

在高可靠性和信息安全保障系统中实现设计分离

传统上，系统设计通过冗余来实现可靠性，这导致元件数量、逻辑容量、系统功耗和成本不断攀升。Altera 的设计分离特性满足了这些相互矛盾的需求，实现了低功耗、小体积和高性能，同时保持了较高的可靠性和信息安全。

引言

FPGA 在当今工艺技术中得到了非常广泛的应用。其应用已经从以前传统的胶合逻辑接口扩展到核心互联网路由器和高性能计算系统所使用的高级信息处理系统。整个发展过程中的共同点是要求在更小的空间中集成更多的功能，同时降低功耗和成本。

高可靠性系统设计有相似的需求，包括减小系统体积、功耗和成本，达到预期的高可靠性。传统上，这些系统设计通过冗余来实现可靠性。依靠增加元件数量、提高逻辑容量、增大系统功耗以及成本来获得冗余。其他系统设计领域也有相同的可靠性要求和特性，这些领域包括：信息安全保障、航空电子和工业安全系统等。

Altera 开发了解决方案来满足这些相互矛盾的需求，同时实现这些应用需要的高可靠性和信息安全保障。Altera® Quartus® II 设计软件以及 Cyclone® III LS FPGA 中的设计分离特性为设计人员提供了一种简单的方法，将已有的高可靠性冗余设计方法集成到单片 FPGA 体系结构中。

容错需求

美国国防部 (DoD) 研究了二战期间的陆军和海军装备后，要求加强可靠性工程研究。例如，轰炸机的平均故障间隔时间 (MTBF) 不到 20 小时，而修理轰炸机的成本要比最初购买价格高出 10 倍以上。自此，系统设计寿命周期总成本这一概念成为设计和系统选择的关键标准。

安全保障加密系统有相似的发展过程。加密系统中的故障会在军用系统安全和商用系统商业价值等方面影响系统的寿命周期。考虑到这些关系，安全保障加密系统与高可靠性系统有相似的设计和分析需求。

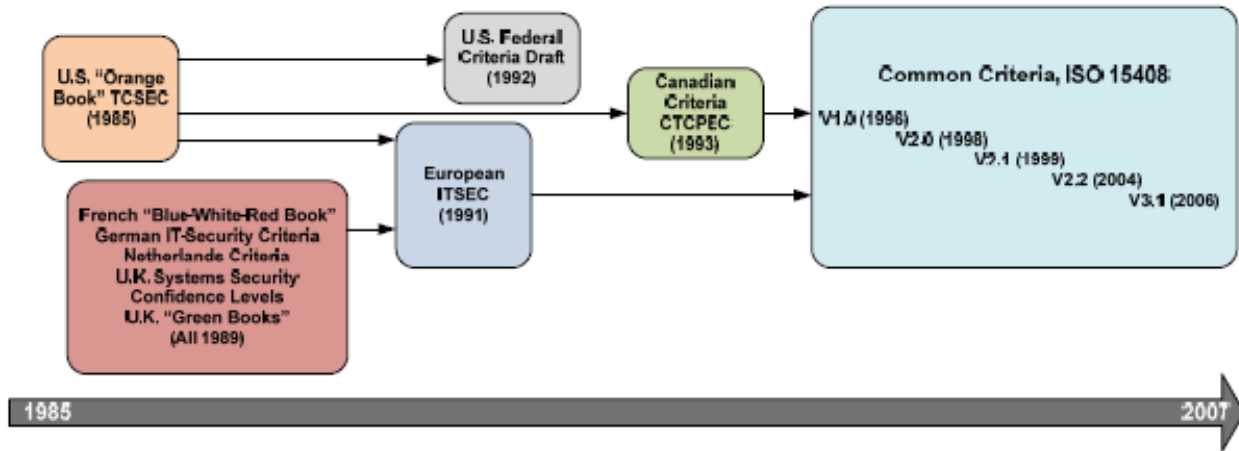
在任何情形下，设计人员的目标都是减小具体应用所需要的 PCB 面积以及元件数量。多年以来这一直是电子行业的发展趋势，首先是芯片系统 (SoC) ASIC 解决方案，以及后来的 SoC FPGA 解决方案。第一步是将外部数字逻辑合并到一个器件中。这一方案进展非常成功，直到 ASIC 开发成本和进度超过了市场能够承受的成本和时间。随着 ASIC 成本的攀升，越来越多的系统设计人员转向 FPGA，其性能和逻辑密度支持将逻辑集成到一个可编程芯片中。SoC 设计多年以来一直稳步增长，FPGA 设计及其复杂性导致无法将冗余设计集成到一起。很多系统和安全分析人士认为很难针对分离和独立数据通路验证进行必要的分析工作。

