SIS 203

验证和确认

15 分钟

概述

我们都知道再好的设计也要看执行的情况是否理想。这也是为什么仅仅设计符合安全要求的安全仪表系统（SIS）是不够的。您必须确保

- 设计中的每一步都能够符合安全要求说明（SRS）中相应的适当要求。
- 安装的 SIS 要能够实现其安全功能。

这里要介绍两种工作：**验证**和**确认**。验证在整个安全生命周期中的每一步都会发生，而确认则是在系统安装好后，在其投入运行之前所要做的工作。

这两项工作都有助于您从 SIS 中去除尽可能多的**系统故障**。与因设备停顿而发生的随机故障相反，系统故障是指那些因人为失误而“内置”到系统中的故障。

本课程将向您展示验证和确认工作是如何确保 SIS 在符合安全要求说明（SRS）的情况下正常工作的。你也将学习到如何构建验证和确认以使其更加容易管理，以及优秀的文档规范如何帮助您生成（并维护）相关文件，以证明您的 SIS 设计正确、执行正常。

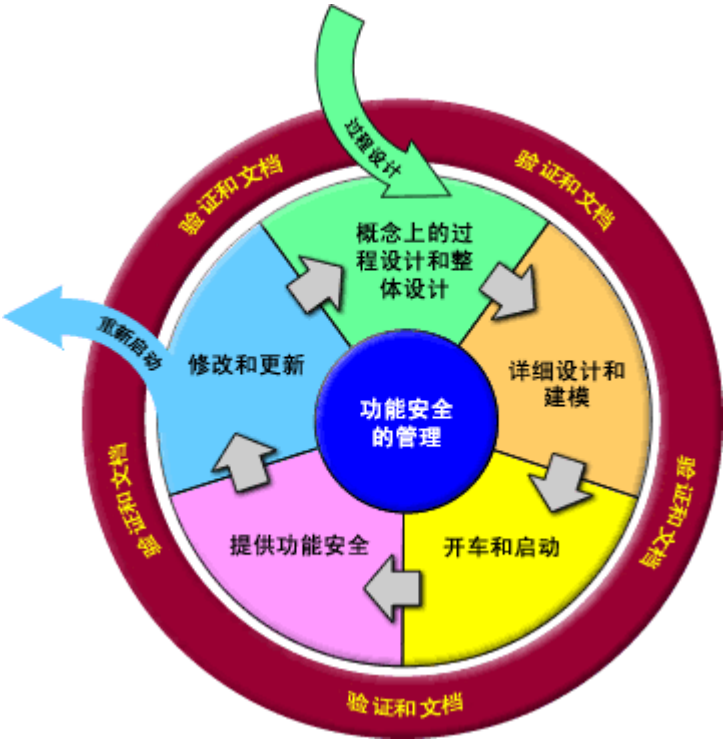
提示

当您在学习本课程时，请注意以下方面：

- 验证和确认之间的不同之处
- 怎样将 SIS 分解成子系统
- 类似于 IQ-OQ-PQ 的验证模型是怎样起作用的
- 您的测试计划需要包括什么
- 良好的文档有什么好处

验证

在安全生命周期的每个阶段的最后都要进行验证。它将验证所做工作是否已经达到了预定目标，满足其特定要求。



验证（以及结果的文档记录）在安全生命周期的每个阶段都要进行。

验证可以通过分析、测试或两者混和来实现。其过程可包括

- 对安全生命周期的各个阶段的文档进行回顾，确保符合目标和要求。
- 设计回顾
- 对已设计的产品进行测试，以确保其性能与说明书一致。这对那些会重复使用好多次的模块化部件来说——比如投票器算法代码——特别有价值。
- 当系统的不同部件被整合起来时，要进行综合测试。

验证过程和其结果需要被完整地记录，以证明其不仅设计符合要求，而且您检查并确信其能正常工作。当然，这些记录也要有必要的整理。

确认

确认是建立在验证基础之上的，而且还要包括对整个 SIS 的完整测试以确认整个系统工作正常。一旦确认，则说明不仅 SIS 本身，还有 SIS 的每一项安全功能都符合了安全要求说明（SRS）。

