产 品 简 介

机械安全用户指南

保证机械安全的六个步骤

safety PLUS®

德国西克传感器

SICK
Sensor Intelligence.

公司简介

SICK——德国总部

SICK—存在于很多行业

- 电子半导体工业
- 汽车行业
- 食品处理、饮料和烟草工业
- 包装、印刷工业
- 物流和仓储系统
- 工业流程
- 环境测量
- 及其它很多行业

欢迎来到全球传感器系统供应商基地

SENSICK— 先进、强大的传感器技术的代名词。SENSICK 自动化解决方案是优化和改进生产过程的理想选择。今天,SICK 公司已在40多个国家建立了分支机构，拥有5000多名雇员，是世界上著名的传感器生产商之一。

优化全部生产过程

现今，企业要发展，必须注重过程而不是功能；必须排除不灵活的工作过程，全面优化价值的生产过程。因此，必须要有一个整体的，而不是单纯地解决某一问题的自动化解决方案。

作为全球自动化、安全技术、环境监测系统和自动识别系统等传感器领域的佼佼者，SICK公司致力于发展工业过程的现代化和合理化。

作为一个有 60 多年传感器技术经验的公司，SICK 熟知工业生产各部分,可以为工业生产各个领域提供最优化的解决方案。

质量是关键

我们遍布全球的客户的成功经验都向我们传递了这样的一条信息：
SICK 传感器的产品质量和产品的长期使用寿命是无可比拟的。这是研发、生产、销售和服务的完全质量管理的结果。质量永远是 SICK 公司的中心目标，每一个员工都把追求高质量作为他们的工作目标。

产品范围

- 工业用光电开关
- 接近开关及磁性气缸开关
- 视觉传感器
- 超声波传感器
- 旋转编码器
- 激光距离检测系统
- 光电安全保护装置
- 环境检测系统
- 自动化辨读系统
- 交通管理及监控系统

保证机械安全的六个步骤

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

安全的机械可以让制造商和运营机构不受控诉的困扰。机器使用者也希望他们的机器或设备是安全的：这种愿望在全世界都一样。世界各地都有关于保护机器使用者安全的法规，这些法规在不同的地区可能会有所不同。然而在机械制造和升级过程中采用的程序是有广泛共识的：

- 在机械制造过程中，机器制造商应该通过风险评估（此前也称危险分析）识别并评估所有的潜在危险和危险点。
- 根据风险评估的结果，机器制造商应采取适当措施消除或**降低风险**。如果风险无法在设计中消除，或者降低后的风险仍不可接受，机器制造商应选用适当的防护设备，并在必要时提供有关该风险的信息。
- 为保证使用的措施能够发挥应有作用，需要对其进行**全面验证**。全面验证包括对设计、技术措施以及对针对具体环境的组织措施进行验证。

我们将会通过六个步骤指导您实现机械安全。这些步骤在左页列出。

关于本指南

主要内容

本指南与机械以及选用防护设备的法律背景相关。在适用欧洲指令、法规和标准的规范下，我们将向你展示各种避免机械和人员发生事故的方法。本文中的示例和内容源自我们的多年实践经验，可视作典型应用。

这些指南对欧盟与机械相关的法律要求及这些要求的具体实施进行了说明。其他地区（如北美、亚洲）对机械相关的法律要求在相应独立版本中说明。

无论基于何种法律，以下信息不能作为索赔依据，因为每一台机器都需根据相应国家及国际法规和标准制定解决方案。

这些指南在交付印刷之际，参考的是此后适用的新版机械指令 (2006/42/EC)。在出版时我们仅参考最新的、已发布的标准。在推行新的标准后，我们拥有使用先前标准的一个过渡期，这些在相关章节中进行说明。

➜ 下文参考的其他标准或辅助材料均使用蓝色箭头标示。

目标读者

本指南主要供制造商、运营机构、设计人员、系统工程师以及所有负责机械安全的人员阅读和使用。（为方便阅读，下文仅使用男性称谓。）

编辑团队

从左到右：Otto Görnemann, Hans Simonyi, RolfSchumacher, Doris Lilienthal, Jürgen Bukowski, GerhardDieterle, Carsten Gregorius

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

工作人员的安全

随着自动化越来广泛的应用，关于机械保护的要求也在不断改变。在过去，保护系统通常是很麻烦的事情，因此经常不被使用。防护设备现在可以通过创新的技术集成到工作过程中，因此不会对操作员造成障碍，实际上它们还经常可以提高生产力。正因如此，将可靠的防护设备集成到工作场所在现在已经成为一种必要措施。

安全是基本需求

安全是人们的一个基本需求。研究显示连续处在压力条件下的人更易患上由心理因素引起的疾病。尽管从长期来看这些极端条件也会为人们所适应，但它们还是会对个人造成极大压力。因此我们可以得出以下目标：**机器的安全性要能够为操作员和维修人员所信任！**

人们通常会说安全性越高生产力就越低，而事实正好相反。更高的安全等级会带来更大的动力和更多的满足感，从而提高生产力。

安全是一项管理任务

工厂中的决策者要对他们的雇员负责，还要为生产的平稳运行及效益负责。仅当安全成为日常工作的一部分时，雇员们才会容易接受安全的理念。

为了增强可持续性，专家呼吁在组织内建立覆盖广泛的“安全文化”。而这也并非毫无道理，毕竟十分之九的事故都是由人为因素造成的。

雇员亲自参与才会真正认可

在对安全理念进行定义时考虑到操作者和维修人员的需求是非常重要的。优秀的安全准则仅在与工作过程和工作人员的理念相匹配时，才会被真正接受。

需要专业知识

机械安全在很大程度上依赖于相关指令和标准的正确应用。在欧洲，各国的法律要求与欧洲指令（例如机器指令）是相协和的。

这些指令给出一般要求，更详细的内容在标准中规定。欧盟标准通常也在欧盟以外的地区被接受。

在实践中执行这些要求需要大量的专业知识、应用知识和多年工作经验。

欧盟指令及标准适用于在欧盟市场上推出机械产品的制造商和组织。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

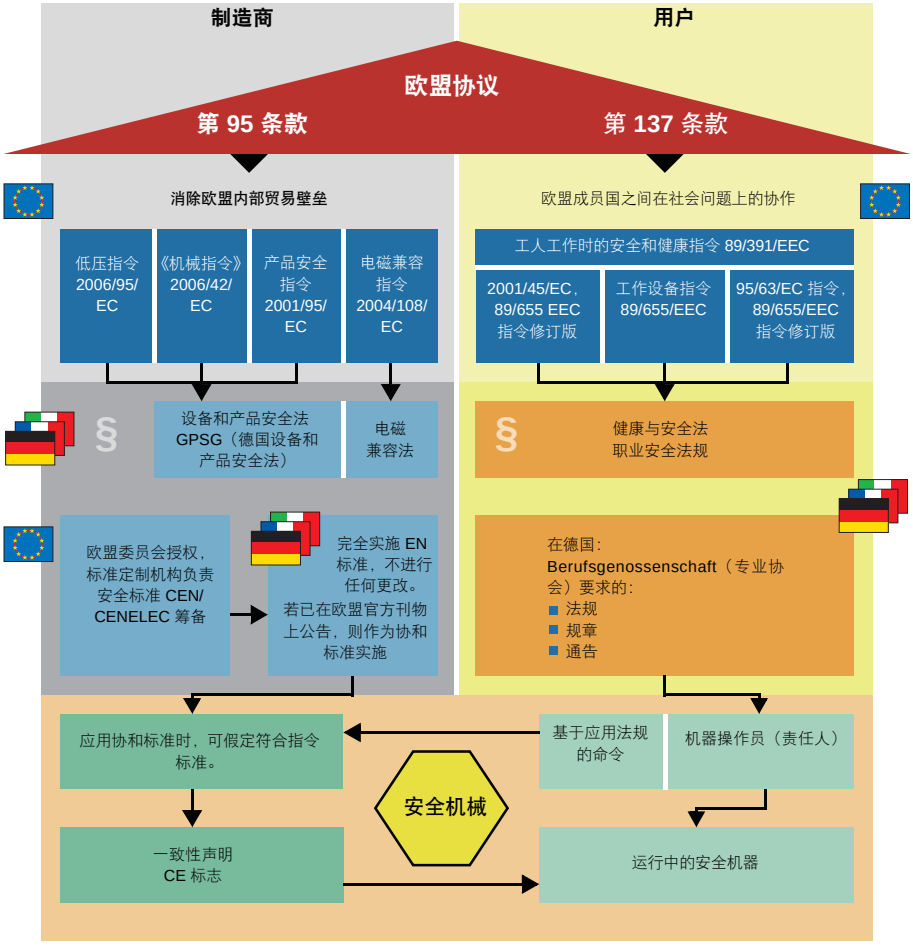
欧洲指令

欧共体的其中一项基本目标就是保护其公民在私人和专业领域的健康。另一项基本目标则是建立共同的自由贸易市场。

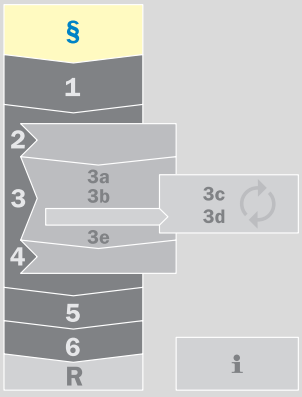
为同时实现自由贸易和公民保护这两项目标，欧盟委员会和欧盟理事会发布了一系列指令。这些指令将在其成员国的法规中强制执行。这些指令规定了基本的对象和要求，并尽可能仅限于技术领域。

在工作健康与安全，以及机械安全领域，颁布了以下指令：

- 《机械指令》，主要针对机械制造商
- 工作设备指令，主要针对机械使用组织
- 其他指令，如低压指令、电磁兼容指令、ATEX 防爆指令等



➜ 任何人均可免费获取这些指令，如访问 http://eur-lex.Europa.eu/



与防护设备所用要求一样，不同国家将针对机械安全有着不同的法规要求和技术标准。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

§

《机械指令》

《机械指令》2006/42/EC 主要针对机器和安全部件制造商以及此类产品的代理商。该指令规定了新机械所要遵循的健康与安全要求。其目的是在消除欧洲内部贸易壁垒的同时，为用户和操作员提供高级别的安全和健康防护。

该指令适用于机器产品以及单独出售的安全部件，同时适用于即将首次在欧盟区域销售的其他国家（如美国或日本）二手机器和设备。

- 1989 年，欧盟理事会在协调其成员国相关法令的前提下，制定了机械相关的指令。后来称为**《机械指令》**(89/392/EEC)。
- 自 1995 年起，该指令成为欧盟理事会成员国的强制法令。
- 1998 年，在将许多不同修订整合后，形成了当前使用的《机械指令》(98/37/EC)。
- 2006 年，欧盟发布了“最新版《机械指令》”(2006/42/ EC)，它将替代之前的《机械指令》。该指令将自 2009 年 12 月 29 日起在欧盟理事会成员国强制实施。

2009 年 12 月 29 日前，依旧仅实施“旧版”《机械指令》(98/37/EC)！
自 2009 年 12 月 29 日起，仅可实施“新版”《机械指令》(2006/42/EC)！

《机械指令》现已在以下国家实施：
- 英国：机械设备（安全）供应法规 2005
- 芬兰：Valtioneuvoston päätös koneiden turvallisuudesta (VNp 1314/1994, ns. “Konepäätös”)
- 丹麦：Warenwet, Besluit machines
- 比利时：KB05/05/1995, AR05/05/1995

对于符合《机械指令》的机器和安全部件，各成员国不得阻止、限制或妨碍其在欧盟范围内的销售和运行。

因此，他们也无权通过国家法律、法规或标准制定更高产品要求！

工作设备指令

工作设备指令中规定了雇主的义务。该指令适用于工作场所的机器和设备。

该指令的目的在于减少工作设备使用期间所需的安全规程，从而更好地保证雇员的健康与安全。

各成员国有权添加自己的规定：如工作设备测试、服务或维护间隔、个人防护设备的使用以及工作场所设计等设计的规定。

工作设备指令要求和各国自身的要求和规范都将作为所在国的法规实施。

- 英国：工作设备的供应和使用规定 1998
- 芬兰：Valtioneuvoston päätös työssä käytettävien koneiden ja muiden työvälineiden hankinnasta, turvallisesta käytöstä ja tarkastamisesta (VNp856/1998, ns.“ Käyttöpäätös”)
- 丹麦：De Arbowet, het Arbobesluit
- 比利时：De Welzijnswet en de Codex over het Welzijn op het Werk, la Loi sur le Bien-être et le Code sur le Bien-être au Travail

➜ 工作设备指令 89/655/EEC：http://eur-lex.europa.eu/

机械制造商的义务是什么?

安全设计机器

机械制造商有义务保证制造的机械符合《机械指令》中健康与安全方面的主要条件。在设计过程中，制造商应将安全因素纳入设计范围。意即设计师在机械研发阶段就应尽早评估风险，然后将应对措施融入研发过程。具体的操作程序可见本指南的第 1 至 5 步。

准备操作指南

机械制造商应准备操作指南，即俗称的“原始操作指南”。每台机器均应附带提供所用国官方语言版操作指南。这些随机器附带提供的操作指南应为原始操作指南，或者原始操作指南的译文版。如为后者，仍需提供原始操作指南。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

§

准备技术性文档

机械制造商应准备好技术性文档。此类技术性文档应：

- 包含证明遵循《机械指令》内主要健康与安全要求的所有图表、计算、测试报告和文档。
- 应至少存档十年以上—自机器（或机器类型）制造之前一日起。
- 按照相关法规要求，提交至相关机构。

说明：《机械指令》中并未规定“制造商有义务向机器买家（用户）提供技术性文档”。

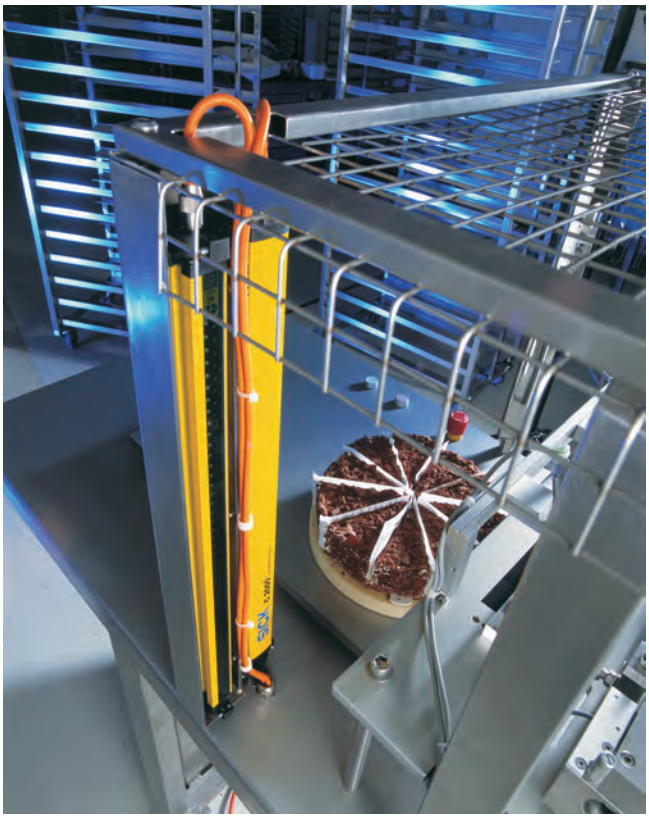
发表一致性声明：

如果机械制造商正确地制造机械，他可发表一个一致性声明并张贴《机械指令》标记（CE 标志），以合法绑定的方式担保其合乎指令要求。此后此类产品将允许在欧洲市场上出售。《机械指令》中说明了一致性检验的整个程序。针对不同机械需要区分两种不同程序（➜第 §-4 页上的“机械和安全部件的 EC 一致性验证过程”）：

- **标准程序：**未在附录 IV 中明确列出的机械须采用标准程序。应遵循《机械指令》附录 I“必备的健康与安全要求”一节所述要求。制造商应自己张贴 CE 标志，无需由特定组织或官方机构进行鉴定（即“自我鉴定”）。然而，制造商首先应编写技术文档，以便提交至官方机构。
- **附录 IV 中列出的机械的程序：**特别危险的机械应该采用特定程序。

  《机械指令》附录 IV 包含一份相关的机械和安全部件列表，此列表囊括了诸如光电安全开关和安全激光扫描器等电敏防护装置。应首先遵循《机械指令》附录 I 中“主要健康与安全要求”一节所述要求。如果存在机械或安全部件适用的协和标准，且这些标准涵盖全部要求范围，则可通过以下三种方法获得一致性声明：
  - 自我鉴定
  - 由经过认证的机构进行 EC 类检验
  - 使用通过认证的完整质量管理体系

如果不存在适用于机器的协和标准，或存在无法按照协和标准制造机器或机器零件，那么只能通过如下方式获得一致性



声明：

- 认证机构进行 EC 类检验：在认证机构进行测试时，制造商应提供机器以及相关的技术性文档，以便通过“EC 类检验”验证机器是否满足必备的健康与安全要求。认证机构负责测试其是否采用规定的机械指令，并提供包含测试结果的 EC 类检验证书。
- 使用通过认证的完整质量管理体系：完整的 QMS（质量管理体系）应保证与《机械指令》要求一致，且须经认证机构进行评估。制造商要永远对 QMS（质量管理体系）的有效性和正确使用负责。另见《机械指令》附录 X。

为机器张贴 CE 标志：

一旦满足了所有的要求，即可在机器上使用 CE 标志。

警告！仅在机器满足所有适用欧洲指令时，才可使用 CE 标志。（此后方可在欧盟市场上销售）

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

§

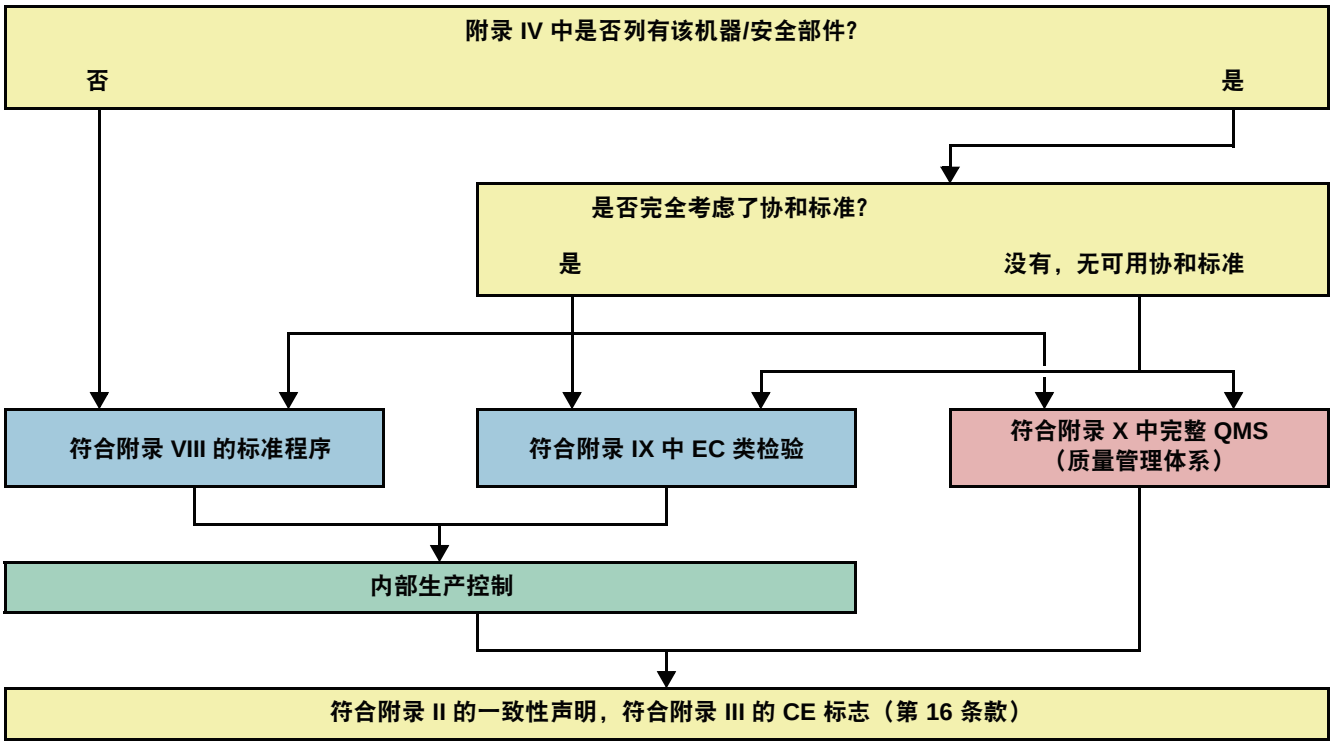
特殊情况：部分完整机械

在许多情况下，所生产和交付使用的机器零件、机器组件或机器部件与机械的定义非常接近，但在《机械指令》中并不认定为一台**完整的机器**。《机械指令》将"部分完整机器"定义为：一组能够组成机器的部件，但仅依靠其自身并不具有任何具体功能。如一个单独的工业机器人就是一个部分完整机器。一个部分完整机器按照规定只能安装在其他机器、其他部分完整机器或设备上，或者将它们组合起来以组成指令中包含的机器。部分完整机器并不符合《机械指令》的所有要求。因此《机械指令》采用一个特殊程序管理其自由贸易：

- 制造商应该满足《机械指令》中所有合理、可行的必备要求。
- 制造商应该发布一个成立声明。此声明须包含所适用和符合的主要指令要求。与完整机器类似，也应准备正式的技术性文档并存档。
- 制造商同样应准备装配指南（而非操作指南），并将它们随"部分完整"机器一起提供。此类装配指南所用语言应由制造商和用户（组装者）共同协商确定。

➜ 另见第 §-8 页“机构、保险商和政府机构”一章。

机器和安全部件的 EC 一致性验证程序



© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

标准

标准是各相关利益方（制造商、用户、权威机构和政府）之间所达成的协议。与我们通常的想法不同，标准并不由政府或官方筹备或认定。标准描述的为其筹备阶段技术水平。数百年来，国家标准到全球通用标准都在改变。机器或产品使用地点不同，适用的法律条款也会有差异，相应标准也会有所出入。正确选择所使用的标准可使机械制造商与法律要求保持一致。

世界标准化组织和结构

ISO（国际标准化组织）

ISO 是一个由来自 157 个国家的标准化组织组成的世界性联合会。ISO 主要筹备和发布非电气技术方面的国际标准。

IEC（国际电工委员会）

国际电工委员会 (IEC) 是一个筹备和发布电气技术（例如电子、通信、电磁兼容、发电）及其相关技术领域国际标准的国际组织。

欧洲标准化组织和结构

CEN（Comité européen de normalisation/欧洲标准化委员会）

CEN 由欧盟、欧洲自由贸易区成员国以及未来的欧盟成员国组成的标准化组织机构。CEN 筹备欧洲非电气领域标准 (EN)。为避免因标准差异形成贸易壁垒，CEN 与 ISO 之间会进行了协商。CEN 采用投票程序确定是否采用 ISO 标准并将其作为欧洲标准进行发布。

CENELEC（Comité européen de normalisation electrotechnique/欧洲电工标准委员会）

CENELEC 是与 CEN 类似的一个电气技术领域机构，负责筹备和发布欧洲电气技术领域标准 (EN)。与 CEN 和 ISO 状况类似，CENELEC 越来越多地采用 IEC 标准以及它们的编号系统。

国家标准化组织和结构

通常，欧盟成员国均有各自的标准化组织，如DIN、ON、BSI和AFNOR等。这些组织根据相应成员国的法律要求筹备和发布国家标准。为在欧共体内实现协调一致的健康与安全标准，消除贸易壁垒，各国的标准化组织将沿用欧洲标准。以下为处理欧洲标准和各国标准所采用的原则：

- 若国家标准中存在与欧洲标准类似的内容，将取缔各国的标准。
- 若欧洲标准中未具体指明方面或机器，则可沿用各国的现有标准。
- 如果其他标准化组织表示要筹备新的国家标准，而在整个欧洲（CEN 或 CENELEC）在知晓后并无异议，方可筹备新的国家标准。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

§

欧洲机械安全相关标准

为了能够具体应用中履行欧洲指令规定的目标和要求，技术标准中应包含详尽、具体的说明。

标准的状态可由不同的缩写来表示：

- “EN”前缀表示整个欧盟均承认并实施该标准。
- “prEN”前缀表示该标准正处于筹备阶段。
- “HD”前缀与 EN 标准类似，但在个别国家需要进行调整（协调文件）。
- “TS”前缀表示为技术规范文件，可作为预备标准使用。文档命名格式为 CLC/TS 或 CEN/TS。
- “TR”前缀表示该文件是当前技术发展水平的研究报告。

欧洲协和标准的产生程序如下：

1. 欧盟委员会作为欧盟的执行机构，向 CEN 或 CENELEC 发布授权，让它们筹备一个欧洲标准，以详尽、具体的阐述某一标准。
2. 筹备工作逐渐由国际论坛承担，在论坛中对满足指令中必备安全要求的技术规范进行定义。
3. 一旦该标准投票通过，就会在欧盟官方刊物上发布。自此起，将成为欧洲协和标准，并且支持相关指令。

- 协和欧洲标准可以用作参考，也可替换同一技术领域的所有国家标准。
- 与安全部件或机器的协和标准一致，即等同于与假定遵循指令（例如《机械指令》）中的“主要健康与安全要求”一致（假定一致性）。

➜ 标准化概述 http://www.normapme.com/
➜ 假定一致性指令标准列表 http://ec.europa.eu/enterprise/newapproach/standardization/harmstds/reflist.html

不同类型标准

总计三种不同类型标准：

A 类标准

（基本安全标准）包含基本术语、设计原则和适用于所有机器的通用内容。

B 类标准

（分组安全标准）定义了适用于广义机器的安全应用或安全设备。B 类标准又可分为：

- B1 类标准，适用于特定安全应用（如机械的电气安全、安全距离的计算、控制系统的要求等）
- B2 类标准，适用于防护设备（如双手控制设备、物理防护设备和电感式防护设备等）

C 类标准

C 类标准包含特定机械或某一类机械的所有安全要求。如果有 C 类标准，那么它比 A 类或 B 类标准具有更高的优先级。尽管如此，C 类标准仍须参考 B 类或 A 类标准。在任何情况下，都应该遵循《机械指令》要求。

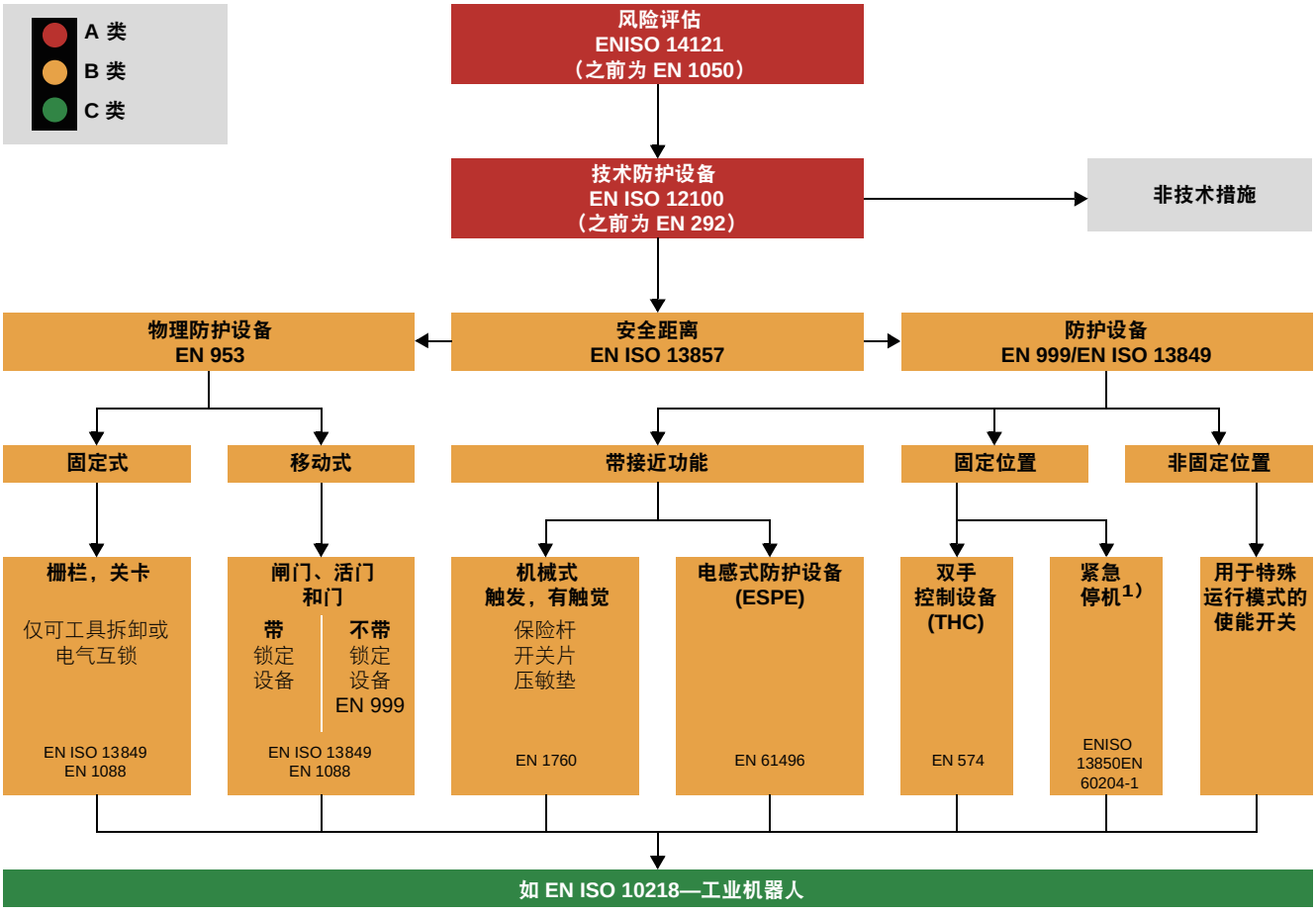
现在许多 A 类和 B 类以及重要的 C 类标准都在进行修订。这将建立新的 ENISO 标准系列编号系统。但是，由于通常标准会有一段时间的过渡期，新标准的实际施行时间仅有 5 到 6 年。

➜ 可在第 i-5 页“相关标准概述”一节附录中找到重要标准列表。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

§

防护设备和相关标准的可能选择



1）紧急停机是一种安全措施，但不是一种防护设备！

- 不管是不是协和标准，其应用都不由《机械指令》规定。然而，协和标准的应用证明了机械能够满足《机械指令》的要求（所谓的“假定一致性”）。
- 如果有针对某一类 3 个标准具有比其他 A 类和 B 类标准以及该指南中任何信息更高的优先级。此时，只有 C 类标准可验证相关指令的假定一致性。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

§

提供安全建议的机构

机构

提供安全建议的机构

企业想要知道它们的机械是否符合适用的欧洲指令和标准，那么它们可以从诸如 HSE 和 DTI 等公司获取相关的安全建议。

认证机构

认证机构负责对测试程序和测试条件进行检验，以验证其是否合乎一致性。这些机构包括法定事故保险和预防机构，这些机构通常超强的专家团队。

公告机构

根据《机械指令》规定，欧共体每一成员国都有义务至少提名几家公告机构，并告知布鲁塞尔欧共体总部，以便将其添加至机构列表。

只有这些机构是获得实施 EC 类检测授权，或为指令附录 IV 中所列出的机械和安全部件颁发 EC 类检测证书。并非每一家公告机构都有权测试所有类型的产品或机械。许多机构仅具有特定领域的相关资质。

保险商

Berufsgenossenschaften（专业协会）

在德国，Berufsgenossenschaften 和其他组织承担了法定事故保险责任。Berufsgenossenschaften 按行业组织，可更好地满足各个经济领域的具体要求。

保险公司

许多保险公司都提供专家建议（尤其是规避应疏忽或失误造成的责任风险，以及避免违法行为的建议）的部门。

市场监管机构

在欧盟和欧洲自由贸易区国家，工作安全和市场监管是官方机构的责任。这些任务是由以下部门执行的：

- 在英国，由称为 Health and Safety Executive（健康与安全署）的国家行政机关执行，
- 在芬兰，由 Sosiaali- ja terveysministeriön alaisena toimivat työsuojelupiirien työsuojelutoimistot 执行，
- 在荷兰，由 de Arbeidsinspectie 执行，
- 在比利时，由 Federale Overheidsdienst (FOD) werkgelegenheid, arbeid en sociaal overleg — Service public fédéral (SPF) emploi, travail et concertation sociale执行。

➜ 你可以在第 i8 页“相关链接”一节附录中找到重要的地址。

总结：法律、指令和标准

作为机械制造商，除须遵循其他要求外，也应遵循《机械指令》；因此，您应该：

- 遵循《机械指令》中“主要健康与安全要求”。
- 在设计过程中尽早规划整体安全性。
- 使用标准程序或者《机械指令》附录 IV 所列机械程序，以获得一致性声明。
- 编写机械技术性文档，尤其安全相关的所有设计文档。
- 随产品提供机器所用国家官方语言版的操作指南。同时提供原始语言操作指南。
- 完成一致性声明，并在机器和安全部件上标记 CE 标志。

作为机器的操作者，用户同样需要遵循工作设备指令；因此用户应当：

- 遵循工作设备指令要求。
- 查询是否有其他国家要求（例如工作设备测试、检修和维护间隔等等），并严格遵守。

标准

- 技术标准对欧洲指令标准的对象进行了详细具体的规定。应用协和标准可验证所谓的“假定一致”，即假定机器
- 符合指令要求。举例来说，如果你为你的机械或系统选择并使用了正确的标准，你就可以假设你将满足所有的法律要求。

共有 A 类标准（基本安全标准）、B 类标准（分组安全标
- 准）和 C 类标准（机械安全相关标准）三种不同类型标准。若存在 C 类标准，那么它比 A 类或 B 类标准具有更高优先级。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

第一步：风险评估

在设计一台机器时，应尽可能对其潜在的风险进行分析，必要时还应采取额外的防护措施，以确保操作人员不受任何潜在危害的影响。

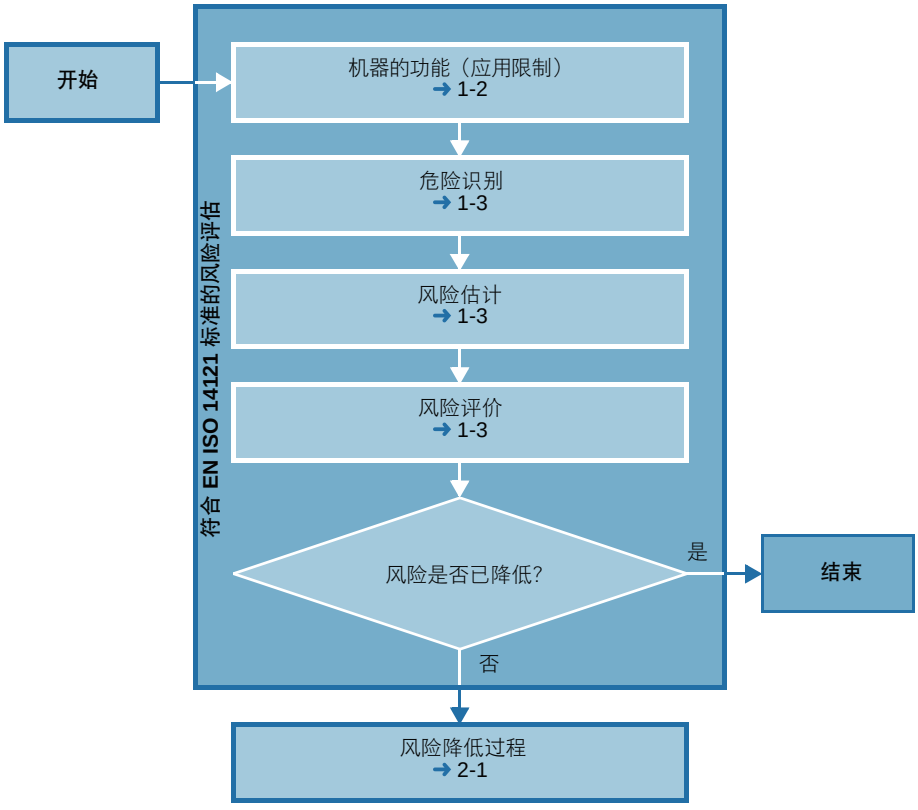
我们定义了一系列标准帮助机器制造商进行风险评估，这些标准由不同的系统性风险分析和评估的逻辑步骤组成。机器的设计和制造应该考虑风险评估的结果。

如有必要，应该在风险评估之后采取适当的防护措施以降低风险。并且采用防护措施后不应造成新的风险。包括风险评估和风险降低在内的整个过程可能需要重复数次，以最大限度地消除危险，并有效地降低所鉴别出的风险。

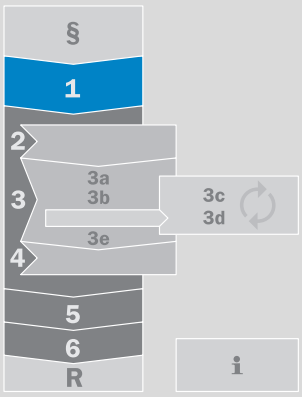
一般 C 类标准只适用于特定的机器或应用。如果没有合适的 C 类标准或者 C 类标准不能满足要求时，可以采用 A 类或 B 类标准。

