

从工厂、机械和过程自动化到发电、供应和运输等各领域的工业自动化应用中，都越来越需要更多的安全设备。本白皮书研究一个工业芯片系统 (SoC) 案例——芯片驱动，向工程师解释在实现符合 IEC 61508 的产品认证过程中，怎样节省 18 个月的设计时间。具有 Altera® FPGA 等经过认证的器件意味着，设计人员可以充分发挥 FPGA 的灵活性优势，不用担心这些 FPGA 能否用于安全应用。

Altera 的 3 级安全完整性 (SIL3) 功能安全数据包包括 TÜV Rheinland 对 Altera 工具、IP 和器件数据的认证，缩短并简化了符合 IEC 61508 安全应用的开发，同时高效的满足了低成本和高集成度嵌入式系统的需求。经过预认证的设计流程和工具，以及经过预认证的嵌入式系统和诊断知识产权 (IP) 降低了安全非常重要的工业应用的认证风险，例如，伺服和逆变驱动器、安全 I/O 和 PLC 以及自动控制器等。

## 引言

工业自动化、物流以及智能电网等很多工业领域都要求机械设备和产品具有安全性，经过了功能安全认证。当开发必须符合全世界安全标准的机械设备时，灵活性和逐渐增高的安全成本是非常重要的决定因素。如果公司计划将产品销售到需要符合当地安全规章制度的国家，例如，新的机械建造规范 (2006/42/EG)，这是产品出口到欧洲必须满足的要求，那么，这些公司必须在整个设计过程中采用安全方法，这样才能参与竞争。在应用中实现安全标准的另一原因是工厂操作人员需要对机械设备进行安全操作，以提高效能，例如，在部分机械设备还在工作时对设备进行维护，显著缩短开机和停机时间等。

在这些应用中，安全要求产生了新的机械开发过程，增加了电子设备的复杂度。复杂度的提高一般会导致硬件成本的显著增加。对于新应用，设计和开发过程越复杂，产品面市时间就越长。

当公司决定开发安全产品时，必须把安全作为核心系统功能。历史上，通过冗余控制器或者通信模块等其他功能，结合电路来监视系统，在系统中增加安全功能。与从一开始就针对安全和成本竞争力进行优化的设计安全应用相比，这些置入的安全组件是事后加入到系统概念中，明显提高了成本，不够灵活，无法更新。

开发安全应用的设计挑战包括：

- 采用“安全”设计方法以及安全概念
- 需要更多的工程投入（时间和技术），结果产品推迟面市，提高了总体拥有成本。
- 工程管理，采集所有系统组件的数据，根据安全规范要求对工程进行记录。

本白皮书将介绍怎样成功实现一个工程，满足安全解决方案的目标要求，同时满足成本和产品及时面市目标。成功的关键是采用经过验证的设计方法，合格的工具和器件作为产品的一部分，从产品开发的一开始就考虑安全问题。

## 设计一个安全驱动器

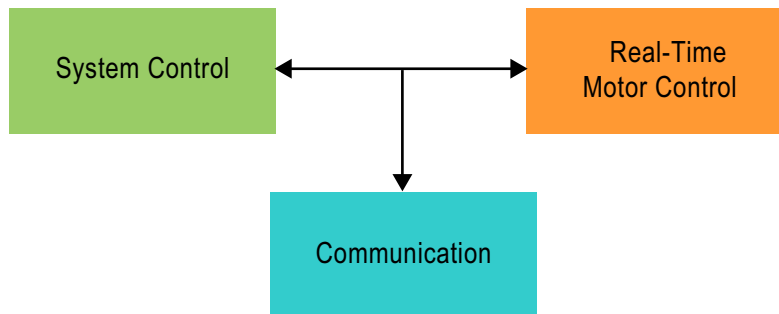
如果没有想到安全问题，开发一个具体应用的典型设计步骤如图 1 所示。

图 1. 典型设计步骤



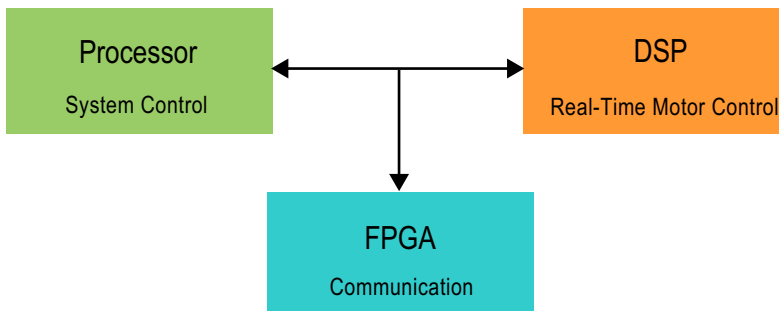
考虑到市场需求，以及企业对市场成功的展望，第一步是开发产品体系结构，如图 2 所示。对于驱动器等典型的电机控制应用，设计步骤把系统分成系统控制、通信和实时电机控制功能等部分。例如，对于系统的控制部分和实时部分，体系结构选择软件实现，对于通信部分确定使用硬件 / 软件方法，以支持实时工业以太网通信协议。

