Allen-Bradley

Guardmaster®

与安全有关的机械控制系统

原理、标准与执行

安全操作手册3

安全操作手册3 - 与安全的有关的机械控制系统 / 原理、标准与执行

LISTEN. THINK. SOLVE.℠

Rockwell Automation

www.rockwellautomation.com

动力、控制和信息解决方案总部

美洲地区：罗克韦尔自动化公司，南二大街 1201 号，密尔沃基市，威斯康辛州，53204-2496 美国，电话：(1) 414.382.2000，传真：(1) 414.382.4444
欧洲/中东/非洲：罗克韦尔自动化公司，Vorstlaan/Boulevard du Souverain 36, 1170 布鲁塞尔，比利时，电话：(32) 2.663.0600，传真：(32) 2 663 0640
亚太地区：罗克韦尔自动化公司，香港数码港道 100 号数码港 3 座 F 区 14 楼，电话：(852) 2887.4788，传真：(852) 2508.1846

出版号：SAFEBK-RM002A-ZH-P — 2009年2月

目录

EU指令与法规

本部分内容作为欧洲联盟内与机械安全，尤其是防护与保护系统有关的任何人员的指南。本指南适用于工业设备的设计与受用人员。

为了在欧洲经济区(EEA)(该组织目前包括所有的EU成员国以及3个其他国家)促进市场开放这一理念，所有成员国应在机械及其使用的基本安全要求方面进行相关立法。

禁止向EEA成员提供将不符合这些法定要求的机械，或者EEA成员之间互相提供以上机械。

目前有多个适用于工业机械设备安全的欧洲指令，但最具直接关系的为以下两条指令：

1 机械指令

2 工人工作时工作设备的使用指令

这些指令中的基本健康与安全要求(EHSR)可用来确认工作设备使用指令中有关设备安全的内容，因此这两个指令有着直接的关系。

本部分将介绍这两个指令的各个方面。我们强烈建议在EEA内部以及其他一些欧洲国家内参与设计、供应、购买或者使用工业设备的人员，或者向这些国家提供、购买工业设备的人员应了解各种要求。如果不能满足这些指令要求，绝大多数机械供应商或者用户在这些国家中会被完全禁止供应或者操作机械。

还有其他一些与工业安全有关的欧洲指令。这些指令中的大多数专门针对某一应用领域，因此不属于本部分。但必须指出，如果这些指令与工业安全有关系，则同时也必须满足这些指令。这一点很重要。例如：低压标准 - ATEX指令。

机械指令

该机械指令(98/37/EC)涉及新机械以及包括安全部件在内的其他设备的供应。不能按照该指令要求供应机械即为违法。也就是说，必须满足该指令附录1中EHSR广泛要求；必须进行评估，确认是否符合标准；必须出具“符合标准声明”；必须加盖CE标志。

在机械上使用CE标志

该指令中有关机械的主要规定于1995年1月1日完全生效，有关安全部件的主要规定于1997年1月1日完全生效。允许有两年的过渡期。在此期间，既可以执行现有的国家规范，也可以遵守新指令规定。设备制造商、进口商或者终端用户有责任确保所供的设备满足该指令的各项要求。

机械指令的新版本2006/42/EC已经出版。新版本指令将在2009年底取代现有指令的各项规定。在过渡期间，现有指令完全有效。下面将介绍现有的98/37/EC指令。不过在新指令，在有关大多数类型机械的基本要求方面的变化很小。

健康与安全的基本要求

机械必须满足EHSR要求

该指令列出了在适用情况下各种机械必须遵守的健康与安全基本要求(也称作EHSR)。这样做是为了确保机械安全，确保按照以下要求设计、制造机械，即在整个使用期间内对机械进行调节、维护时不会使人员处于危险状态。

该指令也提供消除危险的各种分级措施：

(1)本安型设计 - 如有可能，设计本身就能防止各种危险。

如以上不可行，**(2)可采用另外保护装置**，如具采用有联锁接入点的防护罩、光幕、传感垫等非金属屏障。

如果采用上述方法后还存在危险，则必须通过**(3)个人防护装备和/或培训消除这些危险。**机械供应商必须规定什么样的措施最合适。

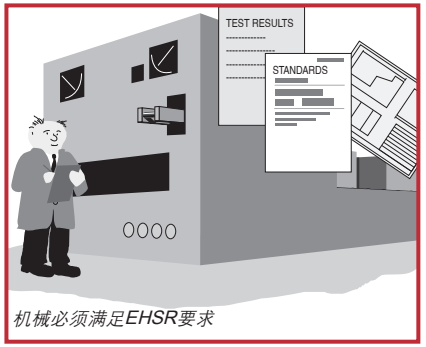
制造、运行时应采用合适的材料。应提供合适充足的照明与搬运设施。控制机构与控制系统必须安全可靠。各种机械不得意外启动，应配备一个或者多个紧急停止按钮。对于上游工艺或者下游工艺可能影响机械安全的复杂装置，必须给予充分考虑。电源或者控制回路失效不应造成危险情况。机械应能保持稳定，并能承受可预见的各种应力。机械上不应有可能造成伤害的边缘或者表面。

必须采用防护罩或者防护装置来防止危险，如移动部件。这些防护部件必须结构坚固，不易忽略。固定式防护罩必须采用通过工具才能拆除的安装方法。活动的防护罩应采用联锁机构。可调式防护罩应能在没有工具的情况下随时进行调节。

必须防止电源或者其他能量源造成的危险。必须将温度、爆炸、噪音、振动、粉尘、气体或者辐射造成的危险降至最低。必须提供便于维护与维修的合适设施设备。必须提供充足的指示与警告装置。必须随设备提供有关正确安装、使用、调节等的说明书。

一致性评估

设计人员或者其他负责机构必须出示证据，证明机械满足EHSR的要求。证明文件中应包括如试验结果、图纸、技术规格等所有相关信息。



机械必须满足EHSR要求

在欧盟官方期刊(OJ)中，机械指令中列出的欧盟标准(EN)的推定合格性终止日期在还未到期时，那么推定与EHSR中的某些要求的终止日期一致(OJ中列出的许多最新标准均包括能够认定该标准涉及EHSR的交叉引用)。

所以，如果设备符合现有的欧洲协调标准，那么就可大大简化证明该设备满足EHSR要求的工作，制造商也会从不断加强的法律确定性中获益。然而，这些标准不属于法定要求标准，并且通过替代性方法证明一致性可能是一个极其复杂的问题，所以只是强烈建议使用这些标准。这些标准支持机械指令并由CEN(欧洲标准委员会)联合ISO，CENELEC(欧洲电气标准委员会)联合IEC编制而成。

必须进行彻底的风险评估并作相应记录，确保消除所有潜在的机械危险。同样，机械制造商有责任确保其机械满足全部的EHSR要求，即使是那些欧洲协调标准未能解决的危险。

技术文件

负责宣布一致性的人员必须确保提前准备好以下文件以供检查。

技术文件包括：

1. 包括控制回路图在内的设备总图。
2. 检查设备是否满足EHSR要求的详细图纸、计算注释等。
3. 下列文件：
   - 与设备相关的EHSR要求。
   - 适用的欧洲协调标准。
   - 其他适用标准。
   - 技术设计规范。
4. 为消除该设备带来的潜在危险而采取的方法介绍。
5. 如需要，由认证机构(实验站)或者实验室出具的技术报告或者认证书。
6. 如果声明满足欧洲协调标准，则出具说明试验结果的相关技术报告。
7. 设备说明书的复印件。

对于系列生产的情况，需要详细的内部措施(如质量系统)以确保生产的所有设备符合一致性要求：

- 制造商必须就设备部件、配件或者整套设备进行必要的研究或者试验，以确定通过设计、制造过程后设备能否安装、能否安全投入使用。
- 技术文件不必单独永久存在，但必须能在合理时间内将其汇集在一起。技术文件必须在制造最后一台设备后的10年内有效。如果不能根据执行机构的具体要求提供技术文件，可能会成为怀疑一致性的依据。

技术文件中不必包括详细的计划或者其他有关设备制造所需的预装组件的专门信息，除非这些文件是验证设备是否满足EHSR要求所需的必要文件。

附录IV“机械”的一致性评估

一致性评估

某些类型的设备需要采用特殊措施。这些设备在该指令的附录IV中列出，包括了如木材加工机械、压力、注塑成型机、地下设备、升降机等危险性机械。

附录IV中还包括一些安全部件，如光幕、手动控制单元。

对于附录IV中满足欧洲协调标准的机械设备，有三种步骤可供选择：

1. 将技术文件发给指定机构，指定机构确认收到技术文件并进行保存。*注意：采用该步骤时不对技术文件进行评估。供日后出现问题或者出现不一致性申诉时作为参考。*
2. 将技术文件发给指定机构，由指定机构验证是否正确应用了欧洲协调标准并出具所提供技术文件充分的证明。
3. 向指定机构(实验站)提供一台设备样机进行EC类型检验。如果通过检验，则给该设备出具EC类型检验证书。


指定机构进行检验

对于附录IV中不符合某个标准或者没有相关的欧洲协调标准的设备，则必须由指定机构(试验j机构)对该机械样机进行EC类型检验。

指定机构

指定机构组成的网络遍布整个EEA以及一些其他国家。他们之间相互沟通，为共同的标准进行工作。指定机构由政府(而非行业)指定，有关详细的组织结构以及各指定机构的状态可登陆以下网站查找：

http://europa.eu.int/comm/enterprise/newapproach/legislation/nb/en 98-37-ec.pdf.

EC类型检验

为便于进行EC类型检验，指定机构需要技术文件并能接触到待检验设备。指定机构将检查该设备是否按照其技术文件制造，是否满足适用的EHSR要求。如通过检验，则指定机构出具EC类型检验证书。如果某个指定机构拒绝出具证书，还必须通知其他指定机构。

EC一致性声明程序

CE 负责人员必须起草一份EC一致性声明，并在提供的所有设备商使用CE标志。所供设备也必须随机附带EC一致性声明。

注意：安全部件应具有EC一致性声明，但对于机械指令来讲，安全部件不需要CE标志(尽管为了说明这些部件符合其他指令要求而采用CE标志，如EMC和/或低压标准)。

CE标志表示设备负荷所有适用的欧洲指令并且相应的一致性评估程序结束。如果设备未满足所有适用指令中的EHSR要求并且实际上也非安全，则在设备上使用CE标志是一种违规行为。在设备上使用容易与CE标志混淆的标志也是一种违规行为。

EC合并声明

如果所供设备用于日后与其他设备部件组成一台完整的机械，则相关负责人应随设备附上合并声明(而不是一致性声明)。同时也不适用CE标志。该声明应说明只有在声明该设备并入后的机械满足一致性要求后才可将该设备投入使用。

但是以上规定不适于独立发挥作用的设备或者会改变机械功能的设备。

Maykit Wright 有限公司
一致性声明

涉及以下标准：

欧洲机械标准 98/37/EC，（也应包括任何与该机械有关的其他标准，如 EMC 标准）

公司：

Maykit Wright 有限公司
Main Street
Anytown Industrial Estate
Anytown, England AB1 2DC
电话：00034 000890. 传真：00034

机械：肉类包装机
类型：Vacustarwrap 7D
序列编号：00516

符合标准
(所有相关的欧洲协调标准。如适用，还包括任何国家标准与规范。)

如果该机械在附录 IV 的范围内，则必须包括以下内容：

– 验证机构的地址与名称，类型检验证书编号，或者

– 起草技术文件充分证书的验证机构的名称与地址，或者

– 接受技术文件的验证机构的名称与地址。

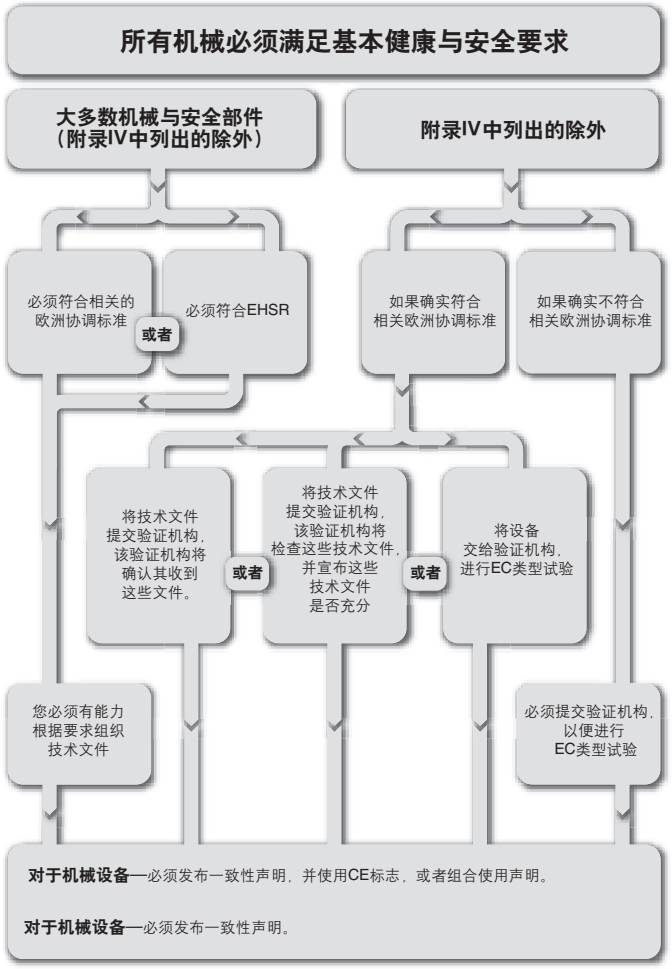
在此声明上述机械符合欧洲协调标准 98/37/EC 标准中有关基本健康与安全要求的规定。

G. V. Wright

G.V. Wright, 总经理
于 2003 年 1 月 17 日发布

自行认证的机械的一致性声明示例

工作设备的使用指令



机械指令概述

与机械指令针对供应商相反，该指令(89/655/EEC，经过95/63/EC、2001/45/EC修正)则是针对机械使用者。该指令涵盖所有工业领域，规定了员工的一般职责以及有关工作设备安全的最低要求。所有EEA国家正为实行该指令加强各自的立法模式。

通过了解工作设备的使用指令在国家法令中的实施情况，我们很容易明白该指令要求的含义。例如，我们可看一下该指令在英国的实施情况。该指令在英国的名称为工作设备的规定与使用规范(通常缩写为P.U.W.E.R)。该指令在各个国家的实行模式可能不同，但其效力不会改变。

规范1 - 10

这些规范给出了该指令涉及的设备与工作场所类型的详细情况。

这些规范规定了雇主的一般职责，如制定有关工作的安全制度，提供必须保持正确维护、合适、安全的设备。必须向机械操作人员提供安全使用机械的正确信息，提供与此相关的培训。

在1993年1月1日后提供的新机械(与来自EEA以外的二手机械)应满足任何相关的产品指令，如机械指令(会受过渡期安排的影响)。来自EEA内部的二手设备首次运抵工作现场时，必须立即满足安全规范11到24的规定。

注意：经过明显大修或者改造的现有机械或者二手机械应按照新设备分类，因此在这些设备商进行工作时必须满足机械指令(即使是公司内部使用)。

规范5“工作设备的合适性”是该指令的核心部分，该规范强调雇主有责任进行正确的风险评估。

规范6“维护”要求正确维护机械。该规范要求必须准备日常与有计划的预防性维护计划表。建议进行记录并保持最新状态。尤其在设备维护、检查有助于保持保护装置或者保护系统的安全完整性的情况下，进行记录尤为重要。

规范11 - 24

这些规范涉及特定的设备危险以及相关保护布局。

对于现有1993年1月1日以前投入使用也未经过改造的机械，这些规范直到1997年1月1日才完全实施。对于其他机械，则立即实施了这些规范。但是，如果设备满足相关的产品标准，如机械标准，那么这些设备将自动满足规范11到24的要求。这是因为这些标准与的EHSR要求本质上类似。

尤其值得关注的是规范11，该规范对保护措施划分了等级，具体如下：

1. 固定式封闭防护罩。
2. 其他防护罩或者保护装置。
3. 保护器具(夹具、固定件、推杆等)。
4. 提供信息、说明、监督与培训。

应最大可能的实际情况使用这些措施，并且通常需要组合使用两个或者多个上述措施。

美国规范

本部分将介绍在美国使用的一些工业机械防护安全规范。这仅仅是一个起点，读者们必须深入调查各自特定应用情况下的各种要求，以确保其设计、使用、维护程序与规程满足自身需要，满足国家的、当地的标准、规范的要求。

在美国由许多组织机构促进工业安全的发展。这些机构为：

1. 各个公司，他们使用已经制定的各种要求，同时也制定内部要求。
2. 职业安全与健康管理局(OSHA)
3. 工业机构如国家消防协会(NFPA)、机器人工业协会(RIA)与制造技术协会(AMT)以及如罗克韦尔自动化等安全产品、解决方案的供应商。

职业安全与健康管理局

在美国，工业安全领域的主要推动部门之一就是职业安全与健康管理局(OSHA)。OSHA按照美国国会的一个法案于1970年成立。该法案的目的是提供安全、健康的工作环境，保护人力资源。该法案授权劳工部制定适用于各州间贸易的强制性职业安全与健康标准。在某个州、哥伦比亚特区、波多黎各自由联邦、维尔京群岛、美属萨摩亚、关岛、太平洋岛屿托管领土、威克岛、外大陆架土地法中规定的外大陆架土地、约翰斯顿岛、运河区内的工作场所进行招工时适用该法案。

该法案的第5条规定了基本要求。每个雇主应使其每位雇用人员、每个工作场所不会发生造成或者可能造成死亡或者严重身体伤害的各种已知危险。每个雇主应遵守该法案公布的职业安全与健康标准。

第5条同时也规定每位雇用人员应遵守适用于其行动、行为的职业安全与健康标准、按照该法案发布的所有规则、规范、指令。

OSHA法案规定雇主与雇用人员各自的责任。该法案与机械指令很不相同。该法案要求供应商投向市场的机械不会发生危险。在美国，供应商可以销售没有任何防护措施的机械。用户必须为所购机械加装防护措施以使机械安全。虽然这种情况该法案被批准后是一种惯例，但由于在设计机械时加入安全理念比在机械设计、制造后增加防护措施会带来更好的成本效益，所以供应商还是倾向于提供带有防护措施的机械。各种标准都尝试要求供应商与用户在各种要求方面进行沟通，以使所制造机械不仅安全而且具有更高的生产能力。

劳工部一直将任何国家标准、联邦标准作为职业安全或者健康标准颁布，除非颁布此类标准不会提高特定雇用人员的安全或者监健康。

为此，OSHA出版标题为联邦法规汇编29(29 CFR)的各项法规。由OSHA出版的工业机械有关的标准位于29 CFR的第1910部分。这些标准可在www.osha.gov上免费获取。与其他绝大多数自愿执行的标准不同，OSHA标准属于法律规定。

这些标准中与机械安全有关的重要部分如下：

A - 概述
B - 采用、增加已制定的联邦标准
C - 安全与健康的一般规定
H - 危险材料
I - 个人防护器具
J - 一般的环境控制 - 包括锁定/悬挂警示牌
O - 机械与机器的防护罩
R - 特殊行业
S - 电气

一些OSHA标准会引用自愿性标准。通过引用形成的合并后法律效力为，象在邦公报中全部公布后那样处理这些引用材料。当某个国家标准通过引用合并到某一子部分时，也应将该标准视作法律规定。例如，S子部分中引用了被视作美国国家电气标准的自愿性标准NFPA 70。这样，NFPA 70标准规定的各项要求就成为强制性要求。

在子部分J中的29 CFR 1910.147涉及了危险能量的控制问题。这就是通常所说的锁定/悬挂警示牌标准。与之等效的自愿性标准是ANSI Z244.1。该标准要求，在机械上进行维修或者维护时必须切断该机械的电源。这样做的目的就是防止机械意外启动或者通电造成人员伤害。

雇主必须制定一项计划，采取相应措施，在切断机械电源的装置上、在禁止机械或者设备意外通电、启动或者释放存储能量的装置上增加锁定装置或者挂牌，以防止造成人员伤害。

在正常生产运行期间进行的次要工具更换、调节以及其他的次要维修活动如果是日常重复性工作，则不属于本标准范围，并且如果进行这样的工作时采取能够提供有效的保护措施，则这样的工作也属于使用设备进行的生产活动。替代性措施为采用防护装置，如光幕、安全踏垫、门联锁机构以及其他与系统连接的小型装置。那么机械设计者与用户面临的挑战是如何确定“次要”、“日常、重复性与完整的生产活动”。

子部分O涉及“机械与机械防护”。该部分列出了针对所有机械的一般性要求以及一些特殊机械的要求。OSHA成文于1970年，采用了许多当时的ANSI标准。例如，有关机械电源的B11.1标准就作为1910.217标准采纳。

1910.212是机械方面的OSHA总标准。该标准规定，应采用一个或者多个机械防护装置以保护操作人员与机械区域内的其他员工，避开如运行点、处于夹压点、转动部件与飞出的碎屑与火花等带来的危险。如可能，防护罩应安装在机械上。如因为某些原因不能安装在机械上，则应安装在其他地方。但防护罩本身不应产生突发危险。

“操作点”是指在材料被处理前操作人员在机械上实际进行工作的区域。会在操作时对使操作人员造成伤害的机械操作点处应采用防护罩。防护装置应符合任何相关标准。如果没有适用标准，则应按照以下原则设计、制造防护装置，即在操作周期内防护罩能够防止操作人员身体的任何部位暴露在危险区域中。

子部分S(1910.399)规定了OSHA的电气要求。如果一套设备或者一台设备经过国家认可测试实验室(NRTL)的验收、认证、公布、粘贴标签或者确定是安全的，则该套/台设备将得到劳工部助理将认可，并在子部分S的范围内得到批准。

何为设备？这是一个统称，包括用作电气装置的一部分或者与电器装置连接的各种材料、配件、装置、器械、固定件、器具以及类似东西。

何为“公布”？如果设备在满足以下的清单中列出，则该设备为“公布“设备。这种清单应满足的条件为(a)由定期检查此类设备生产的、国家认可的实验室出版，(b)并声明此类设备满足国家认可的标准，或者经过试验证明其在某种特定方式使用时是安全的。

到2006年7月为止，以下公司成为国家认可的测试实验室：

- 应用研究实验室公司(ARL)
- 加拿大标准协会(CSA)
- 通讯认证实验室公司(CCL)
- Curtis-Straus LLC (CSL)
- 电气可靠性服务公司(ERSt)
- Entela, Inc. (ENT)
- FM全球技术 LLC(FM)
- 联锁测试服务 NA 公司(ITSNA)
- MET实验室公司(MET)
- NSF国际(NSF)
- 国家技术系统公司(NTS)
- SGS美国测试公司(SGSUS)
- 西南研究学院(SWRI)
- TUV美国公司(TUVAM)
- TUV产品服务 GmbH(TUVPSG)
- 北美TUV Rheinland公司(TUV)
- 安全检测实验室公司(UL)
- Wyle实验室公司(WL)

一些州采用本州当地的OSHA。二十四个州、波多黎各、维尔京群岛采用经OSHA批准的州计划，并采用当地标准与标准执行政策。但其中大部分内容，这些州还是采用与联邦OSHA相同的标准。不过，有些州采用适用于该主题的不同标准，或者采用不同的标准执行政策。

雇主必须向OSHA报告期事故历史。OSHA将汇编事故率，并将该信息传达给当地办事处，然后利用这些信息确定进行检查的先后顺序。主要检查项目为：

- 紧急危险
- 大灾难与死亡事故
- 雇员的抱怨
- 高危险性行业
- 当地的计划性检查
- 跟踪检查
- 国家或者当地的关注计划

违反OSHA标准的规定会受到罚款。罚款明细如下：

- 严重：每违反一次处罚金额可达7000美元。
- 非严重违反：酌情裁定，但不会超过7000美元
- 再次违反：处罚金额可达70000美元。
- 故意违反处罚金额可达70000美元。
- 因违反规定而导致人员死亡：进一步处罚
- 如不能减少死亡：每天7000元

下表摘自2004年10月到2005年9月的14个主要的OSHA标准。

标准	介绍
1910.147	危险能量的控制(锁定/悬挂警示牌)
1910.1200	危险通讯
1910.212	有关所有机械的总要求
1910.134	呼吸保护
1910.305	接线方法、部件以及通用设备
1910.178	动力工业用车
1910.219	机械动力传输
1910.303	总要求
1910.213	木材加工机械
19102.215	砂轮机械
19102.132	总要求
1910.217	机械动力印刷机
1910.095	职业噪音暴露
1910.023	防护底板与墙壁孔洞

加拿大规范

在加拿大，工业安全采取省一级管理方式。每个省均有自己主张的强制性规范。例如，安大略省制订了职业健康语言安全法，规定了工作场所内相关各方的职责与权利。该法的旨在保护工作中的工人，避免健康与安全危险。该法规定了处理工作场所危险的各种步骤，并且在未能自愿执行其规定的地方加强执行力度。

该法案包括对启用前健康与安全检查的规范851的第7部分。该项检查为针对安大略省范围内任何新造、改造或者修改机械提出的要求，并且要求专业工程师提交相应的报告。

标准

本部分将介绍一些与机械安全有关的国际或者国家典型标准。未能列出全部标准，但将深入介绍什么样的机械安全问题是标准化的主题。

应将本章与第1章同时阅读。

全球的许多国家正在致力于全球各个标准之间的协调。在机械安全领域这种努力尤为突出。全球机械安全标准由两个组织管理：ISO与IEC。地区与国家标准仍将存在并继续支撑当地要求，但在许多国家已经在转向使用ISO与IEC指定的标准。

例如。EN(欧洲标准)标准在整个EEA国家内使用。所有新的EN标准将与ISO与IEC标准一致，并在许多情况下与这两种标准的内容相同。

IEC涉及电工技术，而ISO涵盖所有其他问题。旭东工业化国家属于IEC与ISO的成员。机械安全标准由来自全球许多工业化国家的专家组成的工作组编写而成。

在大多数国家将标准内，标准被视作自愿执行的规定，而规范则具有法律强制性。然而，个标准通常被用作各种规范的实际解释。所以，全世界的标准与规范之间是紧密联系的。

有关全面的标准清单，请登录以下网址查看安全分类：www.ab.com/safety。

ISO(国际标准化组织)

国际标准化组织属于非政府组织，由全球大多数国家的国家标准机构组成(本标准出版时包括157国家)。中心秘书处位于瑞士日内瓦马，进行系统协调工作。ISO在设计、制造机械、更加有效、安全、洁净使用机械方面制定各种标准。这些标准也在各个国家之间的贸易更简单、更公平。

ISO标准可用ISO三个字母表示

ISO机械标准的编写结构形式与EN标准相同，包括三种级别：A、B、C类(将稍后章节中的EN欧洲协调标准)。

有关更多的信息，请登陆ISO网址：www.iso.org.

