SIS 202

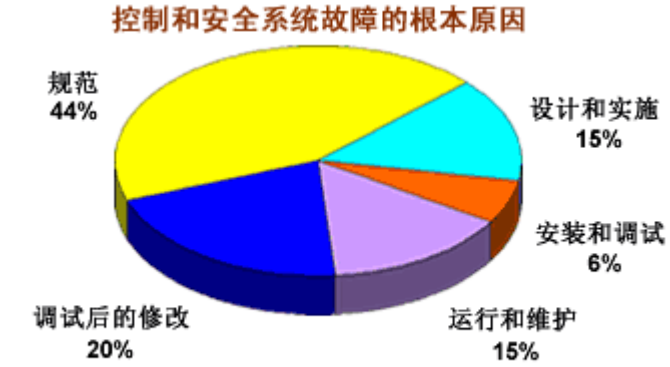
功能设计

15 分钟

概述

在前面的课程中，您已经学过了 SIS 的硬件方面。现在，我们将关注功能（软件）方面。

您可能会认为，软件问题应该很容易解决。但在安全系统里，保证系统正常运转是非常重要的。 大约有一半左右因控制和安全系统失灵的事故来源于设计上的错误或欠考虑的决定。所以在这一点上，优秀的设计决定了 SIS 能够在多大程度上胜任给定的工作。



来源：安全与健康管理

本课程将简要介绍确保您安全系统正常工作软件关键的几个方面。

提示

当您学习本课程的相关主题时，请特别注意以下方面：

- 安全系统软件的三种类型各是什么？
- 软件发展“V 形模型”的两方面各是什么？
- 使用经过验证的 SIS 软件模型有何好处？

软件类型

IEC 61511 标准定义了以下三种软件类型：

1. **应用软件：**专门用于 SIS 解决方案的软件。换句话说，就是系统的配置。
2. **工具软件：** 您用来开发、验证和维护应用软件的软件工具。
3. **集成软件：**那些 嵌入在 SIS 产品里的软件（也被称为固件）。

工具软件和集成软件一般会由仪表和控制系统制造商作为其产品的一部分予以提供。当这些产品经认证可用于 SIS 时，一般由供应商承担主要责任确保软件与 IEC 61508 标准兼容。

另一方面，尽管会有顾问和集成者的帮忙，但确保应用软件达到规定的要求则是您的责任。

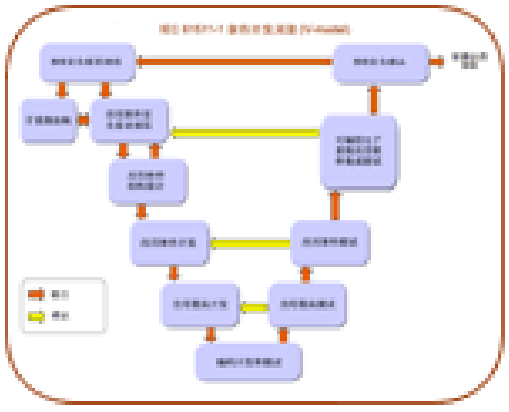
研发生命周期

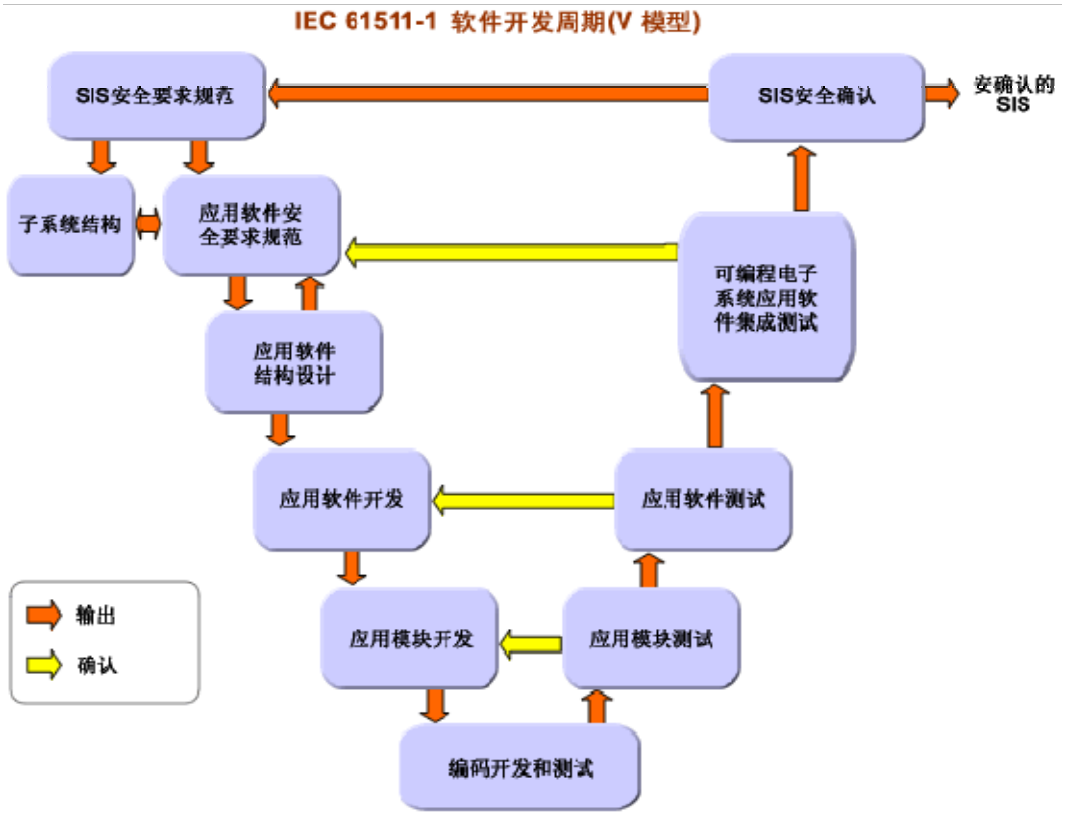
计算机巨头 IBM 使用 “1-10-100 定律” 来说明优秀的软件设计的重要性：在设计阶段少用 1 美元，则在测试阶段为了改正错误就需要 10 美元，到了软件发售的阶段，改正错误就需要 100 美元。

