减少实现安全认证的步骤

WP-01174-1.0

白皮书

本白皮书介绍在功能安全认证应用中，成功获得 FPGA 认证所需要的步骤。在开发符合 IEC 61508 基本功能安全标准等全球标准的机械设备时，安全是最关键的系统要求。Altera 经过预认证的功能安全数据包缩短了安全关键工业应用的开发和认证时间，降低了认证风险。

引言

很多应用开发人员非常关心功能安全的应用。工程管理人员和验证团队成员面临的是新的未知安全认证领域。项目团队所遇到的问题一般是由认证组织、外部审计等因素造成的。工艺步骤和质量方面的权威认证不仅由企业等方面制定；而且还需要由外部进行监督。

安全工程需要越来越多的工艺步骤和文档。然而，并不是所有的工艺步骤都需要重新开发，或者从头开始建立。通过使用经过预验证的工具或者经过预定义的方法和措施，很容易实现安全认证。在一个工程中，文档扮演了非常重要的角色，国际标准要求严格的符合定义好的规则。因此，采用已经经过认证的文档、工艺步骤和方法对于工程开发非常有帮助。

为简化并加速实现认证过程，Altera 与 TüV Rheinland 合作，Altera® FPGA 器件、IP、FPGA 设计流程和开发工具获得了认证。这一认证表明，Altera 工具、方法和器件不会出现系统错误，可以用在安全关键应用中。

怎样开始

功能安全的主要目的是在安全相关系统中出现随机、系统或者共因故障时，降低损害或者伤亡的风险。所谓的随机失败是由安全系统部件或者组件故障造成的，而系统失败是安全功能规范应用不当或者应用不足造成的。共因故障失败是指安全器件几个部件由于同一种原因同时出现故障造成的，例如，电路板上一条电源线对多个元件进行供电等。一般而言，产品开发的目的是尽可能降低操作过程中出现失败的概率，换言之，进一步提高质量和可靠性。功能安全定义了质量和可靠性质检方法，对于产品定义和开发而言，的确很难实现这些方法。

在您的企业或者公司中，启动一个安全工程之前首先要研究的问题是：已经建立了哪些过程，可以使用哪些过程，重新应用这些过程来构建功能安全工程基础？很多企业采用管理工具进一步提高工艺步骤质量，由此而提高产品质量和可靠性。例如，ISO 9000 系列国际标准 (ISO 9000 ff.) 定义了质量管理 (QM) 系统的手段和措施，通常在 QM 手册中进行了总结。这一手册阐述了日常工作流程所采用的方法。是否符合这一质量标准通常是由外部认证组织来裁定的，由此，应确定这些工艺步骤符合全世界公认的标准要求。

ISO 9000 ff. 的八大支柱之一是描述、实现并遵守企业相关过程。在认证组织中，标准需要采用面向工艺步骤的方法。维持定义好的工艺步骤有助于实现高质量结果。过程一般是可追溯的，并不断完善。

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

ISO
9001:2008
认证

质量管理系统

一个组织的 QM 系统有利于启动安全相关的工程，这是因为已经明确定义了企业的责任，很好的理解了文档处理过程。对文档进行检查，含有保证工艺步骤和产品质量的所有相关信息。

下面列出的项目描述了一组属性，每一文档都应含有这些属性，也可以通过相应的文档列表来获得，以保证清晰的文档标识和相关的要求，这都基于国际电工委员会电气 / 电子 / 可编程电子安全相关系统标准 IEC 61508:2010-1 功能安全的第 5 条款和附录 A：

- 文档作者 (包括对工程内功能的描述)
- 文档版本号
- 文档日期
- 文档历史
- 参考文档
- 专用存储系统中的文件位置
- 没有歧义的标准化文档名称
- 对某些工程步骤进行明确的分配

为避免出现错误或者遗漏，或者产品特性有误，对所有文档进行检查，在检查报告中记录检查结果。此外，在整个工程中，所有特定的要求都能够可追溯，以保证能够满足所有要求，并进行测试和验证。企业甚至需要记录对需求的后期修改，以便在几个月甚至几年后还能够理解这些修改。

