ICS 13.110
J 09

中华人民共和国国家标准

GB/T 16855.1—2008/ISO 13849-1:2006
代替 GB/T 16855.1—2005

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 13849-1:2006,IDT)

2008-08-25 发布　　2009-04-01 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

目　　次

前　言

GB/T 16855《机械安全　控制系统有关安全部件》由以下3部分组成：

——第1部分：设计通则；

——第2部分：确认；

——第100部分：GB/T 16855.1的应用指南。

本部分是GB/T 16855的第1部分。

本部分等同采用ISO 13849-1:2006《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)。

本部分等同翻译ISO 13849-1:2006。为便于使用，本部分做了下列编辑性修改：

——删除了国际标准的前言并按照我国标准的要求重新起草了前言；

——用“本部分”代替“ISO 13849的本部分”；

——用小数点“.”代替作为小数点的逗号“,”；

——修改了规范性引用文件的导语；

——对ISO 13849-1:2006引用的其他标准中，用已被等同采用为我国的标准代替对应的国际标准，未被等同采用为我国标准的直接引用国际标准。

本部分代替GB/T 16855.1—2005。与GB/T 16855.1—2005相比，主要内容修改如下：

——增加了术语：性能等级(PL)、所需的性能等级(PL_r)、诊断覆盖率(DC)、平均危险失效时间($MTTF_d$)、危险失效、共因失效、系统失效、伤害、危险、危险状态、风险、遗留风险、风险评价、风险分析、风险评定、机器的预定使用、可预见的误用、安全功能、监测、可编程电子系统、保护措施、任务时间、检测频率、要求频率、维修率、机器控制系统、安全完整性等级、有限可变语言、全可变语言、应用软件、嵌入式系统；

——删除了术语：控制系统安全性、控制系统安全功能；

——第4章中增加了确定所需的性能等级(4.3)、所达到的性能等级(PL)的估计及其与SIL的关系(4.5)、软件的安全要求(4.6)和检验所达到的PL是否满足PL_r的要求(4.7)；

——第6章内容增加了类别与DC_{avg}、CCF和每个通道$MTTF_d$的关系；

——将原标准中的第10章细分为技术文件(第10章)和使用信息(第11章)两章；

——修改了附录A、附录B、附录C和附录D，并增加了附录E、附录F、附录G、附录H、附录I、附录J和附录K。

本部分的所有附录均为资料性附录。

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。

本部分起草单位：机械科学研究总院中机生产力促进中心。

本部分主要起草人：张晓飞、李勤、宁燕、富锐、付大为、张维、杨岭、盛晓敏、程红兵。

本部分所代替标准的历次版本发布情况为：

——GB/T 16855.1—1997、GB/T 16855.1—2005。

引　言

机械安全标准的结构如下：

a) A类标准(基础安全标准)，给出适用于所有机械的基本概念、设计原则和一般特征。

b) B类标准(通用安全标准)，涉及机械的一种安全特征或使用范围较宽的一类安全防护装置：

——B1类，特定的安全特征(如安全距离、表面温度、噪声等)标准；

——B2类，安全装置(如双手操纵装置、联锁装置、压敏装置、防护装置)标准。

c) C类标准(机器安全标准)，对一种特定的机器或一组机器规定出详细的安全要求的标准。

依照GB/T 15706.1中的规定，本部分属于通用安全标准(B1类)。

对于按照C类标准设计和制造的机器，当C类标准中的条款与A类或B类标准中所述的条款不一致时，优先采用C类标准。

本部分的目的是在控制系统的设计和评价中给出对所涉及的控制系统的指南，并为正在准备制定希望符合欧盟指令98/37/EC《机械指令》附录Ⅰ“基本安全要求”的B2类或C类标准的各技术委员会(TC)提供指南。本部分不对符合其他欧盟指令给出具体指南。

作为机器全面风险减小策略的一部分，设计者通常愿意通过应用具有一种或多种安全功能的防护装置来达到某种程度的风险减小。

用于提供安全功能的机器控制系统部件称为控制系统有关安全部件(SRP/CS)，它们由硬件和软件组成，既可独立于机器控制系统，也可是与机器控制系统的组成部分。除了提供安全功能以外，SRP/CS也能提供操作功能(例如：双手操纵装置作为过程启动的一种手段)。

控制系统有关安全部件在预期条件下执行安全功能的能力分为5级，称之为性能等级(PL)。这些性能等级由每小时发生危险失效的概率来定义(见表3)。

安全功能危险失效的概率取决于几个因素，包括：软硬件结构、故障检测装置的范围[诊断覆盖率(DC)]、部件的可靠性[平均危险失效时间($MTTF_d$)、共因失效(CCF)]、设计流程、工作压力、环境条件和操作程序等。

