ICS 21.010
J 09

中华人民共和国国家标准

GB/T 19436.1—2013/IEC 61496-1:2008
代替 GB/T 19436.1—2004

机械电气安全　电敏保护设备
第1部分:一般要求和试验

Electrical safety of machinery—
Electro-sensitive protective equipment—
Part 1:General requirements and tests

(IEC 61496-1:2008,Safety of machinery—
Electro-sensitive protective equipment—
Part 1:General requirements and tests,IDT)

2013-10-10 发布　　2014-02-01 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 19436《机械电气安全　电敏保护设备》分为4个部分：

——第1部分：一般要求和试验；

——第2部分：使用有源光电保护装置(AOPDs)设备的特殊要求；

——第3部分：响应漫反射有源光电保护装置(AOPDDR)的特殊要求；

——第4部分：视觉保护装置设备的特殊要求。

本部分为GB/T 19436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 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》。

本部分与GB/T 19436.1—2004相比主要技术变化如下：

——标准名称改为《机械电气安全　电敏保护设备　第1部分：一般要求和试验》；

——技术内容有增补，表述用词有改动；

——将附录C(资料性附录)的内容由“参考资料”更改为“符合性评估”；

——增加了参考资料。

本部分使用翻译法等同采用IEC 61496-1:2008《机械安全　电敏保护设备　第1部分：一般要求和试验》。

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

——GB 4943(所有部分)　信息技术设备的安全[IEC 60950(所有部分)]

——GB 14048.5—2008　低压开关设备和控制设备　第5-1部分：控制电路电器和开关元件　机电式控制电路电器(IEC 60947-5-1:2003,MOD)

——GB/T 20438(所有部分)　电气/电子/可编程电子安全相关系统的功能安全[IEC 61508(所有部分)]

本部分做了下列编辑性修改：

——删除了国际标准前言；

——根据4.2.4.3注1的引用，将IEC 60204-1:1997增加到参考文献中。

本部分由中国机械工业联合会提出。

本部分由全国工业机械电气系统标准化技术委员会(SAC/TC 231)归口。

本部分起草单位：济宁科力光电产业有限责任公司、厦门市华测检测技术有限公司、北京机床研究所、北京凯恩帝数控技术有限责任公司、山东省科学院激光研究所、济南二机床集团有限公司、天津市天锻压力机有限公司、江苏扬力集团有限公司、九川集团有限公司。

本部分主要起草人：于俊贤、黄祖广、王学军、郭勇、黄麟、刘统玉、李海明、李岸然、贺庆、刘春平、陈春童、陈建国。

本部分所代替标准的历次版本发布情况为：

——GB/T 19436.1—2004。

引　言

电敏保护设备(ESPE)适用于对人体存在伤害风险的机械。它能在人处于危险状态前，使机械回复到安全状态，从而提供保护。

本部分对可广泛应用的电敏保护设备(ESPE)的一般设计和性能要求做出了规定。符合本部分要求的设备的基本特点是具有适当的安全相关性能等级和规定用于确保此性能等级得以保持的内置式周期性功能检查或自检。

每种类型的机械都有自己特定的危险，本部分的目的并不是推荐电敏保护设备(ESPE)在任何特定机械上使用的方法。电敏保护设备的应用应该是此类设备的供方、机械的用户和强制机构之间协商的事，并且关于这一点，需要注意国内外已经制定的相关指导，例如 GB/T 15706。

本部分涉及 ESPE 的技术适用性。除非采取足够的预防措施，否则此应用所要求使用的物质和试验方法可能对人体健康有害。按照本系列标准，在使用本系列标准所涉及的设备期间，决不免除供方或用户承担关于安全和人身健康的法定责任。

机械电气安全 电敏保护设备 第1部分:一般要求和试验

1 范围

GB/T 19436的本部分规定了作为安全相关系统的组成部分专门用于检测人体的非接触型电敏保护设备(ESPE)的设计、制造和试验的一般要求。需要特别注意的是针对其功能和设计要求,要确保达到适宜的安全相关性能。电敏保护设备(ESPE)可以包括可选择的安全相关功能,这些要求在附录A中给出。

敏感功能的具体类型的特殊要求,在GB/T 19436其他部分给出。

本部分没有规定检测区的尺寸或形状以及它在任何特殊应用中涉及危险的布置,也没有规定由什么构成任何机械的危险状态,只限于ESPE的功能及其怎样与机械连接。

当数据接口用于控制可选择的ESPE的安全相关功能时(附录A),本部分没有规定特殊的要求。对于这些安全相关功能的要求,可以通过查阅其他标准(如GB/T 16855.1、IEC 61508、IEC/TS 62046和IEC 62061)来确定。

本部分可能与那些对非人体保护的应用有关,例如,保护机械或产品免于机械损坏。在这些应用中,可能需要附加的要求,例如必须由敏感功能辨认的材料,具有不同于人的一些特性。

本部分不涉及电磁兼容性(EMC)的发射要求。

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 2423.6—1995 电工电子产品环境试验 第2部分:试验方法 试验Eb和导则:碰撞(idt IEC 60068-2-29:1987)

GB/T 2423.10—2008 电工电子产品环境试验 第2部分:试验方法 试验Fc:振动(正弦)(IEC 60068-2-6:1995,IDT)

GB/T 4026—2010 人机界面标志标识的基本和安全规则 设备端子和导体终端的标识(IEC 60445:2006,IDT)

GB/T 4205—2010 人机界面标志标识的基本和安全规则 操作规则(IEC 60447:2004,IDT)

GB 4208—2008 外壳防护等级(IP代码)(IEC 60529:2001,IDT)

GB 5226.1—2008 机械电气安全 机械电气设备 第1部分:通用技术条件(IEC 60204-1:2005,IDT)

GB 7251.1—2005 低压成套开关设备和控制设备 第1部分:型式试验和部分型式试验成套设备(IEC 60439-1:1999,IDT)

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 12100-2:2003,IDT)

GB/T 15969.2—2008 可编程序控制器 第2部分:设备要求和测试(IEC 61131-2:2007,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)

GB/T 16935.1—2008 低压系统内设备的绝缘配合 第1部分:原理、要求和试验(IEC 60664-1:2007,IDT)

GB/T 17626.2—2006 电磁兼容 试验和测量技术 静电放电抗扰度试验(IEC 61000-4-2:2001,IDT)

GB/T 17626.3—2006 电磁兼容 试验和测量技术 射频电磁场辐射抗扰度试验(IEC 61000-4-3:2002,IDT)

GB/T 17626.4—2008 电磁兼容 试验和测量技术 电快速瞬变脉冲群抗扰度试验(IEC 61000-4-4:2004,IDT)

GB/T 17626.5—2008 电磁兼容 试验和测量技术 浪涌(冲击)抗扰度试验(IEC 61000-4-5:2005,IDT)

GB/T 17626.6—2008 电磁兼容 试验和测量技术 射频场感应的传导骚扰抗扰度(IEC 61000-4-6:2006,IDT)

GB/T 17799.2—2003 电磁兼容 通用标准 工业环境中的抗扰度试验(IEC 61000-6-2:1999,IDT)

GB/T 19001—2008 质量管理体系 要求(ISO 9001:2008,IDT)

IEC 60050-191:1990 国际电工词汇(电工技术词汇)(IEV) 第191章:可靠性和服务质量(International Electrotechnical Vocabulary (IEV)—Chapter 191:Dependability and quality of service)

IEC 60249-2 印刷电路板基材 第2部分:技术规范(Base materials for printed circuits—Part 2:Specifications)

IEC 60947-5-1:1997,低压开关设备和控制设备 第5-1部分:控制电路电器和开关元件 机电式控制电路电器(Low-voltage switchgear and controlgear—Part 5-1:Control circuit devices and switching elements—Electromechanical control circuit devices)

IEC 60950(所有部分) 信息技术设备的安全(Information technology equipment—Safety)

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 62061 机械安全 关系安全的电气、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)

3 术语和定义

下列术语和定义适用于本文件。

3.1

屏蔽 blanking

此功能为可选择功能,即允许大于ESPE检测能力的物体,在当位于检测区内被屏蔽的位置时,而不导致输出信号开关电器[OSSD(s)]进入断开状态的功能。

注1:固定屏蔽是指检测区的屏蔽区的位置在运行过程中不发生变动。检测区其他部分的检测能力保持不变。

注2:浮动屏蔽是指检测区的屏蔽区的位置在运行过程中随着运动物体的位置而变动。检测区其他部分的检测能力保持不变。

3.2

控制/监控装置 controlling/monitoring device

电敏保护设备(ESPE)的组成部分,执行下列功能:

——接收和处理来自敏感装置的信息，并为 OSSD(s)提供信号；

——监控敏感装置和 OSSD(s)。

3.3

检测能力 detection capability

引起 ESPE 动作的敏感功能参数极限值(由供方规定)。

3.4

检测区 detection zone

电敏保护设备(ESPE)对位于其中的规定试件进行检测的区域。

3.5

电敏保护设备 electro-sensitive protective equipment;ESPE

作为整体工作的装置和/或部件的组合，为了达到制动保护或物体出现在检测区时引发感应的目的，至少包括：

——敏感装置；

——控制/监控装置；

——输出信号开关电器[OSSD(s)]和/或安全相关数据接口。

注 1：与 ESPE 相联系的安全相关控制系统，或 ESPE 本身，可以进一步包括副开关电器、抑制功能、停止性能监控器等(见附录 A)。

注 2：安全相关通信接口可以被集成在 ESPE 的整体内。

3.6

外部装置监控 external device monitoring;EDM

电敏保护设备(ESPE)用以监控 ESPE 外部控制装置状态的措施。

3.7

失效 failure

执行某项规定能力的终结。

注 1：失效后，该功能项有故障。

注 2："失效"是一个事件，而区别于作为一种状态的"故障"。

注 3：本概念作为定义，不适用于仅由软件组成的项目。

注 4：实际上，故障和失效这两个术语经常作同义语使用。

[GB 5226.1—2008，定义 3.25]

3.8

危险失效 failure to danger

对正常工作状况的响应是使所有输出信号开关电器(OSSD)进入和/或保持断开状态，而危险失效则是阻止或延迟这种断开状态。

3.9

故障 fault

不能执行规定功能的特征状态。它不包括在预防性维护或其他有计划的活动期间，或缺乏外部资源条件下不能执行规定功能。

注 1：故障经常作为功能项本身失效的结果，但也许在失效前就已经存在。

注 2：英语用术语"fault"及其定义与 IEV 191-05-01 给出的等同。在机械领域，这一术语法语用"defaut"，德语用"Fehler"，而不用术语"Panne"和"Fehlzustand"。

[GB 5226.1—2008，定义 3.26]

