

# 过程行业中的功能安全

**FESTO**



**SIL** certified

如果您想要获得安全感  
如果您需要不间断的生产  
我们可以为您带来安全可靠的产品

→ WE ARE THE ENGINEERS  
OF PRODUCTIVITY.



我们的  
专长

您的  
优势

第 3 页

SIL – 安全完整性等级

第 4 页

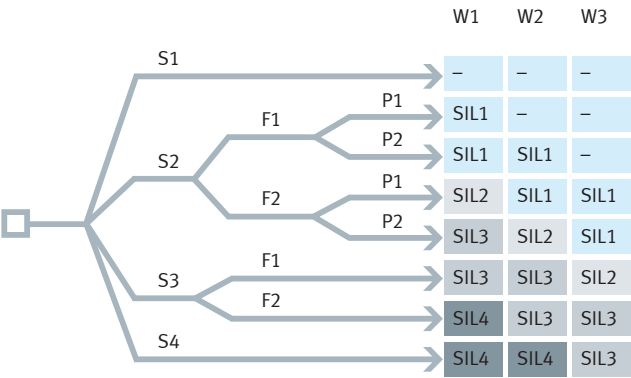
SIL 详述

# SIL – 安全完整性等级

过程工厂中的安全设备旨在将过程对人员、环境和财产造成的危害降低到可接受的最低水平。根据潜在危险，为工厂分配安全完整性等级（SIL1 到 SIL4）。SIL1 代表最低风险，而 SIL4 代表最高可接受风险，具有灾难性后果。

作为一般原则，工厂越危险，其安全设备在紧急情况下必须越可靠地运行。为工厂分配 SIL 等级后，必须遵守特定的安装原则，例如冗余设计。这可以在发生故障时最大程度地降低风险。

SIL（安全完整性等级）



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<br>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  |

## SIL 详述

### 标准：

功能安全的基本标准是 IEC 61508，标题为“电气 / 电子 / 可编程电子安全相关系统的功能安全”。IEC 61511，标题为“功能安全 - 过程工业部门仪表型安全系统”适用于过程自动化。



IEC 61508 描述了评估风险的方法（使用风险图）以及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驱动器。

安全电路或 SIS（安全集成系统）通常由以下组件组成：

- 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

IEC 61511 描述了 IEC 61508 在过程工业中的具体实施。这里的重点是低需求模式的应用。在过程工厂中，这代表了大多数安全功能。

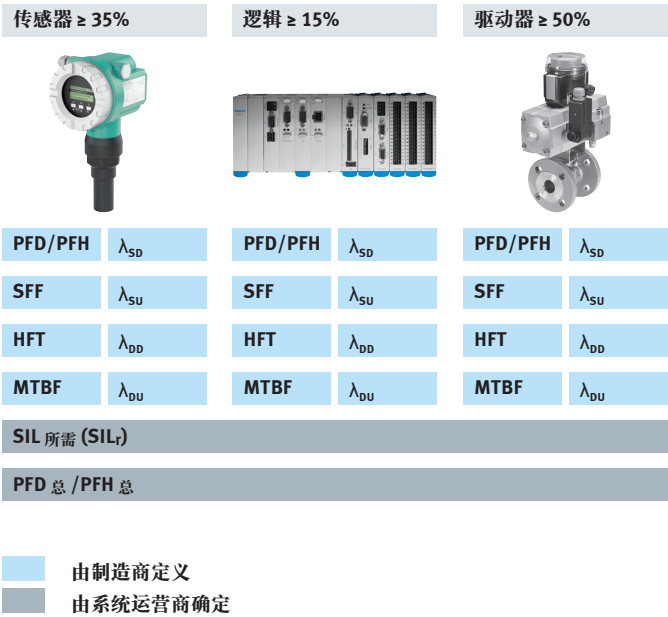
### 重要须知

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可以具有 SIL 等级。

### 计算 SIL 的相关特征值

- **PFD（要求故障概率）：**  
安全功能在低需求操作模式下失效的概率（要求率 / 年 < 10）低需求
- **PFH（每小时故障概率）：**  
连续使用期间安全功能失效的概率（要求率 / 年 > 10）高需求
- **SFF（安全失效分数）：**  
安全故障占故障总数的比例
- **HFT（硬件故障容差）：**  
请求功能在错误和偏差期间继续运行的能力  
**HFT0:** 单个错误可能导致安全功能丧失，例如，1oo1 连接  
**HFT1:** 必须同时发生至少 2 个错误才能导致安全功能失效，例如，1oo2 连接  
**HFT2:** 必须同时发生至少 3 个错误才能导致安全功能失效，例如，1oo3 连接
- **λ（故障率）：**  
S：安全故障的总故障率  
SD：安全、可识别故障的故障率  
SU：安全、无法识别故障的故障率  
D：危险故障的总故障率  
DD：危险、可识别故障的故障率  
DU：危险、无法识别故障的故障率
- **MTBF（平均故障间隔时间）：**  
两次连续故障之间的平均时间
- **设备类型 A：**  
所有组件的故障行为和故障特性都已充分确定的设备，例如通过工作可靠性。
- **设备类型 B：**  
至少一个组件的故障行为和发生故障时的行为未充分确定的设备。

