|  |  |
| --- | --- |
| ICS | 点击此处添加ICS号 |
| CCS | |  | | --- | | D:\000000部门项目\09标准化插件开发\程序源代码\StandardEditor_ShanDongKeXieYuan\团标首页面字母T.pngD:\000000部门项目\09标准化插件开发\程序源代码\StandardEditor_ShanDongKeXieYuan\团标首页面字母T后面的反斜杠.png CNS |   点击此处添加CCS号 |

中国核学会

团体标准

T/XXX XXXX—XXXX

核电厂商品级数字化物项适用性确认方法

Dedication Approaches for Commercial Grade Digital Equipments in Nuclear Power Plants

（本草案完成时间：2022年3月9日）

XXXX - XX - XX发布

XXXX - XX - XX实施

中国核学会  发布

目次

[前言 II](#_Toc132724035)

[1 范围 1](#_Toc132724036)

[2 规范性引用文件 1](#_Toc132724037)

[3 术语和定义 1](#_Toc132724039)

[4 评估和验证 3](#_Toc132724070)

[4.1 流程 3](#_Toc132724079)

[4.2 定义和验证关键特性 3](#_Toc132724082)

[4.3 补充说明 4](#_Toc132724083)

[4.3.1 概述 4](#_Toc132724212)

[4.3.2 不同类型的变更 4](#_Toc132724213)

[4.3.3 流程中各项活动的时间节点 5](#_Toc132724214)

[4.3.4 技术审查及所需的专业知识 5](#_Toc132724215)

[4.3.5 商业级调查的对象和地点 5](#_Toc132724216)

[4.3.6 用于多个应用程序的适用性确认工作 5](#_Toc132724229)

[4.3.7 评估的记录要求 5](#_Toc132724230)

[5 商品级适用性确认有效性的维护要求 5](#_Toc132724231)

[5.1 概述 6](#_Toc132724232)

[5.2 产品变更 6](#_Toc132724233)

[5.3 使用范围 6](#_Toc132724234)

[5.4 对第三方评定机构的要求 6](#_Toc132724240)

[5.5 技术支持 6](#_Toc132724241)

[附录A （资料性） 电厂升级过程中数字化商品级物项评估流程图 0](#_Toc132724242)

[附录B （资料性） 数字化设备的关键特性表 1](#_Toc132724243)

[附录C （资料性） 数字化设备内建质量评估表 3](#_Toc132724246)

[附录D （资料性） 应用示例 6](#_Toc132724247)

[D.1 概述 6](#_Toc132724248)

[D.2 简易指示器 6](#_Toc132724249)

[D.3 带有触点输出的指示器 8](#_Toc132724250)

[D.4 多功能控制器 10](#_Toc132724251)

1. 前言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国核学会标准化技术委员会提出。

本文件由核工业标准研究所归口。

本文件起草单位：中国核电工程有限公司、中核控制系统工程有限公司、北京广利核系统工程有限公司、国核自仪系统工程有限公司、核工业标准化研究所。

本文件主要起草人：

核电厂商品级数字化物项适用性确认方法

* 1. 范围

本文件规定了商品级数字化物项在核电厂安全级电气仪控设备中应用的适用性确认方法。

本文件针对新建核电厂及改造核电厂中不同规模的商品级数字化设备应用，范围从相对简单的数字仪表/指示器到更为复杂的数字控制器。

本文件适用于核电厂安全级电气仪控设备中应用商品级数字化物项的适用性确认活动，在其它核设施中应用商品级数字化物项进行适用性确认时也可参考执行。

* 1. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

NB/Z 20540 商品级物项在核电厂安全级电气仪控设备中的应用指南

GB/T 17624.1 电磁兼容 综述 电磁兼容基本术语和定义的应用与解释

GB/T 13629 核电厂安全系统中数字计算机的适用准则

GB/T 19001 质量管理体系要求

GB/T 19000.3 软件质量管理和质量保证

* 1. 术语和定义

本文件采用下列定义。



**结构 architecture**

系统或部件的组织结构。

[GB/T 13629,定义3.2]



**商品级物项 commercial grade item**

满足下述条件的物项：

a) 不是为核设施专门设计或不以核设施特有的技术要求为条件；

b) 用于非核设施；

c) 按制造厂产品说明（例如样本）中规定的技术条件从制造厂或供应商处采购。

[GB/T 13629，定义3.4]



**计算机 computer**

由一个或多个关联的处理单元和外部设备组成的、由内部贮存的程序控制的、不用人为干预便能执行真实计算（包括大量的算术运算或逻辑运算）的功能可编程装置。

[GB/T 13629,定义3.8]



**计算机程序　computer program**

可使计算机硬件执行运算或控制功能的计算机指令和数据定义的组合。

[GB/T 13629,定义3.10]



**配置项　configuration item**

在配置管理过程中指定要进行配置管理并作为一个整体处理的硬件、软件或两者兼有的集合体。

[GB/T 13629,定义3.14]



**关键特性　critical characteristics**

采用技术及行政管理和监督的一种规定，以识别或用文件证明配置项的功能和物理特性、控制对这些特性的变更、记录和报告变更过程和实施状态，并核实与规定要求的一致性。

[GB/T 13629,定义3.15]



**配置管理　configuration management**

采用技术及行政管理和监督的一种规定，以识别或用文件证明配置项的功能和物理特性、控制对这些特性的变更、记录和报告变更过程和实施状态，并核实与规定要求的一致性。

[GB/T 13629,定义3.15]



**数据　data**

１）以易于交流、理解，或被人员／自动手段处理的方式对事实、概念或指令的一种表达方式；

２）有时用作文档的同义词

[GB/T 13629,定义3.17]



**电磁干扰　EMI**

电磁骚扰引起的装置、设备或系统性能的减低。

[GB/T 17624.1,定义2.1]



**固件　firmware**

硬件装置和以只读软件方式驻留在该装置中的计算机指令和数据的组合。

[GB/T 13629,定义3.26]



**硬件　hardware**

用于处理、贮存或传输计算机程序或数据的物理设备。

[GB/T 13629,定义3.29]



**等同物项替代 like-for-like replacement**

采用与原物项等同的物项进行替代。

[GB/T 13629,定义3.29]



**软件 software**

与计算机系统运行有关的计算机程序、规程，以及相关的文档或数据。

[GB/T 13629,定义3.39]



**软件工具 software tools**

一种用来开发、测试、分析或维护其它程序或其文件的计算机程序。例如：比较程序、交叉引用生成程序、反编译程序、驱动程序、编辑程序、流程图程序、监控程序、测试案例生成程序和时序分析程序。

[GB/T 13629,定义3.42]



**验证与确认 V&V**

确定对一个系统或部件制定的要求是否完整和正确、每个研制阶段的产品是否满足前一个阶段提出的要求或条件，以及最终的系统或设备是否符合预定要求的过程。

[GB/T 13629,定义3.51]

* 1. 评估和验证
     1. 流程

图A.1显示了当涉及商品级数字化设备时的总体设备升级流程图。图的中柱和右柱显示了数字升级设计和验收流程。验收显示在右下角，与变更流程交互（用灰色条表示）。变更流程显示在中柱。右上角所示的故障分析是解决数字问题的关键因素。

