GB/T 12668.502-2013 5-2 GB 12668 5-2
GB/T 12668.502-2013 5-2 IEC 61800-5-2:2007 5-2
GB/T 12668.502-2013 5-2
[PDS(SR)]
GB/T 12668.502-2013 5-2

GB/T 12668.502-2013 5-2 PDS SR
PDS SR 3.10 IEC 61508
GB/T 12668.502-2013 5-2
IEC 61508 PDS SR PDS SR
PDS SR / / E/E/PE PDS

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、秦皇岛科技股份有限公司、北京利德华福电气

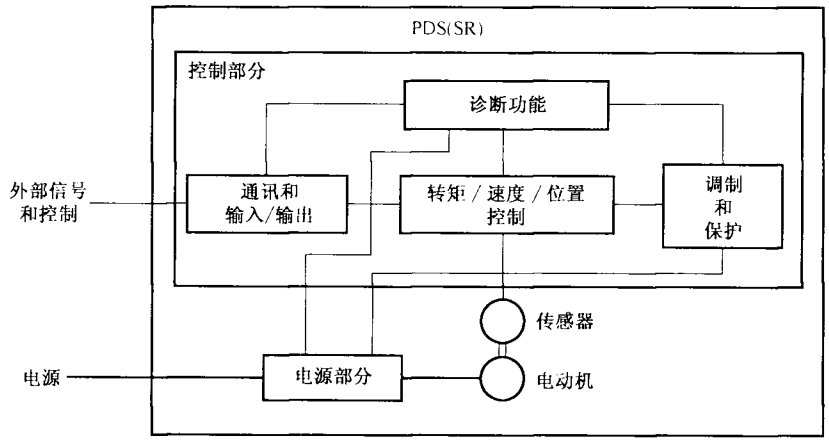


图 1 PDS(SR)的功能元件

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)

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

3.3

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)和被传动设备而考虑一台或数台设备

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

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

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

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。

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

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)

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)。

——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

[redacted]

——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；

——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)[illegible]

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

6.1.1 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

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):

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

[redacted]

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

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：修复时间为平均修复时间(见 IEC

C.2 1.1 E 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

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
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。

6.2.3.3 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。

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

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；

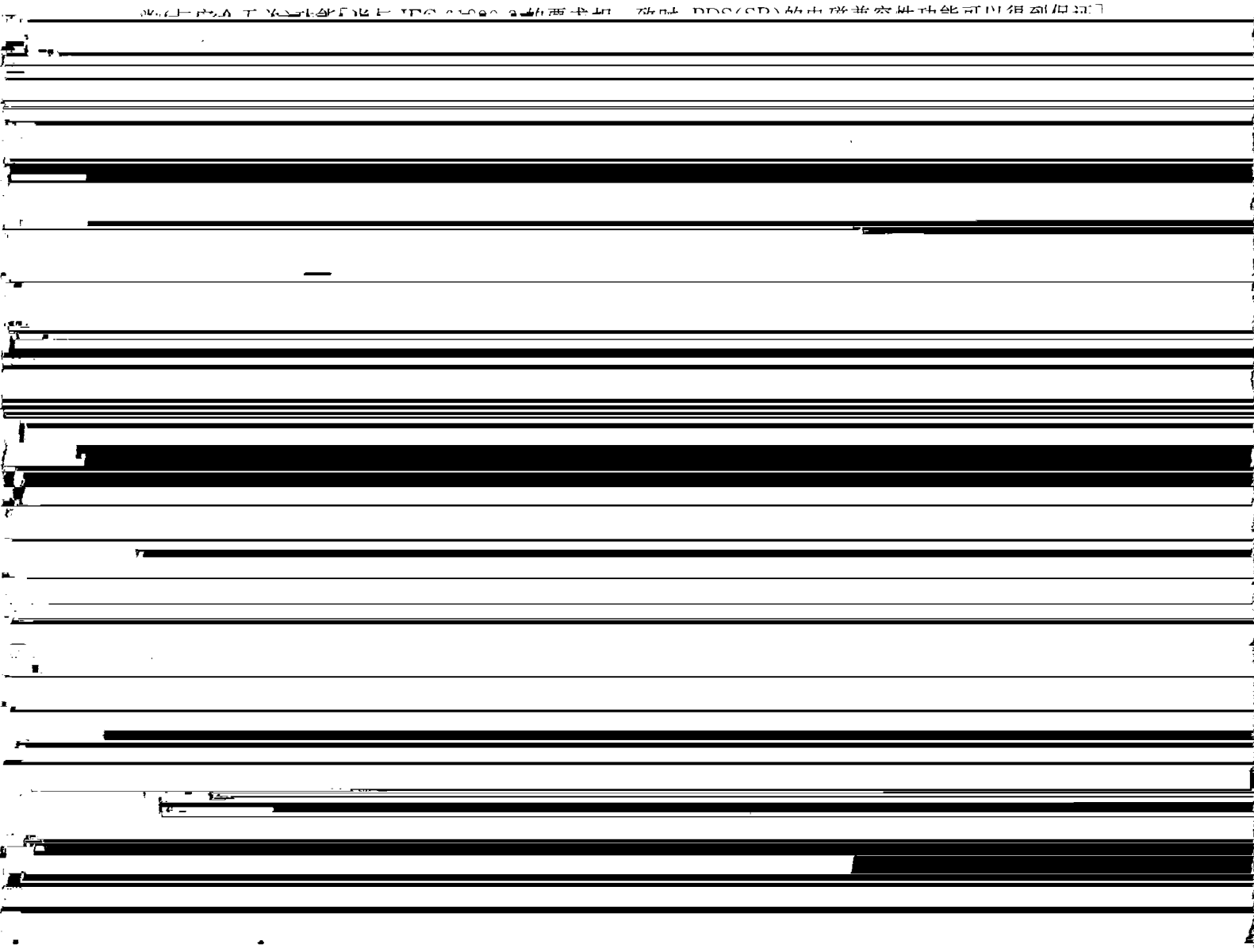
b) 环境应力包括电磁骚扰，应用 GB/T 20438.2—2006 中 A.3 和表 A.17；

