SIS 103

安全标准

15 分钟

本课程将向您介绍:

O 概述
1 新的解决方案
2 从 IEC 61508 到 IEC 61511
3 什么是 S84?
4 生命周期模型
5 在 61511 标准下应用生命周期模型
6 符合标准的条件
7 符合标准的好处
8 小结

概述

如果您的工厂或生产过程还没有使用过 IEC 61508、 IEC 61511 或者 ANSI/ISA S84.00.01-2004 这样的安全标准，您可能会在不久的将来用上它们。

尽管一开始您可能会认为这些标准会导致更多的文书工作、争论乃至麻烦，但实际上这些标准将会在确保并维持您工厂安全方面发挥极为重要的作用。其规范的解决方案可以使您的过程控制系统、操作和维护程序以及安全设备系统能够协调工作，从而进一步优化操作性能。

本课程将向您介绍几个最相关的安全标准——IEC 61508、 IEC 61511 和 ANSI/ISA S84.00.01-2004 —— 并向您说明为何符合这些标准即可提升您工厂的性能。

字母缩写的含义

IEC – 国际电工委员会 <www.iec.ch>
ISA – 仪表、系统和自动化协会 <www.isa.org>
ANSI – 美国国家标准学会 <www.ansi.org>

提示

当您学习本课程中的相关主题时，请特别注意以下方面：

- 安全标准的变革
- 如何选择最适合的安全标准
- 建立基于标准的生命周期模型的好处
- 执行标准需要的条件
- 执行标准的主要好处

新的解决方案

以前，安全标准只是应用在特定的应用场合、工业和国家。例如 ANSI P1.1-1969 就是由美国国家标准学会制定，用于纸浆、造纸和纸板工业的统一标准。

这样做的主要问题是各个工厂乃至整个产业发现自己要遵从多种重复的安全标准，而且这些标准从设计到构架常常是基于完全不同的理念。再考虑到国家或地区标准的差异，完全执行这些标准几乎是不可能的。

更新的安全标准则关注在安全项目生命周期内的每一个执行阶段都能够降低风险并定义相应的可操作等级。

这种以性能为导向的**生命周期**方法生成的标准与其他标准更加容易结合，所以也能得到更广泛的推崇和接受。这也使得以尽可能少的成本取得高质量结果成为可能。

对于过程工业，相关的安全标准为 IEC 61508、IEC 61511 和 ANSI/ISA S84.00.01-2004 (S84)。 这些标准都定义了达到标准所需的**条件**，但是对于工厂业主和操作人员来说，IEC 61511 和 S84 并没有说明**怎样**才能够达到这些标准。

从 IEC 61508 到 IEC 61511

那么，为什么IEC 有***两个***安全标准呢？

IEC 61508 (第1 – 7部分)的标题为 *可编程电子安全系统的功能安全*，是针对工业领域产品制造商和应用商的一个全面综合的、以性能为导向的功能安全标准。

在欧洲，IEC 61508的七个组成部分以EN 61508的形式出版，任何与其冲突的CENELEC 或 CEN 国家标准都被随之而孤立。

IEC 61508 曾被一些过程工业工厂用于执行安全仪表系统（SIS）。但早期的过程工业在采用该标准之后发现其相当麻烦，并且该标准对过程工业如何达到其要求的阐述不甚明确，有太多的模糊空间。

在慎重考虑之后，IEC标准委员会选取、协调并重新编写了IEC61508的相关章节，形成了专用于过程工业的IEC 61511。

IEC 61511 提供了对过程工业如何执行标准的指导以及举例说明，同时还确保了该标准与IEC 61508框架的一致性。

这样一个解决方案使得IEC 61511——*功能安全：用于过程工业的安全仪表系统*，成为了过程工业的不二选择。其影响力可以从中国、爱尔兰、意大利、印度、挪威、英国和美国安全代理机构不断增长的参考资料、由最终用户在各种讨论会和座谈会上提交的文献数量以及控制系统制造商网站上被提及的次数中即可看出。

