FPGA 技术在核安全级仪控系统中的应用探讨

Investigation on Application of FPGA Technology in Nuclear Safety-related I&C System

尹宝娟　毛从吉　张宓　黄伟杰

(环境保护部核与辐射安全中心,北京　100082)

摘　要：FPGA 技术因其具有集成度高等特点而得到了快速广泛的应用。在核电站仪控系统数字化升级改造过程中,FPGA 技术可否应用、如何应用已成为一项紧迫研究的重要课题。分析了 FPGA 的技术特点及其应用于核电站仪控系统中面临的挑战,提出了在使用标准、开发过程、设计技术和工具选用等方面可能的应对措施。最后,对 FPGA 在国内的后续应用进行了探讨。

关键词：IP 核　现场可编程门阵列　安全级仪控系统　软件开发过程　硬件描述语言

中图分类号：TP29　　**文献标志码**：A

Abstract: The technology of FPGA has been widely used because of its advantages of high integrity and etc. In upgrade and revamp of digitization for instrument and control systems in nuclear power station, applicable or not and how to apply of the FPGA technology become an urgent and important topic. The technical features of FPGA and the challenge it is facing in application of I&C systems of nuclear power station are analyzed, and the countermeasures in use of standards, development procedures, design technology and tools selection are proposed. Necessary technical exploration of FPGA subsequent applications in our country is also conducted.

Keywords: Intellectual property (IP) core　Field programmable gate array (FPGA)　Instrumentation and control (I&C) system in safety level　Software development process　Hardware description language (HDL)

0　引言

20 世纪 80 年代中期发展起来的现场可编程门阵列(field programmable gate array,FPGA),相比于早期的可编程逻辑器件 EPROM、PAL、GAL、PLD 等,具有集成度高、可反复编程、可兼容不同的开发软件等特点。因此,得到了广泛应用。随着计算机技术的发展,专业化的开发工具、仿真工具,丰富的开发语言以及可复用的 IP 使 FPGA 的分工更加细化。

FPGA 技术具有可靠性高、速度快、设计简化、能够降低设备复杂性和解决过时问题等方面的优势[1]。

本文以 FPGA 的技术特点分析为基础,对 FPGA 应用于核安全级仪控系统所面临的挑战及可能的应对措施进行了探讨。

1　FPGA 的技术特点

1.1　内部结构

FPGA 内部包括可配置逻辑模块 (configurable logic block,CLB)、输入输出模块 (input output block,IOB)和内部连线资源(inter connect)三个部分。CLB 构成了 FPGA 芯片可编程逻辑的核心部件,是实现用户功能的基本单元;IOB 用于 FPGA 芯片内部与外部信号之间的通信;内部连线资源包括各种长度的连线和一些可编程的连接开关,它们用于逻辑块之间、逻辑块与输入/输出块之间的连接。

1.2　开发过程和工作方式

FPGA 的基本开发流程包括功能定义、设计输入、功能仿真、综合优化、综合后仿真、布局布线、时序仿真、芯片编程与调试等步骤。在完成布局布线后,FPGA 完全是一个硬件系统。布局布线前的设计则是借助软件设计工具完成的软件开发过程,此时 FPGA 则应视为软件系统。因此,FPGA 应作为硬件和软件的综合体来对待,并使用特定的设计和评审指导[2]。基于 FPGA 技术实现的电路在物理上是并行工作的,电路行为的先后顺序需要通过时钟节拍的顺序来控制[1]。

1.3　开发语言

用于 FPGA 开发的硬件描述语言 HDL 是一种用形式化方法描述数字电路和系统的语言。利用这种语言,数字电路系统的设计可以从上层到下层(从抽象到具体)逐层描述自己的设计思想,采用一系列分层次的模块来表示极其复杂的数字系统。然后,利用电子设计自动化工具,进行综合、布局布线,逐层转换为

修改稿收到日期:2013-07-18。

第一作者尹宝娟(1979-),女,2004 年毕业于信息产业部电子六所计算机应用技术专业,获硕士学位,工程师;主要从事核电仪控系统软件验证与确认领域的技术研究以及核电站仪控电设备的技术审评工作。

需要实现的具体电路布线结构。开发过程可选用的语言包括 VHDL、Verilog HDL 等。

1.4　主要工艺

FPGA 的工艺结构包括 SRAM、反熔丝、Flash 三种形式。其中,当 SRAM 结构的器件上电时,要将配置数据读入片内 SRAM 中,配置完成就可进入工作状态;掉电后 SRAM 中的配置数据丢失,FPGA 内部逻辑关系随之消失。SRAM 结构的器件具有可重复编程、低功耗、可进行系统重构的特点。反熔丝结构的器件的逻辑功能定义由专用编程器根据设计实现所给出的数据文件,对其内部的反熔丝阵列进行烧录,从而使器件实现相应的逻辑功能。反熔丝结构的器件具有只能一次性编程、无需外部加载配置、进入工作状态速度快、保密性高、抗干扰性强、功耗低等特点。基于 Flash 结构的 FPGA 具备反复擦写和掉电后内容非易失特性,因而这种 FPGA 同时具备 SRAM 结构的灵活性和反融丝结构的可靠性,具有无需外部加载配置和低成本等特点。