→ 风险评估 — A类标准：EN ISO 14121
→ 降低风险 — A类标准：EN ISO 12100-1，EN ISO 12100-2

风险评估过程



- 应针对所有的风险重复执行此过程（反复过程），直至剩余风险降低至可接受范围内。
- 风险评估的过程及成果都须归档。



1

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

机器的功能（应用限制）

风险评估从机器功能的定义开始。机器的功能包括：

- 机器的产品规格（产品是什么、最大生产性能如何、使用的原材料等）
- 物理限制及应用范围
- 计划的使用寿命
- 预设功能和工作模式
- 可能出现的故障
- 机器操作涉及到的相关人员
- 与机器相关的产品
- 机器的正确使用、操作员的意外操作以及合理的可预见的误操作

可预见的误操作

理论上存在的操作员意外操作以及可预见的误操作包括：

- 操作员失去对机器（尤其是在手持式或便携式机器）的控制
- 机器使用过程中出现失灵、故障或失效事件时个人的反射行为
- 由于注意力不集中或粗心大意造成的错误操作
- 在执行任务期间由于寻求“捷径”而采用的错误操作
- 压力状态下为了确保机器正常运行所采取的操作
- 特定人群（如儿童、年轻人、残疾人等等）的操作

可能出现的故障

当与功能性相关的部件（尤其是控制系统）出现失灵或故障时，极有可能产生危险。例如：

- 滚筒的回转运动（可能将手卷入）
- 机器人在其正常工作区域以外的运动

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

危险识别

完成机器功能定义后，接下来就是风险评估的最重要步骤 — 危险识别。

该步骤包括对可预见的危险、危险情况和/或危险事件的系统化识别。

机器制造商应该尤其注意以下危险...	...在机器使用寿命的所有阶段。
■ 机械危险 ■ 电气危险 ■ 热危险 ■ 噪音危险 ■ 振动危险 ■ 放射性危险 ■ 原材料危险 ■ 由于机器设计忽略了人体工程学原理而造成的危险 ■ 由于打滑、磕绊和坠落引起的危险 ■ 与机器使用环境相关的危险 ■ 由上述危险原因组合带来的危险	■ 运输、装配和安装阶段 ■ 调试阶段 ■ 设置阶段 ■ 正常运行和故障检修阶段 ■ 维修和清洗阶段 ■ 退役、拆卸和废物处理阶段

风险估计和风险评价

完成危险识别后，应针对每一种危险情况进行**风险估计**。

风险 = **损害程度** × **发生概率**

与危险情况相关的风险取决于下列因素：

- 危险可能造成的损害程度（轻度损害、严重损害等等），以及
- 发生这种损害的概率。主要体现为：
  - 处于危险的人/人们
  - 危险事件的发生，以及
  - 技术上人为防止或限制损害的可能性

可采用多种工具进行风险估计，例如表格、风险图、统计方法等等。

在**风险评价**阶段，需要基于风险估计的结果来确定是否需要采取防护措施，以及何时实现降低风险。

➜ 工具和表格：技术报告 — ISO/TR 14121-2

归档

风险评估归档应包括所采用的步骤、获得的成果以及下列信息：

- 关于机器产品规格、限制、正确使用等的信息
- 负载、强度和安全系数等方面的重要假设
- 所有识别出的危险和危险情况以及考虑到的危险事件
- 采用的数据和数据源以及类似机器上与风险降低相关的记录和经验
- 所采取防护措施的相关说明
- 对采取这些防护措施所要达到的风险降低目的的相关说明
- 与机器相关的剩余风险
- 风险评估期间准备的所有文档资料

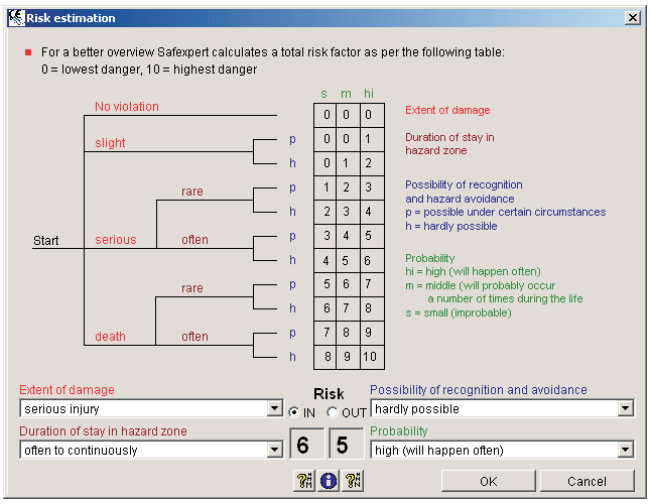
机械指令不要求交付机器时附带风险评估的文档！

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

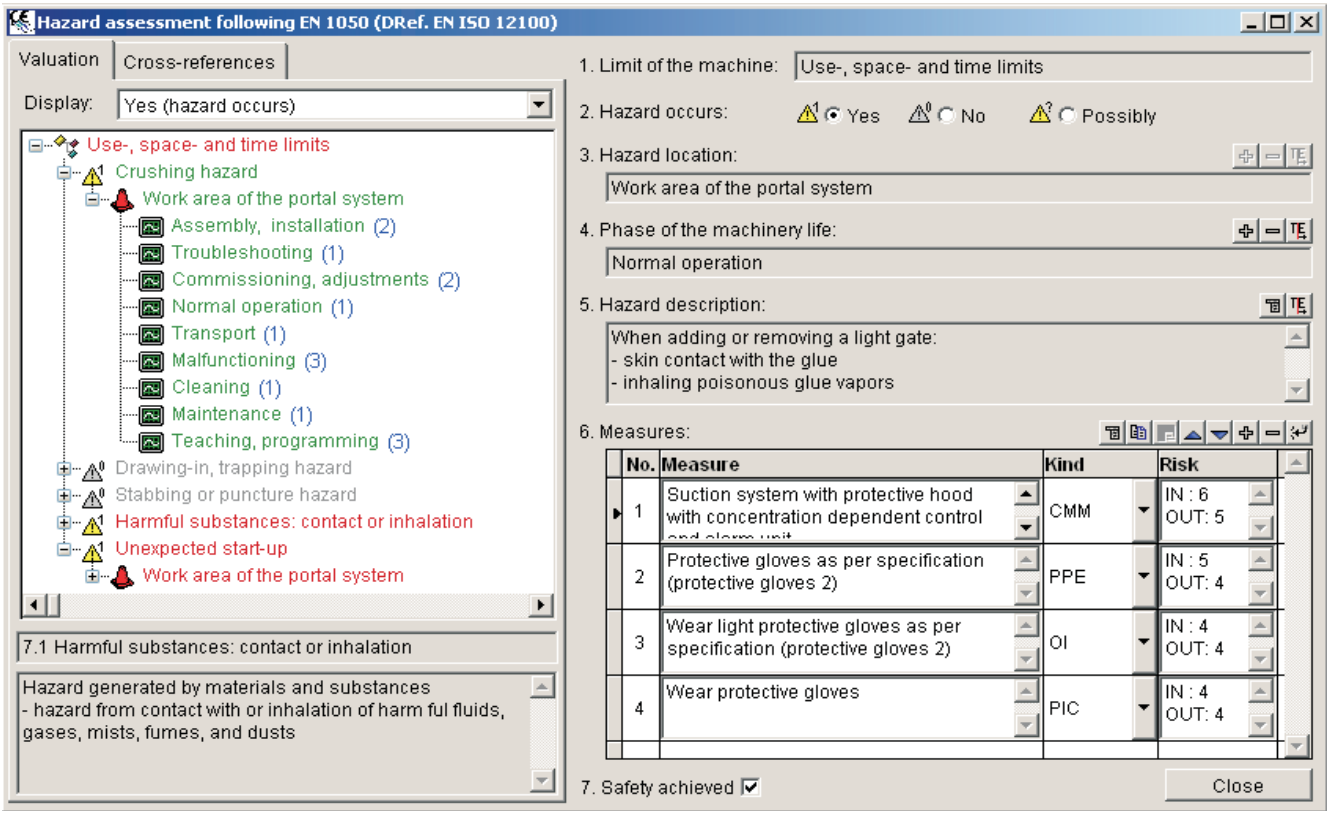
1

使用 Safexpert 进行风险评估

风险评估的过程在 Safexpert® 中进行，它是一个用于安全工程的软件包。在该软件中，风险评估任务被简化为几个部分：危险清单、风险评估树形选择结构、风险评估方案以及控制系统所需的安全等级。用户可以在软件中查看法律要求和标准要求。主要标准都会根据标准管理特性及时更新。评估将会在适当的机器寿命阶段针对所有的危险点一一进行。基于对单个危险的评价将有助于选出最优的风险降低措施。Safexpert 组合使用了风险图和矩阵（表格）。在防护措施（例如防护设备）采用之前 (IN) 和之后 (OUT) 都会进行风险估计，且风险按 0（无风险）到 10（最高风险）的分类标准进行归类。



Safexpert 不仅可以用于风险评估，还可以按照机械指令有效地执行和归档整个评估过程。



➜ 登录网址 http://www.sick.com/safexpert/ 查看 Safexpert 的演示版。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

总结：风险评估

概述

- 对所有危险进行风险评估。这个过程应该考虑到所有的危险和风险，并且需反复执行直至没有任何剩余风险或剩余风险在可接受范围内。

风险评估过程

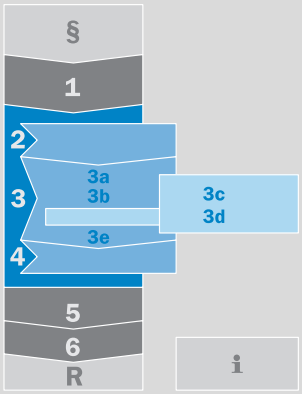
- 风险评估从机器功能的定义开始。
- 在风险评估期间尤其要考虑可预见的误操作和故障。
- 然后对机器的危险进行识别（机械危险、电气危险、热危险等等），并考虑机器在其所有寿命阶段的这些危险。
- 然后估计由这些危险造成的风险。这些都依赖于损害程度和损害发生的概率。
- 对风险评估结果进行归档。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

第 2 步到第 4 步：降低风险

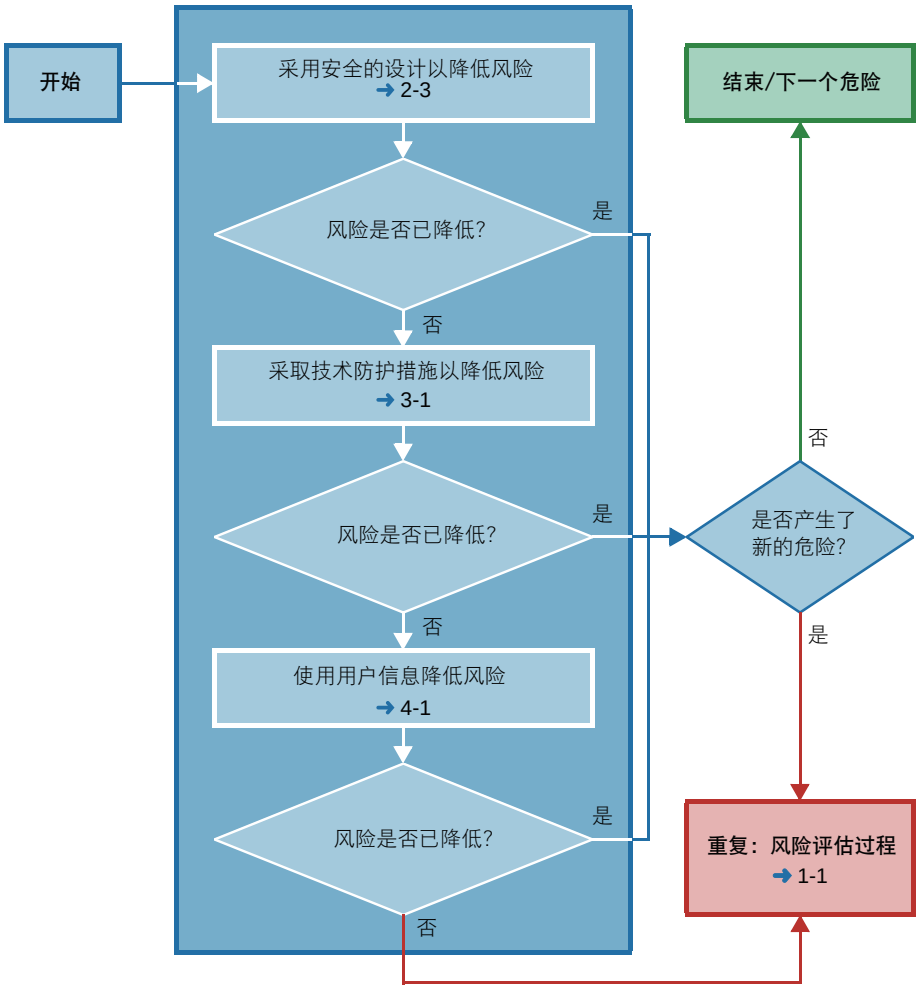
如果风险评价显示需要采取必要措施以降低风险，那么应该采用 3 步法。



3 步法

防护措施的选择应遵循以下准则（并按指定顺序进行）：

1. 安全的设计：应尽可能地消除或最小化剩余风险（在机器设计和制造中集成安全性）
2. 技术防护措施：采取必需的防护措施以降低设计所无法消除的风险
3. 关于剩余风险的用户信息



➜ 风险降低过程的基本原则：EN ISO 12100-1，-2（A 类标准）

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

第 2 步：安全设计（本质安全的设计）

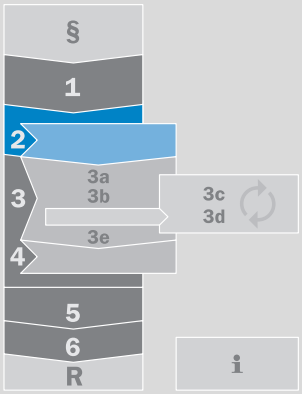
安全设计是降低风险过程的第一步，也是最重要的一步。在此过程中，需要通过设计排除可能的危险。从这个角度来说，安全设计也是（降低风险）最有效的手段。

安全设计因素包括机器本身的设计以及处于危险时人与机器间的相互影响。例如：

- 机械设计
- 操作和维修原则
- 电气设备（电气安全，EMC）
- 紧急停机原则
- 涉及流体的设备
- 使用过的原材料和润滑液
- 机器功能和生产过程

在任何情况下，所有部件的选择、使用和改造都必须保证在出现机器故障时，人们的安全是首要的。同时应该注意防止损坏机器或破坏环境。

必须对机器的各种元件进行规范，以使它们在相应的限制范围内执行各自的职能。设计应尽可能地简单化，同时与安全相关的功能也应尽可能地与其他功能隔离开。



2

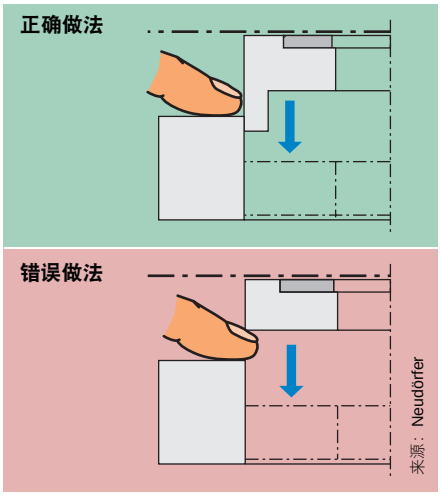
机械设计

安全设计的首要原则是在最基本的机械设计层面防止危险的发生。可以通过以下方法实现该目标：

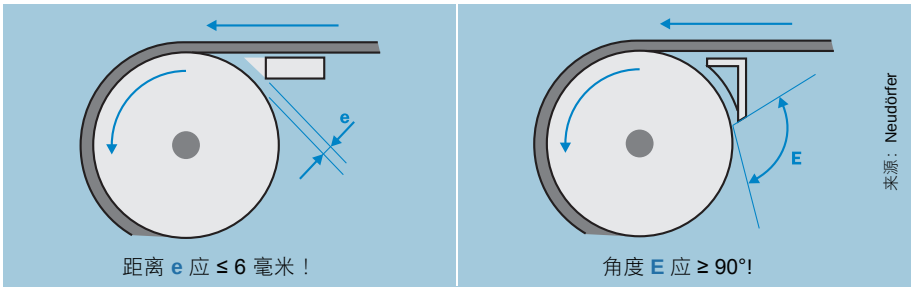
- 避免尖锐的边、角和突出部分
- 避免破碎点、剪切点和缠结点
- 限制动能（质量和速度）
- 考虑人体工程学原理

大多时候常识即能有所帮助，但需要时我们建议您查阅相关资料。

示例：避免剪切点



示例：避免缠结点



距离 e 应 ≤ 6 毫米！　　角度 E 应 ≥ 90°!

➜ “安全机器的设计”（英文版），计划 2010 年出版：ISBN 978-3-540-35791-9

本章主要内容	页码
➜ 机械设计	2-3
➜ 操作和维修理念	2-4
➜ 电气设备	2-4
➜ 关机	2-8
➜ 电磁兼容 (EMC)	2-9
➜ 流体技术	2-10
➜ 在潜在爆炸性环境中使用	2-11
➜ 总结	2-12

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

操作和维修原则

应尽可能减少在危险区域操作的需要。可通过以下各种方法实现这一目标：

- 自动装载和卸载站
- 在“外面”进行设置和维修工作
- 使用可靠和可用的部件以避免维修工作
- 清晰和明确的操作理念，例如控件的清晰标记

彩色标记

按钮上的控件、指示器和监视器上显示的信息会以各种颜色进行标记。不同的颜色具有不同的含义。

➜ 机器中的电气设备标准：EN 60204-1

控件颜色的一般含义

颜色	含义	说明
白色 灰色 黑色	不确定	功能的启动
绿色	安全	安全操作期间或建立正常运行环境时激活
红色	紧急	危险或紧急情况下激活
蓝色	命令	在需要执行强制动作的情况下激活
黄色	异常	在异常情况下激活

指示器颜色的一般含义

颜色	含义	说明
白色	不确定	在不确定使用绿色、红色、蓝色或黄色的情况下使用
绿色	正常情况	
红色	紧急	危险状态，应立即采取行动
蓝色	强制	需要操作员进行强制动作的情况
黄色	异常	异常情况，即将发生危急情况

电气设备

必须采取必要措施排除机器上的电气隐患。在这里需要区分两种不同类型的危险：

- 由电能导致的危险，例如，直接或间接物理接触导致的危险
- 由控制系统故障间接导致的危险

➜ 以下各小节将介绍有关电气设备设计的重要信息。
➜ 机器中的电气设备标准：EN 60204-1
➜ 低压指令2006/95 EC

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

电源连接

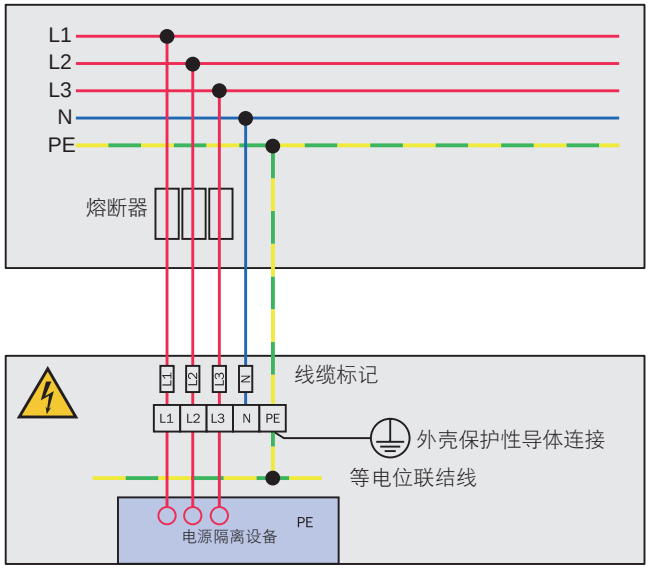
电源连接是机器中的电气设备与电网之间的接口。接线时应该遵守相关设施的规定。在与安全相关的应用中稳定的电源供应是尤为重要的。因此电源电压应该具有承受短暂电网故障的能力。

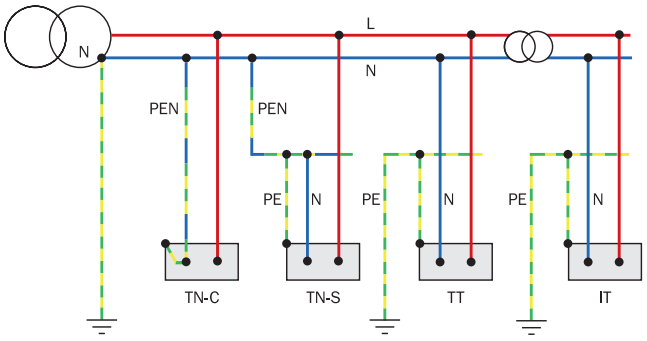
接地系统

接地系统包括两种类型，一种为电源变压器二次侧接地，一种为电气设备机箱接地。国际上有三种标准的接地系统：

- TN 系统
- TT 系统
- IT 系统

接地指的是通向大地的导电连接。接地有保护地 PE 和功能地 FE 之分，其中保护地与电气安全相关，功能地则用于其它目的。保护性导电系统包括接地电极、连接电缆和相关的端子。连接到电网上的所有电气设备的机箱应该等电位地连接到保护性导体系统。等电位联结是一种基本的故障预防措施。





TN 系统

TN 系统是低压系统中最常用的一种网络结构。在 TN 系统中，变压器的星形点是直接接地的（系统地）；所连接设备的机箱通过保护性接地导体 (PE) 连接到变压器的星形点。

根据所铺设线缆的截面积不同，PE 和 N 电缆可以作为一条公共电缆（TN-C 系统）或者两根单独电缆（TN-S 系统）进行布线。

TT 系统

在 TT 系统中电源变压器的星形点的接地方式与在 TN 系统中相同。而连接到导电设备外壳的保护性接地导体则不连接到这个星形点，而是单独接地。设备机箱使用一个公共保护地电极接地。

TT 系统通常只用于采用剩余电流断路器的连接中。

TT 系统的优点在于在偏远地区使用时具有更高的可靠性。

IT 系统

IT 系统中的导电设备外壳的接地方式与在 TT 系统中相同，但是电源变压器的星形点并不以同样的方式接地。对于关闭时存在一定危险，因此在机箱或接地故障时不能关闭的系统，它们通常被设计为 IT 系统。在低压区域中，例如为运营中的剧院和医院中的重点监护室供电时，IT 系统是规定使用的。

➜ 防护措施：HD 60364-4-41（IEC 60364-4-41，各国有不同的修正案）

电源隔离设备

应该为连接至一台或多台机器的每一个电源连接提供电源隔离设备，以将电气设备与电网电源隔离开：

- 用于使用类别 AC-23B 或 DC-23B 的电源断路器
- 带辅助触点的隔离开关，用于容性负载卸载
- 电路断路器
- 16A/3kW 的插头/插座组合

某些电路（如用于互锁的控制电路等）不需要通过隔离设备进行关闭。在这种情况下需特别注意操作的安全性。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

防止意外启动的关机设备

在维修工作期间，机器启动或电力恢复不得对维修人员造成危险！因此需要采取措施以防止意外或错误地关闭电源隔离设备。当电源开关处于关闭位置时在其手柄上装配一个挂锁可以实现这个目的。

由于某些与操作相关的原因，此关机设备不适于用作危险区域内进行简便干预的防护措施。

防止电击

防护等级

防护等级的划分是基于单故障安全性的实现方式进行的，它本身并不代表具有相应等级的防护水平。

防护等级 I

所有具备简单绝缘（基本绝缘）和保护性导电连接的设备都属于防护等级 I。保护性接地导体应该连接到一个标记有接地符号的端子或 PE，并且其颜色应该为绿-黄相间。

防护等级 II

属于防护等级 II 的设备具有增强的绝缘或双重绝缘，并且没有用于保护性接地导体的连接。这种防护措施也被称为保护性绝缘。保护性接地导体是不允许使用的。

防护等级 III

属于防护等级 III 的设备运行于安全特低电压下，因此不需要任何显性的防护措施。

安全特低电压 SELV/PELV

允许将 50 伏（有效值）以下的交流电压和 120 伏以下的直流电压作为安全特低电压。直流电压超过 75 伏时仍然满足低压指令的要求。

在正常干燥的地方使用时，如果交流电压的有效值不超过 25 伏或者不含谐波的直流电压不超过 60 伏，那么没有必要针对直接的物理接触提供防护措施（基本保护）。通过在直流电压上叠加一个大约 10% 有效值的正弦交流部分，可以获得没有谐波的电压。

安全特低电压电路应该与其他电路（足够的空气和爬电距离、绝缘、电路到保护性接地导体的连接等等）安全地隔离开。应该区别以下两者：

- SELV（安全特低电压）
- PELV（保护特低电压）

不允许电源使用自耦变压器、分压器或串联电阻来获取安全特低电压。

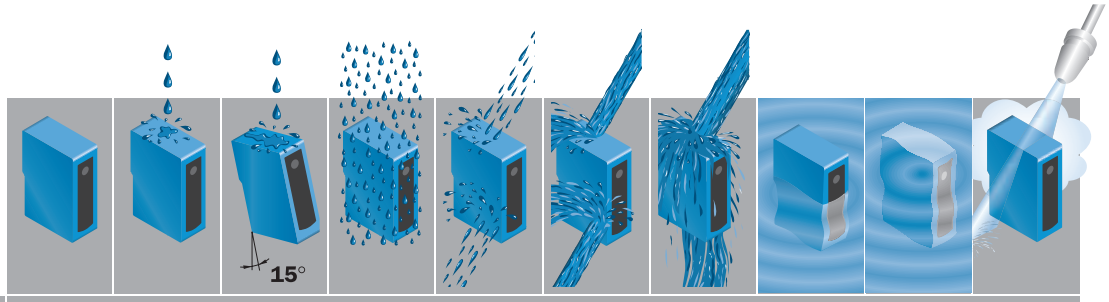
名称	隔离类型		与地或保护性接地导体之间的关系	
	电源	电路	电路	外壳
SELV	带安全隔离的电源，例如安全变压器或等效电源	带安全隔离的电路	未接地电路	外壳不应有意接地，并且也不能连接到一个保护性接地导体
PELV			接地电路	外壳允许接地，或连接到一个保护性接地导体

➜ 防护等级标准：EN 50178
➜ 变压器的安全性标准：EN 61588 系列

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

防护措施/外壳防护等级

外壳防护等级描述的是设备针对水（不是水蒸汽）和异物（灰尘）的防护能力。此外，它还能表示对与带电部件直接物理接触的防护能力。对设备来说，防护能力总是必需的，在低压应用中也不例外。所有与电源隔离后仍然带电的部件都应至少设计为 IP 2x 的外壳防护等级，而开关柜的外壳防护等级则至少应为 IP 54。



第一位数字： 针对异物的防护	**第二位数字：** 针对水（不是水蒸汽，也不是其他液体！）的防护									
	IP ...0	**IP ...1**	**IP ...2**	**IP ...3**	**IP ...4**	**IP ...5**	**IP ...6**	**IP ...7**	**IP ...8**	**IP ...9K**
	无防护	滴水 垂直方向	滴水 成一定角度	淋水	溅水	喷水	强力喷水	浸水 暂时的	浸水 永久性的	100 bar, 16 l/min., 80 °C
IP 0... 无防护	IP 00									
IP 1... 异物直径 ≥ 50 mm	IP 10	IP 11	IP 12							
IP 2... 异物直径 ≥ 12 mm	IP 20	IP 21	IP 22	IP 23						
IP 3... 异物直径 ≥ 2.5 mm	IP 30	IP 31	IP 32	IP 33	IP 34					
IP 4... 异物直径 ≥ 1 mm	IP 40	IP 41	IP 42	IP 43	IP 44					
IP 5... 防尘的	IP 50			IP 53	IP 54	IP 55	IP 56			
IP 6... 绝尘的	IP 60					IP 65	IP 66	IP 67		IP 69K

➜ 外壳防护等级标准：EN 60529EN 60529

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

关机

除了正常运行时需要关机外，出于安全考虑时还应能够进行紧急停机。

要求

- 每台机器都应配备一个用于正常关机的控制设备。
- 机器最起码应具备 0 类停机功能。如果出于机器安全考虑或有相关功能需求时，则可能需要具备 1 类和/或 2 类停机功能。
- 关机指令应该比控制机器运行的指令具有更高的优先级。如果机器或其危险部件已经被关闭，则应中止对驱动系统的供电。

停机功能分类

机器安全以及相关功能的不同决定了停机功能也有不同的类别。不要将停机功能分类与 EN 954-1 和 EN ISO 13849-1 标准中的分类相混淆。

0 类停机功能	驱动部分的电源已经被隔离开（非控制型关机）
1 类停机功能	机器处于安全状态，仅在此时才将驱动部分的电源隔离开
2 类停机功能	机器处于安全状态，但电源并没有被隔离开

2

➜ 机器中的电气设备标准：EN 60204-1

紧急情况下的操作

紧急停机（紧急情况下的关机）

出现紧急情况时，不仅需要停止所有危险运动，还应该释放所有可能产生危险的能量源（例如储存的能量）。该操作被称为紧急停机。每台机器（机械指令中说明的例外情况除外）都应至少配备一个紧急停机设备。

- 紧急停机设备应该易于够到。
- 紧急停机设备应该能够尽快地终止某种危险状态，且不造成额外风险。
- 紧急停机指令应该比所有运行模式下的其他功能和指令具有更高的优先级。
- 紧急停机设备的复位不应触发重启动作。
- 应该采用带机械闭锁功能的直接动作原理。
- 紧急停机应该按照 0 类或 1 类停机功能进行。

紧急断电

如果可能出现由电能引起的危险或损害，则设备需具备紧急断电功能。紧急断电时电源是通过机电开关设备关闭的。

- 仅当所有的紧急断电指令都已复位时，才能开启电源。
- 因此，紧急断电属于 0 类停机功能。

复位

如果用于紧急情况的设备进行了某项操作，那么由此操作触发的设备应该维持在关机状态，直到用于紧急情况的设备被复位为止。

控制开关的复位应该在特定的位置手动进行。复位后机器重新开始运行。

紧急停机和紧急断电只是额外的防护措施，而不是用于降低与机械危险相关的风险的措施。

实施的要求和形式

所使用的控制开关的触点应该是强制断开的常闭触点。控制设备应该是红色的，所有背景都应该是黄色的。允许使用：

- 由圆头按钮启动的开关
- 由线缆、绳索或横杆启动的开关
- 不带盖子的脚动开关（用于紧急停机）
- 电源隔离设备

如果使用线缆和绳索作为急停设备的启动部件，那么在设计时应该保证它们易于启动和触发紧急停机功能。安置复位装置时必须确保从其所处位置能够看到线缆或绳索的全部长度。

➜ 紧急停机设备的设计原理：EN ISO 13850
➜ 紧急情况下的关机：机械指令 2006/42/EC

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

电磁兼容 (EMC)

欧洲 EMC 指令将电磁兼容定义为“某个设备、设备中的功能单元或系统在其电磁环境中能够正常工作，同时不会对其环境中其他设备产生不可忍受的电磁干扰的能力。”

在选择机器或部件时，必须确保其不受电磁干扰的影响。安全部件在这方面具有更高的要求。

电磁干扰可能由以下原因引起：

- 快速瞬变的电气干扰（脉冲群）
- 浪涌电压，例如电网受到闪电电击时引起的浪涌电压
- 电磁场
- 高频干扰（临近电缆）
- 静电放电 (ESD)

对于工业领域和住宅区有不同的干扰限制。在工业领域中对电磁敏感性的要求更高，但是也允许更高的干扰发射水平。因此满足工业领域射频干扰要求的部件在住宅区使用时可能会导致射频干扰。下表列出了不同应用领域中最小干扰场强的示例。

在 900 到 2000 MHz 频率范围内的典型最小干扰场强

应用领域	抗干扰的最小干扰场强
娱乐电子	3 V/m
家用电器	3 V/m
信息技术设备	3 V/m
医疗设备	3…30 V/m
工业电子	10 V/m
安全部件	10…30 V/m
汽车电子	100V/m 以下

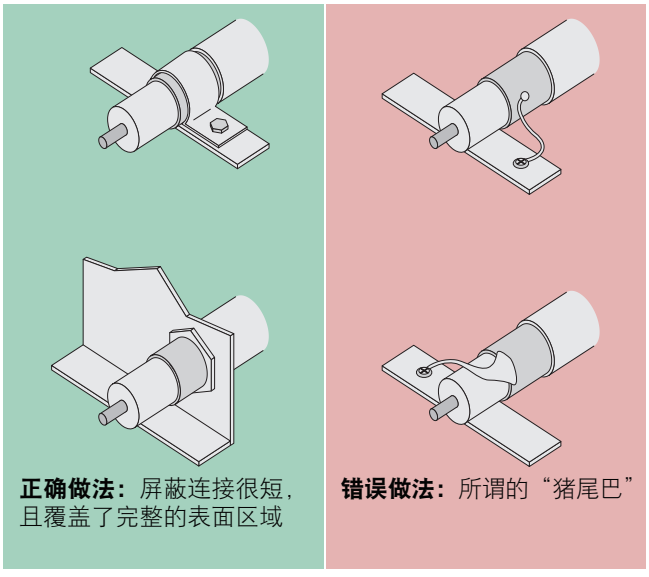
示例：不同场强下移动电话系统的典型距离

应用领域	3 V/m	10 V/m	100 V/m	说明
DECT 基站	大约 1.5 m	大约 0.4 m	≤ 1 cm	基站或手持设备
GSM 手机	大约 3 m	大约 1 m	≤ 1 cm	最大传输功率 (900MHz)
GSM 基站	大约 1.5 m	大约 1.5 m	大约 1.5 m	传输功率大约为 10 W

遵循以下设计准则有助于防止电磁兼容问题：

- 通过机器和系统的不同部件间的导电连接实现连续的等电位联结
- 与电源单元（电源/致动器系统/逆变器）之间进行物理隔离
- 不要使用屏蔽物来承载等电位联结电流
- 使用短的屏蔽物，并覆盖完整的表面区域。
- 连接所有的功能地 (FE)。
- 小心连接已有的通信电缆。通常需要使用绞合电缆传输数据（现场总线）。

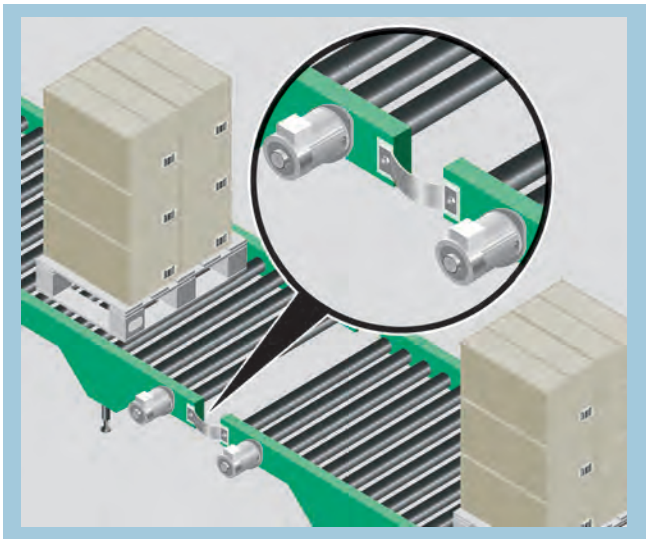
示例：正确连接屏蔽物



正确做法：屏蔽连接很短，且覆盖了完整的表面区域

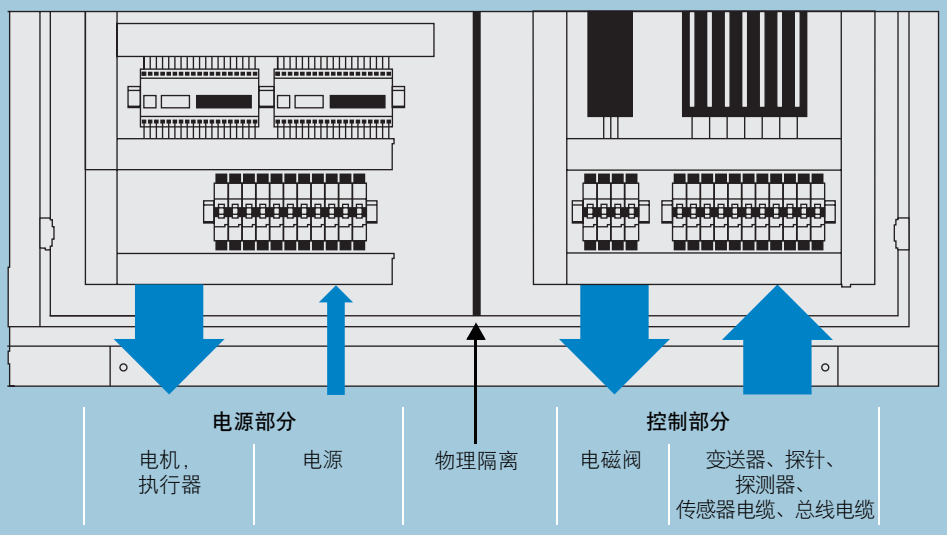
错误做法：所谓的“猪尾巴”

示例：等电位联结



© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

示例：物理隔离



➜ EMC 标准：EN 61000-1 到 EN 61000-1-4
➜ 安全部件的 EMC 标准：EN 61496-1，EN 62061

流体技术

流体技术是使用气体或液体来传输能量的所有过程的总称。因为液体和气体的行为比较相似，所以使用“流体”这一更高级别的称呼。流体技术描述的是在密封管道系统中使用流体传输能量的过程和系统。

流体技术在工程上分为液动（使用液压油传输能量）和气动（使用压缩空气传输能量）两种应用。基于油的液动系统需要一个用于流体（进给和返回）的电路，而气动系统中的废气通过声音衰减器排放到环境中。