图A.1的左柱显示了传统上的采购活动：替代物项的技术评估，以及用作替代品的商品级物项。

设计、验证流程、技术评估及商品级物项专用采购流程（NB/Z 20540）必须协同开展，以支持商品级数字化设备的评估和验收。如图A.1中的灰色条所示，在处理商品级数字化设备时，设计和采购活动之间需要大量的交互，如对供应商评估和组件测试要求、替代物项的故障分析等。

图A.1是通用的，描述了包括商品级数字化设备在内的任何变更所涉及的设计、验收和采购活动的类型。它能够将该通用流程与使用者或其委托方的具体实践联系起来，以组织、分配责任，并设定数字化升级和商品级物项评定活动的时间表。

* + 1. 定义和验证关键特性

针对于商品级数字化设备，除了物理特性和性能特性，可信性也需要作为关键特性进行评估。

表A.1列出了典型的关键特性，并提供了可用于验证这些特性的验收标准和验证方法的示例。表格涵盖了三类关键特性中的每一类：

1. 物理特性：物理特性包括硬件的物理特性，如尺寸、安装和其它类似于机械、电气和模拟电子设备的特性。在大多数情况下，数字化设备的验收标准和方法与模拟设备相同。表格指出了由于需要验证软件或固件版本而在零件识别方面的一些差异。这些特性大多数都是通过检查和测量进行验证的，属于NB/Z 20540中的方法1。
2. 性能特性：性能特性包括设备所需的功能（仅核电应用所需的功能）和与此功能相关的性能（例如，响应时间）及性能相关的环境要求（例如，在特定环境温度范围内满足精度要求）。另外，这类特性还包括与故障管理和“因核电应用不需要而禁止执行”功能相关的特性。这些设备的验收标准和验证方法与模拟设备类似。例如，基于故障分析，使用者或其委托方可能需要设备在某些异常或故障条件下的特定行为。验收标准可包括以下项目：故障类别的检测以及在规定情况下进入的“首选”或故障安全模式（例如，失去电源或信号输入时所需的特定输出状态）。验证方法包括测试和设计审查，并由故障分析和可信的运行历史审查等资料作为支持。这些活动可能涉及NB/Z 20540的方法1、方法2和方法4；
3. 可信性特性：可信性特性是数字化设备与其它类型组件最大的不同之处。它解决了通常不能通过检查和测试进行验证的属性，并且通常会受到设备研制过程的影响。另外，它与制造缺陷、老化和磨损无关，如果软件中存在设备可信性降低的问题，则表明设备中存在设计错误，或者应用程序需求与设备设计不匹配。

可信性属性（包括可靠性和内建质量等条目）通常受到制造商在基于软件设备的设计、开发、验证和确认中使用的过程及相应人员的影响。对于基于软件的系统，需要在软件架构层次来提高其质量，遵循从需求到实施的系统生命周期方法，并为生命周期的每个阶段提供验证与确认的步骤和适当的文档。因此，验证过程中需要深入审查供货商的开发过程供应商的开发过程。

可信性类别需要获取那些必须被评估的关键特性，以形成有关基于软件设备的内建质量的适当判断。它还需要包括与问题报告和配置控制相关的特性。这些特性的验证通常包括对供应商流程的商业级调查（方法2），以及对供应商及其物项以往的性能表现记录的审查（方法4）。源地验证（方法3）可用于在制造过程中验证某些硬件质量特性，或确保软件变更（为核电应用做出的软件升级或配置）的质量。

内建质量特性，作为可信性类别中的关键特性，无法像一般物项的型号或物理尺寸等特性一样有形或可量化。所以需要根据产品开发过程及其文档、运行历史、测试、设计特征（如故障管理）审查以及关键特征表（表B.1）中指出的其它因素的组合做出判断。

表C.1提供了在评估内置质量时的详细示例。评估者在进行评估时应用的具体标准，取决于设备的安全重要性和复杂性。安全重要性取决于设备的功能及其故障的后果，包括考虑备份或其它实现安全功能的方法。这包括考虑对提供不同备份功能的系统和设备进行升级的累积影响，特别是在保持预期多样性方面。复杂性包括设备的复杂性（例如，总体架构、功能数量、输入和输出、处理器或模块之间的内部通信以及与其它系统或设备的接口）和软件的复杂性。

当完成所有关键特性确认后，必须验证所有这些特性，包括物理、性能和可信性特性。附录D中的示例表明了几个案例中关键特性的选择和验证，从简单的仪表到多功能控制器。

* + 1. 补充说明
       1. 概述

本节提供了关于评估和验收商品级数字化物项的附补充说明，扩展了第4.1节和第4.2节中提供的信息。

* + - 1. 不同类型的变更

第4.1节中概述的过程以及第4.2节中给出的定义和验证关键特性的方法适用于使用商品级数字化设备的各种情况。其中包括：

1. 小范围变更，例如对于单个组件（从单个集成电路到完整的控制器或记录仪），由于原型号已经停产，使用替代型号进行更换。替代物项的技术评估（图A.1左上角）决定了该变更是否等同于类似变更，或者新设备是否有“足够不同”，需要进行设计变更。例如：如果旧设备采用模拟技术，而新设备采用数字技术或基于软件的技术，则此类变更通常会导致设计变更，从而引发电厂改造或升级过程（如图A.1中柱所示）。同样的，对于数字化技术本身的升级，如果新设备具有新的或增强的功能（例如，通过对固件的改变），与旧版本相比“足够不同”，也需要进行设计变更；
2. 较大规模的变更，例如使用包含商品级数字化设备的新设备升级部分监控系统；
3. 在安全级相关应用中安装全新的数字化设备或组件。在这种情况下，虽然没有设备替代（只有原始设计），但任何执行安全功能的新商品级设备都需要适用性确认。
   * + 1. 流程中各项活动的时间节点

在流程中需要尽早识别具体有哪些商品级物项（例如，在项目定义阶段，见图A.1），基于需求的初步定义，商品级数字化物项是否需要涉及变更，以及额外应考虑哪些方面，包括候选的供应商和产品。这通常包括将应用程序要求与已发布的商品级物项的规范进行比较。如果涉及商品级数字化物项，这可能会影响对流程其余部分的详细要求及项目进度。例如，需要为审查、商业级调查或特殊测试分配足够的时间。

同时,在商业调查之前，也需要为供应商及其产品的初始评估制定筛选标准，这样可以提前淘汰那些不太可能通过适用性确认的产品或供应商，避免过多无效投入。初步筛选中可能检查的项目应包含供应商是否支持商业级调查并承诺如实报告相关问题等事宜。

商品级物项最终被“接受”的时间点，即适用性确认完毕的时间点各有不同。某些关键特征在安装和最终测试后才可得以验证,所以在这个点之前适用性确认流程不能关闭，即现场安装后的测试是必要的(应建立控制措施,以确保这些项目控制和跟踪,并且在所有关键特性得到验证之前不会正式投入使用)。在其它情况下,设备安装之前所有的关键特性验证需要通过评判、分析和测试。

* + - 1. 技术审查及所需的专业知识

进行审查和验证的人员的资质必须与所执行的任务相适应。

在判断商品级数字化设备的可接受性时，需要重点关注整体设备设计、软件体系结构、控制流和数据流等方面。商业级调查（NB/Z 20540的方法2）可用于判断大多数关键特性，包括对设计和体系结构审查以及程序审查。

