ABB 传动
安全功能

技术指导10

ABB

ABB 传动
安全功能

技术指导10

3ABD0000048753 REV A 中文
基于 : 3AUA0000048753 REV A 英文
生效日期: 2010-07-01

目录

关于该文档 7

第一章 – 理论和背景知识 8

安全和安全功能 8
机器安全指导 9
新机器安全指导当中的变化 10
欧洲安全标准系统的结构图 12

第二章 – 新进展 14

两个标准化组织 – IEC 和 ISO 15
适用于风险最小化的标准 16
适用于电气安全系统的标准 16
产品–特殊安全标准（C类标准） 18
适用于传动系统当中安全相关的特殊标准 18
标准化的安全功能 19

第三章 – 满足机器安全指导要求的步骤 22

第一步：安全功能规划 23
第二步：风险评估 24
第三步：降低风险 26
第四步：安全需求的建立 28
第五步：应用安全功能系统 32
第六步：检验安全功能系统 33
第七步：确认安全功能系统 37
第八步：编制安全功能系统文档 37
第九步：符合性验证 38

术语 40

索引 42

免责声明

该文档是为了帮助机器的最终用户，专门人员（安装和操作人员等）和制造商以及其他相关人员获得关于欧盟机器安全指导要求的更好理解而编写的。另外，还包括为了满足该指导和安全标准应采取的措施。

文档提供信息帮助，而不是应用指导。

文档当中提供的信息和例子仅仅适用于一般用途，并未提供必要细节应用于一个安全系统。

ABB传动公司对应用本文档信息造成的直接和间接伤害或损坏不承担任何责任。机器制造商承担按照使用规程操作的安全责任。因此，ABB声明免除可能由此文档带来的所有责任。

关于文档

文档介绍了机器安全指导以及为了保证操作安全，当设计一台机器的时候应该遵循的安全标准。

文档的目的是为了解释在一般意义上如何满足机器安全指导提出的要求以及CE标志的获得。CE标志意味着产品满足机器安全指导要求。

注意：

此文档仅提供满足机器安全指导深度要求的一般过程。制造商提供产品符合的安全标准以及安全保证。

文档分成三部分：

- 第1章–理论和背景知识–介绍应用背后的想法。安全功能以及如何满足机器安全指导。还包括新机器安全指导的变化。解释了欧盟安全标准系统的结构。
- 第2章–新进展–展示了替换旧标准的新机器安全指导的相关标准。介绍了两个标准系统。罗列了一系列安全相关的标准和安全功能。
- 第3章–满足机器安全指导要求的步骤–介绍了满足机器安全指导深度要求的9个步骤。

第一章-理论和背景知识

欧盟法律规定机器设备必须符合机器安全指导要求的深层次的健康和安全规则，以及该指导包含的安全标准。这就意味着新的机器必须满足同一法律要求才能够在欧盟销售。同一标准也适用于进行机器设备贸易和运输的非欧盟区域的国家。

为什么机器要满足这些要求？因为这些要求可以防止事故和随之带来的人身伤害。而且，满足机器安全指导和相关安全标准要求的机器设备，制造商可以保证他们设计和生产的机器的安全性能满足国家法律的强制要求。

对制造商而言，新改进的安全策略正越来越成为提高生产率和增强市场竞争的手段。传统安全系统的目的是为了获得操作安全和满足法律强制要求，一般通过增加电气和机械部件完成，虽然这会以牺牲生产效率为代价。在特定环境下，用户为了提高生产效率屏蔽这些系统功能，这会导致意外事故。

在现代安全系统中，在保持生产效率的同时，操作过程安全和操作人员的安全得到全面考虑。一个例子是：进行安全维护的时候机器运行在一个较低的转速。安全被集成到机器性能当中，而不是事后再考虑安全措施。这是现代安全系统的一条规则。

安全系统被有效应用在特定过程当中，以获得特别的安全性能以及使用符合规定的安全系统保护的子系统。符合安全标准在工业领域被寄予厚望。在市场领域，符合规定的子系统，诸如传动部件是必须的（符合安全标准）。机器安全是工业自动化市场成长最快的重要领域之一。

安全和安全功能

安全意味着保护操作人员和环境在意外事故当中不会受到伤害。在这里，主要指机器伤害。安全功能系统降低了意外事故发生的可能，因此，操作机器时意外伤害的发生降至很低的程度。安全标准定义了在无法预料的风险下的社会大众可接受的安全性能。机器制造商必须在所有市场领域遵守该标准，不能存在地区差别。

消除风险最有效的办法是通过产品设计避免。如果不能通过设计降低风险，设置静态安全保护或安全功能是一个不错的选择。当机器快速安全停止或者在一个相对低速运行的时侯，可以获得更多的正常运行时间，减少故障停机时间，从而降低风险，提高机器生产效率。另外，同时也满足法律的强制要求，操作人员和工作环境的安全保障得到保证。

机器领域的安全功能通常意味着安全监视的系统以及操作安全得到保证的机器控制。安全相关的系统具备必须的安全功能。安全功能系统设计用来监测恶劣环境下的安全操作状态，或者保证意外发生时一些必要措施的执行，比如安全停车。

监测的内容包括速度、停车过程、旋转方向和停止状态。当安全系统执行一个主动的安全功能，例如监视运行速度，系统状态偏离预定值时（比如系统运行太快），安全系统检测到这个偏差值，主动调整机器到一个安全状态。比如，通过降低电机转子端的负载转矩让机器安全地停下来。这通常是很容易做到的。

安全系统并不是机器操作的标准功能。但是，任何安全系统的失效都将导致机器操作的安全风险。

机器安全指导

机器安全指导，包括安全标准，在欧盟的机器重要健康和安全要求（EHSR）当中给出了定义。重要健康和安全要求（EHSR）列在了机器安全指导附录的第一部分。

机器安全指导背后的思想是保证机器设计、制造、使用和安装维护安全。在机器的整个生命周期中，带给人和环境的伤害风险降至最低。

重要健康和安全要求（EHSR）规定，当设计和制造安全机器的时候，制造商需按照以下步骤进行：

- 在机器的设计和制造阶段，充分考虑安全因素，尽可能消除或最小化安全风险。
- 应用必要的安全保护措施防止不能消除的危险发生。
- 提醒用户即使采用了切实可行的保护措施后，仍旧存在可能发生的危险，需要提供切实有效的用户培训和劳动保护用具。

符合安全指导当中EHSR要求的机器制造商被允许在他们制造的机器上使用CE标志。带有CE标志意味着制造商承诺他们产品的可自由运动部件满足欧洲安全指导，在这里是机器安全指导的相关安全规定。

注意

满足机器安全指导要求的CE标志只表明整个机器满足安全标准，并不意味着组成机器的零部件也满足该要求。因此，机器制造商或者销售代表，而不是组成机器的零部件制造商对CE标志的使用负责。

机器制造商对机器进行的相关风险分析负责，保证满足要求，相关步骤在第三部分表述。零部件制造商对销售出去的部件的安全性能的表现负责（SIL/PL 要求），前提是该零部件是正常使用的。在本文当中，零部件可能是一个安全继电器，或者集成了安全功能的变频器。

