 DOI: https://doi.org/10.12345/hgyjxjz.v3i4.25603

Discussion and research on the mechanical safety of domestic manufacturing equipment

Ping Dai

Shanghai Beixin Surface Technology Co., Ltd., Shanghai, 200000, China

Abstract

The concept of safety design and safety manufacturing of domestic equipment manufacturing enterprises is uneven, and the equipment has hidden dangers, which does not conform to the rules and specifications of foreign equipment manufacturing.The section introduces the relevant standards of equipment manufacturing, and mainly introduces the four key parts of the mechanical instructions in the CE standard. From the beginning of equipment manufacturing, we need to consider the safety issues, and how to assess the equipment, and eliminate the risk from the early design. The introduction of CE standard concept of mechanical protection, and for the mechanical protection of safety distance, safety components, safety level and a series of concepts in detail, make the designer according to the need of safety level, design in equipment machinery, equipment electrical, equipment programming system in line with the CE standard of mechanical safety instruction equipment.

Keywords

mechanical instructions; Secure components; Performance Level (PL); CAT (Safety Structure); SPR -/CE (Safety Control Circuit)

国内制造设备机械安全方面探讨和研究

戴平

上海北新表面技术有限公司，中国 · 上海 200000

摘　要

国内设备制造企业安全设计和安全制造的理念良莠不齐，制作的设备存在隐形的安全隐患，不符合国外设备制造的规则和规范。本文针对设备制造的相关标准进行介绍，重点介绍了CE标准中的机械指令的四大部分重点内容。从设备开始制造需要考虑到安全问题，以及对设备如何进行风险评估，从前期设计上进行风险消除。引入了CE标准的机械防护的概念，并针对机械防护方面的安全距离，安全元器件，安全等级等一系列的概念进行详细的阐述，使设计者根据需要的安全等级，设计出在设备机械、设备电气、设备编程系统的符合CE标准的机械安全指令的设备。

关键词

机械指令；安全元件；性能等级（PL）；CAT（安全结构）；SPR-/CE（安全控制回路）

1 引言

安全第一，安全生产，安全方面已经渗透到企业的各种活动的方方面面中，设备进行生产中，人员是一个随性不可控的因素，利用设备制造的安全设计和安全控制，进行保证安全是一个必经之路。所以设备生产商要达到基本的安全设计和安全制造，符合欧盟的设备标准或通过第三方的安全机构认可，找到安全和经济的一个平衡点。

2 设备制造相关法规

机械安全制造标准：

国际标准：1：ISO 国际化标准组织　2：IEC 国际电工委员会

欧洲标准：1：CEN 欧洲标准化委员会　2:CENELEC 欧洲有关电气行业标准化

其他标准：ANSI　STANDARDS JISSC 等标准

3 CE 标记和机械指令

3.1 CE 标记

CE: 是对机器、流程或者某个符合欧盟指令框架下的工件设备进行有文件存档的物理检查。

欧盟成员国之间必须保证带有 ce 标志且经过 ce 实验标准的产品自由地流通和使用。

下列情况的设备需要由 ce 标记

1) 第一次进入欧盟的新设备；2) 自己为了满足使用而自己制作的设备；3) 为销往欧盟而制造的设备；4) 机器经过改造超出其原有限制的设备；5) 旧设备（已投入市场或大幅改进的）

设备制造，符合 ce 标记，进入欧盟，符合法规的涉及

【作者简介】戴平（1985–），中国上海人，本科，工程师，从事机电一体化研究。

的方面太多，主要大的指令我列举一下：机械指令、低电压指令 LVD、电磁兼容指令 EMC、ATEX 指令、无线电指令、关于现在在电子电气设备中使用某些优化成分的指令 (ROHS)

3.2 机械指令

我主要介绍和解读一下通常设备的 2006/42/CE 机械指令标准。机械指令分为四个部分，十二附录

对于 CE 认证要求的所有设备必须执行并满足基本的健康安全要求（EHSRS）,EHSRS 在机械指令中可分为六个部分。为附录 1，附录 2-6。

附录 1 是所有设备都必须执行基本指令要求，我们介绍一下具体内容。

附录 1 的指令大致分为三个主要方面

1）基本健康与安全要求适用于指令内所有机器 2）指令试图确保使用者在整个机器生命周期中的安全：设计、安装、运行、调整、拆除、清洗、维修、运输、保养、报废 3）制造商必须确保进行风险评估，以确定使用机器的健康和安全要求，设计和制造必须考虑到风险评估的结果

在具体和通俗细分为下面方面：

1) 基本要求：定义（操作者，危险区域，暴露人员）综合安全原则。2) 控制系统（控制系统的安全可靠，控制装置（设计、位置、选择），启动 / 停机，控制系统失效。3) 机械危害：机械稳定性，操作的中断等待。4) 防护和包含装置：固定式防护，连锁活动式防护装置。5) 其他危害：电源静电，安装错误，防错等等

