核安全级软件验证与确认独立性探讨

Discussion of the Independence of Software Verification and Validation

毛从吉　郑睿鹏　李世欣　尹宝娟
(环境保护部核与辐射安全中心,北京　100082)

摘　要：当前法律和法规规定,对核电厂安全系统使用的核安全级数字设备必须进行鉴定。软件验证与确认是核安全级软件通过鉴定的关键环节,软件验证与确认必须具备独立性的特征。对于核安全级软件验证与确认如何满足当前核安全监管要求的研究,是软件厂商和监管当局共同关注的主要问题之一。核安全级软件验证与确认独立性要求的明确,有利于开发成本的控制和监管的规范化,从管理方面为保证核安全级数字设备安全水平打好基础。

关键词：核设施　核安全级　验证与确认　独立性　可确定性
中图分类号：TP29　　**文献标志码**：A

Abstract: According to the current laws and regulations, appraisal must be taken for nuclear safety digital devices applied in safety system of nuclear power plant. Verification and validation (V&V) of software is one of the critical aspects of appraisal for nuclear safety software. The V&V of software must have the characteristics of independence. The research on how to meet nuclear safety regulatory requirements for software V&V is one of the major issues to be commonly concerned by software manufacturers and regulatory authorities. Clarification of requirement for independency is useful for development and regulation, and also makes a good foundation to ensure safety level on Class 1E equipments.

Keywords: Nuclear facilities　Nuclear security level　Verification and validation (V&V)　Independence　Determinability

0　引言

目前,核电厂以及其他核设施已经普遍采用数字化仪表和控制平台。随着国内核安全电气设备的技术和工业的发展,越来越多的生产厂商开始在其产品中引进软件。按照国务院发布的第 500 号令规定[1]和相关释义[2],中国核安全电气设备监管采用许可证管理制度,软件作为数字化核安全电气设备的组成部分,是技术审评中的重中之重,软件验证与确认的独立性是技术审评中一个重要方面。

核安全法规 HAF102 5.5.1 章节指出"必须采用设备鉴定的程序来确认安全重要物项能够在其整个设计运行寿期内满足处于需要起作用时的环境条件(如振动、温度、压力、喷射流冲击、电磁干扰、辐照、湿度或这些因素的任何可能组合)下执行其安全功能的要求"[3],核安全监管当局对核安全级设备提出了必须进行质量鉴定的要求。对基于计算机的系统在保护系统中的应用,核安全法规 HAF 102 6.4.8(3)指出"为了确认基于计算机的系统可靠性的可信度,必须由独立于设计者和供应商的专家对基于计算机的系统进行评价"[3],对基于计算机的系统评价提出了要求。核安全法规 HAD 102-16 中第3.4.5.1章节进一步明确了对安全系统应采用第三方评定"[4]的相关要求。为了贯彻加强核安全监管的要求,结合软件验证与确认实际活动,本文对如何满足相关要求进行了探讨。

1　定义与内涵

核安全级软件验证与确认内涵包括核安全级软件和验证与确认两部分内容。核安全级软件是从核安全角度定义的一个名称,指的是执行核安全功能的数字化设备的软件部分。相对于普通软件,核安全级软件的一个显著设计特征是它的可确定性[5]。软件验证与确认指的是在系统生存周期内保证一个阶段能够满足前一阶段所提需求的过程(验证)和为保证集成后的计算机系统(硬件和软件)符合功能、特性和接口需求,对其进行测试和评价的过程(确认)。

2　独立性分析

2.1　独立性法规要求

核安全级软件验证与确认的独立性指的是开发人员和软件验证与确认队伍之间的独立程度。

对于核安全级软件验证与确认独立性,通常从技

修改稿收到日期:2013-07-22。

第一作者毛从吉(1971-),男,1994 年毕业于哈尔滨工业大学电气自动化专业,获学士学位,高级工程师;主要从事核电厂仪表和控制、民用核安全设备以及人因工程方面的研究。

术、管理和财务方面进行描述。具体独立性要求如下。①技术独立性:工作应由不同的人员使用不同的技术和工具完成。②管理独立性:工作应由不同的人员来领导和推动;验证与确认工作组与开发工作组应有不同的管理渠道,应记录独立小组之间的正式通信。③财务独立性:应有分开的财务预算,以限制资金在开发和验证与确认之间流动。

以上为原则性要求,具体如何在核安全级软件验证与确认活动中要求和评价,法律法规中并没有给出详细的指导书。

2.2　独立性形式和影响

核安全级软件验证与确认的执行方式通常可以分为两种情形:①软件验证与确认,由具备独立法人的单位承担(外部);②软件验证与确认队伍和软件开发队伍同属一个独立法人(内部)。