新机器安全指导当中的变化

新的机器安全指导2006/42/EC将会从2009年12月19日起替代老的98/37/EC机器安全指导。在此日期之后生产的机器适用新的机器安全指导。

新旧安全指导文件并没有本质的差别。新版本文件的目的一是加强旧文件对机器安全的要求，再有就是增加可操作性。

在新版本机器安全指导当中增加的要点如下：

- 机器安全指导附录IV列出的对如何确认危险机器的方法做了改进。
  按照新指导规定，制造商可以进行自我认定，而无需测试中心帮助。前提是，制造商必须确保产品质量检测流程符合机器安全指导附件X罗列的相关要求。

- 机器安全指导 I 列出的重要健康和安全要求。
  机器制造商必须执行EHSR规定的相关风险评估。

- 组成机器各产品部件的安全保证。
  对产品的规定同样适用于机器、可互换件和安全部件等等。产品必须包括CE认证、符合性声明和必要的操作人员的安全信息提示。

- 零部件或半成品机器的安全要求。
  部件或半成品机器只是机器成品的一个或若干组成部分，它们不能自行完成特定功能。各个部件或半成品组合起来才组成一个完整、符合机器安全指导定义、完成特定功能的机器。

  在制造商声明当中必须包括对组成机器的零部件和半成品作出符合安全指导要求的兼容性声明。
  产品文档必须还包括对组成机器的零部件和半成品的安装指导。

- 低压指导的更新部分
  低压指导部分现在是指对产品的要求，而不是过去那种风险评估。机器安全指导和低压指导两者之间区别明显。

- 危险分析的变化
  危险分析被定义成风险评价和风险预估两部分。

- 生产控制部分的变化。
  机器生产序列目前有了内部生产控制流程，在机器安全指导附件VIII部分有特别规定。

- EC规定的检测认证的有效性。
  具有资质的测试中心每5年检查该认证资格一次。制造商和测试中心需保留相关技术文档15年。

欧盟危险等级系统的金字塔结构图

欧盟负责标准化的委员会（CEN）和负责电气标准化的委员会（CENELEC）共同制定了危险等级标准。所有的危险等级标准都以“EN”打头。

危险等级列表可以在欧盟下属的互联网找到：
http://ec.europa.eu

危险等级标准的大部分可以在各个指导文件当中找到。为了保证满足机器安全指导的相关要求，建议使用对应的欧盟危险等级标准。为了设计满足这些标准的机器，制造商需要证明他们的产品符合机器安全指导的要求。一般来说，不需要第三方的认证。

注意：机器安全指导附件IV部分关于机器的要求一定要引起足够的关注。

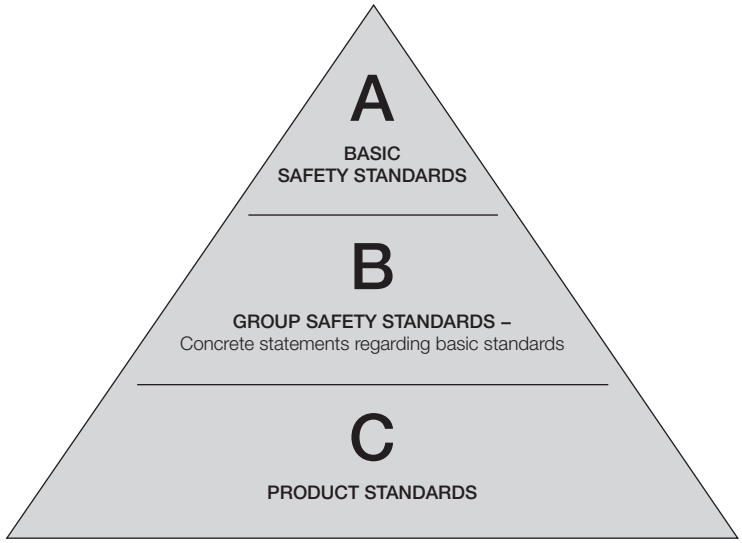


图 1-1 欧盟危险等级的金字塔结构图

- C类标准适用于一台机器或一类的机器。如果一台机器满足C类标准，相关的B类或A类标准就退居次席。当设计安全功能的时候，C类标准定义了机器必要的强制安全要求。但是，如果没有C类标准可供使用，B类或A类标准可以在设计和制造机器的过程中提供满足机器安全指导的帮助。
- B类标准适用于大多数机器的设计安全要求。这些标准给出可能的风险信息以及如何应对来降低风险，同时还提供降低风险的流程安排的相应帮助。B类标准可分成B1和B2。B1标准适用于特定安全方面，而B2适用于一般安全相关设备。例如，属于B1类的标准包括EN 62061:2005和EN ISO13849-1:2008。B2类标准包括定义紧急停止，如EN ISO 13850:2008。
- A类标准包括一般设计原理和基本机器定义说明。EN ISO 12100-1就属于A类标准。

注意：
并不强制使用这些标准。但是这些标准提供了满足机器安全指导要求的方法，而安全指导是必须遵守的。

注意：
旧的标准EN 954-1将会在2009年11月30日过期，新标准EN ISO 13849-1和EN 62061将如期启用。从2006年11月开始的为期三年的过渡期即将结束。在这个过渡期内，EN 954-1和EN ISO 13849-1、EN 62061一起并行生效。

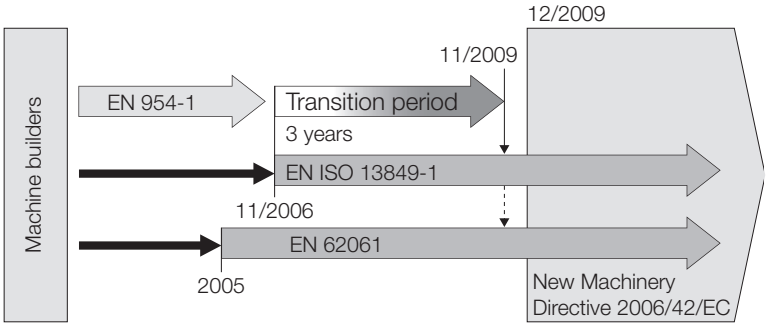


图 2-1 从旧标准到新标准的过渡期

用EN ISO 13849-1和EN 62061（用于电气控制系统）替换EN 954-1在安全相关的系统当中是一个确定无疑的进步，尤其对于可能或确切的原因–影响关系分析。新标准考虑整个安全功能的失效可能性，而不仅仅是组成系统的各个部分。不像旧标准EN 954-1，这些新标准允许使用可编程的安全系统。

新标准使用和EN 954-1一样的结构（分类）。增加了一些新的概念，比如生命周期思想，组件可靠性和质量测试的量化，一般失效原因分析等。

注意：

标准EN ISO 13849-1保留了EN 954-1当中的分类方法。该标准还提供了基于上述分类的设计和验证方法。标准EN 62061包含相似的结构和方法。

EN 954-1 是一个提供直接和便捷过程相对简单的安全标准。
EN ISO 13849-1的过程相对复杂。为了定义系统的分类或结构，机器制造商必须通过评估和计算来保证机器的安全。使用经认证的子系统是一种推荐的做法，因为这可以加快这个过程，并简化计算。