图 2. 体系结构开发



下一步是选择组件（图 3）。做出决定后，具体实施时，控制软件可能运行在标准应用处理器上，在数字信号处理器 (DSP) 上实现实时电机控制部分，而采用基于 FPGA 的方法实现系统中的通信部分。采用 FPGA，系统能够在可以互换的相同器件中灵活的实现各种不同的工业以太网标准，例如以太网 /IP、EtherCat、PROFINET，或者 SERCOS III 等。利用灵活的通信部分体系结构，可以定制标准硬件平台，很容易满足最终用户的特殊协议需求。

图 3. 组件选择



确定如何划分并选择了组件后，设计团队可以针对各自的应用展开开发工作。然后，他们将组件集成为一个完整的系统，测试系统功能，发布产品。

## 增加安全功能

如果按照产品要求，开发功能安全设计，则需要增强其他的工程阶段，如图 4 黄色部分所示。设计安全应用的目的是获得功能安全认证，例如 IEC 61508 等，这样，工程越来越复杂，需要符合标准、而且非常清晰的工程结构。IEC 61508 规范涵盖了从开发具体应用到产品退出市场的整个安全生命周期。本白皮书重点关注安全生命周期的第一阶段，即，从工程启动到获得认证。按照安全标准的步骤和过程，则需要简化与评估人员的通信，以确保能够清楚的理解安全目标、概念、过程和解决方案，满足安全要求。

图 4. 根据安全步骤而增加的设计步骤



### 工程启动和风险分析

在工程启动和风险分析阶段，根据应用的一般要求来确定工程中的安全范围。对于实施阶段，确定并梳理和记录应用所需要和能够实现的 SIL，作为风险分析和评估的基础。在开发安全应用过程后期，必须进行安全评估，而风险分析则是评估的基础。它表明了对产品边界的理解，与产品范围定义密切相关。它是所需 SIL 的基础，详细定义了安全功能，以及产品文档框架。这需要在组件级以及系统级完成。

### 体系结构开发

按照这一步骤，开发应用体系结构以满足功能要求以及安全要求。对安全要求进行提炼，记录在操作和维护阶段实现的某些功能，确定验证能否满足安全要求而需要采取的策略。

### 安全要求规范

对于安全驱动，其范围必须包括几个方面，例如，确定驱动参数是否在允许的范围内，或者，安全 I/O 信号是否是关键事件等。驱动最基本的安全特性是“安全扭矩关闭” (STO)，以安全方式断开电机电源。这一过程还包括与整个安全事件自动化系统的通信，必须在一定的时间窗口内进行评估，例如，在预先确定的时间周期内，按照一系列步骤顺序关断整个应用。

### 验证和认证规划

验证规划的开发包括受控失败插入方法，以测试系统，进行其他的监控，观察系统，对比当前参数和预先确定的参数，以及允许值。

### 组件选择、组件、IP 和工具资格

典型的工程都有组件选择步骤，但是还有其他的需求以确保分配和选择的组件和 IP 功能适合安全应用。对于选择，重要的是考虑残留错误概率，这是计算产品以及最终 SIL 全部失败概率 (FIT) 的基础。部分的，可以通过收集所需的器件和设计工具数据以及信息来实现这一点，这样，很多用户都可以使用产品，不会出现系统错误，能够可靠使用（例如，对于 IP）。还可以通过使用处理器或者 FPGA 等半导体产品错误概率报告以及可靠性信息来实现它。但是，一般很难接触到组件和半导体产品可靠性报告，这些报告提供了必要的信息，特别是与应用相关的设计工具和 IP。

## 应用设计实现

通信协议、FPGA 中使用的存储器接口 IP、或者嵌入在 FPGA 中的 Altera Nios® II 嵌入式处理器 IP 等复杂系统功能，通常用于运行驱动应用中工业以太网协议的软件堆栈，这些都需要进行安全应用分析、测试和认证。