按照法规要求,对基于计算机的整个系统进行评价必须由第三方进行评价,但对于核安全级软件验证与确认并没有明确必须由第三方进行评价。

如果软件开发单位(或核安全设备供应单位)的核安全级软件验证与确认活动只由具有独立法人的单位承担,即在第一种情形下,则会产生以下问题:外部接口比较复杂、手续繁杂,即使是理想情况下,软件交付周期也较长;由于软件设计过程中不可避免会出现不符合项,验证与确认活动出现多次反复,导致工程处于失控状态;需要解决商业保密问题,验证与确认队伍肯定会接触源代码。

在第一种情形下,软件开发单位(或核安全设备供应单位)的核安全级软件具有以下优势:由于独立性高,一方面可以提高采购单位对软件可靠性的信心度;另一方面可以增强安全审评单位对软件可靠性的信心度,缩短审批时间。

核安全级软件验证与确认影响涉及工程使用(采购单位)和安全审评单位(安全审评)。如果软件开发单位(或核安全设备供应单位)的核安全级软件验证与确认活动在第二种情形下,则会产生以下问题:工程单位采购时,通常会认为软件开发独立性不够高、产品可信度不够,拒绝采购;安全审评单位在没有提前介入时,也可能出现由于独立性程度不够导致审评人员信心降低,从而难以获得批准或者导致获批时间很长。

在第二种情形下,软件开发单位(或核安全设备供应单位)的核安全级软件具有以下优势:由于源代码不会泄露,因此可以很好地解决商业保密问题;不出现外部接口,内部协调相对容易,工程进度有保障。

2.3　独立性影响解决方法

针对独立性影响,不同的设备厂商应当根据不同情况进行具体对待。对于软件部分比较简单的,可以采用软件验证与确认由外部具备独立法人的单位承担;但对于软件比较复杂或者软件产品种类比较多且所需人员比较多的厂家来说,比较合理的工作方式为同时采用外部和内部两种软件验证与确认的工作方式。具体操作可以分为内部和外部软件验证与确认均采用同一规范、内部和外部软件验证与确认采用不同的规范两种形式。

当内部和外部软件验证与确认均采用同一规范时,由于存在内部验证与确认活动,因此可以保证外部验证与确认活动一次性通过,工程进度有保障。内部研发队伍和内部验证与确认活动重叠部分的测试不再进行,以便减少费用开支。

当内部和外部软件验证与确认采用不同的规范时,内部采用严格的验证与确认规范,外部单位仅对内部验证与确认的相关活动(包括质量保证、程序、工具、人员和报告等)进行监督和评估。对此,要求外部单位需要具备相当程度的核安全理念,熟悉核安全级软件的要求,能正确地监督和评价相关活动。同时为了保证工程进度,研发队伍必须处于高质量活动状态,减少验证与确认活动反复的可能性。

3　独立性具体实施要求

软件验证与确认遵循的标准通常采用 IEEE 1012,IEEE 1012 将独立性要求分为四级[6]。IEEE 1012 标准是通用性的标准,适用于所有的软件。但对于核安全级软件来说,由于核设施中核安全级设备的安全要求在预计环境条件下进行验证,换句话说,在具备可确定性的情况下考虑概率分析,因此,即使采用 IEEE 1012 的最高等级也并不代表满足核安全级软件的要求。核安全法律法规、IEEE 7-4.3.2[7]以及 IEC 60880[8]都没有具体给出核安全级软件具体的 IEEE 1012 独立性等级,但考虑到核安全电气设备的重要性和安全功能,不同的核安全级软件要求的 IEEE 1012 独立性等级不同,但至少应当达到 IEEE 1012 次高等级。

核安全级软件验证与确认独立性具体实施要求如下。

① 技术独立性

技术独立性是指应当列出软件开发中直接影响软件质量的技术和工具清单,软件验证与确认队伍必须采用不同的技术和工具,具备多样性。

② 管理独立性

软件验证与确认队伍和软件开发队伍在单个项目

上必须满足管理独立性。软件验证与确认队伍发现的异常,软件开发队伍必须按照核质量保证中的不符合项[9]进行处理;软件验证与确认队伍不得对软件异常出现的具体原因进行分析或提出设计要求;软件验证与确认队伍工作文件上不得出现软件开发队伍成员的签字(这个要求不仅是独立性要求,也是防止工程进度失控的要求);软件验证与确认队伍和软件开发队伍不能存在直接接口;内部软件验证与确认队伍和软件开发队伍各自直接负责人不能为同一人。

