ICS 13.110
J 09

中华人民共和国国家标准

GB/T 16855.1—2005
代替 GB/T 16855.1—1997

机械安全　控制系统有关安全部件　第1部分：设计通则

Safety of machinery—Safety-related parts of control systems—Part 1: General principles for design

(ISO 13849-1:1999, MOD)

2005-08-30 发布　　2006-04-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

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 1 部分:设计通则
GB/T 16855.1—2005
*
中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码:100045
网址 www.bzcbs.com
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2 字数 53 千字
2006 年 3 月第一版 2006 年 3 月第一次印刷
*
书号:155066·1-27076 定价 16.00 元

前　言

GB/T 16855《机械安全　控制系统有关安全部件》分为两个部分：

——第1部分：设计通则；

——第2部分：鉴定、试验、故障清单。

本部分为GB/T 16855的第1部分。

GB/T 16855的本部分修改采用国际标准ISO 13849-1:1999《机械安全　控制系统有关安全部件　第1部分：设计通则》(英文版)。

本部分根据ISO 13849-1:1999重新起草，其结构和内容与ISO 13849-1:1999一致，但按照我国标准的编写规则对国际标准做了编辑性修改。本部分与ISO 13849-1:1999的主要差异如下：

——取消了国际标准的前言；

——对国际标准的引言进行了部分修改；

——将第2章中引用的相关国际标准，已转化成我国国家标准的均直接引用相应的国家标准；

——取消了国际标准中第3.4条的注2，该注释是“fault”一词在法语和德语中的理解情况；

——取消了国际标准中表1“其他标准”一栏内ISO 60204中11章和11.3的要求规定，因对应的GB 5226.1—2002无相应内容，而本部分及GB/T 15706标准基本包含了安全功能特性的要求；

——取消了国际标准的“参考文献”中列出的第2章引用的“国际标准与参考文献和相关欧洲标准对应关系表”。

本部分代替GB/T 16855.1—1997《机械安全　控制系统有关安全部件　第1部分：设计通则》。

本部分与GB/T 16855.1—1997相比主要变化如下：

——改引言为资料性概述要素；

——第2章引用文件不同，对标题、引导语做了调整；

——术语和定义个数不同，本部分没有了GB/T 168551—1997中“3.4 控制系统可靠性”这一定义；

——表1中，有关安全功能特性的要求对应的其他标准的条目有所增加；

——第4章总则4.3做了细划，予以了条目编号；

——图1表示内容增加；

——增加了资料性补充要素参考文献。

与本部分相关的其他国家标准：GB/T 16855.100—2005《机械安全　控制系统有关安全部件　第100部分：GB/T 16855.1的应用指南》。

本标准的附录A、附录B、附录C和附录D都是资料性附录。

本部分由全国机械安全标准化技术委员会(SAC/TC 208)提出并归口。

本部分负责起草单位：机械科学研究院中机生产力促进中心。

本部分参加起草单位：长春试验机研究所、北京起重运输机械研究所、国家机床质量监督检验中心。

本部分主要起草人：石俊伟、陈建民、宁燕、李勤、聂北刚、王学智、赵春晖、赵钦志。

本部分所代替标准的历次版本发布情况：

——GB/T 16855.1—1997。

引　言

机械控制系统中的某些部件常常会被赋予安全功能，这些部件被称之为有关安全部件。这类部件可能由硬件和软件构成，并被用来提供控制系统的安全功能。它们可以是控制系统的分立部件或集成部件。

GB/T 16855 的本部分从故障发生的角度把控制系统有关安全部件的性能分为五类(B、1、2、3、4)，这些类别宜被作为参考点。从安全要求角度而言，这些类别(见 6.2)不是用来按任何给定顺序或给定层次应用的。

