ICS 13.110
J 09

中华人民共和国国家标准

GB/T 16855.1—2018/ISO 13849-1:2015
代替 GB/T 16855.1—2008

机械安全　控制系统安全相关部件
第 1 部分:设计通则

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

(ISO 13849-1:2015,IDT)

2018-12-28 发布　　2019-07-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 16855《机械安全　控制系统安全相关部件》由以下两部分组成：

——第1部分：设计通则；

——第2部分：确认。

本部分为GB/T 16855的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GB/T 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》。与GB/T 16855.1—2008相比，除编辑性修改外主要技术变化如下：

——将标准名称修改为《机械安全　控制系统安全相关部件　第1部分：设计通则》；

——删除了引言中的表1(见2008年版的引言)；

——将术语“系统失效”修改为“系统性失效”(见3.1.7，2008年版的3.1.7)；

——将术语“平均危险失效时间”修改为“平均危险失效间隔时间”，并将其缩略语修改为“$MTTF_D$”(见3.1.25，2008年版的3.1.25)；

——增加了术语“高要求或连续模式”“经使用证明”及其定义(见3.1.38和3.1.39)；

——修改了图1(见图1，2008年版的图1)；

——增加了SRP/CS输出部分按类别描述的要求(见4.5.5)；

——修改了对单个元件$MTTF_D$值的计算或估计(见附录C，2008年版的附录C)；

——重新起草了附录I(见附录I，2008年版的附录I)。

本部分使用翻译法等同采用ISO 13849-1:2015《机械安全　控制系统安全相关部件　第1部分：设计通则》。

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 28526—2012　机械电气安全　安全相关电气、电子和可编程电子控制系统的功能安全(IEC 62061:2005，IDT)；

——GB/T 30175—2013　机械安全　应用GB/T 16855.1和GB 28526设计安全相关控制系统的指南(ISO/TR 23849:2010，IDT)。

本部分做了以下编辑性修改：

——修改了表1中的编辑性错误，“表3”改为“表2”，“表4”改为“表3”，“表7”改为“表6”。

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：皮尔磁电子(常州)有限公司、中机生产力促进中心、安徽乐库智能停车设备有限公司、苏州安高智能安全科技有限公司、厦门日拓电器科技有限公司、南安市中机标准化研究院有限公司、福建省闽旋科技股份有限公司、软控股份有限公司、中国软件评测中心、安士能(上海)机电商贸有限公司、华测检测认证集团股份有限公司、南京理工大学、西安旭迈智能家电科技有限公司、南京林业大学/机电产品包装生物质材料国家与地方联合工程研究中心、南安市质量计量检测所、立宏安全设备工程(上海)有限公司、浙江雷鸟供应链管理有限公司。

本部分主要起草人：张晓飞、黄之炯、李勤、朱斌、孙振超、李立言、赵阳阳、王宝珍、于明进、刘发旺、陆晓光、郭永振、刘攀超、居里锴、程红兵、白洪海、居荣华、吉坤、侯红英、黄东升、尹之尧、付卉青、刘英、陈卓贤、李忠、刘治永、宋小宁、李亚莉、周爱萍。

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、GB/T 16855.1—2008。

引　言

机械领域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装置：

——B1 类，特定的安全特征(如安全距离、表面温度、噪声)标准；

——B2 类，安全装置(如双手操纵装置、联锁装置、压敏装置、防护装置)标准。

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

依照 GB/T 15706 中的规定，本部分属于 B 类标准。

本部分尤其与下列与机械安全有关的利益相关方有关：

——机器制造商；

——健康与安全机构。

其他受到机械安全水平影响的利益相关方有：

——机器使用人员；

——机器所有者；

——服务提供人员；

——消费者(针对预定由消费者使用的机械)。

上述利益相关方均有可能参与本部分的起草。

此外，本部分预定用于起草 C 类标准的标准化机构。

本部分规定的要求可由 C 类标准补充或修改。

对于在 C 类标准的范围内，且已按照 C 类标准设计和制造的机器，优先采用 C 类标准中的要求。

本部分的目的是在控制系统的设计和评估中给出对所涉及的控制系统的指南，并为制修订 B 类或 C 类标准提供指南。作为机器全面风险减小策略的一部分，设计者一般愿意通过采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安全相关部件(SRP/CS)，它们由硬件和软件组成，既可独立于机器控制系统，也可以是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)。

控制系统安全相关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 2)。

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、故障检测机制的范围[诊断覆盖率(DC)]、部件的可靠性[平均危险失效间隔时间($MTTF_D$)、共因失效(CCF)]、设计流程、运行负荷、环境条件和操作程序等。

为了便于设计者对所达到的 PL 进行评估，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：类别 B、类别 1、类别 2、类别 3、类别 4。

性能等级和类别适用于如下控制系统安全相关部件，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、监控等的逻辑单元)；

——动力控制元件(例如：继电器、阀等)；

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。

关于 IEC 62061 和本部分推荐应用的信息

IEC 62061 和本部分都规定了机器控制系统安全相关部件的设计和实施要求。按照这两项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。ISO/TR 23849 为机器安全相关控制系统设计中应用 IEC 62061 和本部分标准提供了指导。

机械安全　控制系统安全相关部件
第1部分:设计通则

1　范围

GB/T 16855的本部分规定了包括软件设计在内的控制系统安全相关部件(SRP/CS)设计和集成的安全要求和指导原则。本部分规定了这些SRP/CS部件的特征,包括执行安全功能所需要的性能等级。本部分适用于所有种类机械上具有高要求和连续模式的SRP/CS,不管其采用何种技术和能量(电气、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。

本部分给出了采用可编程电子系统的SRP/CS的具体要求。

本部分未给出SRP/CS的产品的具体设计要求,但可采用给出的类别或性能等级等原则。

注1:SRP/CS的产品示例:继电器、电磁阀、位置开关、PLC、电机控制单元、双手操纵装置、压敏设备等。这类产品的设计需参考专门的标准,例如:GB/T 19671、GB/T 17454.1和GB/T 17454.2。

注2:所需性能等级的定义见3.1.24。

注3:本部分给出的关于可编程电子系统的要求与IEC 62061中给出的机械安全相关的电气、电子和可编程控制系统的设计和开发方法是一致的。

注4:用于PL_r=e的元件的安全相关嵌入式软件见IEC 61508-3:1998中第7章。

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

GB/T 15706—2012　机械安全　设计通则　风险评估与风险减小(ISO 12100:2010,IDT)

GB/T 16855.2—2015　机械安全　控制系统安全相关部件　第2部分:确认(ISO 13849-2:2012,IDT)

GB/T 20438.3—2017　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 61508-3:2010,IDT)