3.10

最终开关电器 final switching device;FSD

当输出信号开关电器(OSSD)进入断开状态时，切断机械主控制元件(MPCE)电路的机械中安全相

关控制系统的元件。

3.11

复杂或可编程集成电路 integrated circuit-complex or programmable

能满足下列一条或一条以上准则的单片、混合或模块电路：

a) 在数字方式中，使用1 000个门以上；

b) 可以使用24种以上功能不同的外部电气连接；

c) 功能可编程。

注1：包括ASICs、ROMs、PROMs、EPROMs、PALs、CPUs、PLAs和PLDs。

注2：电路可以按数字、模拟或二者结合的方式工作。

3.12

简单集成电路 integrated circuit-simple

不能满足3.11中各条准则的单片、混合或模块电路。

注1：例如SSI或MSI的逻辑ICs、比较器。

注2：电路可以按模拟、数字或二者结合的方式工作。

3.13

锁定状态 lock-out condition

由某个故障引起的阻止ESPE正常工作的状态，此时其所有的输出信号开关电器(OSSDs)，以及所有的副开关电器(SSDs)(当配备时)都同时进入断开状态。

3.14

机械主控制元件 machine primary control element;MPCE

直接控制机械正常运行的电力元件，当起动或停止机械运行时，它是最后(按时间顺序)的功能元件。

注：例如，该元件可以是主接触器、电磁离合器或电液阀。

3.15

机械副控制元件 machine secondary control element;MSCE

机械控制元件，独立于机械主控制元件，它能够切除有关危险部件的原动机的动力源。

注1：适合时，MSCE通常由副开关电器(SSD)控制。

注2：例如，该元件可以是主接触器、电磁离合器或电液阀。

3.16

抑制 muting

由控制系统中安全相关部件对于安全功能的临时自动暂停。

注：ESPE的抑制见A.7。

3.17

断开状态 OFF-state

致使受控的机械停止运行并无法启动的ESPE的输出状态(例如，输出电路被断开且不允许有电流通过的状态)。

3.18

接通状态 ON-state

允许受控机械运行的ESPE的输出状态(例如，输出电路闭合并能使电流通过)。

3.19

输出信号开关电器 output signal switching device;OSSD

连接机械控制系统的电敏保护设备(ESPE)的元件，当正常工作期间敏感装置被触发时，做出的响

应是进入断开状态。

3.20

全系统停止性能 overall system stopping performance

由电敏保护设备(ESPE)响应时间和中止危险机械运行时间之和构成的时间间隔。

3.21

响应时间 response time

从引起敏感装置触发事件的出现到输出信号开关电器(OSSDs)进入断开状态之间的最长时间。

注1：当ESPE包含安全相关数据接口时，响应时间所涉及的输出信号则是指安全相关数据接口的输出。

注2：当安全相关通信接口被包含在ESPE的整体内时，响应时间所涉及的输出信号则是指安全相关通信接口的输出。此种情况下，响应时间还取决于通信网络的协议和结构。

注3：如果ESPE同时含有安全相关数据接口和输出信号开关电器(OSSDs)时，那么ESPE对于安全相关数据接口和输出信号开关电器(OSSDs)可能具有不同的响应时间。

3.22

重新起动联锁 restart interlock

在机械工作循环的危险部分持续期间敏感装置触发后，在机械工作模式改变后和机械起动控制方法改变后，防止机械自动重新起动的措施。

注：工作模式包括缓动、单行程、自动。起动控制方法包括脚踏开关、双手控制和对电敏保护设备(ESPE)的敏感装置的单一或双重触发。

3.23

控制系统安全相关部件 safety-related part of a control system;SRCS

控制系统中响应输入信号并产生安全相关输出信号的部件或分部件。

注1：这也包括监控系统。

注2：控制系统中安全相关部件的组合，起始于安全相关信号的开启点，结束于动力控制元件的输出点(见GB/T 15706.1—2007的附录A)。

3.24

副开关电器 secondary switching device;SSD

在锁定状态进入断开状态的装置。它可用于引发适当的机械控制作用，例如断开机械副控制元件(MSCE)。

3.25

敏感装置 sensing device

电敏保护设备(ESPE)的部件，使用电敏方法确定ESPE预期检测的事件或状态。

例如，光电敏感装置将检测进入检测区的不透明物体。

3.26

起动联锁 start interlock

当电敏保护设备(ESPE)的电源接通时或中断后再恢复时，防止机械自动起动的方法。

3.27

停止性能监控器 stopping performance monitor;SPM

确定全系统的停止性能是否在预置限值范围内的监控装置。

3.28

供方 supplier

提供与机械设备相关的设备或服务的实体(例如，制造商、承包商、安装商、集成商)。

注：用户本身可以以供方的资格采取行动。

3.29

安全相关数据接口 safety-related data interface

位于 ESPE 的输出接口和安全相关通信接口之间的能够使其直接(即对等)相连的接口,它被用来表示输出信号开关电器[OSSD(s)]的状况。

注 1:这种数据接口没有寻址功能。

注 2:安全相关数据接口可以是双向的。

3.30

安全相关通信接口 safety-related communication interface

与标准通信网络进行安全地连接,以实现安全相关控制功能的连接接口。

4 功能、设计和环境要求

4.1 功能要求

4.1.1 正常工作

在正常工作情况下,当不小于检测能力(依据 GB/T 19436 相关部分的规定)的人体部位进入或位于检测区内时,ESPE 通过发出适当的输出信号做出响应。

ESPE 的响应时间应不超过供方的规定。如果不使用钥匙、关键字或工具,则应无法调整响应时间。

4.1.2 敏感功能

检测能力在供方规定的整个检测区内应是有效的。如果不使用钥匙、关键字或工具,则对于检测区,或检测能力,或屏蔽功能(包括监控的、非监控的、固定的或浮动的)的调整应是不可能的。

4.1.3 ESPE 的类型

本部分考虑了三种类型的 ESPE。这些类型的差别在于其出现故障时和在环境条件影响下所表现出的性能存在差异。本部分考虑了电气的和电动机械的故障的影响(这些故障列述于附录 B 中)。所考虑的由使用的特殊感应技术而产生的故障的补充要求,在该系列标准的其他部分给出。至于对于特殊应用,具体选用哪种类型的 ESPE,则是机械设备制造商或用户的责任。

注:本部分此次未考虑对于 1 型 ESPE 的要求。

2 型 ESPE 应满足 4.2.2.3 规定的故障检测要求。

2 型 ESPE,在正常工作中,当其敏感功能被触发时,或其电源被切断时,应至少有一个 OSSD 的输出电路进入断开状态。

2 型 ESPE 应当具有周期检测的手段。

3 型 ESPE 应满足 4.2.2.4 规定的故障检测要求。

4 型 ESPE 应满足 4.2.2.5 规定的故障检测要求。

3 型和 4 型 ESPE,在正常工作中,当其敏感功能被触发时,或其电源被切断时,应至少有两个 OSSDs 的输出电路进入断开状态。

当使用单一的安全相关数据接口来实现 OSSD 的功能时,则该数据接口和相关的安全相关通信接口应满足 4.2.4.4 规定的要求。在此种情况下,单一的安全相关数据接口可以代替 3 型或 4 型 ESPE 的两个 OSSDs。

4.2 设计要求

4.2.1 电源

ESPE 的设计应使其在下列规定的电源条件下正常运行，用户另有约定的除外。

交流电源：

电压：0.85～1.1 倍的额定电压。

频率：0.99～1.01 倍的额定频率(连续)；

0.98～1.02 倍的额定频率(短时)。

谐波：2 次～5 次畸变谐波的总和不超过线电压方均根值的 10%；6 次～30 次畸变谐波的总和允许附加线电压方均根值的 2%。

直流电源：

a) 由电池供电

电压：0.85～1.15 倍的额定电压；

0.7～1.2 倍的额定电压(这种情况适用于由电池组供电的车辆)。

b) 由转换设备供电

电压：0.9～1.1 倍的额定电压。

纹波(峰-峰值)：应不超过额定电压的 0.05 倍。

对于电击的防护，见 4.2.3.2。

注：对于电气干扰的防护，电源应满足 GB/T 17799.2—2003 的要求。

4.2.2 故障检测要求

4.2.2.1 一般要求

根据 4.2.2.3～4.2.2.5 的相应要求，ESPE 应当对罗列在附录 B 中的故障做出反应。当导致锁定状态的故障依然存在时，ESPE 应不可能通过中断和恢复主电源从锁定状态中复位。在上电时并在 OSSD(s)进入接通状态之前，应对 ESPE 进行检测，以证实其内部不存在故障。

当 ESPE 使用安全相关通信接口来执行 OSSD 的功能时，可能需要对 4.2.2.3～4.2.2.5 中的故障检测要求加以修改，以使其符合 IEC 61508 或 IEC 62061 中相应的安全完整性等级(SIL，例如，4 型对应 SIL3，3 型对应 SIL2，2 型对应 SIL1)的要求。

4.2.2.2 1 型 ESPE 的特殊要求

注：1 型 ESPE 的特殊要求此次未做考虑。

4.2.2.3 2 型 ESPE 的特殊要求

2 型 ESPE 应具有周期检测的手段用来显示危险失效(如检测能力丧失，或响应时间超过规定值)。

导致检测能力丧失，或响应时间延长超过规定值，或阻止一个或多个 OSSDs 进入断开状态的单一故障，作为下一个周期检测的结果，应导致锁定状态。

在预期使用外部的(如机械设备)安全相关控制系统来开启周期检测的场合，ESPE 应配备适当的输入设施(如端子)。

周期检测的持续时间应确保预期的安全功能不受影响。

注：如果把 2 型 ESPE 作为制动装置来使用(例如用做边界防护)，并且当周期检测的持续时间超过 150 ms 时，那么就有可能出现有人通过检测区而不被检测的情况。在这种情况下，ESPE 应具有重新起动联锁功能。

如果电敏保护设备的周期检测是自动进行的，那么周期检测的正确运行应当被监控，并且执行监控

功能的部件的单一故障也应当实时被监控。在这种情况下如果发生故障，则 OSSDs 应当被显示并进入断开状态。

一旦 ESPE 的一个或多个 OSSDs 不能进入断开状态，则应引发锁定状态。

对于只有一个 OSSD 的 ESPE，至少还应有一个 SSD（见 A.4）。

4.2.2.4 3 型 ESPE 的特殊要求

导致检测能力丧失，或响应时间延长超过规定值，或阻止一个或多个 OSSD 进入断开状态的单一故障，应使 ESPE 在 GB/T 19436 相关部分规定的时间内，或在下列需要改变状态才能对故障进行检测的任何情况下立即进入锁定状态：

——触发敏感功能时；

——若配备，起动联锁或重新起动联锁（见 A.5 和 A.6）复位时。

本身不会导致危险失效的单一故障不能被检测出的情况下，另一个其他故障的发生也不应导致危险失效。此要求的验证见 5.3.4。

4.2.2.5 4 型 ESPE 的特殊要求

导致检测能力丧失的单一故障，应使 ESPE 在响应时间内进入锁定状态。

导致响应时间延长超过规定值的单一故障，或阻止一个或多个 OSSD 进入断开状态的单一故障，应使 ESPE 立即——即在响应时间内，或在下列需要改变状态才能对故障进行检测的任何情况下立即进入锁定状态：

——触发敏感功能时；

——若配备，起动联锁或重新起动联锁（见 A.5 和 A.6）复位时。

本身不会导致危险失效的单一故障不能被检测出的情况下，进一步发生的叠加故障也不应导致危险失效。此要求的验证见 5.3.5。

注 1：4 型 ESPE 的设计方法可以包括：

——使用动态故障检测方法的单通道技术；或

——带有内部生成的自动检测的单通道技术，频繁执行使自动检查故障的检测时间间隔包含在安全装置的响应时间内；和

——通道之间的任何差异都会导致锁定状态的多通道技术。

注 2：复杂或可编程集成电路的附加要求见 4.2.10。

4.2.3 ESPE 的电气设备

4.2.3.1 总则

ESPE 的电气设备（部件）应：

——符合有关现行国家标准和/或 IEC 标准的规定；

——适合预期的用途；

——在规定的额定范围内工作。

4.2.3.2 电击的防护

应按照 GB 5226.1—2008 中 6.1 的规定提供防止电击的保护。

4.2.3.3 电气设备的保护

应根据 GB 5226.1—2008 中 7.2.1、7.2.3、7.2.7、7.2.8 和 7.2.9 的规定配置过电流保护设施。

注：有必要向 ESPE 的用户提供信息，例如连接至 OSSD(s)输出连接点的电路所用熔断器的最大额定值或过流保护器件的整定值。

4.2.3.4 污染等级

电气设备应符合污染等级 2 的规定(见 GB 7251.1—2005 中的 6.1.2.3)。

4.2.3.5 电气间隙、爬电距离和隔离距离

电气设备有关电气间隙、爬电距离和隔离距离的设计和制造应符合 GB 7251.1—2005 中 7.1.2 的规定。

4.2.3.6 布线

电气设备的布线应符合 GB 7251.1—2005 中 7.8.3 的规定。

4.2.4 输出信号开关电器(OSSD)

