CEPIC

ICS 13.110
J 09

# 中华人民共和国国家标准

GB/T 16855.1—2008/ISO 13849-1:2006
代替 GB/T 16855.1—2005

# 机械安全　控制系统有关安全部件　第1部分：设计通则

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

(ISO 13849-1:2006, IDT)

2008-08-25 发布　　2009-04-01 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

CEPIC



# 目　次


前言 · Ⅲ
引言 · Ⅳ
1　范围 · 1
2　规范性引用文件 · 1
3　术语、定义、符号和缩写 · 1
4　设计方面的考虑 · 7
4.1　设计中的安全目标 · 7
4.2　风险减小策略 · 8
4.3　确定所需的性能等级($PL_r$) · 10
4.4　SRP/CS 的设计 · 10
4.5　所需的性能等级 PL 的估计及其与 SIL 的关系 · 11
4.6　软件的安全要求 · 15
4.7　检验达到的 PL 是否满足 $PL_r$ · 18
4.8　设计的人类功效学方面 · 18
5　安全功能 · 18
5.1　安全功能技术规范 · 18
5.2　安全功能详述 · 20
6　类别以及与 $DC_{avg}$、CCF 和每个通道 $MTTF_d$ 的关系 · 22
6.1　一般要求 · 22
6.2　类别规范 · 22
6.3　用于实现全部 PL 的 SRP/CS 组合 · 27
7　故障考虑和故障排除 · 28
7.1　概述 · 28
7.2　故障考虑 · 28
7.3　故障排除 · 28
8　确认 · 29
9　维护 · 29
10　技术文件 · 29
11　使用信息 · 29
附录 A（资料性附录）　要求的性能等级($PL_r$)的确定 · 31
附录 B（资料性附录）　模块法和有关安全的模块图 · 33
附录 C（资料性附录）　单个元件 $MTTF_d$ 值的计算或估计 · 34
附录 D（资料性附录）　估计每个通道 $MTTF_d$ 的简化方法 · 40
附录 E（资料性附录）　对功能和模块的诊断覆盖率(DC)的估计 · 42
附录 F（资料性附录）　共因失效(CCF)的估计 · 44
附录 G（资料性附录）　系统性失效 · 46
附录 H（资料性附录）　控制系统有关安全部件组合的示例 · 48




标准分享网 www.bzfxw.com 免费下载

附录I（资料性附录） 示例 · 50
附录J（资料性附录） 软件 · 55
附录K（资料性附录） 图5的数值表示 · 57
参考文献 · 59

# 前　言

GB/T 16855《机械安全　控制系统有关安全部件》由以下3部分组成：

——第1部分：设计通则；

——第2部分：确认；

——第100部分：GB/T 16855.1的应用指南。

本部分是GB/T 16855的第1部分。

本部分等同采用ISO 13849-1:2006《机械安全　控制系统有关安全部件　第1部分：设计通则》(英文版)。

本部分等同翻译ISO 13849-1:2006。为便于使用，本部分做了下列编辑性修改：

——删除了国际标准的前言并按照我国标准的要求重新起草了前言；

——用“本部分”代替“ISO 13849的本部分”；

——用小数点“.”代替作为小数点的逗号“,”；

——修改了规范性引用文件的导语；

——对ISO 13849-1:2006引用的其他标准中，用已被等同采用为我国的标准代替对应的国际标准，未被等同采用为我国标准的直接引用国际标准。

本部分代替GB/T 16855.1—2005。与GB/T 16855.1—2005相比，主要内容修改如下：

——增加了术语：性能等级(PL)、所需的性能等级($PL_r$)、诊断覆盖率(DC)、平均危险失效时间($MTTF_d$)、危险失效、共因失效、系统失效、伤害、危险、危险状态、风险、遗留风险、风险评价、风险分析、风险评定、机器的预定使用、可预见的误用、安全功能、监测、可编程电子系统、保护措施、任务时间、检测频率、要求频率、维修率、机器控制系统、安全完整性等级、有限可变语言、全可变语言、应用软件、嵌入式系统；

——删除了术语：控制系统安全性、控制系统安全功能；

——第4章中增加了确定所需的性能等级(4.3)、所达到的性能等级(PL)的估计及其与SIL的关系(4.5)、软件的安全要求(4.6)和检验所达到的PL是否满足$PL_r$的要求(4.7)；

——第6章内容增加了类别与$DC_{avg}$、CCF和每个通道$MTTF_d$的关系；

——将原标准中的第10章细分为技术文件(第10章)和使用信息(第11章)两章；

——修改了附录A、附录B、附录C和附录D，并增加了附录E、附录F、附录G、附录H、附录I、附录J和附录K。

本部分的所有附录均为资料性附录。

本部分由全国机械安全标准化技术委员会(SAC/TC 208)提出并归口。

本部分起草单位：机械科学研究总院中机生产力促进中心。

本部分主要起草人：张晓飞、李勤、宁燕、富锐、付大为、张维、杨岭、盛晓敏、程红兵。

本部分所代替标准的历次版本发布情况为：

——GB/T 16855.1—1997、GB/T 16855.1—2005。



标准分享网 www.bzfxw.com 免费下载

# 引　言

机械安全标准的结构如下：

a) A类标准(基础安全标准)，给出适用于所有机械的基本概念、设计原则和一般特征。

b) B类标准(通用安全标准)，涉及机械的一种安全特征或使用范围较宽的一类安全防护装置：

——B1类，特定的安全特征(如安全距离、表面温度、噪声等)标准：

——B2类，安全装置(如双手操纵装置、联锁装置、压敏装置、防护装置)标准。

c) C类标准(机器安全标准)，对一种特定的机器或一组机器规定出详细的安全要求的标准。

依照GB/T 15706.1中的规定，本部分属于通用安全标准(B1类)。

对于按照C类标准设计和制造的机器，当C类标准中的条款与A类或B类标准中所述的条款不一致时，优先采用C类标准。

本部分的目的是在控制系统的设计和评价中给出对所涉及的控制系统的指南，并为正在准备制定希望符合欧盟指令98/37/EC《机械指令》附录Ⅰ"基本安全要求"的B2类或C类标准的各技术委员会(TC)提供指南。本部分不对符合其他欧盟指令给出具体指南。

作为机器全面风险减小策略的一部分，设计者通常愿意通过应用具有一种或多种安全功能的防护装置来达到某种程度的风险减小。

用于提供安全功能的机器控制系统部件称为控制系统有关安全部件(SRP/CS)，它们由硬件和软件组成，既可独立于机器控制系统，也可是与机器控制系统的组成部分。除了提供安全功能以外，SRP/CS也能提供操作功能(例如：双手操纵装置作为过程启动的一种手段)。

控制系统有关安全部件在预期条件下执行安全功能的能力分为5级，称之为性能等级(PL)。这些性能等级由每小时发生危险失效的概率来定义(见表3)。

安全功能危险失效的概率取决于几个因素，包括：软硬件结构、故障检测装置的范围[诊断覆盖率(DC)]、部件的可靠性[平均危险失效时间(MTTF$_d$)、共因失效(CCF)]、设计流程、工作压力、环境条件和操作程序等。

为了帮助设计者对所达到的PL容易进行评价，本部分采用了根据故障条件下具体设计准则和具体行为来进行结构分类的方法。这些类别分为5类，称之为B类、1类、2类、3类和4类。

性能等级和类别适用于如下控制系统有关安全部件，例如：

——保护装置(例如：双手操纵装置、联锁装置)、电敏保护装置(例如：光栅)、压敏装置：

——控制单元(例如：控制功能、数据处理、监测等的逻辑单元)：

——动力控制元件(例如：继电器、阀门等)。

以及所有机械上执行安全功能的控制系统——从简单装置(例如：小型厨房炊机具或自动门等)到复杂制造业设备(例如：包装机械、印刷机械、压力机等)。

本部分的目的是提供明确的基础用以评价应用SRP/CS(以及机器)的设计和性能，例如：第三方评价、自我评价或独立实验室评价。

应用IEC 62061和本部分时推荐的信息

IEC 62061和本部分规定了设计和执行机器控制系统有关安全部件的要求。根据这两个标准的范围，采用其中任何一个标准都可假定满足了相关的基本安全要求。表1概括了IEC 62061和本部分的范围。

CEPIC



表 1 IEC 62061 和本部分的应用推荐

| | 执行有关安全控制功能的技术 | GB/T 16855.1 | IEC 62061 |
|---|---|---|---|
| A | 非电，例如：液压 | X | 没有包括 |
| B | 机电，例如：继电器和(或)简单电子器件 | 限制在指定结构[a]内且最大为 PL=e | 所有结构，最大为 SIL3 |
| C | 复杂电子器件，例如：可编程的 | 限制在指定结构[a]内且最大为 PL=d | 所有结构最大为 SIL3 |
| D | A 与 B 组合 | 限制在指定结构[a]内且最大为 PL=e | X[c] |
| E | C 与 B 组合 | 限制在指定结构内且最大为 PL=d | 所有结构最大为 SIL3 |
| F | C 与 A 组合，或 C 与 A、B 组合 | X[b] | X[c] |

X 表示此项由该栏标题中所示的标准处理。

[a] 指定结构在 6.2 中规定，目的是给出量化性能等级的简单方法。

[b] 对于复杂电子器件，采用按照本部分的指定结构，且最大为 PL=d，或者 IEC 62061 中的任意结构。

[c] 对于非电技术，采用本部分中的部件作为子系统。



标准分享网 www.bzfxw.com 免费下载

# 机械安全　控制系统有关安全部件
# 第1部分:设计通则

## 1　范围

本部分提供了包括软件设计在内的控制系统有关安全部件(SRP/CS)设计和集成的安全要求和指导原则。对于这些SRP/CS的部件,本部分规定了包括执行安全功能所需的性能等级在内的特征。本部分适用于所有种类机械的SRP/CS,不管其采用的何种技术和能量(电、液压、气动、机械等)。

本部分未规定特殊应用中的安全功能或性能等级。

本部分提供了采用可编程电子系统的SRP/CS的具体要求。

本部分未提供设计SRP/CS的部件的具体要求。然而,可使用已给出的原则,例如:类别或性能等级。

注1:SRP/CS的部件示例:继电器、电磁阀、位置开关、PLC、电动机控制单元、双手操纵装置、压敏设备等。对于这些产品的设计,重要的是要参考特别适用的标准。例如:GB/T 19671、GB/T 17454.1和GB/T 17454.2。

注2:所需的性能等级的定义见3.1.24。

注3:本部分提供的关于可编程电子系统的要求与IEC 62061中给出的设计和开发机械有关安全的电气、电子和可编程控制系统的方法原理是一致的。

注4:对于PLC等的嵌入软件中的有关安全部件见GB/T 20438.3—2007中的第7章。

注5:也可见表1。

## 2　规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分。然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

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 12100-1:2003,IDT)

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,IDT)

GB/T 16856.1—2008　机械安全　风险评价　第1部分:原则(ISO 14121-1:2007,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 20438.4—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,IDT)

IEC 60050-191:1990　国际电工词汇　第191章:可信性与业务质量

## 3　术语、定义、符号和缩写

### 3.1　术语和定义

GB/T 15706.1—2007、IEC 60050-191:1990确立的以及下列术语和定义适用于本部分。

3.1.1

**控制系统有关安全部件 safety-related part of a control system**

**SRP/CS**

控制系统中响应有关安全输入信号并产生有关安全输出信号的部件。

注1：控制系统有关安全部件的组成，以有关安全的输入信号被触发为起始点（例如：致动凸轮和位置开关滚轮等），以控制元件的动力输出（例如：接触器的主触点等）为终止点。

注2：如果监测系统用于诊断，也可认为它们是SRP/CS。

3.1.2

**类别 category**

**Cat.**

控制系统有关安全部件在防止故障能力以及故障条件下后续行为方面的分类，它通过部件的结构布置、故障检测和（或）部件可靠性来达到。

3.1.3

**故障 fault**

产品不能执行所需功能的状态，预防性维修或其他计划性活动或缺乏外部资源的情况除外。

注1：故障通常是产品本身失效后的状态，但也可能在失效前就存在。

[IEC 60050-191:1990,05-01]

注2：本部分中，"故障"意思是随机故障。

3.1.4

**失效 failure**

产品执行所要求功能能力的终止。

注1：失效后，产品就有故障。

注2："失效"是事件，区别于作为一种状态的"故障"。

注3：定义的概念不使用与仅由软件组成的产品。

[IEC 60050-191:1990,04-01]

注4：本部分不包括只影响控制器进程的失效。

3.1.5

**危险失效 dangerous failure**

使控制系统有关安全部件（SRP/CS）处于潜在的危险状态或丧失功能状态的失效。

注1：潜在是否成为事实取决于系统的通道结构，冗余系统中，危险硬件失效不太可能导致全面的危险状态或功能丧失状态

注2：改自GB/T 20438.4—2006中的定义3.6.7。

3.1.6

**共因失效 common cause failure**

**CCF**

同一事件引起的不同产品的失效，这些失效相互之间没有因果关系。

[IEC 60050-191-am1:1999,04-23]

注：共因失效不宜与共模失效相混淆（见GB/T 15706.1—2007,3.34）。

3.1.7

**系统失效 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1：没有修正的矫正性维护通常不能消除失效原因。

注2：系统失效可通过模拟失效原因引起。



标准分享网 www.bzfxw.com 免费下载

CEPIC



[IEC 60050-191:1990.04-19]

注3：以下情况中系统失效的原因包括人员错误：

——安全要求规范；

——硬件的设计、制造、安装和操作；

——软件的设计和执行等。

3.1.8

**抑制 muting**

SRP/CS安全功能暂时的自动暂停。

3.1.9

**手动复位 manual reset**

重新启动机器前，控制系统有关安全部件(SRP/CS)中用作手动恢复一种或多种安全功能的功能。

3.1.10

**伤害 harm**

对健康产生的生理上的损伤或危害。

[GB/T 15706.1—2007,3.5]

3.1.11

**危险 hazard**

潜在的伤害源。

注1："危险"一词可由其起源(例如：机械危险和电气危险)、或其潜在伤害的性质(例如：电击危险、切割危险、中毒危险和火灾危险)进行限定。

注2：本定义中的危险包括：

——在机器的预定使用期间，始终存在的危险(例如：危险运动部件的运动、焊接过程中产生的电弧、不健康的姿势、噪声、高温)；

——或者意外出现的危险(例如：爆炸、意外启动引起的挤压危险、泄漏引起的喷射、加速/减速引起的坠落)。

[GB/T 15706.1—2007.3.6]

3.1.12

**危险状态 hazardous situation**

指人员暴露于具有至少一种危险的环境。这类暴露可能会立即或在一定时间之后对人员产生伤害。

[GB/T 15706.1—2007.3.9]

3.1.13

**风险 risk**

伤害发生概率和伤害发生的严重程度的综合。

[GB/T 15706.1—2007.3.11]

3.1.14

**遗留风险 residual risk**

采取保护措施之后仍然存在的风险。

见图2。

注：改自GB/T 15706.1—2007中的定义3.12。

3.1.15

**风险评价 risk assessment**

包括风险分析和风险评定在内的全过程。

[GB/T 15706.1—2007,3.13]

3.1.16

**风险分析 risk analysis**

机器限制的确定，危险的识别和风险的评估的组合。

[GB T 15706.1- 2007,3.14]

3.1.17

**风险评定 risk evaluation**

以风险分析为基础,判断是否已达到减小风险的目标。

[GB T 15706.1—2007,3.16]

3.1.18

**机器的预定使用 intended use of a machine**

按照使用说明书提供的信息使用机器。

[GB/T 15706.1—2007,3.22]

3.1.19

**可预见的误用 reasonably foreseeable misuse**

不是按设计者预定的方法而是按照容易预见的人的习惯来使用机器。

[GB T 15706.1 - 2007,3.23]

3.1.20

**安全功能 safety function**

其失效后会立即造成风险增加的机器功能。

[GB T 15706.1—2007,3.28]

3.1.21

**监测 monitoring**

部件或元件执行其功能的能力下降或过程条件的改变使风险增加时,保证触发保护措施的安全功能。

3.1.22

**可编程电子系统 programmable electronic system**

**PES**

基于一个或多个可编程电子装置的控制防护或监视系统,包括系统中所有的部件诸如电源、传感器和其他输入装置,接触器及其他输出装置。

注:改自 GB T 20438.4 - 2006 中的 3.3.2。

3.1.23

**性能等级 performance level**

**PL**

在可预期条件下,用于规定控制系统有关安全部件执行安全功能的离散等级。

注:见 4.5.1。

3.1.24

**所需的性能等级 required performance level**

$PL_r$

每种安全功能为达到所需的风险减小所应用的性能等级(PL)。

见图 2 和 A.1。

3.1.25

**平均危险失效时间 mean time to dangerous failure**

**$MTTF_d$**

预期的危险失效平均时间。

注:改自 IEC 62061:2005 中的定义 3.2.24



标准分享网 www.bzfxw.com 免费下载

3.1.26

**诊断覆盖率 diagnostic coverage**

**DC**

诊断有效性的度量，它可以是可诊断的危险失效的失效率与所有的危险失效的失效率之间的比率。

注1：诊断覆盖率存在于整个有关安全系统中或其部件中。例如：诊断覆盖率可存在于传感器、逻辑系统和(或)执行元件中。

注2：改自GB T 20438.4 2006中的定义3.8.6。

3.1.27

**保护措施 protective measure**

用于达到风险减小的措施。

示例1 通过设计者实现：本质安全设计、安全防护和附加保护措施、使用信息。

示例2 通过用户实现：组织(安全工作程序、监督、工作许可制度)、附加安全防护装置的提供和使用；个人防护装置的使用；培训。

注：改自GB/T 15706.1—2007中的定义3.18。

3.1.28

**任务时间 mission time**

$T_M$

SRP CS预定使用的时间周期。

3.1.29

**检测频率 test rate**

$r_t$

SRP/CS中检测故障的自动检测频率，即诊断检测时间间隔的倒数。

3.1.30

**要求频率 demand rate**

$r_d$

要求SRP CS进行有关安全动作的频率。

3.1.31

**维修率 repair rate**

$r_r$

从在线检测发现危险失效或系统出现明显故障到系统/部件维修或替换后重启之间时间间隔的倒数。

注：维修时间不包括进行失效检测所需要的时间段。

3.1.32

**机器控制系统 machine control system**

响应来自机器元件、操作者、外部控制设备或它们的组合的输入信号，并产生输出信号使机器按照预定方式工作的系统。

注：机器控制系统能可使用任何技术或各种技术的组合(例如：电气、电子、液压、气动、机械等)。

3.1.33

**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)，用于规定分配给E/E/PE有关安全系统的安全功能的安全完整性要求。在这里安全完整性等级4是最高的，安全完整性等级1是最低的。

[GB/T 20438.4—2006,3.5.6]

3.1.34

**有限可变语言 limited variability language**

**LVL**

能够结合预定义和专用的库函数来实现安全要求规范的一种语言。

注1：改自 IEC 61511-1:2003。

注2：GB/T 15969.3 中给出了 LVL(梯形逻辑、功能框图)的典型应用示例。

注3：采用 LVL 的典型系统示例：PLC。

3.1.35

**全可变语言 full variability language**

**FVL**

能够实现多样功能和应用的一种语言。

示例 C、C++、汇编语言。

注1：改自 IEC 61511-1:2003 中的定义 3.2 80.1.3。

注2：使用 FVL 的典型系统示例：嵌入式系统。

注3：在机械领域，FVL 通常用在嵌入式软件中，很少用在应用软件中。

3.1.36

**应用软件 application software**

由机器制造商完成的、面向应用的软件。通常包括逻辑序列、范围、表达式，它们控制着相应输入、输出计算和结果，以满足控制系统有关安全部件(SRP/CS)的要求。

3.1.37

**嵌入式软件 embedded software**

固件 firmware

系统软件 system software

由控制器制造商提供的作为系统的一部分，并且机器的使用者无法修改的软件。

注：嵌入式软件通常由 FVL 编写。

## 3.2 符号及缩写

见表2。

**表2 符号及缩写**

| 符号及缩写 | 描 述 | 定义或出处 |
|---|---|---|
| a、b、c、d、e | 性能等级标志 | 表3 |
| AOPD | 有源光电保护装置(例如：光幕) | 附录 H |
| B、1、2、3、4 | 类别标志 | 表7 |
| $B_{10d}$ | 直到有10%零件危险失效时的周期数(针对气动元件和机电元件) | 附录 C |
| Cat. | 类别 | 3.1.2 |
| CC | 换流器 | 附录 I |
| CCF | 共因失效 | 3.1.6 |
| DC | 诊断覆盖率 | 3.1.26 |
| $DC_{avg}$ | 平均诊断覆盖率 | E.2 |
| F、F1、F2 | 暴露于危险的频率和(或)时间 | A.2.2 |
| FB | 功能模块 | 4.6.3 |