GB/T 20438.4—2017　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 61508-4:2010,IDT)

ISO/TR 22100-2:2013　Safety of machinery—Relationship with ISO 12100—Part 2:How ISO 12100 relates to ISO 13849-1

ISO/TR 23849　应用ISO 13849-1和IEC 62061设计机械的安全相关控制系统的指南(Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery)

IEC 62061:2012　机械安全　安全相关电气、电子和可编程电子控制系统的功能安全(Safety of machinery—Functional safety of safety-related electrical,electronic and programmable electronic control systems)

3 术语和定义、符号及缩略语

3.1 术语和定义

GB/T 15706 和 GB/T 2900.13 界定的以及下列术语和定义适用于本文件。

3.1.1

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

控制系统中响应安全相关输入信号并产生安全相关输出信号的部件。

注 1：控制系统安全相关部件的组成，以安全相关的输入信号被触发为起始点（例如：致动凸轮和位置开关的滚轮等），以动力控制组件的输出（例如：接触器的主触点等）为终止点。

注 2：如果监控系统用于诊断，也可认为是 SRP/CS。

3.1.2

类别 category

控制系统安全相关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

产品不能完成要求的功能的状态。预防性维修或其他计划的行动或因缺乏外部资源的情况除外。

注 1：故障通常是产品自身失效后引起的，但即使失效未发生，故障也可能存在。

注 2：本部分中，“故障”是指随机故障。

[GB/T 2900.13—2008，191-05-01]

3.1.4

失效 failure

产品完成要求的功能的能力的中断。

注 1：失效后，产品处于故障状态。

注 2：“失效(failure)”与“故障(fault)”的区别在于——失效是一次事件，故障是一种状态。

注 3：这里定义的“失效”，不适用于仅由软件构成的产品。

注 4：本部分不包括只影响控制器进程的失效。

[GB/T 2900.13—2008，定义 191-04-01]

3.1.5

危险失效 dangerous failure

使控制系统安全相关部件(SRP/CS)有可能处于危险状态或功能丧失状态的失效。

注 1：这种可能性是否成为事实取决于系统的通道架构；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：改写 GB/T 20438.4—2017，定义 3.6.7。

3.1.6

共因失效 common cause failure;CCF

由单一事件引发的不同产品的失效，这些失效不互为因果。

注：共因失效不宜与共模失效（见 GB/T 15706—2012，定义 3.36）相混淆。

[GB/T 2900.13—2008，定义 191-04-23]

3.1.7

系统性失效 systematic failure

与某个原因必然有关的，只有通过修改设计或制造工艺、操作程序、文档或其他关联因素才能消除的失效。

注 1：仅作修复性维修而无修改措施通常不能消除这种失效原因。

注 2：这种失效可以通过模拟失效原因诱发。

注 3：以下情况中系统性失效的原因包括人为错误：

——安全要求规范；

——硬件的设计、制造、安装和操作；

——软件的设计和实施等。

[GB/T 2900.13—2008，定义 191-04-19]

3.1.8

抑制 muting

由 SRP/CS 实现的安全功能临时性自动暂停。

3.1.9

手动复位 manual reset

重新启动机器前，控制系统安全相关部件(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—2012，定义 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)。

注 3：改写 GB/T 15706—2012，定义 3.6。

3.1.12

危险状况 hazardous situation

人员暴露于具有至少一种危险的环境。

注：这类暴露可能立即或在一定时间之后对人员产生伤害。

[GB/T 15706—2012，定义 3.10]

3.1.13

风险 risk

伤害发生概率和伤害发生的严重程度的组合。

[GB/T 15706—2012，定义 3.12]

3.1.14

剩余风险 residual risk

采取保护措施之后仍然存在的风险。

注 1：见图 2。

注 2：改写 GB/T 15706—2012，定义 3.13。

3.1.15

风险评估 risk assessment

包括风险分析和风险评价在内的全过程。

[GB/T 15706—2012,定义 3.17]

3.1.16

风险分析　risk analysis

机器限制的确定,危险识别和风险估计的组合。

[GB/T 15706—2012,定义 3.15]

3.1.17

风险评价　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—2012,定义 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—2012,定义 3.23]

3.1.19

可合理预见的误用　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—2012,定义 3.24]

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—2012,定义 3.30]

3.1.21

监控　monitoring

组件或元件执行其功能的能力下降或过程条件的改变而削弱风险减小能力时,确保保护措施被触发的安全功能。

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,包括系统中所有的组件,如电源、传感器和其他输入装置,以及接触器及其他输出装置等。

注:改写 IEC 61508-4:1998,定义 3.3.2。

3.1.23

性能等级　performance level

PL

用于规定控制系统安全相关部件在预期条件下执行安全功能的离散等级。

注:见 4.5.1。

3.1.24

所需性能等级　required performance level

PL_r

每种安全功能为达到所需的风险减小所采用的性能等级(PL)。

注:见图 2 和 A.1。

3.1.25

平均危险失效间隔时间　mean time to dangerous failure

$MTTF_D$

平均危险失效间隔时间期望。

注:改写 GB 28526—2012,定义 3.2.34。

3.1.26

诊断覆盖率　diagnostic coverage

DC

诊断有效性的度量，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安全相关系统中或其部件中。例如：诊断覆盖率可存在于传感器、逻辑系统和/或执行组件中。

注 2：改写 IEC 61508-4:1998，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；个体防护装备的使用；培训。

注：改写 GB/T 15706—2012，定义 3.19。

3.1.28

任务时间　mission time

T_M

SRP/CS 预定使用的时段。

3.1.29

测试率　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

要求率　demand rate

r_D

要求 SRP/CS 进行安全相关动作的频率。

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 安全相关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。

[IEC 61508-4:1998，定义 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：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 2：采用 LVL 的典型系统示例：PLC。

注 3：改写 GB/T 21109.1—2007，定义 3.2.81.1.2。

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：使用 FVL 的典型系统示例：嵌入式系统。

注 2：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。

注 3：改写 GB/T 21109.1—2007，定义 3.2.81.1.3。

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，以满足控制系统安全相关部件(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：嵌入式软件通常用 FVL 编写。

3.1.38

高要求或连续模式　high demand or continuous mode

一种操作模式，在该模式下，需要 SRP/CS 的频率大于每年一次，或者作为正常操作的一部分，安全相关控制功能使机器保持在安全状态。

注：改写 IEC 62061:2012，定义 3.2.27。

3.1.39

经使用证明　proven in use

以针对一个组件的特定配置既往运行的分析为基础，证明危险系统性失效的可能性足够低，以致每个使用该元件的安全功能都能达到所需性能等级(PL_r)。

注：改写 GB/T 20438.4—2017，定义 3.8.18。

3.2　符号及缩略语

见表 1。

表 1　符号及缩略语

符号及缩略语	描述	定义或出处
a、b、c、d、e	性能等级的指标	表 2
AOPD	有源光电保护装置(如光幕)	附录 H
B、1、2、3、4	类别的指标	表 6
B_{10D}	直到有 10%元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