另外，由于商品级数字化设备较为灵活并且容易重新配置，并且它拥有可能被意外输入和影响自身安全功能的内置模式及特征，所以还需要重点检查用户交互的影响，以及通过使用人机接口时发生意外或未经授权的重新配置或其它故障的可能性。

* + - 1. 商业级调查的对象和地点

对于许多数字化物项，关键特征的验证需要在设备的原始制造商或开发商的场地开展。在某些情况下，原始开发者可能不是数字化商品级物项的直接供应商，但是他们具有支持商业级供应商调查所需的信息。此外，还可能存在制造某些部件或组件的子供应商。调查人员应了解商品级物项从最初制造到经销商及其它第三方的整个路径信息，并提供给使用者或者其委托方审查，并且在上述链条中需要特别关注配置控制。

* + - 1. 用于多个应用程序的适用性确认工作

可以若干类型的数字化设备进行标准化，并将其应用于实际工程的多种应用中，以降低进行适用性确认工作的成本。例如,执行一次商业调查可涵盖一台设备的多种应用。然而,如果设备仅仅专用于一个应用，这个设备就不能用于其它应用。同时，应仔细检查新应用的具体情况，因为它们可能会有新的或不同的关键特性和验收标准。例如，更严格的时间响应要求可能意味着需要对采样延迟和其它时间响应因素进行更详细的审查。此外，还应将安全重要性与之前的应用进行比较。应重新审查故障分析，以确保其充分适应于新的应用程序。在一种应用中可接受的设备故障特征在另一种应用中可能不可接受。

需要检查多次变更或升级对多样性或深度防御所依赖的备份的积累影响。在多个地点或多个系统中使用相同的数字化设备可能会减少多样性和纵深防御，这一点应予以评估。

* + - 1. 评估的记录要求

获得合理保证的过程，就是商品级数字化设备项目执行其安全功能的过程，这些判断的依据应记录在案，并作为专用记录的一部分予以保留。最后，这些文件也应当足以让有相同资格的机构得出相同的结论。

* 1. 商品级适用性确认有效性的维护要求
     1. 概述

只要执行过商品级物项适用性确认的设备仍在使用中，使用者就有责任维护其适用性确认的有效性。适当的配置控制和变更管理是保持适用性确认的完整性的关键。

* + 1. 产品变更

除了硬件更换外，使用者的配置控制程序应识别和跟踪软件（包括固件）的修订。安装软件的版本和描述应保存在设备或局部数据库中。为了替代数字化设备或备件而准备采购订单时，应使用合格（经适用性确认的）的版本，并要求供应商通知使用者该设备的任何变更，以便在收到新的修订版本之前，评估其影响。使用者根据对替代物项的技术评估程序对产品变更进行评估（如图A.1）。使用者应特别注意在应用中所需要的，并且在供应商公布的设备规格之外的功能或特性的潜在变化。因为这些变化不会像那些在公布范围内的设备规格那样，被供应商的流程所严格控制。

为了支持对变更的检测和评估，使用者应确认供应商有适当的配置控制程序，并有必要的控制措施，以确保购买的替代物项中实际安装的软件/固件修订版本是可控的，并可追溯到设计变更文件。使用者应该了解供应商改变硬件和软件组件的修订名称的标准和程序，并根据使用者的应用，评估这些程序是否足够。以上环节通常是作为初始适用性确认的一部分，通过商业级调查进行评估。

如果已安装的软件在没有新的修订的情况下被认为是够用的，那么使用者可以选择不更新其软件。在决定是否接受修订时，需要在以下两方面取得平衡：一是尽量减少评定和支持软件连续变化的费用，二是需要保持相对最新，以确保供应商对所安装版本的持续了解和支持。

* + 1. 使用范围

经过商品级适用性确认的设备其使用不应超出初始适用性确认的范围。安装系统之后发生的变化，或系统与部件操作方式的变化，可能会影响应用的关键特性。这些都应该对照初始适用性确认中使用的验收标准进行评估，或者修改验收标准。在进行这些评估时，应考虑到最初确定关键特性和验收标准时的所有假设。

* + 1. 对第三方评定机构的要求

当外部机构作为设备制造商和使用者之间的中介进行商品及适用性确认时，使用者应采取适当的措施，以确保适用性确认工作的有序开展，包括其后续维护。这些措施应涉及评估第三方评定机构的资质、经验和长期经营能力等方面。

* + 1. 技术支持

如果商品级数字化设备中的软件维护工作由使用者自己进行或承包给第三方，使用者应购买所需的工具和报告（编译器、测试工具、配置日志、测试报告等）。如果使用者与原来的供应商签订维护合同，维护协议应规定供应商需要保留哪些材料。这些材料应该和他们自己进行维护时一致，同时这些项目应该在采购时进行评定。

在某些情况下，可能需要在供应商和使用者之间达成特别协议。例如，如果商业供应商选择停止对某一产品的支持，其需要将有关产品设计和维护的所有记录移交给使用者。

2. （资料性）  
   电厂升级过程中数字化商品级物项评估流程图



* 1. 电厂升级过程中数字化商品级物项评估流程图

1. （资料性）  
   数字化设备的关键特性表
   1. 数字化设备的关键特性表

| **关键特性验收** | **验收标准** | **验证方法** | **说明** |
| --- | --- | --- | --- |
| **物理：**  产品/零件标识：   * 型号/零件号； * 固件版本号； * 软件版本级别； * 硬件版本。   硬件物理特性：   * 尺寸； * 安装。   设备接口的物理特性：   * 功率； * 信号； * 数据通信； * 人机界面。 | 产品/零件标识必须与采购要求相匹配，以支持验收的物品是否为指定物品，包括硬件和软件。  基于预期应用的要求的其它物理和接口特性标准。 | 硬件部件标识的处理与其它设备相同（方法1）。对于固件，需要解决当固件版本更改时供应商是否更改零件号的问题。如果没有，则必须单独验证固件版本。  固件版本可通过检查零件号验证（方法1）。进行适当的标记和了解供应商对固件内存加载(烧录)过程的控制（方法2或3）。对于固件中没有编码的软件，验证正确的版本可能更复杂。  物理特性通常通过检验和测量进行验证（方法1）。 | 当批量采购多个产品时，根据项目的复杂性和特定特性，某些特性可能仅在一个样本上进行验证，而不是对每个样本进行全面检查。对于仅在样品基础上验证的特性，应该充分了解设计和制造过程，以及影响这些特征的因素，以确保采样充分。这些基础应该记录下来。 |
| **性能**  所需功能，如：   * 输入处理； * 所需的特定功能或算法； * 输出信号要求； * 人机界面功能； * 测试和诊断功能。   与所需功能相关的性能要求，如：   * 响应时间； * 准确性； * 范围； * 稳定性； * 数据吞吐率； * 包括功率、信号和数据通信的接口； * 人机界面的有效性。   与所需功能和性能相关的环境条件，如：   * 温度； * 湿度； * 震动； * EMI/RFI的敏感性、排放和静电释放。 | 基于预期应用要求的功能和性能标准。 | 大部分功能和性能特性通过试验进行验证（方法1）。  除了EMI试验（方法1）外，部分特性可以通过设计评审来进行验证，例如：检查EMI保护功能的设计（方法2）。故障分析可以支持某些性能特性的定义和验证。 | 专业人员通常会审查由供应商或第三方所执行的测试，并运行补充测试作为部分验证。一些特性可以由供应商或专业人员通过特殊压力或“挑战”测试来验证（例如，高数据速率或计算负担条件下的性能测试）。  一些测试只能对一个或一个项目样本进行，而其它测试可能需要对每个采购的独立项目进行，取决于项目的复杂性和需要验证的特定特性。仅在样本基础上验证的特性，应充分了解设计和影响这些特性的因素，以确保取样充分（例如：是仅由基础设计确定的特性，因此只能在一个或几个单元上进行检查，或者它在制造或装配过程中是否会发生类似的变化，对这些变化的控制较少，因此必须测试更多的单元）。  供应商发布的设备规范中未包含的特性需要进行特别审查，因为这些特性可能不像供应商规范中的特性那样受供应商流程的控制。 |