4.2.4.1 总则

对每一个 OSSD 均应提供单独的输出接点(端子)。

OSSD 的额定值应被规定为即使不使用灭弧装置,负载也能被转换。

注:为了增加可靠性,强烈建议配备开关电压抑制器,应将其并联在负载两端而不是跨接在触点两端。

OSSD 的输出电路应被充分地保护,以防止其发生危险失效,例如在过电流条件下触点被焊接(见 GB 5226.1—2008 中的 7.2.9)。

应采取措施将由共因失效而导致危险失效的可能性降至最低。

ESPE 可以执行机械设备的安全相关控制系统的一些功能,例如它的 OSSD 可以执行 FSD 的功能。

3 型和 4 型 ESPE 都应至少包含两个独立运行的 OSSDs。

OSSD 的动作(例如进入断开状态)也意味着安全相关数据接口的相应动作。一个单独的安全相关数据接口可以满足具有两个 OSSDs 的要求。

4.2.4.2 继电器形式的 OSSDs

如果采用继电器形式的 OSSDs,则触点的状态(即位置)应被监控。可以通过监控带有机械式连接(强制导向)触点的继电器的辅助触点来实现。机械式连接确保被监控触点随 OSSD 触点的状态而变化。

特殊的设计和机械结构应当确保继电器的动合(即常开)触点与动断(即常闭)触点不可能同时处于闭合状态。

注 1:机械式连接确保被监控触点随 OSSD 触点的状态而变化。

注 2:重要的是在标称的寿命周期内,继电器的释放电压和触点之间的间隔距离,都要保持在一个适当的水平上。

4.2.4.3 固态形式的 OSSDs

固态形式的 OSSD 分为拉电流型和灌电流型两种类型。当使用拉电流型输出时,应满足该条款的要求。

注 1:本部分没有对可以在某种应用场合需用的灌电流型输出的要求做出规定。使用时应特别谨慎(例如,当使用灌电流型输出时,对基准电压的短路或开路,会被输入和负载视为接通状态)。IEC 60204-1:1997 中 9.1.4 的要求也应予以考虑。

注 2：对于 24 V(d. c.)的额定电源电压，接通状态和断开状态的输出电压和电流值应符合表 1 的规定。

注 3：对于 24 V(d. c.)的额定电源电压，表 1 中的值满足 GB/T 15969.2—2008（见 GB/T 15969.2—2008 中的 5.2）的要求。当使用其他电源电压时，本部分可以作为指导，GB/T 15969.2—2008 可以提供其他信息。

表 1　固态 OSSDs 接通和断开状态的输出

额定电源电压	断开状态下的 输出电压范围	接通状态下的 输出电压范围	断开状态下的 输出电流(最大漏电流)	接通状态下的 输出电流
24 V(d. c.)	−3 V～+2 V 方均根值 (5 V 峰值)	+11 V～+30 V	<2 mA	>6 mA

输出电路应当具有对过压、过流和短路的保护。

最大漏电流不应超过 2 mA，包括故障情况下(例如开路)。

使用一个以上的 OSSD 时，OSSDs 之间的短路应被检测。

ESPE 供方应在随机文件中提供以下信息：

——阻性负载和感性负载在接通状态时的额定输出电流和最大输出电流；

——断开状态的最高电压；

——断开状态的最大输出电流(漏电流)；

——最大容性负载；

——OSSD(s)与负载之间连接的最大阻抗。

4.2.4.4　安全相关数据接口和安全相关通信接口

正常工作中敏感装置被触发时，ESPE 应通过安全相关数据接口发送表明敏感装置或 ESPE 状态的信息做出响应。此状态信息通过安全相关通信接口转换为数据报文。

安全相关数据接口应具有相应于 ESPE 类型的同等故障防护能力。

根据 ESPE 的设计，安全相关通信接口可以作为一个分离的部件被设置在 ESPE 之外[如图 1a)]，也可以被集成在 ESPE 的整体系统之内[如图 1b)]。

安全相关通信接口在满足本部分(GB/T 19436.1)要求的同时，还应当满足 IEC 61508 或 IEC 62061 中适当的安全完整性等级(SIL，例如，4 型对应 SIL3，3 型对应 SIL2，2 型对应 SIL1)的相关要求。

安全相关通信接口与 ESPE 集成为一体时，整体的 ESPE 应满足 IEC 61508 或 IEC 62061 的相关要求。

注：由于通信接口的特殊技术，GB/T 19436.1 适合引用不同的标准。为避免与其他标准的重叠，本部分没有规定安全相关通信接口的功能要求。

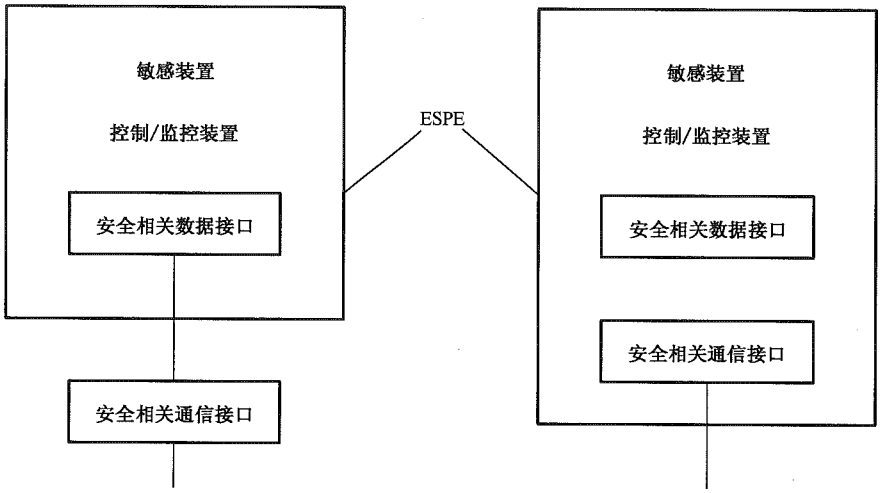

图 1 使用安全相关通信接口的 ESPE 的示例

4.2.5 指示灯和显示器

ESPE 制造商应提供指示灯和显示器：

a) 指示敏感装置的触发状态。从触发敏感装置到指示灯达到 50%最终亮度(冷光)的时间，以及从取消对敏感装置的触发到指示灯亮度减弱到最初亮度 50%的时间，都不应超过 100 ms。

b) 指示 OSSD 的输出状态。用绿色指示灯表示接通状态，用红色指示灯表示断开状态。两个或多个 OSSDs 配合工作时，可以使用单独的一套指示灯。

使用两个或多个相同颜色的指示灯时，每个指示灯所指示的功能应明确标识。

注：对于某些工作模式，用于 a)的同一套指示灯也可用于 b)。

指示灯是为机械设备的操作者设计的。因此，在安装这类保护设备时，指示灯应放置在接近检测区且可以看得到的位置。指示灯可以与传感器部件集成在一起，也可以作为一个外围设备安装在检测区附近。

4.2.6 调整方法

所有调整方法的设计都应满足：调整范围内的任何点都不可能产生危险失效，调整方法的失效不应引起 ESPE 的配置发生意外的变化。

4.2.7 子系统的脱开

当提供有允许任何子系统、子系统的部件或任何插接式组件脱开的方法时，按照 4.2.2 的规定，这类脱开应导致至少一个 OSSD 进入断开状态。

4.2.8 非电元件

非电元件应适合于预期的使用要求。

4.2.9 共因失效

设计应使由下列因素引起共因失效而导致危险失效的可能性降至最低：

——环境影响；

——使用公共基底的多通道系统；

——多通道系统通道间的短路。

注 1：共因失效，也可能是由于使用了因为误操作、误加工等而降级的元器件造成的。

注 2：共因失效被视为单一失效。

同一块半导体基底上的元件不应用于多通道系统中一个以上的通道中。

4.2.10 可编程或复杂集成电路

4 型 ESPE 使用可编程或复杂集成电路时，其安全相关性能应由至少 2 条独立的控制/监控通道保持。此要求应按照 5.5 验证。

4.2.11 集成电路的软件、编程及功能设计

4.2.11.1 总则

ESPE 通过下列任何方法实施其安全相关性能时，应使用 4.2.11.2 的附加要求：

a) 工作期间执行的软件程序；

b) 程序化的器件，其功能是在初始制造后经过程序化处理设置的，如 PAL、PLA、PLD、PROM；

c) 按用户特定的功能要求制造的器件，例如 ASIC、掩膜程序微处理器、ROM。

上述要求应按 5.5 确认。

4.2.11.2 要求

a) 软件、装置程序和装置功能设计，应当按照 IEC 61508-3 中适当的安全完整性等级(SIL，例如，4 型对应 SIL3，3 型对应 SIL2，2 型对应 SIL1)的要求进行开发。

b) 应按照质量管理体系程序提供证明文件，表明已达到所要求的安全相关性能等级。

c) 应形成文件化的质量计划，清楚地识别开发的各个阶段，并明确每个阶段的验收准则。例如开发阶段是要求规范制定阶段、设计规范阶段、验证阶段和确认阶段。

d) 在任何开发之前，为确定安全规范中 ESPE 的安全相关功能，应对 ESPE 的概念设计进行基于危险和失效模式识别的分析。然后 ESPE 的部分或全部安全相关功能应被分配到 4.2.11 的措施中，对每种元件所要求的安全相关性能应加以确定。为了达到安全相关性能的要求，应采用适合于规范、设计、使用和维修的工程技术。

e) 每一部分与 4.2.11.1 有关的软件、程序设计和功能设计的要求，应当完整和明确。每个要求规范应使审核人员或验证人员(即设计者之外的人)能够容易地追溯到安全要求规范，以证实所要求的安全相关功能被充分地处理。

f) 为了证明该项设计正确地实现了安全要求规范所要求的安全相关功能，应制订一项综合性测试计划。软件、程序和功能规范的试验，应在项目记录中加以记录，以证明设计满足安全要求规范。

g) 软件、程序设计和功能规范设计，应受控于有效的配置管理和更改控制。在开发期间，有效的程序应确保关于要求、规范、设计等方面的更改均被充分地记录，并对所有更改的影响进行分析，以确保安全要求规范在设计过程的所有阶段保持可追溯性。应保护设计免于未经授权的更改，并应准确地记录其精确的配置(如模块表、版本号)。

h) ESPE 运行中使用软件程序时，应将整个操作指令软件保存在处理器无法重写的只读存储器中。应采用适当的技术监控正确的程序流程，确保软件的完整性。

此类技术可包括监视器、RAM/ROM 检查、CPU 测试等。

i) 使用软件工具诸如编码器或译码器(而不是组译器)开发软件时,除下列情况外,软件的多样性都应予以考虑:

——用于不同程序的软件工具是完全不相关的;或

——软件工具拥有认可的国家标准或国际标准的"验证证书";或

——测试方案包含充分的措施,以检测因软件工具而导致的共因错误。

j) 作为设计原则,就实用而言,安全相关软件应尽可能与安全无关软件相隔离,这是为了使安全功能被破坏的可能性降至最低,并有助于安全性能评估。

4.3 环境要求

4.3.1 环境空气温度范围和湿度

当环境温度变化范围为0 ℃～50 ℃时,ESPE应符合本部分的要求。超出该范围使用时,供方应规定系统仍能继续正常运行的温度范围。在温度为20 ℃和5.4.2所规定的最高环境温度之间,无凝露湿度为95%时,此项要求应用5.4.2规定的试验进行验证。

