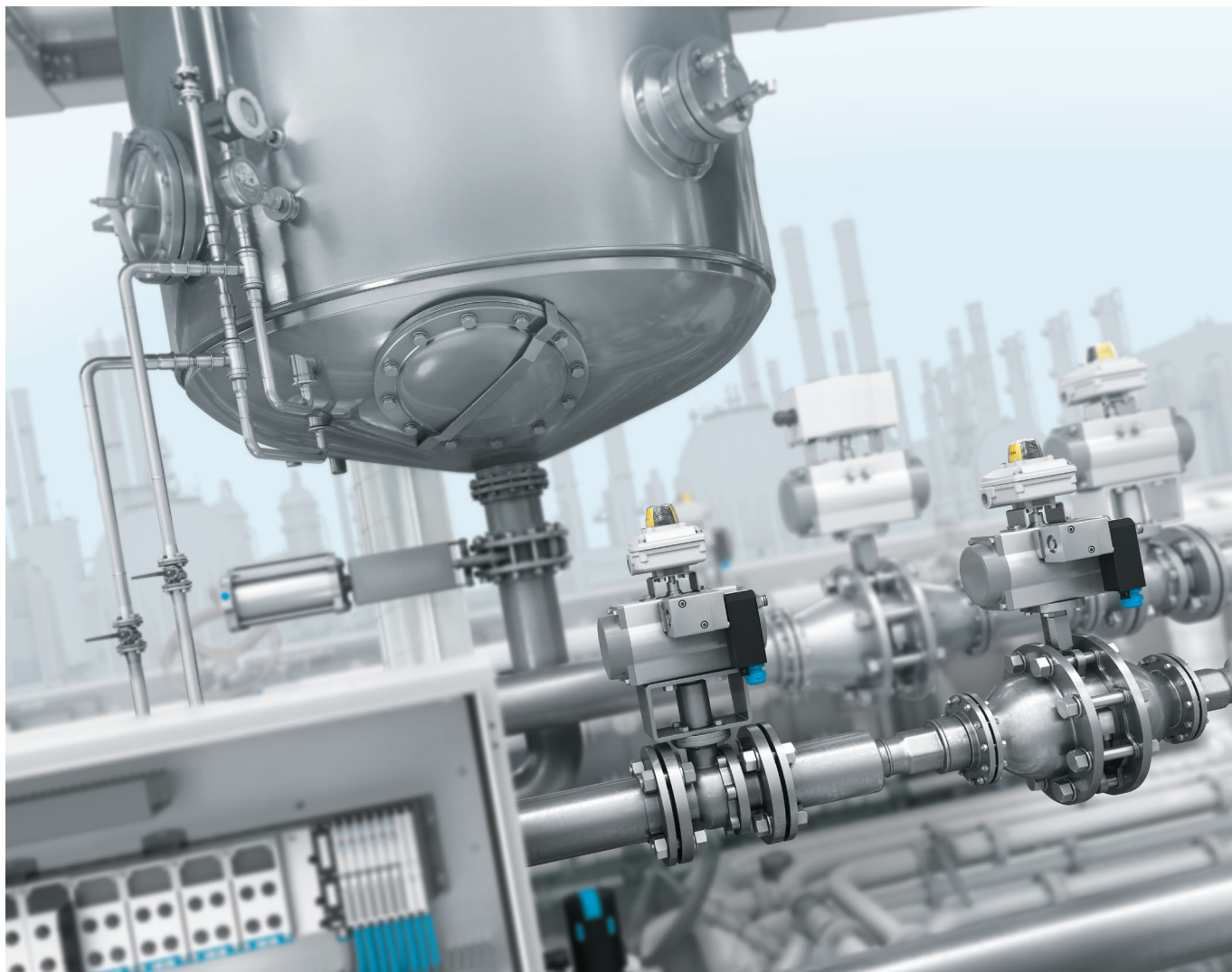


白皮书

控制过程阀门并考虑功能安全 (SIL)



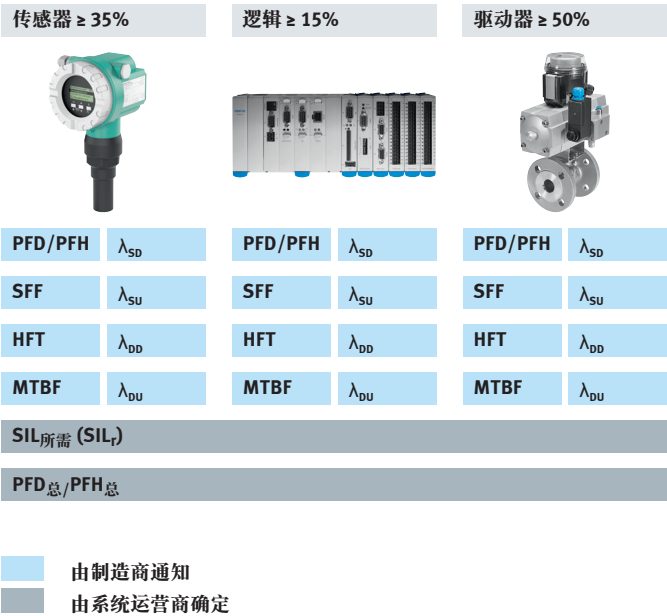
自 IEC 61508 生效以来，过程行业中的功能安全是一个非常重要的话题。通常由缩写 SIL 表示。但是 SIL 到底是什么？它如何用于控制过程阀门？