Altera 与认证权威机构进行合作，解决了棘手的复杂 FPGA 器件分析问题，实现了分离和独立的数据通路。设计人员从一开始选择设计 FPGA 工具以及数据流程时就注意到分析问题，将故障保护逻辑设计集成到单片 FPGA 架构中。这样，设计人员不但达到了 SoC 市场目标，而且还满足了高可靠性和安全保障应用的要求。

信息安全保障应用

应用广泛的信息安全保障设备要求用户在设计中置入一定的信任等级，实现设备加密。要确保实现复杂系统设计，一定要建立设计标准，进行系统评估。目前已经有几种安全设计标准和评估体系。详细解释设计要求和评估标准已经超出了本文的范围，图 1 简要介绍了这一需求的发展及其复杂性。

图 1. 安全标准设计和分析发展



信息技术 (IT) 系统对信息安全保障的影响最大。随着基础设施控制系统数量的增加，通过互联网可以获得大量的企业和个人信息，因此，日益需要 IT 系统来保护敏感的信息和系统不受全球黑客的攻击。

为了能够实现互联网信息安全保障，用户不能只检查数据是否受到病毒感染，还需要使用 IPsec、HTTPS 和其他应用程序来保护敏感信息。HTTPS 加密算法通常在计算机平台的软件上实现，而 IPsec 和虚拟专网 (VPN) 加密应用软件一般需要更高的性能，主要采用硬件加密。需要对网络 IT 设备进行评估以确保系统的整体可信度。

这种可信度必须针对每一 IT 组件进行硬件分析，通过验证，其信息安全保障级别符合通用标准或者联邦信息处理标准 (FIPS) 140-2 和 140-3。进行这种复杂的分析非常重要，如图 1 所示。由于需要进行全面的分析，这些系统的设计周期被大大延长了。

表 1. FIPS 140-2 安全需求总结

#	领域	安全级别 1	安全级别 2	安全级别 3	安全级别 4
1	加密模块规范	加密模块、加密边界、工作认证算法和认证模式等方面的规范 对加密模块的解释，包括所有硬件、软件和固件。 模块安全策略声明			
2	加密模块端口和接口	必须的和可选的接口 所有接口和所有输入输出数据通路的规范		未受保护的关键安全参数数据端口与其他数据端口逻辑分离	
3	任务、服务和认证	必须的与可选的任务和服务逻辑分离	基于任务或者基于身份的操作人员认证	基于身份的操作人员认证	
4	有限状态模型	有限状态模型规范 必须的状态和可选的状态 状态转换图和状态转换规范			
5	物理安全	产品级设备	锁定或者篡改证据	入口篡改探测和响应	EFP 和 EFT 表面篡改探测和响应
6	工作环境	单一操作人员 可执行代码 认证集成技术	在 EAL2 经过评估的参考 PP，规定了任意访问控制机制和审查。	在 EAL3 经过评估的参考 PP 和信任通路，以及安全策略模型。	在 EAL4 经过评估的参考 PP 以及信任通路。
7	密钥管理	密钥管理机制：随机数和密钥产生，密钥建立，密钥分配，密钥输入 / 输出，密钥存储和密钥归零。 使用人工方法建立的秘密和私有密钥可以通过纯文本格式输入输出。			
8	EMI/EMC	7 CFR FCC Part 15, Subpart B, Class A (商业应用) 适用于 PCC 要求 (用于无线电)。		7 CFR FCC Part 15, Subpart B, Class B (家用)	
9	自测试	上电测试：加密算法测试，软件 / 固件完整性测试，电路功能测试，状态测试。		按要求进行统计 RNG 测试	上电时进行统计 RNG 测试
10	设计安全保障	配置管理 (CM) 安全建立和产生 设计和策略响应 指南文档	CM 系统 安全分配 功能规范	高级语言实现	形式模型 详细解释 (形式检验) 预处理和后处理
-	防止其他攻击	防止其他攻击的规范，目前还没有可以衡量的需求。			