4.3.2 电骚扰

4.3.2.1 电源电压波动

当外部电源电压在10 s～20 s内从标称电压平滑地降到零电压,然后以同样的方式从零电压上升到标称电压时,ESPE应不发生危险失效。

当各内部获得的电源电压在10 s～20 s期间,依次从标称电压平滑地降到零电压,然后以同样的方式,从零电压上升到标称电压时,ESPE应不发生危险失效。

4.3.2.2 电源电压中断

电源电压中断(暂降)如表2所示。

表2 电源电压中断

试验编号	额定电压下降值/ %	下降时间/ ms	下降重复频率/ Hz
1)	100	10	10
2)	50	20	5
3)	50	500	0.2

ESPE应对试验1)和2)的响应是连续正常工作,对试验3)的响应是不发生危险失效。

ESPE采用特定类型的电源电压供电(例如,直接由安全相关通信接口供电)时,本条款中的电源中断则可以施加于特定电源的主输入电源,而不是直接对ESPE供电的输入电源。

4.3.2.3 电压快速瞬变脉冲群

4.3.2.3.1 一般要求

当经受GB/T 17626.4—2008规定的电快速瞬变脉冲群试验时,ESPE应继续正常工作,试验要求如表3所示。

表 3 脉冲试验要求

试验项目	试验要求
d.c.或电压<50 V(a.c.)的电源线端口	1 kV(峰值),按照 GB/T 17626.4—2008 的 2 级试验等级规定
长度>1 m 的信号线端口	
电压≥50 V(a.c.)的电源线端口	2 kV(峰值),按照 GB/T 17626.4—2008 的 3 级试验等级规定

4.3.2.3.2 附加要求

当经受 GB/T 17626.4—2008 规定的电快速瞬变脉冲群试验时,3 型和 4 型的 ESPE 应不发生危险失效,附加要求如表 4 所示。

表 4 3 型和 4 型 ESPE 脉冲试验附加要求

试验项目	试验要求
d.c.和<50 V(a.c.)的电源线端口	2 kV(峰值),按照 GB/T 17626.4—2008 的 3 级试验等级规定
长度>1 m 的信号线端口	
电压≥50 V(a.c.)的电源线端口	4 kV(峰值),按照 GB/T 17626.4—2008 的 4 级试验等级规定

4.3.2.4 电压快速瞬变浪涌

4.3.2.4.1 一般要求

当经受 GB/T 17626.5—2008 规定的浪涌(冲击)试验时,ESPE 应继续正常工作,试验要求如表 5 所示。

表 5 浪涌试验要求

试验项目	试验要求
长度>1 m 的信号线端口	共模 1 kV(峰值),按照 GB/T 17626.5—2008 的 2 级试验等级规定
d.c.和电压<50 V(a.c.)的电源线端口	
电压≥50 V(a.c.)的电源线端口	共模 2 kV(峰值)和差模 1 kV(峰值),按照 GB/T 17626.5—2008 的 3 级试验等级规定

4.3.2.4.2 附加要求

当经受 GB/T 17626.5—2008 规定的浪涌(冲击)试验时,3 型和 4 型 ESPE 应不发生危险失效,附加要求如表 6 所示。

表 6 3 型和 4 型 ESPE 浪涌试验附加要求

试验项目	试验要求
长度>1 m 的信号线端口	共模 2 kV(峰值),按照 GB/T 17626.5—2008 的 3 级试验等级规定
d.c.和电压<50 V(a.c.)的电源线端口	
电压≥50 V(a.c.)的电源线端口	共模 4 kV(峰值)和差模 2 kV(峰值),按照 GB/T 17626.5—2008 的 4 级试验等级规定

4.3.2.5 电磁场

4.3.2.5.1 一般要求

当经受 GB/T 17626.3—2006 中 5.1 规定的第 3 级电磁场试验时(试验场强为 10 V/m),ESPE 应继续正常工作。

4.3.2.5.2 附加要求

当经受 GB/T 17626.3—2006 中 5.2 规定的第 4 级电磁场试验时(试验场强为 30 V/m),3 型和 4 型的 ESPE 应不发生危险失效。

4.3.2.6 射频场感应的传导骚扰

4.3.2.6.1 一般要求

当经受 GB/T 17626.6—2008 规定的传导射频骚扰试验时,ESPE 应继续正常工作,试验要求如表 7 所示。

表 7 射频场感应的传导骚扰试验要求

试验项目	试验要求
长度 1 m～10 m 的信号线端口	3 V(方均根值),按照 GB/T 17626.6—2008 的 2 级试验等级规定
长度>10 m 的信号线端口	10 V(方均根值),按照 GB/T 17626.6—2008 的 3 级的试验等级规定
电源端口	
接地端口	

4.3.2.6.2 附加要求

当经受 GB/T 17626.6—2008 规定的传导射频骚扰试验时,3 型和 4 型的 ESPE 应不发生危险失效,附加试验要求如表 8 所示。

表 8 3 型和 4 型 ESPE 射频场感应的传导骚扰试验要求

试验项目	试验要求
长度 1 m～10 m 的信号线端口	10 V(方均根值),按照 GB/T 17626.6—2008 的 3 级试验等级规定
长度>10 m 的信号线端口	30 V(方均根值),按照 GB/T 17626.6—2008 的 X 级试验等级规定
电源端口	
接地端口	

4.3.2.7 静电放电

4.3.2.7.1 一般要求

当经受 GB/T 17626.2—2006 中第 3 级规定的静电放电试验时(接触放电为 6 kV 或空气放电 8 kV),ESPE 应继续正常工作。

4.3.2.7.2 附加要求

当经受 GB/T 17626.2—2006 中第 4 级规定的静电放电试验时(接触放电为 8 kV 或空气放电 15 kV),3 型和 4 型的 ESPE 应不发生危险失效。

4.3.3 机械环境

4.3.3.1 振动

在 5.4.4.1 的振动试验期间,ESPE 应能继续正常工作。

4.3.3.2 碰撞

在 5.4.4.2 的碰撞试验期间,ESPE 应能继续正常工作。

4.3.4 外壳

ESPE 应有自身的外壳。

当 ESPE 的所有外壳,包括远程安装的外壳,按照供方的规定被安装时,应至少具有 IP54 的防护等级(见 GB 4208—2008)。然而当其部件被安装在具有至少 IP54 防护等级的机械设备控制装置外壳内时,ESPE 部件外壳的防护等级应至少达到 IP20。

注:机械损坏的防护可以通过下列措施实现:

——合适的定位;

——使用适当的材料并提供足够强度的结构形式;或

——使用防护屏障。

引入电缆的进入方式应不降低防护等级。

粘接两个结合表面之间的密封剂,不应用来密封维修时需拆去的盖子,因为当连接的表面被分离时,会降低对环境的防护等级。

外壳应没有可损坏电缆绝缘的锐边或棱角,应通过检查确认。

外壳应具有足够的检修口,以便安全有效地执行必要的调整和维修工作。这类检修口的盖子应采用系留紧固件。

5 试验

5.1 总则

5.1.1 型式试验

5.1.1.1 试验样品

如果可行,ESPE 所有部件(做为一个整体)应一起进行试验。如果不可行,ESPE 的部件可以分开试验。就环境试验情况来说,这种情况就需包含整体的 ESPEs(ESPEs 集成于机械装置时,通常不能与机械装置分开)。在这种情况下:

——ESPE 工作所需的任何输入信号都应加以模拟;

——试验中的任何例外和遗漏都应在试验报告中阐述。

在某一特殊试验具有破坏性,但通过隔离测试 ESPE 的部件可得到相同结果的情况下,可以使用部件样品代替整个设备样品,以得到试验结果。

当 ESPE 设计成可用于多种电源电压时(例如适于不同用途),可能需要多个样品。

当 ESPE 设计成由外部专用电源供电时，ESPE 应使用规定的专用电源进行试验(见 6.2)。

5.1.1.2 工作条件

除非在试验程序中另有规定，试验应对试验样品按随机文件所规定的条件进行。

关于电骚扰抗扰度试验，设备应尽可能接近其最终工作配置(如外围设备和附带的罩盖，连接到电源上，可行时，连接外部保护导体和/或外部的功能连接导体，见 GB 5226.1—2008)。

当规定几个安装位置时，应使用最不利的安装位置。

当使用安全相关数据接口代替 OSSD 时，ESPE 应按照供方的具有监控 ESPE 状态方法的说明书与通信系统相连接。

5.1.1.3 进入检测区的模拟

在后面的测试中，如果模拟的方法能够表明是等效的，试件(依据 GB/T 19436 相关部分的定义)进入检测区可以被模拟。

5.1.2 试验条件

5.1.2.1 试验环境

除 5.4 另有规定外，ESPE 应在下列条件下工作时进行试验：

——额定电压(或额定电压范围内的电压)；

——额定频率(或额定频率范围内的频率)；

——周围温度：20 ℃±5 ℃；

——相对湿度：25%～75%；

——空气压力：86 kPa～106 kPa。

注：在标志和随机文件中规定的数值视为额定值。

5.1.2.2 测量精度

测量的误差应不超过：

——ESPE 响应时间测量：±1 ms；

——温度测量：±3 ℃；

——电气测量：±1%，技术上可能和/或适当时；

——相对湿度(RH)测量：±3%RH；

——线性测量：±1 mm 或±1%，取其中的较大值。

所有的测量应在恒温条件下进行。当温度的上升率或下降率小于 2 K/h 时，则认为测量条件满足。

5.1.2.3 ESPE 与安全相关通信接口一起测试的环境条件

ESPE 和安全相关通信接口应一起测试(见图 2)。由于安全相关通信接口不显示静态的输出信号，因此需要使用数据接收器。测试设置包括受试设备和显示 ESPE 或敏感装置状态的数据接收器(如 PLC 或监控装置)。

测试电骚扰的敏感性可能需要使用合适的测试适配器，以隔离受试 ESPE 与通信总线。

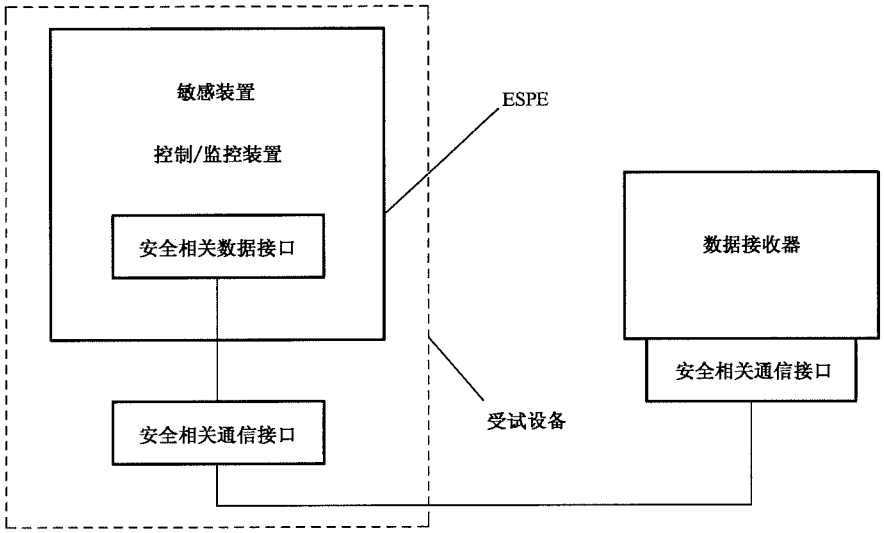

图 2 使用安全相关通信接口的 ESPE 的 EMC 测试设置

5.1.3 试验结果

本章所列试验和分析的结果，应形成文件。试验结果应采用表格展示各项单独试验及其效果的详情。任何特殊试验过程的详情，都应包括在测试报告中。

注：建议按照附录 C 验证试验结果。

5.2 功能试验

5.2.1 敏感功能

ESPE 的敏感功能及其检测能力和检测区(例如大小、形状和位置)的完整性，应按 GB/T 19436 相关部分的规定验证。

5.2.2 响应时间

响应时间应通过系统分析和测试来验证。

如果响应时间包括触发敏感装置的动作事件和此动作之间的最长时间，则响应时间可由动作的电模拟来确定。

ESPE 响应时间测量的附加要求，可在 GB/T 19436 的相关部分给出。

5.2.3 限定功能的试验

5.2.3.1 总则

应进行下列限定功能试验 A、B 和 C，以验证在正常环境条件下 ESPE 应连续正常工作，在非正常环境条件下或故障情况下，ESPE 应不发生危险失效。

如果 ESPE 配置有重新起动联锁功能，在试验期间，此功能应被旁路或不选择。重新起动联锁功能应单独试验(见附录 A)。

使用安全相关通信接口时，在下列的限定功能试验中，OSSDs 的接通或断开状态，将由显示 ESPE 或敏感装置相应状态的安全相关信息(如数据报文)代替。

5.2.3.2 限定功能试验 A(A 试验)