在系统安装完毕并开始调试完成后，验证工作就可以在整个项目中进行。而且那里工作完成，那里的验证就结束。而确认却仅在现场才能进行。

确认试验还要包括…

- 系统功能要能够在相关的操作模式（启动、关断、自动、半自动等等）下正常工作。
- SIS 要能够在 SRS 定义的正常和非正常模式下让人满意地工作。
- BPCS 和其他相连的系统不得影响或限制 SIS 的反应能力。
- 传感器、逻辑运算器和终端控制部件（包括冗余回路）要能够按照要求正常工作。
- 在遇到诸如传感器超量程等不合理的过程数值时，SIS 应能够相应地进行调整。
- SIS 要能够在电源、仪表气源或液压失效或者重启的时候，按照设计要求工作。

确认试验不仅要求有精确的计划以鉴别和记录流程、手段和将要用到的实验，还要求有这些实验的顺序、进度表以及操作人员的资格认证。

这是一项要占用大量资源的浩大工程。但当您知道 SIS 的存在将保护您的社区、邻居、家庭、合作者和环境的时候，少做任何一点都不可以。

幸运的是，我们有办法可以使得以上任务更加易于管理。

结构化的解决之道

您一定还记得，IEC 61511 定义了您做**什么**和为什么要这么做，但让您决定怎样来实现。只要您能够提供书面的证据证明 SIS 符合 SRS，您可以根据您自己的情况组织和实施验证和确认过程。

但与其自己费时费力去开发一种单独的确认方法，还不如采用在业界已经广泛使用的方案。一个在业界被广泛使用的例子是由美国食品和药品管理局（FDA）提出，用来确认基本过程控制系统的结构化解决方案，尽管其没有被 IEC61511 定义过。

这个易于理解、有据可查的模型将整个工作分成了三个阶段：**安装确认（IQ），操作确认（OQ），以及性能验证（PQ）。**

<graphic file: sis203_IQ-OQ-PQ_150x275.gif >

- **安装确认**测试并记录了 SIS 解决方案中的每个物理部分——包括设备和子系统——是否都正确安装。该项工作在给系统上电前就已经完成。

  仍旧以我们在前面课程中介绍的氨水罐为例，IQ 包括了确认罐体上的压力传感器处于正确的模式，有与安全相关的必要文件，已根据设计和制造商的说明进行安装，连线正确，所有的开关和跳线设置正确。

- **操作确认**测试并记录了 SIS 解决方案的每个硬件和软件部分是否正常工作。和 IQ 一样，OQ 的测试也包括了设备和子系统。

  例如，您要检查每个传感器电压是否正确，阀门控制器的部分行程试验设置是否正确，以及逻辑运算器是否已下载其设置并报告正常。

- **性能确认**测试并记录了 SIS 作为一个整体能够根据 SRS 执行规定的安全功能。

  PQ 是对流程、人员、过程以及整个 SIS 的一个集中测试。该项验证只会在测试 SIS 的物理（硬件）和功能（软件）部分的所有 IQ 和 OQ 完成之后，才会进行。任何在 PQ 阶段发现的问题都要进行调查、修理并记录。