为了帮助设计者对所达到的PL容易进行评价，本部分采用了根据故障条件下具体设计准则和具体行为来进行结构分类的方法。这些类别分为5类，称之为B类、1类、2类、3类和4类。

性能等级和类别适用于如下控制系统有关安全部件，例如：

——保护装置(例如：双手操纵装置、联锁装置)、电敏保护装置(例如：光栅)、压敏装置；

——控制单元(例如：控制功能、数据处理、监测等的逻辑单元)；

——动力控制元件(例如：继电器、阀门等)。

以及所有机械上执行安全功能的控制系统——从简单装置(例如：小型厨房炊机具或自动门等)到复杂制造业设备(例如：包装机械、印刷机械、压力机等)。

本部分的目的是提供明确的基础用以评价应用SRP/CS(以及机器)的设计和性能，例如：第三方评价、自我评价或独立实验室评价。

应用IEC 62061和本部分时推荐的信息

IEC 62061和本部分规定了设计和执行机器控制系统有关安全部件的要求。根据这两个标准的范围，采用其中任何一个标准都可假定满足了相关的基本安全要求。表1概括了IEC 62061和本部分的范围。

表 1　IEC 62061 和本部分的应用推荐

	执行有关安全控制功能的技术	GB/T 16855.1	IEC 62061
A	非电，例如：液压	X	没有包括
B	机电，例如：继电器和(或)简单电子器件	限制在指定结构[a] 内且最大为 PL＝e	所有结构，最大为 SIL3
C	复杂电子器件，例如：可编程的	限制在指定结构[a] 内且最大为 PL＝d	所有结构最大为 SIL3
D	A 与 B 组合	限制在指定结构[a] 内且最大为 PL＝e	X[c]
E	C 与 B 组合	限制在指定结构内且最大为 PL＝d	所有结构最大为 SIL3
F	C 与 A 组合，或 C 与 A、B 组合	X[b]	X[c]
X　表示此项由该栏标题中所示的标准处理。			

[a] 指定结构在 6.2 中规定，目的是给出量化性能等级的简单方法。

[b] 对于复杂电子器件：采用按照本部分的指定结构，且最大为 PL＝d，或者 IEC 62061 中的任意结构。

[c] 对于非电技术，采用本部分中的部件作为子系统。

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

本部分提供了包括软件设计在内的控制系统有关安全部件(SRP/CS)设计和集成的安全要求和指导原则。对于这些SRP/CS的部件,本部分规定了包括执行安全功能所需的性能等级在内的特征。本部分适用于所有种类机械的SRP/CS,不管其采用的何种技术和能量(电、液压、气动、机械等)。

本部分未规定特殊应用中的安全功能或性能等级。

本部分提供了采用可编程电子系统的SRP/CS的具体要求。

本部分未提供设计SRP/CS的部件的具体要求。然而,可使用已给出的原则,例如:类别或性能等级。

注1:SRP/CS的部件示例:继电器、电磁阀、位置开关、PLC、电动机控制单元、双手操纵装置、压敏设备等。对于这些产品的设计,重要的是要参考特别适用的标准,例如:GB/T 19671、GB/T 17454.1和GB/T 17454.2。

注2:所需的性能等级的定义见3.1.24。

注3:本部分提供的关于可编程电子系统的要求与IEC 62061中给出的设计和开发机械有关安全的电气、电子和可编程控制系统的方法原理是一致的。

注4:对于PL_r=e的嵌入软件中的有关安全部件见GB/T 20438.3—2007中的第7章。

注5:也可见表1。

2　规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。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/T 15706.1—2007　机械安全　基本概念与设计通则　第1部分:基本术语和方法(ISO 12100-1:2003,IDT)

GB/T 15706.2—2007　机械安全　基本概念与设计通则　第2部分:技术原则(ISO 12100-1:2003,IDT)

GB/T 16855.2—2007　机械安全　控制系统有关安全部件　第2部分:确认(ISO 13849-2:2003,IDT)

GB/T 16856.1—2008　机械安全　风险评价　第1部分:原则(ISO 14121-1:2007,IDT)

GB/T 20438.3—2006　电气/电子/可编程电子安全相关系统的功能安全　第3部分:软件要求(IEC 61508-3:1998,IDT)

GB/T 20438.4—2006　电气/电子/可编程电子安全相关系统的功能安全　第4部分:定义和缩略语(IEC 61508-4:1998,IDT)

IEC 60050-191:1990　国际电工词汇　第191章:可靠性与业务质量

3　术语、定义、符号和缩写

3.1　术语和定义

GB/T 15706.1—2007、IEC 60050-191:1990确立的以及下列术语和定义适用于本部分。