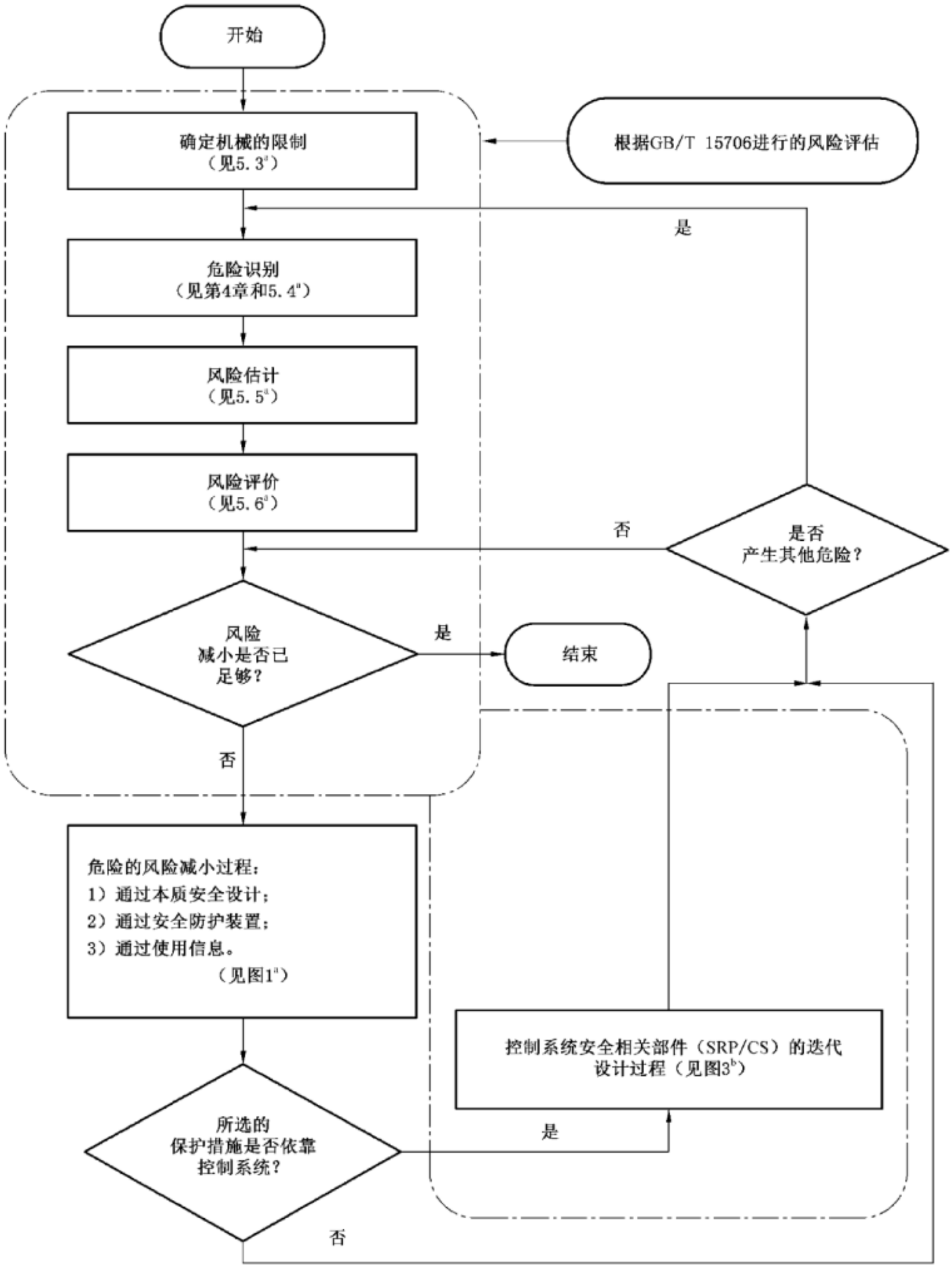
表 1（续）

符号及缩略语	描述	定义或出处
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/功能块	4.6.3
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_{bc}	相互连接方式	图 4
K1A、K1B	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	平均失效间隔时间	附录 C
$MTTF_D$	平均危险失效间隔时间	3.1.25
n、N、$\widetilde{N}$	项目编号	6.3、D.1
N_{low}	在 SRP/CS 组合中，性能等级为 PL_{low} 的 SRP/CS 的数量	6.3
n_{op}	年平均操作次数	附录 C
O、O1、O2、OTE	输出装置，如：执行器	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
PFH_D	每小时平均危险失效概率	表 2、表 K.1
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	所需性能等级	3.1.24
r_D	要求率	3.1.30
r_t	测试率	3.1.29
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 3
SRASW	安全相关应用软件	4.6.3
SRESW	安全相关嵌入式软件	4.6.2
SRP	安全相关部件	一般要求
SRP/CS	控制系统安全相关部件	3.1.1
TE	测试设备	6.2
T_M	任务时间	3.1.28
T_{10D}	直到有 10%元件危险失效时的平均时间	附录 C

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 中的原则(见图 1 和图 3)。还应考虑所有预定使用和可合理预见的误用。



[a] 参见 GB/T 15706—2012。

[b] 参见本部分。

图 1 风险评估/风险减小概况

4.2 风险减小策略

4.2.1 概述

GB/T 15706—2012 中 6.1 给出了关于机器风险减小的策略。GB/T 15706—2012 中 6.2(本质安全设计措施)及 6.3(安全防护和附加保护措施)给出了更进一步的指导。风险减小策略涵盖了机器的全生命周期。

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—2012 中 6.2);

——通过防护装置和可能的附加保护措施减小风险(见 GB/T 15706—2012 中 6.3);

——通过使用信息中关于剩余风险的规定减小风险(见 GB/T 15706—2012 中 6.4)。

4.2.2 控制系统对风险减小的作用

遵循机器总体设计程序的目的是达到安全目标(见 4.1)。设计可提供所需风险减小的 SRP/CS 是机器总体设计过程的子过程。

SRP/CS 以能达到所需的风险减小的 PL 来提供安全功能。就提供安全功能来说,无论作为本质安全设计的一部分,还是作为联锁防护装置或保护装置的控制器,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。