子系统

每个与流体相关的系统都由以下子系统组成：

- 压缩：压缩机/泵
- 调节：过滤器
- 抽吸（泵作用）：管道/软管
- 控制：阀门
- 驱动：汽缸

在任何与流体相关的系统中，都是针对负载对流体进行抽吸以产生压力。当负载增加时，压力也会增加。

设计准则

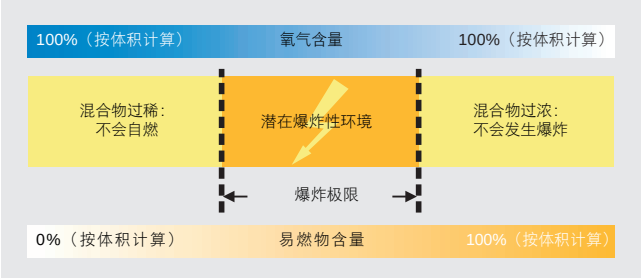
与流体相关的系统中的所有部件都必须针对子系统的最大运行压力或某一个元件的额定压力值被超出的情形采取防护措施。应避免由部件内或管道/软管内的流体泄露导致的危险。应该使用声音衰减器来降低排放空气时产生的噪声。声音衰减器的使用不应额外引发其他危险，并且不能导致任何损害性的回压。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

在潜在爆炸性环境中使用

防爆是一项与安全密切相关的特殊任务。在爆炸事件中人们会面临各种各样的危险，这些危险可能是由不受控制的热辐射、火焰、压力波以及飞溅的残骸造成的，也可能是由危害性的反应产物造成的，也可能是由人类呼吸所必需的氧气耗尽造成的。爆炸和火灾并不属于工业事故中最常见的起因，但它们的后果异常惊人，常常会造成严重的人员伤亡和巨大的经济损失。

在生产、运输、加工或储存粉尘、易燃气体或液体的地方，很可能会形成一个潜在爆炸性环境，例如处于爆炸极限内的燃料与大气中氧气的混合物等。当存在火源时，爆炸就有可能发生。



评估所需防护措施的范围

为了评估所需防护措施的范围，可以根据产生潜在爆炸性环境的概率，将具有爆炸危险的地方划分为不同的区域。下表中列出的信息并不适用于采矿应用（露天矿，地下矿）

区域的定义				
气体	G	2 区	1 区	0 区
粉尘	D	22 区	21 区	20 区
潜在爆炸性环境		少见，持续时间短	偶尔	连续的，频繁的，持续时间长
安全措施		普通	高级	超高级
可以使用的设备类别 (ATEX)				
1		II 1G/II 1D		
2		II 2G/II 2D		
3		II 3G/II 3D		

标记

应该针对在这些区域的使用对设备进行设计、测试并进行相应的标记。

⟨Ex⟩	II	2G	EEx ia	IIC	T4	示例：根据 ATEX 对⟨Ex⟩设备进行标记
						温度等级 可用于 >135°C 的点燃温度中
						爆炸类别 乙炔、二硫化碳、氢气
						防护准则 i = 本质安全 a = 两次失效安全
						设备类别 (ATEX) 可用于 1 区
						设备类别 不能用于有甲烷的地方
						防爆标志

➜ 1994/9/EC 指令（ATEX 95 — 制造商）
➜ ATEX 标准：EN 50021（气体）和 EN 50281（粉尘）

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

总结：安全的设计

机械、电气、运行

- 遵循不在第一时间发生危险的设计准则。
- 设计时应考虑让操作员尽可能少的暴露在危险区域。
- 避免直接由电能导致的危险（直接或间接的接触）或间接由控制系统故障导致的危险。

紧急情况下的操作，关机

- 设计一个用于正常关机的控制设备。
- 使用紧急停机设备中断危险的过程或危险的运动。
- 如果需要安全隔离可能产生危险的电源，那么应该使用紧急断电功能。

EMC

- 机器的设计应遵循 EMC 指令。选择部件时须保证以下几点：
  - 它们不会对其他设备或系统造成电磁干扰。
  - 它们本身具有抗电磁干扰能力。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

第 3 步：技术防护措施

技术防护措施可以通过采用安全防护设备（挡板、门、光幕、双手控制设备）或监控设备（监控位置、速度等）来实现。

机器的控制系统并不会集成有所有的防护设备，固定的物理防护装置（栅栏、盖子等）就是一个例子。只需正确设计这些防护设备即可完成主要任务。

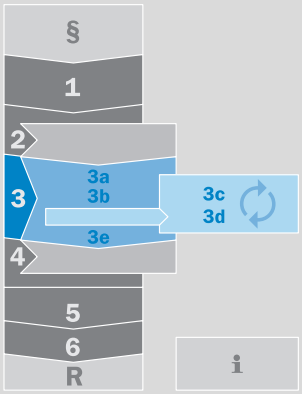
功能安全

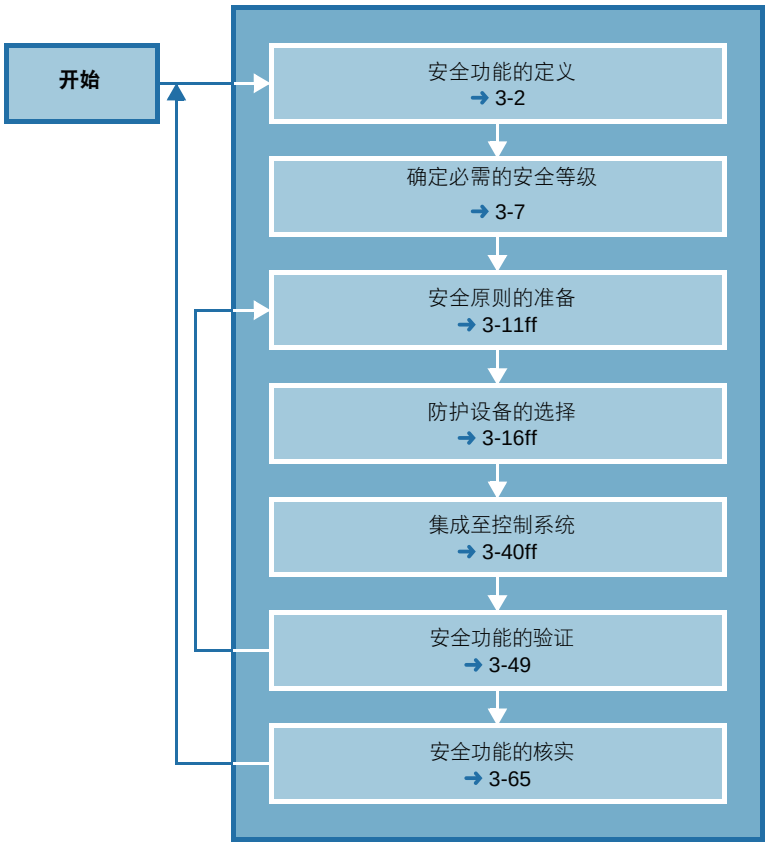
当防护措施的效果取决于某个控制系统正确功能的实现时，我们就需要引入“功能安全”这一概念了。必须首先定义安全功能以及必需的安全等级，然后才能采用恰当的部件来实现功能安全，最后还须进一步进行核实。

核实

对所有技术防护措施进行核实能够确保正确的安全功能具有可靠的效果。

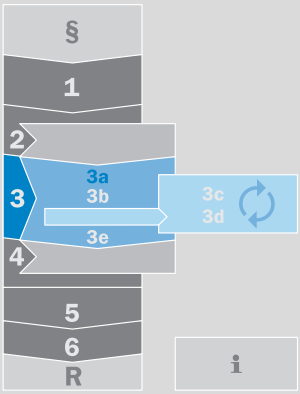
下一章（子步骤 3a 到 3e）将介绍安全功能的设计以及它们在控制系统中的实现方法。





3

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。



3 a

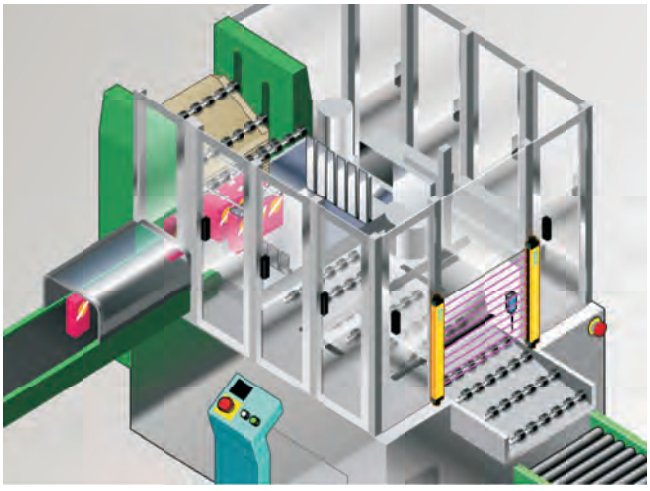
第 3a 步：安全功能的定义

安全功能决定了如何采用防护措施来降低风险。必须为所有尚未排除的可能危险定义一个安全功能。为了获得所需要的合理安全性，必须对安全功能进行精确的定义。通过安全功能的定义我们可以了解实现安全功能所必需的部件类型和数量。

➜ 安全功能定义的示例：BGIA-报告 2/2008“Funktionale Sicherheit von Maschinensteuerungen”（“机器控制的功能安全”）

永久禁止访问

采用机械挡板、屏障或障碍物（亦即所谓的物理防护设备）防止对危险地点的访问。

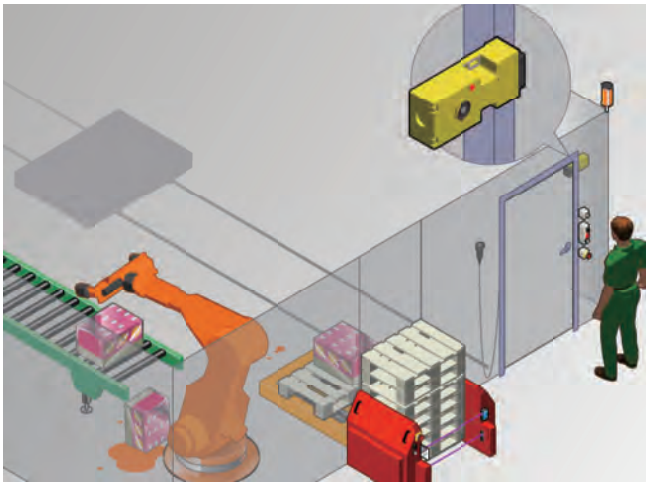


示例：

- 使用防护挡板防止对危险地点的直接访问（如图所示）
- 使用选择性通道防止对危险地点的访问，只允许原料或货物通过（如图所示）
- 使用栅栏防止对危险区域的物理访问

临时禁止访问

在机器处于安全状态前，防止对危险地点的访问。需要时可执行机器停机操作。当机器到达安全状态后，允许进行访问。



本章主要内容	页码
➜ 永久禁止访问	3-2
➜ 临时禁止访问	3-2
➜ 阻挡部件/物体/放射物	3-3
➜ 停机	3-3
➜ 避免意外启动	3-3
➜ 防止启动	3-4
➜ 停机/防止启动的组合使用	3-4
➜ 人/原料的区分	3-4
➜ 监控机器参数	3-5
➜ 手动解除安全功能（有限时间内）	3-5
➜ 组合或更改安全功能	3-5
➜ 紧急情况下的关机	3-5
➜ 指示和报警	3-5
➜ 其他功能	3-6
➜ 总结	3-6

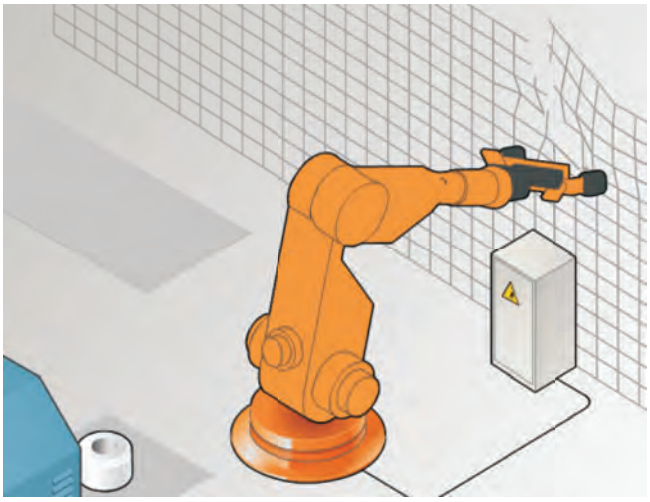
© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

阻挡部件/物体/放射物

如果可能产生放射性的物质或部件会被甩出机器，则在此类情形下应采用机械防护设备（物理防护设备）来防止危险的发生。

示例：

- 车床上使用具有特殊观察窗口的安全盖，以防止飞溅的碎片或工件零件
- 用于阻拦机器人臂的栅栏（如图所示）

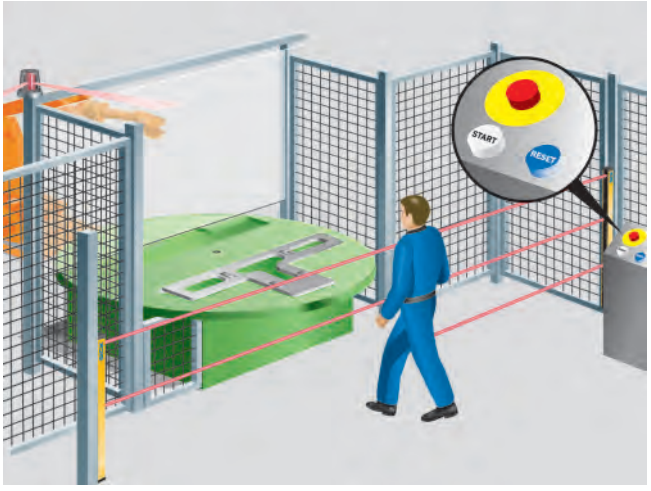


停机

需要时（例如有人靠近机器），可以采用与安全相关的停机功能使机器处于安全状态。为了防止重启动时出现问题，比较明智的做法是在安全停机前进行一次普通的停机。可能需要额外的安全功能以防止意外的重启动。

示例：

- 打开具有互锁功能却没有锁定设备的防护设施
- 阻断光电安全开关（具有访问保护功能）上的光束（如图所示）



避免意外启动

在启用“停机”功能或机器上电后，需要采取一些特定的操作以使机器进入运行状态。手动复位防护设备就属于这类特定操作，其目的在于为重新启动机器做好准备。

示例：

- 复位光电开关（如“停机”图中所示：蓝色“复位”按钮）
- 复位紧急停机设备
- 当所有必需的安全设备都有效时，重新启动机器

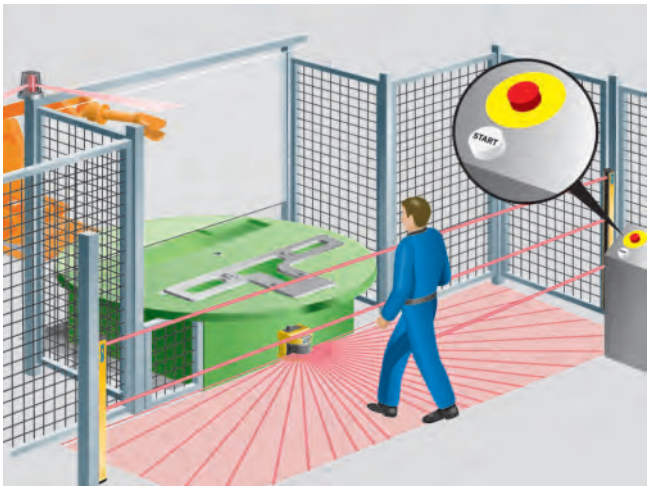
© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

防止启动

在启用与安全相关的“停机”功能后，只要有人处在危险区域，就必须采用技术手段防止机器启动或返回运行状态。

示例：

- 安全钥匙系统
- 在安全激光扫描器的有效防护区域进行检测（如图所示）。“停机”功能由光电安全开关的垂直防护区域实现。



停机/防止启动的组合使用

只要有人或其肢体处于危险区域以内，就需使用与停机时采用的相同防护设备来防止重新启动。

示例：

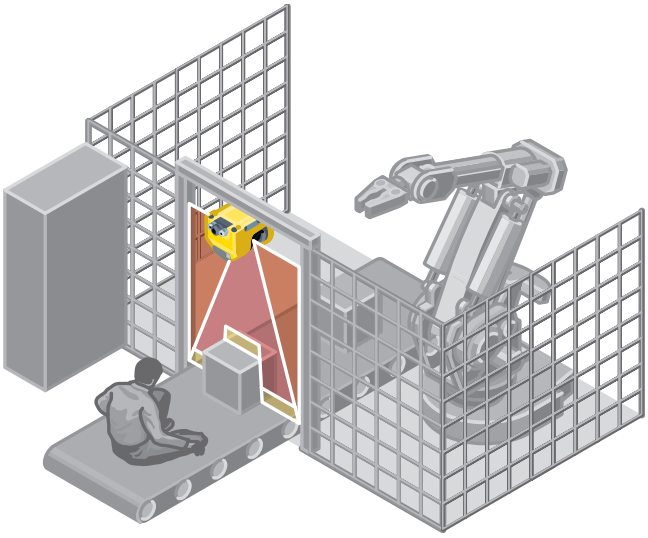
- 在单人工作间使用的双手控制设备
- 使用光幕，从而使操作员不能站到后面或者触及周围（危险地点防护）
- 使用安全激光扫描器进行区域防护（如图所示）

人/原料的区分

为了在危险区域输入或输出原料，需要利用原料的特点以自动区分原料和人。在原料运输期间防护设备不会检测到运输物体，但是可以检测到人。

示例：

- 使用电感式防护设备 (ESPE) 屏蔽某项物品
- 带集成人-原料区分算法的水平光幕
- 启动安全激光扫描器的防护区域（如图所示）



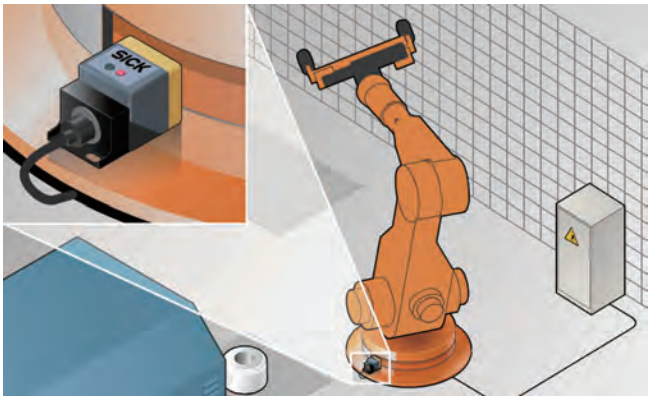
© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

监控机器参数

在某些应用中，必须对各种机器参数的安全限制进行监测。如果超出了限定值，就要采用适当的措施，如停机、发出警告信号等。

示例：

- 监测速度、温度或压力
- 位置监控（如图所示）



手动解除安全功能（有限时间内）

如果在装配或过程监控时需要暂时关闭安全功能，那么应该采用额外的风险降低措施。安全功能必须手动解除。

示例：

- 限制运动速度或动能
- 限制运动的持续时间（点动）
- 带使能开关和 +/– 按钮的手持式控制设备（如图所示）

组合或更改安全功能

机器在不同的运行模式下会呈现出不同的工作状态。这样，可能需要采用不同的安全措施，或组合使用不同的安全功能。应当确保通过控制功能能够实现必需的安全等级。运行模式的切换或安全措施的选择和调整不应导致出现危险的状态。

示例：

- 在机器设置和常规运行之间完成运行模式更改后，机器会停止。此时必须重新输入手动启动指令
- 在无风险的按钮回程期间，解除安全光幕的停机指令
- 将激光扫描器的监控对象调整为车辆的速度

紧急情况下的关机

紧急情况下的关机（紧急停机）是一种额外的防护措施，并不是降低风险的主要方法。因此此功能并不能看作为一个安全功能。

此功能的安全等级取决于机器的风险评估结果，但我们还是建议采用和主要防护措施相同的安全等级来实现这个功能。

➜ 参见 EN 60204-1:2006 和 EN ISO 13850

安全指示和报警

状态指示是传统安全功能的补充措施。

示例：

- 互锁指示
- 启用警告功能
- 屏蔽指示灯

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

其他功能

与安全相关的设备还可提供其他功能，但这些功能不是用于保护人员安全的。实际的安全功能不会受此影响。

示例：

- 工具/机器保护
- PSDI 模式（循环触发）
- 防护设备的状态也用于自动化任务（例如导航）
- 防护措施的状态经由一个总线系统传输至中央控制室

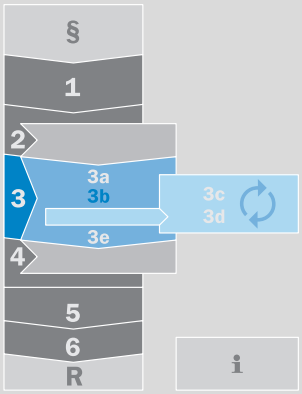
总结：安全功能的定义

定义哪些安全功能是降低风险所必需的：

- 永久禁止访问
- 临时禁止访问
- 阻挡部件/物体/放射物
- 停机
- 防止启动
- 避免意外启动
- 停机/防止启动的组合使用
- 人/原料的区分
- 监控机器参数
- 手动解除安全功能（有限时间内）
- 组合或更改安全功能

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

第 3b 步：确定必需的安全等级



按照规定，在 C 类标准（机器特定的标准）中必须定义必需的安全等级。必需的安全等级会针对每一个安全功能单独定义，并应用到所有相关设备上，例如：

- 传感器/防护设备
- 评估逻辑设备
- 执行器

如果相关机器没有可用的 C 类标准，或者在 C 类标准中没有对此类机器的要求，那么可以根据以下标准确定必需的安全等级：

→ EN 954-1（2009 年 12 月 28 前有效）
→ EN ISO 13849-1:2006
→ EN 62061:2005

通过应用这些标准可以保证有效地降低所定义的风险。

不同职能的操作员所需要的保护是不同的。例如，在金属压机上进行部件插入和卸载操作的操作员所需要的保护与那些最大风险是夹住手指的机器操作员所需要的保护就是不同的。

另外，同一台机器在不同的寿命阶段或者不同的危险地点时，其可能带来的风险也各不相同。在这种情况下，需要对使用寿命的每一个阶段和每一种危险分别定义安全功能。

所有标准的制定都是基于风险评估所使用的参数：

- 可能产生的伤害/损害的严重程度
- 暴露在危险中的频率和/或持续时间
- 预防危险的可能性

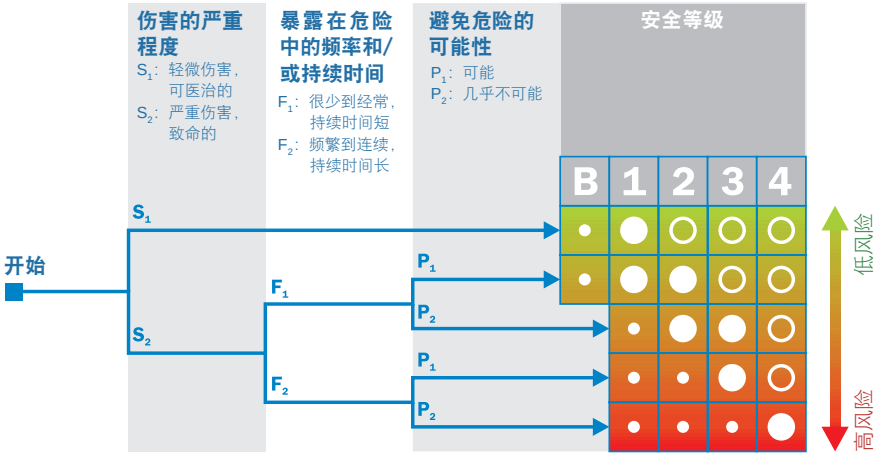
以上参数组合起来才能确定所需的安全等级。

在确定安全等级期间应用这些标准中描述的规程时是假设机器没有防护设备的。

根据 EN 954-1 (1996) 标准的分类

到目前为止，EN 954-1 (1996) 标准中用于选择必需的安全等级的流程叫做风险图。该图对各种必需的安全等级进行了分类。

EN 954-1 仍然有效，将来会被 EN ISO 13849-1 标准取代。



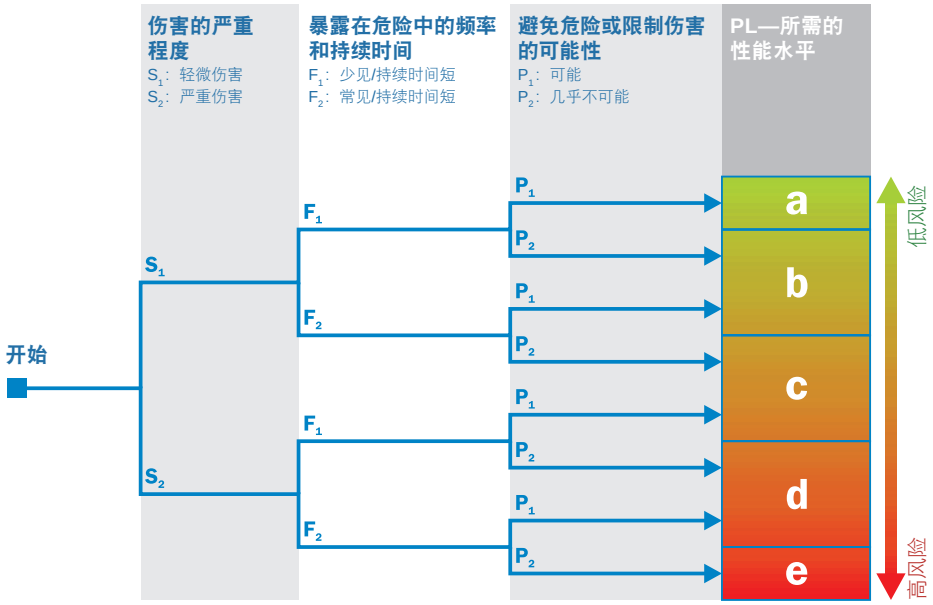
© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

EN ISO 13849-1 和 EN 62061 标准都对控制系统安全相关部件的设计和实现要求进行了定义。参照右边表格中的信息，用户可以根据所使用的技术选择适当的相关标准：

技术	EN ISO 13849-1	EN 62061
液压	适用	不适用
气压	适用	不适用
机械	适用	不适用
电气	适用	适用
电子	适用	适用
可编程电子技术	适用	适用

EN ISO 13849-1 中规定的性能水平

这个标准也使用了一个风险图来确定必需的安全等级。和 EN 954-1 一样，它也使用 S、F 和 P 参数来表示风险的大小。但是此例中最终获得的结果是“所需的性能水平”（PLr：所需的性能水平）。



性能水平通过 5 个步骤进行定义，它取决于控制系统的结构、所使用部件的可靠性、故障检测能力以及在多通道控制系统中对多个共因失效的抵抗力。另外，还需要采用更多措施以避免设计缺陷

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

EN 62061 中规定的安全完整性等级

这里采用的是一个数学计算过程，需要对伤害程度、处于危险区域的频率/时间以及避免伤害的可能性进行一一评估。另外，危险事件的发生概率也要考虑在内。最终获得的结果就是安全完整性等级 (SIL)。

效果	伤害程度 S	等级 K = F + W + P				
		3-4	5-7	8-10	11-13	14-15
致命的，失去眼睛或手臂	4	SIL2	SIL2	SIL2	SIL3	SIL3
永久伤害，失去手指	3			SIL1	SIL2	SIL3
可医治的，需要医学治疗	2				SIL1	SIL2
可医治的，需要急救	1					SIL1

危险事件的频率 1) F		危险事件的发生概率 W		避免危险事件的可能性 P	
F ≥ 1×（每小时）	5	经常	5		
1×（每小时）> F ≥ 1×（每天）	5	很可能	4		
1×（每天）> F ≥ 1×（每两周）	4	可能	3	不可能	5
1×（每两周）> F ≥ 1×（每年）	3	很少	2	可能	3
1×（每年）> F	2	极少	1	很可能	1

1）适用于持续时间大于 10 分钟的情况

可按如下步骤确定 SIL：

1. 确定伤害程度 S。
2. 确定频率 F、概率 W 和避免危险的可能性 P。
3. 由 F+W+P 之和计算等级 K。
4. “伤害程度 S”行与“等级 K”列交会处即为所需的安全完整性等级 SIL。

安全完整性等级 SIL 分为三个等级，它取决于控制系统的结构、所使用部件的可靠性、故障检测能力以及在多通道控制系统中对多个共因失效的抵抗力。另外，还需要采用更多措施以避免设计缺陷。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

总结：确定必需的安全等级

概述

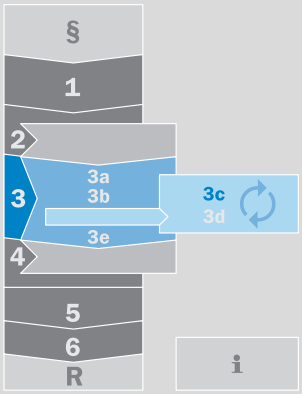
- 为每一种安全功能确定必需的安全等级。
- “潜在伤害的严重程度”、“暴露在危险中的频率和持续时间”和“避免伤害的可能性”决定了所需的安全等级。

所使用的标准

- EN ISO 13849-1 与之前的 EN 954-1 标准类似，都是使用风险图来确定必需的安全等级。该过程所得到的结果是“所需的性能水平” (PLr)。
- EN ISO 13849-1 同样适用于液动、气动和机械系统。
- EN 62061 采用的是一个数学计算过程。最终获得的结果是安全完整性等级 (SIL)。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

第 3c 步：设计安全功能



第 3c 和 3d 步主要介绍如何选择合适的技术以及适当的防护设备和部件来设计和验证安全功能。在某些情况下这些步骤需要反复进行数次。

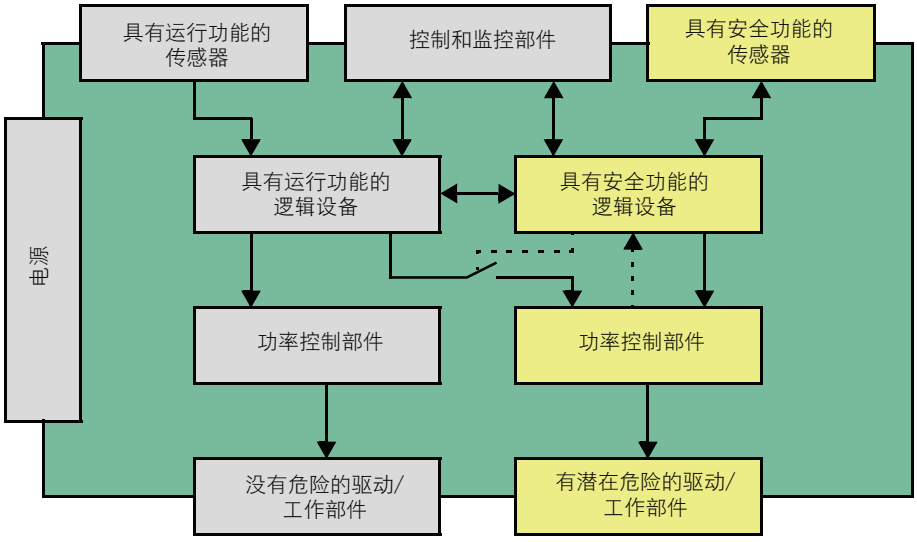
在此过程中需要重复检查所采用的技术是否能够保证足够的安全性、在技术上是否可行以及某种特定技术的使用是否会造成其他风险。

安全原则的准备

一台机器或一个系统包含多个不同的部件，它们相互配合以保证机器或系统的功能。在这里需要对纯粹用于运行的部件和那些具有安全相关功能的部件进行区分。

➜ 关于安全原则的详细内容：BGIA-报告 2/2008 “Funktionale Sicherheit von Maschinensteuerungen”

机器控制器的功能结构



控制系统安全相关部件的选择需要符合安全功能以及必需的安全等级的要求，如传感器、逻辑设备、功率控制部件以及驱动和工作部件。这种选择通常按照安全原则进行。一种安全功能可以由一个或多个安全相关的部件实现，数种安全功能也可以共用一个或多个部件。

3 c

本章主要内容	页码

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

决策特征

在安全原则的准备期间需要考虑以下特征：

- 机器特征
- 环境特征
- 人类因素
- 设计特征
- 防护设备特征 (➜3-15)

根据这些特征可以确定需要集成哪些防护设备。

机器特征

应该考虑以下机器特征：

- 随时停止危险动作的能力（如果不具备这种能力，就需要使用物理防护设备或偏转护栏）。
- 停止危险运动且不造成额外危险的能力（如果不具备这种能力，请选择不同的设计/防护设备。）
- 零件被甩出后产生危险的可能性（如果具有这种可能性，请使用物理防护设备。）
- 停机次数（为了确认防护设备是否有效，必须知道停机次数。）
- 监控停机时间/超时运行的可能性（如果由于老化/磨损使系统产生了变化，那么该功能是非常必需的。）

环境特征

应该考虑以下环境特征：

- 电磁干扰/辐射干扰
- 振动/冲击
- 环境光/传感器、焊接火花和反光表面造成的光干扰
- 污染（薄雾，碎片）
- 温度范围
- 湿度/天气

人类因素

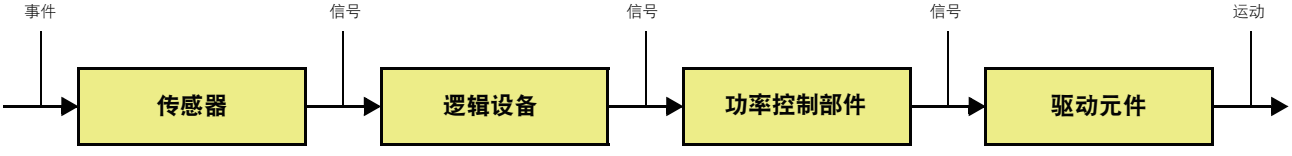
应该考虑以下人类因素：

- 机器操作员的预期资历
- 在相关区域中的预期人数
- 靠近速度 (K)
- 避开防护设备的可能性
- 可预见的误操作

设计特征

使用经过认证的安全部件来实现安全功能总是明智的，因为经过认证的安全部件能够简化设计以及接下来的验证过程。一个安全功能由数个子系统实现。

仅使用已经经过认证且具有安全等级 (PL/SIL) 的安全部件通常不能实现子系统。确实，子系统通常由数个独立元件装配而成。但在这种情况下，安全等级由各种不同的参数决定。

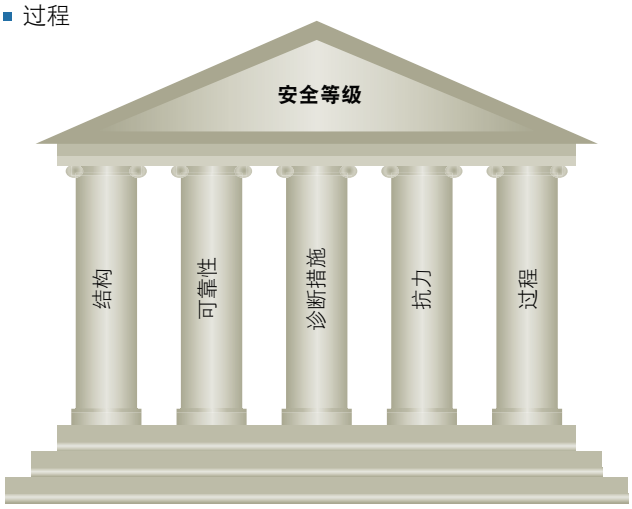


© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

子系统的安全相关参数

子系统的安全等级取决于不同的子系统安全相关参数，例如：

- 结构
- 部件/设备的可靠性
- 检测故障的诊断措施
- 对共因失效的抗力
- 过程

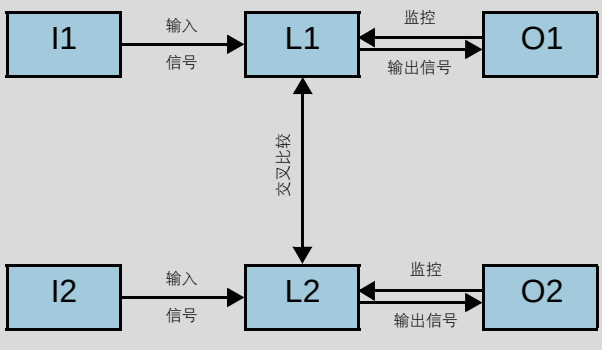


结构

可以在数个通道上并行执行安全相关功能，从而实现以更优的结构来降低安全部件对故障的敏感度。双通道安全部件在机器安全领域是常见的方案（如下图所示）。每一个通道都可以停止危险状态。这两个通道可以有多种设计（一个通道使用机电部件，另一个通道使用电子部件）。第二通道与第一通道不同，它具有监控功能。

单通道安全部件

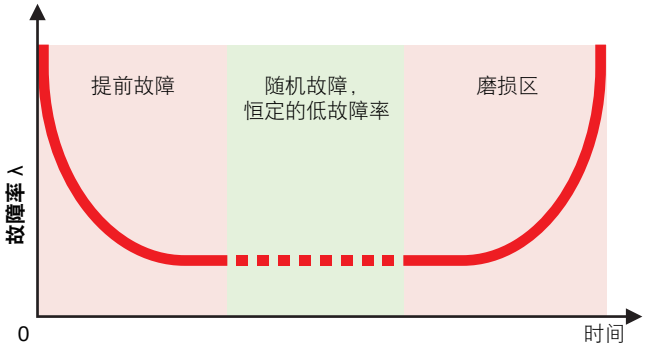
双通道安全部件



部件/设备的可靠性

安全部件出现任何故障时都会导致生产过程的中断。因此使用可靠的部件是非常重要的。当可靠性足够高时，危险的事故的发生概率将会变得更低。可靠性参数是使用寿命期间随机故障发生概率的一种衡量方式，通常如下进行描述：

