GB/T 12668.502-2013 调速电气传动系统 第 5-2 部分：安全要求、功能

GB/T 12668.502-2013 调速电气传动系统 第 5-2 部分：安全要求、功能为 GB 12668 的第 5-2 部分。

GB/T 12668.502-2013 调速电气传动系统 第 5-2 部分：安全要求、功能使用翻译法等同采用 IEC 61800-5-2:2007《调速电气传动系统 第 5-2 部分：安全要求 功能》。

GB/T 12668.502-2013 调速电气传动系统 第 5-2 部分：安全要求、功能规定了从功能安全方面考虑，对电气传动系统（安全相关）[PDS(SR)]的设计开发、集成和验证，详述了要求，给出了建议。

GB/T 12668.502-2013 调速电气传动系统 第 5-2 部分：安全要求、功能适用于《调速电气传动系统》中其他设计调速电气系统的标准。

GB/T 12668.502-2013 调速电气传动系统 第 5-2 部分：安全要求、功能仅当 PDS（SR）的功能安全被认定和 PDS（SR）以高要求或连续模式（见 3.10）操作时适用。对低要求应用，见 IEC 61508。

GB/T 12668.502-2013 调速电气传动系统 第 5-2 部分：安全要求、功能是一个产品标准，阐述了有关 IEC 61508 结构体系中 PDS（SR）安全相关考虑，介绍了 PDS（SR）作为安全子系统的要求。本部分意在促进 PDS（SR）的电气/电子/可编程电子元件（E/E/PE）来实现 PDS 安全功能的安全特性。

ICS 29.020
K 62

中华人民共和国国家标准

GB/T 12668.502—2013/IEC 61800-5-2:2007

调速电气传动系统 第5-2部分:安全要求 功能

Adjustable speed electrical power drive systems—Part 5-2:Safety requirements—Functional

(IEC 61800-5-2:2007,IDT)

2013-11-12 发布　　2014-08-07 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 12668《调速电气传动系统》分为以下几个部分：

——第1部分：一般要求　低压直流调速电气传动系统额定值的规定；

——第2部分：一般要求　低压交流变频电气传动系统额定值的规定；

——第3部分：电磁兼容性要求及其特定的试验方法；

——第4部分：一般要求　交流电压1 000 V以上但不超过35 kV的交流调速电气传动系统额定值的规定；

——第5部分：安全要求；

——第6部分：确定负载工作制类型和相应电流额定值的导则；

——第7部分：电气传动系统的通用接口和使用规范；

——第8部分：电源接口电压的规范。

本部分是GB/T 12668的第5-2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分使用翻译法等同采用IEC 61800-5-2:2007《调速电气传动系统　第5-2部分：安全要求　功能》。

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 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)]；

——GB/T 24339(所有部分)　轨道交通　通信、信号和处理系统　[IEC 62280(所有部分)]。

本部分做了如下编辑性修改：

——小数点符号用“.”代替“,”；

——对于无编号的列项，第一层次的列项之前用破折号；

——删除了国际标准的前言。

本部分由中国电器工业协会提出。

本部分由全国电力电子学标准化技术委员会(SAC/TC 60)归口。

本部分起草单位：天津电气传动设计研究所、深圳市英威腾电气股份有限公司、上海澳通韦尔电力电子有限公司、北京合康亿盛变频科技股份有限公司、希望森兰科技股份有限公司、北京利德华福电气技术有限公司、深圳市库马克新技术股份有限公司、哈尔滨九州电气股份有限公司、山东新风光电子科技发展有限公司、中冶赛迪电气技术有限公司、山东泰开自动化有限公司、广州智光电气股份有限公司、上海雷诺尔科技股份有限公司、北京ABB电气传动系统有限公司、国家电控配电设备质量监督检验中心、广东华拿东方能源有限公司。

本部分主要起草人：赵相宾、董桂敏、吴洪波、董瑞勇、蒲安康、杜心林、任光法、倚鹏、罗自勇、丁兆国、赵树国、张胜民、李凯、许贤昶、陈国成、温湘宁、王书琴、苏勇华、柴青、董天舒。

调速电气传动系统
第5-2部分:安全要求
功能

1 范围

GB/T 12668的本部分规定了从功能安全方面考虑,对电气传动系统(安全相关)[PDS(SR)]的设计开发、集成和验证,详述了要求,给出了建议。

本部分适用于《调速电气传动系统》中其他涉及调速电气传动系统的标准。

注1:术语"集成"是对PDS(SR)本身而言,而不是并入安全相关应用。

本部分仅当PDS(SR)的功能安全被认定和PDS(SR)以高要求或连续模式(见3.10)操作时适用。对于低要求应用,见IEC 61508。

本部分是一个产品标准,阐述了有关IEC 61508结构体系中PDS(SR)安全相关考虑,介绍了PDS(SR)做为安全相关子系统的要求。本部分意在促进PDS(SR)的电气/电子/可编程电子元件(E/E/PE)来实现PDS安全功能的安全特性。

PDS(SR)的制造商和供应商通过使用本部分规范性要求,向用户(控制系统集成商、成套装备设计者等)展示他们设备的安全特性。通过运用IEC 61508的原理和在其相关领域中的实施(例如IEC 61511、IEC 61513、IEC 62061)或ISO 13849,有助于将PDS(SR)纳入安全相关控制系统。

依照本部分满足IEC 61508中PDS(SR)所需的所有要求。

本部分不说明以下要求:

——特定应用的危险和风险分析;

——特定应用的安全功能的识别;

——安全完整性等级(SIL)对那些安全功能的初始分配;

——除接口配置以外的传动设备;

——次生危害(例如生产和制造过程中的失效);

——在IEC 61800-5-1中包括的电气、热和能量的安全考虑;

——PDS(SR)生产过程;

——PDS(SR)信号和指令的有效性。

注2:PDS(SR)的功能安全要求随应用而定,并且必须视为设备整体风险评估的一部分。PDS(SR)供应商不对传动设备负责的地方,装备设计者负责风险评估并且明确说明PDS(SR)的功能和安全整体要求。

注3:纵然恶意的行为能影响PDS(SR)的功能安全,本部分中不考虑担保问题。

本部分仅适用不大于SIL3的SIL的安全功能的PDS(SR)。

图1给出了本部分中所考虑的PDS(SR)的功能元件。

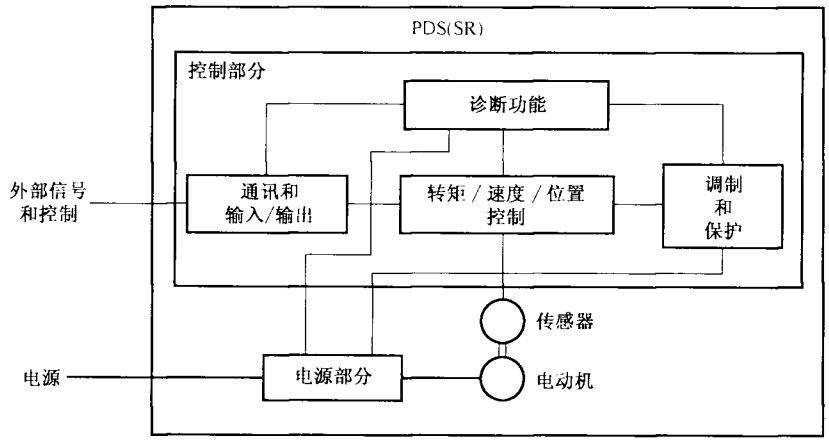


图 1 PDS(SR)的功能元件

图 1 是 PDS(SR)的逻辑表示，而不是物理描述。

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 20438.1—2006 电气/电子/可编程电子安全相关系统的功能安全 第 1 部分：一般要求(IEC 61508-1:1998,IDT)

GB/T 20438.2—2006 电气/电子/可编程电子安全相关系统的功能安全 第 2 部分：电气/电子/可编程电子安全相关系统的要求(IEC 61508-2:2000,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 20438.6—2006 电气/电子/可编程电子安全相关系统的功能安全 第 6 部分：GB/T 20438.2和 GB/T 20438.3 的应用指南(IEC 61508-6:2000,IDT)

GB/T 20438.7—2006 电气/电子/可编程电子安全相关系统的功能安全 第 7 部分：技术和措施概述(IEC 61508-7:2000,IDT)

IEC 60204-1 机械安全 机械电气设备 第 1 部分：通用技术条件(Safety of machinery—Electrical equipment of machines—Part 1:General requirements)

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 61508-5 电气/电子/可编程电子安全相关系统的功能安全 第 5 部分：确定安全完整性等级的方法示例(Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 5:Examples of methods for the determination of safety integrity levels)

IEC 61800-1 调速电气传动系统 第 1 部分：一般要求 低压直流调速电气传动系统 额定值的规定(Adjustable speed electrical power drive systems—Part 1:General requirements—Rating specifications for low voltage adjustable speed d. c. power drive systems)

IEC 61800-2 调速电气传动系统 第 2 部分：一般要求 低压交流变频电气传动系统额定值的规定(Adjustable speed electrical power drive systems—Part 2:General requirements—Rating specifications for low voltage adjustable frequency a. c. power drive systems)

IEC 61800-3 调速电气传动系统 第 3 部分：产品的电磁兼容性标准及其特定的试验方法(Ad-

justable speed electrical power drive systems—Part 3:EMC requirements and specific test methods)

IEC 61800-4 调速电气传动系统 第4部分:一般要求 交流电压1 000 V以上但不超过35 kV的交流调速电气传动系统额定值的规定(Adjustable speed electrical power drive systems—Part 4: General requirements—Rating specifications for a. c. power drive systems above 1 000 V a. c. and not exceeding 35 kV)

IEC 61800-5-1:2003 调速电气传动系统 第5-1部分:安全要求 电气,热和能量(Adjustable speed electrical power drive systems Part 5-1:Safety requirements—Electrical,thermal and energy)

IEC 62280(所有部分) 铁路应用 通信,信号和处理系统(Railway applications—Communication,signalling and processing systems)

3 术语和定义

下列术语和定义适用于本文件。

注:定义按字母顺序排列,见表1。

表1 定义顺序表

术语编号	术语	术语编号	术语
3.1	共同原因失效	3.14	安全失效
3.2	危险失效	3.15	安全失效分数
3.3	诊断覆盖率	3.16	[PDS(SR)的]安全功能
3.4	诊断试验	3.17	安全完整性
3.5	故障反应功能	3.18	安全完整性等级
3.6	功能安全	3.19	安全相关系统
3.7	危险	3.20	安全要求规范
3.8	装置	3.21	安全完整性等级能力
3.9	运行时间	3.22	子系统
3.10	操作模式	3.23	系统性失效
3.11	电气传动系统(安全相关)	3.24	系统安全完整性
3.12	PFH	3.25	确认
3.13	检验试验	3.26	验证

3.1

共同原因失效 common cause failure

一种失效,它是一个或多个事件导致的结果,在多通道系统中引起两个或多个分离通道同时失效,从而导致系统失效。

[GB/T 20438.4—2006,定义3.6.10]

3.2

危险失效 dangerous failure

使安全相关系统处于潜在的危险或丧失功能状态的失效。

[GB/T 20438.4—2006,定义3.6.7]

3.3

诊断覆盖率 diagnostic coverage;DC

进行自动诊断试验而导致的硬件危险失效概率的降低部分。

[GB/T 20438.4 2006,定义 3.8.6]

注 1:这也可表达为检测到的危险失效率的总和 λ_{DD} 与总的危险失效率的总和 λ_D 的比值,即 $DC=\sum\lambda_{DD}/\sum\lambda_D$;

注 2:诊断覆盖率可能存在于整个或部分安全相关系统。例如,诊断覆盖率可能存在于传感器和/或逻辑系统和/或终端元件。

3.4

诊断试验 diagnostic test

意在检测故障或危险并且当故障或危险检测到时产生特定输出信息或动作的试验。

3.5

故障反应功能 fault reaction function

当 PDS(SR)内部可能引起安全功能损失的故障或失效被检测到的时候,此功能开启。此功能意在维护装置的安全状况,防止装置出现危险情况。

3.6

功能安全 functional safety

与 EUC(受控设备)和 EUC 控制系统有关的整体安全的组成部分,它取决于电气/电子/可编程电子安全相关系统、其他技术安全相关系统和外部风险降低设施功能的正确行使。

[GB/T 20438.4—2006,定义 3.1.9]

注:本部分仅考虑依 PDS(SR)的正确工作而定的功能安全定义的那些方面。

3.7

危险 hazard

潜在的危害源。

[ISO/IEC 导则 51:1999,定义 3.5]

注 1:该术语包括短时间内对人身的危险(例如,火和爆炸),也包括那些对人体健康有长期影响的危险(例如,有毒物质的释放)。

注 2:IEC 61508-4:1998 的修改版定义危险情况为:一种形势,在其中人员、财产或环境暴露于一个或多个危险或危险事件下。

3.8

装备 installation

至少包括 PDS(SR)和被传动设备两者的一台或数台设备。

3.9

运行时间 mission time

在整个生命周期中规定的 PDS(SR)的累积运行时间。

3.10

操作模式 mode of operation

根据其要求产生的频率,安全相关系统被使用的方式。

注 1:改写 GB/T 20438.4—2006,定义 3.5.12。

注 2:IEC 61508 中考虑了两种操作模式:

——低要求模式:在这种模式下,对一个安全相关系统提出操作要求的频率不大于每年一次和不大于 2 倍的检验试验频率。

——高要求或连续模式:在这种模式下,对一个安全相关系统提出操作要求的频率大于每年一次或大于 2 倍的检验试验频率。

低要求操作模式通常被认为与 PDS(SR)应用无关。因此,在本部分中,仅考虑 PDS(SR)s 在高要求或连续模

式下操作。

注3：要求模式是指为了将装备转变成指定的状态，仅按要求执行的安全功能。

注4：连续模式是指连续工作的安全功能，例如，PDS(SR)连续地控制装备和它的功能的(危险)失效可能导致危险。

3.11

电气传动系统(安全相关) PDS(SR)

适用于安全相关应用的调速电气传动系统。

3.12

PFH

每小时危险随机硬件失效的概率。

注：在IEC 62061:2005中，使用缩写PFH_D。

3.13

检验试验 proof test

安全相关系统中进行周期试验检测故障，因此，如果必要，系统可恢复为“初始”的状态或实际上尽可能的接近这种状态。

注：检验试验通常用于承担披露没有被诊断试验检测出的危险故障。检验试验的效果取决于系统修复得“初始”状态的接近程度。为了使检验试验充分有效，有必要100%地检测所有危险故障。尽管在实际中，除了不太复杂的系统，100%检测出来是不容易做到，但这应作为目标。

3.14

安全失效 safe failure

不可能使安全相关系统处于潜在的危险或丧失功能状态的失效。

[GB/T 20438.4—2006，定义3.6.8]

3.15

安全失效分数 safe failure fraction;SFF

子系统的平均安全失效率加检测到的平均危险失效率与子系统总平均失效率之比。

$$SFF=(\sum\lambda_S+\sum\lambda_{DD})/(\sum\lambda_S+\sum\lambda_D)$$

注：见GB/T 20438.2—2006附录C。

3.16

[PDS(SR)的]安全功能 safety function[of a PDS(SR)]