IEC(国际电工委员会)

IEC编写、出版电气、电子与相关技术方面的国际标准。IEC其在所有成员之间，就所有电工技术标准化以及相关事务(如评估电工技术标准的一致性)方面的推进国际协作。

有关更多的信息，请登陆IEC网址：www.iec/ch

EN欧洲协调标准

这些标准在所有EEA国家为通用标准，由欧洲标准化组织CEN与CENELEC制定。这些标准为自愿执行的标注，但按照这些标准设计、制造设备是证明其满足EHSR的最直接的方法。

这些标准分为3类：A、B、C类标准

A类标准：涵盖适用于所有机械类型的领域。

B类标准：包括2个子部分：
B1类标准：涵盖机械的特定安全与人机工程学领域。
B2类标准：涵盖安全部件与保护装置。

C类标准：涵盖特殊类型或者组别的机械。

应当指出，假定符合C类标准则自动满足EHSR要求。这点很重要。如果没有可用的C类标准，则可通过指定符合相关的部分使用A、B类标准部分或者完全证明满足EHSR要求。

我们可用太阳系做例子说明机械指令与欧洲标准之间的关系。围绕太阳转的行星代表标准，而太阳则代表机械指令。内部轨道表示“A”与“B”类标准。外部轨道表示“C”类标准。

在CEN/CENELEC与如ISO、IEC等机构之间已经达成协作协议。这最终将实现全球标准通用。在大多数情况下，某个EN标准会在IEC或者ISO中有与之对应的标准。通常，两种标准的内容相同，并且在标准前言部分说明任何区域差异。

第2章中列出了一些与机械指令有关的EN/ISO/IEC以及其他国家与地区性标准。如果EN标准在括号中出现，则说明该EN标准与ISO或者IEC标准相同或者非常接近。有关EN机械安全标准的全部标准列表，请登陆以下网址：http://europa.eu.int/comm/enterprise/mechan_equipment/machinery/index.htm.

美国标准

OSHA标准

如可能，OSHA将把国家标准或者已制定的联邦标准作为安全标准公布。通过引用加入的、这些标准的强制性规定(如，所用词汇暗示具有强制性)与第1910部分列出的标准具有同样的效力。例如，国家标准NFPA 70在29 CFR的S子部分附录A中以引用文件列出。NFPA 70是一种自愿性标准，由国家消防协会制定(NFPA)。NFPA 70也被称作国家电气标准(NEC)。NEC标准中的所有强制性要求经过OSHA合并后属于强制性要求。

ANSI标准

美国国家标准协会(ANSI)作为美国私营机构的自愿性标准化系统的管理域协调部门。该协会属于由私营与公营组织的不同选区支持的非盈利性会员制私有组织。

ANSI不制定标准，而是通过在有资格的团体之间达成共识，促进标准制定。ANSI还确保各有资格的团体需遵循一致同意的指导原则、正当程序与公开性。以下是通过联系ANSI可获得的工业安全标准的部分清单。

这些标准被分为应用型与结构型标准。应用型标准规定在机械上如何使用防护装置。具体如，ANSI B11.1提供有关在动力印刷机上使用机械防护装置的信息，ANSI/RIAI R15.06在介绍用于机器人防护的防护罩的使用。

国际防火协会

国家消防协会(NFPA)于1896年成立，其宗旨是通过宣传与火灾、安全问题有关、基于科学的共识性法令与标准、研究与教育，以减少火灾造成的人员伤亡。为实现其使命，NFPA在支持许多标准。与工业安全、安全防护有关的两个重要标准是国家电气标准(NEC)与工业机械电气标准。

国家消防协会从1911年以来就一直作为NEC的资助方。1897年，经过保险、电气、建筑以及相关利益各方的共同努力制订出原始标准文件。NEC从那时起经过了多次更新，且大约每三年修订一次。NEC标准中的第670条涵盖了有关工业机械安全的一些细节内容，并告知用户可参阅NFPA 79中有关工业机械的电气标准。

NFPA 79适用于采用600V或以下标称电压的工业机械上的电气/电子设备、装置或者系统。NFPA 79的目的详细介绍作为工业机械一部分、用于提高生命财产安全的电气/电子设备、装置或者系统的应用情况。NFPA 79于1962年被ANSI正式采纳，在内容上与IEC 60204-1非常相似。

对于OSHA标准未涉及的机械，则要求不会发生造成死亡或者严重伤害的公认危险。这些机械必须的设计与维护必须满足或者超过适用工业标准的各项要求。NFPA 79适用于OSHA标准没有专门涵盖的机械。

加拿大标准

CSA标准反应生产商与用户的全国性共识 - 包括制造商、消费者、零售商、工会与专业组织、政府机构。该标准广泛应用于工商业领域。联邦政府、省、市的各种规范中通常采用该标准，尤其采用健康、安全、建造与建筑、环境领域的内容。

加拿大全国的许多个人、公司以及各种协会自愿利用自己的时间与技术支持CSA委员会工作，通过成为永久性成员支持该协会实现其目标，从而支持制定CSA标准。共有超过7000多个委员会志愿者与2000多个永久性成员一起组成了CSA。

加拿大标准理事会是一家国家标准系统的协调机构，属于不受联邦控制的自治性组织，致力于国家利益范围内的自愿性标准化的发展与提高。

澳大利亚标准

大部分澳大利亚标准与等效的ISO/IEC/EN标准非常一致。

澳大利亚标准有限公司
悉尼Sussex路286号，NSW 2001
电话：+61 2 8206 6000
电子邮件：mail@standards.org.au
网址：www.standards.org.au

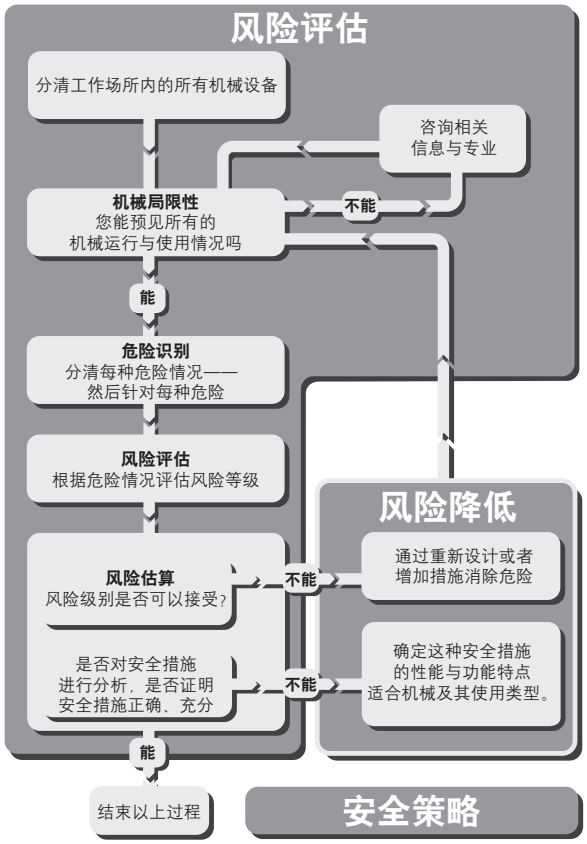
需购买标准副本时：
SAI全球有限公司
悉尼Sussex路286号，NSW 2001
电话：+61 2 8206 6000
传真：+61 2 8206 6001
电子邮件：mail@sai-global.com
网址：www.saiglobal.com/shop

有关全面的标准清单，请登录以下网址查看安全分类：www.ab.com/safety。

安全策略

完全从功能的角度来看，一台机械能够更有效的完成材料处理。但为了使该机械更实际可行，该机械同时又必须是安全的。真正的安全必须是首要考虑因素。

为了制定正确的安全策略，必须执行两个关键的步骤。这两个步骤的联合实施过程如下所述。



风险评估 风险评估的依据是明确机械的局限性、功能及其在使用期限内应进行的各种任务。

降低风险 然后，在必要的情况下降低风险，并按照从风险评估阶段获得的信息选择安全措施。

降低风险采取方式以机械安全策略为依据。

我们需要一个检查清单，同时确保考虑所有的方面，确保在详细内容中不会失去首要原则。应记录整个过程。这样做不仅会确保工作更加彻底，而且其他各方也能检查各种结果。

本部分同时适用于机械制造商与机械用户。机械制造商必须确保其机械使用安全。在机械设计阶段就应开始风险评估。进行风险评估时应考虑需要在机械上进行的所有可预见任务。这种任务型方法在风险评估的早期迭代过程中具有很重要的作用。例如，需要定期调节机械上的活动部件。在设计阶段就应设计能使该过程安全进行的措施。如果在早期设计阶段没有进行此类设计，则在以后阶段很难或者无法执行设计。这样结果是仍旧必须进行活动部件的条件，但必须在要么不安全，要么在无效率的条件下进行，或者在既无安全业务效率的条件系进行。在风险评估期间所有任务得以考虑的机械将会是安全的、更有效的机械。

用户(或者雇用者)需要确保其工作环境下的机械式安全的。即使机械厂家声明机械是安全的，机械使用者仍应进行风险评估，确定该设备在其运行环境中否是安全的。机械通常在其制造商没有预见到的环境下使用。例如，相比在工业工具车间使用的铣床来讲，我们应对教学工厂使用的铣床考虑更多的事项。

我们还应牢记，某个用户公司会拥有两台或者更多独立的机械，并将这些机械和并在某一个工艺过程中。这类用户便是单台机械合并后的组合机械的制造商。

所以，我们现在考虑制定通向正确安全策略的基本步骤。以下步骤可用于工厂现有设备或者新设备。

风险评估

将风险评估作为负担是一种错误认识。风险评估是一个有用的过程。通过风险评估可提供关键信息，使用户或者设计人员在实现安全方面做出合理决策。

目前有许多标准涵盖该主题。ISO 14121：“风险评估原则”与ISO 12100：“机械安全 - 基本原则”包含了全球范围内使用的指导原则。

无论采用何种方法进行风险评估,由多人组成跨部门团队通常比单独某个人考虑的范围更广，做出的决策更好。

风险评估过程是一个重复逼近的过程，将在机械使用期限内的不同阶段进行。在机械使用期限的不同阶段内可用的信息也有所不同。例如。由机械制造商进行的风险评估会考虑机械机构、建造材料的方面，但对其设备的最终工作环境仅作大致的假设。而对于机械使用者来讲，他们没有必要深入考虑技术细节，但会考虑该机械工作环境的门每一个细节。一次重复逼近的结果将是下一次重复逼近的开始。

机械极限判定

该过程包括收集、分析有关机械部件、机构与功能的信息。同时，也应考虑与设备、设备运行环境之间的发生交互作用的、所有类型的任务。这样做的是为了清楚的了解机械以及用途。

如果相互独立的机械通过机械方式或者控制系统连载一起，那么应将这些机械看作是一台独立的机械，除非这些机械按照适当的保护措施经过“区域划分”。

我们应考虑机械使用期限内的所有局限性与各个阶段，其中包括安装、调试、维护、停止使用以及合理预见到的使用不当或者故障导致的后果。

任务与危险识别

必须识别所有危险，并按照其性质、位置一一列出。危险类型包括挤压、剪切、缠绕、部件弹出、气味、辐射、有毒物质、热、噪音等。

应将任务分析结果与威胁识别结果进行对比。对比结果将说明人员遇到危险的可能性，即出现危险情况的可能性。应列出所有的危险情况。根据每个人或者每项任务的特点，相同的危险可能会产生不同的危险情况。例如，一名经过培训的、高度熟练的维护技术人员的表现与一名没有技术、不了解机械的清洁工的表现是不同的。这种情况下，如果列出每种情况并单独解决，则可证明为维护技术人员采取的保护措施与为清洁工采取的保护措施是不同的。如果没有列出各种情况并单独解决，则应采用最严重的情况，并且为维护人员与清洁工采用相同的保护措施。

有时候需要为已经采用适当保护措施的现有机械进行总的风险评估(如，采用联锁防护门的具有危险性活动部件的机械)。这种危险性活动部件是一种潜在危险，会在联锁系统失灵后真正造成危险。除非联锁系统已经过验证(如，通过风险评估或者按照相应的标准进行设计)，则不应考虑该联锁。

风险估算

这是风险评估最基本的方面。我们可采用多种方法处理该主题，在以下几页中将介绍基本原理。

任何会造成潜在危险情况的机械都会导致危险事件发生(如，伤害)。这种风险越大，为此采取措施的重要性就越大。在某种危险情况下，风险很小以至于我们可以将其忽略，允许其存在，但在另一种危险情况下，风险会很大以至于需要我们采取非常措施来防止风险。所以，为了“针对这种风险是否采取措施，采取什么样的措施”做出决策，我们需要对风险进行量化。

就事故造成的伤害严重程度来讲，风险是被单独考虑的。为了对出现的风险进行量化，我们必须考虑潜在危害的严重程度及其出现概率。

我们不主张将以下几页中对风险估算的建议方法作为最终方法，因为具体的环境将决定不同的估算方法。这只是作为一种总的指导原则，用以鼓励采用有条理的记录型结构。

所采用的计分系统并未针对任何特定的应用类型进行调整过，所以该系统可不适于某些应用。目前，我们可采用ISO TR(技术报告)14121-2“风险评估 - 实际指导原则与方法举例”。该报告包括了许多必要的实用指导原则。

以下内容将介绍、说明现有ISO 14121“风险评估原则”中的风险估算部分的内容。

其中考虑了以下因素：

- 潜在伤害的严重程度。
- 潜在伤害出现的概率。

发生概率包括两个因素：

- 暴露频率。
- 伤害概率。

通过单独处理每种因素的方式，我们将为每种因素赋值。

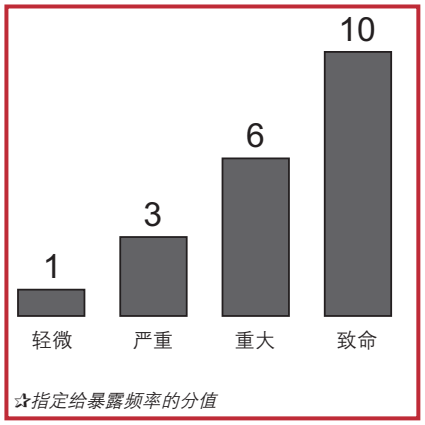
确保仅能获得任何所需数据与专门技术。您所处理的机械可能处于使用期限内的任何阶段，因此避免在每种因素最不利情况下作出过于复杂的决策。

了解基本常识也很重要。各项决策应考虑什么是可行的、实际的、合理的。这样便显示出跨部门小组的价值。

我们应记住，为了实现这一目标我们通常不应考虑任何现有的保护系统。如果风险估算显示需要采用保护系统，那么可以利用本章后部分给出的一些能够确定所需特性的方法。

1. 潜在伤害的严重程度

为此，我们假设事故或者事件是由危险引起的。仔细研究危险会发现可能出现的最严重伤害是什么。请记住：为了考虑伤害的严重程度，我们假设发生伤害是不可避免的，我们仅考虑伤害的严重程度。我们可假设操作人员暴露在危险移动或者过程中。伤害严重程度可按照以下分类进行评估：

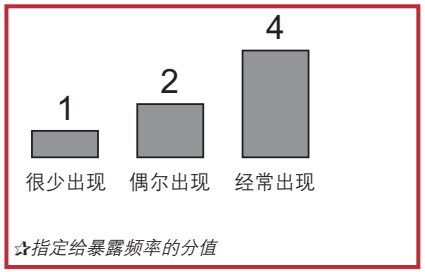


- 致命：死亡
- 重大：(通常不可逆)
  永久性残废，失去视力、截肢、
  呼吸系统损坏...
- 严重：(通常可逆)
  失去知觉、烧伤、划伤...
- 微小：皮肤挫伤、割伤、轻微
  刮伤...

我们将为每种描述赋予一定的分值。

2. 暴露频率

暴露频率可说明操作人员或者维护人员没隔多久就会暴露在危险环境下。暴露在危险环境下的频率可分为以下几类：

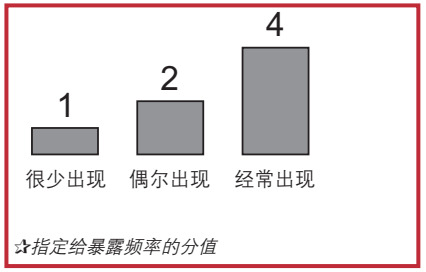


- 经常：每天多次
- 偶尔：每天一次
- 很少：每周一次或者更少

我们将为每种描述赋予一定的分值。

3 伤害概率

我们可假设操作人员暴露在危险移动或者过程中。通过考虑操作人员与机械发生联系的方式以及其他因素(如，机械的启动速度)，我们可将伤害概率分为以下几类：



- 不可能
- 可能
- 很可能
- 一定

我们将为每种描述赋予一定的分值。

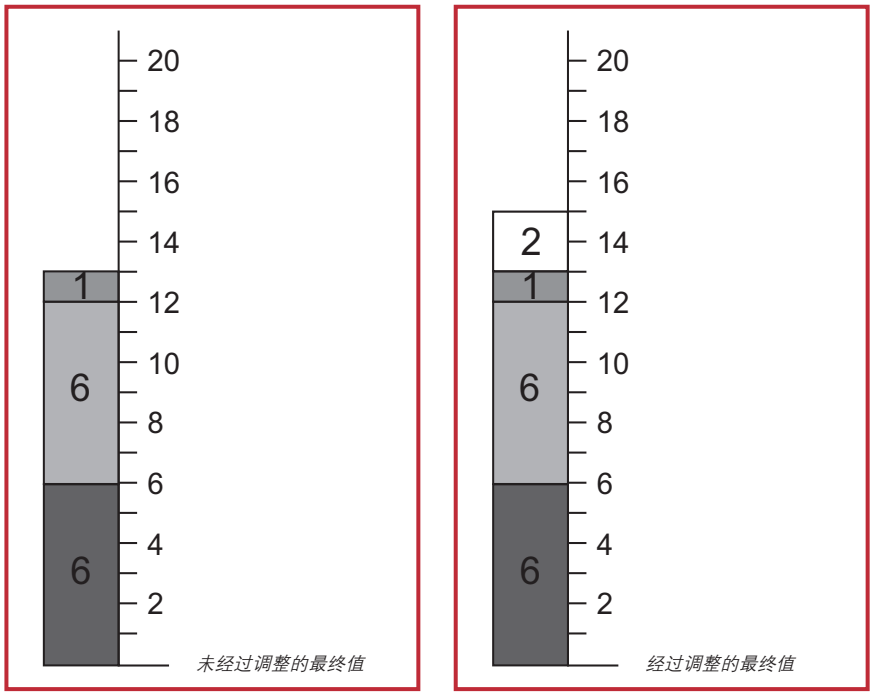
现在，我们为所有的标题分配分值然后相加，得出初始估算值。这三部分相加的和值可达13。但是，我们必须考虑更多的因素。(注释：这种结果没必要以上述图片为依据。)

接下来需要通过考虑其他因素对初始估算值进行调节，具体如下表所列。通常只有机械在其永久性位置固定后才能正确考虑这些因素。

典型系数	建议采取的措施
多个人员暴露在危险中	将严重性乘以人数
电源未完全隔离的情况下在危险区域拖延的时间	如果每次靠近所需的时间超过15分钟，则频率系数增加1分
操作人员技术部熟练或者未经过培训	总分增加
两次靠近之间的时间间隔很长(如，1年)。(尤其在监视系统中，可能存在入侵性与然侧不到的实效情况。)	增加与最大频率系数相等的分值

进行风险估算的其他考虑事项

然后，讲过其他因素的结果与上述总值相加。



降低风险

现在，我们必须依次考虑每台机械及其相应的风险，然后采取措施消除所有风险。

下表所示为建议采用的部分记录程序，该记录程说明了在用机械的所有安全方面。这种记录程序可作为机械用户的指南，但机械制造商或者供应商也可采用相同的原则确认所有设备经过风险估算。这种程序也可作为更详细的风险评估报告的索引。

该程序说明，如果一台机械采用了CE标准，则由于制造商已完成对机械危险估算，因此可以简化记录过程。同时，该程序还说明在该机械上已经采用了所有必要的措施。即使采用CE标志的机械，也可能由于出现制造商未能预见到该设备的应用特点或尤其处理的材料而发危险。

公司 - MAYKIT WRIGHT有限公司
设施 - 工具车间 - 东部工厂。
日期 - 85年8月29日
操作员既能情况 - 熟练。

设备名称与日期	符合标准的情况	风险评估报告编号	事故历史	注释	危险名称	危险类型	需要采取的措施	执行与检查—参考
Bloggs普通车床 序列号 8390726 安装日期1978	没有发布	RA302	无	电气部件符合BS EN 60204标准，采用急停装置（于1989年更换）	防护罩打开时夹具旋转	机械缠绕与切割	安装防护罩联锁开关	11/25/94 J Kershaw 报告编号9567
					切割液	有毒	更换为无毒型	11/30/94 J Kershaw 报告编号9714
					清理木屑	切割	提供手套	11/30/94 J Kershaw 报告编号9715
Bloggs 六角刀架铣床m/c 序列号17304294 制造日期1995 安装日期1995.5	M/c Dir. EMC Dir	RA416	无		移动车床（朝墙的方向）	挤压	移动机器，留出足够的空隙	4/13/95 J Kershaw 报告编号10064

风险评估的措施级别

我们可以考虑三种基本的方法，并依次使用：

1. 尽可能消除或者降低风险(采用本安型机械设计、结构)
2. 对于不能通过设计消除的风险，安装必要的保护系统、采用必要的保护措施(如，联锁防护罩、光幕等)
3. 把由于所采用保护措施的缺陷造成的剩余风险告知用户，说明是否需要进行专门的培训，规定需要采用个人防护器具的情况。

对于来自各个级别的措施，我们应尽可能至上而下注意考虑。这样，我们通常需要组合使用各种措施。

本安型设计

在机械设计阶段，通过仔细考虑诸如材料、接触机械的要求、热表面、传送方法、断点、电压等级因素，我们可以避免许多可能发生的危险。

例如，如果不需要进入有危险区域，则解决方法是将危险限制在机械内部，或者采用某种类型的固定式、封闭型防护装置。

保护系统与措施

如果需要进入危险区域，则确保安全将变得更加困难一些。必须确保只有在机械安全的情况下进入机械区域。此时应采用诸如联锁防护门和/或跳闸系统。选择保护系统还是保护装置将受到机械运行特性的严重影响。当所采用的防护系统会影响机械效率并且未经批准就可被拆除或者忽略时，选择过程极其重要。

这种情况下即使出现故障，机械安全也取决于正确的应用、保护系统的正确运行。

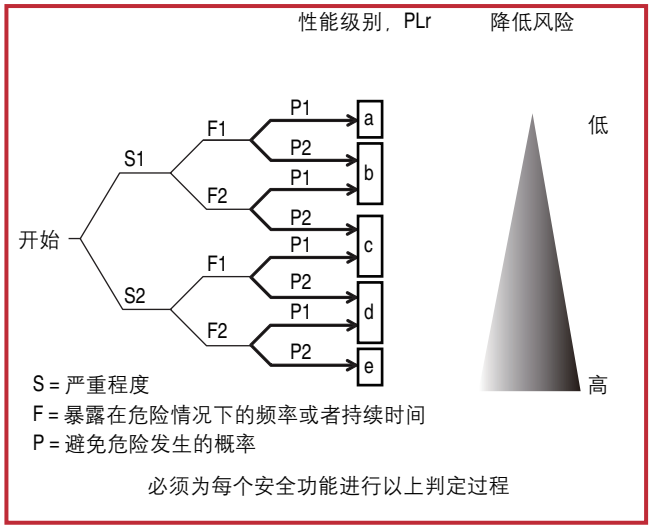
我们现在必须考虑防护系统的正确运行。在每种类型下，可能会按照故障监视、探测或者防止的性能变化程度进行技术选择。

在理想状态下，每种保护系统都是完全可靠的，绝不会造成危险情况。然而在现实世界中，我们会受到当前知识与材料局限性的限制。另一个非常真实的限制就是成本。根据这些因素，很明显需要有主次概念。常识告诉我们，如坚持将安全系统整合到机械上后在最严重情况下只会造成轻微挤压伤害。那么这种认识如同使大型喷气式客机停留在空中一样滑稽。失效后果是截然不同的，因此我们需要一些将保护措施范围与风险估算阶段得出的风险级别联系在一起的方法。

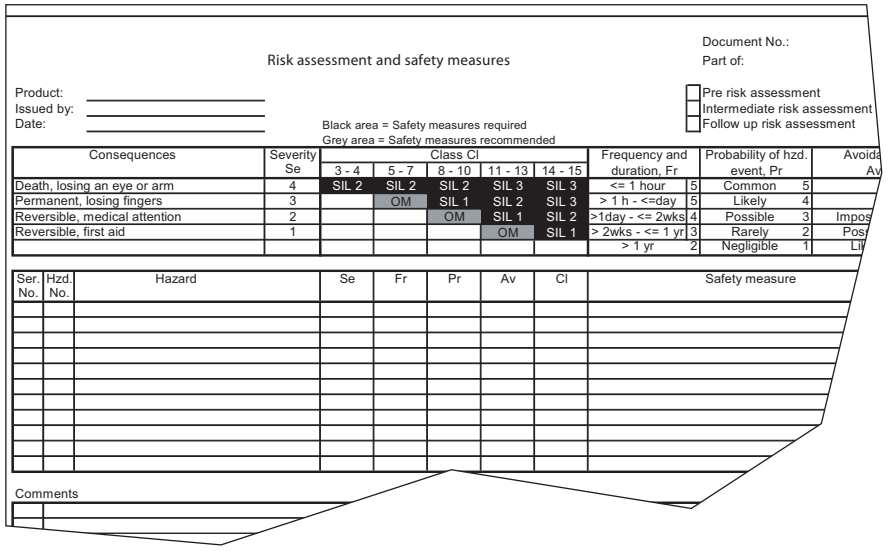
我们必须明白，无论选择哪种类型的保护装置，“与安全有关的系统”中可能含有许多元件，包括保护装置、接线、电源切换装置，有时还包括机械运行控制系统的一些部件。A所有这些元件(包括防护罩、底座、接线等)应具有与其设计原则与技术相对应的、合适的性能特点。ISO 13849-1的修订前版本概括介绍了与安全有关的控制系统部件的不同分类，并在其附录B中给出了风险图。这虽然是一种简单的方法，但在确定保护系统的某些要求方面可提供有用指导。