与功能安全工程相似，ISO 9000 ff. 要求定期进行内部审计，以保证符合 QM 系统，确定有了改进。所有这些措施不但在标准工程中有助于确保提高质量，而且在安全相关工程中也有同样的效果。这是所有安全相关工作的关键先决条件。

工程准备

质量标准一般都是最新的，它们构成了启动安全工程的基础。以下主题总结了 QM 系统的主要特点：

- 企业或者工程团队内部的职责定义
- 对可用和所采用工艺步骤的描述
- 管理和处理工艺步骤附属文档
- 清晰并且可重复的过程

IEC 61508:2010-1 的第 6 条款对这些方面进行了详细的说明。

安全不仅仅是编写高质量 C 语言或者 (V) HDL 代码，装配印刷电路板。安全是在产品整个生命周期中，应用在所有阶段的设计理念。以下章节主要讨论与功能安全相关的其他方面。

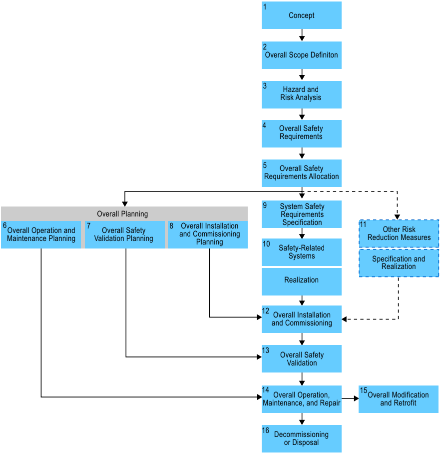
符合 IEC 61508:2010 的功能安全特性

2010 年发布的第二版国际标准 IEC 61508:2010 包括几处改动和增强，产生了目前最新的标准，检验功能安全产品质量的可靠等级。该标准包括几部分：

- 一般要求
- 电气 / 电子 / 可编程电子安全相关系统要求
- 软件要求
- 定义和缩写
- 确定安全完整性等级的实例方法
- IEC 61508-2 和 IEC 61508-3 应用指南
- 方法和措施简介

图 1 显示了 IEC 61508:2010 及其七个组成部分怎样映射到更精细的工艺步骤中，对用户在安全应用的整个生命周期中进行指导。

图 1. 符合 IEC 61508:2010 的安全生命周期



这一国际标准的第 2 版覆盖了其他新主题 FPGA、ASIC 和 CPLD 技术。这些组件在目前的产品开发中扮演了重要角色。由于 FPGA 越来越多的替代了工业应用中常用的电子元器件，因此，IEC 61508 等标准需要支持这些日益发展的技术，才能保持其关联性。这通过对规范不断更新来实现。

产品安全生命周期

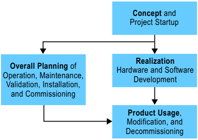
安全作为一种总体理念和要求，包括从开始到产品退出结束的整个产品生命周期。换言之，它必须与系统规划密切相关。安全设备设计方法必须尽早考虑安全问题，而不能事后处理。这与典型的标准化开发过程形成了对比，它一般只涵盖了产品的设计、实施和验证过程。在产品退出之前，不会结束对安全的考虑。IEC 61508:2010 描述了功能安全设备的整个生命周期，从首次概念描述到产品退出结束的整个过程 (图 1)。

工程阶段

初看起来，功能安全仅仅是引入了一些没有价值的额外工作。如果关注概念和规范阶段，那么，工程会更具预测性，质量会进一步提高。在工程早期阶段立即开始进行投入，会大幅度提高今后工作的效能。