由一个PDS(SR)整体或部分实现，具有特定安全性能的功能，以维持装备的安全状态或防止出现在装备上的危险状态。

3.17

安全完整性 safety integrity

在规定的所有条件下，PDS(SR)令人满意的实现所要求的安全功能的概率。

注1：PDS(SR)的安全完整性等级越高，PDS(SR)不能实现所要求的安全功能的概率就越低。

注2：安全完整性同PDS(SR)所执行的每个安全功能可能不一样。

注3：改写GB/T 20438.4—2006，定义3.5.2。

3.18

安全完整性等级 safety integrity level;SIL

一种离散的等级(四种可能等级之一)，用于规定分配(整体或部分)给PDS(SR)的安全功能的安全完整性要求。

注1：SIL4是安全完整性的最高水平，SIL1是安全完整性最低水平。

注2：本部分不考虑SIL4，因为通常它与PDS(SR)s相关的风险降低要求不相关。适用于SIL4的要求，见IEC 61508。

注3：改写GB/T 20438.4—2006，定义3.5.6。

3.19

安全相关系统 safety-related system

包括以下两种系统：

——执行达到或维持 EUC 的安全状态所需及必须的安全功能；和

——通过其自身，或其他电气/电子/可编程电子安全相关系统，或安全相关技术系统或外部风险降低设施，来实现必须的安全功能所需的安全完整性。

3.20

安全要求规范 safety requirements specification；SRS

包含必须由 PDS(SR)执行的安全功能的所有要求的说明。

3.21

安全完整性等级能力 safety integrity level capability；SIL capability

在系统安全完整性和硬件安全完整性结构约束方面，通过 PDS(SR)的设计能实现的安全完整性等级的最大值。

注：PDS(SR)预期执行的每一个指定的安全功能可与一个不同的 SIL 能力相联系。

3.22

子系统 subsystem

安全相关系统顶层结构设计的一部分，它的失效会导致安全功能的失效。

注 1：PDS(SR)本身可以是一个子系统，也可以是由很多独立的子系统组成的，由这些子系统组成整体执行安全功能。一个子系统可以有多个通道。

注 2：PDS(SR)子系统可以是编码器、电源部分、控制部分(见图 1)。

3.23

系统性失效 systematic failure

原因确定的失效，只有对设计或制造过程、操作规程、文档或其他相关因素进行修改后，才有可能排除这种失效。

注：人为错误引起的系统失效的例子有：

——安全要求规范；

——硬件的设计，制造，安装，操作；

——软件的设计和实现。

[GB/T 20438.4—2006，定义 3.6.6]

3.24

系统安全完整性 systematic safety integrity

在危险失效模式中与系统性失效有关的安全相关系统安全完整性的一部分。

[GB/T 20438.4—2006，定义 3.5.4]

注：通常无法量化系统的安全完整性。

3.25

确认 validation

通过检查和提供客观证据来证明满足某一特定预期用途的特殊要求。

[GB/T 20438.4—2006，定义 3.8.2]

注：确认是一个证明 PDS(SR)安装前后，全面满足该系统的安全要求规范的活动。

3.26

验证 verification

通过检查和提供客观证据证实规定要求已经满足。

[GB/T 20438.4—2006，定义 3.8.1]

4 特定的安全功能

4.1 总则

本章描述了被 PDS(SR)供应商标识为安全相关 PDS(SR)的功能。本章中所指的安全功能并不是一个详尽的列表。在一些情况中，当电源断开时，PDS(SR)外部的其他安全相关的系统(比如机械制动)对于维持安全状态是必要的。

实现这些功能要求的技术措施，取决于 SIL 能力和要求的危险硬件失效可能性，如安全要求所指出说明。技术措施在第 6 章中描述。

为了(激活或)与其他功能、子系统或系统(与安全相关或无关)进行必要的通讯，每个安全功能都需要安全输入和/或输出信号。接口的完整性应被包括在与安全功能结合在一起的 SIL 的测定中。

一些安全功能仅执行监测任务，另一些则执行安全相关的控制或其他动作。因此必须进行以下的区分：

——违反极限的反应(仅关于监测功能)：在安全功能正确的操作期中，检测到违反极限时的反应功能；和

——故障反应功能：在安全功能中，诊断检测到发生故障时的反应功能。

两个反应功能都应考虑应用中可能的安全状态。

在选择恰当的反应功能时，必须考虑 PDS(SR)的某些部分可能不起作用。

对于故障检测所需动作的时间要求，应在安全要求说明(见 5.4.2)中阐述。

安全功能的名称包括词语“安全的”或“安全地”，用来表明这些功能可能在经过判断的现场(例如风险分析)的安全相关系统中使用，导致安全相关功能和它们的整体性由 PDS(SR)执行。

4.2 安全功能

4.2.1 限值

安全功能依赖于一些参数的限值，所以应决定限值的最大容差。

注：任何限值的规定应考虑在违反极限的情况中可能超过限值。例如，在 4.2.3.8 中位置限值的规定应考虑到最大允许的超程距离。

一个特定安全功能可能有一个或多个给定的限值，这些值可以在操作中被选择。

4.2.2 停止功能

4.2.2.1 总则

多种停止方法适用于 PDS 的每个类型。

启动停止程序并且维持一个保持模式达到静止状态的控制要求是特定应用。为了达到停止功能要求的性能，将手动操作和控制电路的连接分开是必要的。

装备设计者应该说明停止性能的任何特定要求。下面停止功能的例子常用于实际中。

4.2.2.2 安全转矩取消(STO)

能够引起转动(或运动，如果是直线电动机)的电源不被应用到电动机。PDS(SR)将不对产生转矩(或力，如果是直线电动机)的电动机提供能量。

注 1：本安全功能对应于不可控停止，与 IEC 60204-1 停止类型 0 相对应。

注 2：当需要移走电源来阻止突然的启动时，安全功能可以被使用。

注 3：当外部影响情况(例如，悬挂负载下降)出现，可能有必要采用额外的措施(例如，机械制动)来阻止任何危险。

注 4：为了电击防护，电子手段和接触器是不够的，可能需要额外的隔离措施。

4.2.2.3 安全停止 1(SS1)

PDS(SR)应满足以下条件之一：

a) 在设定的限值内，启动并控制电动机减速使电动机停止，当电动机速度低于规定的限值时启动 STO 功能(见 4.2.2.2)；或

b) 在设定的限值内，启动并监视电动机减速使电动机停止，当电动机速度低于规定的限值时启动 STO 功能；或

c) 在应用规定的时间延时后，启动电动机减速并启动 STO 功能。

注：本安全功能对应于可控停止，与 IEC 60204-1 中停止类型 1 相对应。

4.2.2.4 安全停止 2(SS2)

PDS(SR)应满足以下条件之一：

a) 在设定的限值内，启动并控制电动机减速率来使电动机停止，当电动机速度低于规定的限值时启动安全操作停止功能(见 4.2.3.1)；或

b) 在设定的限值内，启动并监视电动机减速率来使电动机停止，当电动机速度低于规定的限值时启动安全操作停止功能；或

c) 在应用规定的时间延时后，启动电动机减速并启动安全操作停止功能。

注：本安全功能对应于可控停止，与 IEC 60204-1 的停止类型 2 相对应。

4.2.3 其他安全功能

4.2.3.1 安全操作停止(SOS)

SOS 功能防止电动机偏离停止位置大于规定值。PDS(SR)为电动机抵制外力提供能量。

注：操作停止功能的描述基于以没有外部(例如机械)制动的 PDS(SR)的方式实现。

4.2.3.2 安全极限加速度(SLA)

SLA 功能防止电动机超过规定的加速度限值。

4.2.3.3 安全加速度范围(SAR)

SAR 功能保持电动机在规定的限值内加速和/或减速。

4.2.3.4 安全极限速度(SLS)

SLS 功能防止电动机超过规定的速度限值。

4.2.3.5 安全速度范围(SSR)

SSR 功能保持电动机的速度在规定的限值内。

4.2.3.6 安全极限转矩(SLT)

SLT 功能防止电动机超过规定的转矩(或力，当使用直线电动机时)限值。

4.2.3.7 安全转矩范围(STR)

STR 功能保持电动机转矩(或力，当使用直线电动机时)在规定的限值内。

4.2.3.8 安全限位(SLP)

SLP 功能防止电动机轴超过规定的位置限值。

4.2.3.9 安全极限增量(SLI)

SLI 功能防止电动机轴超过位置增量规定的限值。

注：在这个功能中，PDS(SR)控制电动机的移动增量，如下所述：

——一个输入信号(例如启动)启动具有规定的最大行程的增量移动；

——在完成这个增量所要求的行程后，如果适合于应用，则电动机停止并维持这种状态。

4.2.3.10 安全方向(SDI)

SDI 功能防止电动机轴向非预期的方向移动。

4.2.3.11 安全电动机温度(SMT)

SMT 功能防止电动机温度超过规定的上限值。

4.2.3.12 安全制动控制(SBC)

SBC 功能提供安全输出信号以控制外部制动。

4.2.3.13 安全凸轮(SCA)

SCA 功能提供一个安全输出信号来指示电动机轴承的位置是否在规定的范围内。

4.2.3.14 安全速度监控器(SSM)

SSM 功能提供一个安全输出信号来指示电动机速度是否低于规定的限值。

5 功能安全的管理

5.1 目的

为了指明管理活动，以及 PDS(SR)整体开发过程必须的信息，以保证满足功能安全目标。

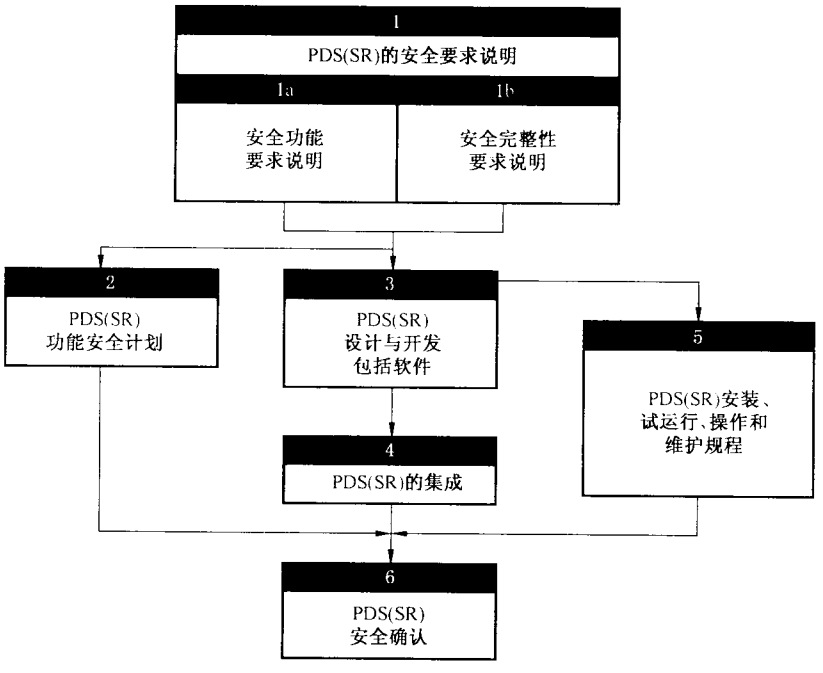
注：本章目的仅在于保证 PDS(SR)功能安全，并区别于工作场所内为达到安全所必须的一般健康和安全措施。

5.2 PDS(SR)开发生命周期

图 2 给出了 PDS(SR)的开发生命周期，并同本部分的相关条款相互参照。

注：这对应于 GB/T 20438.1—2006 中的整体安全生命周期的实现阶段(阶段 9)。

附录 A 以顺序任务表的形式给出这种信息。



阶段1，见5.4	阶段1a，见5.4.2	阶段1b，见5.4.3	阶段2，见5.3
阶段3，见第6章	阶段4，见6.5	阶段5，见第7章	阶段6，见8.3

图 2　PDS(SR)开发周期

5.3　功能安全计划

功能安全应在 PDS(SR)的整个开发过程中产生，并且进行必要的更新。该计划规定为了满足第 5 章～第 10 章所需的行为，并且识别负责完成这些行为的人员、部门或者组织。功能安全计划可能被合并在 PDS(SR)的整个质量计划中作为以“功能安全计划”为题目的一个部分，或者可能是以“功能安全计划”命名的独立文件。

实际上，功能安全计划应考虑或包括以下内容，尤其适合于 PDS(SR)的错综复杂性。

a)　安全要求说明的产生(见 5.4)包括以下因素：

——PDS(SR)特定目标应用中，准则和标准要求的考虑；

——为了避免安全要求说明产生过程中错误的方法选择；

——负责安全要求说明的产生和维护人员；

——负责安全要求说明的验证人员；

——开发开始后，安全要求说明改变的过程。

b)　在 PDS(SR)内安全功能的设计与开发，包括以下(如适用)因素：

——为目标应用设备的设计，考虑可应用的功能安全准则和标准，如过程控制设备或包含 PDS(SR)的装备；

——产品开发和工程管理系统方法的选择(见 GB/T 20438.7—2006 中 B.1.1)；

——负责设计与开发的人员；

——工程文件方法学(见 GB/T 20438.7—2006 中 B.1.2)；

——结构设计技术的应用(见 GB/T 20438.7—2006 中 B.3.2)；

——模拟或其他基于计算机设计工具的使用；

——设计验证方法；
——集成与功能试验技术，进行回归试验，以及负责人员；
——设计改变管理(硬件和软件)。

c) 安全功能的验证计划包括以下因素：
——验证策略与技术的选择；
——验证项目的选择；
——验证的负责人员；
——试验设备的选择与使用；
——来自验证设备与试验的验证结果的评价。

d) 安全功能的确认计划包括以下内容：
——负责确认试验的负责人员；
——PDS(SR)相关操作模式的确认；
——确认的技术策略，例如分析方法或统计试验；
——可接受的条件；
——在失效事件中，为满足可接受条件采取的行动。

e) 安装与试运行的计划包括以下内容(应用时)：
——安装的具体说明和安装的顺序；
——负责安装和试运行的人员；
——试运行项目以及有关功能安全的试验；
——试运行试验和结果的报告方法；
——试验失败及问题的解决机制。

f) 与安全相关的用户文件计划包括：
——必须提供的重要的安全相关信息表；
——负责用户文件的人员；
——保证文件正确性的追溯过程。

g) 当要求评估时(见 GB/T 20438.1—2006 中第 8 章)使用的功能安全评估计划包括以下内容：
——功能安全评估范围；
——负责功能评估人员；
——进行功能安全评估行为的阶段(例如：安全要求说明详细，并且安全相关控制系统已设计完成)；
——功能安全评估项目结果所产生的信息；
——完成功能安全评估项目所要求的资源；
——评估组的独立水平；
——PDS(SR)修改后功能安全评估应被再次验证的方式。

5.4 PDS(SR)的安全要求说明(SRS)

5.4.1 总则

PDS(SR)安全要求说明应以书面形式记录，并包括：
——安全功能性要求说明(见 5.4.2)；和
——安全完整性要求说明(见 5.4.3)。
这些说明应以书面形式呈现，并且：
——清晰；

——准确；
——无歧义；
——切实可行；
——可验证；
——可试验；
——可维护。

为了避免这些说明在编辑过程中的错误，须应用恰当的技术和方法(见 GB/T 20438.2—2006 中表 B.1)。

5.4.2 安全功能要求说明

安全功能要求说明应充分满足 PDS(SR)设计和开发的全面详细要求。

安全功能要求应恰当地描述为：

a) 执行所有的安全功能；
b) PDS(SR)所有预期的应用达到安全状态的状态；
c) PDS(SR)的操作模式，例如设置、启动、维护、正常预期操作；
d) PDS(SR)所有要求的行为模式；
e) 同时激活并且互相抵触的那些功能的优先权；
f) 在安全功能正确的操作中，当检测出违反限值时，所需的动作(例如违反极限反应见 4.1)；
g) 故障反应功能(见 4.1 和 6.3)；
h) 在危险发生在预期应用之前，最大故障反应时间，能执行相应的故障反映(仅要求在诊断试验用于达到 SIL 能力时)；
i) 每个安全相关功能的最大反应时间[例如安全和故障反应功能(见 6.3)]；
j) 硬件和软件之间所有相互作用的意义，即硬件和软件之间相关的任何要求的约束应被识别，并用文件记载；

