机械安全指南

六个步骤实现机械安全

SICK
Sensor Intelligence.

六个步骤实现机械安全

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

安全机械为制造商和使用者提供法律保障。机械使用者期望得到安全的机器或设备。这种期望遍及全球。同样地，世界各地也有保护操作人员免受机械伤害的规定。这些规定在地区间存在差异。但在机械制造与升级的程序上有着广泛共识:
在机械制造中，机械制造商必须通过风险评估（以前也称危险分析）识别和评价所有可能的危害和作业危险点。
根据该风险评估，机械制造商应通过适当的设计措施排除或降低风险。若无法借此排除风险或剩余风险不可容忍，则机械制造商须选择和应用适当的保护设备并在必要时告知剩余风险。
为保证计划的措施正常发挥作用，需要整体确认。在整体确证中，必须结合组织措施评价设计与技术措施。

我们将通过六个步骤引导您实现机械安全。工作步骤见左侧。

关于本指南

指南中包含什么?
在您面前的是一本内容丰富的指南，涉及机械相关法律和保护设备的选择与应用。根据适用的欧盟指令、法规及标准，我们向您介绍保护机器和防止事故的不同途径。列出的示例和陈述源于我们多年积累的实践经验，可被视为典型应用。
本指南说明有关欧共体机械及其落实的法律规定。有关其他地区（如北美、亚洲）机械的法律规定将在本指南的其他版本中介绍。
无论基于哪项法律依据，都不能从以下叙述中产生任何索赔，因为在国内与国际法规和标准的背景下，每台机器都需要特定的解决方案。
原则上，我们仅参考出版时最新发布的标准和指令。如果在新标准的过渡期也可以应用旧标准，我们会在本指南的相应章节中注明。

指南供谁使用?
本指南面向制造商、使用者、设计人员、系统工程师以及负责机械安全的所有人。（为了阅读方便，下面我们将大部分使用男性名称。）

您的编辑团队

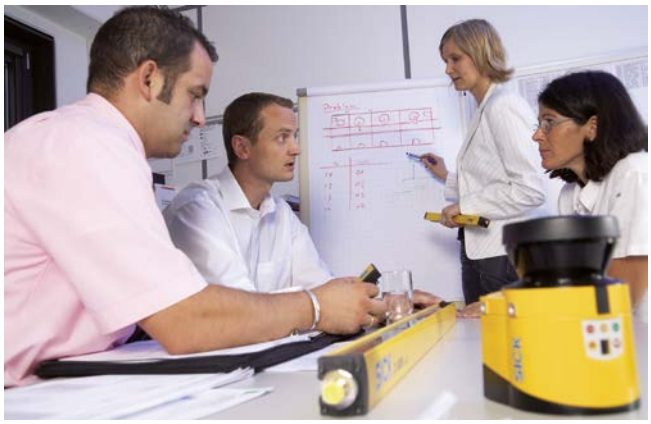
从左至右: Matthias Kurrus、Max Dietrich、Hans-Jörg Stubenrauch、Doris Lilienthal、Harald Schmidt、Rolf Schumacher、Otto Görnemann

➜ 下面我们通过箭头标明参阅更多标准和帮助。

工作流程的防护

随着自动化技术不断发展，对机械防护的要求日新月异。过去，工作流程中的防护装置在某种意义上是一种干扰，所以时常被完全弃用。
创新技术使防护设备集成到工作流程中。因此，它们不再妨碍操作人员，反而经常有助于生产效率的提高。

出于这个原因，集成到工作流程中的可靠防护设备如今已不可或缺。



安全是基本需要

安全是人类的基本需要。研究表明，一直处于紧张环境下的人更容易罹患身心症。尽管人类可以在长时间内适应恶劣环境，但是这将对个人造成巨大负担。
由此得出以下目标：**操作者和维护人员应信赖机器的安全性！**
但人们常常认为，“安全性”提高将导致生产率降低——真实情况正好相反。

更高的安全性意味着更高的积极性和满意度，并最终实现更高的生产率。

安全是一个管理任务

工业中的决策者对其员工以及平稳和合符成本效益的生产负责。只有当管理者在日常事务中践行安全理念时，员工才会同样注意这一问题。

因此，为了改进可持续性，专家提倡在企业内建立广泛的“安全文化”。这不无原因：毕竟十起事故中九起是人为失误导致的。

员工参与促进接受

将操作与维护人员的需要一并纳入理念层面的规划是至关重要。只有与工作流程和人员相协调的智慧安全理念才能实现所需的接受度。

需要专家知识

机械安全在很大程度上取决于指令和标准的正确适用。在欧洲，通过欧盟指令（如机械指令）使国家法规相互协调。
此类指令描述一般要求，并通过标准具体说明。欧洲标准往往也为欧洲以外的国家所接受。

实际地落实所有这些要求，需要广泛的专业知识、应用知识和多年经验。

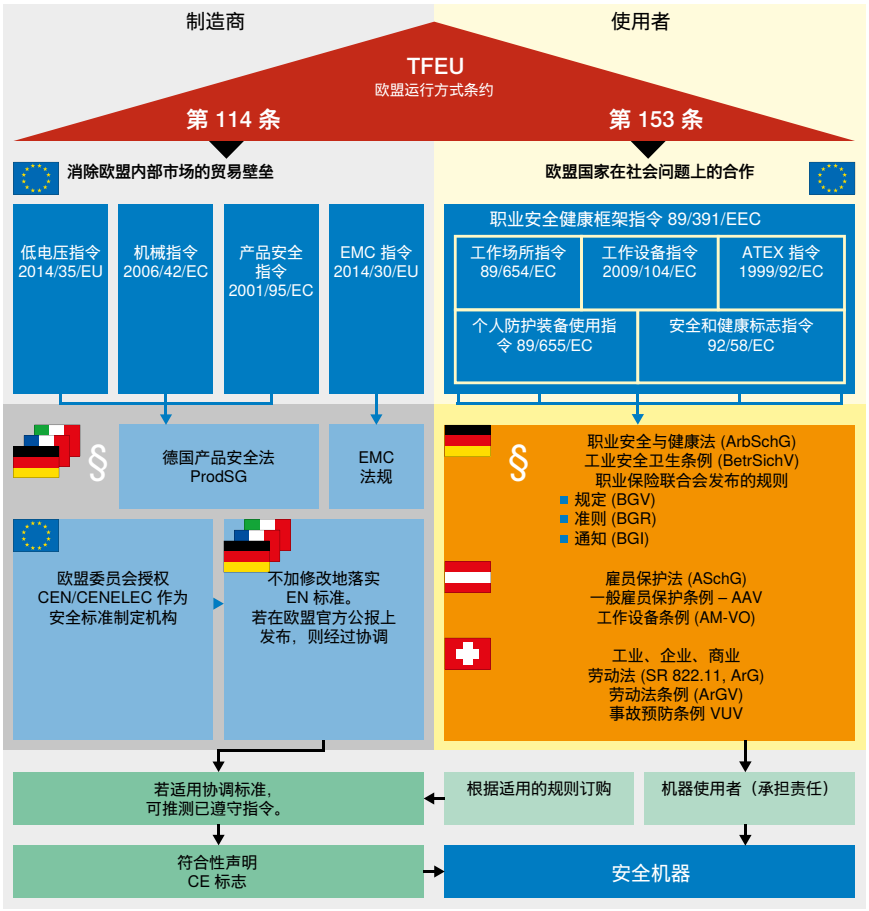
8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

欧盟指令

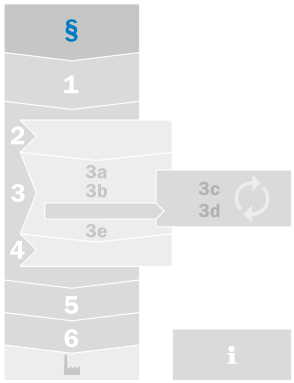
在私人及职业环境中保护公民健康是欧共体的基本原则之一。另一项基本原则是创造保证商品自由流通的单一市场。根据欧盟运行条约，欧盟委员会或欧盟理事会发布了多项指令，旨在同时实现商品自由流通和公民保护。

成员国必须在国内法律中将其落实。这些指令定义了基本目标和要求，并尽可能保持技术中立。在机械安全和劳动保护方面发布了以下指令：

- 面向机械制造商的机械指令
- 面向机械使用者的工作设备指令
- 附加指令，如低电压指令、电磁兼容指令、ATEX 指令



➜ 指令可免费获得，例如登陆 eur-lex.europa.eu



在本章中...

§

欧盟指令和标准适用于制造商或在欧洲经济区供应机械的组织。

机械指令

机械指令 2006/42/EC 面向机械与安全部件的制造商和经销商。其对新机器确定了满足健康与安全要求的任务，以消除欧洲范围内的贸易壁垒并为用户和操作人员保证了一个较高的安全和健康水平 。
其不仅适用于机械制造以及单独投放市场的安全部件，也适用于来自第三方国家 (如美国或日本) 首次在欧洲经济区内投放市场的二手机械和设备。

- 1989 年，欧共体理事会颁布了关于协调各成员国机械法规的指令，即机械指令 (89/392/EEC)。
- 1995 年，该指令必须在所有欧共体成员国适用。
- 1998 年，多项修订汇总并合并在机械指令 98/37/EC 中。
- 2006 年颁布了“新版机械指令”(2006/42/EC) 取代旧版，自 2009 年 12 月 29 日起在所有欧共体成员国强制实施。

自 2009 年 12 月 29 日起，仅实施机械指令 2006/42/EC!

机械指令在德语国家，如下落实:
- 德国: 产品安全法 (ProdSG) 第九条例 (机械条例/9.ProdV) 2011 年 11 月 8 日
- 瑞士: 联邦产品安全法 (PrSG) 2009 年 6 月 12 日和机械安全条例 2008 年 4 月 2 日
- 奥地利: 联邦危险产品防护法 (产品安全法 2004 [PSG 2004]) 和机械安全条例 2010

各成员国不得禁止、限制或妨碍符合机械指令的机器和安全部件投放市场或投入使用。也不得通过国内法律、条例或标准对机械质量提出更高要求!

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

工作设备指令

工作设备指令规定了雇主的义务。其适用于机械和设备在工作场所的使用。该指令确保在使用工作设备时遵守最低要求以改善职业健康与安全。允许各成员国增加本国要求：例如工作设备测试，保养或维护周期，个人防护装备的使用，工作场所设计等。工作设备指令的要求以及国内要求和运行规范又汇编在国内法律中。

- 德国：职业安全与健康法 (ArbSchGes)，工业安全卫生条例 (BetrSichV)
- 瑞士：工业、企业、商业劳动法 (SR 822.11, ArG)
- 奥地利：劳工保护法 (ASchG)

➜ 工作设备指令 2009/104/EC: eur-lex.europa.eu

机械制造商负有哪些义务？

机械的安全设计

制造商有义务遵循机械指令就安全和健康保护的基本要求构造其机器。制造商在设计流程期间就要考虑到安全完整性。在实践中，这意味着设计者在机器的开发阶段就要进行风险评估。由此产生的措施可直接纳入设计。本指南的第 1 到第 5 步详细说明了相关操作。

编制操作指南

机械制造商必须编制操作指南，所谓的“原始使用说明书”。每台机器必须附带一份采用使用国官方语言的操作指南。这份附带的操作指南必须是原始使用说明书或原始使用说明书的译本。在后一种情况下，还要提供原始使用说明书。原始使用说明书——无论采用哪种语言——是机械制造商出版的所有操作指南。

编制技术文件

机械制造商必须根据机械指令的附录 VII 编制技术文件。该技术文件

- 应包括与遵守机械指令中基本安全与健康要求有关的所有平面图、计算说明、测试报告和证明文件。
- 必须从机器 (或机器型号) 制造日期起至少保存十年。
- 必须应合理要求呈交主管部门。

提示： 不能从机械指令得出制造商向机器买主 (用户) 提供完整技术文件的义务。

§

签发符合性声明

机械制造商构建其机器后，须通过签发符合性声明和标记机器（CE 标志）以具有法律约束力的方式证实符合这些规定。然后便可将机器在欧洲经济区内投放市场。

机械指令阐明了完整的符合性评估流程。分为两种机械程序（➜ “对于机械和安全部件的 EC 符合性评估程序” ➜ §-6）

- 标准程序：未在机械指令附录 IV 中明确列出的机械采用标准程序。必须满足附录 I“基本安全和健康要求”一节中的所述要求。据此，制造商自己负责粘贴 CE 标志，不涉及检测机构或主管部门（“自我认证”）。但必须事先汇编机器的技术文件，以便应要求呈交国家主管部门。
- 对于附录 IV 中所列机械的程序：
  高危机械采用特殊流程。机械指令的附录 IV 含有相应机械与安全部件列表，其中也包括电敏防护设备，如安全光电传感器和安全激光扫描仪。必须先满足机械指令附录 I“基本安全和健康要求”一节中的所述要求。若对于机械或安全部件存在覆盖整个要求范围的协调标准，可以三种方式取得符合性证明：
- 自我认证
- 欧盟的认证机构检验样品
- 应用经过检验的全面质量管理体系

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

若对于机械不存在协调标准或是机械或零件并非依据协调标准构造，则只能如下取得符合性证明:

- 欧盟的认证机构检验样品:
  若由认证机构进行检验，则制造商须提供其机械和相关技术文件，以便通过“欧盟样品检验”确定机械是否符合基本安全与健康要求。认证机构将检验与指令的一致性并出具包含检验结果的欧盟样品检验证书。
- 应用经过检验的全面质量管理体系 (QMS): 全面的 QMS 应确保符合机械指令的要求并由认证机构检验。原则上，制造商负责有效和适当地应用 QMS。另请参见机械指令的附录 X。

机器的 CE 标志

满足所有前提条件后，机器必须粘贴 CE 标志。

注意! 只有当机器符合所有适用的欧盟指令时，才能粘贴 CE 标志。(然后才能将产品在欧洲经济区内投放市场。)

特殊情况: 半成品机械

在许多情况下，会制造和交付非常接近机械定义，但不能被视为机械指令意义上的完整机械的部分机械、机械总成或机械组件。机械指令将几乎构成机械，但本身不能履行特定功能的部件总和定义为“半成品机械”。例如单一的工业机器人就是半成品机械。半成品机械仅能用于装入其他机械或其他半成品机械或装置或与其组合成本指令意义上的机械。

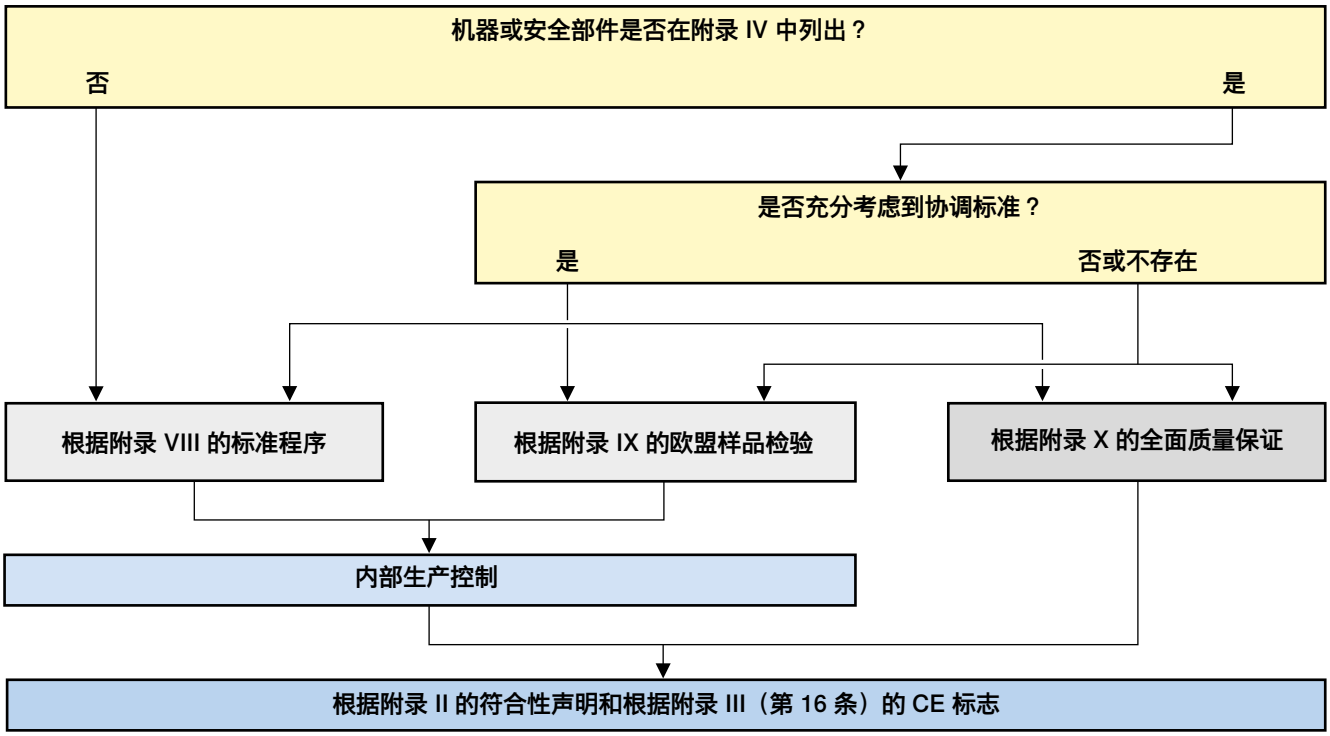
半成品机械不能满足机械指令的所有要求。因此，机械指令也通过特殊程序规定了半成品机械的自由流通:

- 制造商必须遵守机械指令中所有可合理满足的基本安全与健康要求。
- 制造商必须签发公司声明。其中说明适用并遵守了指令的哪些基本要求。半成品机械技术文件的编制和保存与机械类似。
- 制造商必须以相同方式编制装配说明书代替操作指南，随每台“半成品”机械交付。该装配说明书的语言可由制造商与用户（集成商）协定。

➜ 另请参见“检测机构、保险和主管部门”一节 ➜ §-12

§

对于机械和安全部件的 EC 符合性评估程序



总结: 法律、指令

对于机械制造商, 主要适用机械指令:
- 符合机械指令的基本安全与健康要求。
- 在设计流程期间就考虑到安全完整性。
- 采用标准程序或针对机械指令附录 IV 中机械的程序签发符合性声明。
- 汇编机械的技术文件, 特别是所有安全相关设计文档。
- 随附采用使用国官方语言的操作指南。还要附带原始版本。
- 填写符合性声明并用 CE 标志标记机械或安全部件。

对于机械使用者, 适用工作设备指令:
- 遵守工作设备指令的要求。
- 了解是否存在其他国内要求 (如工作设备测试、保养或维护周期等) 并满足这些要求。

8020567/2017-08-22(GCN 2021-07-01)
如有更改, 恕不另行通知

§

标准

本指南基本参考国际标准 (ISO-IEC)。相关标准概览在附录中列出。该概览也包含根据本指南的区域适用性，提到的国际标准 (ISO/IEC) 与区域标准 (EN) 或国家标准的比较。

相关国际和地方标准列在附录 i 中，第 i-6 页及后续各页。

标准是有关各方 (制造商、用户、检测机构、职业安全健康主管部门和政府) 之间达成的约定。与流行观点相反，标准并非由政府或主管部门制定或通过。标准说明在其制定之时的现有技术。在过去的 100 年中，一些可应用于全球性的标准是从一些国家标准发展而成的。根据机器或产品的使用地点，可适用要求应用不同标准的法律规定。正确选择需要应用的标准有助于机械制造商遵守法律要求。

全球标准化组织和结构

ISO (国际标准化组织)
ISO 是一个全球性组织，包括来自 157 个国家的标准化组织。ISO 制定和发布国际标准，重点致力于非电工技术。

IEC (国际电工委员会)
国际电工委员会 (IEC) 是一个全球性组织，制定和发布整个电工领域 (如电子、电信、电磁兼容性、电力) 和相关技术的国际标准。

不同标准类型

分为三种不同标准类型:

A 类标准
(基础安全标准) 包含适用于所有机械的基本概念、设计原则和一般特征。

B 类标准
(通用安全标准) 涉及一种安全特征或广泛用于机械的安全装置。B 类标准又细分为:

- 针对特定安全特征的 B1 类标准，如机器的电气安全、安全距离的计算、对控制系统的要求
- 针对安全装置的 B2 类标准，如双手操纵装置、物理防护设备和电敏防护设备

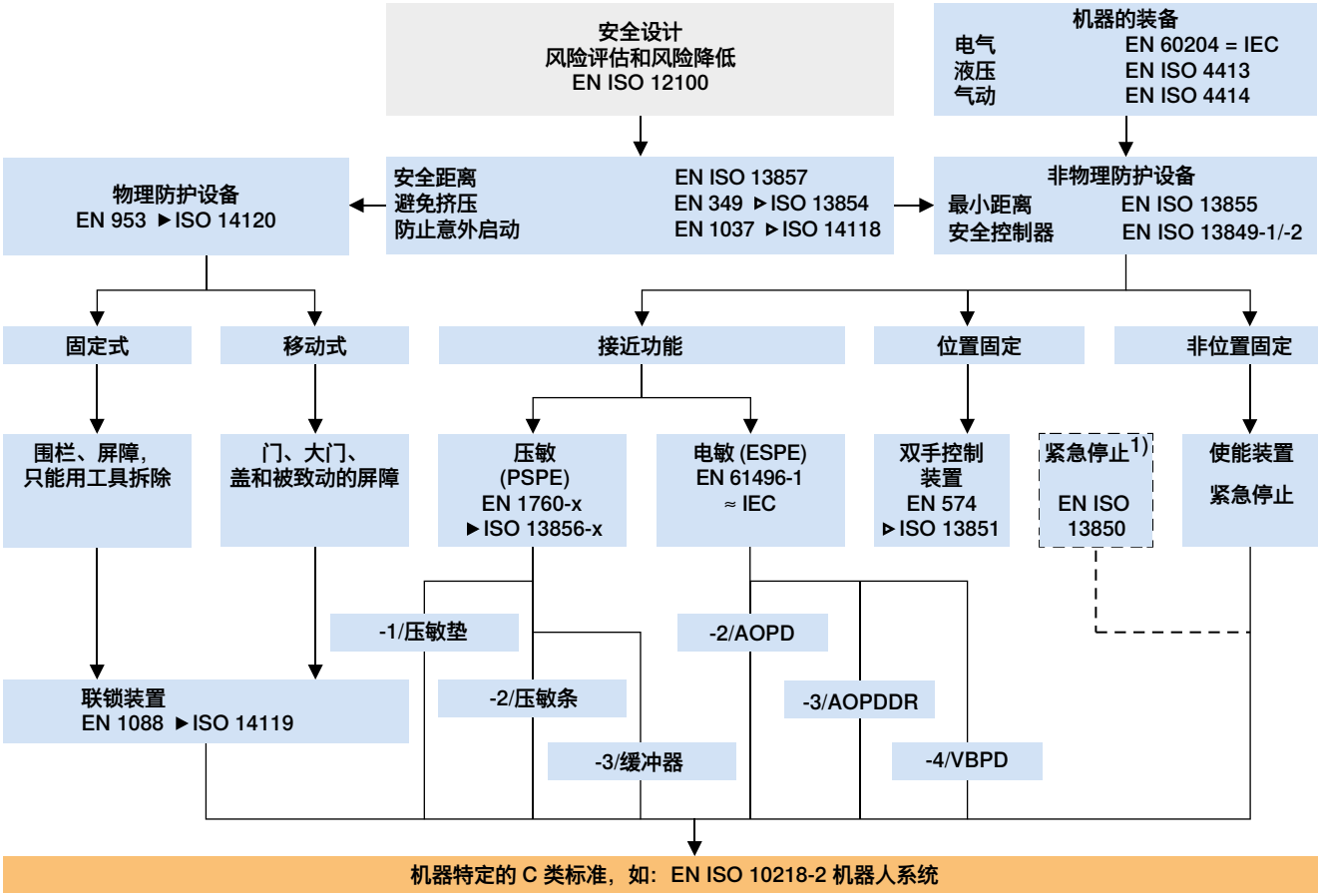
C 类标准
C 类标准包含对特定机械或一种机械结构的所有安全要求。若存在此类标准，则其优先于 A 类或 B 类标准。但 C 类标准仍可引用 B 类或 A 类标准。在任何情况下都应满足机械指令的要求。

许多 A 类和 B 类标准以及重要的 C 类标准目前正在修订。因此，EN ISO 系列标准将引入新的编号体系。但通常有过渡期。因此，五年甚至六年后才能实际适用正在修订的标准。

➜ 重要标准列表参见附录中的“相关标准概览”一节 ➜ i-6

§

防护设备和相关标准概览



1) 紧急停止是一项安全措施，不是防护设备!
▶ EN 标准目前正在修订，将作为 EN ISO 标准发布。
▷ EN 标准未来要进行修订，将作为 EN ISO 标准发布。
AOPD active opto-electronic protective device（有源光电防护设备）
AOPDDR active opto-electronic protective device responsive to diffuse reflection（响应漫反射的有源光电防护设备）
VBPD vision based protective device（基于视觉的防护设备）

A 类标准
B 类标准
C 类标准

欧洲标准化组织和结构

CEN (Comité Européen de Normalisation/欧洲标准化委员会)
CEN 是由欧盟成员国、EFTA 国家以及欧盟新成员的标准化组织组成的团体。CEN 制定非电工领域的欧洲标准 (EN)。为避免这些标准构成贸易壁垒, CEN 尽力与 ISO 紧密合作。CEN 通过表决程序决定是否采用 ISO 标准并将其作为欧洲标准发布。

CENELEC (Comité Européen de Normalisation Electrotechnique/欧洲电工标准化委员会)
CENELEC 是在电工领域与 CEN 相似的机构, 负责制定和公布该领域的欧洲标准 (EN)。类似 CEN 与 ISO 之间的关系, CENELEC 也越来越多地采用 IEC 标准及其编号体系。

国家标准化组织和结构

通常欧盟成员国都有各自的标准化组织, 如 DIN、ON、BSI、AFNOR。其根据相应成员国的法律要求制定和公布国家标准。为保证欧洲共同体内统一的安全及健康要求和消除贸易壁垒, 国家标准化组织采用了欧洲标准。

国家标准与欧洲标准之间的关系适用以下原则:

- 若存在与所采用的欧洲标准类似的国家标准, 应予以撤销。
- 若没有适用于某些特征或机械的欧洲标准, 可适用现有国际标准。
- 只有当已通告该项计划并且在欧洲层面上 (CEN 或 CENELEC) 没有兴趣时, 才允许国家标准化组织制定新的国家标准。

§

欧洲机械安全标准

为了在实践中统一落实欧盟指令中定义的目标和要求，技术标准应详细描述和具体说明这些要求。
以遵守标准即可推定符合指令的方式具体说明欧盟指令要求的标准被视为协调标准。
通过不同缩写显示标准状态:

- 带“EN”前缀的标准在所有欧盟国家承认和适用。
- 带“prEN”前缀的标准目前在准备中。
- 另外包含“TS”作为前缀的文件是技术规范并充当预备标准。其分为 CLC/TS 和 CEN/TS。
- 另外包含“TR”作为前缀的文件是现有技术报告。

欧盟协调标准的产生方式如下:

1. 作为欧盟的执行机构，欧盟委员会授权 CEN 或 CENELEC 制定具体说明指令要求的欧洲标准。
2. 制定工作在国际团体中展开，在此期间将确定满足指令基本安全要求的技术规范。
3. 一旦表决通过标准，即在欧盟官方公报上发布。另外，标准应至少在一个成员国公布（如作为 DIN EN）。欧盟协调标准由此产生。

- 欧盟协调标准作为参考使用，可替代同一主题的所有国家标准。
- 符合适用的协调标准即可推定机械或安全部件满足指令（如机械指令）的相应基本安全与健康要求（符合性推定）。

➜ 标准化概览: www.normapme.com
➜ 对指令具有推定符合性的标准列表参见 ec.europa.eu

- 机械指令不要求适用协调或非协调标准。但适用协调标准为所谓的“推定符合性”（机器满足机械指令要求）提供了依据。
- 若存在针对一种机械类型的 C 类标准，则其优先于所有其他 A 类和 B 类标准及本指南中的任何信息。在这种情况下，只有适用的 C 类标准为满足机械指令要求的推定符合性提供依据。

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

总结: 标准

- 技术标准具体说明欧盟指令中定义的目标。
- 适用协调标准为所谓的“推定符合性”，即推定机器满足指令要求，提供了依据。也就是说，为机械或设备选择和适用正确标准便可认定遵守了法律要求。在个别情况下，制造商义务可能超出标准内容，例如当标准不再符合现有技术时。
- 有 A 类标准（基础安全标准）、B 类标准（通用安全标准）和 C 类标准（机械安全标准）。若存在 C 类标准，则其优先于 A 类或 B 类标准。

§

检测机构、保险和主管部门

检测机构

提供安全建议的检测机构
想知道其机器是否符合适用的各项欧盟指令和标准的公司，可以请检测机构提供安全技术方面的建议。

官方认可的检测机构
官方认可的检测机构是能证明遵守公认国家机构的检测程序和检测标准的检测机构。主要包括通常拥有非常优秀的专业检测机构的意外保险机构和职业保险检测机构。

公告机构
欧共体各成员国有义务按照机械指令中确定的最低要求指定检测机构并将这些机构通报位于布鲁塞尔的欧盟委员会。
只有这些检测机构有权执行欧盟样品检验和为机械指令附录 IV 中列出的机械与安全部件签发欧盟样品检验证书。并非所有公告机构都能检测任何种类的产品或机械。许多检测机构仅获得特定工作领域的授权。

保险

职业保险联合会/IFA——德国法定意外保险的职业安全健康机构
在德国，职业保险联合会和其他组织承担法定意外保险义务。职业保险联合会采用专业协会的组织形式，以便更好地满足各个经济部门的特定要求。

保险公司
许多保险公司都设有咨询处，可提供合理的专业建议，特别是如何避免因不知道或未遵守法律要求而产生的责任风险。

市场监督 - 主管部门

在欧盟和 EFTA 国家，劳动保护和市场监督是国家主管部门的职责。

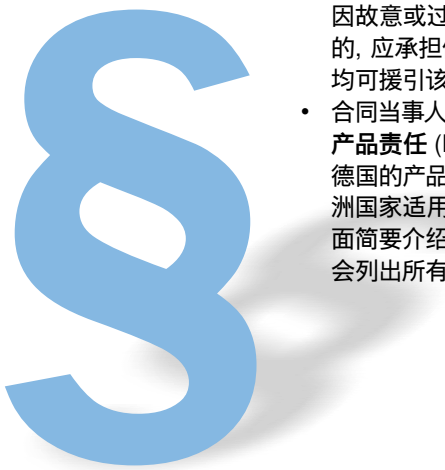
- 在德国，它是联邦州职业安全与健康局的职责。
- 奥地利设有一系列职业安全检查团。机械制造商也可以联系国家主管部门在机械安全与工作安全的问题上获得专业建议。
- 在瑞士，联邦政府经济事务秘书处 (SECO) 负责市场监督。瑞士国家工伤保险机构 (Suva) 凭借其高水平的技术专长负责执行。

➜ 重要地址参见附录中的“常用链接”一节 ➜ i-8.

基础的产品责任

产品责任概念常用作生产者或销售者对产品负有的任何种类责任的总称（包括产品瑕疵责任或损害赔偿责任）。但在法律评价上，根据损害方式或起因的不同存在巨大差异。首先应区分瑕疵责任和广义的产品责任。

瑕疵责任（也称担保）是对产品自身瑕疵所负有的责任。只能在合同当事人之间，不能由第三人提出源于瑕疵责任的索赔。



广义的产品责任可进一步细分：

- **侵权责任**（在《德国民法典》第 823 条中规定）。
  因故意或过失（例如通过所生产的产品）对他人造成损害的，应承担侵权责任。若存在其他必要条件，则任何受害人均可援引该规定，包括非合同当事人（所谓的第三人）。
- 合同当事人和第三人都能援引（实际的）**依照产品责任法的产品责任**（ProdHaftG）。
  德国的产品责任法基于欧盟指令。因此，类似规定在所有欧洲国家适用。另外，相应规定也在许多非欧洲国家适用。下面简要介绍在德国法律中适用的规定。但仅阐明关键点，不会列出所有必要条件或免责事由。

必要条件

在产品责任法第 1 条中对制造人责任的规定如下：

> “如果产品缺陷造成他人死亡、人身或者健康伤害或财产损害，产品制造人有义务对由此产生的损失予以赔偿。”

由此产生以下必要条件：

制造人（产品责任法第 4 条）
其必须将产品投入流通。也包括将产品进口到欧洲经济区或将其他制造人的产品贴上自己的商标作为自有品牌产品销售的人（所谓的“准制造人”）。

缺陷产品（产品责任法第 3 条）
考虑到所有情况，不能提供人们有权期待的安全性的产品。

缺陷产品造成的损害：人身或者健康伤害或财产损害（但并非产品自身，而是通常用于个人使用或消费的和主要由受害人相应使用的财产）。纯粹经济损失不能通过产品责任法赔偿。唯一例外是当经济损失是人身或者健康伤害或产品责任法涉及的财产损害的直接结果（如医疗费用、因谋生能力降低导致的年金）时。
与担保责任或侵权责任引起的损害赔偿不同，依照产品责任法的责任不需要存在过错。也就是说，即便遵守商品流通中必要的注意义务也可能存在责任（亦即在无过失的情况下）。这是一种所谓的严格责任：如果在许可活动范围内存在稍后将变为现实的危险，就有充分的责任依据。

§

制造人义务

可以为依照产品责任法的责任提供依据的缺陷有多种类型:

设计缺陷
此类缺陷由产品设计造成，如技术设计或材料选择，并影响整个生产。

制造缺陷
制造缺陷是单个产品或批次出现的缺陷。根据产品责任法，制造人也对不可避免的缺陷负有责任。

指示缺陷
如果因产品指示有误（例如在操作说明书中）而引起风险，则存在指示缺陷。其中也包括缺少或遮挡警告提示。在此制造人应针对见闻较少的用户，也要考虑到产品可预期的误用。产品责任法使制造人负有在开发和生产期间及指示中确保产品安全的义务。

在此特别要注意遵守强制性法规——如果缺陷（只）是由遵守这些法规造成的，则制造人不承担责任。在这种情况下，技术标准（欧洲标准 – EN – 或 DIN、VDE 等国家标准）应被视为保证所需安全性的最低标准。制造人的义务可能不只是遵守法律或技术标准，如果人们有权期待确保产品安全的进一步措施。

于是，根据高等法院判决，遵守 EN 标准不再足以履行制造人负有的流通安全义务，如果发展情况已超出 EN 标准或使用设备将产生 EN 标准中未考虑到的危险。

损害程度

原则上，制造人应全额赔偿对受害人造成的损害。德国产品责任法仅对人身伤害赔偿规定了限额。在此适用最高 8500 万欧元的责任限额。因缺少合同不能对第三人，也不允许在一般交易条款或个别合同中对合同当事人进一步限制赔偿责任。

制造人可通过购买产品责任险获得充分保护。

总结: 产品责任

- 避免依照产品责任法的制造人责任:
  - 遵守适用标准。
  - 检查是否需要确保产品安全的附加措施。
- 通过持续的质量保证和质量检查避免缺陷。
- 通过足额保险最大限度降低制造人面临的剩余风险。

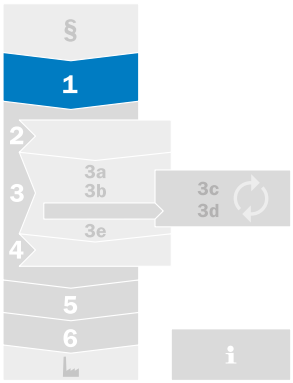
还要指出——如果不存在举证责任倒置——出现损失时，原则上由受害人承担证明缺陷产品造成人身伤害或财产损害并与产生的损失有因果关系的责任。这项任务没有那么简单，特别是有多种可能原因需要考虑时。

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

第 1 步: 风险评估

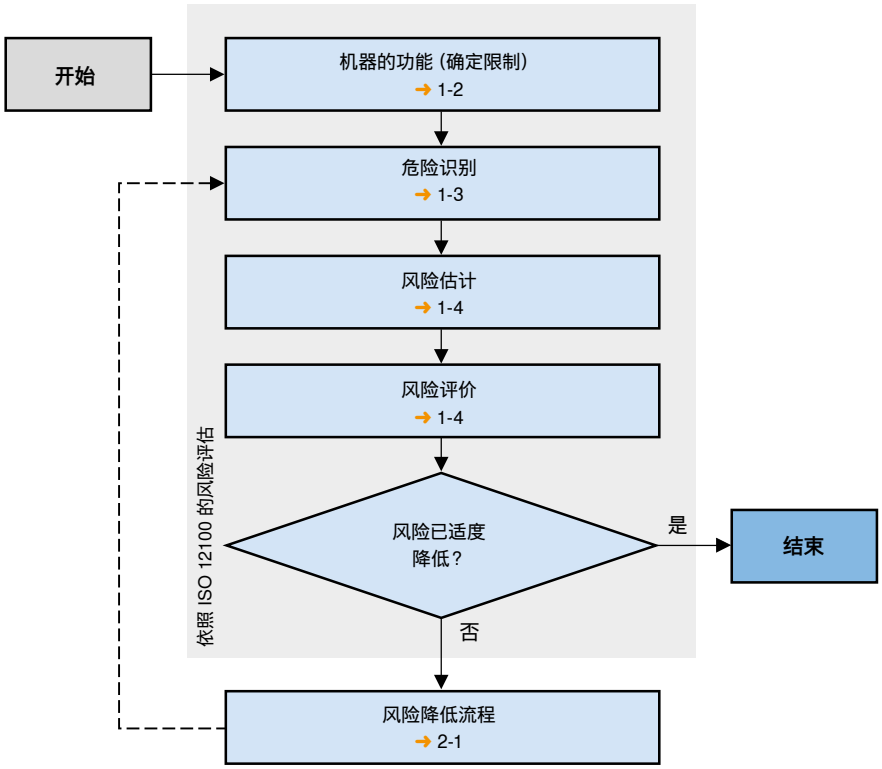
设计机器时，必须分析可能的风险并在必要时采取附加措施保护操作人员免受潜在危险。
为了在这项任务中为机械制造商提供帮助，标准定义并描述了风险评估流程。风险评估是允许系统分析和评价风险的一系列逻辑步骤。必须在考虑到风险评估结果的情况下设计和制造机器。

如有需要，继风险评估后，采取适当的防护措施来降低风险。不能因采取防护措施而产生新的风险。为了尽可能排除危险和充分降低识别到的或新增加的风险，可能需要重复风险评估和风险降低的整个流程。在许多 C 类标准中规定了有关特定机器和贴近应用的风险评估。如无 C 类标准可适用或其不充分，可引用 A 类或 B 类标准的要求。



➜ 安全设计、风险评估和风险降低A 类标准: ISO 12100

风险评估流程



在本章中...

- 必须对所有危险执行上述流程。必须不断重复（迭代过程），直至剩余的遗留风险在可接受的较低水平。
- 应记录所取得的风险评估结果和应用的程序。

机器的功能（确定限制）

风险评估从确定机器的功能开始。可能包括：

- 机器的规格说明书（生产什么、最大产量、所用材料）
- 空间限制和预计使用地点
- 计划使用寿命
- 预期功能和操作模式
- 可预计的故障和干扰
- 参与机器流程的人员
- 与机器有关的产品
- 预期用途、操作人员的意外行为以及可合理预见的机器误用（滥用）

可预见的误用

可合理假定的操作人员的意外行为或可预见的误用主要包括：

- 操作人员对机器失去控制（特别是手持式或便携式机械）
- 在使用机器期间，发生故障、干扰或失效时人员的反射性行为
- 不专心或疏忽导致的人为失误
- 在执行任务过程中，可归因于选择“最小阻力路径”的人为失误
- 处于无论如何都要保持机器运行的压力之下的行为
- 特定人群的行为（如儿童、青少年、残疾人）

可预计的故障和干扰

运行功能相关组件（尤其是控制系统组件）的故障和干扰有巨大潜在危险。示例：

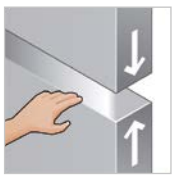
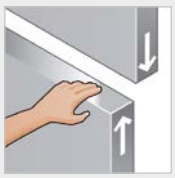
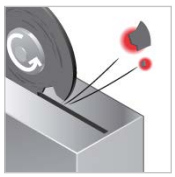
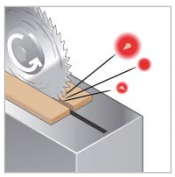
- 辊子反向运动（以致手被卷入）
- 机器人在其程序化的工作区域之外运动

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

危险识别

继确定机器的功能后，是机器风险评估中最重要的步骤。
包括系统识别可预见的危险、危险状态和/或危险事件。

机械制造商尤其应考虑下列危险…	…在机器使用寿命内的所有阶段。
• 机械危险 • 电气危险 • 热危险 • 噪声引起的危险 • 振动引起的危险 • 辐射引起的危险 • 材料和物质引起的危险 • 设计机器时忽视人类工效学原则引起的危险 • 滑倒、绊倒和跌倒引起的危险 • 与机器使用环境有关的危险 • 上述危险组合而成的危险	• 运输、组装和安装 • 调试 • 设置 • 正常使用和故障排除 • 维护和清洁 • 停用、拆卸和处置

机器/设备上的机械危险示例			
	切断		挤压
	剪切		刺穿
	卷入或陷入		卷入或陷入
	缠绕		碰撞
	碎片带来的冲击		飞溅带来的冲击

风险估计与风险评价

识别完危险后，应对考虑到的每种危险状态进行**风险估计**。

风险	=	伤害程度	×	发生概率

与考虑到的危险状态有关的风险取决于以下要素:

- 危险可能造成的损害程度（轻微伤害、严重伤害等）和
- 发生该损害的概率。其由下列因素决定:
  - 人员暴露于危险
  - 危险事件的发生
  - 从技术和人员上避免或限制损害的可能性

有多种工具可用于估计风险，如表格、风险图、数值法等。
在**风险评价**中，根据风险估计结果确定是否需要采取防护措施和何时已实现必要的风险降低。

➜ 工具和表格: 技术报告 – ISO/TR 14121-2

文件

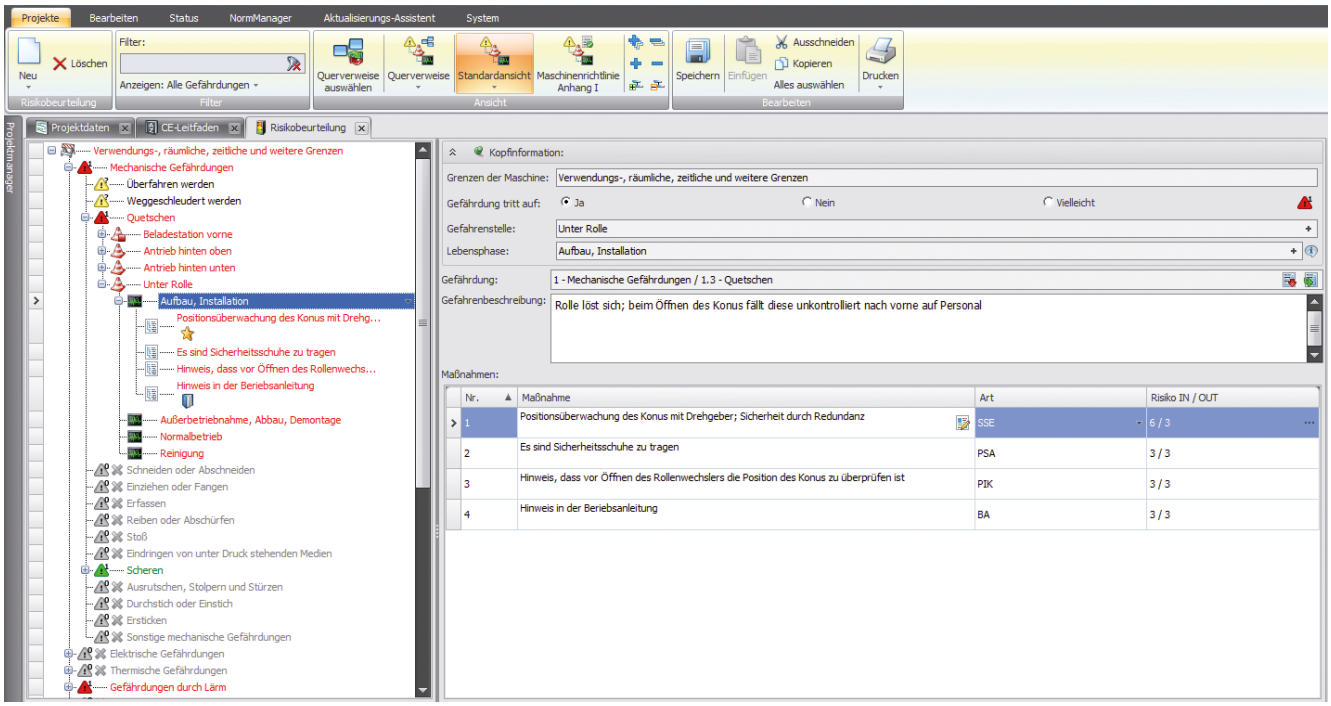
风险评估文件应包含所应用的程序和取得的结果以及下列信息:

- 机器的相关信息，如规格、限制、预期用途等
- 做过的重要假设，如载荷、强度、安全系数
- 所有已识别的危险、危险状态和纳入考量的危险事件
- 所使用的数据及其来源，如事故历史和在类似机器上降低风险的经验
- 所采用防护措施的说明
- 可通过这些防护措施实现的风险降低目标的说明
- 与机器有关的遗留风险
- 在风险评估期间制定的所有文档

机械指令不要求将风险评估文件与机器一起递交!

