ICS 13.110
J 09

中华人民共和国国家标准

GB/T 16855.1—1997

机械安全　控制系统有关安全部件
第一部分　设计通则

Safety of machinery—Safety related parts of control systems—Part1: General principles for design

1997-06-06 发布　　1998-01-01 实施

国家技术监督局 发布

目　　次

前　言

本标准等效采用欧洲标准(草案)PREN954-1:1994《机械安全控制系统有关部件——第1部分:设计通则》。PREN954-1已于1996年10月批准为正式欧洲标准,在内容上没有改变。ISO/TC 199于1993年就将PREN954-1:1992转为国际标准文件(ISO/TC199N45),发至各成员国征求意见,准备转为国际标准。为了加快我国的机械安全标准制定步伐,使之尽快与国际和国外先进标准接轨,经研究,先等效采用该欧洲标准草案PREN954-1:1994制定国家标准,待正式国际标准出来后,若有变化,再进行修订。

本标准与PREN954-1:1994主要有以下两点不同:

1.将引用标准的导言按GB/T 1.1—1993进行了修改,并将引用的有关欧洲标准和IEC标准凡有对应国家标准的均改为相应的国标,而且取消了原标准中引用的一些欧洲标准草案。(prEN 842、prEN981、EN982、EN983、prEN999、prEN1037、prEN50100-1、prEN61310-3),因为这些标准草案都还正处在起草过程中,在EN954-1的条文中也没有具体出现过,故在本标准中未引用。

2.取消了提示的附录E"文献目录"。因为该"目录"所列的IEC和几个欧洲国家的有关可编程电子系统的标准文件,我们国内都没有,即使列出也无处查找。"目录"中所列的有关质量保证体系的几个国际标准,在本标准正文中都没有涉及到,不应作为本标准的参考文献。

附录A至附录D是提示的附录。

本标准自1998年1月1日开始实施。

本标准由中华人民共和国机械工业部提出。

本标准由全国机械安全标准化技术委员会归口。

本标准负责起草单位:机械科学研究院。

本标准的主要起草人:马贤智、李勤、张尔正、徐自芬、萧维、张铭绫、王国扣。

中华人民共和国国家标准

机械安全　控制系统有关安全部件　第一部分　设计通则

GB/T 16855.1—1997

Safety of machinery—Safety related parts of control systems—Part1:General principles for design

0　引言

机械控制系统中有些部件通常用于保证安全，这些部件称为有关安全部件，它们可由硬件和软件组成，提供控制系统的安全功能。它们可以是控制系统的整体部分，或单独部分。

关于出现故障时控制系统有关安全部件的性能在本标准中被分为五种类别(B、1、2、3、4)，这些类别宜用作参考点，不用作有关安全要求方面的某些顺序或层次。

这些类别可以用于：

——所有机械的控制系统，从简单的如小型炊事机械到复杂的制造设施如包装机械、印刷机械、压力机等的控制系统。

——防护装置的控制系统，如双手操纵装置、联锁装置、电敏防护装置(光电屏障)和压敏垫等。

类别的选择将取决于机器和防护措施所用的控制手段。

选择类别和设计控制系统有关安全部件时，设计者至少需要说明以下有关安全部件的信息：

——选择的类别；

——在机械防护措施中起作用的功能特征和确切部分；

——各种确切限制；

——考虑所有与安全有关的故障；

——通过故障排除和采取措施可以排除而勿须考虑的与安全有关的故障；

——有关可靠性参数，例如环境条件；

——所采用的技术。

使用类别作为参考点和设计原理的说明是为了标准可以灵活应用，并为控制系统(和机器)有关安全部件的设计和应用性能提供一个可以通过第三方或内部或独立试验机构进行评定的明确基准。

1　范围

本标准规定了控制系统有关安全部件安全要求和设计导则，并规定了这些部件的类别及其安全功能特征。其中包括所有机械和有关防护装置的可编程系统。本标准适用于所有控制系统有关安全部件，不管使用何种能量形式，如电的、液压的、气动的、机械的。本标准对在特定情况下采用哪些安全功能和那种类别未具体规定。