注：在设计结束前，这些相互作用是不可知的，仅能阐明一般的约束。

k) 操作者通过所有方式与影响安全相关功能的 PDS(SR)相互作用(例如安全和故障反应功能)。在 PDS(SR)和任何其他的系统(直接与内部或外部相联系的装备)之间的所有界面。

5.4.3 安全完整性要求说明

PDS(SR)的安全完整性要求说明应包括：

a) 对每个安全相关功能(或同时使用的安全功能组)，SIL 能力和危险随机硬件失效的最大概率；

注 1：如果 PDS(SR)被看作是与其他组件连接实现安全功能的组件，那么 SIL 能力是相关的。

注 2：为了与其他有关联的组件的危险失效概率相适应，PDS(SR)的危险随机硬件失效概率通常需低于与分配到整体安全功能的 SIL 相联系的目标失效测量。然而，如果 PDS(SR)在一个与其他组件的冗余配置中去实现安全功能，PDS(SR)的危险随机硬件失效概率会更高。

注 3：当 PDS(SR)完全在自己内部实现安全功能时，安全完整性要求说明将识别 SIL，而不是 SIL 能力。

注 4：当普通硬件用于实现多于一个的安全功能，并且安全功能被同时使用，当决定危险随机硬件失效整体概率时，普通硬件的危险随机失效概率应仅被考虑一次。

注 5：对于一个多轴的 PDS(SR)，当要求安全功能多于一个轴时，在决定危险随机硬件失效概率时，普通硬件的危险随机硬件失效概率仅考虑一次。

b) 在贮存、运输、试验、试运行、操作和维护规程中，PDS(SR)遭遇的所有极端的环境条件(包括电磁)；

注：为了满足 IEC 61800-1，IEC 61800-2 或 IEC 61800-4 的要求，这个信息可能已获得并且在这个情况下不必再用文件记载。

c) 对增大的电磁抗扰性的任何要求(见 6.2.5)。

6 PDS(SR)设计与开发的要求

6.1 一般要求

6.1.1 操作状态的改变

在 PDS(SR)操作状态中,可能导致危险状态(例如意外的启动)的改变,应仅由操作者慎重地考虑后,再启动执行。

注:例如,PDS(SR)在保持状态中的任何失效不应导致装备的意外启动。

6.1.2 设计标准

PDS(SR)应依据 IEC 61800-5-1,如有必要,也依据 IEC 61800 系列的其他适用标准设计。

6.1.3 实现

PDS(SR)应根据它的安全要求说明(见 5.4)去实现。

6.1.4 安全完整性和故障检测

PDS(SR)应满足下面 a)~c):

a) 硬件安全完整性要求包括:
   ——硬件安全完整性的结构约束(见 6.2.2);和
   ——每小时危险随机硬件失效概率要求(见 6.2.1);
b) 系统安全完整性要求包括:
   ——避免失效的要求(见 6.2.4.1)和系统故障控制的要求(见 6.2.4.2);或
   ——组件有"经使用证明"的证明。在这种情况下,组件应满足 GB/T 20438.2—2006 相关的要求;
c) 故障检测行为的要求(见 6.3)。

6.1.5 安全和非安全功能

当 PDS(SR)执行安全和非安全功能时,它的所有硬件和软件应作为与安全相关对待,除非能表明安全和非安全功能的实现是充分独立的(例如,任何不安全相关功能的失效不引起安全相关功能的危险失效)。

注:充分表明,与包含的安全功能相关的最高安全完整性等级的危险失效率相比较,非安全和安全相关部分之间的非独立失效率应足够低。

6.1.6 使用的 SIL

当 PDS(SR)执行安全和非安全功能时,它的所有硬件和软件应作为与安全相关对待,除非能表明安全和非安全功能的实现是充分独立的(例如,任何不安全相关功能的失效不引起安全相关功能的危险失效)。

注:充分表明,与包含的安全功能相关的最高安全完整性等级的危险失效率相比较,非安全和安全相关部分之间的非独立失效率应足够低。

6.1.7 软件要求

如果软件用于实现具有特定 SIL 或 SIL 能力(见 5.4.3)的 PDS(SR)安全功能,那么这个软件应依

据为特定 SIL 制定的 IEC 61508-3 定义的要求来实现。

6.1.8 要求的重新检查

安全相关硬件和软件的要求应被重新检查以保证他们被充分说明。实际上，应特别考虑：

a) 安全功能；

b) 安全完整性要求；

c) 设备和操作者界面。

6.1.9 设计文件

除了设计和实行的文件外，PDS(SR)的设计文件应表明用于实现 SIL 声明的那些技巧和措施(例如，失效模式和效应分析、故障树分析)。

6.2 PDS(SR)的设计要求

6.2.1 每小时危险随机硬件失效概率(PFH)要求

6.2.1.1 一般要求

6.2.1.1.1 每个安全功能的 PFH

由 PDS(SR)执行的每个安全功能(或同时使用的安全功能组)目标失效测量的 PFH，按 6.2.1.1.2 和附录 B 估计，应等于或少于在安全完整性要求说明中规定的目标失效测量(见表 2)。

由 SIL 定义的 PFH 值涉及一个完整的安全功能。如果一个 PDS(SR)执行相关的安全控制系统内安全功能的一部分，则传动的 PFH 应明显低于由 SIL 定义的值。

注 1：依据 PHF 表达的目标失效测量，是由安全功能的 SIL 所决定的(见 GB/T 20438.1—2006 中表 3)。除非在 PDS(SR)安全完整性要求说明(见 5.4.3)中，对于安全功能要求满足特定的目标失效测量，而不是特定的 SIL，是有要求的。

表 2 安全完整性等级：PDS(SR)安全功能目标失效测量

安全完整性等级	PFH
3	$\geqslant 10^{-8} \sim < 10^{-7}$
2	$\geqslant 10^{-7} \sim < 10^{-6}$
1	$\geqslant 10^{-6} \sim < 10^{-5}$
注：PFH 有时指危险失效频率或危险失效率，每小时危险失效为一单位。	

PDS(SR)的每个安全功能(或同时使用的安全功能)的 PFH 应单独估算。

注 2：不同的安全功能可能有公共组件和/或独特的组件，导致每个安全功能(或同时使用的安全功能组)有不同的 PFH。

注 3：很多模型方法是适用的，最合适的方法是解析的方法，取决于环境。可用的方法包括：

——故障树分析(见 IEC 61025)；

——马尔科夫模型(见 IEC 61165)；

——可靠性框图(见 IEC 61078)。

也可参见 IEC 60300-3-1。

注 4：可靠性模型中平均恢复时间(见 IEV 191-13-08)需要考虑诊断和检验试验间隔时间、修复时间和任何其他优先于修复的延迟及运行时间。

注 5：共同原因效应和数据通讯处理引起的失效可能受来自硬件组件影响而不是硬件组件的实际(例如解码错误)

失效。但是，鉴于本部分的目的，这种失效也看成为随机硬件失效(见 GB/T 20438.6—2006 的附录 D)。

注 6：GB/T 20438.6—2006 附录 B 描述了为决定满足要求的目标失效测量的结构体系，可用估计安全功能随机硬件失效的危险失效概率的简单方法。

6.2.1.1.2 PFH 的估计

随机硬件失效应使用 GB/T 20438.2 2006 中附录 A 估算。由 PDS(SR)执行的每个安全功能(或同时使用的安全功能组)的 PFH，应考虑以下方面：

a) 考虑每个安全功能有关的 PDS(SR)的结构；

b) 在任何模式中 PDS(SR)每个子系统的可预计失效率，这种模式能够导致 PDS(SR)的危险失效，但是这种模式能够被诊断试验检测到；

c) 在任何模式中 PDS(SR)每个子系统中的可预计失效率，这种模式能够导致 PDS(SR)的危险失效，但是这种模式不能被诊断试验所检测；

d) PDS(SR)对共同原因失效的敏感性(见 GB/T 20438.6—2006 中附录 D)；

e) 诊断试验(依据 GB/T 20438.2—2006 中附录 A 和附录 C)的诊断覆盖率(DC)和相关的诊断试验间隔；

注 1：当确定诊断试验间隔时，诊断覆盖率的所有试验间隔均需要考虑。

f) 检验试验的间隔性用于保证揭示不被诊断试验检测的危险故障；

注 2：在实践中，对于 PDS(SR)的特定部分执行检验试验可能难于完成。在这样情况下，检验试验间隔可能被假定为 PDS(SR)本身或是那些组件的运行时间。应注意到许多机械应用要求运行时间为 20 年。

g) 修复检测到的失效的时间；

注 3：修复时间为平均恢复时间(见 IEV 191-13-08)的一部分，它包括检测一个失效所用的时间和不可能修复的任何时间周期(见 GB/T 20438.6—2006 中附录 B，用于修复的平均时间如何被用于计算失效概率的例子)。当修复仅在一个特定时间周期内执行的情况下，例如当 EUC 关闭并且在一个安全状态，当没有修复可以执行，特别是当这个时间周期比较长时，考虑时间周期尤其重要。

h) 任何数据的通讯过程的危险失效概率(见 6.4)。

6.2.1.1.3 失效率数据

组件失效率数据来自：

——识别源；或

——基于被认为是“经使用证明”的那些组件的估算见 GB/T 20438.2—2006 中 7.4.7.6～7.4.7.12)。

对于一个组件，当估计它的失效率时应使用预期的平均操作温度。

任何使用的失效率数据应至少有 60%的可信度等级。

注 1：数据能从一些来自工业界的资料中获得(参见附录 C)。

注 2：如果可以得到现场特定失效数据，那就更好了。如果不是这种情况，则不得不使用通用数据。

注 3：尽管恒定失效率是由大多数概率估计方法假定的，只有不超过组件的运行时间时才适用。超过了它们的运行时间(例如当失效概率随时间显著增加时)，大多数概率计算方法的结果则没有意义。因此任何概率估计应包括组件运行时间的规定。运行时间主要取决于组件本身和它的操作条件——特别是温度(例如，电解电容器就很敏感)。经验表明运行时间通常在 8 年～12 年之间。尽管如此，如果组件在接近它们的规定限值操作时运行时间可能明显缩短。

注 4：在附录 D 中，给出的故障列表可用于帮助决定失效模式。

6.2.1.1.4 诊断试验间隔

PDS(SR)的任何子系统的诊断试验间隔应能使 PDS(SR)满足 PFH 的要求(见 6.2.1.1.1)。

当危险故障能导致安全功能丧失时，为了防止危险，要求在诊断覆盖率限值内和故障反应开始时检测出这个故障。诊断和故障反应功能应在给定的最大故障反应时间(见 5.4.2)内执行。

6.2.1.1.5 硬件故障裕度为零时的试验间隔

安全功能完全依靠的是具有零硬件故障裕度的 PDS(SR)的任何子系统的诊断试验间隔，应为诊断试验间隔的之和与执行给定动作(故障反应能力)达到或维持安全状态的时间(小于给定最大故障反应时间)。

6.2.2 结构约束

6.2.2.1 SIL 的极限

在硬件安全完整性环境中，最高安全完整性等级可称为由硬件故障裕度和执行安全功能的 PDS(SR)子系统的安全失效分数所限制的安全功能。硬件故障裕度 N 意味着 $N+1$ 次故障就可能引起安全功能的丧失。考虑硬件故障裕度和该子系统安全失效分数(见 GB/T 20438.2—2006 中附录 C)，表 3 和表 4 说明了最高安全整体性水平，此水平可被称为使用该子系统的安全功能。表 3 或表 4 的要求，应用于执行安全功能和 PDS(SR)的每个部分的每个子系统都是合适的；6.2.2.2.1 和 6.2.2.2.2 规定了表 3 或表 4 之一应用于任何特定子系统。这些要求是：

a) 在决定硬件故障裕度中，不应考虑可能控制故障效应的其他方法(例如诊断)；

b) 当一个故障直接导致一个或多个次生故障发生时，这些被认为是单一故障；

c) 在确定硬件故障裕度时，由于与子系统有关的安全完整性要求发生故障的可能性很低，这些故障可被排除。任何这样的故障排除是合理的并应写入文件中(见注 3)。

注 1：考虑到子系统水平的复杂性，为了获得到足够坚固的结构，已经包括了结构约束。源于这些要求的应用过程，PDS(SR)的硬件安全完整性等级是最大的，尽管这种说法是允许的，但在一些情况中，如果 PDS(SR)已采用单一的数学方法，较高的安全完整性等级应能从理论上导出。

注 2：推导出的满足硬件故障裕度要求的子系统的结构在正常操作条件下使用。当 PDS(SR)在线修复时，故障裕度要求可能放松。然而，与其相关的任何放松的主要参数必须提前检测(例如，与要求的概率相比较的平均修复时间)。

注 3：因为如果组件借助于其设计和结构固有的特性而明显具有低的失效概率(例如，机械操动器联动装置)，那么通常不必考虑所使用组件的任何安全功能的安全完整性所需要的约束(基于硬件故障裕度)。

6.2.2.2 类型 A 和类型 B 的子系统

6.2.2.2.1 类型 A

如果组件须符合以下安全功能条件，则子系统可被认为是类型 A：

a) 所有组成的组件失效模式已定义好；和

b) 在故障条件下子系统的行为能被完全确定；和

c) 有足够可靠的来自于经验的失效数据表明，所声明的被检测出的失效率和未被检测出的危险失效率满足了要求。

注：附录 D 列出了可能被考虑的故障和故障排除。

6.2.2.2.2 类型 B

如果组件须符合以下安全功能条件，6.2.2.2.1 中叙述的一个或多个条件不满足，则子系统可被认为是类型 B。

注 1：这意味着如果至少子系统中一个组件满足类型 B 子系统的条件，那么整个子系统应被看作类型 B，而不是类型 A。

注 2：例如，由微型控制器等组成的控制部件被看作类型 B 子系统。

注 3：附录 D 列出了可能被考虑的故障和故障排除。

6.2.2.3 结构约束条件

对于应用表3或表4，结构约束条件：表3应用于PDS(SR)组成部分的每个类型A子系统；表4应用于PDS(SR)组成部分的每个类型B子系统。

表3 硬件安全完整性：A类安全相关子系统的结构约束条件

安全失效分数SFF[a]	硬件故障裕度N(见6.2.2.1)		
	0	1	2
SFF<60%	SIL1	SIL2	SIL3
60%≤SFF<90%	SIL1	SIL3	SIL3[b]
90%≤SFF<99%	SIL3	SIL3[b]	SIL3[b]
SFF≥99%	SIL3	SIL3[b]	SIL3[b]

[a] 如何估计安全失效分数的细则见6.2.3。

[b] 本部分仅适用于具有SIL但不大于SIL3的安全功能。对于SIL4安全功能，宜采用IEC 61508的要求。

表4 硬件安全完整性：B类安全相关子系统的结构约束条件

安全失效分数SFF[a]	硬件故障裕度N(见6.2.2.1)		
	0	1	2
SFF<60%	不允许	SIL1	SIL2
60%≤SFF<90%	SIL1	SIL2	SIL3
90%≤SFF<99%	SIL2	SIL3	SIL3[b]
SFF≥99%	SIL3	SIL3[b]	SIL3[b]