标准分享网 www.bzfxw.com 免费下载

CEPIC



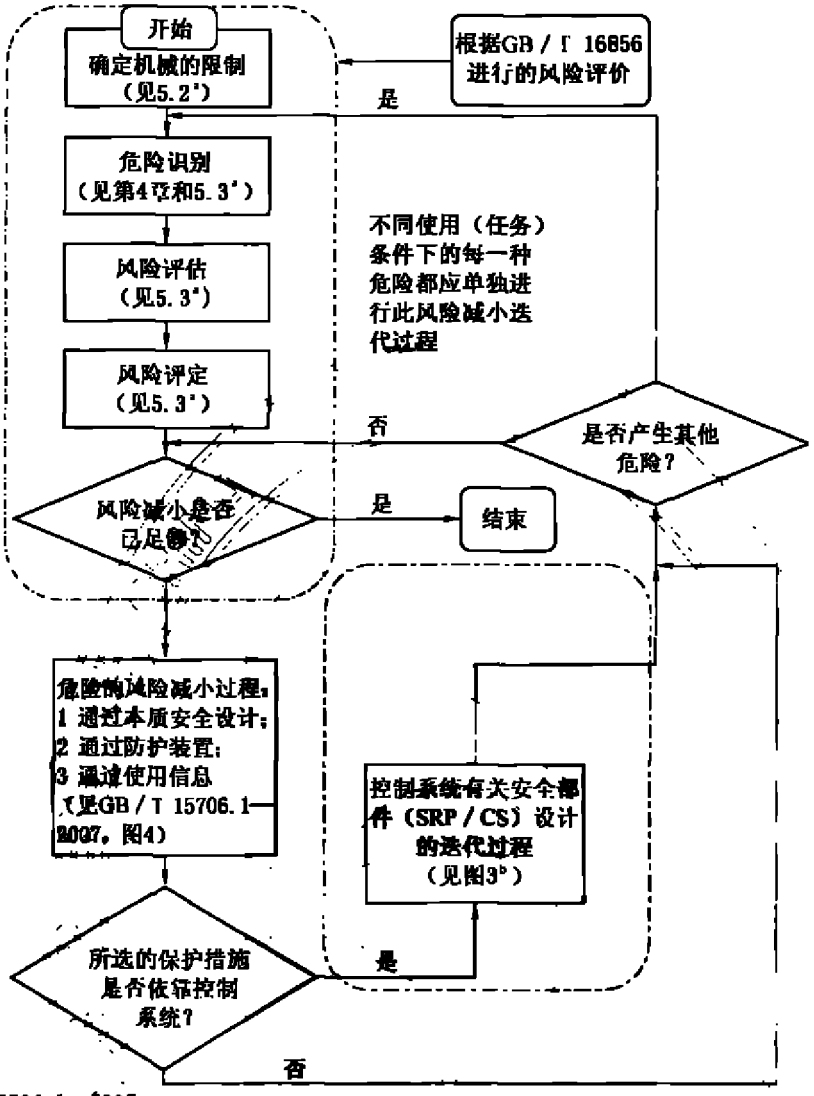
表 2（续）

| 符号及缩写 | 描　述 | 定义或出处 |
|---|---|---|
| FVL | 全可变语言 | 3.1.35 |
| FMEA | 失效模式及影响分析 | 7.2 |
| I，I1，I2 | 输入装置，例如：传感器 | 6.2 |
| $i$，$j$ | 计算指数 | 附录 D |
| I/O | 输入/输出 | 表 E.1 |
| $i_{ab}$，$i_{ac}$ | 相互连接方式 | 图 4 |
| K1B，K2B | 接触器 | 附录 I |
| L，L1，L2 | 逻辑单元 | 6.2 |
| LVL | 有限可变语言 | 3.1.34 |
| M | 电动机 | 附录 I |
| MTTF | 平均失效时间 | 附录 C |
| $MTTF_d$ | 平均危险失效时间 | 3.1.25 |
| $n$，$N$，$\bar{N}$ | 项目编号 | 6.3，D.1 |
| $N_{low}$ | SRP/CS 组合中在 $PL_{low}$ 时 SRP/CS 的编号 | 6.3 |
| O，O1，O2，OTE | 输出装置，例如：致动器 | 6.2 |
| P，P1，P2 | 避免危险的概率 | A.2.3 |
| PES | 可编程电子系统 | 3.1.22 |
| PL | 性能等级 | 3.1.23 |
| PLC | 可编程逻辑控制器 | 附录 I |
| $PL_{low}$ | SRP/CS 组合中 SRP/CS 的最低性能等级 | 6.3 |
| $PL_r$ | 所需的性能等级 | 3.1.24 |
| $r_d$ | 要求频率 | 3.1.30 |
| RS | 旋转传感器 | 附录 I |
| S，S1，S2 | 伤害的严重程度 | A.2.1 |
| SW1A，SW1B，SW2 | 位置开关 | 附录 I |
| SIL | 安全完整性等级 | 表 4 |
| SRASW | 有关安全应用软件 | 4.6.3 |
| SRESW | 有关安全嵌入式软件 | 4.6.2 |
| SRP | 有关安全部件 | 一般要求 |
| SRP/CS | 控制系统有关安全部件 | 3.1.1 |
| TE | 试验要求 | 6.2 |
| $T_M$ | 任务时间 | 3.1.28 |

## 4　设计方面的考虑

### 4.1　设计中的安全目标

SRP/CS 的设计和构造应充分考虑 GB/T 15706 和 GB/T 16856 中的原则（见图 1 和图 3）。还应考虑所有预定使用和可预见的误用。




[a] 参见 GB/T 15706.1—2007；

[b] 参见本部分

图 1 风险评价/风险减小概况

## 4.2 风险减小策略

### 4.2.1 概述

GB/T 15706.1—2007 中的第 5 章给出了关于机器风险减小的策略。(GB/T 15706.2—2007 中的第 4 章(固有设计措施)和第 5 章(安全防护装置和附加保护措施)给出了更进一步的指导。风险减小策略涵盖了机器的整个寿命周期。

机器的危险分析和风险减小过程要求通过以下措施逐步消除或减小危险：

通过设计消除危险或减小风险(见 GB/T 15706.2—2007，第 4 章)；

通过防护装置和可能的附加保护措施减小风险(见 GB/T 15706.2—2007，第 5 章)；

通过使用信息中关于遗留风险的规定减小风险(见 GB/T 15706.2—2007，第 6 章)

### 4.2.2 控制系统对风险减小的作用

下面机器的设计过程的目的是达到安全目标(见 4.1)，对于提供所需的风险减小的 SRP/CS，其设计是机器全部设计过程中的一个完整子过程。SRP/CS 以能达到所需的风险减小的 PL 来提供安全功能。在所提供的安全功能中，无论作为本质安全设计的一部分、还是作为安全防护装置或保护装置，SRP/CS 的设计都是风险减小策略的一部分。该设计过程是一个迭代的过程，见图 1 和图 3。



标准分享网 www.bzfxw.com 免费下载

对于每种安全功能，应在安全要求技术规范中规定和记录其特征(见第5章)和所需的性能等级。

本部分中的性能等级定义为每小时危险失效的概率。5种性能等级(a～e)用每小时危险失效概率的规定范围来表示(见表3)。

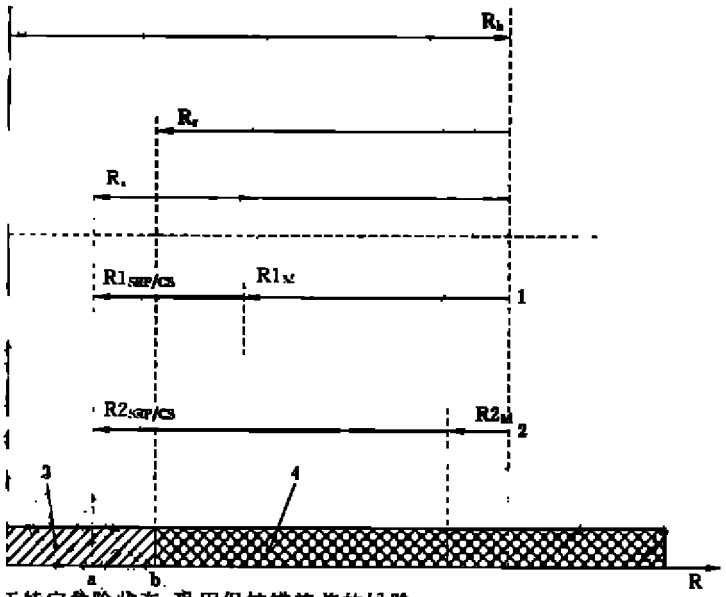
表3 性能等级(PL)

| PL | 每小时平均危险失效概率 (1 h) |
|---|---|
| a | $\geqslant 10^{-5}$ ～$<10^{-4}$ |
| b | $\geqslant 3\times10^{-6}$ ～$<10^{-5}$ |
| c | $\geqslant 10^{-6}$ ～$<3\times10^{-6}$ |
| d | $\geqslant 10^{-7}$ ～$<10^{-6}$ |
| e | $\geqslant 10^{-8}$ ～$<10^{-7}$ |

注：除了每小时平均危险失效概率外，其他措施也是达到PL所必需的。

从对机器进行风险评价(见GB T 16856)开始，设计者应确定SRP/CS的安全功能对相应的风险减小的作用。该作用并不减小受控机器的所有风险(例如：并不涵盖机械压力机或洗衣机的所有风险)，而是应用特定的安全功能减小一部分风险。该功能的示例，如压力机上的电敏保护装置或洗衣机门锁功能触发的停止功能。

风险减小可通过采用各种保护措施(SRP/CS及非SRP/CS)来实现，最终达到安全状态(见图2)。




$R_a$ 对于特定危险状态，采用保护措施前的风险；

$R_r$ 需要保护措施减小的风险；

$R_t$ 保护措施实际减小的风险；

1 方案1：绝大部分风险减小由保护措施(例如：机械方法)实现，小部分由SRP/CS实现；

2 方案2：绝大部分风险减小由SRP/CS(例如：光幕)实现，小部分由保护措施(例如：机械方法)实现；

3 充分减小的风险；

4 没有充分减小的风险；

R 风险；

a 实施方案1和方案2后的遗留风险；

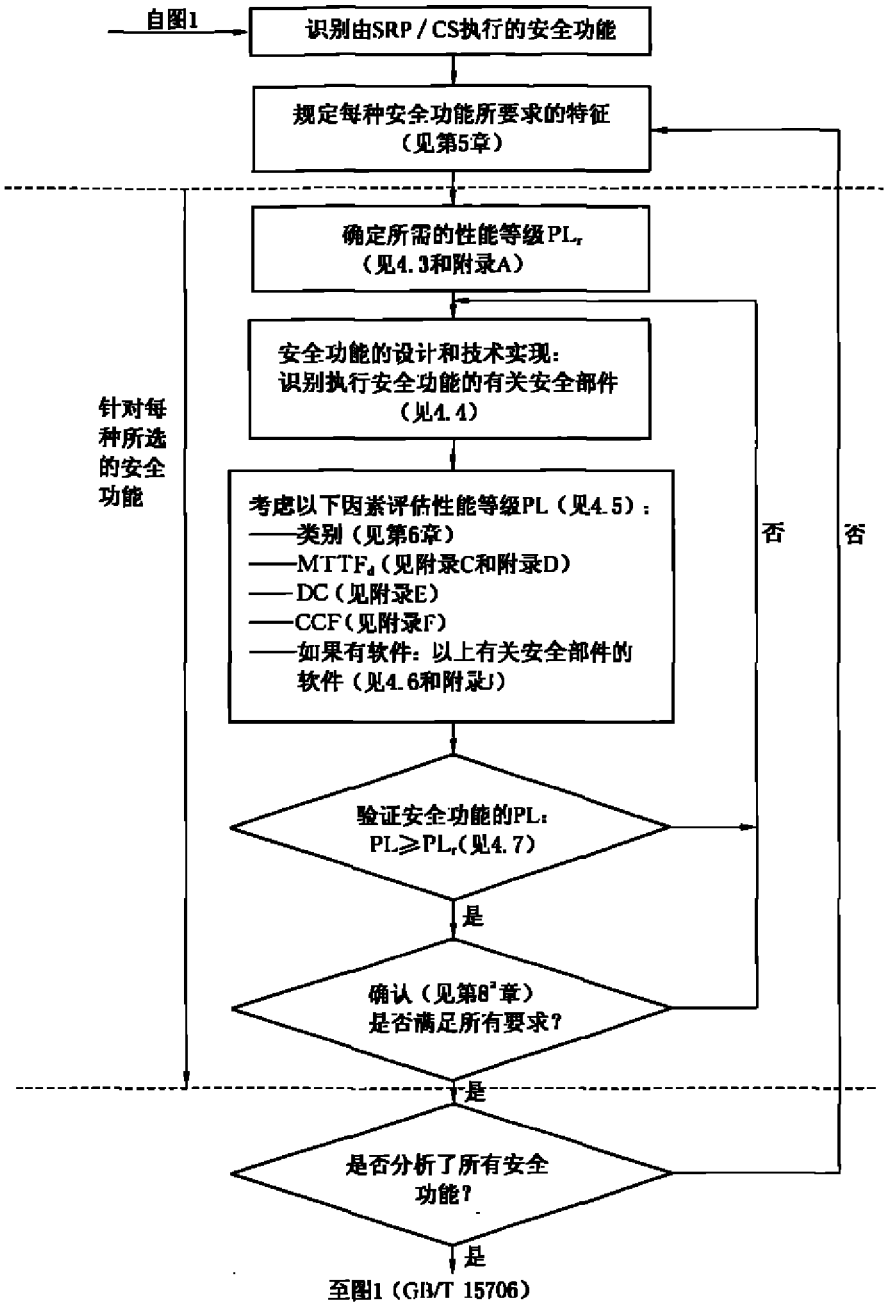
b 充分减小的风险；

$R1_{SRP/CS}$、$R2_{SRP/CS}$ SRP/CS的安全功能实现的风险减小；

$R1_M$、$R2_M$ 保护措施而不是SRP/CS实现的风险减小(例如：机械方法)。

注：关于风险减小的更多信息见GB T 15706。

图2 每种危险的风险减小过程概况




[a] GB/T 16855.2 提供了确认的附加帮助。

**图 3 控制系统有关安全部件(SRP/CS)设计的迭代过程**

### 4.3 确定所需的性能等级($PL_r$)

对于每种所选的由 SRP/CS 执行的安全功能，应确定和记录所需的性能等级($PL_r$)(确定 $PL_r$ 的指南见附录 A)。所需的性能等级的确定取决于风险评价的结果，并且参考了控制系统有关安全部件实现的风险减小量(见图 2)。

SRP/CS 实现的风险减小总和越多，$PL_r$ 就越高。

### 4.4 SRP/CS 的设计

确定机器安全功能是风险减小过程的一部分，包括确定控制系统的安全功能，例如：防止意外启动。

单一安全功能可能由一个或多个 SRP/CS 来实现，几种安全功能可能由一个或多个 SRP/CS 来共同实现(例如：逻辑单元、动力控制元件)。单个 SRP/CS 也可能实现多种安全功能和标准控制功能。设计者可能会单独使用任何可用的技术或组合使用这些技术。SRP/CS 也可能提供操作功能(例如：



标准分享网 www.bzfxw.com 免费下载

AOPD作为循环启动的一种方式)。

图4中给出的典型安全功能图示说明了控制系统有关安全部件(SRP/CS)由以下几方面的组成:

——输入($SRP/CS_a$);

——逻辑/处理($SRP/CS_b$);

——输出/动力控制元件($SRP/CS_c$);

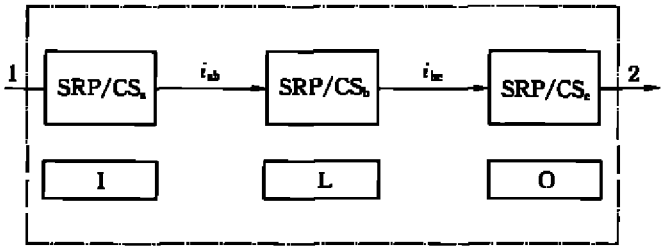
——相互连接方式($i_{ab}$,$i_{bc}$)(例如:电的、光学的)。

注1:在同一机器内,重要的是区别不同安全功能以及执行这些安全功能的SRP/CS。

识别控制系统安全功能之后,设计者应鉴别出SRP/CS(见图1和图3),必要时应把它们分配给输入、逻辑电路、输出以及有冗余时的单独通道,然后估计性能等级PL(见图3)。

注2:指定结构在第6章中给出。

注3:有关安全部件包括所有的相互连接方式。




I——输入;

L——逻辑;

O——输出;

1——触发事件(例如:手动致动按钮、打开防护装置、中断AOPD光束);

2——机器致动器(例如:电动机制动)。

**图4 处理典型安全功能的控制系统有关安全部件组合的示意图**

### 4.5 所需的性能等级PL的估计及其与SIL的关系

#### 4.5.1 性能等级PL

在本部分中,有关安全部件完成安全功能的能力通过确定性能等级PL来表示。

对于所选的完成安全功能的每个SRP/CS和(或)SRP/CS的组合,都应完成其PL的估计。

应通过估计以下参数来确定SRP/CS的PL:

——单个元件$MTTF_d$的值(见附录C和附录D);

——DC(见附录E);

——CCF(见附录F);

——结构(见第6章);

——安全功能在故障条件下的性能(见第6章);

——有关安全的软件(见4.6和附录J);

——系统性失效(见附录G);

——预期环境条件下,完成安全功能的能力。

注1:其他参数,例如:运行情况、需求比率、试验比率等都有一定的影响。

这些与评估过程有关的参数可分为以下两组:

a) 定量的参数(单个零件的$MTTF_d$值、DC、CCF、结构);

b) 影响SRP/CS性能的不可计量参数(故障条件下安全功能的性能、有关安全的软件、系统性失效以及环境条件)。

可定量的参数中,可靠性(例如:$MTTF_d$、结构)的影响随所采用的技术而变化。例如:采用某种技

术的具有高可靠性的单通道有关安全部件，(在一定限制范围内)可能在采用其他技术的较低可靠性容错结构中提供相同或更高的 PL。

任何类型系统(例如：复杂结构)PL 的可计量参数有几种方法来估计，例如：马尔可夫模型、广义随机 Petri 网(GSPN)、可靠性方框图[见 GB/T 20438 等]。

为更容易评价 PL 的可计量参数，本部分给出了一种基于 5 种指定结构定义的简化的方法，这些指定结构满足特殊设计准则和故障条件下性能(见 4.5.4)。

对于按照第 6 章设计的 SRP/CS 或 SRP/CS 组合，危险失效的平均概率可根据图 5 的方法和附录 A 至附录 H、附录 J 和附录 K 给出的程序来估计。

对于偏离指定结构的 SRP/CS，应提供详细计算以证明其达到了所需的性能等级($PL_r$)。

在 SRP/CS 被当作简单结构，且所需的性能等级为 a～c 的应用中，可采用设计基本原理来定性估计 PL。

注 2：对于复杂控制系统的设计，例如：设计用于执行安全功能的 PES，可适当采用其他标准(例如：GB/T 20438、GB/T 19436 或 IEC 62061)。

可应用 4.6 和附录 G 中推荐的方法来证明以达到 PL 的定性参数。

在根据 IEC 61508 制定的标准中，有关安全控制系统完成安全功能的能力用 SIL 给出。表 4 给出了两种概念(PL 和 SIL)的关系。

PLa 级与 SIL 无对应的等级，它主要用于轻微的风险减小，通常与伤害可逆。SIL4 专门用于流程工业中可能的灾难事件，所以 SIL 的范围与机器的风险无关。因此与 SIL3 对应的 PLe 级为最高的等级。

**表 4 性能等级(PL)与安全完整性等级(SIL)之间的关系**

| PL | SIL<br>(参见 GB/T 20438.1)<br>工作模式为高/连续 |
|---|---|
| a | 无对应等级 |
| b | 1 |
| c | 1 |
| d | 2 |
| e | 4 |

因此，应主要采用以下两种保护措施来减小风险：

减小在元件级的故障概率。其目的是减小影响安全功能的故障或失效的可能性。这可通过增加元件可靠性来实现，例如：为了把致命故障或失效减到最少或排除故障(见 GB/T 16855.2)，选用经验证的零件和(或)应用经验证的安全原则。

- 改善 SRP/CS 的结构，其目的是避免故障的危险影响。一些故障是可以检测到的，而且需要冗余和(或)监测结构。

可单独或组合应用这两种措施。对某些技术，通过选择可靠的零件或排除故障可实现风险减小，但对于其他技术，可能需要冗余和(或)监测系统来实现风险减小。另外，还应考虑共因失效(CCF)(见图 3)。

结构约束见第 6 章。

### 4.5.2 每个通道的平均危险失效时间($MTTF_d$)

每个通道的平均危险失效时间的值用 3 种等级给出(见表 5)，且应单独考虑每个通道(例如：单通道、冗余系统的每个通道)。

根据 $MTTF_d$，可考虑最大值为 100 年。



标准分享网 www.bzfxw.com 免费下载

表 5 每个通道的平均危险失效时间($MTTF_d$)

| 每个通道的指标 | 每个通道的范围 |
|---|---|
| 低 | 3 年≤$MTTF_d$<10 年 |
| 中 | 10 年≤$MTTF_d$<30 年 |
| 高 | 30 年≤$MTTF_d$<100 年 |

注 1：每个通道 $MTTF_d$ 范围的选择基于该领域内最新技术的失效率，这种技术构建了一种适合对数 PL 标度的对数标度。现实中，SRP/CS 的 $MTTF_d$ 值预期不能小于 3 年，否则这意味着一年以后市场上 30%的系统不合格且需要更换。每个通道的 $MTTF_d$ 值大于 100 年也不合适，因为高风险下的 SRP/CS 不宜只依靠零件的可靠性。为了加强 SRP/CS 预防系统性和随机失效的能力，推荐采用附加方法，例如：要求冗余和试验。为了更可行，范围的数量限制在 3 个内。$MTTF_d$ 值最大为 100 年的每个通道的限制应参考执行安全功能的 SRP/CS 的单个通道。更高的 $MTTF_d$ 值可用于单个零件(见表 D.1)。

注 2：本表中给出的边界值可假定其精确度在 5%范围内。

对于零件 $MTTF_d$ 的估计，寻找数据的先后程序应按以下顺序给出：

a) 采用制造商的数据；

b) 使用附录 C 和附录 D 的方法；

c) 选为 10 年。

4.5.3 诊断覆盖率(DC)

DC 的值分 4 级给出(见表 6)。

一般地，可使用失效模式及影响分析(FMEA，见 GB/T 7826)或类似方法来估计 DC。因此，宜考虑所有相关的故障和(或)失效模式，建议对照所需的性能等级($PL_r$)检查执行安全功能的 SRP/CS 组合的 PL。估计 DC 的简化方法见附录 E。

表 6 诊断覆盖率(DC)

| 指 标 | 范 围 |
|---|---|
| 无 | DC<60% |
| 低 | 60%≤DC<90% |
| 中 | 90%≤DC<99% |
| 高 | DC≥99% |

注 1：对于由几个部件组成的 SRP/CS，表 5、第 6 章和 E.2 中对 DC 采用了平均值 $DC_{avg}$。

注 2：DC 范围的选择基于三个关键值 60%、90%和 99%，也在涉及诊断覆盖率试验的其他标准(例如：GB/T 20438)中确立。调查表明，试验有效性的特征量度是(1-DC)而不是 DC 本身。(1-DC)的关键值 60%、90%和 99%形成一种适合对数 PL 标度的对数标度。小于 60%的 DC 值只能轻微影响被测系统的可靠性，因此称为"无"。复杂系统的 DC 值很难超过 99%。为了切实可行，范围的数量限制在 4 个以内。本表中给出的边界值可认为精确度在 5%范围内。

4.5.4 概述

可通过考虑所有相关参数和适当计算方法来估计 PL(见 4.5.1)。

本章给出了基于指定结构来估计 SRP/CS 的 PL 的简化程序。为得到 PL 的估计值，其他类似的结构可转换为本章中这样的指定结构。

指定结构以方框图表示，并在 6.2 中的每个类别中列出。关于方框法和有关安全方框图的信息在 6.2 和附录 B 中给出。

指定结构给出了每一类别的系统结构的逻辑表示。技术实现(例如：功能电路图)可能看起来完全不一样。

指定结构是针对 SRP/CS 组合而画的，它起始于触发有关安全信号，终止于动力控制元件的输出(也可见 GB/T 15706.1—2007)。指定结构也可用来描述控制系统中响应输入信号并产生有关安全输