* 1. 数字化设备的关键特性表（续）

|  |  |  |  |
| --- | --- | --- | --- |
| **关键特性验收** | **验收标准** | **验证方法** | **说明** |
| 在特定异常或故障条件下的行为：   * 对特定异常情况和事件的响应； * 事故保险特性。 |  |  |  |
| **可信性a**  与所需功能相关的可靠性和可维护性。  内建质量包括：   * 设计质量； * 制造质量； * 缺陷管理； * 操作员和维护人员的兼容性。   配置控制和可追溯性：   * 硬件； * 软件； * 固件（硬件和软件配置控制方面）； * 问题报告。 | 可靠性、可用性和可维护性的标准应从预期应用程序的需求中得出。具体的标准可能是所需功能的可靠性或可用性，或者包括软件在内的可维护性标准。如果采用定量分析，则应说明论证方法（如：使用经典方法进行硬件可靠性分析，或从现场经验中统计分析故障率数据）。  内建质量的基本标准是等同于根据HAF003开发和应用的设备质量。等效质量的判断基于以下组合：   * 设计和设计评审流程，包括软件生命周期、验证和确认等； * 设计文件； * 配置管理； * 质量保证程序和实践； * 软件需求定义和需求可追溯性； * 设计和验证中考虑失效模式和异常条件或事件； * 参与设计和验证活动的人员的资格和经验 * 产品运行历史； * 由供应商或专业人员进行测试，并由买方或其委托方对测试设计、测试过程和测试结果进行检查。   配置控制和可追溯性的最低标准是它们足以支持使用运行历史数据，并确保交付的项目可以追溯到作为验收的一部分评审的文件。  问题报告必须足以支持产品运行历史的使用。应该制定具体标准（如：覆盖范围、及时性、向正确的组织或部门报告） | 可靠性：审查供应商的可靠性计算、测试方法和结果。审查历史运行数据。审查和设计评估。执行可靠性分析（方法2）。  审查供应商流程和文件（方法2或3）：   * 设计、发展和验证过程； * 质量保证计划和实践； * 验证和确认计划和实践。   设计评审-架构评审、代码评审、运行、分析技术等（方法2）。  系统级和商品级物项本身的故障分析。  比较设备故障模式与应用需求。  产品运行历史回顾（来自供应商、用户、用户团体、行业报告等）（方法4）：   * 文件证明（记录，可追溯）； * 足够的（单位，使用年限）； * 成功的（错误跟踪显示了良好的性能，包括软件在内的设备是稳定的）； * 相关的（相同或类似的硬件/软件配置、使用功能、类似操作等）。   配置控制：审查供应商配置管理过程和操作。检查实际操作记录（方法2或3）。  问题报告：审查供应商程序和操作。与以前的客户评估绩效记录（方法2）。签订合同协议。  评估专业人员的可维护性。 | 所需验证活动的数量和范围取决于设备的复杂性和安全重要性。  可能需要补充活动，如额外的测试、验证或分析以及相关文件。  对于给定类型或型号的设备，许多所需的特性都可以进行一次验证，并且该设备在工厂中的每次应用都不必重复验证。这需要验证管理和质量控制实践确保每次新采购都收到相同的设备（具有相同的验证特性）。此外，如果设备要应用于更关键的应用中，可能需要额外的验证活动。 |
| 1. “可信性”一词在软件和安全级领域中以各种方式使用。在本文件中，它广泛用于包括数字化设备的一些特性，如可靠性、可用性、内建质量和其它相关特性（见第4.2节中的定义）。 | | | |

1. （资料性）  
   数字化设备内建质量评估表

表C.1 商品级数字化设备内建质量评估表

| **项目质量评估中使用的活动** | **评估项目质量时可评估的设计因素示例** |
| --- | --- |
| 审查设计、文档以及硬件和软件的实现 | 设计和文档：   * 完整性； * 准确性和与实际设计的一致性； * 总体系统设计及软件架构； * 简单性； * 程序执行、控制流和数据流的确定性； * 内部一致性； * 支持所需功能的充分性； * 不需要的功能及其对需要功能的影响； * 错误处理功能、内置保护功能、处理预期和意外错误以及异常条件或事件的能力； * 人因和人机接口； * 防止人机接口引起的错误和其它错误； * 需求在整个设计、实现及验证过程中的可追溯性。   软件实现：   * 代码结构； * 遵守公认的编码惯例；   硬件实现：   * 良好制造规范的使用； * 所用组件的质量。 |

表C.1 商品级数字化设备内建质量评估表（续）

|  |  |
| --- | --- |
| **项目质量评估中使用的活动** | **评估项目质量时可评估的设计因素示例** |
| 审查设计/开发过程及其文件（其适用于所评估的项目） | 用于产品开发、V&V的生命周期：   * 符合公认标准和指南。   软件/硬件要求的充分性：   * 完整性； * 正确性； * 清晰性。   从系统需求和设计到软件需求、软件设计、代码和验证测试的可追溯性。  设计审查和验证：   * 审查和分析的范围和覆盖面（设计审查、代码演练和检查、分析工具的使用）； * 审查人员、测试人员与设计人员的独立性。   系统应用从产品早期版本遇到的问题中吸取的教训。 |
| 审查参与设计和验证的人员的资质和经验 | 个人：   * 设计或验证职责相关领域的培训； * 类似项目的经验； * 熟悉设计中使用的特定工具、语言等。   组织机构：   * 开发类似产品的经验； * 与组织能力相关的第三方认证。 |
| 审查供应商质量保证（QA）计划和实践，包括软件质量保证（SQA） | 有记录的质量保证计划：   * 符合相关标准（例如GB、GB/T等）。   供应商计划认证（例如GB/T 19001等）。  质量保证计划在采购项目中的应用：   * 该产品对该计划的遵守程度、相关人员的认可程度； * 所需文件的记录、形式和批准程度。 |
| 审查供应商配置控制程序和实践 | 文件化的配置管理程序：   * 与相关标准（例如GB、GB/T等）和公认实践的一致性。   供应商计划认证（例如GB/T 19001等）。  配置管理程序在采购项目中的应用：   * 该产品遵守程序的程度； * 从最初的开发到变更和发布的文档化程度； * 对分供应商的控制； * 对采购物品经过的分销商或供应商的控制。   供应商和产品跟踪记录，用于控制变更和版本，并通知变更，尤其是维修期间。 |
| 故障分析 | 在系统设计和验证中考虑异常条件或事件：   * 具体确定的硬件和软件的潜在故障模式； * 正式或非正式危害或异常条件或事件分析； * 介入这个过程的时机，以及其指导设计和验证的程度。   设备故障模式的可预测性。 |