这些类别可用于：

——各种机械的控制系统，从简单的，例如小型炊事器具，到复杂的制造装置，例如包装机械、印刷机、压力机等；

——防护装备的控制系统，例如双手控制装置、联锁装置、电敏防护装置(如光电屏障)和压敏垫等。

类别的选择取决于机器和防护措施所采用的控制手段的作用程度。

选择类别和设计控制系统有关安全部件时，设计人员至少宜准备有关安全部件的下列资料：

——选择的类别；

——功能特性；

——在机械防护措施中起的准确作用；

——所考虑的部件的确切限制条件(见 3.1)；

——所有考虑到的与安全相关的故障；

——通过故障排查而仍未考虑到的那些与安全相关的故障以及为了排除这些故障而采取的措施；

——与可靠性有关的参数，如环境条件；

——使用的技术。

使用类别作为参考点和随之在设计过程中所做出的原理说明，是为了使 GB/T 16855 的本部分能得以灵活地运用。本部分也为诸如由第三方、机构内部或独立检测机构对控制系统(和机器)有关安全部件在任何一种应用场合下的设计和运行进行评价提供了一个明确的依据。

目　次

机械安全　控制系统有关安全部件　第1部分：设计通则

1　范围

GB/T 16855的本部分为控制系统有关安全部件的设计原则规定了安全要求和指南。本部分还规定了这些部件的类别并描述了其在安全功能方面的特性，包括用于所有机械和有关防护装置的可编程系统。

本部分适用于所有控制系统有关安全部件，无论其使用何种类型的能源，例如电力的、液压的、气动的、机械的等。本部分对在特定情况下应使用哪些安全功能和哪些类别未作具体规定。

本部分适用于所有专业和非专业用途的机械。在适当的场合，本部分也适用于在其他应用技术中使用的控制系统有关安全部件。

注：见GB/T 15706.1—1995的3.11。

2　规范性引用文件

下列文件中的条款，通过GB/T 16855的本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

GB 1251.1—1989　工作场所的险情信号　险情听觉信号（eqv ISO 7731:1986）

GB 1251.2—1996　人类工效学　险情视觉信号　一般要求、设计和检验（eqv ISO 11428:1996）

GB 1251.3—1996　人类工效学　险情和非险情　声光信号体系（eqv ISO 11429:1996）

GB 4208—1993　外壳防护等级（IP代码）（eqv IEC 529:1989）

GB 5226.1—2002　机械电气设备　第1部分：通用技术条件（IEC 60204-1:2000，IDT）

GB 16754—1997　机械安全　急停　设计原则（eqv ISO 13850:1996）

GB/T 14733.3—1993　电信术语　可靠性、可维护性和业务质量（eqv IEC 60050-191:1999）

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（eqv ISO/TR 12100-1:1992）

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（eqv ISO/TR 12100-2:1992）

GB/T 16856—1997　机械安全　风险评价的原则

GB/T 19436.1—2004　机械电气安全　电敏防护装置　第1部分：一般要求和试验（IEC 61496-1:1997，IDT）

IEC 60447:1993　人机界面（MMI）操作原则

IEC 60721-3-0:1984+A1:1987，环境条件分类　第3部分：环境参数组及其严酷程度的分类分级导言

ISO 14118　机械安全　防止意外启动

EN 292-2:1991/A1:1995　机械安全　基本概念与设计通则　第2部分：技术原则与规范

EN 614-1:1995　机械安全　工效学设计原则　第1部分：术语和通则

EN 982:1996　机械安全　流体动力系统和其元件的安全要求　液压传动装置

EN 983:1996　机械安全　流体动力系统和其元件的安全要求　气动装置

EN 999:1998　机械安全　有关人体各部位接近速度防护装置的设置

3　术语和定义

GB/T 15706.1、GB/T 14733.3 确定的以及下列术语和定义适用于 GB/T 16855 的本部分。

3.1

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

对应于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。

注：组合的控制系统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。

注：上述工况是通过部件的结构配置和(或)通过它们的可靠性形成的。

3.3

控制系统安全性　safety of control systems

根据所规定的类别控制系统有关安全部件在给定时间内执行其安全功能的能力。

3.4

故障　fault

产品呈现出不能执行所要求功能的状态，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不能执行所要求功能的情况。