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)；

6.2.5 PDS(SR)的电磁抗扰性要求

6.2.5.1 总则

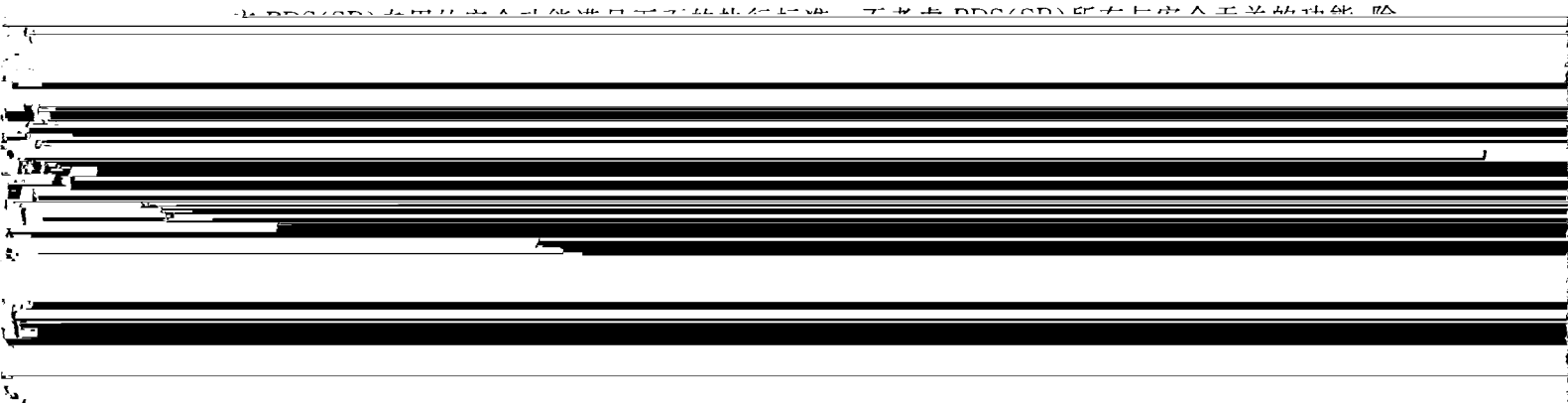
当PDS(SR)进行电磁抗扰性试验时，执行的标准在6.2.5.3中给出。这个标准不能用于设备的正