出信号的部件或子部件。因此,"输入"单元可代表光幕(AOPD)和控制逻辑元件的输入电路或输入开关等。"输出"可代表输出信号开关装置(OSSD)或激光扫描仪等的输出。

指定结构做了以下典型的假设:

——任务时间为 20 年(见第 10 章);

——在任务时间内失效率恒定;

——对于类别 2,需求比率≤试验比率的 1 %;

——对于类别 2,$MTTF_{d\ TE}$大于 $MTTF_{d,1}$ 的一半。

注:当每个通道的方框不能分开时,可应用以下原则:综合试验通道(TE,OTE)的 $MTTF_d$ 大于综合功能通道(I,L,O)$MTTF_d$ 的一半。

该方法考虑把类别作为清楚规定了 $DC_{avg}$ 的结构。每个 SRP/CS 的 PL 取决于结构、每个通道的平均危险失效时间($MTTF_d$)以及 $DC_{avg}$。

还宜考虑共因失效(CCF)(指南见附录 F)。

带有软件的 SRP/CS,4.6 的要求适用。

如果没有或不使用定量的数据(例如:复杂程度低的系统),所有相关的参数宜选用最坏情况下的值。

SRP/CS 组合或单个 SRP/CS 可能只有一个 PL。在 6.3 中考虑了几个具有不同 PL 的 SRP/CS 组合。

在 $PL_r$ 为 a～c 的应用中,有足够的方法来避免故障;更高风险的 $PL_r$ 为 d～c 的应用中,SRP/CS 的结构能提供方法以避免、检测或耐受故障。实际的方法包括冗余、差异化、监测等(也可见 GB/T 15706.2—2007 的第 3 章和 GB 5226.1—2002)。

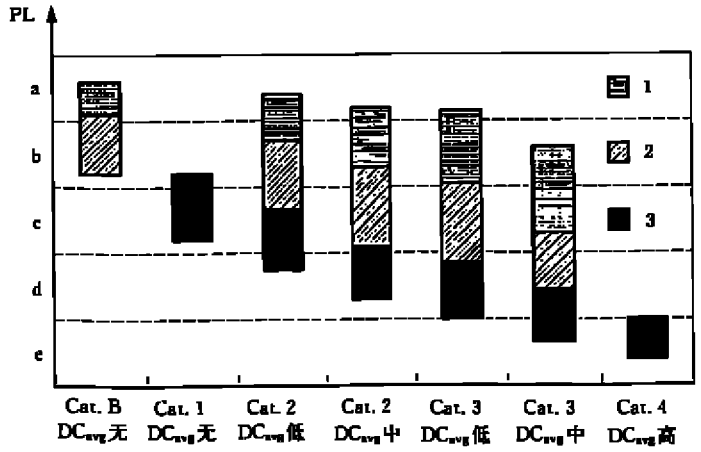
图 5 给出了与每个通道的 $MTTF_d$ 组合的类别以及为了达到安全功能要求的 PL 的 $DC_{avg}$ 的选择。

对于 PL 的估计,图 5 给出了与 $DC_{avg}$ 一起的类别(水平轴)和每个通道的 $MTTF_d$(柱形图)。图中的阴影代表了每个通道的 $MTTF_d$ 的 3 个范围(低、中、高),它可选择用来达到要求的 PL。

在使用图 5 中的简单方法(代表了基于第 6 章中指定结构的不同马尔可夫模型的结果)以前,应确定 SRP/CS 的类别以及每个通道的 $DC_{avg}$ 和 $MTTF_d$(见第 6 章和附录 C～附录 E)。

对于类别 2、类别 3 和类别 4,应采用足以防止共因失效的措施(指南见附录 F)。考虑到这些参数,图 5 提供了确定由 SRP/CS 实现的 PL 的方法图解。类别(包括共因失效)和 $DC_{avg}$ 的组合确定选择图 5 中的那一列。根据每个通道的 $MTTF_d$,应选出有关直方柱的 3 个不同阴影区域中的一个。

这些区域的纵向位置确定能在竖轴上读出的要求的 PL。如果该区域有两种或三种可能的 PL,表 7 中给出了所达到的 PL。数字更精确的 PL 的选择取决于每个通道 $MTTF_d$ 的精确值,见附录 K。




PL——性能水平;

1——每个通道的 $MTTF_d$=低;

2——每个通道的 $MTTF_d$=中;

3——每个通道的 $MTTF_d$=高。

图 5 PL 和每个通道的类别、$DC_{avg}$ 和 $MTTF_d$ 的关系



标准分享网 www.bzfxw.com 免费下载

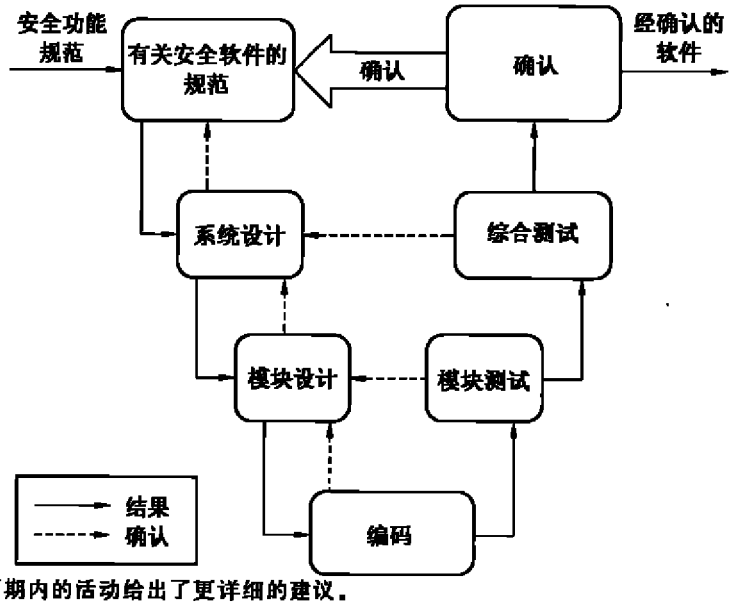
表 7 估计由 SRP/CS 达到的 PL 的简单程序

| 类 别 | B | 1 | 2 | 2 | 3 | 3 | 4 |
|---|---|---|---|---|---|---|---|
| $DC_{avg}$ | 无 | 无 | 低 | 中 | 低 | 中 | 高 |
| 每个通道的 $MTTF_d$ | | | | | | | |
| 低 | a | 不包括 | a | b | b | c | 不包括 |
| 中 | b | 不包括 | b | c | c | d | 不包括 |
| 高 | c | c | c | d | d | d | e |

## 4.6 软件的安全要求

### 4.6.1 一般要求

有关安全的嵌入式软件或应用软件的所有寿命周期内的活动，应主要考虑避免软件寿命周期内出现的故障(见图 6)。以下要求的主要目标是有易读、易理解、可测试及可维护的软件。




注：附录 J 对寿命周期内的活动给出了更详细的建议。

图 6 软件安全寿命周期的简单 V 模型

### 4.6.2 有关安全的嵌入式软件(SRESW)

对于用于 $PL_r$ 为 a～d 的元件的 SRESW，应采用以下基本方法：

——对软件安全寿命周期内的活动进行检验和确认，见图 6；

——对技术规范和设计进行归档；

——模块化和结构化设计和编码；

——系统性失效的控制(见 G.2)；

——使用基于软件方法用于控制随机的硬件失效时，正确执行的检验；

——功能测试，例如：黑盒子测试；

——修改后，合适的软件安全寿命周期内的活动。

对于用于 $PL_r$ 为 c 或 d 的零件的 SRESW，应采用以下附加方法：

——满足一定的计划管理和质量管理系统的要求，例如：GB 20438 或 GB/T 19001 中的要求；

——对软件安全寿命周期内所有的相关活动进行归档；

——用以识别所有的结构项目和与 SRESW 有关的释放文件的结构管理；

——符合安全要求和设计的结构规范；

——使用合适的编程语言和便于使用的基于计算机的工具；

—— 模块化和结构化编程，区别于非有关安全软件、具有充分定义接口的受限模块大小，采用设计和编码标准；

—— 用控制流程分析，通过遍查/复查来验证编码；

——扩展的功能测试，例如：灰盒子测试、性能测试或仿真；

——冲击分析以及修改后软件安全周期内适当的活动。

对于 $PL_r$=e 的元件，SRESW 应满足 GB/T 20438.3 第 7 章中适用于 SIL3 的要求。在规范、设计和编码中采用多样性时，对于用在类别 3 或类别 4 的 SRP/CS 中的两个通道，可用上述用于 $PL_r$ 为 c 或 $PL_r$ 为 d 的方法达到 $PL_r$=e。

注 1：这类方法的具体描述见 GB/T 20438.7—2006 等

注 2：对于在设计和编码中具有多样性的 SRESW，类别 3 或类别 4 的 SRP/CS 使用的零件，通过只考虑结构方面代替每行编码的检查来复查软件局部等方法可减小采取措施避免系统性失效这方面的努力。

4.6.3 有关安全的应用软件(SRASW)

软件安全寿命周期(见图 6)也适用于 SRASW(见附录 J)。

满足以下要求并且以 LVL 编写的 SRASW，可使 PL 达到 a～e。如果 SRASW 以 LVL 编写，则应满足用于 SRESW 的要求，且 PL 可达到 a～e。如果在一个元件中的 SRASW 的一部分影响到几种 PL 不同的安全功能，则应采用与最高 PL 有关的安全要求。用于 $PL_r$ 为 a～e 的零件的 SRESW，应采用以下基本措施：

对开发周期进行检查和确认，见图 6；

- 对技术规范和设计进行归档；
- 模块化和结构化编程；

功能性测试；

-修改后适当的开发。

对用于 $PL_r$ 为 c～e 的元件的 SRESW，需要采用或推荐采用以下提高效率的附加措施(较低效率用于 $PL_r$ 为 c，中等效率用于 $PL_r$ 为 d，较高效率用于 $PL_r$ 为 e)。

a) 应复查有关安全软件的技术规范(也可见附录 J)，使寿命周期内涉及的所有人员可以得到该规范，且应包括以下内容的描述：
   1) 具有要求的 PL 的安全功能以及相关的工作模式；
   2) 性能准则，例如：反应时间；
   3) 具有外部信号界面的硬件结构，以及
   4) 外部失效的探测和控制。

b) 工具、库和语言的选择：
   1) 可放心使用的合适工具：对于达到 PL=e 的一个元件及其工具，该工具应满足适当的安全标准；如果使用了带有不同的工具的两种不同零件，则可放心使用。采用的技术特征应能检测可导致系统性错误(例如：数据类型不匹配、意义不明确的动态存储地址、不完善的命令界面、递归、指针算法等)的条件。检查宜主要在编译时间内而不能仅在运行时间内进行。工具宜加强语言子集和编码指南，或者至少督促或引导开发者使用它们。
   2) 只要合理可行，宜采用经确认的功能模块(FB)库——无论是工具制造商提供的有关安全的 FB 库(强烈推荐 PL=e)，还是符合本部分且用途已被确认的详细 FB 库。
   3) 宜采用合理的适用于模块化方法的 LVL 子集，例如：GB/T 15969.3 中认可的语言子集。强烈推荐采用图示语言(例如：功能模块图、梯形图)。

c) 软件设计的特征应是：
   1) 半正式的方法描述数据和控制流，例如：状态图或程序流程图；
   2) 主要由源自有关安全的经确认的功能模块库的功能模块实现模块化和结构化设计；



标准分享网 www.bzfxw.com 免费下载

3) 限制了编码大小的功能模块；
4) 编码在功能模块内执行，功能模块宜有一个入口和一个出口点；
5) 三个阶段的结构模型，输入⇒处理⇒输出(见图7和附录J)；
6) 在唯一一个程序位置安全输出的安排；
7) 使用用于检测外部失效的技术和用于在输入、处理和输出模块内置于安全状态的预防性编程技术。

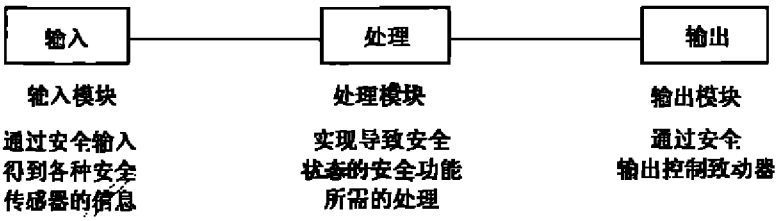



图7 软件的一般结构模型

d) 当SRASW和非SRASW组合在一个元件中时：
1) SRASW和非SRASW应在与有明确定义的数据链接的不同功能块中编码；
2) 不应存在非有关安全数据和有关安全数据的逻辑组合，因为这可导致有关安全信号的完整性下降。例如：结果控制有关安全信号的地方采用逻辑"非"组合有关安全和非有关安全的信号。

e) 软件执行/编码：
1) 代码宜易读、易懂及可测试，为此宜使用符号变量(代替显式硬件地址)；
2) 应使用合理的或公认的编码指南(也可见附录J)；
3) 宜使用应用层(预防性编程)可用的数据完整性和真实性检查(例如：范围检查)；
4) 代码宜接受仿真测试；
5) PL=d或PL=e时，宜通过控制和数据流分析检验。

f) 测试：
1) 合适的确认方法是功能性行为和性能准则(例如：时序性能)的黑盒子测试；
2) PL=d或PL=e时，推荐由分析边界值开始进行试验；
3) 建议制定试验计划，且宜包括具有完成准则和所需工具的试验用例；
4) I/O测试应保证在SRASW内正确使用有关安全信号。

g) 文件：
1) 应对所有寿命周期和修改活动进行归档；
2) 文件应完整、可用、易读和易懂；
3) 源程序正文中的代码文档应包括具有合法实体的模块标题，功能和I/O描述，版本和所使用的库函数模块的版本，以及网络声明及公告中足够的注释。

h) 验证：[1]
例如：复查、检查、遍查或其他的合适活动。

i) 结构管理：
强烈建议建立程序和数据的备份，以识别和归档文件、软件模型、验证确认结果以及与SRASW具体版本有关的工具结构。

j) 修改SRASW后，应进行影响分析以保证规范性。修改后应执行合适的寿命周期内的活动。应控制修改访问权限且应归档修改历史。

注：修改不影响已在使用的系统。

1) 验证只对于专用代码才是必要的，对于经验证的库函数则不是必需的。

#### 4.6.4 基于软件的参数化

应考虑把基于软件的有关安全参数参数化，作为软件安全要求规范中要描述的 SRP/CS 设计的一个有关安全方面。应采用 SRP/CS 供应商提供的专门软件工具进行参数化。该工具应有自己的标识（名称、版本等）且应防止未经授权的修改，例如：采用密码。

应保持所有用于参数化的数据的完整性。这应通过采取措施控制以下方面来达到：

——控制有效输入的范围；

——传输前控制数据损坏；

——从参数传输进程中控制错误的影响；

——控制不完整参数传输的影响，以及

——控制参数化所用工具的硬件和软件故障和失效的影响。

参数化工具应满足本部分中对 SRP/CS 的所有要求，或者也可以设定有关安全参数应使用特别的程序。该程序应包括通过以下两种方式之一来确认 SRP/CS 的输入参数：

——修改后的参数重新发送至参数化工具，或者

——确认参数完整性的其他合适方式。

也包括随后的确认，例如：通过合适的技术熟练人员来确认、通过参数化工具自动检查的方式来确认等。

注 1：当使用不是专门预定用于该目的的装置进行参数化时，这一点尤其重要（例如：个人电脑或相当的装置）。

在传输/转发过程中，用于编码/译码的软件模块以及用户用于有关安全参数可视化的软件模块，应至少在功能方面采用多样性以避免系统性失效。

基于软件参数化的文件应显示所使用的数据（例如：预定义的参数集），用于识别与 SRP/CS 有关的参数所必需的信息，完成参数化的人员以及其他相关信息（例如：参数化日期）。

应对基于参数化的软件进行以下的检验：

——检验每个有关安全参数的正确设置（最小值、最大值和典型值）；

——检验有关安全参数是否进行了合理性检查，例如：使用无效值等；

——检验是否防止了有关安全参数未经授权的修改；

——检验用于参数化的数据/信号的产生和处理是否能够保证不导致安全功能丧失。

注 2：这对于利用不是特定预定用于该目的装置进行参数化时尤其重要（例如：个人电脑或相当的装置）。

### 4.7 检验达到的 PL 是否满足 $PL_r$

对于每种单独的安全功能，有关的 SRP/CS 的 PL 应与 4.3（见图 3）中确定的所需的性能等级（$PL_r$）匹配。如果情况并非如此，需要采用图 3 中描述的迭代过程。

作为安全功能一部分的不同 SRP/CS，其 PL 应大于或等于该安全功能所需的性能等级（$PL_r$）。

### 4.8 设计的人类功效学方面

操作者与 SRP/CS 之间的界面的设计和实现应使得所有预定使用和机器可预见的误用过程中没有人员有危险（也可见 GB/T 15706.2、EN 614-1、ISO 9355-1、ISO 9355-2、ISO 9355-3、EN 1005-3、GB 5226.1—2002 中的第 10 章、GB/T 4205 和 GB 18209）。

人类工效学原则的使用应使得机器和控制系统，包括有关安全部件都容易使用，从而使得操作者不能尝试危险的动作。

GB/T 15706.2—2007，4.8 中给出的遵守人类工效学原则的安全要求适用。

## 5 安全功能

### 5.1 安全功能技术规范

本章给出了 SRP/CS 能提供的安全功能的清单和详细细节。为了实现具体应用中控制系统需要的安全措施，在设计（或 C 类标准制定）时应包括这些功能中必要的功能。



标准分享网 www.bzfxw.com 免费下载

示例：有关安全的停止功能、防止意外启动、手动复位功能、抑制功能、止-动功能。

注：机械控制系统提供操作和(或)安全功能。操作功能(例如：启动、正常停止)也是安全功能，但是这只能在对机械进行了完整的风险评价后才能确定。

表 8 和表 9 分别列出了一些典型的安全功能及其某些特征、安全功能及有关安全参数，并参考其他与安全功能、特征或参数有关的标准。设计者(或 C 类标准的制定者)应保证所有的应用要求满足表中列出的相应的有关安全功能。

本章给出了某些安全功能特征的附加要求。

必要时，特征和安全功能的要求应适用于不同能量源。

表 8 和表 9 中大部分引用标准与电气标准有关，因此其他技术(例如：液压、气动)的应用要求也适用于该范围。

**表 8 适用于典型机器安全功能和它们某些特征的一些标准**

| 安全功能/特征 | 要求 | | | 附加要求 |
|---|---|---|---|---|
| | 本部分 | GB/T 15706.1—2007 | GB/T 15706.2—2007 | |
| 由防护装置触发的有关安全的停止功能[a] | 5.2.1 | 3.26.8 | 4.11.3 | IEC 60204-1:2005 中的 9.2.2，9.2.5.3，9.2.5.5 |
| 手动复位功能 | 5.2.2 | — | — | IEC 60204-1:2005 中的 9.2.5.3，9.2.5.4 |
| 启动/重启功能 | 5.2.3 | — | 4.11.3，4.11.4 | IEC 60204-1:2005 中的 9.2.1，9.2.5.1，9.2.5.1，9.2.6 |
| 局部控制功能 | 5.2.4 | — | 4.11.8，4.11.10 | IEC 60204-1:2005 中的 10.1.5 |
| 抑制功能 | 5.2.5 | — | — | — |
| 止-动功能 | — | — | 4.11.8 b) | IEC 60204-1:2005 中的 9.2.6.1 |
| 使动装置功能 | — | — | — | IEC 60204-1:2005 中的 9.2.6.3，10.9 |
| 防止意外启动 | — | — | 4.11.4 | GB/T 19670 以及 IEC 60204-1:2005 中的 5.4 |
| 受困人员的撤离和营救 | — | — | 5.5.3 | — |
| 绝缘和能量耗散功能 | — | — | 5.5.4 | GB/T 19670<br>IEC 60204-1:2005 中的 5.3，6.3.1 |
| 控制模式和模式选择 | — | — | 4.11.8，4.11.10 | IEC 60204-1:2005 中的 9.2.3，9.2.4 |
| 不同控制系统有关安全部件之间的相互作用 | — | — | 4.11.1<br>(最后一句) | IEC 60204-1:2005 中的 9.3.4 |
| 有关安全输入值参数化的监测 | 4.6.4 | — | — | — |
| 急停功能[b] | — | — | 5.5.2 | GB 16754 以及 IEC 60204-1:2005 中的 9.2.5.4 |

[a] 包括联锁防护装置和限制装置(例如：超速、超温、超压等)。

[b] 补充保护措施，见 GB/T 15706.1—2007。

表 9 给出某些安全功能和有关安全参数要求的一些标准

| 安全功能/有关安全参数 | 要求 | | 附加信息 |
|---|---|---|---|
| | 本部分 | GB/T 15706.2- 2007 | |
| 响应时间 | 5.2.6 | | GB/T 19876 2005 中的 3.2.A.3.A.4 |
| 有关安全参数,例如:速度、温度或压力 | 5.2.7 | 4.11.8 e) | IEC 60204-1:2005 中的 7.1.9.3.2.9.3.4 |
| 动力源的波动、损失和恢复 | 5.2.8 | 4.11.8 e) | IEC 60204-1:2005 中的 4.3.7.1.7.5 |
| 指示和警告 | | 4.8 | GB 1251.1<br>GB/T 1251.2<br>GB 1251.3<br>GB 18209.1<br>IEC 60204-1:2005 中的 10.3.10.4<br>GB/T 15969<br>IEC 62061 |

在识别和规定安全功能时,应至少考虑以下因素:

a) 每种特定危险或危险状态的风险评价结果;

b) 机器的工作特性,包括:

——机器的预定使用(包括可预见的误用);

——工作模式(例如:局部模式、自动模式、与机器区域或部件有关的模式);

——周期,以及

——响应时间;

c) 紧急操作;

d) 不同工作过程和手动行为(例如:修理、调整、清洗、故障查找等)交互作用的描述;

e) 预定用于实现安全功能或预防作用的机器行为;

f) 机器能工作或不能工作的条件(例如:工作模式);

g) 工作频率;

h) 能同时激活并能导致相互矛盾操作的功能的优先级。

## 5.2 安全功能详述

### 5.2.1 有关安全的停止功能

除了表 8 中的要求外,还应包括下列要求。

有关安全的停止功能(例如,由安全防护装置触发)致动后,一旦有必要,应使机器进入安全状态。这种停止功能应优先于由操作原因引起的停止。

当一组机器按照协同方式一起工作时,应规定监督控制和(或)其他存在停止条件的机器的信号发射。

注:有关安全的停止功能可导致操作问题和重启困难,如:应用在电弧焊中。为了减小这种停止功能失效的可能性,可使这种停止功能优先于正常操作的停止,从而决定实际的操作并准备快速容易的从停止位置重启(例如:产品没有任何损坏)。一种解决办法是当循环达到可能容易重启的规定位置时,防护装置的闭锁松开的地方使用带防护装置的联锁装置。