对于如何规定与安全有关的、可以提供保护措施或者具有安全功能的控制系统，修订版ISO 13849-1与IEC 62061均给出了有用的方法与指导。

EN ISO 13849-1:2008在其附录A中给出了增强型风险图。



IEC 62061的附录中也给出了采用以下表格形式的一种方法。



无论采用上述哪种方法都会得到相同的结果。每种方法都试图考虑到其所属标准中的详细内容。

在这两种情况下极其重要的一点是使用标准中的指导性内容。不能独立使用或者过于简单的使用风险图或者风险表。

估算

选好保护措施并在其使用前，还应再次进行风险估算。这点很重要。这是人们经常忽略的一个过程。可能会出现这种情况，如果我们安装了保护措施，操作人员就会认为他们已经受到全面、彻底的保护，可以避免开始预见到的危险。因为他们对危险已经失去最初的认识，所以他们会用不同的方法干预机械。他们会更频繁的暴露在危险之中，或者例如他们会进入机械中。这就是说，如果保护措施失灵，操作人员就会遭遇比以前预见到的风险更大的风险。这就是需要我们估算的真实风险。所以，需要重复进行风险估算，并在风险估算时考虑人员在干预机械方式上的任何可预见变化。通过该活动结果，我们可以检查是否采用了正确的，实际上是合适的保护措施。更详细的信息，请参阅IEC 62061标准的附录A。

培训、个人防护用具等

操作人员接受必要的有关机械安全工作方法的培训具有很重要的意义。但这不表示可以忽略其他措施。禁止不采取任何措施，而只是告知操作人员不得靠近危险区域(作为一种保护措施)。

另外，操作人员也必须使用如专用手套、眼罩、呼吸器等防护用具。机械设计人员应规定采取何种防护用具。虽然采用个人防护用具不构成主要防护方法，但是可作上述所列措施的补充措施。

标准

许多标准与技术报告中都有有关风险评估的指导内容。有些指导内容可广泛应用，有些则仅限于特定的应用环境。

以下标准中包含了有关风险评估信息。

ANSI B11.TR3：风险评估与降低风险 - 有关机械工具的估算风险、评估风险、降低风险的指南

ANSI PMMI B155.1：包装机械与包装机械有关的机械的安全要求

ANSI RIA R15.06：工业机器人与机器人系统的安全要求

AS 4024.1301-2006：风险评估原则

CSA Z432-04：机械的安全防护

CSA Z434-03：工业机器人与机器人系统 - 总安全要求

IEC/EN 61508：与安全有关的电气、电子、可编程电子系统的功能安全性

IEC/EN 62061：电气、电子、可编程电子控制系统的功能安全性

ISO 14121(EN 1050)：风险评估原则

保护措施与配套设备

当风险评估显示一台机械或者一个工艺过程会导致伤害风险，必须限制或者消除危险。实现该目的的方式将取决于机械与危险本身的特点。安全措施被定义为能够防止靠近危险，或者检测是否靠近危险的方法。防护措施包括如下装置：固定式安全罩、联锁式安全罩、光幕、安全垫、双手控制装置与使能开关。

采用固定式防护罩的防靠近方法

如果危险发生在不需要靠近的某一机械部件上，则应在机械上采用永久性防护罩。这些防护罩必须采用工具才能拆卸。固定式防护罩必须满足以下要求：1)适应所处的运行环境，2)必要时可采用防止喷射装置，3)不会带来危险，如由于锋利的边缘。固定式防护罩与机械接触的地方可能有开孔，或者采用金属网防护罩形成的开孔。

当靠近机械上观察窗的位置时，通过观察窗可以方便的监视机械的性能。选择观察窗材料时以必须小心谨慎，因为与切割液、紫外线发生反应、单纯的老化现象就可逐渐使观察窗材料性能降低。

开孔大小必须以防止操作人员接触到危险为标准。美国OSHA 1910.217中的表O-10、ISO 13854、ANSI B11.19中的表D-1、CSA Z432中的表3均对特定开孔与危险之间的距离给出了指导性规定。

探测是否靠近

防护措施用于检测是否靠近危险。选择检测作为降低风险的方法时，设计人员必须明白：一定要使用完整的安全系统；安全防护装置本身不具有降低风险功能。

这种安全系统通常包括以下三个部分：1)检查是否靠近危险的输入装置，2)处理检测信号、检查安全系统状态然后启动或者停止输出装置的逻辑功能装置，3)控制执行机构的输出装置(如电机)。

探测装置

有多种装置可用于探测人员是否进入或者出现在危险区域。对于具体应用情况，是否能做出最佳选择取决于多个因素。

- 靠近频率
- 危险停止时间
- 完成机械周期的重要性
- 包含弹射物体、液体、雾气、蒸汽等

可在已选好的活动式防护装置上采用联锁，以防止弹射、液体、雾气或者其他类型的危险。这种联锁式防护装置通常用于危险不经常出现的地方。联锁式防护罩也可被锁定，防止人员在机器运行期间或者机器正在停机期间(需要很长时间才能停止)靠近危险。

人员在场感应装置，如光幕、安全垫、扫描机等可快速、方便的靠近危险，所以通常用于需要操作人员频繁进入区域的地方。此类型装置不能提供防止弹射、液体、雾气或者其他类型危险的保护。

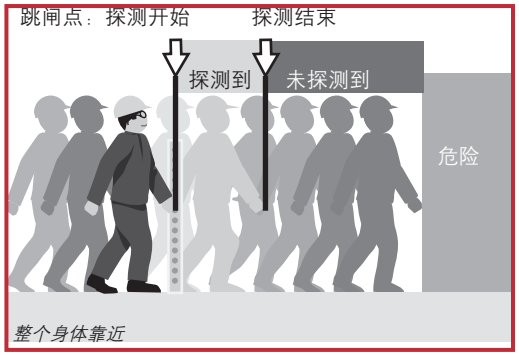
保护措施的最佳选择是能提供最大保护，对机械带来最小影响的一台装置或者一个系统。经验表明难以使用的系统更容易被拆除或者忽略，所以必须考虑机械的所有方面。

人员在场感应装置

确定如何保护某个区域或者分区时，关键是需要十分清楚需要什么样的保护功能。通常，至少需要以下两个功能。

- 当人员进入危险区域时能切断或者禁用动力。
- 危险区域中有人员时能防止启动或者接通动力。

首先，以上功能似乎是一个功能，是一回事。然而，虽然这两个功能很明显有联系并通常由同一设备完成，但实际上是两个独立的功能。为实现第一个功能，我们需要采用某种形式跳闸装置。换句话说，采用能够探测到人体的某一部分越过某一特点后发出信号使动力跳闸的装置。如果该人员能继续通过跳闸点并且装置不再次探测到其存在，那么就不会达到第二个点(防止启动)。



下图所示为人的整个身体靠近时采用垂直安装使光幕作为跳闸装置的例子。在人员进入后再没有其他因素防止联锁式防护门关闭的情况下，这种防护门也可作为仅进行跳闸的保护装置。

如果人员的整个身体不可能靠近危险区域，因此该人员不会继续穿过跳闸点，那么将始终检测到该人员在场，同时达到第二防护点(防止启动)。

在防治人员的某一部分身体进入危险区域的应用情况下，采用同一装置进行跳闸与人员在场检测。唯一不同就是应用类型。

在场检测装置用于探测人员是否在场。此类装置包括安全光幕、单束光线安全屏障、安全垫与安全边缘开关。

安全光幕

简单来讲，安全光幕就是进行在场探测的光电传感器，用于在与机械移动有关的危险情况下保护人员安全，防止收到伤害。光幕也称作AOPD(有源电子保护装置)或者ESPE(电子敏感型保护设备)，可保证达到最佳安全。另外，光幕与机械式防护装置相比更能提高生产力，是一种更经济、更合理的解决方案。在人员很容易的频繁进入运行危险点区域的应用情况下，光幕是最理想的保护措施。

光幕按照IEC 61496-1与-2标准设计与测试。欧洲机械指令的附录IV规定，在光幕进入欧洲共同体的市场前需要第三方机构的认证书。第三方机构测试光幕，确认其满足以上国际标准。安全检查实验室已经采纳了IEC 61496-1标准，将其作为美国标准。

激光式安全扫描仪

激光式安全扫描仪利用旋转镜面探测拱形物上的光脉冲，从而形成一个探测面。物体方位通过镜面的旋转角度确定。采用不可见光反射束的“飞行时间”技术，这种扫描仪也可探测到物体到扫描仪的距离。根据测量出物体方位、距离，激光扫描仪可确定该物体的准确位置。

压力敏感型安全垫

这些装置用于在机械周围的地板区域提供保护。在危险区域附近放置互相连接的安全垫，当有压力施加到安全垫上时(如操作人员的脚步产生的压力)，安全垫的控制单元会切断危险区域的动力源。压力敏感性安全垫通常用在包括多台机械的封闭区域使用 - 如柔性制造单元或者机器人单元。当需要工作人员进入工作单元时(如，进行设定或者机器人“示教”)，如果此时操作人员离开安全区域或者必须进入到设备后面时安全脚垫可以防止危险性动作。

确定安全垫的规格与放置位置时必须考虑安全距离。

压力敏感性边缘开关

这些装置是安装在如工作台或者动力门等会造成挤压、剪切危险的移动部件边缘的柔性边缘条。

如果移动部件撞击到操作人员(反之亦然)，柔性敏感边缘受到压力作用，然后发出切断危险部分动力源的指令。敏感性边缘也认可用于保护存在操作人员被卷入风险的机械。如果操作人员卡在机械中，只要接触到敏感性边缘就会切断机械动力。

有许多技术可用于制造安全边缘。一种广泛应用的技术基本上就是向边缘内插入一种长开关。采用这种方法可用于平直边缘，采用4线连接技术。

光幕、传感器、扫描仪、底板安全垫、敏感性边缘可归到“跳闸装置”类别中。这些装置实际上不会制止靠近危险区域，只是“感知”这种行为。这种装置完全依靠其感知与开关能力提供安全保障。一般来讲，这些装置只适用于那些切断电源后能迅速停机的机械上。因为操作人员可以走入或者直接达到危险区域，所以很明显，移动的机械部件停止所需时间应少于装置跳闸后操作人员到达危险区域所需时间。

有关在场检测的详细内容，可登陆网址www.ab.com/safety。

安全开关

如果不是频繁靠近机械，那么最好采用活动式(可操作式)防护装置。这种防护装置与危险部分的电源采用某种联锁方法，确保只要防护门没关闭就切断危险部分的动力源。采用这种防护方法时需要在防护门上安装一个联锁开关。危险部分的控制电源经过保护单元的开关部分。动力源通常指电源，但也可以是气压或者液压源。探测到防护门运动(打开)时，联锁开关会发出指令直接隔离或者通过接触器(或者阀门)间接隔离危险部分的动力源。

一些联锁开关还配备了锁定装置。这种锁定装置会锁定防护门并且直到机械处于安装状态时才解除锁定。在大多数应用情况下，组合使用活动式防护装置与配备或者不配备锁定功能的联锁开关是一种最可靠、成本最低的解决方案。

目前，许多种类的安全开关供我们选择，具体如下：

- **舌形联锁开关** - 这类装置需要一个在操作时能够插入、抽出的舌形执行机构
- **铰链式联锁开关** - 这类装置放置在防护门的铰链针上，利用防护门的打开动作进行操作。
- **防护装置锁定开关** - 在某些应用情况下，需要将防护装置锁定在关闭状态或者将其延时打开。满足这种要求的装置称作防护装置锁定开关。这类装置适用于具有逐渐停机特性的机械，还能够显著提高大多数类型机械的防护级别。
- **非接触型联锁开关** - 这类装置动作时不需要产生实际接触。这类装置的某些版本加入了编码功能，增强了防改造能力。
- **位置(限位开关)联锁** - 凸轮操作型通常采用正向模式(或者位置)限位开关与线性或者旋转凸轮。这类装置一般用于滑动式防护装置。
- **钥匙安全联锁** - 安全钥匙可执行控制联锁以及动力联锁。联锁装置通过“控制联锁”可以向中间装置发出停止指令，然后由该中间装置停止下一个装置，从而切断执行机构输出的动力。停止指令通过“动力联锁”可直接切断机械执行机构的动力源。

操作人员接口装置

停止功能 - 在美国、加拿大、欧洲以及在国际上，在机械或者制造系统的停止类别描述方面是一致的。

注意：这些类别与EN 954-1(ISO 13849-1)中的类别是不同的。有关更详细的内容，请参阅NFPA79与IEC/EN60204-1标准。停止方法分为以下三类：

0类停止方法通过直接切断机械执行机构的动力实现停止。这种停止方法称作无控制停止。动力切断后，制动所需动力也消失。这样，电机就会自由转动并在一段时间后自然停止。在其他情况下，机械的夹紧装置或松开使材料跌落。这种情况下就需要夹紧材料的动力。不需要动力的机械停止方法也可与0类停止方法配套使用。与1、2类停止方法相比，应优先采用0类停止方法。

1类停止方法是一种受控型停止方法，通过机械执行机构上的动力实现停止。当实现停止后切断执行机构的动力。这种停止方法允许采用动力制动，以实现快速停止危险动作，然后切段执行机构的动力。

2类停止方法属于受控型停止方法，为机械执行机构保留动力。正常的停机方法属于2类停止方法。

这些停止类别必须应用到每一种停止功能上。如通过控制系统中与安全有关的部件对输入做出反应的动作方式实现停止功能，那么应采用0类或者1类停止方法。停止功能必须能抑制相应的启动功能。必须通过风险评估确定每种停止功能应采用何种停止类别。

急停功能

必须按照风险评估结果确定采用0类或者1类的急停功能操作方式。急停功能必须由独立的人为动作启动。执行急停时，必须能抑制所有其他功能、机械操作模式。急停的目的是在不会增加危险的情况下尽可能快的切断动力。

直到最近，急停回路中还需要采用硬连接式电子-机械部件。如IEC 60204-1与NFPA 79各标准的最新更改内容说明安全PLC以及其他形式的电子逻辑装置满足如IEC 61508等标准规定的要求，可用于急停回路。

急停装置

只要操作人员在设备上会处于危险状态，就必须有一种能够快速靠近急停装置的设施。急停装置必须能连续、随时操作。操作盘上必须至少有一个急停装置。如需要可在其他位置采用急停装置。急停装置有多种形式。按钮开关与拉绳开关就是更广泛应用的急停装置类型。急停装置启动后必须处于自锁状态，并且没有自锁时不产生停止指令。复位急停装置时不能造成危险情况。重新启动机器时必须由独立、专门的启动动作完成。

有关急停装置更详细的信息，请参阅ISO/EN13850、IEC 60947-5-5、NFPA79与IEC60204-1、AS4024.1、Z432-94标准。

急停按钮

急停装置被认为是安全防护设备的补充装置。因为急停装置不能防止人员靠近危险区域或者探测得到人员靠近危险区域，所以不能作为主要的防护装置。

实现急停的通常方法是在黄色背景上采用红色蘑菇形按钮，并在出现紧急情况时由操作人员按下(见图4.59)。急停按钮必须数量充足、有计划的分布在机械周围，确保在危险点上总有一个急停按钮在操作范围内。

必须能随时操作急停按钮。在机械的所有运行模式均能使用急停按钮。使用按钮作为急停装置时，必须采用蘑菇(或者便于手掌操作)型、红色并配备黄色背景的按钮。按钮被按下时必须改变状态，同时按钮在按下位置自锁。

在急停按钮上采用的最新技术之一是自检测技术。在急停按钮的背部增加一个触点，用来检测盘面部件的背部是否仍旧存在。这就是所谓的自检测接触功能块。这种功能块包括一个弹簧式触点，并在接触功能块卡入盘面时该触点闭合。图4.60所示为与其中一个直接打开式安全触点串联的自检测触点。

拉绳开关

例如输送机等机械，沿危险区域采用看拉绳开关作为急停装置(如图4.61所示)是一种更方便、更有效的方法。这些装置采用钢丝绳与拉出锁定式开关，以便在任何方向、在钢丝绳的任何长度处来动钢丝绳时会使开关跳闸，切断机械动力。

拉绳开关必须能探测到钢丝绳收到拉力，以及在钢丝绳松弛时受到的拉力。松弛探测功能可确保钢丝绳没有被切断，能随时使用。

钢丝绳长度影响拉绳开关的性能。对于较短的距离，安全开关安装在一端，张紧弹簧安装在另一端。对于较长距离，安全开关必须位于钢丝绳的两端，以确保操作员的一个简单动作就能发出停止指令。钢丝绳拉力不应超过200N(45lbs)或者钢丝绳两个支撑部件间中心点处的距离不应超过400mm(15.75in)。

双手控制装置

双手控制装置(也称作双手动控制装置)是在机械处于危险状态下防止人员靠近危险的通用方法。两个控制装置必须同时动作(在0.5s内)启动机械。这样就可确保操作人员的双手始终处于安全位置(如，均在控制装置上)，因此不会进入危险区域。在危险情况下时，两个控制装置必须同时动作。

双手控制系统主要依靠其控制、监控系统的完整性来探测任何故障，所以按照正确的规范进行这方面的设计具有很重要的意义。双手操作式安全系统已由ISO 13851(EN 574)并入如图所示类型，并与ISO 13849-1中的类别产生联系。在机械方面应用最多的类型是IIIB与IIIC型。下表说明了各类型与各安全性能类别之间的关系。

要求	类型				
	I	II	III		
			A	B	C
同步动作			X	X	X
使用1类(ISO 13849-1标准)	X		X		
使用3类(ISO 13849-1标准)		X		X	
使用4类(ISO 13849-1标准)					X

身体设计间距应能防止不当操作(如，用手、肘)。通过形成距离或者采用遮蔽方法实现该目的。如果两个按钮未被同时释放或者按下，机械不应进入下一个运行周期。这种方式会防止出现两个按钮同时被锁定，使机械继续运行。释放任意按钮时，机械必须停止运行。

由于双手操作控制机构通常会使某些风险暴露，因此使用这种保护方式时应谨慎考虑。双手操作控制机构仅保护使用该控制机构的操作人员。受到保护的操作人员必须能够观察到所有靠近危险的情况。这是因为其他人未受到保护。

ISO 13851(EN574)标准给出了有关双手操作控制机构的指导性内容。

使能装置

使能装置是一种允许操作人员进入正处于危险状态的危险区域的控制机构，但操作人员进入危险区域时必须使使能装置处于工作位置。使能装置采用两位置或者三位置型开关。当执行机构没有动作时，两位置开关断开；执行机构动作时，两位置开关接通。当执行机构未动作时，三位置开关断开(位置1)；保持在中心位置(位置2)时，三位置开关接通；当动作并通过中间位置(位置3)时，三位置开关断开。另外在执行机构从位置3返回位置1的过程中通过位置2时，输出回路不得闭合。

使能装置必须与其他安全功能配套使用。典型示例为将移动模式设置在可控缓慢模式。一旦设置为缓慢模式，操作人员就可手持使能装置进入危险区域。

使用使能装置时，必须有一个专门信号显示使能装置处于工作状态。

逻辑功能装置

逻辑功能装置在控制系统的安全部分发挥核心作用。逻辑功能装置可检查、监视安全系统，允许机械启动或者执行指令使机械停止运行。

我们可采用一整套逻辑功能装置创建一个安全架构，满足机械的复杂性、功能性需要。对于小型机械来讲，如果需要专门的逻辑功能装置实现安全功能，则采用小型硬连接安全监视继电器是最经济的。模块化与配置型安全监视继电器适于需要大量不同类型安全装置以及最小控制区域的情况。对于中型到大型、更复杂的机械，则可采用具有分布式I/O的编程系统。

安全监视继电器

安全监视继电器在许多安全系统中发挥关键作用。这些模块通常由两个或者多个正向导引式继电器以及确保安全功能的补充回路组成。

正向导引继电器属于专门化的“方块”继电器。正向导引式继电器必须满足N50025标准的要求。这种继电器的基本设计功能是防止常闭与常开触点同时闭合。新的设计类型用额定固态输出取代了电动-机械式输出。

安全监视继电器在安全系统中可进行多种检查。这些继电器带电后会对其内部组件进行自检。输入装置激活时，MSR将比较冗余输入的结果。如果检查结果满足要求，则MSR检查外部执行机构。如果外部执行机构正常，则MSR等待复位信号使其输出得电。

安全继电器的正确选型取决于多种因素：所监视的装置类型、复位类型、输出数量与类型。

输入类型

事件发生时，安全防护装置可采用不同类型的指示方法：

触点联锁与急停：机械式触点，具有一个常闭触点的单通道或者具有两个常闭触点的双通道型。MSR必须能够采用单通道或者双通道，能够为双通道结构进行交叉故障探测。

非触点联锁与急停：机械式触点、双通道、一个常开触点、一个常闭触点。MSR必须能够处理各种输入。

输入静态开关装置：光幕、激光扫描仪、固态非触点型装置具有两种源输入，能够进行各自的交叉故障探测。MSR必须能够忽略装置交叉故障探测方法。

压力敏感型安全垫：安全垫会造成两个通道短路。MSR必须能够承受回路重复短路。

压力敏感性边缘开关：一些边缘开关设计类型与4线制安全垫类似：一些边缘开关采用可以改变电阻的两线制。MSR必须能够探测到短路或者电阻变化。

电压：运行期间测量电机反电动势。MSR必须能够承受高压，并能在电机减速旋转时探测到低压。

停止运动：MSR必须能探测到来自不同的、冗余传感器的脉冲流信号。

双手控制装置：MSR必须能够探测不同常开与常闭输入，并能提供0.5s定时与后续逻辑功能。

由于上述装置具有不同的电气特性，安全监视继电器必须采用专门设计与这些类型的装置连接。一些MSR可以连接不同类型的输入。但是，一旦选定防护装置，MSR就只能连接该装置。设计人员必须选择与输入装置兼容的MSR。

输入阻抗

安全监视继电器的输入阻抗确定该继电器可连接多少输入装置、输入装置可以安装在多远的地方。例如，安全继电器的最大允许阻抗可为500欧姆。当输入阻抗大于500欧姆时，继电器将无法接通输出。用户必须认真确定输入阻抗，使其小于最大规定值。所用导线的长度、规格与类型会影响输入阻抗。

输入装置的数量

应借助风险评估过程确定一个安全监视继电器上应连接多少输入装置单元MSR，确定输入装置的检查频率。为确保急停按钮与门联锁状态正常，应按照风险评估结果确定定期检查器功能。例如，连接在每个机械运行周期内必须打开(如，每天多次)的联锁门连接的双通道输入MSR就不需要检查。这是因为打开房主装置会使MSR进行自检、检查器输入、输出(取决于配置情况)有无故障信号。防护装置打开越频繁，检查过程的完整性越高。

另一种类型，如急停装置因为急停装置一般仅在紧急情况下使用，因此很少使用。所以，应制定一个急停装置练习计划并按照预定计划确定其功能是否正常。以这种方式进行安全系统联系称作验证试验，相邻验证试验之间的时间称作验证试验时间间隔。第三个例子为方便机械调节的人孔门。这种装置与急停装置类似很少使用。所以我们再次强调，应制定一个人孔门练习计划并按照预定计划确定其功能是否正常。

风险评估有助于确定输入装置是否需要检查，确定其检查频率。风险级别越高，所需的检查过程完整性也越高。“自动”检查频率越低，“手动”检查的频率就越高。

输入交叉故障探测

在双通道系统中，输入装置的通道间短路故障也称作交叉故障。安全系统必须能够探测到这种故障。通过检测装置或者安全监视继电器可达到探测目的。

基于微处理器的安全监视继电器，象光幕、激光扫描仪以及先进的非接触式传感器一样以多种方式探测这些短路故障。探测交叉故障的通用方法是相异脉冲测试法。输出信号处于快速脉动状态。通道1的脉冲由来自通道2的脉冲补偿。如果发生短路，装置同时出现并由装置探测到。

电动-机械式安全监视继电器采用不同的相异技术：上拉输入与下拉输入。通道1与通道2之间发生短路时会激活过流保护装置，然后安全系统停止。

输出

MSR有多种不同的输出形式。输出类型有助于确定在规定应用中必须使用哪种MSR。

大多数MSR至少配置2个瞬动式安全输出。MSR安全输出的特点是常开输出。由于具有冗余特性与内部检查功能，这些输出达到了安全等级。第二类输出为延时输出。延时输出通常用于1类停止方法中。当在允许进入危险区域前机械需要一定时间执行停止功能时采用1类停止方法。MSR也配备辅助输出。通常这些输出为常闭型输出。

输出额定值

输出额定值表示安全防护装置切负载的能力。典型工业装置的额定值表示为阻性或者电磁性。阻性负载可能指加热器一类的元件。典型的电磁负载为具有感性大负载的继电器、接触器或者电磁阀。IEC 60947-5-1标准的附录A介绍了各种负载的额定值。安全类别的“原则”部分也介绍了这些内容。

字母符号：字母符号后为一个数字，如A300。该字母与通常的密闭热电流有关，与电流为直流还是直流有关。例如，A表示10A交流电流。数字部分表示额定绝缘电压。例如，300表示300V。

使用：使用部分介绍了需要专门通过安全装置切换的负载类型。与IEC 60947-5相关的使用情况见下表所列。

使用	负载说明
AC-12	阻性负载以及采用光耦合器隔离的静态负载的控制
AC-13	采用晶体管隔离的静态负载的控制
AC-14	小型电磁负载的控制(小于72 VA)
AC-15	电磁负载，大于VA
DC-12	阻性负载以及采用光耦合器隔离的静态负载的控制
DC-13	电磁控制
DC-14	回路中采用经济性电阻的电磁负载的控制

热电流Ith：常见的封闭性热电流是指封闭在指定外罩内的设备进行温升试验时所用的电流值。

额定运行电压Ue与运行电流Ie，额定运行电流与电压规定了正常情况下开关的元件的闭合与分断能力。Allen-Bradley Guardmaster产品具体的额定值为125VAC、250VAC、24VDC。采用其他额定值时请咨询厂家。