- 电磁或气动部件：**图 B_{10}**。在这种情况下使用寿命取决于开关频率。B_{10} 定义了一个开关周期数，每个开关周期后会有 10% 的部件出现故障。
- 电子部件：**故障率 λ**（lambda 图）。故障率通常用 FIT（故障率单位）表示。1FIT 就是指平均每 10^9 小时出现一次故障。



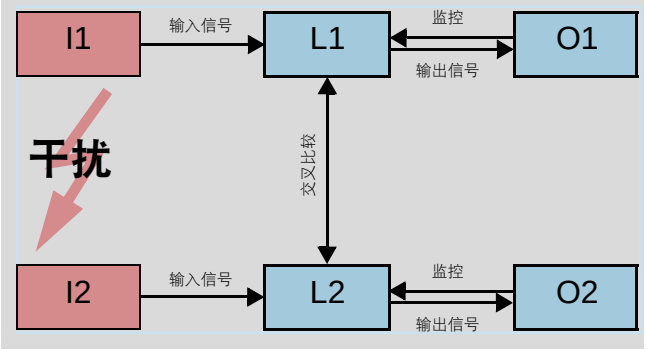
检测故障的诊断措施

某些故障可以通过诊断措施进行检测。这些包括可靠性监控、电流和电压监控、看门狗功能和基本功能测试等。

并不是所有的故障都能被检测到，因此需要确定故障检测的程度。为了达到此目的，应该进行一次故障模式与影响分析 (FMEA)。对于复杂设计来说，标准中的措施和经验数据都能提供辅助作用。

对共因失效的抗力

共因失效表示的是这样一种情况，例如由于相互干扰造成两个通道同时产生故障。在这种情况下需要采取适当的措施，例如单独走线、采用火花抑制电路和分散部件等。



3 c

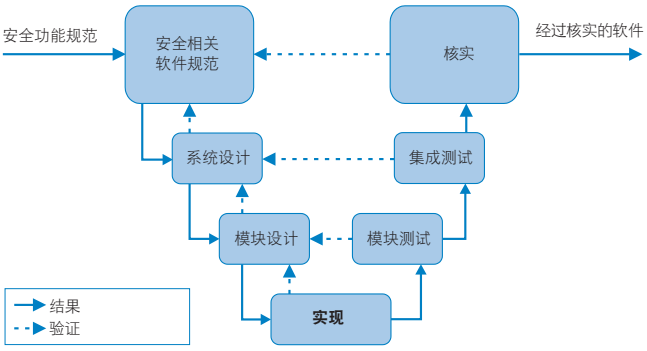
© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

过程

过程由具有相应职能的下列部分组成：

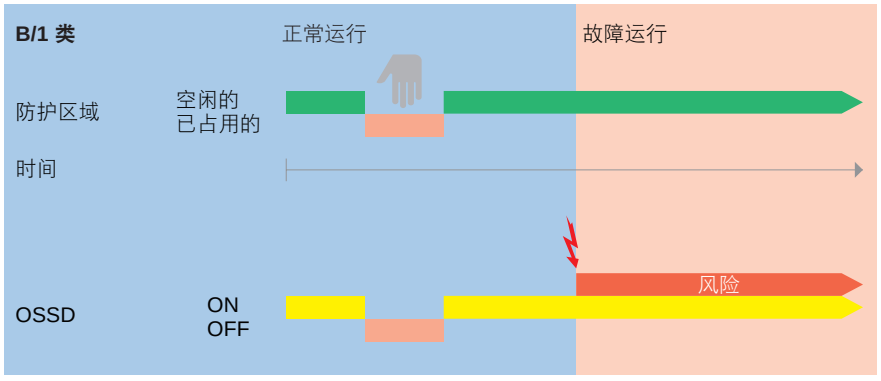
- 组织和能力
- 设计准则（例如规范模板，编码指南）
- 测试原则和测试标准
- 文档和配置管理

在安全技术领域，基于V模型的过程被证明在软件设计实践中特别有效（如图所示）。



按照 EN 954-1 标准进行评估

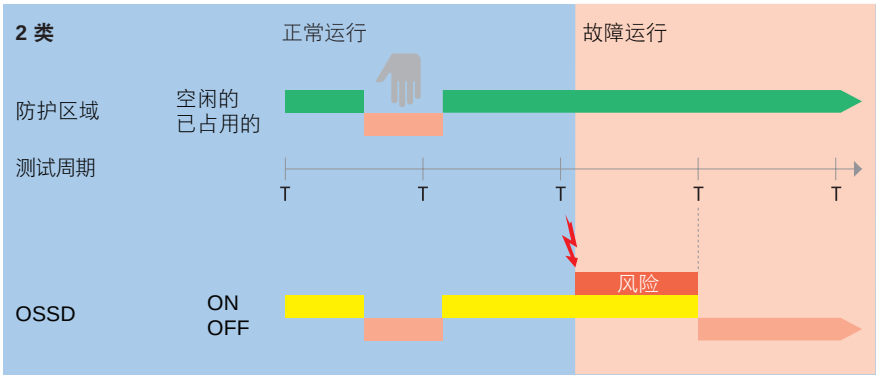
在 EN 954-1 标准中确定安全相关参数时是以分类作为辅助手段的。其替代标准 EN ISO 13849-1 仍然保留这一基本原则。



B 类/1 类

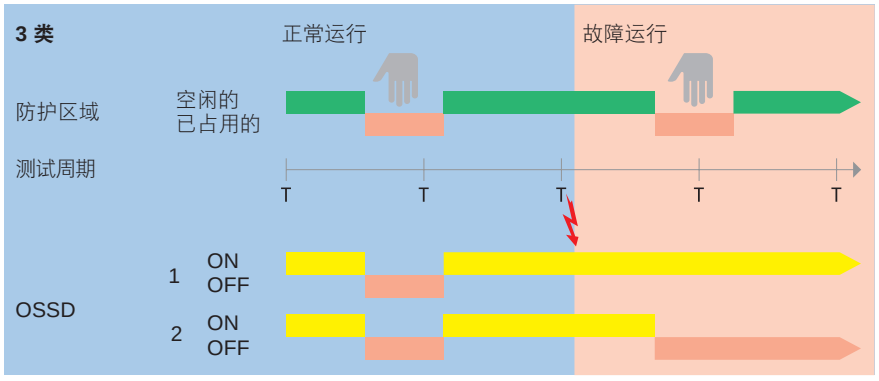
没有故障检测。出现一个故障就会导致风险。

采用可靠和经过验证的部件（1 类）可以降低风险。



2 类

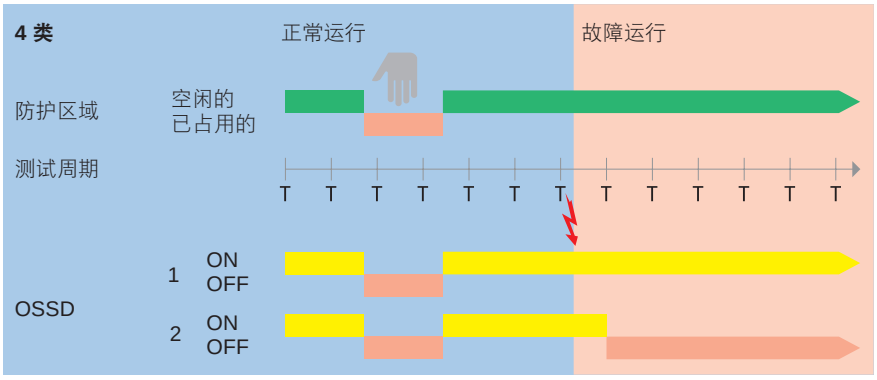
通过测试可以检测故障。在故障发生和下一次测试之间的时间段内会有风险。



3 类

出现一次故障时能够保持安全功能。故障可能由所使用的安全功能检测到，也可能在下一次测试中检测到。多次故障的累加会导致风险。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。



4 类

出现故障时仍然能够保持安全功能。与 3 类不同的是，即使没有检测到第一次故障，其后续故障也不会导致安全功能的丧失。

防护设备特征

需要考虑的防护设备特征包括：

- 防护设备的属性和应用（电敏设备、物理设备等➜3-16)
- 防护设备的布置/尺寸 (➜3-29)
- 集成至控制系统 (➜3-40)

下列各小节会对这几点进行详细说明。

3 c

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

防护设备的选择

电感式防护设备 (ESPE)

使用最广泛的电感式防护设备就是光电设备，例如：

- 光幕和光电开关（也叫 AOPD — 有源光电防护设备）
- 激光扫描器（也叫 AOPDDR —有源光电漫反射防护设备）
- 安全摄像系统

为什么使用光电防护设备?

如果操作员必须接触到机器，从而暴露在危险中，那么建议使用光电防护设备取代机械防护设备（固定防护栏、双手控制设备、栅栏等）。这将减少进出时间（操作员不需要等待防护设备打开）、提高生产力（为机器加载时可以节省时间），并提高工作场所的工作效率。另外，操作员和其他人员都可以得到同等保护。

如果操作员不会处在被飞溅部件（例如由飞溅的熔化原料）伤害的危险中，则可以使用光电防护设备。

选择合适的 ESPE

应该满足以下要求：

- 协和标准的要求，尤其是 C 类标准的要求
- 危险区域前方有可用空间
- 人体工程学标准，例如需要循环插入物料的工作
- 分辨率

ESPE 能够实现什么安全功能?

- 停机 (➜3-3)
- 避免意外启动 (➜3-3)
- 防止启动 (➜3-4)
- 停机/防止启动的组合使用 (➜3-4)
- 人/原料的区分 (➜3-4)
- 监控机器参数 (➜3-5)
- 安全提示和警告 (➜3-5)
- 其他功能，如 PSDI 模式、遮蔽、防护区域开关等 (➜3-6)

安全等级

ESPE 的安全相关参数是在种类划分（2 类、3 类、4 类）中实现的。

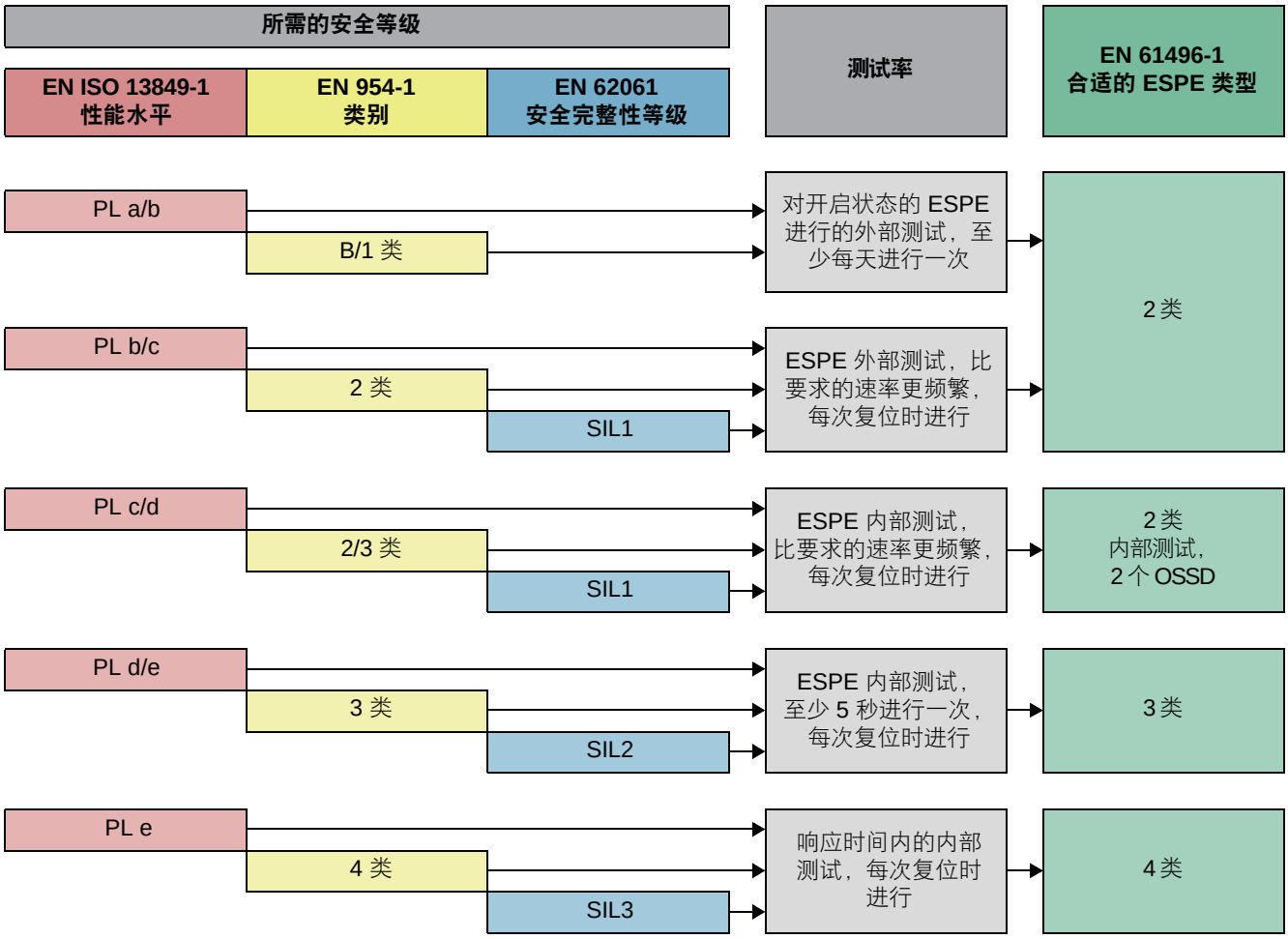
与 EN 954 标准中的分类类似，除结构因素外，与电磁兼容 (EMC)、环境条件和光学系统相关的要求都在种类划分中进行了定义。这些尤其包括与干扰源（阳光、灯光、具有类似设计的设备等）相关的行为以及安全光幕或光电安全开关（对 4 类 AOPD 的要求要比对 2 类 AOPD 的要求更高）上光学器件的视角。

在确定到反射表面的最小距离时，视角是非常关键的。

➜ ESPE 的要求：EN 61496-1，CLC/TS 61496-2，CLC/TS 61496-3

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

选择合适的 ESPE 类型作为必需安全等级的一项功能



3 C

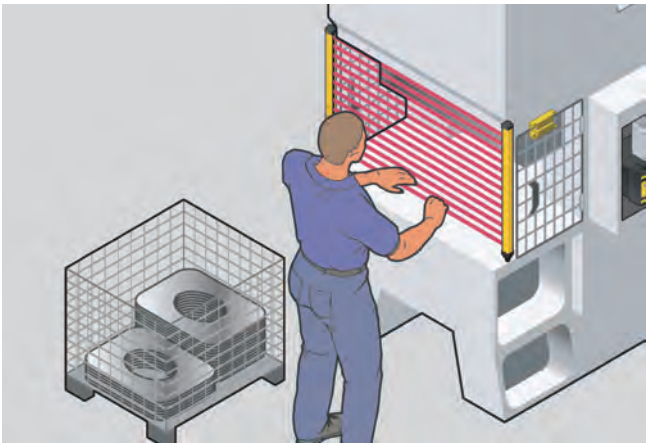
© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

ESPE 检测什么?

危险点防护：手指或手的检测

进行危险地点防护时，能够检测到距离危险地点非常近的情况。

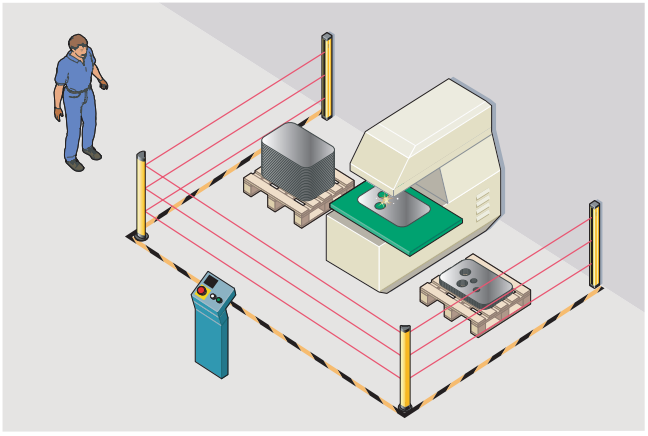
由于可以实现更短的安全距离并且操作员能够更符合人体工程学地工作（例如在按压机上的加载工作期间），这类防护设备更具优势。



接入防护：对接入危险区域的人员进行检测

进行接入防护时，能够检测到靠近人员的身体。

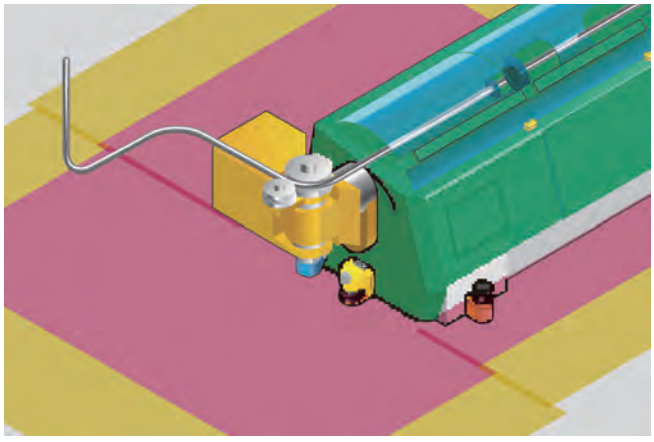
此类防护设备用于对危险区域的访问进行防护。如果进入危险区域就会发出一个停机信号。站在防护设备后边的人将不能被ESPE检测到！



危险区域防护：对危险区域中出现的人员进行检测

进行危险区域防护时，通过检测某人处于区域内可以检测到人员的靠近。

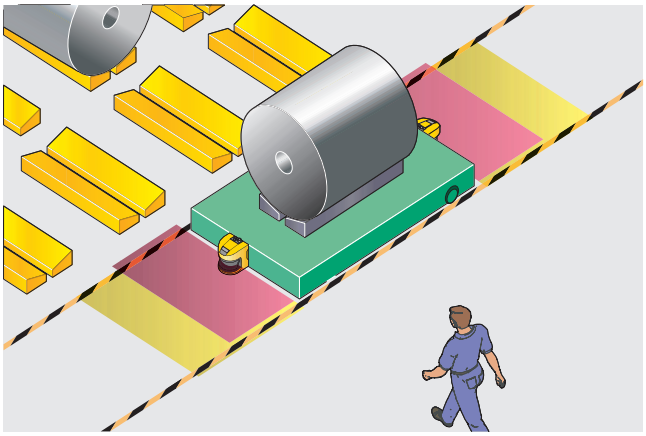
此类防护设备适用于那些从复位按钮处不能完全看到危险区域的机器。如果进入危险区域，就会发出一个停机信号并防止开机。



© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

移动的危险区域防护：对正在靠近危险区域的人进行检测

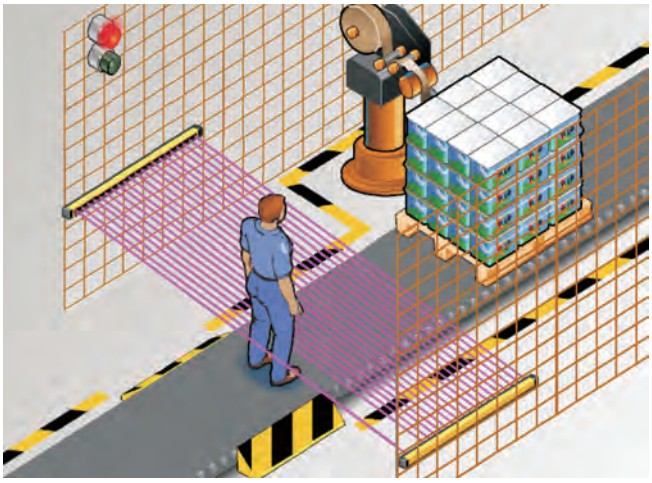
危险区域防护适用于 AGS（自动导航系统）、起重机和码垛机等，用于在车辆运动期间或者将这些车辆停泊到固定站点时对操作人员或第三者进行保护。



可能的其他功能：人/原料的区分

ESPE 的一个特殊应用就是用于区分人和原料的安全功能。这种安全功能对于那些货盘装载上的所有工作都要自动完成的机器（意即仅通过机器自身来完成这些工作）非常有用，如包装机、货盘装载机和货盘卸载机。

有两种可能的类型：



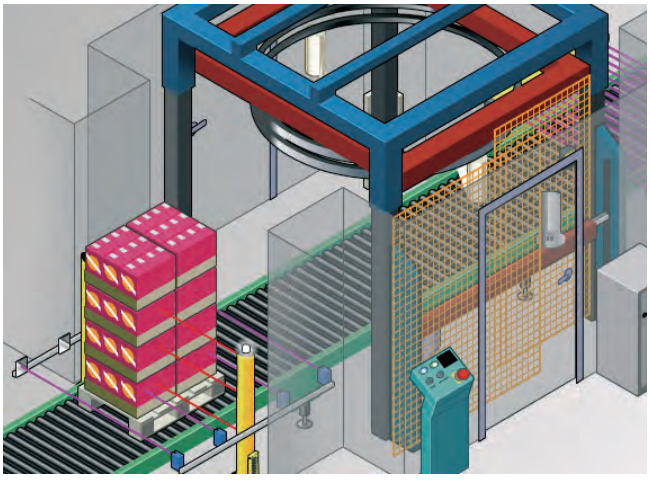
- **集成的 Muting 功能：**

  新型的安全光幕具备集成的 Muting 功能，来区分人和原料。而这里不需要额外的传感器，并且而且也不需要进行复杂的安装和维修工作。

- **使用 Muting 功能：**

  通过 Muting 功能，可以暂时解除防护设备的功能。由于当货盘通过的时候必须解除 ESPE 的功能，此时必须使用功能抑制系统区分人和原料。总的来说，关于这种安全功能状态有多种标准，诸如：

  - 在 Muting 期间，应该采取其他的措施确保处于安全状态，例如禁止对危险区域进行访问。
  - Muting 应该是自动进行的。
  - Muting 不应取决于单个电气信号。
  - Muting 不应完全取决于软件信号。
  - 在无效组合期间发生的 Muting 信号不能引起任何 Muting 状态，并且应该保证仍然保留防护功能。
  - 在系统畅通之后 Muting 状态会立即解除，因此防护设备会重新运行。
  - 仅在载重货盘堵塞访问危险区域的工作周期时间段内，允许激活 Muting。

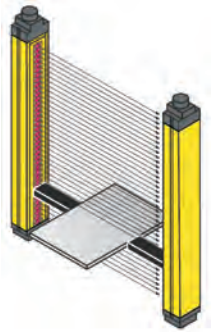


➜ 包装机器的要求：EN 415-4
➜ ESPE 的实际应用：CLC/TS 62046

3 C

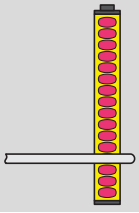
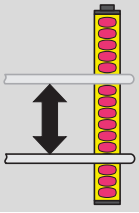
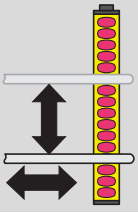
© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

可能的其他功能：屏蔽



使用这个功能时，由于操作流程需要而处在 ESPE 防护区域内的物体会被屏蔽掉，从而不会引发停机过程。

原则上，遮蔽区域就是防护区域的一个漏洞。在计算安全距离时要将这种情况考虑进去。

固定屏蔽	浮动屏蔽	
	有物体	有或没有物体
		

可能的其他功能：PSDI 模式

如果部件是周期性手动插入或移除的，那么这种运行模式就很有优势。在这种模式下，当一次或两次中断后，防护区域将重新变得畅通，机器周期就会自动重新开始。

在以下情况下必须复位 ESPE：

- 机器启动时
- ESPE 在一次危险运动期间被中断后又重新启动时
- 在规定的 PSDI 时间内没有触发 PSDI 时

必须确定操作人员工作时没有处在危险中。这个条件限制了此运行模式只能在小型机器上使用，这些小型机器不允许进入危险区域，并且具有存在检测或机械防护。机器的所有其他方面也应采取合适的措施进行保护。

在 PSDI 模式下，ESPE 的分辨率应不大于 30 毫米（手指或手的检测）。

➜ 回程释放：B 类标准 EN 999，EN 61496-1
➜ 压机上的 PSDI 模式：C 类标准 EN 692，EN 693

物理防护设备

物理防护设备指的是用于防止或避免操作人员直接触及危险地点的机械防护设备。它们可以是固定的或者可移动的。挡板、栅栏、关卡、风门和门等都是物理防护设备。

挡板和盖子能够阻止从任何方向的访问。栅栏通常用于防止完整高度的访问。相反地，关卡只能用于防止对危险地点的意外或无意访问。

安全功能对于物理防护设备的设计来说是至关重要的。物理防护设备只能够防止访问，还是也能遮挡部件/原料和辐射呢？

被甩出的原料示例：

- 碎裂/爆裂的工具（磨轮、钻头）
- 产生的材料（粉尘、片屑、碎片、碎木料）
- 排放物（液压油、压缩空气、润滑液、原料）
- 在夹持或搬运系统发生故障后被甩出的零部件

发出的辐射示例：

- 生产过程或产品（热表面）产生的热辐射
- 激光、IR（红外）或 UV（紫外）源产生的光辐射
- 粒子或离子辐射
- 强电磁场，高频设备
- 测试系统或静电放电系统（纸和塑料网）的高电压

为了遮挡辐射或原料，对物理防护设备的机械要求通常要比防止人员访问的物理防护设备的要求更高。如果风险评估确定物理防护设备的损坏（裂开或变形）不会造成任何危险，那么它的损坏是可以允许的。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

物理防护设备的基本要求

- 物理防护设备应设计得足够坚固和耐用，以确保能够承受运行期间的各种可能环境条件。在机器的整个使用期间物理防护设备的性能必须维持不变。
- 它们不能引起任何额外的危险。
- 物理防护设备不能被轻易绕过或失效。
- 如果对某种工作过程的观察是必需的，则物理防护设备不应限制此观察行为。
- 物理防护设备应牢牢固定。
- 它们应该位于只有通过工具才能打开的系统中，或针对危险的运动进行互锁。
- 如果没有紧固，则不应处在防护位置。

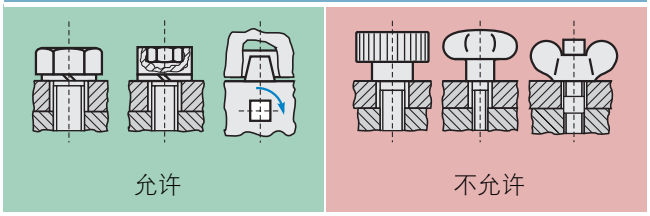
➜ 物理防护设备：EN 953（B 类标准）
➜ 安全机器的设计准则：EN ISO 12100（A 类标准）

物理防护设备的固定

不经常拆卸或打开的物理防护设备，或者仅在维修期间需要拆卸或打开的物理防护设备，应固定在机器框架上。这样，只有通过工具（如扳手、钥匙）才能进行拆卸。拆卸期间会涉及到一个工具选择的过程。

紧固元件应保证不易丢失（如紧固螺钉）。其他类型的紧固件如速卸锁扣、带帽螺钉、滚花螺钉和蝶形螺母等，仅在物理防护设备被互锁时才能使用。

示例：物理防护设备的固定类型



移动式物理防护设备

需要在不使用工具的情况下频繁或定期打开（例如在装配期间）的移动式物理防护设备，应该在功能上与危险运动（互锁、锁定设备）联系起来。所谓的“频繁”打开指的是每次轮班至少打开一次。

如果打开防护设备时可能产生危险（例如长时间超时运行），那么就需要锁定设备。

移动式物理防护设备的人体工程学要求

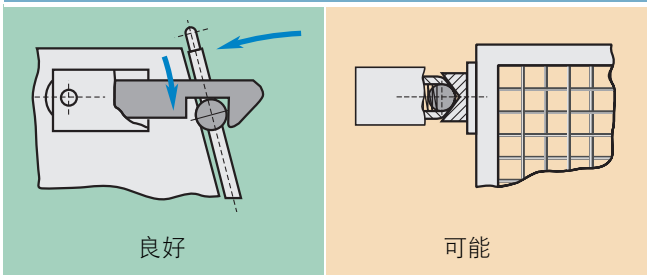
在设计物理防护设备时，人体工程学因素也是非常重要的。只有当物理防护设备不会过分阻碍装配、维修和其他类似工作时，员工才会接受它们。移动式物理防护设备应该满足下列人体工程学要求：

- 易于（例如单手即可完成）打开和关闭、提起或移动
- 符合功能需求
- 防护设备打开后应保证便捷的访问。

移动式物理防护设备的机械固定

如果可行的话，移动式物理防护设备应该连接到机器上，从而使其可以通过铰链、导架等安全地固定在打开位置。我们建议采用定型安装。摩擦安装（例如球形接头）不推荐采用，因为磨损等原因它们的性能会逐渐变差。

示例：紧固设备



3 C

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

物理防护设备的互锁

如果满足以下情况，那么物理防护设备应该被互锁：

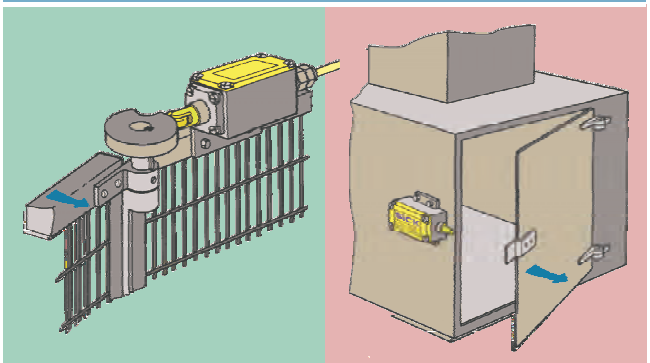
- 防护设备被周期性触发或定期打开（门、风门）
- 不使用工具即可拆卸或可轻易拆卸
- 针对潜在的严重危险进行保护

互锁意味着物理防护设备的打开会转变为一个电气信号，该电气信号能够可靠地停止危险运动。物理防护设备通常使用安全开关进行互锁。

对互锁设备的一个重要要求就是强制驱动。

通过直接接触或刚性部件强制驱动后，互锁（安全开关）的机械部件将被迫随着物理防护设备（例如门）的机械部件一起运动。

示例：强制驱动设计



安全的设计：开门动作会强制移动安全开关上的机械柱塞。此时安全电路会被打开。

错误的设计：安全开关并不总是能打开安全电路，例如在表面沉淀生垢或润滑油渣使柱塞粘住的情况下。

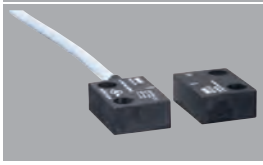
来源：BG Feinmechanik und Elektrotechnik，BGI 575

安全开关

通过安全开关实现的防护设备互锁应满足以下功能：

- 如果防护设备空缺（或者丢失），那么危险的机器功能将不能运行（防止启动）。
- 当防护设备被打开（拆卸）时危险的机器功能将被停止（停机）。

安全开关设计

设计		典型应用
	带独立执行器的安全开关	■对于滑动门和铰链门以及可拆卸挡板应用更有优势 ■可使用锁定设备实现互锁
	带直接执行器的位置开关	■安全限位开关 ■对铰链门和风门的保护
	非接触式安全开关	■安全限位开关 ■对铰链门和风门的保护

强制打开原理

机械安全开关具有几个特征，其开关触点是强制打开的（如果对破坏点来说是必需的），并且即使触点是焊接到一起的或者存在其他的电气故障它们仍然能够执行安全功能。对于具有多个触点的安全开关，基于强制打开原理（EN 60947-5-1：直接打开动作）的接触元件将会集成到安全功能中。

标记按照 EN 60947 标准强制打开的触点。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

机械安装

可靠的机械安装对安全开关的有效性来说是至关重要的。

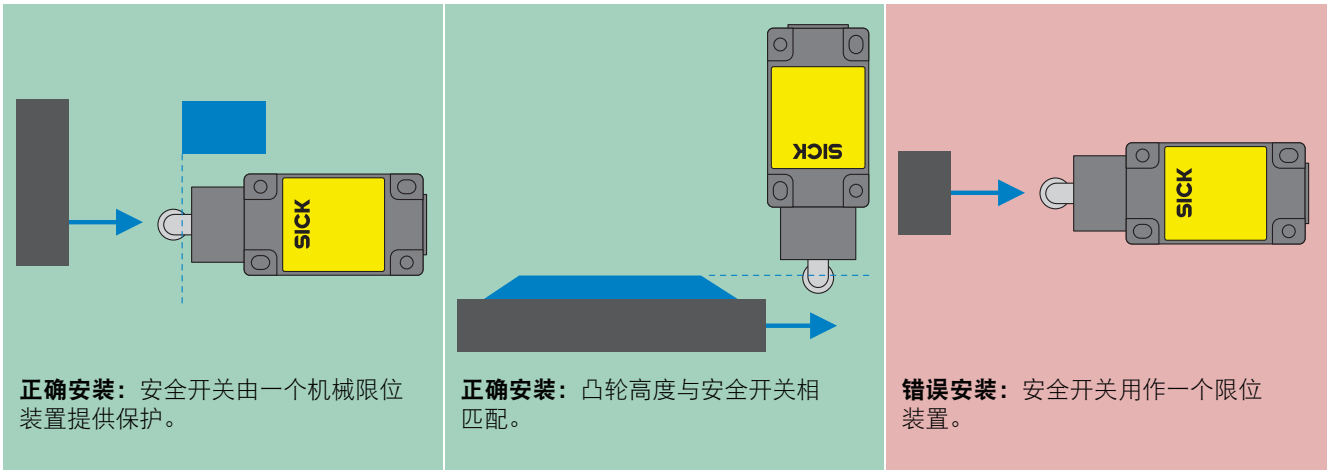
安全开关...