注：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[1)]。

3.5

失效　failure

产品执行所要求功能能力的终止。

注 1：失效后产品具有故障。

注 2："失效"与"故障"的区别是，"失效"是一个事件，而"故障"是一种状态。

注 3：所定义的这种概念不适用于只有软件构成的产品。

[GB/T 14733.3—1993]

注 4：实际上，术语故障和失效经常按同义词使用。

3.6

控制系统安全功能　safety function of control system

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(作为一个系统)达到一种安全状态的功能。

3.7

抑制　muting

由控制系统有关安全部件对一种或几种安全功能的暂时自动中止。

3.8

手动重调　manual reset

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

1)　此术语的定义原有两个注，本部分删除了 ISO 13489-1:1990 中 3.4 的注 2(对法文和德文对应词的说明)。

4 总则

4.1 设计过程中的安全目标

设计和制作提供安全功能的控制系统有关安全部件时，应充分考虑 GB/T 16856—1997 中下列情况下的原则：

——在全部预期使用过程中和出现可预见的误用时；

——出现故障时；

——整个机器在预期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（见 GB/T 16856），判定需要由控制系统有关安全部件的每一个部件对减小风险所起的作用（见附录 B）。这种按作用分担的风险不包括受控机器的全部风险，例如不是一台机械式压力机或洗衣机的全部风险，而只是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。

主要目的是设计者应确保控制系统有关安全部件产生的输出，要达到 GB/T 16856 中规定的减小风险的目的。这不是总能达到的，在这种情况下，设计者应提出其他安全措施。减小风险对策的分布示意图见 GB/T 15706.1—1995 的第 5 章。

设计者选择有关安全部件的类别和其他性能（例如各部件的结构位置、隔离）将取决于这些部件对减小风险的作用、设计与技术（见引言）。设计者应表明：

——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）能够通过可靠性指标和耐故障结构被部分地量化。可靠性和结构两者对有关安全部件耐故障的这种能力都起作用。规定的耐故障性能够通过规定元件可靠性水平和（或）采用改进有关安全部件的结构来达到。可靠性和结构的作用能够随所用的技术而变化。例如，在一项技术中，一种高可靠性的单通道有关安全部件，用于别的技术中容许故障的可靠性较低的结构上可能会具有同样的或较高的耐故障性。

注：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（见附录 D）。例如，在一个冗余的结构中，带有相对不可靠元件的系统的安全性可能比较简单结构中但带有较高可靠性元件的系统的安全性更高。这一概念很重要，因为在某些应用场合，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，就不是考虑所达到的可靠性，而最优先需要考虑的是安全性。在这种应用场合，根据风险评价，应装备一种故障（一个周期允许的故障）检测结构，这种结构能在一次、两次或多次故障后提供所需的安全功能。

在主要是通过改进有关安全部件的结构而获得安全性的场合，本部分不要求计算复杂结构的可靠性值。对于不太复杂的结构，当元件的可靠性对安全性非常重要时，计算的可靠性值通过分担给各有关安全部件来减少全部风险是一个有用的指标。

对于风险较低的应用场合，采取一些避免故障的措施即可；对于风险较高的应用场合，通过改进控制系统有关安全部件的结构能够提出一些避免、检测或容许故障的措施。实际措施包括冗余技术、相异技术、监控（见 GB/T 15706.2—1995 中的第 3 章和 GB 5226.1—2002 中的 9.4）。

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(或构造);
——有关安全文件的质量;
——规范的完善性;
——设计、制造和维修;
——软件的质量和准确性;
——功能试验的范围;
——受控机器或机器零件的工作特性。

这些参数能被归纳到以下三类主要特征:

a) 硬件的可靠性——为避免故障的各元件可靠性水平;

b) 系统结构——为避免、容许或检测故障,对控制系统有关安全部件中各元件的配置;

c) 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

4.3.1 总则

本条规定了最初选择欲采用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。据此,依据 GB/T 16856 在对机器的风险评价过程中,能够确定出有关安全部件对减小风险所起的作用。