### 5.2.2 手动复位功能

除了表 8 中的要求外,还应包括下列要求。

防护装置发出停止指令后,停止状态应保持到有安全重启状态为止。

通过复位防护装置,解除停止指令,再重新恢复安全功能。如果风险评价显示可行,这种停止指令的解除应由手动、独立而慎重的操作(手动复位)来确认。



标准分享网 www.bzfxw.com 免费下载

手动复位功能应：

——通过 SRP/CS 内的一个独立的手动操作装置来提供；

——只有所有安全功能和防护装置处于工作状态时才能实现复位；

——自身不能引起运动或危险状态；

——谨慎操作；

——使控制系统能接受独立的启动指令；

——只有致动器从其接通(on)位置脱开才能完成。

提供手动复位功能的有关安全部件性能等级的选择，应使得手动复位功能不削弱相关安全功能的安全要求。

复位致动器应安装在危险区以外，并具有良好可见度的安全位置，以便检查是否有人处在危险区内。

当危险区不完全可见时，需要专门的复位程序。

注：一种解决办法是采用超过一个复位致动器。复位功能由处于危险区内的第一个致动器和处于危险区外的第二个致动器(靠近安全防护装置)联合触发。该复位程序需要在控制系统接收单独启动指令前有限的时间内实现。

### 5.2.3 启动/重启功能

除了表 8 中的要求外，还应包括下列要求

只有危险状态不可能存在的情况下，重启功能才能自动发生。特别是对于具有启动功能的联锁防护装置，见 GB/T 15706.2—2007 中的 5.3.2.5。

启动和重启的这些要求也应适用于能够遥控的那些机器。

注：传感器反馈给控制系统的信号能够触发自动重启。

示例：在自动化机器操作中，传感器反馈给机器控制系统的信号通常用作控制流程。如果工件离开其位置，则流程停止。如果联锁防护装置的监控不能优先于自动流程控制，则操作者调整工作件时可能存在机器重启的危险。因此，在防护装置再次关闭，且维护人员已离开危险区域之前，不应允许遥控重启。控制系统提供的防止意外启动的作用取决于风险评价的结果。

### 5.2.4 局部控制功能

除了表 8 中的要求外，还应包括下列要求。

当机器通过诸如便携式控制装置或悬吊式操纵装置进行局部控制时，应满足以下要求：

——选用的局部控制应位于危险区之外；

——局部控制应只有在风险评价定义的区域才有可能触发危险状态；

——局部控制和主要控制之间的切换不应产生危险状态。

### 5.2.5 抑制功能

除了表 8 中的要求外，还应包括下列要求。

抑制不应导致任何人暴露于危险状况下。抑制期间安全环境应由其他方式提供。

抑制结束时，SRP/CS 的所有安全功能都应恢复。

提供抑制功能的有关安全部件的性能等级的选择应使得抑制功能不会削弱有关安全功能必需的安全水平。

注：在某些应用中，需要一个抑制指示信号。

### 5.2.6 响应时间

除了表 9 中的要求外，还应包括下列要求。

SRP/CS 的响应时间应在 SRP/CS 的风险评价显示需要确定时确定(也可见 11 章)。

注：控制系统的响应时间是机器全部响应时间的一部分。必需的机器全部响应时间能够影响有关安全部件的设计，例如：需要提供制动系统。

### 5.2.7 有关安全参数

除了表 9 中的要求外，还应包括下列要求。

当有关安全参数，例如：位置、速度、温度或压力等偏离了当前的限制时，则控制系统应启动相应的措施（例如：启动停止功能、警告信号、警报等）。

如果可编程电子系统中有关安全数据手动输入错误能够导致危险状态，那么应在控制系统有关安全部件中提供数据检查系统，例如：极限值、格式化和（或）逻辑输入值的检查。

#### 5.2.8 能量源的波动、损失和恢复

除了表 9 中的要求外，还应包括下列要求。

当能量级的波动超出了设计工作范围时（包括能量供应损失），SRP/CS 应连续提供或触发能使机器系统其他部件保持安全状态的输出信号

## 6 类别以及与 $DC_{avg}$、CCF 和每个通道 $MTTF_d$ 的关系

### 6.1 一般要求

SRP/CS 应满足 6.2 中规定的 5 种类别中的一种或多种类别的要求。

类别是用作达到规定 PL 的基本参数。它们根据第 4 章中描述的设计考虑，规定了 SRP/CS 在耐故障方面所要求的行为。

B 类是基本的类别。当出现故障时，能导致安全功能的损失。在 1 类中，主要是通过选择和应用合适的元件来实现改进耐故障的能力。在 2 类、3 类和 4 类中，提高规定安全功能方面的性能主要是通过改进 SRP/CS 的结构来实现。其中，在 2 类中是通过定期检查正在被执行的规定安全功能来实现；在 3 类和 4 类中是通过保证单一故障不会导致安全功能的损失来实现。在 3 类和 4 类中，只要合理可行，这类故障就会被检测到。在 4 类中，应规定耐故障积累的能力。

表 10 中给出了 SRP/CS 的各个类别、要求和在故障情况下系统性能。

就某些部件失效原因而论，如果有可能就会排除一定的故障（见第 7 章）。

具体 SRP/CS 的类别的选择主要取决于：

——该部件提供的安全功能实现的风险减小；

——要求的性能等级（$PL_r$）；

——采用的技术；

——该部件发生故障时产生的风险；

——在该部件中消除故障发生的可能性（系统性故障）；

——该部件中发生故障的概率以及相关参数；

——平均危险失效时间（$MTTF_d$）；

——诊断覆盖率（DC），以及

——在 2 类、3 类和 4 类中的共因失效（CCF）。

### 6.2 类别规范

#### 6.2.1 概述

每个 SRP/CS 应满足相关类别的要求，见 6.2.3 至 6.2.7。

以下的典型结构满足了各自类别的要求。

以下的图形给出的不是示例而是通用结构。通常可能偏离这些结构，但是任何偏离都应通过适当的分析工具（例如：马尔可夫模型）证明其是合理的，因此该系统满足要求的性能等级（$PL_r$）。

指定结构不仅能当作电路图，也能当作逻辑图。对于 3 类和 4 类，这就意味着并不是所有的部件都需要有物理上的冗余，而是需要有冗余的方法保证故障不能导致安全功能的损失。

图 8～图 12 中的直线和箭头代表逻辑连接方式和可能的逻辑诊断方法。

#### 6.2.2 指定结构

SRP/CS 的结构是对 PL 有重大影响的关键特征。即使可能的结构变化很大，基本概念也通常是类似的。因此，出现在机械领域的大部分结构能够映射到一种类别。每种类别都能够用有关安全模块



标准分享网 www.bzfxw.com 免费下载

图象征性表出。这些典型表示称为指定结构并在以下每种类别的范围内列出。

图 5 中给出的取决于 $DC_{avg}$、类别和每个通道的 $MTTF_d$ 的 PL 是基于指定结构的，这一点很重要。如果图 5 用作估计 PL，则 SRP/CS 的结构宜证明其与要求类别的指定结构是等效的。各自类别的特征设计通常等效于类别的各自指定结构。

注：某些情况下，由于特殊的技术方法或 C 类标准中的规定，类别只能要求 SRP/CS 的有关安全的性能，而不需要附加的 $PL_r$。对于这种特殊情况，安全由结构专门提供，MTTF、DC 和 CCF 的要求不适用。

6.2.3 B 类

根据相关标准，运用具体应用的基本安全原则，对 SRP/CS 的设计、构造、选择、装配和组合至少应与有关标准保持一致并在具体应用中适应基本安全原则：

——预期的工作压力，例如：制动能力和频率的可靠性；

——工艺物料的影响，例如：洗衣机的洗涤剂；

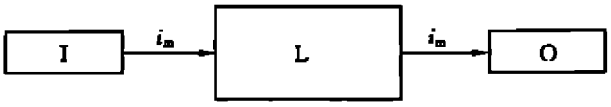
——其他相关的外部影响，例如：机械振动、电磁影响、动力源波动或干扰。

B 类系统中没有诊断覆盖率（$DC_{avg}$＝无），且每个通道的 $MTTF_d$ 可低至中等水平。在这种结构中（通常是单通道系统），不考虑 CCF。

B 类可实现的 PL 最大值为 PL＝b。

注：故障发生时能够引起安全功能失效。

电磁兼容的具体要求见相关的产品标准，例如：动力传动系统见 GB 12688.3。特别是对于 SRP/CS 的功能安全，抗扰度要求也是相关的要求。如果没有产品标准，至少宜满足 GB/T 17999.2 中的抗扰度要求。




$i_m$——连接方式；

I——输入装置，例如：传感器；

L——逻辑模块；

O——输出装置，例如：主接触器。

图 8 B 类的指定结构

6.2.4 1 类

对于 1 类，应满足 6.2.3 中 B 类的要求和以下要求：

属于 1 类的 SRP/CS 应采用经验证的元件和经验证的安全原则来设计和构造（见 GB/T 16855.2）。

有关安全的应用中，“经验证的元件”是指下列之一：

a) 在过去类似的应用中取得了成功效果的元件，或者

b) 在有关安全的应用中，采用证明了其适用性和可靠性的原则而制造的且经过验证的元件。

如果最新开发的元件和形成的安全原则满足 b)中的条件，那么可认为它们与“经验证的”等效。

决定是否接受一个特殊元件作为“经验证的”元件取决于实际应用。

注 1：复杂电子元件（例如：PLC、微处理器、专用集成电路）不能认为是等效于经验证的元件。

每个通道的 $MTTF_d$ 应是高的。

1 类可达到的最大 PL 为 PL＝c。

注 2：1 类系统中没有诊断覆盖率（$DC_{avg}$＝无）。在这种结构中（单通道系统），不考虑 CCF。

注 3：故障的发生能够导致安全功能的损失。然而，1 类中每个通道的 $MTTF_d$ 比 B 类中的高。因此，安全功能的损失可能小一些。

明确区别“经验证的”和“故障排除”（见第 7 章）很重要。一个被当作经验证的元件的条件取决于其

应用。例如：对机床而言，带强制断路触点的位置开关可认为是经验证的元件；但对于食品工业——牛奶业，它是不合适的应用。例如：在几个月后，乳酸能造成该位置开关的损坏。故障排除可导致很高的PL，但允许该故障排除的适当措施宜在装置整个寿命周期内应用。为了确保能做到这样，可能需要控制系统以外的附加措施。对于位置开关，这些措施有如下示例：

——在开关调整后确保其固定牢固的方法；

确保凸轮固定牢固的方法；

确保凸轮横向稳定性的方法；

避免位置开关超行程的方法，例如：减振器和调准装置的足够的配合强度；

保护位置开关免受外部损坏的方法。

$i_m$ 连接方式；

I 输入装置，例如：传感器；

L 逻辑模块；

O 输出装置，例如：主接触器

**图 9 1类的指定结构**

### 6.2.5 2类

对于2类，应满足6.2.3中B类的要求和6.2.4中"经验证的安全原则"的要求。另外还应满足以下要求：

2类SRP/CS的设计应使其功能能按照适当的时间间隔通过机器控制系统进行检查。安全功能的检查应在以下情况下进行：

在机器启动时，以及

某种危险状况发生之前，例如：新周期开始时、其他运动开始时、和(或)如果风险评价和操作类型表明有必要的话，周期性定期运行期间。

该检查可能是自动进行的。安全功能的任何检查应做到：

如果没有检测到故障，允许运行；或者

如果检测到故障，产生触发适当控制动作的输出。

只要可能，这种输出应产生一种安全状态。安全状态应保持到故障清除为止。当不可能产生安全状态时(例如：终级开关装置中的触点焊合)，该输出应发出危险警告。

对于2类的指定结构，如图10所示，$MTTF_d$和$DC_{avg}$的计算宜仅考虑功能通道的模块(即：图10中的I、L和O)，而不考虑测试通道的模块(即：图10中的TE和(TE)。

整个SRP/CS的诊断覆盖率(DC)，包括故障检测应是低的。每个通道的MTTF$_d$应高低可选，它取决于要求的性能等级(PL$_r$)。应采取防止CCF的措施(见附录F)

检查自身不应导致危险状况(例如：由于响应时间的增加)。检查设备和提供安全功能的有关安全部件可以是一体的或是分离的。

2类可达到的最大PL为PL d。

注1：因为安全功能的检查不能应用于所有元件，所以2类不适用某些情况

注2：2类系统性能允许下列情况：

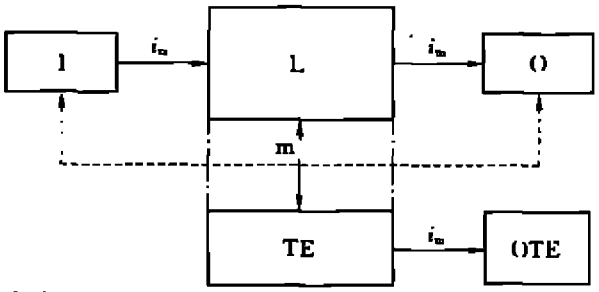
两次检查之间出现故障能导致安全功能的损失；

通过检查可检测到安全功能的损失。

注3：支持2类功能有效性的原则是所采用的技术条款，例如：检查频率的选择能够降低危险状况发生的可能性



标准分享网 www.bzfxw.com 免费下载




虚线代表合理可行的故障检测

| | |
|---|---|
| — | 连接方式； |
| I | 输入装置，例如：传感器； |
| L | 逻辑模块； |
| m | 监测； |
| O | 输出装置，例如：主接触器； |
| TE | 试验设备； |
| OTE | TE 的输出 |

**图 10　2 类的指定结构**

### 6.2.6　3 类

对于 3 类，应满足 6.2.3 中 B 类的要求和 6.2.4 中“经验证的安全原则”的要求。另外还应满足以下要求：

3 类的 SRP/CS 的设计应使得任何这些部件中的单一故障都不会导致安全功能丧失。只要合理可行，在有关安全功能的下一个指令发出时或发出之前应检测出单一故障。

包括故障检测在内的整个 SRP/CS 的诊断覆盖率($DC_{avg}$)应是低的。每个冗余通道的 $MTTF_d$ 应高低可选，它取决于 $PL_r$。应采取防止 CCF 的措施(见附录 F)。

注 1：检测单一故障的这种要求并不意味着所有故障都将查出。因此，未发现的故障累积能够导致意外输出信号使机器处于危险状态。查明故障典型可行的示例，就是利用机械反馈引导继电器接触并进行冗余电子信号输出的监控。

注 2：如果由于技术和应用需要，C 类标准的制定者需要给出故障检测的更详细规定。

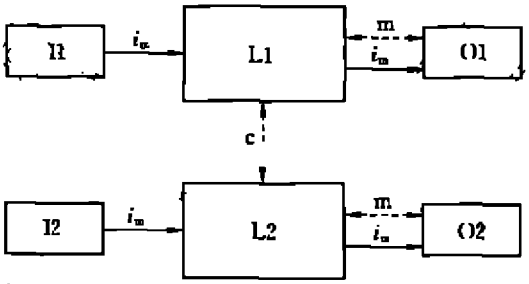
注 3：3 类系统性能允许下述情况：

当发生单一故障时，安全功能总是有效；

某些而不是所有故障将被检测到；

未发现故障的累积能导致安全功能的损失。

注 4：所采用的技术将影响执行故障检测的可能性。




虚线代表合理可行的故障检测

| | |
|---|---|
| — | 连接方式； |
| c | 交叉监测； |
| I1、I2 | 输入装置，例如：传感器； |
| L1、L2 | 逻辑模块； |
| m | 监测； |
| O1、O2 | 输出装置，例如：主接触器。 |

**图 11　3 类的指定结构**

6.2.7 4类

对于4类，应满足6.2.3中B类的要求和6.2.4中“经验证的安全原则”的要求。另外还应满足以下要求：

4类SRP/CS的设计应使得：

——在这些有关安全部件中的任一部件的单一故障都不会导致安全功能的损失；

——在有关安全功能的下一个指令发出或发出之前检测到单一故障，例如：在开关接通时或机器工作循环结束时立即检测。

但是如果不可能进行这种检测时，那么未发现故障的累积也不应导致安全功能的丧失。

出现包括故障累积的整个SRP/CS的诊断覆盖率($DC_{avg}$)应是高的。每个冗余通道的$MTTF_d$应是高的。应采取防止CCF的措施(见附录F)。

注1：4类系统的工况应允许：

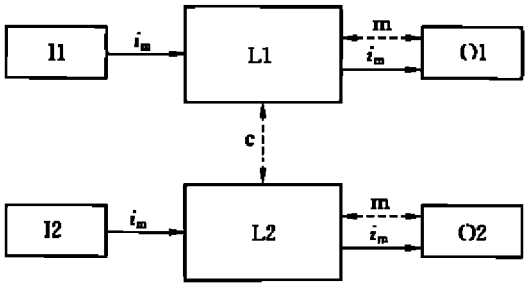
——发生单一故障时，安全功能总是有效；

——及时检测到故障以防安全功能的损失；

——考虑未检测到的故障的累积。

注2：3类和4类之间的差别是4类中的$DC_{avg}$更高，并且每个通道的要求的$MTTF_d$仅为“高”。

实际应用中，可能需要充分考虑两种故障的组合。




用于监测的实线代表诊断覆盖率，该诊断覆盖率大于3类中指定结构的诊断覆盖率。

$i_m$——连接方式；

c——相互监测；

I1、I2——输入装置，例如：传感器；

L1、L2——逻辑模块；

m——监测；

O1、O2——输出装置，例如：主接触器。

图12 4类的指定结构

表10 类别要求摘要

| 类别 | 要求摘要 | 系统性能 | 用于实现安全的原则 | 每个通道的$MTTF_d$ | $DC_{avg}$ | CCF |
|---|---|---|---|---|---|---|
| B<br>(见6.2.3) | SRP/CS和(或)其保护装置以及它们的元件都应根据相关标准进行设计、构造、选择、装配和组合，以使其能承受预期的影响。应使用基本安全原则 | 故障的发生能导致安全功能的丧失 | 主要特征是元件的选择 | 低至中 | 无 | 无关 |
| 1<br>(见6.2.4) | 应采用B类的要求。应使用经验证的元件和经验证的安全原则 | 故障的发生能导致安全功能的损失，但发生的概率低于B类的概率 | 主要特征是元件的选择 | 高 | 无 | 无关 |



标准分享网 www.bzfxw.com 免费下载

表 10（续）

| 类别 | 要求摘要 | 系统性能 | 用于实现安全的原则 | 每个通道的 $MTTF_d$ | $DC_{avg}$ | CCF |
|---|---|---|---|---|---|---|
| 2<br>（见 6.2.5） | 应采用 B 类的要求和经验证的安全原则<br>应通过机器控制系统以适当的时间间隔检查安全功能 | 在两次检查之间发生故障能导致安全功能的丧失<br>通过检查来检测安全功能的丧失 | 主要以结构为特征 | 低至高 | 低至中 | 见附录 F |
| 3<br>（见 6.2.6） | 应采用 B 类的要求和经验证的安全原则<br>有关安全部件的设计应使：<br>——在这些部件中的任何一个部件的单一故障都不会导致安全功能的损失，以及<br>——只要合理可行，都可检测到单一故障 | 当发生单一故障时，安全功能总是有效<br>某些但不是全部故障将被检测到<br>未检测到故障的积累能导致安全功能的丧失 | 主要以结构为特征 | 低至高 | 低至中 | 见附录 F |
| 4<br>（见 6.2.7） | 应采用 B 类的要求和经验证的安全原则<br>有关安全部件的设计应使：<br>——在这些部件中的任何一个部件的单一故障都不会导致安全功能的损失，以及<br>——在下一个有关安全功能指令发出时或发出前检测到单一故障。如果不可能，则未检测到的故障的积累不应导致安全功能的损失 | 发生单一故障时，安全功能总是有效<br>故障积累的检测减小了安全功能损失的概率（高 DC）<br>故障将被及时检测到，以防安全功能的丧失 | 主要以结构为特征 | 高 | 高（包括故障积累） | 见附录 F |
| 注：全部要求见第 6 章。 | | | | | | |

## 6.3 用于实现全部 PL 的 SRP/CS 组合

安全功能能通过几个 SRP/CS 的组合来实现：输入系统、信号处理单元、输出系统。这些 SRP/CS 可能指定一种和（或）多种类别。对于每个所使用的 SRP/CS，应按照 6.2 选择一种类别。对于这些 SRP/CS 的总组合，总的 PL 应根据表 11 来确定。这种情况下，需要对 SRP/CS 的组合进行确认（见图 3）。

根据 6.2，控制系统有关安全部件的组合起始于有关安全信号的触发点，终止于动力控制单元的输出。但组合的 SRP/CS 可由几个线性（串联）或冗余（并联）方式连接的部件组成。所有部件的各自性能等级（PL）都已算出时，为了避免更复杂的估计应由组合 SRP/CS 实现。以下的估计用于串联的 SRP/CS。

假定作为一个整体执行安全功能的串联 SRP/CS 分为 $N$ 个单独的 $SRP/CS_i$。对于每个 $SRP/CS_i$，其 $PL_i$ 已经算出。此情形由图 13 给出图示（也可见图 4 和图 H.2）。

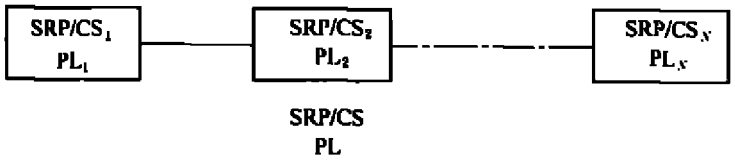



图 13 实现总 PL 的 SRP/CS 组合

以下方法用于执行安全功能的整个 SRP/CS 组合的 PL 的计算：

a) 确定最低的 $PL_r$：$PL_{low}$；

b) 确定 SRP/CS 的个数 $N_{low}$，$N_{low} \leqslant N$ 且 $PL_r = PL_{low}$；

c) 查询表 11 中的 PL。

表 11 串联 SRP/CS 的 PL 计算

| $PL_{low}$ | $N_{low}$ | ⇒ | PL |
|---|---|---|---|
| a | >3 | ⇒ | 无，不允许 |
| | ≤3 | ⇒ | a |
| b | >2 | ⇒ | b |
| | ≤2 | ⇒ | b |
| c | >2 | ⇒ | b |
| | ≤2 | ⇒ | c |
| d | >3 | ⇒ | c |
| | ≤3 | ⇒ | d |
| e | >3 | ⇒ | d |
| | ≤3 | ⇒ | e |
| 注：本查询表中用于计算的值基于每个 PL 中点的可靠性值。 | | | |