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



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。

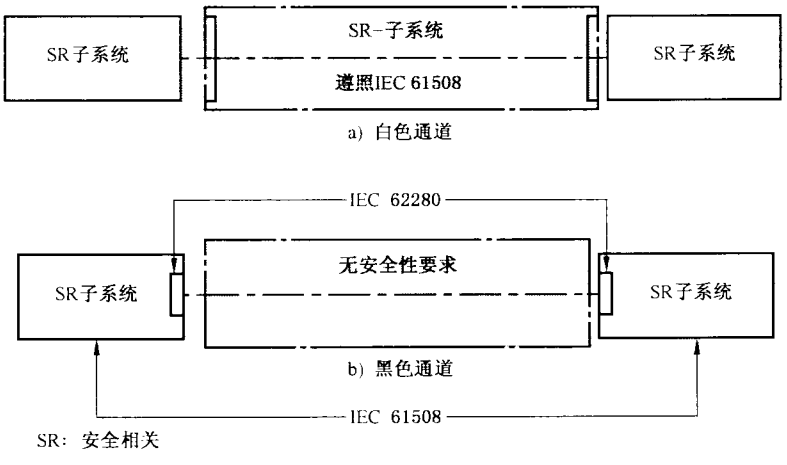


图 3 数据通讯的结构

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。

[redacted]

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

[redacted]

验证。

6.5.4 适用的集成试验

——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。

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可能被保证例如 PS 配置工具)计

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。

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)配置管理中(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	