尽管如此，工厂还是可以选择采用 IEC 61508 标准，其方法是选用仪表和控制系统制造商开发和销售的符合 IEC61511 的 SIS 认证设备 。

什么是 **S84**？

IEC 61508 和 61511 已经取代了很多国家标准。其中一个就是曾在美国广泛使用的 ANSI/ISA S84.01 安全标准。

几年前，在一连串的让人身心具疲的事故之后，过程工业领域的安全专家开始对现有的安全标准进行了一个彻底的回顾。

导致安全标准改进的事故		
1968	Pernis 炼油厂，荷兰	2 人死亡， 85 人受伤
1974	Flixborough, 英国	28 人死亡，上百人受伤
1976	Seveso, 意大利	700 人受伤
1984	Bhopal, 印度	2,500 人死亡, 100,000 人受伤
1998	Piper Alpha, 北海	165 人死亡，61 受伤

从以上悲剧中得出的结论之一就是现存的标准太过于专注于各自的行业，限制了安全专家们之间分享他们的实际经验。

根据这些发现，人们决定成立 ISA SP84 委员会。委员会成员立刻认定，应当采用一种更合适的标准方案来使用基于性能的生命周期模型。他们的辛勤工作换来了 ANSI/ISA S84.01-1996，*过程工业系统中安全仪表系统的应用*（S84）。

最近以来，S84 已经与 IEC61511 实现兼容，唯一例外的是：ANSI/ISA S84.00.01-2004 包含了一个“祖父”级的条款，只要设计、维护、检验、测试和操作符合安全标准，则允许当前使用的符合 S84 1996 版本条款的安全设备继续使用。

因而，除非您已经使用了 S84，您的最佳选择还是放弃陈旧的 ANSI/ISA 标准，采用 IEC 61511—和 S84-2004 等同。

生命周期模型

生命周期模型为我们提供了一个过程序列，可用于对产品或服务的创建和升级。

生命周期模型有很多种形式，但每一种模型都会提供一种结构，可用于完成种种与创建或管理一个复杂产品或服务相关的任务。
< graphic file: sis103_lifecycle-generic_211x210 >

基于生命周期标准的主要好处就是它易于支持和整合其他基于生命周期的标准和惯例。正如下表所示，这样的模型被很多管理机构或其他实体所使用或推荐。

推荐使用生命模型的组织和机构	
国际标准化组织(ISO)	产品和服务质量
英国健康与安全执行局	安全相关行为
美国食品和药品管理局	新药批准和生产
软件工程学院	高可用性软件
美国职业健康与安全管理局	员工安全
美国环保署	环境保护

例如，软件工程学院 <www.sei.cmu.edu>已经建立了很多软件生命周期模型，其中的一些模型已经用于构建“不死”的软件——一种对安全、容错、可靠性、重复使用、性能、确认和测试等各个环节都有严格要求的，用于关键任务执行的软件。

与那些被美国食品和药品管理局管理的行业一样，对那些对产品质量要求很高的行业来说，现有基于生命周期的良好制造规范（cGMP）是不可或缺的。

除了使整合这些标准更加方便以外，生命周期解决方案的规定还有助于以尽可能少的成本获得最好的结果。

在 61511 标准下使用模型

只要您的工厂符合标准的要求，IEC 61511 就允许您定制您工厂的生命周期模型以适应工厂的当前状况。

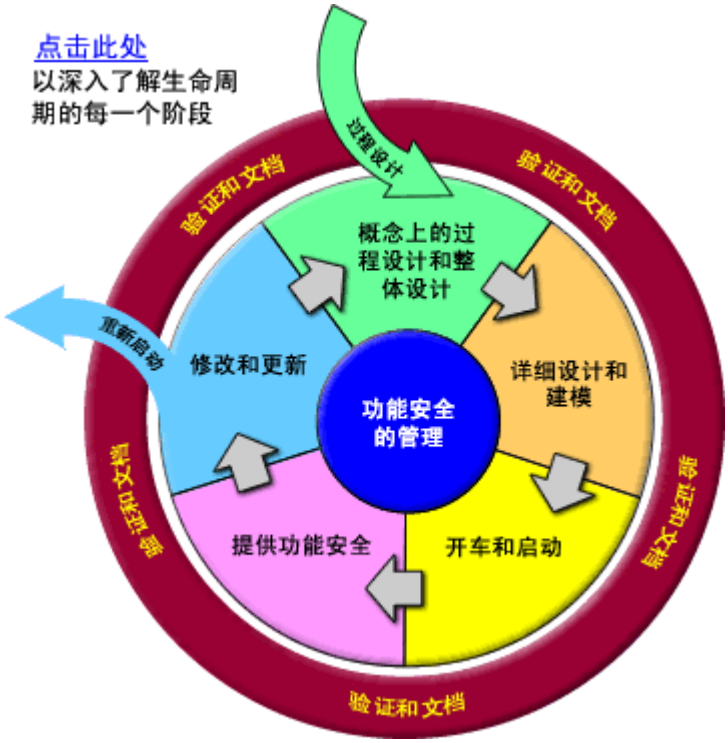
为了符合要求，每个解决方案都有五个主要的生命周期阶段，以及贯穿整个周期的验证和文档流程：