VA：VA(电压×电流)额定值表示开关元件在闭合回路以及分断回路时的额定值。

示例1：A150、AC-15的额定值表示触点可以闭合7200VA的回路。在120V AC时，触点可以闭合60A的冲击回路。因为AC-15是电磁性负载，60A电流仅允许短时内出现；电磁负载的冲击电流。因为电磁负载的稳态电流为额定运行电流6A，所以回路的分断能力仅为720VA。

示例2：N150、DC-13的额定值表示触点可以闭合275VA的回路。在125VAC时，触点可以闭合2.2A的回路。DC电磁负载没有AC电磁负载的冲击电流。因为电磁负载的稳态电流为额定运行电流2.2A，所以回路的分断能力仅为275VA。

机械重启

例如，如果一台运行机械上的连锁型防护装置打开，安全联锁开关会使机械停止运行。在大多数情况下，当防护装置闭合时禁止机械立即重启。满足这一要求的通常做法是依靠闭锁式接触器启动布局。

瞬时按下并释放启动按钮使接触器控制线圈得电，并由控制线圈使动力触点闭合。只要动力触点流过电流，控制线圈就会通过接触器辅助触点保持得电状态(电气闭锁)。该辅助触点与动力触点以机械方式连接。只要主电源或者控制回路电源中断，控制线圈就会失电，打开主电源触点与辅助触点。防护装置联锁连接至接触器控制回路。这就是说，只有防护装置关闭，然后将能够使接触器复位，使机械启动的正常启动按钮处“接通”才能使机械重启。

ISO 12100-1的第3.22.4段明确了正常联锁请情况的要求(摘录)。

“防护装置关闭后，可以执行由防护装置遮盖的危险性功能，但防护装置关闭过程本身不会启动这些性功能”。

许多机械已经配备了按照上文规定的动作的单接触器或者双接触器(或者采用了能够达到相同效果的系统)。在现有机械上安装联锁时，必须确认电源控制布局是否满足这些要求，必要时还需考虑其他措施。

复位功能

Allen Bradley Guardmaster的监视继电器都采用了监视型手动复位或者自动/手动复位的设计。

监视型手动复位

监视手动复位需要采用在门关闭或者急停复位后可以闭合，然后打开回路。动力切换接触器的机械连接式常闭触点与瞬动按钮串联。安全继电器将在防护装置打开并关闭后，复位按钮给按下并释放前将禁止机械重启。当复位按钮被按下并释放后，安全继

电器(即，监视部件)将检查两个接触器是否断开，两个联锁回路是否闭合(联锁回路闭合后防护装置关闭)。如果这些检查顺利结束，那么可以从正常控制机构重新启动机械。复位开关应位于能够清楚看到危险的地方。这样，操作人员才能在操作前检查该区域是否清空。

自动/手动复位

一些安全继电器具有自动/手动复位功能。手动复位模式不受监视，按下按钮时进行复位。不对复位开关中的短路或者卡住状态进行探测。另外，可跨接复位线路，允许进行自动复位。那么，用户必须采用其他机构以防止机械在门关闭后启动。

自动复位装置不需要手动开关动作，但是在停止后，系统复位前始终进行系统完整性检查。不应将自动复位系统与没有复位设施的装置混淆。在没有复位设施的装置中，安全系统在系统停止后会立即启用，但不进行系统完整性检查。

控制型防护装置

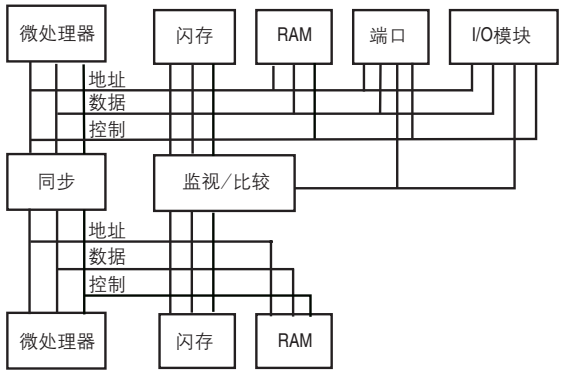
控制性防护装置打开后会使机械停止运行，并在其关闭后直接启动机器。由于在某些紧迫情况下意外启动或者无法停止运行会导致极大危险，所以只有在这种情况下才允许使用控制型防护装置。联锁系统必须具有极高可靠性(通常建议采用防护装置锁定功能)。在操作人员的整个身体或其身体的某一部分在安全防护装置关闭后便不可能处于或者进入危险区域的情况下，可以考虑在机械上采用控制型防护装置。控制型防护装置必须是进入危险区域唯一途径。

安全可编程逻辑控制机构

在规模化、灵活的安全应用方面需求促进了安全PLC/控制器的发展。可编程安全控制器与用户们已经习惯了的标准可编程控制器的灵活性不相上下。但是，标准PLC与安全PLC之间有很大的区别。安全PLC可形成不同的平台，以满足更复杂的安全系统对于规模性、功能性、集成性的要求。

硬件

在安全PLC中加强了CPU冗余性、存储器、I/O回路与内部诊断功能。标准PLC对此没有要求。安全PLC会用更多的时间对存储器、通讯与I/O进行内部诊断。为达到所需的安全认证这些额外工作是必需的。在控制器运行系统中考虑额外冗余与诊断功能,使其对于编程人员来说是透明的，从而安全PLC的程序与标准PLC的程序非常相似。



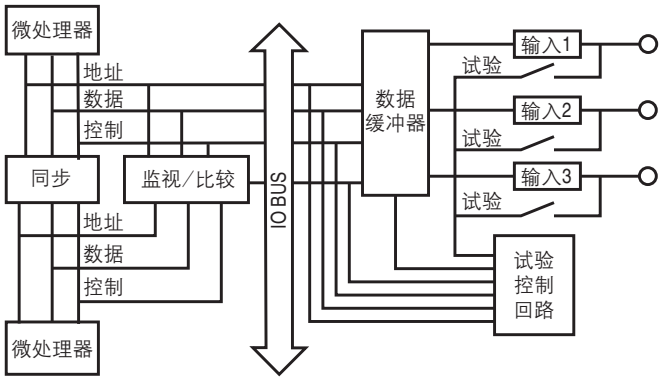
1oo2D 架构

控制这些装置的微处理器执行大量的内部诊断，以确保安全功能装置的性能。下图为安全PLC功能框图示例。虽然基于控制器的、各种系列的微处理器会有少许不同，但是为达到安全等级均采用了相似的原理。

可采用多个微处理器处理I/O、存储器与安全通讯。监控回路执行诊断分析。这种结构类型也就是人们熟知的1oo2D。这是因为两个微处理器中任何一个微处理器都能执行安全功能，然后进行大量的诊断分析以确保两个微处理器同步运行。

另外，对于每个输入回路每秒进行多次内部测试，以保证其运行正常。用户在一个月中可能仅需按一次急停。不过，当按下急停时会对输入回路进行连续测试，以使安全PLC能对急停进行正确的内部检测。

安全PLC的输出为电子通道型或者符合安全等级的固态型。为确保能切断输出，输出回路与输入回路一样在每秒内也经过多次测试。如果三个回路中有一个出现故障，则两外两个输出回路会切断该输出，并由内部监视回路报告故障。



安全输入模块的方框图

当采用机械触点式安全装置时(急停、门开关等)，用于可使用脉冲测试信号探测交叉故障。为了避免用尽昂贵的安全输出，许多安全PLC采用了可以连接机械触电装置的特殊脉冲输出。

软件

安全PLC的编程与标准PLC非常相似。上文提及的所有额外诊断与错误检查已由操作系统完成，因此编程人员甚至不知道这些功能正在执行。大多数安全PLC将采用安全系统编程所需的特殊指令。采用这些指令的目的是模拟相应安全继电器的功能。例如，执行急停指令时与MSR 127极为相似。虽然这些指令背后是复杂的逻辑，但编程人员将这些功能块简单的连在一起后，安全程序看起来还是相对简单的。这些指令以及其他逻辑、数学函数、数据处理等均经过第三方的认证，以确保其运行符合适用标准的规定。

功能块是对安全功能进行编程的主要方法。除了功能块、梯形逻辑图外，安全PLC还提供经过认证的安全应用指令。经过认证的安全指令规定了应用中的具体行为。该示例为急停指令。在梯形逻辑图中实现相同功能需要16行梯形逻辑语句。既然将逻辑行为嵌入急停指令中，那么就不需要测试嵌入指令中的逻辑行为。

经过认证的各种功能块几乎可与所有安全装置链接。该列表的一个例外就是使用阻性技术的安全边缘开关。

安全PLC会生成一个能够跟踪是否发生更改的“签名”。这个签名通常由程序、输入/输出与时间标记共同组成。当程序结束并经过验证时，用户应记录该签名并将其作为验证结果的一部分供以后参考。如果程序需要修改，则需要重新验证并记录新的签名。也可采用密码方式锁定程序，防止在未经授权的情况下修改程序。

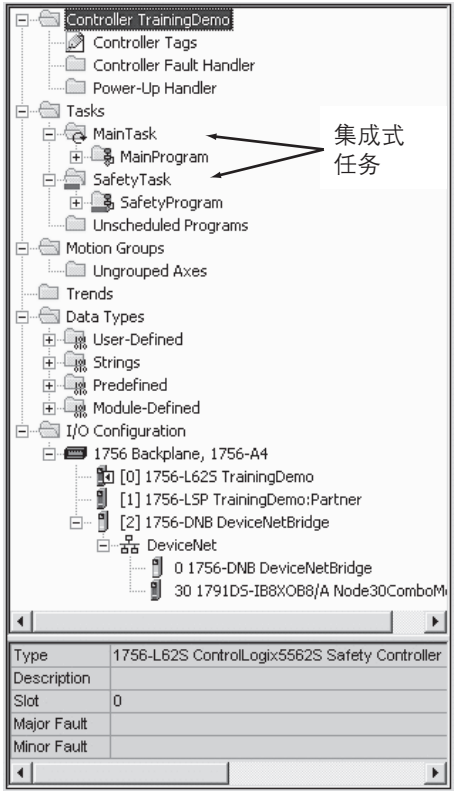
与安全监视继电器相比，采用可编程逻辑系统的接线得到了简化。与在安全监视继电器的具体端子上接线不同，输入装置可连接至任何输入端子，输出装置可连接至任何输出端子。然后，通过软件分配端子。

整合型安全控制器

在拥有安全功能与标准控制功能并且这两种功能一起工作的单一控制架构内，利用安全控制解决方案可进行完全整合。在一个控制器内执行移动、驱动、处理、批处理、高速顺序采样与SIL 3安全具有相当大的优势。通过安全与标准控制机构的整合，我们就可使用通用工具与技术，从而减少相关的设计、安装、调试与维护成本。采用这种安全装置，我们能够在安全网络上使用通用的控制硬件、分布式安全I/O或者设备，能够使用通用的HMI装置，从而能够降低购买欲维护成本，同时缩短开发时间。所有这些优点均能提高生产力、缩短故障排除时间。由于其具有通用型，所以还能降低培训成本。

下图为控制与安全的整合示例。与安全无关的标准功能位于主任务中。与安全有关的功能位于安全任务中。

所有标准功能以及与安全有关的功能之间相互隔离。例如，安全标签可由标准逻辑直接读取。安全标签通过以太网、控制网、设备网在GuardLogix之间交换。通过外部设备、人机接口(HMI)、个人电脑(PC)或者其他控制器可直接读取安全数据标签。



1. 标准标签与逻辑标签的功能与ControlLogix相同。

2. 标准标签数据、程序或者选定范围内的控制器、外部装置、HMI、PC以及其他控制器等。

3. 作为整合控制器，GuardLogix能够将标准标签数据移动(映射)至安全标签，以便在安全任务中使用。用户利用该功能可从GuardLogix的标准侧读取状态信息。不得将该数据直接控制安全输出。

4. 通过标准逻辑可直接读取安全标签。

5. 通过安全逻辑可读取、写入安全标签。

6. 通过以太网，安全标签可在GuardLogix控制器之间交换。

7. 安全标签数据、程序或者选定范围内的控制器可由外部装置、HMI、PC、其他控制器等读取。注意：一旦这些数据被读取，就被当做标准数据，不再是安全数据。

安全网络

按照传统方式，制造商通过现场通讯网络可提高灵活性、增加诊断功能、延长距离、降低安装与接线成本、简化维护，并从总体上提高生产能力。与此相同的动力也促进了工业安全网络的应用。通过安全网络，制造商利用单根网络电缆即可在机械周围分布安全I/O与安全装置，从而在提高诊断功能、启用高复杂度安全系统的同时减少安装成本。通过安全网络也可在安全PLC/控制器之间进行安全通讯，以使用户能在其多个智能系统内进行安全控制分配。

安全网络不能防止通讯错误。但是，安全系统能够更有效的探测传输错误，然后使安全装置采取相应的措施。可以探测到的通讯错误包括：信息插入、信息丢失、信息损坏、信息延时、信息重复、信息顺序错误。

对于大多数应用情况来讲，当探测到错误时装置会进入失电状态，也就是通常所说的“安全状态”。安全输入与输出装置负责探测这些通讯错误，然后在可行的情况下进入安全状态。

早期安全网络是与特定介质类型或者介质访问方案绑定在一起的，因此制造商必须使用成为安全功能一部分的专门电缆、网络接口卡、路由器、桥接器等。这些网络被限定在仅支持安全装置之间进行通讯的范围内。也就是说，制造商必须使用两个或者更多网络用于机械控制(一个网络用于标准控制，其他网络用于与安全有关的控制)，进而增加了安装、培训与备件成本。

在现代安全网络中，可采用单根电缆与安全装置、标准控制装置进行通讯。CIP(通用工业协议)是由ODVA(开放式设备网供货商协会)出版的开放式标准协议。利用该协议可在设备网、控制网与以太网/IP网上的各安全装置之间实现安全通讯。由于CIP安全性协议是标准CIP协议的延伸，所以安全装置与标准装置可存在于同一网络中。用户也可桥接含有安全装置的网络，从而能够细分安全装置以便对安全响应时间进行微调，或者使安全装置更容易分配。因为安全协议仅由终端装置负责(安全PLC/控制器、安全I/O模块、安全部件)，所以采用标准电缆、网络接口卡、桥接器、路由器，进而取消网络专用硬件，从安全功能中取消这些装置。

输出装置

安全控制继电器与安全接触器

控制继电器与接触器用于切断执行机构的电源。为达到安全等级，控制继电器与接触器上增加了特殊功能。

机械连接式常闭触点用于向逻辑装置反馈控制继电器与接触器的状态。使用机械连接式触点有助于确保安全功能。为了满足机械连接式触点的要求，常开与常闭触点不能同时闭合。IEC 60947-5-1标准规定了机械连接式触点的要求。如果常开触点因烧熔粘在一起，则常闭触点将打开且触点间距离至少保持0.5mm。相反，如果常闭触点因烧熔粘在一起，那么常开触点将保持打开状态。

禁止安全系统在特殊位置启动。标准等级的控制继电器与接触器允许衔铁压下后靠近常开触点。在达到安全等级的装置上为了避免意外启动，会防止衔铁具有手动超驰功能。

在安全控制继电器上，常闭触点由主推动杆部件驱动。安全接触器采用加法器块定位机械连接式触点。如果触点块跌落离开基板，则机械连接式触点将保持闭合。机械连接式触点永久性固定在安全控制继电器或者安全接触器上。

在大型接触器上，加法器块已不能准确反应更宽的扳手型部件的状态。在4.81图中，接触器两侧采用了互相对应的触点。

控制继电器或者接触器的释放时间是计算安全距离时的决定因素。通常，使浪涌抑制器跨过线圈以提高线圈驱动触点的寿命。对于AC线圈，释放时间不受影响。对于DC线圈，释放时间会延长。释放时间将延长多少由浪涌抑制类型决定。

控制继电器与接触器用于切换从0.5A到100A以上的大型负载。安全系统低电流运行。安全逻辑装置产生的反馈信号的电压通常为24VDC，电流通常大约为几个到几十个毫安。安全控制继电器与接触器采用镀金分支形触点，以便可靠切换小电流。

过载保护

按照电气标准规定，电机需要采取过载保护。由过载保护装置提供的诊断情况不仅能增强设备安全，还能提高操作人员安全。目前可用的技术可以探测到诸如过载、缺相、接地故障、失速、堵转、欠载、电流不平衡与温度过高等故障情况。在跳闸前探测并传递异常情况有助于延长生产时间，有助于避免操作人员、维护人员处于不可预见的危险情况下。

变频器与伺服装置

达到安全等级的变频器与伺服装置可用于防止输送旋转能量，以便实现安全停机以及急停。

变频器达到安全等级，具有能够切断门的控制回路电源的冗余通道。其中一个通道为使能信号，即取消门控制回路输入信号的硬件信号。第二个通道为正向导引继电器。这种继电器能够切断来自门控制回路的电源。正向导引继电器也向逻辑系统反馈一个状态信号。通过这种冗余方法可在急停回路中使用达到安全等级的驱动装置，而无需使用接触器。

伺服装置实现其目的的方式与采用冗余安全信号的变频器类似，并用于实现安全功能。一个信号用于断开变频器与门控制回路。第二个信号用于切断门控制回路的电源。两个正向导引继电器用于取消这些信号并向安全逻辑装置提供反馈信号。

连接系统

连接系统通过降低安全系统的安装、维护成本实现增值。设计时必须考虑单通道、双通道、指示型双通道、多种装置类型。

当需要串联双通道联锁时，采用接线快可简化安装过程。这种类型的接线箱达到IP67的防护等级，可以安装在远程机械上。需要不同类型的装置时，可采用ArmorBlock Guard I/O接线箱。可通过软件配置各个输入，以满足不同类型装置的需要。

安全距离计算

必须在操作人员进入危险状态前将各种危险状态转变为安全状态。在安全距离计算方面，有两组已经使用的标准。在本章中，这些标准分为以下两组：

ISO EN：(ISO 13855和EN 999)

US CAN(ANSI B11.19、ANSI RIA R15.06与CAN/CSA Z434-03)

公式

最小的安全距离取决于处理停机指令所需的时间、被探测前操作人员穿过探测区域有多远。全球范围内采用的公式形式相同、要求相同。不同之处是各种变量的表示符号与测量单位。

具体公式如下：

ISO EN： $S = K \times T + C$

US CAN： $Ds = K \times (Ts + Tc + Tr + Tbm) + Dpf$

式中：Ds与S为最近探测点与危险区域之间的最小安全距离

路径方向

采用光幕或者区域扫描仪情况下考虑安全距离计算时，必须考虑到探测装置的路径。需要考虑三种路径：

正常路径 - 垂直于探测平面的路径

水平路径 - 与探测平面平行的路径

斜路径 - 与探测平面形成一定角度的路径。

速度常数

K为速度常数。速度常数的值由操作人员的移动情况决定(如手的移动速度、行走速度、每走一步的长度)。该参数的值依据研究数据。根据该数据可做以下合理假设，操作人员静止不动时手的移动速度16mm/s(63in/s)。同时，还必须考虑实际应用环境。按照常规，接近速度应在1600mm/s(63in/s)到2500mm/sec(100in/s)之间变化。相应的速度常数应通过风险评估确定。

停机时间

T为系统的总停机时间。总停机时间以秒为单位，从发出停止指令开始到终止危险结束。为简化分析，可将总停机时间分为几个增量部分(Ts、Tc、Tr与Tbm)。Ts为最严重的机械/设备停机时间。Tc为做严重的控制系统停机时间。Tr为安全装置(包括接口)的响应时间。Tbm在探测到停止时间恶化并超出最终用户预先设定的极限时间前，由制动器监控器允许的附加停机时间。Tbm与部件旋转的机械压力计配套使用。如果具体数值未知，则Ts + Tc + Tr通常通过停止时间测量装置测量。

穿过深度系数

穿过深度系数由符号C与Dpf表示。该系数表示在安全装置探测前向着危险方向经过的最大路程。穿过深度系数随着装置类型、应用类型的变化而变化。为了确定最佳的穿过深度系数，我们必须检查相应的标准。对于物体灵敏度小于64mm(2.5in)的光幕或者区域扫描仪的正常路径，可采用 ANSI与加拿大标准：

Dpf = 3.4 ×(物体敏感度 - 6.875mm)，但不能小于零。

对于物体敏感度小于40mm(1.57in)的光幕或者区域扫描仪的正常路径，可采用 ISO与EN标准：

C = 8 ×(物体敏感度 - 14 mm)，但不能小于0。

这两个公式在19.3mm处有一个交叉点。对于物体敏感度小于19mm的情况，US CAN路径更加严格，这是因为必须使光幕或者区域扫描仪远离危险。对于物体敏感度大于19.3mm的情况，则ISO标准更加严格。所以，如果机械制造商欲使其机械在全球应用，则必须由这两个等式考虑到最严重的情况。

穿过

当采用较大的物体敏感度时，US CAN与ISO EN标准在穿过深度系数与物体敏感度方面有少许区别。图5.2总结了各种差异情况。ISO EN标准规定的值为850mm，而在US CAN标准中则为900mm。这些标准在物体敏感度方面也存在差异。ISO EN标准允许物体敏感度在40 - 70mm之间，而US CAN标准则最大允许600mm。

穿越

这两类标准均规定最低处的光束最大高度为300mm，但对于最高处光束的最小高度的规定有所不同。ISO EN标准将该值规定为900mm，而US CAN则规定为1200mm。最高处光束的值似乎还未确定。在穿过情况下考虑该值时，最高处光束的高度必须很高以满足操作人员处于站立状态的要求。如果操作人员会穿越探测平面，则应采用穿越标准。

单束光或者多束光

ISO EN标准进一步定义了独立的单束光与多束光。下图说明了地面上多光束的“实际”高度。绝大多数情况下的穿过深度为850mm，采用单束光时的深度为1200mm。相比之下，US CAN标准则根据穿过要求考虑这种情况。必须考虑穿越、围绕单束光或者多束光或者位于其下方。

光束数量	距地面高度(mm)	C(mm)
1	750	1200
2	400, 900	850
3	300, 700, 1100	850
4	300, 600, 900, 1200	850

距离计算

对于到光幕的正常路径，ISO EN与US CAN标准下的安全距离计算相近，但确实存在差异。对于最大物体敏感度为40m的情况下到光幕的正常路径，计算时需要两个步骤。首先，利用时间常数2000计算S。

S = 2000 × T + 8 ×(d -1 4)

然后可以确定最小距离为100mm。

当距离超过500mm时可采用第二步。那么，K值可以减少为1600。当K=1600时，最小S = 500mm。

US CAN路径采用一步法：Ds = 1600 × T * Dpf

这样，当响应时间小于560ms时，采用两类标准得出的结果之差会大于5%。

斜路径

在大多数应用情况下的光幕与扫描仪都采用竖直(正常路径)或者水平安装(平行路径)方式。如果专门在±5°范围内设计，则这种安装方式不应属于斜路径。当角度超过5°时，则必须考虑可预见路径的潜在风险(如，最短距离)。一般来讲，如与参考平面形成的角度大于30°(如，地面)，则将该角度视作正常；如小于30，则视作平行。

安全垫

采用安全垫时，必须考虑操作人员的步速与步长。假设操作人员在安装了安全垫的地板上行走。操作人员踏上安全垫的第一步为穿过深度系数1200mm或者48in。如果操作人员必须踏上某个平台，那么穿过深度系数将减小至台阶高度的40%。

示例

例如：操作人员采用14mm光幕的正常路径，该光幕与安全监视继电器连接，安全继电器通过二极管抑制器与DC电源接触器连接。安全系统的响应时间Tr为20 + 15 + 95 = 130ms。机械停机时间Ts+Tc为170ms。未使用制动监控器。Dpf为1，C为零。则具体计算如下

Dpf = 3.4(14 - 6.875)= 1in(24.2mm)

C = 8(14-14)= 0

Ds = K ×(Ts + Tc + Tr + Tbm)+ Dpf
Ds = 63 ×(0.17 + 0.13 + 0)+ 1
Ds = 63 ×(0.3)+ 1
Ds = 18.9 + 1
Ds = 19.9 in(505mm)

S = K × T + C
S = 1600 ×(0.3)+ 0
S = 480mm(18.9in)

因此，对于在全球任一地方都能使用的机械，最小安全距离也就是安全光幕距危险的距离为20in或者508mm。

防止意外接通电源

许多标准都涉及防止意外接通电源。如ISO14118、EN1037、ISO12100、OSHA 1910.147、ANSI Z244-1、CSA Z460-05、AS 4024.1603等标准。这些标准有一个共同主题：防止意外接通电源的主要方法是切断系统电源，然后将系统锁定在断开位置， 以使人员能安全进入机械的危险区域。

锁定/悬挂警示牌

新型机械必须配备可锁定式能量隔离装置。这种装置适用于所有类型的机械，包括电气、液压、气力、重力与激光机械。锁定是指在能量隔离装置上使用锁具。该锁具只有在可控条件下由其所有者或者监督人员才能取消。当多个人在机械上工作时，每个人必须在能量隔离装置上使用自己的锁具。通过每把锁必须能识别其所有者。

在美国，悬挂警示牌是替代锁定的一种方法，适于没有安装锁定装置的老式机械。在这种情况下，先切断机械电源然后悬挂警示牌，提醒所有人员不要启动机械，悬挂警示牌的人在机械上工作。从1990年开始，改造机械时必须进行更新，为其配备可锁定式能量隔离装置。

能量隔离装置是指能从物理上阻止能量传输或者释放的机械装置。这些装置类型如断路器、隔离开关、手动开关、插头/插座组合件或者手动操作的阀门。电气隔离装置必须能够隔离所有未接地的电源导线，并且各种触头不能单独操作。

锁定于悬挂警示牌是为了防止机械意外启动。造成机械意外启动的原因有多种： 控制系统失效、启动控制机构、传感器、接触器或者阀门的误动作、电源中断后又恢复、或者其他的内部或者外部影响。完成锁定或者挂牌程序后，必须验证能量分散情况。

