Reduce Development Time, System Complexity, and Certification Risk

Qualified Functional Safety Data Package

Industrial automation, transportation, the smart grid, automotive, military and aerospace, and medical require that machinery and products are highly reliable, safe, and certified for functional safety. Safety is a central requirement when you develop machinery that must comply with worldwide established safety standards such as IEC 61508 and ISO 26262.

When you develop a safe product, you need to consider safety as a core system functionality. Design challenges include:

- Adopting quality management standards, 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

Impact of Functional Safety

Typical design steps to develop an application, before safety:

|-------------------------------|--------------------------|---------------------------------|-------------------------------|--------------------|-------------------------------------|----------------------------------|------------------------------------------|---------------------------------------|---------|

If you add some of the required steps to design a safe application and achieve functional safety certification (shown in yellow), you can see the significant project complexity:

Having immediate access to qualified semiconductor data, intellectual property (IP), development flows, and design tools from a vendor like Altera can help you significantly shorten your overall project timeline by 1 ½ years to 2 years:

Accelerating Development

To simplify and speed up the certification process for faster time to market, we worked with TÜV Rheinland and obtained approval for Altera® FPGA devices, IP, our established safety FPGA design flow, and development tools for safety designs up to the Safety Integrity Level 3 (SIL3). This certification means that our tools, methodologies, and devices are sufficiently free of systematic errors.

<table>
<thead>
<tr>
<th>Altera Functional Safety Data Package Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Data Safety Package</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Altera FPGA development methodology</td>
</tr>
<tr>
<td>Altera FPGA development tools</td>
</tr>
<tr>
<td>IP</td>
</tr>
<tr>
<td>Diagnostic IP</td>
</tr>
<tr>
<td>Device reliability reports, guidelines</td>
</tr>
<tr>
<td>Formatted according to IEC 61508</td>
</tr>
</tbody>
</table>
Altera FPGAs Provide Flexible Safety Solutions

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® 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.

Architectures where safety typically is an after-thought often use bolt-on safety option boards and dual microcontroller units (MCUs) that detect system failures. Using an option card increases the cost significantly.

Integrating a SIL3 “safe” solution in a pre-qualified FPGA with standard application functions on the main board not only lowers the safety cost footprint, but it also enhances system flexibility and shortens development time. It is designed with safety as a core system functionality in mind.

If you are concerned about the lack of flexibility, long development times, or device certification issues that come with traditional safety architectures, Altera’s FPGAs are the ideal solution.

Figure 1: A Typical SIL3 Industrial “Safe” System