ICS 13.110
CCS J 09

# 中华人民共和国国家标准

GB/T 16855.1—2025/ISO 13849-1:2023
代替 GB/T 16855.1—2018

# 机械安全　安全控制系统
# 第1部分:设计通则

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

（ISO 13849-1:2023,IDT）

2025-08-29 发布　　2025-08-29 实施

国家市场监督管理总局
国家标准化管理委员会　发布

# 目　　次

# 前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分:标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 16855《机械安全　安全控制系统》的第1部分。GB/T 16855已经发布了以下部分:

——第1部分:设计通则;

——第2部分:确认。

本文件代替GB/T 16855.1—2018《机械安全　控制系统安全相关部件　第1部分:设计通则》。与GB/T 16855.1—2018相比,除结构调整和编辑性改动外,主要技术变化如下:

——将术语“控制系统安全相关部件”更改为“安全控制系统”,并更改了其定义(见3.1.1,2018年版的3.1.1);

——增加了术语“安全要求规范”及其定义(见3.1.3);

——更改了术语“类别”的定义(见3.1.4,2018年版的3.1.2);

——增加了术语“故障排除”和“永久故障”及其定义(见3.1.9和3.1.11);

——将术语“抑制”更改为“默停”(见3.1.15,2018年版的3.1.8);

——增加了首选术语“风险减小措施”(见3.1.22,2018年版的3.1.27);

——增加了术语“子功能”“交叉监控”“平均失效间隔时间”和“危险失效比”及其定义(见3.1.28、3.1.30、3.1.33、3.1.34);

——将术语“要求率”更改为“需求率”(见3.1.38,2018年版的3.1.30);

——将术语“应用软件”更改为“安全相关应用软件”(见3.1.41,2018年版的3.1.36);

——将术语“嵌入式软件”更改为“安全相关嵌入式软件”(见3.1.42,2018年版的3.1.37);

——将术语“高要求或连续模式”更改为“高需求或连续模式”(见3.1.43,2018年版的3.1.38);

——增加了术语“低需求模式”“子系统”“子系统组件”“通道”“操作模式”“经验证的安全原则”“经验证的元件”“动态测试”“真实性检查”“验证”“确认”“熟练人员”“黑盒”“灰盒”和“每小时危险失效平均频率”及其定义(见3.1.44～3.1.58);

——删除了术语“手动复位”“维修率”和“经使用证明”及其定义(见2018年版的3.1.9、3.1.31和3.1.39);

——增加了总体要求(见第4章);

——更改了安全功能规范(见第5章,2018年版的5.1);

——更改了设计考虑(见第6章,2018年版的第4章);

——删除了类别及其与$DC_{avg}$、CCF和每个通道$MTTF_D$的关系并将技术内容整合到设计考虑中(见第6章,2018年版的第6章);

——增加了软件安全要求(见第7章);

——更改了实现的性能等级的验证要求(见第8章,2018年版的4.7);

——更改了人类工效学方面的设计要求(见第9章,2018年版的4.8);

——更改了确认的要求(见第10章,2018年版的第8章)。

本文件等同采用ISO 13849-1:2023《机械安全　安全控制系统　第1部分:设计通则》。

本文件做了下列最小限度的编辑性改动:

——将10.6.5第一列项中的“7.2”改为“6.2”。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国机械安全标准化技术委员会(SAC/TC 208)提出并归口。

本文件起草单位:皮尔磁电子(常州)有限公司、中机研标准技术研究院(北京)有限公司、上海辰竹仪表有限公司、立宏安全设备工程(上海)有限公司、莱茵技术—商检(青岛)有限公司、深圳市湾测技术有限公司、贝博华自动化(南京)有限公司、骑鲸瞰海(杭州)科技有限公司、济宁科力光电产业有限责任公司、山东莱恩光电科技股份有限公司、宁波纬诚科技股份有限公司、安士能电器(上海)有限公司、施迈赛工业开关制造(上海)有限公司、南京理工大学、苏州市质量和标准化院、深圳市意普兴科技有限公司、沃德检测(广东)有限公司、奥煌检测技术服务(上海)有限公司、南京优倍电气技术有限公司、泰瑞机器股份有限公司、深圳市多恩技术有限公司、岚图汽车科技有限公司、西门子(中国)有限公司、南京林业大学、四川蜀兴优创安全科技有限公司、济南铸锻所检验检测科技有限公司、格睿安(重庆)工业技术有限公司、斯凯孚(中国)有限公司、特斯拉(上海)有限公司、威凯检测技术有限公司、乐高玩具制造(嘉兴)有限公司、华中师范大学、中铁建大桥工程局集团电气化工程有限公司、东莞市三信精密机械有限公司、湖北高农科技股份有限公司、江苏中睿安全科技发展有限公司、北京控制工程研究所、南通维尔斯机械科技有限公司、中铁建大桥工程局集团建筑装配科技有限公司、深圳市睿达科技有限公司、武汉普迪真空科技有限公司、东莞市固达机械制造有限公司、南京轻机包装机械有限公司、南安市中机标准化研究院有限公司。

