# Safety@Festo

按 EN ISO 13849-1/EN 61508/EN 61511/EN 62061标准评估安全措施

FESTO

**风险评估**

**风险分析 > 风险评估 > 风险降低**

**> 设计对策**
**> 技术对策**
**> 用户信息**

更多信息见 → **www.festo.com/safety-guideline**

**气动技术安全子功能**

**STO** 安全切断扭矩
**PUS** 防止意外启动
**SSC** 安全停止和关闭
**SDI** 安全方向
**SSB** 安全停止和禁用
**SLS** 安全限速
**SLT** 安全扭矩限制 (力)

**电驱技术安全子功能**

**STO** 安全切断扭矩
**SS1** 安全停止 1
**SS2** 安全停止 2
**SDI** 安全方向
**SSB** 安全停止和禁用
**SLS** 安全限速
**SLT** 安全扭矩限制

**安全相关模块图**




哪些事件触发了安全请求?

例如:
- 接近危险区域
- 打开一扇安全门
- 过程超出设定极限值

触发识别设备
- 光栅
- 安全门
- 压力垫
- 紧停
- 故障
- 激光扫描器
- 相机
- 温度传感器
- 压力传感器
- 流量传感器

信号安全处理设备
- 接线
- 安全中继器
- 安全 PLC
- 气动控制系统

安全控制危险动作的设备
- 气动能
- 电能
- 液压能
- 电位（位置）能

## 六步评估安全功能

**EN ISO 13849-1** 适用于控制系统中安全相关的部件以及各类机器，与使用的技术和能源无关 – 电能、气动能、液压能或机械能。

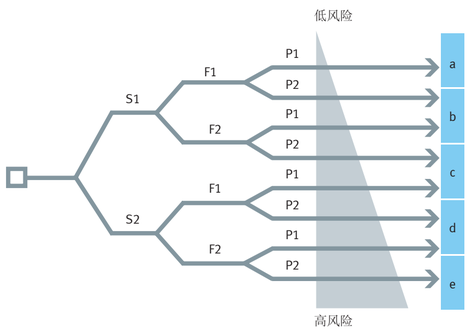
**EN 61508** 电气/电子/可编程电子安全相关系统的功能安全

**EN 61511** 过程行业安全相关系统的功能安全

**EN 62061** 机器安全 – 安全相关电气、电子和可编程电子控制系统的功能安全

应用场景评估

## 1 风险评估 – 确定所需安全性能等级 ($PL_r$)




S 伤害严重性
- S1 轻微 (伤害通常可逆)
- S2 严重 (伤害通常不可逆，包括死亡)

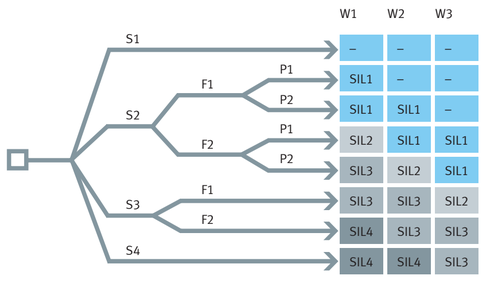
F 暴露在危险下的频率和/或持续时间
- F1 几乎没有到少有和/或短时间
- F2 频繁到持续和/或长时间

P 避免危险的可能性
- P1 在特定条件下可能
- P2 基本不可能

a – e 安全性能等级 ($PL_r$)