注:控制系统的非安全相关部件或机器的纯功能性元件无需采用此风险减小策略(见 GB/T 35081—2018 中第 3 章)。

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

本部分中的性能等级定义为每小时危险失效的概率。性能等级分为 5 级,从最低 PL=a 到最高 PL=e,各自对应一个明确的每小时危险失效概率范围(见表 2)。

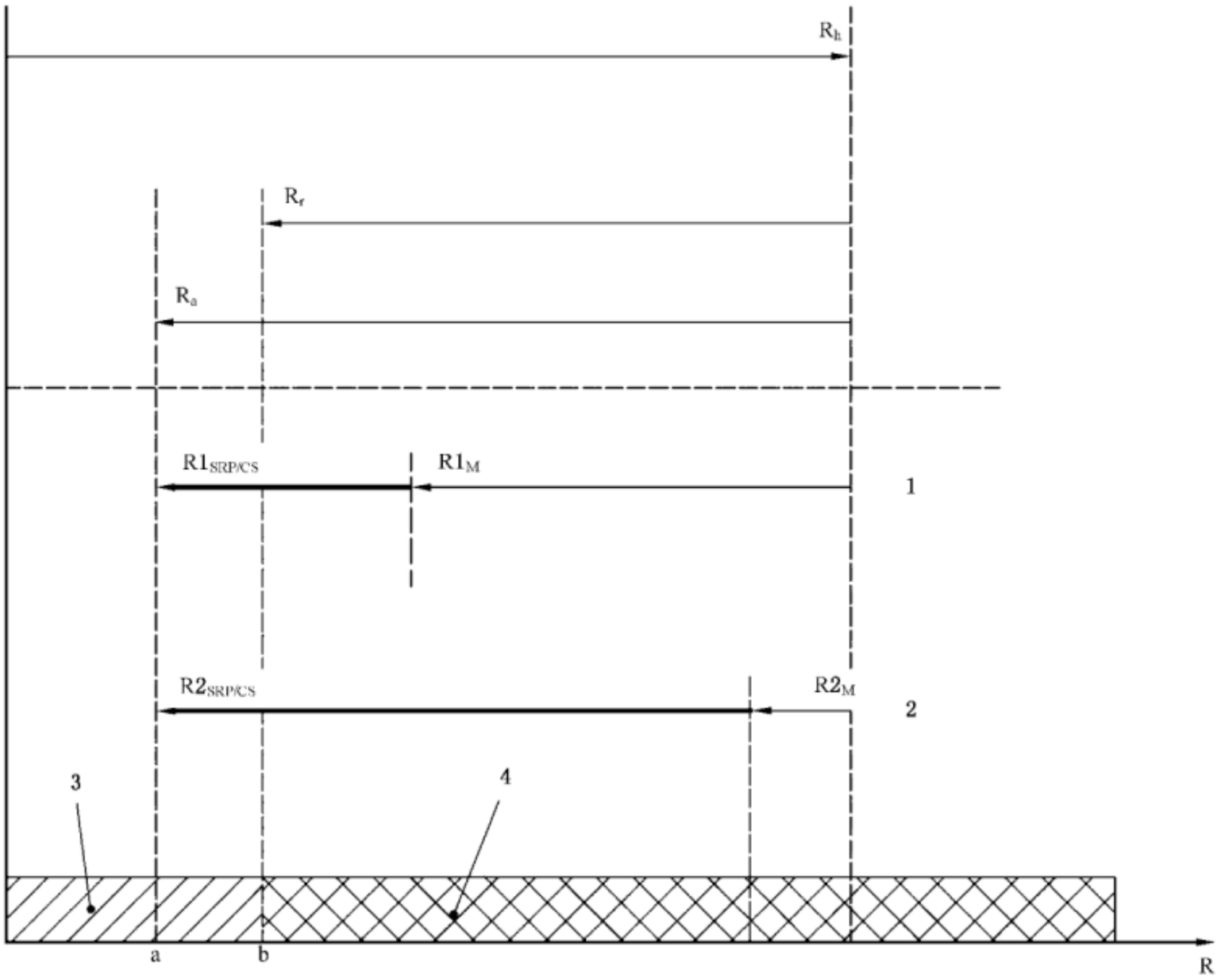
为了实现一个 PL,除了定量因素外,也需满足 PL 在定性方面的相关要求(见 4.5)。

表 2 性能等级(PL)

PL	平均每小时危险失效概率(PFH_D) 1/h
a	$\geqslant 10^{-5} \sim < 10^{-4}$
b	$\geqslant 3\times 10^{-6} \sim < 10^{-5}$
c	$\geqslant 10^{-6} \sim < 3\times 10^{-6}$
d	$\geqslant 10^{-7} \sim < 10^{-6}$
e	$\geqslant 10^{-8} \sim < 10^{-7}$

从对机器进行风险评估(见 GB/T 15706)开始,设计者应确定需要由 SRP/CS 执行的每一种相关的安全功能对风险减小的作用。这种对风险减小的作用并不涵盖受控机器的全部风险,例如:并不考虑机械压力机或清洗机的全部风险,而是考虑采用特定的安全功能减小的那一部分风险。此类功能的示例,如压力机上的电敏保护装置或清洗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)。



说明：

R_h ——对于特定危险状况，采用保护措施前的风险；

R_r ——需要保护措施减小的风险；

R_a ——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（如机械措施）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（如光幕）实现，小部分由保护措施（如机械措施）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 后的剩余风险；