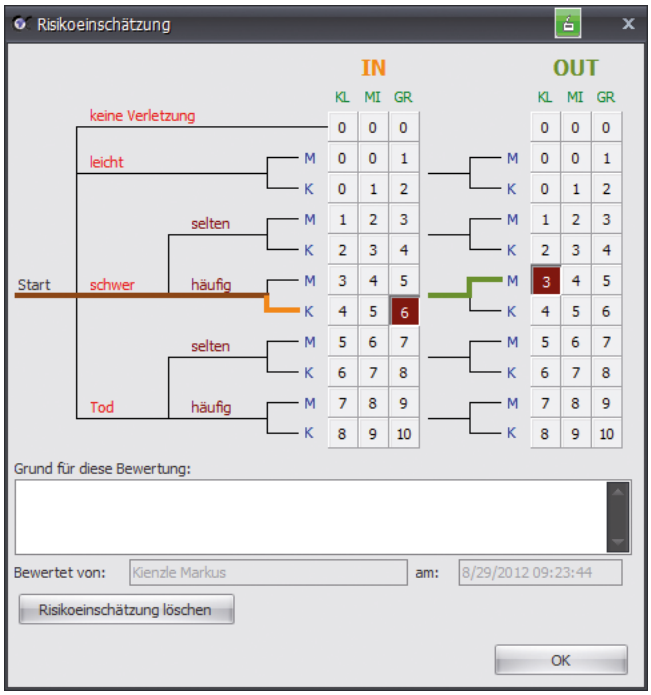
8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

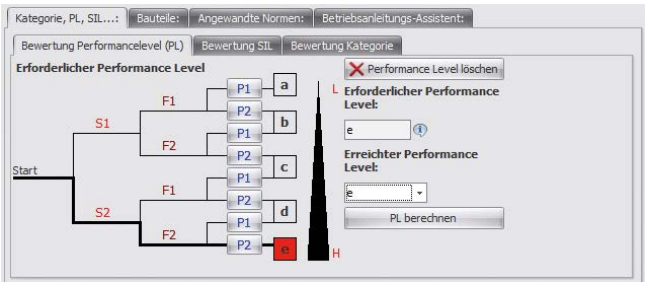
通过 Safexpert® 做风险评估



风险评估流程已在 Safexpert® (CE 管理软件) 中创建。用户在引导下达到法律和标准要求。通过存储的危险列表、用于结构化风险评估的 CE 管理和风险评价图、以及控制技术措施所需安全等级工具简化了工作。借助标准管理和更新助手使所需标准始终保持最新状态。根据作业危险点和机器所处的相应寿命阶段分别考量危险。单独评价危险实现更好的选择排除危 险或降低风险的措施。在 Safexpert® 中采用风险图与矩阵 (表 格) 相结合。在选择防护措施 (如防护设备) 之前 (IN) 和之后 (OUT) 进行评估。风险在 0 (无风险) 到 10 (最高风险) 的范围 内划分。

Safexpert® 不仅用于风险评估。也可以借助 Safexpert® 高效执行并记录依照机械指令的整个符合性流程。





总结: 风险评估

一般性说明

- 对所有危险执行风险评估。该迭代过程必须考虑到所有危险和风险，直至没有或仅剩余可接受的较低遗留风险。

风险评估流程

- 从确定机器的功能开始风险评估。
- 在风险评估中尤其考虑到可预见的误用和干扰。
- 然后识别机器带来的危险（机械危险、电气危险、热危险等）。在机器使用寿命内的所有阶段考虑这些危险。
- 然后估计危险带来的风险。其取决于损害程度和发生损害的概率。
- 记录风险评估的结果。

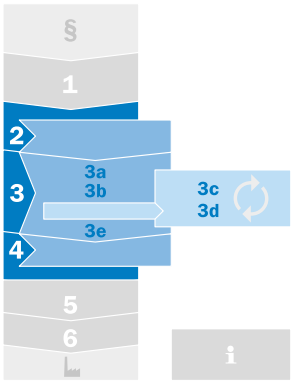
8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

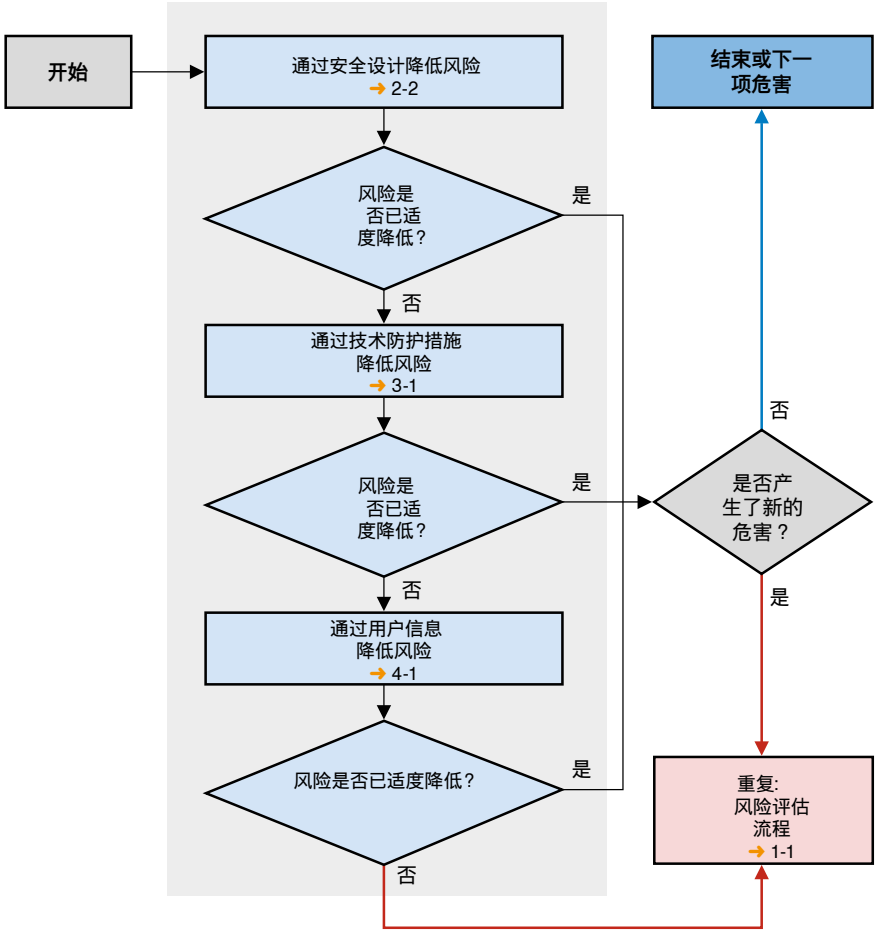
第 2 到第 4 步: 风险降低

若风险评价表明需要最大限度降低风险的措施, 则须采用 3 步法。

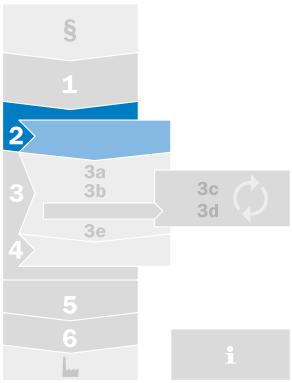
3 步法

1. 机械制造商在选择措施时必须应用以下原则, 亦即按照给定的顺序:
2. 安全设计: 消除或尽可能降低风险 (机器设计与结构上的安全完整性)
3. 技术防护措施: 采取必要的防护措施 防范无法从设计上消除的风险 关于剩余风险的用户信息





→ 风险降低流程的一般原则: ISO 12100 (A 类标准)



2

在本章中...

第 2 步: 安全设计 (本质安全设计)

安全设计是风险降低流程中的第一步, 也是最重要的一步。在此通过设计即可排除可能的危险。所以安全设计是更有 效的方法。
安全设计的方面涉及机器结构和遭到危险的人员与机器之间的相互作用。

示例:

- 机械设计
- 操作与维修理念
- 电气装备 (电气安全、EMC)
- 紧急停机的理念
- 流体技术装备
- 所使用的原料和耗材
- 机器功能和生产流程

在任何情况下, 选择、应用和调整所有组件的方式应确保当机器出现故障时优先考虑人员安全。也要注意避免危害机器和环境。机器结构的所有组成部分应详细说明, 确保其在允许限值内正常工作。原则上, 设计应尽可能简单。安全相关功能应尽可能同其他功能分开。

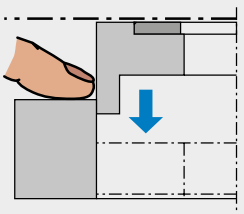
机械设计

每个设计的首要目标必须是防止危险的发生。例如通过以下方式实现:

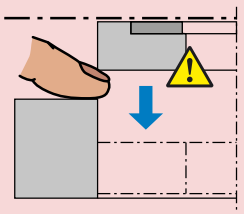
- 避免锐边、尖角和凸出部分
- 避免挤压点、剪切点和绞绕点
- 限制动能 (重量和速度)
- 遵守人类工效学原则

示例: 避免剪切点

正确

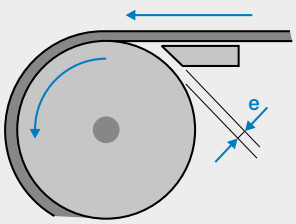


错误

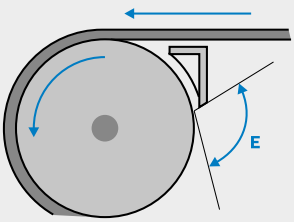


来源: Neudörfer

示例: 避免绞绕点



间距 e 应 ≤ 6 mm !



角度 E 应 ≥ 90° !

来源: Neudörfer

➜ Alfred Neudörfer: sicherheitsgerechter Produkte (符合安全产品的设计), Springer-Verlag, Berlin u. a., ISBN 978-3-642-33889-2 (2013 年第 5 版)

8020567/2017-08-22(GCN 2021-07-01)
如有更改, 恕不另行通知

操作与维修理念

暴露于危险区域的必要性应尽可能的低。例如可通过以下方式实现:

- 自动上下料工作站
- 从“外面”进行设置和维护工作
- 使用可靠且可用的部件以避免维护工作
- 清晰明确的操作理念，例如操作件的清晰标记

颜色标记

按钮的操作件以及指示灯或屏幕上的显示以颜色标记。各个颜色被赋予了不同含义。

➜ 机器的电气装备: IEC 60204-1

操作件颜色的一般含义

颜色	含义	解释
白色 灰色 黑色	非特定	启动功能
绿色	安全	在安全操作期间致动或为了建立正常状态
红色	紧急情况	在危险状态或紧急情况下致动
蓝色	指示	在需要强制行动的状态下致动
黄色	异常	在异常状态下致动

指示灯颜色的一般含义

颜色	含义	解释
白色	中性	对使用绿色、红色、蓝色还是黄色有疑问时使用
绿色	正常状态	
红色	紧急情况	危险状态，通过立即行动回应
蓝色	强制	显示需要操作人员强制行动的状态
黄色	异常	异常状态，即将到来的危急状态

电气装备

需要采取措施来排除机器上的电气危险。在此分为两种危险类型:

- 因电流而产生的危险，也就是直接和间接触电带来的危害
- 由于控制系统的故障情况间接导致的危险

➜ 在下面几节中将提供有关电气装备设计的重要信息。
➜ 机器的电气装备: IEC 60204-1

2

电源接口

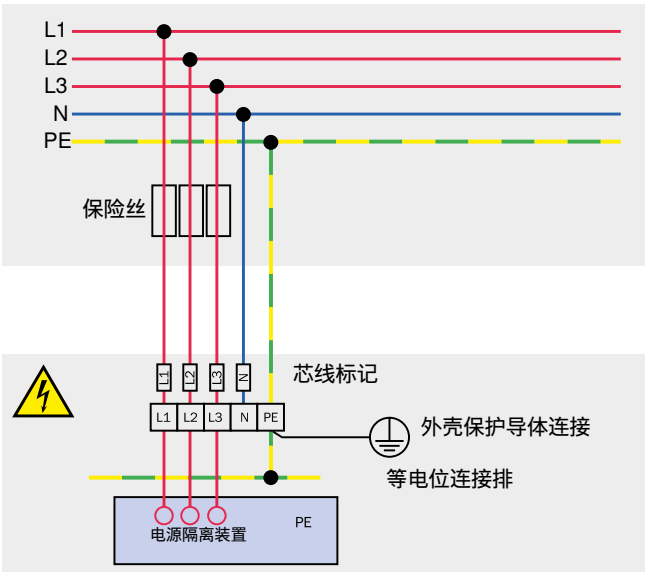
电源接口是机器的电气装备与供电网络之间的接口。应遵守相应电网运营商关于该接口的规定。

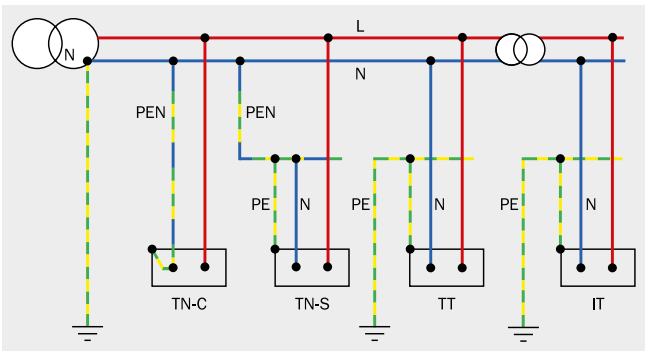
在安全技术应用中尤其需要稳定的电源供给。因此，电源供应器应当能够缓冲短时间停电。

接地系统
接地系统表明馈电变压器二次侧的接地种类和电气装备机箱的接地种类。国际上有三种标准化的接地系统:

- TN 系统
- TT 系统
- IT 系统

接地是指与大地的导电连接。分为有助于电气安全的保护接地 PE 和用于其他目的的功能接地 FE。保护导体系统由接地装置、连接导线和相应端子组成。电源供应器上电气装备的所有机箱都要与保护导体系统相连以实现等电位保护联结。等电位保护联结是在故障情况下提供保护的基本手段。





8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

TN 系统
TN 系统是低压系统中较常见的电网形式。在 TN 系统中，变压器的中性点直接接地（工作接地）；已连接设备的机箱经由保护导体（PE）与变压器的中性点相连。
根据所敷设导线的截面，PE 线和 N 线作为一根合并线（TN-C 系统）或两根独立线（TN-S 系统）。

TT 系统
在 TT 系统中，馈电变压器中性点的接地方式和在 TN 系统中一样。连接到设备导电外壳的保护导体未被敷设至该中性点，而是单独接地。设备机箱也可以通过共用的保护接地装置接地。
TT 系统通常只与漏电断路器配合使用。
TT 系统的优点是在长距离路途中提供更高的可靠性。

IT 系统
在 IT 系统中，设备导电外壳的接地方式和在 TT 系统中一样，但馈电变压器中性点的接地方式不同。断电将有一定危险，因此当仅发生一次碰壳或接地故障时还不得断电的系统被设计为 IT 系统。
例如，在低压范围内规定使用 IT 系统给医院内的手术室和重症监护室供电。

➜ 防护措施：IEC 60364-4-41，包含不同国家修订

电源隔离装置

必须为连接一台或多台机器的各个电源接口提供电源隔离装置。其应当能够使电气装备同电源供应器隔离：
- 使用类别为 AC-23B 或 DC-23B 的负荷隔离开关
- 带有超前切负荷的辅助触点的隔离开关
- 断路器
- 最高 16 A/3 kW 的插头/插座组合

某些电路，如联锁装置的控制电路，不必通过隔离装置断电。在这种情况下，必须采取特殊的预防措施以确保操作人员的安全。

防止意外启动的切断装置

在维修工作期间，机器启动或电力恢复不得对维修人员产生危险。因此，必须采取防止意外和/或错误关闭电源隔离装置的方法。

例如，可通过当主开关处于“关”位置时将挂锁挂在其把手上实现。

该切断装置不适合用作为操作目的而短暂介入危险区域的防护措施。

电击防护

防护等级

不同防护等级的划分表明采用哪些方法实现单一故障安全。该分类不代表防护程度。

防护等级 I

所有采用单一绝缘（基本绝缘）并连接保护导体的设备属于防护等级 I。保护导体必须与标有接地符号或 PE 的端子连接，颜色为绿黄相间。

防护等级 II

防护等级 II 的设备采用加强或双重绝缘，不连接保护导体。该防护措施也称为保护绝缘。不得连接保护导体。

防护等级 III

防护等级 III 的设备在安全超低电压下工作，因此不需要明确保护。

安全超低电压 SELV/PELV

不超过 50 V 有效值 (Vrms) 的交流电压和不超过 120 V 的直流电压允许作为安全超低电压。另外，超过 75 V 限制的直流电压应满足低电压指令的要求。

在通常干燥的场所内应用时，可省去直接触电防护（基本防护），前提是交流电压的有效值不超过 25 V 或无谐波直流电压不超过 60 V。当直流电压与最高 10% rms 的正弦交流电压部分叠加时，便得到无谐波。

安全超低电压电路必须同其他电路安全分开（足够的电气间隙和爬电距离、绝缘、电路与保护导体连接等）。

分为:

- SELV（安全特低电压）
- PELV（保护特低电压）

不得从电源通过自耦变压器、分压器或串联电阻产生安全超低电压。

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

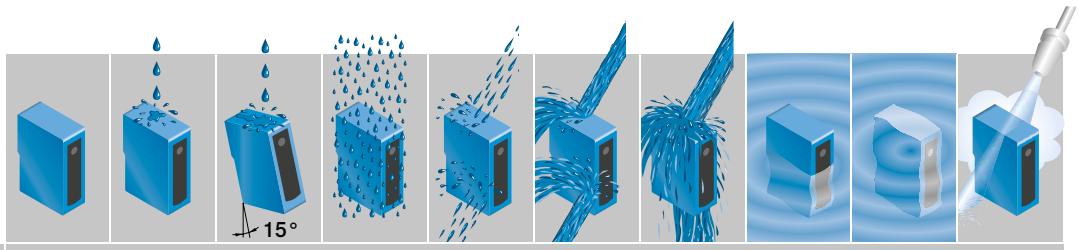
		ELV (AC < 50 V_{rms}, DC < 120 V)	
		SELV	PELV
隔离种类	电源	采用安全隔离 (如安全变压器) 的电源或等价电源	
	电路	• 同其他非 SELV 或非 PELV 电路安全分开的电路 • 在 SELV 与 PELV 电路之间采用基本绝缘的电路	
与大地或保护导体的关系	电路	不接地电路	接地或不接地电路
	外壳	不得将外壳有意接地或与保护导体相连。	允许将外壳接地或与保护导体相连。
附加措施	标称电压: • AC > 25 V 或 • DC > 60 V 或 • 设备在水中	通过符合标准的绝缘或装箱提供基本防护	
	在通常干燥环境下的标称电压: • AC ≤ 25 V 或 • DC ≤ 60 V	无需附加措施校准	基本防护方式: • 符合标准的绝缘或装箱或 • 机箱和带电部件与主接地排相连

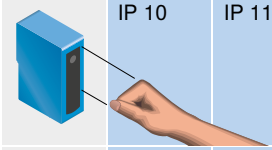
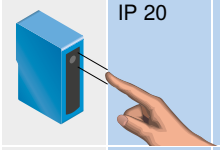
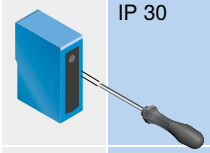
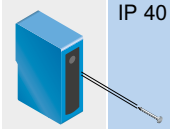
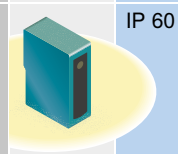
➜ 防护等级: EN 50178
➜ 变压器安全: EN 61558 系列

2

防护措施/外壳防护等级

外壳防护等级说明防止水 (非水蒸气) 和异物 (粉尘) 侵入设备的能力。另外, 其还说明防止直接接触带电部分的能力。原则上始终需要该防护, 即使在低电压下。所有断开后仍然带电的可接触部分必须至少具备外壳防护等级 IP 2 x, 控制柜必须至少达到外壳防护等级 IP 54。



1.特征数字: 防止固体异物侵入的能力		2.特征数字: 防止水（非水蒸气、非其他液体！）侵入的能力									
		IP ...0	IP ...1	IP ...2	IP ...3	IP ...4	IP ...5	IP ...6	IP ...7	IP ...8	IP ...9K
		没有保护	滴水 垂直	滴水 倾斜	淋水	溅水	喷水	猛烈喷水	浸水 短时间	浸水 持续	100 bar, 16 l/min., 80 °C
IP 0... 没有保护		IP 00									
IP 1... 直径 ≥ 50 mm 的固体异物		IP 10	IP 11	IP 12							
IP 2... 直径 ≥ 12 mm 的固体异物		IP 20	IP 21	IP 22	IP 23						
IP 3... 直径 ≥ 2.5 mm 的固体异物		IP 30	IP 31	IP 32	IP 33	IP 34					
IP 4... 直径 ≥ 1 mm 的固体异物		IP 40	IP 41	IP 42	IP 43	IP 44					
IP 5... 防尘		IP 50			IP 53	IP 54	IP 55	IP 56			
IP 6... 尘密		IP 60					IP 65	IP 66	IP 67		IP 69K

➜ 外壳防护等级: EN 60529

8020567/2017-08-22(GCN 2021-07-01)
如有更改, 恕不另行通知

停机

除了在正常操作期间停机，出于安全原因，也必须能够在紧急情况下停止机器。

要求

- 每台机器都要配备用于在正常操作期间停止整台机器的指令装置。
- 必须至少具有类别 0 的停止功能。出于机器在安全技术和功能技术上的要求，可能需要类别 1 和/或类别 2 的附加停止功能。
- 停止机器的指令必须优先于启动机器的指令。使机器或其危险部件停止后，必须切断驱动装置的供电。

停止类别

有不同类别的停止功能满足机器在安全技术和功能技术上的要求。请勿将停止类别与 ISO 13849-1 中的类别混淆。

停止类别 0	断开对驱动元件的电力供应 (非受控停止)
停止类别 1	先使机器处于安全状态，再断开对驱动元件的电力供应
停止类别 2	使机器处于安全状态，但不断开对驱动元件的电力供应

➜ 另请参见“紧急停机”一节 ➜ 3-7

➜ 停止类别，参见“机器的电气装备: IEC 60204-1”

电磁兼容性 (EMC)

欧盟 EMC 指令将电磁兼容性定义为“设备或系统在其电磁环境中令人满意地运行并且不对该环境内其他设备或系统造成无法忍受的电磁干扰的能力”。
选择与验证机器和所使用的组件时，应确保其不受可预计的干扰影响。对安全组件适用更高的要求。
以下因素可能引起电磁干扰:

- 电快速瞬变脉冲群骚扰
- 冲击电压 (浪涌)，例如由闪电击中电网引起
- 电磁场
- 高频干扰 (邻近电缆)
- 静电放电 (ESD)

对于工业区和住宅区有干扰限值。工业区对抗干扰性的要求更高，但也允许更高的干扰放射限值。因此，满足工业区射频干扰要求的组件可能在住宅区内引起射频干扰。下表给出不同应用领域的最小干扰场强示例。
900 至 2000 MHz 频率范围内的典型最小干扰场强

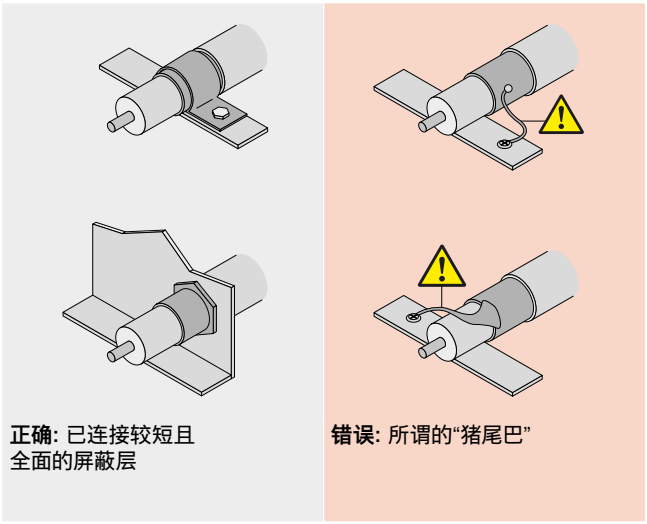
应用领域	兼容的最小干扰场强
娱乐电子设备	3 V/m
家用电器	3 V/m
信息电子设备	3 V/m
医疗器械	3 ... 30 V/m
工业电子设备	10 V/m
安全组件	10 ~ 30 V/m
汽车电子设备	最高 100 V/m

示例: 为达到不同场强与移动通信设备的典型距离				
应用领域	**3 V/m**	**10 V/m**	**100 V/m**	**备注**
DECT 工作站	约 1.5 m	约 0.4 m	≤ 1 cm	基站或手持单元
GSM 移动电话	约 3 m	约 1 m	≤ 1 cm	最大发射功率 (900 MHz)
GSM 基站	约 1.5 m	约 1.5 m	约 1.5 m	发射功率约为 10 瓦

以下设计准则有助于避免 EMC 问题:

- 通过机械部件与系统部件之间的导电连接建立连续等电位联结
- 同供给单元 (电源供应器、促动器、变频器) 物理隔离
- 不要使等电位联结电流穿过屏蔽层
- 铺上较短且全面的屏蔽层
- 连接现有功能接地 (FE)
- 整齐终止现有通信电缆。通常需要绞合电缆传输数据 (现场总线) 。

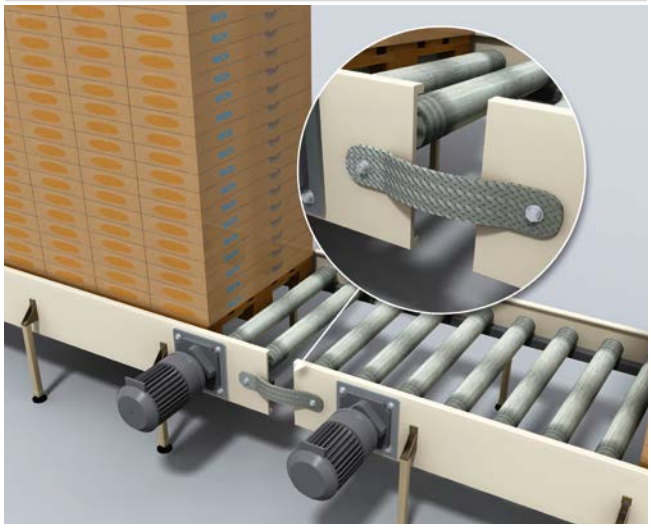
示例: 正确连接屏蔽层



正确: 已连接较短且全面的屏蔽层

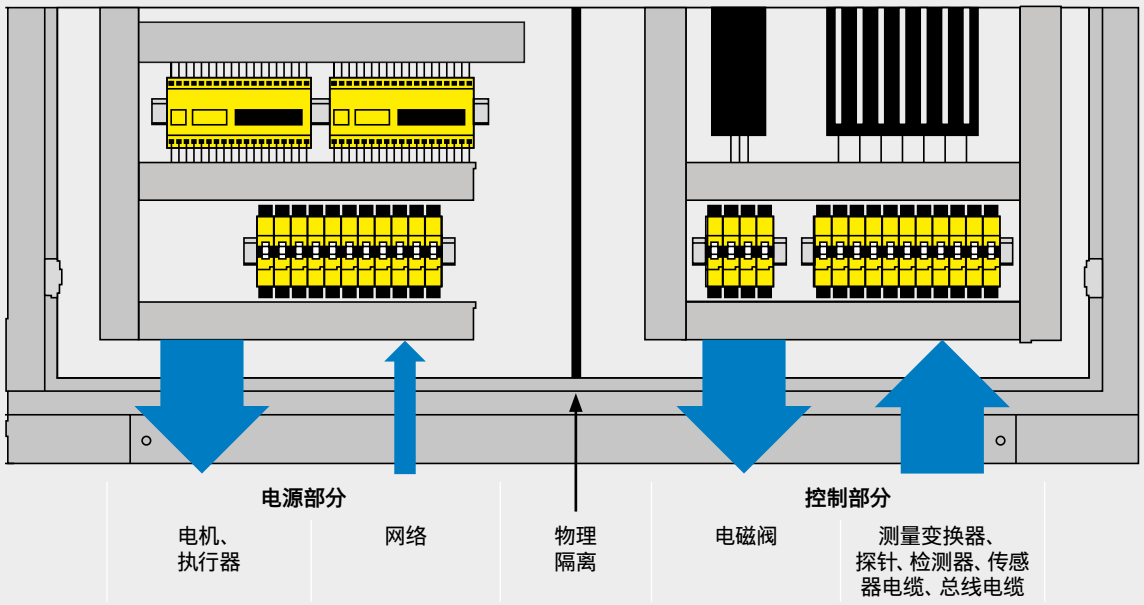
错误: 所谓的“猪尾巴”

示例: 建立等电位联结



8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

示例: 物理隔离



➜ EMC 标准: EN 61000-1 到 -4
➜ 对安全组件的 EMC 要求: IEC 61496-1, IEC 62061

流体技术

流体技术是所有通过气体或液体传输能量的方法的总称。使用上位概念是因为液体和气体具有相似行为。流体技术是指在封闭式管路系统中借助流体传输动力的方法和设备。

子系统
每个流体技术设备由以下子系统组成:
- 压缩: 压缩机或泵
- 预处理: 过滤器
- 输送: 管道或软管
- 控制: 阀门
- 驱动: 气缸

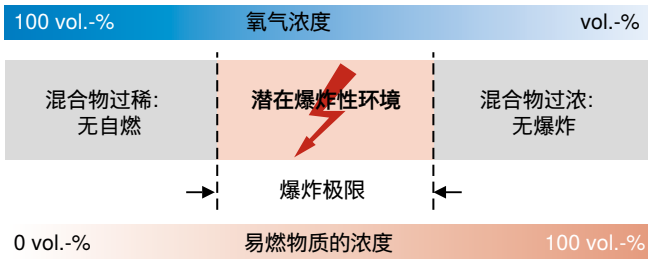
在任何流体技术系统中, 因克服负载输送流体而产生压力。若负载增加, 则压力也会升高。

流体技术应用于液压系统 (通过液压油传输能量) 和气动系统 (通过压缩空气传输) 。液压传动系统需要流体回路 (进流和回流) , 而在气动系统中废气经消声器吹出到环境中。

设计原则
流体技术系统的所有部分均有抗压保护, 可承受超过子系统最大工作压力或组件额定压力的压力。组件内部或管道或软管中泄漏不得带来危险。应使用消声器以减少由空气逸出引起的噪音。消声器的使用不得产生附加危险, 消声器不得造成有害背压。

在爆炸性环境中使用

爆炸防护属于与安全尤为相关的任务之一。发生爆炸时，人员面临众多危险，例如由于不受控制的热辐射、火焰、压力波和飞散的碎片以及由于有害的反应产物和消耗环境空气中呼吸所需的氧气。爆炸和火灾不属于最常见的工伤事故原因。但其后果惊人，经常造成严重的生命和财产损失。
在制造、运输、加工或储存粉尘、可燃气体或液体的地方，可能形成爆炸性环境，亦即处于爆炸极限范围内的燃料与空气中氧气的混合物。若同时存在点火源，将发生爆炸。



2

必要防护措施的范围评估
为评估必要防护措施的范围，将爆炸性环境根据出现危险的潜在爆炸环境的概率分为不同区域，参见指令 1992/92/EC，附录 I。下表中的信息不适用于矿业（井上、井下）。

区域定义				
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		很少、短时 (< 10/年)	偶尔 (10 ~ 100 h/年)	持续、频繁、长时 (> 1000 h/年)
安全措施		普通	高	非常高
可用设备类别 (ATEX)				
1		II 1G/II 1D		
2		II 2G/II 2D		
3		II 3G/II 3D		

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

标记

为了在这些区域内使用,必须设计、检测和相应标记设备。

⟨Ex⟩	II	2G	Ex ia	IIC	T4	示例: 依照 ATEX 标记防爆设备
					温度组别 可用于 > 135 °C 的点燃温度	
				防爆级别 乙炔、二硫化碳、氢		
			防护原理 i = 本质安全 a = 两次故障安全			
		设备类别 (ATEX) 可用于 1 区				
	设备组别 不用于沼气危险区域					
防爆标志						

➜ ATEX 指令: 2014/34/EU
➜ 标准: EN 1127-1, EN 60079-0

总结: 安全设计

机械、电气、操作
- 坚持首先不允许危险发生的原则。
- 采用尽可能无需操作人员暴露于危险区域的设计。
- 避免直接由电流引起 (直接和间接触电) 或间接因控制系统故障产生的危险。

紧急操作, 停机
- 准备用于在正常操作期间停止整台机器的指令装置。
- 使用紧急停止让危险流程或危险运动停止。
- 当必须安全隔离产生危险的电源时, 使用紧急断电。

EMC
- 设计满足适用的 EMC 要求的机器。选择与验证所使用的组件时, 应确保其:
  - 不对其他设备或系统造成电磁干扰。
  - 自身不受可预计的干扰影响。

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

第 3 步: 技术防护措施

通过以下手段实现技术防护措施

- 是安全功能一部分的防护设备, 如盖罩、防护门、光幕、双手操作式装置,
- 监控与限制装置 (位置、速度等) 或
- 减少放射措施。

并非所有防护设备均集成到机器的控制系统中。固定式物理防护设备 (栅栏、盖罩) 就是一个例子。通过正确设计这些防护设备达到安全要求。

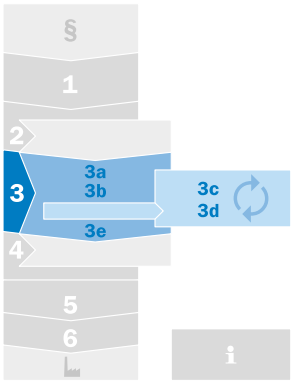
功能安全

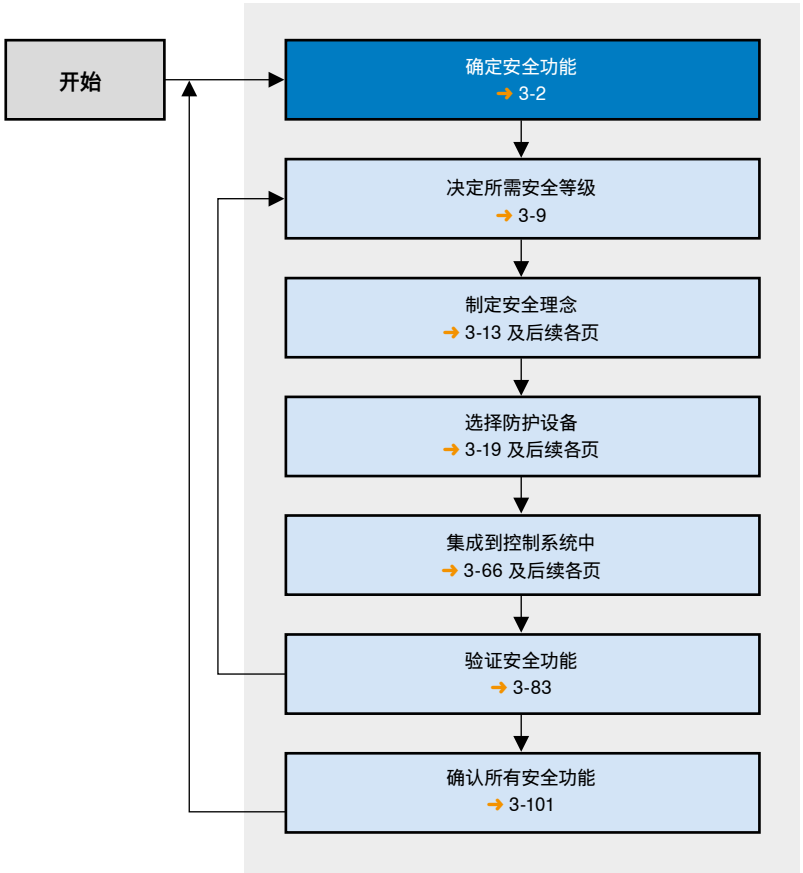
若防护措施的作用依赖于控制系统的正确工作, 则称之为功能安全。为实现功能安全, 必须定义安全功能、确定所需安全等级, 再通过恰当的组件落实和验证。

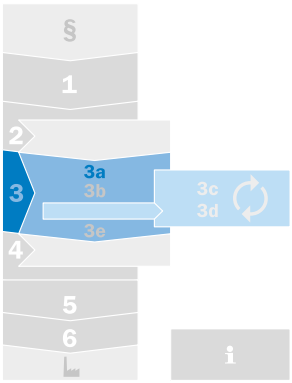
确证

确证所有技术防护措施可保证恰当的安全功能可靠发挥作用。

防护措施和安全功能的设计以及控制技术上的实施方法构成下一章的内容 (子步骤 3a 至 3e) 。







3 a

在本章中...