来源: EN ISO 13849-1

## 风险评估 – 确定所需安全整体性等级 ($SIL_r$)




S 伤害严重性
- S1 轻微人伤
- S2 多人严重受伤，乃至一人死亡
- S3 多人死亡
- S4 众人死亡的灾难性后果

F 频率
- F1 几乎没有到合理频率
- F2 频繁到持续

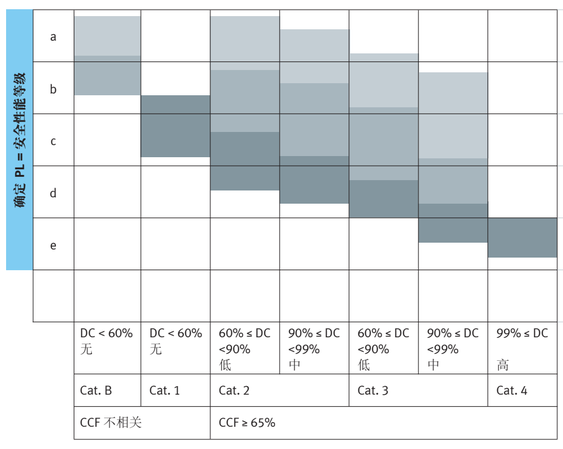
P 避免/减轻危险
- P1 在特定条件下可能
- P2 基本不可能

W 发生的可能性
- W1 相对较高
- W2 低
- W3 非常低

**SIL (安全整体性等级)**
四个等级 (SIL1到 SIL4)。一个安全相关系统的 SIL 越高，该系统不能执行必要安全功能的可能性越低。

## 2 从 $PL_r$ 和 $SIL_r$ 确定必要可靠性参数

**确定 $MTTF_D$ = 至故障的平均时间（危险）**




| 评估 | $MTTF_D$ |
|---|---|
| 低 | 3 年 ≤ $MTTF_D$ < 10 年 |
| 中 | 10 年 ≤ $MTTF_D$ < 30 年 |
| 高 | 30 年 ≤ $MTTF_D$ < 100 年 |

来源: EN ISO 13849-1

## 从 $PL_r$ 和 $SIL_r$ 确定必要可靠性参数

| SIL 等级 | 高需求模式 | 安全系统最大可接受故障 | 设备类型 A 安全故障率 (SFF) < 60% | 60...90% | 90...99% | >99% | 设备类型 B 安全故障率 (SFF) < 60% | 60...90% | 90...99% | >99% | 低需求模式 | 安全系统最大可接受故障 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $10^{-5} \le PFH < 10^{-4}$ | 一次失效风险 每 10,000 小时 | | | | | | | | | | |
| 1 | $3 \cdot 10^{-6} \le PFH < 10^{-5}$ | 一次失效风险 每 1,250 天 | HFT 0 | | | | HFT 1 | HFT 0 | | | $10^{-2} \le PFH < 10^{-1}$ | 每 10 年一次 |
| 1 | $10^{-6} \le PFH < 3 \cdot 10^{-6}$ | 一次失效风险 每 115.74 年 | | | | | | | | | | |
| 2 | $10^{-7} \le PFH < 10^{-6}$ | 一次失效风险 每 115.74 年 | HFT 1 | HFT 0 | | | HFT 2 | HFT 1 | HFT 0 | | $10^{-3} \le PFH < 10^{-2}$ | 每 100 年一次 |
| 3 | $10^{-8} \le PFH < 10^{-7}$ | 一次失效风险 每 1,157.41 年 | HFT 2 | HFT 1 | HFT 0 | HFT 0 | | HFT 2 | HFT 1 | HFT 0 | $10^{-4} \le PFH < 10^{-3}$ | 每 1,000 年一次 |
| 4 | $10^{-9} \le PFH < 10^{-8}$ | 一次失效风险 每 11,157.41 年 | | HFT 2 | HFT 1 HFT 2 | HFT 1 HFT 2 | | | HFT 2 | HFT 1 HFT 2 | $10^{-5} \le PFH < 10^{-4}$ | 每 10,000 年一次 |

[每小时]