表 A.1（续）

工　作	依　据

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

附 录 B
（资料性附录）
确定 PFH 的示例

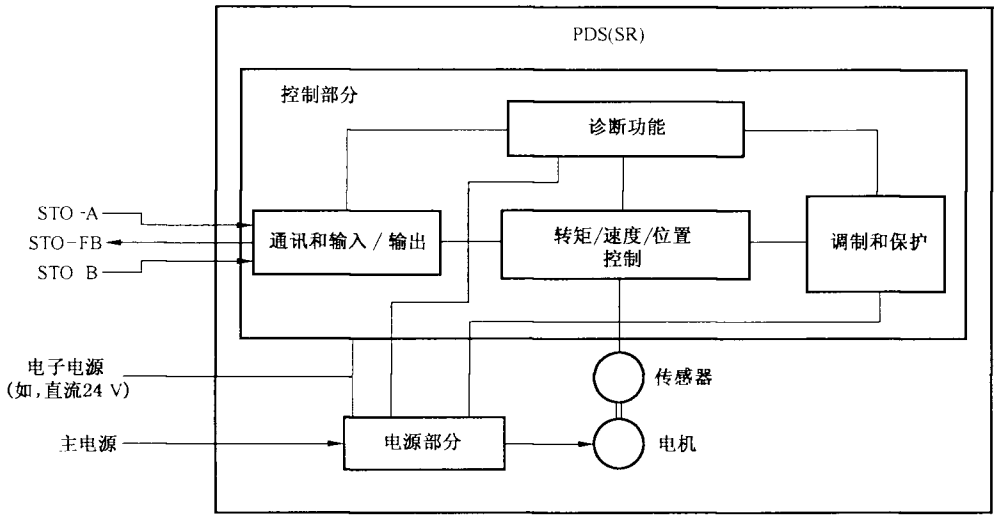
B.1 总则

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。

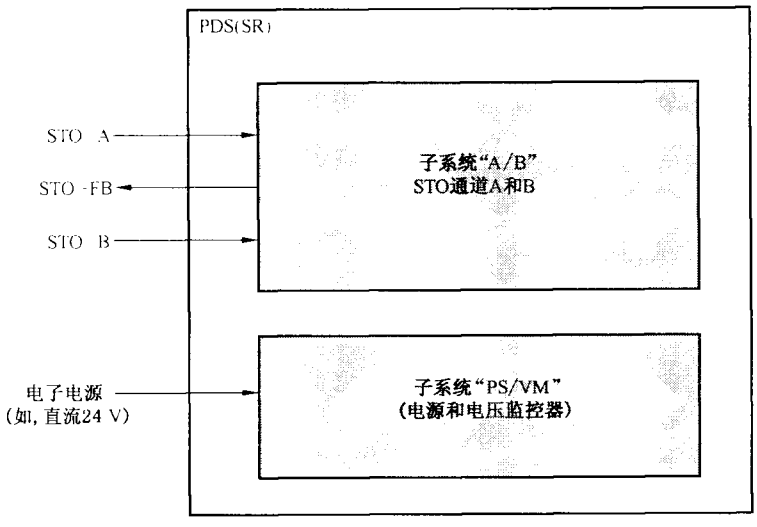


图 B.2 PDS(SR)子系统

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

由于电源(PS)只有一个通道，所以使用一个电压监控器(VM)。电源和电压监控器被模

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。

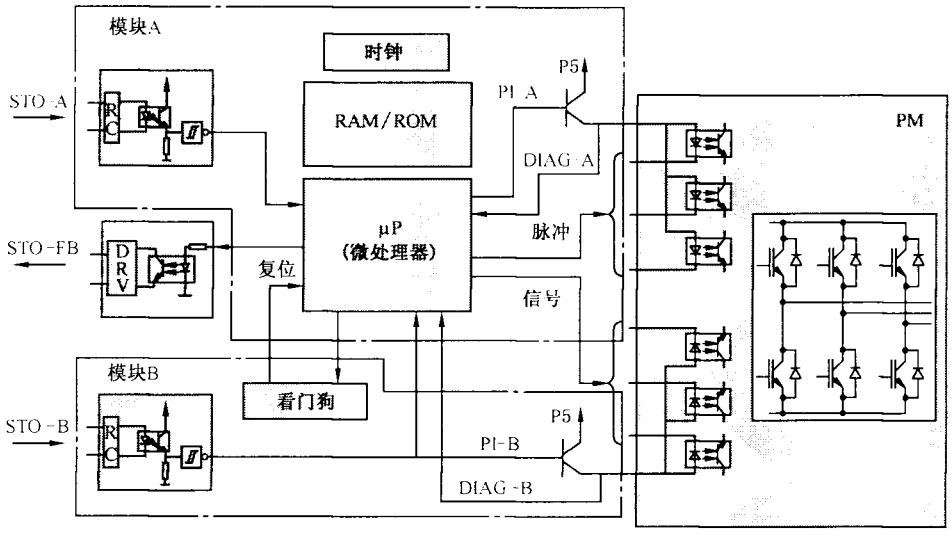


图 B.3　子系统 A/B 的功能模块

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。

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

$\beta_{A/B}=2\%$。

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。

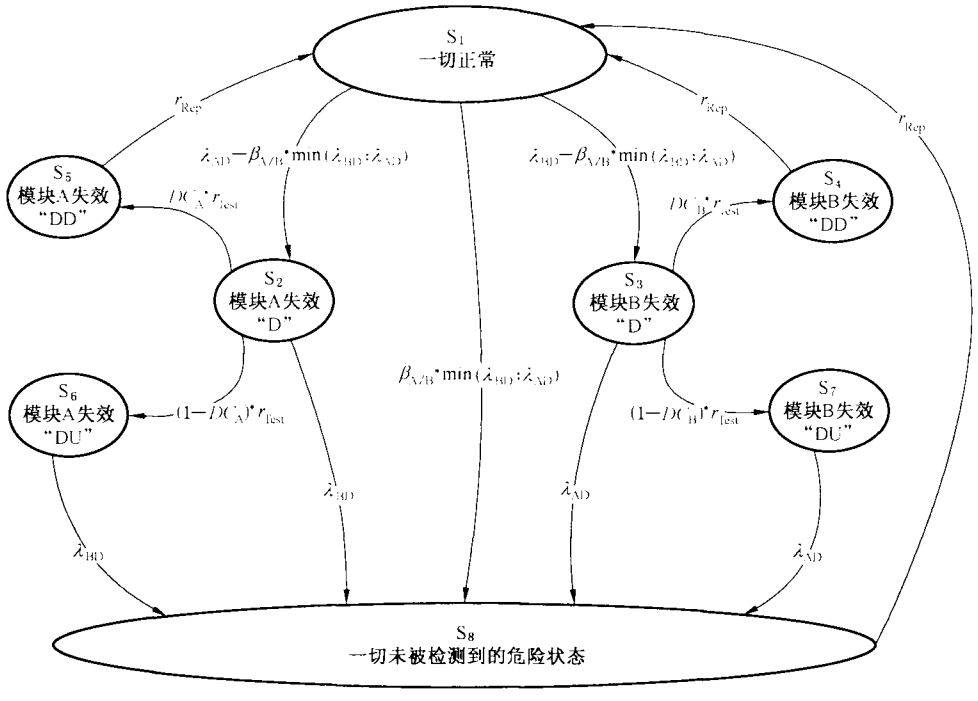


图 B.4 子系统 A/B 的可靠性模型(Markov)