4 风险评估

制造商根据标准进行设计和制造设备，在制造过程中有法规参照，同时要借助风险评估的工具，目的：识别与机器相关风险、识别和减少所有可能的风险、确定所需安全系统的范围。

风险识别主要途径为两个途径进行：

A. 演绎法：从可能的结果（伤害）的检查表开始，并确定那些危险能导致这些风险。--- 主要有失效树分析法。

B. 归纳法：检查所有的危险源，并考虑模型方面发生错误可能导致的危险情况，-- 主要下面几种方法。

i. 预先风险法 (PHA): 是一个用于识别潜在的危险的安全研究方法，使用一个系统危险列表对每个具体的危险点进行评估。

ii. 失效模式分析法（FEMA）：一个向前的逻辑，自上而下，表格式的技术分析系统中每个组成部分的失效会造成怎样的结果。（通过何种方式会失效）

iii. 风险估计工具法。包含：风险矩阵法、风险图法、危险数字分级评分法

●风险矩阵：以风险发生的可能性与可能的伤害或健康损害的程度的组合，和 ISO 风险等值线原理为基础。R(风险)=P(可能性)*S(严重性)

●风险图：是基于几种给予的可能级别，通过不同的参数，根据图表所形成的路径确定风险基本的方法 (SFOA)：见图 4。

●危险数字分级评分法 :HRN=LO(发生可能性)*FE(暴露频率)*DPH（伤害的严重程度）*NP(暴露风险下的人数)

5 风险降低

对设备进行评估后，应该采取不同的措施来消除设备存在的风险。一定从设备的本质上进行控制。接下来我们从下面几个维度进行分析介绍：机械防护安全元件、电气标准元件、电气安全控制系统。

5.1 机械防护

机械防护的设计的基础和理念和一般原则可以参考 ISO12100 的标准，这是最基础的标准，是 A 类的通用准则，比如：隔音罩，合适机器的屏障等最基础的要求。而 ISO14120 则是防护一般要求的 B 类标准的参考，定义了机械防护的总类，介绍各种不同防护的要求和技术规范。如：连锁防护装置，自关闭的防护装置等。有了防护的保护，但我们还有重视一点，防护的距离和高度等参数。这些具体标准要求，可以查看 iso13857 的标准。

5.2 电气标准元件

可以参考 ICE 60204-1 方面的标准要求。 制造设备和改造设备，需要相关的电气元件，就要求相关的元件达到一定的标准，确保人员操作是安全的，设备操作相应的保持的时间是一致的，确保工业安装和使用中的安全 [8]。进线电源，防止触电，防护接地线，控制回路和功能，导体电缆等和设备相关的电源元器件都有详细的标准要求。

5.3 安全元件

安全元件就是比电气标准元件更加安全的元件，在实际操作中安装在重要的位置，可以快速响应和提升设备安全的元件。安全元件的失效会比标准元件概率更低 [2]。安全元件可以分为：安全防护装置、急停装置、安全控制和安全执行系统等。

防护装置分为：联锁装置、安全光栅、安全地毯、安全扫描器、安全脱扣装置、安全边沿等安全元件。他们都有各自的标准和规范。安全光栅要设计成安全控制冗余（双通道）。由于是电气产品，都有反应时间的， 就要求我们光栅安装的时候对危险源具有一定的安全距离。这要更加实际情况进行计算。

计算公式如下。S=(K*T)+C

S: 安全距离　K= 接近速度　T= 完全停止时间　C= 额外距离

不同的工作环境，不同的设备，不同危险源，光栅不同的安装方式，保护的安全距离都不一样。可以参考 ISO13855 的表。也可以自行计算，但计算的结果至少大于 ISO 的标准表为宜。

5.4 电气安全控制系统：

制造设备通过风险评估，各种安全元件，安全防护装置由普通正常电气系统控制起来，就可以初步形成一个初步

设备，但是普通电气系统也有可能失效，和不稳定，导致证系统还是不安全。所以普通电气控制系统也要换成使用电气安全系统 [7]。

6 电气安全控制系统 SRP/CS

电气安全系统是重要的知识点和安全控制组件，所以单独形成一个章节进行介绍。它是由相关的控制系统安全有关部件（SRP/CS）根据电路设计组成一个安全系统。这种系统在检查到无法接受或者是危险的情况下，会执行特定的功能以实现和保持机械 / 过程的安全状态。这种系统具体稳定性高，可靠性强，具有防错和快速响应功能 [1]。

安全控制系统使用的标准，

lISO13849：控制系统有关安全部件

lIEC62061：安全有关电气，电子和可编程电子控制系统的功能安全

6.1 电气安全控制系统设计四大流程

安全控制系统整个流程如下表。分为四大流程过程：风险评估、设计（scs）系统实施、安全验证。风险评估之前章节介绍过了，我们着重介绍一下设计（SCS）流程中的。如何确定需要的安全等级，和如何详细设计，选择结构和组件的部分 [3]。这里引入“安全等级”概念。按目前两种标准。