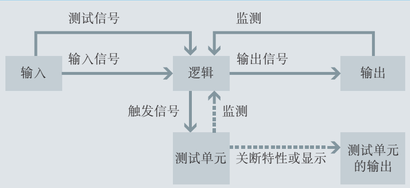
**设备类型 A**
设备所有元件的故障行为和故障特性已被充分确定。

**设备类型 B**
设备至少一个元件的故障行为和故障特性没有被充分确定。

## 3 控制架构 – 类别定义

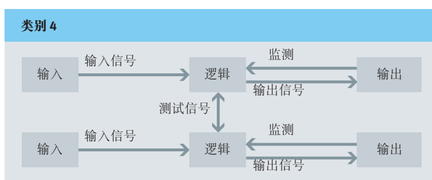
**类别 B/类别 1**

**类别 2**



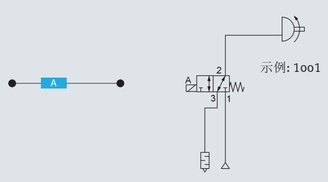

**类别 3**

**类别 4**



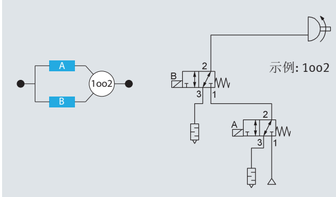

## HFT – 定义硬件故障容差

**HFT 0**



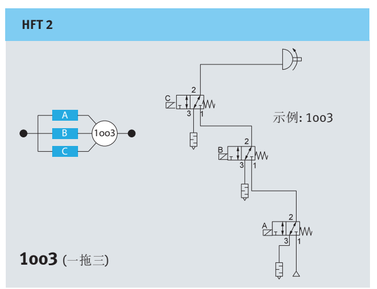

**1oo1** (一拖一)
单次故障导致安全丧失。

**HFT 1**




**1oo2** (一拖二)
至少两次故障必须同时发生才导致安全丧失。

**HFT 2**



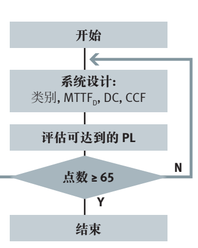

**1oo3** (一拖三)
至少三次故障必须同时发生才导致安全丧失。

**HFT (硬件故障容差)**
万一出现故障和偏差时，继续执行所需功能的能力

## 4 控制和检测故障的对策

**用于共因失效 (CCF) 的对策**

| 措施 | 点数 |
|---|---|
| 隔离/断开 | 15 |
| 多样性 | 20 |
| 设计/应用 | 20 |
| 评估/分析 | 5 |
| 专业能力/培训 | 5 |
| 环境/影响 | 35 |




**诊断覆盖 (DC)**

元件

· 会发生哪些故障?
· 这些故障是否危险?
· 这些危险故障是否可被检测到?

$$DC_1 = \frac{\Sigma \text{ (检测到的危险故障)}}{\Sigma \text{ (危险故障总数)}}$$

**整个系统**

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \dots + \frac{DC_n}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \dots + \frac{1}{MTTF_{DN}}}$$

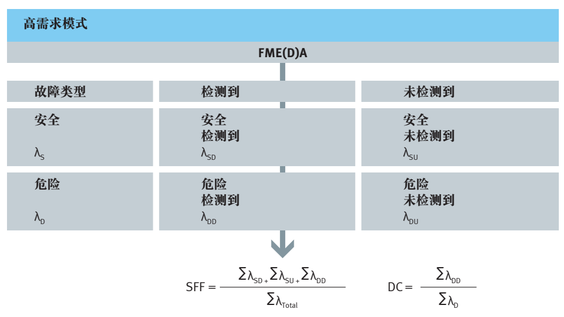
$$SFF = \frac{\lambda_{DD} + \lambda_S}{\lambda_D + \lambda_S}$$

$DC \le SFF \le 1$

for $\lambda_S \rightarrow SFF = DC$
for $\lambda_D \rightarrow SFF = 1$

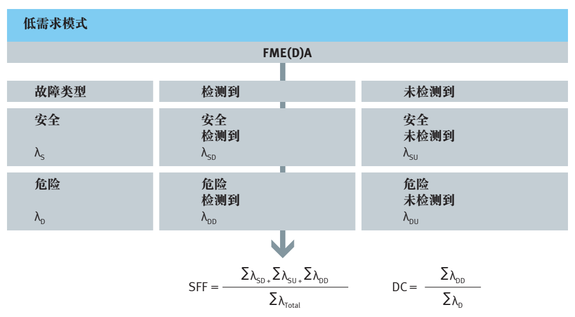
## 安全故障比率 (SFF) – 确定故障比率

**高需求模式**




$$SFF = \frac{\Sigma\lambda_{SD} + \Sigma\lambda_{SU} + \Sigma\lambda_{DD}}{\Sigma\lambda_{total}} \qquad DC = \frac{\Sigma\lambda_{DD}}{\Sigma\lambda_D}$$