因为减小机器风险有多种方式,设计控制系统有关安全部件也有很多方式,所以这种过程是反复的。在程序的任何一步所做的决定和(或)假设可能影响前一步的决定和(或)假设。这方面能够通过任一步程序的反馈进行核查。在鉴定阶段这种核查是必不可少的,以确保所达到的安全性能与规范中规定的那些性能相一致。

图 1 是对该过程的说明。附录 A 中以提问题的方式给出了提示设计者在设计进程中宜考虑的一些重要问题。这些问题说明了在设计有关安全部件中宜遵循的基本原理。不是所有问题都适用于每种应用场合,在有些应用场合还需要增加一些问题。

4.3.2 第 1 步:危险分析和风险评价

遵循 GB/T 15706.1 和 GB/T 16856 的指导,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并针对那种应用场合来确定适当地减小风险。

4.3.3 第 2 步:确定通过控制手段减小风险的措施

确定减小机器风险的设计措施和(或)防护设施。作为设计措施组成部分的和(或)在安全设施的控制装置中起作用的那些控制系统的部件均应视为有关安全部件。

4.3.4 第 3 步:规定控制系统有关安全部件的安全要求

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)。表 1 中列出了选择具体安全功能时均应包括的、比较通用的安全功能和特性的参考资料来源。

