核电站数字化仪控系统软件验证和确认

实用手册

杨永祥　丁　军　著

厦门大学出版社
XIAMEN UNIVERSITY PRESS

核电站数字化仪控系统软件验证和确认实用手册

杨永祥　丁　军　著

厦门大学出版社
XIAMEN UNIVERSITY PRESS

图书在版编目(CIP)数据

核电站数字化仪控系统软件验证和确认实用手册/杨永祥，丁军著. —厦门：厦门大学出版社，2010.5
ISBN 978-7-5615-3509-7

Ⅰ.核… Ⅱ.①杨…②丁… Ⅲ.核电站-自动化仪表-控制系统-系统软件-技术手册 Ⅳ.TM623-62

中国版本图书馆 CIP 数据核字(2010)第 070032 号

厦门大学出版社出版发行
(地址：厦门市软件园二期望海路 39 号 邮编：361008)
http://www.xmupress.com
xmup @ public.xm.fj.cn
厦门市金凯龙印刷有限公司印刷
2010 年 5 月第 1 版 2010 年 5 月第 1 次印刷
开本：787×1092 1/16
印张：6 字数：100 千字
定价：79.00 元
本书如有印装质量问题请直接寄承印厂调换

致谢

厦门大学能源研究院缪惠芳在成书过程中花费了大量的精力校对、绘制图表；厦门大学能源研究院郑剑香、美国宾州州立大学博士研究生史亮和上海交通大学博士研究生叶成进行了校读，并提供了有益的意见；厦门大学能源研究院李宁教授一直支持本书的写作与进展。在此笔者对他们表示衷心的感谢。

在本书的写作过程中，得到上海核工程研究设计院郑明光博士的关心，他于百忙之中为本书写序，我们非常感谢他的支持。

最后要感谢我们的家人，如果没有他们的支持和理解，我们的工作是不可能完成的。

本书是在福建省科技厅平台项目——海西工业技术研究院核能工程技术中心核电数字化仪控技术研发平台信息管理系统(项目编号：NO. 2007H2002）资助下完成的。

序言

1985年3月，由上海核工程研究设计院设计的秦山一期核电站开工建设。1991年12月首次并网发电，1994年4月正式投入商业运行，中国核电实现了“零”的突破。截至2009年，我国已建成浙江秦山、广东大亚湾、江苏田湾三大核电基地，共有11台机组在运行，总装机容量为910万千瓦，核发电量所占份额约为2.2%，在有核电能力国家中仅高于印度和巴基斯坦。

核电对发展清洁能源、低碳经济以及应对全球气候变化的重大意义已经被世界各国所公认，中国政府也越来越重视核电的发展。2007年11月，国务院批准了《核电中长期发展规划（2005—2020年）》，提出到2020年核电装机容量占全部的4%，达到4 000万千瓦，但是根据中国目前的核电发展状况，这一目标可能会得到大幅提高。

要实现核电的快速发展，中国面临严重挑战：人才、技术贮备不足，教育、培训、能力建设任务重。核电产业是一个综合行业，为

此为试读，需要完整PDF请访问：www.ertongbook.com

满足核电体系的运转需要大量的有用人才，包括采矿、化工、冶炼、研发、设计、审评、制造、施工、调试、运行、维护、退役、综合管理与各级监管。人才是核电产业的第一资源，但人才培养有过程，需要前瞻，同时我们必须有序推进产业发展，掌控核电发展风险，避免产业动荡，大起大落，对核电人才负责。

核电需要核安全文化、责任感，到目前为止，大的核电事故都是人因引起的。在 1973 年第一次石油危机后，油价暴涨，极大地推动了世界核电事业的发展，核电的快速发展使当时核电技术储备不足和核安全文化薄弱的问题暴露无遗，各地核电厂事故频发，甚至发生了 1979 年的三哩岛事故和 1986 年的切尔诺贝利事故。为了保障核电的安全，各核电国家开始纷纷建立核安全与管理监督机构，加强核安全文化建设，并逐渐完善纵深防御的设计理念。