**低需求模式**



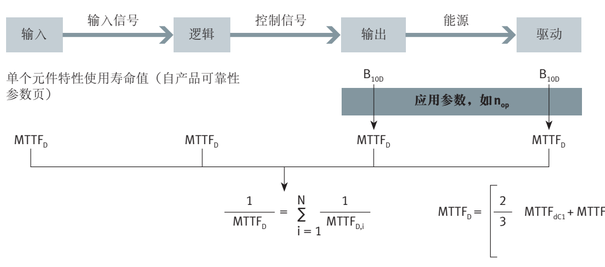

$$SFF = \frac{\Sigma\lambda_{SD} + \Sigma\lambda_{SU} + \Sigma\lambda_{DD}}{\Sigma\lambda_{total}} \qquad DC = \frac{\Sigma\lambda_{DD}}{\Sigma\lambda_D}$$

**λ (故障率)**
$\lambda_S$: 安全故障总故障率
$\lambda_D$: 危险故障总故障率
$\lambda_{SD}$: 总故障率，安全、检测到故障
$\lambda_{SU}$: 总故障率，安全、未检测到故障
$\lambda_{DD}$: 总故障率，危险、检测到故障
$\lambda_{SU}$: 总故障率，危险、未检测到故障

**FME(D)A**
**(故障模式、影响、诊断分析)**
故障类型和故障率定量确定分析法

**SFF**
**(安全故障率)**
基于故障总是的安全故障比例

## 5 $MTTF_D$ – 确定至故障 (危险) 的平均时间




$$MTTF_D = \frac{B_{10D}}{0.1 \cdot n_{op}}$$

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600\ s/h}{t_{cycle}}$$

$$\frac{1}{MTTF_D} = \sum_{i=1}^{N} \frac{1}{MTTF_{D,i}}$$

$$MTTF_D = \left[\frac{2}{3}\ MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}}\right]$$