表C.1 商品级数字化设备内建质量评估表（续）

|  |  |
| --- | --- |
| **项目质量评估中使用的活动** | **评估项目质量时可评估的设计因素示例** |
| 审查供应商测试 | 功能和性能测试。  环境测试，包括电磁干扰/射频干扰（EMI/RFI）。  软件验证测试的范围（例如鲁棒性测试，模块、线路或修正条件/判定覆盖）。  验证测试的范围（例如静态、动态、随机）。  摸高测试的范围（例如专门设计用于发现故障模式的测试）。  测试文件。 |
| 审查产品运行历史 | 记录：   * 指示安装的特定型号和软件/固件版本、时间和位置的记录； * 正式或非正式的问题报告、问题描述和后续行动。   充分性：   * 运行中的机组数量； * 服务年限。   故障统计：   * 低故障率； * 故障率相对稳定，无严重错误，软件稳定，但功能变化的情况除外。   其它相关：   * 相同或类似的软件/硬件配置，以及使用的功能或选项； * 以类似于计划应用的方式安装和操作设备； * 类似的环境条件； * 类似的运行时间。 |

1. （资料性）  
   应用示例
   1. 概述

本附录提供了一些示例，旨在说明第4章中的内容如何适用于不同复杂性和安全重要性的项目。这些示例从一个简单的指示器开始，最后是多功能控制器的升级，说明了随着项目的复杂性和安全重要性的增加，所需的适用性确认活动的水平也在增加。

因为这些示例的目的是说明从选择商品级设备到评估和最终验收的整个过程，所以示例只选择了适用性确认结果成功的案例。然而，并不是所有的商品级物项都能成功通过适用性确认。如果不能证明有合理的保证，或者如果使用者认为提供这种保证在经济上不可行，那么使用本文件的方法对一个商品级物项进行评估将导致该项目不能通过。另外，在项目的执行过程中，会涉及到需求和设计的权衡和迭代。

* 1. 简易指示器

本示例说明了一种情况，即商品级设备的简单性和可测试性及其在工厂中的功能，加上广泛的、可信的成功运行历史，提供了充分的保证，而不需要进行商品级调查或对装置的内部设计和开发过程进行详细评定。

使用者对现有作为安全级相关模拟指示装置或仪表进行升级，将这些设备替代为基于微处理器的设备。这些设备的功能是向控制室的操作人员显示单个变量的值。两个这样的仪表被用来为该变量提供冗余指示，冗余的仪表回路是经过鉴定的、独立的、相互隔离的。一个成熟的制造商提供的商品级、成品数字指示器被选为候选同等物项替代设备，因为它提供了所需的功能，易于购买，并且被广泛使用。它是一个单一功能的设备，没有可编程或软件可配置的功能。(使用一个固定的4-20mA输入。只有面板和内部硬件开关设置可以改变，以便在不同工程单位范围的应用中使用同一仪表）。将应用要求与供应商的规格进行比较，表明这些要求在供应商规定的性能范围内。数以千计的这些指示器已经在一些行业（制药、化学工艺等）中使用了数年，具备良好的可靠性。

使用者使用NB/Z 20540中的指导和程序来计划和执行商品及适用性确认。指示器的设计要求根据预期的应用来确定。使用者还进行了故障分析，提供了关于应用的重要故障模式的信息。基于这些信息，指示器的关键特性被确定，如表A.1所示。

使用者采购了三个指示器，并进行了表D.1、D.2、D.3中描述的检查、测试和复核。对于这种设备和应用，许多物理和性能关键特性的验证是直接的；它们在接收时被成功测量或测试。在可信性类别中，关键特性的验证更加主观，在这种情况下，验收标准反映了这样一个事实：该设备很简单，不能用软件配置，而且只有一个功能，可以充分的测试。

由于该设备的简单性和可测试性，以及其可信的运行历史数据，可以得出结论不需要对供应商的设施进行详细调查和相关访谈。在这种情况下，测试是验证的主要手段，辅之以对设备可信的运行历史的审查。因为该设备只有一个功能，而且单位转换和标定是在不改变软件的情况下完成的，所有的操作历史被认为与计划的应用有关。该设计非常稳定；该装置代表了几乎相同的指示器系列中的第三代，并且所有这些指示器都是数字式的；上一代的变化只影响到面板，而最新的型号已经在许多应用中成功运行了大约一年。

故障分析发现，由于其功能简单，该装置只有几种不同的外部故障模式而且包含了内部组件的所有故障模式。该装置不会自动启动任何工厂设备。在预期的异常条件下（例如，输入信号丢失），指示器的响应可以通过测试来验证。基于对设备的实用测试、相关可信的运行历史以及对仪器进行的正常定期检查和校准可以确定该指示器发生任何其它重要的意外故障（例如，可能给出不正确读数）的概率足够低。此外，还可以使用操作人员可用的其它仪器读取或推断出指示器的指示变量。

基于这些结果，仪表被升级安装并完成了一系列商品及适用性确认活动，记录了关键特性、验收方法和用于设备的适用性确认活动，包括所做工程判断的基础。在这种情况下，指标的简单性和可测试性，加上其在许多类似应用中表现出的稳定性和可靠性，被证明是建立合理保证该装置将执行其安全功能的关键。

表D.1 简单指示器的关键特征-物理特性

|  |  |  |
| --- | --- | --- |
| **物理关键特征** | **验收标准** | **验证方法** |
| 配置：   * 型号； * 软件版本号； * 尺寸； * 安装。 | 供应商模式。  供应商的软件版本。  长x宽x高。  带有安装夹的前面板支架。 | 进厂检验核实这些特征。  注意，由于没有进行调查，所以没有获得关于供应商的配置控制和软件版本跟踪的详细信息。然而，本用户记录了收到和测试的单位的软件（固件）版本号，以便在未来采购中收到不同的修订级别或部件号时进行重新评估。 |
| 接口：   * 输入信号； * 输入阻抗； * 电源； * 柱状图和数字显示。 | 4-20mA。  通过用户手册。  通过用户手册。  6英寸柱状图，精度为1%，  4位数字（需要实用程序规范）。 | 进厂检验测试。 |

表D.2 简单指示器的关键特征-性能指标

|  |  |  |
| --- | --- | --- |
| **性能关键特征** | **验收标准** | **验证的方法** |
| 功能：   * 准确度； * 范围； * 响应时间。 | 通过用户手册。  0-100%(4-20mA)。  通过用户手册。 | 用户进厂检验测试（对所有采购的指标进行而不仅仅是样品）。 |
| 环境兼容性：   * EMI； * 地震； * 温度。 | 通过用户手册或相关标准。  每个位置的响应谱。  基于安装位置（和缓环境）的实用程序规范。 | 第三方测试实验室报告，用于测试一批指标中的一个或少量样本；使用者检查所有获取的指标，以验证批次的同质性，并确保所测试的项目与未测试的项目等效，以验证所验证的特征。 |
| 异常/故障条件下的行为：   * 信号丢失； * 断电； * 信号超出/低于范围。 | 读取指示器时可由操作员检测。 | 进厂检验测试。 |