安全隔离系统

安全隔离系统能够有序的执行机械停机，也能提供简单的机械电源锁定方法。这种方法对于大型机械与制造系统非常有效，尤其在多种能量源位于夹层中或者较远地方的情况下。

隔离负荷

对于现场的隔离装置，可在需要隔离、锁定的装置前安装开关。Bulletin 194EL负荷开关就是这样一种既能够隔离又能锁定的产品。

钥匙安全联锁系统

钥匙安全联锁系统是实现锁定系统功能另外一种方法。许多钥匙安全联锁系统能量隔离装置开始。当通过“主”钥匙将开关断开后，机械所需电能将从所有未接地的电源导线上同时切断。然后拔出主钥匙，将其放在靠近机械需要经过的位置。图6.4所示为最基本的系统，包括一个隔离开关与门锁。我们可通过增加各种不同的组件实现更复杂的锁定结构。

可替代锁定方法

在机械维修与维护期间必须采用锁定机构并悬挂警示牌。正常生产运行期间干预机械时必须采用防护装置遮盖。维修/维护与正常生产运行的不同并不总是很明确。

在正常生产运行期间的小调节与维修任务并不需要将机械锁定。这些情况如加料与卸料、更换次要工具与小调节、维修润滑油液位以及清除废料。这些任务必须是日常重复的，属于利用设备进行生产活动的一部分；在进行这些工作时应采用能够提供有效保护的替代性措施，如防护装置。防护装置包括联锁防护罩、光幕与安全垫等装置。操作人员使用合适的、达到安全等级的逻辑与输出装置可以在正常生产任务期间、小维修期间安全进入机械的危险区域。

与控制系统有关的安全结构

说明

什么样的系统是与安全有关的系统(缩写为SRCS)呢？与安全有关的系统属于机械控制系统的一部分，能够组织危险条件出现。该系统可为独立的专门系统，或者整合在机械的标准控制系统中。

该系统包括与电源接触器控制线圈串联的防护门联锁开关、急停开关等简单系统，也包括通过软件与硬件通讯、由简单与复杂装置组成的混合系统。

与安全有关的控制系统专门执行安全功能。SRCS必须能在所有可预见情况下连续正常运行。那么，什么是安全功能，我们如何设计一个系统来实现该目标，我们什么时候进行设计并如何展现安全功能？

安全功能

对于一个特定危险来讲，由机械控制系统中与安全有关的部件执行安全功能，使机械达到或者维持安全、可控状态。安全功能失效可能会立即导致使用机械时的风险增加，即处于危险情况下。

一台机械肯定至少存在一个“危险”，否则就不能称之为机械。“危险情况”就是操作人员容易受到伤害 危险情况并不表示操作人员已经受到伤害。这种容易受到伤害的操作人员可能会确认风险并避免受伤。这种容易受到伤害的操作人员也可能不会识别危险，或者由于意外启动造成危险。安全系统设计人员的主要任务就是阻止危险条件出现，阻止意外启动。

安全功能通常可用多个要求描述。例如，由联锁防护罩启动的安全功能包括三部分：

1. 防护罩关闭前，由防护罩阻止的危险部分不能运行；
2. 如果在防护罩打时操作，则关闭防护罩会阻止危险；
3. 关闭防护罩不会重新启动由该防护罩保护的危险部分。

规定在具体应用情况下的安全功能时，“危险”就应换成“具体危险”。不能将危险及其造成的后果相混淆。挤压、切割、烫伤便属于危险结果。例如，危险部件是电机、夯锤、刀、焊炬、泵、激光、机器人、末端执行器、电磁阀、阀门以及其他类型的执行机构，或者涉及重力的机械危险。

讨论安全功能时，应使用词组“安全功能执行时的要求或者安全功能前执行前的要求” 什么是对安全功能的要求呢？有关安全功能的要求包括打开联锁式防护罩、阻断光幕、踏上安全垫或者压下急停按钮。如果危险部分已经停止，则操作人员可要求该危险部分停止，或者保持是失电状态。

机械控制系统中与安全有关的部分执行安全功能。安全功能不由某个装置，如仅由防护罩等单独执行。防护罩的联锁机构会向逻辑装置发送指令，然后逻辑装置禁止某个执行机构。安全功能由指令启动并在执行后结束。

安全系统必须具有与机械风险相当的集成度。为确保安全功能，风险越高，安全系统的集成度也应越高。机械的安全系统可按照其设计目的与能力分类，从而确保安全系统的性能。

控制系统的分类

以下有关控制系统类别的讨论基于与EN 954-1:1996等效的ISO 13849-1:1999。ISO 13849-1于2006年经过较大修订，以便与IEC/EN 62061与IEC/EN 61508一致。这两个IEC标准均是与高度复杂的安全系统配套使用的首选标准。ISO 13849-1(EN ISO 13849-1)的2006年版继续使用安全性能分类，其中分类被视作SRCS的“结构”或者“架构”。有关组件与系统设计的其他信息是对该“结构”的补充，用以提供“性能水平”等级。此处讨论的类别适用于ISO 13849-1(EN ISO 13849-1)标准的1999与2006修订版。

初始的EN 954-1/ISO 13849-1标准中“控制系统中与安全有关的部分的第一部分 - 设计总原则”规定了对SRCS进行基准检测、描述时所需的五种类别“语言”。

注意1：B本身没有特定的安全措施，但可作为其他类别的基础部分。

注意2：由于常见原因造成的多个故障，或者由于第一个故障造成的不可避免的后续故障应算作单一故障。

注意3：如果能判定故障，则可将审查故障限定在两个故障的组合范围内；但是，复杂回路(如，微处理器)可能需要考虑多故障组合。

因此，如何确定我们需要哪种类别呢？通过风险评估过程应能得出正确的类别。为了将这些要求转换成系统设计规范，我们必须解释各项基本要求。

人们经常错误的认为1类系统提供的保护最少，4类系统提供的保护最好。这不是分类背后的原因。这些分类目的是作为一种基准点，用于描述与安全有关部分以及组成部分的不同方法具有的功能特性。

1类系统的目的是防止故障。该类系统通过采用适合的设计原理、部件与材料达到其目的。简单的原理、设计以及稳定的、可预见的材料特性是本类系统的关键。

第2、3、4类系统要求，必须在不能防止故障的情况下必须探测到故障，并采取相应的措施。

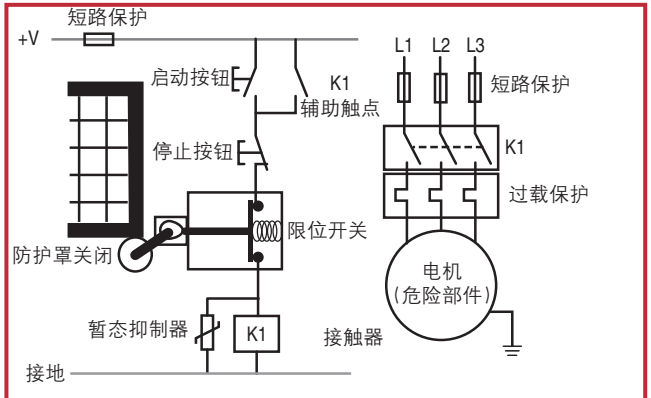
冗余性、多样性、仅是监控是这类系统的关键。冗余性也就是重复相同的技术。多样性是使用两种不同的技术。监控就是检查各装置的状态，然后根据状态检查结果采取相应措施。监控时通常使用的方法(但不是唯一的方法)是重复关键的安全功能，然后比较运行情况。

要求总结	系统行为
B类(见注释1) 与安全有关的机械控制系统和/或起保护设备、组成部件应按照相关标准进行设计、制造、选型、组装、组合，从而能够经受预期的影响。还应遵守基本安全原理。	出现故障时会导致安全功能丧失。
1类系统 适用B类系统要求、使用经过试验验证的安全部件与安全原理。	与B类介绍类似，没有安全有关的功能没有更高的安全可靠性。(可靠性越高，出现故障的可能性越小)。
2类系统 适用B类系统的要求，使用经过试验验证的安全原理。由机械控制系统在机械启动时检查安全功能。如果探测到故障，应启动安全状态，或者如果不可启动安全状态，则报警。	通过检查可以发现安全功能是否丧失。
3类系统(见注释2、3) 适用B类系统的要求，使用经过试验验证的安全原理。该类型系统应满足以下设计要求，即系统中任一部件的单一故障不会导致安全功能丧失。如果有可能，应探测出单一故障。	出现单一故障时应能始终执行安全功能。我们可以探测出一些故障，但无法弹出所有故障。没有探测到的故障累积到一定程度时会导致安全功能丧失。
4类系统(见注释2、3) 适用B类系统的要求，使用经过试验验证的安全原理。该类型系统应满足以下设计要求，即系统中任一部件的单一故障不会导致安全功能丧失。在安全功能接到下一个执行请求时，或者在此之前探测到这种单一故障。如果不能进行故障探测，则故障累积到一定程度会导致安全功能丧失。	出现故障时应能始终执行安全功能。应及时探测到故障，以防失去安全功能。

B类系统

B类规定任何控制系统的基本要求，无论是与安全有关还是无关的系统。控制系统必须能在预期的环境下运行。装置可靠性是指该装置在预期条件下、规定时间段内能够实现其预定功能的概率，因此可靠性理念是控制系统的基础。虽然我们拥有某个满足可靠性目标的系统，但我们清楚这个系统最终会出现故障的。安全系统设计人员需了解该系统故障后进入危险状态还是安全状态。我们的理念是：“系统在故障情况下的性能如何？”。以该理念为起点，我们应采用什么样的原理指导系统设计呢？B类控制系统要求使用基本安全原理。ISO 13849-2为我们规定了电气、气动、液压、机械系统的基本安全原理。现将电气原理总结如下：

- 正确选择、组合、布局、组装与安装(如，按照mfg' rs要求)
- 各部件与电压、电流的相容性
- 承受环境条件
- 使用去电原理
- 暂态抑制
- 缩短响应时间
- 防止意外启动
- 可靠固定输入设备(如，固定连锁机构)
- 保护控制回路(按照NFPA79与IEC60204-1执行)
- 正确的保护连接

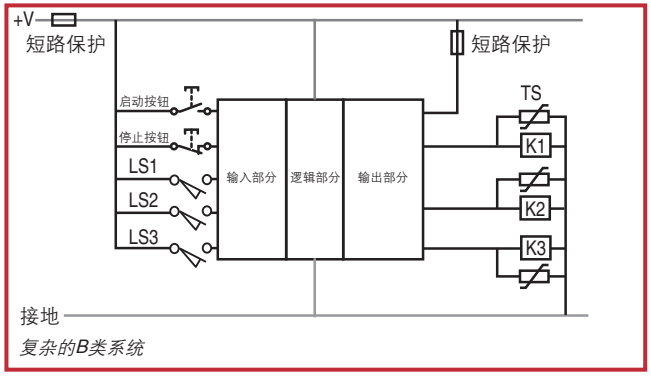


简单的B类系统

此处示例为一个B类系统。防护罩与负向模式(弹簧驱动型)限位开关通过连锁机构连接。采用短路与过载保护以满足电气标准中有关控制回路的保护要求。使用暂态抑制有助于防止接触器线圈失电时触点烧熔粘结。该系统中采

用了去电原理：防护罩联锁会切断电机电源。所用部件必须经过挑选，安装后能满足可预见的环境条件、电压、电流的要求。注意：在使用B类系统的情况下没有应用特殊的安全措施，所以可能需要增加安全措施。

在防护罩关闭的情况下按启动按钮接通电机电源。电机即表示危险部件。当K1接触器闭合时，辅助触点会是该回路保持，然后就可释放启动按钮。按停止按钮或者打开防护罩将切断电机电源。但释放停止按钮或者关闭防护罩不会启动电机。



复杂的B类系统

此处所示为满足B类系统要求的一个复杂系统。在该系统中，多个检测装置(限位开关)、按钮与可编程逻辑控制器(PLC)的输入模块连接。输出模块与多个执行机构连接。逻辑模块利用软件判断哪个输出接通或者断开，以响应检测装置的状态。

我们如何判断这些回路满足B类系统的要求呢？首先，设计人员必须选择、安装，并按照厂家要求进行组装。这些装置必须能在预期的电压与电流额定值下运行。同时，还应考虑预期的环境条件,如电磁兼容性、振动冲击、污染、冲洗等因素。该系统中采用了去电原理。在接触器线圈上安装了暂态保护装置。电机采用了过载保护。连线与接地符合各种适用标准。

安全分析的第二步：将该系统分成几个主要部件，然后考虑各个部件可能出现的失效情况。在以前章节中我们将系统分为输入-逻辑-输出三大块。考虑安全系统性能时也必须分析接线情况。

该B类系统示例包括以下部件：

- 连锁(限位)开关
- 可编程逻辑控制器
- 接触器
- 接线

联锁开关

限位开关属于机械装置。限位开关的任务很简单：当防护罩打开时打开触点。多年以前人们就采用这种方式使用限位开关。但是这种设计存在不利于增强安全性能的缺点。电气标准规定分值回路应采用短路保护装置(如，熔断器或者断路器)。这种保护措施不足以防止限位开关中出现触点烧熔情况。限位开关的触点通过弹簧弹力打开。但令人遗憾的是，弹簧弹力不能始终保持很大以克服烧熔触点的粘结力。第二个需要考虑的因素是弹簧本身。重复弯曲将最终导致其断裂，施加到触点上的力可能不足以打开回路。操作人员脑海中考虑的或者这种连接存在的其他内部故障也会导致防护罩打开时触点保持闭合。另一个重要的考虑因素是可破坏性。当防护罩打开时限位开关容易受到破坏，如将控制杆压至动作位置并用胶带、导线或者其他简单工具将其固定。

可编程逻辑控制器

PLC是机械安全系统的首选设备。限位开关联锁等输入装置与输入模块连接。接触器等输出装置与输出模块连接。逻辑装置按照合适的逻辑条件将输入装置分配至相应的输出装置。

自从PLC推出以来其可靠性有了显著提高，但PLC最终还会损坏，出现故障。安全系统设计人员应明白潜在的失效机理，明白该失效是否会造成危险情况。PLC存在两大类失效情况：硬件与软件故障。硬件失效可能是输入模块、逻辑模块或者输出模块中出现的内部故障。这些失效情况会导致输出保持得电状态，甚至发出停止指令。应用程序或者固件中的软件失效也会造成输出保持得电状态，甚至发出停止指令。

接触器

接触器会使机械的执行机构得电，如电机、电磁阀、加热器或者其他类型的执行机构。这些执行机构使用大电流，有些执行机构使用10倍于稳态电流的浪涌电流。对于接触器的电源触点，应采取过流与短路保护装置避免烧熔。即使采用这种措施，电源切换触点也可能出现一直闭合的情况。这可能由于衔铁烧熔或者卡住造成。出现这类型故障时停止按钮会变得无效，并且必须通过主隔离开关切断电源。应定期检查接触器，确定是否出现可能导致过热或者变形的连接松动情况。接触器必须符合相关标准中有关所需特性与使用条件的规定。IEC60947-4-1于IEC60947-5-1标准详细介绍了接触器在不同应用中的应进行的测试。

接线

虽然按照相应的电气标准接线会降低接线故障几率，但接线失效仍会出现。需要考虑的接线故障包括短路与开路。进行短路分析时必须包括对电源短路、对地短路或者会导致危险情况的对其他回路的短路。

启动与停止开关

另外，还需考虑启动与停止开关。如果启动按钮出现短路，当释放停止按钮或者防护罩关闭时机械会意外重启。庆幸的是启动电机前必须关闭防护罩。如果防护罩关闭，就应防止人员进入危险区域。停止按钮破裂或者触点短路将禁止执行停止指令。所以再次强调：如果防护罩关闭，就应防止人员进入危险区域。

控制系统中与安全有关的部分必须与非安全部分连接。既然启动与停止控制装置故障不会导致安全功能丧失，那么这些装置就不属于安全系统。启动/停止/保持回路表示机械控制系统回路总与安全无关的部分，能用PLC取代。

B类系统是安全系统设计的基础。虽然正确的设计、选型、安装是坚实系统的基础，但许多潜在的单独因素会导致安全系统功能丧失。我们通过处理这些单独因素可以进一步降低失效导致危险的可能性。B类系统不适于在绝大多数与安全有关的应用情况下使用。

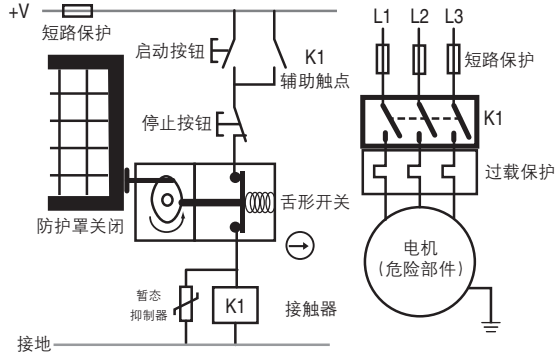
1类系统

1类系统要求系统满足B类系统的各项规定，使用经过试验验证的安全部件。什么是真正的安全部件，我们如何知道这些部件经过试验验证？我们借助ISO 13849-2标准可以回答机械、液压、气动与电气系统方面的那些问题。附录D介绍电气部件。

如果所用部件在许多相似应用中成功使用，那么就可认为这些部件经过试验验证。如果新设计的部件按照相应的标准设计、验证，则就可为这些部件经过试验验证。

经过试验验证的部件	标准
采用正向模式动作的开关(直接打开动作)	IEC 60947-5-1
急停装置	ISO 13850, IEC60947-5-5
熔断器	IEC 60269-1
断路器	IEC 60947-2
接触器	IEC 60947-4-1, IEC 60947-5-1
机械连接式触点	IEC 60947-5-1
辅助接触器(如，接触器、控制继电器、正向导引继电器)	EN 50205 IEC 60204–1、IEC 60947–5–1
变压器	IEC 60742
电缆	IEC 60204-1
联锁机构	ISO 14119
温度开关	IEC 60947-5-1
压力开关	IEC 60947-5-1 + 启动或者液压要求
控制与正向开关设备(CPS)	IEC 60947-6-2
可编程逻辑控制器	IEC 61508、IEC 62061

通过在B类系统上使用经过试验验证的部件，可以用直接打开式舌形开关替换限位开关，可以采用大规格接触器进一步防止触点烧熔。



简单的 1 类安全系统

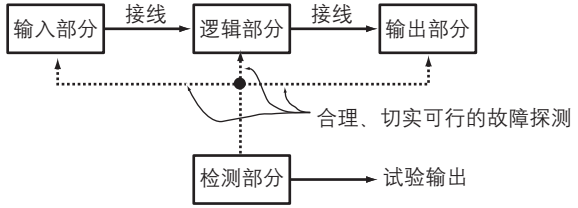
此处所示为将简单的B类系统改造为1类系统。当需要靠近危险部件时，联锁机构与接触器在切断执行机构电源的过程中发挥关键作用。舌形连锁机构满足IEC 60947-5-1标准中有关直接打开动作触点的要求，如圆圈中的箭头符号所指。采用经过试验验证的部件后，1类型系统比B类系统在切断能量方面的几率更高。使用经过试验验证的部件是为了防止丧失安全功能。即使采用了这些改进措施，某个单一故障也会导致安全功能丧失。

我们能在基于PLC的B类系统上使用同样的原理，将安全性能提高到1类系统吗？这种争论的结果是两方面的。有一点是肯定的，使用直接打开工动作联锁机构更换所有在负向模式下运行的限位开关，增大接触器规格将会提高安全功能的执行概率。那么PLC将是我们关注的焦点。PLC在许多类似应用情况下使用吗？逻辑程序经过验证吗，是否稳定，或者微调逻辑程序进行改进与调节吗？固件(用户不能改动其中的软件)最近是都经过修改？在许多类似的应用中，固件以前的失效 - 危险情况如何？是否采取措施消除这些失效情况，或者将这些失效情况减少至可接受的水平。在理论上根据使用结构证明，可以把PLC视作经过试验验证的部件。在如PLC等装置上使用这种方法将会是一项重大任务，需要进行满足极高要求的记录与记录分析。为了简化这种情况，避免随意使用“普通”PLC，ISO 13849-1:1999标准规定：“在只有电子设备的情况下，通常不能满足1类系统的要求”。

B类与1类系统属于基于预防的系统。其设计目的是防止危险情况。当通过预防功能不能充分减少风险时，必须采用故障探测功能。2、3、4类系统均是基于故障探测的系统。这些系统满足更严格的要求，能够更好的减少风险。

2类系统

除了满足B类系统的要求，采用经过试验验证的安全原理外，安全系统必须经过检测以满足2类要求。这些检测必须用于探测控制系统内与安全有关部分的故障。如果没有探测到故障，机械可以继续运行。如果检测到故障，则该检测过程必须能够启动一个指令。只要有可能，该指令必须能使机械处于安全状态。

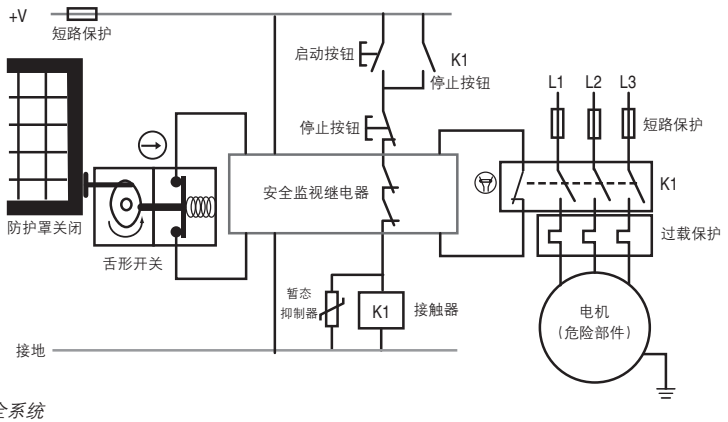


这种检测必须能够以合理、切合实际的方式探测故障。进行检测的设备可以属于安全系统，或者为独立的设备。

必须在以下情况下进行检测：

- 机械最初带电时
- 危险部件启动前
- 如果根据风险评估结果认为有必要，则定期进行检测

“只要有可能”与“以合理、切合实际的方式”说明不是所有的故障能检测到。既然这是一个单通道系统(即，一根导线将输入连接至逻辑装置，连接至输出部分)，所以某个单一故障就可能导致安全功能丧失。在某些情况下，由于2类系统中不是所有部件都能被检查到，所以这类系统不能完全应于安全系统。

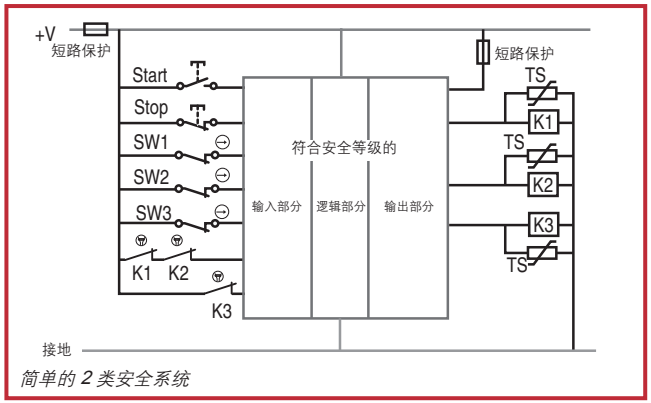


2 类安全系统

此处所示为一个简单的1类系统经过加强后以满足2类系统的要求。其中安全监视继电器(MSR)用于检测。接通电源前，MSR会检查其内部部件。如果没有探测到故障，MSR将通过监视舌形开关的触点周期检查该舌形开关。如果没有探测到故障并且防护罩关闭，MSR接下来会检查输出装置：接触器的机械连接式触点。如果没有检测到故障且接触器断开，则MSR将使其内部输出带电，连接线圈K1与停止按钮。此时，机械控制系统中与安全无关的部件、启动/停止/联锁回路便可启动、停止机械。

防护罩打开会断开MSR的输出。当防护罩重新关闭时，MSR会再次进行安全系统检查。如果没有发现故障，MSR将接通其内部输出。通过MSR对输入装置、逻辑装置(MSR本身)与输出装置进行检测，该回路可满足2类系统的要求。这种检测在最初通电时与危险部件启动前执行。

基于PLC的安全系统凭借其内部逻辑功能可以满足2类系统的要求。如在上述有关1类系统的讨论，判定PLC是否经过试验验证(包括其检测能力)是我们面临的挑战。对于需要达到 2类系统等级的复杂系统，按照IEC61508标准达到安全等级的PLC可用于更换未达到安全等级的PLC。



简单的 2 类安全系统

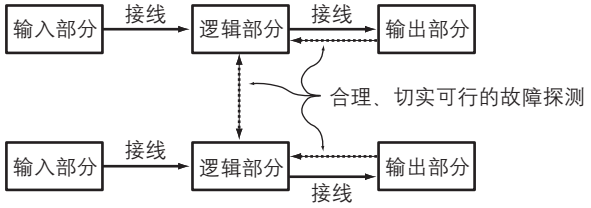
此处所示为采用达到安全等级的PLC的复杂系统。如果达到安全等级的PLC是按照相应标准设计的，则这种PLC满足各种试验验证要求。为便于进行检测，接触器的机械式连接触点与PLC 的输入连接。这些触点将根据程序的逻辑功能可能与一个输入端子串联，或者与单独的端子连接。

虽然使用经过试验验证的安全部件，但是检查中的某个单一故障会导致安全功能丧失。所以，2类系统适于低风险应用情况。如果需要达到更高的故障承受水平，则安全系统必须满足3、4类系统的要求。

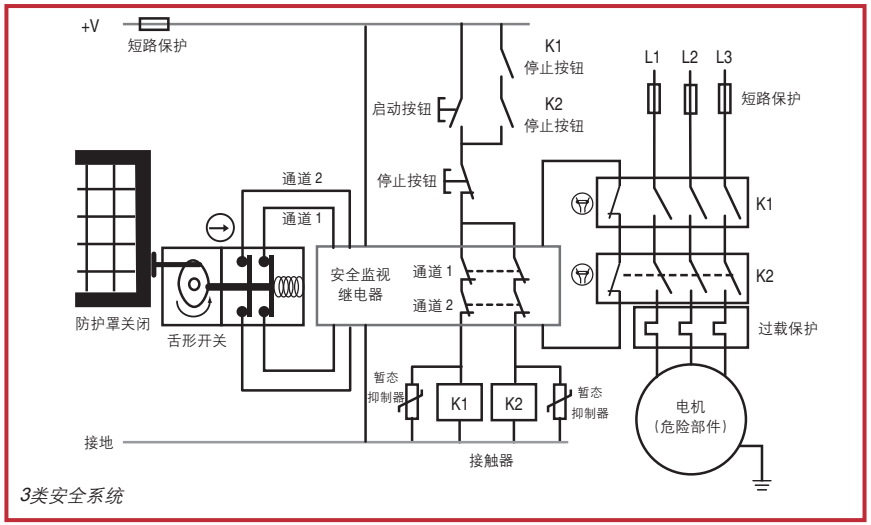
3类系统

除了满足B类系统的各项要求、经过试验验证的安全原理外，3类系统的安全功能部分应在出现单一故障情况下具有出色性能。只要合理、切合实际，就必须在对安全功能的下一个要求出现时，或者出现前探测到故障。