## 7 故障考虑和故障排除

### 7.1 概述

根据所选的类别，有关安全部件的设计应实现要求的性能等级($PL_r$)。应评价部件耐故障的能力。

### 7.2 故障考虑

GB/T 16855.2 中列出了不同技术的重要故障和失效。故障清单并不是唯一的，必要时应考虑和列出附加的故障。此时，也宜明确描述评定的方法。对于 GB/T 16855.2 中没有提及的新元件，应进行失效模式及影响分析(FMEA，见 GB/T 7826)以确定这些元件要考虑的故障。

通常，应考虑以下的故障判别准则：

——如果由于一个故障的结果而导致更多元件失效，则第一个故障和随后所发生的故障均应视为单一故障；

——有共同原因造成的两个或两个以上单独的故障应视为单一故障(即通常所说的 CCF)；

——由各自原因同时发生的两个或多个独立故障被认为是极不可能的，因此无需考虑。

### 7.3 故障排除

如果不假定某些故障能够被排除，则未必能评定 SRP/CS。关于故障排除的详细信息见 GB/T 16855.2。

故障排除是技术上的安全要求和理论上的故障发生可能性之间的折衷。

故障排除可根据：

— 在技术上不大可能发生的某些故障；

——普遍认可的、独立于所考虑的应用的技术经验，以及

— 与应用和特定危险有关的技术要求。

如果已排除故障，在技术文件中应给出详细的理由。



标准分享网 www.bzfxw.com 免费下载

CEPIC



## 8 确认

应对 SRP/CS 的设计进行确认(见图 3)。确认应证明 SRP/CS 的组合提供的每种安全功能满足本部分的所有相关要求。

确认的详细要求见 GB/T 16855.2。

## 9 维护

为了保持有关安全部件的规定性能,预防性或修复性维护通常是必要的。随着时间的推移,规定的性能会产生退化,并能导致安全性能恶化甚至导致危险状态。SRP/CS 的使用信息应包括 SRP/CS 的维护说明(包括定期检查)。

控制系统有关安全部件的可维护性的规定应遵循 GB/T 15706.2—2007,4.7 中规定的原则。维护的全部信息应符合 GB/T 15706.2—2007 中 6.5.1e)的要求。

## 10 技术文件

设计 SRP/CS 时,设计者至少应对以下与有关安全部件有关的信息进行归档:

——SRP/CS 提供的安全功能;

——每种安全功能的特征;

——有关安全部件确切的起始点和终止点;

——环境条件;

——性能等级(PL);

——所选的类别;

——与可靠性有关的参数($MTTF_d$、DC、CCF 和任务时间);

——防止系统性失效的措施;

——所使用的技术;

——考虑所有与安全有关的所有故障;

——故障排除的理由(也可见 GB/T 16855.2);

——设计原理(例如:故障考虑、故障排除等);

——软件文件;

——防止可预见的误用的措施。

注:一般来说,技术文档预期是为制造商内部提供的,而不向机器的用户提供。

## 11 使用信息

应采用 GB/T 15706.2—2007 的 6.5.2 中的原则和其他相关标准(例如:IEC 60204-1:2005 中的第 17 章)中适用的部分。尤其是应向使用者提供安全使用 SRP/CS 的那些重要信息。这包括,但不限于下列信息:

——有关安全部件类别的选择和任何故障排除的限制;

——SRP/CS 和任何故障排除的限制(见 7.3)。在保持所选类别和安全性能的情况下,当故障排除是必不可少时,应给出适当的信息(例如:改进、维护和维修的信息),以保证故障排除的连续合理性;

——规定性能的偏差对安全功能的影响;

——SRP/CS 与保护装置的接口的明确阐述;

——响应时间;

——操作限制(包括环境条件);

——指示和警报；
——安全功能的抑制和暂停；
——控制模式；
——维护(见第9章)；
——维护检查清单：
— 内部零件的易接近性和可换性；
— 方便、安全的故障查找方式；
——说明用于制定引用文件的与使用相关的信息；
—— 相关的检查测试间隔。

应提供关于SRP/CS的类别和性能等级的如下具体信息：

— 本部分中带日期的引用文件(即："GB/T 16855.1—2008")；
— 类别：B类、1类、2类、3类或4类；
— 性能等级：a、b、c、d或e。

示例：根据GB/T 16855.1的本版本中B类和性能等级a设计的SRP/CS，其引用文件如下：
GB/T 16855.1—2008，B类，PL=a



标准分享网 www.bzfxw.com 免费下载

# 附 录 A
## （资料性附录）
## 要求的性能等级($PL_r$)的确定

### A.1 $PL_r$ 的选择

本附录是关于所考虑的控制系统有关安全部件对风险减小的作用。这里给出的方法只是减小风险的一种估计方法，目的是作为设计者和标准制定者在根据 SRP/CS 执行的每种必需的安全功能确定 $PL_r$ 时的指南。

风险评价可假定一种优先于预定安全功能规定的情形：在确定预定安全功能的 $PL_r$ 时，可考虑通过其他独立于控制系统的技术措施（例如：机械防护装置）或附加安全功能来实现风险减小。在这种情况下，执行这些措施后，可选择图 A.1 中的起始点进行风险评价（也可见图 2）。伤害的严重度（用 S 表示）比较容易估计（例如：划伤、断肢、死亡等）。对于发生的频率，采用辅助参数来改进估计。这些参数是：

— 暴露于危险的频率和时间（F），以及

— 避免危险或限制伤害的可能性（P）。

经验表明：这些参数可组合成如图 A.1 所示的由低到高的风险等级。需要强调的是，这仅是给出风险估计的一个定性过程。

### A.2 用于选择风险估计参数 S、F 和 P 的指南

#### A.2.1 伤害严重度 S1 和 S2

在估计由安全功能失效引起的风险时，仅考虑轻微伤害（通常是可恢复的）、严重伤害（通常是不可恢复的）和死亡。

为了做出决定，在确定 S1 和 S2 时宜把事故的通常后果和正常的复原过程考虑进去。例如：把无并发症的擦伤和（或）划伤可定为 S1，而把断肢或死亡定为 S2。

#### A.2.2 暴露于危险的频率和（或）时间 F1 和 F2

不能规定对选择用于参数 F1 或 F2 的通常有效时间段。但在有疑问的情况下，以下说明可能有助于做出正确的选择。

如果人员频繁的或连续的暴露于危险中，宜选用 F2。这与是否是同一个人或不同的人连续暴露于危险无关，例如：使用电梯。频率参数宜根据接近危险的频率和持续时间来选择。

如果设计者知道对安全功能的需求，则可选择用这个要求的频率和持续时间来代替接近危险的频率和持续时间。在本部分中，在安全功能方面要求的频率假定为每年至少一次。

暴露于危险的持续时间宜根据能发现的与设备的总时间周期有关的暴露时间平均值来估计。例如：循环操作期间，为了进给和移动工件，有必要经常接近机器的刀具，则宜选择 F2。如果只是有时需要接近，则宜选择 F1。

注：如果频率为每小时大于一次且没有其他理由，则宜选择 F2。

#### A.2.3 避免危险的可能性 P1 和 P2

重要的是要知道：在导致事故之前，能否识别和避免危险状况。例如：重点考虑危险是否能直接通过其物理特征来识别，或者只能通过技术手段（例如：指示器）来识别。影响参数 P 的选择的其他重要因素包括，例如：

- 操作有无监控；
- 由专业人员或非专业人员操作；

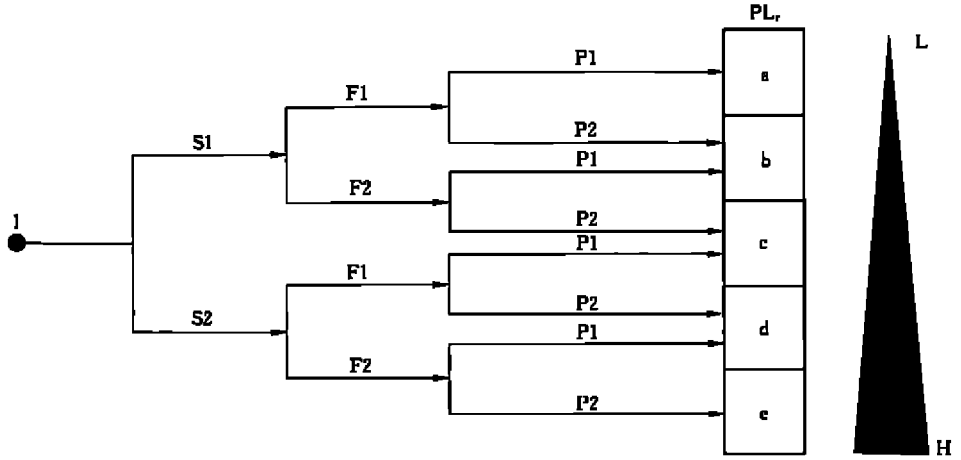
——产生危险的速度(例如:迅速或缓慢);

——避免危险的可能性(例如:通过撤离);

——与过程有关的实际安全经验。

当危险状况发生时,如果有避免事故或明显减小其影响的实际机会,则只宜选择 P1;如果几乎没有避免危险的机会,则宜选择 P2。

图 A.1 给出了根据风险评价确定有关安全部件 $PL_r$ 的指南。宜按下图来考虑每种安全功能。风险评价方法基于 GB/T 16856,且宜按照 GB/T 15706.1 的规定使用。




1——估计安全功能对风险减小的作用的起始点;

L——对风险减小的作用小;

H——对风险减小的作用大;

$PL_r$——要求的性能等级。

风险参数:

S——伤害的严重度;

S1——轻微(通常是可恢复的伤害);

S2——严重(通常是不可恢复的伤害或死亡);

F——暴露于危险的频率和(或)持续时间;

F1——很少—不常和(或)暴露时间短;

F2——频繁—连续和(或)暴露时间长;

P——避免危险或限制伤害的可能性;

P1——在特定条件下的可能性;

P2——几乎不可能。

**图 A.1 用于确定安全功能要求的 $PL_r$ 的风险图**



标准分享网 www.bzfxw.com 免费下载

# 附 录 B
## （资料性附录）
## 模块法和有关安全的模块图

### B.1 模块法

该简化方法需要 SRP/CS 面向块的逻辑表示。SRP/CS 宜根据以下要求分为数量不多的模块：

——模块宜代表与执行有关全功能的 SRP/CS 逻辑单元；

——执行安全功能的不同通道宜分为不同的模块——如果一个模块不再执行其功能，不宜影响经由其他通道的模块执行的安全功能；

——每个通道可由一个或多个模块组成——在指定结构中每个通道 3 个模块（输入、逻辑单元和输出）并不是强制要求的数目，而只是每个通道内逻辑划分的简单示例；

——SRP/CS 的每个硬件单元宜完全归属于一个模块，这样才能允许对建立在属于该模块的硬件单元的 $MTTF_d$ 基础上的该模块的 $MTTF_d$ 进行计算（例如：通过失效模式和影响分析或部件计数法，见附录 D.1）。

——仅用于诊断（例如：试验设备）且在其发生危险失效时不影响不同通道中安全功能执行的那些硬件单元，可以与不同通道中安全功能执行必需的硬件单元分开。

注：本部分中，"模块"并不对应于功能模块或可靠性模块。

### B.2 有关安全的模块图

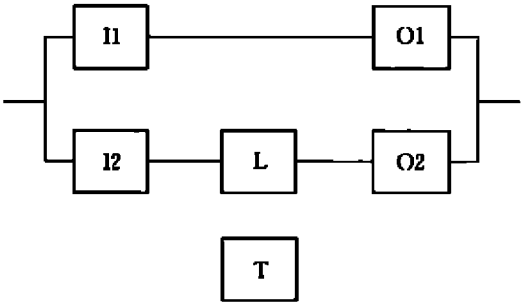
由模块法定义的模块可在有关安全的模块图中用图形方式表示 SRP/CS 的逻辑结构。对于这种图形表示，下列要求可作为指南：

——在串联模块中，一个模块的失效导致整个通道的失效（例如：如果 SRP/CS 中一个通道中的一个硬件单元发生危险失效，则整个通道也许就不再能执行安全功能）；

——在并联模块中，只有所有的通道发生危险失效才导致安全功能的丧失（例如：由几个通道执行的安全功能只要至少有一个通道没有失效就可执行）；

——那些仅用于检测目的且其发生危险失效时不影响不同通道安全功能执行的模块，可与不同通道中的模块分离开。

示例见图 B.1。




I1 和 O1 构成了第一个通道（串联），I2、L 和 O2 构成了第二个通道（串联）。两个通道以冗余方式执行安全功能（并联）。T 仅用于检测。

I1、I2——输入装置，例如：传感器；

L——逻辑模块；

O1、O2——输出装置，例如：主接触器；

T——检测装置。

图 B.1 有关安全功能模块图示例

# 附 录 C
（资料性附录）
单个元件 $MTTF_d$ 值的计算或估计

## C.1 概述

本附录给出几种用于计算或估计单个元件 $MTTF_d$ 值的方法：C.2 中给出的方法建立在不同种类元件良好的工程实践基础上；C.3 中给出的方法适用于液压元件；C.4 给出了根据 $B_{10}$（见 C.4.1）计算气动元件、机械元件和机电元件的 $MTTF_d$ 的方法；C.5 列出了用于电气元件的 $MTTF_d$ 的值。

## C.2 良好的工程实践方法

如果满足以下准则，则能根据表 C.1 估计用于元件的 $MTTF_d$ 值和 $B_{10d}$ 值：

a) 元件是根据符合 GB/T 16855.2—2007 中的基本原则和经验证的原则或根据元件设计的相关标准（见表 C.1）而制造的（元件数据表中确认的）。

注：该信息能在元件制造商的数据表中找到。

b) 元件制造商为使用者规定适当的应用和工作条件。

c) SRP/CS 的设计满足 GB/T 16855.2—2007 中用于元件执行和工作的基本的和经验证的安全原则。

## C.3 液压元件

如果满足以下准则，则单个液压元件（例如：阀门）的 $MTTF_d$ 值估计在 150 年：

a) 液压元件是根据 GB/T 16855.2—2007 中的基本的和经验证的原则或根据表 C.1 和表 C.2 中用于液压元件设计的原则制造的（元件数据表中确认的）。

注：该信息能在元件制造商的数据表中找到。

b) 液压元件制造商为使用者规定适当的应用和工作条件。SRP/CS 的制造商应根据 GB/T 16855.2—2007，表 C.1 和表 C.2，负责对液压元件的执行和工作提供与基本的和经验证的安全原则的应用有关的信息。

如果不能达到 a）或 b）的要求，制造商应给出单个液压元件的 $MTTF_d$ 值。

表 C.1 与元件 $MTTF_d$ 或 $B_{10d}$ 的标准

| 项 目 | 根据 GB/T 16855.2—2007，基本的和经验证的安全原则 | 其他相关标准 | 典型值：<br>$MTTF_d$（年）<br>$B_{10d}$（周期） |
|---|---|---|---|
| 机械元件 | 表 A.1 和 A.2 | — | $MTTF_d$ = 150 |
| 液压元件 | 表 C.1 和 C.2 | EN 982 | $MTTF_d$ = 150 |
| 气动元件 | 表 B.1 和 B.2 | EN 983 | $B_{10d}$ = 20 000 000 |
| 小载荷（机械载荷）继电器和接触式继电器 | 表 D.1 和 D.2 | EN 50205<br>IEC 61810<br>IEC 60947 | $B_{10d}$ = 20 000 000 |
| 最大载荷继电器和接触器 | 表 D.1 和 D.2 | EN 50205<br>IEC 61810<br>IEC 60947 | $B_{10d}$ = 400 000 |



标准分享网 www.bzfxw.com 免费下载

表 C.1（续）

| 项　目 | 根据 GB/T 16855.2　2007，基本的和经验证的安全原则 | 其他相关标准 | 典型值：<br>$MTTF_d$（年）<br>$B_{10d}$（周期） |
|---|---|---|---|
| 小载荷（机械载荷）接近开关 | 表 D.1 和 D.2 | IEC 60947<br>EN 1088 | $B_{10d}$ = 20 000 000 |
| 最大载荷接近开关 | 表 D.1 和 D.2 | IEC 60947<br>EN 1088 | $B_{10d}$ = 400 000 |
| 小载荷（机械载荷）接触器 | 表 D.1 和 D.2 | IEC 60947 | $B_{10d}$ = 20 000 000 |
| 额定载荷接触器 | 表 D.1 和 D.2 | IEC 60947 | $B_{10d}$ = 2 000 000 |
| 与载荷无关的位置开关 | 表 D.1 和 D.2 | IEC 60947<br>EN 1088 | $B_{10d}$ = 20 000 000 |
| 与载荷无关的位置开关（单独带有的致动器、防护锁） | 表 D.1 和 D.2 | IEC 60947<br>EN 1088 | $B_{10d}$ = 2 000 000 |
| 与载荷无关的急停装置[a] | 表 D.1 和 D.2 | IEC 60947<br>GB 16754 | $B_{10d}$ = 100 000 |
| 具有最大工作需要的急停装置 | 表 D.1 和 D.2 | IEC 60947<br>GB 16754 | $B_{10d}$ = 6 050 |
| 与载荷无关的按钮（例如：使能开关） | 表 D.1 和 D.2 | IEC 60947 | $B_{10d}$ = 100 000 |
| $B_{10d}$ 的定义和用法见 C.4。<br>注 1：$B_{10d}$ 被估计为 $B_{10}$ 的二倍（50%的危险失效率）。<br>注 2："小载荷"意指，例如：额定载荷值的 20%（更多信息见 GB/T 16855.2）。 | | | |
| [a] 假如直接打开动作的排除故障是可能的。 | | | |

## C.4　气动、机械和机电元件的 $MTTF_d$

### C.4.1　概述

对于气动元件、机械元件和机电元件（气动阀、继电器、接触器、位置开关、位置开关的凸轮等），可能难以计算出本部分所要求的，以年来表示的平均危险失效时间（元件的 $MTTF_d$）。多数时候，这类元件的制造商只给出元件危险失效的数量达到 10%时的平均周期数（$B_{10d}$）。本章给出了用制造商给出的 $B_{10d}$ 或 $T$（寿命）来计算元件 $MTTF_d$ 的方法，$B_{10d}$ 和 $T$ 与应用中的周期有紧密的联系。

假如满足以下准则，则能根据 C.4.2 估计单个气动元件、机电元件或机械元件的 $MTTF_d$ 值：

a）　元件是根据 GB/T 16855.2—2007 的表 B.1 或表 D.1 中的基本的和经验证的原则制造的（元件数据表中确认的）。

注：该信息能在元件制造商的数据表中找到。

b）　用于 1 类、2 类、3 类或 4 类的元件是根据 GB/T 16855.2　2007 的表 B.2 或表 D.2 中的基本的和经验证的原则制造的（元件数据表中确认的）。

注：该信息能在元件制造商的数据表中找到

c）　元件制造商为使用者规定适当的应用条件和工作条件。SRP/CS 的制造商应根据 GB/T 16855.2　2007中的表 B.1 和表 D.1，负责提供用于元件的执行和工作的基本安全原则方面的信息。对于 1 类、2 类、3 类或 4 类，则应告知使用者，其有责任履行 GB/T 16855.2—2007 的表 B.2 和 D.2 中的用于元件执行和工作的经验证的安全原则。

### C.4.2 根据 $B_{10d}$ 计算元件的 MTTF$_d$

元件制造商宜根据相应的产品测试方法标准(例如:IEC 60957-5-3、ISO 19973 和 IEC 61810 等)来确定 10%的元件达到危险失效时的平均周期数($B_{10d}$)[2)]。应定义出元件的危险失效模式,例如:在终点位置阻塞或开关时间改变。如果不是所有的元件都在测试过程中危险失效(例如:被测试的 7 个元件只有 5 个元件发生危险失效),则应考虑对没有发生危险失效的元件进行分析。

通过 $B_{10d}$ 和 $n_{op}$(年平均操作次数),可计算出元件的 MTTF$_d$:

$$\mathrm{MTTF_d} = \frac{B_{10d}}{0.1 \times n_{op}} \qquad \text{……(C.1)}$$

式中:

$$n_{op} = \frac{d_{op} \times h_{op} \times 3\ 600\ \mathrm{s/h}}{t_{周期}} \qquad \text{……(C.2)}$$

元件应用时做以下的假设:

$h_{op}$——平均工作时间,单位以小时每天计;

$d_{op}$——平均工作时间,单位以天每年计;

$t_{周期}$——元件两个相继周期起的起始点(例如:阀的切换)之间的平均工作时间,单位以秒每周期计。

元件的工作时间限制在 $T_{10d}$ 内,10%元件发生危险失效的平均时间为:

$$T_{10d} = \frac{B_{10d}}{n_{op}} \qquad \text{……(C.3)}$$

注:公式的解释见 C.4.2。

通过使用年平均操作次数 $n_{op}$,10%的元件发生危险失效时的平均周期数 $B_{10d}$ 能转变为 10%的元件发生危险失效时的平均时间 $T_{10d}$:

$$T_{10d} = \frac{B_{10d}}{n_{op}} \qquad \text{……(C.4)}$$

本部分中的可靠性计算方法假定元件的失效为时间的指数分布:$F(t)=1-\exp(-\lambda dt)$。对于气动和机电元件,更可能是威布尔分布。但如果元件的工作时间被限制在 10%的元件发生危险失效的平均时间内($T_{10d}$),则可把该工作时间内的恒定危险失效率($\lambda_d$)可估计为:

$$\lambda_d \approx \frac{0.1}{T_{10d}} = \frac{0.1 \times n_{op}}{B_{10d}} \qquad \text{……(C.5)}$$

等式(C.5)考虑了在与 $B_{10d}$[周期]相对应的 $T_{10d}$[年]后有 10%的元件在假设的应用中失效的恒定失效率。准确的说:

$$F(T_{10d}) = 1-\exp(-\lambda_d\ T_{10d}) = 10\%,\text{其中 } \lambda_d = -\frac{\ln(0.9)}{T_{10d}} = \frac{0.105\ 36}{T_{10d}} \approx \frac{0.1}{T_{10d}} \cdots\text{(C.6)}$$

对于指数分布,由于 MTTF$_d$ = $1/\lambda_d$,代入后得:

$$\mathrm{MTTF_d} = \frac{T_{10d}}{0.1} = \frac{B_{10d}}{0.1 \times n_{op}} \qquad \text{……(C.7)}$$