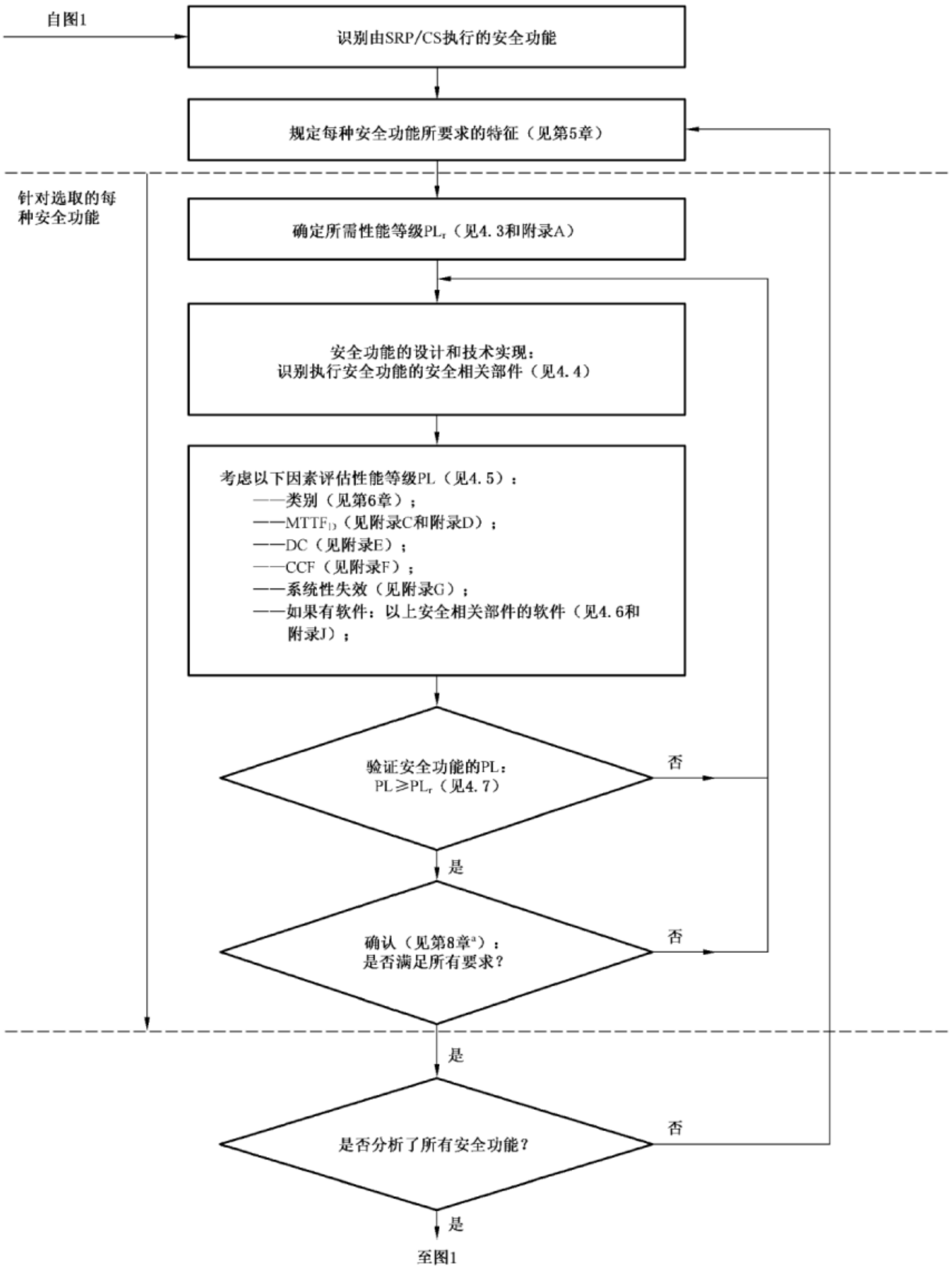
b ——充分减小的风险；

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

$R1_M$、$R2_M$ ——SRP/CS 之外的保护措施实现的风险减小（如机械措施）。

注：关于风险减小的更多信息见 GB/T 15706。

图 2　每种危险状况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　控制系统安全相关部件(SRP/CS)的迭代设计过程

4.3　确定所需性能等级(PL_r)

对于选取的每种由 SRP/CS 执行的安全功能，应确定和记录所需性能等级(PL_r)(确定 PL_r 的指南

见附录 A)。所需性能等级的确定是风险评估的结果,并且参考了控制系统安全相关部件实现的风险减小的量(见图 2)。

要求 SRP/CS 实现的风险减小的量越大,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,这也包括确定控制系统的安全功能,例如:防止意外启动。

一种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、动力控制组件)。单个 SRP/CS 也可能执行多种安全功能及标准控制功能。设计者可能会单独使用或组合使用任何可用的技术。SRP/CS 也可能提供操作功能(例如: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安全相关部件(SRP/CS)由以下几方面组成:

——输入(SRP/CS_a);

——逻辑/处理(SRP/CS_b);

——输出/动力控制组件(SRP/CS_c);

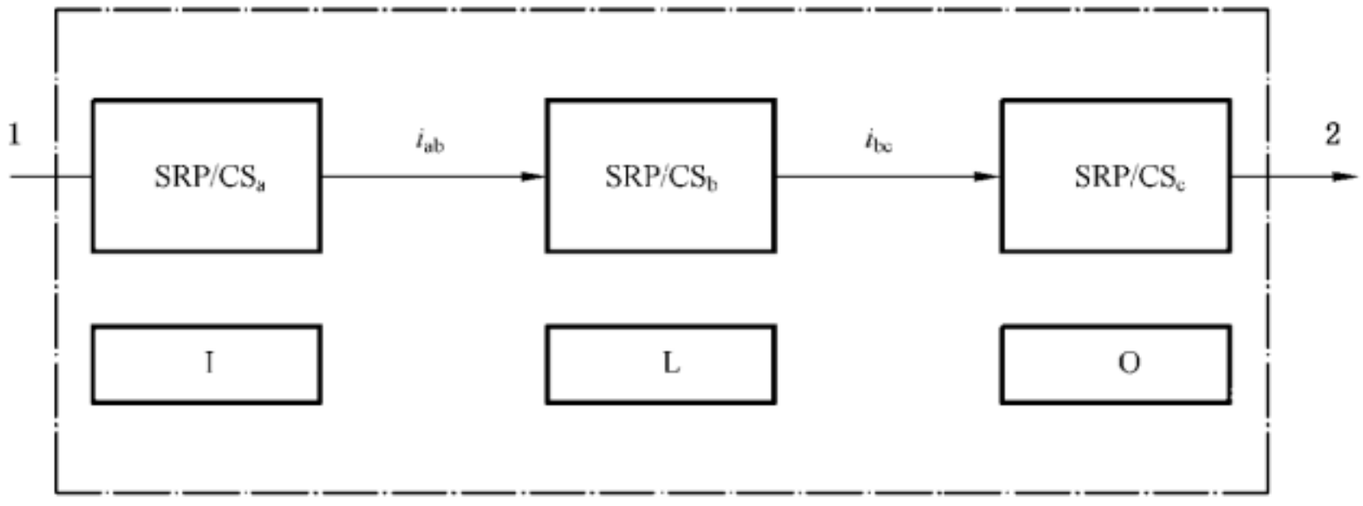
——相互连接方式(i_{ab},i_{bc})(例如:电学的、光学的)。

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。

识别控制系统的安全功能之后,设计者应识别出 SRP/CS(见图 1 和图 3),必要时还应把它们分配给输入、逻辑和输出,以及有冗余时的某具体通道,然后评估性能等级 PL(见图 3)。

注 2:指定架构在第 6 章中给出。

注 3:安全相关部件包括所有的相互连接方式。



说明:

I ——输入(例如:限位开关、传感器、AOPD);

L ——逻辑;

O——输出(例如:阀、接触器、换流器);