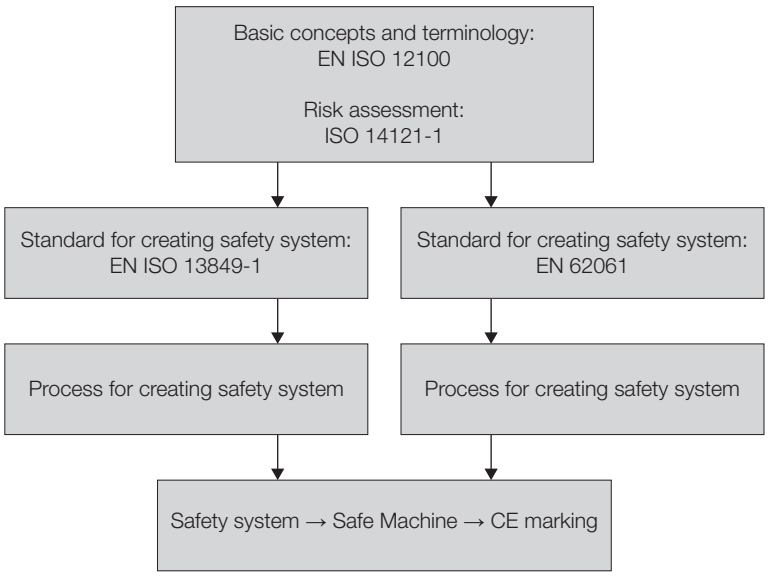


图 2-2 标准介绍

两个标准化组织——IEC和ISO

建立符合机器安全指导的功能安全系统的标准有两个可供参考：国际电工协会（IEC）标准和国际标准化组织（ISO）标准。

参照任何一个标准都将获得相似的结果，它们的安全完整性等级（SIL）和安全性能（PL）基本相当。更多信息，参见第三章步骤6部分的表格。

在设计系统过程中，解释两个标准的匹配性的图表，可以在EN ISO 13849-1 和 EN 62061当中找到。

注意：
机器制造商可以选定在建立安全系统时采用哪一个标准（EN ISO 13849-1或EN 62061）。一旦选定，则从头到尾采用同一标准，以保证标准的一致性。

CEN标准基于ISO标准，并且主要用于机械部件。新标准在10000系列当中包括很多成员。CENELEC基于IEC标准，新标准在60000系列当中包括很多成员。

注意：

EN ISO标准在本文档中以“ISO”形式出现。然而，EN IEC标准并不以“IEC”形式出现，主要是为了和标准列表当中的一致。

风险最小化标准

风险最小化基本安全标准包括：

- EN ISO 12100-1:2003（机器安全——基本概念，设计原理）
- EN ISO 14121-1:2007 （机器安全——风险评估）

为了降低风险，EN ISO 12100提供给设计人员通用设计架构和提示（三步法）。EN ISO 12100-1定义了获得机器安全的基本术语和方法。

EN ISO 14121-1是一个在降低风险的过程中做风险评估的新标准，在EN ISO 12100标准当中有说明。EN ISO 14121-1替代已于2008年6月24日过期的EN 1050:1996。

注意：
所有在本文出现的其他对这些标准的参考内容适用于上述版本的标准。

适用于电气安全系统的标准

适用于电气安全系统的标准有：

- EN ISO 13849-1:2008 （机器安全——控制系统的安全相关部分——一般设计原理）
- EN 62061:2005（机器安全——安全相关的电子器件、电气和可编程电气控制系统的安全功能）
- IEC 61508:1998-2000 （电子器件、电气和可编程电气安全相关系统的安全功能），以及
- EN 60204-1:2006 （机器安全——机器的电器零部件的一般要求）

注意：
所有在本文出现的其他对这些标准的参考内容适用于上述版本的标准。

EN ISO 13849-1是一个为机器安全向设计人员提供指导的标准。这些指导包括在设计、系统集成和验证过程中提供推荐方法，用于各种不同机器的控制系统安全相关部分，无论这些机器采用什么样的技术和使用什么样的动力方式。
该标准还包括对可编程控制系统的安全相关部分的特殊要求。这个标准覆盖设备的所有安全功能（完整安全链，例如，传感器–逻辑处理–执行器）。

该标准还定义了如何确定需要的安全性能（PL）以及在一个系统当中怎样确定获得的性能标准。性能标准表明了一个安全系统在可预见的状况下能够实现的安全功能。性能标准分成五类：a，b，c，d和e。e具有最高安全可靠性，a的安全可靠性最低。

EN 62061标准用于设计电气安全系统。它是IEC61508架构内的机器部分特定标准。EN62061包括对机器安全相关部分的电气、电子和可编程电气控制系统的设计、系统集成和验证过程进行安全指导。整个安全链——例如，传感器——逻辑处理——执行器——都包括在这个标准当中。单独的子系统不需要验证。但是，使用经验证的子系统建立各个组成功能块在该标准中是极力推荐的，因为这将大大节省设计过程中的工作量。

注意：
和EN ISO 13849-1不同，EN 62061不包括对机器非电气安全相关控制部分的要求。

这个标准定义了安全集成水平（SIL）。安全集成水平表示一个系统的安全功能可靠性。共有4个等级：1、2、3和4。SIL 4最高，SIL 1最低。在机器当中只用到了1—3。

IEC 61508 是一个基本的功能安全标准，它涵盖了包括电气、电子和可编程控制部件等系统的整个生命周期。这个系统的作用主要是实现安全功能。IEC 61508并不是一个完善的标准，但它却是在设计包括复杂硬件和软件的安全相关控制系统必须遵循的主要标准。IEC 61508一般用于设计可验证的安全子系统。标准 EN ISO 13849-1 和 EN 62061基于IEC 61508标准。EN 60204-1对机器的电气部分提供推荐值和要求，加强机器的安全性和可用性。

特别产品安全标准（C类标准）

特别产品安全标准，被称作C类标准，用于符合标准涵盖的EHSR要求的特殊机器或者某一类机器。

应当注意的是：

- C类标准的要求远高于一般安全标准（EN 62061，EN ISO 13849-1等）。
- C类标准对一些安全功能设定有SIL/PL要求。这些要求必须满足，无论风险分析的结果如何。

注意：
即使风险评估的过程中各种已知的危险有可能影响机器构成，而且C类标准是独特的，该标准仍未包括EHSR相关的方方面面。该标准仍然需要不断彻底检查，以确保危险从已知列表中排除出去。

安全相关驱动系统的特定标准

适用于安全相关驱动系统的特定标准是：

- EN 61800-5-2:2007（可调速电气驱动系统——功能安全要求）

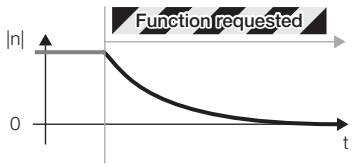
注意：
本文提到的标准其他参照部分仅适用于上述版本的标准。

EN 61800-5-2给出了安全相关应用的电气驱动系统的特别要求和推荐内容。这是一个涵盖在IEC 61508内的与安全相关部分的产品标准，提供了电气驱动系统用于安全系统子系统的一般要求。