本标准适用于所有专业用的和非专业用的机械。需要时，也可用于具有类似危险的在其他技术应用场合使用的控制系统有关安全部件。

2　引用标准

下列标准所包含的条文，通过在本标准中引用而构成本标准的条文。本标准出版时，所示版本均为

国家技术监督局1997-06-06批准　　1998-01-01实施

有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB 1251.1—89 工作场所险情信号 险情听觉信号

GB 2421—89 电工电子产品基本环境试验规程 总则

GB 4208—93 外壳防护等级分类

GB 4706.1—84 家用和类似电气装置安全第1部分：一般要求

GB 4798.10—84 电工电子产品应用环境条件 导言

GB/T 5226.1—1996 工业机器电气设备 第1部分：通用技术条件

GB/T 15706.1—1995 机械安全 基本概念与设计通则 第1部分：基本术语 方法学

GB/T 15706.2—1995 机械安全：基本概念与设计通则 第2部分：技术原则与规范

GB/T 16755—1997 机械安全 安全标准的起草与表述规则

GB 16754—1997 机械安全 急停 设计原则

GB/T 16856—1997 机械安全 风险评价的原则

3 定义

本标准除使用GB/T 15706.1中给出的定义外，还采用下列定义。

3.1 控制系统有关安全部件 safety related part of a control system

对应于来自受控设备(和/或来自操作者)的输入信号而产生有关安全输出信号的控制系统的一个部件或分部件。控制系统组合的有关安全部件起始于有关安全信号被触发处，结束于动力控制元件的输出处(见GB/T 15706.1—1995的附录A)。这也包括监控系统。

3.2 类别 category

根据其耐故障情况和随后在故障条件下的工况对控制系统有关安全部件的分类，这种分类是通过它们的结构安排和(或)通过其可靠性达到的。

3.3 控制系统安全性 safety of control systems

根据在故障情况下的工况所规定的类别的控制系统在给定时间内执行其功能的能力。

3.4 控制系统可靠性 reliability of control systems

在规定的条件下和规定时间内控制系统执行其规定功能的能力。

3.5 故障 fault

无能力执行所需功能的产品特征状态，不包括预防性维修或其他有计划的活动期间或由于缺乏外部资源而无能力执行所需功能。

注：

1 故障通常是产品自身失效的结果，但它可以存在于没有失效之前。

2 在实践中，故障和失效(见3.6)通常用作同义语。

3.6 失效 failure

产品执行所需功能能力的终止。

注：

1 失效后产品具有故障。

2 “失效”与“故障”的区别是，“失效”是一事件，而“故障”是一种状态。

3 所定义的这种概念不适用于只有软件构成的产品。

3.7 安全功能 safety function

由输入信号触发的并通过控制系统有关安全部件处理的能使机器达到安全状态的一种功能。

3.8 抑制 muting

在机器以其他安全条件运转期间，由控制系统有关安全部件暂时自动中止一种或几种安全功能。

3.9 手动重调 manual reset

控制系统有关安全部件内的一种功能，它可以在机器重新起动之前，由手动恢复给定的安全功能。

4 总则

4.1 设计过程中的安全目标

提供安全功能的控制系统有关安全部件应设计得使遗留风险在以下情况下是可接受的：

——在全部预定使用期间和可能预见的误用时；

——出现故障时；

——整个机器在预定使用期间出现可预见的人为差错时。

4.2 一般设计对策

设计者应根据对机器的风险评价，决定需要由控制系统有关安全部件的每一个部件减小风险的分配〔见附录 B(提示的附录)〕。这种分配不包括受控机器的全部风险，例如不考虑一台机械式压力机或洗衣机的全部风险，而只考虑通过应用特定安全功能减小的那部分风险。通过使用压力机电感防护装置触发的停机功能或洗衣机的锁门功能都是这种功能的例子。