规定如何满足安全功能要求和在控制系统有关安全部件中怎样选择每个零件和组件的类别(见第 6 章)。

4.3.5 第 4 步:设计

根据第 3 步形成的规范和 4.2 中的一般设计对策来设计控制系统有关安全部件。列出设计所包括的各种性能,并且要提供所达到类别的基本原理。

验证每一阶段的设计,以确保有关安全部件按所规定的安全功能和类别的相互关系完全满足先前阶段规定的要求。

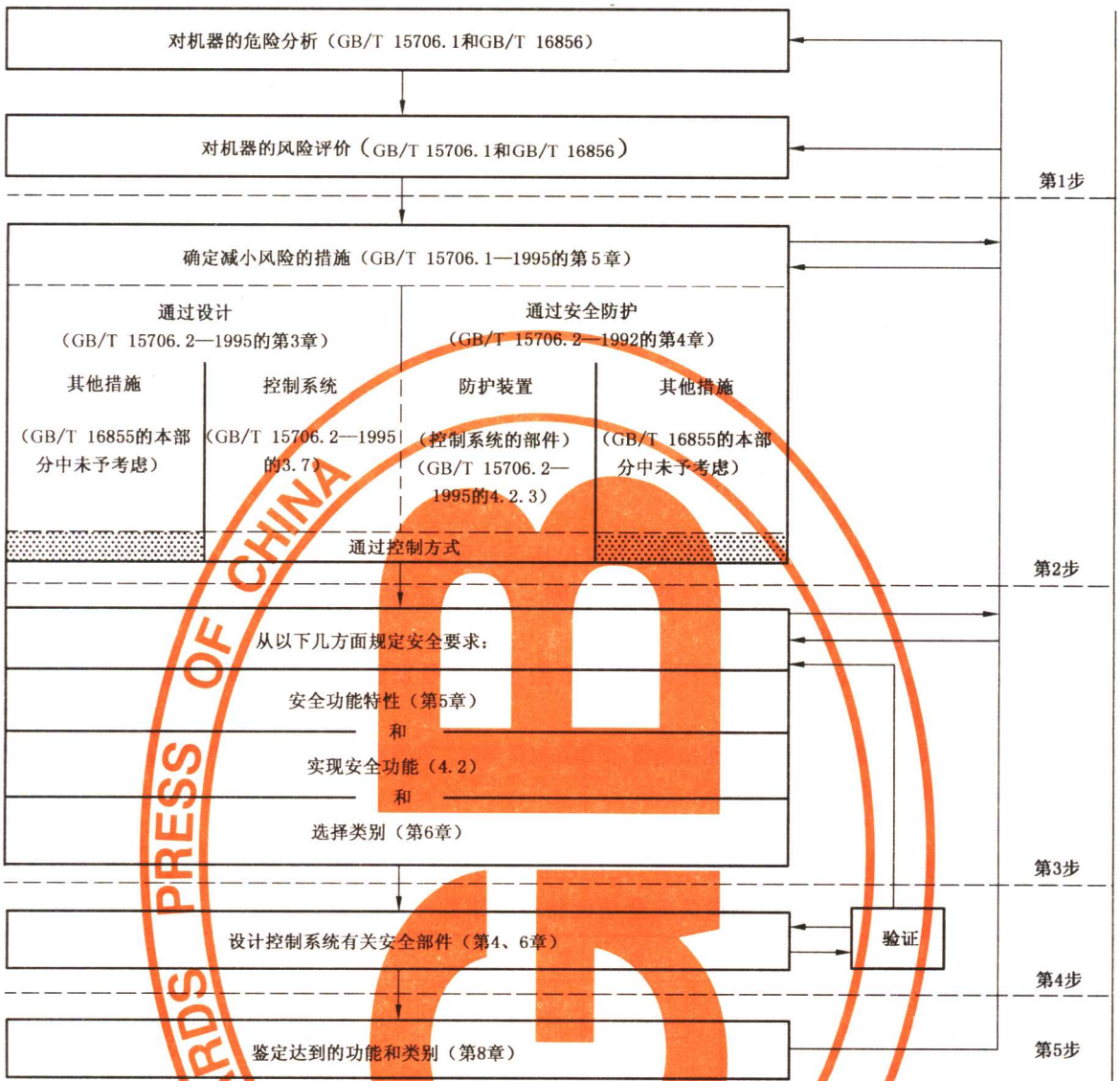

图 1　设计控制系统有关安全部件的迭代过程

4.3.6　第 5 步：鉴定

按照第 3 步的规范鉴定所达到的安全功能和类别，必要时重新设计（见第 8 章）。

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 GB/T 16855 本部分的范围，而宜由机器设计者或相应的 C 类安全标准规定。

在控制系统有关安全部件的设计中，使用可编程电子设备时，还需要其他一些详细程序（见8.4.2）。这些程序正在研发之中（见参考文献）。

注：目前认为，在由于控制系统的错误运行而能够发生重大危险的情况下，很难肯定一点地确信，能够保证对可编程电子设备的单通道器件的正确运行的信赖。在这种情况得以解决之前，单纯依靠这种单通道器件的正确运行是不可取的（依据 GB 5226.1—2002 的 11.3）。

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接口的设计和安装应使人在机器全部预定使用期间和可预见的误用时不会遭到危险（相关信息参见 GB/T 15706.2、GB 5226.1—2002 的第 10 章、IEC 60477:1993 的第 2 章、EN 614-1、EN 894-1、EN 894-2、prEN 894-3、prEN 1005-3）。

宜采用人类工效学原则设计以使机器和控制系统（包括有关安全部件）便于使用，并防止操作者以

危险的方式操作。推荐应用 GB/T 15706.2—1995 中 3.6 给出的有关遵循人类工效学原则方面的安全要求。

5 安全功能特性

5.1 概述

本章提供了控制系统有关安全部件能具有的典型安全功能(见 GB/T 15706.1—1995 的 3.13)的清单。为了实现特定应用场合控制系统所需的安全措施,设计时(或制定 C 类标准时)应包括此清单中的必要安全功能。

表 1 列出了典型安全功能和它们的一些特性并提及了在相关标准中已做出清晰描述的具体章节。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。对于某些功能特性,本章中还提出了附加的详细要求,这些附加的详细要求应包括进去。

在必要的场合,这些特性应适用于不同的动力源。

5.2 停机功能

除了表 1 中相关标准给出的各项要求外,还应包括下列要求:

a) 由防护装置触发的停机功能应在防护装置刚一动作就必须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;

b) 当一组机器以协同方式一起工作时,应采取措施将信号发送给监控器和(或)具有这样停机条件的其他机器。

注:这样停机能够引起操作问题和难于重新启动,例如在电弧焊时。有些应用场合,这种功能能与运行停机结合起来,以减少导致安全功能失效的诱因。

5.3 急停功能

除了表 1 中相关标准给出的各项要求外,还应包括下列要求:

表 1 给出有关安全功能特性要求的一些相关标准

安全功能,特性	要求					附加信息[a]
	GB/T 16855 的本部分	GB/T 15706.1—1995	GB/T 15706.2—1995	EN 292-2;1991/A1:1995 附录 A	其他标准	
术语和定义	3	3			GB 5226.1—2002,第 3 章	GB 4706.1—1998,第 2 章
一般设计对策	4.2		3	1.2.1 1.2.2 1.2.7 1.5.4	GB 5226.1—2002,9.4	GB 4706.1—1998,第 22 章 GB 11291—1997,第 5 章和第 6 章 GB 16655—1996,第 5 章
人类工效学设计原则	4.4	4.9	3.6 3.7.8a	1.2.2 第 1 段	GB 5226.1—2002,第 10 章	GB 11291—1997,6.2 GB 16655—1996,4.6
停机功能	5.2		3.7.1 3.7.8b	1.2.4 1.3.5	GB 5226.1—2002,9.2.2、9.2.5.3	GB 4706.1—1998,7.12 GB 16655—1996,5.11

表 1（续）

安全功能，特性	要求					附加信息[a]
	GB/T 16855 的本部分	GB/T 15706.1—1995	GB/T 15706.2—1995	EN 292-2:1991/A1:1995 附录 A	其他标准	
急停功能	5.3		6.1.1	1.2.4	GB 16754，GB 5226.1—2002，9.2.5.4	GB 11291—1997，6.4.2、7.2.5 GB 16655—1996，5.11.2
手动重调	5.4			1.2.4	GB 5226.1—2002，9.2.5.3、9.2.5.4	GB 11291—1997，6.4.2、6.4.3、7.6；GB 16655—1996，6.4.3
启动和重新启动	5.5		3.7.1 3.7.2	1.2.3 1.3.5	GB 5226.1—2002，9.2.1、9.2.5.1、9.2.5.2、9.2.6	GB 11291—1997，6.10、7.2.5、7.3.1、9.3.4
响应时间	5.6				EN 999：1998，3.2、A.3、A.4	
有关安全参数	5.7		3.7.9e		GB 5226.1—2002，7.1、9.3.2、9.3.4	GB 11291—1997，4.2 GB 4706.1—1998，11.8
局部控制功能	5.8		3.7.9 3.7.10			GB 11291—1997，3.2.9、7.2.6 GB 16655—1996，3.13、4.5、5.9、6.2
抑制	5.9					
安全功能的手动暂停	5.10		3.7.10 4.1.4	1.2.5	GB 5226.1—2002，9.2.4	GB 11291—1997，6.10 GB 16655—1996，5.8
动力源的波动、损耗和复原	5.11		3.7.8e	1.2.6 1.5.3	GB 5226.1—2002，4.3、7.1、7.5	
可编程电子系统			3.7.7		GB 5226.1—2002，11.3	IEC 61508[b]
意外启动			3.7.2	1.2.3 1.2.6 1.2.7	ISO 14118 GB 5226.1—2002，5.4	

表 1（续）

安全功能，特性	要求					附加信息[a]
	GB/T 16855 的本部分	GB/T 15706.1—1995	GB/T 15706.2—1995	EN 292-2:1991/A1:1995 附录 A	其他标准	
指示和报警			3.6.7 5.3	1.2.2 第 4、6 段 1.7.0 1.7.1	GB 1251.1 GB 1251.2 GB 1251.3 GB 5226.1—2002，10.4 IEC 60447	GB 16655—1996，5.6
受困人员的逃离和营救			6.1.2	1.2.2 第 5、6 段		
电气设备		3.9		1.5.1 1.5.7	GB 5226.1—2002	
电源				1.5.1	GB 5226.1—2002，4.3	
其他动力源				1.5.3	EN 982:1992，5.1.4 EN 983:1992，5.1.4	
盖和围栏					GB 5226.1—2002，12.4 GB 4208—1993	
气动和液压装置			3.8	1.5.3	EN 982 EN 983	
隔离和能量耗散			6.2.2	1.6.3	ISO 14118 GB 5226.1—2002，5.3、6.3.1	
实际环境和运行条件			3.7.11		GB 5226.1—2002，4.4	GB 11291—1997，6.9；GB 16655—1996，4.3、4.5
控制模式和模式选择			3.7.9 3.7.10	1.2.5	GB 5226.1—2002，9.2.3	GB 11291—1997，6.10
接口和（或）连接				1.5.4 1.6.1 第 3 段	GB 5226.1—2002，9.1.4、14.4	