表D.3 简单指示器的关键特征--可信性

| **可靠性关键特征** | **验收标准** | **验证的方法** |
| --- | --- | --- |
| 内建质量：   * 设计和制造的质量； * 故障模式和故障管理。 | 检查和测试结果满足验收标准。  视觉检查显示使用了良好的商业生产实践。  成功和相关的产品运营历史。  这些综合起来表明足够的设备的质量。  在故障分析和测试的基础上，充分考虑了故障模式。(注：故障分析还用于帮助确定是否存在未审查的安全问题) | 使用者的检查和测试。  审查应获取具体模型范围、相关性和成功运行经验a。  进行故障分析识别故障模式并评估其重要性。  审查产品可信的运行历史，以帮助验证没有特定的关键故障a。  挑战测试，旨在测试正常操作（在整个范围内的操作，包括慢速和快速扫描以及稳态读数）和异常条件下（例如，电源电压下降、超范围输入、噪音信号等）可能的关键故障模式。 |
| 问题报告 | 供应商有错误报告程序，并将向实用程序提供报告。 | 与供应商就错误报告程序达成协议。 |
| 可靠性 | 成功运营历史。 | 审查产品可信的运行历史a，以证明其可靠性。 |
| 1. 在本示例中，对产品操作历史的回顾相对简单。与供应商的讨论表明，在过去的一年中，许多单位都拥有成功的经验，固件一直保持稳定。该设备的功能简单性有助于建立这种操作经验的相关性。很大一部分单元使用与此处使用的内部开关设置相同的内部开关设置。与选定的用户联系以确认他们对设备的使用与实用程序的预期应用程序相似 (连续服务、定期读取读数、类似的环境、没有静音故障的问题)。 | | |

* 1. 带有触点输出的指示器

这个例子与D.1节中的简单指示器相比，其复杂性和安全意义都有所提高。在这个例子中，一个现有的液位指示器将被一个新的基于微处理器的设备所取代。该指示器位于反应堆厂房地坑液位处。除了指示功能外，该装置还有一个执行控制功能的触点输出。其目的是当水位上升到一个预设值时启动相应的泵。该泵将地坑中物质输送到放射性废物罐中进行处理。如果指示器未能采取控制动作来启动泵，地坑液位可能会上升到超过其极限值，导致放射性废水溢出。

所选择的替代指示器与上一个例子中的简单指示器来自同一供应商和同一产品系列。但是在本示例中的指示器包括一个执行控制功能的触点输出。与D.1节相比本示例中的指示器的新增功能、复杂性和安全重要性，使用者认为此类设备具有更多的关键特性，需要进行更多的验证行动。特别是由于指示器现在执行的自动控制动作同时具有安全和经济后果，使用者决定需要对设备的设计、其内部结构和供应商的质保程序进行更严格的审查，故进行了一次商业级调查。此次对供应商的商业级调查由专业团队进行，团队成员由对数字系统、实时测量和控制问题、软件质量保证、制造质量控制以及其它支持调查所涉及的关键特性的验证所需的专业人员组成。

这个例子的关键特性和验证活动详见表D.4。与D.1节相比增加或改变的内容以斜体显示。根据这些活动的结果，采购并安装了新的数字化设备，并进行了一系列商品级物项适用性确认活动，记录了适用性确认的基准。如同简单指示器的情况一样，该设备的升级开发，以及证明其稳定性和可靠性的相关运行经验，对适用性确认有很大帮助。对这些内容的审查作为商业级调查的一部分为确保该设备能够令人满意地执行其指示和控制功能提供了额外的信息。

表D.4 带触点输出的指示器的关键特性-物理特性

| **物理关键特征*a*** | ***验收标准a*** | ***验证的方法*** |
| --- | --- | --- |
| *配置：*   * *型号；* * *软件版本号；* * *尺寸；* * *安装。* | *供应商型号。*  *供应商的软件版本号。*  *长x宽x高。*  *带有安装夹的前面板支架。* | *进厂检验。* |
| *接口：*   * *输入信号；* * *输入阻抗；* * *电源。* * *柱状图和数字显示；* * *设定点调整；* * *触点输出。* | *4-20mA。*  *根据用户手册。*  *根据用户手册。*  *6英寸柱状图，精度为1%，分辨率4位数字（根据用户手册）。*  *根据用户手册。*  *根据用户手册。* | *进厂检验测试。* |
| 1. *斜体表示与表A.1、A.2、A.3中简单仪表示例的差异。* | | |

表D.5 带触点输出指示器的关键特性—性能

|  |  |  |
| --- | --- | --- |
| **性能关键特性** | **验收标准** | **验证方法** |
| 功能水平指标：   * 精度； * 范围； * 响应时间。 | 根据用户规格书；  0—100%（4-20mA）工作范围；  根据用户手册。 | *供应商的认证（须经调查）*和使用者的进厂检验测试（对所有采购的指示器进行测试，而不仅仅是样品）。 |
| *触点输出功能：*   * *设定值可调节性；* * *滞后；* * *响应时间。* | *根据用户手册。* | *供应商的认证（须经调查）和*使用者*的进厂检验测试。* |
| 环境兼容性：   * EMI； * 抗震； * 温度。 | 根据用户手册或相关标准；  每个位置的响应谱；  基于安装位置（和缓环境）的实用程序规范。 | 第三方测试实验室报告，用于测试一批中的一个或一小部分样本；  使用者检查所有采购的指示器，以验证批次的同质性，并确保测试的项目与未测试的项目等效，以验证其特性。 |
| 异常/故障条件下的反应：   * 信号丢失； * 断电； * 信号过高/过低。 | 操作员在阅读指示器时可检测到。 | 进厂检验测试。 |

表D.6 带触点输出指示器的关键特性—可信性

| **性能关键特性** | **验收标准** | **验证方法** |
| --- | --- | --- |
| 内建质量：   * 设计和制造质量； * 失效模式和故障管理。 | *供应商需维护一份涵盖设计和制造的质量保证方案，其中涉及的关键领域至少包括：*   * *QA人员和组织的定义；* * *QA计划和程序；* * *具体的软件QA要求；*   *证明QA方案已应用于采购物项的生产（至少硬件制造）。*  有文件记载的产品可信的运行历史，这些因素共同证明了设备的质量。  根据失效分析识别失效模式。(注：失效分析还用于帮助确定是否存在未审查的安全问题）。 | *商业级调查a*   * *审查供应商质量保证手册并检查实际质量保证实施情况，包括质量保证计划在设计和生产待采购物项中的应用程度；* * *审查供应商的数字系统/软件开发程序和实施情况，必要时由*使用者*或供应商准备相关补充文件；* * *审查设备设计和软件体系结构，尤其是关于意外失效的可能性；* * *审查供应商测试。*   审查拟采购的特定型号的运行经验的范围、相关性和成功性b。  失效分析从系统角度识别失效模式，并评估其重要性。*审查设备设计和软件架构，以识别重要的内部故障模式、提供的诊断功能及其覆盖范围，以及故障对设备预期功能的影响（重点关注触点输出）。*  审查产品可信的运行历史，以验证不存在特定的关键故障b。测试在整个范围内正常运行操作和在异常条件下（例如，电源电压下降、超出范围的输入、噪音信号等）可能出现的关键故障模式（包括慢速和快速扫描以及稳态读数）。 |
| *配置控制* | *供应商具有合适的配置控制程序。* | *在供应商调查期间对配置控制程序进行审查a。* |
| 问题报告 | 供应商具有错误报告程序，并将向使用者提供报告。 | *在供应商调查期间审查错误报告程序a。* |
| 可靠性 | *根据测试、分析以及可信的运行历史证明可靠性和可用性。* | *审查供应商的测试报告或分析报告。*审查产品可信的运行历史，以证明可靠性。 |
| 1. 如果证实之前的调查充分涵盖了该应用的特定关键特性，包括设备重要失效模式所需的信息，则可使用该公司或其它公司的书面调查（例如存档）。 2. 在这个示例中，对产品可信的运行历史的回顾是相对简单的。调查证实，有一个反馈程序可以记录现场经验。固件在过去一年中一直稳定，许多单位都有成功的经验。该设备的功能简单，便于建立这种操作经验的相关性。供应商确认大部分装置使用与此处使用的相同的内部开关设置，并且在许多应用中使用触点输出功能。与选定的用户联系，确认他们对设备的使用与本公司的预期应用相似（连续运行、定期从指示器上读取数据、类似的环境、用于自动控制功能的触点、没有无声故障的问题） | | |