本白皮书包含有关以下主题的信息：

- 什么是 SIL（安全完整性等级）？
- 标准
- 风险分析
- 证书和制造商声明
- 搅拌槽反应器中的防护设备示例
- 以电磁阀为例，经过验证的性能和延长的使用寿命
- 现场驱动器的冗余激活

1. 什么是 SIL（安全完整性等级）？

安全功能的目的是最大限度地降低过程对人员、环境和财产造成的风险。SIL（安全完整性等级）描述了将风险降低到合理水平的程度。IEC 61508 解释了评估风险的方法（风险图）和设计合适的安全功能所需的措施，范围从传感器和逻辑电路到用于错误预防（系统错误）和错误控制（随机错误）的驱动器。这个依赖于应用的基本标准描述了对安全功能的组件和系统的要求，并促进了特定行业标准的开发，例如 IEC 61511-1：“功能安全 - 过程行业部门仪表型安全系统”。除其他外，IEC 61511-1 定义了为安全功能选择组件的标准，例如传感器和驱动器的运行可靠性。



重要须知

IEC 61508 对故障概率的要求始终针对完整的防护设备，而不是单个组件。因此，组件本身不能具有 SIL 等级；只有完整的安全回路或 SIS（安全集成系统）才能具有 SIL 等级。

通常，安全回路由以下组件组成：

- 传感器，例如，压力、温度、液位计
- 评估和输出单元，例如，安全 PLC
- 自动化过程阀，包括电磁阀、驱动器和过程阀

单通道系统中安全功能子系统之间 PFD/PFH 的典型分布

2. 标准

功能安全标准很广泛，而且并不总是容易理解，即使对于有经验的用户来说也是如此。在本白皮书中，我们将重点关注这些标准的解释和实际应用，但不会对其进行详细介绍。

以下是相关标准：

- IEC 61508：“电气/电子/可编程电子安全相关系统的功能安全”
→ 功能安全基本标准
- EN 61511 “功能安全 - 过程行业部门仪表型安全系统”
→ 适用于过程自动化

3. 风险分析

为了最大限度地降低风险，并达到 IEC 61508 和 IEC 61511 标准，基本上都需要以下步骤：

- 根据从传感器到控制器和驱动器的所有部件的整个使用寿命的详细故障概率进行风险定义和评估。
- 定义和采取措施以最小化剩余风险。
- 使用合适的设备（经评估或认证）。
- 定期测试和检查，以确保正确的安全功能。

3.1. HAZOP 分析等方法

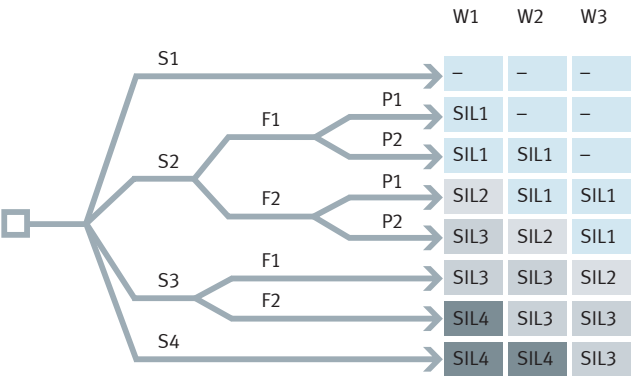
危险被定义为与生产过程计划的潜在严重偏差。换句话说，危险是构成实际或潜在威胁的危害。HAZOP（危险与可操作性分析）用于系统地识别降低生产力的错误和可操作性问题。如今，这种方法可用于所有类型的连续或非连续生产系统。HAZOP 分析的基本步骤是:

- 1) 预测可能的结果
- 2) 调查原因
- 3) 评估后果
- 4) 制定对策

风险评估中使用的其他方法的示例包括故障模式和影响分析 (FMEA)、事件树分析 (ETA) 或故障树分析 (FTA)。这些方法可以分为三组：归纳法，其中原因已知但后果未知；演绎法，例如 FTA，其后果已知但原因未知；以及诸如 HAZOP 之类的探索法，其中偏差的原因和后果都未知。使用不同的方法来查找缺失的信息。

这些方法可以进一步细分为自下而上的搜索和自上而下的搜索。自下而上意味着从严重错误开始并尝试确定后果 (FMEA)。自上而下意味着从危险后果开始并尝试确定原因 (FTA)。

