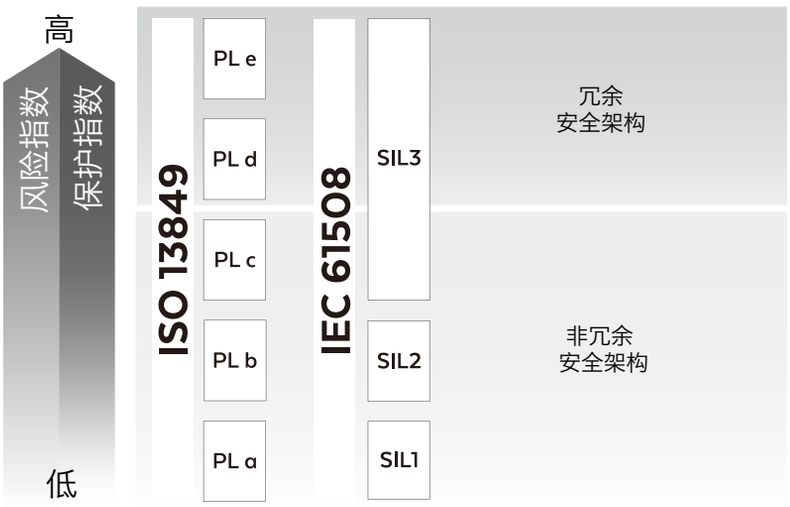
安全型元件的基本信息

IEC 61508安全完整性等级和ISO 13849性能等级 - 通过 TÜV 认证



现代机械工程的安全性正成为保护人们免受机械和系统意外故障潜在风险的首要问题。
机器指令2006/42/EC具有相关规范 **IEC 61508安全完整性等级（SIL）**和**ISO 13849性能等级(PL)**，代表功能安全的框架，就涉及健康影响的设备或系统安全的基本预防原则而言，这是一个关键方面。它规定了机器制造商必须遵守的安全要求，以此获得认证，从而可能在欧洲市场销售机器时使用 CE 标志。
机器指令2006/42/EC取代了现有的98/37/EC，并普遍适用于机械、安全元件和其他特定设备。

1 安全规范

IEC 61508和相关规范IEC 61511（过程控制系统）以及IEC 62061（机器控制系统）介绍了功能安全的综合概率方法。它们规定了执行安全功能所需的安全完整性等级（SIL）。
ISO 13849 规范为控制系统安全相关部分的设计和一体化（包括软件设计）的原则提供了安全要求和指南。
它规定了执行安全功能所需的性能等级 (PL)。
PL：离散值，指定控制系统的安全相关部分在可预见条件下执行安全功能的能力。
这些要求分为五个性能级别，其中 PL e 表示最高保护级别。

2 认证

Atos 安全阀（开关阀和比例阀）通过 TÜV 认证，符合 IEC 61508、IEC 61511、IEC 62061、ISO 13849 标准
该认证保证阀符合相关安全规范，并证明已满足特定阀要求的SIL和PL水平的所有要求。

该认证还确认了机器制造商可用于整个系统认证的以下数据:
- 阀制造商为避免故障而采用的设计过程
- 用于控制故障的设计技术和措施
- 用于定义硬件故障公差的方法
- 用于测量安全失效分数的方法
- 用于测量故障概率的方法

⚠ **使用未经认证的产品，机器制造商有责任验证上述所有方面是否已按照适用标准执行。**

在阀没有认证的情况下，机器制造商必须:
- 从阀制造商处收集评估整个系统安全级别所需的所有可靠性数据
- 考虑安全等级的最坏情况（例如，为阀分配较低的安全等级 PL a 或 SIL 1 以计算系统安全性）

3 风险评估

确定必要风险降低的第一步是风险评估。
这是一个通过安全控制系统（例如激光屏障、截止阀、启用装置等）确定机器中哪些风险需要缓解的程序。每一个控制系统成为一个安全功能。
此时，安全功能必须由机器设计来定义和满足（见3.1）。