请参考图 1，功能安全生命周期含有 16 个相关步骤。整个工艺步骤看起来非常复杂，将其分成四个主要工程阶段有助于更清晰的划分生命周期模型 (图 2)。

图 2. 主要工程阶段



后面的章节会详细讨论这些工程的每一阶段。本白皮书主要介绍 FPGA 应用的功能安全，即，同时描述了 Altera 为不同工程阶段以及每一工程阶段提供的支持。

V 模型

V 模型 (图 3) 通常用于大量的工程中。它继承了瀑布模型 (图 4)，瀑布模型定义了连续设计工艺步骤。与瀑布模型相比，V 模型提高了反馈和监视的可能性，从测试、验证和集成中分离出产品规范工艺步骤。它描述了在工程生命周期中需要完成的一系列步骤，从分解需求开始，清晰的定义了所有必须的系统规范。与这些分解步骤相并行的是对应的验证步骤。这两条路径的交叉点是开发硬件和软件。

图 3. 简化 V 模型

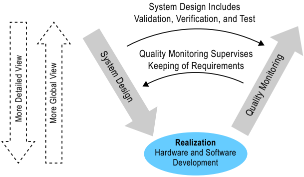
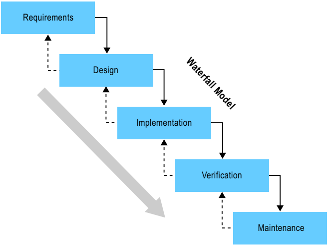


图 4. 瀑布模型



采用 V 模型时需要考虑两个主要方面。它应满足 IEC 61508:2010 生命周期要求，V 模型的每一步骤都需要附加特殊的文档作为前提条件 (输入) 以及成功完成步骤之后的结果 (输出) 。

Altera 的 T ü V 认证功能安全数据包 (FSDP) 含有详细的文档，指导用户起草工艺步骤结构。它提供了一个可以重用的开发 FPGA V 模型，内部 FPGA 开发工艺步骤很容易采用这一模型，以满足安全需求。这一 FPGA V 模型符合 IEC 61508:2010，得到了认可，详细描述了为每一步骤所建议的输入和输出文档。这些 FPGA V 模型步骤的每一个都含有对步骤本身详细的描述，所采用的验证模型以及要使用的工具。这一详细的文档大幅度缩短了工程团队在以安全为中心的 FPGA 开发工艺步骤上投入的时间，如果原样采用 Altera 的建议，那么在这一关键的工程阶段，不需要再投入时间。

配置管理

任何工程必须要安装配置管理，以保证可追溯和可再现。它定义了工程中使用的一组工具。功能安全还要求这些工具能够满足功能安全要求和认证，用在安全工程中。

如果 Altera 等工具供应商对其工具链进行了认证，可以用在功能安全工程中，那么，这将非常有价值。IEC 61508-3:2010 强烈建议在软件设计和开发中使用经过认证的工具。如果工具供应商不能提供这种认证，那么，用户很难独立验证工程所需要的工具。只有工具生产商具有所有详细的信息和知识来完成可信的工具认证。Altera 与 TüV 一起认证了 Quartus® II 开发软件 9.0 SP2，可以用于安全相关工程中。这一认证包括关于怎样使用工具、工具流、知识产权 (IP) 和硅片数据的详细建议。此外，数据包包括 FPGA 文档详细的认证检查和参考。

概念

功能安全概念的草案规范一般是整个安全相关工程中最重要的部分。拥有定义好的概念决定了工程总体上能否成功。安全概念也是认证过程的第一个步骤，在工程进入到下一阶段之前，认证组织应批准这一概念。在后续阶段，评估人员检查这一概念时可能要对系统安全概念进行较大的修改，重新开展实施工作。概念得到批准后，被修改、增加或者去掉安全相关特性的可能性很小。这一安全概念清晰的定义了工程概念。

通过一个实例可以更详细的解释这一问题。硬件故障容限 (HFT) 定义了导致整个安全功能完全失效的最小故障数量。例如，在双通道体系结构中，一个组件出现危险故障不会破坏整个安全功能，这是因为第二个通道仍然能够保持安全功能正常工作。在这种情况下，系统有一个 HFT。HFT 对安全产品能够实现的 3 级安全完整性 (SIL 3) 有明显的影响，是决定体系结构的主要因素。