表 1（续）

安全功能，特性	要求					附加信息[a]
	GB/T 16855 的本部分	GB/T 15706.1—1995	GB/T 15706.2—1995	EN 292-2:1991/A1:1995 附录 A	其他标准	
不同控制系统有关安全部件之间的相互关联			3.7.8e		GB 5226.1—2002，9.3.4	
人机界面			3.6.6 3.6.7	1.2.2	GB 5226.1—2002，第 10 章 IEC 60447	
a 本栏目中列出的标准仅供设计者参考，而不属于 GB /T 16855 本部分所要求的内容。 b 即将发布。						

除了表 1 中相关标准给出的各项要求外，还应包括下列要求：

a) 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状态信号发送给协同系统的各个部分的装置；

b) 在协同系统的一些部分是通过，诸如防护装置或实际位置明显分离的场合，不需要总是对整个系统采用急停，而只是对通过风险评价鉴别为特定的部分采用急停；

c) 对危险的部分急停生效后，该部分与其他部分的接口处不应存在危险。

5.4 手动重调

除了表 1 中相关标准给出的各项要求外，还应包括下列要求：

a) 在防护装置启动了停机指令之后，停机状态应保持到开动了手动重调装置且已具备重新启动的安全条件时为止；

b) 通过重调防护装置，解除了停机指令，再重新恢复安全功能。如果通过风险评价指出来的话，则这种停机指令的解除只有通过手动、独立和慎重的操作（手动重调）才应有效；

c) 手动重调功能应：

——通过控制系统有关安全部件内的一个独立的手动操纵装置提供；

——仅在所有安全功能和防护装置处于运行状态才能实现，如果不可能做到这一点，重调功能就不能实现；

——由其自身不能引发运动或产生危险状态；

——动作准确；

——使控制系统为接受单独的启动指令做好准备；

——只允许操纵器在其释放的位置（OFF）启动。

d) 应选择好具有手动重调功能的有关安全部件的类别以使所包含的手动重调功能不至于削弱相关安全功能的安全要求；

e) 重调操纵器应安装在危险区外边的并具有良好观察条件的安全位置，以便检查是否有人处在危险区内。

5.5 启动和重新启动

除了表 1 中相关标准给出的各项要求外，还应包括下列要求：

a) 只有在危险状态不能存在的情况下，重新启动才应自动地进行。对于控制防护装置，详见 GB/T 15706.2—1995 中 4.2.2.5；

b) 启动和重新启动的这些要求也应适用于能够遥控的那些机器。

5.6 响应时间

除了表1中相关标准给出的要求外，还应包括下列要求：

当控制系统有关安全部件的风险评价表明对此需要时，设计者或供应方应说明响应时间（见第10章）。

注：控制系统的响应时间是机器全部响应时间的一部分。机器所需要的全部响应时间能够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中相关标准给出的各项要求外，还应包括下列要求：

a) 当有关安全的参数（例如位置、速度、温度、压力）偏离预置的限值，控制系统应起用适当措施，例如，启动停机功能、发出报警信号、警报器；

b) 如果在可编程电子系统中有关安全的数据的手工输入差错能导致危险状态，则在有关安全控制系统内应提供数据检查系统，例如检查各种限值、格式化和（或）逻辑输入值。

5.8 局部控制功能

当机器通过诸如携带式控制装置或悬吊式操纵台进行局部控制时，除了表1中相关标准给出的各项要求外，还应包括下列要求：

a) 选用的局部控制装置应位于危险区之外；

b) 从局部控制区的外边应不可能引发危险状态；

c) 局部和外部控制之间的切换（例如遥控）不应产生危险状态。

5.9 抑制

抑制不应导致任何人面临危险状态。

抑制期间安全条件应由其他方式提供。

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类别的选择应使包含的抑制功能不削弱对有关安全功能所要求的安全性。