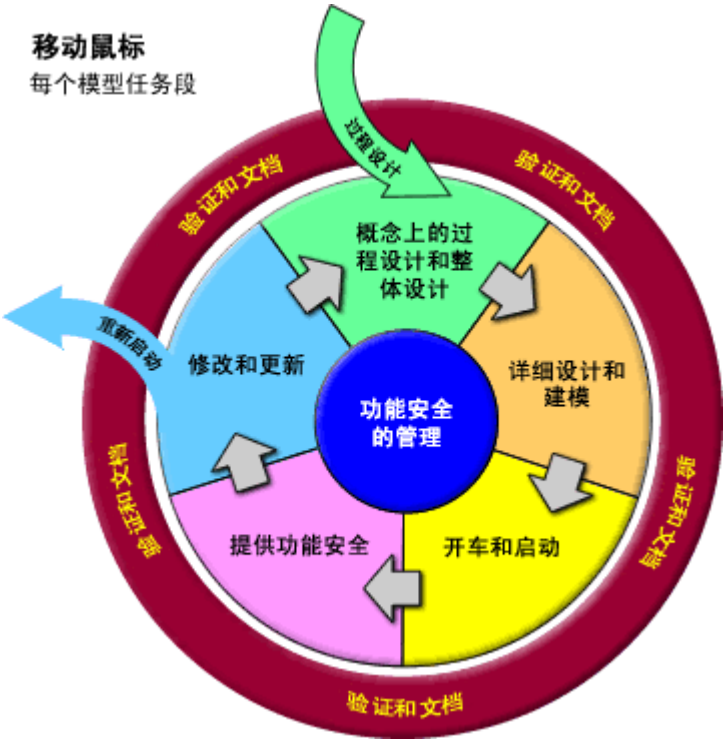
生命周期阶段	IEC 61511 的要求
1. 前端工程和概念设计	o 有害事件和风险评估 (条款 8) o 保护层的安全功能分配(条款 9) o SIS 安全要求的说明(条款 10 和 11)
2. 详尽的设计和工程说明	o SIS 设计和工程 (条款 11 和 12.4) o SIS 的建造、整合以及 FAT (条款 13)
3. 安装和启动	o SIS 安装和调试 (条款 14) o SIS 安全设施的确认 (条款 12.3，12.7 和 15)
4. 功能安全的预备	o SIS 的运转和维护 (条款 16)
5. 更正和升级	o SIS 更正 (条款 17)
- 验证和文档（贯穿所有阶段）	o 验证 (条款 7，12.4 和 12.7) o 文档 (条款 19)

将以上这些行为整合起来，就满足了 IEC 61511 的核心要求：

功能安全的管理	o 功能安全的管理以及功能安全的评估和审查 (条款 5) o 安全生命周期结构(条款 6.2)

下图所示为这些行为如何相互结合。





前端工程和概念设计 • 提出概念性的过程设计 • 鉴别出潜在的危险 • 分配安全要求 • 判断是否需要 SIS • 鉴别出可容忍风险的水平并选择目标 SIL • 建立安全需要的详细说明 • 选择合适的技术、构架以及验证和测试方法 • 针对每个安全功能计算其 SIL	**设计的详细说明** • 详细的设计说明 - SIS 现场设备安装 - SIS 逻辑运算器硬件 - SIS 软件 • 设计验证 • 逻辑运算器硬件安装和验证 • SIS 软件设置和安全功能测试 • SIS 逻辑运算器的集成 • 集成验证 (FAT) • 建立安装和调试的说明文档 • 建立操作和维护的说明文档	**安装和启动** • 安装 SIS 现场器件 • 安装 SIS 逻辑运算器 • 根据需要将 SIS 集成到 BPCS 中 • 安装验证 • 对 SIS 调试 • 验证 SIS
功能安全的准备 • 根据说明文档操作和维护 SIS • 执行设计中制定的验证试验来校验 SIS 的操作	**修改和升级** • 评估修改的范围和程度 • 如果确定修改没有影响安全，则进行修改并完成所有必要的验证和修改管理程序 • 如果变动很显著，则重复安全生命周期	