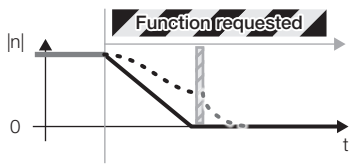
安全功能的标准化

EN 61800-5-2标准包括对众多安全功能的定义。传动可以提供一个或多个安全功能。下面是一些例子：
安全力矩脱扣 （STO）

该功能让机器处于无转矩状态，从而避免意外启动。



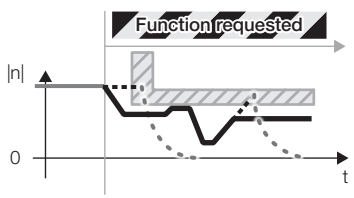
安全停止 1（SS1）
该功能让电机安全停车，在一个特定速度下或者一段预定义的时间后开始执行STO功能。



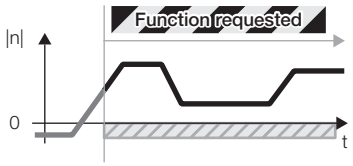
安全停止 2（SS2）
该功能实现安全停车，在一个特定速度下或者一段预定义的时间后开始执行SOS功能。

安全操作停车（SOS）
该功能实现电机保持转矩输出的静态停车。

安全限制速度（SLS）
该功能防止电机运转超过预定的限制速度。

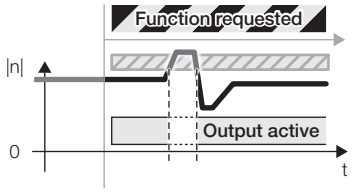


安全方向(SDD)
该功能防止电机反向运转。



安全抱闸控制(SBC)
该功能提供安全输出节点控制外部（机械）抱闸功能。

安全速度监测(SSM)
该功能提供安全输出节点指示电机运行在安全速度。



更多安全功能例子可参见EN 61800-5-2标准。

紧急操作

EN 60204-1标准介绍了两种紧急操作：紧急断电和紧急停止。

紧急断电
当发生触电危险时，紧急断电功能将切断系统或部分电源供应。

该功能需要一个外部电源开关。带有安全转矩脱扣功能（STO）的驱动系统不能完成该功能。

紧急停止
紧急停止功能必须按照如下描述进行：当它有效时，机器的危险移动部件必须停止，并且在任何情况下不能启动。即使紧急停止开关放开，也只是允许机器重新启动（并不启动机器）。

紧急停止可以通过如下方式停止危险运动部件：
- 优化的停车时间，直至机器停止运转。
- 使用0或1类紧急停止，或者
- 使用预定顺序停车

0类紧急停车指的是立即切断电机电源。根据在EN 61800-5-2标准当中的定义，0类停车和安全力矩脱扣（STO）功能等同。

1类紧急停车指的是机器速度按照减速时间控制减速到零，然后切断电机电源。根据在EN 61800-5-2标准当中的定义，1类停车和安全停车1（SS1）功能等同。

在实际操作过程中，紧急停止功能一定不能对机器操作人员造成伤害。

注意：
紧急功能的设计原理在标准EN ISO 13850:2008当中做了介绍。

意外启动的防止
当人员处在危险区域时，确保机器停止在机器安全当中是非常重要的一个方面。

力矩安全脱扣功能可以防止机器意外启动。虽然电机驱动器控制回路的电源仍然有电，却可以阻止电机通电，从而防止电机的意外启动。

防止意外启动的原理和要求在标准EN 1037:1995+A1当中有描述。

第三章-满足机器安全指导要求的步骤

机器安全指导要求机器必须安全。然而，没有零风险的产品，所以，机器安全指导的目的是将风险最小化。

通过以下步骤可满足机器安全指导：

- 满足综合标准的设定要求，或者
- 满足具有相关资质第三方的认证要求

满足使用综合标准的机器指导规定的EHSR要求的过程可分成9个步骤：

- 步骤 1：功能安全管理——在整个机器的生命周期当中管理安全功能
- 步骤 2：风险评估——分析和估计风险
- 步骤 3：降低风险——在设计和使用手册当中消除或最小化风险
- 步骤 4：提出安全要求——消除或降低风险至可接受的水平需要什么（功能，安全性能）
- 步骤 5：使用功能安全系统——设计和制造安全功能
- 步骤 6：验证功能安全系统——确认安全系统满足设计要求
- 步骤 7：确认功能安全系统——回到风险评估流程，确认安全系统在降低特定风险方面有效
- 步骤 8：归档——制作设计文档，生成用户文档
- 步骤 9：符合性验证——通过合规评估和技术文件证明机器符合机器安全指导当中EHSR的要求

在接下来的章节当中会对上述步骤做详细说明。

升级现有机器

当升级现有机器的安全要求时，下面这些方面必须考虑：

- 已经带有CE标志的机器——增加的部件必须也要带CE标志。新部件如何使用在旧系统当中，必须遵照机器安全指导当中的特别规定。
- 不带CE标志的机器——机器的安全水平必须在使用带CE标志的新部件后得到保持，新部件使用声明并不在机器中体现。指导文件89/655/EEC和修正文件95/63/EC必须遵照执行。

最终，由相关权威部门认证该产品升级是否达到更高安全等级。

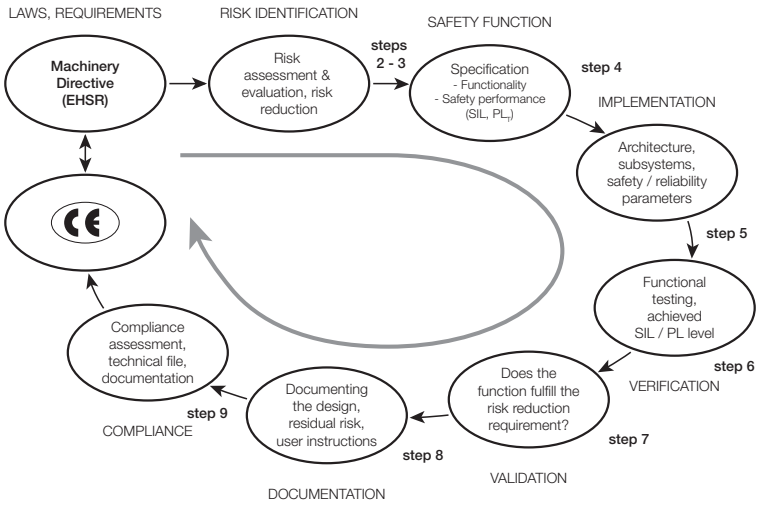


图 3-1 满足机器安全指导的工作流程

步骤1：功能安全管理

为了满足功能安全的要求，必须使用符合标准IEC 61508 或ISO 9001的项目管理和质量管理。管理系统可以使用安全规划的特定形式。

安全规划

标准EN 62061为满足机器安全指导要求特别规定了安全规划。每个安全系统都要设计和记录这种规划，必要的时候还要修改，以满足新的要求。

安全规划：

- 识别所有相关活动
- 满足功能安全要求制定政策和策略
- 明确责任
- 识别和建立文档记录过程及资源
- 描述管理配置的策略
- 验证和确认计划

注意：

虽然上述内容并没有在EN ISO 13849-1:2008标准当中特别规定，相似的举措必须完全符合机器安全指导的要求。
一旦安全计划（参照EN 62061）确立，风险评估就开始了。