例如，通过两个不同的冗余通道可以实现 1 个 HFT，在出现紧急情况时，能够使待控设备 (EUC) 进入安全状态。如果一个通道失效，系统仍然可以依靠剩余的第二个通道继续工作。这是基本设计决定，必须尽早在安全概念中清晰的进行描述。在工程后期，不能轻易的对其进行修改。

除了已经是工程规划组成部分的一般工程管理，在安全概念中还需要考虑以下方面：

- 对系统及其主要组成的整体描述
- 系统边界、应用和任务指标
- 对将要实施的安全功能的定义
- 系统接口
- 分析安全功能能够降低多少风险
- 所需 SIL 的评估，以降低风险
- 根据使用范围而需要遵从的其他标准
- 描述怎样实现所需的 SIL
- 体系结构原理

根据产品种类，这一列表还会增加。每一安全系统可满足特殊的功能安全需求，因此，在安全概念文档中，需要描述不同的主题。很显然，安全概念需要准确的掌握所有需求，尽早接触认证机构才能找到差距。

能够在开始实施之前探测到安全概念中的功能问题。Altera 的 FSDP 提供可以在 FPGA 平台上实现的应用和安全功能的详细信息。这些信息有助于进一步简化概念阶段，加速实现整个规划过程。

准备质量检测

除了所有规范和设计阶段中采用的图 3 中的 V 模型，需要重点说明的是这些步骤中的每一个都需要相关的方法来确保整体质量。为能够使这一模型扩展到功能安全方面，国际标准 IEC 61508:2010 详细定义了应采用哪些方法和措施来保证成功实现功能安全工程。

方法和措施

IEC 61508:2010 的第 2、第 3 和第 7 部分详细列出了方法和措施。取决于所需的 SIL，还需要将某些方法进行一定的扩展。从工程开始，必须确定并记录将要使用哪些方法和措施。

一个例子是 IEC 61508:2010 第 2 部分的表 F.2。这张表结合标准的第 7 部分，定义了如果要实现某些 SIL 所需要采用的方法或者措施。在设计阶段，如果需要 SIL 2，建议采用 “基于脚本的过程”。与 SIL 2 相比，SIL 3 需要更高层的应用方法，因此，强烈建议 SIL 3 应用采用同样的方法。出于这一目的，所建议的工具是 Quartus II 工具命令语言 (Tcl) 流程。Altera 提供详细的信息来帮助满足 IEC 61508:2010 要求，列出了方法和措施以防止在设计和开发阶段出现错误。

采用 Altera 的 FSDP，已经选好了措施和方法，进行了很好的记录，可以供开发团队使用。这有助于理解应用的方法，特别是实现第一个安全相关 FPGA 工程的情况。此外，这些方法也清晰的链接了实现它们的工具。

为避免忘记所需要的文档和设计步骤，Altera 的 FSDP 提供详细的检查表，帮助开发团队获得整个生命周期阶段所需的输入和输出文档。而且，定义了一组生命周期活动，以验证全部完成了所有阶段。由于这些检查表已经经过了 T ü V 认证，不需要进行其他的工作来表明怎样确保正确使用了 Altera FSDP 的 V 模型。

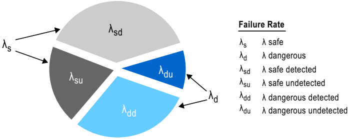
安全要求模式

安全功能被分成两类：工作低要求模式和工作高要求模式。工作低要求模式是指要求以小于每年一次的频率来设置安全状态 EUC 的安全功能。因此，这一类安全功能的特征安全关键值被称为按需危险失败 (PFD) 概率，描述了安全功能在其触发时失效的风险。

工作高要求模式是指一年使用一次以上或者永久使用来设置安全状态 EUC 的安全功能，这作为正常设备工作的一部分。在这种情况下，安全关键值被称为每小时危险失效 (PFH) 平均频率，描述了安全功能在一小时工作时间内失效的概率。作为一个例子，PFH 值应位于 107/h 至 108/h 范围之内，以实现 SIL 3。