SIL（安全完整性等级）



风险图：四个离散能级（SIL1 到 SIL4）。安全相关系统的 SIL 越高，系统无法执行必要的安全功能的可能性就越低。

S	损坏程度
S1	一人轻伤
S2	多人重伤或一人死亡
S3	多人死亡
S4	造成多人死亡的灾难性后果

F	频率和暴露于危险的时间
F1	很少到比较频繁
F2	频繁到连续发送

P	避免/减轻危险
P1	在特定条件下可能
P2	几乎不可能

W	发生概率
W1	比较高
W2	低
W3	非常低

3.2. 重要术语和特征值

HFT

硬件容错是指即使在（多个）错误和偏差的情况下也能执行安全功能的能力。如果基于这些值无法达到所需的 SIL 等级，则可以通过冗余来达到 SIL 等级。

SFF

SFF（安全失效分数）决定了安全故障在故障总数中的比例。安全故障是那些不会导致危险系统状态或可能导致危险系统状态但无法检测到的故障。

产品是否适合所需的 SIL 等级可以根据几个参数来确定：

低需求模式

用于激活安全系统的要求频率较低的工作模式。启动安全系统的要求每年不得超过一次。

→ PFD（要求故障概率）= 要求故障概率是基于事件的。

高需求模式

具有高频率要求或持续要求以激活安全系统的工作模式。安全系统连续运行或要求激活安全系统每年超过一次。

→ PFH（每小时故障概率）= 每小时故障概率是基于时间的

设备类型 A/B

类型 A：已充分描述了所有组件的故障行为。此类型包括简单（新）设备以及具有久经考验性能的设备。

类型 B：至少一个组件的故障行为尚不完全清楚。这种类型包括复杂的设备以及新开发的产品。

目标：SIL ≥ SIL_r

SIL 等级			设备类型 A				设备类型 B					
			安全失效分数（SFF）									
	高需求 工作模式	安全系统的最大可接受故障									低需求 工作模式	安全系统的最大可接受故障
			< 60%	60...90%	90...99%	> 99%	< 60%	60...90%	90...99%	> 99%		
	$10^{-5} \leq \text{PFH} < 10^{-4}$	每 10,000 小时出现一次故障风险										
1	$3 \times 10^{-6} \leq \text{PFH} < 10^{-5}$	每 1,250 天出现一次故障风险	HFT 0				HFT 1	HFT 0			$10^{-2} \leq \text{PFD} < 10^{-1}$	每 10 年出现一次故障风险
	$10^{-6} \leq \text{PFH} < 3 \times 10^{-6}$	每 115.74 年出现一次故障风险										
2	$10^{-7} \leq \text{PFH} < 10^{-6}$	每 115.74 年出现一次故障风险	HFT 1	HFT 0			HFT 2	HFT 1	HFT 0		$10^{-3} \leq \text{PFD} < 10^{-2}$	每 100 年出现一次故障风险
3	$10^{-8} \leq \text{PFH} < 10^{-7}$	每 1,157.41 年出现一次故障风险	HFT 2	HFT 1	HFT 0	HFT 0		HFT 2	HFT 1	HFT 0	$10^{-4} \leq \text{PFD} < 10^{-3}$	每 1,000 年出现一次故障风险
4	$10^{-9} \leq \text{PFH} < 10^{-8}$	每 11,574.1 年出现一次故障风险		HFT 2	HFT 1	HFT 1			HFT 2	HFT 1	$10^{-5} \leq \text{PFD} < 10^{-4}$	每 10,000 年出现一次故障风险
					HFT 2	HFT 2			HFT 2			
(每小时)												

（每小时）

故障概率和硬件故障容差概述

4. 证书和制造商声明

系统运营商需要 SIS（安全仪表系统）中使用组件的 SIL 分类证明。根据 IEC 61511，制造商的声明完全适用。证书既不是法律要求的，也不是标准要求的。为了出具制造商的声明或证书，需要对要使用的安全组件进行技术评估。该评估通常由独立组织（如 TÜV 或 Exida）进行。如果评估成功，制造商可以出具制造商声明并参考评估的测试报告。

