文章编号:1671-4598(2014)09-3001-03 中图分类号:TP3 文献标识码:A

反应堆保护系统 AC160 平台商品级物项适用性确认过程的探讨

刘培扬,杨 洋
(国核自仪系统工程有限公司,上海 200000)

摘要:用于核安全场合的设备传统做法是从核级供应商采购模拟设备或数字化设备,美国核电业界在合格核级供应商数量不断减少的情况下,逐步开始使用商品级物项适用性确认方法(CGD),把成熟商品级产品用于核安全领域;商品级数字化仪控设备因内嵌软件,CGD 方法与传统模拟设备略有不同,软件的 CGD 包括评审开发过程的软件配置项控制、验证和确认活动以及测试活动等要求;文章综述了美国核法规规定的核安全设备的相关要求和 NRC 对于数字化设备 CGD 的接受方法和准则,并重点介绍 AP1000 保护系统 AC 160 平台的 CGD 实施过程和方法,有助于国内数字化仪控设备供应商的 CGD 工作的开展。

关键词:商品级物项适用性确认;关键特性;AC160

Discussion of Reactor AP1000 Protection System AC160 Platform Commercial Grade Dedication Process

Liu Peiyang, Yang Yang
(State Nuclear Power Automation System Engineering Company, Shanghai 200000, China)

Abstract: Generally, the analog and digital equipments used in safety- related application in nuclear plant should be procured from qualified supplier that maintained a 10CFR50, Appendix B. Because of a decrease in the number of qualified nuclear-grade vendors, numerous licensees employ commercial grade dedication method to dedicate commercial grade item for use in safety-related application. For digital I&C equipment, dedication of built-in software has some different from analog. The main works including review of software configuration control, verification and validation activity and test activity, etc, to assure the quality of the software. The paper introduces the requirements of USA nuclear law, and NRC's approved acceptance method and process for digital I&C commercial dedication. The Paper focuses on describing the CGD process and acceptance method of AP1000 protection system AC160 platform. It's helpful for future dedication of digital I&C equipments by civil vendor.

Keywords: commercial grade dedication; critical characteristics; AC160

0 引言

由于核电厂仪控系统设备的老化,以及维护成本的增加,业主需要逐步更换或者改造现有设备,此时数字化技术已经逐渐成熟,设备的性能和可靠性已大幅提高,数字设备的费用、灵活性等优势凸显,所以业主在升级改造过程中更倾向于使用数字化设备。

另一方面,由于核安全领域产品的开发非常严格,美国三里岛核电事故后,美国核电发展进入历史冰冻期,NRC 未再审批过新的核电站。采购订单的减少导致越来越多供应商不再维持核级质保大纲,放弃核级设备供应商资质。至 2005 年,美国国内合格的核级设备供应商减少了约 80%,供应商数量的大幅减少,同时供应商产品研发进程的减缓,导致提供的核级产品功能灵活性很有限,而且价格昂贵。

数字化仪控设备在传统工业领域已得到广泛的使用,一些成熟产品已在石油、化工等充分证明其安全性、可靠性和稳定性,但是由于软件不同于传统硬件的特点,存在软件共模故障等风险,核安全法规和标准对软件产品的开发、集成等过程提出了非常严格的要求,如何对现有成熟的控制系统进行鉴定,充分论证商品级控制系统与在核质保体系下开发的控制系统具有同等性能,完全能够在极限环境条件下完成所需的安全功能,这个问题已成为我国数字化仪控设备在核电厂安全仪控系统中推广应用的关键问题之一。

收稿日期:2014-03-17; **修回日期**:2014-04-17。

作者简介:刘培扬(1982-),硕士,工程师,主要从事控制理论与控制工程,反应堆保护系统工程应用方向的研究。

1 美国法规、标准要求

1.1 法规要求

美国核联邦法规 10CFR50 附录 B 确定了保证安全级物项质量的系统性要求,虽然没有明确提出商品级物项的问题,但是附录中的 III 和 VII 部分建立了相应的控制以保证采购物项的质量,这些控制同样适用于安全领域使用的商品级物项,法规中提出的可用方法包括:1)源地评估和选择;2)供应商提供的客观质量证明;3)供应商检查;4)交货产品检查。