单通道系统中安全功能子系统之间 PFD/PFH 的典型分布



SIL 对运营商意味着什么？

建立和运营对员工、当地居民或环境构成潜在危害的系统的公司必须将故障下过程所带来的风险降至最低。

为了达到 IEC 61508 和 IEC 61511 标准，需要执行以下步骤：

1. 风险定义和评级
- 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。
2. 措施的定义和实施
- 以最小化剩余风险。
3. 使用合适的设备
- （经评估或认证）
4. 定期测试和检查
- 以确保正确安全功能。

目标：SSIL ≥ SIL<sub>r</sub>

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

（每小时）

# 用于安全相关应用的元件

此处介绍的产品系列用于化工和石化行业的安全相关应用系统。符合 SIL3 或更高标准的产品需要由自治组织通过 IEC 61508 认证；对于达到 SIL2 的产品，适用性可由公司自行声明。计算 SIS 系统可达到的 SIL 等级所需的特征值在相关证书或用户文档中有详细说明。

## 具有 SIL 证书的元素

### 先导阀 VOFC



适用于低需求、高需求和 ESD（紧急停机）应用的冗余回路中最高 SIL3 等级或单通道回路中最高 SIL2 等级的安全相关系统。

- 设计原理：先导式
- IEC Ex 防爆认证：EPL Gb / EPL Db
- ATEX 防爆认证：II 2 G / II 2 D
- 电磁线圈防爆类型：  
Ex ia, Ex me, AEx-m
- 外壳防护等级 IP65
- 表面处理：  
铝（Ematal 硬化涂层）- 不锈钢
- 工作条件：室内 / 室外



### 先导阀 VOFD



适用于低需求、高需求和 ESD（紧急停机）应用的冗余回路中最高 SIL3 等级或单通道回路中最高 SIL2 等级的安全相关系统。

- 设计原理：直动式
- IEC Ex 防爆认证：EPL Gb / EPL Db
- ATEX 防爆认证：II 2 G / II 2 D
- 电磁线圈防爆类型：  
Ex me, Ex d, AEx-d
- 外壳防护等级 IP65
- 表面处理：  
铝（Ematal 硬化涂层）- 不锈钢
- 工作条件：室内 / 室外



### 角行程驱动器 DFPD



双作用和单作用，适用于激活在冗余设计中达到 SIL3 等级的安全相关系统或在低需求和高需求应用中的单通道设计中达到 SIL2 等级的安全相关系统中的过程阀。

- 温度范围：50 °C ... + 150 °C
- ATEX 防爆认证：  
II 2 G c T4 X / II 2 D c 125 °C X
- 摆角高达 180°
- 表面处理：不锈钢轴，带有环氧树脂涂层的外壳



### 传感器盒 SRBC



适用于低需求和高需求应用的最高 SIL2 等级的安全相关系统中自动化过程阀的电子和视觉位置指示。

- 外壳防护等级 IP67/NEMA 4/4X
- 防爆类型: Ex ia
- ATEX 防爆认证: II 2G c X / II 2D c X
- cCSAus: 普通位置
- 工作条件: 室内 / 室外



### 传感器盒 SRBE



适用于低需求和高需求应用的最高 SIL2 等级的安全相关系统中自动化过程阀的视觉位置指示和电气位置传感。

- 外壳防护等级 IP67/NEMA 4/4X
- 防爆类型: (A)Ex d, (A)Ex tb
- 防爆类型:
  - IEC Ex 防爆认证: EPL Gb / EPL Db
  - ATEX 防爆认证: II 2G / II 2D
  - CSA 认证:
    - I 类, 1 级; I 类, 2 级
    - II 类, 1 级; III 类, T4A
    - I 类, 1 区; I 类, 21 区
- 工作条件: 室内 / 室外



### 如何查找 SIL 证书 / 声明

#### 第一步:

→ [www.festo.com/supportportal](http://www.festo.com/supportportal)