为防止核电站事故，核电采用的纵深防御措施的设计理念包括五个层次：

1. 防止偏离正常运行及防止系统失效。（控制系统）

2. 检测和纠正偏离正常运行状态，以防止预计运行事件升级为事故工况。（保护系统）

3. 防止某些尽管极少可能的预计运行或假设始发事件升级（仍有可能未被前一层次防御所制止）而发展成一种较严重的事件。（防御 DBA 的专设安全设施）

4. 针对可能已超过设计基准的严重事故，并保证放射性释放尽实际可能的低。（严重事故预防与缓解措施）

5. 最后层次防御的目的是减轻可能由事故工况引起潜在的放射性物质释放造成的放射性后果。（厂内外应急）

核电站数字化仪控系统是第一层次中的关键技术，核电站数字化仪控系统软件验证和确认又是实现核电站数字化仪控系统的关键。本手册的出版，为推进我国的核电数字化仪控技术的进步和人才培养做出了有益的尝试。

数字化仪控系统是核电站的中枢神经系统，相对于模拟仪控系统，它需要额外的设计和验证，两者之间主要的差别在于软件。为了达到对软件质量的高可信度，必须采用严格的技术规范和设计开发手段以保证一个高质量的软件工程开发进程。作为软件质量保证的一部分，严格的软件验证和确认（V&V）手段应贯穿软件生存周期的全过程。V&V 方法包括设计审查、检查、演练、可追踪性分析、软件危害性分析、安全评估、软件确认测试和系统测试，开发活动生存周期中每一阶段的 V&V 进程、活动及任务决定了 V&V 工程师的工作流程。为了确保对开发小组结果检查的客观性，V&V 必须从技术、财务和管理上与开发小组保持独立。为了提高效率，V&V 活动必须和开发活动同步进行。

该手册提供了一个实用的 V&V 方法，指导 V&V 活动的参与者如何计划安排 V&V、实施 V&V 和最终递交 V&V 报告以实现核电站数字化仪控系统软件的高可信度。这个方法在 Areva 公司的应用实践下被证明是卓有成效的。

作者杨永祥博士是 Areva 美国公司核电站仪控验证和确认部经

理，有着20年的数字化仪控的经验。他组建了Areva V&V团队，并帮助Areva在美国Oconee电站实现了近年来第一座被NRC认证通过的核安全级数字化仪控保护系统和安全专设系统。他还是IEEE1012标准的起草者之一。丁军博士原为上海核工程研究设计院仪控室的工程师，去美国后一直从事核电站智能监测和数字化仪控系统的研究。这两位作者合作的这本实用手册思路清楚，可操作性强，是该领域一本不可多得的参考手册，我也期待着他们能够继续提供更详尽的培训教材，让我们一起努力为中国核电事业贡献力量。

国家核电上海核工程研究设计院院长

郑明光 博士

Software Verification and Validation Handbook for Digital I&C System in Nuclear Power Plant

Digital I&C systems, the nervous systems of a nuclear power plant, require additional design and qualification approaches above and beyond analog I&C systems. The major differentiator between the digital I&C systems and the analog I&C systems is the software. To obtain high confidence in the software quality, a high quality software development engineering process is necessary that incorporates disciplined specification and implementation of design requirements. As part of high quality engineering assurance, rigorous software Verification and Validation (V&V) life cycle methodologies are necessary.

Lifecycle methodologies are compliant with the IEEE Standard 1012-1998, which states that V&V is the process of determining whether:

(1) Requirements for a system or component are complete and correct.

(2) Products of each development phase fulfill the requirements or conditions imposed by the previous phase.

(3) Final systems or components comply with specified requirements and their intended use.

To ensure the objectivity and obtain high confidence in examining the design output generated by the development organization, the V&V organizational independence from the development organization must be assured technically, financially, and managerially. The V&V methodologies include design review, inspection, walkthrough, requirement traceability analysis, software criticality analysis, security assessment, software component and integration testing, system integration and system testing, and acceptance testing. The V&V process, activities, and tasks in each phase of the development life cycle dictate the V&V engineers work flow. To be efficient, V&V activities must be in sync with the development organization.

This handbook provides a practical guidance for the V&V practitioners to plan the V&V, execute the V&V, and generate V&V results that aim at reaching high quality and high confidence in the software of digital I&C systems used in nuclear power plants.