步骤2：风险评估

风险评估是风险分析和评价的过程。风险是发生一系列伤害和暴露在危险环境下可能发生伤害的总和。

注意：
按照新的机器安全指导2006/42/EC的要求，必须对机器进行风险评估。

机器安全指导2006/42/EC要求机器制造商进行风险评估并且在设计机器时考虑风险评估的结果。任何高风险必须通过改变设计或使用恰当的安全防护技术降至可接受的水平。

风险评估的过程为机器设计人员如何设计具备安全性能的机器提出要求。在机器设计阶段进行风险评估是非常重要的，因为这比事后对如何安全操作机器设备进行指导有效得多。

符合EN ISO 12100-1标准要求的风险评估过程包括两部分：风险分析和风险评估。风险分析指的是风险识别和风险估计。风险评估则是分析风险是否在可接受的水平，否则必须降低风险。

风险估计是在风险分析后进行的。降低风险的必要措施在风险估计后实施。

注意：
必须对每一个危险独立进行风险评估。

风险分析步骤：

1. 界定机器的应用范围和使用寿命限制。
   这些限制包括：
   - 用途
   - 空间
   - 环境
   - 使用寿命

2. 判断机器可能造成的危险

3. 逐一评价已确定的风险
   - 危险的严重程度（潜在结果）
   - 危险的可能性（发生频次、发生的可能性以及是否可以避免）

- 评估风险：必须降低风险吗？
  - 是：采取降低风险的措施，返回风险分析步骤2

    在下一节当中会介绍EN ISO 12100-1标准当中提供的降低风险三步法。

  - 否：符合降低风险的目标要求，风险评估结束。

记录每个危险因素的风险评估过程和结果。

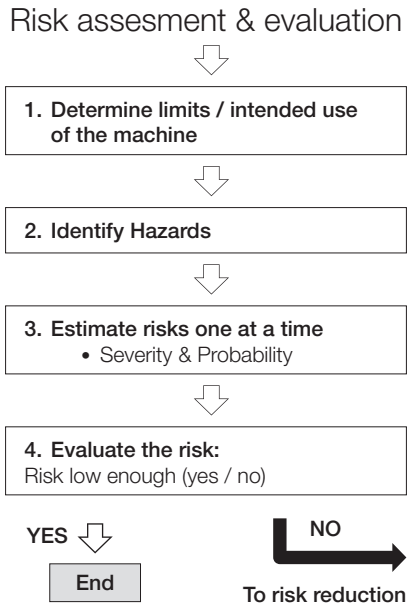


图 3-2 EN ISO 14121-1当中描述的风险评估流程

根据评估结果的不同，风险评估结束后有两个选择：

- 如果评估的结果是不需要采取降低风险的措施，则表明机器符合机器安全指导的对应安全要求。

注意：
为了认证和CE标志的要求，因为总存在残留风险，残留风险必须在操作和维护手册当中标出。

- 如果评估的结果表明风险仍然是不能接受的，降低风险的流程开始启动。

步骤3：降低风险

降低风险最有效的手段是在机器的设计阶段消除风险，例如，更改设计或者改变机器工作流程。如果在设计阶段消除风险已不可能，在降低风险的过程中采取符合机器安全指导当中适当的综合标准的要求也是有效的。

如果风险评估过程指出必须降低风险，需要制定风险最小化策略。按照EN ISO 12100-1标准的要求，降低风险可以分成三个步骤（三步法）：

1. 已有的安全设计方法——更安全的设计，更改设计流程
2. 安全装置和充分的安全保护措施——安全功能，保护措施
3. 信息的使用（残留风险管理）
   - 机器本体——报警指示，型号和报警设施，以及
   - 操作指导文件

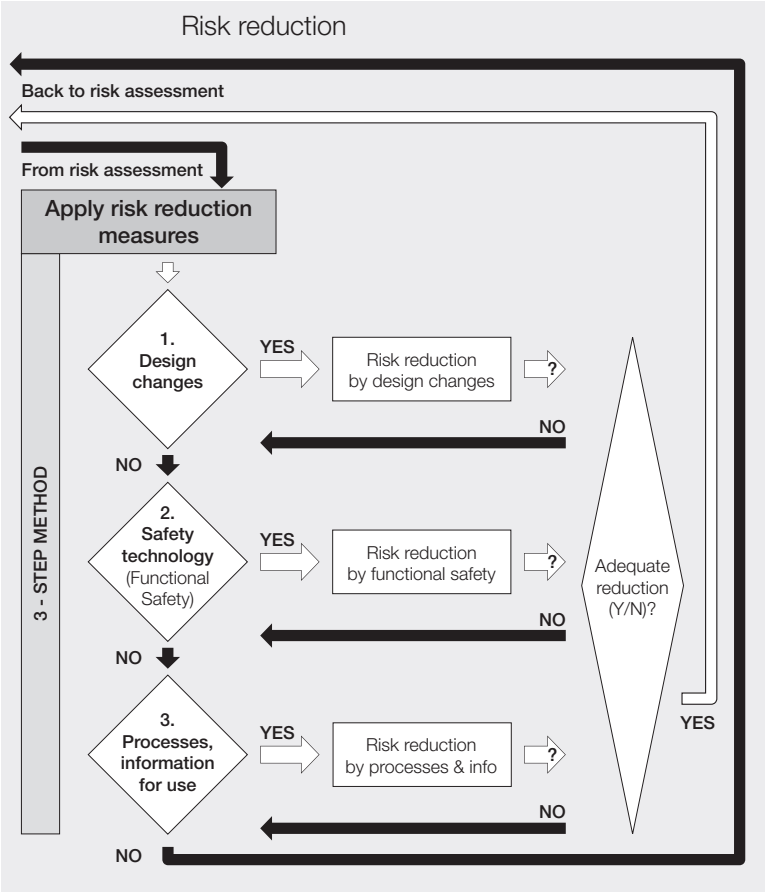


图 3-3 EN ISO 12100-1三步法降低风险

残留风险指的是采取所有保护措施之后仍旧存在的风险。纯技术而言，不可能达到零风险状态，因此，总是存在残留风险。

所有残留风险必须在操作指南当中注明。

用户降低风险部分包括设计（制造）信息。对机器用户降低风险的措施有：

- 用户方采用的降低风险措施包括：
    - 使用安全操作流程，
    - 工作监控，以及
    - 使用工作许可系统。
- 使用附加安全防护。
- 使用个人安全保护用具。
- 客户安全培训。
- 详细阅读操作及安全提示信息，并遵照执行。