在没有物体进入检测区的情况下,应观察至少 5 s,除非另有规定,此期间 OSSD(s)应处于接通状态,而不应进入断开状态。

5.2.3.3 限定功能试验 B(B 试验)

在没有物体进入检测区的情况下,应观察至少 5 s,除非另有规定,此期间 OSSD(s)应处于接通状态,而不应进入断开状态。

将试件放入检测区,OSSD(s)应通过从接通状态进入断开状态做出响应。应观察至少 5 s,除非另有规定,此期间 OSSD(s)在试件存在于检测区时保持断开状态,或保持其他触发状态。

将试件从检测区撤出,或使样品处于其他非触发状态,OSSD(s)应通过从断开状态进入接通状态做出响应。应观察至少 5 s,除非另有规定,此期间 OSSD(s)在试件不存在于检测区时保持接通状态,或保持其他物理上的非触发状态。

根据试验的要求,以上试验可能需要连续地重复进行。

5.2.3.4 限定功能试验 C(C 试验)

这项试验和限定功能试验 B 一样,只不过 B 试验中 OSSD(s)应处在接通状态,而本试验中 OSSD(s)允许处于断开状态,但不应发生危险失效。在 5.4 各相关试验结束时,ESPE 应继续正常工作或从锁定状态中恢复。

如果 ESPE 因元件永久失效不能恢复正常工作,经验证仅是通信接口的元件失效,并且 OSSD(s)仍保持在断开状态,这种情况可以接受。

注:在极端的电骚扰(如危险失效测试)情况下,通信接口的某些元件可能发生永久失效并使 ESPE 无法恢复正常工作。

5.2.4 周期检测

对于 2 型的 ESPE,4.2.2.3 的要求应通过分析和检测进行验证。

5.2.5 指示灯和显示器

应按照 4.2.5 的要求,通过 B 试验验证指示灯和显示器的功能和颜色。

5.2.6 调整方法

4.1.1 和 4.1.2 的要求应通过检查予以验证,4.2.6 的要求应通过检查和进行必要的 C 试验予以验证。

5.2.7 元件的额定值

应通过分析和/或检查来验证遍及 ESPE 的整个工作范围的各元件,在其规定的额定值范围内工作。

5.2.8 输出信号开关电器(OSSD)

5.2.8.1 总则

应验证为各 OSSD 配备了单独的输出接点(端子)。

提供两个 OSSDs 时,通过检查或试验验证两个 OSSDs 相互独立工作。

检查验证 OSSD(s)具有限流装置保护,或限流装置的安装信息已在使用说明书中给出。

应验证可预见的故障不会导致 OSSD(s)进入或保持接通状态，所有试验应在制造商规定的最大感性负载和最长连接电缆的条件下进行。

可预见的故障包括：

——OSSD 与电源电压短路；

——OSSD 与接地线短路；

——OSSD(s)之间短路；

——电源回路的电缆开路；

——功能连接线开路；

——屏蔽电缆的屏蔽线开路；

——错误的接线。

5.2.8.2 继电器形式的 OSSDs

通过检查和测试验证继电器符合 4.2.4.2 的要求。

5.2.8.3 固态形式的 OSSDs

应验证输出电压和电流的值符合 4.2.4.3 的规定。

5.2.8.4 安全相关数据接口和安全相关通信接口

应通过试验验证元件的断开不会导致危险失效。

5.2.8.1 中规定的适用于 OSSD 的电气试验(短路、开路和错误的负载)，如不适用，可不进行。

整体通信接口的安全完整性，应通过试验、系统分析、考察数据表和测试报告，验证满足 4.2.4.4 的要求。

5.3 故障条件下的性能试验

5.3.1 总则

ESPE 所有有关元件都应对按照 4.2.2 选择的单一故障的效果进行试验。如果进一步出现的故障是由第一个单一故障导致的，则第一个和所有接着发生的故障应视为单一故障。

应准备包含所有元件的故障目录，以记录附录 B 中所考虑故障的结果。为了减少不必要的试验，对于 5.3.3、5.3.4 和 5.3.5 中的能够理论预测出单一故障或组合故障结果的情况，分析报告应作为测试报告的一部分。该报告应按照 5.5.4 进行验证。此时，只需进行选择性(样品)试验，以确认这些分析报告。

注 1：用于故障评估的典型方法包括 IEC 60812 的故障模式分析以及 IEC 61025 的故障树分析。

注 2：在复杂电路结构或元件情况下(例如，微处理器、完全冗余)，故障的检查一般是在结构层次上进行。装配电路板上短路的排除见 B.1.2。用于外部连接的相邻端子之间的短路的排除见 B.1.3 和 B.1.4。

5.3.2 1 型 ESPE

注：该版本未对 1 型 ESPE 的要求进行考虑。

5.3.3 2 型 ESPE

根据 4.2.2.3，ESPE 应承受单一故障，以确定导致危险状况(如检测能力丧失或响应时间延长)的故障能够通过周期检测功能被检出，并导致锁定状态。

配备有内部开启的周期检测功能时，应验证监控功能的故障受到检测，并导致锁定状态或引起至少一个 OSSD(s)进入断开状态。

5.3.4 3型 ESPE

根据4.2.2.4,ESPE应承受单一故障,以确定故障通过ESPE进入锁定状态而受到检测,并且不发生危险失效。

当单一故障不能受到检测且又不能进行5.3.1规定的分析时,利用该故障作为初始故障,并依次叠加和撤销所有其他故障,对ESPE进入锁定状态并且没有危险失效发生的试验应继续进行。所有不能受到检测的单一故障都应进行试验。

多于两种故障的累积不需要进行试验。

5.3.5 4型 ESPE

根据4.2.2.5,ESPE应承受单一故障,以确定故障通过ESPE进入锁定状态而受到检测,并且不发生危险失效。

当单一故障不能受到检测且又不能进行5.3.1规定的分析时,利用该故障作为初始故障,并依次叠加和撤销所有其他故障,对ESPE进入锁定状态并且没有危险失效发生的试验应继续进行。所有不能受到检测的单一故障都应进行试验。

当连续的两个故障不能被检测出且又不能进行5.3.1规定的分析时,应依次对这些连续的两个故障继续进行试验,并依次叠加和撤销其他所有单一故障,不应发生危险失效。所有不能被检测出的双重故障都应进行试验。

当多于3个的故障通常互相独立,并且按照特定的时间顺序出现的可能性很低时,则3个以上故障累积的试验不需要进行。

5.4 环境试验

5.4.1 额定电源电压

4.2.1规定的设计措施,应通过检测予以验证。

用4.2.1规定的相关值,ESPE应承受下列顺序的试验:

a) ESPE应配备最低额定电源电压,应进行A、B试验;

b) 电压应在10 s～20 s时段内,增加到最高额定电压,此时应进行A试验;

c) 达到最高试验电源电压后,应进行B试验。

对频率变化和谐波畸变的要求应通过试验或分析方法进行验证。

5.4.2 环境温度变化和湿度

标志或随机文件中应规定不低于50 ℃的最高环境试验温度和不高于0 ℃的最低环境试验温度。

对于ESPE应依照下列顺序进行试验:

a) 使ESPE在5.1.2.1规定的条件下运行工作,应进行A试验,持续时间至少2 h。A试验结束时,应进行B试验。

b) 应使环境温度以不大于0.3 ℃/min的速率上升到最高环境温度,在此期间应进行A试验。

c) 在最高环境温度下应进行A试验,持续时间至少2 h。在此期间,应使湿度上升到95%,并保持此湿度至少1 h。A试验之后,应进行B试验。

d) 应使环境温度以不大于0.3 ℃/min的速率下降,同时使湿度保持在95%,直到降至20 ℃为止。在此过程中应进行A试验。

e) 应使环境温度以不大于0.3 ℃/min的速率下降,但没有凝露发生,至降到最低环境温度为止。在此过程中应进行A试验。

f) 应在最低环境温度下进行A试验，持续时间至少2 h。A试验结束时应进行B试验。

g) 应使环境温度以不大于0.3 ℃/min的速率上升到5.1.2.1所规定的温度，在此期间应进行A试验。

h) A试验应在5.1.2.1所规定的温度下进行，持续时间至少2 h。在A试验结束时应进行B试验。

5.4.3 电骚扰的影响

注：对于使用通信总线接口的ESPE测试的修订，尚在考虑中。

5.4.3.1 电源电压波动

外部的电源电压和内部派生的各电源电压应按4.3.2.1的要求依次变动。在每项试验期间，必要时应进行C试验，以确认在降低电压时没有出现危险失效。

5.4.3.2 电源电压中断

应进行4.3.2.2和表2规定的试验。每项试验持续的时间应足够长，以覆盖至少10次暂降，并应使试验1)及2)进行B试验，试验3)进行C试验。

5.4.3.3 电压快速瞬变脉冲群

5.4.3.3.1 一般要求

ESPE应经受4.3.2.3.1规定等级的电快速瞬变脉冲群试验，依照GB/T 17626.4—2008的规定(对于直流电源端口、50 V以下的交流电源端口和信号端口的耦合试验配置如GB/T 17626.4—2008中图10所示；其他交流电源端口的耦合如GB/T 17626.4—2008中图9所示)。

在各暴露期间，应进行B试验。

5.4.3.3.2 附加试验

3型或4型ESPE还应经受4.3.2.3.2规定等级的电快速瞬变脉冲群试验，依照GB/T 17626.4—2008的规定(对于直流电源端口、50 V以下的交流电源端口和信号端口的耦合试验配置如GB/T 17626.4—2008中图10所示；其他交流电源端口的耦合如GB/T 17626.4—2008中图9所示)。

在各暴露期间，应进行C试验。

5.4.3.4 电压快速瞬变浪涌

5.4.3.4.1 一般要求

ESPE应经受4.3.2.4.1规定等级的浪涌(冲击)试验，依照GB/T 17626.5—2008的规定(信号端口的耦合试验配置如GB/T 17626.5—2008中图11或图14所示；直流电源和50 V以下的交流电源端口的耦合试验配置如GB/T 17626.5—2008中图8所示；其他交流电源端口如GB/T 17626.5—2008中图7和图8所示)。

在各暴露期间，应进行B试验。

5.4.3.4.2 附加试验

3型或4型ESPE还应经受4.3.2.4.2规定等级的浪涌(冲击)试验，依照GB/T 17626.5—2008的规定(信号端口的耦合试验配置如GB/T 17626.5—2008中图11或图14所示；直流电源和50 V以下的交流电源端口的耦合试验配置如GB/T 17626.5—2008中图8所示；其他交流电源端口如

GB/T 17626.5—2008 中图 7 和图 8 所示)。

在各暴露期间,应进行 C 试验。

5.4.3.5 电磁场

5.4.3.5.1 一般试验

ESPE 应经受 4.3.2.5.1 规定等级的电磁场试验,依照 GB/T 17626.3—2006 中 5.1 的规定。在置于严厉等级为 3 的测试期间,应进行 B 试验。