商业加密

金融业推动了商业加密技术和加密设备的发展。从开发安全的银行内和银行间电子数据交换 (EDI) 交易到公共自动取款机 (ATM)，直至电子商务高性能加密等金融业应用，都需要实现信息安全。

与军事应用对信息安全保障的需求相似，电子商务也需要通用标准对加密硬件进行设计和评估。金融业对加密互操作性的需求是这一市场的关键不同点。商务运作不受国界的限制，因此，必须针对这一市场所开发的设备进行加密。完善商业安全方案是国际军火交易条例 (ITAR) 中管制技术的加密分类要求。高性能电子商务加密设备主要是由服务器大生产商开发，例如 IBM 和 Sun，他们投入开发专业技术，通过较长的设计周期推出经过 FIPS 140-2 认证的加密模块。

高可靠性应用

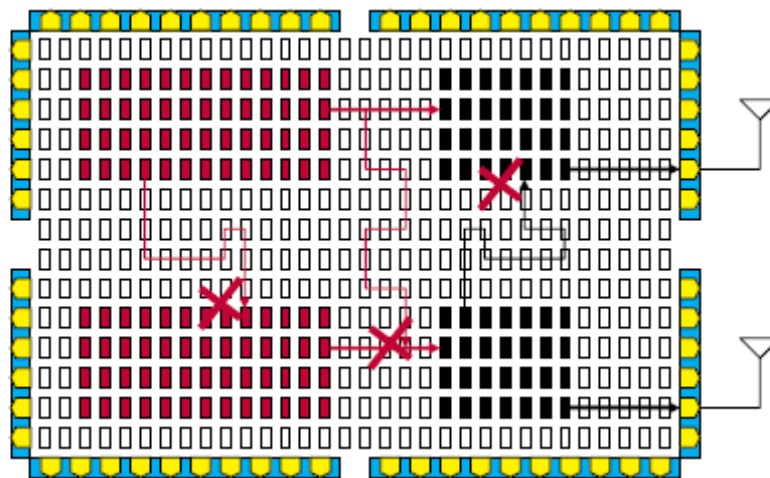
工业应用也采用了 Altera FPGA 支持的设计分离和独立特性。例如，汽车中越来越多的采用了嵌入式控制单元 (ECU)，而且比较复杂，功能越来越强。汽车行业竞争非常激烈，ECU 设计人员必须在提高可靠性的同时降低成本，减小体积。由于能够在单片 FPGA 中分离冗余逻辑，系统设计人员不但减少了硬件元件数量，而且实现了故障隔离。

设计分离解决方案

信息安全保障和高可靠性应用目前需要至少两个芯片来保证逻辑彼此分离，功能相互独立。这样可以确保一个器件中出现的故障不会影响设计的其他部分。在设计分离特性非常重要的应用中，例如，金融应用，必须对数据进行加密，由于故障导致出现意外的通路时，不能让数据从设计中的某一部分泄漏到其他部分。对于高可靠性非常重要的应用，例如，某一设备出现故障导致整条生产线关闭的工业系统，冗余电路会在一条电路出现故障时继续控制系统，尽量缩短停机时间。