第 3a 步: 确定安全功能

安全功能定义了如何通过安全技术措施降低风险。对于无法从设计上消除的每种风险，应至少定义一项安全功能。需要准确定义安全功能，以便通过合理努力达到安全要求。从安全功能的定义得出所需组件的种类和数量。

➜ 安全功能的定义示例: BGIA-Report 2/2008, “机器控制系统的功能安全”

长期防止接近或进入

通过机械盖罩、栅栏或屏障，即所谓的物理防护设备，防止接近作业危险点。

示例:

- 通过盖罩防止直接触及作业危险点
- 间隔式防护设备（如通道）既能防止触及作业危险点，又允许物料或货品通过（见插图）
- 通过物理防护设备防止整个身体进入危险区域

暂时防止接近

防止接近作业危险点，直到机器处于安全状态。

示例:

- 应请求触发运行停止。若机器达到安全状态，则解除通过安全锁定装置对通道的封锁。

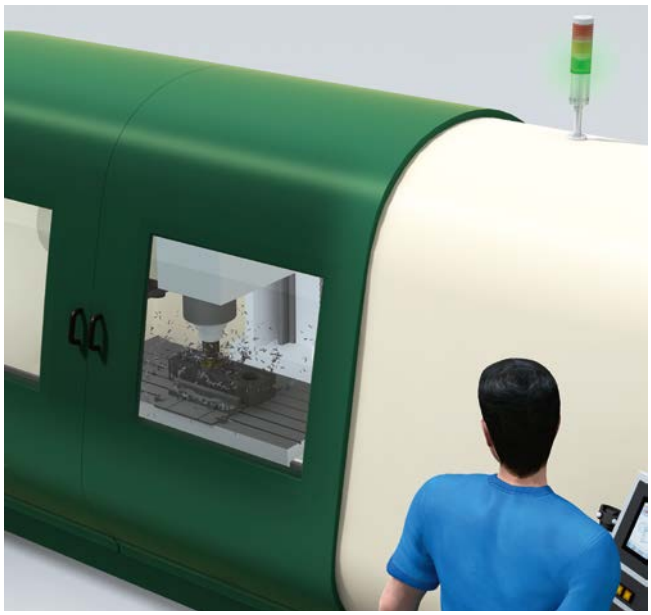
8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

约束零件、物质、辐射

若零件可以从机器甩出或可能出现辐射，则须使用机械防护设备（物理防护设备）避免发生危险。

示例：

- 铣床上带有特殊观察窗的防护罩，用于防止飞出的切屑和刀具碎片造成伤害（见插图）
- 可以约束机械臂的围栏

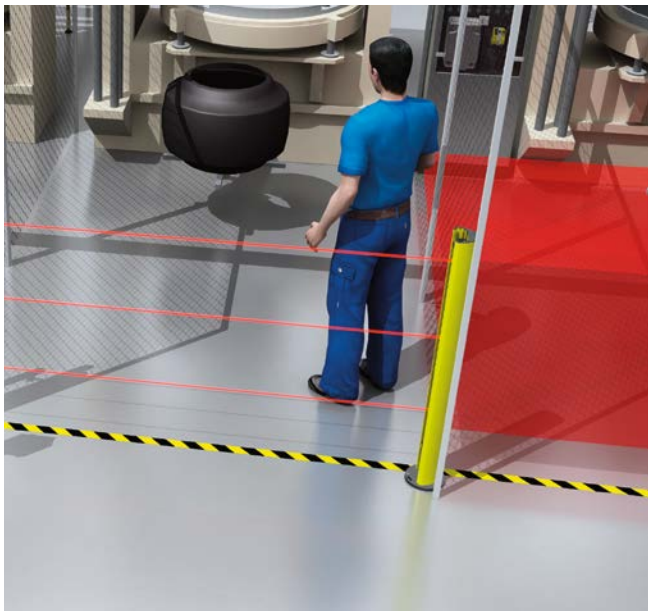


触发停止

安全停止功能应请求（例如有人靠近）将机器置于安全状态。为缩短停止时间，适宜依照停止类别 1 (IEC 60204-1 ➜ 2-9) 执行该停止功能。可能需要附加安全功能以防意外重启。

示例：

- 通过没有锁定的联锁装置打开防护门
- 遮挡提供入口保护的多光束安全光栅的光束（见插图）



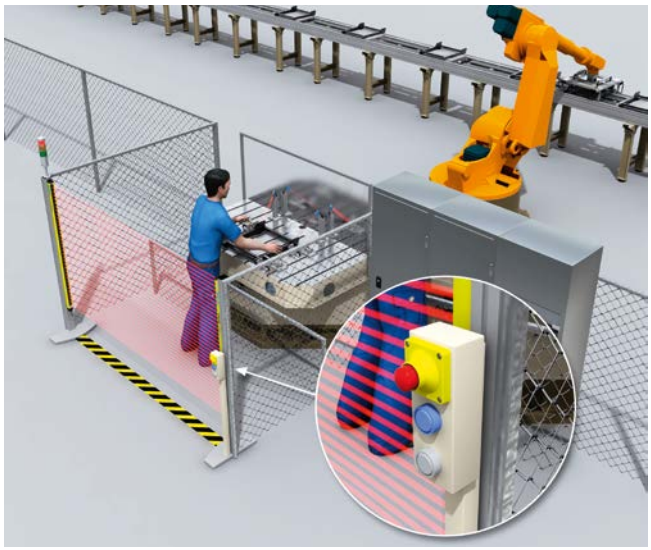
3 a

避免意外启动

触发“触发停止”功能或接通机器后，需要采取特定行动将机器投入运行。其中包括手动复位防护设备以准备重启机器（另请参见“运用复位和重启”一节 ➜ 3-65）。

示例:

- 复位光电保护装置（见插图: 蓝色“复位”按钮）
- 复位紧急停止装置
- 当所有必要的安全装置生效，即重启机器

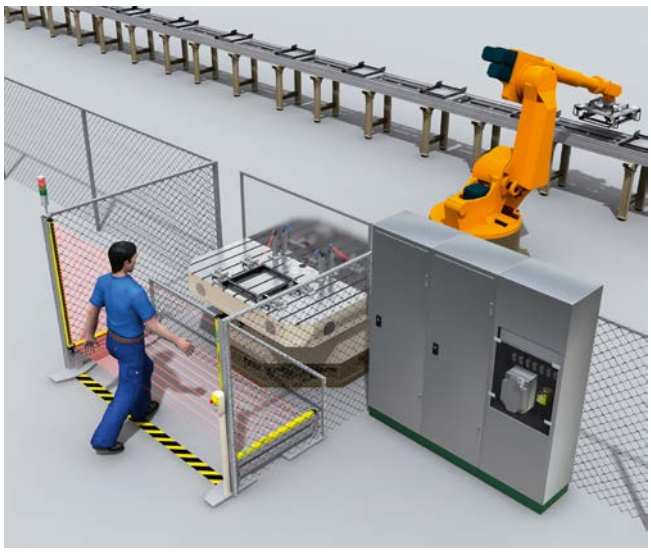


防止启动

只要有人处于危险区域，执行“触发停止”功能后，通过技术措施防止启动或恢复运行。

示例:

- 钥匙安全联锁系统
- 在横向安全光幕的主动保护区域内检测（见插图）。通过安全光幕的纵向保护区域实现“触发停止”功能。



组合: 触发停止并防止启动

只要有人或身体部位处于危险区域，将触发停止的防护设备同样用来防止重新启动。

示例:

- 单人作业场所的双手操作式装置
- 使用光幕避免站在后面或伸手进来（危险点保护）
- 应用提供区域防护的安全激光扫描器（见插图）

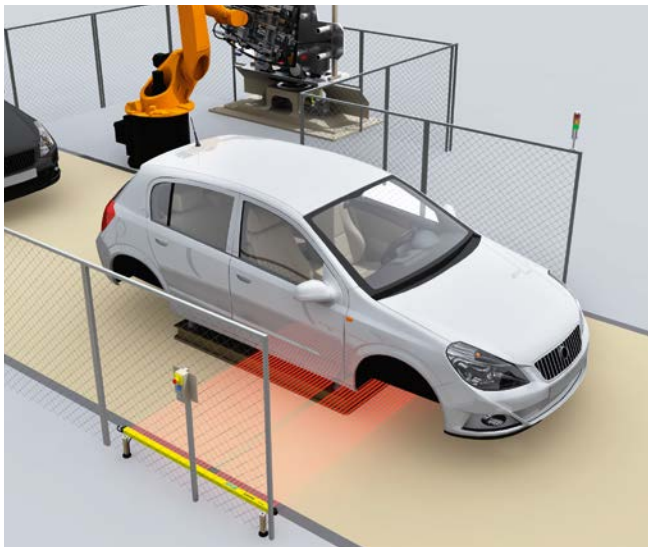
8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

实现物料通道

为将物料输入或输出危险区域，利用输入物料的特性进行物料识别或用于在物料和人员之间进行自动区分。在物料运输时，如果防护设备不起作用，但人员仍会被识别。

示例:

- 通过适当选择和定位传感器来检测物料，在物料通过期间限时解除安全功能（**屏蔽**）。
- 采用集成算法的横向光幕实现**人员/物料区分**（见插图）
- 安全激光扫描器的保护区域切换



➜ 详细说明参见“可集成到 ESPE 中的安全功能”一节 ➜ 3-38。

监控机器参数

在有些应用中，需要监控机器的各种参数是否达到安全相关限制。若超过限值，将采取合适的措施（如停止、警告信号）。

示例:

- 速度、温度或压力监控
- 位置监控（见插图）

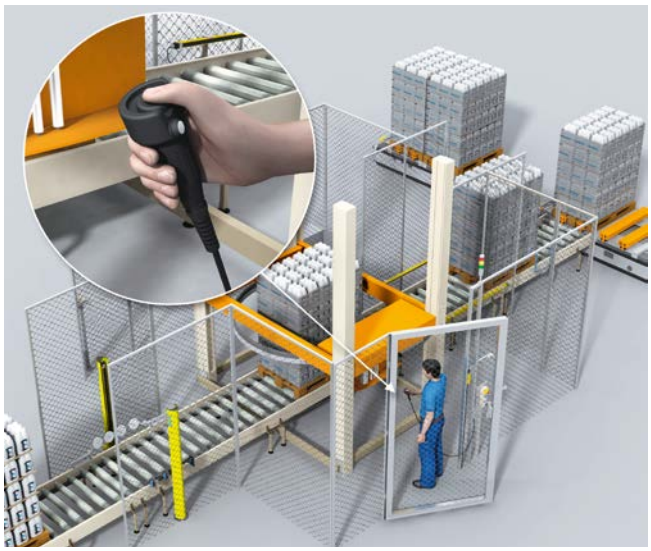
手动和限时解除安全功能

如果在调整工作中或为了观察流程需要机器在解除防护设备的防护作用的情况下运行，则应满足以下条件：

- 使用具有相应操作位置的操作模式选择开关
- 已禁止自动控制，不会因直接或间接影响传感器导致机器运动
- 不得允许指令链。
- 只有当持续操纵指令装置（如使能按钮）时，才能执行危险的机器功能
- 只有当风险降低（如限制速度、运动距离、工作时间）时，才能执行危险的机器功能

示例：

- 仅在按下使能按钮时减速运动



3 a

组合或切换安全功能

机器可采取多种状态或在多种操作模式下工作。在此期间，可能有不同安全措施发挥作用或有多种安全功能相互结合。应确保始终达到所需安全等级。切换操作模式或选择和调整各种安全措施不得导致危险状态。

示例：

- 在调整操作与正常操作模式之间切换后，机器被停止。需要新的手动启动指令。
- 使激光扫描器的监控区域适应车辆速度（见插图）

紧急停机

紧急停机是补充防护措施，不是用于降低风险的主要手段。应根据机器的风险评估确定该功能的所需安全等级。尤其要考虑到环境影响（如震动、致动方式）（另请参见“紧急操作”一节 ➜ 3-46）。

➜ 参见 IEC 60204-1 和 ISO 13850

安全相关显示和报警

安全相关显示是提醒用户注意迫在眉睫的危险（如超速）或可能的剩余风险的措施。此类信号也可用于在触发自动防护措施之前提醒操作人员注意。

- 警告装置的设计和布置应确保方便进行检查。
- 用户信息应包括定期检查警告装置。
- 应避免过度刺激，尤其是声音报警。

示例:

- 联锁显示
- 启动警告装置
- 屏蔽灯

其他功能

安全技术装置也可以执行其他功能，即使其并非用于人员保护。这不影响实际的安全功能。

示例:

- 工具或机器保护
- PSDI 模式 (循环触发 ➜ 3-40)
- 防护设备的状态一同用于自动化任务 (如导航)

总结: 确定安全功能

确定需要哪些安全功能来降低风险:

- 长期防止接近或进入
- 暂时防止接近
- 约束零件、物质、辐射
- 触发停止
- 防止启动
- 避免意外启动
- 组合: 触发停止并防止启动
- 区分人员与物料
- 监控机器参数
- 在特定的时间，手动解除安全功能
- 组合或切换安全功能

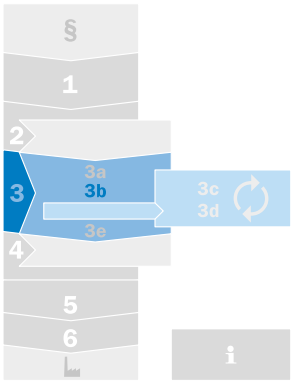
3 a

第 3b 步: 决定所需安全等级

通常在 C 类标准 (机器特定标准) 中规定了所需安全等级。
应单独确定每项安全功能的所需安全等级, 然后适用于所有相关设备, 例如:

- 传感器或防护设备
- 负责评价的逻辑单元
- 执行元件

若没有针对相应机器的 C 类标准或 C 类标准中未作相关规定, 可根据以下标准之一确定所需安全等级:



→ ISO 13849-1
→ IEC 62061

通过适用标准确保确定风险付出的努力是合理的。
保护操作人员手动地将零件用手放入金属压力机或从中取出的思考方法, 与保护操作人员在机器上工作最大风险是夹住手指是不同的。
此外, 同一台机器在各个寿命阶段也有承担不同风险的不同作业危险点。在此应针对每个寿命阶段和每种危险单独确定安全功能。

以下风险评价参数是所有标准的基础:
可能伤害/健康危害的严重程度、暴露于危险的频率和/或持续时间以及避免危险的可能性。这三个参数的组合决定了所需安全等级。
应用这些标准中所描述的方法来决定安全等级时, 默认机器没有防护设备。

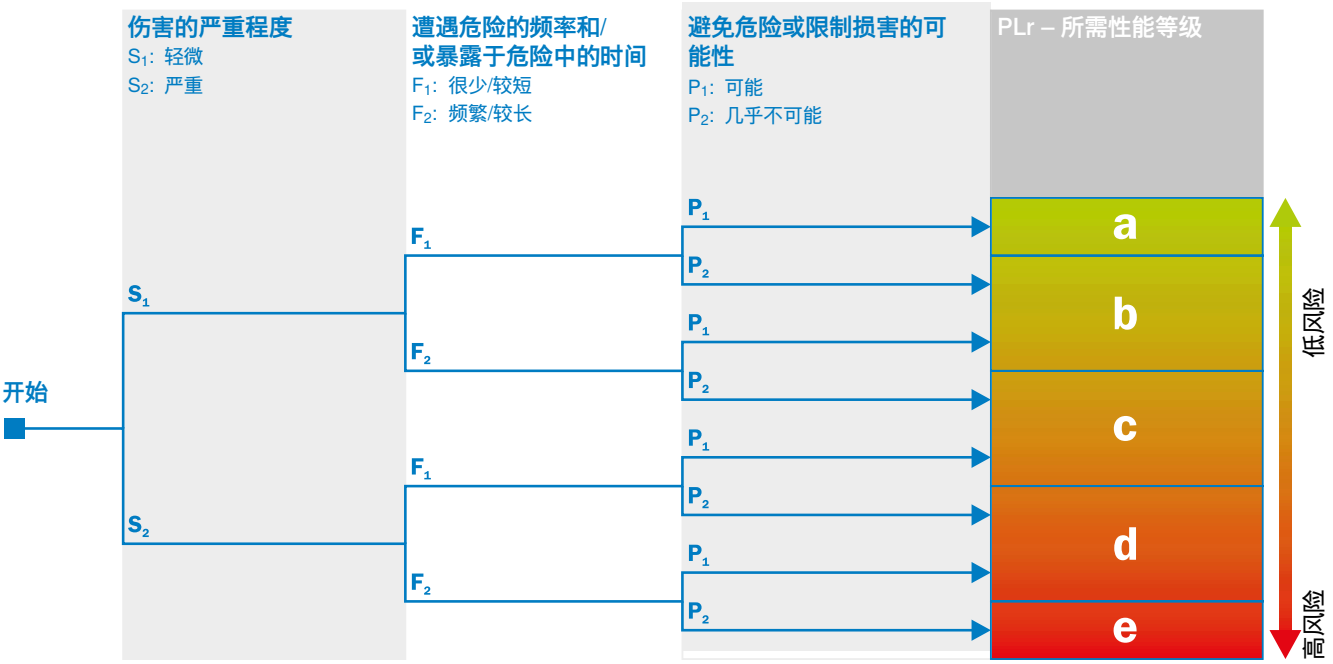
3 b

在本章中...

依照 ISO 13849-1 的所需性能等级 (PLr)

该标准同样使用风险图来决定所需安全等级。通过参数 S、F 和 P 决定风险大小。

方法的结果是“所需性能等级”(PLr: required Performance Level)。



根据 ISO 13849-1 的风险图

性能等级分为五个等级。性能等级取决于控制系统的结构、所用部件的可靠性、检测故障的能力以及对多通道控制系统中共因故障的耐受性 (参见“子系统的安全技术参数”一节 ➜ 3-16) 。另外, 还需要进一步措施避免设计设计故障。

8020567/2017-08-22(GCN 2021-07-01)
如有更改, 恕不另行通知

依照 IEC 62061 的所需安全完整性等级 (SIL)

这里使用的方法是数值法。将评估伤害程度、处于危险区域的频率和持续时间以及避免的可能性。还会考虑危险事件发生的概率。结果是所需安全完整性等级 (SIL)。

后果	伤害程度 S	等级 K = F + W + P				
		4	5-7	8-10	11-13	14-15
死亡、失明或断臂	4	SIL2	SIL2	SIL2	SIL3	SIL3
永久，断指	3			SIL1	SIL2	SIL3
可复原，需要医疗	2				SIL1	SIL2
可复原，需要急救	1					SIL1

危险事件 [1] 的频率 F	
F ≥ 1 × 每小时	5
1 × 每小时 > F ≥ 1 × 每天	5
1 × 每天 > F ≥ 1 × 2 周内	4
1 × 2 周内 > F ≥ 1 × 每年	3
1 × 每年 > F	2

危险事件发生的概率 W	
非常高	5
较高	4
一般可能	3
较低	2
可忽略	1

避免危险事件的可能性 P	
不可能	5
一般可能	3
很可能	1

1) 停留持续时间超过 10 分钟

如下确定 SIL:

1. 确定伤害程度 S。
2. 确定频率 F、概率 W 和避免可能性 P 的分数。
3. 等级 K 由 F + W + P 之和算出。
4. 所需 SIL 是“伤害程度 S”行与“等级 K”列的交叉点。

SIL 分为三个等级。实现的 SIL 取决于控制系统的结构、所用部件的可靠性、检测故障的能力以及对多通道控制系统中共因故障的耐受性。另外，还需要进一步措施避免设计设计故障 (参见“子系统的安全技术参数”一节 ➜ 3-16) 。

ISO 13849-1 和 IEC 62061的适用范围

ISO 13849-1 和 IEC 62061 都定义了对控制系统的安全相关部件的设计和实现的要求。用户可根据所使用的技术依照旁边表格中的信息选择相关标准。

技术	ISO 13849-1	IEC 62061
液压	适用	不适用
气动产品	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	适用	适用

总结: 决定所需安全等级

一般性说明

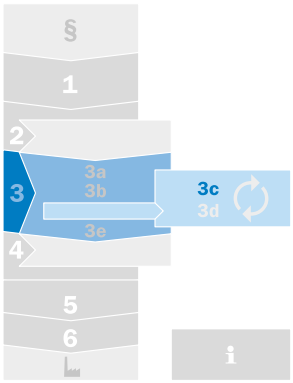
- 确定每项安全功能的所需安全等级。
- 参数“可能伤害的严重程度”、“暴露于危险的频率和持续时间”以及“避免危险的可能性”决定了所需安全等级。

可用标准

- ISO 13849-1 使用风险图来决定所需安全等级。方法的结果是“所需性能等级”(PLr)。
- ISO 13849-1 也适用于液压系统、气动系统和机械系统。
- IEC 62061 采用数值法。结果是所需安全完整性等级 (SIL)。

第 3c 步: 设计安全功能

在 3c 和 3d 步中, 通过选择正确的技术、合适的防护设备与组件来设计和验证安全功能。在迭代过程中, 可能要多次执行这些步骤。



在此期间要反复检查所选技术能否保证足够安全和在技术上实现或使用特定技术是否产生其他或附加风险。

制定安全理念

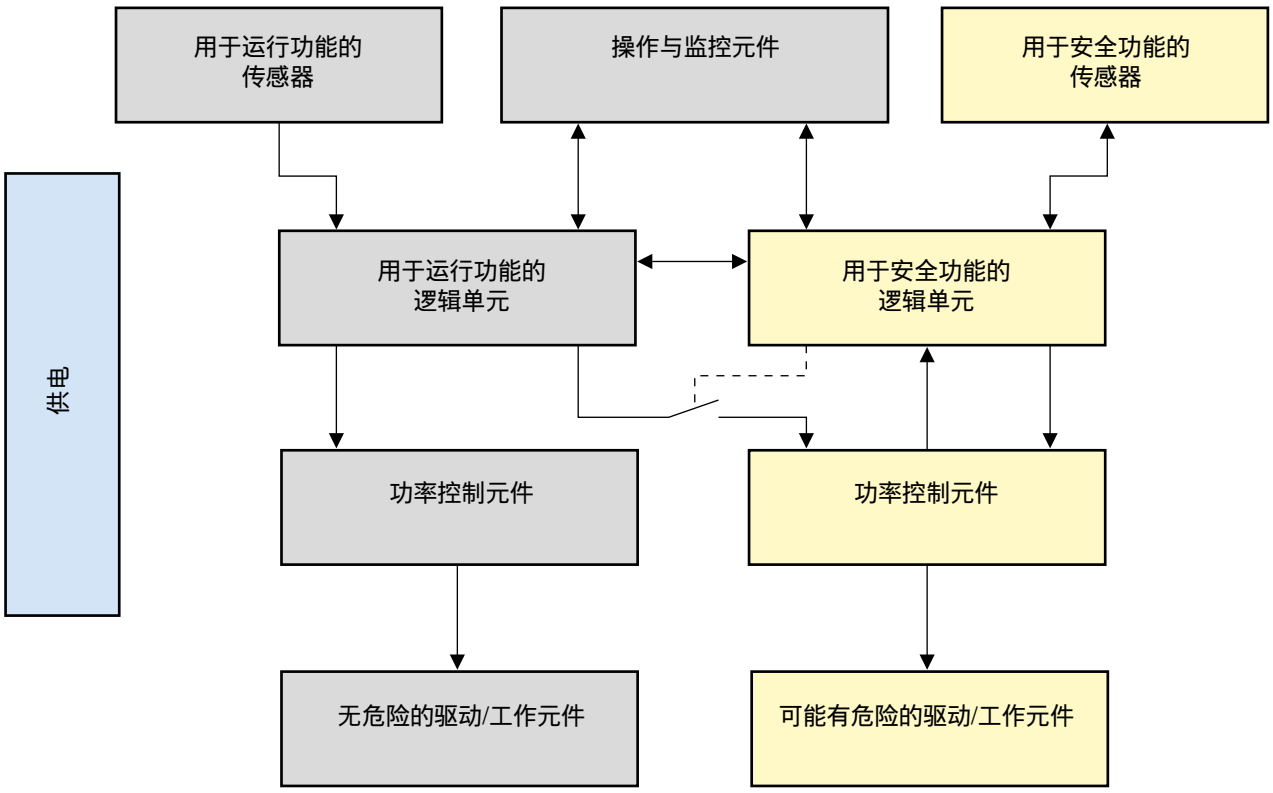
机器或设备包含各种组件, 它们共同发挥作用并确保机器或设备正常工作。在此应区分仅承担操作任务的组件和负责安全技术功能的组件。

➜ 关于安全理念的详细信息: BGIA-Report 2/2008, “机器控制系统的功能安全”, 访问 www.dguv.de/ifa/de/pub

3 C

在本章中...

机器控制系统的功能布局



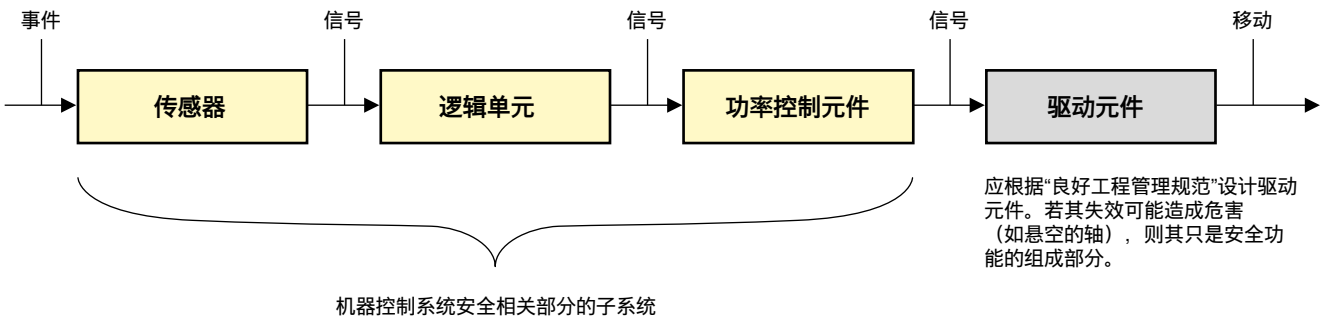
应根据安全功能和所需安全等级来选择控制系统的安全相关部件，如传感器、逻辑单元、功率控制元件以及驱动和工作元件。通常以安全理念的形式执行该选择。

一项安全功能可以由一个或多个安全相关组件实现。多项安全功能可以共用一个或多个组件。控制系统的设计应当能够避免危险状态。仅允许通过有意致动为此准备的指令装置，将机器投入运行。

若机器重启将引发危险，则须在接通工作电压时从技术上排除重启。

若重启不会引发危险，则可在没有操作人员干预的情况下（自动）进行重启。

机器控制系统安全相关部分的子系统



决定性特点

制定安全理念时，应考虑以下特点：

- 机器特点
- 环境特点
- 人员特点
- 设计特点
- 防护设备特点 (➜ 3-19)

应根据上述因素确定以何种方式
集成哪些防护设备。

机器特点

应考虑机器的
以下特点：

- 随时停止危险动作的能力 (如不能，则使用物理式或屏障式防护设备)
- 无附加危险地停止危险动作的能力 (如不能，则选择其他设计或防护设备)
- 飞出的零件造成危害的可能性 (如可能：使用物理防护设备)
- 停止时间 (需要了解停止时间以保证防护设备发挥作用)
- 监控停止时间或惯性距离的可能性 (若由于老化或磨损会发生变化，则需要监控)

环境特点

应考虑环境的以下特点：

- 电磁干扰、干扰放射
- 振动、冲击
- 环境光、传感器的干扰光、焊接火花
- 反射面
- 脏污 (雾气、碎屑)
- 温度范围
- 潮湿、天气

人员特点

应考虑人员的以下特点：

- 机器操作人员的预期资格
- 预期人员的数目
- 靠近速度 (K)
- 绕过防护设备的可能性
- 可预见的误用

设计特点

原则上，建议使用经认证的安全组件实现安全功能。从而简化设计流程和后续验证。一项安全功能由多个子系统执行。
往往无法仅使用已提供所需安全等级 (PL/SIL) 的经认证安全组件实现子系统。事实上，子系统必须由多个分立元件装配而成。在这种情况下，安全等级取决于不同参数。

子系统的安全技术参数

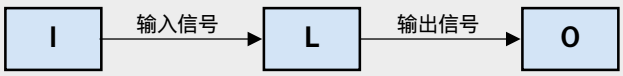
子系统的安全等级取决于不同安全技术参数，如:

- 结构
- 组件或装置的可靠性
- 故障检测诊断
- 对共因故障的耐受性
- 流程

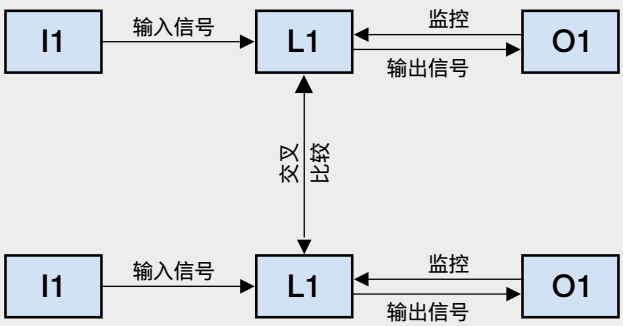
结构

为通过改善结构降低安全组件易受故障影响的特性，可以由多个通道并行执行安全技术功能。双通道安全组件常见于机械安全领域（见下图）。各通道都能停止危险状态。两个通道也可以有不同结构（例如一个通道由机电组件构成，另一个通道则仅采用电子元器件）。该通道也可以代替第二个等价通道承担纯粹的监控功能。

单通道安全组件



双通道安全组件

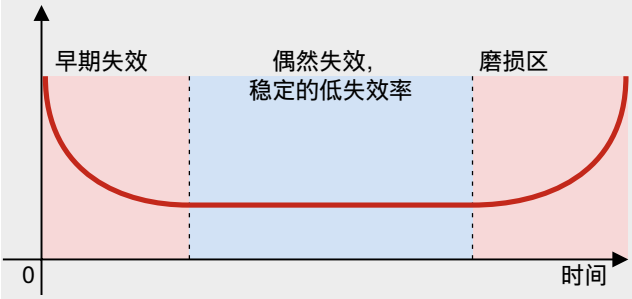


组件或装置的可靠性

安全组件的任何失效都对生产过程造成干扰。因此，使用可靠组件非常重要。可靠性越高，发生危险失效的概率越低。可靠性参数是衡量使用寿命期偶然失效的指标，通常以如下方式给出:

- 对于机电或气动组件: **B_{10} 值**。在此使用寿命取决于开关频率。B_{10} 说明 10% 的组件发生失效前的开关循环次数。
- 对于电子元器件: **失效率 λ**（λ 值）。失效率常以“菲特”（FIT，时基失效）为单位。一菲特是指每 10^9 个小时发生一次失效。

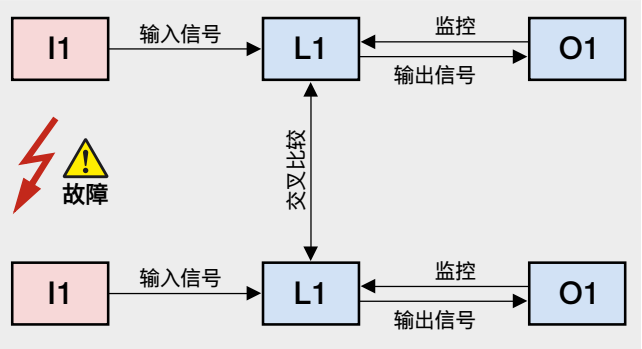
失效率 λ（浴缸曲线）



8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

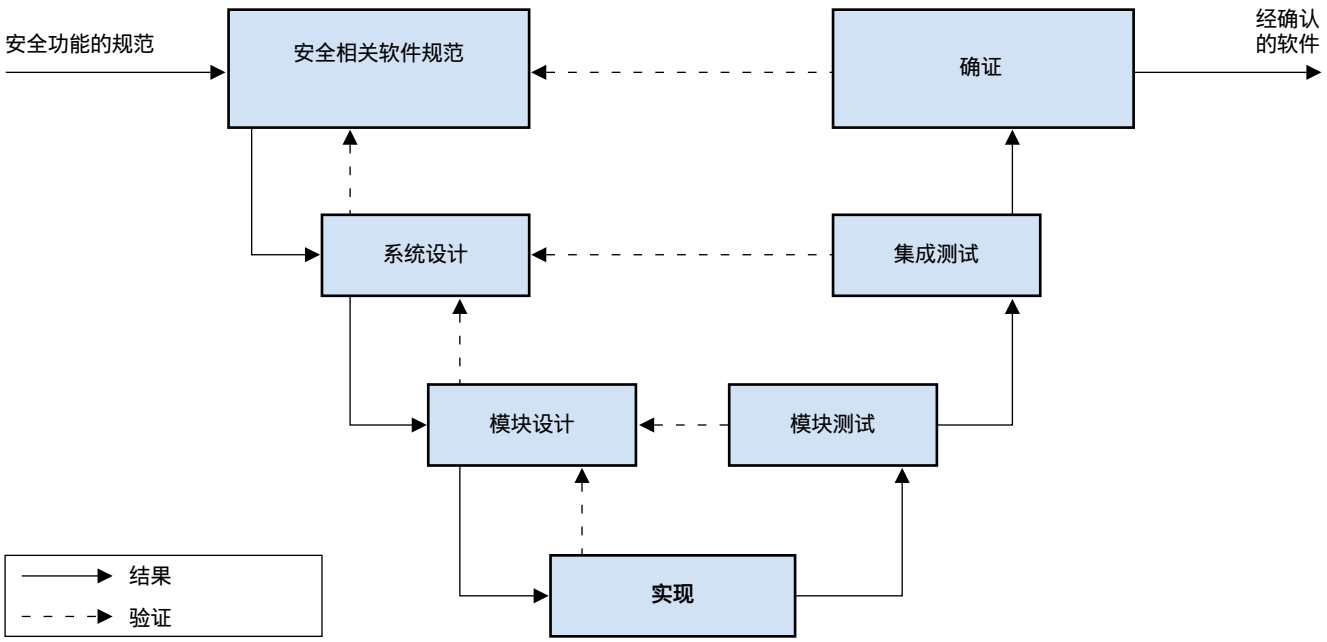
故障诊断检测
某些故障可通过诊断措施发现。其中包括相互监控、电流和电压监控、看门狗功能、短时功能测试等。
并非所有故障都能发现，因此需要确定故障检测的尺度。为此可进行失效模式及影响分析 (FMEA = Failure Mode Effects Analysis)。标准中的措施和经验值有助于复杂设计。

对共因故障的耐受性
例如两个通道因干扰影响而同时失效就是共因故障。
在此应采取相应措施，如分开布线、抑制器、部件的多样化等。



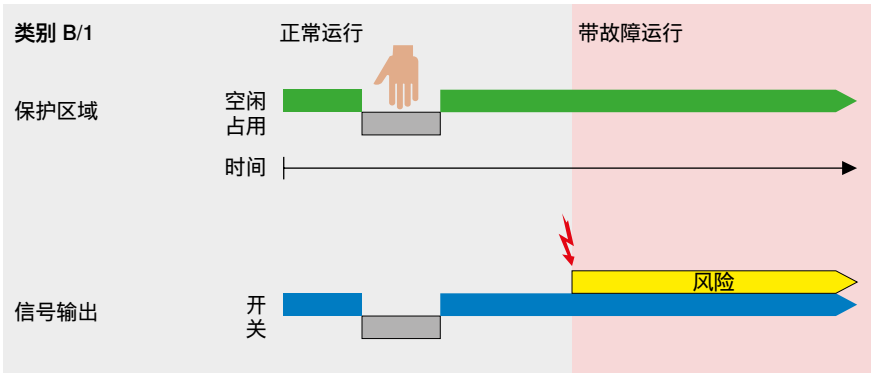
流程
流程将以下有影响的要素合并:
- 组织和能力
- 设计规则 (如规范模板、编码准则)
- 测试理念和测试标准
- 文件编制和配置管理

在安全技术领域，基于 V 模型的流程对软件设计的有效性尤其得到证明 (见插图)。

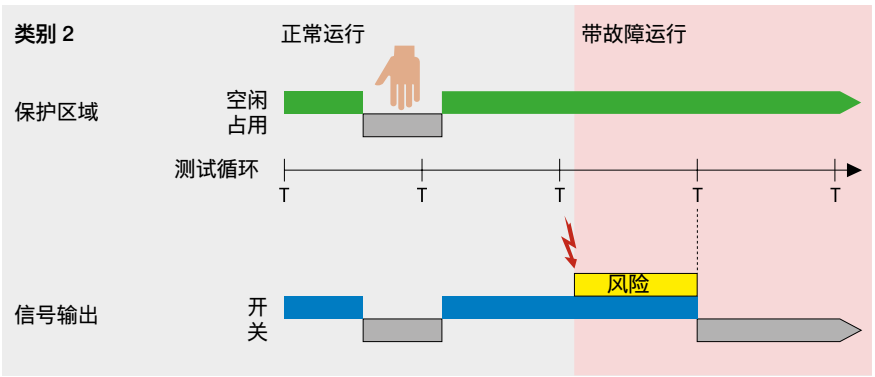


依照 ISO 13849-1 的考虑*
在 ISO 13849-1 标准中，通过下列类别说明结构。

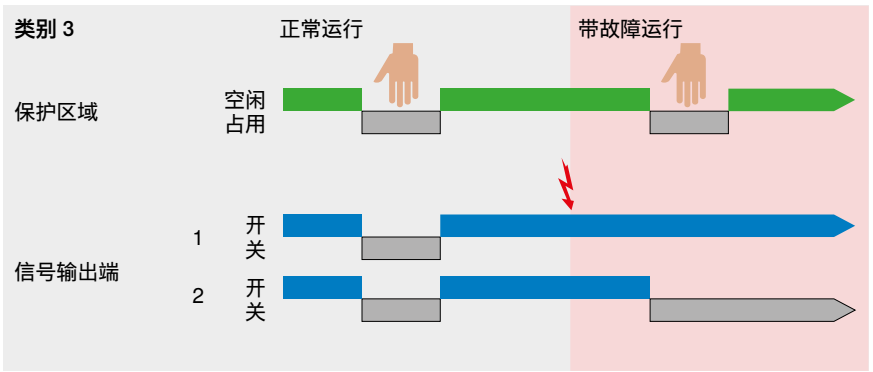
* 备注：安全功能是指它的失效可能导致风险立即升高的功能。因此，失去安全功能必须被视为出现风险或风险升高。



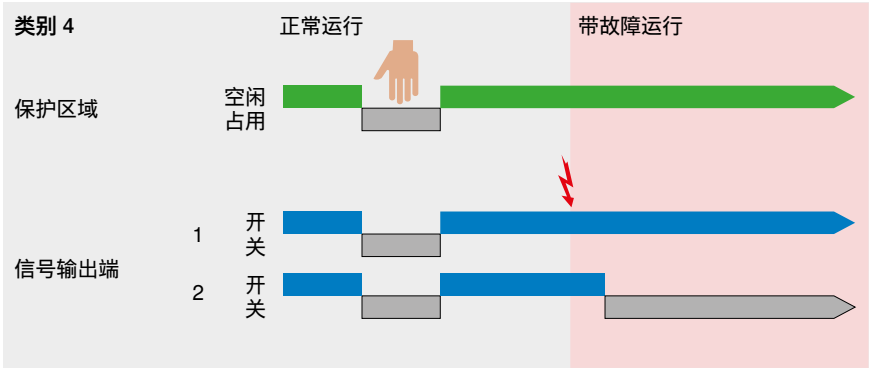
类别 B/类别 1
无故障检测。发生故障将招致风险。通过可靠而有效的组件 (类别 1) 可以最大限度降低风险。



类别 2
通过测试进行故障检测。在发生故障与下一次测试之间的时段内存在风险。应遵守符合 ISO 13849-1的测试频率。



类别 3
在故障情况下，仍然保留安全功能。在执行安全功能或进行下一次测试时检测到故障。故障累积导致失去安全功能。



类别 4
即使发生故障，仍然保留安全功能。与类别 3 相反，在未检测到最初故障的情况下，后续故障不得导致失去安全功能。

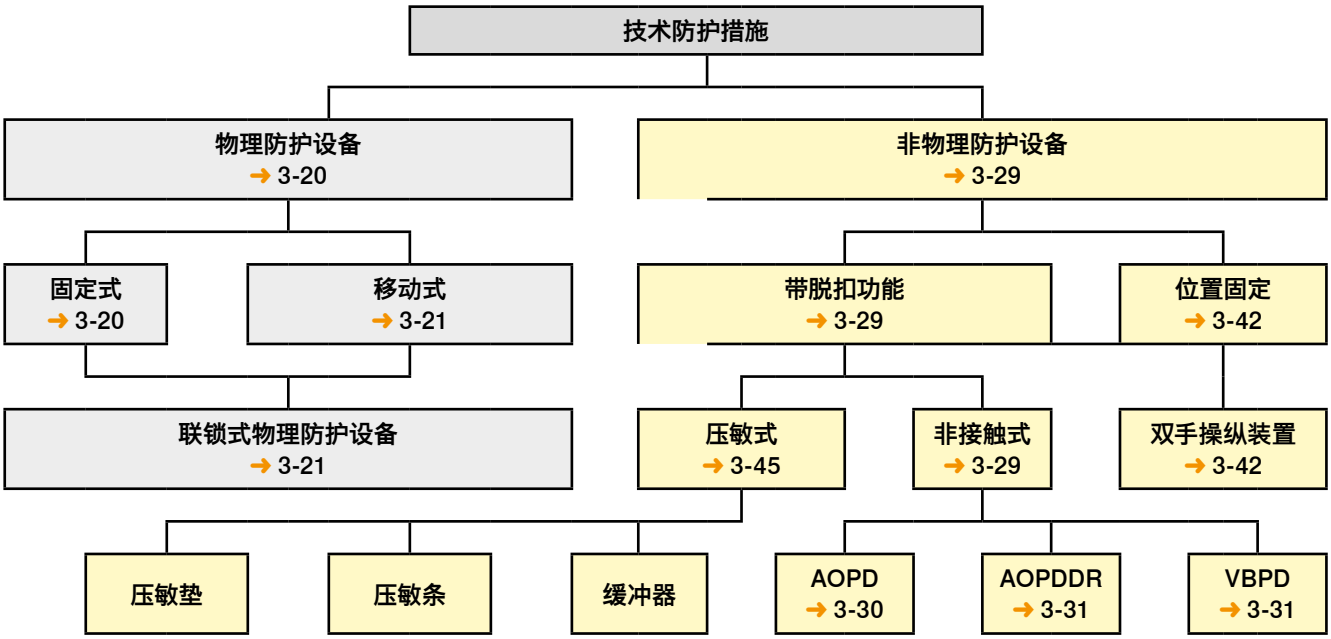
防护设备特点

应考虑的防护设备特点包括:

- 防护设备的特性和应用
  (电敏防护设备、物理防护设备等 ➜ 3-19)
- 防护设备的位置或尺寸 (➜ 3-47)
- 集成到控制系统中 (➜ 3-66)

下面的章节将详细说明这几点。

防护设备的技术、选择和应用



物理防护设备

物理防护设备是防止或避免身体部位直接触及作业危险点的机械防护设备。其可以设计为固定式或移动式。物理防护设备包括盖罩、栅栏、屏障、翻盖、防护门等。盖罩和外壳可防止从任何侧面接近。防护栅栏通常用于防止全身进入。与此相反，屏障只能避免无意或不自觉地进入作业危险点。
安全功能是物理防护设备设计的根本。例如物理防护装置只是防止进入，还是也要约束零件和辐射？

飞出的零件示例：

- 断裂/破碎的刀具（砂轮、钻头）
- 产生的物质（粉尘、切屑、碎片、微粒）
- 溢出的物质（液压油、压缩空气、润滑剂、原料）
- 抓取或搬运系统失效后抛出的零件

产生的辐射示例：

- 工艺流程或产品的热辐射（高温表面）
- 激光、红外或紫外光源的光辐射
- 粒子或离子辐射
- 强电磁场、高频装置
- 测试系统或用于导出静电荷的系统的高电压（纸张和塑料幅面）

对旨在约束辐射或物质的物理防护装置的机械要求通常必须高于对避免人员进入的物理防护装置的要求。
若风险评估表明不会由此产生危害，则允许物理防护装置损坏（破裂或变形）。

对物理防护装置的基本要求

- 防护装置必须设计得足够坚固耐用才能在运行期间承受可预计的环境负荷。在机器的整个使用期内，物理防护装置必须维持其特性。
- 不得引起附加危险。
- 不得被简单绕过或失效。
- 如果需要观察，则不得超过必要限度地限制观察工作过程。
- 必须牢固就位。
- 必须通过系统保持，只能用工具打开或者联锁到机器的危险功能。
- 松开紧固件后尽可能不要留在保护位置。

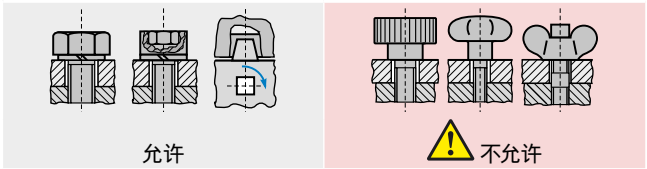
3 C

➜ 物理防护设备：ISO 14120
➜ 机械安全的设计通则：ISO 12100（A 类标准）

物理防护装置的固定

不经常或仅在维修工作中取下或打开的防护装置，原则上必须与机架相连，只能用工具（如扳手、旗杆钥匙）将其打开。移除它们的过程必须与安装操作类似，需要使用工具。
定期拆除或取下的防护装置的紧固件必须设计成不会丢失（如松不脱螺钉）。
仅在物理防护装置联锁后才允许其他固定方式，如快拆锁扣、带手柄螺钉、滚花和翼形螺钉。

示例：物理防护装置的固定方式



8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

可移动物理防护装置

在不使用工具的情况下频繁或定期 (例如在安装工作中) 打开的可移动防护设备, 必须与机器的危险功能在功能上联合 (联锁、锁定) 。例如若防护装置在一个工作班次内至少打开一次, 即为频繁打开。
若预计打开防护装置会有危险 (例如非常长的惯性运行时间) , 则需要锁定装置。

对可移动物理防护装置的人类工效学要求

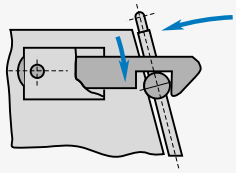
设计防护装置时, 人类工效学方面也很重要。只有当防护装置不超过必要限度地妨碍安装和维修及类似工作时, 才会被员工接受。可移动物理防护装置必须满足以下人类工效学标准:

- 轻松 (如单手) 打开和关闭、举起或移动
- 符合功能要求的把手
- 打开防护装置后, 应允许便捷进入。

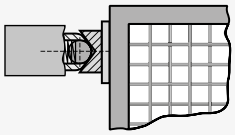
可移动物理防护装置的机械锁定

只要可行, 就必须将可移动物理防护装置与机器相连, 以便通过铰链、导向件等使其稳妥地保持在打开位置。应首选形状配合的固定装置。不推荐摩擦配合的固定装置 (如球头) , 因为其效用不断降低 (磨损) 。

示例: 物理防护装置的锁定



良好



可行

物理防护装置的联锁

在下列情况中, 物理防护装置必须联锁:

- 循环致动或定期打开 (门、盖)
- 可以不使用工具或不费力地移除 (如盖罩)
- 防护潜在的严重危害

联锁意味着防护装置的打开将转化为使危险动作停止的控制信号。物理防护装置通常使用位置开关以电气方式联锁。

物理防护装置的联锁装置应履行以下功能:

- 当防护设备打开 (缺失) 时, 无法执行危险的机器功能 (防止启动) 。
- 当防护装置被打开 (移除) 时, 机器的危险功能停止 (触发停止) 。

ISO 14119 标准说明对物理防护设备的联锁装置的要求, 目前正在修订。
下一节将介绍修订的内容。

联锁装置细分为四种结构型式:

名称	致动		执行元件		SICK 产品	
	原理	示例	原理	示例	示例	
1型式结构	机械式	接触、用力、按压	未编码	转换凸轮	i10P	
				转换杆	i10R	
				铰链	i10H	
2型结构			带编码	成型的执行器 (转换棒)	i16S	
				扳手	–	
3型结构	电感应式	感应式	未编码	合适的铁磁材料	IN4000	
		磁式		磁铁、电磁铁	MM12 [1]	
		电容式		所有合适的材料	CM18 [1]	
		超声波式		所有合适的材料	UM12 [1]	
		光学式		所有合适的材料	WT 12 [1]	
4型结构		磁式	带编码	编码磁铁	RE11	
		无线射频识别		带编码的 RFID 应答器	TR4 Direct	
		光学式		带编码的光学执行器	–	

1) 这些传感器不是为安全应用开发。在联锁装置内应用时，设计者必须非常谨慎地考虑可能的系统失效和共因故障并相应采取附加措施。

只有当风险评估表明干扰是不可预见的或附加措施能充分防止干扰时，才能应用结构3型的联锁装置。

安全开关、位置开关和联锁装置

被广泛使用的“安全开关”这一概念并未出现在标准中，因为适用于联锁装置的传感器设计和技术众多，无法定义通用要求。

无论采用哪种技术 (机械、电气、气动、液压)，均适用以下定义:

- 联锁装置由执行器和位置开关组成。
- 位置开关由执行元件和输出信号元件组成。

根据所用位置开关的技术和功能安全要求，物理防护装置需要一个或多个联锁装置。

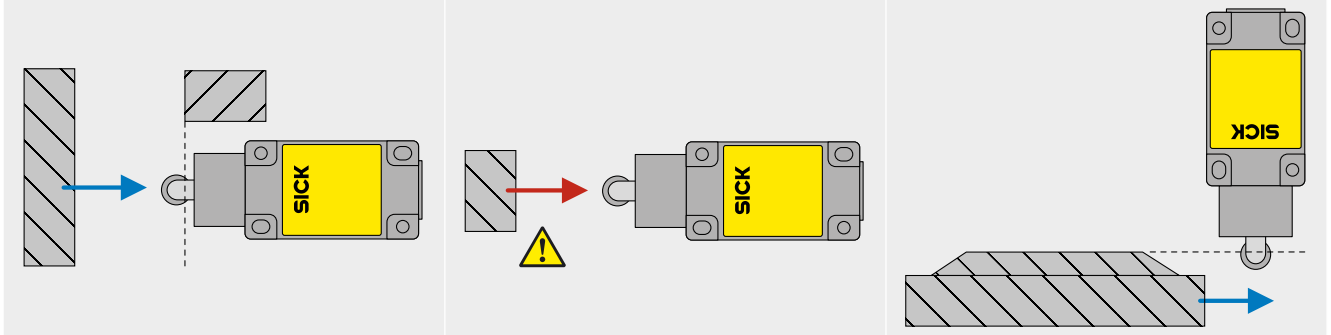
8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

机械安装和固定

位置开关和执行器的可靠的机械安装对其可靠性至关重要。联锁装置的元件:

- 必须以免受可预见的外部影响损坏的方式安装。
- 不得用作机械限位器。
- 必须通过布置和设计防止意外致动和损坏。
- 必须通过布置、设计和固定防止意外变位。如有需要，通过形状配合实现开关和执行器的固定，例如使用圆孔、定位销、限位器。
- 必须通过它的打开方式或集成到控制系统中确保不会被简单绕过。
- 必须允许易于接近以便检查和检查其是否正常工作。

示例: 位置开关的机械安装



正确安装: 通过机械限位器保护位置开关。

错误安装: 位置开关用作限位器。

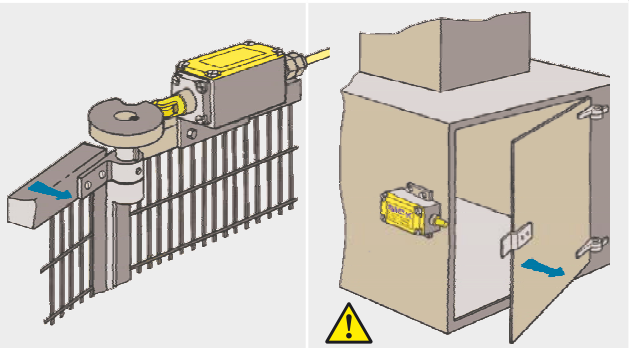
正确安装: 凸轮的高度与位置开关匹配。

动作方式或强制动作

强制动作是对机械联锁装置的重要要求。强制动作是指联锁装置 (安全开关) 的可移动机械部件被物理防护装置 (如防护门) 的机械部件

强制带动，例如通过直接接触或刚性零件。在联锁装置中使用强制动作确保位置开关在物理防护装置打开时致动并降低干忧的可能性。

示例: 强制动作设计



安全: 防护门打开迫使位置开关的机械柱塞移动。安全电路由此断开。

有缺陷的设计: 位置开关不会总是断开安全回路，例如当结垢或树脂化的润滑油粘住柱塞时。

来源: BG 精密机械与电气工程，BGI 575

强制打开

如果直接由执行原件通过非弹性零件（如弹簧）的限定移动隔离开关触点，则接触元件为强制打开常闭触点。在机械动作式位置开关中使用强制打开常闭触点确保当触点磨损或发生其他电气故障时仍可执行电路隔离。

对于采用强制打开常闭触点的机械位置开关，还适用：

- 必须依照制造商说明根据强制打开行程设置动作行程。
- 必须遵守制造商指定的最小柱塞行程，以保证强制打开所需的开关距离。

强制打开常闭触点的标记依照 IEC 60947-5-1，附录 K

使用非接触式位置开关的两个受到冗余监控的电子输出被视为与强制打开等同。若3型结构 或4型结构 的联锁装置是物理防护装置上的唯一联锁装置，则其必须满足 IEC 60947-5-3 的要求。

防干忧保护

设计联锁装置时，设计者应考虑到干忧防护装置的可能动机和可预见的干忧。

应采取使用简单工具的防干忧措施。

简单工具包括例如螺钉、针、薄片、硬币、弯曲的金属丝等。

避免简单干忧联锁装置的可能措施包括：

- 通过隐藏式安装或在够不到的地方安装，增加接近联锁装置的难度
- 使用带编码执行器的位置开关
- 通过“一次性”紧固件（如防拆螺丝、铆钉）固定联锁装置的元件
- 控制系统内的干忧监控（真实性检查、测试）

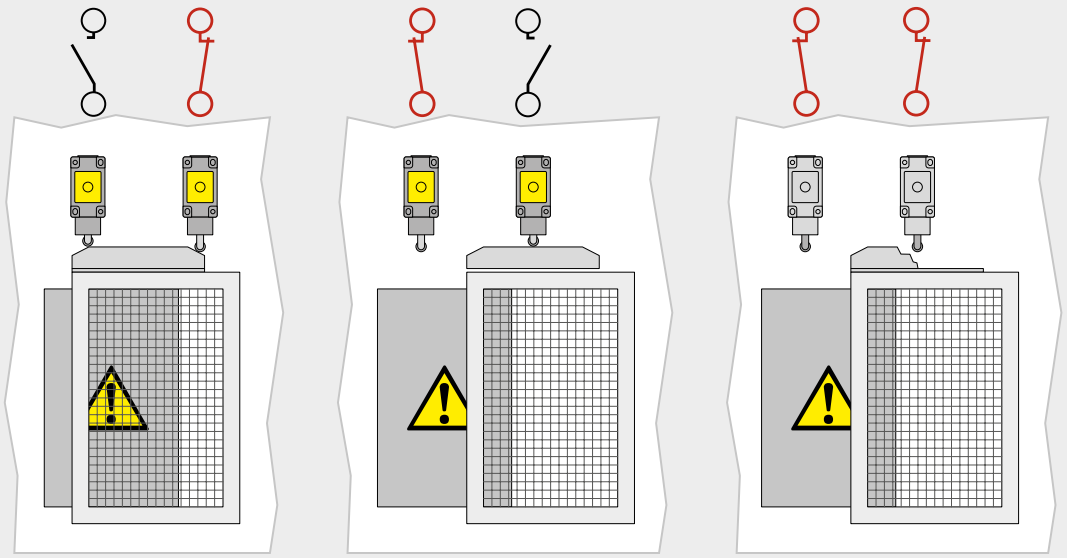
8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

冗余设计

由于干忧、执行器或位置开关的机械故障 (如老化) 或外部环境条件的影响 (如粉尘沉积粘住滚轮柱塞)，单个安全开关可能发生致命失效。当所需安全等级较高时，尤其要使用另一个位置开关 (如具有反向功能的)，并通过控制系统监控二者。

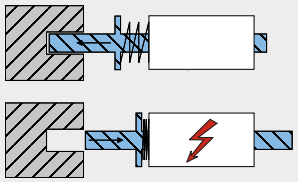
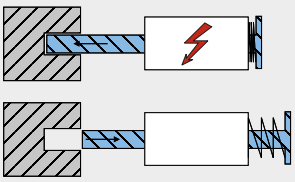
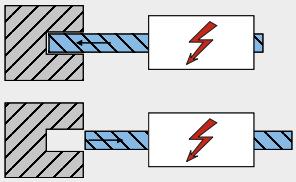
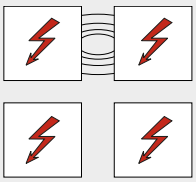
示例: 前部防护门被循环动作的注塑机。规定在此使用两个机械开关。

示例: 通过多样化冗余布置检测机械故障



锁定装置

锁定装置用于防止物理防护装置打开。若机器危险状态的停止时间长于人员到达危险区域的所需时间，则应使用锁定装置（安全功能“暂时防止接近”）。锁定装置应防止进入危险区域，直至不再存在危险的机器状态。当不应中断流程时，也需要锁定装置（仅提供流程保护，不属于安全功能）。
下图所示为锁定装置的可能设计。

原理	形状			动力
				
工作方式	弹簧力动作与通电解锁	通电动作与弹簧力解锁	通电动作与通电解锁	通电动作与通电解锁
名称	机械锁定装置 （首选用于人员保护）	电气锁定装置 （首选用于流程保护）	气动或液压锁定装置	磁性锁定装置

可如下进行通电解锁锁定装置：

- 定时：若使用时间开关，则该装置失效不得减少延迟时间。
- 自动：只有当不存在危险的机器状态时（如通过停机监测器）。
- 手动：防护装置解锁与启用之间的时间必须长于机器危险状态的停止时间。

锁定装置的机械与电气集成

锁定装置通常与安全开关使用相同的规定。在强制打开原理上，应注意哪些触点采用了强制打开的设计。当执行器拔出后，门信号触点显示门已打开。这些触点可以是，但不必总是强制打开常闭触点。

辅助解锁和紧急解锁

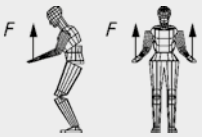
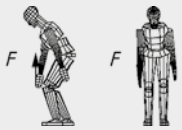
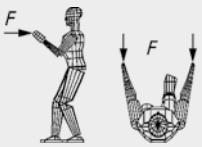
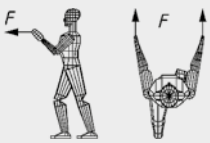
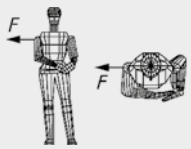
风险评估可能显示，在故障情况或紧急情况下需要将受困人员从危险区域救出的措施。应区分辅助解锁（使用工具）和紧急或逃生解锁（无需工具）的理念。

必要的锁定力

选择锁定装置时，一项根本标准是锁定物理防护装置所需的力。ISO 14119 (2013) 标准草案的附录 I 规定了可施加到最常用的可移动防护装置的最大静态力。

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

根据 ISO 14119 (2013) 标准的附录 I，防护设备的必要锁定力

力的方向		姿势	施力	力 [N]
	水平拉 (拖)	坐姿	单手	600
	垂直向上	站立，躯干和 腿弯曲， 双脚平行	双手， 水平把手	1400
	垂直向上	自由站立	单手， 水平把手	1200
	水平，平行于身体的对 称平面向后，拉	站立，双脚平行 或呈迈步姿势	双手， 垂直把手	1100
	水平，平行于身体的对 称平面向前，推	站立，双脚平行 或呈迈步姿势	双手， 垂直把手	1300
	水平，垂直于身体的对 称平面推	站立，躯干弯向一侧	肩膀压到金属板上	1300
	水平，垂直于身体的对 称平面推	站立，双脚平行	单手， 垂直把手	700

3 C

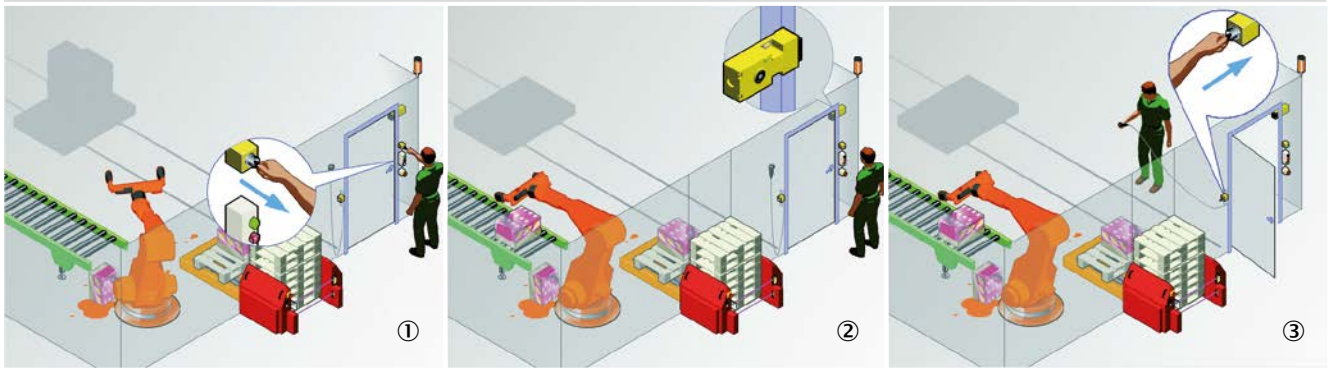
钥匙安全联锁系统

物理防护设备具有当进入危险区域并随后关闭防护设备时，无法有效防止重启的缺点。需要附加措施，如复位装置或使用 U 型锁锁住2型结构的联锁装置的执行器。但这项组织措施依赖于用户的意愿或注意力。

钥匙安全联锁系统可强制防止启动。必须使用当转到某些位置时可卡在钥匙开关内的钥匙来激活特定功能和操作模式。

拔出钥匙时（图 ①），将生成一个停止信号并结束危险状态。在安全状态中（停机时）可以开门（图 ②）。处于内部区域时，插上钥匙实现“调整”操作模式（图 ③）并借助使能按钮触发“危险的机器动作”（机器人转到一边）。在此期间自动操作模式将被阻止。

示例: 钥匙安全联锁系统



8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

电敏防护设备 (ESPE)

与“物理防护装置”不同，电敏防护设备 (ESPE) 的保护作用并非基于遭受危险的人员与危险本身的物理隔离。通过定时隔离实现保护作用。只要有人位于限定区域，危险的机器功能就不会发生。若此类功能已经发生，则必须使其停止。停止需要一定时间，所谓的“停止/停机时间”。

ESPE 必须及时检测到有人靠近该危险区域，并且根据应用情况也要检测到危险区域内有人存在。

国际标准 IEC 61496-1 规定了对 ESPE 的安全技术要求，与所用技术和工作原理无关。

电敏防护设备具备哪些优势？

如果操作人员不得不频繁或定期干预机器并在此期间暴露于危险，则使用 ESPE 代替 (机械式) 物理防护装置 (盖罩、防护栏等) 有利于:

- 减少进入时间 (操作人员无需等待防护装置打开)
- 提高生产效率 (节省机器的装料时间)
- 从人类工效学上改善工作场所 (操作人员无需操纵物理防护装置)

此外，操作人员和其他人员得到同样保护。

电敏防护设备无法防护哪些危险？

电敏防护设备并非物理屏障，所以不能保护人员免受放射伤害，如飞出的机器零件、工件或切屑、游离辐射、高温 (热辐射)、噪声、喷溅的冷却液和润滑油等。ESPE 也不能用于较长的停止/停机时间需要无法实现的最小距离的机器。

在此类情况下，必须使用物理防护装置。

ESPE 技术

电敏防护装置可通过不同原理实现人员检测: 光学、电容、超声波、微波和被动式红外检测。

多年来，光学防护装置已在大量实践中证明其有效 (见插图)。

光电保护装置

最常见的电敏防护装置是光电设备，如

- 安全光幕和安全光栅 (AOPD: 有源光电防护装置)
- 安全激光扫描仪 (AOPDDR: 使用有源光电漫反射防护器件设备)
- 基于图像的防护设备 (VBPD: 基于视觉的防护设备)

光电保护装置示例

若操作人员不会暴露于飞出的部分材料 (如材料熔化后的飞溅) 带来的受伤危险，可使用光电保护装置。

3 C

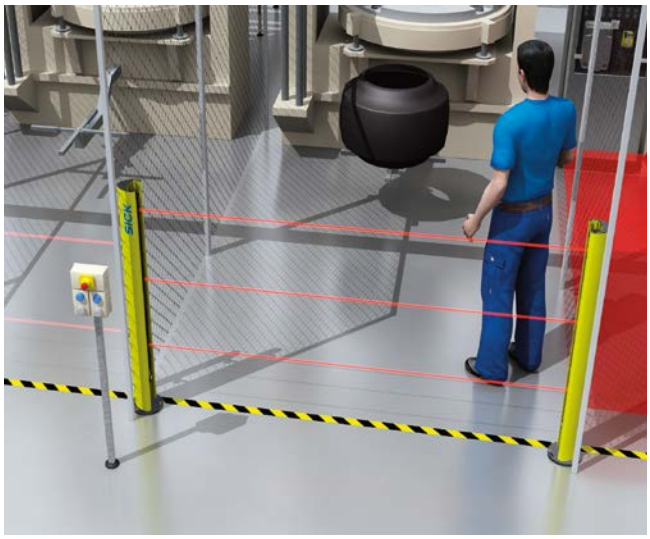
安全光幕和安全光栅 (AOPD)

AOPD 是通过光电发射与接收器件在指定二维区域内检测人员的防护设备。从发射器发射到接收器的一系列平行光束 (通常为红外线) 建起防护危险区域的保护区域。如有不透光的物体完全中断一条或多条光束, 将被检测出来。在此期间, 接收器通过信号切换 (关闭状态) 感知光束中断, 向其切换装置 (OSSD)输出信号 。

OSSD 的信号用于停止危险的机器状态。

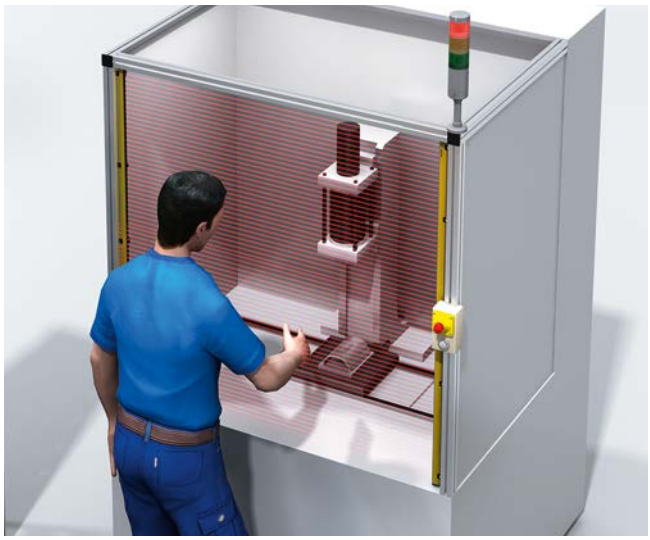
国际标准 IEC 61496-2 规定了对 AOPD 的安全技术要求。

典型的 AOPD 包括多光束安全光栅及安全光幕。检测能力大于 40 mm 的 AOPD 被称为多光束安全光栅。其用于防护进入危险区域的通道 (见插图) 。



使用多光束安全光栅的通道保护

检测能力小于等于 40 mm 的 AOPD 被称为安全光幕, 用于直接防护作业危险点 (见插图) 。



使用安全光幕的危险点保护

多光束安全光栅及安全光幕一般不会同时激活全部光束, 而是迅速依次接通和关闭光束。这增强了对其他光源的抗干扰性并因此提高了可靠性。最新 AOPD 的发射器和接收器在光路上自动同步。

通过使用微处理器可单独评价各条光束。借此实现单纯保护功能之外的附加 ESPE 功能 (➜ 3-40)。

8020567/2017-08-22(GCN 2021-07-01)
如有更改, 恕不另行通知

安全激光扫描器 (AOPDDR)

AOPDDR 是防护设备利用光电发射与接收器件，通过接收设备制造的光辐射的反射光。该反射光由指定二维区域内的目标产生。

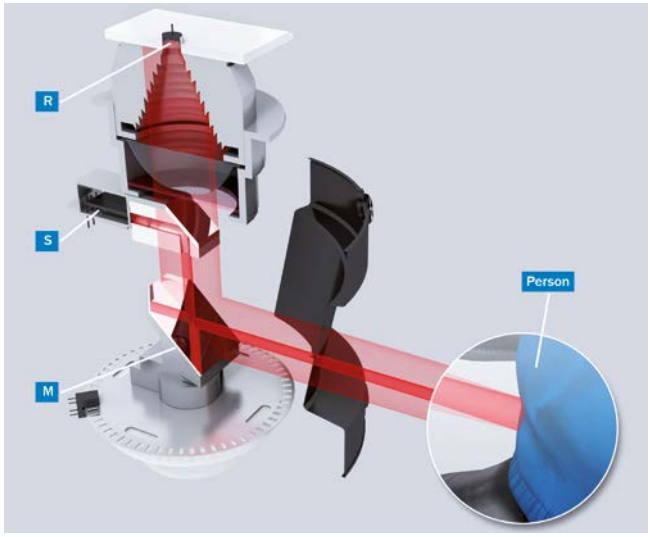
接收器通过信号切换 (关闭状态) 感知光束，向其切换装置 (OSSD)输出信号 。

OSSD 的信号用于停止危险的机器状态。

安全激光扫描器是一种光学传感器，利用同一平面上的红外激光束扫描周围环境并借此监控机器或车辆上的危险区域。

其根据飞行时间测量原理 (见下一页的插图) 工作。扫描器发出非常短的光脉冲 (S)。并同时运行“电子秒表”。若光线碰到目标，则反射后的光线将被扫描器接收 (R)。通过发射与接收之间的时间差，扫描器可算出到目标的距离。

扫描器内均匀旋转的反射镜使光脉冲偏转以覆盖一个扇形面。根据测得的距离和反射镜的相应旋转角度，扫描仪可确定目标的准确位置。



激光扫描器的基本结构

用户可以编程检测目标的区域 (保护区域) 。最新设备允许同时监测多个区域或在运行期间切换这些区域。这样便可例如使监测区域适应车辆速度。

安全激光扫描器利用朝特定方向准确发射的单一光脉冲工作，亦即并非连续覆盖待监测区域。通过这种工作方式实现 30 mm 到 150 mm 之间的分辨率 (检测能力) 。基于主动式扫描原理，安全激光扫描器无需外部接收器或反射器。安全激光扫描器也必须能够可靠检测反射能力极低的目标 (如黑色工作服) 。国际标准 IEC 61496-3 规定了对 AOPDDR 的安全技术要求。

基于图像的防护设备 (VBPD)

VBPD 是基于图像的防护设备，凭借图像捕捉与处理技术可靠检测人员 (见插图) 。

目前使用特殊的光发射器作为光源。VBPD 也可以使用现有环境光。

可运用多种原理检测人员，包括:

- 由反射器反射的光线被中断
- 目标反射光线的飞行时间测量
- 监控背景图案的变化
- 根据人类特点检测人员

基于图像的防护设备

未来的国际标准系列 IEC 61496-4 将包含对 VBPD 的安全技术要求。

检测能力 (分辨率)

光电防护设备

检测能力被定义为使电敏防护设备 (ESPE) 响应的传感器参数极限。

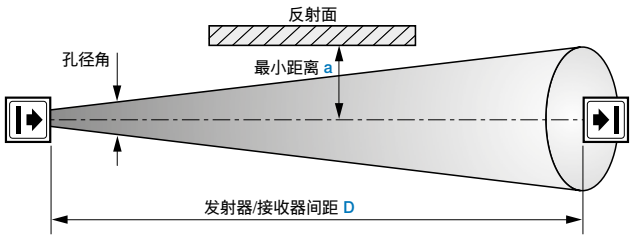
实际上, 它指的是在 ESPE 的限定监测区域 (保护区域) 内始终检测到的最小目标尺寸。

检测能力由制造商指定。通常由光束间距与有效光束直径之和确定。由此确保具有该尺寸的目标无论在保护区域内的什么位置总能完全覆盖一条光束, 从而被检测出来。

安全激光扫描器 (AOPDDR) 的检测能力取决于到目标的距离、单一光束 (脉冲) 之间的角度以及发射光束的形状与尺寸。检测能力的可靠性通过 IEC 61496 标准系列中的类型分级确定。

AOPDDR 属于 3 型。AOPD 属于 2 型和 4 型 (要求见表格)。抗光干扰源 (日光、不同灯泡种类、相同结构型式的设备等)、抗反射面、正常运行期间不对光的行为和安全激光扫描器漫反射的要求起到重要作用。

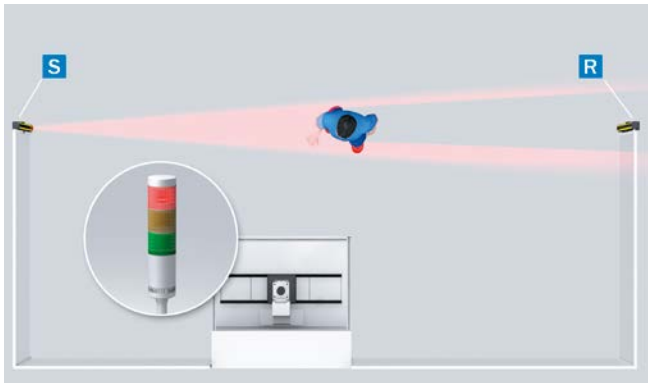
	2 型	4 型
功能安全	若在测试间隔之间发生故障, 则可能失去保护功能	即使发生多个故障, 仍维持保护功能
EMC (电磁兼容性)	基本要求	更高要求
透镜的最大孔径角	10°	5°
在 < 3 m 的距离 D 下, 与反射面的最小距离 a	262 mm	131 mm
在 > 3 m 的距离 D 下, 与反射面的最小距离 a	= 距离 x tan (10°/2)	= 距离 x tan (5°/2)
一套设备内多个相同结构的发射器	无特殊要求 (建议光束编码)	无影响或 OSSD 在受到影响时关闭



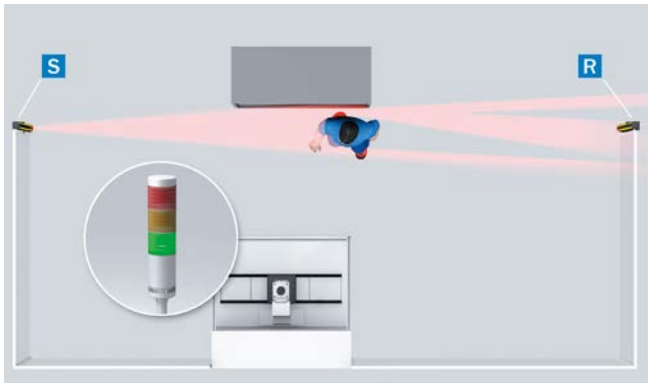
根据 IEC 61496, 2 型与 4 型 AOPD 的主要区别

避免来自 AOPD 的反射

AOPD 而言，光束从发射器聚焦。透镜的孔径角尽可能缩小，因此即使存在细微的对准误差也能保证无故障运行。这同样适用于接收器的孔径角（依照 IEC 61496-2 的有效孔径角）。但即使孔径角较小，发射器的光束也可能因反射面而偏转，导致未能检测到目标（见插图）。



人员被可靠检测出来，停止危险动作。



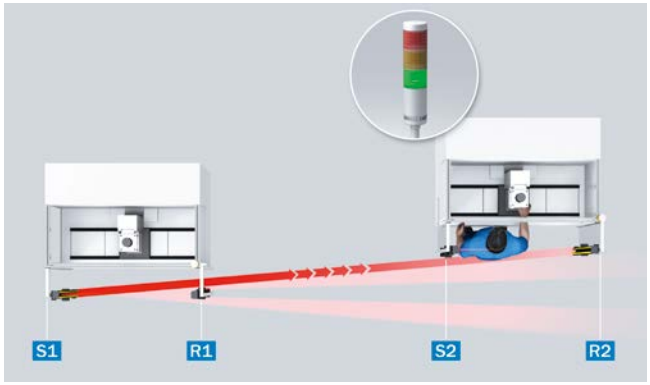
由于反射，ESPE 的保护作用失效，危险动作不会停止。

因此，所有反射面和反射体（如料箱、反光地面等）必须与系统的保护区域保持最小距离 a（见表格“根据 IEC 61496，2 型与 4 型 AOPD 的主要区别” ➜ 3-32）。

该最小距离 **a** 取决于发射器与接收器之间的距离 **D**（保护区域宽度）。必须在保护区域的所有方向遵守最小距离。

AOPD 的相互干扰

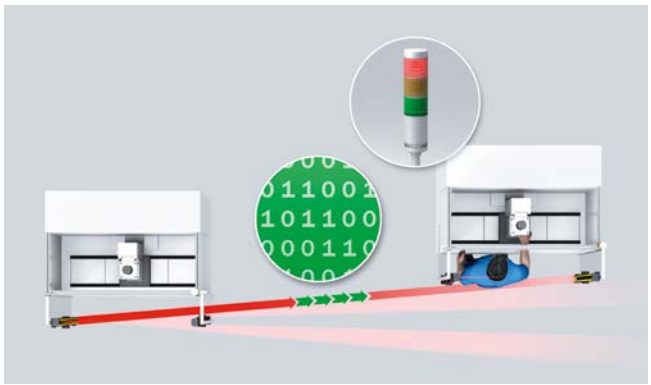
如有多台 AOPD 彼此相邻工作，则一个系统 (S1) 的发射器光束可能影响另一个系统 (R2) 的接收器。受此影响的 AOPD 有不再具备保护能力的危险 (见插图)。



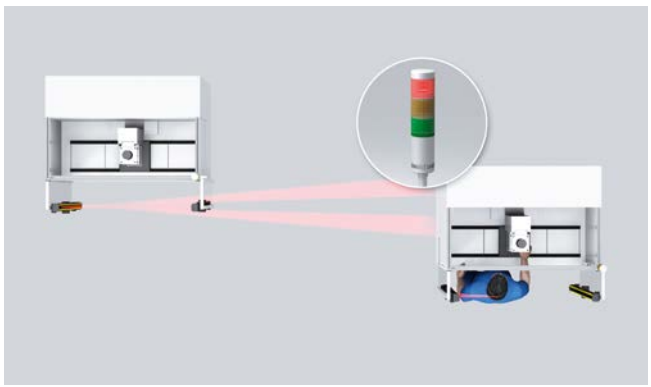
由于相互干扰，ESPE 的保护能力失效，危险动作不会停止。

必须避免此类安装情况。若无法避免，则须采取合适的措施防止相互干扰，如安装不透光的隔离墙或将其中一个系统的发射器方向调转。

4 型 AOPD 必须具备合适的外部发射器检测并在受到影响时转到安全状态 (输出端处于关闭状态) 或具备防止影响的技术措施。通常采用光束编码，以便接收器仅响应所匹配 (具有相同编码) 发射器的光束 (见插图)。



通过使用光束编码避免防护设备的相互干扰——人员被可靠检测出来，危险动作停止。



通过适当布置避免防护设备的相互干扰

选择合适的 ESPE

标准可能包括:

- 协调标准，特别是 C 类标准中的要求
- 危险区域前面的可用空间
- 人类工效学标准，如循环放料工作
- 分辨率范围

ESPE 应执行哪些安全功能？

- 触发停止 (➜ 3-3)
- 避免意外启动 (➜ 3-4)
- 防止启动 (➜ 3-4)
- 组合: 触发停止并防止启动 (➜ 3-4)
- 实现物料通道 (➜ 3-5)
- 监控机器参数 (➜ 3-5)
- 安全相关显示和报警 (➜ 3-7)
- 其他功能，如 PSDI 模式、消隐、保护区域切换等 (➜ 3-40)

安全等级

安全技术参数体现在 ESPE 的类型分级 (2 型、3 型、4 型) 中。

除了结构方面 (根据 ISO 13849-1分类)，在类型分级中还定义了就电磁兼容性 (EMC)、环境条件和光学系统而言应遵守的要求。其中尤其包括抗干扰源 (太阳、灯泡、相同类型的设备) 的行为以及安全光幕或安全光栅透镜的孔径角 (对 4 型 AOPD 的要求高于对 2 型 AOPD 的)。

孔径角对确定与反射面的最小距离至关重要 (表格 ➜ 3-32)。

➜ 对 ESPE 的要求: IEC 61496-1、IEC 61496-2、IEC 61496-3

通过光电防护设备可实现的安全功能可靠性

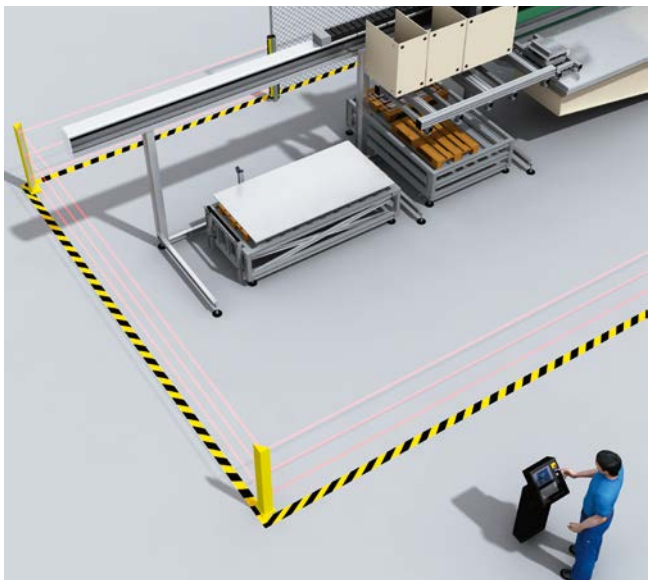
		ISO 13849-1					设备示例
		a	b	c	d	e	
符合 EN 61496-1 的 ESPE 类型	2						安全光幕、单光束安全光栅、多光束安全光栅
	3						安全激光扫描器、安全摄像系统
	4						安全光幕、单光束安全光栅、多光束安全光栅
			1		2	3	
			SIL (IEC 62061)				

始终遵守光电防护设备操作指南中包含的其他使用说明、信息和指示!

ESPE 应检测什么?

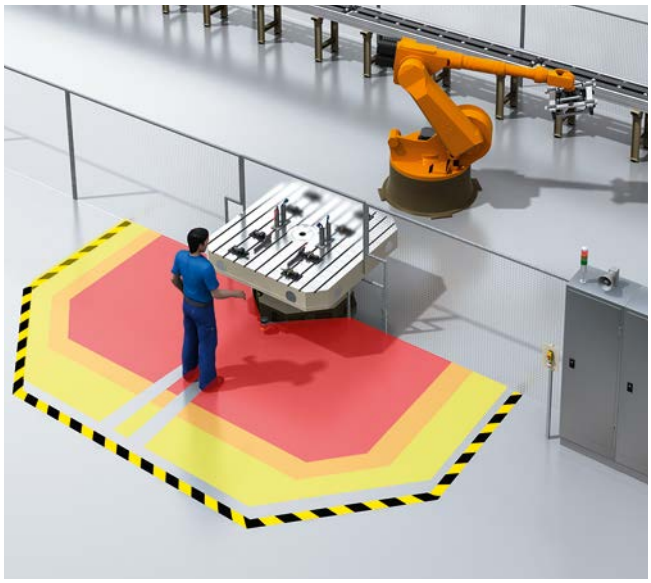
危险点保护:
手指或手部检测
在危险点保护中会检测作业危险点附近的靠近行为。
此类防护设备的优势在于允许较短的最小距离, 操作人员可以更加符合人类工效学地工作 (例如压力机上的放料工作) 。

通道保护:
检测即将进入危险区域的人员
在通道保护中, 通过检测身体来检测人员靠近。
这种类型的防护设备用于防止通道危险区域。踏入危险区域时将触发停止信号。站在防护设备后面的人不会被 ESPE 检测到!



8020567/2017-08-22(GCN 2021-07-01)
如有更改, 恕不另行通知

危险区域保护:
识别危险区域中有人存在
在危险区域保护中, 通过区域内的检测来识别人员靠近。此类防护装置适用于例如从复位按钮处无法完全看到危险区域的机器。踏入危险区域时将触发停止信号并阻止启动。



移动式危险区域保护:
识别有人靠近危险区域
移动式危险区域保护适用于 AGVS (自动导引系统)、起重机和叉车, 在车辆移动或将车辆对接到固定站期间保护人员。

可集成到 ESPE 中的安全功能

以下安全功能可集成到逻辑单元或直接集成到合适的 ESPE 中。

屏蔽 (Muting)

屏蔽功能允许暂时停用防护装置的保护功能。当物料必须在不中断工作进程 (机器危险状态) 的情况下穿过防护装置的保护区域时, 需要屏蔽功能。

在某些机器状态允许的情况下, 其也可以合理用于优化工作进程: 例如在压力机块无危险地向上运动期间屏蔽安全光幕的功能, 使操作人员更容易取出工件。

只有当通过的物料不会阻碍接近作业危险点时, 才可以进行屏蔽。对于不能从后面进入 (不能穿行) 的防护装置, 则仅允许在不存在危险的机器功能时进行屏蔽 (见插图) 。

通过屏蔽传感器或信号确定该状态。

就屏蔽功能而言, 在选择与定位屏蔽传感器和所用控制信号时, 需要非常谨慎。

缠绕包装机上利用安全光幕和屏蔽传感器的屏蔽功能

为了安全地实现符合标准的屏蔽功能, 应遵守以下条件:

- 屏蔽期间, 必须通过其他手段保证安全状态, 也就是说不得允许进入危险区域。
- 屏蔽必须自动而不得手动进行。
- 屏蔽不得依赖于单一电气信号。
- 屏蔽不得完全依赖于软件信号。
- 在无效组合过程中出现的屏蔽信号不得允许屏蔽状态。
- 物料通过后应立即取消屏蔽状态。

为提高区分质量, 可使用附加限制、联锁或信号, 如:

- 物料的移动方向 (屏蔽信号序列)
- 屏蔽持续时间的限制
- 机器控制系统的物料请求
- 输送元件的运行状态
  (如输送带、滚筒输送机)
- 借助附加特性的物料识别 (如条形码)

➜ ESPE 的实际应用: IEC / TS 62046

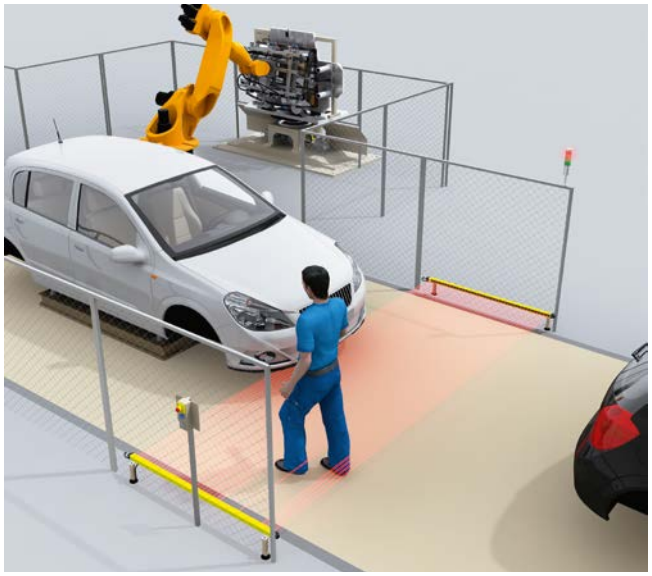
8020567/2017-08-22(GCN 2021-07-01)
如有更改, 恕不另行通知

带进出口功能的安全光幕

允许物料在防护区域内移动的另一种方法是主动区分人和物料（进出口功能）。

在该应用中采用水平布置的安全光幕 (AOPD)。在此借助单独评价每条光束来区分物料或物料载体 (如托盘) 的遮光形式与人员的遮光形式。

通过应用自示教动态消隐及其他区分标准 (如移动方向、速度进出保护区域等) 可实现安全的相关区分。由此可靠防止人员不被检测地进入危险区域 (见插图)。



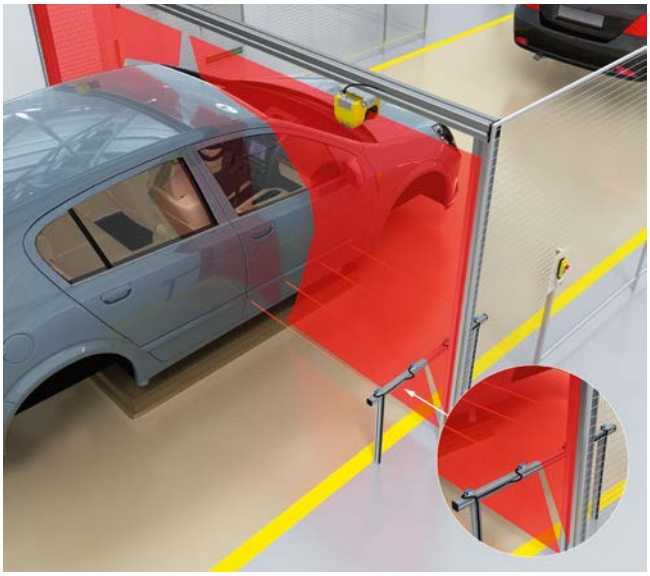
汽车生产线加工站内利用水平安全光幕的进出口功能

带保护区域切换的安全激光扫描器

允许物料在防护区域内移动的一种替代方法是主动切换保护区域。

在该应用中，通常采用提供垂直 (或略微倾斜) 保护区域的安全激光扫描器。

根据来自机器控制系统和相应位置上传感器的适当信号，从一系列预编程保护区域中激活适当的保护区域。保护区域轮廓的设计使得物料通过不会导致防护装置响应，而且不受监测的区域足够小，以至人员无法不被检测地进入危险区域 (见插图)。

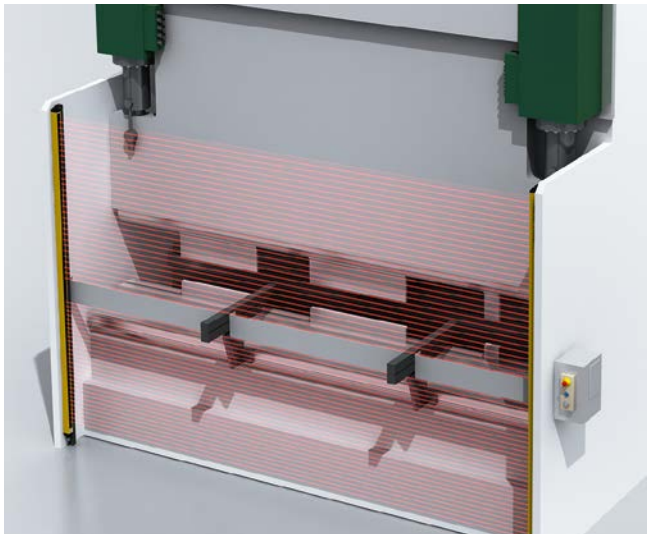


利用安全激光扫描器、垂直保护区域和借助适当布置的传感器切换保护区域实现物料通过

ESPE 的附加功能

消隐 (Blanking)

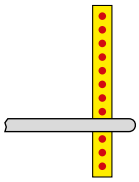
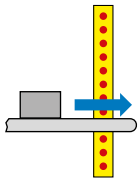
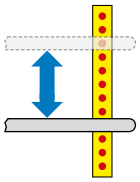
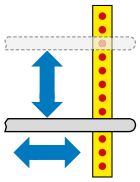
许多 AOPD 的检测能力和/或保护区域配置可以设计成，在保护区域内的特定部分存在一个或多个目标物时，不会触发安全功能（关闭状态）。消隐可用于允许特定目标穿过保护区域，如冷却润滑剂软管、工件滑道或载体（见插图）。



弯边压力机上对光幕光束的固定消隐

在消隐区域，ESPE 的检测能力增大（变差）。计算最小距离时，遵守制造商的相应说明。

固定消隐是指消隐区域的尺寸和位置固定。**浮动消隐**仅确定消隐区域的尺寸，而不限制在保护区域内的位置（见插图）。

固定消隐		浮动消隐	
固定消隐	增加尺寸公差的固定消隐	完全监控目标的浮动消隐	部分监控目标的浮动消隐
固定尺寸的目标必须位于保护区域内的特定位置。	有限尺寸的目标允许从操作人员一侧穿过保护区域。	固定尺寸的目标必须位于保护区域内的特定区域。允许物体移动。	固定尺寸的目标允许位于保护区域内的特定区域。允许物体移动。
			

固定消隐与浮动消隐的标准

为避免保护区域内存在漏洞，可利用目标的消失（或在有些情况下目标尺寸或位置的变化）触发安全功能（关闭状态）。

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

PSDI 模式

使用防护装置触发机器功能 (控制型防护设备) 被称为 PSDI 模式。该操作模式有利于手动循环放入或取出零件。

根据标准, 仅允许使用有效分辨率 d ≤ 30 mm 的 4 型 AOPD 执行 PSDI 模式。在 PSDI 模式下, 机器于限定位置等待操作人员完成指定中断次数。被遮光特定次数后, 安全光幕自动重新启用危险动作。

在以下条件下需要复位 ESPE:

- 机器启动时
- 重启时, 如果 AOPD 在危险移动内被遮挡
- 在规定 PSDI 时间内未触发 PSDI 时

需要检查在工作流程期间能否对操作人员产生危害。因此, 该操作模式的使用限制在危险区域不可进入, 且操作人员无法不被检测地留在保护区域与机器之间 (后方进入防护) 的机器。

单次遮光PSDI 模式是指 AOPD 在操作人员结束遮光后触发机器功能。

双次遮光 PSDI 模式是指 AOPD 在操作人员第一次遮光 (如取出已加工的工件) 后使机器功能留在联锁状态。只有在操作人员结束第二次遮光 (如送入坯件) 后, AOPD 才重新启用机器功能。

PSDI 模式常用于压力机和冲压机, 但也可以在其他机器上使用 (如转台、自动装配机) 。应用 PSDI 模式时, 不得允许从后面进入光幕。压力机上的 PSDI 模式适用特殊条件。

自动装配机上采用安全光幕的单次遮光 PSDI 模式。放料时, 工具位于顶点。操作人员离开保护区域后, 装配流程开始。

就 PSDI 模式而言, AOPD 的分辨率必须小于或等于 30 mm (手指或手部检测) 。

➜ PSDI 触发: B 类标准 ISO 13855、IEC 61496-1
➜ 压力机上的 PSDI 模式: C 类标准 EN 692、EN 693

固定位置防护装置

固定位置防护装置属于非物理防护装置，使人员或个别身体部位固定在危险区域之外的某个位置。

固定位置防护设备的完整概览参见:
➜ Alfred Neudörfer: Konstruieren sicherheitsgerechter Produkte (符合安全产品的设计) , Springer-Verlag, Berlin u. a., ISBN 978-3-642-33889-2 (2013 年第 5 版)