在此我们再一次使用“只要合理、切合实际”。这样就会涵盖那些未被探测到的故障。只要未探测到的故障不会导致安全功能丧失，安全功能就满足3类系统的要求。由此可知，各种未探测到的故障聚集后可能导致安全功能丧失。



以下方框图说明了3类系统的原理。该系统采用冗余性与合理、切合实际的交叉监视、输出监视，以确保安全功能部分的性能。



3类安全系统

以下为3类系统的示例。在舌形开关上增加了一组冗余触点。安全监视继电器(MSR)内部含有交叉监视的冗余回路。电机电源通过一组冗余接触器切断。MSR通过合理的、切合实际的机械连接式触点监视这些继电器。

故障探测过程必须考虑安全系统的每一部分以及连接(即，系统)。双通道舌形开关会有什么样的故障模式？MSR会有什么样的失效形式？接触器k1与k2会有什么样的失效形式？接线部分会有什么样的失效形式？

舌形联锁开关采用直接打开式触点。因此，我们可知打开防护罩用于打开烧熔的触点。这样就会消除一种故障模式。是否还存在其他故障模式？

直接打开式开关通常采用弹簧驱动的返回部件。如果端部被取消或者断裂,安全触点会弹回闭合(安全)状态。许多联锁开关在设计时采用了可拆卸式端部以满足各种应用情况下的安装要求。这种端部可拆除或者在两个到四个位置之间旋转。

这种端部固定螺钉的紧固力矩不正确会导致失效情况。在这种情况下，机械上的预期震动可能造成端部的固定螺钉脱落。在弹簧压力作用下的端部会抵消来自安全触点的压力，然后安全触点闭合。然后，打开防护罩却不会打开安全触点，进而导致危险性失效发生。

同样，必须检查开关内部的操作机构。单一部件失效导致安全功能丧失的概率有多大？在不久的将来将会找到这些问题的答案。同时，必须提供危险性故障、诊断范围、安全失效分数的情况，以满足在确保安全功能部分性能方面所需的知识不断增长的要求。

常规做法是，在3类系统的回路中使用带有双触点的舌形联锁机构。采用这种方法时，必须排除打开安全触点这种单一开关失效情况。我们把这种情况视作“排除故障”，相关内容将在本章稍后部分介绍。

电动机械式安全监视继电器(MSR)属于经常由第三方机构评估并指定为符合某一类型要求的低复杂性装置。MSR通常具有双通道能力、通道交叉监视、外部装置监视与短路保护功能。目前在MSR设计或者使用方面还没有专门标准给出指导性内容。MSR执行安全功能的能力将按照ISO 13894-1或者后续标准EN954-1评估。为满足系统弄个安全要求，MSR必须具有相同或者更高的安全等级。

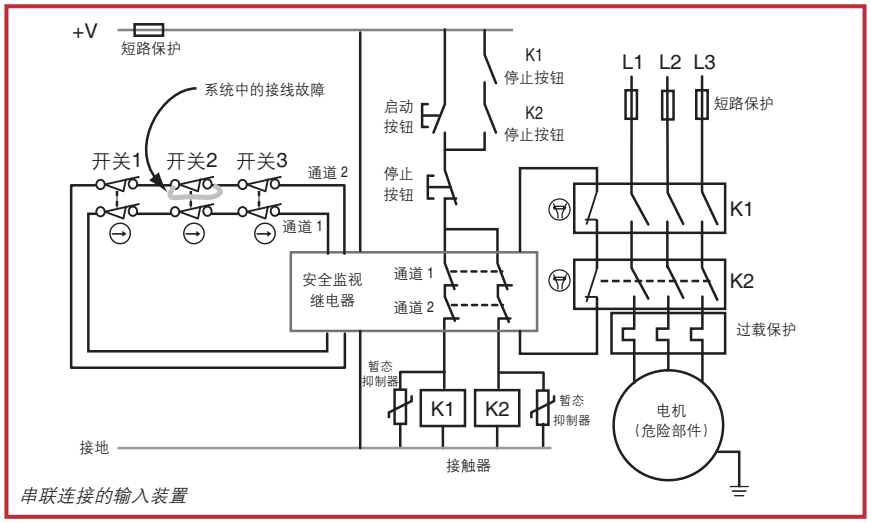
两个接触器有助于确保外部装置执行安全功能。采用过载与短路保护后减小了接触器触点烧熔故障的概率，但不是不可能的。接触器也会出现由于衔铁卡住其电源触点闭合的故障。如果一个接触器处于危险状态，另一个接触器就会切断危险部件的电源。MSR将在进行下一个机械周期前探测故障接触器。当安全门关闭，启动按钮按下时，故障接触器的机械连接式触点将保持打开状态，MSR将不能闭合其安全触点，由此识别出故障。

没有探测到的故障

如前文所述，一些故障是探测不到的。这些故障本身不会导致安全功能丧失。评估这些故障时必须先提出一些列问题。第一个问题的答案会引出不同的后续问题：*开始问题*：是否能探测到这类故障？

如果能探测到，则我们需要了解故障探测需要立即进行还是下一步进行。我们还需要了解这类故障是否能有其他装置遮蔽(即，清除)。

如果不能，那么这类故障是否会导致安全功能丧失？后续故障是否会导致安全功能丧失？

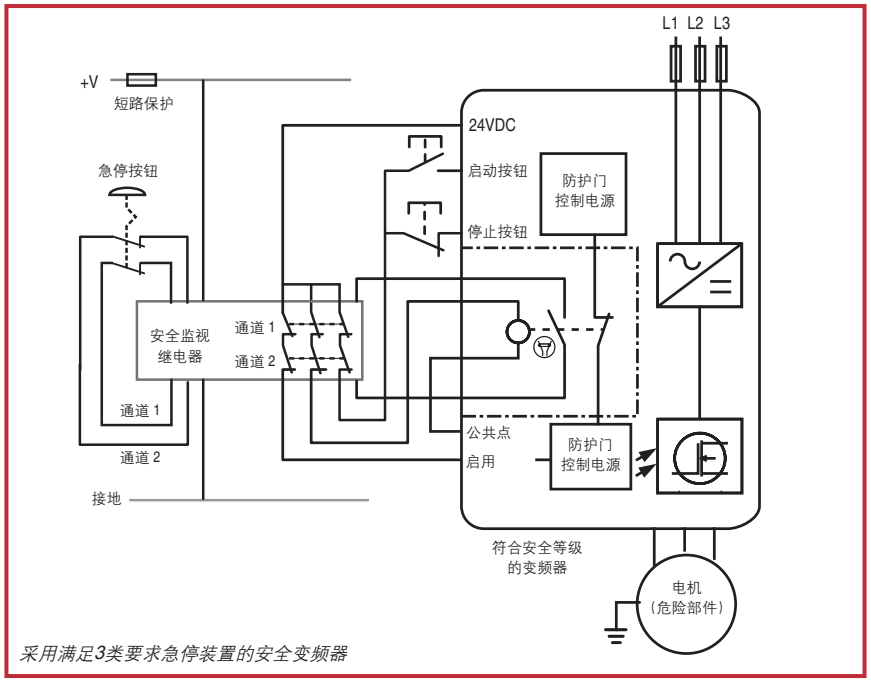


串联连接的输入装置

以下所示为一种被广泛使用的方法 - 将多个装置与一个安全监视继电器连接。每个装置中都有两个常闭型直接打开动作触点。这些装置可以是联锁机构或者急停按钮的混合装置。当输入装置采用菊花链型的连接方式时这种方法可以节省接线成本。假设在某对触点上发生短路故障。这种故障是够能被探测到？

当开关Sw1与Sw3打开时，MSR能成功切断危险部件的电源。当开关 Sw1与Sw3 闭合时，按下启动按钮后危险部件将重启。在执行这三个动作的过程中，故障被探测到，但没有导致安全功能丧失。当开关Sw2打开会出现什么情况呢？

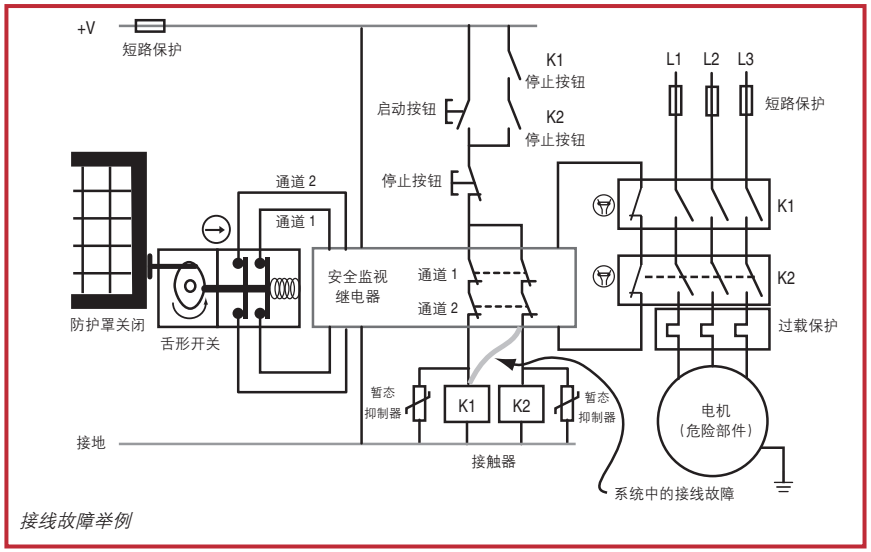
当Sw2打开，Ch1打开，Ch2保持闭合。因为Ch1打开，所以MSR切断危险部件的电源。当Sw2闭合，由于Ch2没有打开所以按下启动按钮电机也不能启动。该故障可以探测到。这种设计的弱点是Sw1 或者Sw3能够打开、闭合，也能清除故障。但后续故障(第二个触点或者Sw2发生短路)将导致安全功能丧失。因为故障聚集后可能会导致安全功能丧失，所以机械触点采用串联连接方式仅限在3类系统中使用。



采用满足3类要求急停装置的安全变频器

以下所示为3类系统的回路，回路中采用了达到安全等级的变频装置。随着近来在驱动技术方面的发展以及电气标准的不断更新，我们可以在急停回路中采用达到安全等级的变频器，而不需要为执行机构(如，电机)等级采用电动-机械式隔离开关。

按下急停按钮将打开MSR的输出。该操作将向变频器发出一个停止信号，撤销使能信号，打开防护门的控制电源。变频器执行0类停止过程 - 立即切断电机电源。因为变频器具有切断电机电源的冗余触点，所以变频器达到3类系统要求：启动与正向导引继电器。正向导引继电器向执行机构提供合理的、切合实际的反馈信号。经过对变频器本身的分析，确定单一故障不会导致安全功能丧失。

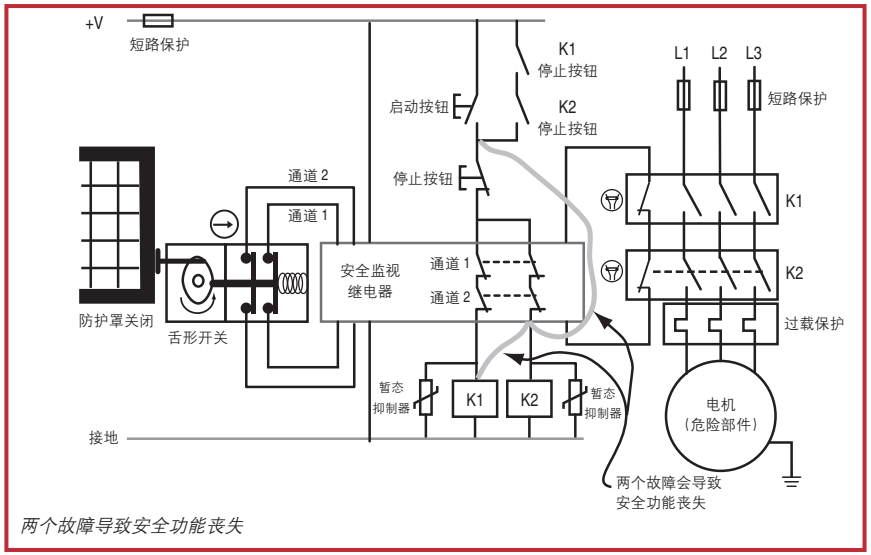


接线故障举例

以下示例为接线故障：从MSR通道2安全输出到接触器K1之间发生接线短路。所有部件工作正常。这种接线故障可能在机械调试前或者在以后的维护或者改进期间出现。

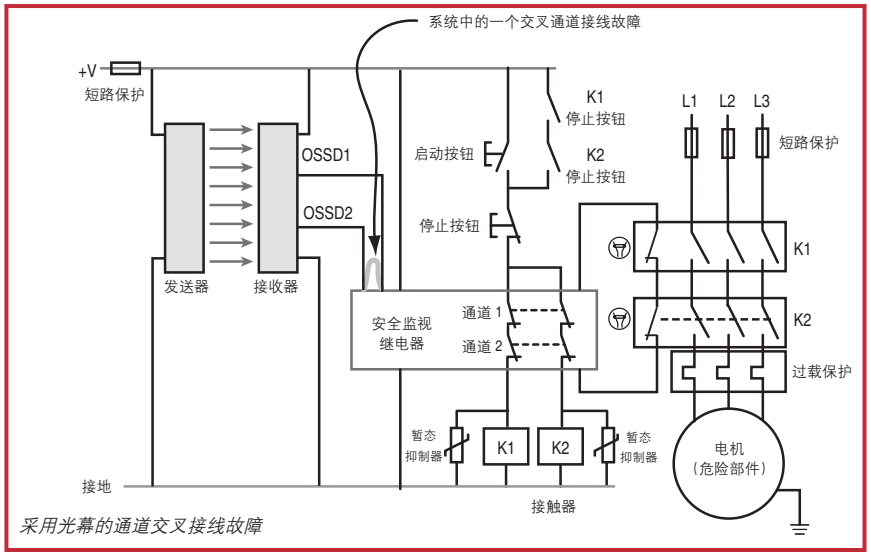
这种故障是够能被探测到?

如图所示的安全系统探测不到这种故障。但幸运的是，该故障不会导致安全功能丧失。必须在调试期间探测到该故障以及从Ch1到K2的故障。



两个故障导致安全功能丧失

以下所示为能导致安全功能丧失的第二个故障。该故障为SR输出与启动按钮之间发生短路。接通电源并且防护罩关闭后，这两个故障就无法探测到了。按下启动按钮将启动危险部件。但是，打开防护罩不会使危险部件停止运行。



采用光幕的通道交叉接线故障

以下所示为采用光幕(OSSD输出)的安全系统示例

这种安全系统是否能探测到这种故障?

因为两个输入均被抬高至+V，所以MSR不能探测到该故障。在该示例中，光幕可以探测到接线故障。一些光幕采用称作脉冲检测的故障检测技术。采用这些光幕后可以直接进行故障探测，光幕关闭其输出。其他情况下，故障探测是在光幕清除时进行的。当光幕试图使其输出带电时，已探测到故障并且光幕输出仍旧保持关闭。在以上

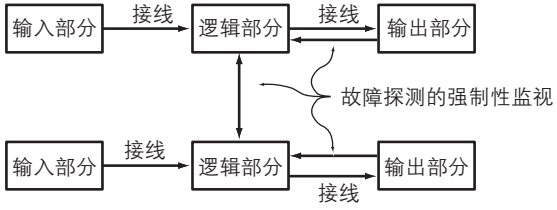
任一种情况下，在出现故障时危险部件始终保持停止状态。

脉冲检测式故障探测

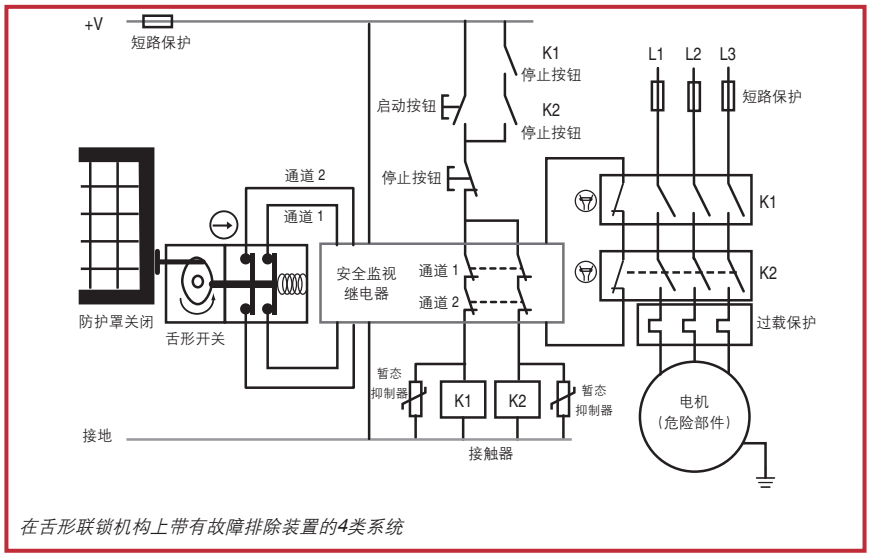
安全回路在安全系统激活，危险部件受到防护时流过电流。脉冲检测是一种回路电流在很短时间内降为零的技术。安全回路做出响应，使危险部件停止运行所需的时间很短，但是在如此短的时间内基于微处理器的系统足以进行故障探测。各通道内的脉冲会互相补偿。如果回路内出现交叉短路故障，微处理器会探测两个通道内的脉冲，然后发出危险部件停止运行的指令。

4类系统

与4类系统一样，4类系统要求安全系统满足B类系统的要求，使用安全原理并在出现单一故障时执行安全功能。与3类系统中聚集故障会导致安全功能丧失不同，4类系统要求在故障聚集时执行安全功能。当考虑故障聚集时，虽然在有些设计中需要考虑3个故障，但考虑两个故障就足够了。



以下所示为4类系统的方框图。监视两个输出装置与交叉监视是基本要求，而不是在合理、切合实际的情况下才需满足该要求。这是4类系统与3类系统的不同之处。

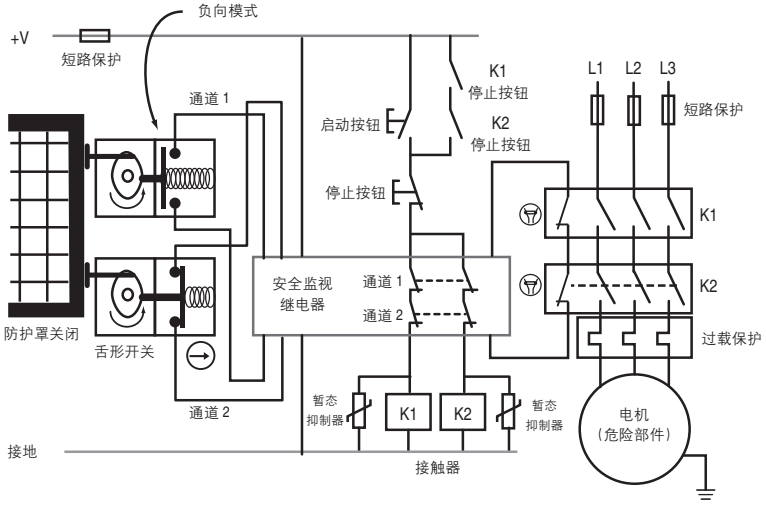


在舌形联锁机构上带有故障排除装置的4类系统

以下示例为4类系统。该系统在舌形联锁机构上采用故障排除部件。采用故障排除部件后不需要考虑舌形联锁触点打开的失效情况。故障排除部件必须经过技术论证并做记录。进行技术论证时必须考虑执行机构速度、执行机构找正情况、机械止动件、稳固的操作端部。

如果安全系统设计人员偏向使用舌形联锁机构，而不是在联锁机构上采用故障排除部件，则采用两个舌形联锁机构即可满足4类系统的要求。安全监视继电器必须达到满足4类系统要求的等级，必须监视采用机械式连接触点的两个输出接触器。

为了进一步减小由于常见模式或者常见原因造成的失效情况导致安全功能丧失的概率，我们可以进行改变部件。如果一个开关使用直接打开动作触点，则另一个开关就可采用负向动作模式。以下示例即为经过改变的方法。在这种方法中，MSR必须采用常闭与常开型输入。



采用不同冗余性舌形联锁机构的4类系统

部件与系统等级

ISO 13849-1标准要求部件与系统具有相同的等级。这样会造成混淆，但可以通过了解部件及其容量来澄清。我们会发现，根据系统的具体结构满足1类系统要求的部件可用于满足 2、3、4类系统要求的系统中。

B类与1类系统基于预防，而2、3、4类系统则基于探测。使用这些类型既可基于某个部件也可基于某个系统。典型的安全系统包括安全联锁开关、安全继电器与安全接触器。因为联锁机构与接触器仅仅是基于预防，所以属于满足1类系统的装置。这些装置采用安全原理，但是不执行任何故障探测与自检。如果在3、4类型系统中由逻辑装置执行故障探测，则可在冗余方式下使用这些装置。

逻辑装置不仅基于故障功能，而且基于故障探测功能。逻辑装置会进行内部自检，以确保功能正常。所以，安全监视继电器、可编程控安全制器经过评估后满足2、3、4类系统的要求

故障考虑事项与故障排除

进行安全分析时需要对故障进行大量分析，同时需要了解故障情况下安全系统的性能。ISO 13849-1与ISO 13849-2标准对故障考虑事项与故障排除做出了详细的规定。

如果一个故障造成随后的部件失效，则第一个故障与由此引起的后续故障应视作一个故障。

如果两个或更多的故障由同一个原因引起，则这些故障应视作单一故障。这就是人们熟知的常见故障。

两个或者多个故障同时出现的可能性很小，不属于本分析范围。在对安全系统提出的要求中，基本假设是仅出现一个故障。

如果按照相应标准设计部件与系统，则可以避免故障发生。例如，如果按照IEC 60947-5-1标注的附录K制造，则可以避免发生常闭触点打开的失效情况。ISO 13894-2 标准中列出了可排除的故障。

满足1类停止要求的系统

上述所有示例均采用0类停止方法(立即切断执行机构的电源)。采用延时输出可以实现1类停止(应用制动器直到停止工程结束)。1类型通常采用具有防护罩锁定功能的联锁式防护罩。这种结构就可在机械达到安全状态(如，停止)前防护罩保持关闭。

没有正确考虑可编程控制器的机械停止过程会影响到机械重启，使工具或者机械造成严重损坏。与安全有关的停止过程不能仅仅依靠标准(非安全性)PLC，所以需要考虑其他方法。

以下为三种解决方案：

1. 安全PLC

在涉及安全的应用中采用具有较高安全集成水平的PLC。实际上，将诸如GuardLogix等安全PLC用于安全与非安全控制系统就可实现该目的。

2. 采用延时超驰指令的安全继电器

采用具有即时输出与延时输出的安全继电器(如，MSR138DP)。即时动作输出与可编程装置的输入(如PLC)，延时动作输出与接触器连接。当防护罩联锁开关动作时，安全继电器的即时输出动作。该动作会向可编程系统发出信号执行正确顺序停止过程。该过程经过足够长的允许时间后，安全继电器的延时输出会切断主接触器电源并将其隔离。

注意：通过计算确定总停止时间时必须考虑安全继电器的延时。当根据安全距离计算结果利用该系数确定装置的位置时，这点尤其重要。

3. 由可编程系统控制的防护罩锁定装置

这种解决方案具有很高硬接线集成度以及进行正确顺序停机的能力，但这种解决方案仅适于通过防护罩保护危险部件的情况。

为能打开防护罩门，联锁开关的电磁阀锁必须收到由PLC发出的释放信号。为了降低工具损坏或者防止程序丢失，该释放信号仅在停止指令顺序结束后才能发出。电磁阀得电时，可以打开防护罩门。防护罩门打开可使联锁开关上的控制回路触点动作，将机械的主接触器隔离。为了克服机械缓慢停机或者出现假释放信号，PLC需要配套使用与延时单元(如，MSR178DP)或者停止动作探测器(如，CU2)。

美国的安全控制系统要求

在美国，可在许多不同标准了与安全有关的系统的具体要求，但其中两个标准最突出： ANSI B11.TR3与ANSI R15.06。ANSI B11.TR3规定了四种等级 。每种等级均以该等级下可预计减少的风险数量为其特征。

每种等级的具体要求如下：

最低等级

ANSI B11.TR3标准规定，安全防护装置降低风险的等级最低，包括电器、电子、液压、气动装置以及使用当通道配置的相应控制系统。这些要求的含义是要求使达到安全等级的装置。这与ISO 13849-1标准中的1类系统要求非常接近。

风险降低的低/中等级

ANSI B11.TR3的规定，达到低/中等风险降低的安全防护装置包括具有冗余功能的控制系统，并能对这些冗余功能进行手动检查以验证安全系统的性能。单纯看各项要求，系统采用了简单的冗余功能。故不需要使用检查功能。如果不进行检查，其中一个冗余安全部件会出现故障，所以安全系统无法实现该冗余部件的功能。因此，我们需要单通道系统。都能使用检查功能时，风险降低等级与2类系统要求最吻合。

风险降低的高/中等级

ANSI B11.TR3的规定，达到高/中等风险降低等级的安全防护装置包括具有冗余功能的控制系统，并能在启动后进行自检以确认安全系统的性能。对于每天都启动的机械，自检功能显著提高了单纯冗余系统的安全集成度。对于24/7时间内运行的机械来讲，自检功能没有什么意义。定期对安全系统进行监视便达到3类系统的要求。

风险降低的最高等级

ANSI B11.TR3规定，控制系统采用具有连续自检功能的冗余部件后可以实现最风险降低的最高等级。自检功能必须能够验证安全系统的性能。判定什么是连续性是安全系统设计人员面临的挑战。在启动、安全系统接到执行请求时，许多安全系统执行自检。