因为 IEC 61511 所追求的是将良好的规范加以应用，以取得一个具有鲁棒性的解决方案。所以采用现有类似于 IQ-OQ-PQ 的良好规范比自己独创要更有意义。

您还可以对安全功能一个一个地进行试验，从而进一步简化您的工作。下面我们将向您介绍对系统的“分解”。

系统分解

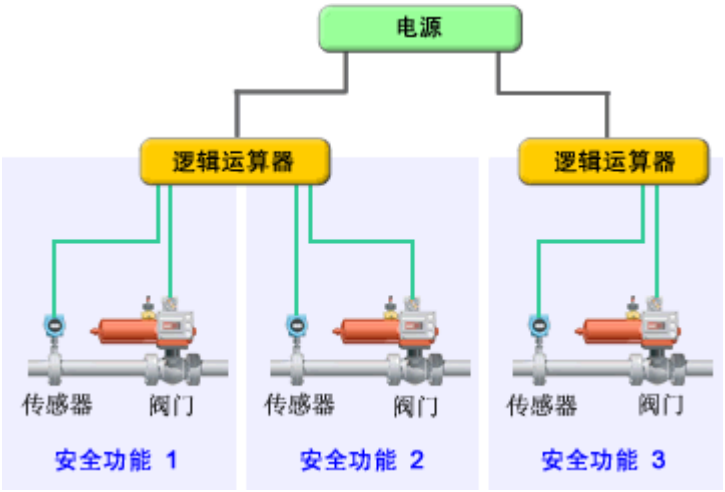
对一整个系统进行验证和确认看上去是（确实也是）一项让人头皮发麻的任务——除非您能够将其分解成易于处理的条块。

一种方法是将 SIS 按照安全仪表功能（SIFs）进行**分解**，并鉴别出实现每个单独 SIF 所需的设备和子系统，从而可以对每个部件进行单独检视。这将会给鉴别和记录必要的技能、测试设备和与测试相关的结构，以及对特定的部分和子系统签字认可带来方便。

例如，您将会发现一些部分或子系统，诸如传感器和终端控制元件等，是专门针对某个特定安全功能的。而其他比如交流和直流电源、接地系统，以及通信等，相对而言更加“通用”。

您首先要努力确认通用元件对所有的安全功能给予了必要的支持。一旦您验证确实如此，您就可以对针对每个安全功能的元件进行测试，以证明其工作正常。这种方法避免了对每个安全功能相同的通用元件进行重复测试。

例如，对下图的系统进行分解，使您对电源仅需进行一次验证。对由其支持的每项安全功能，就无需再做同样的测试。



同样的原则也可运用到上图左边的逻辑运算器。一旦您已经确定其通用的功能工作正常（例如，无诊断错误，电源供应正常，网络工作正常），对该运算器支持的每个 SIF 您就无需重复测试这些相同的功能。然而，您必须确认，每个 SIF 都是按照安全要求说明（SRS）工作，且工作正常。

将系统分解成部件和子系统也有助于您更加方便和有效地使用来自生产制造商、第三方顾问和公共资源，以创建您自己的测试计划。

例如，如果要对经安全认证的压力变送器作一个 IQ 测试的计划，可以借鉴制造商的有合适 IQ 签单认可的安装文件。

与此类似，压力变送器的 OQ 测试计划同样也可参照制造商的安全手册和标准。

PlantWeb 的优势

艾默生过程管理公司的公共网站提供了大量的资料，可帮您达到 IEC 61511 标准。

例如，如果您想制定对罗斯蒙特 3051S 系列压力传感器的 IQ 和 OQ 测试计划，您可以访问 www.rosemount.com/document/ 并下载该器件的安装指南。该指南中包括了该器件在安全仪表系统中的使用章节。

有关其他 SIS 产品的类似信息也可在线查询到。建议您首先从www.EmersonProcess.com/SIS 开始搜索。

测试计划

每个阶段的验证和确认都必须证实一点，即相应的开发阶段完全满足其预定目的。要实现这样的目标，您需要完整和严格的计划。

例如，您应当考虑和证明

- 测试策略——包括测试内容，预期结果和怎样进行偏差修正
- 测试过程——包括了测试结束的标准
- 人员要求——数量、持续时间以及需要的技能
- 技术要求——工具、分析仪器以及需要的支持软件。

尽管一般而言，在您接受产品之前，SIS 设备供应商应负责对集成软件和工具软件进行测试，但您的计划还是应该包括当诸如因操作系统、部件、固件和通信协议变化（包括升级）时，如何对已安装的设备重新进行测试。

将测试试验交给那些非设计和执行该系统的人员进行也是一个很好的办法。因为这些独立的测试者更有可能以一种设计者和执行者都没有预计到的方式对设备和软件进行操作，比如输入合法和不合法的数据值。