双手操纵装置

双手操纵装置只保护一个人! 如有多名操作人员，则须每人操纵一台双手操纵装置。危险动作只能通过有意识地双手操纵双手操纵装置触发，并且必须在一只手松开装置时立即停止。
有多种类型的双手操纵装置。不同之处在于操作件的设计以及控制技术上的要求。
以下基本原则适用于所有类型:

- 必须确保双手使用。
- 松开两个操作件中的一个必须使危险动作停止。
- 必须防止意外激活。
- 不得允许轻松废弃保护作用。
- 双手操纵装置不得允许携带进入危险区域。

对于 II 型和 III 型双手操纵装置，原则上适用:

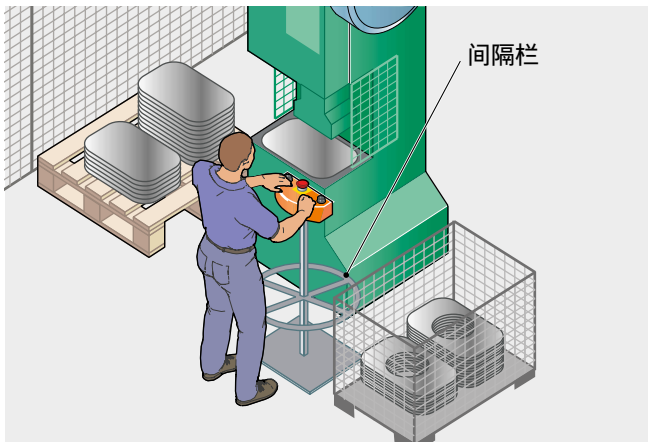
- 松开两个操作件再操纵后，才允许重新开始动作。

对于 III 型双手操纵装置，原则上适用:

- 只有在两个操作件 (按钮) 于 0.5 秒内同步操纵后，才允许开始动作。

针对 III 型双手操作式装置，定义了符合详细的控制技术要求的子类型。最为重要的子类型包括:

- III A 型: 评价每个操作件 (按钮) 的常开触点 (2 个输入)
- III C 型: 评价每个操作件 (按钮) 的常开触点和常闭触点 (4 个输入)



➜ 对双手操作式装置的要求: ISO 13851 (B 类标准)

➜ 双手操作式装置的最小距离计算 ➜ 3-52

使能装置

在调整和维修机器期间以及需要近距离观察生产过程时，可能需要暂时取消防护装置的功能。除了最大限度降低风险的其他措施（减小作用力或速度等），在防护装置功能取消期间，还必须控制装置被激活。在这种情况下，使能装置是一个选项。
使能装置是通过身体致动的控制开关，借此获得操作人员对机器功能的许可。通常使用按钮或脚踏开关作为使能装置。
操纵杆或点动按钮可用作使能装置的附加启动控制器。三位置使能装置已在工业中证明其有效性，因此推荐使用。

不得仅通过致动使能装置触发机器启动。事实上，仅在使能装置被致动期间允许动作。

三位置使能装置的工作方式：

姿势	致动器	功能
1	未被致动	关闭
2	在中间位置（压力点）	使能
3	超出中间位置	紧急停止（关闭）

从位置 3 切换回位置 2 时，使能功能不得启用。
若使能装置在位置 3 采用单独触点，则其应当集成到急停电路中。

使用使能装置时，防干忧保护也非常重要。

➜ 对使能装置的要求：IEC 60204-1（B 类标准）

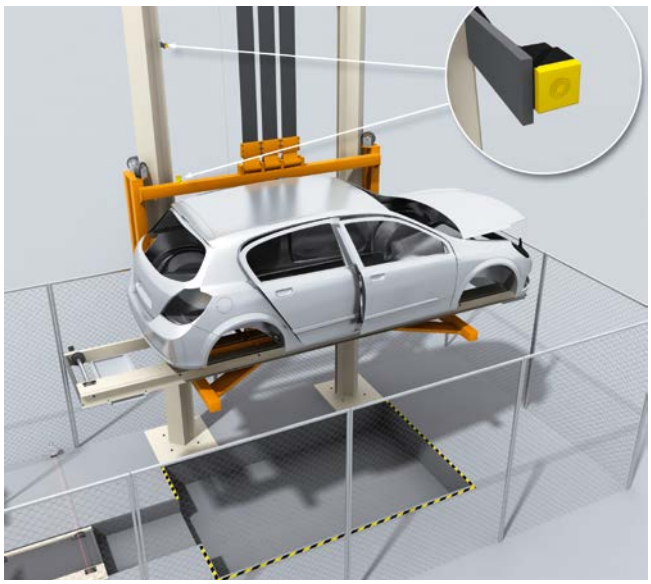
用于监控机器参数的传感器

风险评估可能显示，在运行过程中必须监控和记录某些机器参数。

安全的位置监控

若机器不应越过或离开特定位置，则可使用安全相关传感器或位置开关 (➜ 3-19)。

电敏安全感应式位置开关特别适合这项任务。其不需要特殊的配合件、不会磨损并具有较高的外壳防护等级，可监控机器人轴某一部分或可移动机的器部分的存在性。



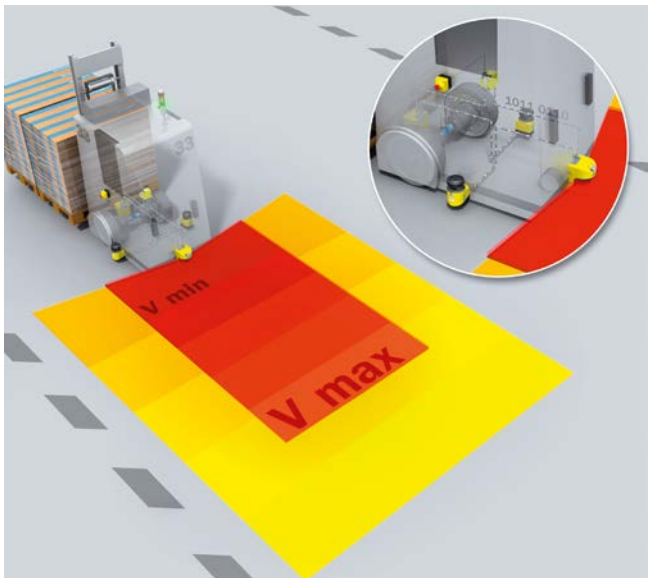
汽车生产线上升降机的安全位置监控

转速、速度、惯性运行监控

编码器或行程测量系统实现对转速、速度或惯性运行的检测和评价。

就自动导引系统而言，编码器信号可用于调整安全激光扫描器的保护区域大小以适应行驶速度。

安全的停机或旋转评价模块借助传感器或编码器监控驱动装置的移动，以便在停机或偏离所设参数时生成安全控制信号。若安全技术要求更高，可使用安全编码器或冗余编码器。另一种方法是监测由正在停转的电机通过剩磁感生的电压。



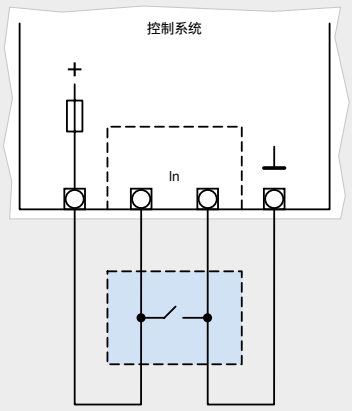
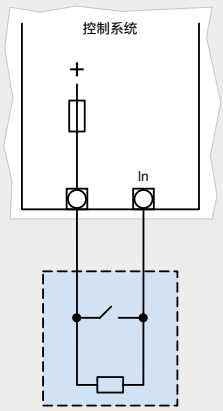
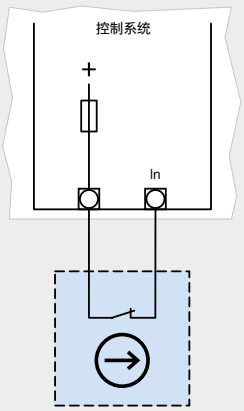
用于自动导航车上保护区域切换的速度监控

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

压敏垫、压敏条、缓冲器

在有些应用情况中，可能适宜采用压敏防护装置。工作原理大多基于空心体的弹性变形，空心体内部的信号发生器（以机电或光学）方式执行安全功能。

机电系统通常有不同规格。
在所有情况下，应务必遵守正确的机械设计与集成以实现有效的保护功能。在压敏垫与压敏板的产品标准中，未涉及对体重低于 20 kg 的儿童的检测。

短路设计（得电跳闸原理）		强制打开常闭触点设计（失电跳闸原理）
4 线版本	电阻版本	
		
当防护装置激活时，将出现短路。就 4 线版本而言，电路会被短接（几欧姆）。就电阻版本而言，会检测到变为目标电阻值（几千欧）。该设计形式需要更为复杂的评价。		该设计形式更加普遍，并提供更多优势。防护装置激活使开关触点断开。通过特别布线排除导线之间短路。

➜ 压敏防护设备的设计：B 类标准 ISO 13856（标准系列）

脚踏开关

脚踏开关用于控制工作进程。在有些机器上（如压力机、冲压机、折弯机与板材加工机上），脚踏开关仅允许在单独的操作模式下并配合其他技术防护措施（如慢速）用于安全功能。

但为此应采用特殊设计：

- 通过防护罩防止意外致动
- 类似使能开关原理的三位置设计（参见“三位置使能装置的工作方式” ➜ 3-43）。
- 作动致动器超过压力点时，允许手动复位（用手）
- 危险动作停止后，松开并重新作动脚踏开关后才允许用脚重启脚踏开关
- 至少评价一个常开触点和一个常关触点
- 如有多名操作人员，则须每人操纵一个脚踏开关

补充防护措施

如有需要，必须采取本体安全设计和技术防护措施之外的进一步防护措施。
此类补充防护措施主要包括:

- 紧急停机装置
- 解救受困人员措施
- 断开与导出能量措施
  (➜ 2-4 和 2-5)
- 轻松安全地搬运机器和重型部分的预防措施
- 安全接近机器的措施

若这些补充措施依赖于相应控制部件的正确工作，则其属于“安全功能”，应满足功能安全的要求 (参见“运用复位和重启”一章 ➜ 3-65) 。

紧急操作

紧急停止 (在紧急情况下停机)
在紧急情况下，不仅要停止所有危险动作，而且应安全释放产生危险的所有能量源，如储存的能量。该操作被称为紧急停止。除了机械指令中提到的例外，(ISO 13850) 每台机器必须至少装备一个紧急停止装置。

- 紧急停止装置必须容易接近。
- 紧急停止必须尽快结束危险状态，同时不产生附加风险。
- 紧急停止指令必须在所有操作模式下均优先于所有其他功能和指令。
- 复位紧急停止装置不得触发重启。
- 必须采用通过机械卡止功能直接致动的原理。
- 必须根据停止类别 0 或 1 进行紧急停止 (➜ 2-9)。

紧急断电 (在紧急情况下断电)
若电能可能导致危险或损坏，则应采取紧急断电。由此将通过机电开关放大器切断电能供给。

- 只有在所有紧急断电指令均复位后，才能允许通电。
- 紧急断电对应停止类别 0 (➜ 2-9)。

复位
若紧急停止装置被致动，则由此触发的设置必须留在关闭状态，直至紧急停止装置复位。
必须现场手动复位控制开关。仅允许通过复位，使机器准备恢复运行。

紧急停止和紧急断电属于补充防护措施，不是针对机器危险的风险降低手段。

要求和设计形式
所用控制开关的触点必须为强制打开常闭触点。操作件必须为红色，现有背景必须为黄色。可以使用:

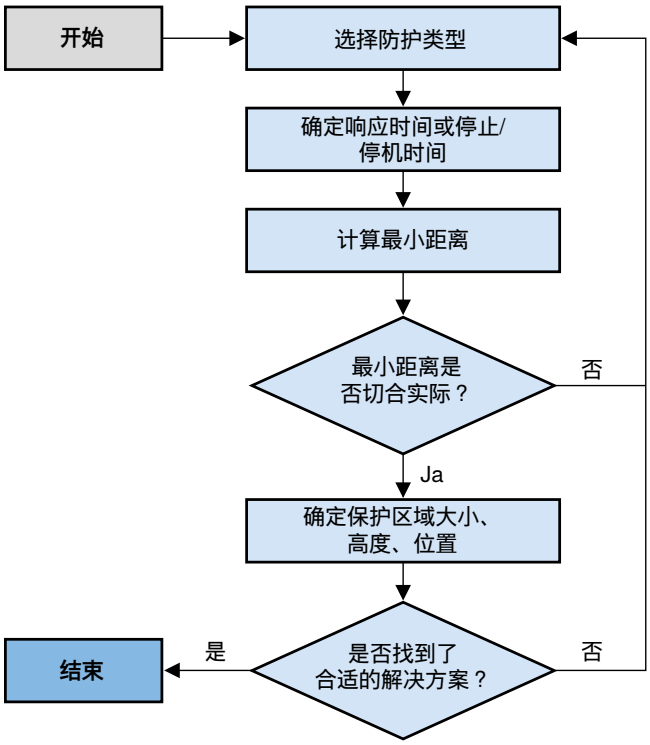
- 通过蘑菇头按钮致动的开关
- 通过金属丝、绳索或导轨致动的开关
- 无罩脚踏开关 (用于紧急停止)
- 电源隔离装置

若使用金属丝和绳索作为紧急停止装置的致动器，则其设计和安装应确保方便致动和触发功能。复位装置的布置应确保可从复位装置的位置看到金属丝或绳索的全长。

➜ 紧急停止装置的设计原则: ISO 13850
➜ 紧急停机: 机械指令 2006/42/EC

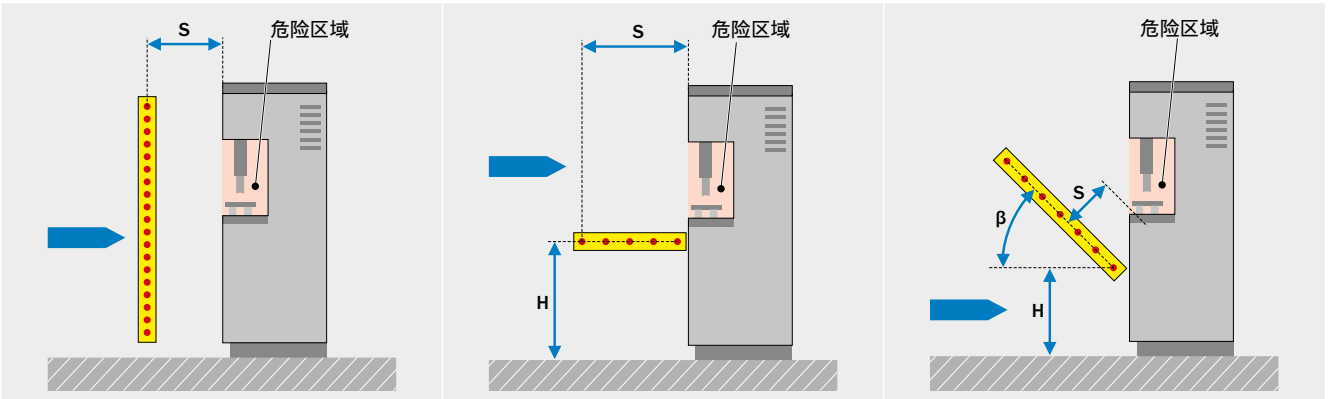
确定防护装置的位置或尺寸

可用空间对最佳防护装置的选择至关重要。必须确保在到达作业危险点前还能及时解除危险状态。
所需最小距离也主要取决于防护装置的尺寸和类型。



与靠近有关的 ESPE 的最小距离

最小距离考量适用于提供二维保护区域的 ESPE，如光幕、光电传感器 (AOPD)、激光扫描器 (AOPDDR) 或二维摄像机系统。一般分为三种靠近方式。



垂直靠近或垂直于保护区域平面侵入 | 平行靠近或平行于保护区域平面侵入 | 有角度靠近

选择好可触发停止的 ESPE 后，应计算 ESPE 的保护区域与最近作业危险点之间的最小距离。

需要考虑以下参数:

- 机器的停止时间
- 安全相关控制系统的响应时间
- 防护设备 (ESPE) 的响应时间
- 附加距离视 ESPE 的分辨能力、保护区域高度和/或靠近方式而定

若最小距离过大并且从人类工效学的角度不可接受，则须减少机器的总停止时间或使用分辨率更好的 ESPE。应避免从后面进入的可能。

➜ 针对 ESPE 的最小距离计算在 ISO 13855 标准中说明 (B 类标准)。

一般计算公式

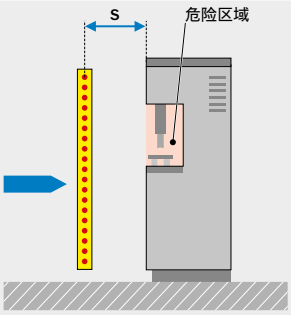
$$S = (K \times T) + C$$

其中:

- S 是以毫米为单位的最小距离，从最近的作业危险点到 ESPE 检测点或检测线或检测面。
- K 是以毫米每秒为单位的参数，从身体或身体部位的靠近速度得出。
- T 是以秒为单位整个系统的停止/停机时间。
- C 是以毫米为单位的附加距离，表示防护设备被触发前侵入危险区域的深度。若 ESPE 的保护区域不会被越过，则 C 取决于 ESPE 的检测能力 (分辨率) 并被称为 C_{RT} (reach through = 伸过)。若 ESPE 的保护区域可以被越过，则 C 取决于 ESPE 的保护区域高度并被称为 C_{RO} (reach over = 越过)。

下表包含与靠近保护区域有关的最小距离 S 的计算公式。

垂直靠近: β = 90° (± 5°)

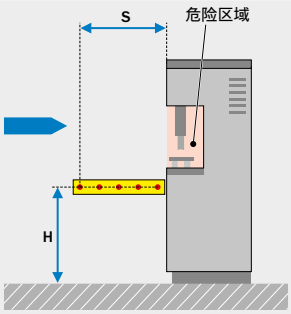


第 1 步: 计算最小距离 S

d ≤ 40 mm	S = 2000 × T + 8 × (d – 14) 若 S > 500 mm, 则使用: S = 1600 × T + 8 × (d –14)。 在这种情况下, S 不得 < 500 mm。	最小距离 S 不得 < 100 mm。 C = 8 × (d – 14) 在此是以毫米为单位的附加距离, 表示防护设备被触发前侵入危险区域的深度。
40 < d ≤ 70 mm	S = 1600 × T + 850	底光束高度 ≤ 300 mm 顶光束高度 ≥ 900 mm
d > 70 mm	S = 1600 × T + 850	**光束数量** / **推荐高度** 4 / 300、600、900、1200 mm 3 / 300、700、1100 mm 2 / 400、900 mm (若没有爬过的危险, 则仅允许使用 400 mm)

第 2 步: 计算保护区域上缘的所需高度 (➜ 3-57)

平行靠近: β = 0° (± 5°)



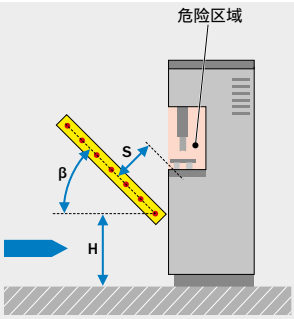
第 1 步: 计算最小距离 S

S = 1600 × T + (1200 – 0.4 × H) 其中 C = (1200 – 0.4 × H) ≥ 850 mm	H ≤ 1000 mm

第 2 步: 计算视保护区域高度而定的所需分辨率

$d \leq \frac{H}{15} + 50$ mm	H ≤ 1000 mm d ≤ 117 mm

有角度靠近: 5° < β < 85°



β > 30°	参照垂直靠近。	$d \leq \frac{H}{15} + 50$ mm 与底光束有关。
β < 30°	参照平行靠近。	S 适用于距离危险区域最远且高度 ≤ 1000 mm 的光束。

S: 最小距离
H: 保护区域高度 (检测面)
d: ESPE 的分辨率
β: 检测面与靠近方向之间的角度
T: 整个系统的停止/停机时间

特殊情况

压力机应用

在机器特定的 C 类标准中，可能包含不同于一般标准的特殊要求。下表尤其适用于金属加工压力机：

压力机的附加距离计算		
ESPE 的分辨率 d (mm)	**附加距离 C (mm)**	**ESPE/PSDI 模式触发滑块**
d ≤ 14	0	允许
14 < d ≤ 20	80	
20 < d ≤ 30	130	
30 < d ≤ 40	240	不允许
> 40	850	

➜ 压力机标准：EN 692/693 (C 类标准)

3 C

检测人员是否存在的防护 ESPE

该防护类型推荐用于可从地面接近的大型设备。在该特殊情况下，必须防止机器在里面有操作人员期间启动（“防止启动”安全功能）。在此涉及一种次要防护设备，可检测危险区域内有无人员，同时防止危险的机器状态启动。除了提供后方进入防护的 ESPE，还要采取用于“触发停止”安全功能的主要防护措施，例如其他 ESPE 或联锁的可移动物理防护装置。

在这种情况下，必须计算主要防护装置（例如负责停止设备的垂直光幕）的最小距离。

加工站的安全激光扫描器承担“触发停止”安全功能（序号 1）和“防止启动”安全功能（后方进入防护）（序号 2）

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

ESPE 在车辆上的应用
若车辆产生危险状态，则在确定最小距离时通常以车辆的行驶速度，而非人员的靠近速度为依据。若车辆（带着防护装置）与人员相互靠近，则一般认为人员将发现危险并站住或走开。因此，最小距离只需要足够大到允许安全停车。
根据应用情况和所用技术，可能还需要安全附加距离。

与工具一起移动的ESPE 的固定式应用
有些机器受功能限制需要操作人员非常靠近危险区域。在折弯机或卷边机上，小块板材必须与弯边保持非常接近。在工具开口周围形成保护区域的随行系统被证明是实用的防护装置。在此不考虑拿取速度，所以不适用一般公式。

对分辨能力的要求非常高，并且必须排除金属表面的反射。所以，为此使用带有基于图像评价功能的激光聚焦系统。在 C 类标准中，规定该防护类型与其他措施（如 3 位置脚踏开关、自动停机时间测量、戴手套义务等）配合使用。

3
C

➜ 折弯机安全: EN 12622 (C 类标准)

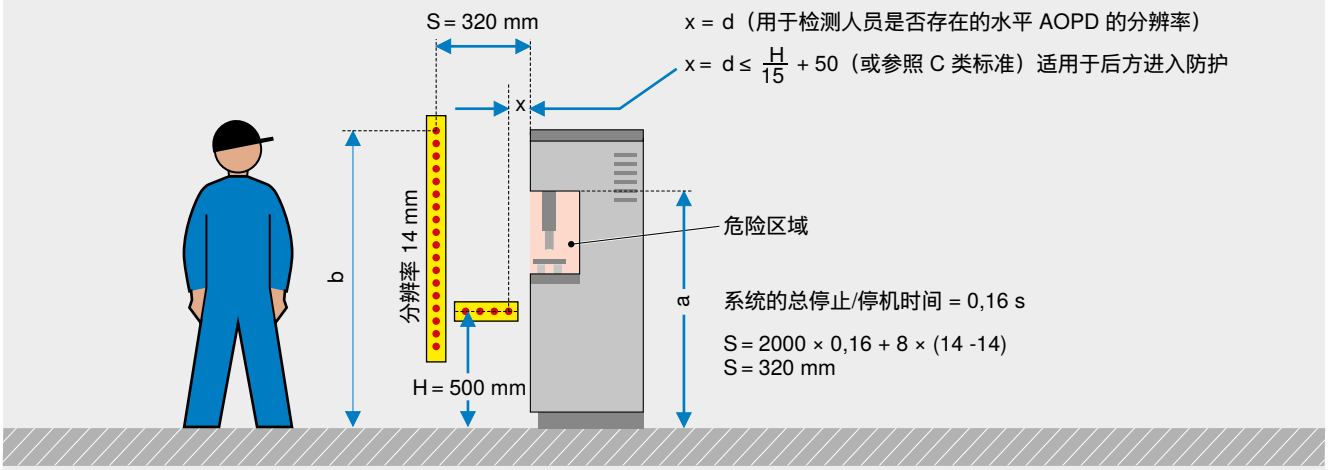
测量停止/停机时间和所需最小距离需要特定的专有技术和设备。
SICK 提供这些测量服务。

最小距离计算示例

解决方法 1: 垂直靠近——带后方进入防护的危险点保护

如图所示, 计算得出最小距离 S = 320 mm。通过使用具有较佳 分辨率的安全光幕, 这已经是最理想的最小距离。

为确保危险区域内任何地方的人员都能被检测到, 使用两种 AOPD: 根据算出的最小距离来定位的垂直 AOPD (垂直靠近), 和消除后方进入危险的水平 AOPD。



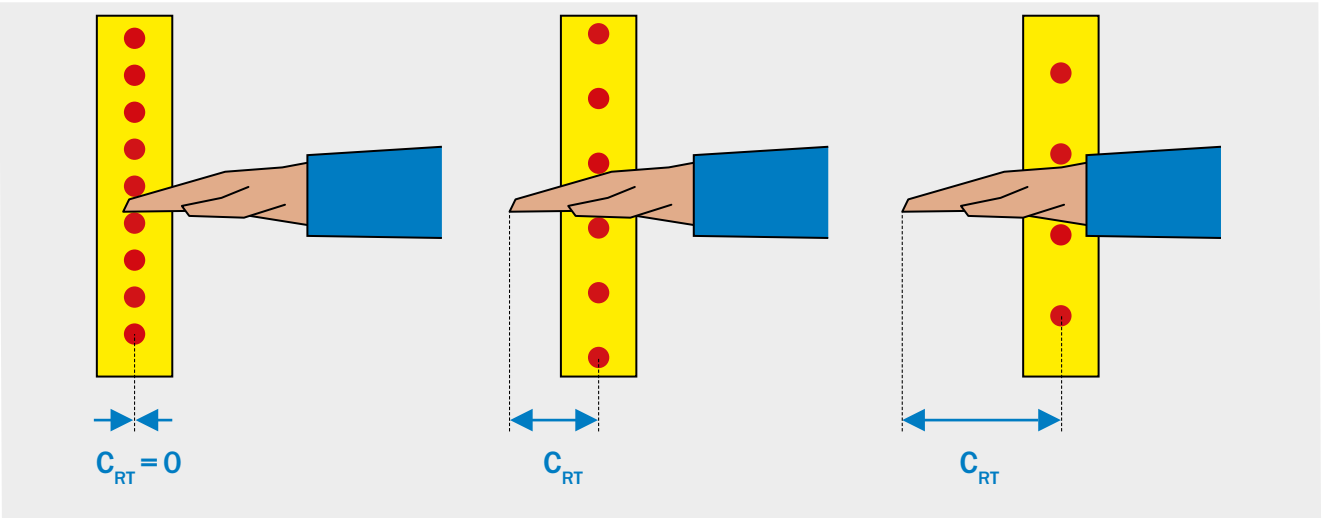
a = 危险区域高度
d = 检测能力 (AOPD 的分辨率)
H = 安装高度
S = 最小距离

x = 保护区域末端到机器的距离
b = 顶光束高度, 参见
"ESPE 的所需保护区域大小/高度" ➜ 3-55

视分辨率而定的附加距离 C_{RT}

根据 ESPE 的检测能力 (分辨率), ESPE 可能在身体部位穿过保护区域后才被触发。

因此, 必须加上视分辨率而定的附加距离 C_{RT}。



插图所示为不被检测地侵入具有不同检测能力的安全光幕的示例。

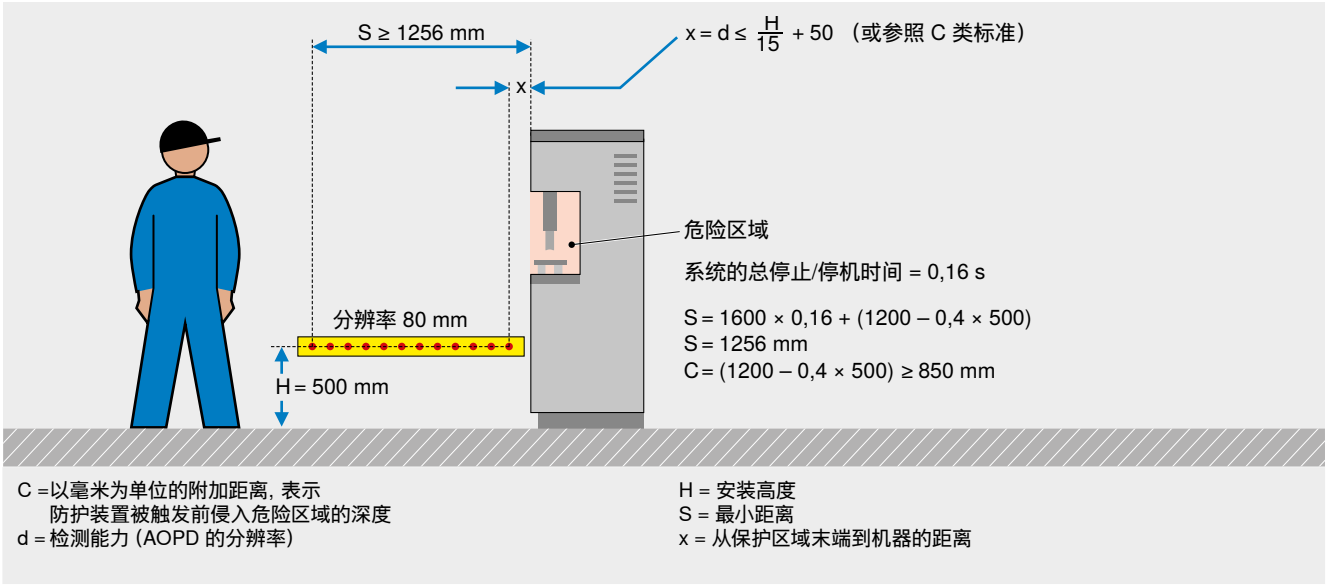
8020567/2017-08-22(GCN 2021-07-01)
如有更改, 恕不另行通知

解决方法 2: 平行靠近——危险区域保护

使用水平 AOPD。下图所示为最小距离 S 的计算和 AOPD 的定位。若 AOPD 的安装高度提高到 500 mm，最小距离将缩短。在该高度下，可使用分辨率小于等于 80 mm 的 AOPD。

但不得允许从 AOPD 下方进入危险区域。

该防护类型也经常通过 AOPDDR（激光扫描器）实现。但对于这些设备，必须加上受技术限制的附加距离。

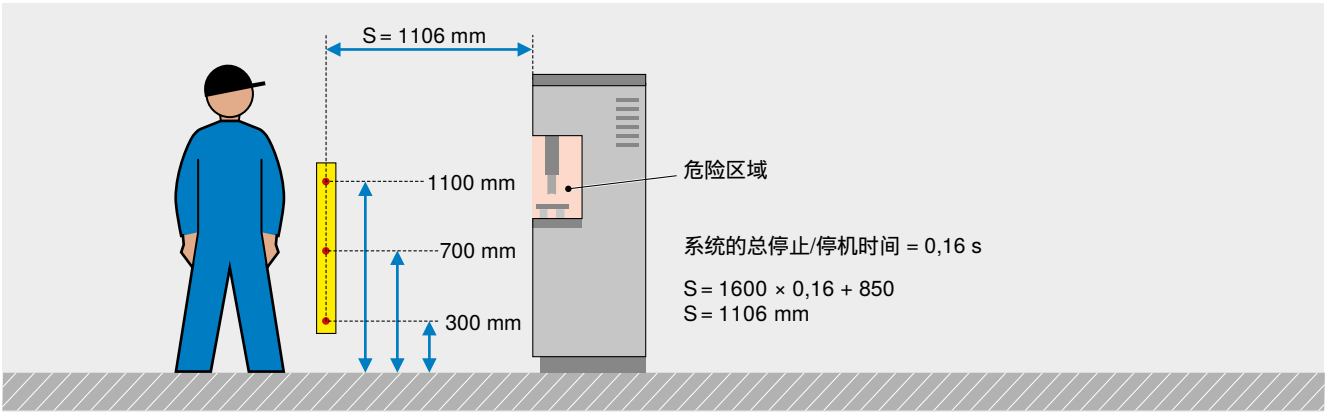


C =以毫米为单位的附加距离，表示
防护装置被触发前侵入危险区域的深度
d = 检测能力（AOPD 的分辨率）

H = 安装高度
S = 最小距离
x = 从保护区域末端到机器的距离

解决方法 3: 通道保护

借助三条光束（在 300 mm、700 mm 和 1100 mm 的高度下）的通道保护允许垂直靠近。该解决方案允许操作人员不被检测地位于危险区域与 AOPD 之间。因此必须采取附加安全措施以降低该风险。在这种情况下，指令装置（如复位按钮）的定位应确保能看到整个危险区域。其不得允许从危险区域内摸。



效果概览

下表列出解决方案的效果。操作需要决定了选择以下哪种解决方案:

解决方法当停止/停机时间 = 0.16 s 时		优点	缺点
1	**危险点保护** S = 320 mm	• 提高生产效率, 因为操作人员更靠近工作流程 (路程较短) • 可以自动启动或采取 PSDI 模式 • 所需空间极少	• 由于更好的分辨能力和核测人员是否存在, 防护装置的价格更高
2	**危险区域保护** S = 1256 mm	• 可以自动启动 • 允许不受危险区域高度影响地防护通道	• 操作人员明显离得更远 (路程较长) • 所需空间更多 • 降低生产效率
3	**通道保护** S = 1106 mm	• 较经济的解决方案 • 允许不受危险区域高度影响地防护通道 • 可借助偏转镜防护多个侧面	• 操作人员明显离得更远 (路程较长) • 生产效率较低 (始终需要复位 ESPE) • 要考虑到站在后面的风险。当多人在同一工位工作时, 不推荐使用。

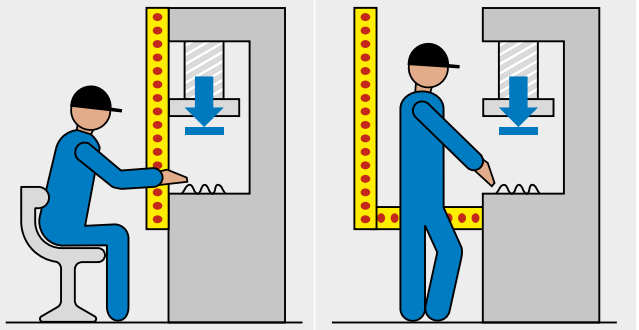
8020567/2017-08-22(GCN 2021-07-01)
如有更改, 恕不另行通知

ESPE 的所需保护区域大小/高度

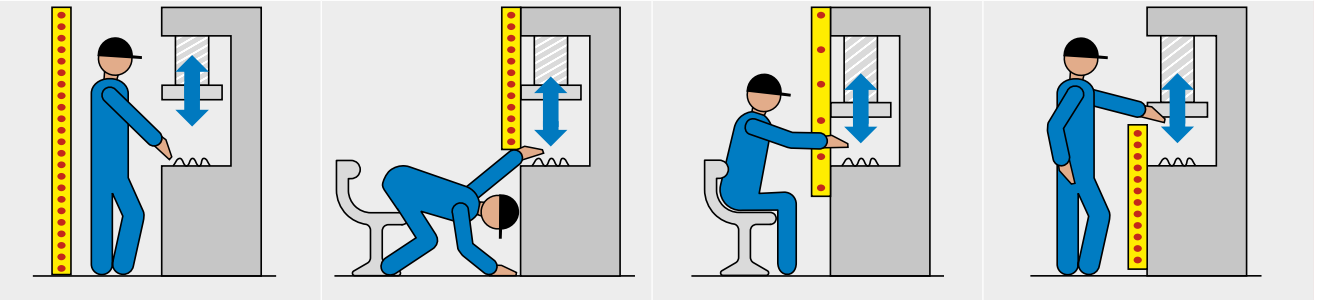
一般情况下，在安装防护设备时，必须排除以下错误：

- 只能允许穿过保护区域够到作业危险点。
- 尤其不得允许从上方、下方或周围伸手够到作业危险点。
- 若可以站在防护设备后面，则附加措施必须发挥作用（如重启联锁、次要防护设备）。

正确安装示例



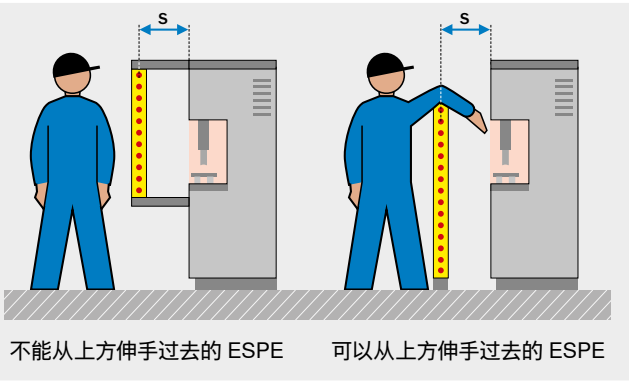
危险的安装错误示例



算出保护区域与最近作业危险点之间的最小距离后，下一步应确定所需保护区域高度。由此防止可从上方摸到作业危险点。

可从上方伸手过去的防护装置

根据 ESPE 的保护区域高度和位置、机器的形状和其他因素，ESPE 的保护区域可能被从上方伸手过去以致人员可在危险结束前摸到作业危险点，从而无法提供预期保护作用。插图所示为不能从上方伸手过去和可以从上方伸手过去的 ESPE 比较。



不能从上方伸手过去的 ESPE　　可以从上方伸手过去的 ESPE

若从垂直保护区域上方到达（触碰）时必须进入危险区域，则必须确定保护区域高度和电敏防护设备的最小距离。该工作可通过对比基于四肢或身体部位可行检测的计算值与通过触碰得出的值进行。使用由该对比得出的较大值。依照 ISO 13855 章节 6.5 进行该对比。

考虑从上方伸手过去的可能

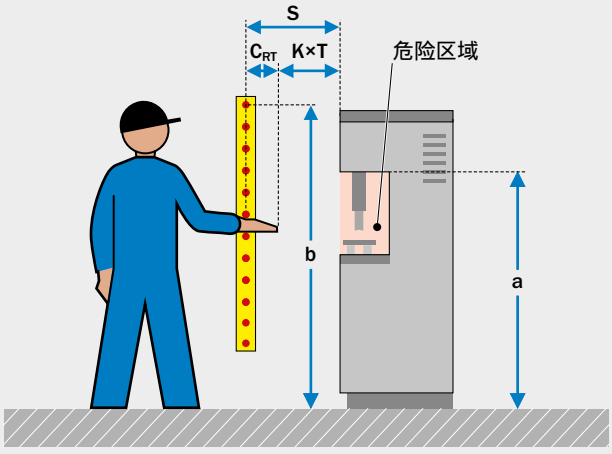
若 ESPE 的垂直保护区域可能被从上方伸手过去，则须增加保护区域上缘的高度 b 或调整延伸距离 C。这两种方法都要使用 ISO 13855 标准中的相应表格。

结论

在使用 d > 40 mm 的 ESPE（多光束系统）的一些应用中，最小距离可以增大或必须使用 d ≤ 40 mm 的 ESPE（光幕）。这在适用 ISO 13855 时适用。
有些 C 类标准在最小距离计算上不同于 ISO 13855。

提高保护区域上缘

如需提高保护区域上缘 b，则除了危险区域的高度 a，还要使用视分辨率而定的延伸距离 C_{RT} 以便在最小距离保持不变的情况下确定所需保护区域上缘高度。在该保护区域上缘高度下，不能从上方伸手过去够到危险区域，不需要附加距离 C_{RO}。

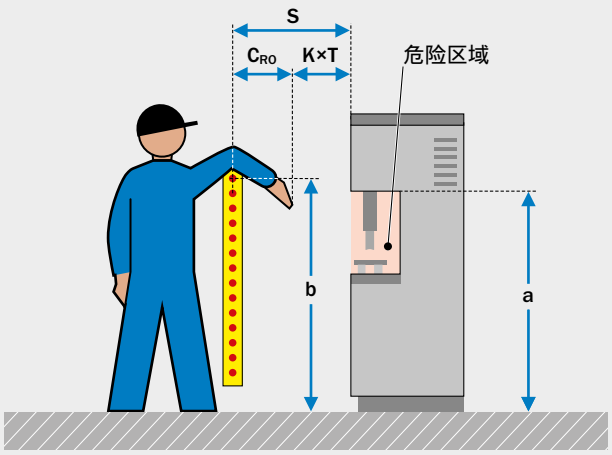


用于确定伸手穿过所需最小距离的参数

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

增大最小距离 (已规定保护区域上缘)

若保护区域上缘 b 已为例如现有产品所规定, 则须增大最小距离。通过确定危险区域高度 a 和保护区域上缘高度 b 实现。表格中产生的交叉点的结果表示侵入距离 C_{RO}。若 $C_{RO} \geq C_{RT}$, 则计算最小距离时用 C_{RO} 值代替 C_{RT} 值。若 $C_{RO} < C_{RT}$, 则计算最小距离时仍然用 C_{RT} 值。



用于确定从上方伸手过去所需最小距离的参数

一般情况下适用:

$$C \geq C_{RO}\text{ (从上方伸手过去)} \text{ 和 } C \geq C_{RT}\text{ (伸手穿过)}$$

在下面几页上可以看到 ISO 13855 中的所需表格和使用示例。

如下确定必需的保护区域上缘高度:

1. 确定作业危险点高度 a 并在左列中找到相等或最接近的较大值。
2. 根据适用于垂直靠近的已知公式计算视分辨率而定的延伸距离 C_{RT}:
   - ESPE, 分辨率 d ≤ 40 mm: $C_{RT} = 8 \times (d - 14)$
   - ESPE, 分辨率 d > 40 mm: $C_{RT} = 850$ mm
3. 在由第 2 步确定的列的底行中读取得到的保护区域上缘高度 b

在由 a 确定的行中找到附加水平距离 C 小于等于算出的视分辨率而定的延伸距离 C_{RT} 的最后一列。

危险区域高度 a (mm)	与危险区域的附加水平距离 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 ①	1200	1200	1100	1000	900	850 ②	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
	保护区域上缘高度 b (mm)											
	900	1000	1100	1200	1300	1400 ③	1600	1800	2000	2200	2400	2600

示例

- ESPE 的分辨能力: > 40 mm
- 危险区域的高度 a: 1400 mm ①
- 视分辨率而定的附加距离 C: 850 mm ②

ESPE 的保护区域上缘高度 b 不得低于 1400 mm ③, 否则应增大与危险区域的水平距离。

8020567/2017-08-22(GCN 2021-07-01)
如有更改, 恕不另行通知

若无法实现所需保护区域上缘高度，则须如下确定附加距离 CRO：

1. 确定可能（计划或现有 ESPE）的保护区域上缘高度 b 并在底行中找到相等或最接近的较小值。
2. 确定作业危险点高度 a 并在左列中找到值。如有中间值，应选择在第 3 步中得出较大距离的相邻行（上方或下方）。
3. 在两值的交叉点处读取所需水平距离 C。

危险区域高度 a (mm)	与危险区域的附加水平距离 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 ②	1200	1200	1100 ③	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
	保护区域上缘高度 b (mm)											
	900	1000	1100 ①	1200	1300	1400	1600	1800	2000	2200	2400	2600

示例

- 三光束标准 ESPE (300/700/1100 mm)
- 保护区域上缘高度 b: 1100 mm ①
- 危险区域高度 a: 1400 mm ②
- 受可能从上方伸手过去限制的附加距离 C_{RO}: 1100 mm ③ (代替以前通常的 850 mm)

3 C

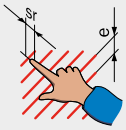
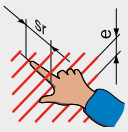
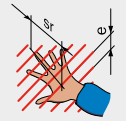
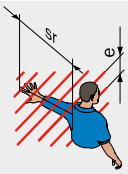
考虑到可能从上方伸手过去，ISO 13855 标准提供以下表格。
借助该表格进行提高保护区域上缘或增大最小距离的计算。

危险区域高度 a (mm)	与危险区域的附加水平距离 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
	保护区域上缘高度 b (mm)											
	900	1000	1100	1200	1300	1400	1600	1800	2000	2200	2400	2600