* 1. 多功能控制器

与前两个示例中的仪表相比，该示例的复杂度进一步提高。该示例包含了根据使用者为该应用开发的软件配置，使用多用途、高度可配置的设备来执行特定的一套功能的情况。

由于设备老旧并且难以获得备件，该公司认为必须更换现有的用于开关室的加热、通风和空调（HVAC）的气动控制系统。一个商品级的、基于微处理器的、多功能控制器被选择来取代气动系统。选择该特定设备的依据是它能够提供控制HVAC系统所需的闭环控制和开关功能。此外，它还包括一个整体的气动输出，可以控制现有的气动风门。将此多功能控制器的性能要求与供应商的指定性能进行比较，表明所要求的性能在供应商指定的范围内。

因为房间里有与安全有关的开关设备，所以HVAC控制系统与安全有关。因此，此多功能控制器必须经过适用性确认才能使用。

HVAC系统控制器所需的基本功能如下：

1. 监测开关柜室内的空气温度和室外空气温度（用于冬季通风和冷却）
2. 提供两种开关柜室内温度的控制模式，并根据外界空气温度自动切换。两种控制模式为：
   1. 冬季（室外空气寒冷）：通过调节现有风门，控制通风用的内部和外部空气的混合，对开关柜室温度进行比例-积分-微分（PID）控制
   2. 夏季（室外空气温暖）：提供空调压缩机的开关控制，以将开关设备室内的温度保持在控制范围内，并将室外空气风门固定在10%的开度
3. 以规定的（安全）方式对控制器的异常或故障情况做出响应

该替代控制器通过存储在可编程只读存储器（PROM）中的预编码功能块的软件互连，为用户提供控制策略的配置。特定应用的配置存储在非易失性存储器中，以防止发生电力中断时数据丢失。控制器配置和本地操作所需的数据输入键盘和数字显示器位于装置面板上。

使用者开发配置加载到控制器中以实现HVAC控制应用。该配置是遵循HAF003质量保证计划下开发的，遵循为安全相关软件的开发、验证和确认制定的程序。软件需求规格书定义了控制器软件的功能要求。根据这些要求开发配置，并根据这些要求为控制器的内置固件定义关键特性。同时，进行故障分析，检查可能的故障模式及其对开关设备HVAC控制功能的影响。这包括考虑GB/T 13629中所述的异常状态和事件。

控制器的关键特性和相关验证活动如表D.7、D.8、D.9所示。由于控制器的额外复杂性，以及为了满足作为多功能设备的使用为特定控制器进行的“软件配置”，使专用控制器所涉及的适用性确认活动比先前示例中所呈现的活动更复杂。

进行商业级供应商调查，以检查供应商的质量保证计划和软件开发过程。此活动需要在供应商现场进行，在此期间，调查小组可以查阅档案并与关键人员面谈；使用者向供应商支付技术支持费用。与上一个示例相比，该调查在许多方面进行了更详细的介绍。例如，它包括一个线程审计，在整个过程中跟踪选定的“线程”，检查从需求到设计、编码和测试的文档和可追溯性。审计检查供应商遵循的实际做法以及书面程序。如果供应商计划所要求的和公司所期望的文件有缺失或者不完整，供应商应纠正这些缺陷，并最终随交付的设备提供一套完整的文件。

调查小组还审查了控制器的设计，以及包括实时任务管理、程序控制和数据流在内的软件架构。特别回顾了诊断和错误检测功能（如看门狗定时器）的实现。对软件代码样本进行评审，以检查是否符合既定的编码实践，并支持线程审核。审查产品可信的运行历史记录，包括产品失效报告。发现供应商具有针对现场报告的有效反馈机制和强有力的纠正措施计划。审查产品缺陷数据库发现，现场约有1500件设备，在控制器的使用寿命内未报告软件相关缺陷。

该调查还检查了供应商的设计和质量保证组织，并评估参与产品设计、制造和支持的人员的资格和能力。

审查供应商的测试，包括在控制器软件的开发、验证和确认过程中进行的单元测试（单个软件组件的测试）的证据。特殊测试由使用者进行，以补充供应商的测试，并验证为该控制器开发的具体配置。特殊测试包括功能测试（可追溯到软件要求规范），测试控制器对预期异常情况的反应（例如，测试失去电源和各种输入故障条件下的安全行为），以及挑战测试，检查在各种异常状态和事件下的行为，包括输入瞬态的组合，以及操作界面使用的错误。

此外，为了帮助解决有关未检测到或未通知的故障的可能性的问题，本使用者对控制器进行编程，以在控制程序执行的任何时候在前面板显示器上显示连续闪烁的符号。这使操作员能够一眼检测到控制器是否在工作，或者程序或处理器是否停止。（电厂的操作规程包括由巡回操作员对开关设备室进行定期检查。）对操作人员进行培训，包括使用“心跳”指示器验证控制器的可操作性。此外，还确认在之前未检测到的控制器故障的情况下，其它独立指示和警报将提醒操作员采取必要的手动措施，操作员将有时间和手动控制能力采取手动措施，恢复开关设备室的冷却。

验收控制器并进行一系列适用性确认活动，记录关键特性、采用的验证方法以及验收控制器时所做判断的依据。总而言之，根据以下几个因素，使用者得出结论，控制器在其预期应用中的性能令人满意：

1. 调查发现，供应商遵循了系统的开发流程，并提供了合理水平的文件，尽管不完全符合HAF003的规定，但被认为是充分的；
2. 调查还发现，供应商具有良好的配置管理程序和错误报告方案，符合使用者的标准；
3. 故障分析、对产品的设计和诊断功能的审查以及特殊的测试显示了对设备可能的故障模式的良好覆盖；所添加的“心跳”指示提供了额外的保证，即任何意外故障都将被检测到，并且在控制器出现故障时可以使用操作员备份；
4. 成功的、可信的运行历史，主要是在非核工业的应用中获得的，这些其它领域的典型使用情况与此控制器在核电站中的计划应用功能是相关的；
5. 使用者根据安全相关质量保证和配置管理程序控制控制器特定应用配置的开发、安装和维护；
6. 通过调查、测试和检查以及产品性能记录的审查，充分验证所有关键特性。