主要目标是设计者应保证控制系统有关安全部件在内部失效或外部干扰的情况下，不产生会导致高于可接受遗留风险的风险输出。这不是总能达到的，但设计者应将出现高于可接受风险的输出减至最小，并且在这种情况下应提供其他安全措施。减小风险对策的分步示意图见 GB/T 15706.1—1995 的第 5 章。

设计者对有关安全部件选择的类别和其他特征(例如各部分的物理位置、隔离)将取决于该部件对减小风险的作用和在设计与工艺中使用的技术。设计者应负责说明：

——哪些类别将被用作设计参考点；

——有关安全部件的确切起点和终点；

——达到那种(些)类别设计的设计基本原理(例如考虑的故障、排除的故障)。

由控制系统有关安全部件减小的风险越大，需要那些部件具有的耐故障能力越高。这种能力(理解为所需执行的功能)可通过可靠性值和耐故障结构部分地量化。可靠性和结构两者都影响有关安全部件耐故障的这种能力。规定的耐故障性可通过规定元件可靠性水平和(或)采用改进的有关安全部件结构来达到。可靠性和结构的作用可随所用的技术而变化。例如，在一种技术条件中，一种高可靠性的单通通道有关安全部件，可能提供与在别的技术中故障容许的可靠性较低的结构具有同样的或更高的耐故障性。

注 1：有关安全部件耐故障性越高，不能执行所需安全功能的概率就越低。

可靠性和安全性不是同一概念(见 3.3 和 3.4)。例如，在一个冗余的结构中，具有相对不可靠性元件系统的安全性可能比具有较简单结构但具有较高可靠性元件系统的安全性更高。弄清这一概念很重要，因为在有些应用场合，不管达到的可靠性如何，优先需要最高的安全性。例如，当失效的后果总是严重的并且通常是不可挽回的时候。在这种应用场合，应根据风险评价，提供一种故障探测(一个周期允许的故障)结构，这种结构能提供一次、两次或多次故障后所需的安全功能。

在安全性主要是通过改善系统结构获得的场合，对复杂结构本标准不要求计算可靠性值。在元件的可靠性对安全性是重要的场合，对于简单结构(例如一个单通道)计算可靠性值对通过各有关安全部件分担全部风险的减小是有用的。

注 2：机械的安全性、可靠性和可用性之间的关系在附录 D(提示的附录)中进一步讨论。

在低风险应用的情况下，避免故障的一些措施可能是合适的；对于高风险应用场合，要通过改善控制系统有关安全部件的结构未提供避免、查明或容许故障的一些措施。实际措施包括冗余、多样性、监控。

所达到的控制系统有关安全部件的耐故障工况是一种多参量函数，包括：

——与执行安全功能有关的可靠性；

——控制系统的结构；

——有关安全文件的质量；

——规范的完善性；

——设计和维修；

——软件的质量和正确性；

——功能试验的范围；

——受控机器或机器零件的工作特性。

这些参量可归咎于以下三个主要特征：

——硬件的可靠性——为避免故障的各元件可靠性水平；

——系统结构——为避免、容许或查明故障，对控制系统有关安全部件中各元件的配置；

——影响控制系统有关安全部件工况的不可能定量的一些定性特征。

4.3 安全措施选择和设计的过程

本条规定了选择待提供的安全措施及随后设计控制系统有关安全部件的过程。重要的是判别控制系统有关安全部件和非有关安全部件与机器的所有其他部件间的接口，以实现由有关安全部件减小风险的作用。

因为减小机器风险可有多种方式，设计控制系统有关安全部件也可有很多方式，所以这种过程是反复的。在程序的某一步所做的决定和(或)假设可能影响前一步的决定和(或)假设。这方面可通过某一步程序的反馈进行核查。在鉴定阶段的这种核查对确保所达到的安全性能与在规范中所规定的相同是重要的。

图1是该过程的说明。提醒设计者在设计进程中应考虑的一些重要方面以问题的形式给在附录A(提示的附录)中。这些问题说明了在设计有关安全部件中应遵循的基本原理。对于每种应用场合不是所有问题都适用，在有些应用场合还需要增加一些问题。