- 其安装应该使其能够防止可预见的外部影响带来的损害。
- 不能用作机械停机装置。
- 它们的布置和设计应该使其能够有效地防止无意操作、位置改变以及损害等。开关和控制凸轮应该使用匹配的形状（而不是强制力）卡紧，例如圆孔、圆销和圆形限位装置等。
- 它们应该由其致动方法进行保护，或者它们在控制中的集成应该保证其不能被轻易地避开。（因此，位置开关应该具有常闭触点（断电脱扣原理）。）
- 应该能够核查开关是否正确运行。如果可能的话，开关应该便于检修。

对位置开关来说，以下一点同样适用：

- 致动回程应与强制打开行程相匹配，并与制造商的操作说明相一致。应该遵守制造商确定的最小柱塞行程，为强制打开提供必要的开关距离。

示例：安全开关的机械安装



正确安装：安全开关由一个机械限位装置提供保护。

正确安装：凸轮高度与安全开关相匹配。

错误安装：安全开关用作一个限位装置。

操作限制

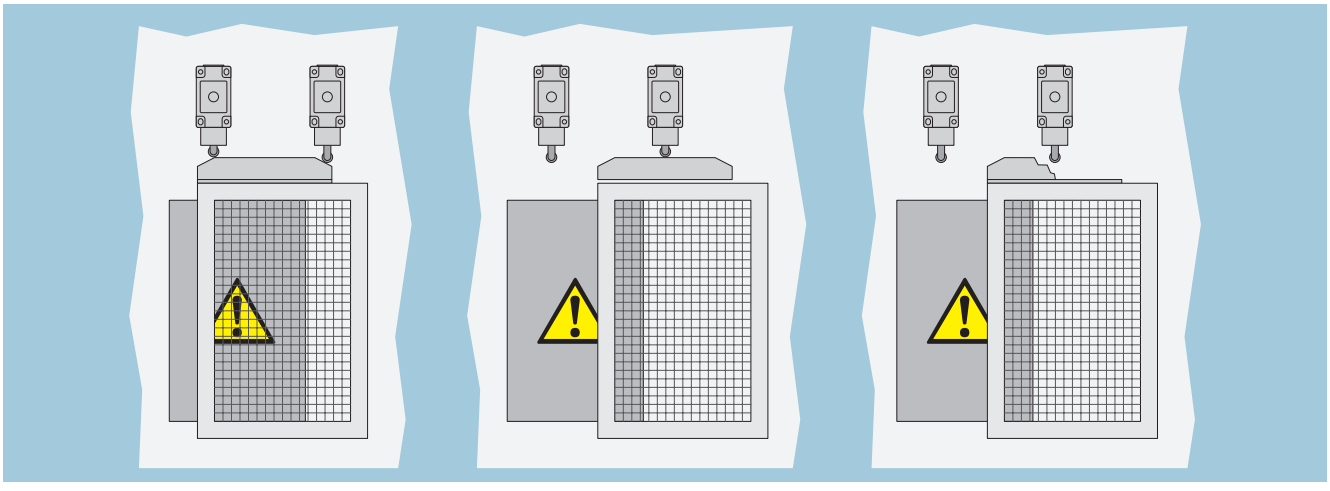
适用于所有安全开关：不能使用简单的物件对安全开关进行随意操作。简单的物件包括螺钉、钉子、金属片、硬币、弯导线以及其他类似物件。

冗余设计

当对执行器或容器（如老化设备）操作不当或其出现机械故障，或环境条件苛刻（例如：粉末污染堵塞了辊筒柱塞）时，安全开关会发生关键故障。尤其是在需要高安全等级的应用中，除了安全开关以外还要使用一个额外的开关（可以具有相反的功能），并且控制系统需要同时监控这两个开关。

示例：一个使用门来防止严重危险且需要周期性致动的注塑机。在这种情况下规定每一扇门都要使用数个机械开关。

示例：通过冗余的分散布置检测机械故障



© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

非接触型安全开关

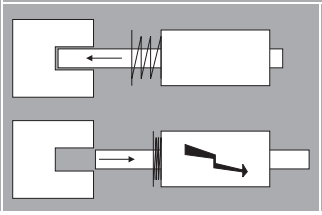
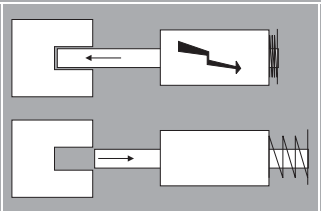
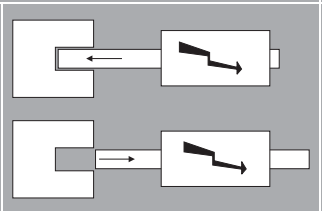
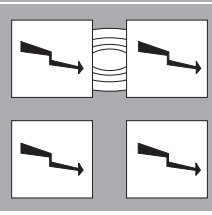
非接触型安全开关采用冗余内部设计或使用特殊的原理，如磁性编码、感应耦合、带编码的发射机等。

- ➜ 安全开关/互锁设备的要求：B 类标准— EN 1088
- ➜ 强制打开原理：B 类标准 EN 60947 -5-1
- ➜ 塑料/橡胶注塑机：C 类标准 EN 201

安全锁定设备

安全功能“暂时阻止访问”通常使用锁定设备来实现。如果需要很长时间才能停止危险运动（人员保护），或者某个过程不允许被中断（过程保护），那么必须使用锁定设备。

安全锁定设备指的是能够防止物理防护设备打开的设备。另外，锁定设备应该使物理防护设备保持关闭状态，直至伤害危险不再存在。通常需要对以下几种类型进行区分：

原理	形状			力
				
运行原理	弹簧致动，使用能量解锁	能量致动，使用弹力解锁	能量致动，使用能量解锁	能量致动，使用能量解锁
术语	机械锁定设备（更适用于人员保护）	电气锁定设备（更适用于过程保护）	液动/气动锁定设备	磁性锁定设备

可以按如下方式使用能量对锁定设备进行解锁：

- 定时控制：在使用定时器的情况下，此设备的故障不应减小延时。
- 自动：仅在没有危险机器状态时（例如，监控设备静止时）。
- 手动：解锁和防护设备解除之间间隔的时间应该比结束危险机器状态所花费的时间更长。

机电一体化

对安全开关适用的规则同样适用于锁定设备。

应该根据强制打开原理确定哪些触点是需要强制打开的。门信号触点用来指示当执行器停止运行时门是打开的。这些触点可以强制打开，但不必总是强制打开的。

选择锁定设备的一个主要原则就是，物理设备应该以多大的力进行锁定。

手动解锁和紧急解锁

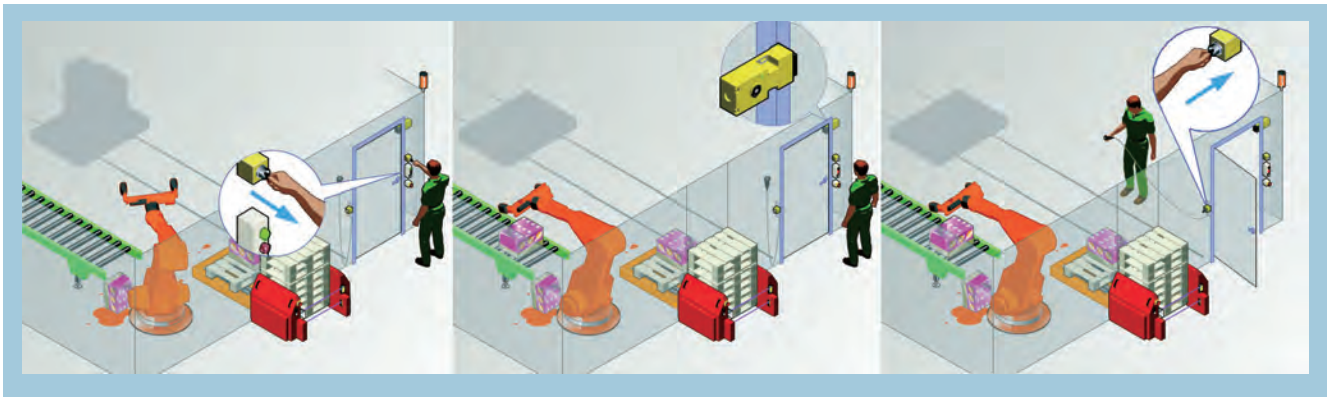
危险评估用于表明在出现故障或紧急情况下，需要采取一定的措施把困在危险区域的人员解救出来。这里需要对机械解锁（使用工具）和紧急或逃离解锁（不使用工具）这些概念进行区分。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

危机钥匙系统

物理防护设备有一个缺点，那就是在进入危险区域后关闭防护设备时，不能有效防止重启动。此时需要采取一些额外措施，例如采用复位设备，或者在安全开关执行器中插入一个铁锁环。然而，这些措施的使用还得取决于使用者的警觉。一种防止意外启动的可行办法是结合使用危机钥匙系统和锁定设备。从外部插入的钥匙可以使能自动运行，并使门保持锁定状态。拔出钥匙（如图 ①）就能停止危险状态。安全状态（例如静止）时门可以被打开（如图 ②）。从内部插入的钥匙可以使能装配操作模式（如图 ③）。 在这种情况下不允许自动运行。

示例：危机钥匙系统



固定位置防护设备

固定位置防护设备能够迫使操作员或操作员的四肢处于危险区域以外。

关于固定位置防护设备的完整概述可参见：
➜ Alfred Neudörfer, Konstruieren sicherheitsgerechter Produkte, Springer Verlag, Berlin u.a., ISBN 978-3-540-21218-8（2005 年第三版)。（英文版“安全机器的设计”，计划 2010 年出版：ISBN 978-3-540-35791-9）

双手控制设备

一台双手控制设备通常只能保护一个人！如果有数名操作员，那么每人都应配备一台双手控制设备。只有在双手控制设备运行时才允许危险的运动，并且只要一只手松开了控制设备就应马上停机。

有许多不同类型的双手控制设备。这些控制设备的主要区别在于按钮设计和控制系统相关的要求方面。

以下基本原则适用于所有类型的控制设备：

- 应该确保必须使用两只手。
- 释放两个按钮中任何一个都应该能够停止危险运动。
- 应该防止无意的触发。
- 防护功能不可轻易避开。
- 双手控制设备不允许在危险区域使用。

以下原则总是适用于 II 类和 III 类双手控制设备：

- 只有在两个按钮都释放开并重新触发之后，才允许重新开始运动。

以下原则总是适用于 III 类双手控制设备：

- 只有当两个按钮在 0.5 秒内同步操作时，才允许进行一次运动。

在 III 类双手控制设备中，还对具有详细系统相关要求的子类进行了定义。最重要的子类有以下几个：

- III 类 A：每个按钮使用一个常开触点（2 路输入）
- III 类 C：每个按钮使用一个常开触点和一个常闭触点（4 路输入）

➜ 双手控制设备要求：EN 574（B 类标准）

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

使能设备

在机器装配、维修和必须观察生产过程停止期间，某些情况下需要解除防护设备的功能。除了其他能够将风险最小化的措施（减小力/速度等）之外，还需要设备在防护设备失效的整个期间进行控制。一个可行的方法是使用使能设备。
使能设备是物理触发的控制开关，操作员使用这种设备控制机器功能。作为惯例，按钮或脚踏开关被用作使能设备。
使能设备的其他启动控制包括操纵杆或点动按钮。3 段式使能设备是经过业界实践证明的，因此推荐使用。

仅激活使能设备不应触发机器的启动。相反，只有激活使能设备时才允许运动。

3 段式使能设备的运行原理：

位置		功能
1		关闭
2		使能
3		紧急停机（关闭）

在从位置 3 改变回位置 2 的过程中，不能解除使能设备功能。在位置 3 处，如果使能设备配有独立触点，那么这些触点应该集成到紧急停机电路内。

防止胡乱操作对使能设备的使用来说也具有重要的意义。

➜ 使能设备要求：EN 60204-1（B 类标准）

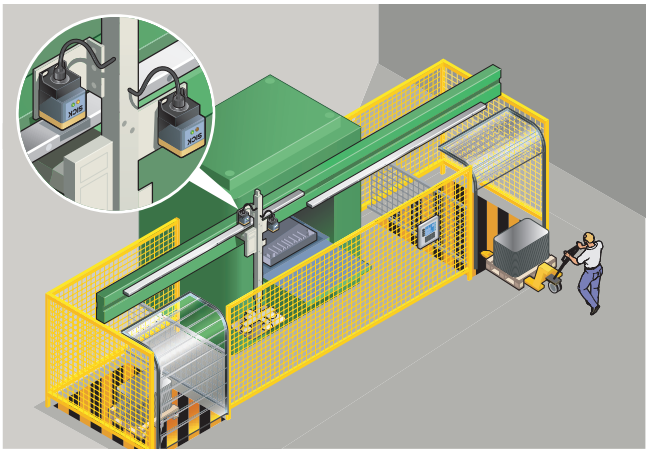
© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

监控机器参数的传感器

风险评估可能表明，应该对运行期间的某些机器参数进行监控和检测。

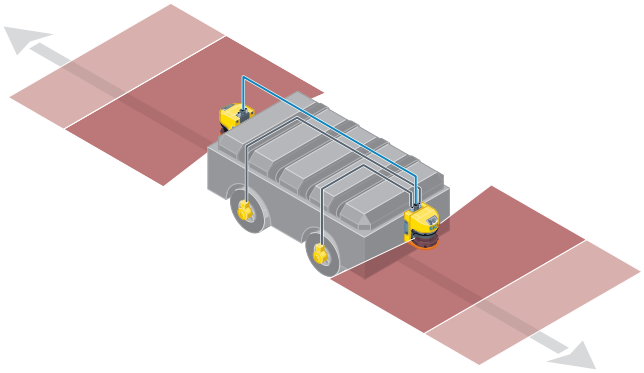
安全位置监控

如果机器运动时经过某个特定位置，就会开始停机过程。
在这种情况下可以使用安全开关 (➜ 3-22)。
电敏感应安全开关尤其适用于此类情形。它们不需要特定的配套元件、没有磨损、具有很高
的外壳防护等级，可以监控机器人轴的某个部分或者机器的运动部分是否在指定的位置。



速率/速度/超时运行监控

安全编码器或行程测量系统可以用于检测和评估速率、速度或超时运行。
在自动运输系统中，编码器通常用于轴上。在这种情况下，一种智能评估算法可用于确定必需的运动参数。
通过使用传感器或旋转编码器以产生一个指示与设定参数的偏差的安全控制信号，安全静止模块或旋转监控模块可以对驱动系统的运动进行监控。还有许多不同的方法，例如通过检测停转过程中电机剩磁的感应电压等。



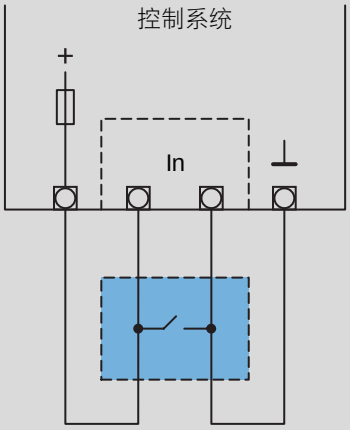
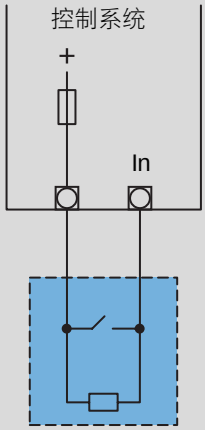
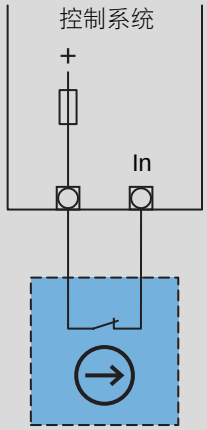
© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

压敏垫、压敏带和防撞条

在某些应用中，压敏型防护设备是非常有用的。其运行原理是基于大多数情况下中空物体的弹性变形，能够确保内部信号发生器（机电或光信号）执行安全功能。

常用的机电系统有许多不同的设计。

在任何情况下，正确的机械布局和一体化对于有效的防护功能来说都是极其重要的。

短路赋能设计（上电脱扣原理）		强制打开触点设计（断电脱扣原理）
4 线型	电阻型	
		
防护设备激活时形成一个短路。在 4 线型中，电路为短路状态（电阻仅有几欧姆）。而在电阻型中则有一个设定电阻（大约几千欧姆）。这些设计需要更复杂的评估（算法）。		这种设计更为广泛，也具有一些优点。用在一个安全开关上时，防护设备的触发会打开一个开关触点。以特殊方式进行布线可以排除短路的可能。

➜ 压敏防护设备设计：B 类标准 EN 1760 -1/-2

脚踏开关

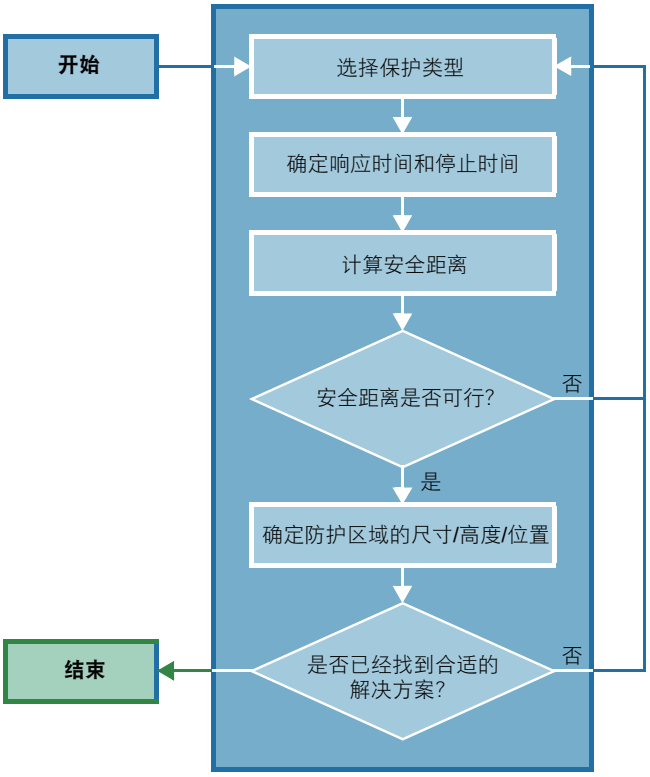
脚踏开关用于启动和停止工作过程。脚踏开关只能用于某些采用独立工作模式运行机器（如压机、冲床、折弯机和金属加工机器等）以实现安全功能，并且只能与其他防护措施（例如低速度）联合使用。尽管如此，脚踏开关也需要经过特殊设计：

- 采用一个防护盖以防止无意触发
- 采用与使能开关原理类似的三段式设计（见上文）
- 当执行器在压力点之上触发时，能够手动复位
- 在危险运动停止之后，仅当脚踏开关已经释放并重新触发后，才允许用脚重新启动。
- 至少使用一个常开触点和一个常闭触点
- 如果有多个操作员，那么每个人都应该配备一个脚踏开关

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

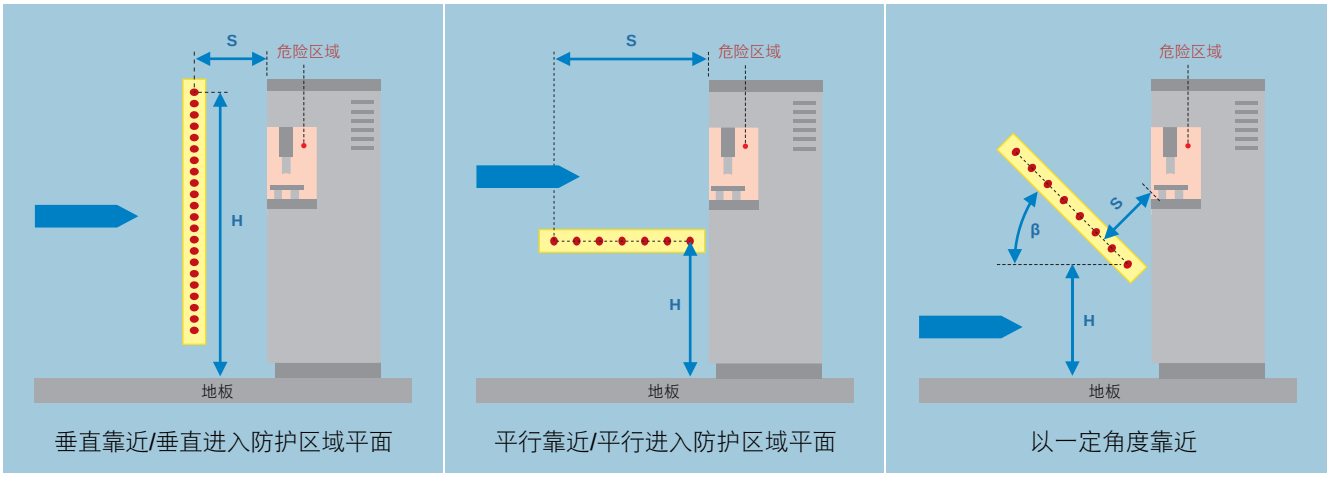
防护设备的布置/尺寸确定

在选择最佳防护设备时，一个重要因素就是可用的空间。应该保证在到达危险地点之前就及时地消除危险状态。
必需的安全距离取决于许多因素，其中就包括防护设备的尺寸和类型。



ESPE 靠近时的安全距离

安全距离的评估适用于带二维防护区域的 ESPE 设备，例如光幕、光电开关 (AOPD) 的光电功能、激光扫描器 (AOPDDR) 或二维摄像头系统。总的来说，在这三种不同的接近方式之间需要进行区分。



垂直靠近/垂直进入防护区域平面　　平行靠近/平行进入防护区域平面　　以一定角度靠近

在选择好用于启动停机过程的 ESPE 后，应该计算 ESPE 的防护区域和最近的危险点之间的必需安全距离。
应该考虑以下参数：

- 机器的停止时间
- 安全相关控制器的响应时间
- 防护设备 (ESPE) 的响应时间
- 作为 ESPE 分辨率或接近类型功能的补充

如果最小距离过大，并且从人体工程学角度来说不可接受，那么应该减小机器停止的总时间，或者应该使用更小分辨率的 ESPE。应该禁止站在防护设备后面。

➜ 在 EN 999（后来的 EN ISO 13 855）标准（B 类标准）中对 ESPE 安全距离的计算进行了说明。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

通用计算公式
$S = (K \times T) + C$

在公式中：

- S 是从最近的危险点到 ESPE 检测点/检测线/检测面之间的最小距离，单位是毫米。
- K 是从人体或人体部位的靠近速度得出的一个参数，单位为毫米/秒。
- T 是整个系统的停机时间，单位是秒。
- C 是在防护设备触发之前进入危险区域的额外距离，单位是毫米。

下表包含了安全距离 S 的计算公式，S 是接近防护区域方式的一个函数。

垂直靠近			
β = 90° (±5°) d ≤ 40 mm	S = 2000 × T + 8 × (d – 14) 如果 S > 500 mm, 则使用以下公式: S = 1600 × T + 8 × (d –14)。 在此情况下，S 不能小于 500 mm。	安全距离 S 不应小于 100 mm。	
40 < d ≤ 70 mm	S = 1600 × T + 850	底部光束高度 ≤ 300 mm。 顶部光束高度 ≥ 900 mm。	
d > 70 mm		光束数量	建议高度
多光束	S = 1600 × T + 850	4	300, 600, 900, 1200 mm
		3	300, 700, 1100 mm
		2	400, 900 mm
单光束	S = 1600 × T + 1200 只有在风险评估或 C 类标准允许的情况下，才能使用单光束保护。	1	750 mm
平行靠近			
β = 0° (±5°)	S = 1600 × T + (1200 – 0.4 × H) 其中 (1200 – 0.4 × H) > 850 mm		
以一定角度靠近			
5° < β < 85°	在 β> 30° 时，可参考垂直靠近所使用的公式。 在 β< 30° 时，可参考平行靠近所使用的公式。 那么 S 适用于高度 ≤ 1000 mm 且距离最远的光束。	$d \le \frac{H}{15} + 50$ 是就底部光束而言的。	

S：最小距离
H：防护区域高度（检测平面）
d：ESPE 分辨率
β：在检测平面和进入方向之间的角度
T：整个系统的停机时间

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

特殊情况

压机应用

与一般标准不同，机器特定的 C 类标准具有特殊的要求。

压机距离裕量的计算		
ESPE 的分辨率 d (mm)	**裕量 C (mm)**	**通过 ESPE/PSDI 模式启动回程**
d ≤ 14	0	允许
14 < d ≤ 20	80	
20 < d ≤ 30	130	
30 < d ≤ 40	240	不允许
> 40	850	

➜ 压机标准：EN 692/693（C 类标准）

ESPE 用于存在检测

对于可以从地面进入访问的大型系统，建议使用此类保护。在此特殊情况中，如果有操作员处在机器内部，则应防止机器的启动（安全功能：**防止启动**）。这是一个次要防护设备。在此情况下，应计算主要防护设备（如用于停止机器的光幕）的安全距离。次要防护设备（具有水平的防护区域）用于检测机器中是否有人存在 — 当机器内有相关人员存在时，它会防止机器的启动。

车辆上的移动应用

如果车辆出现了危险状态，那么通常使用车辆的速度（而不是人的靠近速度）来计算安全距离。

如果车辆（包括防护设备）和人相互靠近，那么通常情况下人会意识到危险，从而停止前进或离开。因此安全距离需要设置得足够大，以确保车辆能够安全停止。

对于某些采用特定技术的应用来说，安全裕量可能是必需的。

移动 ESPE 应用

对于某些机器来说，由于相关的操作要求，操作人员需要离危险区域很近。在压机的制动器中，小制动片应该放置在与弯曲边沿非常接近的地方。

事实证明，实际的防护设备是一个运动系统，它能够在工具开口四周形成防护区域。由于此类情形中并没有考虑手的靠近速度，所以通用的计算公式并不适用。

由于对分辨率的要求非常高，因此应该防止出现金属表面的反射问题。可以采用基于基于摄像原理的激光安全防护系统。这类保护在 C 类标准中进行了定义，是与其他防护措施（例如 3 段式脚踏开关、自动停机时间测量、佩戴手套需求等）相联系的。

➜ 使用移动 ESPE 的折弯机的安全标准： prEN12622（C 类标准）

停机时间和必需安全距离的测量需要特殊的技术知识和设备。SICK 公司可以为您提供测量服务。

3 C

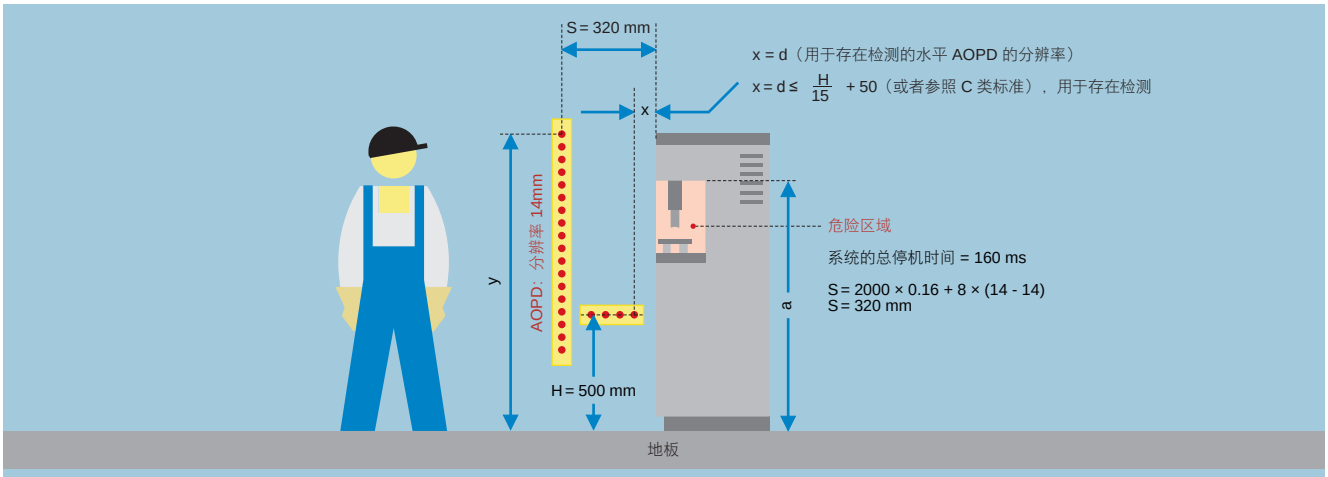
© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

安全距离计算的示例

方案 1：垂直安装 — 带存在检测的危险点保护

如图所示，计算出的结果是安全距离 S = 320 mm。此处使用了具有最高分辨率的安全光幕，因此得到的是最优的安全距离。

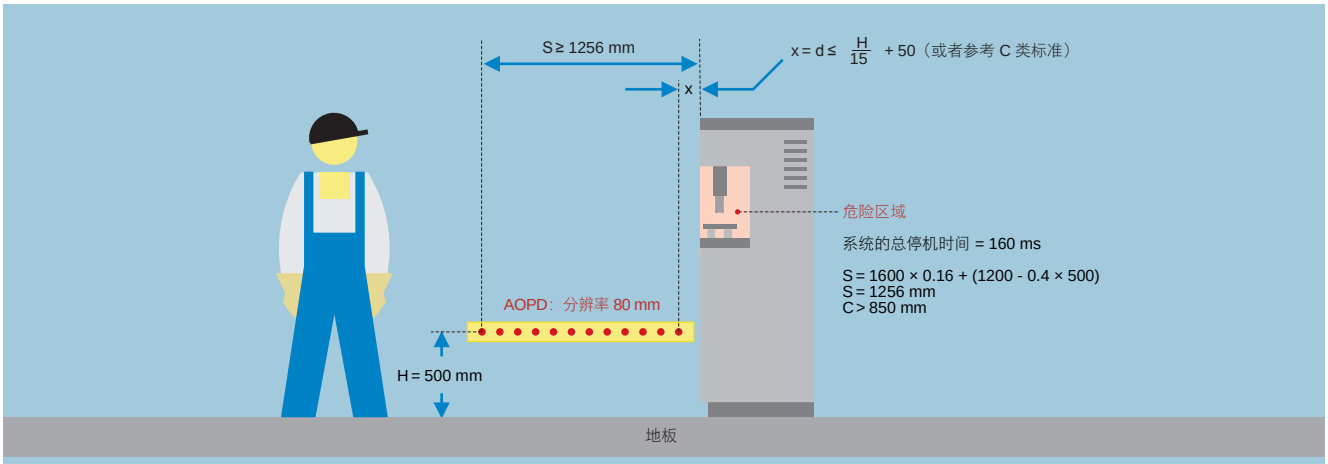
为了保证能够检测到危险区域内任何位置的人，此处使用了两个 AOPD：一个是垂直 AOPD，位于所计算出的安全距离（垂直靠近）处；另一个是水平 AOPD，用于消除站在垂直 AOPD 后面的危险情况。



a = 危险区域高度
d = 检测能力（AOPD 的分辨率）
H = 安装高度
S = 安全距离
x = 防护区域端线到机器的距离
y = 顶部光束的高度，关于安全距离计算的信息请参见第 334 页的“必需的防护区域尺寸/ESPE 高度”

方案 2：平行安装 — 危险区域保护

该方案采用水平 AOPD。下图所示为安全距离 S 的计算和 AOPD 的定位。如果 AOPD 的安装高度增加到 500 mm，那么安全距离就会减小。针对此高度，可使用分辨率小于或等于 80 mm 的 AOPD。但是仍需确保不能访问 AOPD 下方的危险区域。此类保护通常使用 AOP-DDR（激光扫描器）实现。然而，由于技术方面的一些原因，应该为这些设备设置一定的裕量距离。

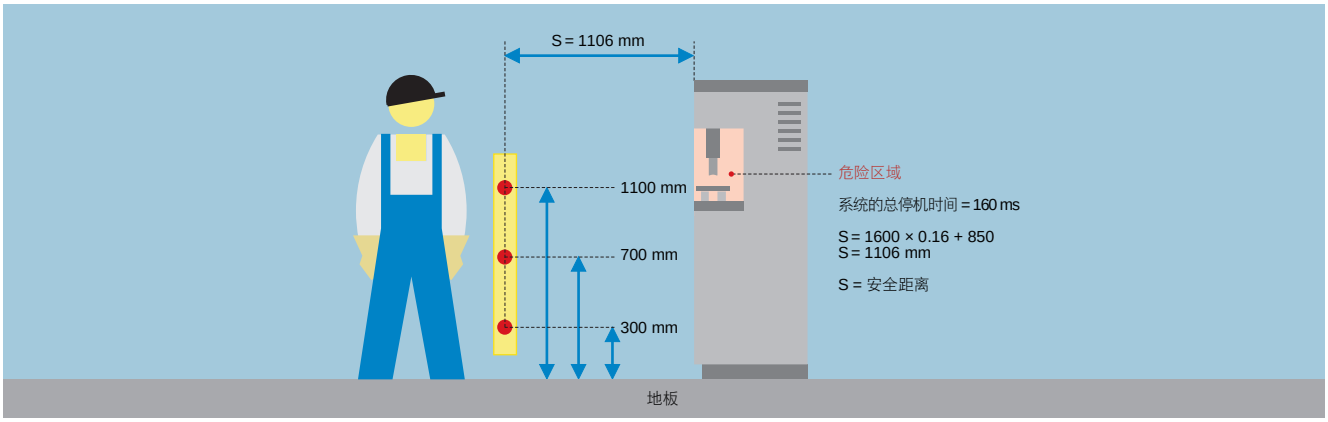


C 是指防护设备触发前距离危险区域入口的距离，单位是毫米
d = 检测能力（AOPD 的分辨率）
H = 安装高度
S = 安全距离
x = 防护区域端线到机器的距离

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

方案 3：访问保护

使用三束光（高度分别为300 mm、700 mm和1100 mm）进行访问保护时，允许垂直方向的靠近。使用此方案时，如果操作员站在危险区域和AOPD之间，系统是检测不出来的。因此，需要采取额外的安全措施以降低这种风险。控制设备（例如复位按钮）应该放置在能够看到整个危险区域的地方。从危险区域内不能触及到按钮。



结果综述

下表所示为采用这些方案的结果。具体的操作要求决定了方案的选择使用：

解决方案 用于停止/停机时间=160ms的情况		优点	缺点
1	**危险点保护** **S = 320 mm**	■由于操作员距离工作过程更近（短路径），因此生产率更高 ■可以实现自动启动或 PSDI 模式 ■所需空间小	■由于分辨率更高且具有存在检测功能，因此防护设备价格更高
2	**危险区域保护** **S = 1256 mm**	■可以自动启动 ■访问时不受危险区域高度的影响	■操作员距离更远（远距离） ■需要更大的空间 ■生产率更低
3	**访问保护** **S = 1106 mm**	■最经济的方案 ■访问时不受危险区域高度的影响 ■使用偏转镜可以对多侧进行保护	■操作员距离更远（远距离） ■生产率更低（总是需要复位 ESPE） ■已经考虑到站到防护设备后面的风险。如果工作场所有多人工作，则不建议采用此方案

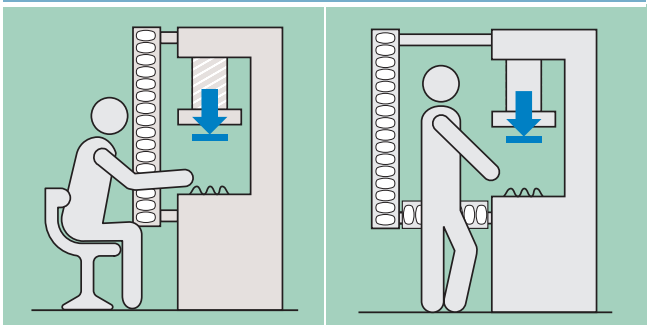
© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

ESPE 必需的防护区域尺寸/高度

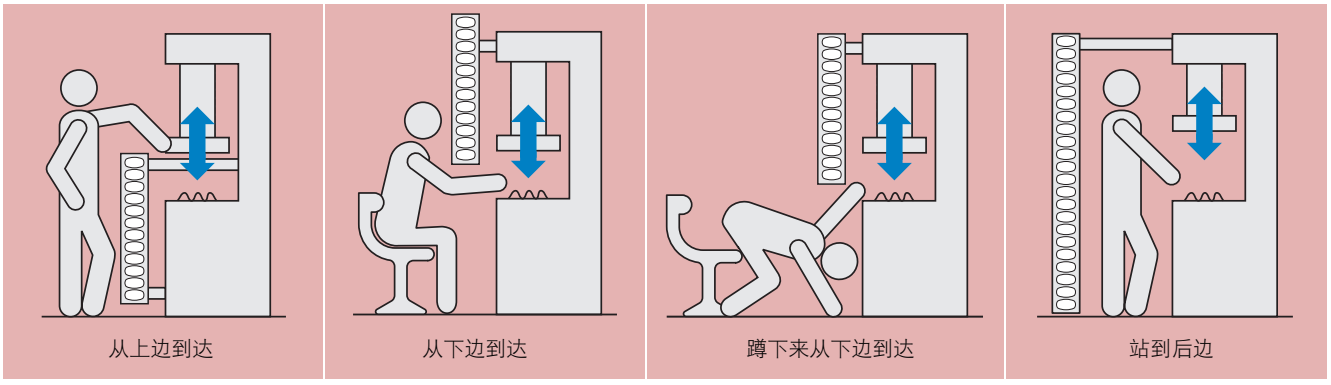
一般来说，在安装防护设备时应该排除以下错误可能：

- 应该确保只有通过防护区域才能到达危险地点。
- 尤其不能从上边/下边/周围到达危险地点。
- 如果能够站到防护设备后边，那么需要采取额外的措施（例如重启互锁、次要防护设备）。

正确安装的示例



危险的安装错误示例



计算出防护区域和最近的危险点之间的最小安全距离后，下一步就是确定防护区域的高度。通过这种方式可以保证不会从上边到达危险地点。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

ESPE 所必需的防护区域高度（根据 prEN ISO 13855 标准）

危险区域高度 a (mm)	到危险区域的水平距离 c (mm)											
2600	0	0	0	0	0	0	0	0	0	0	0	0
2500	400	400	350	300	300	300	300	300	250	150	100	0
2400	550	550	550	500	450	450	400	400	300	250	100	0
2200	800	750	750	700	650	650	600	550	400	250	0	0
2000	950	950	850	850	800	750	700	550	400	0	0	0
1800	1100	1100	950	950	850	800	750	550	0	0	0	0
1600	1150	1150	1100	1000	900	850	750	450	0	0	0	0
1400	1200	1200	1100	1000	900	850	650	0	0	0	0	0
1200	1200	1200	1100	1000	850	800	0	0	0	0	0	0
1000	1200	1150	1050	950	750	700	0	0	0	0	0	0
800	1150	1050	950	800	500	450	0	0	0	0	0	0
600	1050	950	750	550	0	0	0	0	0	0	0	0
400	900	700	0	0	0	0	0	0	0	0	0	0
200	600	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0
	所得到的防护区域顶端高度 b (mm)											
	900	**1000**	**1100**	**1200**	**1300**	**1400**	**1600**	**1800**	**2000**	**2200**	**2400**	**2600**

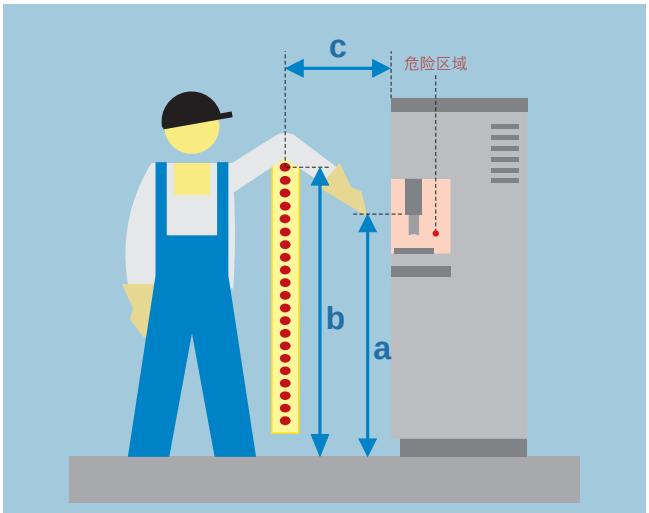
对于此安全距离，应按以下步骤确定必需的防护区域顶端高度：

1. 确定危险点高度 a 并在左列中找到该值，例如 1000 mm。
2. 在此行中找到水平距离 c 小于所计算出的安全距离的第一列，例如值为“0”的第一个字段。
3. 读出最后得到的防护区域距离地板的顶端高度 b，例如底行的 1600 mm。

示例：

所计算出的防护区域和最近的危险点之间的安全距离为 240 mm。

在此例中防护区域顶端高度应该为 1600 mm，以保证不能从上边到达危险点。如果防护区域是从参考平面之上 700 mm 处开始的，那么可以使用一个防护区域高度为 900 mm 的光幕。



用于确定所必需的防护区域高度的参数

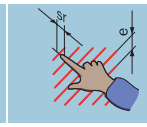
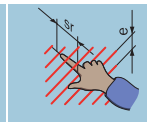
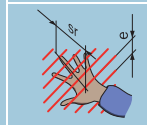
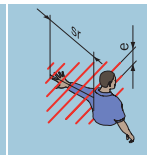
➜ 在本文即将印刷的同时，我们正在制订一个符合 prEN ISO 13855 标准的特殊表格，以用于确定 ESPE 所必需的防护区域高度。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