设计人员在设定防护措施时必须考虑使用者意见反馈。
当采取降低风险的措施的时候，必须保证这些措施能够将风险降低至可以接受的水平。风险是否降至需要的水平可以通过反复进行风险评估完成。

在接下来的章节当中列出的是三步法的第二部分：使用功能安全方式进行安全防护。

步骤4：提出安全要求

所有可以通过更改设计降低风险的措施实施以后，需要采用其他的安全防护手段来降低风险。功能安全作为附加降低风险的措施可以用于对付剩余的风险。

安全功能

安全功能是一项一旦失效造成风险立即增加的机器功能。它包括必须采取的举措，避免在意外事件发生时暴露在危险当中。安全功能不是影响机器运行的功能，只是该功能失效会增加机器操作造成的意外伤害。

定义一种安全功能一般包括两部分：

- 措施 （为降低风险应该做什么）
- 安全作用 （安全完整性等级 – SIL 或者安全性能 – PL）

注意：
安全功能必须特别定义、验证（功能和安全作用）以及确认对每个已知的危险的有效性。

安全功能举例：
要求：一根裸露的电机旋转轴可能在太接近它时带来人身伤害。

措施： 为了避免人身伤害，当防护门打开的时候，电机轴必须在一秒钟之内停下来。

当采取措施的安全功能定义之后，必需的安全等级就确认下来了。

安全作用/完整性
安全完整性用来衡量安全功能的作用。安全完整性表示基于需求获得的安全功能的性能的可能性。功能的安全完整性取决于风险评估和已获得的安全完整性等级（SIL）或安全性能（PL）所使用的标准。

两个标准对安全功能采用不同的评估技术，但基本是一致的。评价的项目和定义在两个标准中是相似的。

定义要求的SIL（EN 62061）
定义要求的安全完整性等级（SIL）的过程如下：

1. 确定一个危险事件的各个顺序的严重性。
2. 确定人员暴露在危险当中的频次和时长。
3. 当发生人员暴露在危险环境当中时，确定危险事件发生的可能性。
4. 确定阻止危险发生和限定危险发生范围的可行性。

例如：
用于决定安全完整性的参数，呈现在下列的SIL指定列表中。

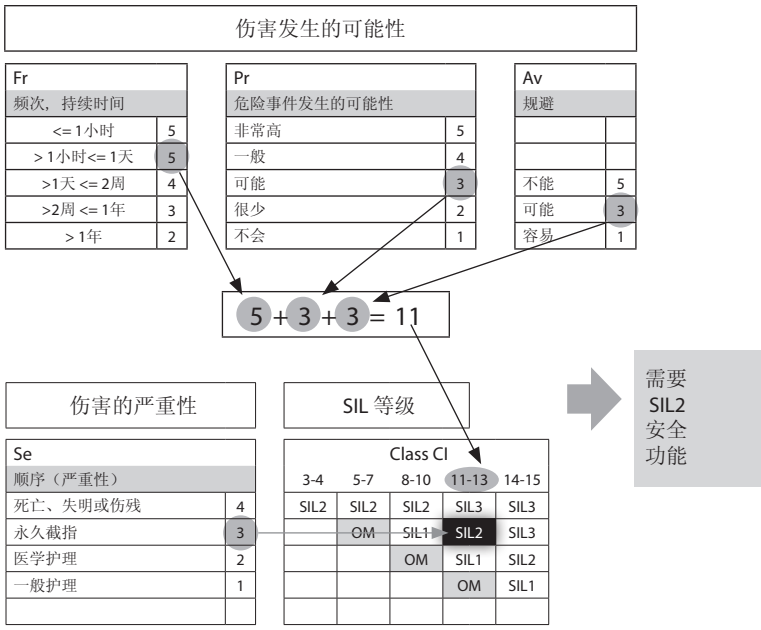


图 3-4 SIL指定列表的例子

在这个例子当中，是对暴露在电机旋转轴当中作出的危险分析。

- 危险等级是永久伤害，比如，可能失去手指。严重程度Severity (Se) = 3.
- 一个人一天当中有五次需要暴露在危险当中。频率Frequency (Fe) = 5.
- 危险很有可能发生。发生的可能性Probability (Pr) = 3.
- 危险可以被规避。规避的可能性Avoidance (Av) = 3.
- 5 + 3 + 3 = 11, 根据事先的定义， 符合SIL 2.

表格中各个要素的定义在标准中有说明。

SIL的要求定义之后，可以开始使用安全系统。

确定PL（EN ISO 13849-1）需求

为了确定PL要求，从下列目录中选择一种方法，制定一种途径满足PL的要求。

1. 确定危险的紧迫程度。
   紧迫性的定义如下：
   S1 轻微的，通常指可康复的伤害
   S2 严重的，通常指永久伤害，包括死亡

2. 确定暴露在危险当中的频次和时间长度
   频次和时长的定义如下：
   F1 极少短时暴露在危险环境当中
   F2 频繁长时间暴露在危险环境当中

3. 确定阻止危险发生的可行性或者限制危险带来的伤害
   防止危险发生和限制危险带来的伤害定义如下：
   P1 在一定条件下可以实现
   P2 几乎不可能

例如：
表现类别分成a， b， c， d和e，如下图描述。

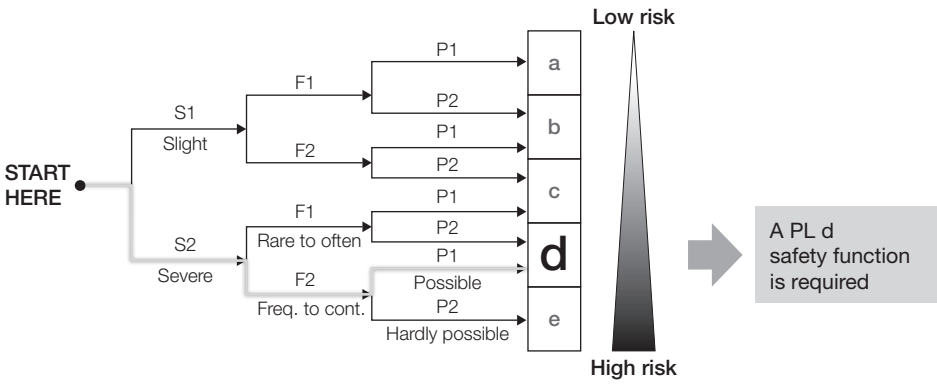


图 3-5 PL风险示例

在这个例子当中，对一个裸露的电机旋转轴进行危险分析。
- 危险发生是严重不可恢复的永久伤害。 严重程度Severity = S2.
- 人员暴露在危险环境当中是一天数次。频率Frequency = F2.
- 避免或限制危险造成的伤害是几乎不可能的。可能性Possibility = P2.