10CFR21《缺陷和不符合报告》明确了 Dedication 定义,提出它是将商品级物项用于安全领域的鉴定过程,经过鉴定后,能够提供证据证明商品级物项与在核质保体系下制造的设

备具备同等性能，能够执行其安全功能。法规要求用于安全相关的商品级物项仍然按照采购方的 10CFR50 附录 B 质量保证大纲进行处理。

1.2 NRC 的立场

1989 年，NRC 发布通用信函 GL 89－02[1]，指出 NRC 有条件采纳 EPRI NP－5652[2] 提出的用于接受商品级物项的 4 种方法，即：

(1) 特殊测试和检查；

(2) 供应商商业级调查；

(3) 源地验证；

(4) 可接受的供应商的业绩报告。

NRC 认可在 CGD 过程中使用一种或多种方法作为接受商品级物项的依据，但是对方法 (2) 和方法 (4) 的单独使用进行相应限制，如果要单独使用这两个方法作为验收基本部件，需要满足相关要求。

1993 年，NRC 发布检查程序 IP38703[3]，程序中对于 CGD 提出一些重要的原则，包括关键特性的选择和验证、追溯性、采样、商业级调查、合格材料报告及合格证等。

1996 年，劳伦斯利弗莫尔国家实验室发布 NUREG/CR－6421[4]，该标准结合 IEEE，ANSI/ANS，IEC 等相关标准的验收准则，列出数字化系统的关键特性的评估方法，同时也为安全相关应用的现有软件的测试提供指导，该标准被 NRC SRP (STANDARD REVIEW PLAN) 第七章作为参考，作为数字化设备执行 CGD 的附件导则。

1997 年，NRC 采纳 EPRI TR－106439[5] 的方法，认可它作为商品级软件鉴定的指导准则，TR－106439 针对如何验证数字化商品级仪控设备的软硬件关键特性，提出了一系列的方法和验收准则。

BTP－14[6] 指出“应该对智能仪表、断路器或者报警器模块中所包含的商品级软件进行评价，以确定其能够满足所要求的各项特性。EPRI TR－106439 给出了执行这种评价的一种可接受方法。NUREG/CR－6421 提供了更为详细的关于商品级软件鉴定方面的信息”。

2 AC160 平台 CGD 过程

AP1000 反应堆保护系统平台为 Common Q 系统，该系统的核心控制部件是 ABB 公司开发生产的 AC160 序列产品，该产品已在传统工业领域广泛使用，具有高可靠性和良好的运行经验反馈。但是该产品并不是在核质保体系下开发、制造的，不能直接应用于核安全领域，根据法规、标准相关要求，必须经过 CGD 才能将其用于核安全相关领域。

商品级物项的 CGD 应由业主或者被委任负有验收责任的供应商来进行，但不管由谁来负责验收，负责验收商品级物项的组织对商品级物项的验收必须在 10CFR50 附录 B 大纲下进行。西屋公司满足 10 CFR 50 附录 B 质保体系要求，具有核级产品制造和 CGD 资质，是 AP1000 Common Q 系统的 CGD 机构。

2.1 CGD 总体流程

根据 EPRI NP－5652，商品级物项 CGD 过程包括两部分，即技术评估过程和验收过程，如图 1 所示。技术评估过程是为了确定设备的安全功能，明确物项的关键特性、验收准则和采用的验收方法，并采购要求文件明确相关技术指标和质量要求；验收过程是为了确保所接收的商品级物项能满足采购文件的要求，验收过程共有四种方法可供选择使用。

第一步，对物项进行评估，确定设备安全相关功能；

第二步，确定是否需要采购商业级物项，如果有合适的核级供应商，可以直接采购该核级产品；

第三步，确定适当的技术和质量要求，基于物项的性能或者设计基准，确定重要的特性和属性，识别出关键特性，通过验证该关键特性，就可接受该商品级物项。关键特性的选择、数量基于该设备的安全功能、应用要求、故障分析报告、性能要求，抗震和环境鉴定应作为关键特性进行验证；