注:此试验结果取决于环境结构,与 ESPE 安装在机械上所得结果可能有差异。

5.4.3.5.2 附加试验

3 型和 4 型的 ESPE 还应经受 4.3.2.5.2 规定等级的电磁场试验,依照 GB/T 17626.3—2006 中 5.2 的规定。在置于严厉等级为 4 级的测试期间,应进行 C 试验。

注:此检验结果取决于环境结构,与 ESPE 安装在机械上所得结果可能有差异。

5.4.3.6 射频场感应的传导骚扰

5.4.3.6.1 一般试验

ESPE 应经受 4.3.2.6.1 规定等级的传导性射频骚扰试验,依照 GB/T 17626.6—2008 的规定。在各暴露期间,应进行 B 试验。

5.4.3.6.2 附加试验

3 型或 4 型 ESPE 还应经受 4.3.2.6.2 规定等级的传导射频骚扰试验,依照 GB/T 17626.6—2008 的规定。

在各暴露期间,应进行 C 试验。

5.4.3.7 静电放电

5.4.3.7.1 一般试验

ESPE 应经受 4.3.2.7.1 规定等级的静电放电试验,依照 GB/T 17626.2—2006 的规定。在各暴露期间,应进行 B 试验。

5.4.3.7.2 附加试验

3 型或 4 型 ESPE 还应经受 4.3.2.7.2 规定等级的静电放电试验,依照 GB/T 17626.2—2006 的规定。在各暴露期间,应进行 C 试验。

5.4.4 机械影响

5.4.4.1 振动

试验样品应经受 GB/T 2423.10—2008 规定的振动试验。

试验条件如下:

频率范围	10 Hz~55 Hz;
扫描速度	1 倍频程/min;
振幅	(0.35±0.05)mm,试验应在无减振装置的情况下进行;
扫描次数	每轴为 20,三轴(没有因共振频率产生延迟)。

每轴都应进行以下限定功能试验：

——A 试验应在最初和最后的扫描期间进行；

——进行 B 试验，试件应在第二次扫描开始时进入检测区，并在第 19 次扫描结束时移开。

5.4.4.2 碰撞

试验样品应经受 GB/T 2423.6—1995 规定的碰撞试验。

试验条件如下：

加速度　　10 g；

脉冲持续时间　　16 ms；

碰撞次数　　3 轴的每轴各为 1 000±10。

各轴应进行下列试验：

——在最初的和最后的(100±10)次的每次碰撞期间，应进行 A 试验；

——应在最初的(100±10)次碰撞之后，把试件放入检测区，进行 B 试验。

5.4.5 外壳

5.4.4 的试验完成后，4.3.4 对于防护等级的要求应按照 GB 4208—2008 的规定进行试验。其余的要求应通过检查予以核实。

5.5 复杂或可编程集成电路的确认

5.5.1 总则

本条款用于验证 4.2.10 和 4.2.11 的要求，以及 5.3.1 要求的试验结果报告，包括分析报告。

复杂或可编程集成电路的确认工作，应由独立于负责系统设计、硬件设计和软件设计之外的具备专业资格的检验人员承担。确认后，应出具书面确认报告。

注：该确认提供特殊要求已经达到的独立证明。此过程是为了确认系统的故障在设计上已经予以避免，为了确认安装的程序能够保持产品在生命周期内的安全性能(包括，例如以后的更改)，为了确认 ESPE 的设计满足适应其类型的故障检测要求。

5.5.2 复杂的或可编程的集成电路

对于采用复杂的或可编程的集成电路的 4 型 ESPE，应通过分析确认下列要求：

a) 至少有两条独立的决策通道；

b) 检测通道间的差异和引发锁定状态应在所有适用的故障状态下进行。

5.5.3 集成电路的软件、编程及功能设计

应当验证系统设计和软件开发所依据的质量体系规定的程序和支持性文件符合质量管理体系(如 GB/T 19001—2008)的要求。

质量体系的运行，应通过审核关于开发此类设备所形成的文件记录和为保持产品在生命周期内的质量所建立的程序进行验证。

项目开发文件的适合性、完整性及可追溯性应通过审查得到验证。

应分析安全要求规范，以确认未在其中提到的关于软件、程序设计及功能设计的要求已在系统设计的其他地方提到。

应分析试验计划，以确认能够通过成功地完成试验来验证安全要求规范中的全部要求。

当运行中使用专门的故障检测软件时，应分析测试计划，以确认 B.4.4 中考虑的所有不能被直接的硬件故障模拟所检测到的故障，都通过此软件被检测到。

最新设计版本的测试结果，应当经历过审查。为了确认，应随机选择样品测试项进行重复，并且测试结果应与项目记录中的结果完全一致。

当运行中使用专门的故障检测软件时，模拟故障的测试结果应当证实所规定的覆盖范围被满足，并且应与试验结果报告中所包含的任何分析报告进行比较。

对于运行中使用的软件，应证实全部操作指令程序都储存在处理器不能改写的只读存储器中。

对于可编程装置，验证装置执行其全部可编程功能的方法应被确认。

注 1：错误的或不完整的可编程装置，可能允许此类设备正确执行主要的保护功能而无法执行故障检测功能，尤其是在设计中使用多个相似的可编程装置，且故障检测又是依靠交叉监控时。

用于监控程序流程和/或复杂/可编程装置运行的方法应被确认。此方法应适合于供方声称的安全相关性能等级和使用的系统结构。

注 2：进一步的指导可参见 IEC 61508-3。

5.5.4 试验结果分析报告

当使用分析去判定由 5.3 所要求的任何试验结果时，应对所使用技术的充分性、适用性和有效性进行验证。应通过对随机选定的部分分析进行重复分析的方式对所用方法被执行的正确性进行验证。

6 识别标志和安全使用标志

6.1 总则

按照 GB/T 15706.2—2007 中 6.4 的规定，ESPE 的所有部件应带有下列必要的标志：

——用于明确识别的；

——为了安全使用的。

并应适当提供补充信息：

——永久地标志于 ESPE 上；

——在随机文件如指导手册中；

——在包装上。

ESPE 最适宜部件的外壳上应具有下列永久性标志：

a) 产品标志，包括供方的名称和地址、系列名称或类型、序列编号及制造年份；

b) 检测区的参数，如尺寸；

c) 检测能力；

d) 响应时间；

e) 额定电压，包括相数及有关的频率；

f) 额定输入功率(若大于 25 W 时)或额定电流；

g) IP 代码；

h) 仅对Ⅱ类设备，防止触电保护的分类符号；

i) 危险电压引起危险的警告标志；

j) 符合 4.1.3 规定的 ESPE 的类型。

6.2 专用电源供电的 ESPE

当 ESPE 设计成由外部专用电源供电时，专用电源的型号或类型及与其一起已经测试过的一些详细情况，应永久性地标记在 ESPE 最适宜部件的外壳上，和/或包含在使用说明书中。

6.3 内部电源供电的 ESPE

从内部电源获得供电的 ESPE，若可行时，应在其最适宜部件的外壳上，标记电源保险丝的额定电

流的详细情况。

6.4 调整

当 ESPE 为适应不同的额定电压或不同输入而能调整时，表明对 ESPE 进行调整的电压或输入的标志，应清楚地和容易识别地标注于调整点处。

6.5 外壳

包含有电气装置的外壳都应标上符合 GB 5226.1—2008 中 16.2 规定的警告标志。

6.6 控制装置

6.6.1 开关、指示灯及其他控制器件的标志应标注在其邻近处，而不应标注在可拆卸的部件上，以免由于更换这些部件而使人误解。

6.6.2 控制和指示器件的功能性标识应符合 GB 5226.1—2008 中 16.3 的规定。

6.6.3 任何电源开关的通/断位置应按照 GB 5226.1—2008 中 5.3.1 标记。

6.6.4 在安装期间或之后，预期调整特性的装置应具有调整的方向标志，以明示特性值的增加或减小。亦见 GB/T 4205—2010。

6.7 端子标志

6.7.1 在安装时连接电缆，或在 ESPE 维修后被重新设置的端子，应做标志并附相关示图。

6.7.2 为外部连接所提供的，与 ESPE 相关的且带有用户可更换零部件的端子，应做标志并附相关示图。

6.7.3 所有引入电源的端子应按 GB/T 4026—2010 做标志。

6.7.4 保护性导线的连接点应按照 GB 5226.1—2008 中 8.2.6 的规定做标志。该标志不应放置在螺钉、可拆除的垫圈上及在导线连接或拆开时有可能被拆除的其他零部件上。

6.7.5 当 ESPE 需被连接到两条以上的供电导线上时，应在 ESPE 上固定标志接线图，除非正确的连接方式非常明显。

6.7.6 如 ESPE 采用的电源不止一种，则标志应包括警告内容：在端子罩盖可能被拆开之前，必须切断所有电源。

6.8 标志的耐久性

标志应能承受本部分规定的温度和湿度以及液体如水、肥皂水、机油、汽油等工业环境的影响。

标志应能承受用汽油浸渍的织物和用水浸渍的湿布分别轻擦 15 s。

7 随机文件

ESPE 供方应提供以供方和用户双方同意的语言书写的文件。

随机文件应包含 ESPE 的安装、使用和后续处理所需要的资料，适当时包含下列信息：

a) ESPE 内部生成的电源上不应连接其他装置的说明；

b) 附录 A 中所描述的 ESPE 已经包含的选择性功能的详细情况；

c) 用于连接停止性能监控器(若配备时)的设施的说明；

d) 需要时，2 型 ESPE 使用外部测试信号方法的信息(见 4.2.2.3)；

e) 若配备了调整、操作或进入的安全钥匙或特殊工具，建议由担负责任的或经过授权的人管理控制；

f) 试件的尺寸和类型及测试方法，或检查检测能力和可见指示灯工作的其他方法的说明；

g) 响应时间。

当使用安全相关通信接口时，应对确定整个系统响应时间的方法予以说明；

h) ESPE 额定工作条件包括：

——温度范围；

——湿度；

——电压范围；

——各分部件之间的间隔距离范围和相互连接电缆的最大长度。

i) 防止敏感功能相互干扰的建议；

j) 表明继电器开关动作顺序的框图、功能图表；

k) 所有输入/输出端子的位置；

l) 所有输入/输出端子的额定值和特性；

m) OSSDs(和 SSDs，若配备时)能够对阻性、容性或感性负载转换的最小与最大的电压和电流，及在带有该负载时的最大转换速率，和取决于负载的预期寿命；

n) 用户使用供方推荐的零部件进行维修的资料；

o) 如果适用，有关输入电缆和终端连接的特殊要求；

p) ESPE 总负载/功率的要求；

q) 移动和维修此类设备所需周围空间的详细情况；

r) 由供方规定的用户可替换的零部件一览表；

s) 颜色和编码系统的列表(见 GB 5226.1—2008)；

t) 该设备的外形尺寸；

u) 使用说明书；

v) 检测区的位置和尺寸，和其他功能界限的定义；

w) 为使此类装置正确运行，提供在安装后、维修后或周期性的检查时间表；

x) 确保维持正确运行的常规测试方法和频次；

y) 外壳 IP 等级的说明，或当 ESPE 预期安装在机械控制装置的外壳内时，按照 4.3.4 要求的外壳最低 IP 等级；

z) ESPE 预期特殊应用的清楚说明；

aa) 所推荐的 2 型 ESPE 周期检测之间的最大间隔周期；

bb) 远离 ESPE 安装并与 ESPE 相连的开关、控制装置和指示灯的安装和装配说明；

cc) 重新起动联锁部件应设置于有关危险区的说明；

dd) 敏感功能部件应设置于有关危险区，以及这些部件与危险区之间的安全距离的确定方法(如计算公式)的说明；

ee) 有关 ESPE 怎样与机械控制系统相连接的说明；

ff) 任何必需考虑的特别预防措施的详细情况；

gg) ESPE 所需的空间尺寸；

hh) 支撑和固定 ESPE 的支架的尺寸和定位；

ii) ESPE 的各部件和相邻设施的部件之间的最小间距；

jj) ESPE 至电源的连接方法，和各分立部件之间相互连接的方法，若存在时；

kk) 若使用时，4.2.4.3 规定的固态输出的适当连接信息；

通信接口(4.2.4.4)集成于 ESPE 时，应当提供适当整合所需的工作极限和时序特性；

ll) 提供屏蔽功能(监控的、非监控的、固定的或浮动的)或检测能力的调整功能时，应对这些功能的预期使用做出说明。

附 录 A
（规范性附录）
ESPE 的选择性功能

A.1 总则

ESPE 可能包含附加的功能，或在安全相关控制系统中安排执行功能的装置。ESPE 和专门用来执行这些可选择功能的任何分立装置都应符合本部分的要求。

注：当这些可选择功能不是专门作为 ESPE 的组成部分而是由分立的装置执行时，这些分立的装置应符合其他适当标准（例如，GB/T 16855.1、IEC 61508、IEC 62061）的有关要求。此种情况下，本附录的要求连同其他标准可以作为使用指南。