另一方面，一些部件进行连续自检。例如光幕会按照一定顺序接通、熄灭其LED指示灯。由于光幕在进行连续自检，所以出现故障时，光幕会在安全系统接到执行请求前关闭其输出。基于微处理器的继电器与安全PLC属于能够进行联系自检的其他类型部件。

满足控制系统的“连续”自检要求并不是说限定在选择光幕与基于微处理器的逻辑单元。自检过程应在启动时、安全系统的每一个执行请求后进行。这种风险降低等级的目的是满足ISO 13894-1标准中4类系统的要求。

机器人标准：美国与加拿大

美国(ANSI RIA R15.06)、加拿大(CSA Z434-03)采用相似的机器人标准。这两种标准均分为四个等级，与EN954-1:1996标准中的分类相似。

简单级

在该最低等级中，必须设计简单的安全控制系统，采用认可的单通道回路制造。同时，这些系统可以是可编程型系统。在加拿大，这种等级仅对信号发送与通知目的进行了进一步限制。判定什么是“被认可的”是安全系统设计人员面临的挑战。什么是被认可的单通道回路？采用这样通道的系统会被认可吗？该简单级与 EN954-1:1996 标准中的B类最接近。

信号通道

第二个等级为满足以下要求的单通道安全控制系统。

- 基于硬件的系统或者达到安全等级的软件/固件装置
- 包括达到安全等级的部件
- 根据厂家的建议使用
- 使用经过认证的回路设计。

如能在失电状态下发送停止信号的、单通道电动机械正向分断装置就是经过认证的回路设计。因为是单通道系统，所以单一部件失效就能导致安全功能丧失。该简单级与EN954-1:1996标准中的1类最接近。

与安全有关的软件/固件装置

虽然基于硬件的系统一直是为机器人提供防护的首选方法，但由于其应对复杂系统的能力，软件/固件装置越来越成被广泛使用。如果软件/固件装置(安全PLC或者安全控制器)达到安全等级，则允许使用这些装置。该等级要求，单个达到安全等级的部件或者固件失效后不会导致安全功能丧失。当探测到故障时，直到该故障清除前阻止机器人继续自动运行。

为达到安全等级，必须由认可的实验室按照认可的标准对软件/固件装置进行测试。在美国，OSHA保留了一份国家认可的测试实验室(NRTL)清单。在加拿大，加拿大标准协会保留了一份类似的清单。

具有监视功能的单通道

具有监视功能的单通道安全控制系统必须满足有关单通道的要求，必须达到安全等级，能应用检查功能。必须机械启动时检查安全系统功能，也必须在正常运行期间定期检查安全系统的功能。相对于手动检查而言，最好采用自检功能。

如果没有探测到故障，则允许机器人运行。如果探测到故障则发出停止信号。如果停止后还存在危险，则应进行报警。当然，检查过程本身不应造成危险情况。探测到故障后，直到故障清除前机器人必须保持安全状态。

具有监视功能的单通道与EN954-1:1996标准中的2类最接近。

控制可靠性

在美国与加拿大，通过采用满足控制可靠性要求、达到安全等级的控制系统实现最高级风险降低标准。控制可靠、达到安全等级的控制系统为具有监视功能的双通道结构。禁止由任何单通道部件失效阻止机器人执行停止功能，也包括监视功能。

在监视过程中如果探测到故障时应发出停止指令。如果停止动作结束后危险仍存在，则必须发出警告信号。安全系统在故障清除前必须保持安全状态。

故障最好能在失效期间探测到。如果不能做到这一点，则必须在安全系统的下一个执行请求前探测到该失效情况。

如果某种失效情况发生的概率很大，则应将其视作常见失效情况。

加拿大标准语美国标准不同，前者多出两个要求。首先，与安全有关的系统应与正常控制系统无关。第二，安全系统必须不易被破坏，在未经过探测之间不得忽略安全系统。

控制可靠性系统与EN954-1:1996标准规定的3、4类系统一致。

控制可靠的部件：

控制可靠性的最基本方面是能够承受单一故障。该要求规定了安全系统在“单一故障”、“任何单一故障”或者“任何单一部件失效”的情况下必须做出怎样的响应。

关于这些故障，必须考虑三个非常重要的概念：(1)没有探测到所有故障，(2)增加“故障”二字后会产生有关接线的问题，(3)接线输入安全系统。接线故障会导致某个安全功能丧失。

控制可靠性的目的很明确，那就是故障时的安全工功能系统的性能。探测到故障时，安全系统必须执行安全措施，发出故障通知，阻止机械在故障清除前继续运行。如果没有探测到故障，在安全系统的下一个执行请求前必须仍能执行安全功能。

控制系统功能安全的说明

重要事项：*本部分考虑相对较新的标准与要求。我们的工作仍将在某些方面展开，尤其是在阐明与组合这些标准方面。所以，有些细节地方会出现变化。有关最新的信息，请登陆网址：http://www.ab.com/safety.*

本文件出版的同时，人们也越来越意识到，需要有新一代的标准能够涉及到对安全等级的系统与装置的功能安全性的要求。

何为功能安全？

功能安全属于总安全的一部分。总安全由过程的正确功能或者对其输入做出响应的设备正确功能决定。为了帮助阐明安全功能的含义，IEC网站给出了一下示例。“例如，温度过高保护装置利用安装在电机绕组中的温度传感器在绕组过热前使电机停止就是安全功能的一个示例。但是，采用能够承受高温的绝缘材料不属于功能安全(尽管这种绝缘材料是一个安全示例，也能预防完全相同的危险)。” 另外一个示例就是比较硬防护装置与联锁式防护罩。虽然应防护装置也能像联锁安全门一样阻止靠近危险部件，但也不应视作“功能安全”。联锁安全门就是功能安全的一个示例。当防护罩打开时，联锁机构便作为能够达到安全状态的某个系统的“输入”。同样，个人防护器具(PPE) 是作为一种防护性措施，有助于增加人员自身安全。PPE也不属于功能安全。

IEC 61580:1998标准引入了安全功能术语。至此，该术语便有时只与可编程安全系统联系在一起。这是一种错误认识。安全功能涵盖许多用于创建安全系统的装置。光幕、安全继电器、安全PLC、安全接触器等装置以及安全变频器相互连接后可组成安全系统，能够执行与具体安全有关的功能。这就是安全功能。所以，电气系统的功能安全、对机械移动部件造成危险的控制两者之间存在很大联系。

满足功能安全必须满足两类要求：

- 安全的功能
- 安全的完整性

在提出功能安全要求的过程中，风险评估过程具有关键作用。有危险分析可推导出安全功能要求(该安全功能的目的)。由风险评估得出安全完整性要求(安全功能顺利执行的可能性)。

有关机控制系统械功能安全最重要的三个标准是：

1. **IEC/EN 61508**“电气、电子、可编程电子控制系统的功能安全性”

   该标准包含了适于设计复杂电子与可编程系统及子系统的各种要求与规定。该标准属于通用标准，所以没有限定为机械领域。

2. **IEC/EN 62061**“机械安全性 - 电气、电子、可编程电子控制系统的功能安全”

   该标准为IEC/EN 61508标准在机械方面专门补充内容。该标准中提出的各种适用于按照系统级别设计所有与机械安全有关的所有电子控制系统，也适用于设计非复杂性系统及子系统。该标准要求，复杂的或者可编程子系统应满足IEC/EN 61508。

3. **EN ISO 13849-1:2008**“机械安全性 - 控制系统中达到安全等级的部件”

   该标准旨在为从类型要求向功能安全过渡提供路径。

相比如可靠控制与ISO 13849-1:1999(EN 954-1:1996)等现有要求，功能安全要求领先了一大步。目前各种类型要求还在使用，原来的标准将一致使用到2010年，以便有时间向新的修订版本过渡。ISO/EN 13849-1标准的新版本使用了功能安全概念，引入了新技术，提出了新要求。在这部分，我们将引用新版标准EN ISO 13849-1:2008。

由于有关功能安全的新标准不仅代表着未来技术，而且使用更加灵活，可以简化新机械安全技术的使用，所以人们会对这些标准越来越有兴趣。

IEC/EN 62061与EN ISO 13849-1:2008 标准

IEC/EN 62061与EN ISO 13849-1:2008标准均包含了与安全有关的电气控制系统。最终目的是运行通用术语将这两个标准合并成一个标准的两部分。这两个标准采用的方法不同，但结果相同。这些标准旨在让用户自行选择最适合自己条件的标准。用户可选择这两种标准中的任何一种。

采用这两种标准后，可获得同样等级的安全性能与安全完整性。每种标准采用的方法存在差异，但都适于各自的读者。EN ISO 13849-1:2008在其说明部分的表1中给出一种限定情况。当采用复杂的可编程技术时，应将最高PL视作PLD。

为了能够采用复杂的、可由先前非传统系统结构执行的安全功能，IEC/EN 62061标准提供相应的方法。为了提供采用传统的系统结构执行更传统的安全功能所需的更直接、更简单的路径，EN ISO 13849-1:2008标准也给出了相应的方法。

这两种标准的重要区别是适用于不同的技术领域。IEC/EN 62061标准仅限于在电气系统领域。EN ISO 13849-1:2008标准则适用于启动、液压、机械以及电气系统。

以下概括介绍说明两种标准在价值与合理性方面隐含的相似性。不过我们必须明白这些仅是简要的概括性内容。两种标准所涵盖的内容远超过本文所示，所以必须考虑这两种标准的全部内容。

下表给出的简单流程图有助于安全系统设计人员确定使用哪一种标准。每个路径的共同点是：安全功能与风险评估。由于以上路径走向这个标准或者那个标准，所以系统设计信息也不同(如，PFH、MTTF、DC、SFF)。

SIL与IEC/EN 62061 标准

IEC/EN 62061标准介绍了应减少的风险数量，也介绍了用SIL(安全完整性)表示的控制系统减少风险的能力。在机械领域应用3种SIL，其中SIL 1属于最低级别，SIL属于最高级别。

在诸如过程工业等其他领域会出现更大的风险。为此，IEC61508标准与过程领域的专用标准IEC61511均包含了SIL 4。一个SIL应用于一个安全功能。执行安全功能系统的子系统必须具有相应的SIL能力。这种情况有时候作为SIL要求极限(SIL CL)。应用IEC/EN 62061前，需要全面详细研究其内容。该标准中一些最常见适用要求总结如下：

PL与EN ISO 13849-1:2008

EN ISO 13849-1:2008标准不使用术语SIL，而是使用PL术语(性能等级)。在许多方面，PL与SIL 存在联系。有五种性能等级，PLa为最低级别，PLe为最高级别。

PL与SIL的比较

该表说明了PL与SIL应用于采用低复杂性电动机械技术的典型回路结构时，PL与SIL之间的大致关系。

PL (性能级别)	PFH_D (每小时的危险性失效概率)	SIL (安全完整性级别)
A	$\geq 10^{-5}$ to $<10^{-4}$	无
B	$\geq 3 \times 10^{-6}$ to $<10^{-5}$	1
C	$\geq 10^{-6}$ to $<3 \times 10^{-6}$	1
D	$\geq 10^{-7}$ to $<10^{-6}$	2
E	$\geq 10^{-8}$ to $<10^{-7}$	3

PL与SIL之间的大致相同部分

***重要事项**：上表所述为一般性指南，可用于转换。必须考虑该标准规定的全部要求。*

按照IEC/EN 62061进行系统设计

IEC/EN 62061“机械安全 - 与安全有关的电气、电子、可编程电子控制系统的功能安全”标准是IEC/EN 61508标准中的专门面向机械领域部分。该标准为与机械安全有关的、所有类型的电气控制系统的系统级设计，为非复杂性系统或者装置的设计提出了相应要求。

通过风险评估可得出风险减少策略。通过该风险减少策略又可确定是否需要与安全有关的控制系统。必须记录这些功能，并且这些功能必须包括：

- 功能要求规范
- 安全完整性要求规范。

功能要求包括诸如运行频率、所需的响应时间、运行模式、工作制周期、运行环境与故障反应功能。安全完整性要求用称作安全完整性级别(SIL)的级别形式表示。根据系统的复杂程度确定系统是否满足所需的SIL级别时，我们必须考虑表中列出的一些或者全部因素。

SIL 的考虑要素	符号
每小时危险性失效的概率	PFH_D
硬件的故障承受能力	HFT
安全失效分数	SFF
验证试验时间间隔	T1
诊断试验时间间隔	T2
对常见原因失效的敏感度	ß
诊断范围	DC

SIL所需的考虑因素

与电动机械装置的大量操作相比，造成电子系统失效的重要原因就是时间。所以，电子系统的失效率将以小时为基础考虑。必须进行部件分析以确定其失效概率。对于安全系统来讲，我们关注的不仅是失效概率，而且更重要的是以小时为单位统计危险性失效概率 - PFHD。一旦知道具体概率，我们就能使用下表确定系统达到哪级SIL。

SIL (安全完整性级别)	PFH_D (每小时危险性失效的概率)
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

各SIL级别的危险性失效概率

安全系统可分为多个子系统。硬件安全完整性等级可由硬件的故障承受能力、子系统的安全失效分数确定。硬件的故障承受力即系统在故障情况下完成其功能的能力。故障承受力为零即表示出现单一故障时系统不能执行其功能。某个系统的故障承受能力就是在出现故障时子系统能够执行其功能。安全失效分数属于不会造成危险性失效情况的总失效率的一部分。这两部分组合后便是我们熟知的结构性限制，用SILCL表示。下表说明了结构限制与SILCL的关系。

安全失效分数 (SFF)	硬件的故障承受能力		
	0	1	2
<60%	不允许， 除非出现特殊例外情况。	SIL1	SIL2
60% - <90%	SIL1	SIL2	SIL3
90% - < 99%	SIL2	SIL3	SIL3
≥99%	SIL3	SIL3	SIL3

SIL的结构性限制

例如，无论危险性失效的概率有多大，具有单一故障承受力且安全失效分数为75%的结构的安全完整性等级不得超过SIL2。

为了计算危险性失效的概率，必须就爱那个每个安全功能分解成多个功能块，然后按照子系统实现这些功能。多安全功能系统的设计包含于逻辑装置连接的检测装置，其中逻辑装置又与执行机构连接。这样就形成了子系统的布局。如果我们能够确定每个子系统的危险性是小概率，知道其SILCL，那么通过将各个子系统的失效概率相加就可得很容易的算出系统的失效概率。这种方法如下所示。

例如，如果我们需要达到SIL 2级，则每个系统的SIL要求极限值(SIL CL)至少为SIL，系统的PFHD总值不得超过以上“SIL危险性失效概率”表中的允许值。

在IEC/EN 62061标准中术语“子系统”具有特殊的含义，是一个系统分为多个部分后的一级再分部分，并且如果这些再分部分失效会导致安全功能失效。所以，如果两个冗余型开关用于一个系统中，则任何一个开关都不能作为一个子系统。子系统应由两个开关及其相关的故障诊断功能(如有)组成。

子系统设计 - IEC/EN 62061标准

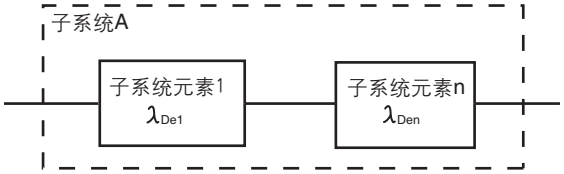
例如，如果系统设计人员按照IEC/EN62061标准采用能够随时“封装”入子系统的部件，则设计工作就简单多了，因为此时不需要满足有关子系统设计的具体要求。通常，是否满足这些要求由装置(子系统)厂家负责，并且这些要求比系统设计要求要复杂的多。

IEC/EN 62061标准要求诸如安全PLC等复杂系统应符合IEC 61508标准。这就是说，IEC 61508标准的所有严格条款适用于采用复杂电子部件或者可编程部件的装置。这将是一个非常困难、复杂的过程。例如，采用复杂系统估算PFH_D可能会是非常复杂的过程，在该过程中将使用到如Markov模型、可靠性功能框图或者故障树分析等技术。

IEC/EN 62061标准未对低复杂性子系统设计作出要求。一般来讲，这种设计包括相对简单的联锁开关、电动机械式安全监视继电器。虽然不像IEC 61508标准中的要求那样棘手，但也是相当复杂的。

IEC/EN 62061标准给出了四个子系统逻辑结构、估算低复杂性子系统达到的PFHD时可能用到的公式。这些结构是单纯的逻辑表示法，不应视作实际结构。这四个子系统逻辑结构以及伴随公式如下文四个图所示。

对于如下图所示的基本型子系统而言，仅需把各个危险性失效概率简单相加即可。



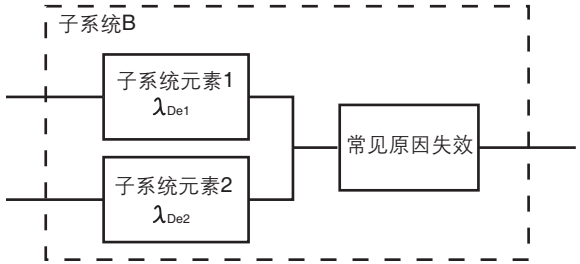
子系统逻辑结构A

$\lambda_{DssA} = \lambda_{De1} + \ldots + \lambda_{Den}$

$PFH_{DssA} = \lambda_{DssA} \times 1h$

拉姆达λ表示视效率。失效率单位为失效数量每小时。λ_D拉姆达带下脚标D表示危险性失效率。λ_{DssA}拉姆达带下脚标DssA表示子系统A的危险失效率。拉姆达带下脚标DssA是单独元件e1、e2、e3、... en之和。危险性失效概率乘以1得到1小时内危险性失效的概率。

下一幅图所示为没有诊断功能的单故障承受系统。当该结构包含了单故障承受能力后，就会存在常见原因失效可能性，同时也必须考虑这种可能性。常见原因失效的的推导过程将在本章稍后部分做简要介绍。



B类子系统逻辑结构

$\lambda_{DssB} = (1-ß)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + ß \times (\lambda_{De1} + \lambda_{De2}) / 2$

$PFH_{DssB} = \lambda_{DssB} \times 1h$

这种结构采用的公式考虑了子系统元件并联布置的情况，并从上表“SIL的考虑要素”中增加两个要素。

ß – 对常见原因失效的敏感性(贝它)

T1 – 验证试验时间间隔或者使用期限，选其中时间较短的。验证试验用于探测子系统的故障、性能降低情况，以使子系统恢复到运行状态。

我们假设以下值：

ß = 0.10

$\lambda_{De1} = 1 \times 10^{-6}$ 失效/小时

$\lambda_{De2} = 1 \times 10^{-6}$ 失效/小时

T1 = 87600 小时(10年)

该系统的视效率为1.70956E-07次失效/小时(SIL2)。

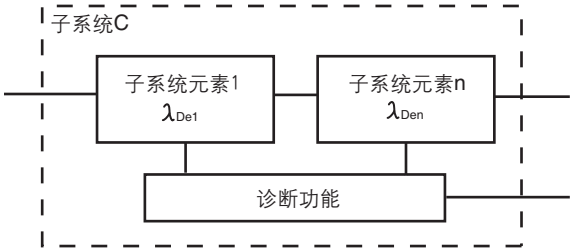
验证试验时间间隔的影响

让我们看一下验证试验时间间隔对系统的影响。假设将验证试验时间间隔缩短为一年两次。T1将减小为4380小时，危险性视效率将提高到1.03548E-07此失效/小时。但仍属于 SIL2 级。如果验证试验时间间隔缩短至每月一次(730小时)，则危险性视效率将提高至1.0059E-07次失效/小时。但仍属于SIL2级。如果还需要提高视效率，则验证试验时间间隔或者常见原因失效应达到SIL3级。另外设计人员必须清楚，将该子系统与其他子系统合并后才可计算总的危险失效率。

常见原因失效影响的分析

让我们看一常见原因失效对系统的影响。假设我们采用其他方法，其中ß值提高到最佳值1%(0.01)，验证试验室时间间隔仍保持10年。系统失效率提高至9.58568E-08。现在，该系统达到SIL3级。

下一幅图所示为具有诊断功能的、零故障承受系统的功能表达式。诊断范围可用于降低危险性硬件失效的概率。诊断试验自动进行。诊断范围是探测到的危险性失效率与所有危险性失效率的之比。计算诊断范围时不考虑安全失效的类型或者数量，诊断范围仅用探测到的危险性失效数量的百分值表示。



C类子系统逻辑结构

$\lambda_{DssC} = \lambda_{De1} (1\text{-}DC_1) + \ldots + \lambda_{Den} (1\text{-}DC_n)$

$PFH_{DssC} = \lambda_{DssC} \times 1h$

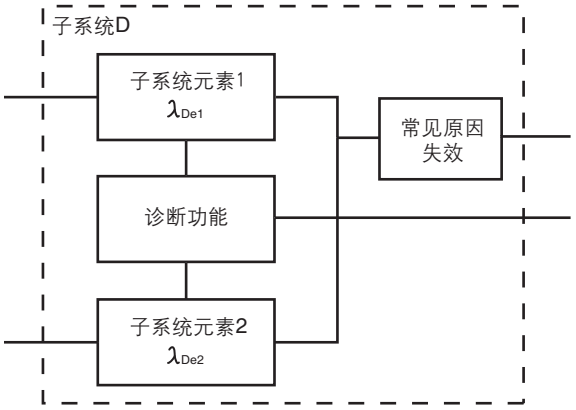
这些公式中包含了每个子系统要素的诊断范围、DC。每个子系统的通过其诊断范围可降低各自失效率。

第四个示例的子系统结构如下图所示。该子系统能够承受单故障，具有诊断功能。考虑单故障承受系统时，也必须考虑潜在的常见原因失效情况。

如果子系统的各个要素相同，那么可用以下公式：

$\lambda_{DssD} = (1 - ß)^2 \{ \lambda_{De}^2 \times 2 \times DC \times T_2 / 2 + \lambda_{De}^2 \times (1\text{-}DC) \times T_1 \} + ß \times \lambda_{De}$

$PFH_{DssD} = \lambda_{DssD} \times 1h$



D类子系统逻辑结构

如果子系统的各个要素不同，那么可用以下公式：

$\lambda_{DssD} = (1 - ß)^2 \{ \lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2) \times T_2 / 2 + \lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2) \times T_1 / 2 \} + ß \times (\lambda_{De1} + \lambda_{De2}) / 2$

$PFH_{DssD} = \lambda_{DssD} \times 1h$

注意，两个公式均适用一个补充参数诊断间隔T2。

例如，我们可为子系统要素不同的示例假设以下值：

ß = 0.10

λ_{De1} = 1 x 10 -6失效/小时

λ_{De2} = 2 x 10 -6失效/小时

T1 = 87600小时(10年)

T2 = 876小时

DC1 = 0.8

DC2 = 0.6

PFH_{DssD} = 2.36141E-07次危险性失效/小时

各分类之间转换方法

在编写IEC/EN 62061期间，技术委员会发现系统与装置所需的全部数据经过一定时间会变成完全有效的数据。该标准给出了两个表格。借助这两个表格可转换那些基于原始分类概念、经过使用证明是有效的现有子系统设计。通过这两个表格可以得到等效的PFH_D与结构限定条件。这些表格为功能安全标准的转换提供便捷的路径。在本文中这些表格经过了稍稍简化。如果对这些表格进行研究，前几章中给出的许多分类系统的示例结构可保留在功能安全标准概念范围内。这样的结果很明显。

类别	故障承受能力	诊断范围	可以要求子系统达到的PFH_D
1	0	0%	见IEC/EN 62061
2	0	60%-90%	$\geq 10^{-6}$
3	1	60%-90%	$\geq 2 \times 10^{-7}$
4	>1	60%-90%	$\geq 3 \times 10^{-8}$

基于 PFHD 要求的分类

上表“SIL的结构限定条件”是该标准中表7的简化版本。当某个基于分类的子系统属于必须满足IEC/EN62061标准的SRCS的一部分时，应使用该表。为简单起见，设计人员可要求$PFH_D = 2 \times 10^{-7}$用于诊断范围为60%，基于3类的系统。另外，安全设计人员可进行全面的分析，确定是否能要求更好的PFHD。

类别	故障承受能力	SFF	按照架构限制条件确定的最大SIL要求极限值
1	0	< 60%	见IEC/EN 62061
2	0	60%-90%	SIL 1
3	1	< 60%	SIL 1

基于分类的结构限定条件

利用“基于分类系统的PFHD要求”可确定一个基于分类的子系统的SIL要求限制条件。基于分类的系统第诊断范围必须转换为安全失效分数。

了解PFH_D与基于分类的系统的SIL CI后，安全系统设计人员可将这些值应用到上述所示的某个系统中。如果基于类别的系统属于完全的SRCS，则等效的SIL与PFH_D“SIL的结构限制条件”表与“基于分类的PFHD要求”表确定。安全系统设计人员也必须满足有关常见原因失效、系统失效与验证试验时间间隔的要求。在每种标准中，用于常见原因失效的分值系统会稍稍不同。在这两种标准中，系统安全完整性的概念相似。在两种标准均没有采用分值系统。验证试验时间间隔可与任务执行时间相同，或者选择较短的时间间隔。

结构限制条件

一个系统或者子系统能够达到的安全完整性等级会受到结构特性的限制。两个主要的特性是硬件的故障承受力与安全失效分数。其他特性包括常见原因故障与故障排除。

当组合子系统时，由SRCS达到的SIL会受到限制，只能低于或者等于与安全有关的控制系统中任何子系统的最低SIL要求限制。

B10与$B10_d$

对于电动机械式子系统，估算其失效概率时应考虑厂家声明的运行周期、负载与工作制周期。失效概率用B10值表示，其含义为一段预计时间，在该时间将有10%的子系统失效。$B10_d$也是一段预计的时间。在该时间内，将有10%的子系统进入危险状态。

常见原因失效(CCF)

当单个原因造成的多个故障导致危险性失效时就是常见原因失效。一般来讲，子系统设计人员，通常是制造商仅需要有关CCF的信息。这些信息将用作估算子系统PFHD时给定公式的一部分。进行系统级别设计时不需要这些信息。IEC/EN62061标准的附录F中介绍了估算CCF的方法。下表总结了分值确定过程。