第四步，选择合适的接受方法，验证关键特性。

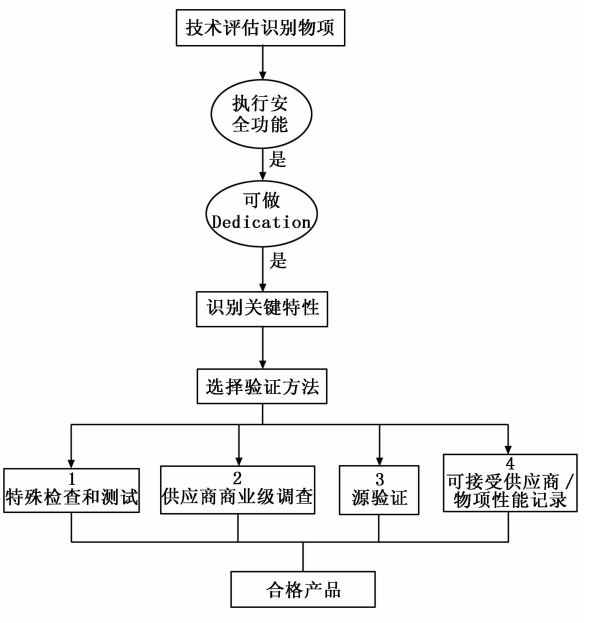

图 1 CGD 流程

2.2 AC160 CGD 采用的验收方法[7]

西屋公司对 AC160 平台进行技术评估，制定鉴定导则 (commercial dedication instruction，CDI)，CDI 中明确描述了设备的标识、安全相关功能、抗震要求、所识别的关键特性及其验证方法等，该导则用于指导 CGD 整个过程。

西屋在 CGD 过程中结合特殊检查和试验、供应商调查、供应商/产品记录评估 3 种方法对 AC160 平台进行鉴定。

3.2.1 特殊检查和试验

西屋公司与瑞典 ABB 公司签订了有关 AC160 硬件和软件部件供应协议，确定文件要求和配置控制信息，ABB 公司按照要求在数据库中对配置信息进行维护，模块和组件都经西屋的来料接收检查，所有相关 AC160 设备的印刷电路版 (PCB) 都用数码照片记录，可显示所有部件的物理位置和标识，只能使用合格的供应商的合格部件清单中确定的部件。在接收产品时，对软件版本号、硬件设备编码进行确认。

同时西屋公司对 AC160 组成的 Common Q 系统进行 EQ 鉴定，使用两组样机进行 EMI/RFI 测试、环境测试和抗震测试，其中一组用于 RMI/RFI 测试，一组用于其它所有测试，对于 EMI/RFI 测试，该组样机模拟平台系统可能面对最严酷环境条件；另一组样机模拟预期的负荷条件进行测试。测试依据 IEEE Std 323 和 EPRI TR－102323 执行。

3.2.2　供应商调查

西屋调查组在瑞典 ABB 自动化产品工厂开展调查，调查时，根据 CGD 计划的要求和安排，与质保人员及工程师进行沟通交流，并审核系统软件开发生命周期每个阶段的文档。

西屋根据调查结果，最终形成《设计和生命周期评估报告》，该报告涵盖：产品描述；功能要求；设计要求；软件开发；硬件/软件集成；确认（测试）；用户文件；维护。报告对软件生命周期的系统要求、开发方法、测试程序、配置项管理、维护程序及文档进行充分评估，通过调查评估确认 ABB 自动化产品开发过程总体满足相关要求。

IEEE Std 7－4.3.2 没有强制要求 ABB 软件开发工具进行 V&V，只要使用该软件开发的最终产品进行了 V&V，因为西屋在保护系统软件编程手册中规定了应用软件的 V&V 和测试大纲，此过程能够发现由开发工具引起的缺陷，西屋排除了 CGD 过程中软件开发工具的 V&V 要求。