⚠ **机器制造商有责任确保满足所有安全要求，并进行记录在案的风险评估，以确保涵盖所有潜在的机器危险。**

3.1 机器制造商

“机器制造商”是指为自己的需要制造机器的原始设备制造商或最终用户，或执行“重大改装”的所有人：

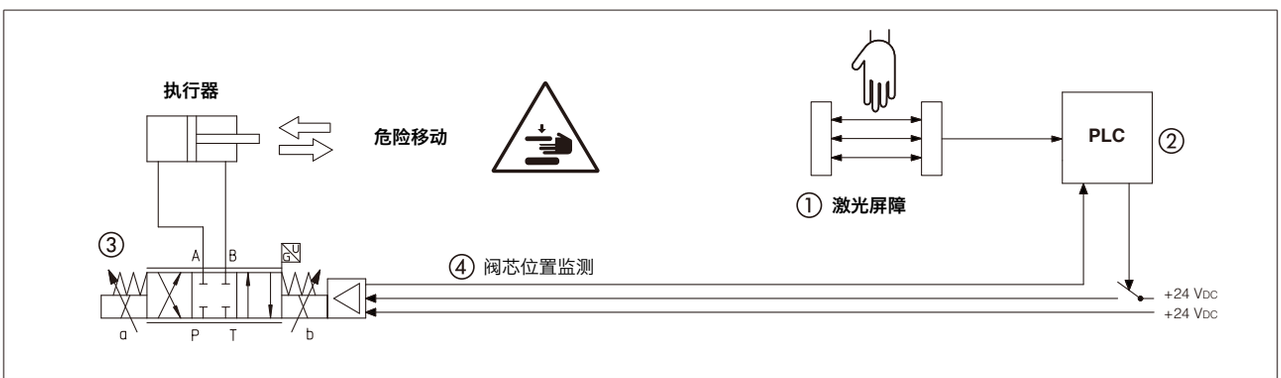
- 改变机器功能
- 更改机器应用区域
- 更换设备
- 改变机器性能

如果改变上述任何参数导致预期用途的改变或安全系统或安全部件的改变，则机器改装应被视为“重大改装”。

举例：
添加气枪气动连接 = 无重大改装
增加液压蓄能器以提高机器的速度并改善循环时间 = 重大改装

4 安全相关部件

它们是执行安全功能的机器控制系统的一部分，允许系统达到或保持安全状态。
这些部件由硬件或软件以及机器控制系统的独立或集成组件组成。
安全相关部件包含由控制单元、阀、传感器和执行器提供的安全功能的整个有效链。



①	②	③	④
传感器	逻辑级	阀	阀诊断功能
发现危险情况	控制机器运行，并在 危险情况下启动安全程序	控制执行机构， 避免危险移动	监控阀正确操作

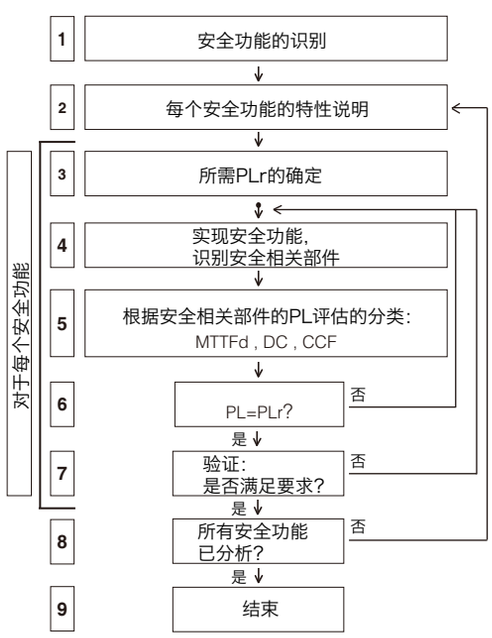
5 安全分析

风险识别后的第二步是安全分析。
控制系统安全相关部分的设计过程是重复的。

一旁方案显示了EN ISO 13849-1使用的方案：

- 第一步是识别安全功能。
- 必须描述和记录所有安全功能的任何特征。
- 必须定义每个安全功能所需的性能等级 (PLr)。
  ISO13849-1 使用类似于 5.1 节中所示的路径。
- 机器制造商必须设计一个系统来保护操作员，授予等于或高于所需性能等级 (PLr) 的性能等级 (PL)。 必须考虑以下参数来定义性能级别 (PL)：

- MTTFd，安全系统的可靠性——见第5.2节
- DC，检测故障的能力 - 见第5.3节
- CCF，系统易受故障影响——见第5.4节
- 安全系统的架构类别——见第 6 节