第1步：危险分析和风险评价

——根据GB/T 15706.1和GB/T 16856鉴别机器在各种运行模式期间和在其寿命期的每一阶段所存在的各种危险。

——根据GB/T 15706.1和GB/T 16856评价由这些危险产生的风险和确定对那种应用场合合适的风险减小。

第2步：确定减小风险的措施

——在机器和(或)安全防护设施方面的设计措施都能起到减小风险的作用。作为设计措施组成部分起作用的控制系统各部件或在安全防护装置的控制中起作用的控制系统部件都应视为控制系统有关安全部件。

第3步：规定需由控制系统有关安全部件提供的安全要求。

——规定由控制系统提供的安全功能(见第5章和其他参考文件)。有些特性将出自于设计，有些出自于使用的其他方法，还有些出自于控制系统的直接要求。表1中列出了选择具体安全功能时均应包括的、比较通用的各种安全功能和特性的参考资料来源。

——规定如何达到安全(如通过使用经过验证的元件和(或)通过使用故障探测系统)和如何选择控制系统有关安全部件内的每个零件和组件的类别(例如选择结构)。

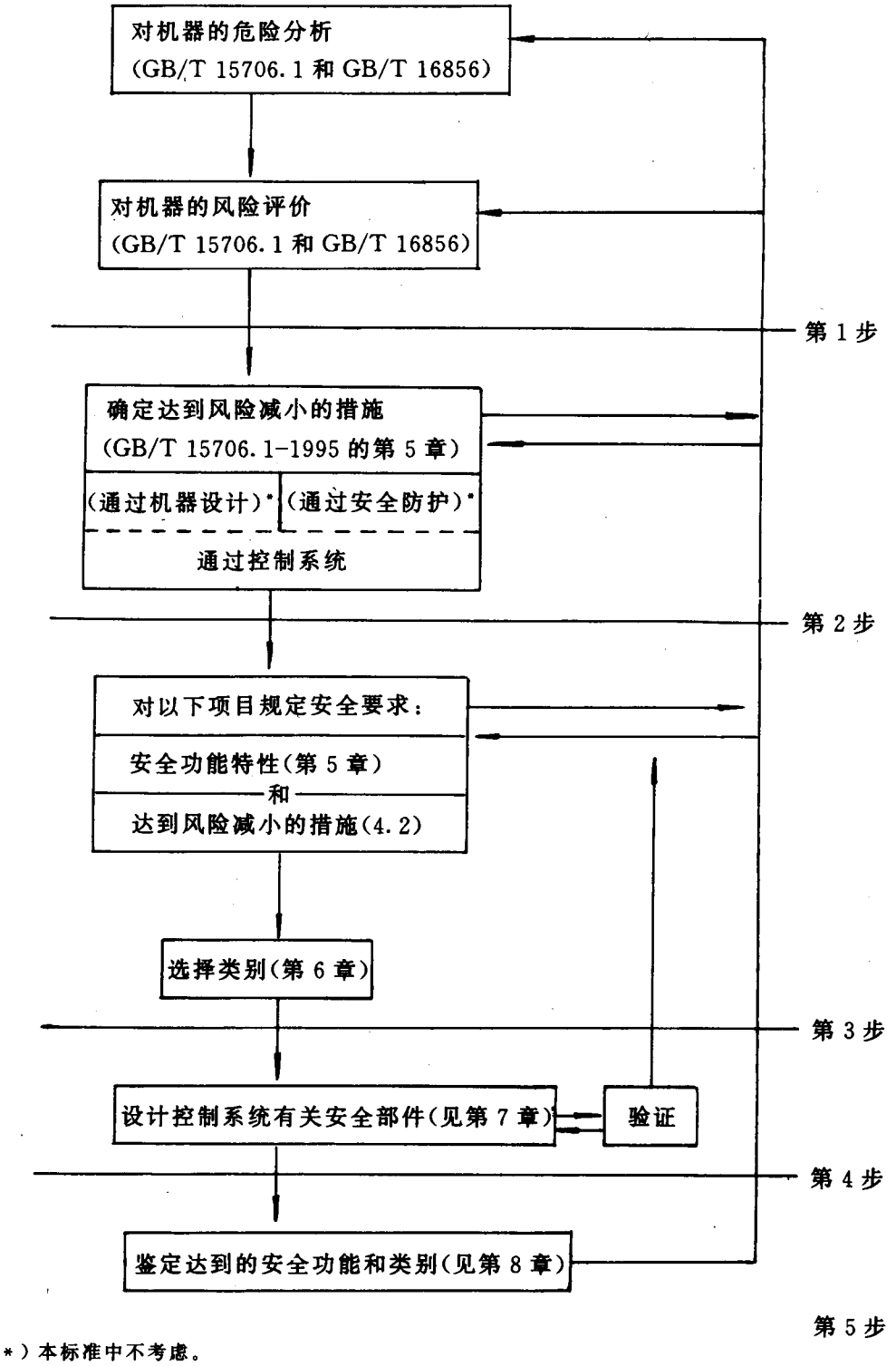
第4步：设计

——根据第3步形成的规范和4.2中的一般设计对策，设计控制系统有关安全部件。列出所应包括的为达到相应类别提供设计原理的各种设计特征。

——考虑可预见的故障(见第7章)验证每一阶段的设计。

注：验证是确定控制系统有关安全部件是否满足设计过程每个阶段全部规定要求的过程。

第5步：鉴定



*）本标准中不考虑。

图 1　设计控制系统有关安全部件的迭代过程

——对照第3步中的规范，鉴定设计所达到的安全功能和类别，必要时重新设计(见第8章)。

——在控制系统有关安全部件设计中，使用可编程电子设备时，还需其他一些详细程序(见8.3.2)。

注