## 功能 / 诊断功能

除了实现应用程序，还必须在设计中加入其他功能。需要采用时钟和电源等基本参数监视功能以及数据监视等复杂功能，观察脉冲宽度调制 (PWM) 的输出，从而保证系统正常工作。需要实现能够自动发现错误的功能，使系统进入安全状态。基本功能包括保证存储器内容不会由于外部影响设计而发生改变，监视系统时钟以保证在设定的系统参数范围内驱动设计（或者由于外部组件的失效导致出现错误），电源正常工作。

## 集成和测试

开发了每一组件后，将其集成到安全驱动方案中，进行测试，实现预期的系统功能，提供设定好的安全功能。通过安全验证，保证所需的安全特性能够在工作期间发挥作用，例如，确保外部因素对设计的安全功能没有不利影响，偶然的禁用不会影响系统。

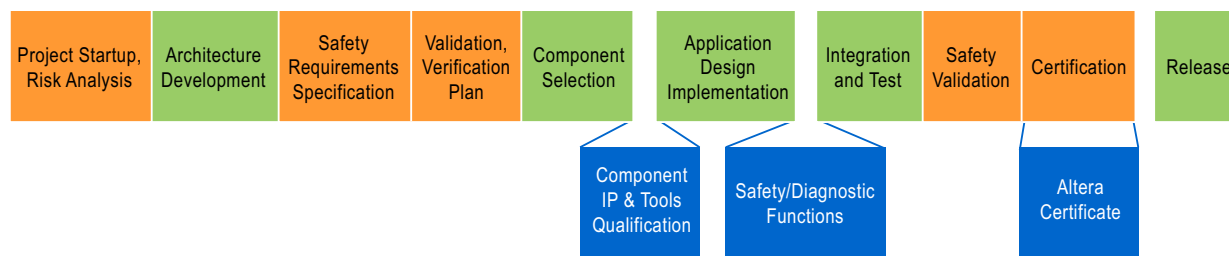
## 安全验证、认证和发布

在整个过程中，要求与评估人员密切合作，以保证在开发过程中所进行的评估是合理的，提供合适的安全功能。最后，评估人员对产品的安全功能进行认证，可以向市场推出该产品。

## 增加预认证安全功能

Altera 等半导体供应商提供某些步骤帮助实现这一过程，减少了在安全应用开发上的投入。例如，立即使用经过功能安全预认证的半导体数据、IP、开发流程和设计工具等，大幅度缩短整个产品开发过程，如图 5 所示。