按上图指示，PL数值是d。确定各个因素数值在标准当中有说明。安全性能（PL）确定之后，就可以开始使用安全系统了。

步骤5：应用功能安全系统

当设计和规划一个安全功能时，为了满足前面章节提到的特定的SIL/PL要求，在功能安全系统当中使用经过验证的子系统对安全系统的设计人员来说可以大大节省工作量。当精心计算安全和可靠性，使用验证过的子系统之后，应用安全功能将变得很方便。

注意：
如果不使用经验证的子系统，就必须对每个子系统做安全性计算。标准EN 62061和EN ISO 13849-1包含了相关的过程和必需的计算参数信息。

使用和验证过程在子系统之间反复同步进行。在应用过程中验证被当作一个工具，检查应用系统是否满足安全水平的预定要求。更多验证过程，参照下述步骤。

注意：
系统的强健性取决于最薄弱的位置。这就意味着，为了满足机器安全指导EHSR要求设定的要求，所有功能安全子系统必须满足系统的SIL/PL的要求。

市场上有多款计算软件用于验证功能安全系统。这些程序可以对整个过程进行方便的验证。

应用功能安全系统的一般步骤包括：

1. 确定符合标准EN 62061 或 EN ISO 13849-1的SIL/PL的要求。

2. 选择用于安全系统的系统结构。标准EN ISO 13849-1 和 EN 62061提供了带计算公式的基本结构。

3. 确定

- 类别B，1，2，3 或 4，在标准ISO 13849-1有说明
  或者
- 指定结构A，B，C 或 D，在标准EN 62061有对子系统和整个系统的说明。

更多指定结构的系统，参见相关说明。

4. 从安全相关子系统构建系统 – 传感器/位置开关,输入, 逻辑, 输出和执行器

   或者：
   - 使用已验证的子系统（推荐），或
   - 对每个子系统进行安全计算。

   整个系统的安全水平等于各个子系统安全水平的总和。

5. 安装安全系统。

   系统必须被正确安装，避免因为不当接线、环境或其它类似因素造成的失效。安全系统因为不当安装造成不能正常工作，那就没有保障安全的用处，甚至有可能带来危险。

6. 验证系统功能。

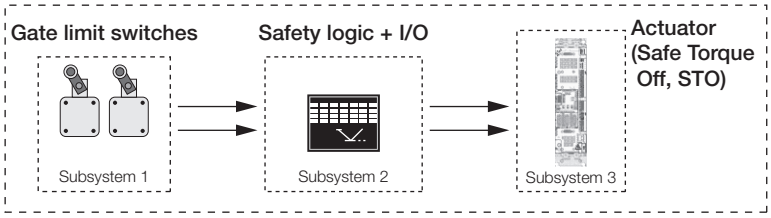


图 3-6 安全功能的结构

步骤6：验证功能安全系统

功能安全系统的验证用于确保应用安全系统满足特定的安全要求以及安全功能是否可行。

验证不能在应用过程结束后进行，而是同时完成。从而保证整个应用过程满足特定要求。

为了验证系统的SIL和PL，安全系统的修正操作也必须完成功能测试。

验证安全系统的安全完整性等级（SIL）（EN62061）
为了验证安全完整性等级，必须展示安全表现，也就是可靠性，安全功能必须等于或高于在风险评估当中给出的安全目标要求。建议使用经验证的子系统，因为子系统制造商已经确定了决定系统安全完整性（SILCL）和随机硬件安全完整性（PFH_d）的相关内容。

验证使用经验证的子系统的安全系统的安全完整性等级（SIL）的方法如下：

1. 使用子系统定义的SIL限制要求（SILCL）来确定系统安全完整性。

   SILCL 代表子系统的最大SIL值。SILCL用来确定已获得的安全完整性等级（SIL）：整个系统的SILCL不高于最低子系统的SILCL。

2. 用子系统定义的每小时危险失效发生的可能性（PFH_d）来衡量系统随机硬件的安全完整性。经验证的子系统的制造商通常会提供他们系统的PFH_d 值。

   PFH_d 是随机硬件失效数据，它决定安全完整性等级（SIL）。

3. 使用常见失效原因分析（CCF）列表去检查所有必需的相关项目在创建的安全系统当中没有遗漏。

   CCF 检查列表可以在标准EN 62061 附录F当中找到。

   根据列表计算每个点的值，整个得分和标准EN62061附录F，表F.2的CCF因子（β）比较。这个数值用于估算PFH_d 的数值。

4. SIL：根据SIL的定义确定获得SIL的水平。

验证SIL的例子：
验证电机旋转轴功能安全系统：

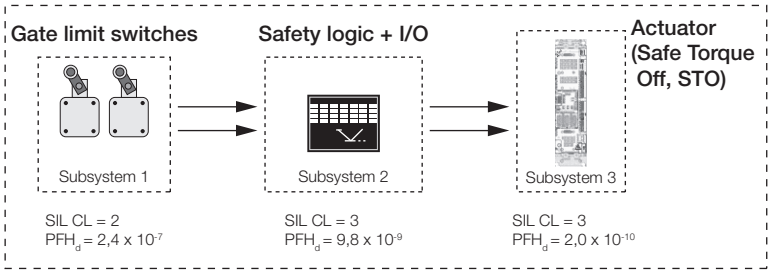


图 3-7 验证SIL的例子

系统安全完整性：
$SIL\ CL_{sys} \leq (SIL\ CL_{subsystem})_{lowest}$ -> SIL Claim Limit 2

随机硬件安全完整性：
$PFH_d = PFH_{d1}+PFH_{d2}+PFH_{d3} = 2{,}5 \times 10^{-7} < 10^{-6}$

系统满足SIL 2.

按照整个系统PFH_d数据确定SIL的表格：

SIL	每小时可能发生的危险（1/h）
SIL 1	$\geq 10^{-6}$ up to $< 10^{-5}$
SIL 2	$\geq 10^{-7}$ up to $< 10^{-6}$
SIL 3	$\geq 10^{-8}$ up to $< 10^{-7}$

表 3-1 确定SIL的表格

验证安全系统（EN ISO 13849-1）的安全性能（PL）

为了验证安全性能，必须先确定相应安全功能要求的安全性能。如果安全功能是由多个子系统组成，这些子系统的安全性能必须等于或大于上述安全功能的要求。
推荐使用经验正的子系统，因为安全性能对这些子系统已经有规定。