物理防护装置的安全距离

若物理防护装置具有开口，则须与危险区域保持足够距离。这同样适用于防护装置与机架、夹板等之间的开口。

根据 ISO 13857 与物理防护装置开口有关的安全距离

身体部位		开口 e (mm)	安全距离 (mm)		
			窄缝	正方形	圆形
指尖		e ≤ 4	≥ 2	≥ 2	≥ 2
		4 < e ≤ 6	≥ 10	≥ 5	≥ 5
手指到手腕		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		30 < e ≤ 40	≥ 850	≥ 200	≥ 120
		40 < e ≤ 120	≥ 850	≥ 850	≥ 850

3 C

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

联锁式物理防护装置的安全距离

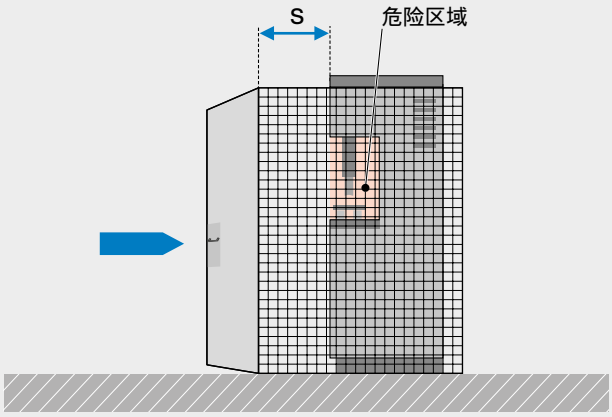
对于触发停止的联锁式物理防护装置，必须类似对 ESPE 的处理方法遵守安全距离。或者可通过带锁定装置的联锁装置防止进入，直至不再存在危险。

其中:

- S 是以毫米为单位的最小距离，从最近的作业危险点到最近的开门点。
- K 是以毫米每秒为单位的参数，从身体或身体部位的靠近速度得出，一般为 1600 mm/s。
- T 是以秒为单位整个系统的停止/停机时间。
- C 是取自 ISO 13857: 中相应表格（与物理防护装置开口有关的安全距离）的安全距离。如果在产生停止信号之前可能将手指或手部朝着危险区域穿过开口，则需要该安全距离。

一般计算公式

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

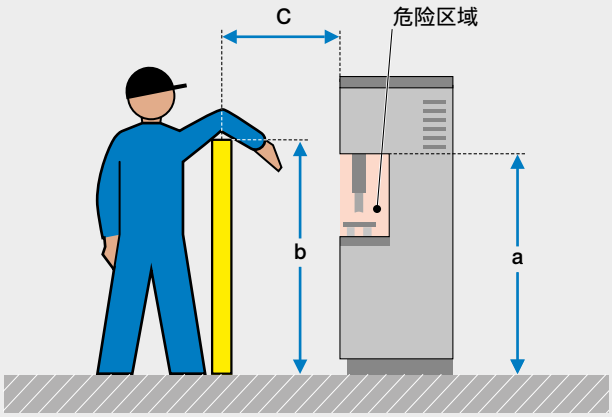


联锁式物理防护装置的安全距离

→ 联锁式物理防护装置的最小距离计算: ISO 13855 (B 类标准)

物理防护装置的必要高度

类似对 ESPE 的处理方法，对物理防护装置也可采用相同方法。应根据潜在危险使用不同计算表格。
正常情况下，从基准面上方 200 mm 开始防护足以避免钻过物理防护装置。



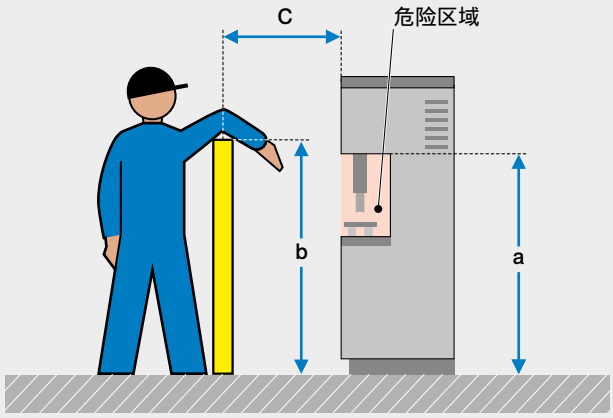
用于确定物理防护设备所需高度的参数

依照 ISO 13857 当潜在危险较低时的所需物理防护装置高度

危险区域 高度 a (mm)	与危险区域的水平距离 C (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
	物理防护装置高度 b (mm)								
	1000	1200	1400	1600	1800	2000	2200	2400	2500

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

依照 ISO 13857 当潜在危险较高时的所需物理防护设备高度



用于确定物理防护设备所需高度的参数

危险区域 高度 a (mm)	与危险区域的水平距离 C (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 ①	1500	1400	1000	800	0 ②	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
	物理防护装置高度 b (mm)									
	1000	1200	1400	1600	1800 ③	2000	2200	2400	2500	2700

按如下步骤确定该安全距离所必需的防护装置上缘高度:

1. 确定作业危险点高度 a 并在左列中找到值, 如 1000 mm。
2. 在该行中确定水平距离 C 小于算出的安全距离的第一列, 例如具有值“0”的第一栏。
3. 在底行中读取得到的物理防护装置高度 b, 如 1800 mm

高危险示例

物理防护装置必须从基准面上方 200 mm 开始到 1800 mm 结束。若物理防护装置的高度为 1600 mm, 则安全距离必须增大到至少 800 mm。

➜ 安全距离和所需保护区域高度: ISO 13857

固定位置防护设备的最小距离

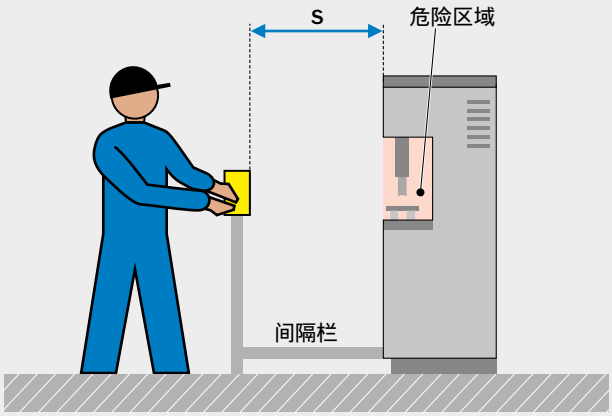
其中:

- S 是以毫米为单位的最小距离，从操作件到最近的作业危险点。
- K 是以毫米每秒为单位的参数，从身体或身体部位的靠近速度得出，一般为 1600 mm/s。
- T 是以秒为单位整个系统的停止/停机时间，从松开操作件（按钮）起计算。
- C 是附加距离: 250 mm。在某些条件下可以省去（如覆盖控制开关）。

若双手操纵装置安装在位置可变的支架上，则须通过间隔栏或有限电缆长度（以防超出范围的携带）确保遵守所需最小距离。

示例: 双手操纵装置最小距离

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



➜ 最小距离计算: ISO 13855 (B 类标准)

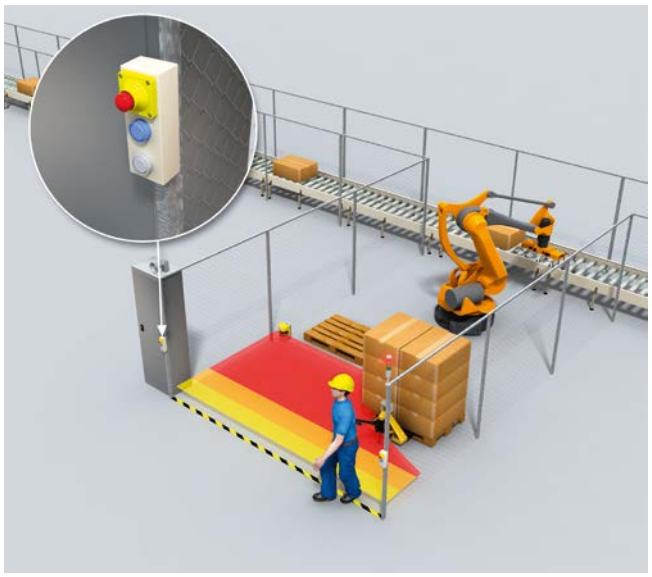
8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

运用复位和重启

若防护装置已发出停止指令，则停止状态必须保持到手动复位装置被致动并且随后可重启机器。该要求的一个例外是使用持续检测危险区域内是否人员存在（如提供后方进入防护）的防护装置。

必须通过单独的、可手动操作的装置提供手动复位功能。该装置的设计方式必须使其能承受可预见的负荷且只能通过有意致动实现预期效果（⚠ 触控面板可能不合适）。根据 ISO 13849-1（第 5.2.2 款），仅允许通过放指令元件从被致动的（开启）位置释进行复位。因此，要求信号处理检测到控制开关的信号下降沿。也就是说，仅允许通过指令元件从被致动的（开启）位置释放进行确认。只有当所有安全功能和防护设备均正常工作时，才允许执行复位。

用于复位的致动元件必须安装在危险区域之外的安全位置。必须能够从该位置完全看到危险区域。借此可靠检查是否有人在危险区域内停留。



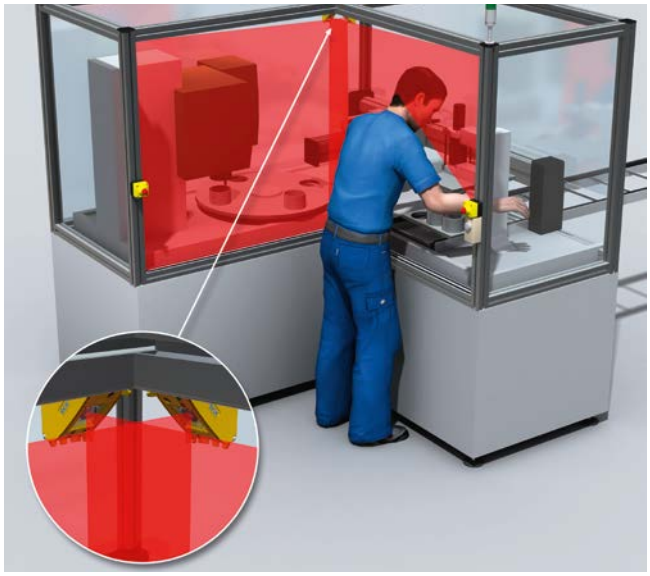
复位按钮的位置允许查看整个危险区域以复位防护装置。

复位装置的信号是安全功能的组成部分，因此必须

- 直接连到安全相关逻辑单元或
- 通过安全系统总线系统传输。

复位不得引起动作或危险状态。相反，机器控制系统只能在复位后接受单独的启动指令。

无复位的危险点保护



在这样的安排下，无法停留于危险区域但又不触发防护装置。因此，不需要单独复位防护装置。

防护装置集成到控制系统中

除了在机械上，也要在控制技术上集成防护装置。

“控制系统是机器信息系统的功能总成，可实现逻辑功能。其工作任务是在工具与工件系统的作用区域内协调物料流和能量流。[…] 根据应用的技术，亦即根据信息载体，控制系统分为流体、电气和电子控制系统。”

译自：Alfred Neudörfer: Konstruieren sicherheitsgerechter Produkte（符合安全产品的设计），Springer-Verlag, Berlin u. a., ISBN 978-3-642-33889-2（2013 年第 5 版）

作为一般概念，**控制系统**指的是整条控制链。控制系统由输入元件、逻辑单元、功率控制元件以及执行或工作元件组成。控制系统的安全相关部件应执行安全功能。因此，对其可靠性和抗故障能力提出了特殊要求。其基于控制故障和避免故障的原理。

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

控制系统			安全技术方面	
控制系统的工作原理		**典型部件**	**干扰因素**	**注释**
流体	气动 	• 多路阀 • 排气阀 • 手动截止阀 • 脱水过滤器 • 软管	• 能量变化 • 压缩空气的纯度与含水量	大多被设计为电动气动控制系统。 需要维护单元来调整压缩空气。
	液压 	• 蓄压器 • 限压器 • 多路阀 • 过滤器 • 液面计 • 温度计 • 软管和管路 • 螺纹接头	• 纯度 • 粘度 • 液压液温度	大多被设计为电动液压控制系统。 需要限制系统内压力和温度和过滤介质的措施。

电气	机电 	• 控制开关:
		  • 位置开关
		  • 选择开关
		  • 按钮
		• 开关放大器:
		  • 接触器
		  • 继电器
		  • 断路器
			• 设备的防护等级
			• 部件与设备的选择、尺寸确定和布置
			• 电缆的设计和敷设
				由于其结构型式和明确的开关位置，若恰当选择，则零件不受潮湿、温度波动和电磁干扰影响。

	电子 	• 单独部件，如:
		  • 晶体管
		  • 电阻器
		  • 电容器
		  • 线圈
		• 高度集成部件，如集成电路 (IC)
			同“机电”下所列。
			另外:
			• 温度波动
			• 通过电缆或场耦合的电磁干扰
				无法将故障排除在外。
				只能通过控制系统理念，而非通过部件选择实现可靠的效果。

	微处理器控制 	• 微处理器
		• 软件
			• 硬件安装错误
			• 包括共模故障在内的系统故障
			• 编程错误
			• 处理错误
			• 操作错误
			• 干忧
			• 病毒程序
				• 避免错误的措施:
				  • 结构化设计
				  • 程序分析
				  • 模拟
				• 控制错误的措施:
				  • 冗余硬件和软件
				  • RAM /ROM 测试
				  • CPU 测试

译自: Alfred Neudörfer: Konstruieren sicherheitsgerechter Produkte (符合安全产品的设计) , Springer-Verlag, Berlin u. a., ISBN 978-3-642-33889-2 (2013 年第 5 版)

与安全相关的输入元件已通过安全传感器（防护装置）说明。因此下面仅介绍逻辑单元和执行器。
可参考功率控制元件从安全技术上考虑执行器。通常可排除执行器或工作元件的故障和失效。（在没有供电的情况下，电机切换到无危险状态。）

流体控制系统通常被设计为电动气动或电动液压控制系统。也就是说，电信号通过阀门转化为流体能量，借此使气缸和其他执行元件动作。

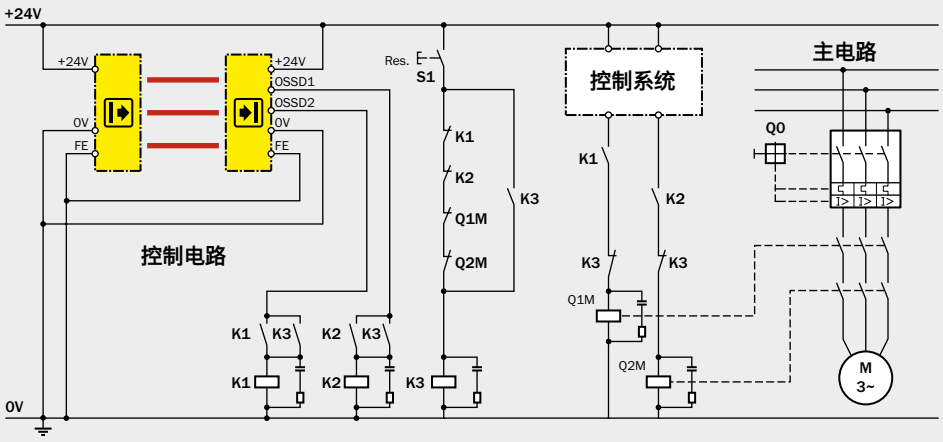
➜ 防护装置的集成线路示例参见www.sick.com

逻辑单元

在逻辑单元内，来自安全功能的不同输入信号相互结合形成输出信号。为此可使用机电、电子或可编程电子组件。

注意：根据所需可靠性，不允许仅由标准控制系统处理防护装置的信号。可能需要另外提供并行关断路径。

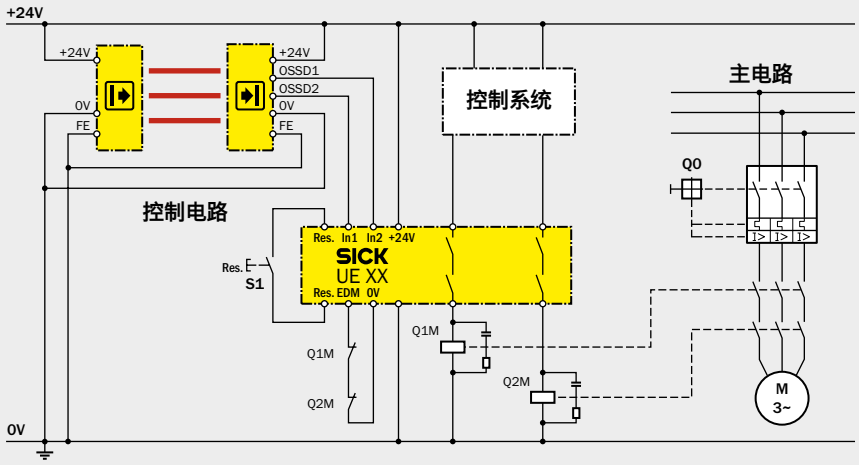
由接触器构成的逻辑单元



带强制导向触点的单个辅助接触器可构成几乎任意复杂程度的控制系统。该安全原理的特征在于冗余和通过强制导向触点监控。通过布线实现逻辑连接。

工作方式：当接触器 K1 和 K2 处于静态位置时，通过 S1 的致动使接触器 K3 接通并自保持。若在主动保护区域内未检测到物体，则输出端 OSSD1 和 OSSD2 带电。接触器 K1 和 K2 通过 K3 的常开触点接通并自保持。K3 在松开按钮 S1 时断开。然后输出回路才闭合。若在主动保护区域内检测到物体，则接触器 K1 和 K2 被输出端 OSSD1 和 OSSD2 关断。

作为安全继电器的逻辑单元（安全接口）



安全继电器在一个外壳中合并了一项或多项安全功能。通常具有自监控功能。关断路径可基于触点或使用半导体。还可以包括信号触点。

较复杂安全应用的结构得到简化。经过认证的安全继电器还减少了确证安全功能的工作量。半导体元件可代替继电器承担机电开关元件的任务。通过故障检测措施（如动态信号评价）或故障控制措施（如多通道信号处理），纯电子控制系统可实现所需可靠度。

3
C

带有基于软件的组件的逻辑单元

与自动化技术类似，安全技术从硬布线辅助接触器经安全继电器（部分带可设定参数和可配置安全逻辑）进一步发展到复杂的故障安全 PLC。“被证明有效的部件”和“被证明有效的安全原理”的理念必须转换到电气系统和可编程电子系统。

在此通过软件实现安全功能的逻辑连接。软件不同于固件——由控制系统的制造商开发和认证——和实际安全应用。其由机械制造商用固件提供的语言范围开发。

参数设置

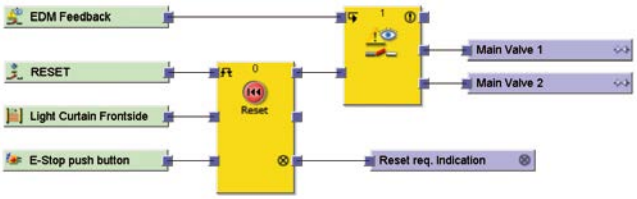
调试时，通过选择开关或软件参数从指定功能池选择特性。

特点：逻辑深度低，与/或逻辑

配置

以编程界面在经认证逻辑中指定功能块的灵活连接，例如控制系统输入和输出配置与时间的参数设置。

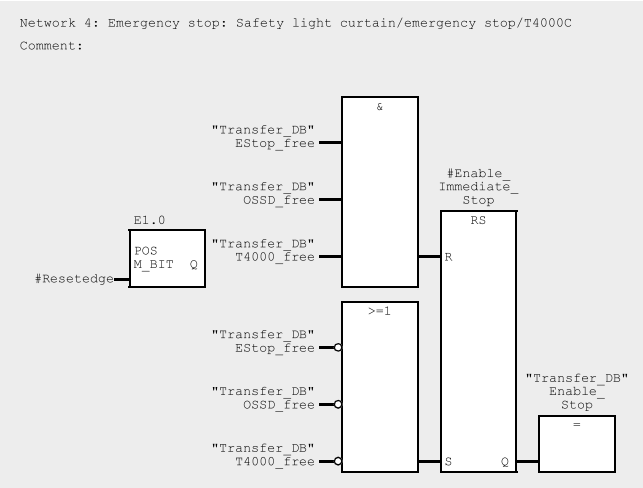
特点：任意逻辑深度，二进制逻辑



编程

以指定编程语言之一根据功能范围自由设计逻辑，大多使用经认证的功能块。

特点：任意逻辑深度，字处理

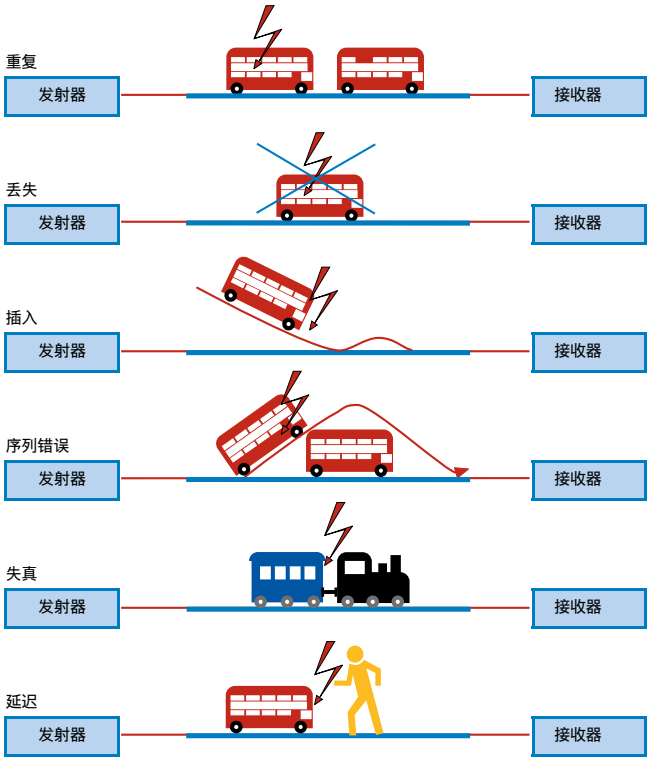


3 C

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

可靠的数据传输

总线系统一方面用于在控制系统与机器上的传感器或执行元件之间传送信号。另一方面，总线系统还负责在控制系统的不同部件之间传输状态。总线系统通过简化布线减少了可能的故障。在安全相关应用中，适宜使用成熟的总线系统。



来源：印刷和纸品加工机械的安全设计 – 电气装备与控制系统；BG 印刷和纸品加工；2004/06 版；第 79 页

上一级控制系统中的大量措施可抵抗上述传输故障，例如安全相关报文的连续编号或即将到来的带确认报文的时间预期。基于所用现场总线的协议扩展包括此类措施。

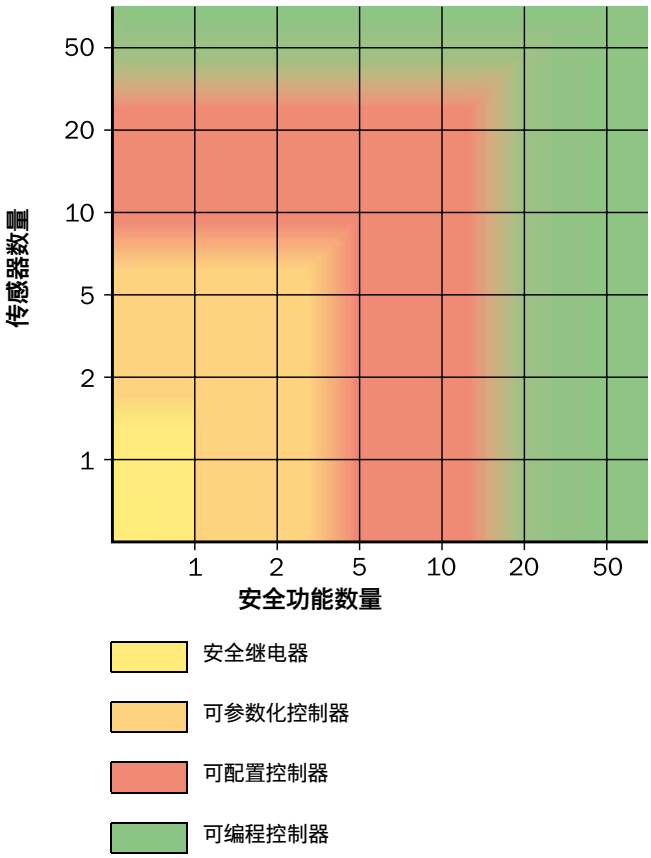
对不同软硬件故障的详细研究表明，此类故障始终表现在少量相同的总线系统传输故障。

根据 ISO/OSI 分层模型，其在传输层以上发挥作用并利用现场总线及其所有组件作为“黑色通道”(Black channel)。成熟的安全总线系统包括例如：

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

选择标准

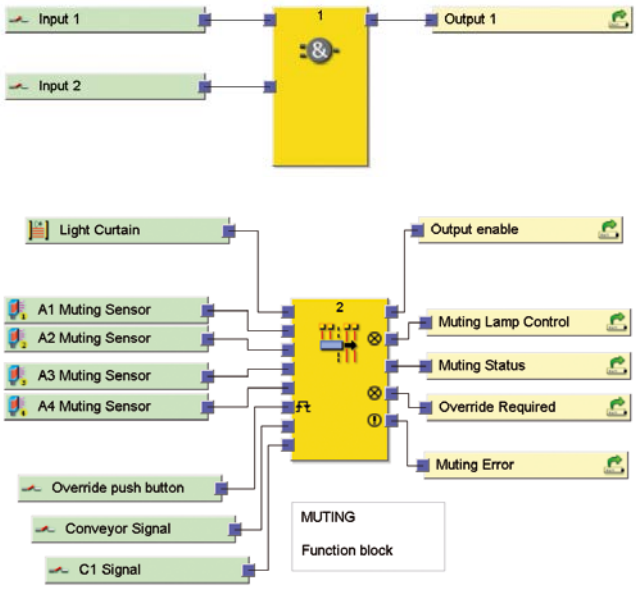
控制系统模型的选择标准首先是待实现安全功能的数量以及输入信号之间逻辑连接的范围。
所需连接逻辑的功能——如简单与、flipflop 或特别功能（如屏蔽）——也会影响选择。



设计矩阵

0 = 逻辑 0 或断开
S = 启用执行元件（重启）
I = 逻辑 1 或接通
– = 任何状态

安全输入 \ 事件	作用	安全输出				
		机器人	左侧工作台	右侧工作台	...	...
失去位置		0	–	–		
左侧机器人		S	–	–		
右侧机器人		S	–	–		
中间机器人		S	–	–		
左侧通道		S	I	–		
右侧通道		–	–	I		
紧急停止		0	0	0		
...						



软件规范

为了避免出现危险状态，尤其要设计能可靠避免逻辑错误的基于软件的逻辑单元。为了检测系统错误，应当由除开发者以外的其他人进行系统检查，即运用四眼原则。
所谓的**设计矩阵** (design matrix) 是实现该规范的一种简便方法。在此合并了针对特殊情况（如“失去位置”或“左侧机器人”）安全相关输入信号的某些组合。这些情况应根据安全功能要求通过安全相关输出作用于机器功能。SICK 也将该简便方法用于应用软件的项目化。
适宜与所有项目参与者一起复审。
若程序的文件编制较差且结构散乱，则在稍后修改时将产生错误，尤其存在未知依赖性（所谓的副作用）的危险。对于外部开发软件，良好的规范和程序文档尤其具有特别强的避免错误的作用。

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

功率控制元件

由防护设备和逻辑单元触发的安全功能必须使危险动作停止。
为此执行或工作元件通常被功率控制元件关闭。

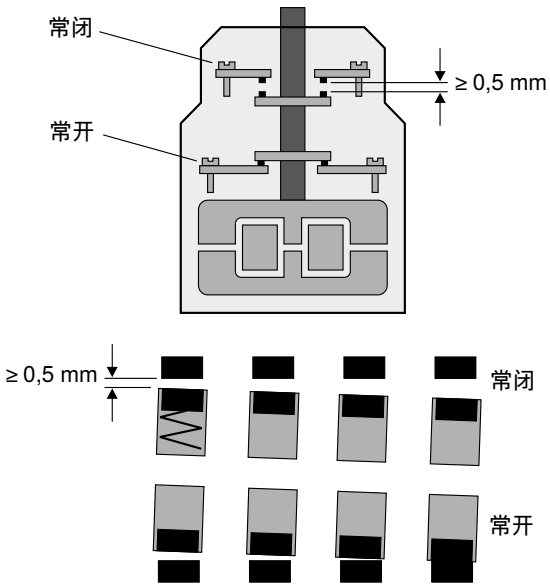
➜ 关闭或断电原理: ISO 13849-2 (B 类标准)

接触器

电磁接触器是最常使用的功率控制元件类型。通过特定选择标准、布线和措施，一个或多个接触器可构成安全功能的子系统。通过防止触点过电流和短路、留出裕量 (通常为 2 倍) 和其他措施，接触器被视为经证明有效的部件。为了能够诊断安全功能的接触器，需要明确的开关状态反馈 (EDM)。这可通过带强制导向触点的接触器实现。若一组触点中的触点以机械方式相互连接，使得在整个使用寿命期间常开触点与常闭触点绝不可能同时闭合，则为强制导向。

“强制导向触点”的概念首先指的是辅助接触器和辅助触点。即使在故障状态下 (常开触点磨损)，也要确保常闭触点上至少 0.5 mm 的限定触点间距。因为用于小开关功率 (< 4 kW) 的断路器在主开关元件与辅助开关元件之间没有本质区别，所以小型断路器同样可被称为“强制导向触点”。

大型断路器采用所谓的“对称触点”：在接触器的任一主触点闭合期间，对称触点 (辅助常闭触点) 不得闭合。对称触点的典型应用是高可靠性地监控机器控制电路中接触器的开关状态。



来源：Moeller AG

带强制导向触点接触器的接触系统。
常开触点已磨损。

3 C

压弧器

电感（如接触器或阀门的线圈）必须配有压弧器来限制关断时的瞬时过电压。借此保护开关元件，尤其是对过电压特别敏感的半导体，免受过载损坏。此类线路通常会影响延迟释放，进而影响所需的防护设备最小距离(➜ 3-42)。用于压弧的简单二极管可导致断开时间最多延长 14 倍。

压弧器（通过电感）	二极管	二极管组合	变阻器	RC 元件
				
防止过电压	非常高	高	有限	高 [1]
释放延时	非常长（安全相关）	短（但必须纳入考量）	非常短（非安全相关）	非常短 [1]（非安全相关）

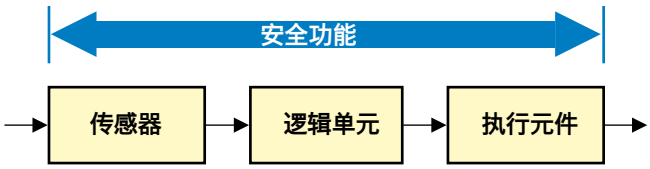
1) 元件必须与电感精确匹配!

3 C

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

驱动技术

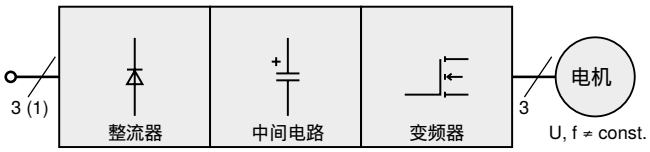
在考虑安全功能时，驱动器是一项中央子功能，因为意外动作的危险主要来自它们。
安全功能从传感器延伸到执行元件（见插图）。



执行元件可包括多个组件（接触器、驱动器、反馈），视技术设计和安全功能而定。对于承受重力的轴，同样要考虑到制动系统和保持系统。
实际驱动器（电机）不是考虑的对象。

伺服放大器和变频器

在驱动技术中，带变频器的三相电机在很大程度上取代了直流驱动器。变频器从固定不变的三相电源生成频率和幅度可变的输出电压。根据设计，稳压整流器可在制动期间将中间电路吸收的能量反馈至电源。
整流器对电源供应的电能进行转换，再将其供应给直流中间电路。变频器通过使用半导体开关的脉宽调制在电机内构成合适的旋转场以执行所需控制功能。开关频率通常在 4 kHz 与 12 kHz 之间。



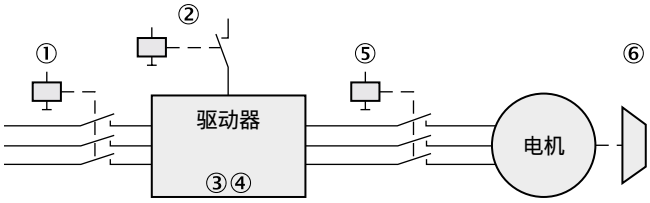
为了通过开关直流与交流电路中的负载来限制瞬时过电压，可使用抗干扰元器件，特别是在相同控制柜内有敏感的电子组件使用时。

检查表

- 变频器上是否安装电源输入滤波器？
- 变频器的输出电路是否配有正弦滤波器？
- 连接电缆是否尽可能短并带屏蔽？
- 组件和屏蔽层是否大面积接地或连接到 PE？
- 是否串联了换向扼流圈以限制峰值电流？

伺服放大器和变频器的安全功能

为了落实安全功能，在执行元件子系统中允许不同关断路径：



① 电源接触器——因重新通电时间较长而不利，因启动电流而磨损较大
② 控制器启用——非安全相关
③ 脉冲禁止“安全重启联锁（停止）”
④ 设定值——非安全相关
⑤ 电机接触器——并非所有变频器都允许
⑥ 保持制动器——通常不是工作制动器

可使用驱动器以不同方式实现安全功能：

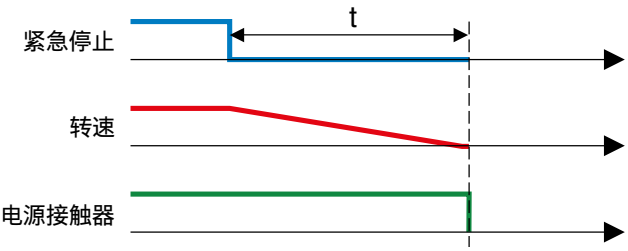
- 通过**断开供电**，例如通过电源接触器 ① 或电机接触器 ⑤。
- 通过用于监控的**外部电路**，例如通过编码器的监控
- 通过**直接集成在驱动器中元件安全功能** (➜ 3-76)

断开供电

使用变频器时，应在风险评价中考虑到中间电路电容器内储存的能量或通过再生制动流程产生的能量。

考虑剩余行程时，应假定运动控制系统不会引起制动斜坡。

断电后，驱动器根据摩擦力或大或小逐渐快速停止（停止类别 0）。通过影响设定值和/或启用控制器并随后关断接触器或脉冲禁止来控制制动斜坡（停止类别 1）可缩短制动距离。



外部监控单元的转速检测

外部监控单元需要报告当前运动参数的信号来监控驱动器。在这种情况下，信号源自传感器和编码器。其必须根据所需 PL 或 SIL 作为安全传感器或采用冗余设计。

或者也可通过读回由正在逐渐停止的电机感生的电压实现停机监控。该功能对于调速驱动器也可正常工作。

集成在驱动器中的元件安全功能

安全功能由控制系统的安全相关部件执行 (SRP/CS)。其中包括检测（传感器）、处理（逻辑单元）和开关或作用（执行元件）等子功能。在这种情况下，集成在驱动器内的安全相关功能应被视为元件安全功能。

一般分为两组:

- 安全停止与制动功能: 其用于使驱动器安全停止（如安全停止），
- 安全动作功能: 其用于在运行期间安全监控驱动器（如安全限速）。

所需驱动监控功能一般视应用而定。第二条件主要包括是否存在动能、所需制动距离等参数。

关断反应随所选元件安全功能而不同。例如安全转矩关闭功能（STO）在有停止请求时使动作，受控制地逐渐停止。安全停止（SS1 或 SS2）实现受控减速。元件功能也可搭配使用作为合适的措施。

用于控制直接集成在驱动器中的安全子功能的可能接口包括:

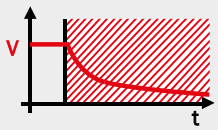
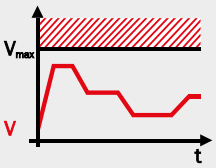
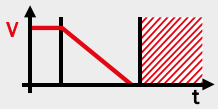
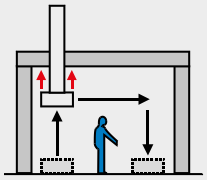
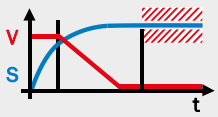
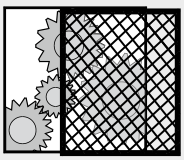
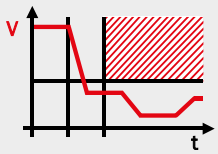
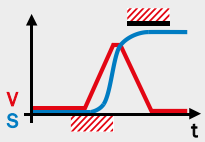
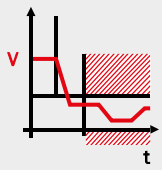
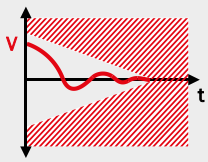
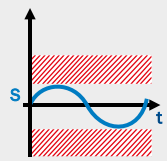
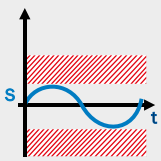
- 离散的 24 V 信号
- 管理通信（通道 1）/24 V 离散（通道 2）
- 安全通信系统（现场总线系统/网络接口）

管理通信是指标准控制系统通过非安全相关现场总线或网络向驱动器发送转速或位置的设定值。

如今可用于变速驱动器的大多数元件安全功能在协调标准 IEC 61800-5-2“可调转速电力传动系统”第 5-2 部分“安全要求 - 功能安全”中有详细说明。满足该标准的驱动器可用作符合 ISO 13849-1 或 IEC 62061 的控制系统的安全相关部件。

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

符合 EN 61800-5-2 的驱动安全功能

	安全转矩关闭功能 (STO) • 符合 IEC 60204-1 中的停止类别 0 • 通过立即中断向执行元件供电实现非受控停止 • 安全重启联锁: 防止电机意外启动		安全最大速度 (SMS) [1] • 安全监控最大速度, 不受操作模式影响
	安全停止 1 (SS1) [2] • 符合 IEC 60204-1 中的停止类别 1 • 在保持向执行元件供电的情况下实现受控停止 • 停止后或低于限速时: 激活 STO 功能 • 可选: 监控制动斜坡		安全制动与保持系统 (SBS) [1] • 安全制动与保持系统控制和监测两个独立制动器。
	安全停止 2/安全操作停止(SS2, SOS) [2] • 符合 IEC 60204-1 中的停止类别 2 • 在保持向执行元件供电的情况下实现受控停止 • 停止后: 安全监控驱动轴在定义区域内的位置		安全防护门锁定 (SDL) [1] • 只有当受保护区域内的所有驱动器均处于安全状态时, 才解锁防护门锁定装置。
	安全限速 (SLS) • 发出使能信号后, 在特殊模式下监控安全减速。 • 若超过限速, 将触发安全停止功能。		安全限制的增量 (SLI) • 发出使能信号后, 在特殊模式下监控安全限制的增量。 • 之后驱动器被安全停止并保持在该位置。
	安全方向 (SDI) • 除了安全动作, 还监控安全方向 (顺时针/逆时针) 。		安全监控的减速度 (SMD) [1] • 安全监控以可预见行为停止时的减速度
	安全限位 (SLP) [1] • 除了安全动作, 还监控安全的绝对位置范围。 • 若违反限值, 则通过停止功能使驱动器停止 (注意惯性运行) 。		安全监控的位置 (SMP) • 监控安全软件开关

来源: Bosch Rexroth AG

1) 未在 IEC 61800-5-2 中定义。
2) 非安全制动: 如果未定义制动斜坡, 延时期间将检测不到电机加速度。

➜ 电力传动装置的功能安全 IEC 61800-5-2 (B 类标准)

流体控制系统

阀门

所有阀门均包含可移动开关元件（活塞滑套、柱塞、阀座等），并由于其功能而遭受机械磨损。

导致阀门发生安全相关失效的较常见原因有:

- 阀门的功能元件（复位功能、开关功能、密封功能）失效
- 流体污染

污染属于非预期使用，一般会导致故障。对所有阀门而言，污染普遍会导致提前磨损。因此，根据限定失效概率而进行设计的依据不复存在。

在单稳态阀门上用于复位功能的机械弹簧一般采用高持久力设计，并可被视为符合 ISO 13849-2。但无法排除弹簧断裂失效。

阀门之间的重要区别特征在于阀门内可移动开关元件的设计。阀门的相应失效模式基本上由其设计结构决定。座阀可能泄漏，而活塞滑阀的滑套可能阻塞。

座阀的开关功能由可移动开关元件（阀盘）构成，其相对于外壳内的阀座改变其位置。该设计实现以短行程开启大截面。可通过相应设计避免泄漏风险。

活塞阀的阀体通过越过钻孔或圆周槽来关闭或打开流通路径。活塞滑套的截面变化与外壳内截面变化的相对关系可影响体积流量，被称为控制边缘。该阀门设计值得注意的基本特点是所谓的重叠（英语: lap）。其表示滑阀的固定与移动控制边缘之间的纵向距离。硬密封阀门需要活塞与外壳钻孔之间的缝隙，当存在压差时将导致泄漏。

安全技术设计原则

在阀门的安全相关使用中，可能需要反馈阀门位置。

为此采用不同方法:

- 由嵌入可移动阀体的磁铁致动的簧片开关
- 由阀门的可移动开关元件直接致动的感应式接近开关
- 阀门的可移动开关元件的模拟行程检测
- 阀门之后的压力测量

电磁致动阀与接触器类似，需要电磁线圈的压弧器。ISO 13849 从安全技术上定义，阀门可参考作为功率控制元件。还要根据可能的影响考虑驱动器或工作元件的失效。

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

过滤理念

流体控制系统的绝大多数失效可归因于与相应流体脏污有关的故障。两个主要原因:

- 安装期间发生的污染=安装污物 (如切屑、型砂、抹布纤维、基本污染)
- 运行时发生的污染 = 运行污物 (如环境污物、组件磨损)

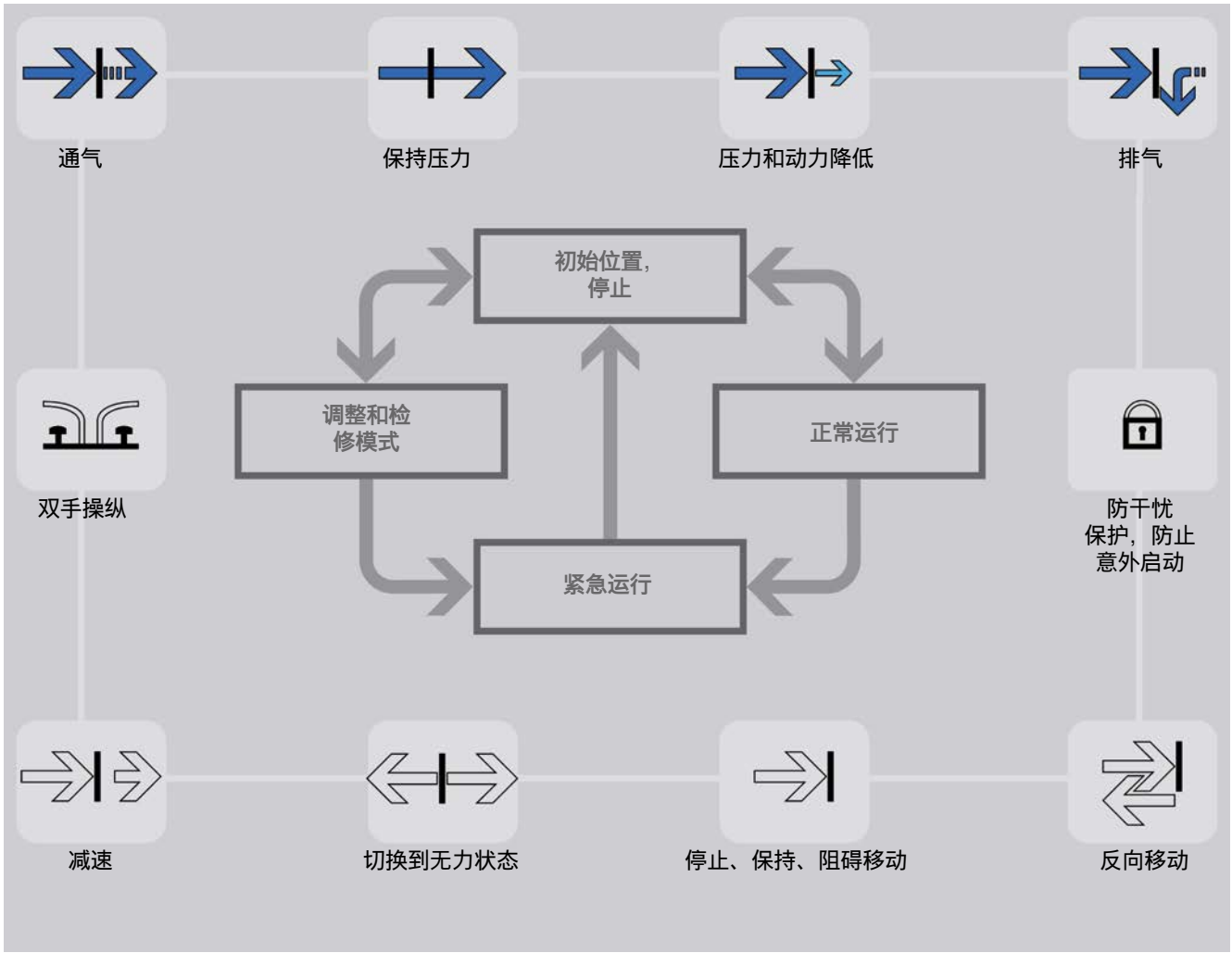
必须借助过滤器将这些污染降至可接受的程度。

过滤理念是指适当选择用于所需任务的过滤原则以及在恰当地点布置过滤器。过滤理念的设计必须能够在过滤器内拦住整个系统新增加的污物, 由此在持续运行时间内保持所需纯净度。

➜ 被证明有效的安全原则: EN ISO 13849-2 (B 类标准)
➜ 对液压/气动设备的安全技术要求: ISO 4413, ISO 4414
➜ 液压阀的老化过程: BIA-Report 6/2004

与安全相关的气动装置

电动气动控制系统实现安全功能的方法是由逻辑单元提供的电信号通过多个阀门相结合作为功率控制元件来影响驱动或工作元件。典型的安全相关功能可作为元件安全功能分配给机器的操作模式。除了电动气动控制系统，还存在纯气动控制系统。这些解决方案的优势是由于气动装置的决定性特性以相对简单的方式纯气动执行元件安全功能。

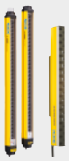
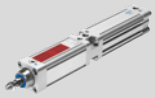
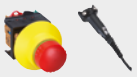
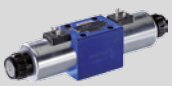


➔ 直接气动作用于移动
➔ 间接气动作用于移动

来源：Festo AG & Co. KG – 安全技术指南

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

用于机械安全的安全技术产品概览

传感器	逻辑单元	功率控制元件
安全光幕 	 安全继电器	 带元件安全功能的电气驱动器 [1]
安全摄像系统 		
多光束安全光栅 		 安全气动阀 [2]
单光束安全光栅 		
安全激光扫描器 	 安全控制器和运动控制	
联锁装置		 接触器 [3]
带独立执行元件 		
带锁定装置的执行元件 		 变频器 [4]
用于转换凸轮、转换杆 		 制动器 [2]
磁性编码 		
无线射频识别编码 	 安全传感器级联	 气动阀 [1]
感应式 		
紧急停止按钮使能开关 		 液压阀 [1]
电机反馈系统，编码器 		
光电传感器，磁性传感器和感应式传感器 		

SICK 的服务解决方案

承蒙许可: 1) Bosch Rexroth AG, 2) FESTO AG & Co. KG, 3) Eaton Industries GmbH, 4) SEW-EURODRIVE GmbH & Co. KG。

➜ SICK 的产品参见在线产品查找，登陆 www.sick.com

总结: 设计安全功能

基本原则

- 制定安全理念。在此期间考虑机器特点、环境特点、人员特点、设计特点和防护设备的特点。
- 设计具有所需安全等级的安全功能。安全功能由传感器、逻辑单元和执行元件等子系统构成。
- 根据结构、可靠性、诊断、耐受性和工艺条件等安全技术参数确定每个子系统的安全等级。

防护装置的特性和应用

- 确定防护装置的所需特性。需要例如一个或多个电敏防护设备 (ESPE)、物理防护装置、可移动物理防护装置还是固定位置防护装置？
- 确定每个防护装置的正确定位和尺寸，特别是相应防护装置的安全距离或最小距离和所需保护区域大小或高度。
- 按照操作指南中的说明和安全等级的要求集成防护装置。

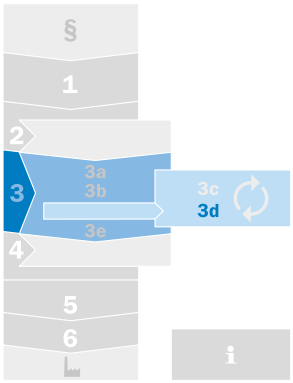
逻辑单元

- 根据安全功能的数量和逻辑深度选择恰当的逻辑单元。
- 利用经认证功能块并保持设计一目了然。
- 使设计和文件得到彻底检查 (四眼原则) 。

第 3d 步: 验证安全功能

在验证过程中, 通过分析和/或检查证明安全功能在任何方面都符合规范的目的和要求。

验证主要由两部分组成:
- 机械设计验证
- 功能安全验证



防护装置的机械设计验证

应检查机械防护装置的设计是否满足分离或间隔作业危险点的要求或约束飞出零件或辐射的要求。尤其要注意符合人类工效学要求。

分离和/或间隔作用
- 足够的安全距离和尺寸 (从上方伸手过去、从下方伸手过去等)
- 围栏元件适当的网目尺寸或格栅间距
- 足够的强度和适当固定
- 合适的材料选择
- 安全设计
- 抗老化
- 防护装置的设计使得无法攀爬防护装置

约束飞出的零件和/或辐射
- 足够的强度、抗冲击和抗断裂性 (约束能力)
- 足够的约束能力用于涉及的辐射种类, 尤其当存在热危险 (高温、低温) 时
- 围栏元件适当的网目尺寸或格栅间距
- 足够的强度和适当固定
- 合适的材料选择
- 安全设计
- 抗老化

人类工效学要求
- 可看穿或透明 (以便观察机器运行)
- 造型、颜色、审美
- 操纵 (重量、致动等)

3 d

在本章中...