[a] 如何估计安全失效分数的细则见6.2.3。

[b] 本部分仅适用于具有SIL但不大于SIL3的安全功能。对于SIL4安全功能，宜采用IEC 61508的要求。

6.2.3 安全失效分数(SFF)估算

6.2.3.1 分析方法

为了估算子系统的安全失效分数，应进行分析(例如，故障树分析或失效模式和效应的分析)以确定所有相关故障和它们相应的失效模式。子系统每个失效模式的概率应基于相关故障概率确定。

6.2.3.2 数据的基础

SFF的估算应基于下面的条件之一：

——从现场经验收集的统计有效的失效率数据；或

——来自可识别源的组件失效数据。

也见6.2.1.1.3。

注：已知源的规范性列表参见附录C。

6.2.3.3 安全继电器

在具有硬件零故障裕度的子系统内，当使用具有强制性反馈触点的安全继电器提供安全功能和该功能的诊断覆盖率时，由子系统的结构约束安全整体性被限制为 SIL2 的要求。

6.2.3.4 SFF 的计算

子系统的安全失效分数应使用 GB/T 20438.2 2006 中附录 A 和附录 C 计算。

6.2.4 PDS(SR)和 PDS(SR)子系统的安全完整性要求

6.2.4.1 避免失效的要求

6.2.4.1.1 总则

在 PDS(SR)硬件的设计和开发过程中应利用技术和措施使故障的引入最小化。

试验将按计划，依据 6.2.4.1.4 执行。见第 9 章。

6.2.4.1.2 设计方法的选择

依据要求的安全完整性等级，所选择的设计方法应促进：

a) 透明性，模块化和最小化复杂性的其他特性和提高设计可理解性的其他特征；

b) 清晰和精确说明：

——实用性；

——子系统界面；

——顺序和有关时间的信息；

——同时性和同步性；

c) 清晰和精确的文件证据和信息交流；

d) 验证和确认。

6.2.4.1.3 设计措施

下面的设计措施应被使用。

a) PDS(SR)和/或子系统的正确设计包括：

——按制造商的说明使用组件，例如温度、负载、供电电源、额定功率和时间参数；

——通过设计参数降级来提高目标失效率的可靠性是必要的；

——子系统正确的结合、组装，例如布线、接线和任何互相连接；

——为尽早发现设计中的缺陷，应对设计进行复查和检验。

b) 兼容性：

——使用具有兼容性操作特征的子系统。

c) 特定环境条件：

——确保 PDS(SR)在所有特定环境中的安全操作能力，例如温度、湿度、振动、电磁现象、污染等级、过电压类别、海拔等。

6.2.4.1.4 试验计划

在设计中，下面不同的试验类型应按需要列入计划：

a) 子系统试验；

b) 集成试验；

c) 确认试验；

d) 配置试验(见 7.1)。

试验计划文件应包括：

e) 执行的试验类型及其步骤；

f) 试验环境、工具、配置和程序；

g) 通过/失败判定标准。

当允许时，自动试验工具和集成开发工具将被使用。

注：这些工具的整体性可以通过特定试验，通过满意使用的悠久历史或通过正在设计的特定 PDS(SR)的输出独立验证来证实其完整性。

6.2.4.1.5 设计维护要求

为保证 PDS(SR)的安全完整性，在后续的设计修改中仍要保持要求的水平，设计维护和再试验的过程应在设计阶段决定。

6.2.4.2 系统故障控制的要求

6.2.4.2.1 设计特征

为了控制系统故障，设计应使 PDS(SR)及其子系统具有承受以下条件的特征：

a) 硬件中的潜在设计故障，除非应用 GB/T 20438.2—2006 中 A.3 和表 A.16，硬件设计故障的可能性才可以被排除；

b) 环境应力包括电磁骚扰，应用 GB/T 20438.2—2006 中 A.3 和表 A.17；

c) 由 PDS(SR)的操作者造成的错误(见 GB/T 20438.2—2006 中 A.3 和表 A.18)；

d) 在软件中的潜在设计故障(见 GB/T 20438.3—2006 中 7.4.3 和相关的表)；

e) 任何数据通讯过程的错误和其他效应的出现(见 6.4)。

6.2.4.2.2 可试验性和可维护性

在设计和开发过程中应考虑可试验性和可维护性，这样是为了在最终 PDS(SR)中顺利执行这些功能。

6.2.4.2.3 人的约束

PDS(SR)的设计应考虑人的能力和极限，分配给操作人员和维护人员的行为的适宜性。操作界面的设计应遵循良好的人为因素的实践，并且适应操作人员的训练或认识的适当水平。

6.2.4.2.4 防止非故意修改

PDS(SR)应装入安全相关软件、硬件、参数化和 PDS(SR)配置的防止非故意修改(或利于保护)措施。

注：见 GB/T 20438.7—2006 中 B.4.8。

6.2.4.2.5 输入确认信号和操作者的错误

PDS(SR)的设计应输入确认信号去控制操作失效。设计也应通过仿真性检查去防止操作者的错误[PDS(SR)相关的安全功能]。

注：见 GB/T 20438.7—2006 中 B.4.6 和 B.4.9。

6.2.4.2.6 电源失电

PDS(SR)的规定和设计应考虑电源失电的影响。

6.2.5 PDS(SR)的电磁抗扰性要求

6.2.5.1 总则

当PDS(SR)进行电磁抗扰性试验时,执行的标准在6.2.5.3中给出。这个标准不能用于设备的正常(与安全无关)功能[当与IEC 61800-3的要求相一致时,PDS(SR)的电磁兼容性功能可以得到保证]。

6.2.5.2 预期的环境

为了PDS(SR)的预期使用,规定或期待的EM环境将被用来判断EM抗干扰性的试验等级。

当PDS(SR)制造商不了解EM环境时,抗扰性试验应使用IEC 61800-3的试验等级。

6.2.5.3 执行标准

应PDS(SR)专用的安全功能满足下面的执行标准。不考虑PDS(SR)所有与安全无关的功能,除了应用6.2.5.4外。

PDS(SR)在安全应用方面的(FS)功能:

- 不要偏离它们对安全功能给定的限值;或
- 如果PDS(SR)对EM骚扰是这样的方式,即PDS(SR)定义的安全状态,在规定的最大故障反应时间内维持或达到,则功能安全可能临时或永久偏离它们给定的限值。

假定安全状态在给定的最大故障反应时间内维持或者达到,则安全功能的永久降级或组件的损坏是允许的。

这个标准适用于与PDS(SR)预期应用相关的所有电磁现象。

6.2.5.4 危险状态的引入

当应用电磁抗扰性试验时,PDS(SR)不应引起非安全状态或危险。

6.2.5.5 验证

当执行EM抗干扰性试验时,应采取给定的缓解措施。

依据PDS(SR)预期应用的电磁环境分析,为了验证增强的抗扰性(如GB/T 20438.2),要么:

——必要时(取决于电磁现象和要求的SIL),提高试验等级,和/或试验时间,和/或试验循环次数;或

——验证给出的任何附加缓解措施(见GB/T 20438.7—2006中A.11.3)的效果。

6.3 故障检测行为

6.3.1 故障检测

PDS(SR)内的故障检测由诊断试验执行。

当能导致安全功能丢失的危险故障被检测到时,为了阻止危险,故障反应功能应启动。诊断和故障反应功能在给定的最大故障反应时间内执行。

6.3.2 故障裕度大于零

具有硬件故障裕度性大于零的任何子系统的危险故障检测(由诊断试验或由任何其他方式)应启动:

a) 故障反应功能;或

b) 当故障部分修复时,子系统的故障部分的隔离允许机械和/或设备部分的连续安全操作。如果

修复不是在危险随机硬件失效概率计算所假定的平均恢复时间 MTTR 内结束，那么应启动故障反应功能。

6.3.3 零故障裕度

在具有零硬件故障裕度且其上的安全功能是完全不独立的任何子系统，其危险故障的检测（由诊断试验或由任何其他方式）应启动故障反应功能。

6.4 数据通讯附加要求

当数据通讯在安全功能执行时使用，则通讯过程未检测到的失效概率估算，应考虑传输错误、重复、删除、插入、重排序、篡改、延迟和伪装。由于随机失效（见 6.2.1.1.2），当估计安全功能的 PFH 时，应考虑这种概率。

注："伪装"意味着一条信息的真实内容没有被正确识别。例如，来自不安全组件的信息被错误地识别为来自安全组件的信息。

为保证通讯过程要求的失效措施的必要测量，应依据 GB/T 20438.2 和 IEC 61508-3 的要求来执行完成。这允许两种可能的方法：

a) 通讯通道应完全依据 IEC 61508[所谓"白色通道"见图 3 a)]设计、执行和确认；或者

b) 通讯通道的有些部分不按照 IEC 61508 设计或确认[所谓"黑色通道"见图 3 b)]。在这种情况下，为保证通讯过程的失效性能的必要测量，应在与通讯通道接口的 PDS(SR)安全相关元件中执行。执行应与 IEC 62280 相一致。

当数据通讯用于安全相关数据与 PDS(SR)外的子系统交换时，上述要求适用于 PDS(SR)及相关子系统。

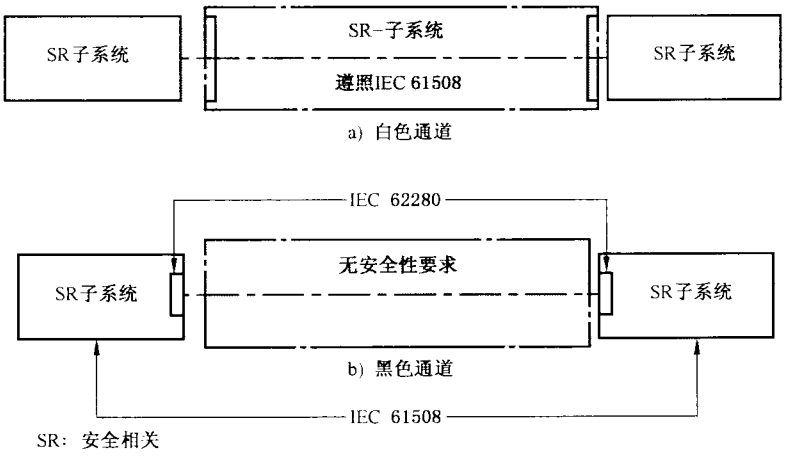


图 3 数据通讯的结构

6.5 PDS(SR)的集成和试验要求

6.5.1 硬件集成

PDS(SR)应依据其规定的设计进行集成。因为所有子系统和组件集成的部分在 PDS(SR)内，所以 PDS(SR)应依据给定的集成试验进行试验。这些试验按验证计划上的规定，并且应表明所有模块正确的相互作用，执行它们的预期功能，而不执行非预期功能。

或者，当依据 6.2.5 和 IEC 61800-5-1 和附加的 IEC 61800-1 或 IEC 61800-2 或 IEC 61800-4（如果合适）的 PDS(SR)型式试验成功通过时，硬件集成的要求也就被包括在内了。

6.5.2 软件集成

PDS(SR)内安全相关软件部分/模块的集成应依据 IEC 61508-3 执行。它应包括软件验证计划中规定的试验以保证软件和硬件的兼容性以此来满足功能和安全性能的要求。

注：这不意味所有输入组合的检测。试验所有等效的类别(见 GB/T 20438.7—2006 中 B.5.2)就足够了。静态分析(见 GB/T 20438.7 2006 中 B.6.4)、动态分析(见 GB/T 20438.7 2006 中 B.6.5)或故障分析(见 GB/T 20438.7 2006 中 B.6.6),可减少试验次数到可接受水平。

6.5.3 集成过程中的修改

在集成过程中,PDS(SR)的任何修改或改变均应进行影响分析,它应识别受影响的组件及附加验证。

6.5.4 适用的集成试验

集成试验将在验证计划中加以说明。应用功能试验赋予 PDS(SR)的输入值或设定值完全揭示了正常期望的操作。安全功能是要求的(例如,触发了 STO 或者超出了 SLS 的速度限值),将观察到的结果操作与说明中给出的预期操作进行比较。(见第 9 章)

6.5.5 试验文件

在 PDS(SR)的集成试验期间,应形成下面的文件:

a) 所使用的试验计划的版本;
b) 集成试验的验收标准;
c) 被试验的 PDS(SR)的类型或版本;
d) 使用带校准数据的工具和设备;
e) 每项试验的结果;
f) 预期与实际结果之间的差异。

7 使用信息

7.1 PDS(SR)安全使用信息及说明

以下信息应由制造商建文档,提供给用户:

a) 用于执行安全功能的每个功能和界面的功能说明应包含:
   ——安全功能的详细描述(包括超出限值的反应);
   ——故障反应功能;
   ——每个安全相关功能以及相关故障反应功能的响应时间;
   ——安全功能计划被激活或禁止的状态(例如,操作模式);
   ——那些同时起作用并且相互冲突的功能,哪些有优先权。
b) 各个安全功能的安全完整性信息,包括:
   ——SIL 能力;
   ——PFH 值。
c) 将被使用的 PDS(SR)的环境和操作条件(包括电磁性)的定义(亦见 IEC 61800-1 或 IEC 61800-2或 IEC 61800-4,IEC 61800-3 和 IEC 61800-5-1)。应考虑到贮存、运输、安装、试运行、试验、操作和维护。
d) PDS(SR)的任何约束的明示:

——应该观察环境，以保持所估算的失效率的有效性；

——PDS(SR)的运行时间和检验试验间隔时间，依据实际情况而定；

——试验、校准或维护要求；

——观察 PDS(SR)应用的任何限制，以避免发生系统失效；

——各个安全功能的 SIL 能力；

——识别 PDS(SR)的硬件和软件配置的任何信息，以确保配置管理符合第 4 章。

e) 安装及试运行指导(见 IEC 61800-5-1:2003 中第 6 章)包括设定和参数化。

f) 安全功能配置试验的要求，当配置的安全功能的整体方法不能被保证(例如，PC 配置工具)时。

配置试验应在具体应用、试运行或整改后进行，以确保 PDS(SR)使用的安全功能如预期的那样配置。尤其是，试验应确认 PDS(SR)内参数的预定值。试验通常使用 PDS(SR)制造商提供的试验程序，由负责 PDS(SR)试运行的人员执行并以文件形式写出。