### C.4.3 示例

对于气动阀,制造商确定以 $6\times10^7$ 个周期的平均值作为 $B_{10d}$。该阀门在一年中工作 220 天,每天切换两次。阀门两次相继切换的起始点之间的平均时间估为 5 s。这就产生了以下的值:

——$d_{op}$=220d/a;

——$h_{op}$=16h/d;

——$t_{周期}$=5s/cycle;

——$B_{10d}=6\times10^7$ 个周期。

2) 如果没有给出 $B_{10}$ 的危险分数,则可使用 $B_{10}$ 的 50%,因此推荐采用 $B_{10d}=2B_{10}$。



标准分享网 www.bzfxw.com 免费下载

把这些值代入下列方程式进行计算：

$$n_{op}=\frac{d_{op}\times h_{op}\times 3\,600}{t_{周期}}$$

$$=\frac{220\times 16\times 3\,600}{5}$$

$$=2.53\times 10^{6}\ 周期/年 \qquad \cdots\cdots(C.8)$$

$$T_{10d}=\frac{B_{10d}}{n_{op}}=\frac{60\times 10^{6}}{2.53\times 10^{6}}=23.7\ 年 \qquad \cdots\cdots(C.9)$$

$$MTTF_d=\frac{23.7\ 年}{0.1}=237\ 年 \qquad \cdots\cdots(C.10)$$

根据表 5 可给出该元件的 $MTTF_d$ 为“高”。阀门的有效工作时间 23.7 年仅为假设。

## C.5 电气元件的 $MTTF_d$ 数据

### C.5.1 概述

表 C.2 至表 C.7 给出了电子元件 $MTTF_d$ 的某些典型平均值。这些数据来源于 SN 29500 系列数据库[51]。所有数据均为普通类型的。各种不同的数据库(见参考文献目录中未全收列的参考文献)可用于表示各种不同的电子元件的 $MTTF_d$ 值。如果 SRP/CS 的设计者具有所用元件的可靠的专用数据，则强烈推荐以专用数据代替所用的数据。

表 C.2 至表 C.7 中给出的值对于温度为 40 ℃时的电流和电压的额定载荷有效。

在这些表的 MTTF 栏中，来源于 SN 29500 的值用于通用元件所有可能的失效模式，这些失效模式并不一定造成危险失效。在 $MTTF_d$ 栏中，典型的假设是：并不是所有的失效模式都会导致危险失效。这主要取决于实际应用。准确确定元件“典型”$MTTF_d$ 值的方法是进行失效模式及影响分析(FMEA)。某些元件，例如用作开关的晶体管，可能会遇到短路或断路而失效。这两种失效模式中只有一种可能是危险的，因此，在“备注”栏中假设危险失效的概率只有 50%，这就意味着元件的 $MTTF_d$ 是给出的 MTTF 值的两倍。对于用途不确定、在最坏情况下使用的元件，其 $MTTF_d$ 在 $MTTF_d$ 一栏的“最坏情形”栏中给出，它的安全裕度为 10。

### C.5.2 半导体

见表 C.2 和表 C.3。

表 C.2 晶体管(用作开关)

| 晶体管 | 示 例 | 元件的 MTTF/年 | 元件的 $MTTF_d$/年 | | 备 注 |
|---|---|---|---|---|---|
| | | | 典型情形 | 最坏情形 | |
| 两极 | TO18、TO92、SOT23 | 34 247 | 68 493 | 6 849 | 危险失效概率 50% |
| 两极、低功率 | TO5、TO39 | 5 708 | 11 416 | 1 142 | 危险失效概率 50% |
| 两极、功率 | TO3、TO220、D-Pack | 1 941 | 3 881 | 388 | 危险失效概率 50% |
| FET | MOS 交叉点 | 22 831 | 45 662 | 4 566 | 危险失效概率 50% |
| MOS、功率 | TO3、TO220、D-Pack | 1 142 | 2 283 | 228 | 危险失效概率 50% |

表 C.3 二极管、功率半导体和集成电路

| 二极管 | 示 例 | 元件的 MTTF/年 | 元件的 $MTTF_d$/年 | | 备 注 |
|---|---|---|---|---|---|
| | | | 典型情形 | 最坏情形 | |
| 一般用途 | — | 114 155 | 228 311 | 22 831 | 危险失效概率 50% |
| 干扰抑制器 | — | 15 981 | 31 963 | 3 196 | 危险失效概率 50% |

表 C.3（续）

| 二极管 | 示 例 | 元件的 MTTF/年 | 元件的 $MTTF_d$/年 | | 备 注 |
|---|---|---|---|---|---|
| | | | 典型情形 | 最坏情形 | |
| 齐纳二极管 $P_m<1$ W | | 114 155 | 228 311 | 22 831 | 危险失效概率 50% |
| 整流二极管 | -- | 57 078 | 114 155 | 11 416 | 危险失效概率 50% |
| 桥式整流器 | — | 11 415 | 22 831 | 2 283 | 危险失效概率 50% |
| 闸流晶体管 | -- | 2 283 | 4 566 | 457 | 危险失效概率 50% |
| 双向三极管开关、二端交流开关 | | 1 484 | 2 968 | 297 | 危险失效概率 50% |
| 集成电路（可编程的和不可编程的） | 采用制造商的数据 | | | | 危险失效概率 50% |

## C.6 无源元件

见表 C.4～表 C.7。

表 C.4 电容

| 电容 | 示例 | 元件的 MTTF/年 | 元件的 $MTTF_d$/年 | | 备 注 |
|---|---|---|---|---|---|
| | | | 典型情形 | 最坏情形 | |
| 标准的无源电容 | KS、KP、KC、KT、MKT、MKC、MKP、MKU、MP、MKV | 57 078 | 114 155 | 11 416 | 危险失效概率 50% |
| 陶瓷电容 | — | 22 831 | 45 662 | 4 566 | 危险失效概率 50% |
| 铝电解质电容 | 非固态电解质 | 22 831 | 45 662 | 4 566 | 危险失效概率 50% |
| 铝电解质电容 | 固态电解质 | 37 671 | 75 342 | 7 534 | 危险失效概率 50% |
| 钽电解质电容 | 非固态电解质 | 11 415 | 22 831 | 2 283 | 危险失效概率 50% |
| 钽电解质电容 | 固态电解质 | 114 155 | 228 311 | 22 831 | 危险失效概率 50% |

表 C.5 电阻

| 电 阻 | 示 例 | 元件的 MTTF/年 | 元件的 $MTTF_d$/年 | | 备 注 |
|---|---|---|---|---|---|
| | | | 典型情形 | 最坏情形 | |
| 碳膜 | | 114 155 | 228 311 | 22 831 | 危险失效概率 50% |
| 金属膜 | | 570 776 | 1 141 552 | 114 155 | 危险失效概率 50% |
| 金属氧化物和线绕电阻 | -- | 22 831 | 45 662 | 4 566 | 危险失效概率 50% |
| 可变电阻 | | 3 767 | 7 534 | 753 | 危险失效概率 50% |

表 C.6 感应器

| 感应器 | 示例 | 元件的 MTTF/年 | 元件的 $MTTF_d$/年 | | 备 注 |
|---|---|---|---|---|---|
| | | | 典型情形 | 最坏情形 | |
| MC 应用 | | 37 671 | 75 342 | 7 534 | 危险失效概率 50% |
| 低频感应器和变压器 | | 22 831 | 45 662 | 4 566 | 危险失效概率 50% |
| 主变压器、用于开关方式以及动力供应的变压器 | | 11 415 | 22 831 | 2 283 | 危险失效概率 50% |



标准分享网 www.bzfxw.com 免费下载

CEPIC



表 C.7 光耦合器

| 光耦合器 | 示例 | 元件的 MTTF/年 | 元件的 $MTTF_d$/年 | | 备 注 |
|---|---|---|---|---|---|
| | | | 典型情形 | 最坏情形 | |
| 双极输出 | SFH 610 | 7 648 | 15 296 | 1 530 | 危险失效概率 50% |
| FET 输出 | LH 1056 | 2 854 | 5 708 | 571 | 危险失效概率 50% |

# 附 录 D
（资料性附录）
估计每个通道 $MTTF_d$ 的简化方法

## D.1 部件计数法

采用“部件计数法”适用于分别估计每个通道的 $MTTF_d$。计算时要用到组成该通道的所有单个元件的 $MTTF_d$ 值[3)]。

通用公式为：

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\bar{N}} \frac{1}{MTTF_{di}} = \sum_{j=1}^{\bar{N}} \frac{n_j}{MTTF_{dj}} \qquad \text{……(D.1)}$$

式中：

$MTTF_d$——用于整个通道；

$MTTF_{di}$、$MTTF_{dj}$——对安全功能有一定作用的每个元件的 $MTTF_d$。

第一个和是每个独立元件的 $MTTF_d$ 相加之和；第二个和是一个等效的简化形式，其中所有的 $n_j$ 个具有相同 $MTTF_{dj}$ 的完全相同的元件被分类归集在一起。

表 D.1 中的示例给出了该通道的 $MTTF_d$ 为 21.4 年，根据表 5，该示例的 $MTTF_d$ 为“中”。

表 D.1 电路板的零件表示例

| $j$ | 元件 | 元件数 $n_j$ | 最坏情形的 $MTTF_{dj}$/年 | 最坏情形的 $1/MTTF_{dj}$ | 最坏情形的 $n_j/MTTF_{dj}$ |
|---|---|---|---|---|---|
| 1 | 晶体管、两极、低功率(见表 C.2) | 2 | 1 142 | 0.000 876 | 0.001 752 |
| 2 | 电阻、碳膜(见表 C.5) | 5 | 22 831 | 0.000 044 | 0.000 219 |
| 3 | 电容、标准、无功率(见表 C.4) | 4 | 11 416 | 0.000 088 | 0.000 350 |
| 4 | 继电器(有小载荷，见 C.2)($B_{10d}$= 20 000 000 周期、$n_{op}$=633 600) | 4 | 315.66 | 0.003 168 | 0.012 672 |
| 5 | 接触器(有公称载荷，见 C.2)($B_{10d}$= 2 000 000 周期、$n_{op}$=633 600) | 1 | 31.57 | 0.031 676 | 0.031 676 |
| $\Sigma(n_j/MTTF_{dj})$ | | | | | 0.046 669 |
| $MTTF_d = 1/\Sigma(n_j/MTTF_{dj})$[年] | | | | | 21.43 |

注 1：本方法建立在假设一个通道中的任何元件的危险失效会导致该通道的危险失效的基础上。表 D.1 中通过示例说明的 $MTTF_d$ 的计算就基于这个假设。

注 2：本示例中，主要影响来自于接触器。本示例为 $MTTF_d$ 和 $B_{10d}$ 所选择的值是建立在附录 C 的基础上的。对于该示例的应用，$d_{op}$=220 天/年，$h_{op}$=8 小时/天以及 $t_{cycle}$=10 秒/周期是一种假定，从而给出 $n_{op}$=633 600 周期/年。通常，采用制造商提供的 $MTTF_d$ 和 $B_{10d}$ 值将会产生更好的结果，即对于该通道来说，将达到更高的 $MTTF_d$。

## D.2 用于不同通道的 $MTTF_d$，每个通道的 $MTTF_d$ 的平衡

6.2 中的指定结构假设：对于冗余的 SRP/CS 中的不同通道，每个通道的 $MTTF_d$ 值是相同的。每

3) 部件计数法通常是一种在安全上经常过于苛刻的近似方法。如果需要更加精确的值，设计者宜考虑失效模式，但这非常复杂。



标准分享网 www.bzfxw.com 免费下载

个通道的 $MTTF_d$ 值宜输入到图 5 中。

如果这些通道的 $MTTF_d$ 不同，则有两种可能：

——作为最坏情形假设，宜考虑采用较低的值；

——可以用等式(D.2)来估计一个替代值来代替每个通道的 $MTTF_d$：

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}}\right] \quad \cdots\cdots\cdots(D.2)$$

式中，$MTTF_{dC1}$ 和 $MTTF_{dC2}$ 是两个不同的冗余通道的 $MTTF_d$ 值。

示例：一个通道的 $MTTF_{dC1}=3$ 年，另一个通道的 $MTTF_{dC2}=100$ 年，则每个通道最终的 $MTTF_d=66$ 年。这就是说一个通道的 $MTTF_d$ 为 100 年，另一个通道的 $MTTF_d$ 为 3 年的冗余系统等效于每个通道的 $MTTF_d$ 都为 66 年的系统。

根据上面的公式，具有两个通道并且每个通道具有不同的 $MTTF_d$ 值的冗余系统，能由在每个通道中具有相同 $MTTF_d$ 值的冗余系统来代替。这个过程是正确使用表 5 所必需的。

注：本方法假设采用独立的并联通道。

# 附 录 E
（资料性附录）
对功能和模块的诊断覆盖率(DC)的估计

## E.1 诊断覆盖率(DC)的示例

见表 E.1。

表 E.1 诊断覆盖率(DC)的估计

| 措 施 | DC |
|---|---|
| 输入装置 | |
| 通过输入信号的动态变化促进循环测试 | 90% |
| 真实性检查，例如：使用常开和常闭的机械连接接触器 | 99% |
| 对无动态测试的输入的交叉监测 | 0～99%，取决于应用中信号改变的频率 |
| 如果无法检测到短路，对有动态测试的输入的交叉监测(多路 I/O) | 90% |
| 对逻辑(L)中和程序流的临时逻辑软件监视器中的输入信号和中间结果的交叉监测，以及静态故障和短路的检测(用于多路 I/O) | 99% |
| 间接监测(例如：通过压力开关进行监测，通过驱动器的电气位置进行监测) | 90%～99%，取决于实际应用 |
| 直接监测(例如：控制阀的电气位置监测，通过机械连接的接触器元件监测机电装置) | 99% |
| 通过过程实施故障检测 | 0～99%，取决于实际应用；单用本措施是达不到要求的性能等级"e"的 |
| 监测某些传感器的特征(响应时间、相似信号的范围，例如：电阻、电容) | 60% |
| 间接监测(例如：通过压力开关进行监测，通过驱动器的电气位置进行监测) | 90%～99%，取决于实际应用 |
| 直接监测(例如：控制阀的电气位置监测，通过机械连接的接触器元件监测机电装置) | 99% |
| 逻辑模块的简单暂时时间监测(例如：定时器用作监视器，逻辑模块程序中的触发点) | 60% |
| 当试验设备进行逻辑模块性能的真实性检查时，由监视器暂时对逻辑进行逻辑监测 | 90% |
| 启动自检以检测逻辑中部件的潜在故障(例如：程序和数据存储器、输出 输出端口、接口) | 90%(取决于测试技术) |
| 启动时通过主通道，或通过安全功能或外部信号所要求的输入设备来检查监测设备(例如：监视器)的反应能力 | 90% |
| 动态原则(安全功能需要时，逻辑模块的所有元件需要按状态 ON-OFF-ON 状态改变)，例如：由继电器执行的联锁电路 | 99% |
| 恒定存储器：单字节信号(8bit) | 90% |
| 恒定存储器：双字节信号(16bit) | 99% |



标准分享网 www.bzfxw.com 免费下载

表 E.1（续）

| 措　施 | DC |
|---|---|
| 输入装置 | |
| 可变存储器：使用冗余数据进行 RAM 测试，例如：标记、标志、恒址、定时器及这些数据的交叉比较 | 60% |
| 可变存储器：检查存储器单元数据的可读性和可写性 | 60% |
| 可变存储器：由改进的汉明码或 RAM 自检进行 RAM 监测（例如："galpat"码或"Abraham"码） | 99% |
| 处理单元：通过软件自检 | 60%～90% |
| 处理单元：编码处理 | 90%～99% |
| 通过过程检测故障 | 0～99%，取决于实际应用；单独用本措施是达不到要求的性能等级"e"的 |
| 无动态试验的由一个通道对输出的监测 | 0～99%，取决于应用中信号改变的频率 |
| 无动态试验的输出的交叉监测 | 0～99%，取决于应用中信号改变的频率 |
| 带动态试验，无短路检测的输出信号交叉监测（多路 I/O） | 90% |
| 对逻辑（L）中和程序流的临时逻辑软件监视器中的输出信号和中间结果的交叉监测，以及对静态故障和短路的检测（用于多路 I/O） | 99% |
| 无致动器监测的冗余截止路径 | 0 |
| 通过逻辑模块或试验设备监测其中一个致动器的冗余截止路径 | 90% |
| 通过逻辑模块和试验设备监测致动器的冗余截止路径 | 99% |
| 间接监测（例如：通过压力开关进行监测，通过致动器的电气位置进行监测） | 90%～99%，取决于实际应用 |
| 通过过程检测故障 | 0～99%，取决于实际应用；单独用本措施是达不到要求的性能等级"e"的 |
| 直接监测（例如：控制阀的电气位置监测，通过机械连接触点元件监测机电装置） | 99% |
| 注 1：对于 DC 的附加估计，见 GB/T 20438.2—2006 中的 A.2 至 A.15 等。<br>注 2：如果声明逻辑模块的 DC 为中或高时，至少采用一种措施，使有各自 DC 的可变存储器、恒定存储器和处理单元必须至少应用其 DC 的 60%。除本表中列出的措施外，可能也还用到其他措施。 | |

## E.2　平均 DC（$DC_{avg}$）的估算

在很多系统中，可能用到多种故障检测措施。这些措施能检查 SRP/CS 的不同部件且有不同的 DC。当根据表 5 来估计 PL 时，执行安全功能的整个 SRP/CS 只有一个平均 DC 可用。

DC 可能被确定为被检测到的危险失效的失效率与全部危险失效的失效率之间的比率。根据这个定义，用以下公式来估计平均诊断覆盖率 $DC_{avg}$：

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \cdots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \cdots + \frac{1}{MTTF_{dN}}} \qquad \cdots\cdots\cdots\cdots\cdots\cdots (E.1)$$

式中，所有未经故障排除的 SRP/CS 元件都必须考虑在内并求和。对于每个模块，都应考虑 $MTTF_d$ 和 DC。本公式中的 DC 是指部件检测到的危险失效的失效率（不管用何种方法检测失效）与部件全部危险失效的失效率之间的比率。因此，DC 与被测试的零件有关，而与测试装置无关。无故障检测的元件（例如：没有进行测试的元件）其 DC=0，它只改变 $DC_{avg}$ 的分母。

# 附 录 F
（资料性附录）
共因失效(CCF)的估计

## F.1 共因失效(CCF)的要求

GB/T 20438.6—2006 的附录 D 中给出了传感器/致动器防止 CCF 的措施的综合程序，并单独给出了控制逻辑模块防止 CCF 的措施的综合程序。但并不是其中所有的措施都适用于机械场合。在本附录中给出了最重要的措施。

注：在本部分中作出的假设是：根据 GB/T 20438.6—2006 中附录 D，用于冗余系统的系数 $\beta$ 宜小于或等于 2%。

## F.2 CCF 影响的估计

此定量过程宜通过整个系统进行。宜考虑控制系统有关安全部件的每个部件。

基于工程学的判断，表 F.1 中列出了措施和关联值，它表示了每种措施对减小共因失效的作用。

对于列出的每种措施，只能声明完全得分的或没有得分的。如果只是部分满足某种措施，则该措施的得分为零。

表 F.2 给出了量化的 CCF。

表 F.1 防止 CCF 的措施的打分和量化过程

| 编 号 | 防止 CCF 的措施 | 得 分 |
|---|---|---|
| 1 | 分离/隔离 | |
| | 信号路径之间的物理分离：<br>以配线/管路方式分离；<br>印刷电路板上足够的间隙和爬电老化距离。 | 15 |
| 2 | 差异性 | |
| | 采用不同的技术/设计或物理原则，例如：<br>第一个通道为可编程电子的，第二个通道为硬布线的；<br>启动的种类；<br>压力和温度。<br>距离和压力的测量：<br>数字的或模拟的。<br>不同方法制造的元件。 | 20 |
| 3 | 设计/应用/经验 | |
| 3.1 | 过电压、过压力、过电流等的保护。 | 15 |
| 3.2 | 所用的元件是经验证的 | 5 |
| 4 | 评价/分析 | |
| | 为了避免共因失效，设计中是否考虑了失效模式和影响分析的结果。 | 5 |
| 5 | 能力/培训 | |
| | 设计者/维护者是否已经过培训，使其了解共因失效的原因和结果。 | 5 |
| 6 | 环境 | |



标准分享网 www.bzfxw.com 免费下载

表 F.1（续）

| 编　号 | 防止 CCF 的措施 | 得　分 |
|---|---|---|
| 6.1 | 根据适当的标准，通过防止污染和电磁兼容(EMC)来防止 CCF。<br>流体系统：传压介质的过滤、入口处污垢的防止、受压气体的排泄，例如：依照元件制造商关于传压介质净化的要求。<br>电气系统：是否检查了系统的电磁抗扰性，例如：按照相关标准中防止 CCF 的规定。<br>对于流体和电气组合的系统，这两个方面都宜予以考虑。 | 25 |
| 6.2 | 其他影响：<br>是否已考虑了对所有的环境因素，例如温度、冲击、振动、湿度等（例如：相关标准中所规定的）的抗扰性的要求？ | 10 |
| | 总和 | 最大可达到 100 |

| 总　分 | 避免 CCF 的措施[a] |
|---|---|
| 65 或 65 以上 | 满足要求 |
| 小于 65 | 处理失败⇒选择附加措施 |

[a] 与技术措施无关时，在综合计算中可以考虑附加于本栏的分值。

# 附 录 G
（资料性附录）
系统性失效

## G.1 概述

GB/T 16855.2 给出了宜用于防止系统性失效的综合措施表，例如基本的或经验证的安全原则。

## G.2 系统性失效的控制措施

宜采用以下措施：

——采用去能法（见 GB/T 16855.2）
控制系统有关安全部件（SRP/CS）的设计宜使其在动力供应损失时能达到或保持安全状态。

——控制击穿电压、电压变化、过电压和电压不足的影响的措施
宜预先确定 SRP/CS 对击穿电压、电压变化、过电压和电压不足等条件的响应工况，使 SRP/CS 能实现或保持机器的安全状态（也可见 GB 5226.1 和 GB/T 20438.7—2006 中的 A.8）。

——控制或避免物理环境（例如：温度、湿度、水、振动、灰尘、腐蚀性物质、电磁干扰及其影响）影响的措施
宜预先确定 SRP/CS 对物理环境响应的工况；使 SRP/CS 能实现或保持机器的安全状态（也可见 GB 5226.1 和 IEC 60529 等）。

——为了检测有缺陷的程序次序，应以包含软件的 SRP/CS 来使用程序次序监测
如果以错误的次序或在错误的时间段内处理一个程序的独立程序（例如：软件模块、子程序或指令），或者如果处理器的时钟有故障，则存在有缺陷的程序次序（见 EN 61508-7:2001，A.9）。