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

[redacted]

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)。

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)。

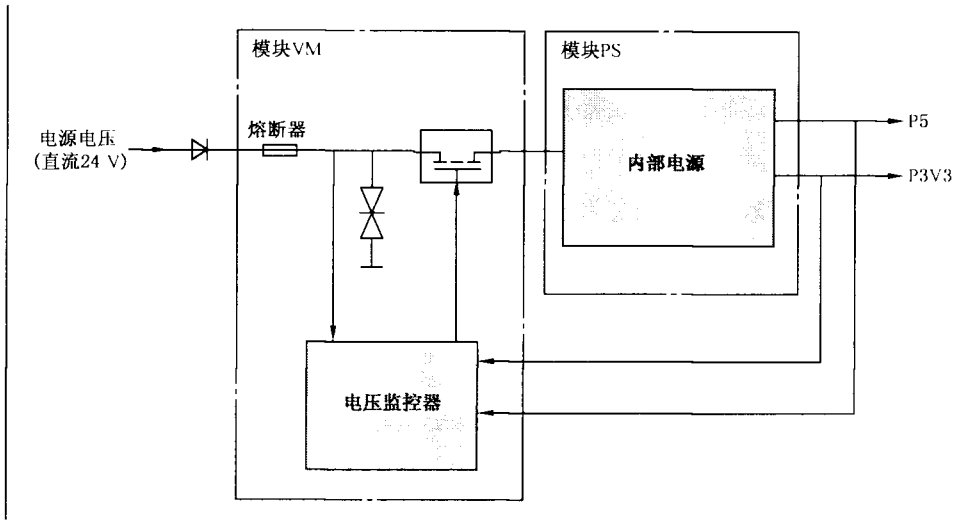
为了确定 PFH 值，必须计算 Markov 模型的每个状态[S_i] 以时间为变量的概率级数[$p_i(t)$]。除了状态 S_1 外所有状态的概率初值为 0，状态 S_1 的概率初值为 1。一直计算到运行时间 T_M。

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

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



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监控(冗余式断电	高	通过电压监控器给 PDS(SR)断电

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 β

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。

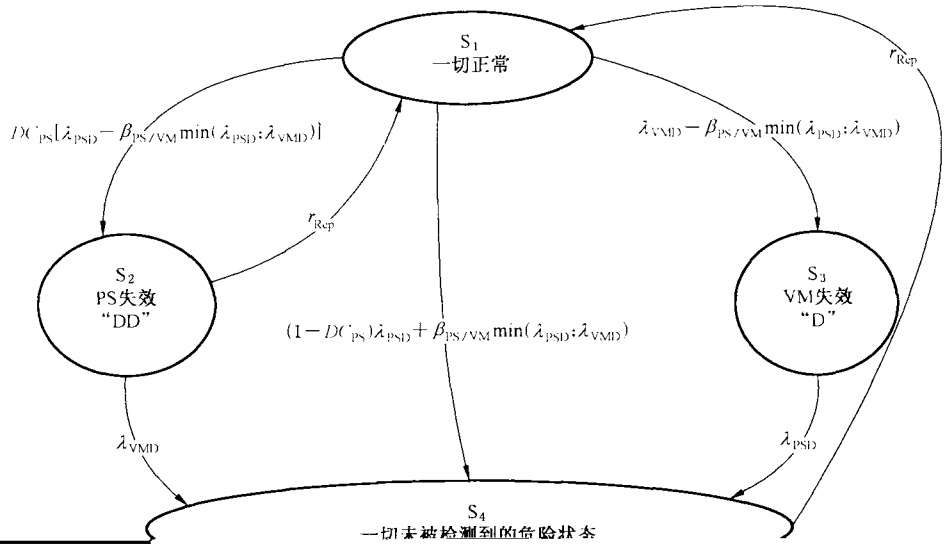


图 B.6 子系统 PS/VM 的可靠性模型（Markov）

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。

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 代表用 PDS(SD)出现危险失效而导致的"危险事件"无管人安全功能仍然要求

B.3.2.6 PFH 值计算

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。

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

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。

[redacted]

——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 l'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。

[redacted]

——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)。

[redacted]

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。

[redacted]

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

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
		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

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	1)使用的端子和连接点符合 IEC 61800-5-1 的要求。