3.2.3　供应商/产品记录评估

西屋根据产品运行历史记录和运行经验反馈，形成了《总体运行历史评估报告》，该报告了覆盖下述范围：产品发布历史评估（包括 AC160 产品的前身 AC110 的历史）；从最初发布开始的所有硬件和软件问题，和解决时间；错误通告程序；变更通告程序。

NRC 已审核并接受了 AC160 硬件和软件的 CGD 报告，认可该平台可用于核安全系统，AC160 PLC 系统满足 BTP HICB－18[8] 的要求，CGD 过程遵循 EPRI TR－106439 导则。

3　结束语

反应堆保护系统属于安全级的仪控系统，系统的设计、制造应满足核监管部门的要求。当前主流的的核级仪控系统，包括英维思的 Tricon 系统、阿海珐能源集团的 TXS、三菱 MLETAC，都是由具有核级设计、制造资质的单位进行开发的，设计、制造过程严格执行核级设备的相关要求，确保了系统的安全性、高可靠性和设计全过程资料的完整性。

在 AP1000 项目中，西屋采取了不同于阿海珐、三菱、英维思的主流做法，选择市场上安全、可靠、运行经验好的商品级仪控系统，使用 CGD 方法，依靠自身长期积累的设计、制造实力，结合 NRC 的相关要求，完善 ABB 公司 AC160 产品的相关资料，并对一些功能进行限制，同时对部分产品提出新的需求，进行升级改造，在保证产品高可靠性、安全性的同时，有效的降低了研发成本。

在国内，HAD 102/16 是基于安全重要系统的软件的生存周期各个阶段，为安全论证提供收集证据和编制文件的指导。导则附录 1 专门针对已有软件的使用和确认提出相关要求和建议，提到对于按其他工业安全关键应用中的高标准开发的软件，可在核工业中使用，但该软件应经受与新开发的应用软件的最终产品同样的评定（分析和审查），如果需要，应实施反演法以评价已有软件的全部规格说明。如果得不到足够的相关软件开发信息，应进行软件故障对安全影响的分析（风险评价），特别注意可能发生在已有软件和（或）其他软件部件接口级别上的边界效应和故障。

GB/T 13629－2008，5.4.2 节阐述了商品级物项适用性确认（CGD）方法的总体活动，提出在那些传统的鉴定过程不适用的情况下，为验证一个设备可用于安全应用的一种替代方法是 CGD，CGD 的目的是验证被确认过的物项在质量上与按照 HAF 003 的设备是相当的。

虽然我国目前已在核安全导则以及相关国标中提出了 CGD 概念，但是还未形成完善、可实施的方法和程序。对于 CGD 的实施具体方法、程序和验收准则，包括审查的方法和准则，都是下一步研究的重要问题。

参考文献：

[1] GENERIC LETTER 89－02，Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products [Z]. NRC，1989.

[2] EPRl NP－5652，Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications [Z]. Electric Power Research Institute，1988.

[3] IP38703，Commercial Grade Dedication [Z]. NRC，1996.

[4] NUREG/CR－6421，A Proposed Acceptance Process for Commercial Off－the－Shelf（COTS）Software in Reactor Applications [Z]. Electric Power Research Institute，1996.

[5] EPRl TR－106439，Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications [Z]. Electric Power Research Institute，1996.

[6] NUREG 0800，Chapter 7，Appendix 7－A，Branch Technical Position HICB－14. Guidance on Software Reviews for Digital Computer－based Instrumentation and Control System [Z]. USA. NRC，2007.

[7] WCAP－16097－NP－A. Common Qualified Platform Topical Report [R]. Westing house，2003.

[8] NUREG 0800，Chapter 7，Appendix 7－A，Branch Technical Position HICB－18. Guidance on the Use of Programmable Logic Controllers in Digital Computer－Based Instrumentation and Control Systems [Z]. USA. NRC，1997.