1.5　IP 核

IP 核一般分为硬核、软核和固核三种。硬核是指经过预先布局且不能由系统设计者修改的功能单元模块;软核指利用 HDL 语言设计并经过综合验证的功能单元模块,通常以 HDL 语言形式提交;固核是指由 RTL 描述和可综合的网表组成的功能单元模块。IP 核能实现标准功能模块的可复用度,加快开发速度。

2　FPGA 应用于核电行业的挑战

FPGA 作为一项发展历史并不长的新技术,其应用于核电站的时间较短,尚处于探索阶段,在核电仪控系统中的应用面临诸多挑战。

2.1　标准的缺失

目前,2012 年新发布的 IEC 62566,作为业内唯一指导用于核电站安全重要仪控系统 A 类功能的 HDL 编程的集成电路开发的标准,它保持了与已有标准 IEC 61513、IEC 60880、IEC 60987 的一致性。该标准提出的要求包括:用于核电厂安全级 I&C 系统的 HDL 编程的器件按照严格、完整的生命周期过程进行开发,对各阶段采用的技术与成果输出进行 V&V,对开发和验证过程中使用的预开发组件和工具的选择进行指导。HDL 编程器件应满足与安全级软件相同的简单化与确定性要求[3]。

2010 年,美国核管会发布的报告 NUREG/CR-7006,是对基于 FPGA 开发的核电站安全级系统的评审指南。该报告提出了基于 FPGA 的核安全级系统开发生命周期过程和安全的设计行为应满足可靠性、健壮性、可追踪性、可维护性方面的建议与指导[2]。

2009 年发布的报告 EPRI/TR-1019181,是在对相关机构和人员开展调查、查阅资料的基础上完成的。该报告总结了 FPGA 技术应用于核安全级仪控系统的经验,可作为从业者的参考性资料[4]。

基于 EPRI/TR-1019181 和 IEC 62566 标准草稿,EPRI 于 2011 年发布了技术报告 EPRI/TR-1022983。该报告对基于 FPGA 的核安全级仪控系统的设计、开发、V&V、安全评价等方面提出了相关方法与设计原则建议[5]。

以上这些标准和报告显示了从业者对该领域持续高涨的关注与积极有益的探索成果,但还不足以对基于 FPGA 的核级仪控系统的开发、V&V、监管形成全面的指导与约束。

2.2　安全性论证方法的缺失

美国核管会报告 NUREG/CR-7006 提出了 FPGA 的设计行为应满足可靠性、健壮性、可追踪性、可维护性等方面的要求,并给出了相关建议。然而,该报告并非美国核管会的审评导则,不具有强制性;而以上行为建议也不是在整体安全性论证方法框架下形成的。因此,当前状况距离形成明确、可实施的指导方法还有很大的空间。

2.3　固有的技术难点

FPGA 技术应用于核安全级仪控系统需要解决以下难点。

① 原理图的验证

在 FPGA 开发语言中,除常用的几种硬件描述语言外,原理图因其良好的直观性与易学性,也常被设计者采用。如何对开发过程中的原理图进行验证缺少必要的指导。

② 开发工具的验证

在 FPGA 产品开发过程中,使用了多种 EDA 工具,包括芯片厂商提供的开发工具、第三方供应商提供的完整的产品线仿真验证工具等。其中,开发工具对最终产品产生直接影响,而此类工具功能复杂、灵活度高,其验证工作非常困难。

③ IP 核的验证

由于 IP 核以“黑盒子”的方式被用于产品开发,本身缺少透明度、不易于验证和维护,这与安全级软件的确定性要求不符。如何对这类广泛应用的模块进行有效验证是一项严峻挑战。