#### 第二步:

输入产品类型或部件号

Search

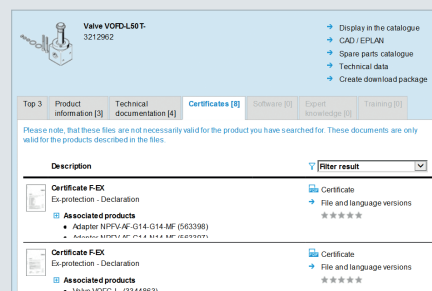
VOFD

Find

Help

#### 第三步:

单击“证书”选项卡



#### 第四步:

SIL 证书 / 声明



## 具有 SIL 制造商声明的元件

### 先导阀 VSNC



带可更换密封件，适用于两位三通或两位五通阀功能、两位五通双电控和三位五通阀功能。适用于最高 SIL2 等级的安全相关系统。

- 结构特点：先导式
- 电磁线圈防爆类型：  
Ex ia, Ex m, Ex na, AEx-m
- 外壳防护等级 IP65
- 表面处理：铝
- 工作条件：室内



### 直行程驱动器 DLP

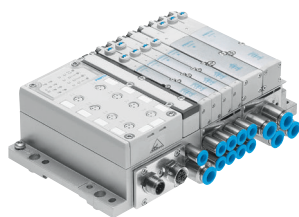


双作用开 / 关直线驱动器，适用于激活最高 SIL2 等级的安全相关系统中的过程阀。

- 适用于户外安装的高耐腐蚀性 (CRC 3)
- 非接触式位置感应
- 用于安装电磁阀的 Namur VDI/VDE3845 孔型
- ATEX 防爆认证：II 2 GD



### 气动阀岛 MPA



最大的功能集成、多种电气连接选项、多针插头、Festo I-Port、现场总线和综合诊断技术。适用于最高 SIL2 等级的安全相关系统。

- 不同的歧管块材料
- 大流量的优化版本
- 可提供高速阀
- IP20 版本是控制柜解决方案的理想选择



### 气动阀岛 CPV



用于复合气动连接板和穿板连接的本安阀岛，适用于最高 SIL2 等级的安全相关系统。

- 防护等级 IP65
- 用于控制柜组件的防护等级 IP65 的复合气动连接板
- CE 标记
- 可直接安装在防爆 1/21 区



# 安全相关应用的冗余系统条件

使用冗余系统时，过程安全性和可靠性始终处于首位。目前过程工程中的安全电路有 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。

## 电路图中的功能

|                                    |                                                                     |                                                                |                                                   |
|------------------------------------|---------------------------------------------------------------------|----------------------------------------------------------------|---------------------------------------------------|
| <div><p><b>1oo1（一拖一）</b></p></div> | <div><p><b>1oo2（一拖二）</b></p></div>                                  | <div><p><b>2oo2（二拖二）</b></p></div>                             | <div><p><b>2oo3（二拖三）</b></p></div>                |
| <p>单个故障可能导致不安全的情况。</p>             | <p><b>安全性</b><br/>如果在阀中检测到故障，则整个系统都将关闭。这会导致不安全的情况，并且系统会切换到安全位置。</p> | <p><b>增加正常运行时间</b><br/>只有当两个阀都发生故障时，才无法确保正确的功能，这会导致不安全的情况。</p> | <p><b>安全性和可靠性</b><br/>至少三个故障必须同时发生才会导致不安全的情况。</p> |

为了在阀发生故障时提供冗余，上述系统安装在安全或过程关键系统中。其紧凑的设计降低了管道成本，时降低了系统泄漏的可能性。这降低了工厂的装配和运营成本。

现场级使用最广泛的冗余系统

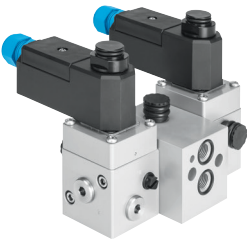
安全性 (1oo2)

安全性增强 (1oo2)，两个阀串联。两个阀在运行期间都通电。如果阀或电磁线圈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。

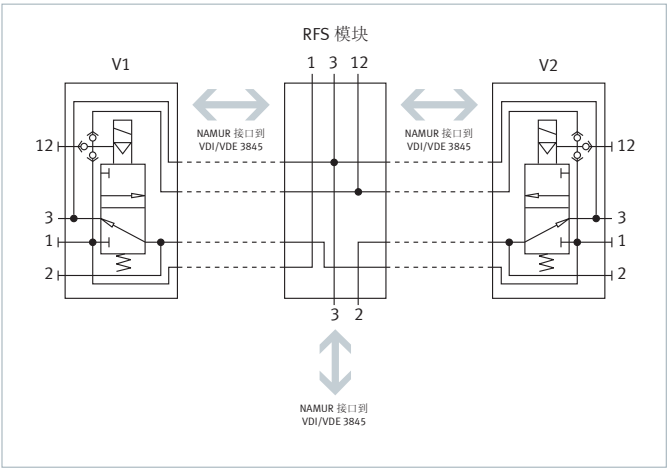
增加正常运行时间 (2oo2)