与制造商的声明不同，证书只能由经认可的组织（例如 TÜV）出具。

系统越安全，评价功能安全和出具评估的单位就必须越独立：

安全完整性等级	评估单位
SIL 1	独立人
SIL 2	独立部门
SIL 3	独立组织
SIL 4	独立组织

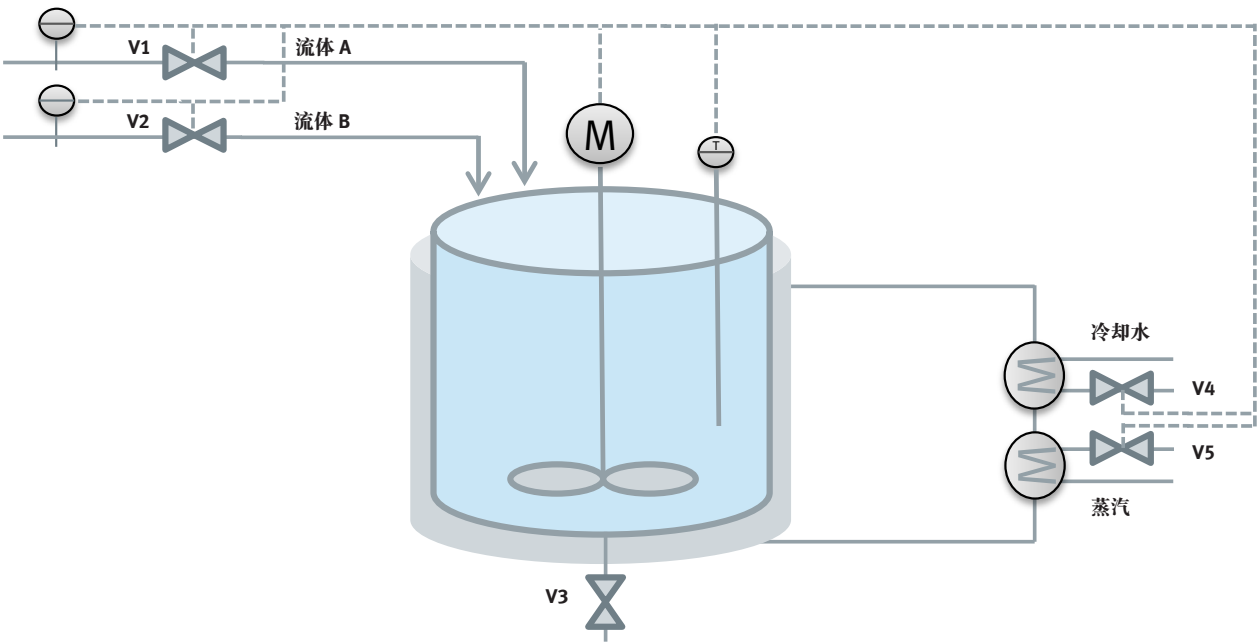
5. 搅拌槽反应器中的防护设备示例

在搅拌槽反应器中，不同的组件连接（通过下例中的阀门 V1 和 V2）并通过热量输入（吸热）或热量释放（放热）进行反应。通过搅拌内容物彻底混合。在放热反应期间必须避免过热。