③ 财务独立性

采用外部软件验证与确认时应当满足以下条件:双方签署正式合同;合同执行费用支付方式为一次性提前支付,不得出现分阶段、分批或按比例等其他支付方式。

采用内部软件验证与确认时应当满足以下条件:软件验证与确认队伍和软件开发队伍的费用支付批准签字人不同,保证软件验证与确认队伍经费不受软件开发队伍的约束;软件验证与确认队伍的待遇不受软件开发的影响,避免软件验证与确认队伍由于项目的影响导致质量下降,丧失客观性。

4　结束语

软件验证与确认作为核安全级中重要一环,应当高度重视软件验证与确认的独立性,同时要考虑工程的实际情况,选取合适的工作方式。软件验证与确认费用比较高,必须在保证核安全的基础上,合理减少相关商业风险和费用。由于核安全相关法规或标准没有给出具体的独立性指导,对软件验证与确认独立性的探讨肯定存在局限性,文中不当之处敬请指正。

参考文献

[1] 中华人民共和国国务院. 民用核安全设备监督管理条例[Z]. 2007.

[2] 张穹,李干杰. 民用核安全设备监督管理条例释义[M]. 北京:中国法制出版社,2007.

[3] 国家核安全局. HAF102 核动力厂设计安全规定[S]. 北京,2004.

[4] 国家核安全局. HAD102-16 核动力厂基于计算机的安全重要系统的软件[S]. 北京,2004.

[5] 毛从吉,毋琦. 核电厂安全系统软件设计及编码研究[J]. 核电子学与探测技术,2012,32(4):497-500.

[6] The Institute of Electrical and Electronics Engineers, Inc. IEEE Std 1012™-2004 IEEE standard for software verification and validation[S]. New York,2005.

[7] The Institute of Electrical and Electronics Engineers, Inc. IEEE Std. 7-4. 3. 2™-2003 IEEE standard criteria for digital computers in safety systems of nuclear power generating stations[S]. New York, 2003.

[8] The International Electrotechnical Commission. CEI/IEC 60880-2006 Nuclear power plants-instrumentation and control systems important to safety-software aspects for computer-based systems performing category A functions[S]. Switzerland,2006.

[9] 国家核安全局. HAF003 核电厂质量保证安全规定[S]. 北京,1998.

(上接第 42 页)

面垂直;②对液位波动较大的容器的液位测量,需采用附带测量筒来进行测量,以减少液位波动的影响;③导波管内壁一定要光滑,清洁度好;④不可装在圆型或椭圆型的容器顶的中心处,否则雷达波在容器壁多重反射后,汇集于容器顶的中心处,形成很强的干扰波,会影响测量的准确性。

根据上述安装注意问题,同时根据福清一期项目中设备接液口为侧开口,安装方式选择为侧装,测量筒通过法兰与被测设备 9ASG002BA 相连,法兰遵照 ANSI 标准选择,导波雷达液位计通过螺纹连接到测量筒。安装后满足设计及测量要求。

5　结束语

综上所述,液位仪表在核电厂中应用广泛。通过福清核电厂液位测量仪表的原理、用途、安装及现场问题分析,说明了核电厂液位测量的现状,证明了选择科学合理的仪表不仅可以节约成本,而且有利于现场的安装、调试和控制。

同时,通过探索将新的测量方式应用到福清项目,证明了导波雷达液位计具有安装方便、易调教、易维护等优点,对今后项目的液位仪表选型、更新起到一定的指导意义。

参考文献

[1] 廖圣勇. 核电站中液位仪表的选型[J]. 仪器仪表用户,2009,16(3):123-125.

[2] 杨万国,贾延刚. 多种液位仪表的应用对比[J]. 石油工程建设,2004,30(1):38-43.

[3] 袁明. 磁翻板液位计现场校准方法探究[J]. 工业计量,2011,21(3):63.

[4] 何宏克. Magnetrol 电动沉筒液位变送器在 PX 装置中的应用及维护[J]. 石油化工自动化,2005,16(3):75-76.

[5] 张钧. 导波雷达液位测量装置在大型火力发电厂的应用[J]. 宁夏电力,2007(z):85-86.

[6] 陈仕钦. 关于导波雷达液位测量的应用[J]. 湖北电力,2007,31(10):83-86.

[7] 姬晓波,涂亚庆,任开春,等. 雷达液位仪测量原理的分析及应用探讨[J]. 石油化工自动化,2005(1):68-70.