在安全应用领域，代价可能会更加高昂——特别是考虑到有人身伤害事故的情况下。这也就是为什么从一开始就要强调确保软件质量的重要性，并在软件的整个研发过程中一直进行验证工作。

IEC 61511 允许您在研发用于 SIS 的应用软件时有一定的自由度。然而，它也要求在软件的研发过程中要仔细构架，以避免产生导致运行中出现危险故障的工程失误。它还要求对软件进行验证和确认，以保证软件应用解决方案的实际表现与设计文档保持一致。

标准中还包括了流行的软件研发“V 型模式”，并说明了必要的步骤以确保上述目标能够实现。V 型的左边为软件研发行为，右边为相应的验证和确认行为。





该过程从安全要求说明（SRS）开始，通过详细的设计说明和研发过程相继进入各个阶段。而一系列不断增加、内容广泛的测试则对每阶段工作是否符合安全要求进行了验证。在过程的结尾，成功的集中测试将会得到经过验证的软件。

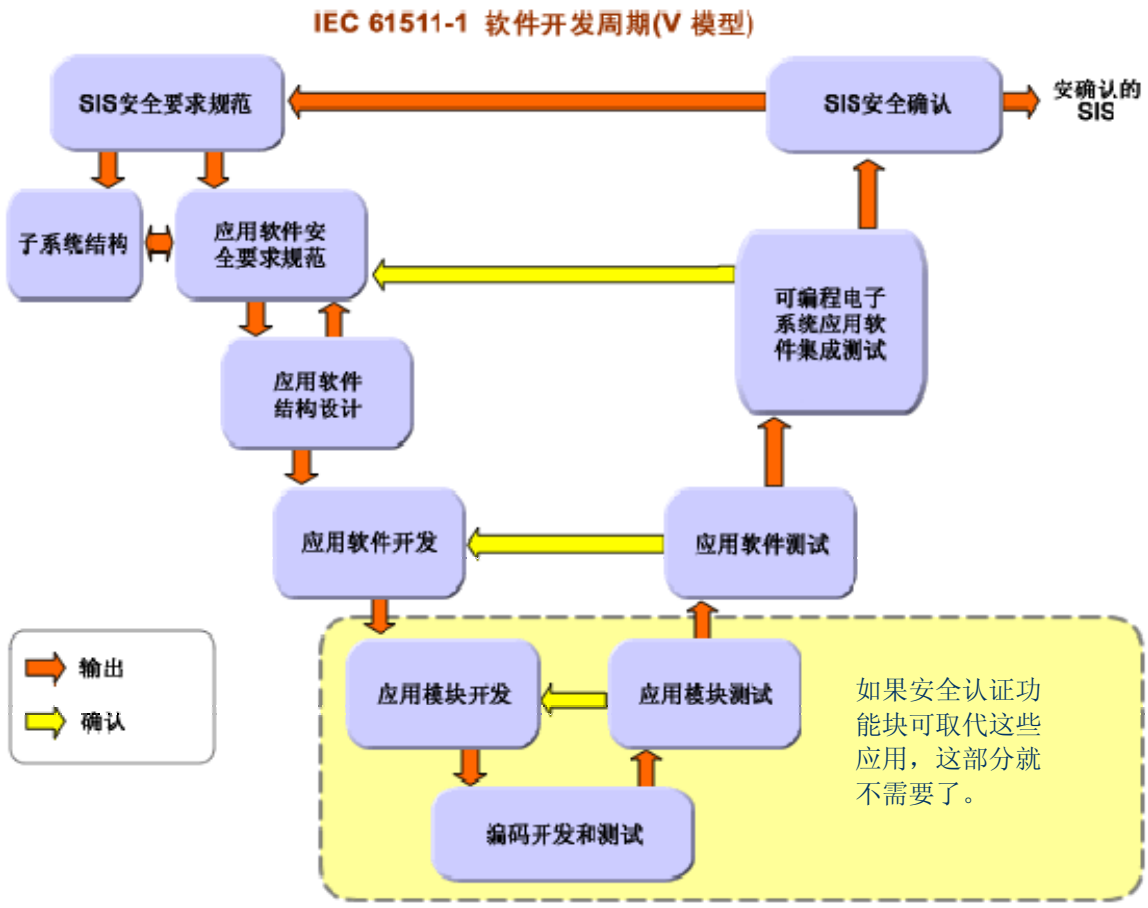
该过程——包括测试计划和文档，将在下一课程 **SIS 203 - SIS 验证和确认**中详细说明。