随着正常运行时间的增加 (2oo2)，两个阀并联连接。两个阀在运行期间都通电。如果阀或电磁线圈在运行过程中出现故障，设备仍处于激活状态，整个系统继续工作。例如，冷却回路需要增加正常运行时间。

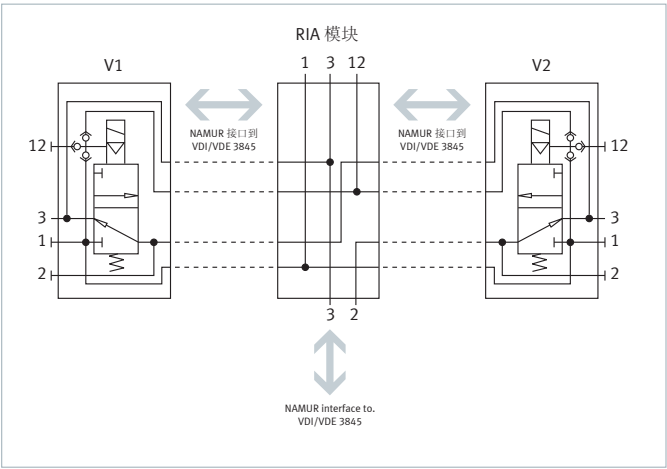
NAMUR 冗余模块  
(1oo2 和 2oo2)



- NAMUR 模块可以安装两个电磁阀 VOFC 或 VOFD。NAMUR 接口使冗余易于实施。优点：仓储成本低，电磁阀更换方便。
- 两个电磁阀冗余互连，为自动化过程阀提供冗余功能。这些模块可用于故障安全功能 (1oo2) 或增加正常运行时间 (2oo2)
- NAMUR 模块可以使用标准化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 1oo2 并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。
- 由于可用电磁线圈的防爆类型和全球认证，因此具有很高的灵活性。
- 提供 G 和 NPT 接头。



冗余故障保护 – 1oo2



冗余增加正常运行时间 – 2oo2

## 冗余管式阀 (1oo2 & 2oo2)

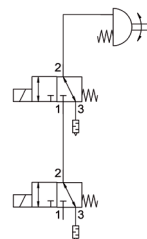


有了这些紧凑的系统，Festo 借助 VOFD 阀门久经考验的技术（在使用中得到证明），并将其组合到一个外壳中。借助 Ematal 硬化涂层，这些阀门符合过程工程中的最高安全标准，并且可以承受最恶劣的环境条件。

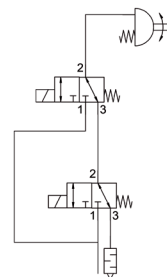
可用的防爆类型：Ex me, Ex d.

- 单个阀更换方便。
- 阀的冗余电路可确保冗余故障安全功能 (1oo2) 或为自动化过程阀提供增加正常运行时间 (2oo2)。
- 由于可用电磁线圈的防爆类型和全球认证，因此具有很高的灵活性。
- 紧凑而坚固的外壳，适用于安装在恶劣环境条件下。
- 提供 G 和 NPT 接头。

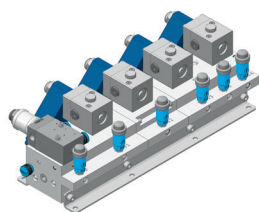
### 1oo2（一拖二）



### 2oo2（二拖二）

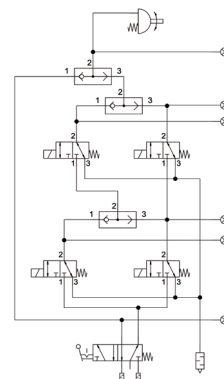


## 管式/Namur 安全性和可靠性 (2oo3)



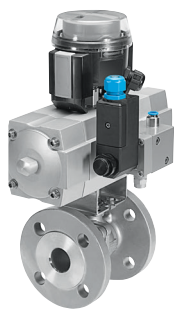
有一种组合可以同时提供最大的安全性和可靠性。这个所谓的 2oo3 系统结合了这两种技术，满足了系统的最高需求。该模块是内联版本，集成在您的系统中。内置标准阀通过 NAMUR 接口安装在模块上。这为设计的多样性提供了机会。这也意味着可以轻松更换单个阀。此外，使用 2oo3 系统可以绕过四个阀的功能。可以用钥匙解锁该旁路，以便在运行期间进行维护。直接安装在阀模块上的机械压力指示器或压力表在阀加压时始终提供可靠和快速的指示。此外，机械显示器可以用电子压力传感器代替，以反映控制系统中的状态。