物理防护设备的安全距离

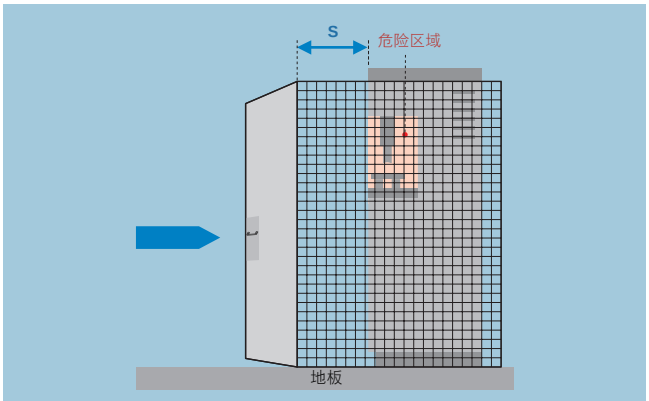
如果物理防护设备上有开口，那么这些设备应该距离危险区域足够远。当防护设备、机器框架或紧固板上存在开口时该要求同样适用。

物理防护设备的安全距离（与开口大小的函数关系）

身体部位		开口大小 e (mm)	安全距离 (mm)		
			槽形	方形	圆形
指尖		e ≤ 4	≥ 2	≥ 2	≥ 2
		4 < e ≤ 6	≥ 10	≥ 5	≥ 5
手指到手腕之间		6 < e ≤ 8	≥ 20	≥ 15	≥ 5
		8 < e ≤ 10	≥ 80	≥ 25	≥ 20
		10 < e ≤ 12	≥ 100	≥ 80	≥ 80
		12 < e ≤ 20	≥ 120	≥ 120	≥ 120
		20 < e ≤ 30	≥ 850	≥ 120	≥ 120
手臂到肩膀之间		30 < e ≤ 40	≥ 850	≥ 200	≥ 120
		40 < e ≤ 120	≥ 850	≥ 850	≥ 850

互锁物理防护设备的安全距离

对于用于触发停机的互锁物理防护设备来说，它应该采用和 ESPE 类似的步骤以保持一定的安全距离。也可以使用锁定设备进行互锁以实现防护，直至不再存在任何危险。



互锁物理防护设备的安全距离

通用计算公式

$$S = (K \times T)$$

在公式中：

- **S** 是从最近的危险点到下一个门开口点的最小距离，单位为毫米。
- **K** 是由人体或人体某部位的靠近速度得出的参数，单位为毫米/秒，一般为 1600mm/s。
- **T** 是整个系统的停机时间，单位为秒。

➜ 互锁物理防护设备的安全距离计算标准：EN 999，prEN ISO 13855（B 类标准）

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

物理防护设备所必需的高度

与 ESPE 类似，物理防护设备也采用同样的步骤确定其必需的高度。根据潜在危险的不同，应该使用不同的计算表格。

为避免在物理防护设备下边爬行通过，防护设备通常需要位于参考平面 200mm 以上。

潜在危险较低时物理防护设备所必需的高度（根据 pr EN ISO 13857 标准）

危险区域高度 a (mm)	到危险区域的水平距离 (mm)								
2500	0	0	0	0	0	0	0	0	0
2400	100	100	100	100	100	100	100	100	0
2200	600	600	500	500	400	350	250	0	0
2000	1100	900	700	600	500	350	0	0	0
1800	1100	1000	900	900	600	0	0	0	0
1600	1300	1000	900	900	500	0	0	0	0
1400	1300	1000	900	800	100	0	0	0	0
1200	1400	1000	900	500	0	0	0	0	0
1000	1400	1000	900	300	0	0	0	0	0
800	1300	900	600	0	0	0	0	0	0
600	1200	500	0	0	0	0	0	0	0
400	1200	300	0	0	0	0	0	0	0
200	1100	200	0	0	0	0	0	0	0
0	1100	200	0	0	0	0	0	0	0
	所得到的防护区域顶端的高度 b (mm)								
	1000	**1200**	**1400**	**1600**	**1800**	**2000**	**2200**	**2400**	**2500**

3 C

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

潜在危险较高时物理防护设备所必需的高度（根据 pr EN ISO 13857 标准）

危险区域高度 a (mm)	到危险区域的水平距离 (mm)									
2700	0	0	0	0	0	0	0	0	0	0
2600	900	800	700	600	600	500	400	300	100	0
2400	1100	1000	900	800	700	600	400	300	100	0
2200	1300	1200	1000	900	800	600	400	300	0	0
2000	1400	1300	1100	900	800	600	400	0	0	0
1800	1500	1400	1100	900	800	600	0	0	0	0
1600	1500	1400	1100	900	800	500	0	0	0	0
1400	1500	1400	1100	900	800	0	0	0	0	0
1200	1500	1400	1100	900	700	0	0	0	0	0
1000	1500	1400	1000	800	0	0	0	0	0	0
800	1500	1300	900	600	0	0	0	0	0	0
600	1400	1300	800	0	0	0	0	0	0	0
400	1400	1200	400	0	0	0	0	0	0	0
200	1200	900	0	0	0	0	0	0	0	0
0	1100	500	0	0	0	0	0	0	0	0
	所得到的防护区域顶端的高度 b (mm)									
	1000	1200	1400	1600	1800	2000	2200	2400	2500	2700

对于此安全距离，应按以下步骤确定必需的防护区域顶端高度：

1. 确定危险点高度 **a**，并在左列中找到该值，例如 1000 mm。
2. 在此行中找到水平距离 **c** 小于所计算出的安全距离的第一列，例如值为“0”的第一个字段。
3. 读出底行中物理防护设备的高度 **b**，例如高风险时为 1800 mm。

潜在危险较高的示例

物理防护设备应该位于参考平面以上 200 mm 至 1800 mm 处。如果防护设备的顶端位于 1600 mm 处，那么安全距离应该增加到至少 800 mm。

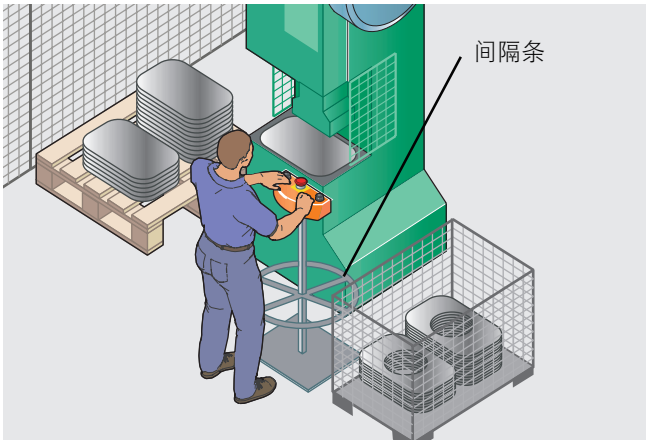
➜ 安全距离和必需的防护区域高度：EN ISO 13857

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

固定位置防护设备的安全距离

示例：双手控制设备的安全距离

$$S = (K \times T) + C$$



在公式中：

- **S** 是从控制设备到最近危险点的最小距离，单位为毫米。
- **K** 是由人体或人体某部位的靠近速度得出的参数，单位为毫米/秒，一般为 1600mm/s。
- **T** 是整个系统的停机时间，从控制设备被释放后开始测量，单位为秒。
- **C** 是一个补充因子：250 mm。在某些情况（例如被遮盖时）下可能并不需要。

如果双手控制设备安装在便携底座上，则应使用间隔条或有限长度的线缆（防止操作员将控制设备带到不允许使用的地方），以保证必需的安全距离。

➜ 安全距离计算：EN 999，prEN ISO 13855（B 类标准）

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

防护设备在控制系统中的集成

和其他机械部件一样，防护设备也应该集成到控制系统中。

“控制系统作为机器信息系统的组成部分，是实现逻辑功能的功能性组件。它们根据任务的具体要求将物料和能量调节到不同的工具和工件系统的操作区域中。[...]当采用的技术不同时，控制系统也是不同的。比如，根据信息载体的不同，可以分为流体、电气和电子控制系统。”

以上内容译自：Alfred Neudörfer, Konstruieren sicherheitsgerechter Produkte, Springer Verlag, Berlin u.a., ISBN 9783540212188（2005 年第三版）。
（英文版“安全机器的设计”计划 2010 年出版：ISBN9783540357919）

控制系统作为一个总称，描述的是一个**控制系统**的整个系列组成部分。控制系统包括一个输入元件、逻辑单元、功率控制元件以及执行器/工作元件等。

控制系统的安全相关部分应该执行安全功能。因此对它们的可靠性和抗故障能力有特殊的要求。它们基于一定的原理进行控制，并防止故障的发生。

控制系统			安全相关因素	
控制系统的运行原理		**典型部件**	**干扰因素**	**说明**
流体	气动 	■ 多路阀 ■ 排气阀 ■ 手动关闭阀 ■ 带脱水器的过滤器 ■ 软管	■ 能量强度的改变 ■ 压缩空气的纯度和含水量	通常设计为电—气控制系统 需要检修设备对压缩空气进行调节。
	液动 	■ 蓄能器 ■ 限压器 ■ 多路阀 ■ 过滤器 ■ 液位计 ■ 温度表 ■ 软管和电缆 ■ 螺纹配件	■ 纯度 ■ 黏度 ■ 加压流体的温度	通常设计为电—液控制系统 必须采取措施以限制系统中的压力和温度，并对媒质进行过滤。

电气	机电 	■ 控制开关：
		  ■ 位置开关
		  ■ 选择开关
		  ■ 按钮
		■ 开关设备：
		  ■ 接触器
		  ■ 继电器
		  ■ 断路器
			■ 设备防护等级
			■ 部件和设备的选择、尺寸确定和布置
			■ 电缆的设计和布线
				当选择得当时，由于它们本身的设计以及明确的开关位置等因素，部件对潮湿、温度波动和电磁干扰等都是不敏感的。

	电子 	■ 单独部件，例如：
		  ■ 三极管
		  ■ 电阻
		  ■ 电容
		  ■ 线圈
		■ 高度集成部件，如集成电路 (IC)
			和“机电”中相同。
			其他还包括：
			■ 温度波动
			■ 通过电缆或磁场感应的电磁干扰
				不可能排除故障。只有遵循控制系统准则（而不是部件选择）才能实现可靠的动作。

	微处理器控制 	■ 微处理器
		■ 软件
			■ 硬件安装故障
			■ 包括共模故障的系统故障
			■ 编程错误
			■ 应用错误
			■ 运行错误
			■ 恶意病毒
				■ 预防故障的措施：
				  ■ 结构化设计
				  ■ 程序分析
				  ■ 模拟
				■ 控制故障的措施：
				  ■ 冗余硬件和软件
				  ■ RAM/ROM 测试
				  ■ CPU 测试

以上内容译自：Alfred Neudörfer, Konstruieren sicherheitsgerechter Produkte, Springer Verlag, Berlin u.a., ISBN 9783540212188（2005 年第三版）。
（英文版“安全机器的设计”计划 2010 年出版：ISBN9783540357919）

在上述关于安全传感器（防护设备）的描述中已经对安全相关输入元件进行了说明。因此，下文仅对逻辑单元和执行器进行说明。执行器安全因素的评估可以参考对功率控制元件安全因素的评估。执行器/工作元件中的故障和失效可能通常已被排除。（无电能的电机切换到无危险状态。）

流体控制系统通常设计为电—气或电—液控制系统。举例来说，电气信号通过阀门转换为流体能量，以移动气缸和其他执行器。

➜ 您可以登录 http://www.sick.com/ 查找关于防护设备集成的接线图。

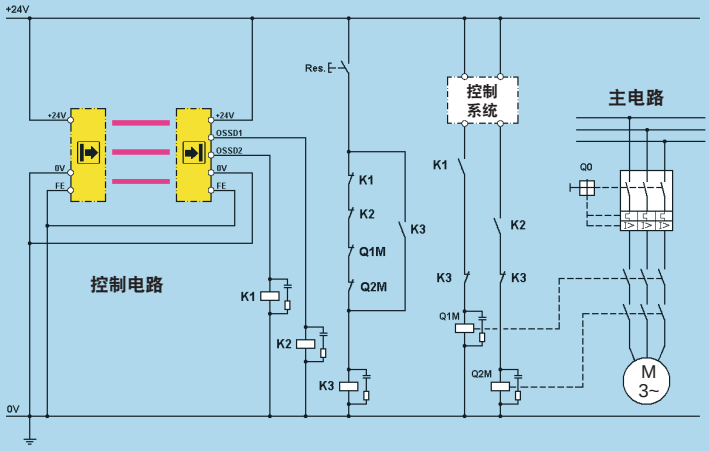
© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

逻辑单元

在逻辑单元内安全功能的不同输入信号被连接到一起以组成输出信号。出于这种考虑可以使用机电、电子或可编程电子部件。

警告：防护设备的信号不能只由标准控制系统 (PLC) 来处理，它们还必须通过平行的切断路径。

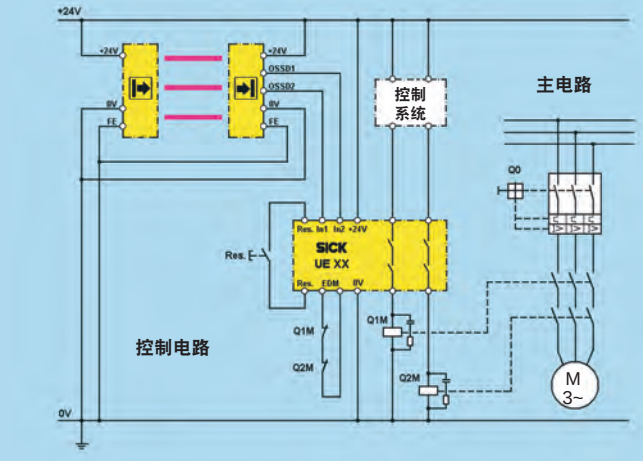
独立接触器组成的逻辑单元



使用带强制断开触点的单独辅助接触器，可以设计任何复杂等级的控制系统。这种安全原理的特征就是通过强制断开触点实现冗余和监控。通过布线可以实现逻辑操作。

功能：如果接触器 K1 和 K2 断电，按下 S1 时接触器 K3 会上电并保持上电状态。如果在有效防护区域内没有检测到任何物体，那么输出 OSSD1 和 OSSD2 是高电平。K3 上的常开触点会将 K1 和 K2 接触器上电并将它们自身锁存起来。释放 S1 按钮可以使 K3 断电。仅在此时输出电路闭合。当检测到有效防护区域内存在物体时，OSSD1 和OSSD2 输出将使 K1 和 K2 接触器断电。

带安全继电器组合的逻辑单元（安全继电器）



安全继电器将一个或多个安全功能集成在一个外壳中。它们一般都具有自监控功能。切断路径可以使用触点或半导体器件实现。它们也可以有信号触点。

经过认证的安全继电器不仅使复杂的安全应用更为简化，而且还减少了安全功能的验证工作。

在安全继电器中，半导体元件可以代替继电器执行机电开关元件的任务。动态信号传输和多通道信号处理（带错误检测功能）等开关技术可以保证纯电子解决方案的可靠运行。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

带基于软件的部件的逻辑单元

与自动化技术类似，安全技术已经从硬连线的辅助接触器，经由安全继电器、参数可设置的可配置安全逻辑设备，发展到复杂的、可自动防故障的 PLC。“经过验证的部件”和“经过验证的安全原理”等概念也开始应用到电气和可编程电子系统。

在此，安全功能的逻辑运算是使用软件实现的。

软件和硬件不同，硬件是由控制系统制造商开发和认可的；同时软件和实际的安全应用也不同，安全应用是由机器制造商使用硬件支持的语言开发出来的。

参数设置

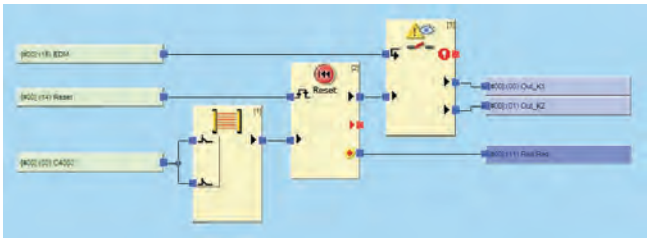
在调试时，使用选择开关/软件参数从一个定义的功能库中选择属性，

具有以下特征：逻辑简单，与/或逻辑

配置

认证逻辑设备(带编程接口)上已定义功能块的灵活运算功能，对时间等进行参数化，对控制系统上输入/输出进行配置，

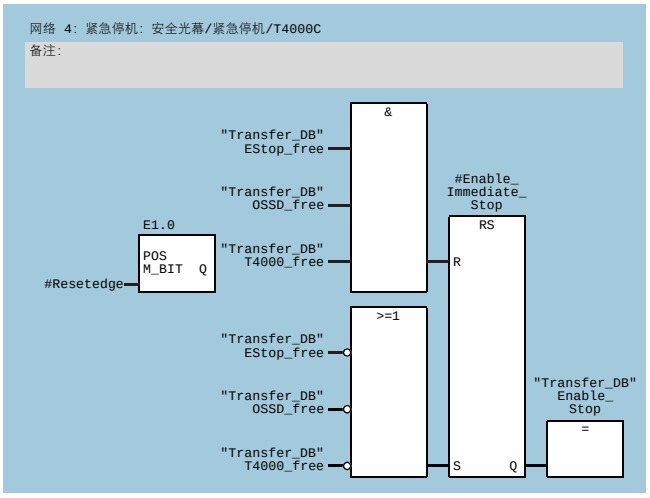
具有以下特征：可实现复杂逻辑功能，二进制逻辑



编程

按照要求使用由预定义编程语言定义的功能性来设计逻辑设备，通常使用经过认可的功能块，具有以下特征：

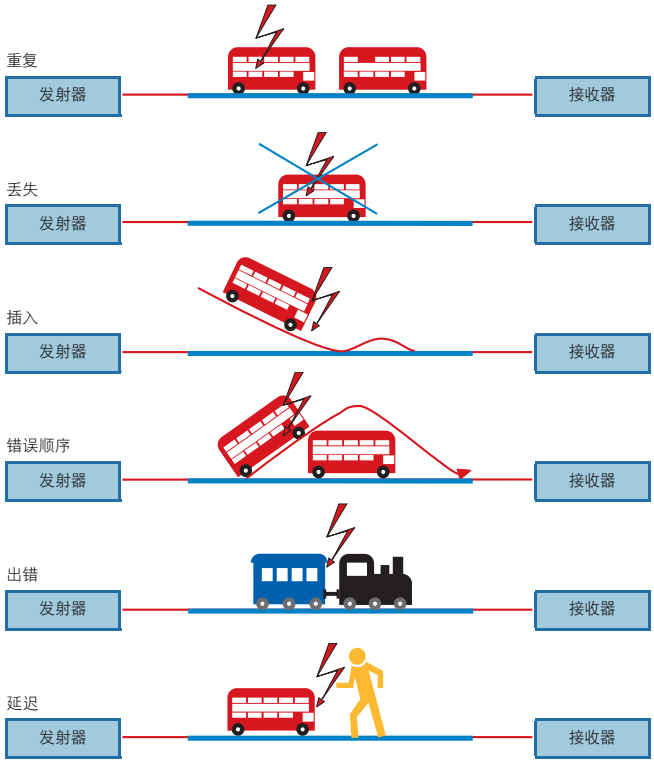
可实现复杂逻辑功能



可靠的数据传输

总线系统用于在机器上的控制系统和传感器或执行器之间传输信号。总线系统负责控制系统不同部分之间的状态传输。总线系统使布线更为简便，因此减少了可能发生的错误。推荐使用安全相关应用中已经确立的总线系统。

对硬件和软件中不同故障和错误的详细研究显示，这类故障在总线系统中出现较少的相同传输错误中较为常见。



来源：Sicherheitsgerechtes Konstruieren von Druck- und Papierverarbeitungsmaschinen — Elektrische Ausrüstung und Steuerungen; BG Druck- und Papierverarbeitung；2004 年第 6 版；第 79 页

在高级控制系统中可以针对上述传输错误采取多种措施，如安全相关消息的顺序编号、为带确认功能的接受信息规定时间等。所使用的基于现场总线的协议扩展包括这些措施。

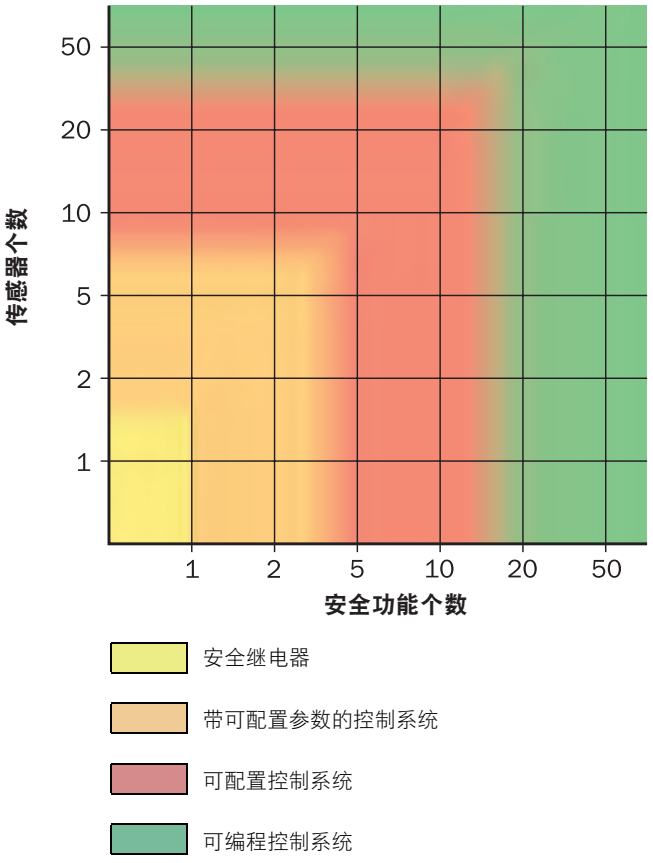
在 ISO/OSI 层模型中，它们在传输层之上起作用，从而将现场总线及其所有部件作为“黑色通道”来使用（不进行任何修改）。下列总线系统均为安全的总线系统：

- AS-i Safety at Work
- DeviceNet Safety
- PROFIsafe

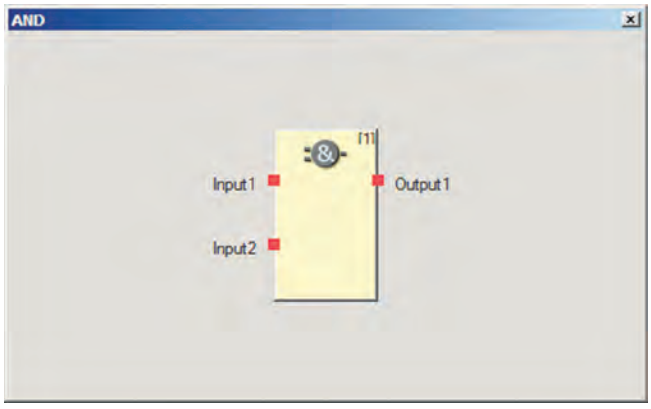
© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

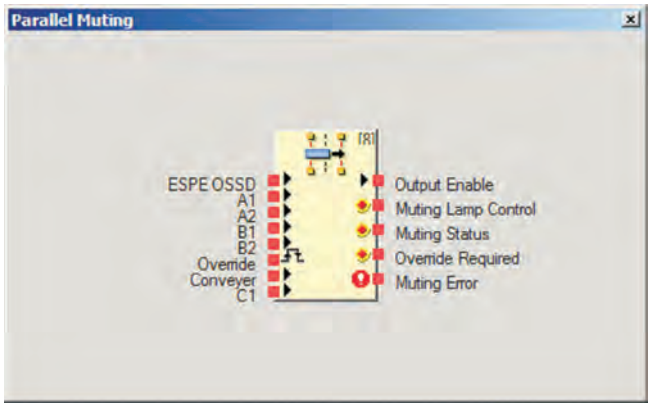
选择标准

控制系统的选择标准是先确定所要实现的安全功能个数以及输入信号上的逻辑运算范围。



逻辑运算的功能性（例如简单的“与”运算、触发器以及诸如功能抑制等特殊功能）也会对控制系统的选择造成影响。





软件规范

为了防止出现危险状态，尤其应该对基于软件的逻辑单元进行特殊设计以有效防止产生逻辑故障。为了检测系统故障，必须由开发者以外的其他人对其进行彻底的系统检查。此种情况下采用的是由第二人进行复查的原则。

安全功能应该由具有特定规范的基于软件的方案来实现。这个规范应该是完整的、没有矛盾的、可阅读且可扩展的。推荐在项目执行的过程中对这些内容进行一次检查。

如果程序的文档拙劣且不规范，那么之后更改时就会产生错误（尤其存在未知不可靠风险时），这就是所谓的副作用。良好的规范和程序文档具有强大的防错效果，尤其是在软件不是由自己开发的情况下。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

功率控制部件

由防护设备和逻辑单元触发的安全功能应该能够停止危险的运动。因此，执行器元件/工作元件由功率控制元件关闭。

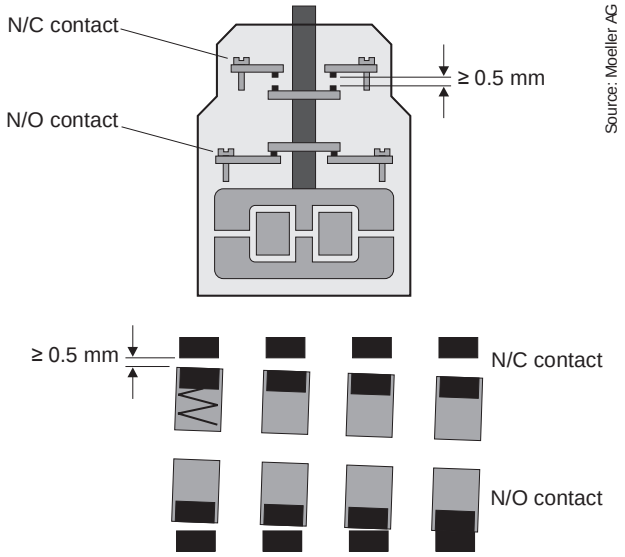
➜ 关闭/断电原理：EN ISO 13849-2（B 类标准）

接触器

最为常见的功率控制元件类型就是机电接触器。通过采用特殊的选择标准、布线方式和措施，一个或多个接触器可以组成安全功能子系统。接触器是经过认证的部件，可以通过防止过流、短路、规格过大（通常因子为 2）或其他措施来保护触点。为了对接触器进行安全功能诊断，输出状态的清晰反馈是必需的。使用带强制断开触点的接触器可以实现这一要求。当一组触点中的触点通过机械方式连接起来时，触点是被强制断开的，这样在整个使用寿命期间常开触点和常闭触点始终不会同时关闭。

“强制断开触点”这个术语主要指的是辅助接触器和辅助触点。即使出现故障事件（焊接触点）时，也要保证常闭触点之间至少有 0.5 mm 的规定距离。就像在开关容量较小 (<4kW) 的断路器上一样，主触点元件和辅助触点元件之间基本上没有区别，因此在小断路器上也可以使用“强制断开触点”这个称呼。

在较大的断路器上，则使用所谓的“镜像触点”：当接触器上所有主触点闭合时，不允许任何镜像触点（辅助常闭触点）闭合。镜像触点的一个典型应用就是在机器的控制电路内对接触器的输出状态进行高度可靠的监控。



Source: Moeller AG

抑制器

电感器（如阀门或接触器上的线圈等）应该配备一个抑制器，以在关闭时限制暂态电压尖峰。通过这种方法可以对开关元件进行过载保护，尤其能对特别灵敏的半导体进行过压保护。一般来说，这样的电路对释放延时也有影响。用于电弧抑制的简单二极管可以使释放时间延长 14 倍。

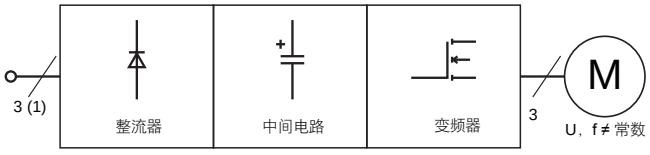
抑制器（跨接电感）	二极管	二极管组合	变阻器	RC 元件
过压	++	+	o	+[1)]
释放延时	- -	o	+	+[1)]

1) 必须根据电感正确选择使用的元件！

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

伺服放大器和变频器

在驱动技术领域，带变频器的三相驱动系统已经大范围地取代了直流驱动系统。变频器通过固定的三相电源可以产生出频率和振幅可变的输出电压。根据变频器类型的不同，稳压整流器在制动期间通过中间电路将获得的能量回馈到电网。整流器将电网提供的能量储存在直流中间电路中。为了实现所需的控制功能，变频器使用脉宽调制和半导体开关形成一个合适的电机旋转磁场。常用的开关频率为 4 kHz 到 12 kHz 之间。



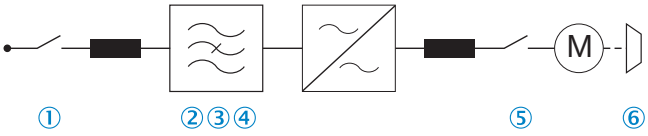
核对清单

- 变频器是否配有电源滤波器?
- 逆变器上的输出电路是否配有正弦滤波器?
- 连接电缆是否已屏蔽且尽可能地短?
- 是否使用大面积连接将部件和屏蔽接地/PE?
- 是否串联有整流斩波器以限制尖峰电流?

为了限制在直流和交流电路中开关负载造成的暂态过压，需要使用干扰抑制部件，尤其是在同样的控制柜中使用敏感电子组件的情况下。

伺服放大器和变频器上的安全功能

电源电压和电机之间有数个用于安全隔离的切断路径。



① 电源接触器 — 由于其重新上电时间很长，因此性能比较差；开通电流造成磨损较高。
② 控制器使能
③ 脉冲抑制“安全重启互锁（停机）”
④ 设定点
⑤ 电机接触器 — 不允许用于所有逆变器上
⑥ 保持制动 — 通常不是主制动

伺服驱动系统和变频器集成了越来越多的安全功能。

示例:

- STO — 安全转矩关闭 = 安全重启互锁
- SS1 — 安全停机 1 = 监控制动、STO 剩余时间或静止状态
- SS2 — 安全停机 2 = 监控制动，直到 SOS 为止
- SOS — 安全运行停机 = 通过位置控制实现安全运行停机
- SLS — 安全限定速度 = 安全限定速度
- SLI — 安全限定位置增量 = 安全限定步进大小

使用最多的功能是 STO。出于安全因素考虑，会使用一个单通道或双通道（取决于本身的设计）关闭逆变器的脉冲控制阶段。

当使用单通道时，应该采取额外的措施，以保证逆变器发生内部故障时的安全性。因此在控制系统中需要对反馈信号进行评估。

➜ 功率驱动系统的功能安全标准：EN 61800-5-2（B 类标准）

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

流体控制系统

阀门

所有的阀门都要求运动部件上具有圆柱导轨。阀门故障的常见原因：

- 回位弹簧故障
- 流体污染

实践证明，使用“经过安全相关应用验证的弹簧”是一条实用的安全准则。

阀门之间最重要的区别就是阀体的设计。

阀门关闭时座阀会与外壳上对应的底座啮合，并停止在某一固定位置上。使用磨削表面可以将流动路径完全封闭起来。

在活塞阀门上，阀体运动时经过缸筒/槽，从而关闭或打开流动路径。阀体从一个开关位置运动到另一个开关位置时两个位置间会有一定的交叉重叠，而决定这个重叠大小的闭合边缘就是控制边缘。为实现其功能，活塞和外壳间需要有一定的间隙，而该间隙会导致高压侧到低压侧的泄漏。

安全相关的设计准则

在安全相关的应用中使用阀门时，阀门位置的反馈是必需的。以下为常用的几种技术：

- 通过磁体（固定在运动阀体中）致动的磁簧开关
- 由运动阀体直接致动的感应式光电开关
- 运动阀体上的模拟行程测量
- 阀门之后的压力测量

如果阀门为电磁触发，则在需要接触器的同时还需要一个抑制器。

过滤器准则

绝大多数流体控制系统的故障都是由与流体污染相关的故障引起的。以下为流体污染的两个主要原因：

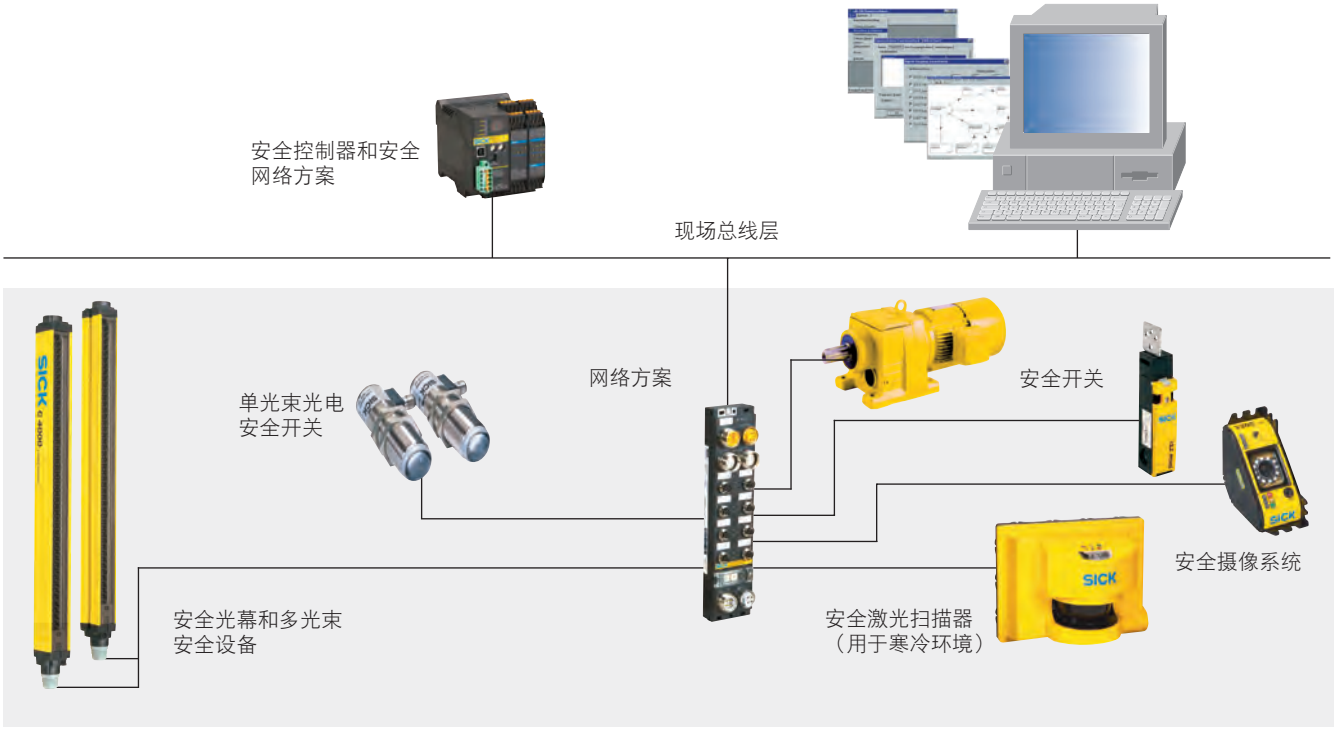
- 装配期间发生的污染 = 装配污染（例如，碎片、铸沙、布料纤维以及其他基础污染）
- 运行期间发生的污染 = 运行污染（例如环境污染、部件磨损）

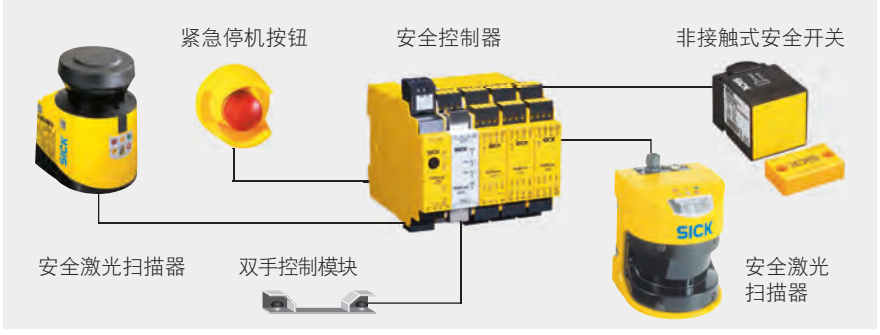
此类污染应该使用过滤器以将其降低到一个可接受的程度。过滤器准则包括为所需的任务选择合适的过滤器原理，以及将过滤器布置在合适的位置。过滤器应该能够过滤整个系统的污染物，从而在整个运行期间维持所需的纯度。

➜ 经过验证的安全原理：EN ISO 13849-2（B 类标准）
➜ 液动/气动系统上安全相关的要求：EN 982，EN 983
➜ 液动阀的老化过程：BIA-报告 6/2004

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

产品选型





配置和诊断软件

Safexpert®

机器和系统上的安全工程：安全的设计、风险评估和归档

➜ 您可以登录 http://www.sick.com/，使用产品搜索器在线查找所有的产品。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

总结：设计安全功能

基本原理

- 制订安全准则。在此过程中需要考虑机器特性、环境特性、人为因素、设计特性和防护设备特性等诸多方面。
- 安全功能通常由子系统传感器、逻辑设备和执行器组成。每个子系统的安全水平可以由以下安全相关的参数确定：结构、可靠性、诊断、抵抗力和过程。

防护设备的属性和应用

- 确定防护设备的必需属性。比如，您确实需要一个或多个电感式防护设备 (ESPE)、物理防护设备、移动式物理防护设备或者固定位置防护设备吗？
- 确定每个防护设备的正确安放位置和尺寸，尤其是相关防护设备的安全距离和必需防护区域大小/高度。
- 如操作指南所述集成防护设备，这也是保证安全等级所必需的。

逻辑单元

- 选择合适的逻辑单元，它是与安全功能数量和逻辑深度相关的。
- 使用经过鉴定的功能块，并保持一个清晰的设计思路。
- 彻底地核对设计和归档（采用由第二人进行复查的原则）。

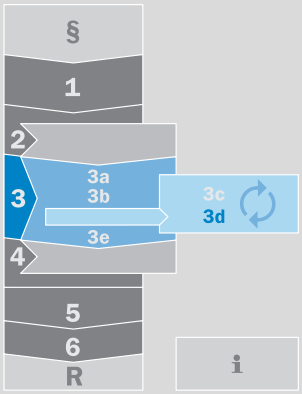
© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

第 3d 步：安全功能的核实

在核实期间，要分析和/或测试安全功能是否满足规范中目标和要求的所有方面内容。

核实主要包括两个部分：

- 机械安全的核实
- 功能安全的核实



核实防护设备的机械设计

对于机械防护设备，需要核对与危险地点的间距或与其隔离相关的要求，以及（如果必需的话）关于遮挡甩出部件或辐射的要求是否已经得到满足。尤其应该注意是否满足人体工程学的要求。

隔离和/或间距效果

- 足够的安全距离和尺寸（从上方和下方等）
- 合适的网孔尺寸或栅栏部件上的格栅间距
- 足够的强度和正确的安装
- 适当的材料
- 安全的设计
- 抗老化
- 防护设备的设计应该保证不能爬到防护设备上

遮挡甩出部件和/或辐射

- 足够的强度/抗冲击和抗断裂能力（遮挡能力）
- 对相关类型的辐射（特别是高温、寒冷等热能危险事件）有足够的遮挡能力
- 合适的网孔尺寸或栅栏部件上的格栅间距
- 足够的强度和正确的安装
- 适当的材料
- 安全的设计
- 抗老化

人体工程学要求

- 半透明或透明（监控机器的运行）
- 设计、颜色、美学
- 操作（重量，驱动等）

3 d

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

使用核对列表可以对防护设备的有效性进行彻底的核对：

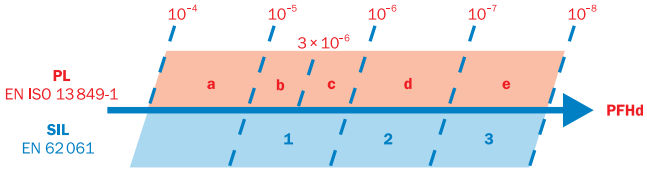
示例：制造商/安装人员安装防护设备（如 ESPE 设备）用的核对列表		
1.	是否能够有效防止人员进入危险区域/危险地点，并且只有先通过防护区域（ESPE/带互锁设备的物理防护设备）才能进入到危险区域/危险地点？	是 ☐ 否 ☐
2.	在保护危险区域/危险地点时是否已采取了适当措施以防止（机械保护）或监控危险区内不受保护的（人员）存在，是否针对设备可能被移除的情况对防护设备采取了安全加固措施？	是 ☐ 否 ☐
3.	是否已测量过机器的最大停机时间和停机/减速时间，并且已将测量值输入机器并归档至机器文档？	是 ☐ 否 ☐
4.	防护设备的安装位置是否和最近的危险地点间保持有必需的安全距离？	是 ☐ 否 ☐
5.	是否能够有效防止从下面/上面够到、从下面/上面爬过或从防护设备四周够到危险区域等情况？	是 ☐ 否 ☐
6.	设备/开关是否已经正确安装，调校后是否针对防止他人操作采取了安全紧固措施？	是 ☐ 否 ☐
7.	针对电击的防护措施是否有效（防护等级）？	是 ☐ 否 ☐
8.	用于复位防护设备或重启机器的控制开关是否存在并已正确安装？	是 ☐ 否 ☐
9.	用于防护设备的部件是否已按照制造商的说明集成到一起？	是 ☐ 否 ☐
10.	每次设置运行模式选择开关时，预设的防护功能是否有效？	是 ☐ 否 ☐
11.	在整个危险状态期间，防护设备是否都有效？	是 ☐ 否 ☐
12.	一旦危险状态出现以后，关闭防护设备、更改运行模式或切换到另一防护设备时危险状态是否会停止？	是 ☐ 否 ☐
13.	防护设备上是否贴有注意事项？操作员能否清晰看见？	是 ☐ 否 ☐

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

核实功能安全

基于功能安全标准，必需核对所需的安全等级是否与实际安全等级相匹配。可以使用两种不同的方法：

- 根据 ENISO13849-1 标准确定所达到的性能水平 (PL)
- 根据 EN62061 标准确定所达到的安全完整性等级 (SIL)



两种方法都要核对残留风险是否可以接受。此处所确定的 PFHd 值是一个量化参数。

在后面的例子中（➜ 3-57 和 ➜ 3-62）有传感器和逻辑设备的数据，但是没有执行器的数据。

- PL 性能水平：安全相关部件在预期条件下执行安全功能并降低风险的能力
- PFHd（危险性失效概率）：每小时发生危险故障的概率
- SILCL：SIL 要求限制（适用性）。用于定义安全功能完整性的离散等级

EN ISO 13849-1

传感器	逻辑设备	执行器
PL	PL	?