经认证的软件模块

现代软件设计一般使用一次编写但可重复使用的模块化代码，以节省时间和成本，并避免多此一举带来的错误。

IEC 标准向您提供了两个选择：建立并验证您自己的应用软件模块库，或者使用预先设计、测试、并经第三方认证的模块。

当您使用由 SIS 产品制造商提供的经过认证的模块时，您不仅可以节省时间和成本，对其每一个模块您也不用再去测试。供应商和第三方认证机构已经为您做好了这一切。



一旦您选择自行开发您自己的应用模块，您应当了解，IEC 标准对这些可重复使用软件模块的设计、开发和测试，都有非常严格的要求。

应用软件模块至少应该是能够被证明有一定的严密性，并且其开发者应承担确保其正常工作的责任和风险。

PlantWeb 的优势

作为艾默生智能SIS的一部分，DeltaV SIS 系统包括了一个经TÜV认证的完整功能模块，这其中有表决器（Voter），因果关系矩阵（ Cause and Effect Matrix），步进顺序器（ Step Sequencer）和状态转换表（ State Transition Table）。

强大的智能功能模块，比如可扩展的MooN (M out of N) 表决器模块（Voter blocks）及内置的旁路功能将过去需要的很多梯形逻辑减少为仅需一个简单的拖放设置即可。

其他的DeltaV SIS 软件功能，包括符合EEMUA 191标准的警报状态引擎、离线仿真、事件序列记录仪、旁路管理和超调限制，使SIS维护更加简便容易。

所有的这些内置的功能能自动与IEC 61511标准相符，这样就简化了对文档的要求，也降低了在整个生命周期中的投资和风险。

软件应用工具

和其他工艺一样，软件开发也有特定的工具以加速和简化开发工作。

IEC 61511 标准还包括了诸如应用编程语言、设置管理工具、仿真、测试工具和标题为**软件应用工具**的自动全面测试工具 。该标准允许您以较大的自由度去选择这些工具，包括您使用和开发的工具在内。

然而，在任何工具（不管是购买的还是您自行开发的）被用于去帮助达到 IEC 的标准之前，其工具手册必需仔细说明以下几个方面：

- 怎样使用工具
- 使用限制
- 已知的缺点
- 发放的限制

…以及类似的主题。

因为应用开发工具的重要性，IEC 61511 标准要求有一个能够检查编程和语法错误的**成熟软件语言转换器/编辑器**，而且自身还不能有错误。

PlantWeb 的优势

在艾默生智能 SIS 中一个关键的软件应用工具是 AMS™ 设备管理组合：智能设备管理系统, 它可以使您在现场设备的安装时进行正确的设置。它的快速检测（ QuickCheck ）功能通过允许您在固定校验模式下同时设置几个仪表而简化了互锁的确认过程。 当 SIS 被修改时，它也可以用来比较新旧设备组态。

对以上功能和其他功能的第三方研究，可参见“AMS 安全分析：在安全仪表系统应用场合中使用 AMS 设备管理组合 ”。
<www.emersonprocess.com/sis/resources/ams_safety_analysis.pdf>

小结

在本课程中，您已经学过：

- 为了避免安全问题被“设计”到 SIS 中，良好的软件工程是必要的。
- IEC 61511 定义了三种软件类型：应用软件、工具软件和集成软件（也被称为固件）。
- 一般而言，供应商主要对工具软件和集成软件承担责任，而您应当确保应用于特别场合的软件与标准兼容。
- 对软件设计和开发的每个阶段，都要有相应的测试阶段去验证软件是否符合相应的要求。
- 使用预先经过认证的软件模块，可以减少开发和验证的时间和成本。