### 2oo3（二拖三）



## 安全相关应用的解决方案

### 1. Festo 的驱动器单元 – 可随 时安装



完整的驱动器单元，无论是单作用还是双作用，都能为您节省时间和资金。我们将根据您的要求为您制造可随时安装并经过测试的驱动器单元 - 包括安全相关系统。为此，我们使用基于相应 SIL 制造商声明认证元件的自动化过程阀门。

- 完全按照您的规格装配
- 节省成本和时间
- 可随时安装
- 可通过相应制造商声明对驱动器进行 SIL 或 ATEX 评估
- 为低温环境设计

### 2. 用于安全相关应用的面板和 控制柜解决方案



#### 管道气动控制系统

Festo 提供范围广泛的气动控制系统。我们的产品涵盖价值链的所有阶段，从即用型面板最初的规划和工程设计到装配、测试和交付。

#### 用于过程工业的控制柜

根据您的规格和要求量身定制的控制柜解决方案可保护使用的组件免受环境因素、流体和异物的影响。由您决定是管道连接还是管路连接更适合您的目的。

无论您使用的是气动、电驱还是电动气动元件，您都会收到完全符合您要求的控制柜。根据要求，我们可以对整个控制柜进行 SIL 评估。对于防爆，我们还制造具有国际认证并符合美国 NEC 标准的 2GD 或 3GD 设计的控制柜。



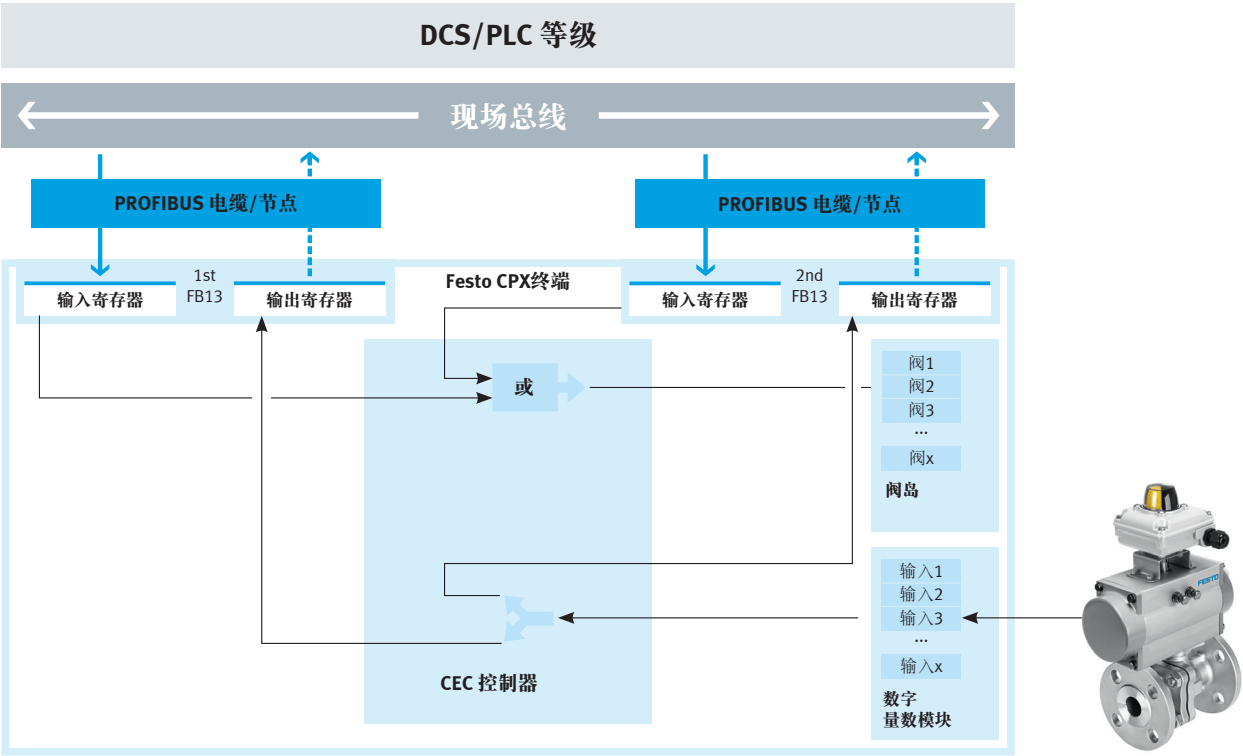
3. 批量生产的当前解决方案

3.1 PROFIBUS 冗余

Festo 使用冗余 PROFIBUS 解决方案来提高控制系统 (DCS) 和远程 I/O 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。这能够可靠地发送和接收控制系统协议。