在有些应用场合需要一个指示抑制的信号。

5.10 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中相关标准给出的要求外，还应包括下列要求：

a) 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；

b) 在（机器）能够继续正常运行之前，应恢复控制系统有关安全部件的安全功能；

c) 选择担负手动暂停的控制系统有关安全部件时，应充分考虑GB/T 16856规定的原则。

在有些应用场合需要一个指示手动暂停的信号。

5.11 动力源的波动、损耗和复原

除表1中相关标准给出的要求外，还应包括下列要求：

当发生能级波动超出设计的运行范围以外时，包括能源损耗，控制系统有关安全部件应持续提供或激发能使机器系统其他部件保持安全状态的输出信号。

6 类别

6.1 概述

控制系统有关安全部件应符合6.2中规定的五种类别中的一类或几类的要求。就安全要求而言，这些类别不预备按照任何给定的顺序或给定的层次应用。

根据4.2中阐述的对策，类别表明对控制系统有关安全部件在其耐故障方面所要求的工况。

B类是基本类。当出现故障时，能导致安全功能的丧失。在1类中主要是通过选择和应用合适的元件来实现改进耐故障的能力。在2、3、4类中对提高规定安全功能方面的性能主要是通过改进控制系统有关安全部件的结构来实现。这在2类中，是通过定期检查正在被执行的规定安全功能来实现，而在3类和4类中，是通过保证单一故障不会导致安全功能的丧失达到的。在4类中和在3类中，只要合理可行的，这类故障就会被检测到，在4类中，并要规定承受故障累积的能力。

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(见4.2)变化时才能进行。编号数字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，才能被理解为具有更高的耐故障性。

表2给出了控制系统有关安全部件的各个类别、要求和在故障情况下系统工况的一览表。

当考虑某些元件失效原因时，有些故障可能不予考虑(见第7章)。

表2 类别要求的摘要

(完整的要求见第6章)

类别[a]	要求摘要	系统工况[b]	实现安全的原则
B (见6.2.1)	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相关标准进行设计、构造、选择、装配和组合，以使其能承受预期的影响	发生故障能导致安全功能的丧失	主要以选用元件为特征
1 (见6.2.2)	应采用B类的要求。 应使用经过多次验证的元件和经过多次验证的安全原则	发生故障能导致安全功能的丧失，但发生的概率低于B类时的概率	
2 (见6.2.3)	应采用B类要求和经过多次验证的安全原则。 应通过机器控制系统以适当的时间间隔检查安全功能	——在两次检查之间发生故障能导致安全功能的丧失； ——通过检查来检测安全功能的丧失	主要以结构为特征
3 (见6.2.4)	应采用B类要求和经过多次验证的安全原则。 有关安全部件的设计应使： ——在这些部件中的任何一个部件的单一故障都不导致安全功能的丧失； ——在任何合理可行的情况下都可检测到单一故障	——在发生单一故障时，安全功能始终在执行； ——有些而非全部故障会被检测到； ——未发现的故障累积能导致安全功能的丧失	
4 (见6.2.5)	应采用B类要求和经过多次验证的安全原则。 有关安全部件的设计应使： ——在这些部件中的任何一个部件的单一故障都不导致安全功能的丧失； ——在下一个有关安全功能指令发出时或发出前检测到单一故障。如果不可能，则故障累积不应导致安全功能的丧失	——在发生故障时，安全功能始终在执行。 ——故障会被及时检测到，以防安全功能的丧失	

a 类别在安全要求方面不预备按任何给定的顺序或给定的层次使用。

b 风险评价要指明由故障引起的总体或部分安全功能的丧失是否可接受。