符合标准所需的条件

显然，仅仅说您的公司一直致力于提供一个安全的工作环境是不够的。管理层应当为实现该项义务而提供相当的资源，包括适当的资金、人员和培训。 而这只是为满足 IEC 61511 而营造优良环境和文化的一部分。

IEC 61511 需要对安全工程有相当知识和经验的人员，并且这些知识和经验要和正在使用的过程和 SIS 技术相适应。该标准还要求被指派管理、设计和执行安全系统的人员必须：

- 有足够的训练
- 有与其在安全生命周期中角色相适应的管理和领导才能
- 有相关法律知识，对安全调整的要求有足够的了解。

这样，给出书面证据来证明已经采取合适的措施制定、达到并维持 IEC 安全标准就成了那些安全专家的事情了。

如果您没有全部的内部资料，专业的供应商和顾问可以向您提供帮助。IEC 61511 是一个国际化的标准，其生命周期模型已广为人知，并被众多的公司所采用。随着该标准的越来越广泛的使用，专业的资料来源也越来越多。这也使得寻找高质量的帮助更加容易。

PlantWeb 的优势

作为业内首家智能 SIS 提供商，艾默生可向您提供全方位的服务，帮助您确保安全系统能够提供您所需的保护，并保持这种状态。这些服务——包括分析和设计、执行、维护和修正——加上符合经过 TUV 认证的 IEC61511 最优方法，有效地扩展了系统的整个生命周期。如果您愿意，还可以对员工进行培训以使您的 SIS 能够被充分利用，或者就实时的支持和维护问题联系艾默生现场安全工程师。

符合标准的好处

根据您所在的地方的不同，符合 IEC61511 或其他安全标准也许还可能是一个法律强制的要求。即便没有强制要求，符合这些标准也很有意义。

首先，制定 IEC 61511 的委员会包括了全球公认的安全专家。该标准集中了他们的知识和经验。其最终标准是一个严格的“最优方法”的集合，涵盖了针对功能强大且性能可靠的安全仪表系统的各个实施阶段，包括工程、执行、检验、操作以及维护。

简而言之，这是一个确保您的工厂和社区安全的好方法，同时还尽可能地减少了生命周期的开支。

即便有安全事故发生，符合这些标准也有助于事情的解决。

认可 IEC 61511 的机构包括

- 制造商互助保险公司 www.fmglobal.com
- 美国职业健康和安全管理局 (OSHA) www.osha.gov
- 美国环保署(EPA) www.epa.gov
- TÜV 工业服务有限集团 ASI 公司 www.tuvasi.com
- 英国健康和安全执行局(HSE) www.hse.gov.uk

一旦因出现事故或者污染泄漏，随之而来的政府机构的调查经常伴随着罚款、判刑、关闭工厂，或者三者都有。 他们可能有以下方面的疑问：

- 在该公司或设备中以前是否发生过同样的事故？
- 事前有什么措施可以鉴别风险？
- 有什么样的方法可以量化风险？
- 有什么措施可以降低风险？
- 有何后继措施可以确保缓解措施适当地展开？
- 有什么措施可以确保缓解方案如预期持续作用？

使用了 IEC61511，您就可以准确地回答这些问题。也许您还要进行复杂的调查，但是一旦您能确定您的工厂已经制定、取得并保持与 IEC 安全标准的一致，您将降低检查机关判决任何人入狱或关闭工厂的风险。

小结

在本课程中，您已经学过：

- 对于过程工业而言，关键的安全标准包括了 IEC 61508,，IEC 61511 以及 ANSI/ISA S84.00.01-2004.
- 今天，对于执行安全项目或者操作和维护安全系统的终端用户而言，IEC61511 或新的 S84 标准是过程工业中最好的选择。
- 三种标准都采用了基于性能的生命周期模型，这使得将其与其他标准进行集成更为方便，并能尽可能少的成本获得最好的效果。
- 只要您的工厂符合标准的要求，IEC 61511 允许您可以根据自身的需求在一定程度上来定制生命周期模型。当然，这需要提供足够的资金、人员和培训。
- 除了能够帮助您保持工厂、人员和社区的安全，遵从标准还可以使安全事故后的调查更为简便。