其另一个好处是，您可以通过带有以太网接口的控制器直接在现场访问远程 I/O，并进行参数化或实施附加过程。久经考验的 CPX-P 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。

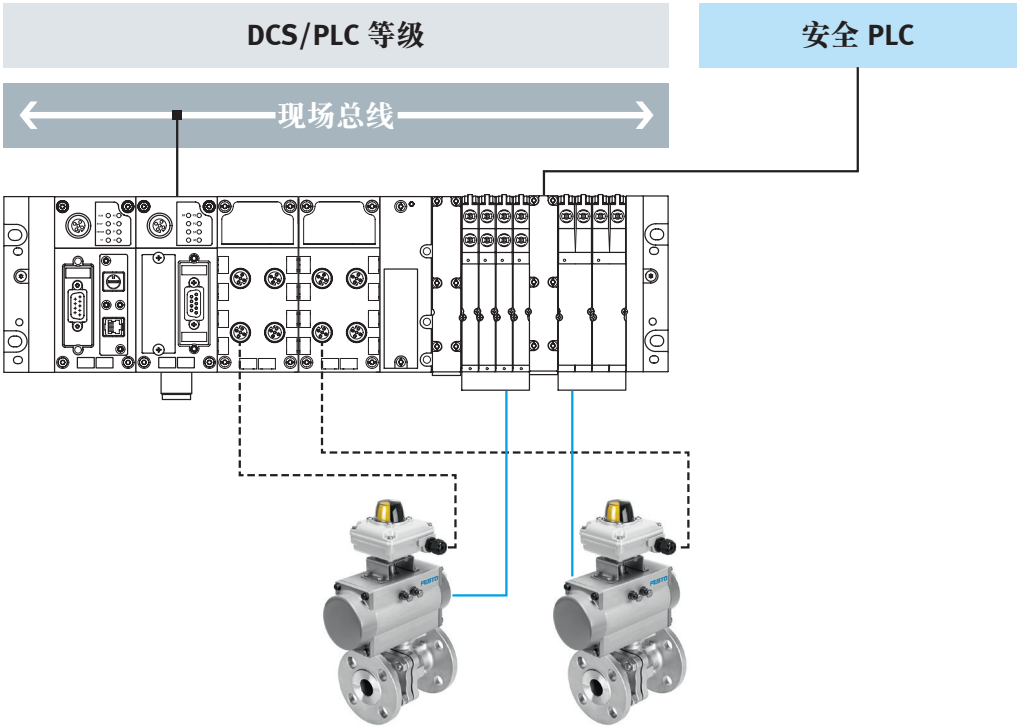
模块化终端 CPX 与 SIL2 等级的阀岛 MPA 是一种紧凑的替代方案。



3.2.1 带安全 PLC 的 CPX/MPA

带有集成安全关断功能的阀岛，用于控制单独的驱动器。

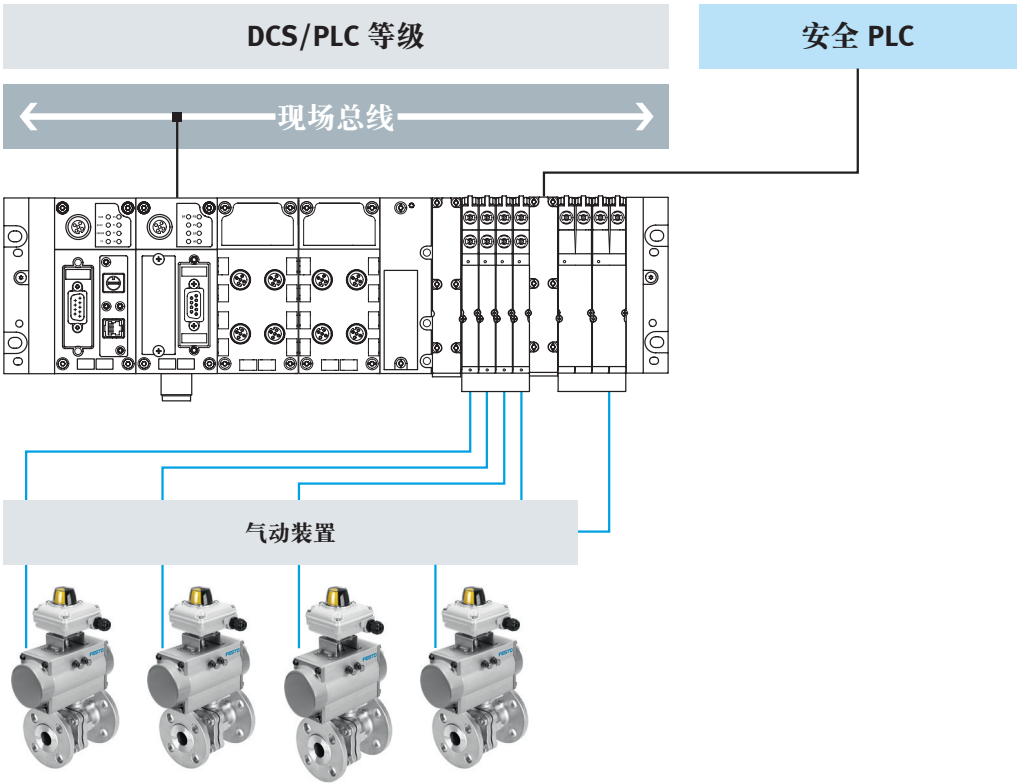