5.1 要求的性能水平 - PLr

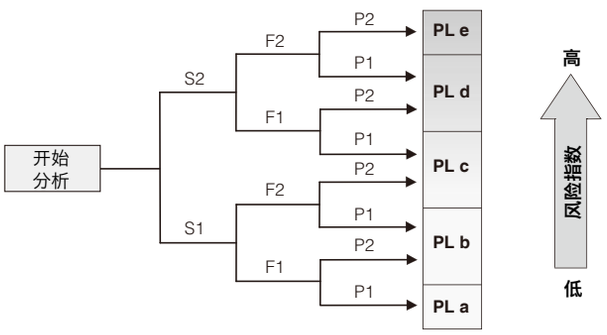
通过分析以下参数，确定ISO 13849-1的PLr：

• 伤害的严重程度：
S1 = 轻微
S2 = 严重

• 暴露于危险的频率和持续时间：
F1 = 不经常
F2 = 频繁

• 避免危害或限制危害的可能性：
P1 = 可能
P2 = 几乎不可能

根据每小时发生危险故障的概率，五个性能等级中的每一个都对应一个进一步的参数等级。



性能等级	每小时危险故障的平均概率，h-1
PL e	≥10^{-8} to < 10^{-7}
PL d	≥ 10^{-7} to < 10^{-6}
PL c	≥10^{-6} to < 3 x 10^{-6}
PL b	≥ 3 x 10^{-6} to < 10^{-5}
PL a	≥ 10^{-5} to < 10^{-4}

5.2 平均无危险故障时间 - MTTFd

特定PL或SIL的实现取决于系统的可靠性。
可靠性通过以小时为单位的平均无危险故障时间（MTTFd）进行量化。
MTTFd应根据元件制造商的数据确定。

5.3 诊断覆盖率 - DC

诊断覆盖率 (DC) 衡量监控系统检测潜在危险故障的有效性。
EN ISO 13849-1 建议如何定义 DC。
诊断覆盖率定义为诊断有效性的度量：它被确定为检测到的危险故障的故障率与总危险故障的故障率之间的比率；

诊断覆盖范围类别：

类别	范围
无	DC < 60%
低	60% ≤DC < 90%
中	90% ≤DC < 99%
高	DC ≥ 99%

DC = 0% 未检测到危险故障

DC ≈100% 检测到大多数危险故障（不可能达到DC=100%，因为诊断不完全可靠）

5.4 共因故障 - CCF

CCF 值是用于评估针对共因故障的措施的参数。
这是冗余系统中的故障，其中两个或多个通道由于一个共同原因而同时发生故障。
如果两个通道由于相同的原因同时出现故障，则冗余可能会受到影响。
EN ISO 13849-1为CCF提供了一个评分，用于确定性能级别(PL)。

为此，EN ISO13849-1定义了7项重要对策：

1. 不同通道的信号路径物理分离(得分= 15分)
2. 通道的技术、设计或物理原理的多样性(得分= 20分)
3. 对可能过载的防护(15分)和使用经验丰富的组件[这些组件已被广泛使用或制造，并验证用于安全相关的应用(得分= 5分)]
4. 开发过程中的故障模式和影响分析，以识别潜在的共同原因故障(得分= 5分)
5. 设计/服务人员CCF培训及规避(得分= 5分)
6. 防止污染(流体过滤)和电气部件电磁干扰引起的常见故障(得分= 25分)
7. 不利环境条件引起的共因故障保护(得分=10分)

对于架构类别2、3和4，最低得分要求为65分（见第6节）。
注：CCF始终取决于系统和应用程序。

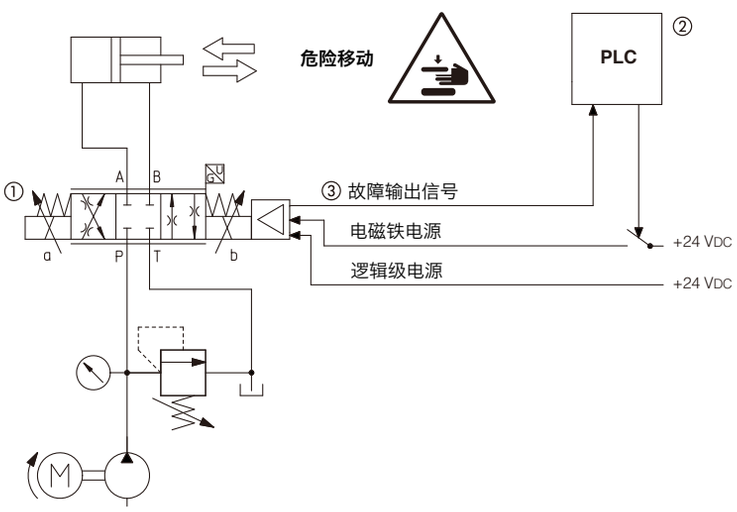
6 架构类别

SIL 和 PL 级别不仅取决于单个元件的特性，还取决于液压系统的架构和信号诊断。
架构类别有助于定义故障概率和控制系统安全相关部分的 PL，与它们对故障的抵抗力及其在故障条件下的后续行为有关
有五种架构类别，标识为：B、1、2、3、4
数字越高，安全系统的复杂性越高，达到的性能等级 PL 也越高。