使用经验证子系统的安全系统安全性能（PL）的步骤如下：

1. 按照一般失效的检查列表，确定系统的一般失效的安全程度

   一般失效列表（CCF）可以在标准EN ISO 13849-1:2008 附录 I 当中

找到。

最小值是65分。

2. 根据已建立的柱状图标确定获得的安全性能：

- 种类，
- 平均危险失效时间（$MTTF_d$），和
- 全面诊断（DC）。

$MTTF_d$ 是危险失效发生的平均时间。DC表示可以通过诊断检测到的危险失效的次数。

更多和计算相关的信息细节可以在在标准EN ISO 13849-1当中找到。

3. 在PL图当中输入结果数值，可以确定PL。

验证PL的例子：
验证电机旋转轴功能安全系统：

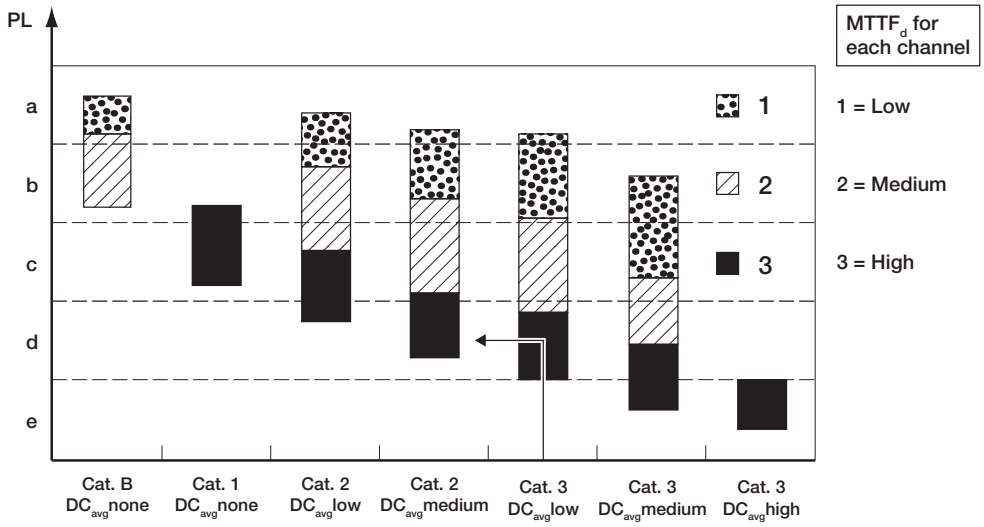


图 3-8 确定PL的例子

上面例子的安全表现水平如下：

- 结构是类别3，
- $MTTF_d$ 是高，
- DC 平均数值低。

系统满足PL数值d。

通过PFH_d数值确定PL

PL	每小时危险失效时间发生可能（1/h）
a	$\geq 10^{-5}$ up to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ up to $< 10^{-5}$
c	$\geq 10^{-6}$ up to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ up to $< 10^{-6}$
e	$\geq 10^{-8}$ up to $< 10^{-7}$

表 3-2 确定PL的表格

对比SIL和PL
虽然两个标准的评价体系完全不同，评估结果在随机硬件失效方面是相似的。

安全完整性等级SIL	表现水平 PL
无对应	a
1	b
1	c
2	d
3	e

表 3-3 SIL和PL对比表

步骤7：验证功能安全系统

每一个安全功能都必须通过验证，以确保对降低在风险评估环节得出的风险是有效的。

为了确定功能安全系统的有效性，在系统进行符合机器安全指导的EHSR要求的风险评估过程的时候，就必须进行系统检查。

步骤8：功能安全系统的文件化

在机器符合机器安全指导要求之前，必须准备机器设计文档和用户手册。

文档必须精心准备以备查阅。
文档必须准确、简练，同时又必须信息完备方便用户理解。所有危险都必须在用户手册中注明，并且提供机器安全操作的指导。
文档必须方便查阅和保存。
用户手册随机器发给用户。

更多关于文档的信息，参见机器安全指导EHSR的附录 I 部分。

步骤9：符合性验证

在一台机器上市销售之前，制造商必须保证机器的应用满足安全标准的要求。还必须证明机器的安全相关部分的安全功能组合满足设计要求。

证明机器符合安全指导的步骤如下：

- 机器满足机器安全指导规定的相关重要健康及安全（EHSR）要求。
- 机器满足其它相关指导的要求。
- 这些要求的符合性可以通过相关标准提供的指导来验证。
- 技术文件实时更新并且易于获得。
  技术文档包括表明机器符合机器安全指导相关规定的部分。

  注意：
  技术文档的缺失可以被认为机器不符合EHSR。

  技术文件的内容必须涵盖设计、制造和机器操作，这些对机器的符合性验证要求都是必须的。更多相关信息可以参见机器安全指导98/37/EC的附录VI部分，或者在新的指导生效之后参见新机器安全指导2006/42/EC的附录VII部分。

- 必须已经进行符合相关标准的符合性评估过程。对机器的特殊要求满足机器安全指导的附录IV部分。
- 必须给出EC符合性声明，并且随机器发货。

符合性通过后，可以使用CE标志。

带有CE标志和EC符合性声明的机器是一定符合机器安全指导要求的。

术语

CE 标记
机器或其它在欧盟经济区（EEA）销售的商品强制遵照的标准。对于带有CE标志的产品，制造商保证产品符合相关欧盟标准的特定要求。

CCF，一般失效
一个事件导致多个子系统失效的情况。所有的失效因事件本身引起，并不会顺序发生。

DC，全面诊断
全面诊断（DC）对监视系统或子系统故障是很有效的。它可以用来表示可检测危险失效的发生频次或者所有危险失效率。

EHSR，重要健康和安全要求
机器必须符合欧盟机器指导要求，并且获得CE标志。这些要求参见机器指导附录I的列表。

EN
表示 “EuroNorm”。该前缀表示一组标准。

Harm
身体伤害或健康伤害

Harmonized standard
欧盟委员会或EFTA秘书处为了支持指导的深层次要求在欧盟法律许可范围内制定的欧盟标准。

Hazard
伤害源（危险）。

IEC，国际电工协会
由各个国家电工协会组成的国际标准化组织
www.iec.ch

ISO，国际标准化组织
由各个国家标准化成员组成的联合组织。
www.iso.org

$MTTF_d$，平均危险失效时间
危险失效发生的预期时间。

PFH_d，每小时危险失效发生的可能性
危险失效平均每小时发生的可能性。PFH数值在安全功能当中决定SIL或PL数值。

PL，安全性能
安全性能（a，b，c，d，e）代表了一个安全系统在已知条件下的安全功能的表现。

PL_r
要求的安全性能（基于危险评估）。

Risk
伤害发生的可能性和伤害程度的组合。

Safety function
该功能设计用于增加机器的安全性。该功能失效会导致伤害风险快速增加。

SIL，安全完整性等级
安全完整性等级（1, 2, 3, 4）表示一个电气安全系统在已知条件下的安全功能。在机器当中仅使用1-3。

SILCL，SIL 限制性声明
在考虑结构约束和系统安全完整性之后，对一个电气安全系统的最大安全安全完整性等级(SIL)声明。

Subsystem
安全功能的一部分，有自己的安全性能（SIL/PL），会影响整个系统的安全功能。如果一个子系统失效，则整个系统的安全功能失效。

3ABD00000048753 REV A 中文
基于: 3AUA0000048753 REV A 英文
生效日期: 2010-07-01

北京ABB 电气传动系统有限公司
中国，北京，100015
北京市朝阳区酒仙桥北路甲10号D区1号
电话：+86 10 58217788
传真：+86 10 58217618
24小时×365天咨询热线：(+86) 400 810 8885
网址：http://www.abb.com/motors&drives

3ABD64514482 REV A 中文
基于：3AFE64514482 REV D 英文
生效日期: 2010-10-01

北京ABB 电气传动系统有限公司
中国，北京，100015
北京市朝阳区酒仙桥北路甲10号D区1号
电话：+86 10 58217788
传真：+86 10 58217618
24小时×365天咨询热线：(+86) 400 810 8885
网址：http://www.abb.com/motors&drives