通过 Quartus II 软件中的设计分离特性，设计人员能够保持一片 FPGA 中关键功能的彼此分离。使用 Altera 的 LogicLock™ 特性来建立分离，这样，设计人员将设计分区划分到器件中的某一特定区域。启动设计分离流程后，如图 2 所示，每一个安全分区都有自己的自动安全线，或者“隔离”区。通过这种方式，不允许把其他逻辑放在附近，从而提高了容错级别。

图 2. 在高可靠性和信息安全保障系统中实现设计分离



然而，为保证真正的分离，还必须将走线分开。因此，所有走线都限制在设计分区的 LogicLock 区域中。这意味着，隔离区中没有逻辑和走线，保证了器件中其他功能的物理隔离。这与使用两个物理器件来确保分离的效果完全一样。

Altera 不但设计了 Cyclone III LS 体系结构，而且还进行了严格的评估和优化，以最小的隔离区保证分离结果，容错能力更强，使设计人员能够在设计中使用 80% 以上的资源。设计分离流程还支持特殊的银行标准，关键设计分区架构中建立的分离区能够扩展到 I/O。Cyclone III LS 封装经过设计，支持这类 I/O 分离。

总结

高可靠性和信息安全保障系统之间有很多相似的设计需求。由于每一系统需要冗余来保证出现硬件故障时设计能够正常工作，因此，这两类系统都需要设计分离和独立功能。传统上，由于冗余是在电路板级实现的，因此，冗余会增大系统体积、重量、功耗和成本。为减小这些不利因素的影响，采用低功耗 FPGA 和安全保障设计流程来满足严格的 NSA FSDA 要求。

为确保设计分离和独立，作为 SoC 设计方法的一部分，可以将冗余逻辑从电路板级转到单片 FPGA 中。结合低功耗、高密度逻辑和设计分离特性，高可靠性、安全保障加密和工业系统开发人员使用可编程逻辑，降低了设计开发和进度风险，使用成熟可靠的渐进式编译设计流程，提高了效能。

详细信息

- Cyclone III FPGA——安全：
www.altera.com/products/devices/cyclone3/overview/security/cy3-security.html
- 网播：“划分 FPGA 设计，实现冗余和信息安全”：
www.altera.com/education/webcasts/all/wc-2009-partitioning-fpga-redundancy.html
- 资料：Cyclone III 器件：
www.altera.com/products/devices/cyclone3/literature/cy3-literature.jsp
- *AN 567: Quartus II 设计分离流程*：
www.altera.com/literature/an/an567.pdf
- *保护 FPGA 设计不受常见的入侵威胁*：
www.altera.com/literature/wp/wp-01111-anti-tamper.pdf
- Quartus II 订购版软件：
www.altera.com/products/software/quartus-ii/subscription-edition/qts-se-index.html

致谢

- Paul Quintana, 高级技术经理, 军用业务部, Altera 公司。
- Juwayriyah Hussain, 产品营销高级工程师, 低成本产品, Altera 公司。



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

版权 © 2009 Altera 公司。保留所有版权。Altera、可编程解决方案公司、程式化 Altera 标识、专用器件名称和所有其他专有商标或者服务标记，除非特别声明，均为 Altera 公司在美国和其他国家的商标和服务标记。所有其他产品或者服务名称的所有权属于其各自持有人。Altera 产品受美国和其他国家多种专利、未决应用、掩模著作权和版权的保护。Altera 保证当前规范下的半导体产品性能与 Altera 标准质保一致，但是保留对产品和服务在没有事先通知时的变更权利。除非与 Altera 公司的书面条款完全一致，否则 Altera 不承担由使用或者应用此处所述信息、产品或者服务导致的责任。Altera 建议客户在决定购买产品或者服务，以及确信任何公开信息之前，阅读 Altera 最新版的器件规范说明。