可选择的装置或功能如下：

——外部装置监控（见 A.2）；

——停止性能监控器（见 A.3）；

——副开关电器（见 A.4）；

——起动联锁（见 A.5）；

——重新起动联锁（见 A.6）；

——抑制（见 A.7）；

——用于重新起动机械的 ESPE（见 A.8）。

下列要求是最低要求，可能不满足所有的应用。作为风险评估的结果，这些要求需要与其他标准（如 GB 5226.1、GB/T 16855.1）的相关要求结合使用。

在由安全相关数据接口为选择性功能提供信号的场合，如果相同的功能由具有适应 ESPE 类型或安全相关功能的安全完整性等级（SIL）要求限度的安全相关通信系统实现，可不考虑 ESPE 硬连接的要求。其他的要求不变。

注：安全完整性等级要求限度 SIL3 适合于 4 型 ESPE，SIL2 适合于 3 型 ESPE，SIL1 适合于 2 型 ESPE。

A.2 外部装置监控（EDM）

A.2.1 功能要求

EDM 应提供对外部触点（如 FSDs 或 MPCEs）状态监控的方法。

当正受 EDM 监控中的某个装置被检测为错误状态时，ESPE 应进入锁定状态。

A.2.2 故障状态的要求

ESPE 应按照 4.2.2 对 EDM 的故障做出响应。

A.2.3 验证

应通过检查及试验进行如下验证：

——对于预期使用 EDM 的装置的监控，ESPE 中应提供必要的措施；

——当任何一个被监控的装置正处于错误状态时，ESPE 应进入锁定状态；

——ESPE 应根据 4.2.2 对 EDM 出现的故障做出响应。

A.2.4 使用信息

ESPE 供方应提供用于 EDM 连接到适当装置上的说明，同时也应规定需安装 EDM 要使用的任何装置的类型。有些场合对受监控的装置要求特殊性能(如机械地连接的触头，复式输入、N/O、N/C)，对这些应做出规定。

除非外部触点的响应时间受到监控，否则，使用信息应提示需要采取监控触点响应时间的外部措施。

A.3 停止性能监控器(SPM)

A.3.1 功能要求

SPM 应对 ESPE 提供有关机械危险部件进入停止状态或恢复到安全状态所用时间或运行量的信号。当 SPM 的信号显示预置的停止性能极限已被超出时，ESPE 应进入锁定状态。

对 4 型 ESPE，SPM 应提供至少两个信道至 ESPE。每个信道都应能够引发 ESPE 的锁定状态。

SPM 应使用自动的停止性能测试，以监控整套系统的停止性能。

当敏感装置实际地或模拟地触发时，SPM 应能立即响应来自 ESPE 的信号，开启自动的停止性能测试。

SPM 的预置极限可进行调整的任何方法，应要求使用钥匙、关键字或专用工具。

A.3.2 故障状态的要求

在下列任何条件下，ESPE 都应进入锁定状态：

——当不能进行或不能完成自动测试时；

——当到达停止性能监控器的运动传递失效时，或当复式传递装置中的任一装置失效时；

——当停止性能监控器与 ESPE 分离时。

A.3.3 验证

通过检查进行下列验证：

——当停止性能预置极限被超出时，SPM 输出的信号将使 ESPE 进入锁定状态；

——使用 4 型 ESPE 时，从 SPM 到 ESPE 应至少拥有两个独立的信号源，且任一信号源失效均导致 ESPE 进入锁定状态；

——作为对 ESPE 信号的响应，SPM 开启自动测试；

——敏感功能实际地或模拟地触发，ESPE 开启自动的 SPM 测试；

——任何调整方法都要求使用钥匙、关键字或专用工具；

——当自动测试不能进行或没有完成时，ESPE 进入锁定状态；

——当任何一种运动装置的传递出现失效时，ESPE 进入锁定状态；

——当 SPM 从 ESPE 或从安全相关的控制系统中分离时，ESPE 进入锁定状态；

——标志符合 A.3.4 的规定并正确无误。

A.3.4 标志

供方应将 SPM 贴上永久性标志。标志包含下列信息：

——供方的名称和地址；

——型号和系列号；

——SPM 配用的 ESPE 的型号；

——装置的精度。

A.4 副开关电器(SSD)

A.4.1 功能要求

当 ESPE 的电源被切断或当 ESPE 处于锁定状态时,SSD 应处于断开状态。

SSD 执行安全相关功能的能力应通过自动地测试进行检查,此测试应在 ESPE 接通电源且在 OSSD(s)进入接通状态之前进行。

A.4.2 故障状态的要求

如果 A.4.1 所说的自动测试表明 SSD 无法进入断开状态时,OSSD(s)应仍保持断开状态。

A.4.3 验证

通过检查和试验,进行下列验证:

——故障情况下,如当 SSD 被约束在保持导通状态且当 ESPE 通电时,OSSD(s)应保持在断开状态,即使进行复位时;

——ESPE 在锁定条件下,SSD 处于断开状态。

A.5 起动联锁

A.5.1 功能要求

当电源接通,或被中断后再恢复时,起动联锁应阻止 OSSD(s)进入接通状态。

OSSD(s)的断开状态,应一直保持到起动联锁被人工(如通过开关操作,或通过对敏感装置的触发和撤销触发)复位到接通时。

在锁定状态下,起动联锁的复位不应使 OSSD(s)恢复到接通状态。

A.5.2 故障状态的要求

引起起动联锁进入或永久保持接通状态的起动联锁的失效,应使 ESPE 进入或保持锁定状态。

A.5.3 验证

通过检查和试验进行下列验证:

——起动联锁装置处于断开状态时,OSSD(s)处于断开状态;

——当电源接通时,OSSD(s)的断开状态一直持续到人工操作此起动联锁装置时;

——当电源的中断时间足以使 OSSD(s)进入断开状态后,再当恢复供电时,OSSD(s)应保持断开状态,直到对起动联锁装置进行人工操作时;

——在锁定状态下,对起动联锁的复位不允许 OSSD(s)进入接通状态;

——起动联锁装置出现故障时,开启锁定状态。

A.5.4 指示

起动联锁装置阻止 OSSD(s)进入接通状态时,配备的黄色指示灯应点亮。

A.6 重新起动联锁

A.6.1 功能要求

下列情况下，重新起动联锁装置应阻止 OSSD(s)进入接通状态：

——当机械运行正处于其工作循环的危险阶段时，检测区被中断；

——当机械处于自动或半自动方式时，检测区被中断；

——当机械的工作模式或操作方式改变时。

这种联锁状态应一直持续到重新起动联锁装置被人工复位时。然而，当敏感装置被触发时，重新起动联锁装置应不可能复位。

A.6.2 故障状态的要求

不能满足 A.6.1 的功能要求时，应导致 ESPE 进入锁定状态。

A.6.3 验证

通过检查和试验进行下列验证：

——当重新起动联锁装置处于断开状态时，OSSD(s)处于断开状态；

——当敏感装置被触发期间，重新起动联锁装置将不能复位到接通状态；

——危险机械运行期间敏感装置触发时，重新起动联锁装置进入断开状态；

——当机械的工作模式或操作方式改变时，重新起动联锁装置进入断开状态；

——当重新起动联锁装置失效时，则开启锁定状态。

A.6.4 指示

重新起动联锁装置阻止 OSSD(s)进入接通状态时，配备的黄色指示灯应点亮。

A.7 抑制

A.7.1 功能要求

A.7.1.1 当 ESPE 处于抑制状态，对敏感装置触发时，OSSD(s)应保持接通状态。

A.7.1.2 应提供至少两个独立的硬连接的信号源来用以开启抑制功能。OSSD(s)已处于断开状态时，抑制功能应不能被开启。

A.7.1.3 抑制功能仅应通过抑制信号的正确顺序和/或时序才能被开启。抑制信号出现冲突时，ESPE 应不允许抑制发生。

A.7.1.4 应提供至少两个独立硬连接抑制信号源用以终止该功能。一旦任意一个抑制信号改变状态时，抑制功能则应终止。抑制功能的终止不应仅依赖于 ESPE 检测区的无遮挡状态。

注：开启和停止抑制功能的信号源可以是同一个。

A.7.1.5 在抑制发生期间，抑制信号应连续地存在。当抑制信号不能连续存在，顺序出错或/和预定时限超出时，应导致进入锁定状态或重新起动联锁状态。

注：对于某些应用场合(例如传送机械和包装机械)，抑制能够通过旁路(覆盖)功能予以提供。为了清除机械设备上抑制传感器所在区域的堵塞物，该功能允许抑制功能被进一步使用。只有当至少有一个抑制传感器被触发时，才应有可能触发该旁路功能。出现单一故障时应不能开启该旁路功能。该旁路功能在正确的抑制信号顺序被识别，预定时限超出时，或者当确定的抑制区域是畅通的和正常运行能恢复时，应立即自动被取消。对于旁路功能的触发应使用持续作用式装置，该装置应被放置在操作者能够看得到危险点的位置处。

