such data, the manufacturer of the electronic component and tools can provide extensive data, which shortens the qualification process for the designer significantly. The data is usually provided in the form of safety manuals that have been reviewed and qualified by TÜV. This prior qualification enables the designer to skip this task with TÜV, thereby shrinking the time to market for the development of the safety device.

Evaluating System Performance for Safety Designs

Adding a safety sensor input where an emergency stop button was previously, and cutting off power via a safety output really does not sound like rocket science. Because of this, low-cost microcontrollers are often used in such systems.

With the introduction of Industrial Ethernet networking, safety protocol stacks (e.g., Profisafe) must be executed on these safety controllers beside the safety application. These safety stacks not only significantly inflate the size of the safety firmware, but, depending on the system update cycle time, also introduce significantly higher processing performance since the safety protocol stack must be run with every system cycle (e.g., 1 ms). Still, a good portion of the lowest cost microcontrollers are easily able to perform such tasks.

However, the real performance threat lies in the diagnostic coverage of the entire safety system. As an example, the complete memory (external as well as internal) of the safety controller must be checked continuously on consistency in parallel to the execution of the safety application. In a regular microcontroller system used for safety purposes, the diagnostic tests for system consistency consume between 50% and 80% of the system performance (depending on the system cycle time and SIL category).

This is where FPGAs again can bring in tremendous advantages, because the devices offer the parallel execution of extremely performance-hungry tasks in hardware. With the provision of hardware-based diagnostic tests, such as RAM test IP, overall system performance can be reduced significantly and processing resources for the safety application can be freed accordingly.

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 major fieldbus- and Industrial Ethernet-based safety concepts can be implemented in a very limited number of hardware design variations. The TÜV-qualified safety data package for Altera's tools, IP, and semiconductor devices simplifies and shortens the usually lengthy overall qualification and certification process because the package is accepted by TÜV as a pre-approved topic. In addition, hardware-based diagnostic tests significantly reduce overall system performance requirements by using the FPGA's intrinsic parallel processing capabilities for processing-hungry test routines. Finally, the typically long product lifetimes of FPGAs as well as the migration option for application-specific functions and firmware reduce functional obsolescence for the safety design.

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

Further Information

- Industrial Market:
www.altera.com/industrial
- White Paper: *Lowering the Total Cost of Ownership for Industrial Applications*:
www.altera.com/literature/wp/wp-01122-tco-industrial.pdf
- Video Demo: “Support Multiple Industrial Ethernet Protocols with a Single FPGA”:
www.altera.com/b/support-multiple-industrial-ethernet-protocols-single-fpga.html
- Webcast: “Designing with Multiple Industrial Ethernet Standards on a Single Hardware Platform”:
www.altera.com/education/webcasts/all/wc-2009-industrial-ethernet-single-fpga.html
- White Paper: *A Flexible Solution for Industrial Ethernet*:
www.altera.com/literature/wp/wp-01037.pdf
- About Cyclone Series FPGAs:
www.altera.com/products/devices/cyclone-about/cyc-about.html
- Webcast: “Reduce Total System Costs with Market’s Lowest Cost, Lowest Power FPGAs”:
www.altera.com/education/webcasts/all/wc-2009-cyclone-iv.html
- Nios II Processor: The World’s Most Versatile Embedded Processor:
www.altera.com/nios
- New BeMicro FPGA Evaluation Kit:
www.altera.com/b/nios-bemicro-evaluation-kit.html
- Design Software:
www.altera.com/products/software/sfw-index.jsp
- Altera Training:
www.altera.com/education/training/trn-index.jsp

Acknowledgements

- Frank Foerster, Market Development Manager/Author, Industrial and Automotive Business Unit, Altera Corporation
- Stefano Zammattio, Product Marketing Manager, Altera Corporation
- Adam Titley, Sr. Design Engineer, Embedded System Solutions Group, Altera Corporation
- Jason Chiang, Sr. Technical Product Marketing Manager, Industrial and Automotive Business Unit, Altera Corporation



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

Copyright © 2010 Altera Corporation. All rights reserved. Altera, The Programmable Solutions Company, the stylized Altera logo, specific device designations, and all other words and logos that are identified as trademarks and/or service marks are, unless noted otherwise, the trademarks and service marks of Altera Corporation in the U.S. and other countries. All other product or service names are the property of their respective holders. Altera products are protected under numerous U.S. and foreign patents and pending applications, maskwork rights, and copyrights. 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 Corporation. 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.