本文件主要起草人:徐凯、黄之炯、周婷、李立言、曹永梅、孟昭瑞、陈卓贤、许一、王振伟、邵光存、尹之尧、李海明、胡进芳、陆晓光、何俊、居里锴、李彦涛、戴闻杰、刘晓英、刘明汉、黄飞、王林、魏建鸿、于恒、陈国良、李佳、居荣华、秦培均、卢军、殷高俊、董行、刘志隆、钟锦铭、徐文超、周潮亮、曹高辉、姚天金、高雪刚、尤小阳、戴骁蒙、马荣胜、史传明、褚卫中、刘治永、张硕、孙帅华、陈能玉、朱斌、陈小全、谢炳勋、凌益民、张合庆、姜涛、周成、赵晓东、张传甲、杨景隆、傅燕敏、张晓飞、马艳、郑华婷、周焱文。

本文件于1997年首次发布,2005年第一次修订,2008年第二次修订,2018年第三次修订,本次为第四次修订。

# 引　言

机械领域安全标准体系由以下几类标准构成。

——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 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 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。

根据 GB/T 15706—2012,本文件属于 B1 类标准。

本文件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,本文件预定用于起草 C 类标准的标准化机构。

本文件规定的要求可由 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。

注 1:本文件的主要内容和示例绝大部分都是针对工厂内的固定式机器,但本文件并没有排除其他机器。本文件没有考虑某些机械(如移动式机械)是否有特殊要求,但本文件尽可能做到适用于跨行业使用,且作为 C 类标准制修订的基础。

安全控制系统是机器控制系统中执行安全功能的部分。GB/T 16855 旨在明确安全控制系统各项关键指标的要求,确保机器的安全功能,进而保障人员的安全,拟由两个部分构成。

——第 1 部分:设计通则。目的在于指导安全控制系统的设计,以及为 B2 或 C 类标准的制修订提供指导。

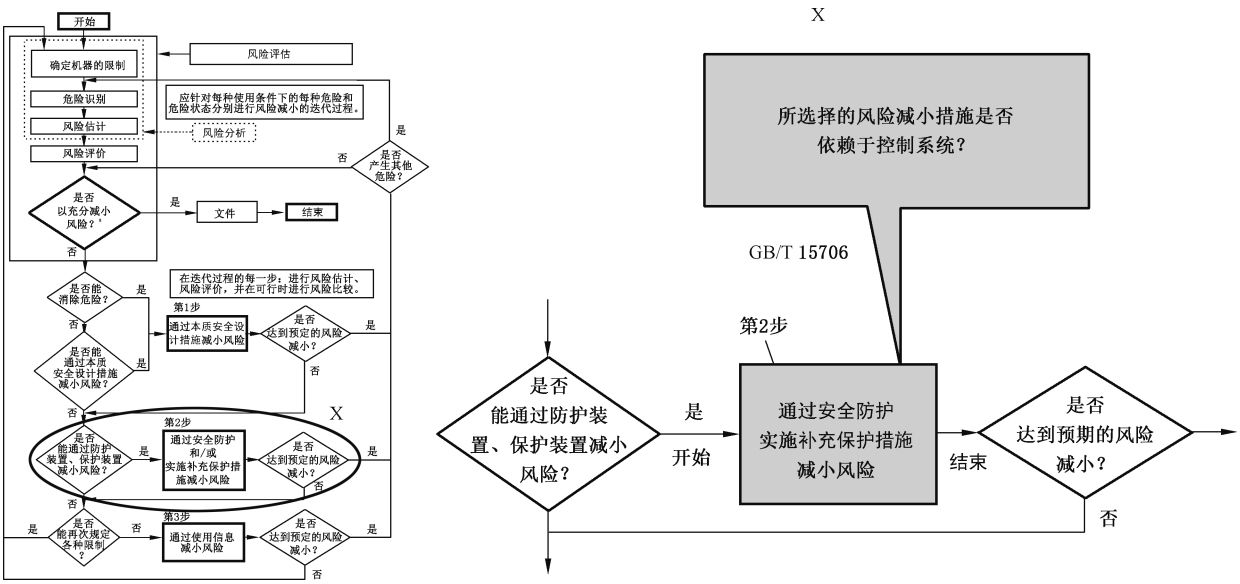
——第 2 部分:确认。目的在于指导安全控制系统的评估与验证。

按本质安全设计措施、安全防护和/或补充风险减小措施、使用信息的顺序采取风险减小措施,实现符合 GB/T 15706—2012 中的风险减小。设计者能够通过具备安全功能的风险减小措施减小风险。机器控制系统中分配用于提供安全功能的那一部分称之为安全控制系统(SRP/CS)。安全控制系统由硬件或硬件和软件的组合构成,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。除了实现安全功能以外,SRP/CS 也能实现操作功能。