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 ——机器执行器(例如:电动机、气缸)。

图 4 处理典型安全功能的控制系统安全相关部件组合的示意图

4.5 所需性能等级 PL 的评估及其与 SIL 的关系

4.5.1 性能等级 PL

在本部分中,安全相关部件执行安全功能的能力通过确定性能等级 PL 来表示。

对于所选的执行安全功能的每个 SRP/CS 和/或 SRP/CS 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表现(见第 6 章);
——安全相关软件(见 4.6 和附录 J);
——系统性失效(见附录 G);
——预期环境条件下,执行安全功能的能力。

注 1:其他参数,例如:运行情况、要求率、测试率等都有一定的影响。

这些参数可按照与评估过程的关系分为以下两组:

a) 可定量的参数(单个元件的 $MTTF_D$值、DC、CCF、结构);
b) 影响 SRP/CS 表现的不可定量参数(故障条件下安全功能的行为、安全相关软件、系统性失效以及环境条件)。

可定量的参数中,可靠性(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安全相关部件,相比采用其他技术、但具有较低可靠性的容错结构中,(在一定限制下)可能提供相同或更高的 PL。

任何类型系统(例如:复杂结构)PL 的可定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 的可定量参数,本部分给出了一种基于 5 种指定架构定义的简化的方法,这些指定架构满足特定设计准则和故障条件下的表现(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~附录 H、附录 J 和附录 K 给出的程序来估计。

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

在 SRP/CS 被当作简单结构,且所需性能等级为 a~c 的应用中,可采用设计基本原理来定性估计 PL(也可见 4.5.5)。

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,可适当采用其他相关标准(例如:GB/T 19436 或 GB/T 20438)。

可应用 4.6 和附录 G 中推荐的方法来证明获得的 PL 的定性参数。

在基于 GB/T 20438 制定的标准中,安全相关控制系统完成安全功能的能力用 SIL 给出。表 3 给出了两种概念(PL 和 SIL)的关系。

PL=a 与 SIL 无对应的等级,主要用于轻微的风险减小,通常为可恢复的伤害。SIL4 专门用于流程工业中可能的灾难事件,SIL4 与机器的风险无关。因此与 SIL3 对应的 PL=e 为最高的等级。

表 3 性能等级(PL)与安全完整性等级(SIL)之间的关系

PL	SIL (参见 GB/T 20438.1) 工作模式为高/连续
a	无对应
b	1
c	1
d	2
e	3

尽管本部分中的 PL 与 GB/T 20438 和 IEC 62061 中的 SIL 有关联，但当一种安全相关控制功能由一个或多个 SRP/CS 实现时，也应根据本部分或 GB/T 20438/IEC 62061 设计每个 SRP/CS(也可见 ISO/TR 23849)。SRP/CS 可根据 6.3 进行组合。

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概率。这可通过增加元件可靠性来实现，例如：为了最大程度减少或排除重大故障或失效(见 GB/T 16855.2)，选用经验证的元件和/或应用经验证的安全原则。

——改进 SRP/CS 的结构，其目的是避免故障的危险影响。有些故障是可以检测到的，而且可能需要冗余和/或监控结构。

可单独或组合应用这两种措施。对某些技术，通过选择可靠的元件或通过故障排除可实现风险减小；但对于其他技术，可能需要冗余和/或监控系统来实现风险减小。另外，还应考虑共因失效(CCF)(见图 3)。

关于架构的约束见第 6 章。

4.5.2 每个通道的平均危险失效间隔时间($MTTF_D$)

每个通道的平均危险失效间隔时间的值用 3 种等级给出(见表 4)，且应单独考虑每个通道(例如：单通道，冗余系统的每个通道)。

对于表 4 的每个 SRP/CS(子系统)，每个通道的最大 $MTTF_D$ 值为 100 年。对于类别 4 的 SRP/CS(子系统)，每个通道的最大 $MTTF_D$ 值增加至 2500 年。

注：更高的值是合理的，因为在类别 4 中，其他定量因素、结构及 DC 已达到最大值。这就准许将 3 个以上类别 4 的子系统(SRP/CS)串联，且根据 6.3，可达到 PL=e。

表 4 每个通道的平均危险失效间隔时间($MTTF_D$)

$MTTF_D$	
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 $MTTF_D$ 的范围的选择基于该领域内当前技术水平的失效率，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 每个通道的 $MTTF_D$ 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，因为用于高风险的 SRP/CS 不宜只依靠元件的可靠性。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：要求冗余和测试。为了切实可行，范围的数量限制在 3 个内。每个通道 $MTTF_D$ 值最大为 100 年的限制针对的是执行安全功能的 SRP/CS 的单个通道。更高的 $MTTF_D$ 值可用于单个元件(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。

对于元件 $MTTF_D$ 的估计，应按以下顺序查找数据：

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 5)。

大多数情况下,可采用失效模式及影响分析(FMEA,见 GB/T 7826)或类似方法来估计 DC。在这种情况下,宜考虑所有相关的故障和/或失效模式。估计 DC 的简化方法参见附录 E。

表 5 诊断覆盖率(DC)

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,图 5、第 6 章和 E.2 中采用了 DC 的平均值 DC_{avg}。

注 2:DC 范围的选择基于三个关键值:60%、90%和 99%,在其他关于诊断覆盖率测试的标准(例如:GB/T 20438)中也有采用。研究表明,测试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 估计 PL 可定量因素的简化程序

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架构来估计 SRP/CS 的 PL 可定量因素的简化程序。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架构。

指定架构以模块图表示,并在 6.2 中的每种类别中列出。关于模块法和安全相关模块图的信息在 6.2 和附录 B 中给出。

指定架构给出了每种类别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。

指定架构是针对 SRP/CS 组合而绘制的,它起始于安全相关信号的触发,终止于动力控制组件的输出(也可见 GB/T 15706—2012 中附录 A)。指定架构也可用来描述控制系统中响应输入信号并产生安全相关输出信号的部件或子部件。因此,“输入”可代表光幕(AOPD)、控制逻辑组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等。

指定架构基于以下典型的假设:

——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,要求率小于等于测试率的 1 %(也可见附录 K 中的注),或者一旦要求安全功能就立刻进行测试,并且检测故障和使机器处于非危险条件(通常为机器停止)的总时间小于触及危险的时间(见 GB/T 19876);

——对于类别 2,测试通道的 $MTTF_D$ 大于功能通道 $MTTF_D$ 的一半。

该方法考虑把类别作为具有规定 DC_{avg} 的架构。每个 SRP/CS 的 PL 取决于架构、每个通道的平均危险失效间隔时间($MTTF_D$)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,应满足 4.6 的要求。

