Eight reasons to use FPGAs in functional safety applications

Author: Ron Wilson, Intel Programmable Solutions Group

FPGA, ASIC, and CPLD technologies are playing an increasing role in functional safety product development. International functional safety standards such as IEC 61508 are adding guidance for FPGA vendors on the standard's requirements, showing assessors how to certify FPGA-based designs, and offering customers advice on using FPGAs in their safety applications. So here are eight reasons to use FPGAs instead of microcontrollers or DSPs in an IEC 61508 compliant functional safety project.

1: Flexibility
Customers with a system in production are often asked to produce an update that meets a certain Safety Integrity Level (SIL). There are two ways of doing this: by adding an option board to an existing design, or by starting a new design. Adding an option card means adding costs and dealing with potential interfacing issues.

The other approach is to create a design from scratch that maintains backwards compatibility. Industry often uses redundant channels to meet safety requirements, which works but is inefficient and can introduce common-cause failures due to features that are common to both channels, such as supplies or clocks.

FPGAs provide more architectural and implementation options. Simple designs can include dual channels and arbiter logic. More intelligent architectures can use fault-robust circuitry, which reduces the likelihood of common cause failures. The design can also interface to existing non-safety products in a flexible way, using as many I/Os and other functions necessary to deliver a bolt-on solution. Using FPGAs also means that designers are not restricted to the set functionality of a standard device.

2: Integration
Figure 1 shows 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 soft-core processors. This approach can cut the total cost of ownership, design footprint, and power consumption of a design while meeting functional safety requirements.

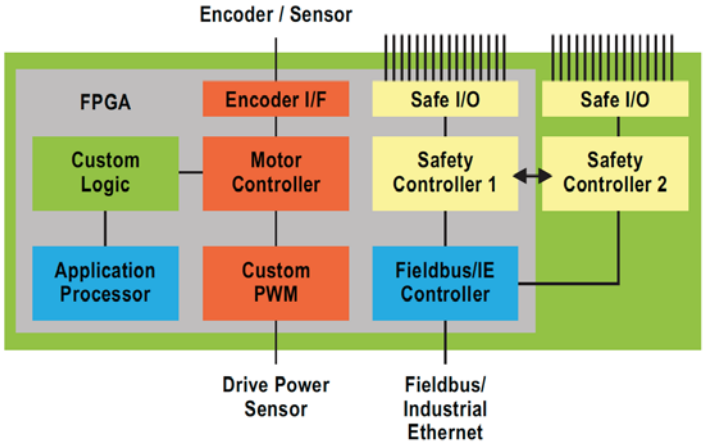

Figure 1: A typical SIL3 industrial 'safe' system

3: Product range

The standard approach to producing IEC 61508-compliant microcontrollers or digital signal processors is to develop a product range which has the necessary qualification, certification of 'a safety element out of context', and documentation. However, these standard parts may not fit your needs exactly, often being over-or under-specified.

With FPGAs, designers only need to use the blocks that are essential to achieve certification for their system. This results in a more efficient design, and also makes it possible to use standard mainstream, rather than safety-certified, products, which reduces the risk of obsolescence.

4: Performance

Speed is essential in functional safety design to ensure that decisions can be made quickly enough to prevent harm. This is particularly the case with the computationally intensive control algorithms necessary to create an intelligent control system that can handle more complex responses to safety issues than the simple "emergency stop" or "safe torque off" functionality of basic safety concepts.

Safety issues also have to be managed when the system is operating normally. For example, a system that can run diagnostics while operating needs higher performance than a system without such diagnostics, performance that can be provided using FPGAs. For example, a combination of hardened processor cores, soft-core processors, and dedicated logic can meet timing or latency requirements and enable pre-diagnostics, as well as runtime diagnostics, without affecting the way the system works.

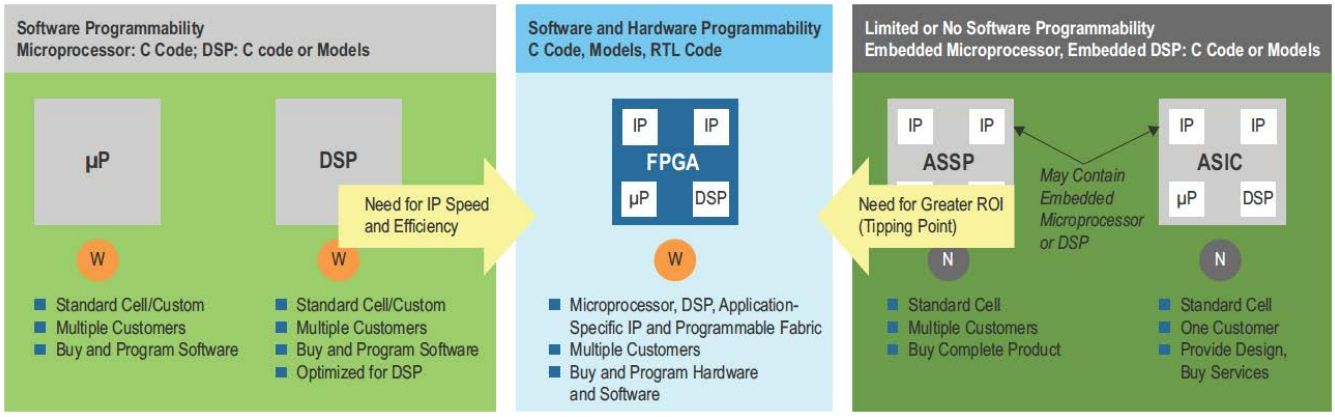

Figure 2: Applications are converging on to FPGA-based technology

5: Tools and methodology

Designing a safe product demands considering safety across all aspects of product development, such as adopting quality management standards, developing a "safe" design methodology, and applying safety concepts.