配置试验手册至少要求记录以下内容：

包括图形的应用描述；

应用中使用的安全相关组件(包括软件版本)说明；

——将应用于 PDS(SR)的安全功能列表；

——通过给出的试验程序，得到这些安全功能的每个试验结果；

PDS(SR)内所有安全相关参数及其值的列表；

——试验人员检查所有项目、试验日期并确认。

重复应用的 PDS(SR)的配置试验可以作为重复应用的一个型式试验来执行，以确保所有单元里都配有安全功能。

g) 由用户或部分设备包括 PDS(SR)(如 PLC，监视控制器)来执行的诊断试验。

h) PDS(SR)的操作和维护规程应包括以下内容：

——为了维持 PDS(SR)的功能安全，需要执行的常规动作，包括有限寿命组件的替换(如冷却风扇，电池等)；

为了防止不安全状态和/或减少危险事件的后果所必需的动作和约束；

当 PDS(SR)内发生故障或失效时，维护规程应包括：

- 故障诊断及维护的规程；
- 重新确认的规程。

——维护和重新确认所必需的工具，以及维护工具和设备的规程。

注：PDS(SR)操作和维护规程可以通过以下形式进行不间断的升级，如：

——功能安全审核；

——PDS(SR)的试验。

8 验证和确认

8.1 总则

本章的目的是为了确保遵从功能安全计划(见 5.3)。

8.2 验证

设计过程中，每个已满足要求的设计阶段完成后，应对其进行检查。可通过评估、分析、检查、复查和/或试验进行验证。

8.3 确认

设计完成后，应检查 PDS(SR)是否满足安全要求所规定的全部要求。可采用评估、分析、检查、复

查和/或试验的方法进行确认。确认过程中应给出避免故障的建议，见 GB/T 20438.2—2006 中表 B.5。

8.4 文件

关于 PDS(SR)验证和确认的文件包含：

a) 所使用的验证和确认计划的版本；

b) 处于试验(或分析)下的安全功能，同时提及的在 PDS(SR)安全验证和确认计划期间所提出的要求；

c) 所使用的工具和设备；

d) 每个验证和确认的结果。

9 试验要求

9.1 试验计划

PDS(SR)安全功能的试验应与开发过程中的每个阶段同时进行。

试验计划应以文件形式出现并包括下列详细说明：

a) 每个安全功能的功能试验；

b) 每个安全功能的每个诊断功能的功能试验；

c) 验收标准。

试验可使用“黑盒”或“白盒”方法，所谓“黑盒”是指不考虑安全功能的内部执行；所谓“白盒”是指执行的特定知识用于确定试验(例如，故障插入)。

若经相关要求允许，可放弃试验或被其他验证或确认方法代替。

9.2 试验文件

在 PDS(SR)安全功能试验过程中，以下内容应写入文件中：

a) 所使用的试验计划的版本；

b) 试验验收准则；

c) 被试验的 PDS(SR)的类型及版本；

d) 使用带校准数据的工具和设备；

e) 试验条件；

f) 试验人员；

g) 每项试验的详细结果；

h) 预期与实际结果之间的差异；

i) 试验结论：试验合格或失败的原因。

10 修改

10.1 目的

当初始设计已经发送给制造商后，设计需要修改时，为确保 PDS(SR)安全功能被保持。

10.2 要求

在进行任何修改之前应安排步骤。如同 PDS(SR)最初开发时的安排和管理一样，至少在同等水平

的专业技能、自动工具下进行修改。修改应按计划执行。

10.2.1 修改申请

只有通过了功能安全的管理步骤下的修改申请，修改工作才可以开始(见第5章)。申请应包括如下内容：

a) 改变的原因；

b) 建议如何更改(软件和硬件)。

10.2.2 效果分析

应对PDS(SR)的功能安全的建议修改进行评估。评估应包括有足够的分析区确定宽度和深度，并需要依据5.2返回该宽度和深度的开发阶段。

10.2.3 批准

是否批准执行修改申请应依据影响分析的结果而定。

10.2.4 文件

应为每个PDS(SR)修改项目建立和维护适当的文件。文件应包括：

a) 修改的详细说明；

b) 影响分析的结果；

c) 对于更改的所有认可；

d) 组件的试验状况，包括再确认数据；

e) PDS(SR)配置管理史(硬件和软件)；

f) 与以前操作和条件的差异；

g) 使用说明的必要改变；

h) 依据5.2的所有可适用的开发阶段。

附 录 A
（资料性附录）
顺序任务表

依据 IEC 61508 中描述的生命周期，以下设计步骤适用于 PDS(SR)。表 A.1 给出了必要开发阶段的顺序以及所参照的本部分或 IEC 61508 中的相应条款。

注 1：作为设计工程的通常惯例，生命周期的设计和开发已经被分成“概念”与“设计和开发”两部分。

注 2：当需要第三方认证时，在设计步骤开始时应建立 PDS(SR)制造商与认证机构之间的联系。

注 3：在表 A.1 中，参照 IEC 61508 应用于所引用部分的第一版。在后续的版本中，条款号可能有所改变。

表 A.1 顺序任务表

	工 作	依 据
1	**一般要求**	
	所有相关条款应受控于一个适当的文件控制方案 项目管理的描述 质量认证管理系统	GB/T 20438.1—2006 中第 5 章； GB/T 20438.2—2006 中 7.3、7.7、7.8、7.9； GB/T 20438.3—2006 中 6、7.3、7.4.2.1、7.7、7.8、7.9
2	**PDS(SR)安全性要求规范**	**PDS(SR)安全生命周期(见 5.2)第 1 段**
	安全性要求规范(SRS)的开发包含安全功能性要求和安全完整性要求	见 5.4； GB/T 20438.1—2006 中 7.6； GB/T 20438.2—2006 中 7.2、表 B.1、B.6； GB/T 20438.2—2006 中 7.4.4-6，附录 A； GB/T 20438.3—2006 中 7.2，表 A.1，B.7； GB/T 20438.3—2006 中 7.4.2/4，表 A.3，B.1； GB/T 20438.7—2006 中表 C.1； IEC 61508-5 中示例； GB/T 20438.6—2006 中示例，附录 A
3	**PDS(SR)安全性要求规范的验证**	
	a) PDS(SR)安全性要求规范的复查； b) 需要时，由无关人员或部门检查	a)见 8.2； b)GB/T 20438.2—2006 和 GB/T 20438.3—2006 中 7.9
4	**概念**	**PDS(SR)安全生命周期(见 5.2)第 3 段**
	a) 基于结构水平的硬件设计包括： ● 安全相关硬件的方块图； ● 用户与程序界面； ● 安全相关的信号路线； ● 供电电源； ● 独立通道隔离以达到故障裕度； ● 独立通道间通讯连接以达到诊断覆盖率。	a) 见第 6 章 GB/T 20438.2—2006 中 7.4、附录 A、表 B.2、B.6 GB/T 20438.6—2006 中示例、附录 A 和附录 D

表 A.1（续）

	工　作	依　据
4	**概念**	**PDS(SR)安全生命周期(见 5.2)第 3 段**
	b) 基于结构水平的软件设计包括： ● 有安全相关软件提供的功能描述； ● 与硬件的相互作用； ● 软件预定行为的状况机械图； ● 用户和程序界面； ● 故障检查可能性和故障反馈； ● 软件结构的描述，例如采用方块图形式； ● 安全性相关数据的控制和存储； ● 版本程序； ● 使用的工具，如编译器、代码检验装置。 c) 建议对于在功能方块图水平上随机硬件失效导致的安全功能失效的可能性的预测	b) GB/T 20438.2—2006 中 7.2.3.1(h)； GB/T 20438.3—2006 中 7.2.2.8，7.2.2.10，7.4.2/3，表 A.2、表 B.7、表 B.9； GB/T 20438.7—2006 中表 C.1 c) GB/T 20438.1—2006 中表 2； GB/T 20438.2—2006 中 7.4.3，表 3，A.1，附录 C； GB/T 20438.3—2006 中表 B.4(FMEA)； 示例见 GB/T 20438.6—2006 中附录 C 和附录 D
5	**概念的验证**	
	a) 系统设计的复查； b) 当需要时，由无关的人员或部门检查	a) 见 8.2； b) GB/T 20438.2—2006 和 GB/T 20438.2—2006 中 7.9
6	**计划确认**	**PDS(SR)安全生命周期的第二阶段(见 5.2)**
	a) 相关 PDS(SR)安全性验证的详细安排； b) 应依据 9.3 设计和开发规定确认安排	a) 见 8.3； b) GB/T 20438.2—2006 中 7.3，表 B.5 和 GB/T 20438.3—2006 中 7.3，表 A.7，B.3，B.5
7	**确认安排的验证**	
	a) 确认安排的复查； b) 当需要时，由无关的人员或部门检查	a) 见 8.2； b) GB/T 20438.2—2006 和 GB/T 20438.3—2006 中 7.9
8	**设计和开发**	**PDS(SR)安全生命周期的第三阶段(见 5.2)**
	a) 硬件设计； b) 软件设计； c) 可靠性预测(由于随机硬件失效导致的安全功能失效可能性的计算)包括： ● PDS(SR)类型； ● SFF； ● 功能框图； ● 可靠性模型； ● 模型(装置列表)数据基础； ● PFH 计算； ● 运行时间； ● 维护间隔时间，检验试验间隔时间(如果相关)	见第 6 章 a) GB/T 20438.2—2006 中 7.4，附录 A，表 B.2，B.3，B.6； b) GB/T 20438.3—2006 中 7.4.5，7.4.6，表 A.4； c) GB/T 20438.1—2006 中表 2； GB/T 20438.2—2006 中 7.4.3，表 3，A.1，附录 C； GB/T 20438.3—2006 中表 B.4(FMEA)； 示例见 GB/T 20438.6—2006 中附录 C 和附录 D

表 A.1（续）

	工　作	依　据
9	**设计的验证**	
	a) 系统设计的复查； b) 模块水平上的功能试验； c) 当需要时，由无关的人员或部门检查	a) 见 8.2 c) GB/T 20438.2　2006 中 7.9； GB/T 20438.3—2006 中 7.4.7，7.4.8，7.5，7.9，表 A.5，A.9
10	**PDS(SR)集成**	**PDS(SR)安全生命周期的第四阶段(见 5.2)**
	安全相关 PDS(SR)的集成及试验	见 6.5
11	**集成验证**	
	HW/SW 集成试验结果和文件的复查	见 8.2 GB/T 20438.2—2006 中 7.5，7.9，表 B.3，B.6； GB/T 20438.2—2006 中 7.4.3.2(f)，7.4.5.5，7.4.6.2，7.4.7，7.5，7.9，表 A.5，A.6，A.9
12	**安装，调试和操作(用户文件)**	**PDS(SR)安全生命周期的第 5 阶段(见 5.2)**
	用户文件增加对 PDS(SR)的安装、试运行、操作和维护的说明	见第 7 章 GB/T 20438.2—2006 中 7.6，表 B.4
13	**用户文件的验证**	
	a) 对描述 PDS(SR)安装、试运行、操作和维护的用户文件的复查； b) 当需要时，由无关的人员或部门检查	a) 见 8.2； b) GB/T 20438.2—2006 和 GB/T 20438.3—2006 中 7.9
14	**PDS(SR)的确认**	**PDS(SR)安全生命周期的第 6 阶段(见 5.2)**
	a) 为 PDS(SR)确认提供所有所需信息； b) 全套软件和合适的文件； c) 依据确认计划确认试验和步骤； d) 确认试验结果的文件； e) 需要时，为第三方确认准备合适的文件	a) 见 8.3； c) GB/T 20438.2—2006 中 7.7，表 B.5，B.6； GB/T 20438.3—2006 中 7.5.2.7，7.7，7.9，表 A.7
15	**PDS(SR)修改步骤**	
	a) 修改请求和分析； b) PDS(SR)所有被修改部分的合适文件； c) 被修改部分的重新验证 d) 如果修改已经影响到故障裕度、危险故障概率、诊断覆盖率或共同原因失效，则可靠性预测更新； e) 至少对 PDS(SR)被修改的部分进行再确认； f) 软件修改	a) 见第 10 章； b) GB/T 20438.1—2006 中 7.16； GB/T 20438.2—2006 中 7.5.2.5，7.8； 示例见 GB/T 20438.1—2006 中图 9。 f) GB/T 20438.3—2006 中 7.1.2.8，7.5.2.6，7.6.2，7.8.2，表 A.8

附 录 B
（资料性附录）
确定 PFH 的示例

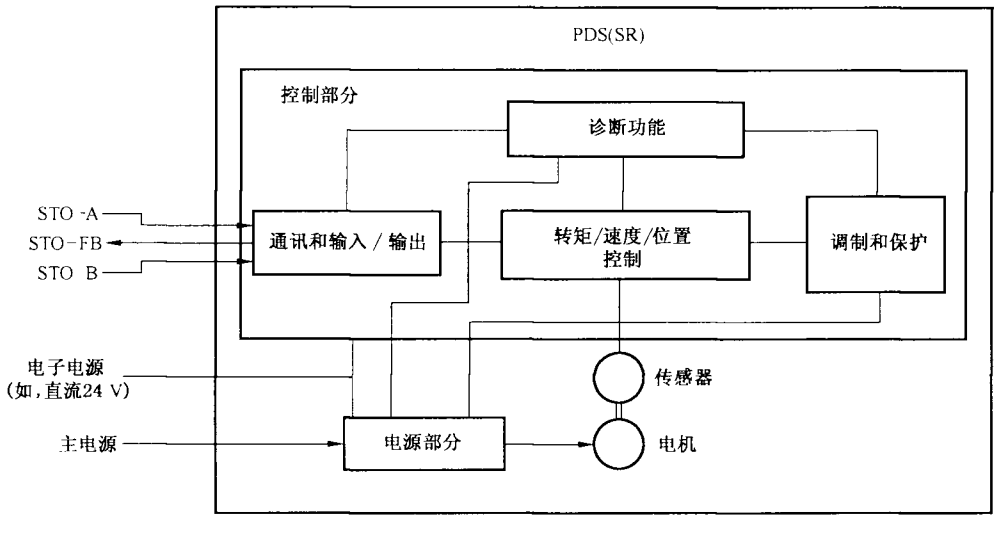
B.1 总则

本章以带有安全转矩取消(STO)安全功能的 PDS 为例，描述 PFH 值的确定。通过详细给出 PDS(SR)所需的要求及其内部结构组件，来表示如何计算 PFH 值。

B.2 PDS(SR)结构举例

B.2.1 总则

本章所述的 PDS(SR)包括安全功能 STO，它是由两个冗余数字输入接口触发，并通过一个数字输出接口给出单个反馈信号(见图 B.1)。



说明：

STO-A ——STO 触发输入通道 A；

STO-B ——STO 触发输入通道 B；

STO-FB——STO 反馈输出。

图 B.1 PDS(SR)示例

示例要求如下：

——SIL2；

——连续运行模式。

在 PDS(SR)内，利用几个安全功能专用组件使安全功能 STO 与 PDS(SR)的标准功能一起执行。

由于内部单通道供电，PDS(SR)被分成两个独立的子系统：两通道子系统 A/B 和供电/电压监控器子系统 PS/VM(见图 B.2)。

本例 PDS(SR)安全功能(STO)的 PFH 值计算如下：

$$PFH_{PDS(SR)} = PFH_{A/B} + PFH_{PS/VM}$$

式中，$PFH_{A/B}$和 $PFH_{PS/VM}$分别为子系统 A/B 和 PS/VM 的 PFH 值。

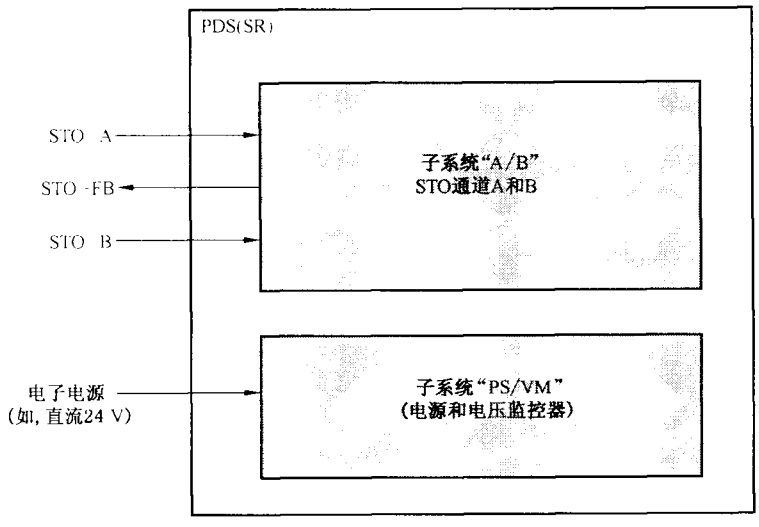


图 B.2 PDS(SR)子系统

B.2.2 子系统 A/B

安全功能 STO 是通过两个通道来执行，以达到硬件故障裕度 1 以及通过子系统 A/B 来模型化，对于子系统 A/B 要计算单独的 PFH 值。这个子系统的执行提供以下关于安全功能的系统特性：