6.1 架构类别 B 和 1

在 B 类和 1 类中，抗故障性能主要是通过选择合适的元件来实现的。 它们不是冗余架构，因此发生故障可能会导致安全功能的丧失。
1 类比 B 类具有更大的抵抗力，因为使用了在安全方面经过充分试验和测试的特殊元件和原理

架构类别 1 示例



安全功能 = 防止油缸在循环的某一阶段或紧急情况下发生危险移动

安全功能是通过切断到安全型比例阀电磁铁的电流来实现的。这样阀芯就可以通过弹簧移动到静止位，正遮盖。

通过对阀芯位置的连续监测，机器PLC验证“安全状态”是否完全完成。

⚠ **阀发生故障时，不执行安全功能①**
故障容差HFT=0

① 带双电源的数字比例阀 - 选项/U
(i.e. DHZO-TES-SN-NP-07*-L5 **/U**)

② 机器PLC监控安全功能

③ 用于安全诊断的故障输出信号

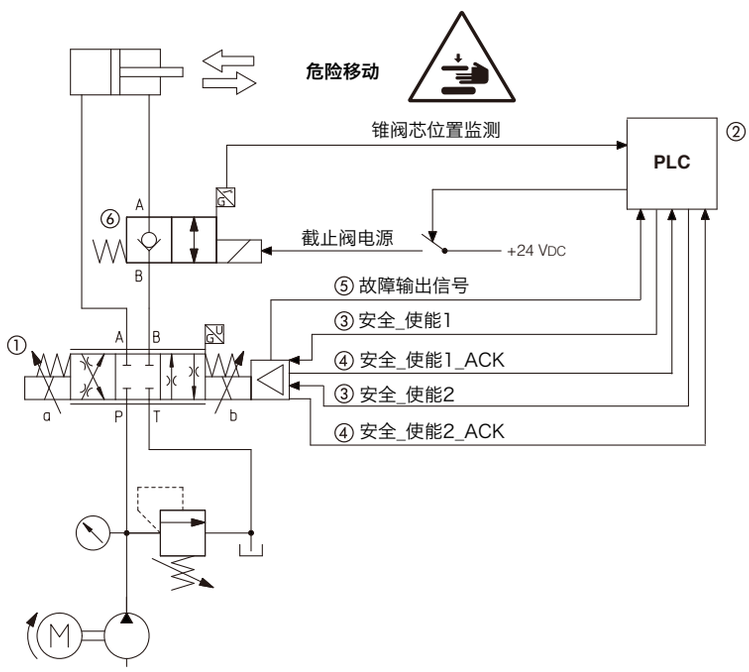
6.2 架构 - 类别 2

在类别2中，架构B和1的所有需求都被合并。此外，对系统进行监控，以拦截影响安全功能的故障。
这些监控是定期进行的，例如在启动时或在下一次要求安全功能之前。
通过选择适当的测试间隔，可以获得适当的风险降低。

6.3 架构类别 3 和 4

在第 3 类和第 4 类中，单个故障的发生不会导致安全功能的丧失。
在类别 4 中会自动检测到此类故障。
故障累积不会导致安全功能丧失。

架构类别 4 示例



① 数字比例阀 - 选项/K
(i.e. DHZO-TES-SN-NP-07*-L5 **/K**)

② 机器PLC监控安全功能

③ 用于启用/切断阀电磁铁电流的信号

④ 确认阀安全状态的信号

⑤ 用于安全诊断的故障输出信号

⑥ 带锥阀芯位置监测的安全截止阀（如 JO-DL /FV)

安全功能 = 防止油缸在循环的某一阶段或紧急情况下发生危险移动

在本例中，安全比例阀增加了一个带锥阀芯位置开关的安全型截止阀，以实现冗余安全架构。

安全功能是通过切断到安全型比例阀和安全型截止阀电磁铁的电流来实现的。这样阀芯就可以通过弹簧移动到静止位，正遮盖。

安全条件通过以下方式确认：
- 安全_使能_ACK 状态 = 24 VDC
- 截止阀锥阀芯位置监控信号

⚠ **即使在一个阀发生故障的情况下也能执行安全功能，①或⑥**
故障容差HFT=1