GB/T 15706—2012 用于机器的风险评估。C 类标准中没有规定 SRP/CS 实现的安全功能的所需性能等级($PL_r$)时,可根据附录 A 确定 $PL_r$。依据 GB/T 15706—2012 进行风险评估后,确定需要采取依靠安全功能(如联锁防护装置)的风险减小措施时,可根据本文件采用安全控制系统执行安全功能。本文件预定用于 SRP/CS 的设计和评价。本文件的范围只包括安全相关控制系统。

图 1 给出了 GB/T 15706—2012 与本文件的关系。详细情况见图 2。

注 2:更多信息,见 ISO/TR 22100-2:2013。




[a] 基于 ISO/TR 22100-2:2013 中的图 2。

**图 1　本文件(GB/T 16855.1)集成到 GB/T 15706—2012 的风险减小过程**

**注 3**：图 1 给出了 SRP/CS 对 GB/T 15706—2012 的风险减小过程第 2 步的贡献。SRP/CS 通过执行安全功能支持风险减小措施的组合。安全控制系统在预期条件下执行安全功能的能力分为 5 级，称为性能等级(PL)。具体安全功能(取决于所需的风险减小)的所需性能等级($PL_r$)由风险估计确定。

本文件的资料性附录 A 给出了风险估计的方法，能够用于确定 SRP/CS 执行的安全功能的 $PL_r$。由于评价准则的主观性，不同的风险估计方法之间存在差异。与附录 A 相比，C 类标准能够针对特定机器给出更具体的风险估计方法。

安全功能危险失效的频率取决于几个因素，包括但不限于：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)]、设计过程、运行应力、环境条件和操作程序等。

为了便于 SRP/CS 的设计并评估所实现的 PL，本文件采用了基于故障条件下特定设计准则(如 $MTTF_D$、$DC_{avg}$)和规定行为来进行架构分类的方法。这些架构分为 5 种类别：类别 B、类别 1、类别 2、类别 3、类别 4。

功能安全考虑执行安全功能的组件/元件的失效特征。对于每种安全功能，其失效特征通过每小时危险失效的频率(PFH)来表示。

性能等级和类别适用于 SRP/CS，例如：

——控制单元(如控制功能、数据处理、监控等的逻辑单元)；

——电敏保护装置(如光幕)、压敏保护装置。

对于采用安全部件(元件)的 SRP/CS 的子系统，能够确定其性能等级和类别。安全部件(元件)的示例包括：

——保护装置(如双手操纵装置、联锁装置)；

——动力控制组件(如继电器、阀)；

——传感器和人机交互组件(如位置传感器、使能开关)。

本文件涵盖从简单的机器(如小型厨房炊机具或自动门)到复杂的机器(如包装机械、印刷机械、压力机和集成制造系统等)。

本文件和 IEC 62061 均给出了机器安全控制系统的设计和实施要求。

# 机械安全　安全控制系统
# 第1部分:设计通则

## 1　范围

本文件规定了包括软件设计在内的执行安全功能的安全控制系统(SRP/CS)的设计和集成方法、相关要求、建议和指南。

本文件适用于包括子系统在内的用于高需求和连续操作模式的SRP/CS,无论其采用何种技术和能量(如电气的、液压的、气动的、机械的)。本文件不适用于低需求操作模式。

注1:低需求操作模式见3.1.44和IEC 61508(所有部分)。

本文件未规定特定应用的安全功能或所需性能等级($PL_r$)。

注2:本文件规定SRP/CS设计方法时未考虑某些机械(如移动式机械)的特殊要求。此类特殊要求由C类标准考虑。

本文件未给出构建SRP/CS的产品/元件的具体设计要求。适用于某些SRP/CS元件设计的具体要求由适用的ISO和IEC标准涵盖。

本文件未给出物理安全、IT安全和网络安全等方面的具体措施。

注3:物理安全、IT安全和网络安全等问题可能会影响安全功能。更多信息见ISO/TR 22100-4和IEC/TR 63074。

## 2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 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 19876—2012　机械安全　与人体部位接近速度相关的安全防护装置的定位(ISO 13855:2010,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 42598—2023　机械安全　使用说明书　起草通则(ISO 20607:2019,IDT)

IEC 61508(所有部分)　电气/电子/可编程电子安全相关系统的功能安全(Functional safety of electrical/electronic/programmable electronic safety-related systems)

IEC 62046:2018　机械安全　检测人体存在的保护设备应用(Safety of machinery—Application of protective equipment to detect the presence of persons)

IEC 62061:2021　机械安全　安全相关控制系统的功能安全(Safety of machinery—Functional safety of safety-related control systems)

IEC/IEEE 82079-1:2019　产品使用信息准备(使用说明)　第1部分:原则和一般要求[Preparation of information for use (instructions for use) of products—Part 1: Principles and general requirements]