SIS 102

降低风险

15 分钟

本课程中将向您介绍：

O 概述
1 必要的风险降低
2 安全整合等级 (SIL)
3 保护层
4 安全仪表系统
5 整合应用
6 小结

概述

在先前的课程中，我们已经得知**固有风险**是那些存在于过程中的风险（包括了设备和原材料），而**可容忍风险**则由人身伤害、死亡的数量和频率以及我们能够承受的经济损失决定。

当固有风险超过了可容忍风险时，我们的第一选择就是消除风险。如果不能消除，至少也要将风险**减小或降低**——或者是采用诸如安全阀或安全系统这样的积极措施，或是采取封闭或阻挡这样的消极措施。

但什么程度的安全才是足够的？

如果对风险本身没有很好的理解，则很有可能采用了多余的风险降低措施，而这将降低利润。相对应的，如果没有采取工程上足够的安全措施，则其潜在的代价则可能更加高昂。

这就是为什么确定需要降低**多少**风险然后设计一个提供**适当**的解决方案是如此的重要。这也是我们在本课程中要关注的问题。

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：

- 必要风险降低的两种方法
- 安全整合水平的目的
- 安全层怎样预防或缓解风险
- 安全仪表系统的组成

必要的风险降低

我们到底需要将风险降低到什么程度？这里我们有两种方法：定量和定性。

定量法. 我们可以将与每个有害事件有关的固有风险进行量化，并将其总和与可容忍的风险水平相比较。

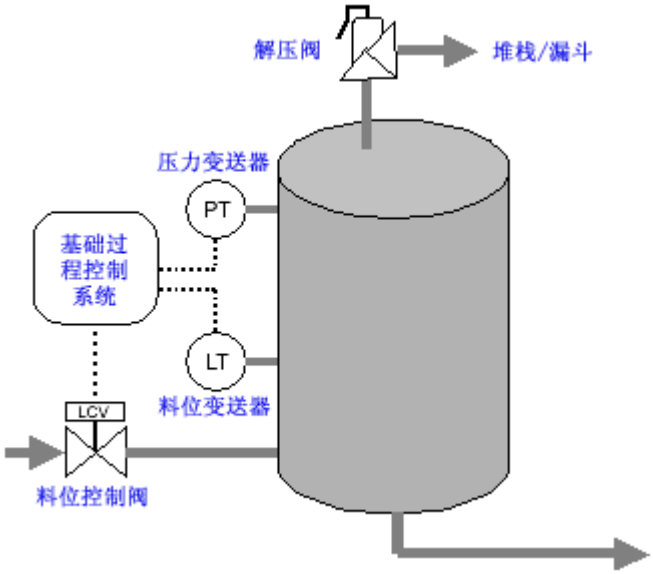
例如，我们想将致命事故的频率从每 10 年一次降低到每 10,000 年一次。换句话说，我们想将风险　降低 1000 倍，这也是您需要经常参考的**风险降低因子**（**RRF**）。

尽管本方法得到了越来越多的应用，但它也面临着两大挑战：

- 您需要收集相当多的数据才能使计算有意义。
- 您需要明确地表达出您准备忍受风险的量化水平，比如每年一次严重伤害事故，而这会使公众以及公司感觉不舒服。

定性法. 第二种评估必要的风险降低方法是定性评级，比如像在 SIS 101 中介绍的***后果***和***可能性***模型。

还记得前面课程里氨水罐的例子么？我们曾定义罐体破裂的可能性为“中等”而其后果为“严重”。



定性评估也有几种方法，包括风险图标和有害事件矩阵。例如，我们可以使用类似于下面的一个有害事件矩阵来鉴别必要的风险降低水平——本例中，为水平 2。

具有代表意义的是，风险管理专家们发展了这些矩阵，并给出了使用建议。这些矩阵中的数值被称为安全整合水平（SIL）。我们将在下一个主题介绍矩阵中数字的涵义。

安全整合水平 (SIL)

前图所示的安全整合水平鉴别出了对于一个特定**安全功能**所必须的**风险降低**水平。

（**安全功能**是指减少或消除特定条件或有害事件的能力。还以氨水罐为例，就是防止过压导致罐体破裂的能力。）

每个安全整合水平都是根据风险降低的程度来定义的，并依照数量级的顺序进行排列（避免纠缠细节）：

安全整合水平（SIL）	目标风险降低系数
4	>10,000 to ≤100,000
3	>1,000 to ≤10,000
2	>100 to ≤1,000
1	>10 to ≤100
改编自 IEC 61511-1 Table 3 **注意:** SIL 4 相关的应用在工业生产中并不常见。可编程的单独系统一般不能适合 SIL 4 标准的应用。	