1 目前认为，在由于控制系统的操作不当而可能出现重大危险的一些情况下，很难以某种程度的确然性断定，依赖单通道可编程电子设备的正确运行是可靠的。在这种情况得以解决之前，单纯依靠这种单通道装置的正确运行是不可取的(见GB 5226.1—1996的12.3.5)。

2 控制系统的有关安全部件还需要和整个控制系统一起并作为机器的一部分进行鉴定。这种鉴定要求不是本标准的范围，而应由机器设计者或适当的C类标准规定。

4.4 人类工效学设计原则

人与控制系统有关安全部件之间的接口应设计和安装得在机器全部预定使用期间和可预见的误用时不会使人遭到危险(还可见GB/T 15706.2和GB 5226.1—1996的第10章)。

应采用人类工效学原则使得机器和控制系统(包括有关安全部件)便于使用，使操作者不试图以危险的方式操作。

表1 有关标准中给出的适用于控制系统有关安全部件要求的一览表

要 求	本标准	GB/T 15706.1—1995	GB/T 15706.2—1995	GB/T 5226.1—1996	GB 4706.1—84	其他标准
定 义	3	3		3	2	
设计原则	4.2		3	9.4	22	
人类工效学原则	4.4	4.9		10		
停机功能	5.2		3.7.1	9.2.2 9.2.5.3 9.4.1	7.12 24.9	
急停功能	5.3			9.2.5.4		GB 16754
手动重调	5.4					
起动和重新起动	5.5		3.7.1 3.7.2	9.2.1 9.2.5.1 9.2.5.2 9.2.6		
响应时间	5.6					
有关安全参数	5.7		3.7.9e	7.1 9.3.2 9.3.4	11.8	
局部控制功能	5.8		3.7.9 3.7.10			
动力源的波动、丧失和恢复	5.9			4.3 7.1 7.5		

表 1(完)