ISO13849：性能等级 PL(a、b、c、d、e)

IEC 62061 : 安全完整性能等级 SIL(1 2 3)

6.2 安全性能等级

安全等级高，就是控制系统相关部件随机硬件失效和控制系统的失效低。两种失效都有相关的标准说明。随机失效控制参考 (IEC62061/ISO13849-1)[4]。每个安全功能都需要确定 PFH-d.(每小时危险失效概率)。在 IEC62061 中，是利用元件各个参数，通过公式计算出来。而 ISO13849-1 则由对应的 PFH-d 的表格对应以及对应的指定 结构（catb-cat4）.

性能等级的国际标准 ISO(PL A,B,C,D,E) , 和欧盟标准 IEC(1,2,3) 和 PFH-d（每小时失效概率）对应关系如图， 从图中可以看到 PLD 到 PLE 对应的失效小时，折算出来是 30 年 - 到 100 年内。

6.3 安全性能等级的设计

安全性能等级的设计流程和步骤如下图：由设计 SRP/CS（安全控制回路）和验证两个部分组成，这个部分和它的四个组成流程。

A.SPR-/CE 中所需性能等级的确认。

从下面三个维度进行设计需求；

S 伤害严重程度（S1：轻微 S2: 严重）、

F 频率 / 或对危险暴露程度 (F1: 短时间 F2 频发持续)、

P 避免危害的可能性 (P1: 特定情况可能 P2 几乎不可能)。

B. 系统结构的确定：

设计人员需为设备的相关安全功能指定一个基本控制结构，为实现此目标，需要选择符合所需性能等级的元器件（如传感器，过程单元，执行器）[5]。一个基本的结构。输入 - 逻辑 - 输出。系统结构分为 CAT(B 、1、2、3、4) 五个结构。不同的结构有着不同的特点和需要的元件。系统机构和 PL 的对应的关系如下图 . 所选的不同的结构极大影响最终获得的性能等级 PL. 根据下图和其他的设计指标，可以看出要达到 PLE , 要求就是 Cat4. 系统结构具体之间的区别和要求可以参考相关的标准。

C. 细节设计：

需要考虑的三个方面，满足用于安全功能的特定设计，如果停止功能，手动复位。系统结构，遵循先前阐述定义的类型，元件的选择：基于产品认证，性能等级，可靠性数据。

D. 设计评估：

6.5 IEC62061 对安全控制系统介绍

根据结构，通道，确定 MTTF-d 确定 DC-agv 等方面进行评估。确定最终方能后进行第二部分中 的施工，施工完成后，工程验收等工作。进而整个设备的完成这里就简单带过 [6]。具体可参考 ISO18349 的相关资料。

IEC62061 也对系统机构有介绍和规定，简单介绍一下

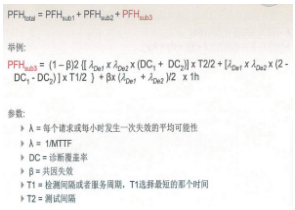
1：确定安全性能等级：CI（最终发生伤害的可能性）= FR(面临风险的时间和频率)+PR（发生危险的可能性）+AV（避免危险的可能性） 见图 1

2：计算出 PFE-d（每小时危险失效概率），见图 2

3：为了达到 SIL 等级，需满足够的结构性和系统失效完整性

Severity Se	Class CI				
	3 - 4	5 - 7	8 - 10	11 - 13	14 - 15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		OM	SIL 1	SIL 2	SIL 3
2			OM	SIL 1	SIL 2
1				OM	SIL 1

图（1）安全性能等级



图（2）PFE– 计算公式

7 结论

工程师根据以上介绍了机械指令机构组成，风险评估等基础知识后。在设备设计和改造中，得到了相应的风险点的知识，确定需要的安全风险等级，系统设计 cat 的类型，进行设备风险降低的几个维度方面具体措施：机械防护安全元件，安全电气控制，防护的安全距离，安全元件中的光栅防护距离计算等。选择出设计的几大步骤原则，工程师们可以设计出符合 ce 机械安全的设备。保证设备对人员的安全保护。

参考文献

[1] 黄祖广,张承瑞,赵钦志等.基于IEC62061标准的SRECS风险评估与SIL分配[J].制造技术与机床,2013。

[2] 袁晓慧,尹震宇,黄祖广等.基于故障树分析的数控装置硬件平台功能安全设计与实现[J].组合机床与自动化加工技术,2015.

[3] 张建国.浅谈机械安全-E/E/PE控制系统的功能安全标准IEC 62061[J].中国仪器仪表,2009.