请牢记 IEC 61511 标准并没有定义**怎样**实现以上测试，所以您可能要向其他方面进行咨询，或者征集外部的帮助，从而制定一个综合的软件测试计划。

您无需因向他人求助而不安。专业的供应商和顾问能够提供相应的工具和专业知识，从而帮助您更加容易地达到 IEC 61511 标准。另外，新的技术和产品设计会简化甚至自动完成测试和文档的很大一部分工作。

PlantWeb 的优势

除了易于获得的文件可以帮助您达到 IEC 61511 的标准之外，当您需要额外的资源或者专业知识时，艾默生还可向您提供其经过专业认证的安全专家。

验证和确认工作还可以从内置于艾默生智能 SIS 的技术中获益——从简单的设备安装确认、设置和操作状态到系统设置变化的自动存档。

文档整理

在这几次课程里，您已经知道 IEC 61511 需要对 SIS 安全生命周期里的每个阶段和活动都进行存档。

对每个阶段文档都应该说明输入什么，目标是如何实现的，以及输出是否符合要求。简而言之，这就是您的证据，证明您确信该安全解决方案已经建立，适合并确实能够对减少已知的有害事件发挥作用。文档在验证和确认中特别重要，因为它能够证明工作 SIS 确实符合要求。

对要使用和维护的文档，需要进行精心地组织和整理。良好的存档规范，例如在 ISO 9000 质量管理标准中定义的那些规范，是用来确保对文档的创建、回顾、批准、分发和保存的控制。尽管 IEC 61511 标准并没有特别规定文档应如何整理，但一般还是要有下列内容：

- 对有害事件和风险评估的结果
- 在确定安全整合水平时用到的假设
- 安全要求说明（SRS）
- 文档和 SRS 之间的溯源性
- 包括使用经认证的模块在内的应用逻辑

- 设计文档
- 更改信息和文档
- 验证和确认的记录
- 调试和 SIS 确认程序
- SIS 操作程序
- SIS 维护程序
- 检验测试程序
- 评估和核查结果

“完成文书工作”在一般人的日程安排里优先级别一般不高，但是它确实是 SIS 项目必不可少的一部分。如果要对出现的事故进行调查，则您的 SIS 文档将有助于查明哪里出错，怎样才能在以后防止或减少类似的错误。

您当然可以将其他的一些文书工作丢在一边，但无论如何不可以是 SIS 文档。

PlantWeb 的优势

艾默生过程管理公司的智能 SIS 包括了简化文档创建和管理的功能，例如：

- DeltaV SIS 组态管理器（Configuration Studio）包括了备有完整证明的、经 TÜV 认证的功能模块，应用逻辑文档器，登陆密码保护以及自动核查追踪功能。
- AMS Suite 设备管理组合软件提供了登陆密码保护。它能够自动对将要进行的检查和测验进行提示，追踪验证测试和检查的结果，以及对现场设备的参数变化进行报警和追踪。
- 与 费希尔 FIELDVUE DVC6000 数字阀门控制器配套的阀门可以设置成自动进行部分行程测试，而且其结果可通过 AMS 设备管理系统进行记录和报告。

小结

在本课程中，您已经学过：

- 通过验证和确认，可以确保 SIS 符合安全要求说明（SRS）。
- 验证在安全生命周期的每个阶段都会进行。它保证了每个周期的工作都符合相应的要求。
- 确认仅在系统被安装和调试完毕之后才进行。它说明整个 SIS 都能够执行其安全功能。
- IQ-OQ-PQ 模型提供了一个成熟的模型，从而将验证和确认工作分成了几个逻辑（和易于管理的）阶段。
- 系统分解提供了一个额外的方法，可将整个工作分成几个易于管理的部分。
- 计划所有验证和确认所必需的测试从根本上来说是一项主要（也是非常重要）的任务。
- 每一项测试及其结果都必须存档，而且所有的文档都必须可用，并易于维护。