SIS 303

停用

15 分钟

概述

停用安全仪表系统可以看成是更改的一个特例，这意味着要满足 SIS 302 中讨论过的全部要求。

然而，在 SIS302 中我们介绍的更改一般都比较小，倾向于维持甚至增加安全。另一方面，当我们停用一个 SIS 时，从一个单独的安全功能到整个安全系统，我们**去掉了保护层。**因而我们需要确认剩下的部分

- 对仍存在的有害事件有足够的防预
- 没有被我们移除的软硬件所干扰（或削弱）
- 在不搞乱“失效”代码层的情况下，仍然可有效地进行设置

提示

当您在学习本课程中的相关主题时，请特别注意以下方面

- 全部和部分停用的区别
- 停用计划应包括的内容
- 停用软件好的和不好的方法
- 测试、确认和文档整理的作用

整体还是部分？

SIS 停用既可以**全部**，也可以只是**部分**。

仅当 SIS 提供的保护不再需要时，才需**全部停用。**典型的情况是 SIS 所服务的过程不再被使用了。

在以上这个案例中，停用相对简单明了：工厂停工，SIS 被移走。可能还会有些人身方面的风险，例如来自有害化学物质方面的。但过程方面的风险没有了，因为连过程本身都不再存在了。

部分停用一般发生在为减少 SIS 提供安全功能的数量而进行的过程更改中。例如，换用一种危险更低的添加剂或消除一个放热反应等。

对于这种情况，在不影响那些保护系统免于尚存风险的设备情况下，停用包括了从 SIS 中移除不再需要的 SIS 传感器、终端控制元件、逻辑运算器以及软件。

要想确保您移除了应该移除的部分，且***仅仅***是应该移除的部分，您应该认真细致地进行计划。

停用计划

IEC 61511 标准要求在停用前，有资格的相关人等应一起制定、评估并通过一个完整的停用计划。计划应该包括

- 由谁来鉴别、监管、实施、批准相关的停用行为和重要节点，以及该如何去实施
- 对仍在的 SIS 功能安全如何进行评估，这其中包括了对有害事件和相关风险评估的一个更新的审查
- 如果在过程运行时就要进行停用，如何保持一定的功能安全
- 一个物理单元的停用是如何影响相邻的操作单元及设施的服务和应用。

该计划还需包括一个对安全要求说明（SRS）文档详尽的前后对照，并且要鉴别出哪一段文档和其他文档受到停用的影响。

总而言之，停用计划对细节的重视程度要和对原始 SIS 设计和任何更改一样。

软件问题

保留或去除传感器和终端控制元件的标准和程序相当简单明了。停用软件相对而言更复杂一点，因为不同代码之间的相互关系相对不怎么明显。

没有死码. 我们常犯的一个错误是认为这些无用的软件“总有一天会用上”。其实，没有用的代码必须要被清除或重构。

软件审查员不喜欢我们称之为“死码”的软件留在逻辑运算器里。特别是对 SIS 软件中的死码，他们将难以容忍。除了将安全功能审查复杂化，死码还带来更多的系统故障。如果没有软件，则不会出错或者干扰安全功能。也就不会占用处理器时间来扫描和执行，占用存储器来储存。

同样地， 虚假或虚拟的输入被认为是不好的做法。例如，如果一个“**与**”门包括了一个已经停用的输入，则最好不要将其用一个记录值来替换。相反，最好是根据剩余的 SIS 逻辑的需要，用合适的输入量重新构建该“**与**”门。

“这是做什么的？” 您不仅不应当将老程序留在系统里，您也必须确信您没有把系统需要的 SIS 功能移除。您可能会发现您要经常要发问：“如果我的行为妨碍了 SIS 正常工作，那该怎么办？”

如果您有我们在每一课程里都涉及到的文档——从原始要求和设计规格到任何更改的详细记录，您将更容易回答这个问题。但是如果没有这些文档，您只能对软件进行逆向工程，甚至要猜测每一行代码的意思。

清楚、精确、全面的文档将使得以上工作更加简便、更快捷和更安全。您花在设计、应用和归档软件上的所有时间将在您停用部分软件时，给您带来莫大的好处。

PlantWeb 的优势

DeltaV SIS 会存储和执行在独立软件模块中的每一项安全仪表功能（SIF）。所以如果您想停用一个 SIF，您仅需将其所在的独立模块移除，而不必担心影响其他 SIF。

DeltaV 的版本控制和审查追踪器（ Version Control and Audit Tracking ）可以自动记录所有变动，因而相应的文档整理也更加容易。

测试

停用阶段的测试和在 SIS 生命周期更早阶段的测试一样重要。

制定停用计划的相关人员应当回顾当初用于调试 SIS 时的测试计划，根据需要进行修改，并在必要时制定全新的计划。但与确保由剩余 SIS 提供的功能安全相关的任何事情都不能缩水。

如果在过程运转中，就要对 SIS 进行停用，您可能需要用中间测试计划。例如，如果只是在白班停用，而 SIS 在第二班和第三班提供功能安全，则为了确保 SIS 能够覆盖到第二班和第三班，需要重新进行中间测试。

重新确认

正如我们在 SIS 203 中所学到的，确认是证实 SIS 按设计工作的一种行为。它包括了一个完整的输入输出测试，且该测试包括一个与 IEC61511 兼容的 SIS 解决方案。

一旦部分停用结束，则任何可能受影响的剩余安全功能都必须重新确认。对一些系统而言，这意味着将要重复全面功能安全确认测试。

文档整理

显然，停用行为也要进行归档整理，而且其标准与 SIS 相关其他工作的标准要一致。

我们也已经知道先前的文档对停用工作的重要性。在当前的文档确实反映了当前 SIS 状况的情况下，停用计划的可靠性就大大增加了。

相反，如果 SIS 文档不能反映当前状况，除非有一个完整的 SIS 审查且所有提交的文档说明 SIS 已达到了设计状态，否则停用计划必须停止。

小结

基于同一理由——细微的错误可能导致人身事故，SIS 停用需要和生命周期其他阶段同等程度的精心计划和对细节的关注。在本课程中，我们已经学过

- SIS 停用，特别是部分停用，其最主要目的还是为了对剩余过程中的风险有足够预防保护措施。
- IEC 61511 要求在停用前，有一个经过批准的完整停用计划。
- 在停用 SIS 软件时，特别注意只能移除特定的代码，让剩余的代码刚好完成 SIS 的功能。
- 测试和确认对 SIS 停用来说，和将其投入运行一样重要。
- 良好的归档整理不仅仅是一种要求，它使得停用更为简便容易。