缩略语

10CFR50	美国联邦法规第十章
BTP7-14	技术分支 7-14
IEEE	国际电工委员会
NRC	美国核管会
NUREG	美国标准审查计划
RG	核管会导则
SAD	硬件和软件体系架构描述
SCMP	软件配置管理计划
SDD	软件设计文档
SDP	软件开发计划
SDS	软件设计规范书
SIL	软件安全等级
SInstP	软件安装计划
SIntP	软件集成计划
SMaintP	软件维护计划
SMP	软件管理计划
SOP	软件操作计划
SQAP	软件质量保证计划
SRS	软件需求规范书
SSP	软件安全计划
STP	软件测试计划
STrngP	软件培训计划
SVVP	软件验证和确认计划
SyRS	系统规范书
V&V	验证和确认

此为试读,需要完整PDF请访问: www.ertongbook.com

content 目 录

第一章

绪 论

仪控系统监测核电站的安全与运行状况，并帮助调整应对核电站运行和维护的需要。因而，仪控系统可以说是核电站的神经系统。

较之模拟仪控系统，基于计算机和微处理器的数字化仪控系统能提供更高的可靠性、更好的设备性能及更多的诊断功能。因此，模拟系统将逐渐被淘汰。而且，目前，全世界约 40% 的运行反应堆已全部更新或包含部分数字化仪控系统。目前在建的核电站或将兴建的核电站都准备使用数字化仪控系统。

数字化仪控系统有三个特点：

首先，数字化仪控系统的组成部分间有更多的联系，比其前身的模拟系统更复杂。

其次，数字化仪控系统更依赖于软件。

第三，数字化仪控系统整体上对计算机的依赖，进一步强调了网络安全的重要性。

为了达到数字化仪控系统，尤其是软件的高可信度，规范的要求和设计实施是必需的。在软件开发过程中，要求采用严格的贯穿生存周期的验证和确认（V&V）方法。

本手册将提供一个实用的 V&V 方法，指导 V&V 活动的参与者如何计划安排 V&V、实施 V&V 和最终递交 V&V 报告以实现核电站数字化仪控系统软件的高可信度。

1.1 进行软件 V&V 的必要性

数字化仪控系统需要有超出模拟仪控系统额外设计和评测办法。数字系统和模拟系统之间的主要差别是软件。为了获得高可信度的软件，优质并且符合严格标准规范和满足设计要求的软件工程开发程序是必要的。只有严格执行贯穿生存周期过程的 V&V 方法才能保证软件工程的高质量。

生存周期方法符合 IEEE 1012-1998 标准 [1]，其中规定 V&V 是为了决定：

(1) 对系统或组件的要求是完整和准确的；

(2) 每一个开发阶段的产品都满足前一阶段的要求或条件；

(3) 最终的系统或组件符合规定的要求及用途。

为了确保对开发小组结果检查的客观性，V&V 小组必须从技术、财务和管理上与开发小组保持独立。V&V 方法包括设计审查、检查、演练、要求可追踪性分析、软件危害性分析、安全评估、软件确认测试和系统测试。在开发活动生存周期中每一阶段的 V&V 进程、活动及任务，决定了 V&V 工程师的工作流程。为了提高效率，V&V 活动必须和开发活动同步进行。

1.2 V&V 导则(美国监管导则，IEEE Std 1012)

V&V 的目的是为了开发高质量的软件。安全性和可靠性是核级仪控系统最终的考虑因素。因此，这个目标是非常符合其设计规范的。核工业是一个高度管制的行业。所以，当务之急是要使核级仪控系统的 V&V 符合监管部门的要求。

如第二章所述，IEEE1012-1998 标准中给出的软件生存周期的 V&V 方法符合 10CFR50 附录 B [2] 的要求。

美国标准审查计划 NUREG-0800 给出了仪控系统审查的原则。

NUREG-0800 的技术分支 BTP 7-14 [3] 表明对于软件生存周期过程，美国核管会导则 RG 1.173 [4] 支持 IEEE 1074-1995 [5] 标准。另外，关于软件 V&V，导则 RG 1.168 [6] 支持 IEEE 1012-1998 标准。BTP 7-14 还在 RG 1.168 中指出软件评审和审计的标准。

第二章给出了关于软件 V&V 的美国核管会导则和相应 IEEE 标准一一对应的层次关系。

1.3 V&V 概述

详细的计划是 V&V 活动的开端。第六章提供了计划 V&V 活动的概述。为了实行该计划，需要有一个仔细规划的 V&V 机构。非常重要的是，一个独立的 V&V 机构对安全级软件的 V&V 活动是非常必需的，只有这样才能达到客观性并保证高质量软件。事实上，美国核管会要求安全级软件的 V&V 必须由技术、财务及管理上和开发小组独立的 V&V 小组完成。

除了这个独立性要求以外，V&V 小组成员的人数和技能要与开发小组相当。

如果 V&V 小组人员大大少于设计小组的人员，要么他们不能完成所有应该完成的任务，要么 V&V 的工作会落后。V&V 组成人员

需要完整PDF请访问：www.ertongbook.com