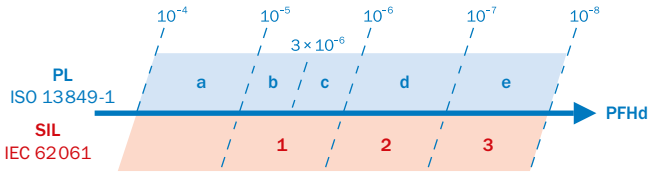
可借助检查表检查防护设备的有效性:

示例: 用于安装防护设备 (如 ESPE) 的制造商或装备商检查表			
1.	是否已充分防止或只能通过防护区域 (ESPE、带联锁装置的防护门) 进入或接近危险区域或作业危险点?	是 ☐	否 ☐
2.	在危险区域或危险点保护中, 是否已采取相应措施防止不受保护人员逗留在危险区域 (机械式后方进入防护) 或监视受保护人员逗留在危险区域 (防护设备), 并确保其不被移除或进行联锁?	是 ☐	否 ☐
3.	防护设备是否符合安全功能要求的可靠性等级 (PL 或 SIL)?	是 ☐	否 ☐
4.	是否已复测机器的最长停止时间或停止/停机时间并 (在机器上和/或机器资料中) 注明和记录?	是 ☐	否 ☐
5.	是否遵守防护设备与最近作业危险点的所需安全距离或最小距离?	是 ☐	否 ☐
6.	是否有效防止从下方、上方或周围将手伸入防护设备或从下方钻过或从上方爬过防护设备?	是 ☐	否 ☐
7.	设备或开关是否正确固定并在完成调整后防止干忧?	是 ☐	否 ☐
8.	所需电击防护措施是否有效 (防护等级)?	是 ☐	否 ☐
9.	用于复位防护设备或重启机器的控制开关是否存在并正确安装?	是 ☐	否 ☐
10.	集成的防护设备所用组件是否符合制造商说明?	是 ☐	否 ☐
11.	指定保护功能是否在操作模式选择开关处于任何设置下都有效?	是 ☐	否 ☐
12.	防护装置是否在整个危险状态期间有效?	是 ☐	否 ☐
13.	在关闭或断开防护设备以及切换运行模式或切换到另一个防护设备时, 已经开始的危险状态是否被停止?	是 ☐	否 ☐
14.	防护设备附带的提示是否处于对操作人员清晰可见的位置?	是 ☐	否 ☐

验证功能安全

根据功能安全标准，实际安全等级应至少符合目标安全等级。在此有两种不同方法可用:

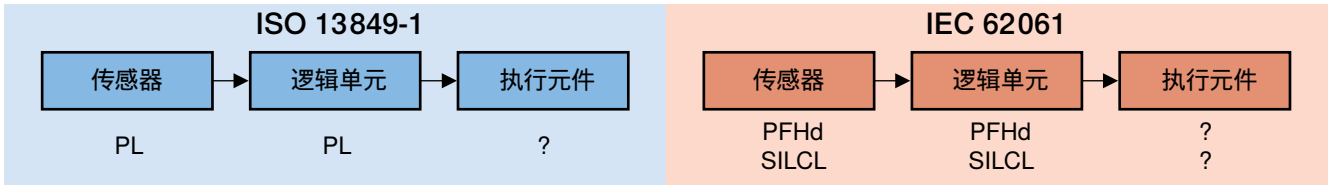
- 依照 EN ISO 13849-1 确定达到的性能等级 (PL)
- 依照 IEC 62061 确定达到的安全完整性等级 (SIL)



可通过这两种方法检查能否达到所需安全等级。为此将 PFHd 值确定为量化参数。

在以下两个示例 (➜ 3-93 和 ➜ 3-98) 中有传感器和逻辑单元的数据，但没有激励元件的数据。

- 性能等级 (PL): 安全相关部件在可预见的条件下执行安全功能以实现预期风险降低的能力
- PFHd: 每小时危险失效概率
- SILCL: SIL 要求限度 (适合性) 。用于确定安全功能完整性的离散等级。



依照 ISO 13849-1 确定达到的性能等级 (PL)

ISO 13849-1 规定了两种确定性能等级的方法:

- **简化方法** (➜ 3-87):
  根据每个子系统的性能等级以表格形式确定性能等级
- **详细方法** (➜ 3-88):
  根据子系统的 PFHd 值计算性能等级。(该方法在标准中仅间接说明。)

与简化方法相比, 使用详细方法可算出更切合实际的性能等级。使用两种方法时, 还要将与达到性能等级有关的结构和系统方面纳入考量。

子系统

借助控制技术措施实现的安全功能通常由传感器、逻辑单元和执行元件组成。此类链条一方面可包括防护门联锁装置或阀门等分立元件, 另一方面也可包括复杂的安全控制器。因此, 通常需要将安全功能分成子系统。

在实践中, 某些安全功能已经频繁使用经认证的子系统。这些子系统可以是例如光幕或安全控制器, 由组件制造商提供其已经"预先算好"的 PL 或 PFHd 值。

➜ 关于确证的更多说明: ISO 13849-2
➜ 关于依照 ISO 13849-1 验证的综合信息参见: www.dguv.de/bgia/13849

8020567/2017-08-22(GCN 2021-07-01)
如有更改, 恕不另行通知

简化方法

即使不知道单个 PFHd 值，也可在许多应用中通过该方法对总 PL 进行足够准确的估计。若已知所有子系统的 PL，可借助下表确定安全功能所达到的总 PL。

该方法基于不同 PL 的 PFHd 值域内的平均值。因此，使用详细方法（见下一节）可获得更准确的结果。

步骤

- 确定一个或多个子系统的 PL 以及安全功能中的最低 PL: **PL (low)**
- 确定具有该 PL (low) 的子系统数量: **n (low)**

示例 1:

- 所有子系统均达到 PL“e”，因此最低 PL (low) 为“e”
- 具有该 PL 的子系统数量为 3 (即 ≤ 3) 。
  因此达到的总 PL 为“e”。
- 如果再增加一个 Pl“e”子系统，那么根据该方法总 PL 降到“d”

示例 2:

- 一个子系统达到 Pl“d”，两个子系统为子系统为 PL“c”。
  因此最低 PL (low) 为“c”。
- 具有该 PL 的子系统数量为 2 (即 ≤ 2) 。
  因此达到的总 PL 为“c”

PL (low) (子系统的最低 PL)	n (low) (具有该 PL 的子系统数量)		PL (最高可达到的 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

➜ 若并非所有子系统的 PL 都已知，则可根据后面的“依照 ISO 13849-1 确定子系统的安全等级”一节确定其安全等级。

详细方法

确定 PL 的主要 (但不唯一) 标准是安全组件的“每小时危险失效概率 (PFHd)”。产生的 PFHd 值由单个 PFHd 值之和构成。

此外，安全组件的制造商也可能作出附加结构限制，必须在总体考虑中将其考虑进去。

➜ 若并非所有子系统的 PFHd 值均已知，则可确定其安全等级。 参见后面的“依照 ISO 13849-1 确定子系统的安全等级”。

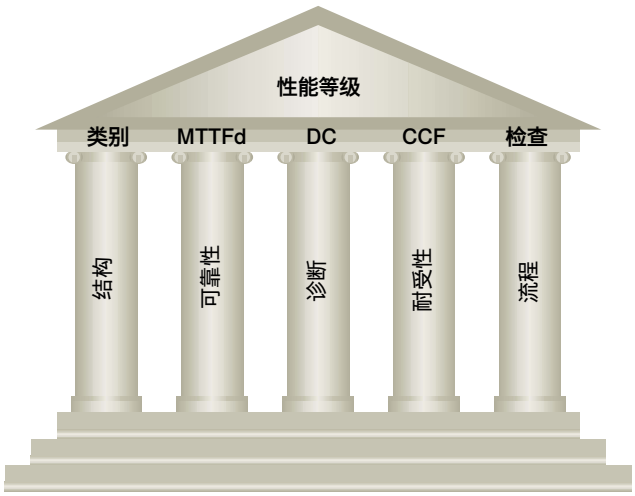
依照 ISO 13849-1 确定子系统的安全等级

安全相关子系统可以由可能来自不同制造商的众多单个组件构成。此类组件包括例如:

- 输入侧: 物理防护装置上的两个安全开关
- 输出侧: 用于停止危险动作的接触器和变频器

在这些情况下，必须单独确定该子系统的 PL。
子系统达到的性能等级由以下参数组成:

- 安全功能在故障条件下的行为以及结构 (类别 ➜ 3-89)
- 单个部件的 MTTFd 值 (➜ 3-90)
- 诊断覆盖率 (DC ➜ 3-91)
- 共因故障 (CCF ➜ 3-91)
- 与安全相关的软件方面
- 系统失效



3 d

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

控制系统安全相关部件的
类别 (ISO 13849-1)

子系统通常为单通道或双通道结构。单通道系统在没有进一步措施的情况下响应伴随危险失效的故障。通过附加测试组件或相互检查的双通道系统可识别故障。在 ISO 13849-1 中通过类别对结构进行分级。

类别	要求简介	系统行为	实现安全的原理
B	控制系统的安全相关部件和/或其防护装置及其部件的设计、结构、选择、装配和组合必须符合适用的标准，以便能够承受可预计的影响。	• 出现故障可能导致失去安全功能。	主要特征在于部件选择
1	必须符合类别 B 的要求。必须应用经证明有效的部件和经证明有效的安全原理。	• 出现故障可能导致失去安全功能，但出现的概率低于类别 B。	
2	必须符合类别 B 的要求并使用经证明有效的安全原理。安全功能必须以合适的时间间隔由机器控制系统检查（测试频率高于要求频率 100 倍）。	• 出现故障可能导致在两次检查之间失去安全功能。 • 通过检查识别失去安全功能。	主要特征在于结构
3	必须符合类别 B 的要求并使用经证明有效的安全原理。安全相关部件的设计必须确保 • 任何部件的单一故障不会导致失去安全功能 • 尽可能以适当方式识别单一故障。	• 当出现单一故障时，始终保留安全功能。 • 能识别一些，但不是所有故障。 • 未识别到的故障累积可能导致失去安全功能。	
4	必须符合类别 B 的要求并使用经证明有效的安全原理。安全相关部件的设计必须确保: • 任何部件的单一故障不会导致失去安全功能**并且** • 在下一次请求安全功能之时或之前识别到单一故障**或者** • 故障累积不会导致失去安全功能。	• 当出现故障时，始终保留安全功能。 • 及时识别故障以免失去安全功能。	

平均危险失效间隔时间 (MTTFd)

MTTF 是“平均危险失效间隔时间” (英语: Mean Time To Failure) 的缩写。从 ISO 13849-1 的角度看，只需要考虑危险失效 (因此“d”代表英语中的“dangerous”) 。
作为理论参数，该值表示一个组件 (不是整个子系统) 在其使用寿命内发生危险失效的概率。子系统的实际使用寿命总是更短。

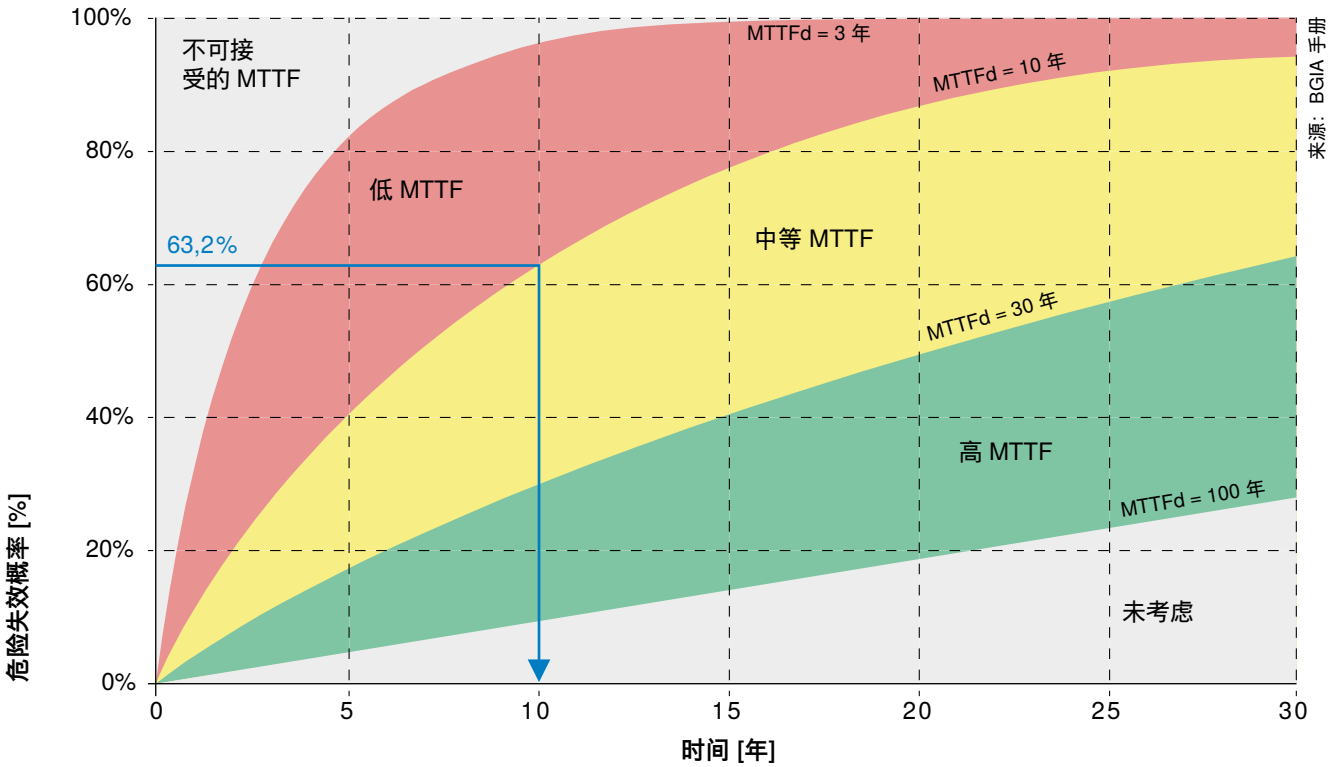
MTTF 值可从失效率得出。在此适用:

- 针对机电或气动组件的 B_{10} 值。在此磨损和最大允许使用时间取决于开关频率。B_{10} 表示 10% 的组件发生失效前的开关循环次数。
- B_{10d} 值表示 10% 的组件发生危险失效前的开关循环次数。若没有B_{10d} 值，可笼统假设 $B_{10d} = 2 \times B_{10}$。
- 对于电子元器件: 失效率 λ。失效率常以“菲特” (FIT，时基失效) 为单位。一菲特是指每 10^9 个小时发生一次失效。

ISO 13849-1 将 MTTFd 值合并成范围:

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

由组件数据可算出整个系统以年为单位的平均危险失效间隔时间 (MTTFd)。
为避免高估可靠性的影响，MTTFd 的可用最高值已限制在 100 年。



8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

诊断覆盖率 (DC)

若在子系统中实现故障识别，则安全等级可以提高。诊断覆盖率 (DC – Diagnostic Coverage) 是衡量发现危险故障能力的尺度。不良诊断只能发现少量故障，良好诊断可发现许多甚至全部故障。

ISO 13849-1 提出了代替详细分析 (FMEA) 的措施并量化了 DC。在此也分成不同范围。

名称	范围
无	DC < 60%
低	60% ≤ DC < 90%
中等	90% ≤ DC < 99%
高	99% ≤ DC

共因失效 - 耐受性

外部影响 (如电平、超温) 可能使相同组件同时无法使用，无论其失效的概率多低或经过多好的测试。(如果突然熄灯，即使有两只眼睛也无法继续看报。) 应始终避免这些共因失效 (CCF – Common Cause Failure)。

ISO 13849-1 的附录 F 提供了基于积分系统的简化方法，用以确定是否已采取足够措施来防止 CCF。每采取一项措施就得到相应分数。若至少取得 65 分，可认为采取了足够的 CCF 措施。

要求		最大值	最低要求
分离	信号电路分离、分开布线、绝缘、电气间隙等	15	总分 ≥ 65
多样性	不同技术、组件、工作方式、设计	20	
设计、应用、经验	防止过载、过电压、过压力等 (视技术而定)	15	
	使用经受住多年考验的组件和方法	5	
分析、评估	通过故障分析避免共因故障	5	
能力、培训	培训设计者以理解和避免CCF 的原因与后果	5	
环境影响	测试系统受 EMC 的影响	25	
	测试系统受温度、冲击、振动等的影响	10	

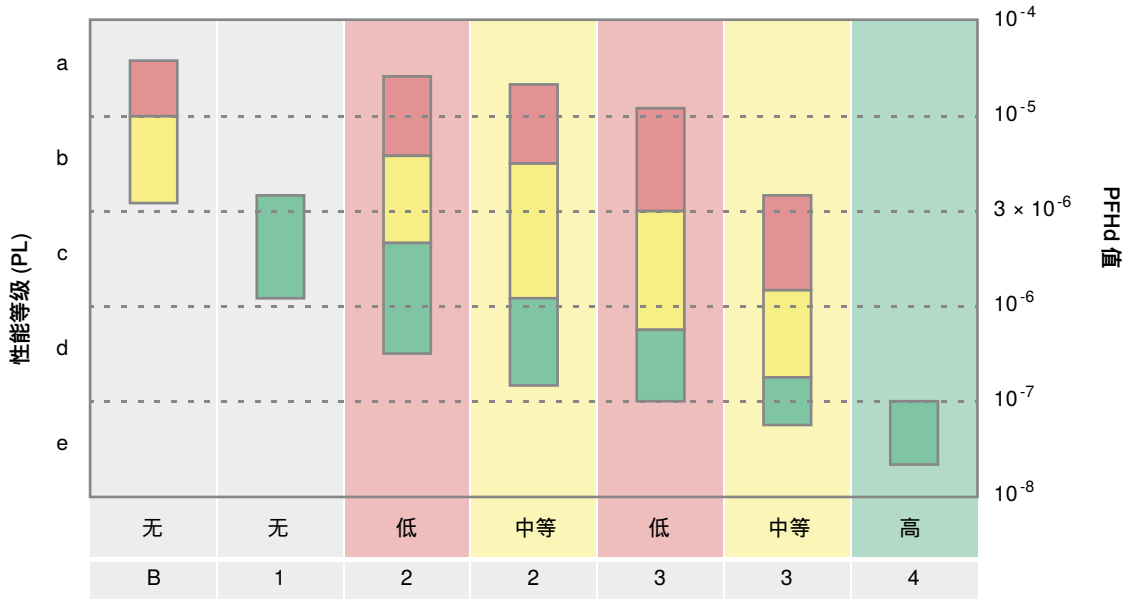
流程

为确保在硬件和软件上正确落实并彻底测试 (四眼原则) 上述方面以及在全面的文档中记录版本和修订状态，应考虑标准中提供的多项帮助。

正确落实安全相关主题的流程是领导与管理任务，并包括适当的质量管理。

确定子系统的 PL

下图所示为 MTTFd 值 (各通道) 、DC 以及类别之间的关联。



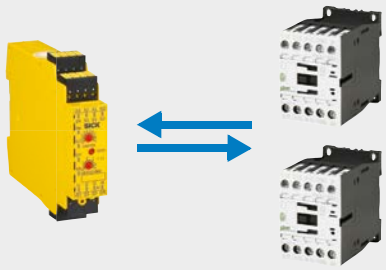
例如性能等级“d”可利用双通道控制系统 (类别 3) 实现。这可在良好的部件质量下 (MTTFd = 中等) 达到，若几乎所有故障被识别到 (DC = 中等) ；或者在非常好的部件质量下 (MTTFd = 高) 达到，若许多故障被识别到 (DC = 低) 。

该方法基于不被用户察觉的复杂数学模型。为保证实用，预先定义了类别、MTTFd 和 DC 等参数。

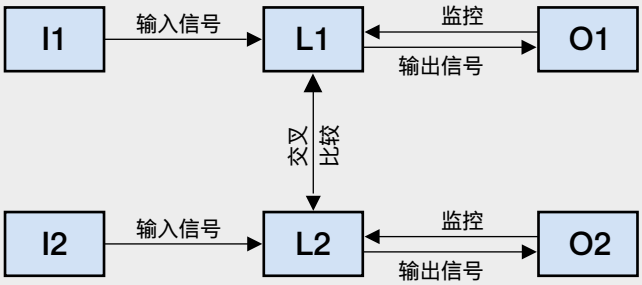
8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

示例: 确定“执行元件”子系统的 PL

1) 定义“执行元件”子系统
“执行元件”子系统由两个带“反馈”的接触器组成。通过接触器触点给定的强制导向可识别接触器的安全相关失效 (EDM)。
UE410 逻辑单元本身不属于“执行元件”子系统，但用于诊断目的。



2) 确定类别
因单一故障安全 (带故障识别) 而**适合于类别 3 或 4**。
提示: DC 值确定后才能最终确定类别。



3) 确定各通道的 MTTFd
因为接触器属于会磨损的组件，所以须借助 B_{10d} 值和估计开关频率 (nop) 确定 MTTFd。适用以下公式:
开关频率数由工作小时/日 [hop]、工作日/年 [dop] 以及每小时开关频率 [C] 组成:
制造商指定的边界条件:

- B_{10d} = 2600000
- C = 1/h (假设)
- d_{op} = 220 d/a
- h_{op} = 16 h/d

在这些一般条件下，得出每个通道 **7386 年的 MTTFd**，该值被视为“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
中等	10 年 ≤ MTTFd < 30 年
高	30 年 ≤ MTTFd < 100 年

4) 确定 DC
由于强制导向触点，可依照 EN ISO 13849-1 中的措施表得出**高 DC (99%)**。

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

3 d

示例: 确定“执行元件”子系统的 PL

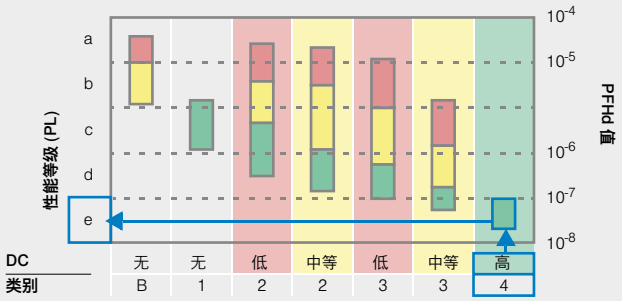
5) 评价避免共因失效的措施
在多通道系统中落实了避免共因影响的措施。评价措施取得 75 分。因此满足最低要求。

要求	值	最低要求
分离	15	
多样性	20	
设计、应用、经验	20	总分 75 ≥ 65
分析、评估	5	
能力/培训	5	
环境影响	35	
	75	

6) 评价流程措施
同样要考虑到涉及避免和管理故障的系统方面。例如:
- 组织和能力
- 设计规则(如规范模板、编码准则)
- 测试理念和测试标准
- 文件编制和配置管理

✔

7) 结果
从用于确定子系统 PL 的插图(➜ 3-86) 可确定子系统的 PL。在该示例中达到 **PL“e”**。
可从 ISO 13849-1 的详细表格中查到得出的该子系统 **PFHd 值为 2.47×10^{-8}**。高 DC 表示双通道结构满足**类别 4** 的要求。



➜ 现在可利用子系统的结果数据确定整个安全功能达到的性能等级 (参见“依照 ISO 13849-1 确定达到的性能等级 (PL)” ➜ 3-86) 。

或者: 依照 IEC 62061 确定达到的安全完整性等级 (SIL)

基于以下标准确定达到的安全完整性等级 (SIL):

- 硬件的安全完整性
  - 要求限度 (SILCL)
  - 硬件的危险随机失效概率 (PFHd)
- 系统安全完整性的要求
  - 避免失效
  - 管理系统故障

与 ISO 13849-1 类似, 在此先将安全功能拆分为功能块再转移至子系统。

硬件的安全完整性

考虑整体安全功能时, 硬件的安全完整性由以下因素决定:

- 子系统的最低 SILCL 限制整个系统最高可达到的 SIL。
- 由单个 PFHd 之和组成的整个控制系统的 PFHd 不超过"验证功能安全"插图 ➜ 3-99 中的值。

示例

在上图中所有子系统均达到 SILCL3。PFHd 值相加小于 1×10^{-7}。已落实与系统安全完整性相关的措施。因此安全功能达到 SIL3。

系统安全完整性

若不同子系统相互结合形成控制系统, 则须另外采取针对系统安全完整性的措施。

避免系统硬件故障的措施主要包括:

- 符合功能安全计划的
- 设计
- 正确选择、组合、布置、组装和安装子系统, 包括电缆敷设、布线和其他连接
- 在制造商的规范内使用
- 遵守制造商的应用说明, 如目录资料、安装说明和应用经证明有效的实践经验
- 考虑根据 IEC 60204-1 关于电气装备的要求

此外, 还要考虑管理系统故障, 例如:

- 切断供电以创造安全状态
- 管理故障影响和其他由相关数据通信流程所造成影响的措施, 包括传输故障、重复、丢失、插入、序列错误、失真、延迟等。

依照 IEC 62061 确定子系统的安全等级

在 IEC 62061 中，也提供了确定由单个组件相互连接所构成的子系统安全等级的方法。

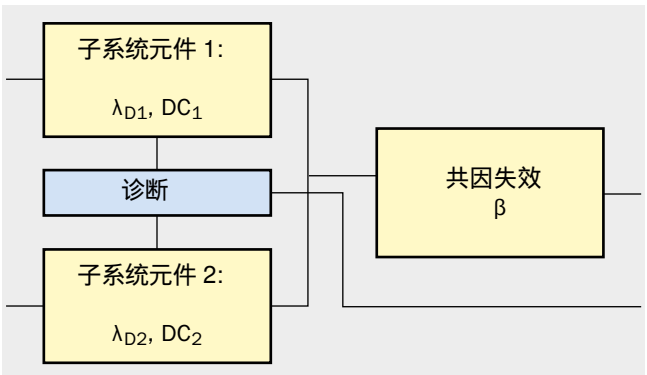
子系统达到的安全完整性等级 (SIL) 由以下参数组成：

- 硬件裕错 (HFT)
- PFHd 值
- 安全失效系数 (SFF)
- 共因失效 (CCF)
- 与安全相关的软件方面
- 系统失效

硬件裕错 (HFT)

在 IEC 62061 中确定了硬件裕错 (HFT) 和子系统类型的结构。

HFT 0 表示单一硬件故障可导致保护功能丧失（单通道系统）。HFT 1 表示即使存在单一硬件故障，仍维持保护功能（双通道系统）。



硬件的危险随机失效概率 (PFHd)

除了结构限制，还要考虑每个子系统的“危险随机硬件失效概率”。根据数学模型，针对每种子系统类型都有一个用于确定 PFHd 值的公式，以下参数被纳入计算：

- 诊断覆盖率
- 持续运行时间
- 诊断测试间隔
- 元件的失效率 (λ_D)
- 共因失效
  （共因原因失效因子 β）

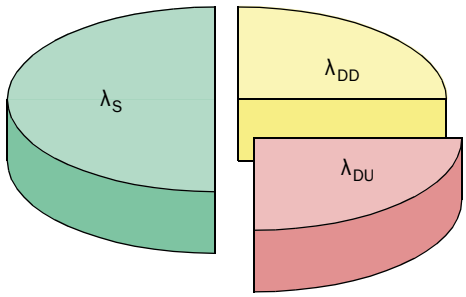
HFT = 1
包括 DC_1 与 DC_2 的诊断

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

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

安全失效系数 (DC/SFF)

DC = 50 %
SFF = 75 %



“安全失效系数”SFF (safe failure fraction) 从诊断覆盖率 DC (λ_{DD} /λ_{DU}) 及“安全故障”系数 (λ_S) 得出。

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

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

共因原因失效 (CCF) – 耐受性

IEC 62061 也要求就共因失效的耐受性进行一系列考虑。根据积分得出共因失效因子 (β)。

要求		最大值
分离	信号电路分离、分开布线、绝缘、电气间隙等	15
多样性	不同技术、组件、工作方式、设计	20
设计、应用、经验	防止过载、过电压、过压力等 (视技术而定)	15
	使用经受住多年考验的组件和方法	5
分析、评估	通过故障分析避免共因故障	5
能力、培训	培训设计者以理解和避免 CCF 的原因与后果	5
环境影响	测试系统受 EMC 的影响	25
	测试系统受温度、冲击、振动等的影响	10

值	CCF 因子 (β)
≤ 35	10%
36 到 65	5%
66 到 85	2%
86 到 100	1%

流程

由于 IEC 62061 与可编程电子系统密切相关, 其中——除了前述方面 (V 模型、质量管理等) ——还有针对安全相关系统软件开发的正确程序的众多详细提示和要求。

结果 - 确定子系统的 SIL

先单独确定每个子系统的硬件安全完整性:
若子系统是已经开发的子系统 (如安全光幕) , 则制造商在其技术规范的框架内一并提供相应参数。此类子系统一般通过 SILCL、PFHd 和持续运行时间等数据充分说明。
但对于由子系统元件 (如防护门的联锁装置或接触器) 组成的子系统, 必须确定安全完整性。

SIL 要求限度 (SILCL: SIL claim limit)

确定了硬件故障裕错 (结构) 后, 可确定子系统最高可达到的 SIL (SIL 要求限度) 。

安全失效系数 (SFF)	硬件故障裕错	
	0	1
< 60%	–	SIL1
60 到 < 90%	SIL1	SIL2
90 到 < 99%	SIL2	SIL3
≥ 99%	SIL3	SIL3

HFT 1 双通道系统可在 90% 的 SFF 下宣称达到 SILCL3。

3 d

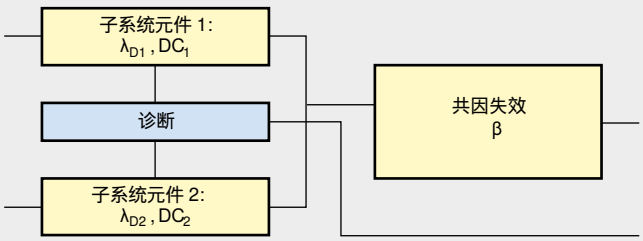
示例: 确定“执行元件”子系统的 SILCL 和 PFHd

1) 定义“执行元件”子系统

“执行元件”子系统由两个带“反馈”的接触器组成。通过接触器给定的强制导向, 可识别接触器上的安全相关失效 (EDM)。
UE410 逻辑单元本身不属于“执行元件”子系统, 但用于诊断目的。

2) 确定硬件故障裕度 (HFT)

由于单一故障安全 (带故障识别) 得出 HFT = 1。



3) 确定 PFHd

a) 根据故障率 λ_D

因为接触器属于会磨损的组件, 所以须借助 B_{10d} 值和估计开关频率确定 每小时开关频率 [C]。
IEC 62061 未陈述机械部件的行为。因此根据 ISO 13849-1 确定故障率 λ_D。假设故障率在使用期间保持恒定。
制造商指定的边界条件:

- B_{10d} = 2600000
- C = 1/h(假设)

在这些边界条件下, 得出
λ_D 为 3.8×10^{-8} 1/h。

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

b) 根据 CCF 因子 (β)

在多通道系统中需要避免共因影响的措施。根据符合 IEC 62061 要求的措施确定影响。在示例中因子为 5% (见下方: “5) 评价避免共因故障的措施”)
PFHd ≈ 1.9×10^{-9}。

值	CCF 因子 (β)
≤ 35	10%
36 到 65	5%
66 到 85	2%
86 到 100	1%

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

$$\approx \beta \times \lambda_D$$

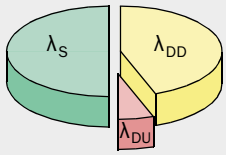
$$\approx 0,05 \times 0,1 \times \frac{C}{B_{10d}}$$

$$PFHd \approx 1,9 \times 10^{-9}$$

示例: 确定“执行元件”子系统的 SILCL 和 PFHd

4) 通过 DC 确定 SFF
因强制导向触点而得出“高”DC (99%)。也就是说，可 99% 识别到接触器 70% 的危险故障 λ_D。据此，
SFF = 30% + 69.3% = 99.3%。

DC = 99 %
SFF = 99.3 %



5) 评价避免共因故障的措施
在多通道系统中需要避免共因影响的措施。在该示例中，依照 IEC 62061 评价措施得出
CCF 因子 (β) 为 5%。

值	CCF 因子 (β)
≤ 35	10%
36 到 65	5%
66 到 85	2%
86 到 100	1%

6) 评价流程措施
同样要考虑到涉及避免和管理故障的系统方面。例如:
- 组织和能力
- 设计规则(如规范模板、编码准则)
- 测试理念和测试标准
- 文件编制和配置管理

✔

结果
在最后一步中应考虑结构限制。基于现有冗余 (硬件故障裕度 1) 和 SFF > 99%，由此得出该子系统的 SIL 宣称限制 (SIL claim limit) 为 SILCL3。

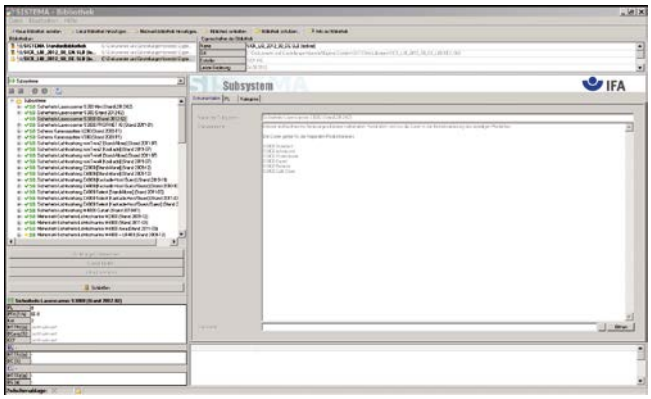
安全失效系数 (SFF)	硬件故障裕错	
	0	1
< 60%	–	SIL1
60 到 < 90%	SIL1	SIL2
90 到 < 99%	SIL2	SIL3
≥ 99%	SIL3	SIL3

PFHd ≈ $1{,}9 \times 10^{-9}$

➜ 现在可利用子系统的结果数据 SILCL 和 PFHd 值如上所述确定整个安全功能所达到的 SIL (参见“硬件的安全完整性” ➜ 3-95) 。

有力支持

所述验证方法需要专有技术和处理性能等级 (PL) 与安全完整性等级 (SIL) 的经验。SICK 可提供相应服务 (➜ “SICK 提供哪些支持” ➜ i-1) 。合适的软件工具有助于系统地操作。
由 IFA 开发并可免费使用的 SISTEMA 软件助手提供计算性能等级的有效方法。SICK 为此提供经认证的安全元件库。
此外, 我们的研讨会还传授实用的专有技术以方便日常工作。



➜ 关于 SISTEMA、SICK 的组件库及培训的更多信息参见: www.sick-safetyplus.com

3 d

总结: 验证安全功能

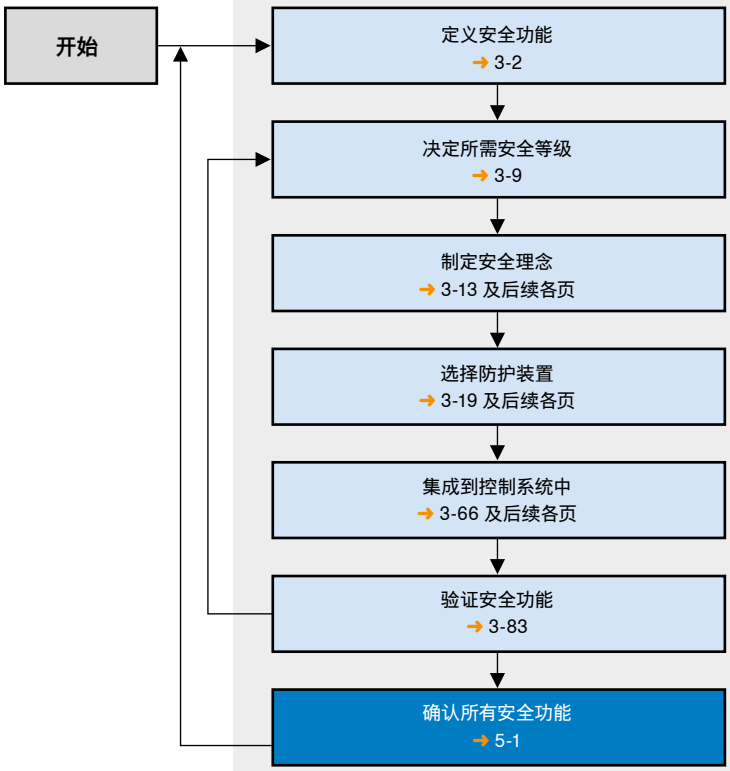
基本原则
- 验证计划的安全功能是否满足所需安全等级。为此验证机械安全和功能安全。

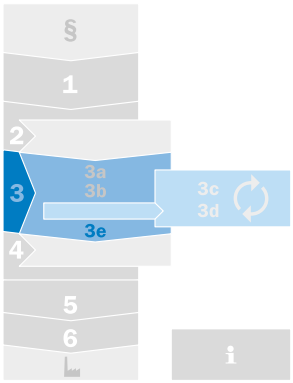
方法
- 依照 ISO 13849-1 确定得到的安全等级 (PL)。可用方法:
  - 简化方法 (根据 PL)
  - 详细方法 (根据 PFHd 值)
- 若子系统 (如执行元件) 的 PL 或 PFHd 值未知, 则从结构、可靠性、诊断、耐受性和流程等参数确定子系统的安全等级。
- 或者依照 IEC 62061 确定得到的安全等级 (SIL)。在此也可以确定未经认证子系统的安全等级。

帮助
- 使用推荐工具和采纳建议。

第 3e 步: 确认所有安全功能

确认是联系一个待解决的问题，检查一种理论、一项计划或一个解法。因此，与验证不同——仅依照规格说明书评价解决方案是否正确落实——确认是最终评价解决方案是否普遍适用于必要的风险降低。





3e

确认程序的目的是检查机器上参与安全功能的组件设计的规格说明书和符合性。
确认应表明，控制功能的安全相关部件满足 ISO 13849-2 的要求，特别是对规定安全等级的要求。
在合理情况下，应当由未参与控制系统安全相关部件设计的人员执行确认。
在确认流程中，检查所制订规格说明书中的错误，特别是遗漏非常重要。
安全相关控制功能设计的关键部分通常是规格说明书。
相关示例：应通过光幕防护进入白车身单间。因此，安全功能的详细说明如下：
“若光幕的保护区域被中断，则须尽快停止所有危险动作。”

但除此之外，设计者还要考虑到当保护区域重新空闲，特别是可从后面进入保护区域时的重启。确认证流程必须揭示这些方面。

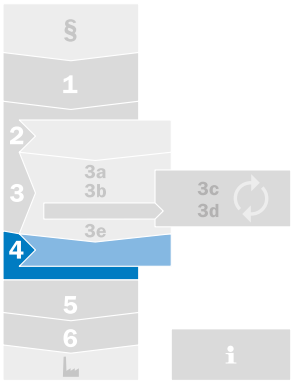
在确证流程中，通常采用相互补充的多个程序。
其中包括：
- 防护设备的定位和有效性的技术检查
- 通过实际响应的检查对比模拟故障预计结果
- 通过功能测试确认对环境的要求：
  - 充分防护环境因素的影响，如温度、潮湿、冲击、振动与冲击载荷等。
  - 充分抵抗电磁影响的干扰

第 4 步: 关于剩余风险的用户信息

若安全设计或技术防护措施不能完全发挥作用, 则须另外提醒用户注意现有剩余风险, 并告知采取进一步防护措施, 特别是使用个人防护装备的必要性。

关于剩余风险的用户信息包括例如:

- 声光警告装置
- 机器上的信息和警告提示
- 操作指南中的警告提示
- 工作指导、培训要求或用户入门
- 个人防护设备的使用提示



用户信息不得代替其他措施!