图 5. 具有预认证安全步骤的设计步骤

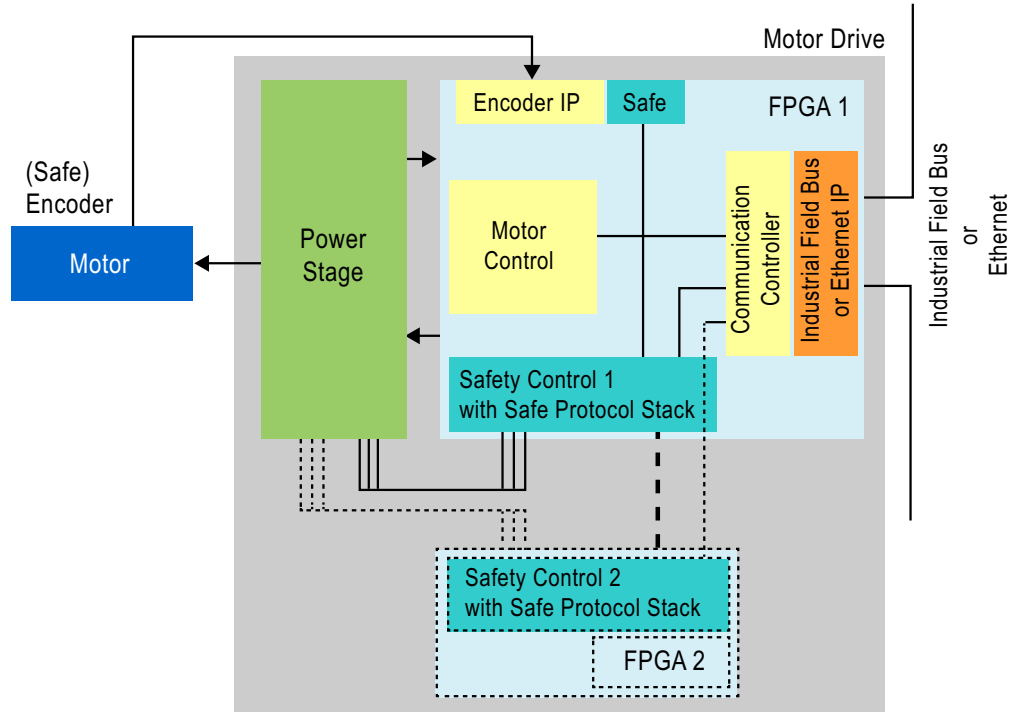


Altera 投入了近两年的时间来实现其产品的认证。对 IP 和设计工具以及器件可靠性数据的测试和应用数据进行了总结和梳理，可以提交进行功能安全验证。开发了 TÜV 认可的设计方法 (V-Flow) 以满足 FPGA 设计的特殊需求。以 FPGA IP 的方式设计了必要的诊断功能，以功能安全包的形式提供。功能安全包用户受益于 Altera 在 TÜV 上的前期投入，在工程投入上能够节省同样的时间。

## 安全驱动的例子

具有安全 I/O 的这一驱动实例采用了 Altera 认证过的 FPGA 设计工具 Quartus® II 软件 9.0 SP2，以及所建议的设计方法实现这一应用实例。此外，如图 6 所示，这一应用使用了两片 FPGA，而没有采用外部处理器和 DSP。该应用被划分成几个 Nios II 软核处理器内核。第一个 Nios II 软核处理器提供通信堆栈支持，第二个处理系统控制，第三个 Nios II 处理器集成在电机控制模块中。对电机控制算法进行了划分，其软件部分运行在 Nios II 处理器上，针对这一应用而专门开发的硬件模块加速电机控制环的实现。外部安全控制器提供 SIL3 应用所需要的冗余功能。

图 6. 安全驱动的两片 FPGA 实现



这一解决方案在一片 FPGA 中结合了安全控制器和现场总线控制器，使用 Altera 的 SOPC Builder 系统集成工具，集成了 Nios II 软核处理器、其他通信 IP 模块，以及编码器接口和存储器接口。

## 芯片驱动的安全性

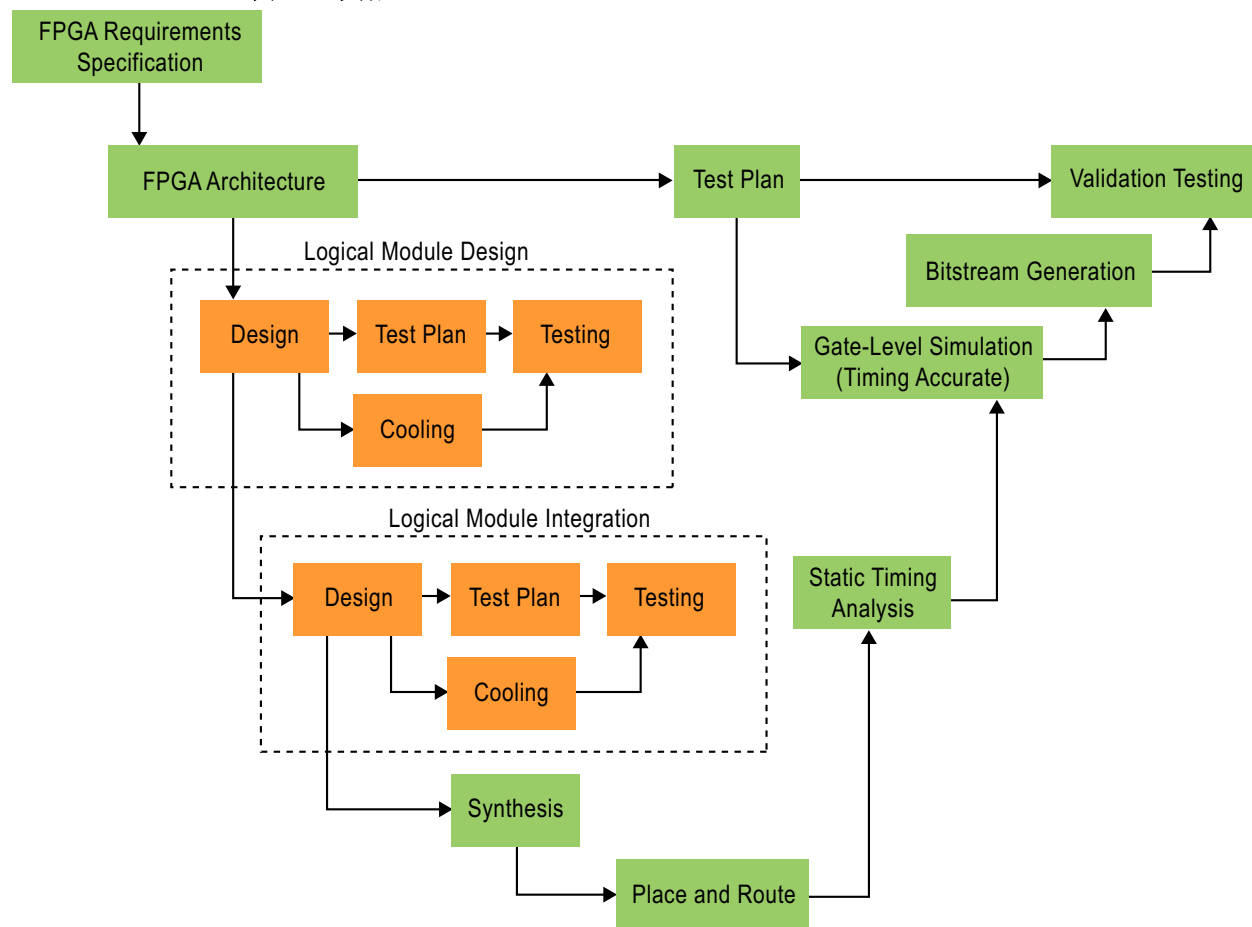
对于 FPGA 中关键而又常用诊断任务的底层监视功能，这一实例使用了 Altera 提供的的安全认证诊断 IP 模块。这些诊断 IP 设计满足 IEC 61508 规范要求，完成以下常用诊断功能：