这就使得我们可以以下两种方法之一建立必要的安全整合水平：

1. 我们可以像本课程的前一页一样，以定量的方式评估有害事件的后果和可能性。这给了我们宽广的必要风险降低。例如，定量评估告诉我们要达到 SIL2 ，我们需要将风险降低，其系数在 100 到 1000 之间。

2. 我们也可以精确地计算必要的风险降低，从而得到安全功能的 SIL 等级。例如，如果我们的计算表明必要的风险降低因数为 500，则可得知我们需要提供 SIL2 水平的保护能力。

IEC 61511 标准的主要好处就是它能够帮助使用者获得**成本最低的合适安全水平**。对每项安全功能精确地计算其风险并采用合适的 SIL 等级有助于避免您在保护方面投资过多或过少。

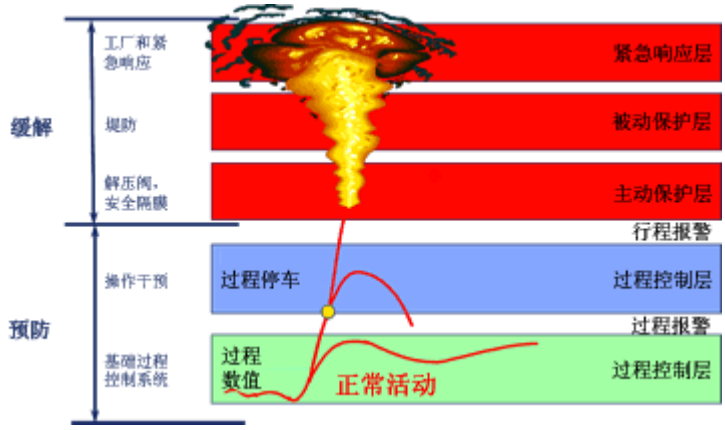
保护层

那么，我们怎样才能获得必要水平的风险降低呢？我们可以采用**保护层。**

安全标准中有一个关于保护层的定义，即“任何以控制、预防和缓解方法来降低风险的独立机制”。这些保护层的集合提供了我们所谓的**功能安全**——能够确保我们免于不可接受风险的功能。

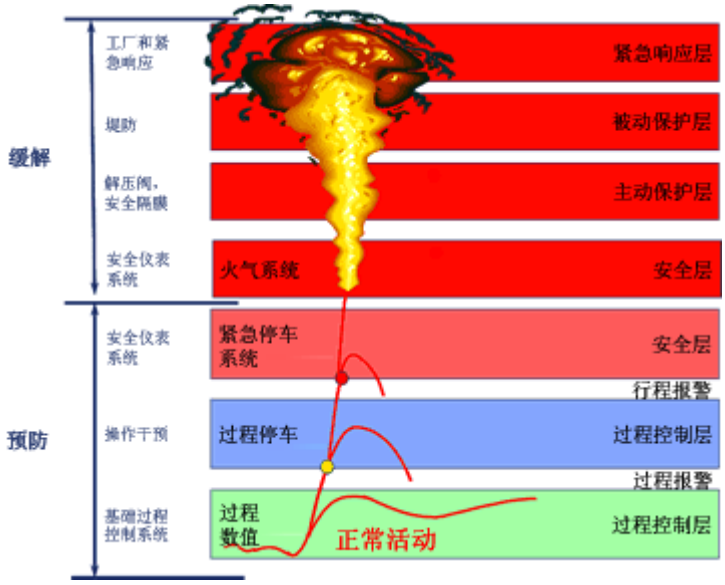
我们一般采用基本过程控制系统（BPCS）来**控制**生产过程（以避免那些可能导致事故的情形）。所谓基本过程控制系统，就是根据输入信号的反馈控制整个过程的系统。最常见的基本过程控制系统包括了回路控制器、DCS、PLC或者是混合自动系统。

另外，用于**预防**和**缓解的**独立保护层，一般包括了下图所示层次。



氨水罐例子中已经包含了 BPCS 和安全阀。 BPCS 有助于防止诸如像罐体过压而导致泄漏这样的事件发生。安全阀可以将过量的氨气排出从而避免了罐体破裂和大量泄漏。但这却使工厂员工和公众面临有害氨气的危险。