公式，用于确定 $MTTF_D$ 值（用于一条通道内的一个机械元件）

年驱动次数平均数 $n_{op}$（用于机械元件）

计算多条平行通道的总 $MTTF_D$

$MTBF = MTTF + MTTR$

for $MTTF \gg MTTR$
$MTBF = MTTF$

$$PFH = \frac{1}{MTTF_D}$$

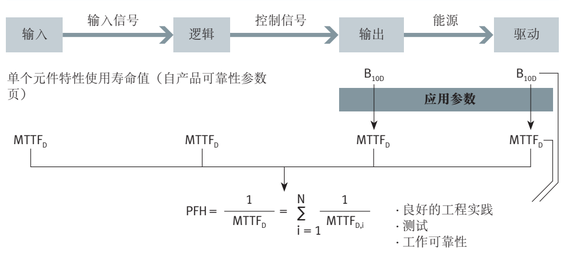
**$MTTF_D$ (至故障的平均时间)**
直至发生一次危险故障的平均时间

**MTTR (至恢复的平均时间)**
平均维修时间

**评估 $MTTF_D$**
低: 3 年 ≤ $MTTF_D$ < 10 年
中: 10 年 ≤ $MTTF_D$ < 30 年
高: 30 年 ≤ $MTTF_D$ < 100 年
(来源: EN ISO 13849-1)

## PFH/PFD – 确定故障的可能性

**高需求模式**



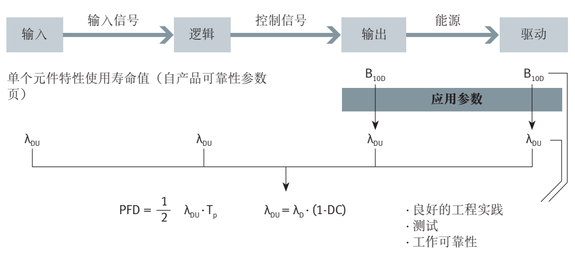

$$PFH = \frac{1}{MTTF_D} = \sum_{i=1}^{N} \frac{1}{MTTF_{D,i}}$$

· 良好的工程实践
· 测试
· 工作可靠性

**PFH (每小时发生故障的可能性)**
一次安全功能故障的可能性

**MTBF (故障平均间隔时间)**
先后两次故障平均间隔时间

**低需求模式**




$$PFD = \frac{1}{2} \lambda_{DU} \cdot T_p \qquad \lambda_{DU} = \lambda_D \cdot (1\text{-}DC)$$

· 良好的工程实践
· 测试
· 工作可靠性

**PFD (按需故障可能性)**
一次安全功能故障的可能性

**$T_p$ (验证测试间隔时间)**
验证测试的间隔时间

## 6 整个系统 – 目标: $PL \ge PL_r$

**一个控制系统安全相关部分的布局示例**

| 输入 | 逻辑 | 输出 | 驱动 |
|---|---|---|---|
| $B10_D$ | | $B10_D$ | |
| | | $MTTF_D$ | |
| $MTTF_D$ | | $MTTF_D$，每条通道 | |
| Cat. | | Cat. | |
| DC | | DC | |
| CCF | | CCF | |
| PL | PL | PL | |

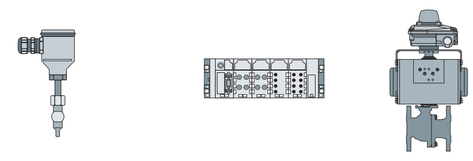
基于应用待确定

制造商告知
(制造商应提供用于确定 $B10_D$ 值的信息)

**PL ≥ $PL_r$**

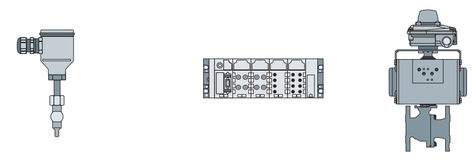
## 目标: $SIL \ge SIL_r$

**典型分布 PFH**
**单通道系统内一个安全功能子系统之间**



| 传感器 ≥ 35% | | 逻辑 ≥ 15% | | 驱动器 ≥ 50% | |
|---|---|---|---|---|---|
| PFH | $\lambda_{SD}$ | PFH | $\lambda_{SD}$ | PFH | $\lambda_{SD}$ |
| SFF | $\lambda_{SU}$ | SFF | $\lambda_{SU}$ | SFF | $\lambda_{SU}$ |
| HFT | $\lambda_{DD}$ | HFT | $\lambda_{DD}$ | HFT | $\lambda_{DD}$ |
| MTBF | $\lambda_{DU}$ | MTBF | $\lambda_{DU}$ | MTBF | $\lambda_{DU}$ |
| $SIL_{required}$ ($SIL_r$) | | | | | |
| $PFH_{total}$ | | | | | |

**典型分布 PFD**
**单通道系统内一个安全功能子系统之间**



| 传感器 ≥ 35% | | 逻辑 ≥ 15% | | 驱动器 ≥ 50% | |
|---|---|---|---|---|---|
| PFD | $\lambda_{SD}$ | PFD | $\lambda_{SD}$ | PFD | $\lambda_{SD}$ |
| SFF | $\lambda_{SU}$ | SFF | $\lambda_{SU}$ | SFF | $\lambda_{SU}$ |
| HFT | $\lambda_{DD}$ | HFT | $\lambda_{DD}$ | HFT | $\lambda_{DD}$ |
| MTBF | $\lambda_{DU}$ | MTBF | $\lambda_{DU}$ | MTBF | $\lambda_{DU}$ |
| $SIL_{required}$ ($SIL_r$) | | | | | |
| $PFD_{total}$ | | | | | |

**SIL ≥ $SIL_r$**

当要从 PL 转换为 SIL 或反之，必须考虑适用标准 (EN ISO 13849-1, EN 61508, EN 61511, EN 62061) 所含的附加要求。



136100 cn 2021/02 – Errors and omissions excepted