➜ 安全设计、风险评估和风险降低A 类标准: ISO 12100

4

声光警告装置

如机器运行不受监控，则须给机器配备警告装置以报告故障造成的危险。警告装置必须清晰易懂、可轻松感知，而且允许操作人员检查一直准备就绪。若仍然存在剩余风险，则制造商应当指出。

机器上的信息和警告提示

机器上的信息和警告提示应尽可能采用符号或象形图的形式。其必须以机器被投放市场的所在国家的官方语言撰写。允许采用其他官方语言的附加警告。安全相关信息必须以清晰、易懂、简洁和准确的方式表述。交互式通信工具必须易于理解并可直观操作。

4

操作指南中的警告与注意事项

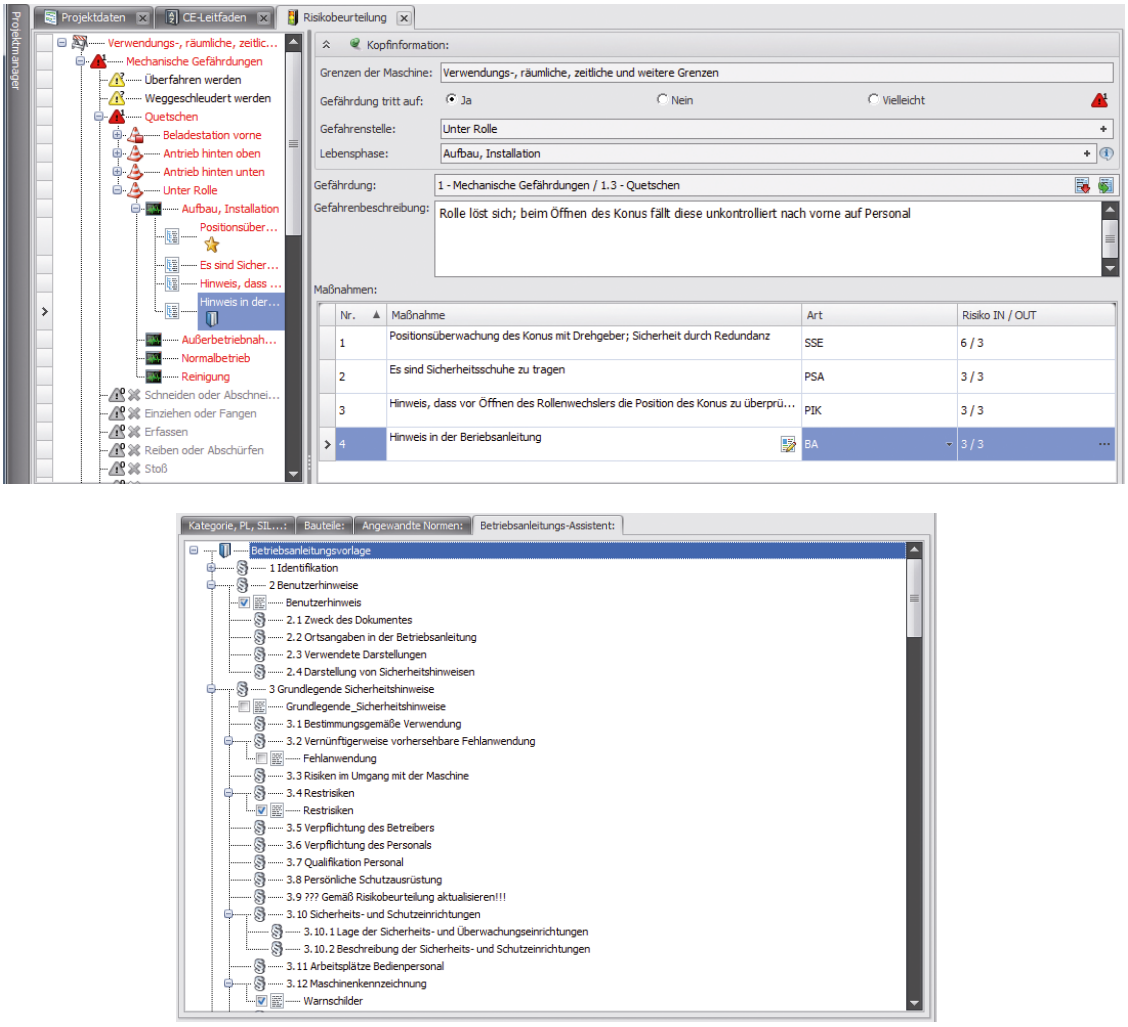
操作指南必须包括机器的所有安全相关信息，特别是：

- 对根据经验可能发生的机器误用的警告
- 有关机器调试和使用以及必要培训或操作人员入门的提示
- 尽管已采取安全设计和使用防护设备与补充防护措施仍然留有的剩余风险信息
- 应当由用户采取的防护措施和所需个人防护装备的指示
- 在机器的各个寿命阶段满足稳定性要求的条件
- 关于运输、装卸和储存的注意事项
- 如果发生事故和为了安全排除故障而需遵循的程序指示
- 安全调整与维护的指示和所需防护措施
- 可能影响操作人员的安全与健康的可用备件规格

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

使用 Safexpert® 编制文件

借助 Safexpert® 软件 (➜ 页码 1-5) 也可轻松落实对技术文件的要求。这样用户便可例如将风险评估中的注意事项直接集成到操作指南中。



Safexpert® 操作说明助手

第 2、第 3 和第 4 步的总结: 风险降低

基本原则

按照 3 步法降低所分析危害的风险:

1. 设计机器时, 确保尽可能消除风险。
2. 定义、采取和检验必要的防护措施。
3. 了解遗留的剩余风险。定义可降低遗留的剩余风险的方式并向用户提供该信息。

技术防护措施

- 就功能安全而言, 有两项标准可提供帮助: ISO 13849-1 (PL) 或 IEC 62061 (SIL)。
- 定义安全功能并逐一确定所需安全等级。
- 起草安全理念。选择最有效的防护设备和安装与集成到控制系统中的方式。
- 确保有效落实防护措施并达到所需安全等级。

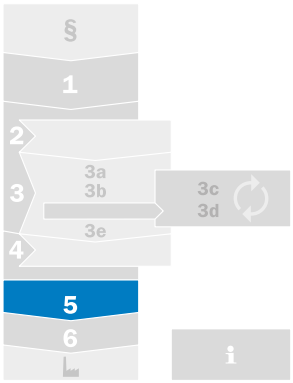
第 5 步: 整体确认

因为功能安全只是风险降低的一部分，所以需要在整体确认过程中评价所有相关措施，即设计、技术与组织措施。

因此，在实践中单独一项技术措施可能不会实现风险降低，但在全盘考虑中可以得到满意结果。若以下问题都能得到肯定答复，可视为已充分实现风险降低：是否已考虑到机器各个寿命阶段的所有运行条件？

- 是否运用了 3 步法？
- 是否已在切实可行的范围内尽量消除危害或降低危害的风险？
- 是否已确保所采取的措施不会造成新的危害？
- 是否已充分告知并提醒用户注意剩余风险？
- 是否已确保操作人员的工作条件不会因所采取的防护措施而受到影响？
- 所采取的防护措施是否相互协调？
- 是否已充分考虑到在非商业或非工业区域内使用机器可能产生的后果？
- 是否已确保所采取的措施不会过度影响机器的预期功能？
- 风险是否已适度降低？

在由 SICK 的安全专家进行安全技术检查期间，就基本危害对整台机器进行检测。

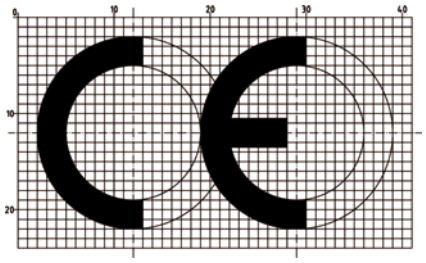


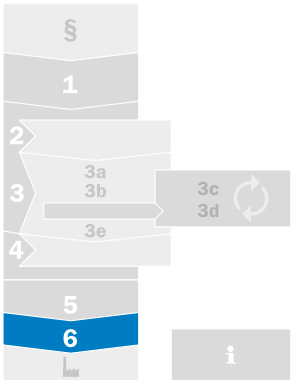
5

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

第 6 步: 投放市场

在整体确认过程中确定了符合性 (必要时诉诸检测机构) 后, 可在编制技术文件期间签发符合性声明并在机器上粘贴 CE 标志。符合性声明必须考虑到适用于机器的所有欧盟指令。





技术文件

技术文件的范围已在机械指令附录 VII 的 A 部分中说明。对于半成品机械, 适用机械指令附录 VII B 部分中的特殊要求。

必须能够根据技术文件评估机器符合机械指令的要求。只要为评估所需, 技术文件就必须包括机器的设计、构造和工作方式。

这些文件必须采用欧共体的一种或多种官方语言撰写; 机器的操作指南除外, 其适用于附录 I 第 1.7.4.1 条的特殊规定。

保管时间和期限

应保留技术文件供成员国的主管部门备查:

- 从机器制造之日起
- 在完成最后一个单元后至少为期 10 年
- 技术文件不必位于欧共体地区, 也不必始终以实体形式存在 (如数字化保存) 。但欧盟合规性声明中的指定人员必须能够在合理期限内提供技术文件。

注意: 若技术文件未能应合理要求提交国家主管机关, 则可以有充分理由怀疑相关机器是否符合基本安全与健康要求!

6

技术文件的范围

- 机器的一般说明:
  - 机器的概览图、控制回路的电路图以及理解机器工作方式所需的说明和解释
  - 完整详图 (可能包含计算) 、测试结果、检验机器是否符合基本安全与健康要求所需的证明等
- 适用标准列表和其他技术规范以及摘自这些标准的基本安全与健康要求
- 风险评估文件 (➜ 1-1), 由此得知应用了哪种方法:
  - 适用于机器的基本安全与健康要求列表
  - 所采取的避免已确定危害或降低风险的防护措施说明以及机器产生的剩余风险列表 (必要时)
- 所有技术报告, 包含由制造商亲自进行或由制造商或其代理人选择的机构所进行检测的结果
- 机器的操作指南
- 欧盟合规性声明复本
- 安装到机器内的其他机械或产品的欧盟合规性声明副本 (必要时)
- 半成品机械的公司声明和装配说明书 (必要时)

操作指南

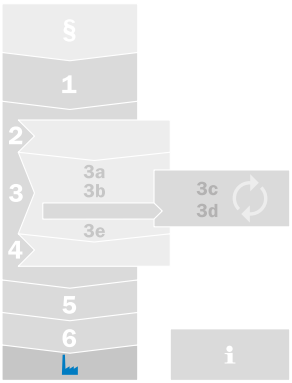
机器必须附带一份采用使用国官方语言的操作指南。这份附带的操作指南必须是“原始使用说明书”或“原始使用说明书”的译本; 在后一种情况下, 还要提供原始使用说明书。更多信息参见“第 4 步: 关于剩余风险的用户信息” ➜ 4-1。

8020567/2017-08-22(GCN 2021-07-01)
如有更改, 恕不另行通知

使用者的责任

雇主对其雇员的安全负责。机器必须符合人类工效学并能根据操作人员的资格安全运行。

除了交付时的安全技术验收和检查，在采购机器时就应考虑到安全技术要求的恰当规范。



应如何采购机器？

购置是建立一个现代化生产设施项的重要手段 。这一阶段决定了未来走向。

- 对于复杂的机械设备，依照机械指令确定一名“施工负责人”。
- 事先澄清如何处理所提供的 (部分) 机械。
- 通过合同确定应提供哪些附加文件 (如风险评估)，以便稍后更容易进行修改。
- 在合理范围内以使用重要标准 (欧盟协调标准) 为基础。
- 偏离协调标准时，约定处理方式。

安全检查

经验表明，机械安全在实践中不是完美的。防护装置经常被干忧以便不受阻碍地工作。其他问题包括防护装置定位错误以及不当集成到控制系统中。
工作设备和系统在运行中的安全技术状态由欧盟指令 2009/104/EC (“工作设备指令”) 规定，并且应根据具体适用的国家法律进行检查。该指令的第 4a 条专门定义了工作设备检查。技术规程和标准或特定法规可作为设计的依据。据此，相应设备的使用者应安排检查和正式确定工作安全。
使用者应确保按照各个国家对工作设备指令的落实情况组织工作设备检查。

在此必须满足以下要求:
1. 检查类型
2. 检查范围
3. 检查深度
4. 检查期限
5. 检查员的资格等级

借助 SICK 的安全检查，可快速了解机器安全状态的概况。
位于杜塞尔多夫的 SICK 销售总部以及 SICK 的捷克子公司已成为官方认可的检查机构。
来自独立机构的认证确认了 SICK 能够以高可靠性和所需质量执行认证范围内确定的工作。
我们将与您一起探讨改进潜力并付诸实施。

DAkkS Deutsche Akkreditierungsstelle D-IS-12060-01-01

I 4051

工作设备指令第 4a 条: 工作设备检查

6. 雇主应确保安全性视安装条件而定的工作设备，由各国法规和/或实践意义上的合格的安全人员在安装后和首次调试前以及每次安装在新的施工现场或新地点后，进行检查以保证该工作设备正确安装和正常工作。
7. 雇主应确保可能导致危险情况的工作设备
   - 由各国法规和/或实践意义上的合格的安全人员定期检查并在必要时测试以及
   - 由各国法规和/或实践意义上的合格的安全人员在每次发生可能对工作设备的安全性有不利影响的异常事件（如改动、事故、自然现象、长时间不用）后进行特殊检查，以便遵守健康与安全要求并及时发现和排除这些损害。
8. 检查结果必须以书面形式记录并供主管部门使用。其必须留存适当时间。若相关工作设备在企业外面使用，应附上最近一次检查的证明。
9. 成员国应确定进行这些检查的条件。

SICK 提供哪些支持

将安全功能高效集成到机器或机器理念中需要高超的安全技术能力。这种能力不仅涉及技巧、与时俱进和安全知识储备，还包括应用合适流程的经验。所有这些因素兼备的安全合作伙伴才表示具有安全技术能力。

SICK 在机械安全领域积累了 60 多年的经验，通过定制化服务提供依照指令落实机械安全所需的专门知识。

SICK 以此为进一步发展企业的安全文化作出贡献，目的是：

- 提高现有机器和设备的安全性
- 在购置新机器和设备时保证整体的安全性
- 在运用 CE 程序和采取用于降低风险的设计措施上为设计人员提供支持

对合作伙伴提出高要求是理所应当的。合作伙伴必须：

- 拥有多年经验
- 提供创新想法
- 立足国际市场

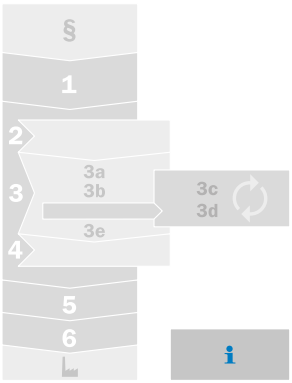
通过在早期阶段咨询 SICK 专家，

- 将安全问题规划为项目的组成部分。
- 及早发现潜在弱点。
- 避免超尺寸。
- 确保有效性和竞争力。

SICK 的服务提升了安全性和经济附加值。

关于安全机器与设备的设计与符合性服务的 SICK 流程

SICK 的“机械安全咨询与设计”服务依照下图中的流程实现。在此可看到 SICK 于每个阶段提供的服务产品。可单独或作为 CE 符合性流程范围内的综合服务解决方案订购这些产品。



在本章中…

关于安全机器与设备的设计与符合性服务的 SICK 流程

SICK 的“机械安全咨询与设计”服务依照下图中的流程实现。在此可看到 SICK 于每个阶段提供的服务产品。可单独或作为 CE 符合性流程范围内的综合服务解决方案订购这些产品。

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

培训和研讨会

用户的实践知识
一般来说，经验越丰富，越能安全地处理应用。传授经验进而优化应用是 SICK 培训和研讨会的重要组成部分。因此其特别实用

定制化培训
我们将根据学员的需要和所传授的内容选择适当措施来传授知识和保证知识转移:
- 培训
- 研讨会
- 电子媒体上的学习
- 模块化培训理念
- 更新培训

保证增进知识
法律规定和标准随着时间的推移而变化。技术变革要求人们适应创新。在关于安全技术基础的模块化培训中，我们将重点传授以下领域的最新专有技术:
- 依照标准选择合适的防护装置
- 防护装置集成到总体控制系统中
- 根据适用的指令、标准和条例正确评估防护措施

加强应用安全
我们的培训以产品为导向，目的是将产品高效且长期安全地集成到计划应用中。学员将在此获得安全、高效地使用设备工作所需的全部基础知识——也涉及分析与诊断方法。
我们培训的一般结构包括选择与集成产品流程的不同阶段:
- 选择
  - 安全方面
  - 产品特性和可能应用
- 集成
  - 添加至应用 (安装) 和布线
  - 编程
  - 调试
- 安全运行
  - 故障诊断与排除

SICK 根据需要为您的应用量身定制培训理念。该服务有助于优化工作质量和加速与安全相关的知识转移。

与时俱进
为了让您始终与时俱进、把握时代脉搏，我们可为您提供特别的进修措施——与您的知识水平相协调。

➜ 最新详细信息可登陆网站 www.sick.com/training 或在我们的研讨会计划中查看。
➜ 欲了解海外研讨会，请咨询您的 SICK 代理商或访问 www.sick.com

如有需要，我们也可以到现场举行研讨会和用户培训。请与我们联系!

SICK——我们在整个产品生命周期中陪伴您的设备

凭借经认证的安全技术产品和单独为您的任务量身定制的服务，SICK 在机器的整个生命周期中为您提供支持。
从规划到调试再到维修和升级。

SICK 的服务	六个步骤实现机械安全				
	§ 法律、指令、标准	第 1 步 风险评估	第 2 到第 4 步 风险降低： 3 步法	第 5 到第 6 步 整体确认和投放市场	使用者的责任
咨询与设计					
• 风险评估		✔			
• 安全理念			✔		
• 硬件设计			✔		
• 软件设计			✔		
• 安装			✔		
• 调试			✔		
• CE 符合性评估				✔	
• 机械安全评估					✔
验证和优化					
• 首次调试前检查				✔	✔
• 定期检查					✔
• 机械安全检查				✔	✔
• 电气设备检查				✔	✔
• 事故调查					✔
• 停机时间测量				✔	✔
培训和进修					
• 研讨会	✔	✔	✔	✔	✔
• 用户培训					✔
• 网络培训	✔	✔	✔	✔	✔
升级和改型					
• 升级包					✔
产品和系统支持					
• 调试检查					✔
• 服务热线					✔
• 现场故障排除					✔
• 交换设备					✔
• 备件					✔
• 车间修理					✔

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

元件（产品）
使用经认证产品让机械制造商更易于证明与机械指令及各种标准的要求的符合性。作为解决方案供应商，SICK 为机械制造商提供广泛产品：从简单的单光束安全光电传感器到安全光幕、安全激光扫描仪、安全摄像系统和安全开关再到可联网的模块化安全控制器以及保证机器符合性的软件解决方案。

咨询：我们的知识有益于您的应用
SICK 在全球 87 个工业国设立了子公司或代表处。在那里我们高素质的技术人员将为您提供所需的专业咨询。他们不仅凭借关于产品的技术知识，还依靠对市场和国内法律与标准的了解为您提供支持。

➜ 安全技术产品概览 ➜ 3-81
➜ 所有产品参见在线产品查找，登陆 www.sick.com
➜ 欲更多了解您所在国家的可用服务，请咨询您的 SICK 代理商或访问 www.sick-safetyplus.com

相关标准概览

型	欧洲标准 EN	协调	国际标准 ISO/IEC	标题或参考
A	EN ISO 12100 代替以下标准	✔	ISO 12100	机械安全 – 一般设计原则 – 风险评估和风险降低
	EN ISO 12100-1		ISO 12100-1	机械安全 – 基本概念和一般设计原则 • 第 1 部分:基本术语、方法学
	EN ISO 12100-2		ISO 12100-2	机械安全 – 基本概念、一般设计原则 • 第 2 部分:技术原则
	EN ISO 14121-1		ISO 14121-1	机械安全 – 风险评估 • 第 1 部分:原则
B	EN 349	✔	ISO 13854	避免人体部位挤压的最小间距
	EN 574	✔	ISO 13851	双手操纵装置 - 功能方面 - 设计原则
	EN 953	✔	ISO 14120	防护装置 – 设计和制造的一般要求(目前正在修订,未来将作为 EN ISO 14120 发布)
	EN 1037	✔	ISO 14118	防止意外启动
	EN 1088	✔		带防护设备的联锁装置 – 设计和选择原则(目前正在修订,不久将作为 EN ISO 14119 发布)
	EN ISO 13849-1	✔	ISO 13849-1	控制系统有关安全相关部件 • 第 1 部分:一般设计原则
	EN ISO 13849-2	✔	ISO 13849-2	• 第 2 部分:确认
	EN ISO 13850 (代替 EN 418)	✔	ISO 13850	紧急停止 – 设计原则
	EN ISO 13855 (代替 EN 999)	✔	ISO 13855	与人体部位接近速度相关的防护设施的定位
	EN ISO 13857 (代替 EN 294 和 EN 811)	✔	ISO 13857	防止上下肢触及危险区域的安全距离
	EN 60204-1	✔	IEC 60204	机器电气装备 • 第 1 部分:一般要求
	EN 61496-1	✔	IEC 61496-1	电敏防护设备 • 第 1 部分:一般要求和试验
	CLC/TS 61496-2	–	IEC 61496-2	• 第 2 部分:使用有源光电保护装置的设备的特殊要求
	CLC/TS 61496-3	–	IEC 61496-3	• 第 3 部分:响应漫反射的有源光电防护设备 (AOPDDR) 的特殊要求
	CLC/TS 62046	–	IEC/TS 62046	检测人的存在的防护设备的应用
	EN 62061	✔	IEC 62061	安全相关电气、电子和可编程电子控制系统的功能安全

型	欧洲标准 EN	协调	国际标准 ISO/IEC	标题或参考
C	EN 1114-1	✔	–	橡胶和塑料机械 – 挤出机和挤出生产线 • 第 1 部分:挤出机的安全要求
	EN 12622	✔	–	液压折弯机
	EN 13736	✔	–	气动压力机
	EN 1459	✔	–	机械安全 – 可变前移式叉车
	EN 1525	–	–	工业卡车的安全 – 无人驾驶卡车及其系统
	EN 1526	✔	–	工业卡车的安全 – 卡车自动功能的附加要求
	EN 1612-1	✔	–	橡胶和塑料机械 – 反应成型机 • 第 1 部分:混合和计量单元的安全要求
	EN 1672-1	–	–	食品加工机械 – 安全和卫生要求 – 一般设计原则
	EN 201	✔	–	橡胶塑料机械注射成型机安全要求
	EN 289	✔	–	橡胶和塑料机械;模压机和喷压机;设计的安全技术要求
	EN 415-X	✔*	–	包装机 (*:该标准仅第 1、第 3 以及第 5 到第 9 部分经过协调)
	EN 422	✔	–	橡胶和塑料机械;安全 - 用于制造空心体的吹塑机 – 设计和制造要求
	EN 528	✔	–	存储和检索系统 - 安全
	EN 692	✔	–	机械压力机
	EN 693	✔	–	液压机
	EN 710	✔	–	铸模和制芯机械及设备和有关装置的安全要求
	EN 869	✔	–	金属压力铸造设备的安全要求
	EN ISO 1010-X	✔*	ISO 1010-X	印刷和纸品加工机械 (*:该标准的第 1 到第 4 部分经过协调)
	EN ISO 10218-1 (代替 EN 775)	✔	ISO 10218-1	工业环境用机器人 – 安全要求 • 第 1 部分:机器人
	EN ISO 10218-2	✔	ISO 10218-2	• 第 2 部分:机器人系统与集成
	EN ISO 11111-X	✔*	ISO 11111-X	纺织机械(*:该标准的第 1 到第 7 部分经过协调)

常用链接

从哪里可以找到…?	
指令文本 (EU)	指令全文可在互联网上，例如在欧盟法律的门户网站上找到 ➜ eur-lex.europa.eu
标准列表	欧盟官方公报 德国联邦职业安全和健康机构 (BAuA): ➜ www.baua.de 德国机械设备制造业联合会 (VDMA): ➜ www.vdma.org 欧盟委员会 ➜ www.ec.europa.eu/growth/index_en.htm Beuth Verlag GmbH: ➜ www.beuth.de
标准发布机构，国际	CEN: ➜ www.cen.eu/cenorm/homepage.htm CENELEC: ➜ www.cenelec.eu ISO: ➜ www.iso.org/iso/home.htm IEC: ➜ www.iec.ch
标准发布机构，德语国家	德国 (DIN): ➜ www.din.de 奥地利 (ON): ➜ www.as-institute.at 瑞士 (SVN): ➜ www.snv.ch
标准发布机构，欧洲	比利时 (NBN): ➜ www.nbn.be 保加利亚 (BDS): ➜ www.bds-bg.org 丹麦 (DS): ➜ www.ds.dk 爱沙尼亚 (EVS): ➜ www.evs.ee 芬兰 (SFS): ➜ www.sfs.fi 法国 (AFNOR): ➜ www.afnor.org 希腊 (ELOT): ➜ www.elot.gr 英国 (BSI): ➜ www.bsigroup.com 爱尔兰 (NSAI): ➜ www.nsai.ie 冰岛 (IST): ➜ www.stadlar.is 意大利 (UNI): ➜ www.uni.com/it 拉脱维亚 (LVS): ➜ www.lvs.lv 立陶宛 (LST): ➜ www.lsd.lt 卢森堡 (SEE): ➜ www.see.lu 马耳他 (MSA): ➜ www.msa.org.mt 荷兰 (NEN): ➜ www2.nen.nl 挪威 (SN): ➜ www.standard.no 波兰 (PKN): ➜ www.pkn.pl 葡萄牙 (IPQ): ➜ www.ipq.pt 罗马尼亚 (ASRO): ➜ www.asro.ro 瑞典 (SIS): ➜ www.sis.se 斯洛文尼亚 (SIST): ➜ www.sist.si 斯洛伐克 (SUTN): ➜ www.sutn.sk 西班牙 (AENOR): ➜ www.aenor.es 捷克 (CNI): ➜ www.unmz.cz/urad/unmz 匈牙利 (MSZT): ➜ www.mszt.hu 塞浦路斯 (CYS): ➜ www.cys.org.cy
关于德国公告机构、其他欧盟成员国或 EFTA 国家及其他与欧盟达成互认协议国家的最新信息可通过欧盟的 NANDO 信息系统查询。	德国联邦职业安全和健康机构提供迄今为止欧共体成员国公告的认证机构列表: ➜ ec.europa.eu/enterprise/newapproach/nando

从哪里可以找到...?	
德国各州职业安全机构（彼此结构不同）	巴登-符腾堡: ➜ www.gewerbeaufsicht.baden-wuerttemberg.de 巴伐利亚: ➜ www.lgl.bayern.de/arbeitsschutz/index.htm 柏林: ➜ www.berlin.de/lagetsi 勃兰登堡: ➜ www.arbeitsschutzverwaltung.brandenburg.de 不来梅: ➜ www.gewerbeaufsicht.bremen.de 汉堡: ➜ www.hamburg.de/arbeitsschutz 黑森: ➜ www.sozialnetz.de/ca/b/b 梅克伦堡-前波莫瑞: ➜ www.lagus.mv-regierung.de 下萨克森: ➜ www.gewerbeaufsicht.niedersachsen.de 北莱因-威斯特法伦: ➜ www.arbeitsschutz.nrw.de/bp/index.html 莱茵兰-普法尔茨: ➜ www.masgff.rlp.de/arbeit/arbeitsschutz 萨尔兰: ➜ www.lua.saarland.de 萨克森: ➜ www.arbeitsschutz.sachsen.de 萨克森-安哈尔特: ➜ www.verbraucherschutz.sachsen-anhalt.de/arbeitsschutz 石勒苏益格-荷尔斯泰因: ➜ www.schleswig-holstein.de/DE/Themen/A/arbeitsschutz 图林根: ➜ www.thueringen.de/th7/tlv/arbeitsschutz
奥地利	奥地利职业安全检查团: ➜ www.arbeitsinspektion.gv.at CD-ROM“ArbeitnehmerInnenschutz expert”（雇员保护专家） ➜ www.a-expert.at
瑞士	瑞士职业安全检查团: ➜ www.seco.admin.ch
职业保险专业委员会列表（德国）	德国法定意外保险协会 (Deutsche Gesetzliche Unfallversicherung, DGUV) 中的专业委员会和专业小组重新调整。DGUV 准则 401“DGUV 的部门和专业领域”为应对未来挑战的统一的安全与健康能力网络奠定了基础。先前的专业委员会被新部门替代。 ➜ www.dguv.de/de/Pr%c3%a4vention/Fachbereiche-der-DGUV/index.jsp
职业保险联合会的地址（德国）	➜ www.dguv.de/de/Berufsgenossenschaften-Unfallkassen-Landesverbände
意外险承保单位	德国: 德国法定意外保险协会 ➜ www.dguv.de 奥地利: 综合意外保险机构: ➜ www.auva.at 瑞士: 瑞士事故预防机构 ➜ www.suva.ch

术语表/索引

缩写/概念		解释	索引
单次遮光和双次遮光 PSDI 模式		该操作模式有利于手动循环放入或取出零件。在该模式下，通过在一次或两次遮光后，保护区域在通光状态下，使机器自动循环重新启动。 应在以下条件下必须重新复位: • 机器启动时 • 如果 ➜ AOPD 在危险动作时，光电保护装置被中断 • 危险动作 • 等待持续 30 s 以上 (参见 IEC 61496-1/EN 61496-1)需要重新启动 ➜ 更多信息: EN 692 但需要检查在工作流程期间，是否对操作人员存在危害。该操作模式仅限用于危险区域不可进入的小型机器，并可以检测人员是否存在。还应通过适当措施去防护机器的所有其他侧面。 若启动该操作模式，则 AOPD 的分辨率必须小于或等于 30 mm（参见 ISO 13855、EN 692 和 EN 693）。 一般情况下，在安装防护装置时，必须排除以下错误: 从上方、下方、四周伸手进去或从后方进入。	➜ 3-41

λ	Failure rate per hour	λ: 每小时失效率，λ_S 与 λ_D 之和
		• λ_S: 安全失效率
		• λ_D: 危险失效率，可分为:
		  • λ_{DD}: 通过诊断功能检测到的危险失效率
		  • λ_{DU}: 未检测到的危险失效率
			➜ 3-96
			➜ 3-98

β 因子		对共因失效的易感性 (IEC 62061) ➜ CCF	➜ 3-97 ➜ 3-98
响应延迟时间		使触点延迟响应的时间。对于带响应延迟的开关放大器，该时间可变化调整。	
响应时间		发生导致传感器单元响应的事件和输出信号切换装置 (OSSD) 实现关闭状态之间的最长时间	➜ 3-47
AOPD	Active opto-electronic protective device (**有源光电防护设备**)	防护装置利用光电发射器件制造的光辐射，通过接收装置检测到位于指定保护区域内 (就光电传感器而言: 位于光束轴线上) 的不透明目标遮挡后产生的反射光。(CLC/TS 61496-2) 在 DIN EN 692“机械压力机”、EN 693“液压机”和 EN 12622“液压折弯机”中，使用缩写 **AOS** 作为 **AOPD** 的同义词。	➜ 3-30
AOPDDR	Active opto-electronic protective device responsive to diffuse reflection (**响应漫反射的有源光电防护设备**)	防护装置利用光电发射器件制造的光辐射，通过接收装置检测到位于位于二维保护区域内的目标后产生的反射光。(CLC/TS 61496-2)(IEC/TS 61496-3, CLC/TS 61496-3)	➜ 3-31
分辨率/传感器检测能力		使电敏防护设备 (ESPE) 响应的传感器参数极限。由制造商确定。	➜ 3-31
B_{10d}		在此周期数之后，10% 的元件会导致可能带来危险的故障 (例如针对气动和机电组件)	➜ 3-17 ➜ 3-93
BGIA		➜ IFA	
ESPE	Electro-sensitive protective equipment (**电敏防护设备**)	协同工作实现通道保护或存在性检测且至少包括以下元件的设备和/或组件的集合 (IEC 61496-1/EN 61496-1): • 传感器元件 • 控制或监控装置 • 输出信号切换装置 (OSSD) 其用于保护靠近有身体伤害风险的机器和设备的人员。其促使机器或设备在人员可能陷入危险状态前采取安全状态。	➜ 3-29
CCF	Common cause failure	共因失效: 不同单元因单一事件而失效，而且这些失效相互之间没有因果关系	➜ 3-16 ➜ 3-95 ➜ 3-97 ➜ 3-98
CENELEC	Comité Européen de Normalisation Electrotechnique	欧洲电工标准化委员会。负责协调欧盟范围和整个欧洲经济区内的电工标准。 ➜ www.cenelec.eu	➜ §-7
CLC		CENELEC 所采用的标准前缀	➜ §-7

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

缩写/概念		解释	索引
DC	Diagnostic coverage	诊断覆盖率: 衡量诊断有效性的尺度, 可表示为检测到的危险失效的失效率与所有危险失效的失效率之间的比	→ 3-95 → 3-96 → 3-98
d_{op}		平均工作时间, 以天每年为单位	→ 3-93
E/E/PES	Electrical, electronic and programmable electronic safety-related systems	电气、电子和可编程电子安全相关系统 (IEC 62061/EN 62061)	
EDM	External device monitoring	外部设备监控: 电敏防护设备 (ESPE) 用来监控布置在 ESPE 之外的控制元件状态的方法 (IEC 61496-1/EN 61496-1)。EDM 不限于配合 ESPE 使用。	→ 3-73 → 3-93 → 3-98
EFTA	European free trade association	欧洲自由贸易联盟, 由欧洲国家建立的国际组织	→ §-7
元件安全功能		安全功能的一部分, 由安全相关元件 (如执行元件) 执行以降低风险	→ 3-76
EMC	Electromagnetic compatibility	→ EMC	
EMC	电磁兼容性	电气设备在其电磁环境中令人满意地运行并且不过分影响该环境内其他设备的能力	→ 2-9 → 3-95 → 3-97
ESPE	Electro-sensitive protective equipment	→ ESPE	→ 3-29
FIT	Failure in time	在 10^{-9} 小时内的失效率 → $\lambda = 1 \times 10^{-9}$ 1/h	→ 3-16
FMEA	Failure mode effects analysis	失效模式及影响分析。用于分析失效影响的方法 (IEC 812/EN 60812)。	→ 3-17
功能安全		总体安全的一部分, 与依赖于 → SRECS 的正确工作、其他技术的安全相关系统和外部风险降低装置的机器与机器控制系统有关	→ 3-1 → 3-85
HFT[n]	Hardware fault tolerance (硬件故障裕错)	发生故障或失效时继续执行所需功能的能力 (IEC 62061/EN 62061)	→ 3-96
检测人员是否存在		设备的次级防护装置可从评估从地面接近, 且防止在内部有操作人员期间启动机器 (安全功能: 防止启动)	→ 3-50 及后续各页
h_{op}	Operating hours	平均工作时间, 以小时每天为单位	→ 3-93
IFA	Institut für Arbeitsschutz	德国法定意外保险协会的职业安全健康机构。 截至 2009 年: BGIA。	→ §-12
投放市场		根据产品安全法: 首次在市场上流通	→ 6-1
类别		就其耐故障性和发生故障时的后续行为将控制系统的安全相关部件分类	→ 3-18 → 3-89
拉姆达 λ		→ λ	→ 3-96 → 3-98
光幕		分辨率 ≤ 116 mm 的 AOPD	→ 3-29 → 3-47
最小距离		防护设备与危险区域之间的计算距离, 目的是防止在危险的机器功能结束前人员或身体部位进入危险区域	→ 3-47 及后续各页
MTTFd	Mean time to failure	出现危险失效前的平均时间期望值 (ISO 13849-1/EN ISO 13849-1)	→ 3-90
屏蔽		屏蔽功能。暂时自动屏蔽由控制系统的安全相关部件执行的一项或多项安全功能 (IEC 61496-1/EN 61496-1)	→ 3-38
N/C	Normally Closed	常闭	→ 3-21
N/O	Normally Open	常开	→ 3-45 → 3-73

缩写/概念		解释	索引
n_{op}	Numbers of operation per year	取自 EN ISO 13849-1 的文本: 年平均致动次数 (ISO 13849-1/EN ISO 13849-1) $n_{op} = \frac{d_{op} \times h_{op} \times 3600\frac{s}{h}}{t_{cycle}}$ d_{op} 年平均工作天数 h_{op} 日平均工作小时数 t_{cycle} 部件连续两次循环开始之间的平均时间, 以每循环秒数为单位	→ 3-93
OSSD	Output signal switching device (输出信号切换装置)	电敏防护设备 (ESPE) 的一部分, 与机器控制系统相连并在传感器单元于正常运行期间响应时切换到关闭状态	→ 3-18 → 3-66
PDF	Proximity device with defined behaviour under fault conditions	在故障条件下具有确定功能的接近开关	
PFHd	Probability of dangerous failure per hour	平均每小时危险失效率 (1/h)	→ 3-85 → 3-94 → 3-95
PL	性能等级	离散等级, 控制系统的安全相关部件在可预见的条件下执行安全功能的能力 (ISO 13849-1 / EN ISO 13849-1)	→ 3-86
测试棒		不透明的圆柱形元件, 用于测试 AOPD 的检测能力 (IEC/TS 61496-2, CLC/TS 61496-2)	
复位		将防护设备复位到受监控状态。 • 通过单独的、需要手动操作的设备(如复位按钮)进行手动复位。 • 仅在特殊情况下允许通过防护设备自动复位:不得使人员可以在不触发防护设备的情况下在危险区域内停留或必须确保无人在复位时和复位后在危险区域内停留。	→ i-16 → 3-65
保护区域		制造商所定义的测试对象被电敏防护设备 (ESPE) 检测到的区域。 • 安全光幕:保护区域在发射与接收单元之间。通过保护区域高度和保护区域宽度来定义。 • 安全激光扫描器:保护区域防护机器或车辆的危险区域。通过所用设备的扫描范围、扫描角度、响应时间和分辨率确定(参见技术参数)。	→ 3-47
传感器检测能力/分辨率		使电敏防护设备 (→ ESPE) 响应的传感器参数极限。由制造商确定。	→ 3-32
SFF	Safe failure fraction (安全失效系数)	安全失效占不会导致危险失效的 子系统的总失效率的比例 (IEC 62 061/EN 62 061)	→ 3-96
安全功能		机器的功能, 如果该功能失效将直接导致风险提高 (ISO 12100)。安全功能由控制系统的安全相关部件执行 (SRP/CS)。	→ 3-2
SIL	Safety Integrity Level	安全完整性等级: 离散等级 (三个可能等级之一), 指明分配给安全相关系统的安全功能的安全完整性, 其中安全完整性等级 3 为最高级, 安全完整性等级 1 为最低级 (IEC 62061/EN 62061)	→ 3-96
SILCL	SIL claim limit	SIL 要求限度 (就子系统而言) : 在结构限制和系统安全完整性上, → SRECS 子系统所能宣称的最高 SIL (IEC 62061/EN 62061)	→ 3-85 → 3-97 → 3-99
SRECS	Safety-related electrical control system	机器的电气控制系统; 若其失效, 将导致一种或多种风险立即上升	
SRP/CS	Safety-related part(s) of control system	控制系统的安全相关部件: 响应与安全相关的输入信号并产生与安全相关的输出信号的控制系统部件 (ISO 13849-1/EN ISO 13849-1)	→ 3-85
T_{10d}		部件的工作时间限制。10% 的元件发生危险失效前的平均时间。 $T_{10d} = \frac{B_{10d}}{n_{op}}$ 所确定的受磨损部件的 MTTFd 仅在该时间内适用。	
VBPD	Visual based protection device	基于图像评价的防护装置, 如安全摄像系统	

8020567/2017-08-22(GCN 2021-07-01)
如有更改, 恕不另行通知

缩写/概念	解释	索引
联锁	联锁装置是旨在防止机械元件在特定条件下运行的机械、电气或其他装置。	→ 3-21 及后续各页
重启	使机器恢复运行。触发保护功能或发生故障后，可对防护设备进行复位，以便随后使机器重启。	→ 3-4 → 3-55 → 3-75
重启联锁	在机器工作循环的危险部分期间触发安全功能后或更改机器的操作模式或致动方式后或切换到机器的启动控制装置后，用于防止机器自动重启的装置 (IEC 61496-1/EN 61496-1)。 • 操作模式包括: 点动、单次行程、自动 • 启动控制装置包括: 脚踏开关、双手控制装置、依靠 ESPE 的传感器功能的单次打断 PSDI 模式和双次遮光 PSDI 模式触发装置 • 重启联锁 (RES): 当至少一条光束被中断时，机器停止且重启联锁 (RES) 启动。其确保在光路畅通的情况下按下再松开复位按钮后，机器才能重新启动。	
强制打开	开关正向打开表示在执行元件与开关元件之间必须进行形状配合的力传递。执行机构的设计必须确保在发生机械失效时，例如当弹簧断裂或触点磨损时，接触处也能可靠断开并在致动状态下保持断开 (IEC 60947-5-1/EN 60947-5-1)。	→ 3-24

共同作者和致谢

SICK AG 及编辑团队衷心感谢参与本指南编写的所有共同作者，他们或是指出了必要的修正，或是提供了照片或文本。本指南前一版的众多读者也通过他们高水平的专业知识和实践反馈为这次成功更新做出了贡献。感谢您的支持!

在此特别感谢
（按字母顺序排列）：

- Tilmann Bork 博士, Festo AG & Co. KG
- Pablo Ruiz, Festo AG & Co. KG
- SEW-EURODRIVE GmbH & Co KG

8020567/2017-08-22(GCN 2021-07-01)
如有更改，恕不另行通知

8020567/2017-08-22 · SKOM7ITL (2018-03) · (GCN 2021-07-01)Pre USmod zh47

SICK 概况

SICK 是工业用智能传感器和传感技术解决方案的主要制造商之一。SICK 在全球范围内拥有 8,000 多名员工和 50 多家子公司和股权投资机构以及众多的代理机构，方便客户随时随地与我们取得联系。独特的产品和服务范围为安全有效地控制流程创造更好基础条件，以防止发生人身事故及避免环境污染。

我们在诸多领域拥有丰富的经验，熟知其流程和要求。我们可以使用智能传感器为客户提供其所需。在欧洲、亚洲和北美洲的应用中心，我们会根据客户的需求测试并优化系统解决方案。SICK 是值得您信赖的供应商和研发合作伙伴。

全面的服务更加完善我们的供货：SICK LifeTime Services 在机器整个寿命周期中提供帮助并保证安全和生产率。

即“Sensor Intelligence”。

遍及全球：

澳大利亚、比利时、巴西、智利、中国、丹麦、德国、芬兰、法国、英国、印度、以色列、意大利、日本、加拿大、马来西亚、墨西哥、新西兰、荷兰、挪威、奥地利、波兰、罗马尼亚、俄罗斯、瑞典、瑞士、新加坡、斯洛伐克、斯洛文尼亚、 西班牙、南非、韩国、台湾地区、泰国、捷克共和国、土耳其、匈牙利、美国、阿联酋、越南。

联系人以及其它分公司所在地 → www.sick.com

SICK
Sensor Intelligence.