——控制错误的影响或由任何数据通信处理引起的其他影响的措施（见 GB/T 20438.2—2006 中的 7.4.8）。

另外，考虑到 SRP/CS 的复杂性及其 PL，还宜采用下列的一种或多种措施：

——通过自动测试的失效检测；
——通过冗余硬件的测试；
——多样的硬件；
——强制模式中的操作；
——机械连接的接触器；
——直接打开动作；
——定向失效模式；
——当制造商能证明降低额定值可提高可靠性时，用一个适当的系数进行超尺寸——在适宜进行超尺寸的情况下，超尺寸系数宜至少为 1.5。

也可见 GB/T 16855.2—2007 中的 D.3。

## G.3 避免系统性失效的措施

宜采用以下措施：

——采用合适的原料和适当的制造工艺
与应力、耐久力、弹性、摩擦、磨损、腐蚀、温度、传导率、电介质刚度等有关的材料、制造方法和处理方法的选择。

——正确的外形和尺寸



标准分享网 www.bzfxw.com 免费下载

应力、应变、温度、表明粗糙度、公称和制造工艺等的考虑。

——元件的适当选择、组合、安排、装配和安装，包括布电缆、布线和其他连接等

采用合适的标准和制造商应用说明，例如：目录单、安装手册、技术规范，并且使用好的工程实践。

——兼容性

使用具有可兼容工作特征的元件。

——经受规定环境条件的能力

SRP/CS 的设计应使其能在所有预期的环境和任何可预见的不利的环境下工作，例如：温度、湿度、振动和电磁干扰(EMI)(见 GB/T 16855.2—2007 中的 D.2)。

——使用按照合适标准且有明确定义的失效模式的元件

通过采用具有规定特征的元件来减小未检测到的故障的风险(见 GB/T 20438.7—2006 中的 B.3.3)。

另外，考虑到 SRP/CS 的复杂性及其 PL，宜采用下面的一种或多种措施：

——复查硬件的设计(例如：通过检查或遍查)

通过复查和分析技术规范和执行情况之间的差异进行查找(见 GB/T 20438.7—2006 中的 B.3.7 和 B.3.8)。

——有仿真或分析能力的计算机辅助设计

系统的执行设计程序且包括适当的自动构造单元，这些构造单元已经过试验被证明是有效的(见 GB/T 20438.7—2006 中的 B.3.5)。

——模拟

同时从功能特征和形成 SRP/CS 元件的正确尺寸两个方面对 SRP/CS 的设计进行系统和完整的检查(见 GB/T 20438.7—2006 中的 B.3.6)。

## G.4 SRP/CS 集成过程中避免系统性失效的措施

SRP/CS 集成过程中宜采用以下措施：

——功能性测试；

——方案管理；

——文档；

另外，考虑到 SRP/CS 的复杂性及其 PL，宜采用黑盒子测试法。

# 附 录 H
## （资料性附录）
## 控制系统有关安全部件组合的示例

图 H.1 是提供一种控制机器致动器功能的有关安全部件的示意图。这不是功能/工作图，且仅用于证明在这一种功能中类别和技术的组合原则。

控制器由电子控制逻辑单元和液压方向阀提供。风险由 AOPD 减小，AOPD 通过检测进入危险区并在光束被遮断时阻止流体致动器的启动来减小风险。

提供安全功能的有关安全部件包括：AOPD、电子控制逻辑单元、液压方向阀和连接方式。

这些有关安全部件提供停止功能作为安全功能。AOPD 被遮断时，输出把信号传递至电子控制逻辑单元，电子控制逻辑单元提供信号给液压方向阀来停止液压流作为 SRP/CS 的输出。在机器上，它就停止了致动器的运动。

有关安全部件的组合产生3种证明基于第 6 章的要求的不同类别和技术的组合的安全功能。采用本部分给出的原则，图 H.2 中的有关安全部件可描述如下：

——对于电敏保护装置（光栅）：2 类、PL＝c。为了减小故障发生的概率，该装置采用经验证的安全原则；

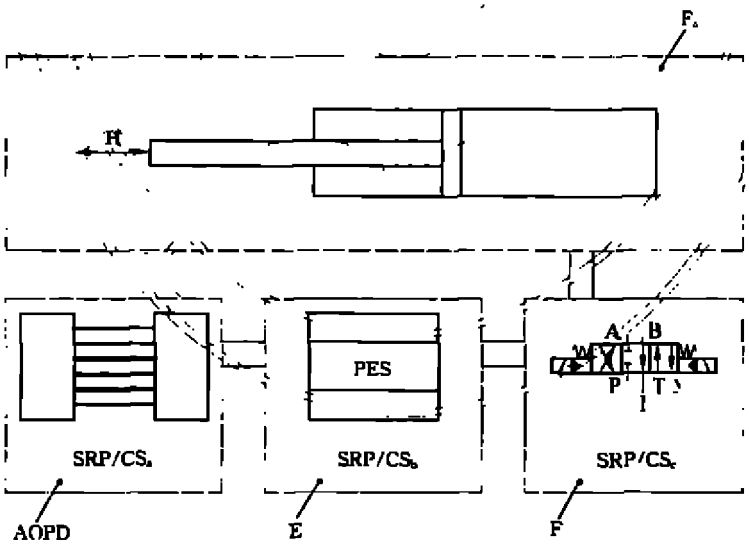
– 对于电子控制逻辑单元：3 类、PL＝d。为了提高该电子控制逻辑单元的安全性能等级，SRP/CS 的结构采用冗余结构，并采用几种能检测大多数单一故障的故障检测方法；

——对于液压方向阀：1 类、PL＝c。经验证的情形主要是指具体应用。在本例中的阀门可认为是经验证的，为了减小故障发生的概率，该装置由经验证的元件组成，采用经验证的安全原则，并考虑所有的应用条件（见 6.2.4）。

注 1：还必须考虑连接方式的位置、尺寸和设计。

当 $PL_{low}$＝c 和 $N_{low}$≠2 时的组合，其整体性能等级 PL≠c（见 6.3）。

注 2：就图 H.2 中 1 类或 2 类部件的故障而言，可能有安全功能的损失




AOPD　有源光电保护装置（例如：光栅），SRP/CS：2 类、PL＝c；

E　电子控制逻辑单元，SRP/CS：3 类、PL＝d；

F　流体，SRP/CS：1 类、PL＝c；

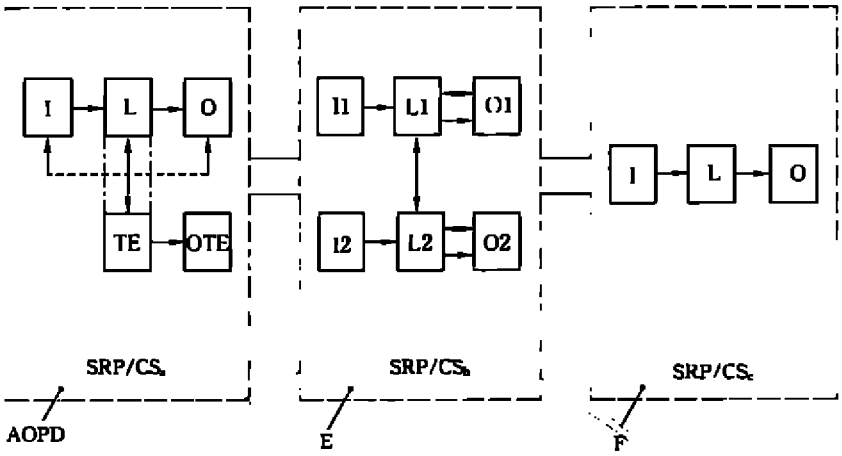
F　流体致动器；

H　危险运动。

图 H.1　示例——说明 SRP/CS 组合的模块图



标准分享网 www.bzfxw.com 免费下载




AOPD——有源光电保护装置(例如:光幕);

E——电子控制逻辑单元;

F——射流元件;

I、I1、I2——输入装置,例如:传感器;

L、L1、L2——逻辑单元;

O、O1、O2、OTE——输出装置,例如:主接触器;

TE——试验设备。

**图 H.2　被指定结构替换的图 H.1**

# 附 录 I
（资料性附录）
示 例

## I.1 概述

本附录举例说明了前面附录中给出的用以识别安全功能和确定 PL 的方法的使用。给出了两种被广泛使用的控制电路的数量表示。见图 3 中的步进过程。

示例 A 和示例 B 由两种不同的控制电路示例来检查，见图 I.1 和图 I.3。两个示例都说明了防护门联锁功能的性能。第一个示例由具有高 $MTTF_d$ 值的机电元件组成一个通道，而第二个示例则由两个通道组成——一个为机电式，另一个是可编程电子式——包括试验，但是由较低 $MTTF_d$ 的元件组成。

## I.2 安全功能和要求的性能等级（$PL_r$）

对于这两个示例，都可以选择如下的联锁防护的安全功能：

防护门打开时，危险运动将停止（通过释放电动机的能量）。

根据风险图解法（见图 A.1），确定下列风险参数：

——伤害的严重度，S=S2，严重；

——暴露于危险的频率和（或）时间，F=F1，很少和（或）暴露时间短；

——避免危险的可能性，P=P1，特定条件下可能。

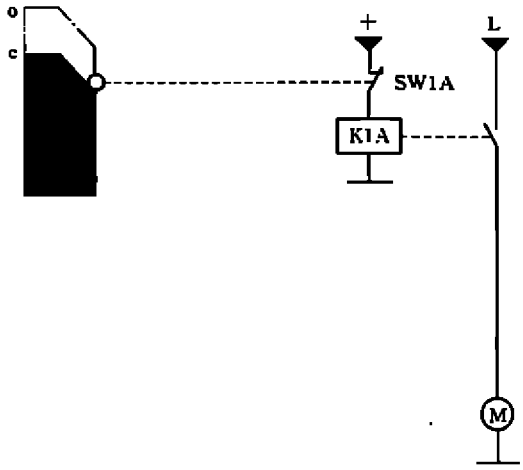
这些参数决定了要求的性能等级为 $PL_r$=c。

优先类别的确定：性能等级 c 可通过相当可靠的单通道系统（1 类）或冗余结构（2 类或 3 类）典型实现（见图 5 和第 6 章）。

## I.3 示例 A，单通道系统

### I.3.1 安全功能的识别

影响安全功能的所有部件在图 I.1 中给出。省略了不影响联锁安全功能（作为启动和停止开关）的功能性详细资料。




o——打开；

c——关闭；

M——电动机；

K1A——接触器；

SW1A——开关（NC）。

图 I.1 执行安全功能的控制电路 A



标准分享网 www.bzfxw.com 免费下载

本例中,门开关具有常闭触点(但并不证明可以不进行故障排除),且连接到一个接触器上,该接触器能关闭连接电动机的电源:

——机电元件的一个通道;

——有中等 $MTTF_d$ 的开关 SW1A;

——有低 $MTTF_d$ 的接触器 K1A。

根据 GB/T 16855.2.本例中所选的接触器是经验证的元件。

因此,有关安全部件和它们通道之间的界限可由图 I.2 中的有关安全功能模块图来表示。

K1A——接触器;

SW1A——开关。

图 I.2 识别示例 A 中有关安全功能部件的有关安全模块图

### I.3.2 $DC_{avg}$、共因失效、类别、PL 以及每个通道 $MTTF_d$ 的量化

$DC_{avg}$、共因失效以及每个通道 $MTTF_d$ 的值假定根据附录 C、附录 D、附录 E 和附录 F 来估计,或由制造商给出。类别由 6.2 来估计。

——$MTTF_d$

接触器 K1A 和开关 SW1A 对于通道的 $MTTF_d$ 有影响。由制造商给出假设的接触器和开关的 $MTTF_d$,该假设为:$MTTF_{d,K1A}=50$ 年,$MTTF_{d,SW1A}=20$ 年。根据 D.1 中的部件计数法,得出一个通道的 $MTTF_d$ 为:

$$\frac{1}{MTTF_d}=\frac{1}{MTTF_{SW1A}}+\frac{1}{MTTF_{K1A}}=\frac{1}{20\text{ 年}}+\frac{1}{50\text{ 年}}=\frac{0.07}{\text{年}} \quad \cdots\cdots\cdots\cdots(I.1)$$

由计算结果导出该通道的 $MTTF_d=14.3$ 年,或根据 4.5.2 中的表 5,该通道的 $MTTF_d$ 为"中"。

注:如果没有关于 K1A 的信息,可根据 C.2 或 C.4 做出最坏情形的假设。

——DC

由于控制电路 A 中没有完成测试,因此根据 4.5.3 中的表 6,DC = 0 或"无"。

——类别

虽然用于该电路的优先类别为 1 类,但通道的最终的 $MTTF_d$ 为"中"。这是本设计只能达到 B 类的一个理由。

图 5 中的输入数据:每个通道的 $MTTF_d$ 为"中"(14.3 年),$DC_{avg}$为"无",类别为 B 类。

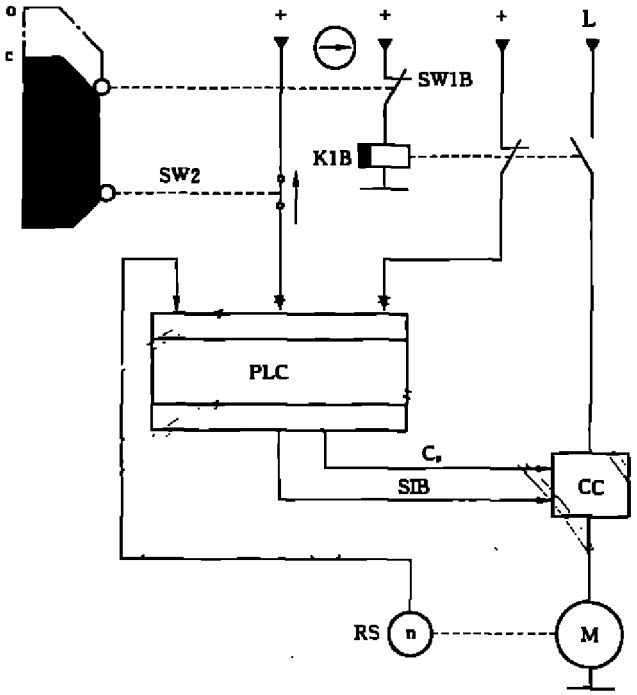
这可能由性能等级 b 来解释。

这个结果与根据 I.2 中要求的性能等级 $PL_r=c$ 不匹配。因此,为了满足 I.2 对该示例应用的风险减小的要求,该电路必须重新设计且重新估计,直到性能等级达到 $PL_r=c$ 为止。

## I.4 示例 B,冗余系统

### I.4.1 有关安全部件的识别

所有影响安全功能的部件在图 I.3 中给出。省略了不影响联锁安全功能(作为启动和停止开关或 K1B 的延时开关)的功能性详细资料。




PLC　可编程逻辑控制器；
CC　—变流器；
M　—电动机；
RS　转动传感器；
o　-打开；
c　关闭；
C,　—停止功能(标准的)；
SIB　-　安全脉冲阻断；
K1B　接触器；
SW1B　—开关(NC)；
SW2　-　开关(NO)。

图 1.3　执行安全功能的控制电路 B

在本例中，采用两个有冗余的通道。第一个通道类似于示例 A 中的通道，采用有直接打开动作的门开关，并用在强制致动模式中。这个门开关与一个接触器相连，接触器能关闭与电动机相连的动力电源。在第二个通道中，采用了附加的(可编程的)电子元件。第二个门开关与可编程逻辑控制器相连接，能够控制变流器关闭与电动机相连的动力电源：

——冗余通道，一个为机电元件通道，另一个是可编程电子元件通道；

——具有强制接触动作的触点的开关 SW1B，具有中等 $MTTF_d$ 的 SW2；

——具有中等 $MTTF_d$ 的接触器，本例中所选的接触器是未经验证的元件；

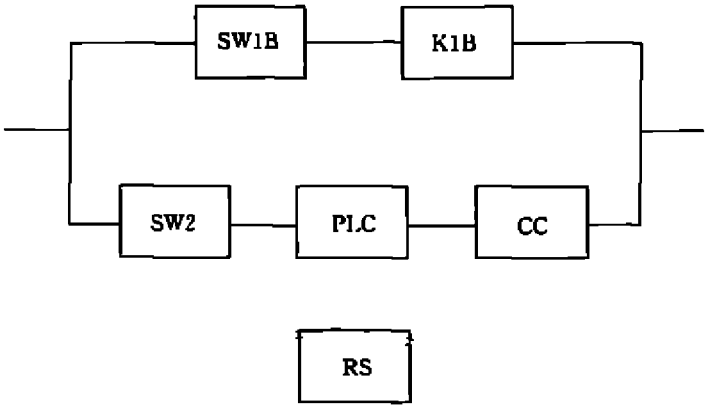
有中等 $MTTF_d$ 的电子元件。

因此，有关安全部件和它们通道之间的界限可由图 1.4 中的有关安全功能模块图来表示。

注：在冗余差异性方面，根据 4.6 中关于软件的要求，对 LC 路径的软件要求不作相应的考虑。



标准分享网 www.bzfxw.com 免费下载




SW1B 和 K1B 组成第一个通道；SW2、PLC 和 CC 组成第二个通道；RS 只用于测试变流器。

SW1B ——联锁装置；

K1B ——接触器；

SW2——开关；

PLC ——可编程逻辑控制器；

CC ——变流器；

RS ——转动传感器。

**图 L.4 识别示例 B 中有关安全部件的模块图**

### L.4.2 $DC_{avg}$、共因失效、类别、PL 以及每个通道 $MTTF_d$ 的量化

$DC_{avg}$、共因失效以及每个通道 $MTTF_d$ 的值假定根据附录 C、附录 D、附录 E 和附录 F 来估计，或由制造商给出。类别则根据 6.2 来估计。

开关 SW1B 具有直接打开动作且用于强制致动模式中。因此，对于因机械失效（例如：活塞破裂、致动凸轮磨损、调节不良等）而引起的触点无法打开和开关无法致动，应进行故障排除。

注：这些假设对依照 IEC 60957-6-1:1997 中的附录 K 的辅助电路的开关有效，且对依照制造商的技术规范的开关的适当机械固定和致动有效。

——$MTTF_d$

接触器 K1B 是只对这一个通道的 $MTTF_d$ 起作用的元件。$MTTF_{K1B}$ = 30 年的假设是由制造商给出的。根据 D.1 中的部件计数法，得出这一个通道的 $MTTF_d$ 为：

$$\frac{1}{MTTF_{dC1}} = \frac{1}{MTTF_{dK1B}} \qquad \cdots\cdots(L.2)$$

由计算结果导出该通道的 $MTTF_d$ = 30 年。

在第二个通道中，SW2、PLC 和 CC 对 $MTTF_{dC2}$ 有影响。对于这三个元件及 RS，$MTTF_d$ 为 20 年是由制造商给出的假设。D.1 中的部件计数法导出第二个通道的 $MTTF_{dC2}$ 为：

$$\frac{1}{MTTF_{dC2}} = \frac{1}{MTTF_{dSW2}} + \frac{1}{MTTF_{dPLC}} + \frac{1}{MTTF_{dCC}} = \frac{1}{20\text{ 年}} + \frac{1}{20\text{ 年}} + \frac{1}{20\text{ 年}} = \frac{0.15}{\text{年}} \cdots(L.3)$$

由计算结果导出该通道的 $MTTF_d$ = 6.7 年。

由于这两个通道具有不同的 $MTTF_d$，公式 D.2 能用来计算对称两通道系统的单个通道的 $MTTF_d$ 的代替值。此公式计算出的 $MTTF_d$ = 20 年，或根据 4.5.2 中的表 5，通道的 $MTTF_d$ 为"中"。

——DC

在控制电路 B 中，由 PLC 测试 4 个有关安全部件：SW2 和 K1B 由 PLC 读回，PLC 执行自检，CC 则由 PLC 经由 RS 读回。每个被测部件相关的 DC 为：

1) $DC_{SW2}$ = 60%，"低"，由于无动态测试监测输入信号，见表 E.1（输入装置部分的第 3 行）；

2) $DC_{K1B}$ = 99%，"高"，由于常开和常闭机械式连接触点，见表 E.1（输入装置部分的第 2 行）；

3) $DC_{PLC}$ = 30%，"无"，由于自检的低效率（假设制造商已通过 FMEA 计算出该值）；

4) $DC_{CC}$=90%,"中",由于带有由控制逻辑单元的致动器监测的冗余关闭路径,见表 E.1(输入装置部分的第 6 行)——如果 PLC 监测 CC 的失效,则可由安全脉冲阻塞(附加的停止路径)停止运动。

对于 PL 的估计,需要一个平均的 DC 值($DC_{avg}$)作为图 5 中的输入。

$$DC_{avg}=\frac{\frac{DC_{SW2}}{MTTF_{dSW2}}+\frac{DC_{K1B}}{MTTF_{dK1B}}+\frac{DC_{PLC}}{MTTF_{dPLC}}+\frac{DC_{CC}}{MTTF_{dCC}}}{\frac{1}{MTTF_{dSW2}}+\frac{1}{MTTF_{dK1B}}+\frac{1}{MTTF_{dPLC}}+\frac{1}{MTTF_{dCC}}}$$

$$=\frac{\frac{0.6}{20y}+\frac{0.99}{30y}+\frac{0.3}{20y}+\frac{0.9}{20y}}{\frac{1}{20y}+\frac{1}{30y}+\frac{1}{20y}+\frac{1}{20y}}=\frac{0.123}{0.183}=67.1\% \quad \cdots\cdots\cdots\cdots(I.4)$$

因此,根据 4.5.3 和表 6,$DC_{avg}$为"低"。

——CCF

假定已根据 F.2 对控制电路 B 进行了防止 CCF 措施的评估。得分在表 I.1 中给出。

**表 I.1 示例 B 中防止 CCF 方法的评估**

| 编 号 | 条 目 | 控制电路的得分 | 最大可能得分 |
|---|---|---|---|
| 1 | 分离/隔离 | | |
| | 信号路径之间的物理分离 | 15 | 15 |
| 2 | 多样性 | | |
| | 采用不同技术/设计或物理原则 | 20 | 20 |
| 3 | 设计/应用/经验 | | |
| 3.1 | 防止过电压、过压、过电流等 | 无 | 15 |
| 3.2 | 使用的元件是经验证的 | 5 | 5 |
| 4 | 评价/分析 | | |
| | 设计中是否考虑了失效模式及影响分析的结果以避免共因失效? | 5 | 5 |
| 5 | 资格/培训 | | |
| | 设计者是否已经过培训以理解共因失效的原因和结果? | 无 | 5 |
| 6 | 环境 | | |
| 6.1 | 根据适当的标准,预防污染和电磁兼容(EMC)以防止 CCF | 25 | 25 |
| 6.2 | 其他影响<br>是否已考虑了所有相关环境影响的抗性要求,例如:温度、冲击、振动、湿度(例如:在相关标准中规定)? | 10 | 10 |
| | 总和 | 80 | 最大 100 |