——B 型(复杂的硬件)；

——硬件故障裕度 1(两通道执行)。

B 型子系统结构约束(见 6.2.2.3)表明，为了达到 SIL2 和硬件故障裕度 1，安全失效分数(SFF)必须至少为 60%。

B.2.3 子系统 PS/VM

由于内部电源(PS)只有一个通道，所以使用一个电压监控器(VM)。内部电源和电压监控器被模型化为独立子系统 PS/VM，为此要计算单独的 PFH 值。这个子系统的执行提供以下有关安全功能的系统特性：

——B 型(复杂的硬件)；

——硬件故障裕度 0(单通道执行)。

B 型子系统结构约束(见 6.2.2.3)表明，为了达到 SIL2 和硬件故障裕度 0，安全失效分数(SFF)必须至少为 90%。

B.3 PDS(SR)PFH 值确定实例

B.3.1 子系统"A/B"(主子系统)

B.3.1.1 功能模块划分

在 PDS(SR)内，子系统 A/B 是安全功能 STO 的一部分。由于硬件故障裕度为 1，子系统 A/B 需要由两个通道组成。图 B.3 给出了 PDS(SR)示意方块图，此图突出了参与执行安全功能 STO 的组件。

为了计算 PFH 值，子系统 A/B 进一步被划分为功能模块，并确定每个模块的失效率。由于使数字

触发输入电路和开关电路的组件数量最小化，仅需要两个功能模块。

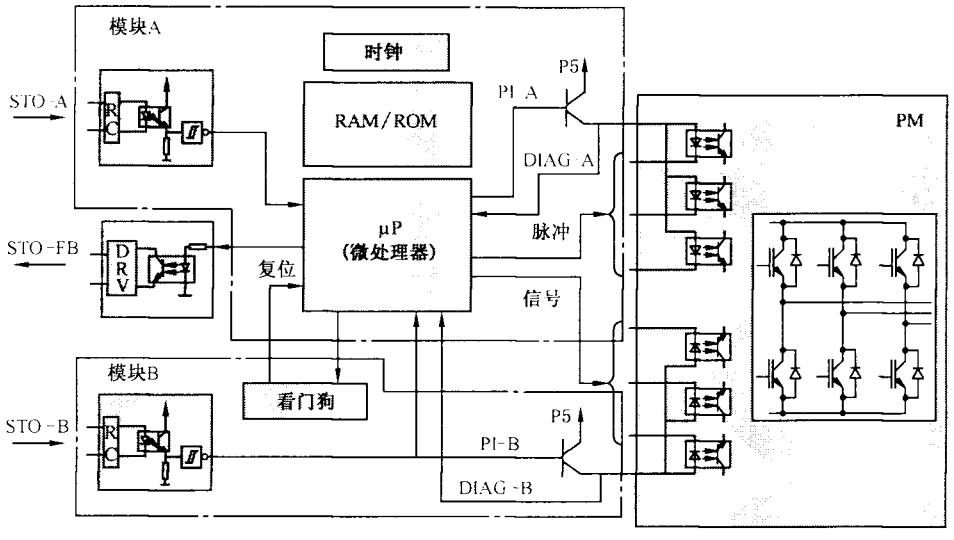


图 B.3　子系统 A/B 的功能模块

说明：

P5　……供电电压 5V；

PI-A(B)　——脉冲抑制通道 A(B)；

DIAG-A(B)——诊断信号通道 A(B)；

RC　——阻容滤波器；

DRV　——输出驱动器；

PM　——功率模块。

功率模块内的组件失效不会引起安全功能的丢失，因而功率模块没有必要包含任何与确定 PFH 值有关的子系统。

B.3.1.2　功能模块失效率的确定

B.3.1.2.1　功能模块分析

对于每个功能模块，必须确定哪种失效是属于危险失效。其结果意味着功能模块的组件进行下面的 FMEA(失效模式效应分析)。

B.3.1.2.2　组件的 FMEA

功能模块电路组件的 FMEA 决定哪些组件与安全功能有关，然后利用 B.3.1.2.1 功能模块分析中的判定标准，给每个安全相关组件的失效模式分配安全的或是危险的属性。对于简单的组件，如果安全失效模式和危险失效模式这两部分没有可靠性数据，则单个危险失效模式将导致所有组件失效。对于复杂的组件，GB/T 20438.6　2006 中的附录 C 假定安全失效模式和危险失效模式各占 50%。

除此之外，FMEA 定义了由有效诊断功能检测的每个组件的危险失效率。对于复杂组件，必须使用 IEC 61508-2 中表定义被检测出危险失效的那一部分。这个比例定义了组件的失效率 λ_{DD}(可检测到的危险)和 λ_{DU}(不可检测到的危险)。

功能模块总失效率(λ_S、λ_{DD}、λ_{DU})是功能模块内所有安全相关组件的安全失效率，可检测到的危险失效率以及检测不到危险失效率的总和。

B.3.1.2.3　确定各种失效率的简单方法

在多组件的复杂硬件电路中，在组件基础上对一组件进行 FMEA 并不总是真实的。所以，依据

GB/T 20438.6—2006 附录 C，可选择广泛接受的简化方法。

复杂电路内所有功能模块的失效率，计算为所有组件失效率之和，安全失效率和危险失效率各占50%。利用 GB/T 20438.2—2006 中的表可确定被检测到失效的那一部分。

本方法亦适用于功能模块失效率 λ_S、λ_{DD} 和 λ_{DU}。

B.3.1.3 完全失效分数

使用 B.3.1.2.3 中所示的简化方法，功能模块失效率确定如下：

——印制线路板失效中安全故障所占比例为 50%（见注）。

注：印制线路板危险失效所占比例也为 50%。

诊断覆盖率(DC)是用 GB/T 20438.2—2006 中的表估算的。

——功能模块 A 的 DC_A：90%（见表 B.1）；

功能模块 B 的 DC_B：90%（见表 B.1）。

表 B.1 子系统 A/B 的诊断覆盖率因数的确定

方法(GB/T 20438.2—2006)	诊断覆盖率水平要求	诊断试验的执行
表 A.3 通过在线监视检测失效	90%	循环试验检查冗余通道
表 A.3 监控的冗余	99%/90%	循环试验检查冗余通道
表 A.4 通过软件(漫步位)自检(一个通道)	90%	微处理器的自检
表 A.6 RAM 的“galpat”测试	90%	通过微处理器完成
表 A.10 带有分离时基和时间窗的看门狗(亦见表 A.12)	90%	看门狗设计
表 A.8 利用试验模式检查	99%	通过 RAM 试验实现
表 A.15 多个操动件的交叉监视	99%	循环试验监视两个开关操动件

功能模块 A 和功能模块 B 的电路失效率[实际示例值，表示为失效率(FIT)，单位 $10^{-9}/h$]：

模块 A：λ_A	（总失效率）		450FIT
λ_{AS}	（安全失效比例）	0.5×450FIT	225FIT
λ_{AD}	（危险失效比例）	0.5×450FIT	225FIT
λ_{ADD}	$DC_A \times \lambda_{AD}$	0.9×225FIT	202.5FIT
λ_{ADU}	$(1-DC_A)\times\lambda_{AD}$	(1−0.9)×225FIT	22.5FIT
模块 B：λ_B	（总失效率）		70FIT
λ_{BS}	（安全失效比率比例）	0.5×70FIT	35FIT
λ_{BD}	（危险失效比例）	0.5×70FIT	35FIT
λ_{BDD}	$DC_B \times \lambda_{BD}$	0.9×35FIT	31.5FIT
λ_{BDU}	$(1-DC_B)\times\lambda_{BD}$	(1−0.9)×35FIT	3.5FIT

依据 GB/T 20438.2—2006 中 C.1 的 g)项计算子系统 A/B 的安全失效分数为：

$$SFF_{A/B} = [(\lambda_{AS}+\lambda_{BS})+(DC_A\times\lambda_{AD})+(DC_B\times\lambda_{BD})]/[(\lambda_{AS}+\lambda_{BS})+(\lambda_{AD}+\lambda_{BD})]$$
$$= [(225+35)+(0.9\times225)+(0.9\times35)]FIT/[(225+35)+(225+35)T]FIT$$
$$= 494FIT/520FIT$$
$$SFF_{A/B} = 95\%$$

B.3.1.4 共同原因失效因数 $\beta_{A/B}$

利用 GB/T 20438.6—2006 中附录 D 的表 D.4 估算共同原因失效因数 $\beta_{A/B}$。

$\beta_{A/B}=2\%$。

B.3.1.5 可靠性模型(Markov)

子系统 A/B 的可靠性模型被当做 Markov 模型来执行,其状态图见图 B.4。

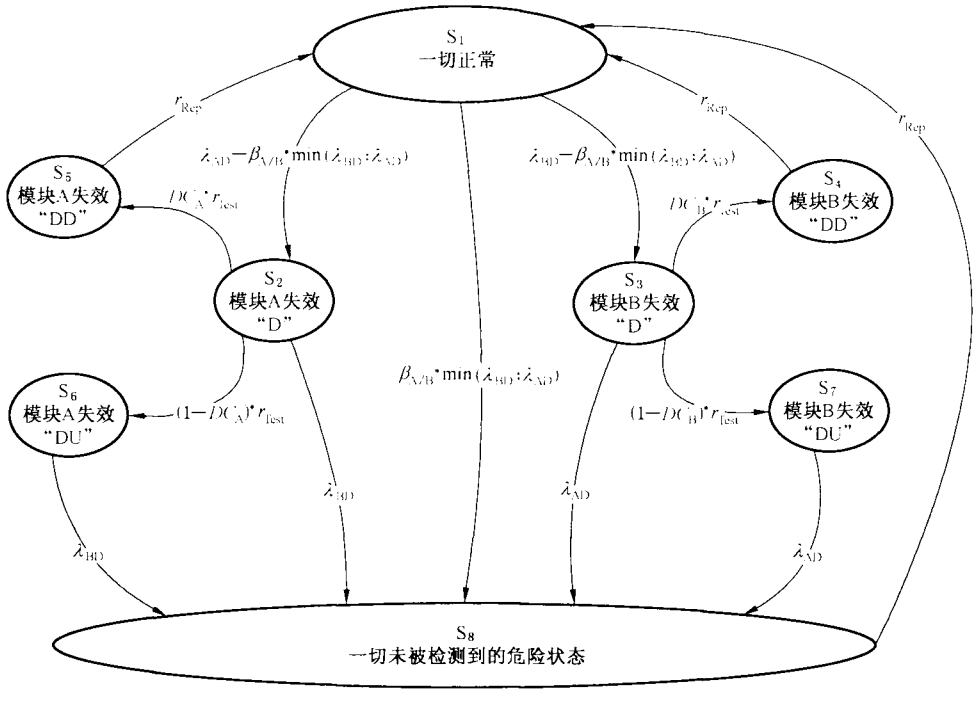


图 B.4 子系统 A/B 的可靠性模型(Markov)

注 1:以上 Markov 模型应认为是一种近似法。因为由于其自身的性质,从数学角度上严格来讲,与诊断试验及事件触发的修复对应的过渡过程不符合 Markov 技术所需的条件。

注 2:图 B.4 所示的模型详细地表明诊断试验的内容。由于失效率和试验率的通常值,模型可被简化。通常,测试率是 1/8 h 还是 1/168 h 并不重要(见表 B.2)。

注 3:图 B.4 中,$\min(\lambda_{BD}、\lambda_{AD})$表示 λ_{BD} 和 λ_{AD} 中的较小值。

由于"安全"失效对 PFH 值没有重要影响,所以模型不考虑"安全"失效。本模型假定为检测到失效后,PDS(SR)断开电源,并被修复。

共同原因失效率是由因数 $\beta_{A/B}$ 以及功能模块 A 和功能模块 B 的危险失效率的较小值决定的(见注 3)。

注 4:两模块同时失效的比率不可能大于两个失效率的较小值。

在状态 S_2 中,功能模块 A 已经出现危险失效。依据诊断试验的操作,可能会有以下 3 种状态:

——如果诊断试验检测到失效,且功能模块被修复,则接着进入状态 S_5;

——S_6 紧跟着,如果诊断试验没有检测到失效,则接着进入状态 S_6;

——如果在诊断试验检测到功能模块 A 失效之前,功能模块 B 出现失效,则接着进入状态 S_8。

在状态 S_6,功能模块 A 已经出现检测不到的危险失效。如果模块 B 出现危险失效,则接着进入状态 S_8。

状态 S_8 代表安全功能失效以及试验不再起作用的危险状态。对于 PDS(SR)假定的连续试验模式,状态 S_8 代表因 PDS(SR)出现危险失效而导致"危险事件"不符合安全功能的要求。

B.3.1.6 PFH 值计算

在 B.3.1.3 和 B.3.1.4 中给出了 λ 值、诊断覆盖率因数和 β 因数。

附加的定义：

——$r_{Test}=1/8$ h,1/24 h,1/168 h,…(诊断试验率)；

——$r_{Rep}=1/8$ h(修复率)；

$T_M=10$ 年或 20 年(运行时间)。

为了确定 PFH 值，必须计算 Markov 模型的每个状态[S_i] 以时间为变量的概率级数[$p_i(t)$]。除了状态 S_1 外所有状态的概率初值为 0，状态 S_1 的概率初值为 1。一直计算到运行时间 T_M。

$$PFH_{A,B}=\frac{1}{T_M}\int_0^{T_M}[\beta_{A/B}\times\min(\lambda_{AD},\lambda_{BD})\times p_1(t)+\lambda_{BD}\times p_2(t)+\lambda_{AD}\times p_3(t)+\lambda_{BD}\times p_5(t)+\lambda_{AD}\cdot p_7(t)]dt$$