要　求	本标准	GB/T 15706.1—1995	GB/T 15706.2—1995	GB/T 5226.1—1996	GB 4706.1—84	其他标准
抑制	5.10					
安全功能的手动暂停	5.11		3.7.10 4.1.4	9.2.4		
盖和电柜				13.4		
可编程电子系统			3.7.7 3.7.10	12.3		
意外起动				5.4		
指示与报警			3.6.7			
人们陷入危险时的躲避和援救			6.1.2			
电气设备				全部		
断开和能量消散				5.3 6.3.1		
物理环境和运行条件				4.4		
控制模式和模式选择			3.7.9 3.7.10 3.7.11	9.2.3		
接口/连接				9.1.4 11 15.4		
控制系统不同有关安全部分之间的关系			3.7.8e	9.3.4		
人-机接口				10		

5　安全功能特性

5.1　概述

本章给出了一个可能由控制系统有关安全部件提供的典型安全功能(见 GB/T 15706.1—1995 的 3.13)清单(见表 1)。为了实现特定应用场合控制系统所需的安全措施,设计者(或 C 类标准的制定者)应采纳这一清单中的必要安全功能。

表 1 列出了典型安全功能。有关这些安全功能特性的细节可参考相应的引用标准。对于每项安全功能,可参考这些标准(见第 2 章)的有关部分。设计者(或 C 类标准的制定者)应保证所选择的安全功

能要满足所有这些标准的要求。对于有些功能特性，在本章中也提出了附加详细要求，在选择安全特性时这些附加详细要求应包括进去。

在必要场合，这些特性应适合采用不同动力源。

5.2 停机功能

除了表1中引用的各项要求外，还应做到：

由防护装置触发的停机功能应在防护装置刚一动作就使机器处于安全状态。这种停机功能应优先于运行停机功能。

当一组机器以协同方式一起工作时，应采取措施将信号提供给监控器和(或)存在安全停机条件的其他机器。

注：这种停机可能会引起操作问题和难于重新起动，例如在电弧焊时。有些应用场合，这种功能可与运行停机结合起来，以减少起用安全功能。

5.3 急停功能

除了表1中引用的各项要求外，还应做到：

当一组机器以协同方式工作时，有关安全部件应具有将急停功能信号传给协同系统的各个部分的装置。

在协同系统的一些部分是明显分离的场合(例如通过防护装置或物理装置)，不需要总是对整个系统采用急停，而只是对通过风险评价认为必要的特定部分采用急停。

有危险的部分急停生效后，该部分与其他部分接口处应不存在危险。

5.4 手动重调

除了表1中引用的各项要求外，还应做到：

由防护装置触发停机指令后，这种指令应一直保持到具备重新起动的安全条件。

重调防护装置安全功能，解除停机指令。如果由风险评价指明了这一点，这种停机指令的解除应通过手动分步仔细的操作加以确认(手动重调)。

手动重调应：

——通过控制系统有关安全部件内的分离式手动操纵装置进行；

——保证所有安全功能和安全装置处于运行准备状态；如果不可能做到这一点，重调就不能实现；

——不触发运动或危险状态；

——动作准确；

——使控制系统为接受单独的起动指令做好准备；

——只允许通过释放的操纵器操作。

重调操纵器应位于危险区外边并能清楚地看到危险区内是否有人的安全位置。

5.5 起动和重新起动

除了表1中引用的各项要求外，还应做到：

当有关安全装置给出起动或重新起动指令时，只有在危险状态不可能存在的情况下，起动或重新起动才应自动地进行。

对起动和重新起动的这些要求应当也适用于可能被遥控的那些机器。

5.6 响应时间

除了表1中引用的要求外，还应做到：

当对控制系统有关安全部件的风险评价表明需要时，设计者或供应方应说明响应时间。

注：控制系统的响应时间是机器全部响应时间的一部分。机器系统所需要的全部响应时间可能影响有关安全部件的设计(例如需要提供制动系统)。

5.7 与安全有关的参数

除了表1中引用的各项要求外，还应做到：

当与安全有关的参数(例如位置、速度、温度、压力)偏离规定限制时,控制系统应起用适当措施(例如驱动停机装置、报警信号、报警器)。

如果在可编程电子系统中与安全有关的参数的手动输入差错会导致危险状态,那么在有关安全控制系统内应提供数据检查系统(例如检查各种限制、格式和(或)逻辑输入数值)。

5.8 局部控制功能

当机器被局部控制时(例如通过可携带控制装置、吊挂操纵板),除了表1中引用的各项要求外,还应做到:

——选用的局部控制措施应位于危险区外;

——由局部控制区外边应不可能引致危险状态;

——局部和外部(例如遥控)控制之间的切换应不产生危险状态。

5.9 动力源的波动、丧失和恢复

除了表1中引用的各项要求外,还应做到:

当出现能级超出设计运行范围的波动时,包括能源丧失,控制系统有关安全部件应继续提供或激发能使机器系统其他部分保持安全状态的输出。

当能源恢复时,只有在不存在危险状态的情况下,才能自动重新起动。

5.10 抑制(见3.8)

抑制不得导致任何人面临危险状态。

抑制终止时控制系统有关安全部件的所有安全功能都应恢复。

提供抑制功能的有关安全部件的类别应选择得使包含的抑制功能不削弱安全所需的有关安全功能。

注:在有些应用场合需要一个抑制指示信号。

5.11 安全功能的手动暂停

当有必要手动暂停安全功能时(例如,设定、调整、维护、修理),除了表1中引用的要求外,还应做到:

——在那些不允许手动暂停的运行模式中,提供有效而可靠措施防止手动暂停;

——在(机器)可能继续正常运行之前,应恢复控制系统有关安全部件的安全功能;

——担负手动暂停的控制系统有关安全部件应选择得使其遗留风险是可接受的。

注:在有些应用场合需要一个手动暂停指示信号。

6 在故障情况下控制系统有关安全部件的设计

6.1 概述

控制系统有关安全部件应符合本标准中规定的五种类别的一项或多项要求。

根据4.2中阐述的对策,类别表明控制系统有关安全部件在其耐故障方面所需的工况。

B类是基本类。当出现故障时,不能执行安全功能。在1类中主要是通过选择和应用合适的元件提高耐故障的能力。在2、3、4类中对特定安全功能方面的性能提高主要是通过改进控制系统有关安全部件结构实现的。这在2类中,是通过定期检查正在被执行的特定安全功能达到的,在3类和4类中是通过保证单项故障不会导致安全功能丧失达到的。在3类中,只要合理可行,要查明单项故障,而在4类中,要查明单项故障,并要规定承受故障积累的能力。

各类别之间耐故障工况的直接比较只有在一次仅有一个参数变化时才能进行。较高的类别只有在可比较的条件下,例如使用类似的制造技术、可靠性可比较的元件、类似的维修规范和在可比较的应用场合,才能被理解为可提供更大的耐故障性。

表2是控制系统有关安全部件的各个类别、要求和在故障情况下的系统工况一览表。

当考虑一些元件失效原因时,有些故障可不包括在内(见第7章)。

表 2 控制系统有关安全部件类别

类别	要求	系统工况	实现安全的主要原则
B	控制系统有关安全部件和(或)其防护装置以及它们的元件都应根据有关标准设计、选择、装配和组合,以使其能承受预期的影响	——出现故障时可能导致安全功能的丧失	通过选用元件
1	应采用B类的要求 使用经过验证的安全元件和安全原则	像上述的B类那样,但安全功能具有更高的与安全相关的可靠性	
2	应采用B类的要求和经过验证的安全原则 应通过机器控制系统以适当的时间间隔检查安全功能 注:适当的时间间隔取决于机器的类型和应用场合	——两次检查期间出现故障会导致安全功能丧失 ——安全功能丧失通过检查判明	通过结构设计
3	应采用B类的要求和使用经过验证的安全原则。 控制系统应设计得: ——控制中的单项故障应不导致安全功能丧失,和 ——只要合理可行,查明单项故障	——出现单项故障时安全功能始终执行 ——有些(但不是全部)故障将被查明 ——未查明的故障积累可能导致安全功能丧失	
4	应采用B类的要求和使用经过验证的安全原则。 控制系统应设计得: ——控制中的单项故障不应导致安全功能丧失,和 ——在下一个有关安全功能指令发出时或发出之前查明单项故障。如果不可能查明,那么,故障的积累不应导致安全功能丧失	——故障出现时安全功能始终执行 ——故障要及时查明,以防止安全功能丧失	
注:风险评价应指明由故障引起的总体或部分安全功能丧失是否可接受。			