编号	避免CCF的措施	分值
1	单独/隔离	25
2	密度	38
3	设计/应用/经验	2
4	评估/分析	18
5	能力/培训	4
6	环境	18

计算防止常见原因失效措施的分值

使用特殊的措施防止CCF会增加分值。将分值相加后确定常见原因失效分数，具体如下表。在子系统模型中使用的系数贝塔ß用于调节“失效率”。

总分值	常见原因失效系数(ß)
<35	10% (0,1)
35 - 65	5% (0,05)
65 - 85	2% (0,02)
85 - 00	1% (0.01)

常见原因失效的系数ß

诊断范围(DC)

自动诊断试验用于减小危险性硬件失效的概率。能够探测到100%的危险性硬件失效是一种理想状态，实际中很难达到。

诊断范围是探测到的危险性失效数量与所有的危险性失效数量的比值。

$$DC = \frac{\text{探测到的危险性失效率}\lambda_{DD}}{\text{总的危险性失效率}\lambda_{D\text{总}}}$$

诊断范围的值将在0与1之间。

硬件的故障承受能力

硬件的故障承受能力是指某个子系统在造成危险性失效前能够承受的故障数量。例如，硬件的故障承受能力为1时表示有2个故障会导致一个与安全有关的控制功能丧失，但是一个故障不会。

功能安全的管理

标准中规定了实现与安全有关的电气控制系统所必需的控制管理与技术活动的要求。

危险性失效的概率(PFH_D)

实现一个系统或者子系统的任何给定SIL能力的部分要求就是由于硬件随机失效导致的 PFH_D数据(每小内危险性失效概率)。

这些数据由厂家提供。最近，罗克韦尔自动化已经公布了其安全部件与系统的数据(例如，GuardLogix、GuardPLC、SmartGuard与Kinetix(采用GuardMotion)、联锁开关、急停装置)。

IEC/EN 62061标准也做出了明确规定，在可行的情况下可采用可靠性数据手册。

对于复杂程度低的电气装置，失效机构通常与操作频率与数量有关，而非只与时间有关。所以对于这些部件来讲，这些数据将从使用期限试验中获得(如，B10试验)。B10是基于每年的预计操作数量的各种操作应用数量。然后，就需要将$B10_d$或者其他类似数据转换为$MTTF_d$(危险时效的平均时间)。然后，再将该数据转换为PFH_D。

通常，我们可以做一下假定：

$$PFH_D = 1/MTTF_d$$

对于电动机械式装置来讲：

$MTTF_d = B_{10d} /(0.1 \times$ 每年操作次数的平均值)

$MTTF_d$公式基于假设视效率为常数。失效的累积分布值为$F(t) = 1 – \exp(-\lambda dt)$。

验证试验时间间隔

验证试验时间间隔表示一段时间，经过时间后子系统必须经过彻底检查或者更换以确保该子系统达到“新系统”的状态。实际中，在机械领域通过更换达到这一目的。因此，验证试验时间间隔通常就是使用期限。EN ISO 13849-1:2008标准则指进行任务的时间。

验证试验用以进行检查，确认SRCS中的故障与性能降低情况，从而能使SRCS可以恢复至接近于“新系统”的状态。验证试验必须能探测出100%的危险性失效。单独通道必须单独进行验证试验。

与自动进行诊断试验比较，验证试验通常是在离线状态下手动进行。由于诊断试验自动进行，所以进行诊断试验时通常与很少进行的验证试验比较。例如，回路会对防护罩上的联锁开关进行自动检测，通过诊断试验(如，脉冲)确认有无短路或者开路状态。

验证试验时间间隔必须由厂家公布。厂家有时会提供验证试验时间间隔的范围。那么，应通过对用于选定结构的公式进行审核确定正确的验证试验时间间隔。一般来讲，验证试验时间间隔越短，视效率越低。

安全失效分数(SFF)

安全失效分数与诊断范围类似，同时也考虑许多有故障到安全状态的固有趋势。例如，当熔断器烧熔时出现一个失效情况，但是这种失效情况很可能会导致开路，而在大多数情况下开路是一个“安全”失效。SFF是(“安全失效率” + 探测到的危险性失效率)与(“安全”失效率 + 探测到的与未探测到的失效率)之比。重要的一点是，只有那些被考虑的失效类型才会是会对安全功能又影响的失效类型。

绝大多数复杂程度低机械装置，如急停按钮、联锁开关(本身)的SFF将小于60%，所以在冗余、监视设计过程中安全性电子装置的SFF大于90%是普遍的。SFF值通常由厂家提供。

可采用以下公式计算安全失效分数(SFF)：

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD}) / (\Sigma\lambda_S + \Sigma\lambda_D)$$

式中

λ_S = 安全失效率

$\Sigma\lambda_S + \Sigma\lambda_D$ = 总安全失效率

λ_{DD} = 探测到的危险性安全失效率

λ_D = 危险失效率

系统失效

该标准对控制与避免系统失效提出了相应要求。与随机发生的硬件随机失效不同，系统失效一般是由在硬件的某些部分性能降低后造成的。可能出现的典型系统失效为软件设计错误、硬件设计错误、技术规范要求错误与运行步骤。为避免系统失效而必须采取的措施包括：

- 部件的正确选型、组合、布局、组装、安装。
- 采用良好的工程惯例
- 遵守制造商提供的技术规范与安装说明
- 确认部件之间相互兼容
- 能够承受外部环境条件
- 采用合适的材料

该标准规定了避免系统失效所需的更多、更详细的要求。该标准中不包含确定潜在系统失效所占百分比时所用的分值系统。为满足SIL3的要求，设计人员必须满足有关避免系统失效的所有要求。如果无法满足所有要求，则必须降低SIL等级。

按照EN ISO 13849-1:2008进行系统设计

为能正确应用EN ISO 13849-1:2008标准，需要全面详细研究其内容。以下为该标准的简要介绍：

该标准规定了有关控制系统中安全性部件的设计与整合的要求，其中也包括有关软件方面的要求。该标准不仅适用于安全性系统，而且还是用于该系统的中组成部件。该标准适应范围广，适用于包括电气、液压、气动、机械等所有的技术领域。虽然ISO 13849-1标准适用于复杂系统，但还是在复杂的嵌入式软件系统方面建议读者参阅IEC 62061与IEC 61508 标准。

采用该标准，可将系统的安全完整性分成5个PL等级(性能等级)。PLa表示完整性级别最低，PLe表示完整性级别最高。评估完整性级别时采用考虑一下因素：

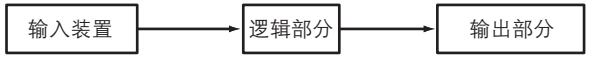
结构(架构) 结构域前文所述类型具有直接的关系。

任务执行时间 – 预计的运行期限
MTTFd – 危险性失效的平均时间
DC – 诊断范围
CCF – 常见原因失效
出现故障时的行为
软件
系统失效
新环境条件

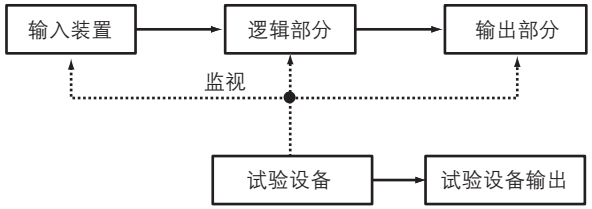
系统架构(结构)

该标准规定了基于简化类型的PL估算步骤。这种方法旨在为了从基于初始分类的标准向基于性能等级的2006版标准过渡时提供一个认可的过渡路径。该标准规定5中指定结构，具体如下。这五种结构分别对应现有的5中类别：B、1、2、3、4类。需要通过该标准的第6条中仔细研究这些图形。该标准第6条解释了相关的要求、差异与假设。B 类与1类，3类与4类可能看起来相同，但该标准在包括诊断范围在内的各项要求方面详细介绍了这些类别之间的差异。

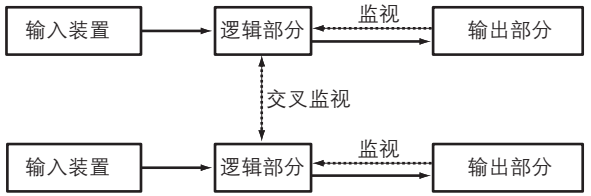
着同样有助于研究本文件对于类别的解释。本文件通过实际应用实例详细讨论了这些类别。以下三幅图说明了5种分类架构的方框图，如ISO/EN13849-1标准所示。



B 类与 1 类架构



2 类架构



3类与4类架构

任务执行时间

任务执行时间表示子系统(或者系统)可使用的最长时间。经过该时间后必须更换子系统或者系统。任务执行时间必须由部件厂家公布。任务执行时间与IEC/EN62061标准中使用的“验证试验时间间隔”相同。那么，安全系统设计人员在确定每个安全功能的任务执行时间时必须考虑各部件的任务执行时间。

危险性失效的平均时间($MTTF_d$)

$MTTF_d$(危险性失效的平均时间)直接在EN ISO 13849-1:2008标准中使用，作为估算PL的一部分。该标准给出了三种确定$MTTF_d$的方法：1)使用厂家提供的数据，2)利用附录C与D，这两个附录中给出了部件的失效率，3)使用默认值10年。如下表所示，选择默认值会限制在中等时间范围内。

每个通道的MTTF名称	每个通道MTTFd的范围
低级	3年<= MTTFd < 10年
中级	10年<= MTTFd < 30年
高级	30年<= MTTFd < 100年

$MTTF_d$等级

当安全系统中含有与IEC62061标准的接口时，$MTTF_d$的值必须转换为PFH_D使用以下关系式可完成转换：

$$PFH_D = 1 / MTTF_d$$

对于电动机械式装置来讲：

$$MTTF_d = B10_d /(0.1 \times 每年的平均操作次数)$$

在有些情况下，要求用该值确定PFH_D。该值由将由厂家提供。The $MTTF_d$与PFH_D可通常由相同的实验或者分析数据推导。对于复杂程度低的电气装置，失效机构通常与操作频率与数量有关，而非只与时间有关。所以对于这些部件来讲，这些数据将从使用期限试验中获得，如B10试验。那么，就需要基于应用情况的信息，如预期每年的数量与操作，以便将$B10_d$或者类似数据转换为$MTTF_d$。

诊断范围(DC)

诊断范围(DC)表示系统或者子系统故障监视的有效性。DC为探测到的危险性失效与总危险性失效两者的失效率之比。EN ISO 13849-1:2008标准语IEC 61508标准中给出了推导DC所需的表格，不过在有些情况下DC可由厂家提供。

常见原因失效(CCF)

当单个原因造成的多个故障导致危险性失效时发生常见原因失效(CCF)。这些不同项目的失效由单一事件造成。每个失效之间不存在因果关系。EN ISO 13849-1:2008标准的附录F中给出了一个简单的确定CCF的量化方法。下表总结了分值确定过程。

编号	避免CCF的措施	分值
1	单独/隔离	15
2	密度	20
3	设计/应用/经验	20
4	评估/分析	5
5	能力/培训	5
6	环境	35

确定常见原因失效的分值

要达到 2、3、4类的要求，所得分值必须至少达到65.

系统失效

各标准对控制与避免系统失效提出了相应要求。可能出现的典型系统失效为软件设计错误、硬件设计错误、技术规范要求错误。

与随机发生的硬件随机失效不同，系统失效一般是由在硬件的某些部分性能降低后造成的。EN ISO 13849-1:2008标准的附录G介绍了控制与避免系统失效的措施。

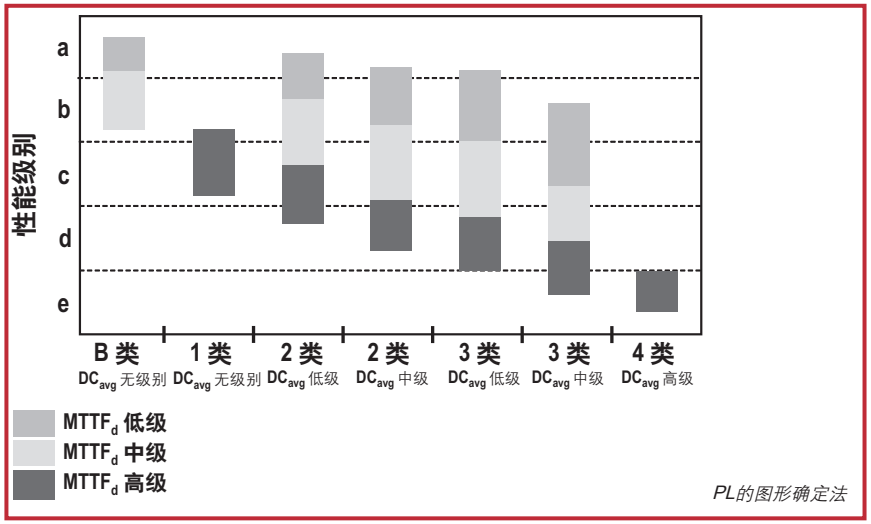
性能级别(PL)

当上一表格中的设计标准说明“TD_d级别”是通过估算所得，则应为SRCS指定一个性能级别。性能级别是一个离散性级别，该级别规定了控制系统中与安全有关的部件执行安全功能的能力。

为了评估执行5类架构中任一架构所能达到的PL，系统或者子系统需要采用以下数据：

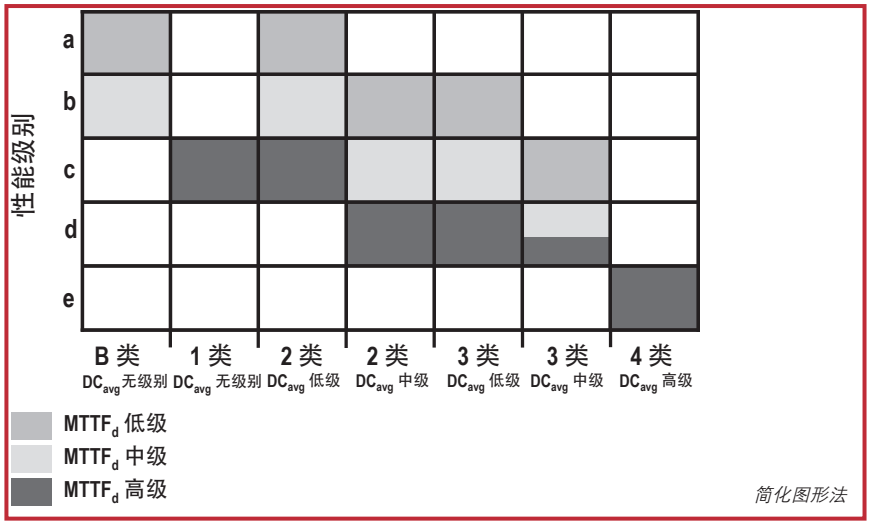
- $MTTF_d$(每个通道危险性失效的平均时间)
- DC(诊断范围)
- 架构(类别)

下图说明了通过组合这些因素确定PL的图形法。本部分最后的表格说明了不同Markov模型的表格化结果。其中Markov模型是该图的基础。需要更精确的判定时，请参阅该表。



PL的图形确定法

读者会看到，在PL区分线上有一些重叠的地方。如果MTTF仅在类别术语中使用最为低级、中级或者高级)，则使用下幅图确定PL。



简化图形法

例如采用第3类指定的架构的应用情况。如果DC在60%与90%之间，并且如果每个通道的$MTTF_d$在10与30年之间，则按照图10.7，可以达到PLd。

为满足所需的PL要求，也必须满足有关其他因素的要求。这些要求包括提供一下各相关：常见原因失效、系统失效、环境条件与任务执行时间。

如果系统或者子系统的PFH_D已知，则可利用表10.4(将该标准的附录 K)推导处PL。

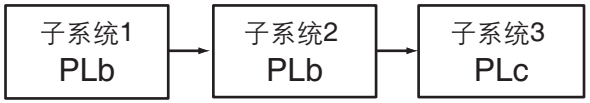
子系统的设计与组合

利用表10.3可将满足PL要求的子系统组合到系统中。该表的合理性显而易见。首先，系统只能达到与其最弱子系统相同的满意度。第二，子系统越多，失效的可能性越大。

$PL_{低级}$	$N_{低级}$	PL
a	>3	不允许
	≤3	a
b	>2	a
	≤2	b
c	>2	b
	≤2	c
d	>3	c
	≤3	d
e	>3	d
	≤3	e

串联组合子系统PL的计算

在下图所示系统中，最低性能级别为子系统1与子系统2。这两个子系统的性能级别均为PLb。所以，我们可以在该表中从 b(在$PL_{低级}$列)开始，穿过2(在$N_{低级}$列)，然后就可发现系统达到的PL为b级(在PL列中)。如果所有三个子系统为PLb级，那么达到的PL等级为PLa级。



将子系统串联组合成PLb系统

验证

在开发安全系统与调试过程中，验证具有至关重要的作用。ISO/EN 13849-2:2003标准就按照原始ISO 13849-1(EN 954-1)标准设计的系统提出了具体的验证要求。可以预计，该标准将会经过修订，使其与按照EN ISO 13849-1:2008标准设计的系统标准EN ISO 13849-1:2008一致。在ISO 13849-2标准中对验证过程做了规定，要求制定验证计划，并通过试验以及故障树分析、故障模型、效果与关键性分析等技术讨论验证过程。以上大多数要求适用于子系统制造商而非子系统用户。

机械调试

在系统或者机械的调试阶段，必须在所有运行模式下验证安全功能，并且还应包括所有的正常情况以及可预见的异常情况。输入组合以及顺序操作也必须给予考虑。这个过程很重要，因为始终需要我们检查系统是否适合实际的运行特性、环境特性。

有些特性可能与设计阶段的预计有所不同。

故障排除

安全系统的主要分析工具之一就是失效分析。设计人员与用户必须明白故障情况下安全系统如何执行其功能。我们可以利用许多技术进行分析。这些技术包括：故障树分析、失效模式、效果与关键性分析、事件树分析、复杂强度检查。

在分析期间，我们可能会发现一些在自动诊断检测过程中由于经济成本问题无法探测到的故障。另外，通过减少设计、制造与试验方法可将故障发生概率可以控制得极其小。在这些条件下，我们可能通过进一步考虑就会排除故障。因为我们不能忽略特定的SRCS失效概率，所以故障排除就是控制故障出现。

EN ISO 13849-1:2008标准允许 故障排除可基于故障出现的技术可能性、通常认可的技术经验以及与应用相关的技术要求。ISO 13849-2:2003标准提供了有关电气、气动、液压与机械系统故障排除的示例与排除理由。必须在技术文件中说明故障排除情况并提供详细理由。

通过故障排除可以达到很高的PL等级。必须在整个任务执行期间采取允许进行故障排除的相应措施。如果不假定可以排除某些故障，就无法进行SRCS估算。有关故障排除的详细内容，请参阅ISO 13849-2。

每个通道的MTTFd用年表示	每小时危险性失效的概率(1/h)以及相应的性能级别(PL)													
	类别B	PL	类别1	PL	类别2	PL	类别2	PL	类别3	PL	类别3	PL	类别4	PL
	$DC_{平均}$ = 无		$DC_{平均}$ = 无		$DC_{平均}$ = 低级		$DC_{平均}$ = 中级		$DC_{平均}$ = 低级		$DC_{平均}$ = 中级		$DC_{平均}$ = 高级	
3	$3,80 \times 10^{-5}$	a			2.58×10^{-5}	a	1.99×10^{-5}	A	1.26×10^{-5}	a	6.09×10^{-6}	b		
3,3	3.46×10^{-5}	a			2.33×10^{-5}	a	1.79×10^{-5}	A	1.13×10^{-5}	a	5.41×10^{-6}	b		
3,6	3.17×10^{-5}	a			2.13×10^{-5}	a	1.62×10^{-5}	a	1.03×10^{-5}	a	4.86×10^{-6}	b		
3,9	2.93×10^{-5}	a			1.95×10^{-5}	a	1.48×10^{-5}	a	9.37×10^{-6}	b	4.40×10^{-6}	b		
4,3	2.65×10^{-5}	a			1.76×10^{-5}	a	1.33×10^{-5}	a	8.39×10^{-6}	b	3.89×10^{-6}	b		
4,7	2.43×10^{-5}	a			1.60×10^{-5}	a	1.20×10^{-5}	a	7.58×10^{-6}	b	3.48×10^{-6}	b		
5,1	2.24×10^{-5}	a			1.47×10^{-5}	a	1.10×10^{-5}	a	6.91×10^{-6}	b	3.15×10^{-6}	b		
5,6	2.04×10^{-5}	a			1.33×10^{-5}	a	9.87×10^{-6}	b	6.21×10^{-6}	b	2.80×10^{-6}	c		
6,2	1.84×10^{-5}	a			1.19×10^{-5}	a	8.80×10^{-6}	b	5.53×10^{-6}	b	2.47×10^{-6}	c		
6,8	1.68×10^{-5}	a			1.08×10^{-5}	a	7.93×10^{-6}	b	4.98×10^{-6}	b	2.20×10^{-6}	c		
7,5	1.52×10^{-5}	a			9.75×10^{-6}	b	7.10×10^{-6}	b	4.45×10^{-6}	b	1.95×10^{-6}	c		
8,2	1.39×10^{-5}	a			8.87×10^{-6}	b	6.43×10^{-6}	b	4.02×10^{-6}	b	1.74×10^{-6}	c		
9,1	1.25×10^{-5}	a			7.94×10^{-6}	b	5.71×10^{-6}	b	3.57×10^{-6}	b	1.53×10^{-6}	c		
10	1.14×10^{-5}	a			7.18×10^{-6}	b	5.14×10^{-6}	b	3.21×10^{-6}	b	1.36×10^{-6}	c		
11	1.04×10^{-5}	a			6.44×10^{-6}	b	4.53×10^{-6}	b	2.81×10^{-6}	c	1.18×10^{-6}	c		
12	9.51×10^{-5}	b			5.84×10^{-6}	b	4.04×10^{-6}	b	2.49×10^{-6}	c	1.04×10^{-6}	c		
13	8.78×10^{-5}	b			5.33×10^{-6}	b	3.64×10^{-6}	b	2.23×10^{-6}	c	9.21×10^{-7}	d		
15	7.61×10^{-6}	b			4.53×10^{-6}	b	3.01×10^{-6}	b	1.82×10^{-6}	c	7.44×10^{-7}	d		
16	7.31×10^{-6}	b			4.21×10^{-6}	b	2.77×10^{-6}	c	1.67×10^{-6}	c	6.76×10^{-7}	d		

每个通道的MTTFd用年表示	每小时危险性失效的概率(1/h)以及相应的性能级别(PL)													
	类别B	PL	类别1	PL	类别2	PL	类别2	PL	类别3	PL	类别3	PL	类别4	PL
	$DC_{平均}$ = 无		$DC_{平均}$ = 无		$DC_{平均}$ = 低级		$DC_{平均}$ = 中级		$DC_{平均}$ = 低级		$DC_{平均}$ = 中级		$DC_{平均}$ = 高级	
18	6.34×10^{-6}	b			3.68×10^{-6}	b	2.37×10^{-6}	c	1.41×10^{-6}	c	5.67×10^{-7}	d		
20	5.71×10^{-6}	b			3.26×10^{-6}	b	2.06×10^{-6}	c	1.22×10^{-6}	c	4.85×10^{-7}	d		
22	5.19×10^{-6}	b			2.93×10^{-6}	c	1.82×10^{-6}	c	1.07×10^{-6}	c	4.21×10^{-7}	d		
24	4.76×10^{-6}	b			2.65×10^{-6}	c	1.62×10^{-6}	c	9.47×10^{-7}	d	3.70×10^{-7}	d		
27	4.23×10^{-6}	b			2.32×10^{-6}	c	1.39×10^{-6}	c	8.04×10^{-7}	d	3.10×10^{-7}	d		
30			$3,80 \times 10^{-6}$	b	2.06×10^{-6}	c	1.21×10^{-6}	c	6.94×10^{-7}	d	2.65×10^{-7}	d	9.54×10^{-8}	e
33			3.46×10^{-6}	b	1.85×10^{-6}	c	1.06×10^{-6}	c	5.94×10^{-7}	d	2.30×10^{-7}	d	8.57×10^{-8}	e
36			3.17×10^{-6}	b	1.67×10^{-6}	c	9.39×10^{-7}	d	5.16×10^{-7}	d	2.01×10^{-7}	d	7.77×10^{-8}	e
39			2.93×10^{-6}	c	1.53×10^{-6}	c	8.40×10^{-7}	d	4.53×10^{-7}	d	1.78×10^{-7}	d	7.11×10^{-8}	e
43			2.65×10^{-6}	c	1.37×10^{-6}	c	7.34×10^{-7}	d	3.87×10^{-7}	d	1.54×10^{-7}	d	6.37×10^{-8}	e
47			2.43×10^{-6}	c	1.24×10^{-6}	c	6.49×10^{-7}	d	3.35×10^{-7}	d	1.34×10^{-7}	d	5.76×10^{-8}	e
51			2.24×10^{-6}	c	1.13×10^{-6}	c	5.80×10^{-7}	d	2.93×10^{-7}	d	1.19×10^{-7}	d	5.26×10^{-8}	e
56			2.04×10^{-6}	c	1.02×10^{-6}	c	5.10×10^{-7}	d	2.52×10^{-7}	d	1.03×10^{-7}	d	4.73×10^{-8}	e
62			1.84×10^{-6}	c	9.06×10^{-7}	d	4.43×10^{-7}	d	2.13×10^{-7}	d	8.84×10^{-8}	e	4.22×10^{-8}	e
68			1.68×10^{-6}	c	8.17×10^{-7}	d	3.90×10^{-7}	d	1.84×10^{-7}	d	7.68×10^{-8}	e	$3,80 \times 10^{-8}$	e
75			1.52×10^{-6}	c	7.31×10^{-7}	d	3.40×10^{-7}	d	1.57×10^{-7}	d	6.62×10^{-8}	e	3.41×10^{-8}	e
82			1.39×10^{-6}	c	6.61×10^{-7}	d	3.01×10^{-7}	d	1.35×10^{-7}	d	5.79×10^{-8}	e	3.08×10^{-8}	e
91			1.25×10^{-6}	c	5.88×10^{-7}	d	2.61×10^{-7}	d	1.14×10^{-7}	d	4.94×10^{-8}	e	2.74×10^{-8}	e
100			1.14×10^{-6}	c	5.28×10^{-7}	d	2.29×10^{-7}	d	1.01×10^{-7}	d	4.29×10^{-8}	e	2.47×10^{-8}	e