在这两种情况 (PFD、PFH) 中，需要计算安全相关产品的剩余失败概率 (图 5)。

图 5. 不同类型的失败率



硬件确定了这一概率值，国际标准提供了电子元器件和公开的 λ 值失败概率的详细信息。采用微控制器或者 FPGA 等半导体器件，由于需要非常了解晶体管和芯片内部结构才能支持对 λ 值的全部计算，因此，这些情况更复杂一些。

通常很难找到半导体器件内部结构的详细信息。Altera 为其用户提供年度可靠性报告，以及每一类可用器件故障时间 (FIT) λ 值的详细信息。Altera 提供应用笔记，解释了可靠性报告中的数据怎样应用于 IEC 61508 认证。提供这一信息作为认证数据包的一部分，显著节省了工程文档阶段以及产品认证期间的投入和时间。

实现

工程实现阶段涵盖了硬件和软件开发以及诊断功能。

硬件和软件

为能够对安全相关电子系统进行建模并实现这些系统，可以结合使用自己开发的 Verilog HDL 或者 VHDL 模块以及商用复杂知识产权 (IP) 功能，例如 Nios® II 处理器等，对于 Altera，这已经通过认证，可以用在安全相关设计中。对于处理器与系统中功能安全部分一起使用的情况，需要采用与 IEC 61508:2010 标准相关的所有要求。IEC 61508:2010 的第 2 部分涵盖了功能安全的硬件方面，第 3 部分涉及到软件相关主题。最后，第 7 部分简要介绍了第 2 和第 3 部分提到的方法和措施。

功能安全软件也要求对整个软件生命周期进行考虑。IEC 61508:2010 的第 3 部分包括了软件生命周期所有步骤的详细信息。它还列出了软件规范、检验、设计和开发以及软件修改和验证的要求。

在使用 Nios II 处理器时，Altera 还具有其他的优势，根据所需要的 SIL，指明相关的不同条目。这些条目处理中断、Quartus II 软件和 Nios 集成开发环境 (IDE) 版本、汇编器、编译器和链接器工具型号应用等主题。

诊断范围

不可能开发确保 100% 不出错的安全相关产品。最重要的一点是尽可能多的探测到错误，在出现错误时，将 EUC 移至安全状态。将可能出现的失败情况分成两类。第一类错误不会导致危险状态 (λ_s)，第二类错误导致不安全或者危险状态 (λ_d)。此外，这些失败概率被分成可探测 (λ_{sd} 和 λ_{dd}) 以及不可探测 (λ_{sd} 和 λ_{du}) 失败类，如图 5 所示。如果能够探测到失败，EUC 被置入安全状态，以降低失败导致的风险。安全功能可靠性方面最重要的因素是相对于所有可能出现的失败，能够探测到多少失败，不会导致出现危险状态。

IEC 61508-2:2010 通过以下方程以及图 5 中的 λ 值定义了安全失败分数 (SFF)：

$$\mathrm{SFF} = \frac{\sum\lambda_s + \sum\lambda_{dd}}{\sum\lambda_s + \sum\lambda_{dd} + \sum\lambda_{du}}$$

很显然，在安全相关设计中，如果未探测到的危险失败 (λ_{du}) 值减小，那么，SFF 值会增大。

IEC 61508:2010 第 2 部分定义了安全系统使用的两类元素。例如，如果定义好了失败模式，并且完全知道故障条件下的元素行为，那么，认为元素是 A 类。如果安全系统仅由 A 类元素构成，那么，它是 A 类系统。在其他情况下，或者安全系统的一个元素不能满足 A 类要求，那么，整个系统被认为是 B 类。B 类系统至少含有一个具有未知失败模式的元素，或者不可预测失败行为的元素。