在下图中，反应过程的压力调节是功能需要防护设备的示例。如果反应器中的压力过高，则热量可能无法正常散发并导致故障。结果，混合比例将不正确。

这种情况将对防护设备提出以下要求：关闭进料阀 V1、V2 和蒸汽阀 V5，同时打开冷却阀 V4 以冷却反应器。

根据风险分类，解决上述问题有不同的选择：



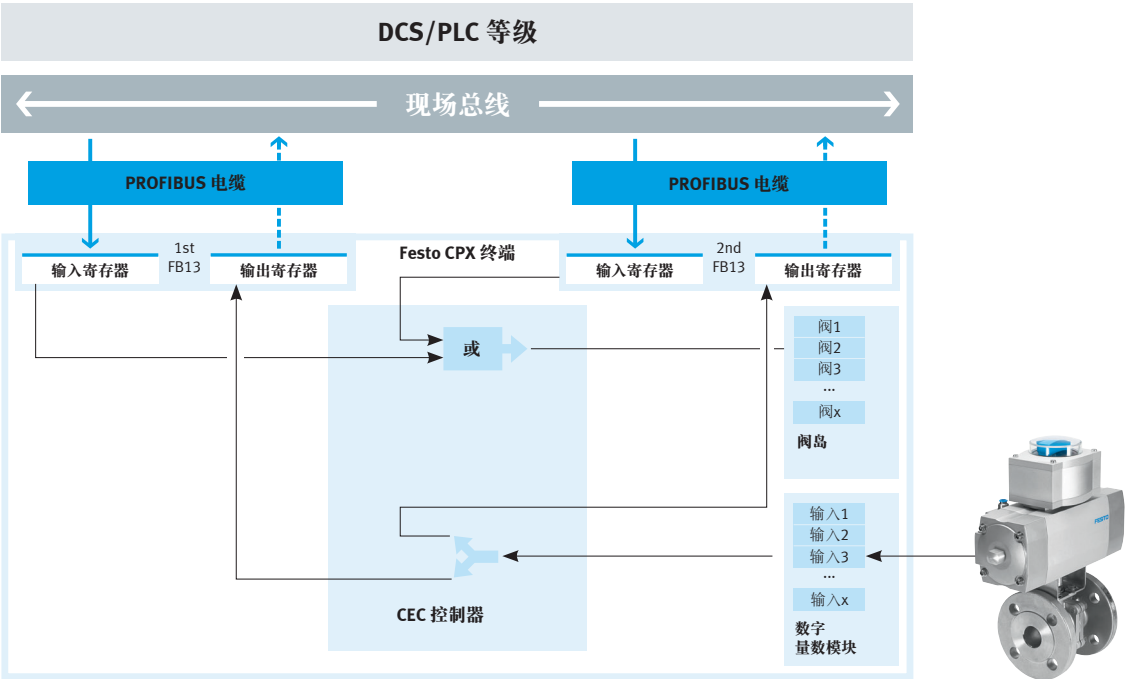
搅拌槽反应器示意图

5.1. 冗余 PROFIBUS 解决方案可用于提高控制系统 (DCS) 和远程 DCS 之间的安全性。

如果移除了一条 PROFIBUS 线路或 PROFIBUS 节点出现故障，则由第二条 PROFIBUS 线路 / 节点接管。将继续可靠地发送和接收控制系统协议。

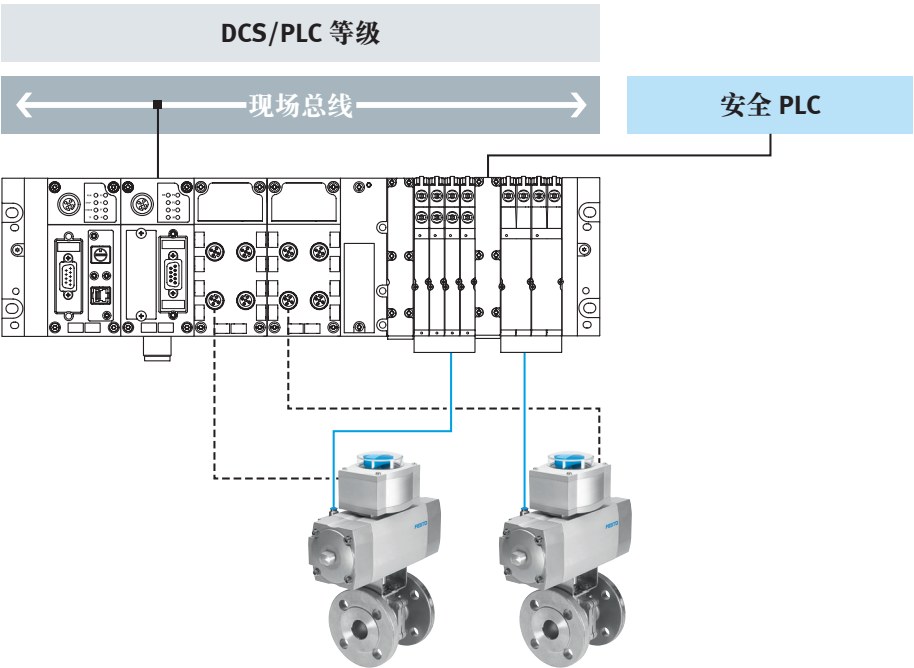
附加优势：

远程 I/O 可以通过带有以太网接口的控制器在现场直接访问，并且可以进行参数设置或执行其他过程。久经考验的远程 I/O 技术及其用于连接 NAMUR 传感器的输入模块，可靠地接管了控制层的任务。模块化终端与 SIL2 等级的阀岛是一种紧凑的替代方案。



5.2. 带集成安全关闭功能的阀岛

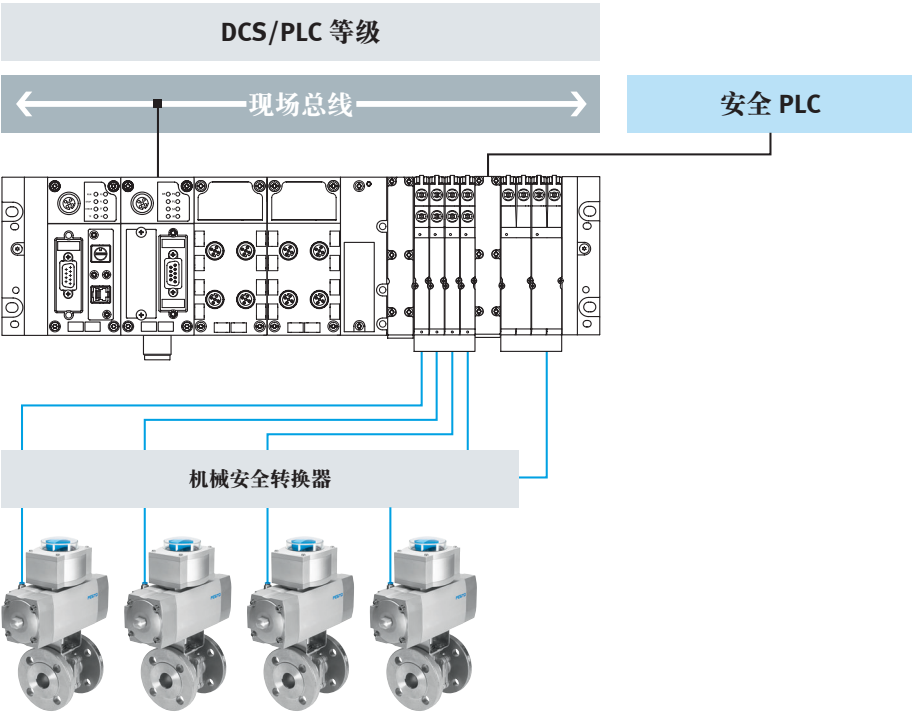
工作模式通过现场总线模块和带有串联布置的驱动器的阀岛激活。阀岛为安全 PLC 提供单独的电源，用于驱动单独的阀。还用于激活安全关闭过程的驱动器。该解决方案适用于 SIL2 等级的电路。为了提高安全等级，还可以选择冗余互连阀。