- 循环冗余校验 (CRC) 计算——这一计算功能用于很多系统中，特别适用于现场总线应用。
- 提取时钟检查——这一内核检查是否有系统时钟以及时钟频率。
- SEU 检查控制器——这一模块采用了器件中的内置软错误检查硬件，监视软错误导致的变化。

由于这些硬核 IP 是在 FPGA 逻辑区中实现的，因此，系统处理器不再承担这些任务。

设计按照 Altera 的建议来实现。在认证方法方面，Altera 采用了 IEC 规范，分析了 FPGA 设计方法和相关要求。从这一分析中，Altera 形成了工具流文档。这一工具流的中心主题是对 Altera 开发的 FPGA V-Flow 的描述，如图 7 所示。

图 7. 工具流



V-Flow 及其相关文档将 Altera FPGA 安全应用设计的所有步骤映射到 IEC 规范上，满足其要求。此外，它解释了哪些设计步骤采用哪些 Altera 工具。讨论了 IEC 规范中的某些章节，并进行了解释，以指导 Altera 用户依照合适的开发步骤来开发安全应用。

Altera 提供业界第一款经过 TÜV 认证的功能安全数据包，涵盖了特定工具流（例如，Quartus II 软件 9.0 SP2）经过认证的器件开发工具、IP 以及硅片数据。包括了评估人员所需要的认证文档和数据，以完全符合 IEC 61508 规范的格式提供，因此，评估人员很容易处理它们。以正确的格式提供这些文档节省了安全工程大量的文档工作。

在功能安全数据包的可靠性报告中，Altera 对 Altera FPGA 的可靠性统计信息进行了大量的分析。计算失效时间 (FIT) 所需的全部信息都含在文档中，还包括指南，解释怎样完成这一计算，这样，很容易提交给评估人员进行认证。

## 结论

通过重新使用符合预认证两芯片方法的驱动系统概念，按照经过认证的设计方法、设计流程、工具和 IP，通常能够加速实现典型的应用开发过程。由于能够立即使用组件的可靠性数据，提供的格式很容易集成到安全认证的所有文档中，因此，加速实现了认证过程。在安全设计和系统设计中，设计人员可以充分利用灵活的 FPGA 设计集成功能。由于安全已经成为具体应用的关键需求之一，因此，它含在整个概念中，通过满足成本和产品及时面市目标来实现它。

## 详细信息

- 适用于功能安全设计的 TÜ 认证 FPGA：  
[www.altera.com/end-markets/industrial/functional-safety/ind-functional-safety.html](http://www.altera.com/end-markets/industrial/functional-safety/ind-functional-safety.html)

## 致谢

- Christoph Fritsch, 战略营销, 工业和汽车业务部, Altera 公司。

## 文档修订历史

表 1 列出了本文档的修订历史。

表 1. 文档修订历史

日期	版本	进行的修改
2011 年 9 月	1.0	初次发布。