EN 62061

传感器	逻辑设备	执行器
PFHd（危险性失效概率）	PFHd（危险性失效概率）	?
SILCL	SILCL	?

根据 ENISO13849-1 标准确定所达到的性能水平 (PL)

1

EN ISO 13849-1标准包括两个用于确定性能水平的步骤：

- **简化步骤** (3➜52)：

基于子系统性能水平来确定性能水平的表格计算法

- **详细步骤** (3➜52)：

基于子系统 PFHd 值的性能水平计算方法。（此步骤仅在标准中进行了间接的说明。）

通常使用详细步骤计算出的性能水平比使用简化步骤计算出的结果更具可靠性。两种方法都考虑了用于实现性能水平的额外结构和系统因素。

子系统

由防护措施辅助实现的安全功能通常包括传感器、逻辑设备和执行器三部分。这样一系列部件包括物理防护设备互锁或阀门等分立元件，以及复杂安全控制器等。因此原则上必须为安全功能划分为子系统。

实际上，某些安全功能已经在使用一些被认可的子系统了。这些子系统包括是光幕、以及部件制造商已经标注有 PL 或 PFHd 值的安全控制器。这些数据仅在制造商规定的时间内有效。除可量化的因素外，对系统故障防护措施的核对也是必需的。

➜ 关于验证的更多信息：EN ISO 13849-2
➜ 您可以在 www.dguv.de/bgia/13849 找到关于使用 EN ISO 13849-1 标准进行验证的大量信息。

3 d

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

简化步骤

即使在每个 PFHd 值都未知的情况下，该步骤也能非常精确地估计出整体性能水平 (PL)。如果所有子系统的性能水平 (PL) 都是已知的，则利用下表可以确定安全功能所能实现的整体性能水平。

步骤

- 确定子系统安全功能的PL/最低PL：**PL（低）**
- 确定性能水平为PL（低）的子系统数量：**n（低）**

例 1:

- 当所有子系统的性能水平为“e”时，PL（低）就是“e”。
- 此时，达到该性能水平的子系统有 2 个（因此 n ≤ 2）。整体性能水平则为“c”。
- 使用这种方法时，如果再增加一个性能水平为“e”的子系统则会使整体性能水平降至“d”。

例 2:

- 如果其中一个子系统的性能水平是“d”，另外两个子系统是“c”时。则PL（低）为“c”。
- 此时，达到该性能水平的子系统有 2 个（因此 n ≤ 2）。整体性能水平则为“c”。

PL（低） （子系统的最低性能水平 PL）	n（低） （达到该性能水平的子系统个数）	PL PL（可以达到的最高PL）
a	> 3	-
	≤ 3	a
b	> 2	a
	≤ 2	b
c	> 2	b
	≤ 2	c
d	> 3	c
	≤ 3	d
e	> 3	d
	≤ 3	e

→ 如果所有子系统的性能水平 (PL) 都是未知的，则可以根据下文“根据 EN ISO 13849-1 标准确定子系统的安全等级”这一节的内容确定它们的安全等级。

详细步骤

对于确定性能水平 PL 来说，安全部件的“危险性失效概率 (PFHd)”是必不可少（但又不是唯一的）标准。所得到的 PFHd 值为所有单个 PFHd 值的总和。另外，整个评估期间还需考虑制造商对安全部件规定的结构限制等因素。

→ 即使所有子系统的 PFHd 值都是未知的，它们的安全等级也可以确定。请参见下文“根据 EN ISO 13849-1 标准确定子系统的安全等级”。

根据 EN ISO 13849-1 标准确定子系统的安全等级

一个安全相关的子系统可以由许多单独部件组成，这些单独部件也可能来自不同的制造商。例如：

- 输入侧：物理防护设备上的两个安全开关
- 输出侧：用于停止危险运动的一个接触器和一个变频器

在这些情况下，子系统的 PL 应该单独确定。

子系统所能达到的性能水平取决于以下参数：

- 结构以及故障条件下安全功能的行为（类别, → 3-53）
- 单独部件的 MTTFd 值 (→3-54)
- 诊断覆盖率 (DC, → 3-55)
- 共因失效 (CCF, →3-55)
- 安全相关软件因素
- 系统失效

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

控制系统安全相关部件的分类 (EN ISO 13849-1)

子系统通常采用单通道或双通道设计。对于单通道系统来说，出现故障时如不采取进一步措施，就会产生一个危险性的系统失效。使用额外测试部件或者能够互相测试的双通道系统可以检测故障。EN ISO 13849-1 标准对不同的结构进行了划分。

分类	简明要求	系统行为	实现安全的原理
B	对于控制设施的安全相关部件、防护设备以及其部件来说，它们的设计、制造、安装和组合都应该遵守恰当的标准，从而保证具有期望的承受能力。	■ 出现故障会导致安全功能的丧失。	主导因素是部件选择
1	应该满足 B 类要求。且应使用经过验证的部件和安全准则。	■ 出现故障会导致安全功能的丧失，但是故障率比 B 类要小。	
2	应该满足 B 类要求，且应使用经过验证的安全准则。机器控制应该以适当的间隔（测试频率为所需频率的 100 倍）检查安全功能。	■ 在检查间隔期间，出现故障时会导致安全功能的丧失。 ■ 检查时能够检测到安全功能的丧失。	主导因素是结构
3	应该满足 B 类要求，且应使用经过验证的安全准则。安全相关部件的设计应该保证： ■ 任何部件出现单独故障时都不会导致安全功能的丧失 ■ 在合理的限制范围内，任何时候单个故障都能被检测到。	■ 单个故障发生时，总能维持安全功能。 ■ 只能检测到一些（不是所有）故障。 ■ 未检测到的故障的累积可能会导致安全功能的丧失。	
4	应该满足 B 类要求，且应使用经过验证的安全准则。安全相关部件的设计应该保证： ■ 任何部件出现单独故障时都不会导致安全功能的丧失 ■ 在下一次需要防护功能时（或之前）能够检测到单个故障，或者 ■ 如果不能满足上述要求，则应保证故障的累积不会导致安全功能的丧失。	■ 故障发生时总能维持安全功能。 ■ 能够及时检测到故障，从而实现避免安全功能的丧失。	

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

平均无危险故障时间 (MTTFd)

MTTF 是“平均无故障时间”的简称。根据 EN ISO 13849-1 标准，评估时仅需考虑危险故障的情况（“d”表示“危险故障”）。

此值为一个理论参数，用来表示在部件的整个使用寿命中该部件（而不是整个子系统）发生危险性故障的概率。子系统的实际使用寿命通常更短。

MTTF 值可由故障率得到。故障率是指：

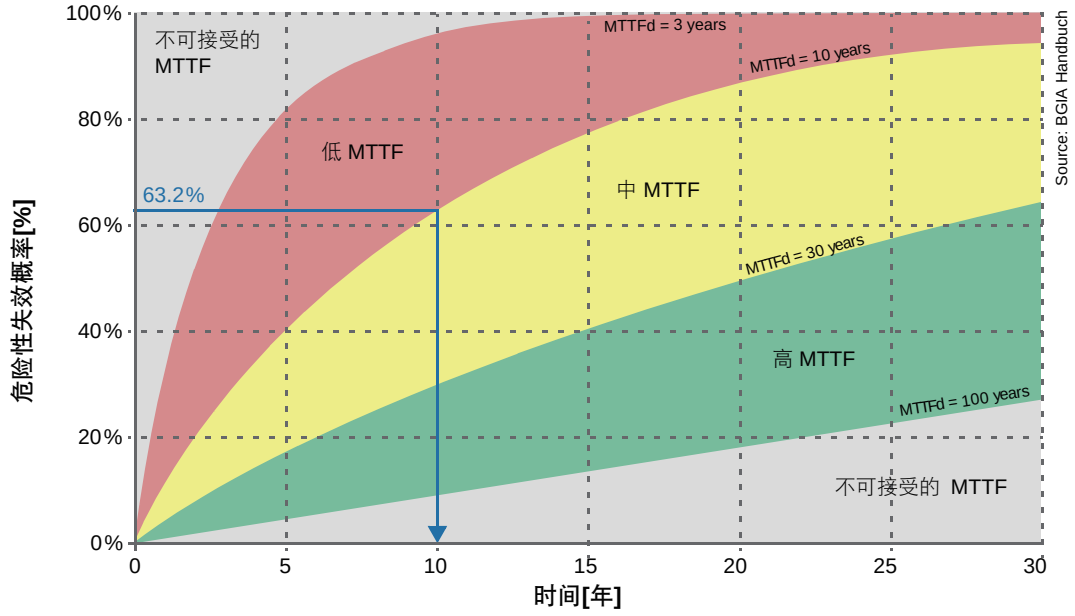
- 机电或气动部件的 B10 值。在这种情况下使用寿命取决于开关频率。B10 定义了开关周期数，在开关周期数中，最多有 10% 的部件会失效。
- 用于电子部件：故障率 λ。故障率通常以单位 FIT 来描述。1FIT 就是指每 10^9 小时发生一次故障。

EN ISO 13849-1 标准将 MTTFd 值划分成不同的范围：

名称	范围
低	3 年≤ MTTFd < 10 年
中	10 年≤ MTTFd < 30 年
高	30 年≤ MTTFd < 100 年

通过部件信息可以计算出以年为单位的平均无危险故障时间 (MTTFd)。

为了避免过于看重可靠性，最高的 MTTFd 值限定为 100 年。



© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

诊断覆盖率 (DC)

如果子系统是内部测试的，就可以提高安全等级。诊断覆盖率 (DC) 是故障检测的一种度量。测试结果不佳时仅能检测出少数故障，而良好的测试则能够检测出大量的（甚至是所有的）故障。

EN ISO 13849-1 标准并没有使用复杂的分析（FMEA，失效模式与影响分析），而是对 DC 进行测量并量化。在测量过程中还会进一步划分为不同的范围。

名称	范围
没有	DC < 60%
低	60% ≤ DC < 90%
中	90% ≤ DC < 99%
高	99% ≤ DC

共因失效 (CCF) —抗力

外部影响（例如电压等级、过热等）会使同样的部件突然不能使用，这与它们出现故障的频率及测试结果无关。（如同光线突然消失时，双眼是不能正常阅读报纸的。）应该防止这些共因失效（CCF — 共因失效）的情形。

EN ISO 13849-1 会对一系列的评估进行核对，并采取最低限度的积极措施。

要求		最大值
分离	信号电路的分离、独立路径、隔离、气道等	15
多样性	不同的技术、部件、工作原理和设计	20
设计，应用，经验	针对过载、过电压、过压等的防护（取决于所采用的技术）	15
	长期使用证明的部件和规程用法	5
分析，评估	使用失效分析防止共因失效	5
技能/培训	培训设计者以使其理解 CCF 的原因和后果并避免造成 CCF	5
环境影响	测试系统的电磁兼容敏感度	25
	测试系统对温度、冲击和振动等的敏感度。	10

最低要求
总分 ≥ 65

过程

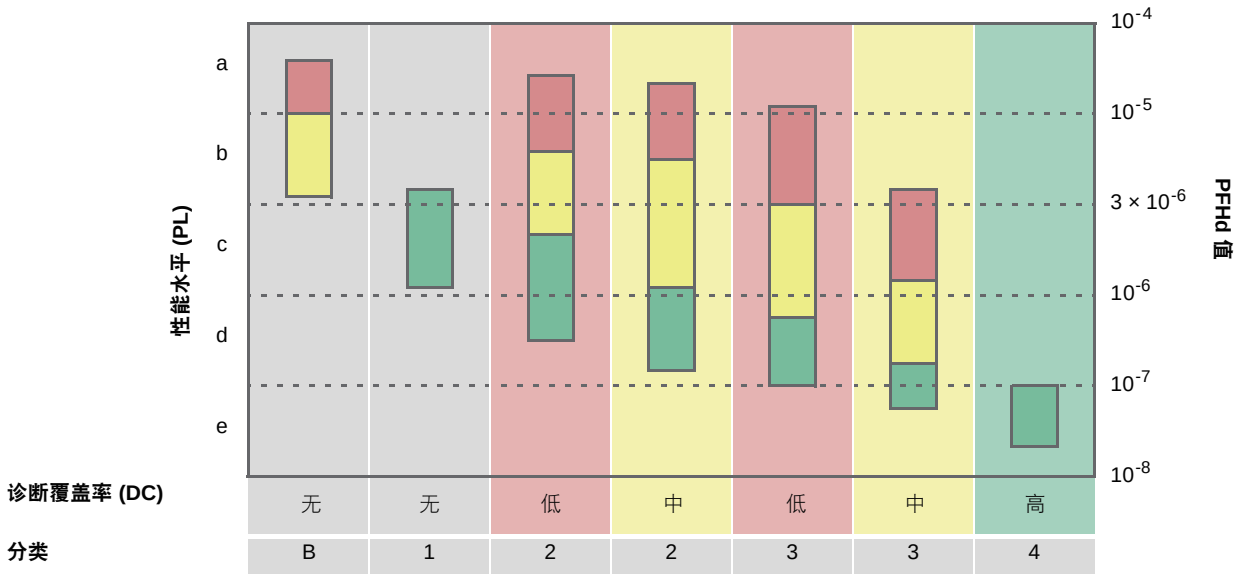
为了确保上述各方面能够在硬件和软件中正确地实施，需要进行全面的检查（采用由第二人进行复查的原则），并且保证彻底的归档能够提供关于版本和更改的溯源信息，可以考虑在标准中使用的各种不同的工具。

安全相关主题的正确实施过程是一项管理任务，需要进行适当的质量管理。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

确定子系统的 PL

下图所示的是 MTTFd 值（每通道的数值）、DC 及分类之间的关系。



例如，等级为“d”的性能水平可以通过使用一个双通道控制系统（第 3 类）来实现。如果几乎能检测到所有故障（DC = 中），则使用高质量的部件（MTTFd = 中）即可达到该等级；但如果只能检测到大部分故障（DC = 低），则需使用质量极高的部件（MTTFd = 高）来实现。

该步骤背后其实隐含了一个复杂的数学模型，只不过用户没有察觉而已。

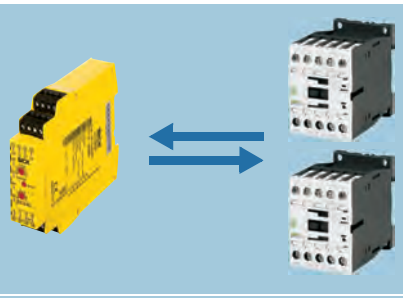
为了确保该方法的实用性，参数分类、MTTFd 和 DC 都是预定义的。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

示例：确定“执行器”子系统的性能水平

1)“执行器”子系统的定义

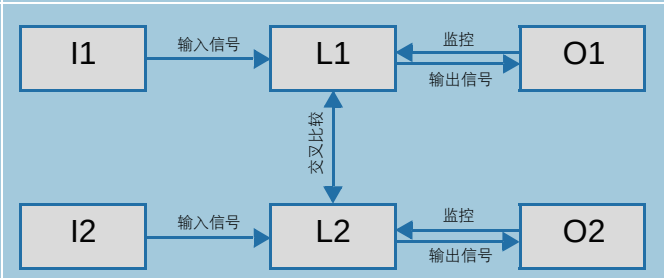
“执行器”子系统包括两个带“反馈”的接触器。可以利用其触点的主动导引功能，检测接触器的相关安全故障。逻辑单元 UE410 本身并不是“执行器”子系统的一部分，但是可用于诊断。



2) 类别的定义

单个故障安全（带故障检测功能）适用于第 3 或 4 类。

注意：完成 DC 值的定义后才能最终确定分类。



3) 确定每个通道的 MTTFd 值

鉴于触点易于磨损，因此必须使用 B10d 值及估计的开关频率 (nop) 来确定 MTTFd 值。可以使用右边的公式：

开关频率的数据包括每天的运行时间 [hop]、每年的工作天数 [dop] 以及每小时的切换频率 [C]：

制造商需提供的次要条件：

- B10d = 1300000
- C = 1/h（假设）
- dop = 220 d/a
- hop = 16 h/d

在上述次要条件下得出的 **MTTFd 值为每个通道 7386 年**，即“高”。

$$MTTFd = \frac{B_{10d}}{0,1 \times n_{op}}$$

$$MTTFd = \frac{B_{10d}}{0,1 \times d_{op} \times h_{op} \times C}$$

MTTFd	范围
低	3 年≤ MTTFd < 10 年
中	10年≤ MTTFd < 30 年
高	30 年≤ MTTFd < 100 年

4) 确定 DC 值

由于触点具有主动引导功能，基于 EN ISO 13849-1 标准中的测量表格可以得到一个高的 DC 值 (99%)。

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

3 d

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

示例：确定“执行器”子系统的性能水平

5) 评估防止共因失效的措施

防止共因失效的措施需在多通道系统中实施。这些措施的评估结果为 75 分。因此满足了最低要求。

要求	数值	最低要求
隔离性	15	总分数 75 ≥ 65
多样性	20	
设计、应用、经验	20	
分析、评估	5	
技能/培训	5	
环境影响	35	
	75	

6) 评估过程措施

还应考虑预防和控制故障的系统因素。例如：

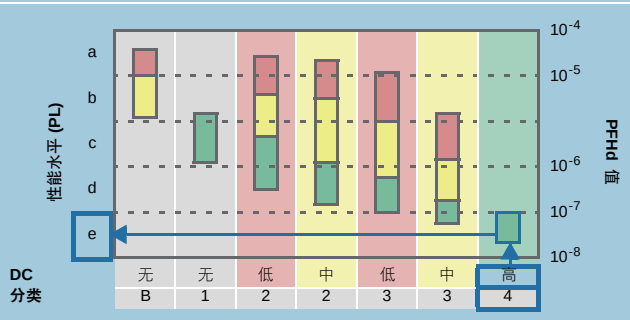
- 组织和技能
- 设计规则（例如规范模板、编码指南）
- 测试准则和测试条件
- 文档和配置管理

✔

7) 结果

从确定子系统 (➜3-56) 性能水平的图表中可以获得子系统的性能水平。本例中，可以**达到等级为“e”的性能水平**。

可从 EN ISO 13849-1 标准中的详细表格中得到 **PFHd 值：2.47×10^{-8}**。由于DC值比较高，因此双通道结构可以满足第 **4 类**的要求。



➜ 有了子系统的数据，现在就可以确定整个安全功能所达到的性能水平了（参见第 3-51 页的“根据 ENISO13849-1 标准确定所达到的性能水平 (PL)”）。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

可选方案：根据 EN62061 标准确定所达到的安全完整性等级 (SIL)

可以基于以下准则来确定所达到的安全完整性等级 (SIL)：

- 硬件的安全完整性
  - 结构限制 (SILCL)
  - 硬件的危险性失效概率 (PFHd)
- 系统的安全完整性要求
  - 预防故障
  - 控制系统故障

这里与 EN ISO 13849-1 类似，先将安全功能划分为功能块，然后传递给子系统。

硬件的安全完整性

在评估总体安全功能期间，可以确定硬件的安全完整性，从而...

- 子系统的最低 SILCL 限制了整个系统所能达到的最高 SIL 水平。
- 将单个 PFHd 值相加得到的总体控制系统 PFHd 值不能超过第 3-51 页“核实功能安全”图示中的值。

示例

上例中，所有的子系统都满足 SILCL3 的要求。PFHd 值的总和小于 1×10^{-7}。系统安全完整性的相关措施已实施。因此该安全功能满足 SIL3 的要求。

系统的安全完整性

如果控制系统同时连接了不同的子系统，则应为确保系统的安全完整性而采取额外的措施。

预防系统硬件故障的措施包括：

- 与功能安全规划相符的设计
- 正确选择、组合、安放、组装和安装子系统，包括电缆、布线及其他连接
- 使用方法符合制造商的规范
- 注意制造商的应用说明，例如分类信息、安装指导以及经过验证的设计实践应用
- 考虑符合 EN 60204-1 标准的相关电气设备要求

另外，为了控制系统故障还应考虑以下内容，例如：

- 关闭电源以保证其处于安全状态
- 采取用于控制故障影响以及其他与数据通信过程（包括传输故障、重复、丢失、插入、错序、数据出错、延时等）相关的影响的措施

3 d

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

根据 EN 62061 标准确定子系统的安全等级

如果子系统中包括由独立元件组成的电路，其安全等级也可根据 EN 62061 标准确定。

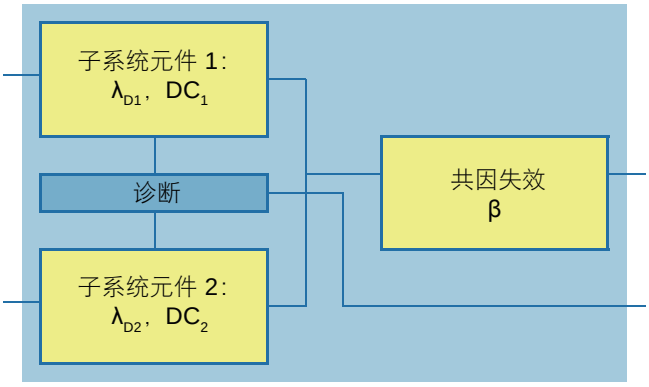
子系统的安全完整性等级 (SIL) 由以下参数决定：

- 硬件容错 (HFT)
- PFHd 值
- 安全失效率 (SFF)
- 共因失效 (CCF)
- 安全相关软件因素
- 系统故障

硬件容错 (HFT)

根据 EN 62061 标准，结构是由子系统类型和硬件容错 (HFT) 共同决定的。

HFT 0 意味着硬件中的单个失效就会导致安全功能丧失（单通道系统），而 HFT1 则表示硬件中发生单个失效时仍然能够维持安全功能（双通道系统）。



危险性失效概率 (PFHd)

除结构限制外，还需考虑子系统的“危险性失效概率”。可以基于一个数学模型通过使用公式计算每一个子系统的 PFHd 值。在计算过程中将用到以下参数：

- 诊断覆盖率
- 任务完成时间
- 诊断测试间隔
- 部件失效率 (D)
- 共因失效（共因因子）

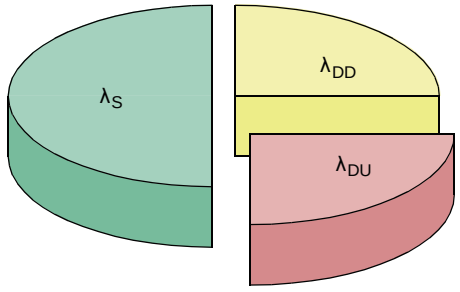
HFT = 1
采用 DC_1 和 DC_2 进行诊断

$$PFHd = (1-\beta)^2 \times \left\{ \frac{\lambda_{D1} \times \lambda_{D2} \times (DC_1 + DC_2) \times T_D}{2} + \frac{\lambda_{D1} \times \lambda_{D2} \times (2 - DC_1 - DC_2) \times T_P}{2} + \beta \times \frac{\lambda_{D1} + \lambda_{D2}}{2} \right\}$$

$$PFHd \approx \beta \times \frac{\lambda_{D1} + \lambda_{D2}}{2}$$

安全失效率 (DC/SFF)

DC = 50%
SFF = 75%



“安全失效率” (SFF) 是由诊断覆盖率 DC (λDD/λDU) 和“安全失效” (λS) 的分数共同决定的。

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

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

共因失效 (CCF)—抗力

EN 62061 还要求对共因失效抗力进行一系列的相关评估。共因因子 (β) 是完全执行次数的一个函数。

要求		最大值
分离	信号电路、独立路径、隔离、气道等的分离	15
多样性	不同的技术、部件、工作原理和设计	20
设计、应用和经验	针对过载、过电压、过压等的防护（依赖于所采用的技术）	15
	经过长期使用并证明行之有效的部件和规程用法	5
分析和评估	使用失效分析以防止共因失效	5
技能/培训	培训设计者并使其理解CCF的原因和后果	5
环境影响	测试系统的电磁敏感度	25
	测试系统对温度、冲击和振动等的敏感性。	10

数值	CCF 因子 (β)
< 35	10%
35 to < 65	5%
65 to < 85	2%
≥ 85	1%

过程

鉴于 EN 62061 标准非常依赖于可编程电气系统，它不仅包括上述各种因素（V 模型、质量管理等），还包括安全相关系统软件正常开发期间的诸多详细提示和要求。

结果 – 确定子系统的SIL

对于每一个子系统，首先分别确定其硬件的安全完整性：

如果是已经开发好的子系统（例如安全光幕），制造商会在“技术规范”中提供相关的特性数据，通常会包括 SILCL、PFHd 和任务完成时间等相关信息。换句话说，安全完整性等级应由包含子系统元件（例如防护装置或接触器上的互锁装置）的子系统决定。

SIL 要求限制 (SILCL)

在定义好硬件容错（架构）之后，就可以确定出子系统可实现的最高 SIL 等级（SIL 要求限制）。

安全失效率（SFF）	硬件容错	
	0	1
< 60%	-	SIL1
60 to < 90%	SIL1	SIL2
90 to < 99%	SIL2	SIL3
≥ 99%	SIL3	SIL3

硬件容错为 HFT1 的双通道系统具有 SILCL3 的等级要求（SFF 为 90%）。

3 d

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

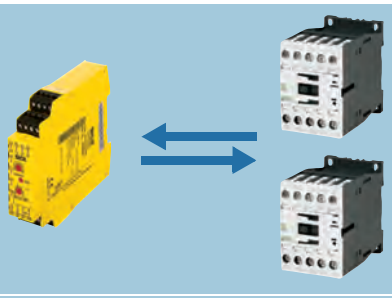
3 d

示例：确定“执行器”子系统的 SILCL 和 PFHd 值

1) “执行器”子系统的定义

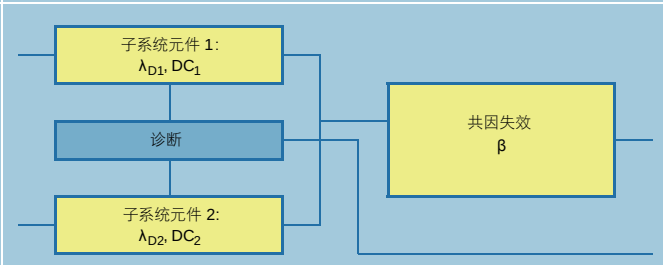
“执行器”子系统包括两个带“反馈”的接触器。可以利用其触点的主动导引功能，检测接触器的相关安全故障。

逻辑单元 UE410 本身并不是“执行器”子系统的一部分，但是可用于诊断。



2) 硬件容错的定义：

考虑到单个故障安全性（带故障检测功能），硬件容错 **HFT = 1**。



2) 确定 PFHd 值

a) 基于故障率 λ_D

鉴于触点易于磨损，因此必须使用 B10d 值来确定每小时的估计开关频率 [C]。

制造商需提供的次要条件：

- B_{10d} = 1300000
- C = 1/h (假设)

根据以上次要条件可得出：**λD 为每小时 7.7×10^{-8} $\frac{1}{h}$**

$$\lambda_D = \frac{0,1 \times C}{B_{10d}}$$

b) 基于 CCF 因子 (β)

防止共因失效的措施需在多通道系统中实施。其效果由符合 EN62061 标准的措施来确定。此例中 β 因子为 5%（参见下文：“5) 评估防止共因失效的措施”）

PFHd ≈ 1.9×10^{-9}.

