ICS 13.110
J 09

中华人民共和国国家标准

GB/T 16855.2—2015/ISO 13849-2:2012
代替 GB/T 16855.2—2007

机械安全　控制系统安全相关部件 第2部分:确认

Safety of machinery—Safety-related parts of control systems—Part 2:Validation

(ISO 13849-2:2012,IDT)

2015-12-10 发布　　2016-07-01 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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　确认过程 …… 1
4.1　确认原则 …… 1
4.2　确认计划 …… 2
4.3　一般故障清单 …… 3
4.4　特殊故障清单 …… 3
4.5　确认信息 …… 3
4.6　确认记录 …… 5
5　分析确认 …… 5
5.1　一般要求 …… 5
5.2　分析方法 …… 5
6　测试确认 …… 5
6.1　一般要求 …… 5
6.2　测量精度 …… 6
6.3　更严格的要求 …… 6
6.4　试验样品数量 …… 6
7　安全功能的安全要求规范的确认 …… 7
8　安全功能的确认 …… 7
9　性能等级和类别的确认 …… 7
9.1　分析和测试 …… 7
9.2　类别规范的确认 …… 8
9.3　$MTTF_d$、DC_{avg}和 CCF 的确认 …… 9
9.4　与 SRP/CS 性能等级和类别相关的系统性失效防止措施的确认 …… 10
9.5　安全相关软件的确认 …… 10
9.6　性能等级的确认和验证 …… 11
9.7　安全相关部件组合的确认 …… 11
10　环境要求的确认 …… 11
11　维护要求的确认 …… 12
12　技术文件和使用信息的确认 …… 12
附录 A（资料性附录）　机械系统的确认工具 …… 13
附录 B（资料性附录）　气动系统的确认工具 …… 16

附录 C（资料性附录） 液压系统的确认工具 …… 23
附录 D（资料性附录） 电气系统的确认工具 …… 29
附录 E（资料性附录） 故障特性确认及诊断措施示例 …… 39
参考文献 …… 59

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2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 16855.2—2007《机械安全　控制系统有关安全部件　第2部分：确认》。与GB/T 16855.2—2007相比，除编辑性修改外主要技术变化如下：

——在范围中增加了适用于对性能等级的确认(见第1章，2007年版的第1章)；

——增加了安全功能的安全要求规范的确认(见第7章)；

——增加了性能等级及其相关参数($MTTF_d$、DC_{avg}和CCF)、安全相关软件的确认(见第9章，2007年版的第1章)；

——增加了技术文件和使用信息的确认(见第12章)；

——增加了故障特性确认及诊断措施示例(见附录E)。

本部分使用翻译法等同采用ISO 13849-2:2012《机械安全　控制系统安全相关部件　第2部分：确认》(英文版)。

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：如皋市包装食品机械有限公司、国家机床质量监督检验中心、南京理工大学、欧姆龙自动化(中国)有限公司、中机生产力促进中心、南京林业大学光机电仪工程研究所、皮尔磁工业自动化贸易(上海)有限公司、ABB(中国)有限公司、西门子(中国)有限公司。

本部分主要起草人：史传明、居里锴、赵钦志、张晓飞、李勤、宁燕、居荣华、李立言、褚卫中、张天强、罗广、程红兵、刘英、陈能玉、黄之炯、张亚荣、宋小宁、吴健、王正、付卉青、刘治永、姜涛、于恒。

本部分所代替标准的历次版本发布情况为：

——GB/T 16855.2—2007。

引　言

机械领域安全标准的结构如下：

——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(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，本标准属于 B1 类标准。

C 类标准可补充或修改本标准中的要求。

对于 C 类标准范围内的机器，如果已按照该标准设计与制造，则优先采用该 C 类标准中的要求。

本部分规定了控制系统安全相关部件的安全功能、类别和性能等级的确认过程。本部分认识到通过分析(见第 5 章)和测试(见第 6 章)的组合可实现控制系统安全相关部件的确认，并规定了试验的特殊环境条件。

本部分规定的大多数程序和条件都是基于一种假设，即采用了 GB/T 16855.1—2008 中 4.5.4 规定的估计性能等级(PL)的简化程序。本部分没有给出采用其他程序(例如：马尔科夫建模)的指南，这种情况下，本部分的某些条款不再适用，并且有必要满足附加的要求。

无论控制系统安全相关部件采用了何种技术(电气、液压、气动、机械等)，其设计通则(见 GB/T 15706)的指南都在 GB/T 16855.1 中给出。这包括一些典型安全功能的描述，所需的性能等级的确定，以及类别和性能等级的通用要求。

本部分给出的一部分确认要求是通用性的，而其他确认要求则是专门针对所采用的技术类型。

机械安全　控制系统安全相关部件
第2部分:确认

1　范围

本部分规定了通过分析和测试确认以下参数时需遵循的程序和条件:

——规定的安全功能;

——按照GB/T 16855.1设计的控制系统安全相关部件(SRP/CS)达到的类别;

——按照GB/T 16855.1设计的控制系统安全相关部件(SRP/CS)达到的性能等级。

注:可编程电子系统(包括嵌入式软件)的附加要求在GB/T 16855.1—2008的4.6和GB/T 20438中给出。

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 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 16855.1—2008　机械安全　控制系统有关安全部件　第1部分:设计通则(ISO 13849-1:2006,IDT)

3　术语和定义

GB/T 15706—2012和GB/T 16855.1—2008界定的术语和定义适用于本文件。

4　确认过程

4.1　确认原则

确认过程的目的是为了确定SRP/CS的设计是否支持机械的所有安全要求规范。

确认应证明每个SRP/CS满足GB/T 16855.1的要求,特别是:

a)　设计原理提出的,由该部件所提供的安全功能的规定安全特性。

b)　规定的性能等级的要求(见GB/T 16855.1—2008中4.5):

　1)　规定的类别的要求(见GB/T 16855.1—2008中6.2);

　2)　控制和避免系统性失效的措施(见GB/T 16855.1—2008中附录G);

　3)　适用时,软件的要求(见GB/T 16855.1—2008中4.6);

　4)　在预期环境条件下执行安全功能的能力。

c)　操作者界面的人类工效学设计,例如,不会因此诱使操作者采用危险的操作方式,如废弃SRP/CS(见GB/T 16855.1—2008中4.8)。

宜由独立于SRP/CS设计的人员进行确认。

注:"独立人员"并不意味着需要第三方测试。

确认包括分析确认(见第5章),以及按照确认计划在可预见的条件下进行的功能测试(见第6章)。图1给出了确认过程。分析与测试之间的平衡取决于安全相关部件所采用的技术和所需的性能等级。