参数 $\beta_{A,B}$、r_{Rep}、r_{Test} 和 T_M 的不同值的计算结果见表 B.2。

表 B.2 子系统 A/B 的 PFH 值计算结果

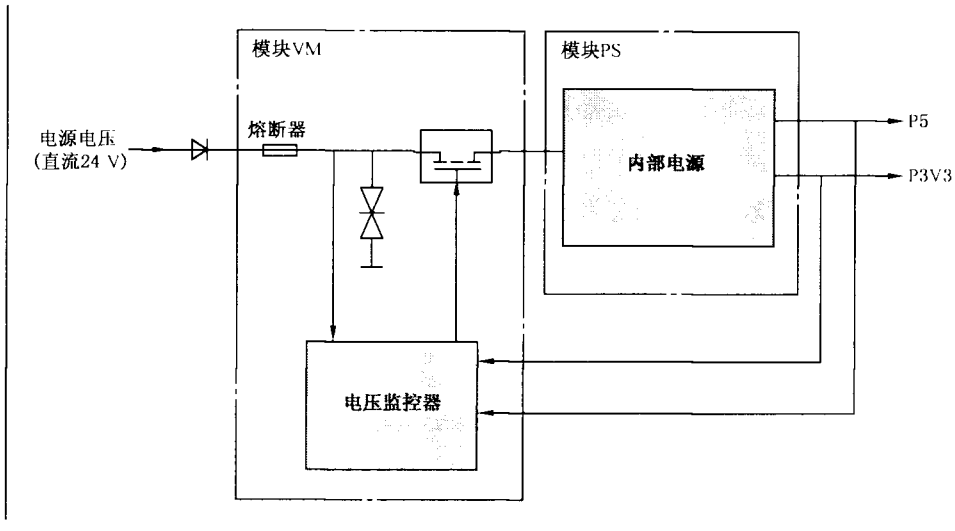
$\beta_{A/B}$	r_{Rep}	r_{Test}	T_M (年)	$PFH_{A/B}$
2%	1/8 h	1/8 h	10	6.84×10^{-10}/h
2%	1/8 h	**1/24 h**	10	6.84×10^{-10}/h
2%	1/8 h	**1/168 h**	10	6.86×10^{-10}/h
2%	1/8 h	**1/672 h**	10	6.91×10^{-10}/h
2%	1/8 h	**1/8 760 h**	10	7.72×10^{-10}/h
2%	**1/8 760 h**	1/8 h	10	6.83×10^{-10}/h
2%	1/8 h	1/8 h	**20**	7.38×10^{-10}/h
2%	1/8 h	**1/672 h**	20	7.46×10^{-10}/h
3%	1/8 h	1/8 h	20	1.05×10^{-9}/h
5%	1/8 h	1/8 h	20	1.68×10^{-9}/h
注：黑体数值为依据上一行给出的修正值。				

表 B.2 表明试验率影响的结果，持续操作时间和共同原因失效因数对 PFH 值的影响。通过参数变化给出了每个参数对 PFH 值的影响。

B.3.2 子系统“PS/VM”

B.3.2.1 功能模块的划分

对于安全功能 STO，子系统 PS/VM 内含有一个带有专用的监控器的通道。图 B.5 表明子系统被进一步分为两个功能模块，一个为内部单独电源 (PS)，一个为电压监控器电路(VM)。



说明：

P5 ——电源电压 5 V；

P3V3 ·· 电源电压 3.3 V。

图 B.5 子系统 PS/VM 的功能模块

B.3.2.2 功能模块失效率

使用 B.3.1.2 的方法确定每个功能模块的失效率。

B.3.2.3 安全失效分数

使用 B.3.1.2.3 的简化方法，功能模块失效率确定如下：

——印制线路板中安全失效所占失效比例为 50%(见注)。

注：印制线路板中危险失效所占比例也为 50%。

诊断覆盖率可依据 GB/T 20438.2—2006 中附录 A 的表进行估算。

—— 功能模块 PS 的诊断覆盖率：99%(见表 B.3)；

——功能模块 VM 的诊断覆盖率：0%(没有使用电压监控器)。

表 B.3 子系统 A/B 的诊断覆盖率因数的确定

方法(IEC 61508-2)	诊断覆盖率水平要求	方法的执行
表 A.9 使用安全断电或切换到备用电源单元进行电压控制(次级)或断电	高	通过电压监控器给 PDS(SR)断电

功能模块 PS 和 VM 电路的失效率(实际示例值)：

模块 PS：	λ_{PS} (总失效率)		250FIT
	λ_{PSS} (安全失效比例)	0.5×250FIT	125FIT
	λ_{PSD} (危险失效比例)	0.5×250FIT	125FIT
	λ_{PSDD} $DC_{PS}\times\lambda_{PSD}$	0.99×125FIT	123.75FIT
	λ_{ADU} $(1-DC_{PS})\times\lambda_{PSD}$	0.01×125FIT	1.25FIT
模块 VM：	λ_{VM} (总失效率)		250FIT
	λ_{VMS} (安全失效比例)	0.5×250FIT	125FIT

λ_{VMD} （危险失效比例） 0.5×250FIT 125FIT

依据 GB/T 20438.2—2006 中 C.1 中的 g)，计算子系统 PS/VM 的安全失效分数为：

$$SFF_{PS/VM}=[\lambda_{PSS}+(\lambda_{PSD}\times DC_{PS})]/\lambda_{PS}$$

$$=[125+(125\times 0.99)]FIT/250FIT$$

$$SFF_{PS/VM}=99.5\%$$

注：监控器模块不属于 SFF。

B.3.2.4 共同原因失效因数 $\beta_{PS/VM}$

利用 GB/T 20438.6—2006 中附录 D 的表 D.4 估算共同原因失效因数 $\beta_{PS/VM}$。

$\beta_{PS/VM}=2\%$。

B.3.2.5 可靠性模型(Markov)

子系统 PS/VM 的可靠性模型被作为 Markov 模型来执行，其状态图见图 B.6。

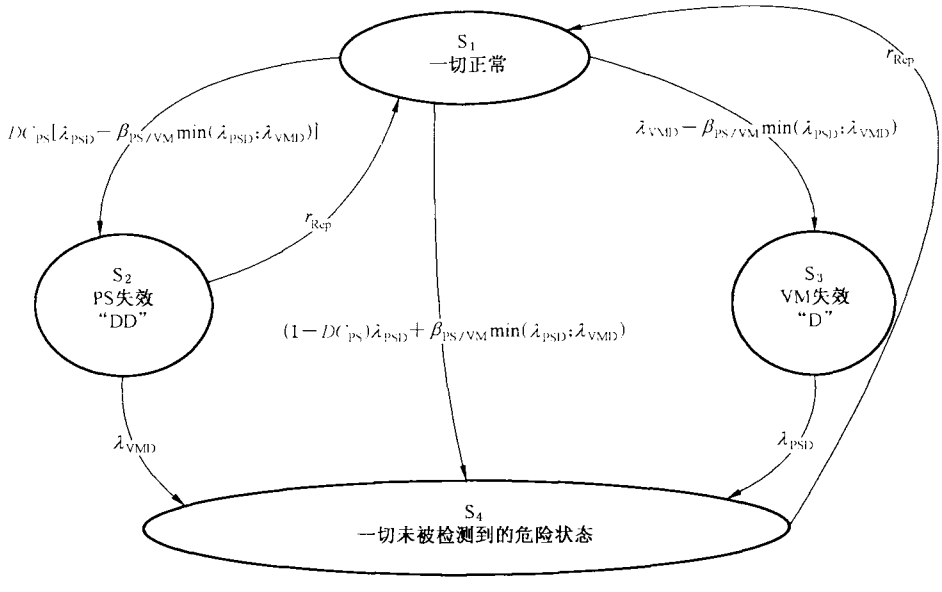


图 B.6 子系统 PS/VM 的可靠性模型(Markov)

注 1：以上 Markov 模型应被认为是一种近似法。因为由于其自身的性质，从数学角度上严格来讲，与诊断试验及事件触发的修复对应的过渡过程不符合 Markov 技术所需的条件。

注 2：电压监控器提供供电电路连续监视，所以模型内不出现试验率。由于失效率和修复率的通常值，模型可被简化。说明版本会详细描述。

由于安全状态对 PFH 值不起作用而会增加模型的复杂性，所以此模型给出了可能的危险状态，但没有安全状态。模型假定检测到失效后将 PDS(SR)断电，修复。

共同原因失效率是由因数 $\beta_{PS/VM}$ 以及功能模块 PS 和 VM 的危险失效率的较小值决定(见注)。

注 3：进一步说明：由于事实上共同原因失效率表示模块 PS 和 VM 同时发生失效而且模块的失效率是不同的，所以共同原因失效率不可能大于两个失效率的较小值。

在状态 S_2，功能模块 PS 已经检测出危险失效。如果在修复前模块 VM 出现失效，则进入状态 S_4。

在状态 S_3，功能模块 VM 出现危险失效，由于此模块内没有监控器所以没有被发现。如果功能模块 PS 出现危险失效，则进入状态 S_4。

如果功能模块 PS 未被检测到危险失效，或两个模块同时出现失效，则进入状态 S_4 且安全功能不再适用。

状态 S_4 代表，安全功能失效以及试验不再起作用的危险状态。对于 PDS(SR)假定的连续操作模式，状态 S_4 代表因 PDS(SR)出现危险失效而导致的“危险事件”不符合安全功能要求。

B.3.2.6 PFH 值计算

在 B.3.2.3 和 B.3.2.4 中给出了 λ 值、诊断覆盖率因数和 β 因数。

附加的定义(测定)：

$r_{Rep}=1/8$ h(修复率)；

$T_M=10$ 年或 20 年(运行时间)。

为了确定 PFH 值，必须计算 Markov 模型的每个状态[S_i]以时间为变量的概率级数。除了状态 S_1 外所有状态的初值为 0，状态 S_1 的初值为 1。一直计算到运行时间 T_M。

$$PFH_{PS/VM}=\frac{1}{T_M}\int_0^{T_M}[((1-DC_{PS})\times\lambda_{PSD}+\beta_{PS/VM}\times\min(\lambda_{PSD},\lambda_{VMD}))\times p_1(t)+\lambda_{VMD}\times p_2(t)+\lambda_{PSD}\times p_3(t)]dt$$

参数 $\beta_{PS/VM}$、r_{Rep} 和 T_M 的不同值的计算结果见表 B.4。

表 B.4 子系统 PS/VM 的 PFH 值计算结果

$\beta_{PS/VM}$	r_{Rep}	T_M (年)	$PFH_{PS/VM}$
2%	1/8 h	10	4.39×10^{-9}/h
2%	1/8 h	**20**	5.03×10^{-9}/h
3%	1/8 h	20	6.25×10^{-9}/h
5%	1/8 h	20	8.70×10^{-9}/h
注：黑体字值为依据上一行给出的修正值。			

B.3.3 PDS(SR)的安全功能 STO 的 PFH 值

举例，当 $r_{Rep}=1/8$ h，T_M 为可变量参数时的 PFH 值：

$PFH_{STO/PDS(SR)}=PFH_{A/B}+PFH_{PS/VM}$(见表 B.2 和表 B.4 的值)；

$PFH_{STO/PDS(SR)}$($T_M=10$ 年)$=(6.84\times10^{-10}/h+4.39\times10^{-9}/h)=5.074\times10^{-9}/h$；

$PFH_{STO/PDS(SR)}$($T_M=20$ 年)$=(7.38\times10^{-10}/h+5.03\times10^{-9}/h)=5.768\times10^{-9}/h$。

附 录 C
（资料性附录）
适用的失效率数据库

C.1 数据库

以下参考文献不是一个全部包括的表，它是一个无序排列的，是电子或非电子组件失效率数据源。需要声明的是，这些源之间并不完全一致，所以应谨慎地使用这些数据。

——IEC/TR 62380，可靠性数据手册-电子组件、PCBs 和设备的可靠性预测用通用模型，等同于 RDF 2000/可靠性数据手册，UTE C 80-810，Union Technique de I' Electricit et de la Communication(www. utc-fr. com)。

——西门子标准 SN 29500，组件失效率，(1～14 部分)；可获得于 Siemens AG，CT SR SI，Otto-Hahn-Ring6，D-81739，Munich。

电气设备可靠性预测，MIL-HDBK-217E，国防部，华盛顿 DC，1982。

电气设备可靠性预测过程，Telcordia SR-332，Issue 01，5 月(telecom-info. telcordia. com)，(Bellcore TR-332，Issee 06)。

——EPRD-电气零件可靠性数据(RAC-STD-6100)，可靠性分析中心，201Mill Street，Rome，NY13440(rac. alionscience. com)。

——NNPRD-95-非电子零件可靠性数据(RAC-STD-6100)，可靠性分析中心，201Mill Street，Rome，NY13440(rac. alionscience. com)。

——用于通讯系统的组件的可靠性数据英国手册，British Telecom(HRD5，last issue)。

——中国军用标准 GJB/z 299B。

——AT&T 可靠性手册-Klinger，David J，Yoshinao Nakada，and Maria A. Menendez，Editors，I，AT&T 可靠性手册，Van Nostrand Reinhold，1990，ISBN：0442318480。

——FIDES。2004 年 1 月的一本可靠性数据手册，由法国工业财团起草，法国国防部武器装备局指导。可向 fides@innovation. net 索取。

——IEEE Gold book。IEEE 推荐的、用于可靠的工商业电力系统设计的规程，提供工商业配电系统使用的设备的可靠性数据。IEEE 客户服务：445 Hoes Lane，PO Box 1331，Piscataway，NJ 08855-1331，U. S. A.，电话：+1 800 678 IEEE(美国和加拿大)或+1 732 981 0060(美国和加拿大之外)，传真：+1 732 981 9667，电子邮箱：customer. service@ieee. org。

——IRPH ITALTEL 可靠性预测手册-是意大利通讯公司的 CNET PDF 版本。此标准是依据同样的数据，只有一些程序和因数发生变化。Italtel IRPH 手册可用于备索：Dr. G Turconi，Direzione Qualita，Italtel Sit，CC1/2 Cascina Castelletto，20019 Settimo Milanese Mi，Ttaly。

——PRISM(RAC/EPRD)。该软件可通过以下地址获得，或包含在几个商业化的可靠性软件包中。可靠性分析中心：201 Mill Street，Rome，NY 13440-6916，U. S. A.。

C.2 与组件失效相关的有用标准

IEC 60300-3-2 可靠性管理 第 3-2 部分：应用导则 现场收集可信性数据

IEC 60300-3-5 可靠性管理 第 3-5 部分：应用导则 可靠性试验条件和统计试验原则

IEC 60319 电子元器件可靠性数据的表示和规范

IEC 60706-3 设备维修性 第3部分:数据的验证、收集、分析和表示
IEC 60721-1 环境条件分类 第1部分:环境参数及其严酷程度
IEC 61709 电子元器件 可靠性 失效率的基准条件和应力模型转换

附 录 D
（资料性附录）
故障表和故障排除

D.1 总则

表 D.1～表 D.16 中列出了一些故障模型，故障排除以及他们的逻辑依据。

为了确认，无论是永久性的故障还是非永久性的故障都应该被考虑。

故障发生的准确时刻是很关键的。如果有必要，应采取理论分析和试验确定最坏的情况，例如在系统启动、操作及停止过程中。

D.2 适用于故障排除的备注

D.2.1 排除的有效性

所有的故障排除只有当其内部器件在规定的额定值内工作时是有效的（只有当部件在额定值内操作时，所有的故障排除才有效）。

D.2.2 锡晶须生长

如果应用无铅工艺和产品，可能会发生由于锡晶须导致的电气短路（见注 1）。当使用任何组件的故障排除“短路...”时应考虑和估计（见注 2）晶须的危险（见注 3 和注 4）。

注 1：锡晶须生长这一现象主要与镀纯亮锡最后工序有关。针状突出物可增长到几百微米并可能会引起电气短路。流行理论认为晶须是由锡镀层聚集压力引起的。

注 2：以下出版物可能有利于估计：

关于测量锡和锡合金表面最后工序晶须生长的试验方法，JESD22A121.01，JEDEC 固体技术协会，2500Wilson Boulevard Arlington，VA22201-3834，www.jedec.org/ download/search/22a121-01.pdf.