The V-Model (see Figure 3) is commonly used to separate the phases of product specification from test, verification, validation, and integration while also improving feedback and monitoring processes. It describes a set of steps to be undertaken during a project life cycle and begins with the decomposition of requirements and the clear definition of all necessary system specifications. Each of these decomposition steps is matched with a verification step.

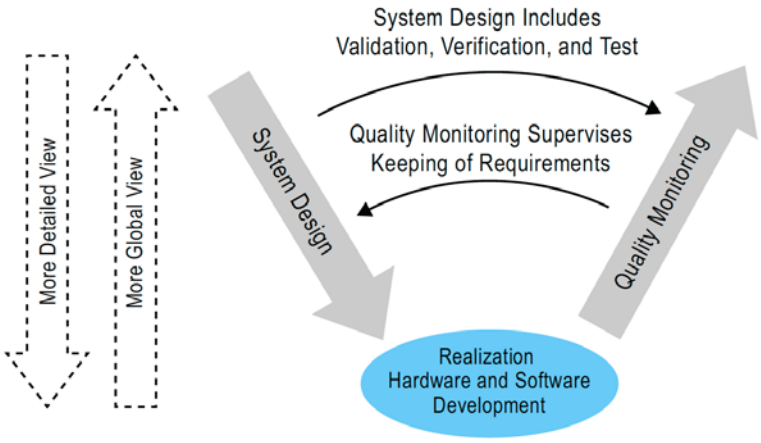

Figure 3: Simplified V-model

To apply the V-Model to functional safety design, the process must follow the IEC 61508:2010 life cycle requirements, and each step in the V-Model must be accompanied by documents that define a precondition (input) and result (output) after a successful completion of the step. Altera's TüV-qualified Functional Safety Data Package (FSDP) includes a detailed document that helps users to define a process structure for applying the V-Model to FPGA development.

This FPGA V-Model is approved according to IEC 61508:2010 and comes with a detailed description of the input and output documentation for each step, the verification methods to be applied, and the tools to be used. This also saves time in establishing a safety-centric FPGA development process (see Figure 4).

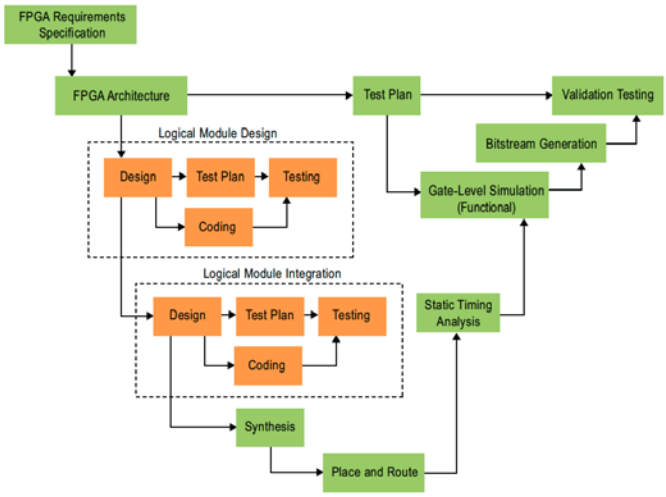

Figure 4: Tool flow

The V-Flow and its related documentation maps all the steps in the design of a safe application for FPGAs to the IEC specification and its requirements. It explains which tools should be used for each step, while chapters in the IEC specification guide users through the steps necessary to develop a safe application.

The Altera Quartus II design tool suite has been reviewed by TUV Rheinland and qualified for use in the design of safety-related systems.

Altera also provides detailed information on how to fulfil the needs of IEC 61508:2010 with a list of techniques and measures that prevent the introduction of faults during design and development. These are linked to the tools that implement them, and backed up by checklists to remind development teams of every step they must take and every document they must generate.

6: Certified data
A lot of functional safety design rests on having enough rigor to develop or source the right documentation at every step of the process. Altera helps out here by providing an extensive statistical analysis of the reliability of Altera FPGAs, enabling users to calculate failure-in-time rates. The safety data package also contains a silicon integration guide, relevant silicon data for use in typical safety calculations, and information about specific IEC61508 compliance items.

7: Diagnostic IP
Functional safety design strategies may require the inclusion of monitoring systems for basic signals such as clock and power, and complex data monitors to ensure correct system operations. It may also be necessary to include ways to automatically identify failures, and move the system into a safe state.

One benefit of using FPGAs is that diagnostic features can be implemented in their hardware, which saves the effort of writing additional software and has less impact on system performance than software-based diagnostics. Some functions that could be added to the hardware include mechanisms to monitor the frequency of a clock signal against a reference, diagnostic IP that detects single-event upsets, and even dedicated system diagnosics processors.

8: Proven in use, reduced risk of obsolescence
Building functional safety systems using FPGAs offers two more advantages. The first is that you can base the functional safety aware part of your product range on an existing design that is well-proven in use, increasing your confidence in it. The second advantage is that standard FPGAs are likely to have longer product lifetimes than functional-safety specific parts that have only ever sold in low volumes to a limited number of customers.

Conclusion
Building efficient functional safety design takes rigor. Working with FPGAs can enable greater design flexibility and system optimization than standard parts can offer. Developing an FPGA-based functional safety product using a certified flow that helps you maintain the necessary rigor can help smooth the path to safety certification.

ENDS