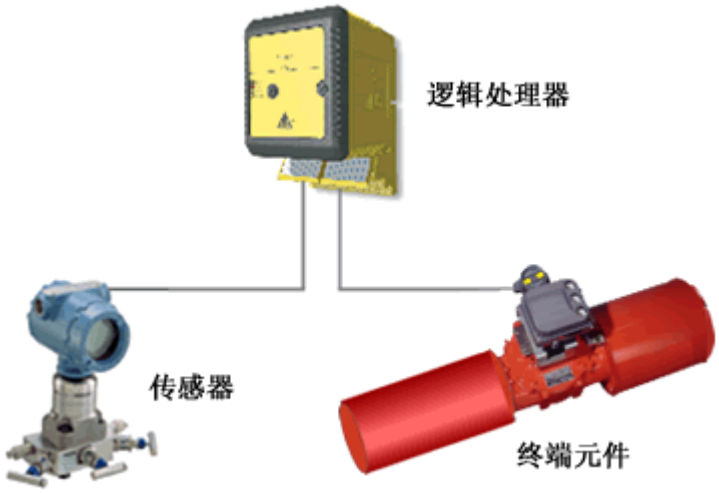
我们需要的是另外一层保护，一种可以避免安全阀达到临界点而工作的保护。该层是**安全仪表系统（SIS）**——一种集成的解决方案，也可以被称之为紧急关断系统，安全关断系统，火灾和气体保护系统和燃烧器管理系统。



安全仪表系统

当有害事件发生时，安全仪表系统将使得生产过程保持在一个安全状态，从而提供了一个独立的保护层。对于一些工厂来说，它是工厂运作的主要部分，也是进行调整的必要条件。

每一个 SIS 都是由传感器、逻辑运算器和终端元件进行任意组合而成的。任何一个系统要正常工作，都必须有这三种部件，并且都要工作正常。



尽管在结构上与基本过程管理系统（BPCS）类似，但SIS与其有本质上的差别。BPCS 是用来使生产过程平稳运行而制造出高质量的产品。另一方面，SIS 是监控不安全的生产过程条件，并采取合适的动作——典型的动作就是关断整个生产过程。

SIS 与 BPCS 是相分离的. 这种分离反映的不仅是两者在功能上的不同，而且反映了在 BPCS 不断变化的情况下，保持 SIS 完整性的重要程度。安全标准允许在器件和系统之间存在受控的通信，所以可以实施一个集成的但又是彼此独立的 BPCS 和 SIS 安装方案。

PlantWeb 的优势

艾默生已经将其成熟的 PlantWeb 数字结构拓展到了安全仪表系统。

艾默生的智能 SIS 第一个提出了完整安全环路的解决方案——从传感器到逻辑运算器到终端控制元件——所以您可以避免将独立元件拼凑到一起的风险和麻烦。

它也是第一个通过使用数字智能来实现更多的自动化安全回路测试、设备诊断以及其他一些特性，在增加系统可用性的同时降低了整个生命周期的成本，并简化符合法规的程序。

智能化的设计确保了艾默生 DeltaV 数字自动化系统在被用作 BPCS 的同时也被赋予了相应的安全整合水平。例如，在根据安全标准要求保持分离的同时，BPCS 和 SIS 使用相同的操作员界面和组态工具。

整合应用

让我们试着将到目前我们所学应用到氨水罐的例子上来。

一旦氨水罐过压（功能错误），如果预防或保护系统在缓解系统动作之前能够降低罐体的压力至设定安全操作范围，则说明安全功能工作正常。

在本课程的前面部分，我们认为氨水罐的 SIS 功能安全目标为 SIL2 等级。这就意味着风险降低的目标水平必须在 100 和 1000 之间。

我们认为 BPCS 在一定程度上可以增加风险降低的水平。依据 IEC 61511 标准，对一个非安全相关的控制系统而言，其最大风险降低水平系数为 10。

尽管我们不想在 SIS 方面有过多的工程性花费，但我们必须要确保我们有足够的保护手段。所以我们在作如下假定时稍稍有点保守：

1. 全部的必要风险降低因数(RRF)＝1,000
2. 赋予 BPCS 的风险降低因数= 2
3. 安全阀将不被考虑在内。因为安全阀一旦启用，则附近学校的学生将有暴露在逸散的氨气中的危险。

全部的 RRF 是各独立保护层 RRF 的乘积。在本例中，新添加的 SIS 所需的 RRF 为 1,000 / 2 = 500，还是对应着 SIL 2 等级（在 100 和 1,000 之间）。

如果风险降低没有达到以上的程度，则有害事件发生的可能性会高到不能容忍。但应用一个更高等级的安全功能（例如，采用 SIL 3 保护）将增加用于设计、采购、安装、调试和维护 SIS 的不必要成本。

小结

本课程中，您已经学过：

- 必要的风险降低可以通过使用定性或定量方法来实现。
- 安全整合水平（SIL）是一种用于将风险降低到可容忍水平的统计学表达。
- 独立保护层是控制、预防或缓解有害条件的一种机制。
- 安全仪表系统（SIS）使用传感器、逻辑运算器和终端元件来监控生产过程中的不安全状况，并在必要时采取措施使之回到安全状态。