ICS 13.110
J 09

中华人民共和国国家标准

GB/T 16855.1—2018/ISO 13849-1:2015
代替 GB/T 16855.1—2008

机械安全　控制系统安全相关部件 第1部分:设计通则

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

(ISO 13849-1:2015,IDT)

2018-12-28 发布　　2019-07-01 实施

国家市场监督管理总局
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　控制系统安全相关部件》由以下两部分组成：

——第1部分：设计通则；

——第2部分：确认。

本部分为GB/T 16855的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GB/T 16855.1—2008《机械安全　控制系统有关安全部件　第1部分：设计通则》。与GB/T 16855.1—2008相比，除编辑性修改外主要技术变化如下：

——将标准名称修改为《机械安全　控制系统安全相关部件　第1部分：设计通则》；

——删除了引言中的表1(见2008年版的引言)；

——将术语“系统失效”修改为“系统性失效”(见3.1.7，2008年版的3.1.7)；

——将术语“平均危险失效时间”修改为“平均危险失效间隔时间”，并将其缩略语修改为“$MTTF_D$”(见3.1.25，2008年版的3.1.25)；

——增加了术语“高要求或连续模式”“经使用证明”及其定义(见3.1.38和3.1.39)；

——修改了图1(见图1，2008年版的图1)；

——增加了SRP/CS输出部分按类别描述的要求(见4.5.5)；

——修改了对单个元件$MTTF_D$值的计算或估计(见附录C，2008年版的附录C)；

——重新起草了附录I(见附录I，2008年版的附录I)。

本部分使用翻译法等同采用ISO 13849-1:2015《机械安全　控制系统安全相关部件　第1部分：设计通则》。

与本部分中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB 28526—2012　机械电气安全　安全相关电气、电子和可编程电子控制系统的功能安全(IEC 62061:2005，IDT)；

——GB/T 30175—2013　机械安全　应用GB/T 16855.1和GB 28526设计安全相关控制系统的指南(ISO/TR 23849:2010，IDT)。

本部分做了以下编辑性修改：

——修改了表1中的编辑性错误，“表3”改为“表2”，“表4”改为“表3”，“表7”改为“表6”。

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：皮尔磁电子(常州)有限公司、中机生产力促进中心、安徽乐库智能停车设备有限公司、苏州安高智能安全科技有限公司、厦门日拓电器科技有限公司、南安市中机标准化研究院有限公司、福建省闽旋科技股份有限公司、软控股份有限公司、中国软件评测中心、安士能(上海)机电商贸有限公司、华测检测认证集团股份有限公司、南京理工大学、西安旭迈智能家电科技有限公司、南京林业大学/机电产品包装生物质材料国家与地方联合工程研究中心、南安市质量计量检测所、立宏安全设备工程(上海)有限公司、浙江雷鸟供应链管理有限公司。

本部分主要起草人：张晓飞、黄之炯、李勤、朱斌、孙振超、李立言、赵阳阳、王宝珍、于明进、刘发旺、陆晓光、郭永振、刘攀超、居里锴、程红兵、白洪海、居荣华、吉坤、侯红英、黄东升、尹之尧、付卉青、刘英、陈卓贤、李忠、刘治永、宋小宁、李亚莉、周爱萍。

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、GB/T 16855.1—2008。

引　言

机械领域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装置：

——B1类，特定的安全特征(如安全距离、表面温度、噪声)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(机械产品安全标准)，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中的规定，本部分属于B类标准。

本部分尤其与下列与机械安全有关的利益相关方有关：

——机器制造商；

——健康与安全机构。

其他受到机械安全水平影响的利益相关方有：

——机器使用人员；

——机器所有者；

——服务提供人员；

——消费者(针对预定由消费者使用的机械)。

上述利益相关方均有可能参与本部分的起草。

此外，本部分预定用于起草C类标准的标准化机构。

本部分规定的要求可由C类标准补充或修改。

对于在C类标准的范围内，且已按照C类标准设计和制造的机器，优先采用C类标准中的要求。

本部分的目的是在控制系统的设计和评估中给出对所涉及的控制系统的指南，并为制修订B类或C类标准提供指南。作为机器全面风险减小策略的一部分，设计者一般愿意通过采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安全相关部件(SRP/CS)，它们由硬件和软件组成，既可独立于机器控制系统，也可以是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)。

控制系统安全相关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2)。

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、故障检测机制的范围[诊断覆盖率(DC)]、部件的可靠性[平均危险失效间隔时间($MTTF_D$)、共因失效(CCF)]、设计流程、运行负荷、环境条件和操作程序等。

为了便于设计者对所达到的PL进行评估，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：类别B、类别1、类别2、类别3、类别4。

性能等级和类别适用于如下控制系统安全相关部件，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、监控等的逻辑单元)；

——动力控制元件(例如：继电器、阀等)；

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。

关于 IEC 62061 和本部分推荐应用的信息

IEC 62061 和本部分都规定了机器控制系统安全相关部件的设计和实施要求。按照这两项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。ISO/TR 23849 为机器安全相关控制系统设计中应用 IEC 62061 和本部分标准提供了指导。

机械安全　控制系统安全相关部件 第1部分:设计通则

1　范围

GB/T 16855的本部分规定了包括软件设计在内的控制系统安全相关部件(SRP/CS)设计和集成的安全要求和指导原则。本部分规定了这些SRP/CS部件的特征,包括执行安全功能所需要的性能等级。本部分适用于所有种类机械上具有高要求和连续模式的SRP/CS,不管其采用何种技术和能量(电气、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。

本部分给出了采用可编程电子系统的SRP/CS的具体要求。

本部分未给出SRP/CS的产品的具体设计要求,但可采用给出的类别或性能等级等原则。

注1:SRP/CS的产品示例:继电器、电磁阀、位置开关、PLC、电机控制单元、双手操纵装置、压敏设备等。这类产品的设计需参考专门的标准,例如:GB/T 19671、GB/T 17454.1和GB/T 17454.2。

注2:所需性能等级的定义见3.1.24。

注3:本部分给出的关于可编程电子系统的要求与IEC 62061中给出的机械安全相关的电气、电子和可编程控制系统的设计和开发方法是一致的。

注4:用于PL_r=e的元件的安全相关嵌入式软件见IEC 61508-3:1998中第7章。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 2900.13—2008　电工术语　可信性与服务质量[IEC 60050(191):1990,IDT]

GB/T 15706—2012　机械安全　设计通则　风险评估与风险减小(ISO 12100:2010,IDT)

GB/T 16855.2—2015　机械安全　控制系统安全相关部件　第2部分:确认(ISO 13849-2:2012,IDT)

GB/T 20438.3—2017　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 61508-3:2010,IDT)

GB/T 20438.4—2017　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 61508-4:2010,IDT)

ISO/TR 22100-2:2013　Safety of machinery—Relationship with ISO 12100—Part 2:How ISO 12100 relates to ISO 13849-1

ISO/TR 23849　应用ISO 13849-1和IEC 62061设计机械的安全相关控制系统的指南(Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery)

IEC 62061:2012　机械安全　安全相关电气、电子和可编程电子控制系统的功能安全(Safety of machinery—Functional safety of safety-related electrical,electronic and programmable electronic control systems)