④ 大规模测试问题

FPGA 技术实现了大规模逻辑单元的高度集成化,可在单一芯片上实现相当复杂的功能。如按照传

统方法对具有输入数目很多的功能模块进行遍历测试,耗时相当长,因此,需要采用不同于传统的仿真验证技术手段,以便在缩短验证时间的同时实现 100% 的覆盖率。

2.4　有限的行业应用经验

FPGA 技术应用于核电站仪控系统是近些年才呈现的一种趋势。目前,世界范围内也出现了将该技术应用于核电站的停堆保护系统、安全专设系统及其他安全系统中的产品,主要包括:①日本三菱公司的 Meltac 平台,使用了带有 PowerPC 硬核的 FPGA,实现控制网络接口模块、总线主设备模块、电源接口模块等;②日本 Toshiba 公司开发的无 MCU 的 DCS 系统,应用于 South Texas Project Units 3 and 4;③芬兰的 Olkiluoto-3 电厂使用 FPGA 技术,完成自动硬接线后备系统,用于实现部分保护功能和负责处理某些设计基准事件的自动停堆功能;④乌克兰 RADIY 公司研制的基于 FPGA 的仪控平台,应用于 CANDU 核反应堆的控制系统及乌克兰核电站的保护、功率控制、专设安全系统。然而,仅有西屋下属公司 CSI 的 ALS 平台在 Wolf Creek MSFIS 升级中的部分应用内容通过美国核管会的审评。

3　可能的应对措施

3.1　标准方面

核行业内对安全重要仪控系统及其软硬件开发与应用有完善的法规标准指导,主要包括以下几个方面。

① 系统方面:IAEA NS-G-1.3(已转化为中国的核安全导则 HAD102/14)、NUREG0800、RG1.174、IEEE 7-4.3.2(已转化为中国的国家标准 GB/T 13629)、IEEE 603(已转化为中国的国家标准 GB/T 13284)、IEC 61513;

② 软件方面:IAEA NS-G-1.1(已转化为中国的核安全导则 HAD102/16)、IEC 60880(已转化为中国的能源标准 NB/T20054)、IEC 62138(已转化为中国的能源标准 NB/T20055)、IEEE 1012;

③ 硬件方面:IEC 60987。

以上这些标准提出了诸多方面的设计要求,包括防共因故障、单一故障、多样性、纵深防御、冗余、独立性、人机接口、质量保证、验证与确认、时间特性、诊断技术、环境鉴定等,基于 FPGA 技术实现的仪控系统同样应该遵循。

随着 FPGA 应用趋势日趋明显,设备厂商、独立研究机构、监管机构、行业标准委员会、FPGA 芯片供应商等应从自身角度促进该领域的立法与标准制定工作的落实。

3.2　安全性论证方法体系

航空航天业作为另一体系标准发展较成熟的安全行业,其广泛采用技术报告 DO254 中提及“自顶向下”的安全论证方法。该方法关注系统安全对硬件设计的要求与约束,并根据硬件故障对系统造成的影响进行安全分级,采用 FTA、共模分析、FMEA、统计可靠性分析、功能 FMEA 等方法,对随机故障进行定量分析、对硬件设计缺陷进行定性分析[6]。该方法可以在基于 FPGA 技术的产品开发过程中参考使用。

3.3　开发过程方面

基于 FPGA 的开发过程等同于软件开发的认识,其开发过程的每个阶段应严格按照核安全级软件开发过程标准要求,制定严格的软件开发、质量保证、配置管理、验证与确认、文档要求等方面的制度,有效提升 FPGA 产品开发过程与各阶段输出成果的质量。

3.4　设计技术与工具选用方面

针对设计技术与工具选用方面的问题,建议采取如下措施。

① 在项目规划阶段做好开发语言的选择,对原理图的使用加以适当限制或规避,并制定符合安全级软件要求的编程规范,以满足软件的确定性要求[7]。同时,在代码实现后选择不同于开发者的代码走查工具,进行所有代码的静态分析。

② IP 核的使用应尽可能加以限制。如在必须使用的情况下,需要对选用的 IP 核进行严格的验证与确认,可借鉴商品级软件的评价方法,对拟使用的 IP 核完成包括适用性、质量、使用经验等方面的评价。

③ 芯片厂商提供的 FPGA 开发工具均为复杂的商用平台产品,应参照商品级软件评价的方法对此类工具进行评价,并选用不同于开发者使用的仿真验证工具对每一阶段的输出成果进行充分的验证与确认。

④ 对于因大规模逻辑单元的使用带来的测试困难,可以通过设计之初采用分割大规模功能模块简化设计以及使用形式化等效性验证方法开展验证等手段解决。目前,独立的 EDA 工具厂商可提供等效性验证工具,验证人员在熟悉 FPGA 产品设计的同时,需要具备等效性验证理论与编程方面的能力。

⑤ FPGA 所具有的硬件特性问题,包括时钟信号偏移、亚稳态、毛刺、电压降、单颗粒翻转等,需要在设计过程中采取特定的设计措施与故障监测手段加以解决,并固化良好的设计行为;同时在验证与确认过程中进行重点分析与测试。

(下转第 58 页)