这些控制器进入了使用者的经过适用性确认的商品级设备跟踪系统。这包括将固件以及硬件进行组态控制，未来购买替代部件或备件时将对适用性确认后的固件版本和要求通知的任何变化进行参考，从而使用者可以评估是否接受，或对修改后的产品重新进行适用性确认。此外，供应商同意将设备可能发现的任何错误或问题向使用者提供报告。

表D.7 多功能控制器的关键特性-物理特性

| **物理关键特征** | **验收标准** | **验证的方法** |
| --- | --- | --- |
| 配置   * 型号； * 软件版本号； * 尺寸； * 安装。 | 供应商型号。  供应商的软件版本号。  长x宽x高。  根据用户手册 | 进厂检验。 |
| 接口   * 气动供气连接； * 电源； * 输入信号； * 输入阻抗； * 气动输出； * 继电器输出； * 前面板接口（人机接口）； * *设定点调整；* * *触点输出。* | 根据用户手册。 | 进厂检验和测试验证正确的接口/连接类型、输入阻抗、人机接口功能等。 |

表D.8 多功能控制器的关键特性—性能

|  |  |  |
| --- | --- | --- |
| **性能关键特性** | **验收标准** | **验证方法** |
| PID控制能力，例如：   * PID可调范围； * 防复位发条； * 自动/手动控制能力； * 无障碍传输功能； * 程序周期时间； * 数据采样率； * 信号调节、抗锯齿等。 | 根据用户手册，包括对系统稳定性要求的分解，以根据系统稳定性分析确定PID可调节性、数字采样率和循环时间的要求，以及影响稳定性的信号调节电路的特性。 | 主要通过配置控制器的实用程序进行的特殊测试。此外，审查供应商文献，审查商业级调查期间的设计（特别是PID功能块），审查供应商对PID控制能力的测试。 |
| 切换控制功能，例如：   * 设定值可调性； * 滞后； * 响应时间。 | 根据用户手册。 | 审查供应商文献中的开关控制功能，商业级调查期间的审查；审查供应商测试文件；利用为本应用的特定开关功能配置的控制器进行特殊测试。 |
| 人机界面性能、易用性（包括操作、配置、维护和故障排除期间的使用）。 | 根据用户手册，包括操作要求、配置能力、维护和故障排除以及一般人为因素标准。 | 供应商文献审查、商业级调查期间的设计和操作审查、用户的特殊测试以及用户工程和操作的人因评估。 |

表D.8 多功能控制器的关键特性—性能（续）

|  |  |  |
| --- | --- | --- |
| **性能关键特性** | **验收标准** | **验证方法** |
| 环境兼容性   * EMI； * 抗震； * 温度； * 湿度。 | 根据用户手册或相关标准；  每个位置的响应谱；  根据用户手册；  根据用户手册。 | 第三方测试实验室报告。 |
| 异常/故障条件下的行为，例如：   * 功率损失和重新获得； * 一个或多个信号输入丢失； * 输入信号超出/低于范围； * 供气损失。 | 基于控制器故障安全条件的特定用户需求。 | 审查供应商测试，审查商业级调查期间的设计和软件架构，加上公用设施进行的特殊测试，以检查预期异常/故障条件下的行为，验证控制器的安全响应。 |

表D.9 多功能控制器的关键特性—可信性

| **性能关键特性** | **验收标准** | **验证方法** |
| --- | --- | --- |
| 内建质量：   * 设计和制造质量； | 供应商需维护一份涵盖设计和制造的质量保证方案，其中涉及的关键领域至少包括：   * QA人员和组织的定义； * QA计划和程序； * 具体的软件QA要求；   证明QA方案已应用于采购物项的生产（至少硬件制造）。  有文件记载的产品、，这些因素共同证明了设备的质量。  供应商目前遵循数字系统/软件开发流程，包括：   * 软件开发计划和组织； * 记录的设计要求，包括软件要求； * 需求可追溯性； * 文件化软件设计说明； * 记录的验证和确认计划； * 验证测试报告。   软件最新版本遵循数字系统/软件开发流程的证据。  记录的产品可信的运行历史，显示产品稳定性、可靠性，以及在类似应用中不存在与软件相关的关键错误或故障。这些因素综合起来证明了设备的足够质量。 | 商业级调查a，包括：   * 根据相关标准审查供应商QA计划； * 审查数字系统/软件开发、验证和确认、测试的供应商程序和实践。必要时编制补充文件； * 线程审计，以检查QA和软件开发与控制的实际实践； * 审查控制器设计、软件架构（包括实时任务）诊断和错误检测的管理和实施，例如看门狗定时器功能； * 审查软件代码样本，以检查是否符合既定的编码实践，并支持线程审计； * 审查拟采购控制器的特定型号的操作经验的范围、相关性和成功性b。 |

表D.9 多功能控制器的关键特性—可信性（续）

|  |  |  |
| --- | --- | --- |
| **性能关键特性** | **验收标准** | **验证方法** |
| * 失效模式和故障管理。 | 根据失效分析识别失效模式。(注：失效分析还用于帮助确定是否存在未审查的安全问题）。 | 故障分析从系统角度识别重要故障模式，并评估其重要性。作为商业级调查的一部分，对设备设计和软件架构进行审查，确定重要的内部故障模式和提供的诊断功能，包括看门狗计时器等项目，并评估故障对系统的影响。  故障分析确定，如果开关设备室温度因控制器故障而超出界限，则会有独立的警报提醒操作员，并且操作员有足够的时间使用手动控制功能采取行动。  审查产品可信的运行历史，以验证是否存在特定的关键故障b。审查供应商测试和特殊挑战测试的性能，这些测试旨在测试异常情况下可能出现的关键故障模式（例如，电源电压降低、噪声信号、功率和信号瞬变、输入信号故障组合、HMI错误等）。  只要控制程序正在执行，对设备进行编程以显示“心跳”指示，就可以进一步确保检测到控制器故障。 |
| 配置控制 | 供应商有一个配置控制程序，包括：   * 记录的计划和程序； * 基线维护； * 变更控制； * 错误报告过程。 | 在供应商调查期间对配置控制程序进行审查a。 |
| 问题报告 | 供应商具有错误报告程序，并将向使用者提供报告。 | 在供应商调查期间审查错误报告程序a。 |
| 可靠性 | 在规定的环境条件下证明足够的可靠性和可用性 | 审查供应商的测试报告或分析报告。审查产品可信的运行历史，以证明可靠性b。 |
| 1. 如果证实之前的调查充分涵盖了该应用的特定关键特性，包括设备重要失效模式所需的信息，则可使用该公司或其它公司的书面调查（例如存档）。 2. 与前面示例中的仪表相比，控制器的产品操作历史回顾更为复杂。调查证实，有一个强有力的计划来记录现场对服务中任何问题的反馈。固件在最近的可信的运行历史中一直保持稳定，其中许多单元在许多不同的应用中运行。尚未报告与软件相关的故障。因为控制器是多用途设备，建立操作历史的相关性涉及确定控制器的许多其它应用程序使用与计划应用程序相同的功能块。在这种情况下，功能块是标准的PID控制和切换功能；根据与供应商和控制器的选定用户的讨论，确定使用这些功能的应用程序具有重要的操作历史。 | | |