A.7.2 故障状态的要求

按照 4.2.2 的规定，抑制功能中的故障应当被检测，至少不允许有另外的抑制状况发生。

A.7.3 验证

通过检查和测试验证：

——在抑制状态下，触发敏感装置时，OSSD(s)保持接通状态。

——有两个独立的硬连接的抑制信号源来开启和终止抑制功能，并且无论何时，无效的信号组合出现时，抑制状态被阻止。

——对于 2 型 ESPE，任何能够导致抑制状态一直持续的失效，能够通过周期检测被显示。这类失效被检测到时，抑制状态的持续状况被阻止。

——当两个“停止抑制”信号中的任意一个改变状态时，抑制功能即终止。

A.7.4 指示

应提供抑制状态的信号或指示灯(某些应用中，抑制的指示信号是必需的，见 GB/T 16855.1—2008 的 5.2.5)。

A.8 用于重新起动机械的 ESPE

A.8.1 总则

除了作为保护装置使用之外，ESPE 还能用于起动机械设备运行。可使用的起动操作方式如下：

——对敏感装置一次触发和撤销触发重新起动机械设备运行，被称为单次中断；

——对敏感装置两次连续地触发和撤销触发重新起动机械设备运行，被称为双重中断。

这一选择功能作为 ESPE 的组成部分被提供时，还应对 ESPE 提供 A.5 规定的起动联锁功能和 A.6 规定的重新起动联锁功能。

A.8.2 功能要求

a) 当 ESPE 的电源接通或中断后再恢复时，在起动联锁装置复位之前，应不可能使用 A.8.1 所述的任何一种操作方式；

b) 在危险运行期间敏感装置触发后，在重新起动联锁装置复位之前，应不可能使用 A.8.1 所述的任何一种操作方式；

c) 对于机械设备运行的连续重新起动，只应在限定的时间内方可使用 A.8.1 所述的任何一种操作方式；

d) 当选择双重中断方式执行重新起动时，在任何顺序的事件或动作情况下，都应不可能通过单次中断方式实现重新起动；

e) 如果超出了 c)中所述的限定时间，在重新起动联锁装置复位之前，机械下一步的重新起动应是不可能的；

f) 当重新起动方式改变之后，在重新起动联锁装置复位之前，使用 A.8.1 所述的任何一种操作方式重新起动机械应是不可能的；

g) 应提供通过外部方式对控制 c)所述限定周期的定时器进行复位的装置；

h) 对于定时器的调整方法，应要求使用钥匙、关键字或专用工具。

注：连续的重新起动所允许的时间长度，对于循环时间小于 5 s 的机械设备，不应超过 30 s。

A.8.3 故障状态的要求

附录B所列的任何导致机械重新起动方式改变的故障，应至少导致起动联锁或重新起动联锁起作用。

A.8.4 验证

通过检查和试验进行下列验证：

——ESPE的电源接通或中断了再恢复后，在起动联锁装置复位之前，不可能使用A.8.1所述的任何一种操作方式；

——在危险运行期间敏感装置触发后，在重新起动联锁装置复位之前，不可能使用A.8.1所述的任何一种操作方式；

——只应在限定的时间内使用A.8.1所述的任一操作方式才能连续重新起动机械；

——当选择双重中断方式执行重新起动时，在任何顺序的事件或动作情况下，都不能通过单次中断方式实现重新起动；

——当重新起动方式改变之后，在重新起动联锁装置复位之前，不可能通过A.8.1所述的任何一种操作方式使机械重新起动；

——提供了由外部方式对控制上述限定周期的定时器进行复位的装置；

——定时器的调整应在需要使用工具才能进入的外壳中；

——附录B所列的导致机械重新起动方式改变的故障，应至少引起起动联锁或重新起动联锁起作用。

附 录 B
（规范性附录）
影响 ESPE 的电气设备的单一故障一览表

本附录中的各表根据 5.3 的规定运用。

B.1 导线和连接器

B.1.1 导线/电缆故障及排除方法见表 B.1。

表 B.1 导线/电缆故障及排除方法

考虑到的故障	排除方法
任何两导线间短路	导线使用永久式连接（例如不使用插头插座组合）并保护导线防止外部损坏，例如通过电缆套管、铠装
	使用独立多芯电缆中的导线
任一导线开路	无
任一导线与外露可导电部分或保护导线之间短路	无
任何导线与带电部分之间短路	导线通过多接点端子集支撑和/或端接，以防止来自例如由于靠近导线端接点的机械失效而发生的故障

B.1.2 印刷电路板和印刷电路部件故障及排除方法见表 B.2。

表 B.2 印刷电路板和印刷电路部件故障及排除方法

考虑到的故障	排除方法
两邻近导线间短路	——基本材料应符合 IEC 60249-2 的规定，爬电距离和电气间隙至少应符合 GB/T 16935.1—2008 规定的污染等级 2/安装类别 3；和 ——组装的电路板应安装在防护等级至少为 IP54 的外壳中，印刷板上所有导体路径均应覆盖抗老化清漆或保护层
任何导体的路径开路	无

B.1.3 接线座故障及排除方法见表 B.3。

表 B.3 接线座故障及排除方法

考虑到的故障	排除方法
邻近端子间短路	使用的端子应符合相关的 IEC 标准，并满足 GB 5226.1—2008 中的 13.1.1 和 13.1.2 的要求
个别端子的开路	无

B.1.4 多插脚连接器(如电缆、继电器、集成电路用的插头和插座)故障及排除方法见表 B.4。

表 B.4 多插脚连接器(如电缆、继电器、集成电路用的插头和插座)故障及排除方法

考虑到的故障	排除方法
两邻近插脚间短路	邻近的插脚满足 B.1.2 的要求
通过机械方法不能防止连接器互换和误插	无
个别连接器插脚开路	无

B.2 开关

B.2.1 机电式开关、手动操作开关和按钮(如复位操动器、自锁开关)故障及排除方法见表 B.5。

表 B.5 机电式开关、手动操作开关和按钮故障及排除方法

考虑到的故障	排除方法
触头不闭合	无
触头不断开	无
彼此绝缘的邻近触头短路	此处所用开关应符合 IEC 60947-5-1:1997(见 K.7.1.4.6.1)的规定,变得松动的导电部件不能跨越触头之间的绝缘体
转换触头间的 3 个端子间同时短路	此处所用开关应符合 IEC 60947-5-1:1997(见 K.7.1.4.6.1)的规定,变得松动的导电部件不能跨越触头之间的绝缘体

B.2.2 机电式电器(如继电器、接触器)故障及排除方法见表 B.6。

表 B.6 机电式电器(如继电器、接触器)故障及排除方法

考虑到的故障	排除方法
不释放(例如由于机械故障,所有触头保持通电状态)	无
不导通(例如由于机械故障、线圈断路,所有触头保持断开状态)	无
个别触头不断开	无
个别触点不闭合	无
3 个转换触头的端子之间同时短路	此处爬电距离和电气间隙至少应符合 GB/T 16935.1—2008 规定的污染等级 2/安装类别 3,变得松动的导电部件不能跨越触头之间的绝缘体
在触头电路之间、触头与线圈端子之间发生短路	此处爬电距离和电气间隙至少应符合 GB/T 16935.1—2008 规定的污染等级 2/安装类别 3,变得松动的导电部件不能跨越触头之间及触头与线圈之间的绝缘体
常开和常闭触点同时闭合	使用强制驱动(或机械地连接)的触头,可以排除常开和常闭触头的同时闭合

B.3 分立电气元件

B.3.1 变压器故障及排除方法见表 B.7。

表 B.7 变压器故障及排除方法

考虑到的故障	排除方法
单个绕组开路	无
绕组之间短路	绕组按照 GB 4943 的要求隔离

B.3.2 固定或可调电感器故障及排除方法见表 B.8。

表 B.8 固定或可调电感器故障及排除方法

考虑到的故障	排除方法
断路	无
短路	扼流线圈是单层的、涂瓷漆的或密封的，并采用轴向线连接和轴向安装
变值：$0.5L_N<L<L_N$+公差 其中 L_N 是标称电感值 或者，对于可调电感器 变值：$L_{min}<L<L_{max}$	无

B.3.3 电阻器故障及排除方法见表 B.9。

表 B.9 电阻器故障及排除方法

考虑到的故障	排除方法
开路	无
短路	具有防止破损绕线松散保护的薄膜型或线绕型电阻器，采用轴向线连接、轴向安装并涂漆； 使用表面贴装技术的无引线电阻器
变值：$0.5R_N<R<2R_N$ 其中 R_N 是标称电阻值	无

B.3.4 电阻器网络故障及排除方法见表 B.10。

表 B.10 电阻器网络故障及排除方法

考虑到的故障	排除方法
单个电阻器开路	无
任何两个接点之间短路	无
单个电阻器变值：$0.5R_N<R<2R_N$ 其中 R_N 是标称电阻值	无

B.3.5 电位器故障及排除方法见表 B.11。

表 B.11 电位器故障及排除方法

考虑到的故障	排除方法
每个单独的连接线开路	无
所有连接线之间同时短路	无
任何两个连接线之间的阻值变值：$0.5R_p<R<2R_p$ 其中 R_p 是标称值	无

B.3.6 固定或可调电容器故障及排除方法见表 B.12。

表 B.12 固定或可调电容器故障及排除方法

考虑到的故障	排除方法
开路	无
变值：$0.5C_N<C<C_N$+公差 其中 C_N 是标称值或设定值	无

B.4 固态电气元件

B.4.1 分立半导体元件[如二极管、晶体管、三端双向晶闸管、稳压器、光电晶体管和发光二极管(LED)]故障及排除方法见表 B.13。

表 B.13 分立半导体元件故障及排除方法

考虑到的故障	排除方法
任何连接的开路	无
任何两个连接之间短路	无
所有连接之间短路	无
变化的电气特性导致安全相关的输出信号超出额定信号范围上限值或下限值的 25%	无

B.4.2 光耦合器故障及排除方法见表 B.14。

表 B.14 光电耦合器故障及排除方法

考虑到的故障	排除方法
单个连接的开路	无
任何两个连接之间短路： ——输入连接线(发射器)； ——输出连接线(接收器)； ——在输入和输出之间	 无 无 元件应具有承受 GB/T 16935.1—2008 表 F.1 规定的过电压类别Ⅲ冲击电压能力

表 B.14（续）

考虑到的故障	排除方法
变化的电气特性导致安全相关的输出信号超出额定信号范围上限值或下限值的 25%	无

B.4.3 简单集成电路故障及排除方法见表 B.15。

表 B.15 简单集成电路故障及排除方法

考虑到的故障	排除方法
每个单独的连接开路	无
任何两个连接之间短路	无
在所有的输入端和输出端，或者个别地或者同时地存在持久不变的“0”或“1”信号（即负极或正极与分离的输入端或非连接的输出端相连短路）	无
输出的寄生振荡 注：测试频率和脉冲占空比的选择取决于转换技术和外部电路。测试时，激励级存在的问题是被隔离的。	无
变化的电气特性导致安全相关的输出信号超出规定信号范围上限值或下限值的 25%	无

B.4.4 复杂集成电路或可编程集成电路故障及排除方法见表 B.16。

表 B.16 复杂集成电路或可编程集成电路故障及排除方法

考虑到的故障	排除方法
部分或全部功能（见 4.2.10 和 4.2.11）中的缺陷可能是： ——处于静态； ——改变逻辑； ——依赖于比特顺序	无
由于集成电路的复杂性（见 4.2.10 和 4.2.11），硬件中未被检测到的失效未被注意到	无
存储和处理元件中的缺陷未能通过完全执行程序显露出来	无
B.4.3 所列的各种故障	见 B.4.3

B.5 电动机

电动机故障及排除方法见表 B.17。

表 B.17 电动机故障及排除方法

考虑到的故障	排除方法
电动机停止	无
速度高于额定值	无
速度低于额定值	无

附 录 C
（资料性附录）
符合性评估

本标准（GB/T 19436）包含了产品与标准的符合性评价条件，然而这些要求却是高度地依赖于测试设备和专家的分析。为了对电敏保护设备（ESPE）相对本标准和至少是本标准的某一部分的符合性进行恰当地评定，应该实施由第三方依据本标准的要求进行测试和评价的过程。第三方应是经过认证的具有检测这些类型设备资质的实验室。该测试和评价过程独立于本标准的规范性要求，并且可能需要通过法律或法规规定进行实施，或通过合同约定进行实施。

参 考 文 献

[1] ISO 9000-3:1997 Quality management and quality assurance standards—Part 3:Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of software

[2] IEC 60204-1:1997 Safety of machinery—Electrical equipment of machines—Part 1:General requirement

[3] IEC 60812:1985 Analysis techniques for system reliability—Procedure for failure mode and effects analysis (FMEA)

[4] IEC 61025:1990 Fault tree analysis (FTA)

[5] IEC/TS 62046 Safety of machinery—Application of protective equipment to detect the presence of persons

中 华 人 民 共 和 国
国 家 标 准
机械电气安全 电敏保护设备
第 1 部分：一般要求和试验
GB/T 19436.1—2013/IEC 61496-1:2008
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100013)
北京市西城区三里河北街 16 号(100045)
网址 www.spc.net.cn
总编室：(010)64275323 发行中心：(010)51780235
读者服务部：(010)68523946
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 3 字数 84 千字
2013 年 12 月第一版 2013 年 12 月第一次印刷
*
书号：155066·1-47807 定价 42.00 元

GB/T 19436.1-2013

GB/T 19436.1—2013/IEC 61496-1:2008