在工作模式下，阀岛通过现场总线激活，并在此过程中切换驱动器。此外，阀岛有一个单独的电源供应给安全 PLC，该 PLC 驱动阀岛上的阀以实现安全关闭。运行模式的驱动器和安全关断的驱动器串联。该解决方案适用于 SIL2 等级的回路。为了提高安全等级，还可以选择冗余互连阀。



3.2.2 连接安全 PLC 的 CPX/MPA

带有集成安全关断功能的阀岛，用于控制驱动器的操作和安全模式。

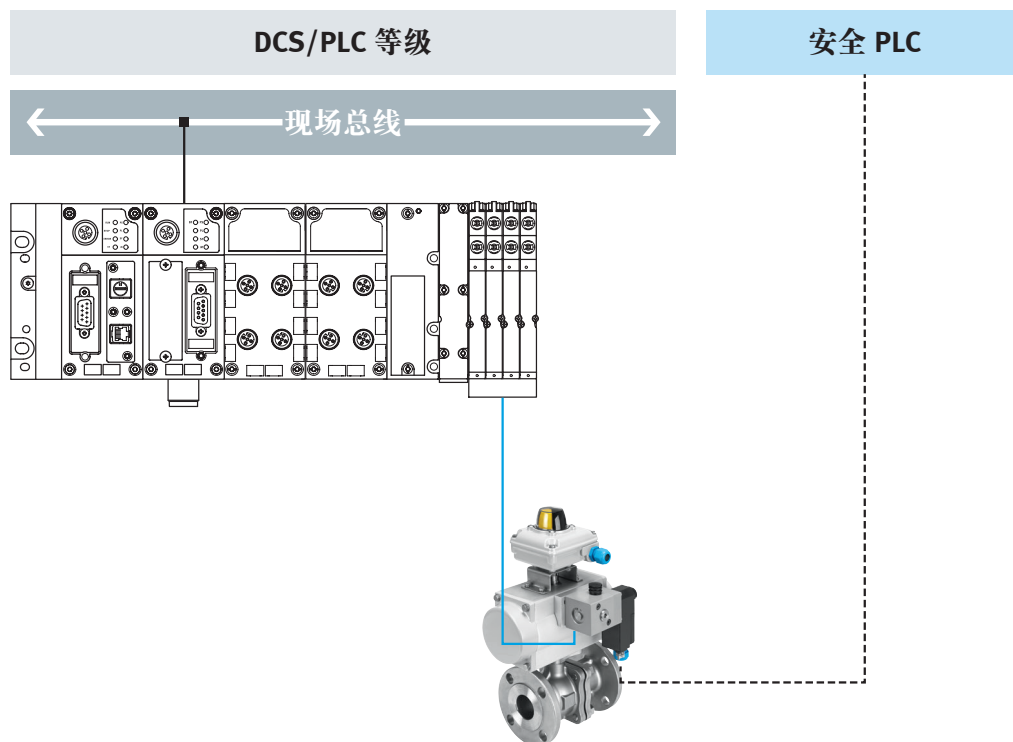
在运行模式下，阀岛通过现场总线驱动，并在此过程中切换驱动器。此外，阀岛有一个单独的电源供应给安全 PLC，该 PLC 驱动阀岛上的阀以实现安全关断。它还激活相同的驱动器以安全地关闭该过程。该解决方案适用于 SIL2 等级的回路。为了提高安全等级，可以选择冗余切换阀。