6.2 类别规范

6.2.1 B类

根据有关标准,采用针对具体应用场合的一些基本安全原则,将控制系统有关安全部件至少应设计、制造、选择、装配和组合得能承受:

——预期的操作应力(例如与开关容量和频次有关的耐久性和可靠性);

——加工物质的影响(例如洗衣机中的洗涤物质);

——其他相关的外界影响(例如机械振动,外部场,电源波动或中断)。

注:

1 对遵循B类的部件不采用专门安全措施。

2 出现故障时可能导致安全功能丧失。

6.2.2 1类

1类应采用B类要求和本条要求。

1类控制系统有关安全部件应采用经过验证的元件和原则来设计、制造。

有关安全应用的经过验证的元件是指：

——在类似应用场合已广泛使用过并且具有成功经验的那些元件，或

——采用经过证明对有关安全应用是适用而可靠的原则制作并经过验证的那些元件。

在有些经过验证的元件中，某些评估出的故障由于已知故障率很低，也可以不包括在内。

可根据应用场合，决定将某一特定元件认可为经过验证的元件。

注1：在只有单一电子元件水平上，通常不可能实现1类。

经过验证的安全原则的例子是：

——避免某些故障（例如通过隔离避免短路）；

——减小故障概率（例如元件的超标定或低估）；

——采用定向故障模式（例如在故障事件中除去动力是至关重要的时，采用保证开路）；

——尽早查明故障（例如早期故障检查）；

——限制故障后果。

新开发的元件和原则如果满足上述条件，它们可以考虑视为等效“经过验证的”。

注2：1类中的失效概率低于B类的，因此，安全功能丧失可能性较少。

注3：出现故障时可能导致安全功能丧失。

6.2.3 2类

应采用B类的要求和经过验证的安全原则以及本条的要求。

2类控制系统有关安全部件的安全功能应按适当的时间间隔通过机器控制系统进行检查。安全功能检查应在以下情况下进行：

——在机器起动时和在某种危险状态产生之前，和

——如果风险评价和操作类型表明有必要的话，在运行期间定期进行。

这种检查可以自动地或手动地进行。安全功能的某种检查应做到：或

——如已查明没有故障允许运行，或

——如果查明有故障，产生一个触发合适控制动作的输出。只要可能，这种输出应产生安全状态。当这种输出不可能产生安全状态时（例如执行开关装置中的触头焊合），该输出应提供危险警报。

这种检查自身应不导致危险状态。

故障查明后，安全状态应保持到故障被排除。

注

1 因为安全功能检查不可能应用于所有元件，例如压力开关或温度传感器，所以在有些情况下，2类是不适用的。

2 一般2类可以借助电子技术实现，例如在防护设备和特定控制系统中。

3 这种系统工况允许：

——一种故障出现可能导致两次检查之间安全功能丧失；

——通过检查发现安全功能的丧失。

检查设备可以与提供安全功能的有关安全部件是一个整体或者是分离的。

6.2.4 3类

应采用B类的要求和经过验证的原则以及本条的要求。

3类控制系统有关安全部件应设计得在这些部件中任何一个出现单项故障，都不会导致安全功能丧失。应考虑共因失效。只要合理可行，在有关安全功能的下一个指令发出时或在发出之前应查明单项故障。

注

1 检查单项故障的这种要求并不意味着所有故障都将查明。因此，未查明的故障积累可能导致意外输出和机器危险状态。继电器触头的持连动作或冗余电输出的监控是查明故障的实际可行措施的典型例子。

2 如果技术上和应用上需要的话，C类标准的制定者应对查明故障给出进一步详细规定。