表 D.4 多层连接器

所考虑的故障	故障排除	备 注
		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:

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。
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	

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	

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

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：	准备 FMEA 以及证明机械固定的	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。

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	如果增量数据和绝对数据只能	应用举例：对于位置和速

表 D.16（续）

所考虑的故障	故障排除	备　注
基准信号发生器无能量期信号		

参 考 文 献

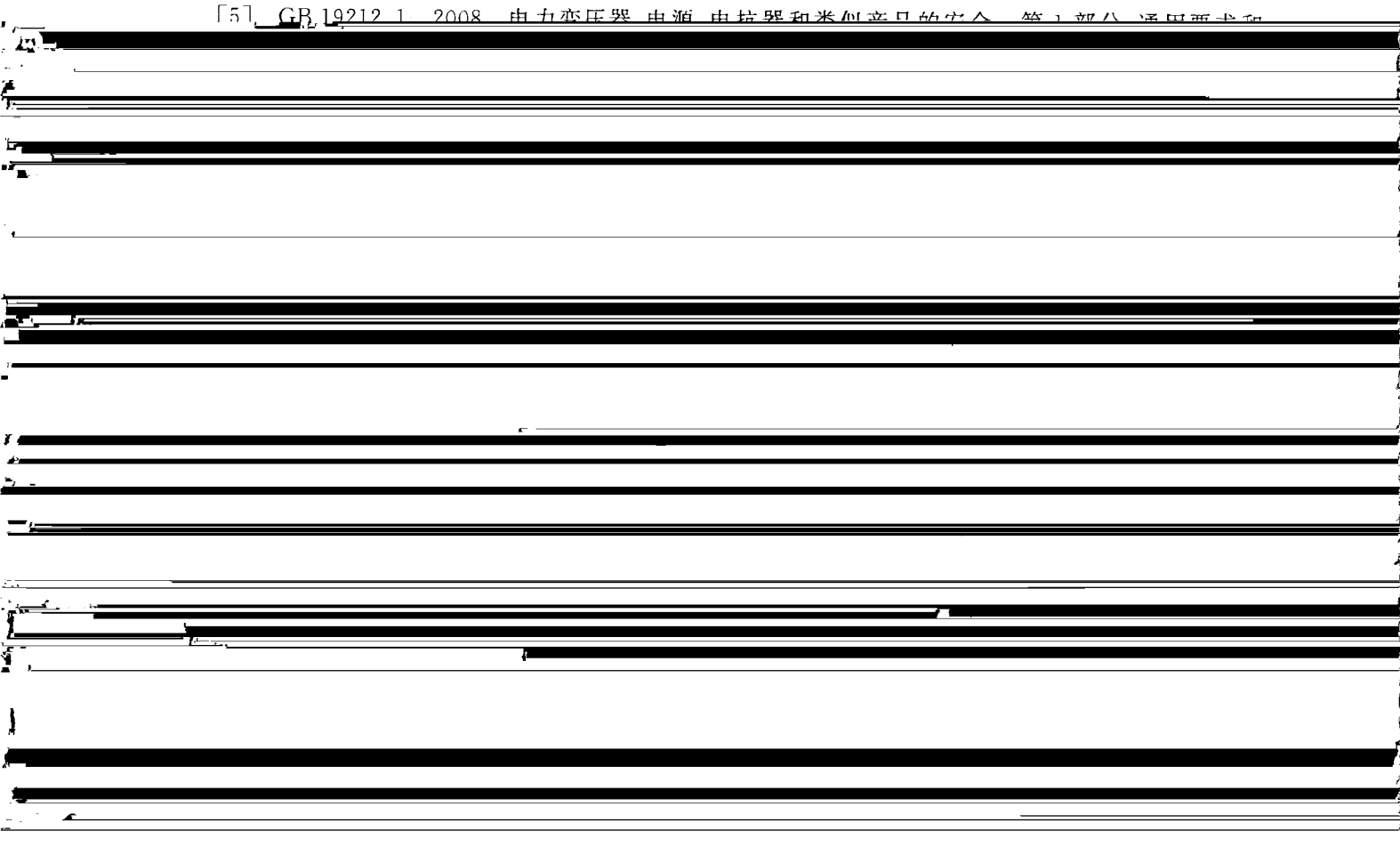
[1] GB/T 2900.13—2008 电工术语 可信性与服务质量(IEC 60050-191:1990)

[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



[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—

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)