5.3. 带集成安全关闭功能的阀岛

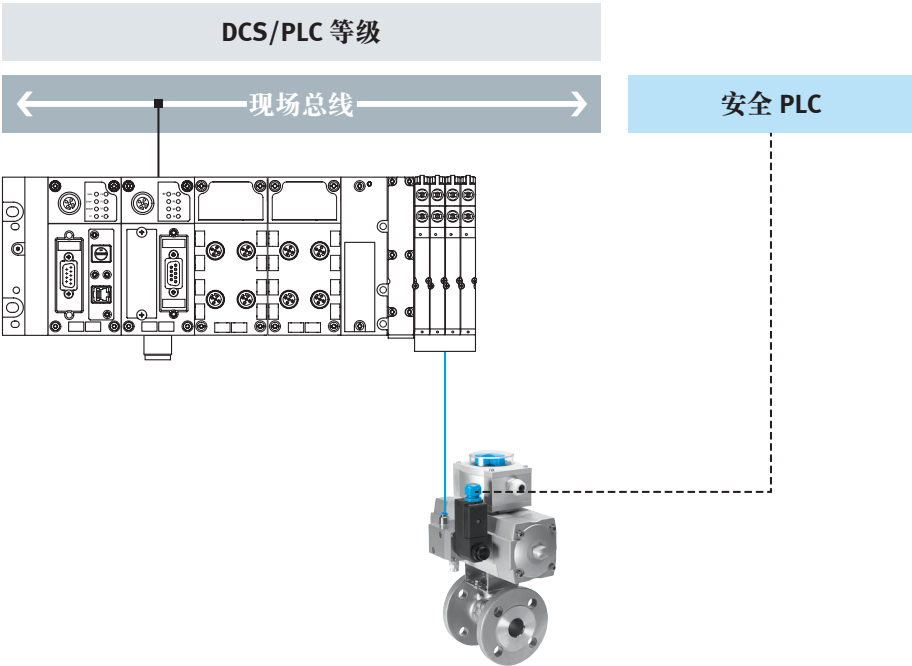
在工作模式下，阀岛通过现场总线激活并控制过程中的驱动器。此外，阀岛有一个单独的电源供应给安全 PLC，该 PLC 驱动阀岛上的阀以实现安全关闭。这通过一个额外的两位三通阀排气，该阀在正常模式下运行，从而防止安装在支线中的止回阀打开。此外，通过

监测压力，阀的开关位置得到保障。它还控制相同的驱动器，以安全地关闭过程。该解决方案适用于 SIL2 等级的电路。为了提高安全等级，可以选择冗余切换阀。



5.4. 用于安全关闭的阀岛加独立阀

通过现场总线和阀岛激活工作模式，用于控制现场驱动器。安装在同一驱动器上的经过认证的单个阀门由安全 PLC 直接驱动，并在需要时安全关闭。这些阀可用于最高 SIL3 等级的安全相关回路。



6. 以电磁阀为例，经过验证的性能和延长的使用寿命

全球化，尤其是在化工行业，正迫使公司不断提高其系统性能。这主要是为了弥补市场价格的下跌并保持竞争力。由于现代过程工程系统经过高度优化，只有通过可靠运行、高产且无需停机的系统才能实现更高的输出水平。这意味着减少检查周期和检查时间，以及避免因在维护或停机计划之外进行的维修而导致的空闲时间或停机时间。

实现这一目标的一种方法是使用经过 IEC 61508 认证的可靠电气仪表和控制技术组件，例如电磁阀。

然而，即使是经过认证的电磁阀在性能和安全规范方面也存在很大差异。市场上有许多用于安全安装的电磁阀解决方案，尤其是用于低需求工作模式的解决方案。其中许多解决方案的使用寿命有限，或者在停机时间或每年所需的开关周期数方面有要求，以满足安全规范。

提高可靠性是延长测试间隔的前提条件。这也意味着可以节省大量资金。在炼油厂中，每五年才停产一次的现象早已司空见惯。高可靠性主要得益于“二拖三原理” (2oo3)，并得到冗余系统和设备的支持。由于这些系统的高容量，这种更昂贵的选择得到了回报。这并不总是适用于化工厂。如今，工厂正试图通过使用经过认证的高

可靠性设备（电动机、变送器、控制器、电磁阀甚至过程阀）来达到与冗余组件相似的可靠性水平。

市场上提供具有 TÜV 认证（符合 IEC 61508 并达到 SIL 3 等级）的先导提升式电磁阀。这些阀符合最新的 SIL 分类，可保证 2.41 E-4 的故障概率。换言之，如果使用得当，在 2,410 个开关周期内最多会出现 1 个错误操作。

自 2002 年以来，经 SIL 认证的电磁阀已投入使用。从那时开始使用的电磁阀在实验室测试期间已经检查了它们的原始安全水平。这意味着现在有 SIL 认证的电磁阀不需要对其证书进行时间限制。当这些电磁阀在实验室重新测试时，提升式电磁阀即使在使用超过 12 年之后也显示出几乎相同的短暂切换时间，甚至与新阀相比也是如此。此外，它们在密封座外部和周围的密封性得到完全保障。