足够防止 CCF 的措施要求最小得分为 65。在示例 B 中,80 分足以满足防止 CCF 的要求。

任何部件中的单一故障不会导致安全功能的丧失。只要合理可行,应在关于安全功能的下一个指令发出时或发出前探测到单一故障。诊断覆盖率($DC_{avg}$)为 60%~92%。防止 CCF 的措施应足够。这些是 3 类的典型特征。

图 5 中的输入数据为:通道的 $MTTF_d$ 为"中"(20 年),$DC_{avg}$为"低",类别为 3 类。

这可解释为性能等级 PL=c。

该结果与 I.2 中要求的性能等级 $PL_r$=c 相匹配。因此,控制电路 B 满足 I.2 的应用示例对风险减小的要求。



标准分享网 www.bzfxw.com 免费下载

# 附 录 J
（资料性附录）
软 件

## J.1 示例描述

本附录介绍了用于实现 $PL_r=d$ 的 SRP/CS 的 SRESW 的示范活动。该 SRP/CS 与机器设备通过接口连接。它确保了：

——获得各种传感器发出的信息；

——用于操纵考虑安全要求的控制元件所要求的处理；

——致动器的控制。

本应用中，功能模块层级上的 SRESW 的设计如图 J.1 所示。

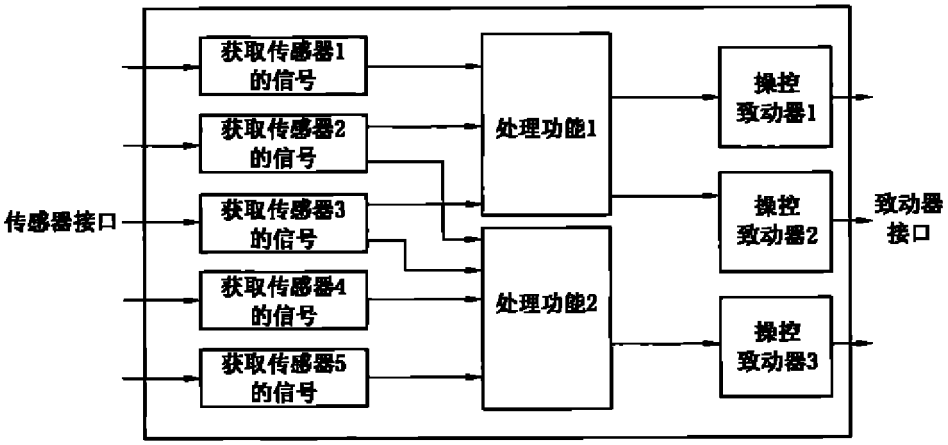



图 J.1 功能模块层级的软件设计示例

## J.2 软件安全寿命周期的 V 模型的应用

表 J.1 介绍了将软件安全寿命周期 V 模型应用于机器控制方面的活动和文件的示范性综合。

表 J.1 软件安全寿命周期内的活动和文件

| 设计活动 | 检验活动 | 相关文件的提供 |
|---|---|---|
| 机器方面：<br>包括 SRP/CS 的功能检验 | 有关安全功能的识别 | "用于机器控制的有关安全的技术规范" |
| 结构方面：<br>带传感器和致动器的控制结构的确定 | 所选元件安全特征的评注 | "控制结构的定义" |
| 软件技术规范方面：<br>软件功能中机器功能的副本 | 描述的重新读取(见 J.3) | "软件描述" |
| 软件结构方面，<br>将各种功能细分到功能模块中 | 确定关键模块，这些模块是重大的复审和确认工作的对象 | "功能模块建模" |
| 编码方面：<br>根据编程规则编码(见 J.4) | 代码的重新读取。功能和符合规则的检验 | "代码中的编码注释"<br>"重新读取表的编码" |
| 确认方面：<br>测试方案的制定：<br>功能的操作方面<br>失效特征方面 | 测试范围的检验<br>测试结果的检验 | "对应矩阵"：它交叉参照技术规范段落和测试结果<br>"测试表"：包括测试方案和对测试结果的注释 |

## J.3 软件技术规范的检验

作为软件安全寿命周期的一部分，在软件技术规范层面上的检验活动存在于对描述内容的读取中，以此来检验是否适当地描述了所有的敏感点。在检验每种功能时，宜考虑以下方面：

——限制系统技术规范错误解释的情况；

——避免技术规范中出现会导致 SPR/CS 产生预先未知行为的漏洞；

——精确地规定用于激活和撤消（去活）功能的条件；

明确的保证所有可能的情况都已处理；

——相容性测试；

——不同的参数化情况；

——失效后的反应。

## J.4 编程规则示例

对于 CCF，通常宜可能由作者、载入时间、版本和最新的存取类型来鉴别。关于编程规则，可区分以下规则。

a) 程序结构层面上的编程规则

程序设计应构建得能显示一个相容和易懂的通用骨架，允许进行不同的处理使其易于地方化。这意味着：

1) 对典型程序或功能模块使用样板；

2) 为了识别对应于“输入”、“处理”和“输出”的主要组成部分，把程序分为几段；

3) 对源程序中的每段程序进行注释，以便于修改后注释更新；

4) 调用一个功能模块时，描述该模块的作用；

5) 单独种类的数据类型宜仅采用存储地址，并唯一的标记加以标识；

6) 工作顺序不宜取决于变量，例如：程序运行期间计算出的跳跃地址，得到授权的附有条件的跳跃。

b) 关于使用变量的编程规则

——任何输出的激活或撤消（去活）宜只发生一次（集中条件）；

——程序应构建得使用于更新一个变量的方程都集中在一起；

——每个全局变量，应具有一个足够明确的记忆名称，并应在源程序中通过一个注释对其进行描述。

c) 功能模块层的编程规则

——更适宜的使用经 SRP/CS 供应商确认的功能模块，检查这些经确认的模块的假定工作条件是否符合程序的条件。

——编码模块的大小宜限制在以下指导值：

i) 参数　　最大 8 个字节、两个整形输入和一个输出；

ii) 功能代码—— 最大 10 个局部变量、最大 20 个布尔等式。

——功能模块不宜改变全局变量。

——数字值宜由与预先设置的基准程序来控制，以保证该定义域的有效性。

功能模块宜尽量检测出待处理变量之间的不一致性。

——模块的故障代码应该容易理解，以便在其他故障中辨别出一个故障。

——应通过注释来描述故障检测后的故障代码和模块状态。

——应通过注释来描述模块的复位或正常状态的恢复。



标准分享网 www.bzfxw.com 免费下载

# 附 录 K
（资料性附录）
## 图 5 的数值表示

见表 K.1。

表 K.1 图 5 的数字表示

| 每个通道的 $MTTF_d$/年 | 每小时危险失效的平均概率(1/h)以及相应的性能等级(PL) | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | B 类 PL<br>$DC_{avg}$ 无 | | 1 类 PL<br>$DC_{avg}$ 无 | | 2 类 PL<br>$DC_{avg}$ 低 | | 2 类 PL<br>$DC_{avg}$ 中 | | 3 类 PL<br>$DC_{avg}$ 低 | | 3 类 PL<br>$DC_{avg}$ 中 | | 4 类 PL<br>$DC_{avg}$ 高 | |
| 3 | $3.80\times10^{-5}$ | a | | | $2.58\times10^{-5}$ | a | $1.99\times10^{-6}$ | a | $1.26\times10^{-6}$ | a | $6.09\times10^{-7}$ | b | | |
| 3.3 | $3.16\times10^{-5}$ | a | | | $2.33\times10^{-5}$ | a | $1.79\times10^{-6}$ | a | $1.13\times10^{-6}$ | a | $5.41\times10^{-7}$ | b | | |
| 3.6 | $3.17\times10^{-5}$ | a | | | $2.13\times10^{-5}$ | a | $1.62\times10^{-6}$ | a | $1.03\times10^{-6}$ | a | $4.86\times10^{-7}$ | b | | |
| 3.9 | $2.93\times10^{-5}$ | a | | | $1.95\times10^{-5}$ | a | $1.48\times10^{-6}$ | a | $9.37\times10^{-7}$ | b | $4.40\times10^{-7}$ | b | | |
| 4.3 | $2.65\times10^{-5}$ | a | | | $1.76\times10^{-5}$ | a | $1.33\times10^{-6}$ | a | $8.39\times10^{-7}$ | b | $3.89\times10^{-7}$ | b | | |
| 4.7 | $2.43\times10^{-5}$ | a | | | $1.60\times10^{-5}$ | a | $1.20\times10^{-6}$ | a | $7.58\times10^{-7}$ | b | $3.48\times10^{-7}$ | b | | |
| 5.1 | $2.24\times10^{-5}$ | a | | | $1.47\times10^{-5}$ | a | $1.10\times10^{-6}$ | a | $6.91\times10^{-7}$ | b | $3.15\times10^{-7}$ | b | | |
| 5.6 | $2.04\times10^{-5}$ | a | | | $1.33\times10^{-5}$ | a | $9.87\times10^{-7}$ | b | $6.21\times10^{-7}$ | b | $2.80\times10^{-7}$ | c | | |
| 6.2 | $1.84\times10^{-5}$ | a | | | $1.19\times10^{-5}$ | a | $8.80\times10^{-7}$ | b | $5.53\times10^{-7}$ | b | $2.47\times10^{-7}$ | c | | |
| 6.8 | $1.68\times10^{-5}$ | a | | | $1.08\times10^{-5}$ | a | $7.93\times10^{-7}$ | b | $4.98\times10^{-7}$ | b | $2.20\times10^{-7}$ | c | | |
| 7.5 | $1.52\times10^{-5}$ | a | | | $9.75\times10^{-6}$ | b | $7.10\times10^{-7}$ | b | $4.45\times10^{-7}$ | b | $1.95\times10^{-7}$ | c | | |
| 8.2 | $1.39\times10^{-5}$ | a | | | $8.87\times10^{-6}$ | b | $6.43\times10^{-7}$ | b | $4.02\times10^{-7}$ | b | $1.74\times10^{-7}$ | c | | |
| 9.1 | $1.25\times10^{-5}$ | a | | | $7.94\times10^{-6}$ | b | $5.71\times10^{-7}$ | b | $3.57\times10^{-7}$ | b | $1.53\times10^{-7}$ | c | | |
| 10 | $1.14\times10^{-5}$ | a | | | $7.18\times10^{-6}$ | b | $5.14\times10^{-7}$ | b | $3.21\times10^{-7}$ | b | $1.36\times10^{-7}$ | c | | |
| 11 | $1.04\times10^{-5}$ | a | | | $6.44\times10^{-6}$ | b | $4.53\times10^{-7}$ | b | $2.81\times10^{-7}$ | c | $1.18\times10^{-7}$ | c | | |
| 12 | $9.51\times10^{-6}$ | b | | | $5.84\times10^{-6}$ | b | $4.04\times10^{-7}$ | b | $2.49\times10^{-7}$ | c | $1.04\times10^{-7}$ | c | | |
| 13 | $8.78\times10^{-6}$ | b | | | $5.33\times10^{-6}$ | b | $3.64\times10^{-7}$ | b | $2.23\times10^{-7}$ | c | $9.21\times10^{-8}$ | d | | |
| 15 | $7.61\times10^{-6}$ | b | | | $4.53\times10^{-6}$ | b | $3.01\times10^{-7}$ | b | $1.82\times10^{-7}$ | c | $7.44\times10^{-8}$ | d | | |
| 16 | $7.13\times10^{-6}$ | b | | | $4.21\times10^{-6}$ | b | $2.77\times10^{-7}$ | c | $1.67\times10^{-7}$ | c | $6.76\times10^{-8}$ | d | | |

表 K 1（续）

| 每个通道的 $MTTF_d$/年 | 每小时危险失效的平均概率(1/h)以及相应的性能等级(PL) | | | | | | |
|---|---|---|---|---|---|---|---|
| | B类 PL<br>$DC_{avg}$=无 | 1类 PL<br>$DC_{avg}$=无 | 2类 PL<br>$DC_{avg}$=低 | 2类 PL<br>$DC_{avg}$=中 | 3类 PL<br>$DC_{avg}$=低 | 3类 PL<br>$DC_{avg}$=中 | 4类 PL<br>$DC_{avg}$=高 |
| 18 | $6.34\times10^{-6}$ b | | $3.68\times10^{-6}$ b | $2.37\times10^{-6}$ c | $1.41\times10^{-6}$ c | $5.67\times10^{-7}$ d | |
| 20 | $5.71\times10^{-6}$ b | | $3.26\times10^{-6}$ b | $2.06\times10^{-6}$ c | $1.22\times10^{-6}$ c | $4.85\times10^{-7}$ d | |
| 22 | $5.19\times10^{-6}$ b | | $2.93\times10^{-6}$ c | $1.82\times10^{-6}$ c | $1.07\times10^{-6}$ c | $4.21\times10^{-7}$ d | |
| 24 | $4.76\times10^{-6}$ b | | $2.65\times10^{-6}$ c | $1.62\times10^{-6}$ c | $9.47\times10^{-7}$ d | $3.70\times10^{-7}$ d | |
| 27 | $4.23\times10^{-6}$ b | | $2.32\times10^{-6}$ c | $1.39\times10^{-6}$ c | $8.04\times10^{-7}$ d | $3.10\times10^{-7}$ d | |
| 30 | | $3.80\times10^{-6}$ b | $2.06\times10^{-6}$ c | $1.21\times10^{-6}$ c | $6.94\times10^{-7}$ d | $2.65\times10^{-7}$ d | $9.54\times10^{-8}$ e |
| 33 | | $3.46\times10^{-6}$ b | $1.85\times10^{-6}$ c | $1.06\times10^{-6}$ c | $5.94\times10^{-7}$ d | $2.30\times10^{-7}$ d | $8.57\times10^{-8}$ e |
| 36 | | $3.17\times10^{-6}$ b | $1.67\times10^{-6}$ c | $9.39\times10^{-7}$ d | $5.16\times10^{-7}$ d | $2.01\times10^{-7}$ d | $7.77\times10^{-8}$ e |
| 39 | | $2.93\times10^{-6}$ c | $1.53\times10^{-6}$ c | $8.40\times10^{-7}$ d | $4.53\times10^{-7}$ d | $1.78\times10^{-7}$ d | $7.11\times10^{-8}$ e |
| 43 | | $2.65\times10^{-6}$ c | $1.37\times10^{-6}$ c | $7.34\times10^{-7}$ d | $3.87\times10^{-7}$ d | $1.54\times10^{-7}$ d | $6.37\times10^{-8}$ e |
| 47 | | $2.43\times10^{-6}$ c | $1.24\times10^{-6}$ c | $6.49\times10^{-7}$ d | $3.35\times10^{-7}$ d | $1.34\times10^{-7}$ d | $5.76\times10^{-8}$ e |
| 51 | | $2.24\times10^{-6}$ c | $1.13\times10^{-6}$ c | $5.80\times10^{-7}$ d | $2.93\times10^{-7}$ d | $1.19\times10^{-7}$ d | $5.26\times10^{-8}$ e |
| 56 | | $2.04\times10^{-6}$ c | $1.02\times10^{-6}$ c | $5.10\times10^{-7}$ d | $2.52\times10^{-7}$ d | $1.03\times10^{-7}$ d | $4.73\times10^{-8}$ e |
| 62 | | $1.84\times10^{-6}$ c | $9.06\times10^{-7}$ d | $4.43\times10^{-7}$ d | $2.13\times10^{-7}$ d | $8.84\times10^{-8}$ e | $4.22\times10^{-8}$ e |
| 68 | | $1.68\times10^{-6}$ c | $8.17\times10^{-7}$ d | $3.90\times10^{-7}$ d | $1.84\times10^{-7}$ d | $7.68\times10^{-8}$ e | $3.80\times10^{-8}$ e |
| 75 | | $1.52\times10^{-6}$ c | $7.31\times10^{-7}$ d | $3.40\times10^{-7}$ d | $1.57\times10^{-7}$ d | $6.62\times10^{-8}$ e | $3.41\times10^{-8}$ e |
| 82 | | $1.39\times10^{-6}$ c | $6.61\times10^{-7}$ d | $3.01\times10^{-7}$ d | $1.35\times10^{-7}$ d | $5.79\times10^{-8}$ e | $3.08\times10^{-8}$ e |
| 91 | | $1.25\times10^{-6}$ c | $5.88\times10^{-7}$ d | $2.61\times10^{-7}$ d | $1.14\times10^{-7}$ d | $4.94\times10^{-8}$ e | $2.74\times10^{-8}$ e |
| 100 | | $1.14\times10^{-6}$ c | $5.28\times10^{-7}$ d | $2.29\times10^{-7}$ d | $1.01\times10^{-7}$ d | $4.29\times10^{-8}$ e | $2.47\times10^{-8}$ e |



标准分享网 www.bzfxw.com 免费下载

# 参 考 文 献

关于可编程电子系统的出版物

[1] GB/T 17626.4 电磁兼容 试验和测量技术 电快速瞬变脉冲群抗扰度试验.

[2] GB/T 19436.1 机械安全 电敏防护装置 第1部分:一般要求和试验.

[3] GB/T 19436.2 机械电气安全 电敏防护装置 第2部分:使用有源光电防护器件(AOPDs)设备的特殊要求.

[4] GB 19436.3 机械电气安全 电敏防护装置 第3部分:使用有源光电漫反射防护器件(AOPDDR)设备的特殊要求.

[5] 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.

[6] 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.

[7] GB/T 20438.5—2006 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.

[8] 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.

[9] 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.

[10] IEC 61511-1:2003 功能安全——过程工业部门用安全仪表系统 第1部分:结构、定义、系统、硬件和软件的要求.

[11] IEC 62061 机械安全 有关安全的电子、电气和可编程电子系统的功能安全.

[12] HSE指南,有关安全应用中的可编程电子系统,第1部分(ISBN 0 11 883906 0)和第2部分(ISBN 0 11 883906 3).

[13] CECR-184 微处理控制系统中的个人安全(电子,丹麦).

更多出版物

[14] GB/T 1251.1 人类工效学 工作场所的险情信号 险情听觉信号.

[15] GB/T 1251.2 人类工效学 险情视觉信号 一般要求、设计和检验.

[16] GB/T 1251.3 人类工效学 险情和非险情声光信号体系.

[17] GB/T 3766 液压系统通用技术条件.

[18] GB/T 4205 人机界面(MMI)操作规则.

[19] GB 4208 外壳防护等级(IP代码).

[20] GB 5226.1—2002 机械安全 机械电气设备 第1部分:通用技术条件.

[21] GB/T 7826 系统可靠性分析技术 失效模式和效应分析(FMEA)程序.

[22] GB/T 7932 气动系统通用技术条件.

[23] GB 12668.3 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.

[24] GB/T 15969.1~15969.8 可编程序控制器.

[25] GB 16754 机械安全 急停 设计原则.

[26] GB/T 17454.1 机械安全 压敏保护装置 第1部分:压敏垫和压敏地板的设计和试验通则.

[27] GB/T 17454.2 机械安全 压敏保护装置 第2部分:压敏边和压敏棒的设计和试验通则.

[28] GB/T 17799.2 电磁兼容 通用标准 工业环境中的抗扰度试验.

[29] GB 18209.1 机械安全 指示、标志和操作 第1部分:关于视觉、听觉和触觉信号的要求.

[30] GB 18209.2 机械安全 指示、标志和操作 第2部分:标志要求.

[31] GB 18209.3 机械安全 指示、标志和操作 第3部分:操作件的位置和操作的要求.

[32] GB T 19001 质量管理体系 要求.

[33] GB/T 19670 机械安全 防止意外启动.

[34] GB/T 19671 机械安全 双手操纵装置 功能状况和设计原则.

[35] GB/T 19876—2005 机械安全 与人体部位接近速度相关防护设施的定位.

[36] ISO 9355-1 显示器和控制致动器设计的人类工效学要求 第1部分:与显示器和控制致动器的人机交互.

[37] ISO 9355-2 显示器和控制致动器设计的人类工效学要求 第2部分:显示器.

[38] ISO 9355-3 显示器和控制致动器设计的人类工效学要求 第3部分:控制致动器.

[39] ISO 19973(所有部分) 气动流体动力 元件可靠性测试的评价.

[40] IEC 60204-1:2005 机械安全 机器电气设备 第1部分:通用技术条件.

[41] IEC 60947(所有部分) 低压开关设备和控制设备.

[42] IEC 61810(所有部分) 基本电磁继电器.

[43] IEC 61300(所有部分) 纤维光学互连器件和无源器件 基本试验和测量程序.

[44] EN 457 机械安全 听觉危险信号 通用要求、设计和测试.

[45] EN 614-1 机械安全 人类工效学设计原则 第1部分:术语和通则.

[46] EN 982,机械安全 流体动力系统及其元件的安全要求 液压.

[47] EN 983,机械安全 流体动力系统及其元件的安全要求 气动.

[48] EN 1005-3 机械安全 人类物理性能 第3部分:用于机械操作的推荐的力的限制.

[49] EN 1088,机械安全 带防护装置的联锁装置 设计和选择原则.

[50] EN 50205,带强制导向(机械式连接)触点的继电器.

[51] SN 29500(所有部分) 元件的失效率.

[52] GOBLE.W.M.控制系统 评估和可靠性.第二版.美国设备协会(ISA),北卡罗莱州,1998.

数据库

[53] SN 29500(所有部分) 元件的失效率.1999-11版.Siemens AG 1999,www.pruefinstitut.de.

[54] 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,同样的为RDF'可靠性数据手册,UTE C 80-810,Union Technique de l'Electricité et de la Communication (www.ute-fr.com).

[55] *Reliability Prediction of Electronic Equipment*, MIL-HDBK 217E. Department of Defense, Washington DC, 1982.

[56] *Reliability Prediction Procedure for Electronic Equipment*, Telcordia SR-332. Issue 01.



标准分享网 www.bzfxw.com 免费下载

CEPIC



May 2001 (telecom-info. telcordia. com), Bellcore TR-332, Issue 06.

[57] *EPRD, Electronic Parts Reliability Data* (RAC-STD-6100), Reliability Analysis Centre, 201 Mill Street, Rome, NY 13440 (rac. alionscience. com).

[58] NPRD-95, *Non-electronic Parts Reliability Data* (RAC-STD-6200), Reliability Analysis Centre. 201 Mill Street. Rome, NY 13440 (rac. alionscience. com).

[59] *British Handbook for Reliability Data for Components used in Telecommunication Systems*, British Telecom (HRD5. last issue).

[60] 中国军用标准 GJB/Z 299B.