如果没有或不使用定量的数据(例如:低复杂度的系统),宜选用最坏情况下的所有相关参数。

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 的组合。

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～e 的应用中,SRP/CS 的结构可提供避免、检测或耐受故障的方法。切实可行的方法包括冗余、相异、监控等(也可见 GB/T 15706—2012 的第 6 章和 GB 5226.1—2008)。

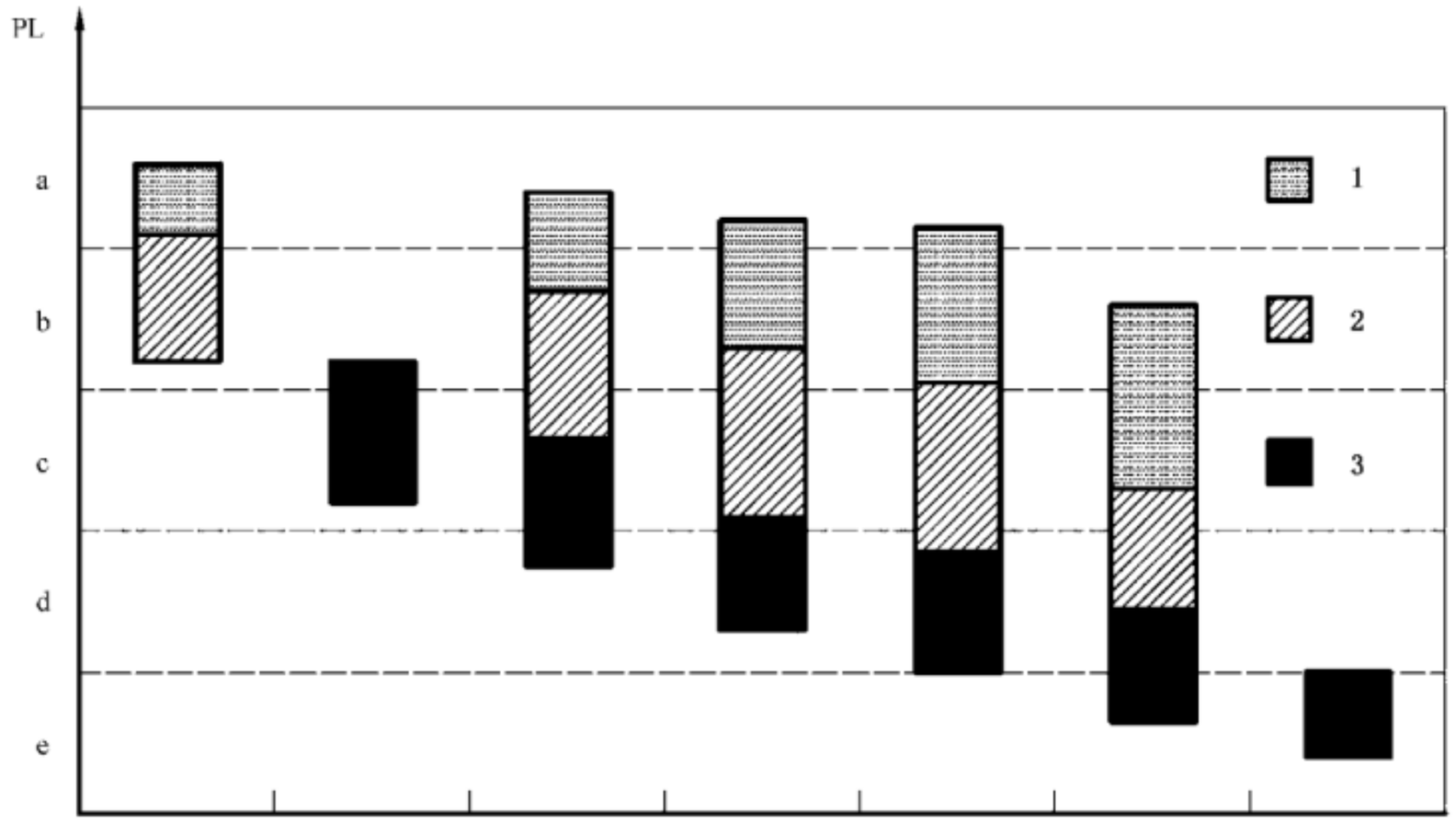
图 5 给出了结合各通道 $MTTF_D$ 和 DC_{avg} 来选择类别的程序,以达到安全功能所需的 PL。

对于 PL 的估计,图 5 给出了 DC_{avg} 和类别(水平轴)与每个通道的 $MTTF_D$(柱形图)可能的不同组合。柱形图中的阴影代表每个通道的 $MTTF_D$ 的 3 个范围(低、中、高),可选择用来达到所需的 PL。

在使用图 5 中的简化方法(代表了基于第 6 章中指定架构的不同马尔可夫模型的结果)之前,应确定 SRP/CS 的类别、DC_{avg} 和每个通道的 $MTTF_D$(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 达到的 PL 的图解方法。类别(包括共因失效)和 DC_{avg} 的组合确定选择图 5 中的哪一柱列。根据每个通道的 $MTTF_D$,应选出相关柱列的 3 个不同阴影区域中的一个阴影区域。

此区域的纵向位置确定能在纵轴上读出的达到的 PL。如果该区域的 PL 有两种或三种可能,则表 6 中给出了所达到的 PL。精确 PL 数值的选择取决于每个通道 $MTTF_D$ 的精确值,见附录 K。



说明:

PL ——性能等级;

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 与类别、DC_{avg} 和每个通道的 $MTTF_D$ 的关系

表 6　评价由 SRP/CS 达到的 PL 的简化程序

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	不包括	c	c	d	d	d	e

4.5.5　SRP/CS 输出部分按类别的描述

如果机械、液压或气动元件(或包含混合技术的元件)没有特定应用的可靠性数据,则机器制造商可以在没有计算 $MTTF_D$的情况下评估 PL 的可定量因素。

对于这种情况,可以由架构、诊断及防止共因失效的措施实现安全相关性能等级(PL)。

表 7 显示了可实现的 PL(对应图 5)与类别之间的关系。可通过类别 B 实现 PL=a 和 PL=b。如果使用了经验证的元件及经验证的安全原则,可通过类别 1 或类别 2 实现 PL=c。

通过类别 1 实现 PL=c 的安全功能时,需确定过程中没有被监控的安全相关元件的 T_{10D}值。该数值可依据机器制造商提供的经使用证明的数据来确定。

类别 2 中测试通道的 $MTTF_D$应至少为 10 年。

如果使用了经验证的元件及经验证的安全原则,可通过类别 3 实现 PL=d。

如果使用了经验证的元件及经验证的安全原则,可通过类别 4 实现 PL=e。

基本上:使用类别 2、类别 3 或类别 4 实现安全功能时需要考虑共因失效(CCF)及充分的诊断覆盖率(DC)(类别 2 和类别 3 为低、中,类别 4 为高)。