数值	CCF 因子 (ß)
< 35	10%
35 至 < 65	5%
65 至 < 85	2%
≥ 85	1%

$$PFHd \approx \beta \times (\lambda_{D1} + \lambda_{D2}) \times ½$$

$$\approx \beta \times 0.5 \times \lambda_{Contactor}$$

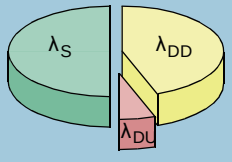
$$\approx 0.05 \times 0.5 \times 0.1 \times \frac{C}{B_{10}}$$

$$PFHd \approx 1.9 \times 10^{-9}$$

4) 通过 DC 确定 SFF

由于触电具有主动引导功能，可以得到一个“高”的 DC (99%)，即危险故障 λ_D 为 50% 时，可检测到 99% 的故障。因此 **SFF = 50% + 49.5% = 99.5%**。

DC = 99%
SFF = 99.5%



5) 评估防止共因失效的措施

防止共因失效的措施需在多通道系统中实施。此例中，评估符合 EN 62061 标准的措施的 CCF 因子 (β) 为 5%。

数值	CCF 因子 (ß)
< 35	10%
35 至 < 65	5%
65 至 < 85	2%
≥ 85	1%

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

示例：确定“执行器”子系统的 SILCL 和 PFHd

评估过程措施

还应考虑预防和控制故障的系统因素。例如：

- 组织和技能
- 设计规则（例如规范模板、编码指南）
- 测试准则和测试条件
- 文档和配置管理

✔

结果

在最后一步中还需考虑结构限制。由于该子系统已有冗余性（硬件容错 1）及其 SFF > 99%，因此这个子系统的 **SIL 声称限制为 SILCL3。**

安全故障系数 (SFF)	硬件容错	
	0	1
< 60%	-	SIL1
60 至 < 90%	SIL1	SIL2
90 至 < 99%	SIL2	SIL3
≥ 99%	SIL3	SIL3

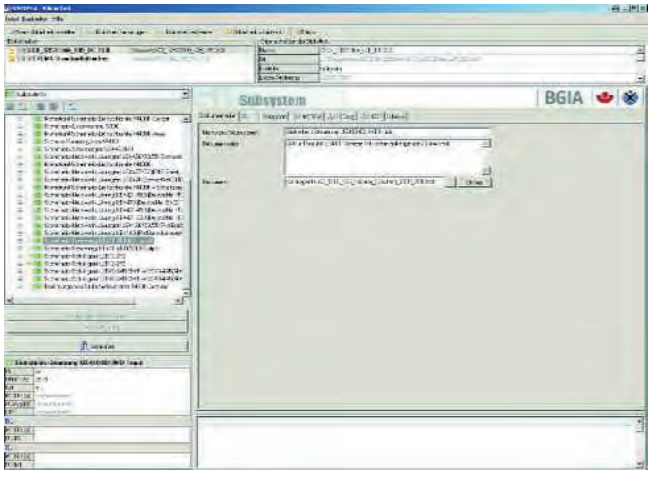
PFHd ≈ 1.9×10^{-9}

➜ 有了子系统的 SILCL 数据及 PFHd 值，就可以确定整个安全功能所达到的 SIL 了（参见第 3-59 页的“硬件的安全完整性”）。

帮助和支持

本文所述核查方法需要具有使用性能水平 (PL) 和安全完整性等级 (SIL) 方面的专业知识和经验。SICK 公司可提供相关服务（➜ 参见第 1 页的“SICK 公司提供的支持”）。合适的软件工具可提供带有系统步骤的帮助。

由 BGIA 开发的 SISTEMA 软件向导可为性能水平的计算提供有效的方法，此软件可在线免费获取。SICK 公司还为该应用提供了一个经过认证的安全部件库。此外，我们的研讨会也可为你的日常工作提供实际的专业知识。



➜ 您可以访问 http://www.sick.com/ 查找关于 SISTEMA 软件及培训课程的信息。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

总结：安全功能的核实

基本原理

- 核实所规划的安全功能是否具有必要的安全等级。因此需要对机械安全和功能安全进行核实。

方法

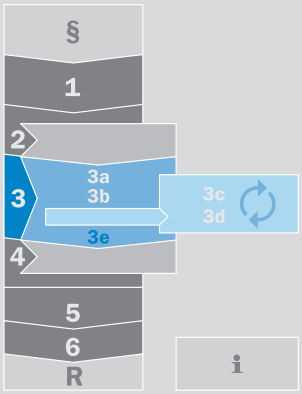
- 根据 EN ISO 13849-1 (PL) 确定安全等级。
  - 可以使用简化步骤（基于 PL）
  - 以及详细步骤（基于 PFHd 值）。
- 如果不知道子系统（例如执行器子系统）的 PL 和 PFHd 值，则可由结构、可靠性、诊断、抗力和过程等参数来确定子系统的安全等级。
- 或者，也可根据EN ISO 62061 (PL) 确定安全等级。也可以自己确定未认证子系统的安全等级。

帮助

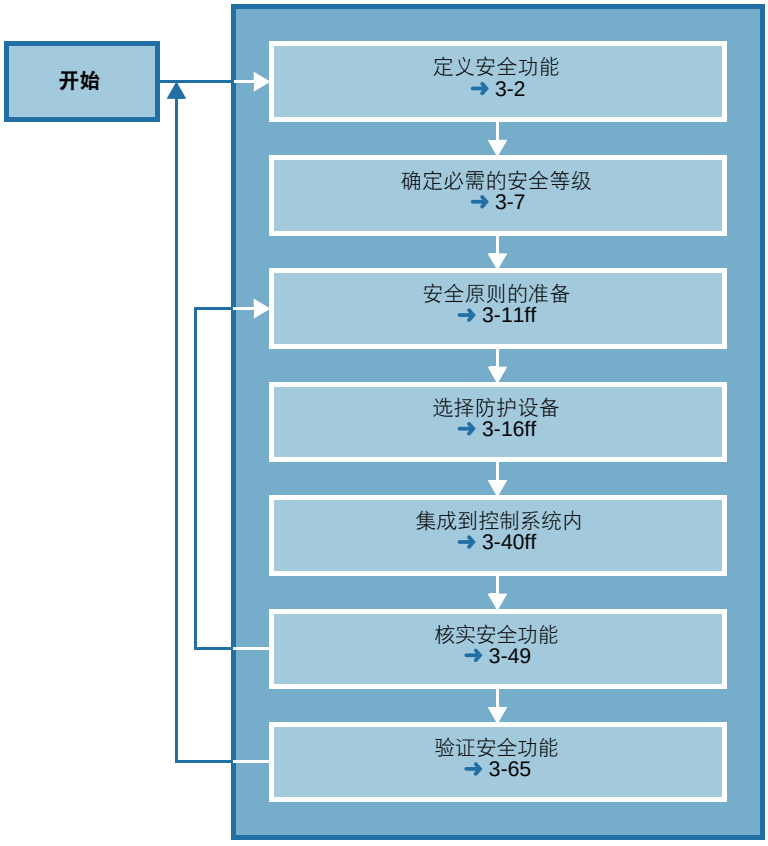
- 使用推荐的工具，并寻求建议。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

第 3e 步：安全功能的验证



验证就是对与所要解决问题相关的论题、规划或方案进行彻底检查。与核实不同（核实期间仅根据规范评估方案是否正确实施），而验证则是最终的评估，用以确定方案是否可以降低必要的风险。



© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

验证过程的目的就在于检查规范以及安全功能所涉及的机器部件设计是否符合规范。
验证应表明控制功能的相关安全部件满足 EN ISO13849-2 的要求，尤其是所规定的安全等级要求。
如果可行，验证应由与控制系统相关安全部件的设计不相关的人员进行。
验证过程期间，检查所制定规范中的错误，尤其是遗漏十分重要。
通常，相关安全控制功能设计的关键部分就是规范。
举个例子：人员进入制造车间时使用光幕对其进行保护。因此规定安全功能如下：

“一旦光幕的保护区域被中断，则所有的危险运动都应尽快停止。”另外，当防护区域重新畅通时（尤其是当其可能处于防护区域后边时），设计者也应考虑重启。验证过程应该发现这些问题。
验证过程期间，通常会使用可互相补充的几个步骤。
包括：

- 对防护设备的定位和有效性进行彻底的技术检查
- 使用模拟方法对与预期结果相关的故障的反应进行实际检查
- 采用功能测试对环境要求进行验证：
  - 防止诸如温度、湿度、冲击、振动行为等相关环境因素所造成的影响
  - 具有足够强的电磁抗扰度

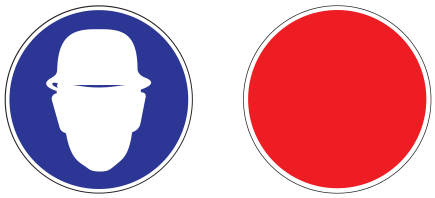
© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

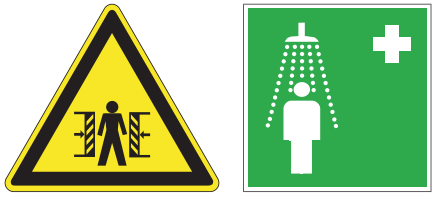
第 4 步：关于剩余风险的用户信息

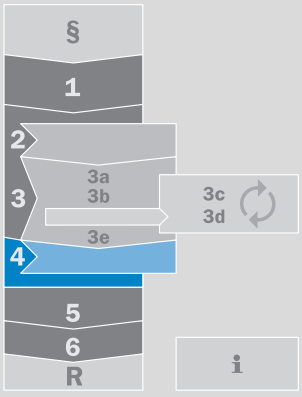
用户信息不能取代其他安全措施。如果安全设计或技术防护措施不能完全发挥效用，应向用户警示剩余风险并提供必要的处理建议。

警示和建议包括：

- 操作指南中的警告
- 工作指导、培训要求或用户熟悉过程
- 图示
- 使用个人防护设备的注意事项







© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

第 2、3、4 步的总结：降低风险

基本原理

为了降低风险，可以使用下面的 3 步法：

1. 设计机器时应尽可能消除该危险。
2. 确定、设计并核查必需的防护措施。
3. 确定组织措施和有关剩余风险的警示信息。

技术防护措施

- 涉及到功能性安全时，可以借助下述两个标准：EN ISO 13849-1 (PL) 或 EN 62061 (SIL)。
- 定义安全功能，为每一个安全功能确定必需的安全等级。
- 设计安全理念。确定最有效的防护设备及其在控制系统中的安装和集成。
- 确保防护措施的正确执行，并实现所需的安全等级。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

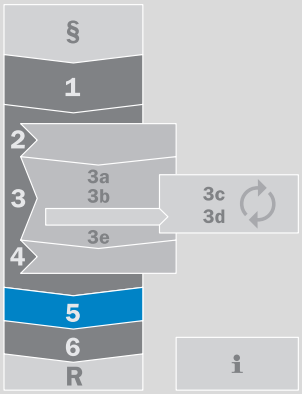
第 5 步：全面验证

鉴于功能性安全仅是降低风险所用措施的一部分，因此全面验证时还应对其它所有措施（包括设计的、技术的和组织的）进行评估。

尽管降低风险不能依靠单一的技术措施来实现，但实际操作中进行全面的风险评估仍然能够达到所期望的结果。
如果以下问题的回答都是肯定的，那么可以认为风险已经充分降低：

- 是否考虑了机器在各个使用阶段的所有运行条件?
- 是否使用了3步法?
- 危险是否已被消除，该危险的风险是否已降低到可接受的程度?
- 是否可以保证所采取的措施不会导致新的危险?
- 是否已经向用户警示并告知有关剩余风险的必要信息?
- 是否可以保证所采取的防护措施不会妨害操作员的工作环境?
- 是否采取的防护措施可以同时执行且互不阻碍?
- 是否已经充分考虑在非商业/非工业领域使用机器时可能出现的后果?
- 是否可以保证所采取的措施不会过度妨害机器的正常功能?
- 风险是否已降低?

SICK 公司的安全专家在进行安全检查时，会对整个机器所有可能存在的危险进行检查。

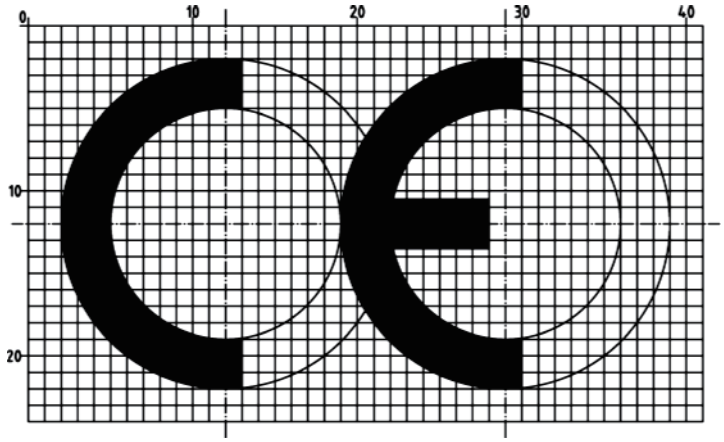


© SICK AG •工业安全系统•德国。版权（包括技术规范和信息

5

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

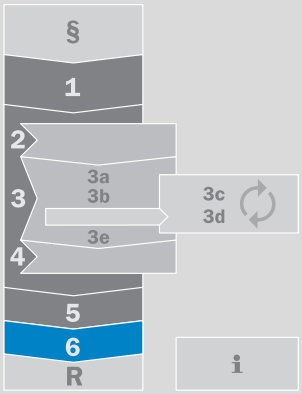
第 6 步：投放市场



在全面验证期间确定了一致性后（必要时可由一个相关机构参与），可以签署一致性声明，并在完成技术文档时使用 CE 标示。一致性声明应考虑所有适用的欧盟指令。

在一致性评估过程中，Safexpert (➜1-4) 可以为您提供支持。

机器交付时还需提供采用机器使用国语言的操作指南。该操作指南应该是原版操作指南或者是原版操作指南的翻译版本；对于第二种情形，我们同时会提供原始操作指南。



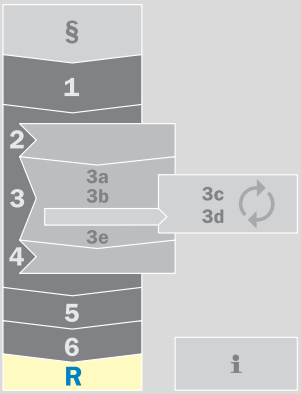
© SICK AG •工业安全系统•德国。版权（包括技术规范和信息

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

机器使用方的责任

雇主要对雇员的安全负责。机器的操作应符合人体工程学，同时与操作员的资格相匹配；机器本身也应该是安全的。

除了在交货期间进行安全验收和检查外，在采购时还应考虑安全相关的要求，检查对应规格是否正确。



如何采购机器?

成功的生产设施的安装和现代化改造都是从采购开始的。要根据不同选择做出决定。

- 进行复杂机械的安装时，应根据机械指令指定一个“管理者”。
- 事先应弄清如何处理所提供的机械（或机械部件）。
- 以合约形式确定需要提供的其他文档（例如风险评估文档等）从而使后续更改更容易。
- 尽可能规定使用重要的 EN 调和标准为基础。
- 商定与调和标准不符时使用的程序。

安全检查

经验表明机械安全措施在实际使用时是局限的。为保证不妨碍工作，防护设备通常被改动。其他安全防护错误包括防护设备位置不正确，以及在控制系统中使用了错误的集成方式。

工作设备和系统在运行时的安全状态由欧盟指令 89/655/EEC（“工作设备指令”）进行规范，并且须与相关国法律一致。

指令中的 4a 条款特别规定要对工作设备进行彻底核查。该检查过程可以以技术规则和标准或具体规范为基础。彻底核查和正式确定设备运行的安全性须由操作相关系统的机构安排。

在此过程中，运行机构应该按照工作设备指令在相关国家的实施法令，安排对工作设备进行彻底检查。该过程中，以下 5 个因素应满足该指令的相关国实施要求：

1. 核查类型
2. 核查范围
3. 核查深度
4. 核查的最后期限
5. 执行该核查任务人员的能力水平

在进行安全检查时，SICK 公司会对您机器的安全状态进行快速浏览。

Deutscher Akkreditierungs Rat
DAT-I-003/01
SICK Safety Inspection

SICK 公司是被 ➜ DATech 认可的安全检查机构。

该认可由独立机构提供，表明 SICK 公司能够执行认可范围内的行为，且能确保其行为的可靠性与质量。

我们将与你一起发掘提升空间并通过实际操作实现改善。

- 英国：《工业设备供应和使用条例 1998》，Betriebssicherheitsverordnung (BetrSichV)
- 芬兰：Valtioneuvoston päätös työssä käytettävien koneiden ja muiden työväline-iden hankinnasta, turvallisesta käytöstä ja tarkastamisesta (VNp856/1998, ns. “Käyttöpäätös”)
- 荷兰：De Arbowet, het Arbobesluit
- 比利时：De Welzijnswet en de Codex over het Welzijn op het Werk, la Loi sur le Bien-être et le Code sur le Bien-être au Travail

➜ 工作设备指令 89/655/EEC：http://eur-lex.europa.eu/

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息

工作设备指令，第 4a 条：工作设备的检查

1. 雇主应该确保：在工作设备的安全性取决于安装条件时，应对其进行初始检查（在设备安装后以及第一次使用前），以及在新的场地或位置安装后的检查，这些检修应该由胜任人员按照国家法律和/或惯例进行，以保证工作设备已经正确安装并且运行正常。
2. 雇主应该确保：当设备暴露在可能导致其性能恶化的条件下时，应进行以下操作：

- 定期检查，并在适当时由胜任人员按照国家法律和/或惯例进行测试；以及
- 在发生会危及工作设备安全性的异常情况后（例如改动、事故、自然现象或长期未使用等），由胜任人员按照国家法律和/或惯例进行特别检查，以维持设备的良好性能和安全状态，并检测出设备性能的恶化从而及时进行补救。

3. 必须记录检查结果并将其保存适当时间供相关人员使用。

   工作设备用于许可范围以外的应用时，必须有实物证明其已完成最后一次检查。

4. 欧盟成员国应确定进行此种检查的执行条件。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

SICK 公司提供的支持

SICK 公司一直致力于将安全理念融入您的组织，以实现：

- 改进现有机器和系统的安全性。
- 采购新机器和系统期间的安全完整性。

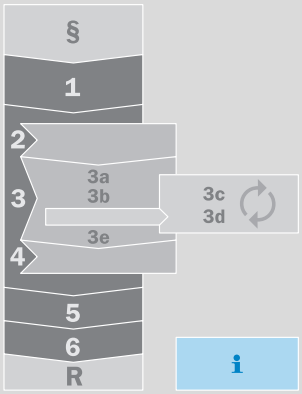
您的合作伙伴应符合以下要求：

- 具有多年的经验
- 能够提供创新的想法
- 国际化

SICK 专家的早期参与可实现以下目的：

- 将安全性作为项目的一个有机组成部分进行规划。
- 在早期阶段就可以识别出潜在的不足。
- 防止安全措施所占比重过大。
- 确保有效性和竞争力。

SICK 公司的服务可以确保更高的安全性和商业价值。



一致性和设计

我们的杰出专家会和您一起进行系统的安全规划，并帮助完成您的项目。通过这种方式我们可以尽早消除危险源 — 从而节省您的时间及成本。在一致性的评估过程中，SICK 公司将和您一起执行以下步骤：

第 1 阶段

确定基本参数
- 正确使用
- 接口定义
- 标准研究

第 2 阶段

预规划
- 风险评估
  - 对与系统相关的危险和风险进行分析和评估
  - 对控制系统的所有相关安全部件进行评估和分类

第 3 阶段

设计和实施规划
- 安全原则的制订
  - 安全功能的定义
  - 紧急停机原则
  - 安全规范

第 4 阶段

核实
- 设计开始时检查设计和系统规划
- 首次将机器投放市场时进行安全检查

第 5 阶段

检查最终的一致性
- 总体一致性的定义

本章主要内容	页码

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

研讨会和用户培训

源于实践并用于实践的用户知识

通常您越有经验，处理应用时就越安全。SICK 研讨会和培训课程的一个重要目标就是传递经验并对应用进行优化。因此所有课程都是针对实际应用的。

知识推动进步

法律和标准会随时间不断改变，技术也是如此。从带继电器的传统硬连线技术，到可编程的安全模块，再到带总线系统的整个网络，我们必须学会适应这些创新技术。在我们关于安全原理的系列研讨会中，将讲授关于以下主题的最新专业知识：

- 根据标准选择合适的防护设备
- 防护设备在总体控制系统中的完整性
- 在可行指令、标准及规定的基础上对防护措施进行正确的评估

改进应用的安全性

我们的用户培训课程都是针对产品的，因此可以有效并可靠地集成到所规划的应用中去。在此过程中你将获得关于如何使用设备以及分析和诊断特征的相关信息。

用户培训课程的总体结构涵盖了在产品的选择和集成期间将会出现的不同阶段：

- 选择
  - 安全因素
  - 产品特性和可能的应用
- 集成
  - 应用（装配）和布线中的集成
  - 编程
  - 调试
- 安全运行
  - 故障诊断和修正

如果需要，SICK 公司可以为您的应用量身定制一项合格准则，以实现优化工作质量，并加快相关安全知识的传播。

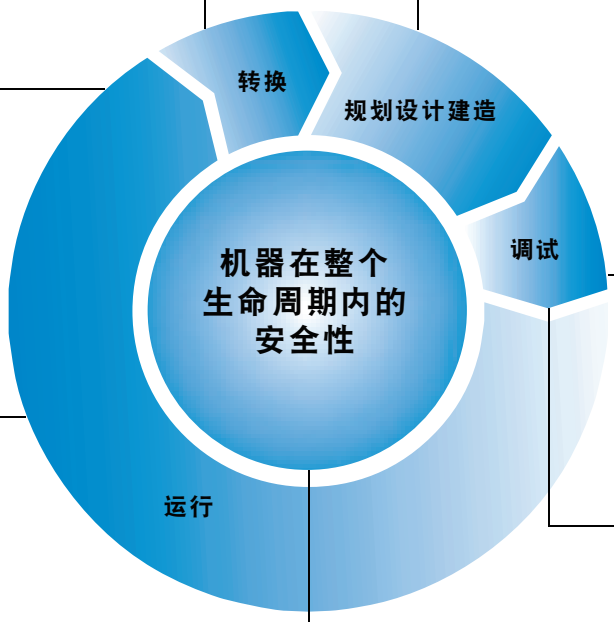
➜ 关于研讨会的相关信息，请联系附近的 SICK 公司代理商，或者访问我们的网站 http://www.sick.com/。

我们也可根据要求到您的经营场所现场举办研讨会和用户培训。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

SICK — 在产品的整个生命周期内均可为您的系统提供支持

从规划到调试、再到维护和现代化改造，在机器的整个生命周期内，SICK 公司都会使用经过认证的安全产品以及为你量身定做的独特服务来提供支持。



SICK 国际服务方案
一致性和设计
- 风险评估
- 安全原则
- 项目管理
- 软件设计
- 硬件设计
- 安装
- 调试
- 功能安全性评估
- CE 合规性检查
- CE 认证
- 工厂验收

SICK 国际服务方案
升级服务
- 升级包

SICK 国际服务方案
产品支持
- 现场故障检修
- 热线服务电话支持
- 服务工具
- 备用部件
- 更换设备
- 车间维修

SICK 国际服务方案
产品支持
- 调试检查
- 热线服务电话支持

SICK 国际服务方案
核实和测量
- 事故调查
- 电气设备检查
- 定期检修
- 机器安全性检修
- 停机时间测量
- 噪声测量

SICK 国际服务方案
核实和测量
- 电气设备核查
- 初始检修
- 机器安全性检修
- 停机时间测量
- 噪声测量

SICK 国际服务解决方案
培训和教育
- 用户培训
- 研讨会
- 网络培训

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

部件（产品）

使用经过认证的产品可以使机器制造商更符合机器指令和许多不同标准之间的一致性要求。作为方案的提供商，SICK 公司可为机器制造商提供各种各样的产品，从简单的单束光电安全开关、安全光幕、安全激光扫描器、基于摄像头的安全传感器和安全开关，到带网络支持的模块化安全控制仪以及用来评估机器一致性的软件方案等，应有尽有。

建议：我们的专业知识 — 您的优势

SICK 公司在所有主要工业国家都有子公司或代理商。你可以从我们的熟练技术雇员那里获得必要的专家建议。除了相关产品的专家知识，他们还可为你提供有关市场、国家法律和标准的知识。

➜ 产品选择在 3-47 页
➜ 您也可以访问 http://www.sick.com/ 在线查找所有产品信息。
➜ 更多关于在贵国家提供服务的信息，请联系贵国的 SICK 代理商或访问我们的网站 http://www.sick.com/。

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

相关标准概述

现在许多 A 类、B 类以及重要的 C 类标准都正在修订中。这将导致许多 EN 标准变成所谓的 EN-ISO 标准。但是通常都会有 3 年的过渡期。因此当前正在修订的标准实际上只能适用于 5 或 6 年以后。

标准类型	欧洲标准 EN	协和标准?	国际标准 ISO/IEC	标题
A	EN ISO 12100-1 （以前是 EN 292-1） EN ISO 12100-2 （以前是 EN 292-2）	✔ ✔	ISO 12100-1 ISO 12100-2	机械安全 — 基本准则，一般设计原理
	EN ISO 14121 （以前是 EN 1050）	✔	ISO 14121	风险评估
B	EN 349	✔	ISO 13854	机械安全 — 避免人体部位挤压的最小间距
	EN 574	✔	ISO 13851	机械安全。双手控制设备 — 功能因素；设计原理
	EN 953	✔	ISO 14120	机械安全。防护设备。一般要求
	EN 1037	✔	ISO 14118	机械安全。防止意外启动
	EN 1088	✔	ISO 14119	机械安全。与防护设备相关联的联锁设备。设计和选择原理
	EN ISO 13849-1 （也可以是 EN 954-1） EN ISO 13849-2	✔ ✔	ISO 13849-1 ISO 13849-2	控制系统的相关安全部件 ■ 第 1 部分：一般设计原理 ■ 第 2 部分：确认
	EN ISO 13850 （以前是 EN 418）	✔	ISO 13850	机械安全。紧急停机。设计原理
	prEN ISO 13855 （目前仍然是 EN 999）	✔	ISO 13855	根据人体部位的接近速度进行防护设备定位
	EN ISO 13857 （以前是 EN294 和 EN811）	✔	ISO 13857	机械安全 — 防止上肢和下肢到达危险区域的安全距离
	EN 60204-1	✔	IEC 60204-1	机器中的电气设备 ■ 第 1 部分：一般要求
	EN 61496-1 CLC/TS 61496-2 CLC/TS 61496-3	✔	IEC 61496-1 IEC 61496-2 IEC 61496-3	机械安全 — 电感式防护设备 (ESPE) ■ 第 1 部分：一般要求和测试 ■ 第 2 部分：使用有源光电防护设备的特殊要求 ■ 第 3 部分：使用有源光电漫反射防护设备 (AOPDDR) 的特殊要求
	EN 61508		IEC 61508	电气/电子/可编程电子相关安全系统的功能安全性
	CLC/TS 62046		IEC/TS 62046	机械安全 — 用于检测人员存在的防护设备应用
	EN 62061	✔	IEC 62061	相关安全电气/电子/可编程电子控制系统的功能安全性

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

标准类型	欧洲标准 EN	协和标准?	国际标准 ISO/IEC	标题
C	EN 415-4	✔		码垛机和散垛机
	EN 692	✔		机械压力机
	EN 693	✔		液压机
	EN 13736	✔		气动压力机
	EN 12622	✔		气动压力机
	EN ISO 10218-1 (以前是 EN 775)	✔	ISO 10218-1	工业机器人。安全要求 ■ 第 1 部分：机器人
	prEN ISO 10218-2		ISO 10218-2	■ 第 2 部分：机器人系统及其完整性 （注意：EN 775 已被撤销，但是在 EN ISO 10218-2 出现之前还将继续适用于机器人系统。）
	EN ISO 1010	✔	ISO 1010	打印机和纸加工机
	EN ISO 11111	✔	ISO 11111	纺织机械
	EN 811	✔		建造和安装升降机的安全规则 ■ 第 1 部分：电动升降机
	EN 280	✔		移动升降工作平台 — 设计计算 — 稳定条件— 建造 —安全 — 检验和测试
	EN 1570	✔		升降台的安全要求
	EN 1493	✔		汽车电梯
	EN 1808	✔		高处作业吊篮的安全要求 — 设计、计算、稳定条件、建造测试
	EN 691			木工机械 — 安全和健康 — 通用要求
	EN 1870-1	✔		木工机械的安全性 — 圆盘锯床 ■ 第 1 部分：圆盘锯架（带和不带滑动台）和方板锯
	EN 1870-4	✔		■ 第 4 部分：手工装卸多刀片锯床
	EN 848-1	✔		木工机械的安全性 — 带旋转工具的单面模压机 ■ 第 1 部分：单轴立式模压机
	EN 940	✔		木工机械的安全性 — 组合木工机械
	EN 1218-1	✔		木工机械的安全性 — 制榫机 ■ 第 1 部分：带滑动工作台的单端制榫机
	EN 289	✔		橡胶和塑料机械。压塑压机和压铸压机。设计的安全要求
	EN 201	✔		橡胶和塑料机械。注塑机。安全要求
	EN 422	✔		橡胶和塑料机械。安全性—专用于生产空心物体的吹塑机—设计和建造要求
	EN 1114-1	✔		橡胶和塑料机械—挤压机和挤压工作线 ■ 第 1 部分：挤压机的安全要求
	EN 1612-1	✔		橡胶和塑料机械 — 反应模塑机 ■ 第 1 部分：配量和搅拌设备的安全要求

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

标准类型	欧洲标准 EN	协和标准?	国际标准 ISO/IEC	标题
C	EN 528	✔		轨道式存储和调用设备—安全性
	EN 281			带驾驶员座位的自推式工业卡车；设计和布局踏板的规则
	EN 1459	✔		机械安全—可伸缩臂式堆垛机
	EN 1525	✔		工业卡车的安全性。无人驾驶卡车及其系统
	EN 1526	✔		工业卡车的安全性—卡车上自动化功能的其他要求
	EN 1672-1	✔		食品加工机械 — 安全和卫生要求—基本准则
	EN 972	✔		制革机—往复式滚压机—安全要求
	EN 869	✔		压力金属拉模铸造设备的安全要求
	EN 710	✔		铸造厂模铸和制芯机械、设备及相关设备的安全要求

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

相关链接

以下内容的出处?	
指令文本 (EU)	在因特网上其他网站中的欧盟法律入口可以找到完整的指令文本: ➜http://eur-lex.europa.eu/
标准列表	欧盟官方公报 Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA): ➜http://www.baua.de/ Verband Deutscher Maschinen- und Anlagenbau (VDMA): ➜http://www.vdma.org/ 欧洲委员会 ➜ http://ec.europa.eu/enterprise/newapproach/standardization/harmstds/reflist.html Beuth Verlag GmbH: ➜http://www.beuth.de/
国际化标准出版社	CEN: ➜http://www.cen.eu/cenorm/homepage.htm CENELEC: ➜http://www.cenelec.org/cenelec/Homepage.htm ISO: ➜http://www.iso.org/iso/home.htm IEC: ➜http://www.iec.ch/
标准出版社（德语）	德国 (DIN): ➜http://www.din.de/ 奥地利 (ON): ➜http://www.on-norm.at/publish/home.html 瑞士 (SVN): ➜http://www.snv.ch/
标准出版社（欧洲）	比利时 (NBN): ➜http://www.nbn.be/ 保加利亚 (BDS): ➜http://www.bds-bg.org/ 丹麦 (DS): ➜http://www.ds.dk/ 爱沙尼亚 (EVS): ➜http://www.evs.ee/ 芬兰 (SFS): ➜http://www.sfs.fi/ 法国 (AFNOR): ➜http://www.afnor.org/ 希腊 (ELOT): ➜http://www.elot.gr/home.htm 英国 (BSI): ➜http://www.bsi-global.com/ 爱尔兰 (NSAI): ➜http://www.nsai.ie/ 冰岛 (IST): ➜http://www.stadlar.is/ 意大利 (UNI): ➜http://www.uni.com/it/ 拉脱维亚 (LVS): ➜http://www.lvs.lv/ 立陶宛 (LST): ➜http://www.lsd.lt/ 卢森堡 (SEE): ➜http://www.see.lu/ 马耳他 (MSA): ➜http://www.msa.org.mt/ 荷兰 (NEN): ➜http://www2.nen.nl/ 挪威 (SN): ➜http://www.standard.no/ 波兰 (PKN): ➜http://www.pkn.pl/ 葡萄牙 (IPQ): ➜http://www.ipq.pt/ 罗马尼亚 (ASRO): ➜http://www.asro.ro/ 瑞典 (SIS): ➜http://www.sis.se/ 斯洛文尼亚 (SIST): ➜http://www.sist.si/ 斯洛伐克 (SUTN): ➜http://www.sutn.gov.sk/ 西班牙 (AENOR): ➜http://www.aenor.es/ 捷克共和国 (CNI): ➜http://www.cni.cz/ 匈牙利 (MSZT): ➜http://www.mszt.hu/ 塞浦路斯 (CYS): ➜http://www.cys.org.cy/
第三方指定机构（德国）	可以从这里获得目前为止由欧盟成员国指定的认证机构列表: ➜ http://www.baua.de/prax/geraete/notifiz.htm
奥地利	Arbeitsschutzinspektion Österreich: ➜http://www.arbeitsinspektion.gv.at/ CD-ROM “ArbeitnehmerInnenschutz expert” ➜http://www.a-expert.at/
瑞士	Arbeitsschutzinspektion Schweiz: ➜http://www.seco.admin.ch/
BG 预防委员会列表（德国）	➜ http://www.hvbg.de/d/bgz/praevaus/index.html
Berufsgenossenschaften（专业机构）的地址 (德国)	➜ http://www.dguv.de/inhalt/BGuUK/bgen/index.html
法定事故的保险提供商	德国: Deutsche gesetzliche Unfallversicherung: ➜http://www.dguv.de/ 奥地利: Allgemeine Unfallversicherung: ➜http://www.auva.at/ 瑞士: :Schweizerische Unfallverhütungsanstalt: ➜http://www.suva.ch/

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

术语表

缩写/术语		说明
λ	**每小时的故障率**	每小时的故障率，λ_S 和 λ_D 之和 ■ λ_S：安全故障率 ■ λ_D：危险故障率，可以分为以下两部分： ▪ λ_{DD}：由诊断功能检测到的危险故障率 ▪ λ_{DU}：未能检测到的危险故障率
β 因子		摘自 EN IEC 62061：因子是对共因失效的敏感度 ➜ 共因失效
A		
AOPD	**有源光电防护设备**	摘自 CLC/TS 61496-2：通过设备的光电发射和接收元件对指定检测区域内不透明物体所造成的光辐射中断进行检测来实现该设备的传感功能。 在 DINEN692“机械压机”、EN693 “液压机”和 EN12622 “液压制动器”中将 **AOS** 用作 **AOPD** 的同义词。
AOPDDR	**有源光电漫反射防护设备**	摘自 CLC/TS 61496-3：由该设备的光电发射器和接收器元件所形成的传感器功能，可对光线在指定的二维防护区域中的物体上的漫反射进行检测。
B		
B_{10d}		当 10% 的部件（气动和机电部件）发生了危险故障前的循环次数。
C		
分类		控制系统中相关安全部件的分类，与它们的抗故障能力以及发生故障后的后续行为有关
CCF	**共因失效**	共因失效：不同设备的故障由单一事件造成，且这些故障不会互为诱因
CENELEC	**Comité Européen de Normalisation Electrotechnique**	欧洲电气技术标准化委员会
CLC		CENELEC 已采纳标准的前缀
D		
DC	**诊断覆盖率**	诊断覆盖率：这是诊断有效性的度量，等于检测到的危险故障率与全部危险故障率之比
d_{OP}		平均运行时间（天/年）
E		
EDM	**外部设备监控**	摘自 EN 61496-1：电感式防护设备 (ESPE) 对其外部控制设备状态进行监控所采取的措施
E/E/PES	**电气、电子和可编程电子相关安全系统**	摘自 EN 62061：电气、电子和可编程电子相关安全系统
EFTA	**欧洲自由贸易协会**	欧洲自由贸易协会，由欧洲国家创立的一个国际组织
EMC	**电磁兼容性**	设备在电磁环境中有效工作且不过度干扰包含其他设备的环境的能力
ESPE	**电感式防护设备**	摘自 EN 61946-1：设备组件和/或部件协同工作，以实现保护脱扣或存在感应的目的。至少应由以下几个部分组成： ■ 一个感应设备 ■ 控制/监控设备 ■ 输出信号开关设备 (OSSD)
F		
FIT	**故障率单位**	故障率 (10^{-9} h) ➜ $\lambda = 1 \times 10^{-9}$ 1/h
FMEA	**故障模式和影响分析**	故障模式和影响分析。分析影响的步骤 (EN 60812)
功能安全性		与机器和机器控制系统相关的部分总体安全性，取决于 SRECS 的正确功能、其他技术的相关安全系统以及降低风险的外部特征

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

缩写/术语		说明
H		
HFT[n]	**硬件容错**	摘自 EN 62061：在出现故障或失效时继续执行所需功能的能力
h_{OP}	**运行时间**	平均运行时间（天/年）
I		
联锁		联锁设备是一个机械、电气或其他设备，其目的在于防止机器部件在某些特定条件下的运行。
L		
Lambda 值 λ		➜ λ
光幕		一种精确度为 116mm 的 AOPD 设备 （40mm 的精确度适用于手指和手的保护）
LVL	**有限可变语言**	适用范围有限的编程语言。此类语言可以通过组合预定义函数、用户特定函数和库函数以实现安全要求的规范。
M		
MTTFd	**平均无故障时间**	摘自 EN ISO 13849-1：发生危险故障的平均时间
功能抑制		摘自 EN 61496-1：功能抑制。由控制系统的相关安全部件将一个或多个安全功能自动暂停
N		
NC	**常闭**	常闭触点
NO	**常开**	常开触点
n_{OP}	**每年运行的次数**	摘自 EN ISO 13849-1：每年运行的平均次数 $n_{op} = \frac{d_{op} \times h_{op} \times 3600 \frac{s}{h}}{t_{cycle}}$
O		
OSSD	**输出信号切换设备**	连接到机器控制系统的部分电感式防护设备 (ESPE)，在正确运行期间，当传感器部分被触发时会切换到关闭状态
P		
PFHd	**危险性失效概率**	每小时发生危险故障的平均概率 (1/h)
PL	**性能水平**	摘自 EN ISO 13849-1：用于确定控制系统的相关安全部件在可预见的条件下执行安全功能能力的分立等级
防护区域		电感式防护设备 (ESPE) 检测制造商所指定的测试物体的区域
R		
精确度/传感器的检测能力		触发电感式防护设备的传感器参数限制。由制造商确定。
ESPE 的响应时间		从传感器被触发到输出切换元件 (OSSD) 达到关闭状态的最长时间
重启联锁		摘自 EN 61496-1：重启联锁是指在机器运行周期的危险阶段，传感器设备触发之后、机器的运行模式改变之后以及启动机器控制的方式改变之后，为预防机器自动重启而采取的措施

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

缩写/术语		说明
S		
SFF	**安全失效率**	摘自 EN 62061：不会导致危险故障的子系统的总体故障率的系数
SIL	**安全完整性等级**	安全完整性等级。摘自 EN 62061：分立等级（从 1 级到 3 级）用于确定分配给 SRECS 的相关安全控制功能所要求的安全完整性，3 级是安全完整性的最高等级，1 级是最低等级。
SILCL	**SIL 要求限制**	摘自 EN 62061：SIL 要求限制（用于子系统）：SRECS 的子系统有权要求达到的最大安全完整性等级，与结构限制和系统的安全完整性都有关
SRECS	**相关安全电气控制系统**	机器的电气控制系统，其故障将会导致单个或多个风险的立即增加
SRP/CS	**控制系统的相关安全部件**	控制系统的相关安全部件。摘自 EN ISO 13849-1：负责相关安全输入信号以及产生相关安全输出信号的部分控制系统
T		
T_{10d}		部件的运行时间限值。10% 的部件都已经发生了一次危险故障之前的平均时间。 $T_{10d} = \frac{B_{10d}}{n_{op}}$ 对于易磨损部件所确定的 MTTFd 值仅在此时间内适用。
测试棒		摘自 CLC/TS 61496-2：用于验证有源光电防护设备 (AOPD) 检测能力的不透明圆柱形元件

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

用户备注

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

用户备注

© SICK AG •工业安全系统•德国。版权（包括技术规范和信息的更改）所有。

产 品 系 列

工业传感器

我们品种齐全的传感器系列产品可以为任一自动化领域提供应用解决方案，即使在恶劣的条件下仍能可靠地对各种不同形状、表面颜色、光洁度的目标物实现检测，及对计数、定位、距离、位置实现精确的测量。

工业安全保护系统

全面保障人员和机械的安全！作为在传感器技术领域的专家，SICK是最早开发和制造可在危险区域提供保护的产品的先驱。对使用危险设备例如冲床或机器人之间人行通道，提供围绕人身安全防护及保安的解决方案。

自动化辨别系统

我们依照最新的标准，创新自动化识别系统和激光测量系统，使它极其可靠地于短暂的阅读时间内完成包括识别、处理、分类和容量测量。

流程控制系统及分析仪器

由 SICK MAIHAK 根据各种标准及应用，提供过程测量和分析的仪器及服务，解决系统控制、定量，优化过程控制和监测物资流程。


8007988.1005 中文译本 内容如有变更，恕不另行通知

广州市施克传感器有限公司
中国广州市越秀区天河路 45 号
之二天伦大厦 24 楼
电话：020-38303155
传真：020-38303350
网址：www.sick.net.cn

北京分公司
中国北京市朝阳区光华路 12A 号
科伦大厦 A1212 室
电话：010-65812283/5/7
传真：010-65813131
网址：www.sick.net.cn

上海分公司
中国上海市浦东新区民生路 1403 号
上海信息大厦 1603-1605 室
电话：021-33926500/11/22/33
传真：021-33926566
网址：www.sick.net.cn

Guangzhou Head Office:
24/F.Talent Center, No.45 Tian He Road,
Guangzhou, China
Tel: 020-38303155
Fax: 020-38303350
Postal Code: 510075
E-mail: info.china@sick.net.cn

Beijing Branch Office:
A1212, Kelun Tower, 12A Guang Hua Road,
Chaoyang District, Beijing, China
Tel: 010-6581 2283/5/7
Fax: 010-6581 3131
Postal Code: 100020
E-mail: gbj@sick.net.cn

Shanghai Branch Office:
Room 1603-1605, Shanghai Information Tower,
No.1403, Minsheng Road, Pudong New Area Shanghai,China
Tel: 021-3392 6500/11/22/33
Fax: 021-3392 6566
Postal Code: 200135
E-mail: gsh@sick.net.cn

客户服务专线：020-3830 3223　传真：020-3830 3303 / 3830 3250　技术咨询热线：020-3830 3155-251

SICK
Sensor Intelligence.