锡和锡合金表面最后工序晶须易感性的环境要求，JESD201，JEDEC 固体技术协会，2500 Wilson Boulevard Arlington，VA22201-3834，www.jedec.org/ DOWNLOAD/search/JESD201.pdf。

注 3：例如：如果过高估计晶须的危害，对“电阻器短路”的故障排除是无用的，因为这种组件触点间的短路必须被注意。

注 4：关于印制线路板的晶须还没有相关报告。印刷线通常由无涂层的铜组成。衬垫可能是锡合金涂层，但是生产工艺看起来似乎不会激发晶须生长的敏感性。

D.2.3 PWB 安装部件的短路

如表 D.2 中描述的“2 条相邻的印刷线/衬垫之间的短路”的故障排除，则只能排除安装在印刷线路板（PWB）上的部件的短路。

D.3 故障模型

表 D.1 导体/电缆

考虑到的故障	故障排除	备 注
任意两导体间短路	导体间的短路包括如下： —比如通过电缆管道或铠装，进行永久的连接(固定)并且防备外来损害；或 独立的多芯电缆；或 放在电气外壳内，见备注 1)；或 用接地线单独防护	1)如果导体和外壳都满足相应要求(见 IEC 60204-1)
任一导体断路	不能	
任一导体与裸露导电部件或与地或与保护连接导体的短路	电气外壳内导体间的短路，见备注 1)	

表 D.2 印刷线路板/部件

所考虑的故障	故障排除	备 注
两个连接印刷线/印刷板的短路	依据备注 1)～3)相邻导体间的短路	PWB 的基础材料应满足 IEC 61800-5-1 的要求。 2)爬电距离和电气间隙的最小值应符合 IEC 60664-1 污染等级 2/安装类别Ⅲ；如果两条印刷线路都由一个 SELV/PELV 供电，污染等级 2/安装类别Ⅱ采用 0.1mm 的最小电气间隙。 3)安装板安装在能够防止导体被污染的外壳内，如防护等级至少达到 IP54 的外壳，印刷面被涂抗老化漆或保护层，能够覆盖所有导体路线。 注 1：试验表明焊膜可作为保护层。 注 2：依据 IEC 60664-3 进一步的防护层可减小爬电距离和间隙尺寸的尺寸
任一印刷线的断路	不能	

表 D.3 接线板

所考虑的故障	故障排除	备 注
相邻端子间短路	依照备注 1)或 2)相邻端子间短路。	1)使用的端子和连接点符合 IEC 61800-5-1 的要求。 2)通过设计保证,例如在连接点处使用热缩塑料套管
单独的端子断路	不能	—

表 D.4 多层连接器

所考虑的故障	故障排除	备 注
任两相邻插针间的短路	依照备注 1)相邻插针间短路。 如果连接器是安装在 PWB 上,备注 2)也适用	1)在多股线上使用端套或其他合适的办法。爬电距离、电气间隙及所有间隙的尺寸至少满足 IEC 60664-1:1992 安装类别Ⅲ。 2)组装板应被安装在防护等级至少为 IP54(见 EN 60529)的外壳内,并且依照 IEC 60664-3 组装板的印刷面被涂上抗老化漆或保护层并能致覆盖所有导体路线
当没有机械预防措施时,相互交换或错误的插入连接器	不能	—
任一导体[见备注 3)]对地或导电部件,或对保护导体短路	不能	3)电缆芯被看作是多针连接器的一部分
单独连接器插针的断路	不能	—

表 D.5 机电器件(例如继电器、接触器式继电器)

所考虑的故障	故障排除	备 注
当线圈失电,所有触点仍然保持在得电位置(例如由于机械故障)	不能	—
当电源通电,所有触点仍然保持在失电位置(例如由于机械故障,线圈开路)	不能	
触点不能断开	不能	
触点不能闭合	不能	
转换触点的三个端子间同时短路	如果满足备注 1)和 2),同时短路可被排除	1)爬电距离和电气间隙的最小值符合 IEC 60664-1:1992 污染等级 2/过电压类别Ⅲ。 2)变松散的导电部件不能桥接在触点和线圈之间的绝缘件上
两对触点间的短路和/或触点与线圈端子间短路	如果满足备注 1)和 2),短路可被排除	
常开触点和常闭触点同时闭合	如果满足备注 3),触点同时闭合可被排除	3)使用强制性驱动(或机械链接)的触点

表 D.6 变压器

所考虑的故障	故障排除	备 注
单独绕组的开路	不能	—
不同绕组间短路	如果满足备注 1)和 2),不同绕组间短路可被排除	1)应满足 IEC 61558 中相关部分的要求。 2)在不同的绕组间使用双层或加强绝缘或保护屏蔽。 依据 IEC 61558-1 中第 18 章试验。在 IEC 61558-1 中表 8 a)中给出了适用试验电压。 需要采取适当的措施避免线圈和绕组的短路,例如: —浸透线圈以充满单独线圈与线圈及杆体的本体之间所有的空隙;和 —在绕组导体绝缘和高温级别内使用绕组导体。 3)一旦副边短路,不应该出现高于规定的操作温度
一个绕组的短路	如果满足备注 1),一个绕组内的短路可被排除	
有效匝数比的变化	如果满足备注 1),有效匝数比的变化可被排除。亦见备注 3)指导	

表 D.7 电感

所考虑的故障	故障排除	备 注
断路	不能	—
短路	如果满足备注 1),短路可被排除	1)线圈是单层的,漆色线或浇注轴向布线轴向安装
电感值的随机变化: $0.5L_N<L<L_N$+容许偏差 在此:L_N 为电感标称值[见备注 2)]	不能	2)依据结构的类型,可能会考虑其他范围

表 D.8 电阻器

所考虑的故障	故障排除	备 注
断路	不能	—
短路	如果满足备注 1)和备注 2),短路可被排除	1)电阻器是液膜式或绕组式,它使用轴向连接,轴向安装,漆膜保护措施,以防止一旦电阻器破损,导线散开。 2)表面安装工艺的电阻器必须是薄膜金属型,封装形式 MELF,mini-MELF 或 μMELF
电阻值的随机变化: $0.5R_N<R<2R_N$ 在此:R_N 为电阻标称值[见备注 3)]	不能	3)依据结构的类型,可以考虑其他范围

表 D.9 电阻网络

所考虑的故障	故障排除	备 注
断路	不能	—
任意两个连接点间短路	不能	
任何连接点间短路	不能	
电阻值的随机变化： $0.5R_N<R<2R_N$ 式中，R_N 为电阻标称值[见备注 1)]	不能	1)依据结构的类型，可以考虑其他范围

表 D.10 电位器

所考虑的故障	故障排除	备 注
单独连接点间断路	不能	—
所有连接点间短路	不能	
任意两个连接点间短路	不能	
电阻值的随机变化： $0.5R_P<R<2R$ 式中，R_P 为电阻标称值[见备注 1)]	不能	1)依据结构的类型，可以考虑其他范围

表 D.11 电容器

所考虑的故障	故障排除	备 注
断路	不能	—
短路	不能	
电容值的随机变化： $0.5\ C_N<C<C_N$ + 容许偏差 式中，C_N 为电容标称值[见备注 1)]	不能	1)依据结构的类型，可以考虑其他范围
变化值 $\tan\delta$	不能	—

表 D.12 半导体分立器件(例如，二极管、齐纳二极管、晶体管、双向晶闸管、GTO、IGBT、电压调节器、石英晶体、光敏晶体管、发光二极管[LEDS])

所考虑的故障	故障排除	备 注
任一连接点断路	不能	—
任意两个连接点间短路	不能	
所有连接点间短路	不能	
特性变化	不能	
装置盒的爆炸	如果满足备注 1)，则可被排除	1)供电线路短路容量局限于器件盒耐受能力

表 D.13 光耦合器

所考虑的故障	故障排除	备 注
单独连接点间断路	不能	
任意两个输入连接点间短路	不能	
任意两个输出连接点间短路	不能	
任意两个输入和输出连接点间短路	如果满足备注 1)和 2),两个输入和输出连接点间的短路可被排除	1)依据 IEC 60664-1:1992 中表 1,光耦合器符合 IEC 61800-5-1 过电压类别Ⅲ。如果使用 SELV/PELV 电源,污染等级 2/过电压类别Ⅱ适用。 2)采取措施确保光耦合器的内部故障不能导致绝缘材料的温度过高

表 D.14 不可编程式集成电路

所考虑的故障	故障排除	备 注
每个单独连接点的断路	不能	—
任意两个连接点间短路	不能	
固定故障(例如,隔离输入或断开的输出 0 和 1 短路)所有输入输出的静态信号分别或同时为“0”和“1”	不能	
输出的寄生震荡	不能	
变化值(例如模拟器件的输入/输出电压)	不能	
注:在本部分,认为小于 1 000 个门电路和/或小于 24 针的 ICs(集成电路)、运算放大器、移位寄存器和混合模块是不复杂的。此定义是任意的。		

表 D.15 可编程和/或复杂集成电路

所考虑的故障	故障排除	备 注
功能的所有或部分出现故障	不能	—
每个独立连接点的断路	不能	
任意两个节点的短路	不能	
固定故障(例如,隔离输入或断开的输出 0 和 1 短路)所有输入和输出的静态信号分别或同时为“0”和“1”	不能	
输出的寄生震荡	不能	
变化值(例如模拟器件的输入/输出电压)	不能	
由于集成电路的复杂性,被忽视的未被发现的硬件故障	不能	
注:在本部分中,认为多于 1 000 个门电路和/或多于 24 针的 IC(集成电路)是复杂的。此定义是任意的。分析应该识别其余的能够影响安全功能操作的故障。		

表 D.16 运动和位置反馈传感

所考虑的故障	故障排除	备 注
总则		
接线电缆上任意两个导体间短路	表 D.1 适用	
接线电缆上任一导体的断路	不能	
单个或多个输入或输出信号同时固定在 0 或 1	不能	
单个或多个输入或输出同时出现断路或高阻抗情况	不能	
输出振幅减少或增加	不能	
一个或多个输出发生振荡	不能	考虑同相多个输出相的震荡
输出信号间的相移变化	不能	例如，由于编码器码盘被污染
静止时连接的损耗： —安装在电动机底盘的传感器壳体； —安装在电动机轴的传感器轴	准备 FMEA 以及证明机械固定的长期完整性	输出信号等于停止 如果要排除故障，底盘上传感器外壳以及电动机轴零件上传感器轴的设计通常能够承受几乎 20 的过压因数，并应提供专业维护信息
工作时连接的损耗或松动： —安装在电动机底盘的传感器壳体； —安装在电动机轴的传感器轴	准备 FMEA 以及证明机械固定的长期完整性	可能产生的效应： —传感器轴的静态偏移； —传感器轴的动态移位； —错误输出信号/零速信号。 如果要排除故障，底盘上传感器外壳以及电动机轴零件上传感器轴的设计通常能够承受几乎 20 的过压因数，并应提供专业维护信息
固定措施的松动[a]（如光学编码器的码盘）	不能	输出指示错误位置
二极管不发光	不能	
附加的由旋转传感器产生的带 Sin/Cos 输出信号，模拟信号发生器		
静态输入和输出，一个或多个信号，供电电压的幅值内	不能	
信号形状的变化	不能	例如，无 Sin/Cos 类型信号，信号偏移
Sin 和 Cos 输出信号互换	如果没有采用电气组件从多个信号源选择输出信号，则允许故障排除	
附加：带有方波输出信号的增量旋转传感器		
输出震荡	不能	
输出信号停止	不能	例如，由于划伤的盘
0 脉冲故障：太短、太长或重复	不能	例如，由于机械破坏

表 D.16（续）

所考虑的故障	故障排除	备　注
附加：带有增量和绝对值信号的编码器		
来自增量和绝对值信号的同时错误位置变化	如果增量数据和绝对数据是分别产生的，可排除故障	应用举例：对于绝对位置和/或通讯的附加输出的 Sin/Cos 编码器
附加：带有基于接口处理器的旋转传感器		
通讯故障： 重复； 丢失； 插入； 错误的顺序； 错误的数据； 延时	不能	等同于通讯总线的故障模型
附加：旋转传感器，多匝		
错误转数	不能	可能对单个旋转信号不能产生影响
附加：合成输出信号的旋转传感器		
由于合成故障导致的错误输出信号	不能	
附加：通过计数器获得位置值的旋转传感器		
由于计算错误导致位置错误	不能	
附加：线性传感器		
所安装的可读传感器已破坏	准备 FMEA 以及证明机械固定的长期完整性	如果要求排除故障，传感器外壳的设计通常能承受过载，并应提供专门维护信息
容量测定的静态偏移（例如，光编码器条）	不能	
被损坏的容量测定（例如，光编码器条）	不能	脉冲形状的变化，在增量编码器上脉冲故障
附加：带有信号处理/基准信号发生器的分解器		
基准频率的交叉耦合	不能	
—中央计时器出现故障； —A/D 变流器不能变换启动； —错误的时间采样 & 关断间隔	不能	
A/D 变流器误值		例如，由于过调制导致过高基准点压
A/D 变流器值		
基准信号发生器上无频率		
基准信号发生器频率错误		

表 D.16（续）

所考虑的故障	故障排除	备　注
基准信号发生器不能周期信号		
单个信号处理器的增益误差或震荡(Ref,Sin,Cos)		
对装置的磁影响	对装置采取适当屏蔽	例如,由于电磁制动器的磁场
[a] 不适用于分解器。		
注：此表格是假定使用指定的光学传感器,如果使用其他传感器(例如感应传感器),则产生相应的故障。		

参 考 文 献

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

[2] 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)

[3] 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)

[4] GB/T 16935.3—2005 低压系统内设备的绝缘配合 第3部分:利用涂层、罐封和模压进行防污保护(IEC 60664-3:2003)

[5] GB 19212.1 2008 电力变压器、电源、电抗器和类似产品的安全 第1部分:通用要求和试验(IEC 61558-1:2005)

[6] 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)

[7] GB/T 21109.1—2007 过程工业领域安全仪表系统的功能安全 第1部分:框架、定义、系统、硬件和软件要求(IEC 61511-1:2003)

[8] GB/T 24339.1—2009 轨道交通 通讯、信号和处理系统 第1部分:封闭式传输系统中的安全相关通讯(IEC 62280-1:2002)

[9] GB/T 24339.2 2009 轨道交通 通讯、信号和处理系统 第2部分:开放式传输系统中的安全相关通讯(IEC 62280-2:2002)

[10] IEC 61511(all parts) Functional safety -Safety instrumented systms for the process industry sector

[11] IEC 61558 (all parts) Safety of power transformers, power supplies, reactors and similar products

[12] IEC 60300-3-1 Dependability management—Part 3-1: Application guide—Analysis techniques for dependability—Guide on methodology

[13] IEC 60664-1:1992 Insulation coordination for equipment within low-voltage systems—Part 1 :Principles, requirements and tests

[14] IEC 61025 Fault tree analysis(FTA)

[15] IEC 61078 Analysis techniques for dependability—Reliability block diagram and boolean methods

[16] IEC 61165 Application of Markov techniques

[17] IEC 61513 Nuclear power plants—Instrumentation and control important to safety—General requirements for systems

[18] IEC 62061 Safety of machinery—Functional safety of safety-related electrical, electronic and programmable electronic control systems

[19] ENV 50129 Railway application—Safety-related electronic systems for signalling

[20] ISO/IEC Guide 51:1999 Safety aspects—Guidelines for their inclusion in standards

中 华 人 民 共 和 国
国 家 标 准
调速电气传动系统
第 5-2 部分：安全要求
功能
GB/T 12668.502—2013/IEC 61800-5-2:2007
*
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 3.5 字数 93 千字
2014 年 4 月第一版 2014 年 4 月第一次印刷
*
书号：155066·1-47987 定价 48.00 元

打印日期：2014年4月16日 F009A