取决于安全系统的类型及其硬件故障容限，SFF 与 PFD 或者 PFH 值一起对能够实现的 SIL 产生很大的影响。FPGA 设计主要考虑 B 类，这是因为它们基于复杂半导体器件。这样的结果是，要求 SFF 在 90% 至 99% 范围内才能实现具有双通道体系结构的 SIL 3。

最好的一种方法是增大安全失败分数，以提高设计中的诊断范围。这可以通过其他的诊断软件或者具有监视功能的冗余硬件来实现。使用 FPGA 技术的优点是可以在硬件级实现诊断功能。与基于软件的诊断相比，这减少了在编写其他软件代码上的投入，花费的时间也不多，对系统性能影响不大。FPGA 在逻辑阵列中很容易提供资源和功能，这样，不需要额外的电子元件或者器件。

Altera 的 FSDP 提供 IP 内核，具有基本诊断功能。时钟检查器诊断 IP 内核可以用于监视频率以及相对于稳定参考时钟的时钟信号。单事件干扰 (SEU) 诊断 IP 内核能够识别 FPGA 中的 SEU，向系统发出告警。SEU 内核还提供测试诊断 IP 和系统响应的功能，通过插入错误信息来发出告警。循环冗余校验 (CRC) 诊断 IP 内核可以用于计算并检查通信链路上的 CRC 值。

Nios II 处理器的专用软件算法运行存储器、寄存器和其他处理器组成的诊断功能，必须按照与独立微控制器相同的方式来实现这些算法。

结论

对于您的第一个功能安全工程，与最标准的工程相比，可能需要更大的投入。然而，由于功能安全标准提供了详细的工艺步骤、措施和方法，因此，在后续工程中可以很好的应用可重用功能。对于企业中的安全工程，对现有工具、质量措施以及资源进行详细的检查会带来更多的优势，简化了新应用开发工艺步骤的建立。FPGA 能够灵活的进行设计，通过 Altera 在方法、合格工具和器件以及合格 IP 与诊断 IP 上的前期投入，可以很好的支持功能安全的实现。

V 模型是整个功能安全工程的关键，因此，在工程的这一部分上花费一些时间非常必要。在 FPGA 上重新使用 Altera 提供的成熟的方法以及经过验证的 V 模型，对于工程的这一阶段非常有帮助。

对规划系统进行清晰的定义，能够很好的理解它，重新使用经过预认证的技术，这可以很快的成功实现工程。

Altera 的 FSDP 有助于工程管理和开发团队满足安全工程的要求，节省了大量的工程规划和开发时间。对于开发符合最新 IEC 61508:2010 标准的 SIL 3 设计安全相关应用，这具有明显的优势。

详细信息

- 适用于功能安全设计的 TüV 认证 FPGA：
  www.altera.com/end-markets/industrial/functional-safety/ind-functional-safety.html
- 白皮书：*使用经过 TüV 认证的 FPGA 开发功能安全系统*：
  www.altera.com/literature/wp/wp-01123-functional-safety.pdf
- 白皮书：*设计安全工业芯片系统的验证方法*：
  www.altera.com/literature/wp/wp-01168-safe-industrial-soc.pdf
- Altera 设计软件：
  www.altera.com/products/software/sfw-index.jsp
- *Quartus II 手册 9.0 版*：
  www.altera.com/literature/hb/qts/archives/quartusii_handbook_9.0.pdf
- *Quartus II 软件器件支持发布声明*：
  www.altera.com/literature/rn/rn_qts_90sp2_dev_support.pdf
- ISO 9000 ff.：
  www.iso.org/iso/iso_9000_essentials
- Altera 可靠性报告：
  www.altera.com/literature/rr/rr.pdf
- 功能安全和 IEC 61508：
  www.iec.ch/functionalsafety/

致谢

- Roland Rauch，功能安全工程师，工程处，Rauch。
- Christoph Fritsch，战略市场高级经理，工业和汽车业务部，Altera 公司。
- Jason Chiang，技术市场高级经理，工业和汽车业务部，Altera 公司。
- Adam Titley，设计工程师 MTS，嵌入式解决方案，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 11 月	1.0	初次发布。