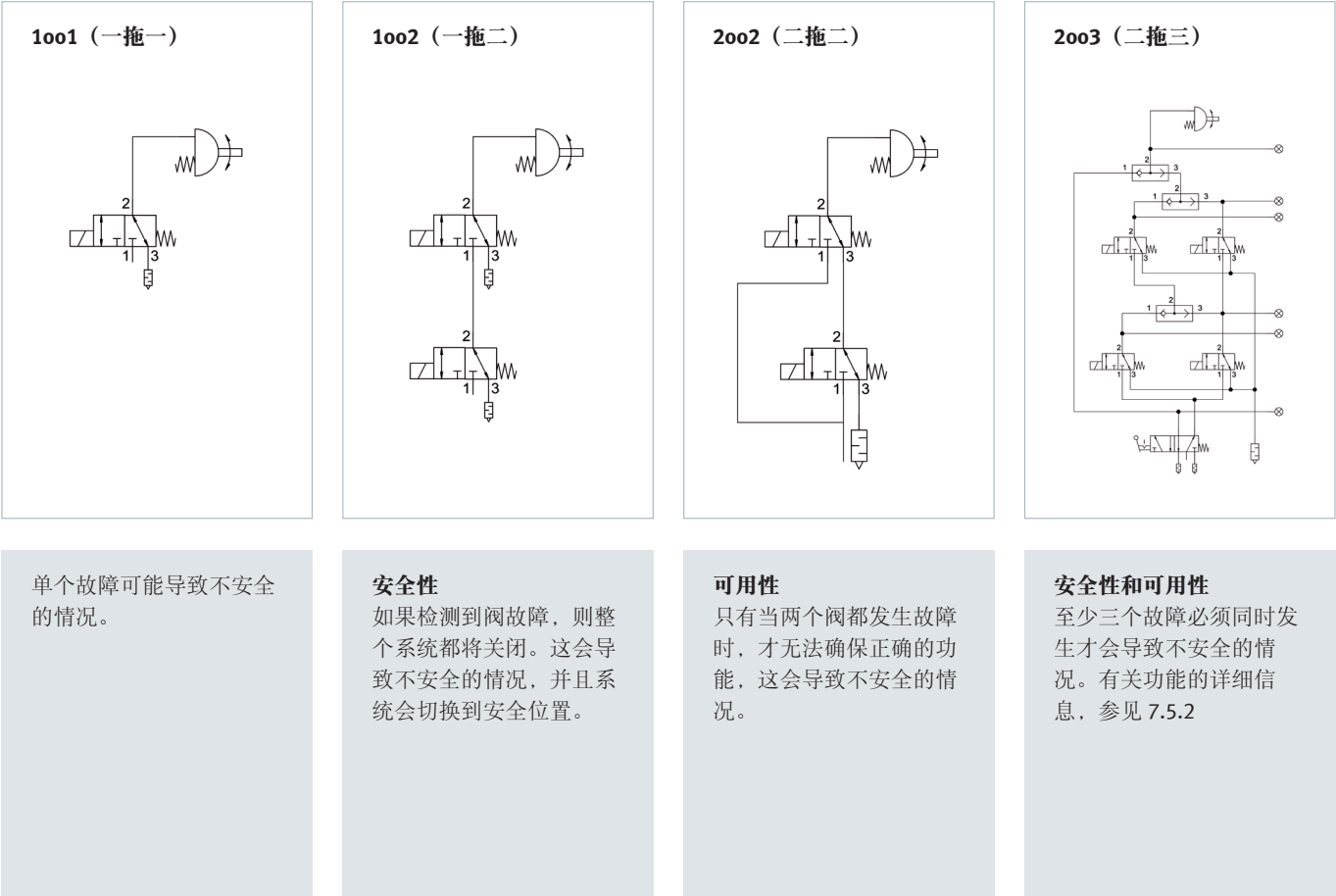


带扩展 NAMUR 端口和符合 IEC 61508 的 TÜV 证书的两位三通活塞提动阀

7. 现场驱动器的冗余激活

如果“第六章节：以电磁阀为例，经过验证的性能和延长的使用寿命”中所述的措施不充分，电磁阀仍可如上所述冗余互连（HFT1 或 HFT2）。

使用冗余时，过程安全性和可用性始终是最重要的。目前过程工程中的安全回路有 1oo2（一拖二）、2oo2（二拖二）和 2oo3（二拖三）。用于原油、天然气、化学品等高价值和危险物质的生产和加工。



现场最常见的驱动器冗余激活概述

7.2. 安全性提高 (1oo2)

安全性增强 (1oo2)，两个阀串联。两个阀在运行期间都通电。如果一个阀或其中一个控制信号在运行过程中出现故障，整个系统将关闭，以保护其免受后续损坏。介质输送线经常需要这种更高级别的安全性。

7.3. 可用性提高 (2oo2)

可用性增强 (2oo2)，两个阀并联。两个阀在运行期间都通电。如果一个阀或两个控制信号中的一个在运行期间出现故障，设备将保持激活状态，整个系统继续工作。例如，冷却回路需要这种增强的可用性。