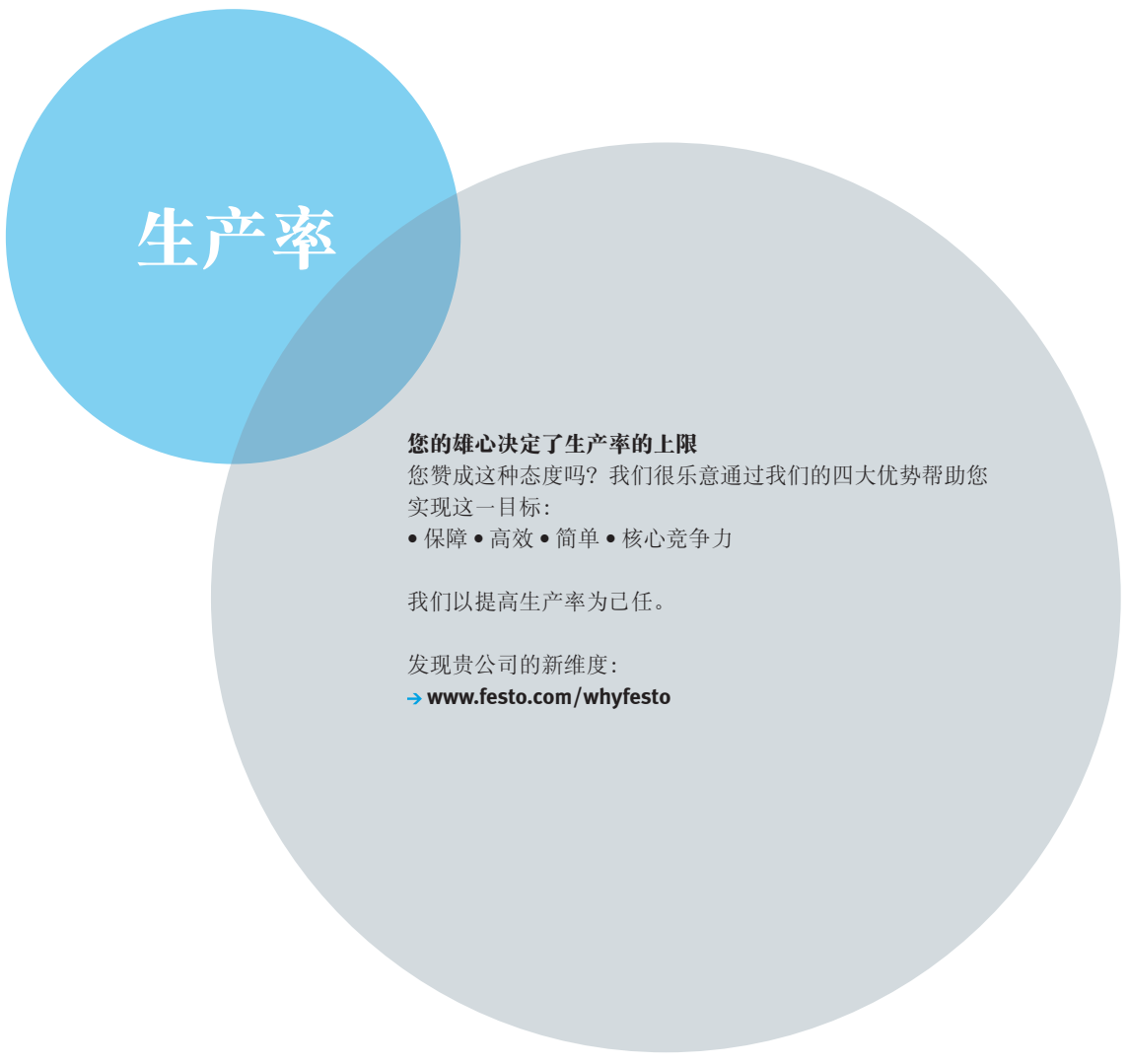


### 3.3 VOFC/D 作为安全阀

阀岛加独立阀，用于安全关断。

通过现场总线和阀岛控制工作模式，用于在现场切换驱动器。安装在同一驱动器上的经过认证的独立阀门由安全 PLC 直接驱动，并在需要时安全关断。这些阀可用于最高 SIL3 等级的安全相关回路。





# 生产率

## 您的雄心决定了生产率的上限

您赞成这种态度吗？我们很乐意通过我们的四大优势帮助您实现这一目标：

• 保障 • 高效 • 简单 • 核心竞争力

我们以提高生产率为己任。

发现贵公司的新维度：

→ [www.festo.com/whyfesto](http://www.festo.com/whyfesto)