7.1. 回路图中的功能

为了在阀发生故障时提供冗余，系统安装在安全或过程关键系统中。其紧凑设计降低了管道成本以及系统泄漏的可能性。也节省了装配和运行阶段的成本。

7.4. 安全性和可用性提高 (2oo3)

2oo3 电路结合了更高的安全性和可用性。其优点是可以在运行期间测试各个阀的功能，而无需激活驱动器。这种阀组合也用于石油和天然气行业以及炼油厂的高度关键应用中。

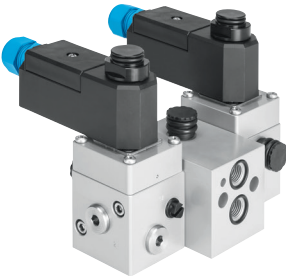
7.5. 可用的解决方案

7.5.1. NAMUR 模块安全性 (1oo2) 和可用性 (2oo2) 提高

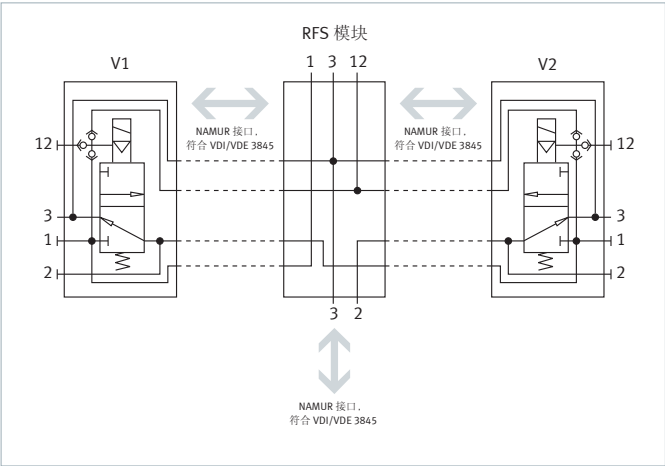
NAMUR 模块可以安装两个具有 NAMUR 端口模式的电磁阀。
NAMUR 接口使冗余易于实施。优点：仓储成本低，电磁阀更换方便。

NAMUR 模块可以使用 NAMUR 接口直接安装在角行程驱动器上。也可以使用合适的管道进行单独安装。

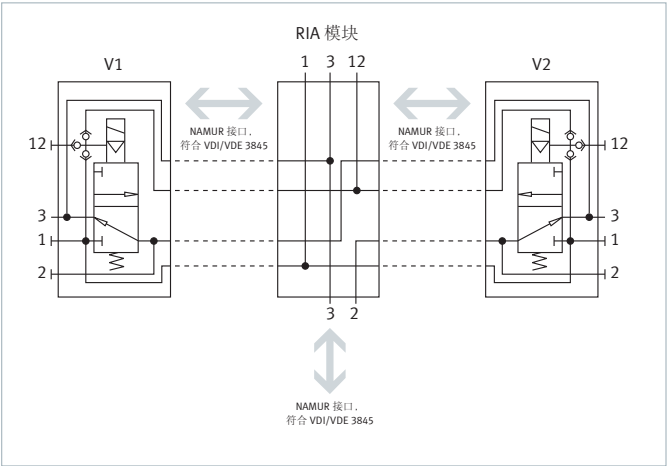
使用附加的辅助电源终端，NAMUR 模块也可以与具有用于故障安全功能的定位器的驱动器上的先导电磁阀一起使用。



冗余 NAMUR 模块



冗余故障保护 – 1oo2



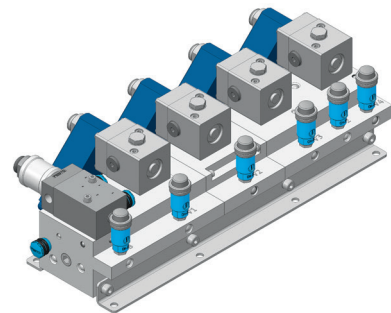
冗余可用性增加 – 2oo2

7.5.2. Inline/NAMUR 安全性和可用性 (2oo3)

有一种组合可以同时提供最大的安全性和可靠性。这个所谓的 2oo3 系统结合了这两种技术，满足了系统的最高需求。

该阀模块是内联版本，集成在系统中。安装在模块上的标准阀通过 NAMUR 接口根据 VDI/VDE 3845 定义并安装在模块上。这种组合意

味着模块只需安装一次，且阀仅根据使用寿命 / 安全生命周期计划通过 NAMUR 接口在必要时更换。此外，使用 2oo3 系统可以绕过四个阀的功能。可以用钥匙解锁该旁路，以便在运行期间进行维护。压力指示器直接安装在阀模块上，如果阀处于压力状态，则始终提供可靠且快速的指示。



2oo3 功能模块示例

作者：
Reiner Laun
行业细分管理

Festo AG & Co. KG
Rechbergstr. 19
73770 Denkendorf, Germany
电话：+49 711 347 76585
reiner.laun@festo.com