在此情况下,DC_{avg}的计算就简化为功能通道中所有元件各自 DC 的算数平均值。

表 7　基于类别、DC_{avg}以及经验证元件按最差情况估计 PL 及 PFH_D

	PFH_D(1/h)	类别 B	类别 1	类别 2	类别 3	类别 4
PL=a	2×10^{-5}	·	o	o	o	o
PL=b	5×10^{-6}	·	o	o	o	o
PL=c	1.7×10^{-6}	—	·2*	·1*	o	o
PL=d	2.9×10^{-7}	—	—	—	·1*	o
PL=e	4.7×10^{-8}	—	—	—	—	·1*

·　——推荐的类别;

o　——可选的类别;

—　——不准许的类别;

1*　——需采用经使用证明(见 3.1.39)或经验证(经元件制造商确认适用于特定应用)的元件及经验证的安全原则;

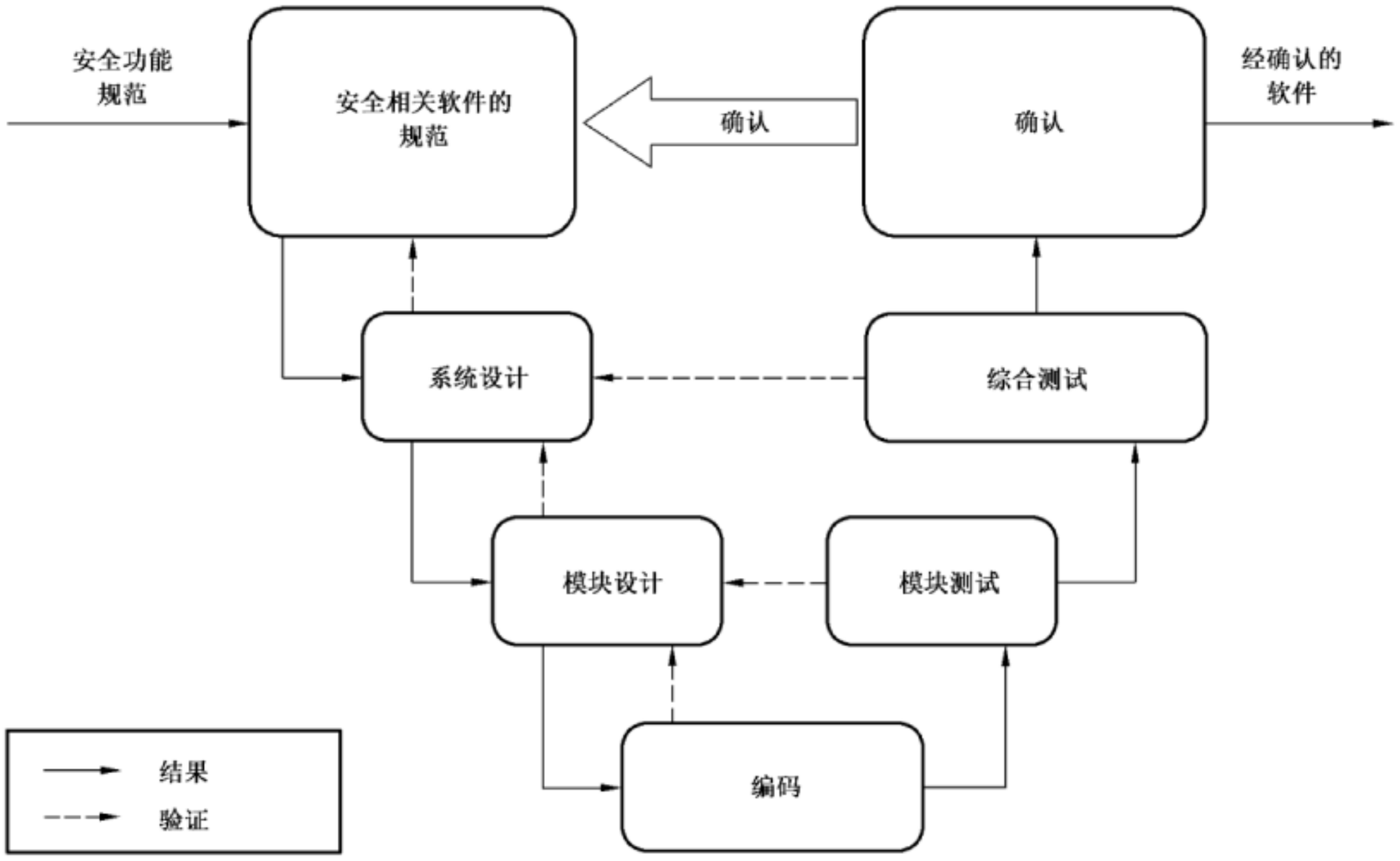
2*　——必需采用经验证的元件以及经验证的安全原则。

对于过程中没有被监控的安全相关元件,可以依据机器制造商经使用证明的数据确定 T_{10D}值。

4.6 软件的安全要求

4.6.1 一般要求

安全相关的嵌入式软件或应用软件全生命周期内的所有活动，应主要考虑避免软件全生命周期内出现的故障(见图 6)。以下要求的主要目标是要有可读、可理解、可测试及可维护的软件。



注：附录 J 对全生命周期内的活动给出了更详细的建议。

图 6 软件安全生命周期的简化 V 模型

4.6.2 安全相关的嵌入式软件(SRESW)

对于用于 PL_r 为 a～d 的元件的 SRESW，应采用以下基本方法：

——对软件安全全生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)；

——将基于软件的方法用于控制随机的硬件失效时，检验是否正确执行；

——功能测试，例如：黑盒测试；

——修改后，检查软件安全生命周期内的活动是否正确。

对于用于 PL_r 为 c 或 d 的元件的 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/T 19001 或 GB/T 20438 中的要求；

——对软件安全全生命周期内所有的相关活动进行归档；

——配置管理，以识别所有与某一 SRESW 发布版本相关的所有配置项和文档；

——包含安全要求和设计结构化技术规范；

——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，与非安全相关软件分离，限定模块大小且接口完全确定，采用设计和编码标准；

——采用控制流分析，通过走查/复查来验证编码；

——扩展的功能测试，例如：灰盒测试、性能测试或仿真；

——修改后进行影响分析以及合理的软件安全生命周期活动。

对于 PL_r=e 的元件，SRESW 应满足 IEC 61508-3:1998 中第 7 章中适用于 SIL3 的要求。对于用在类别 3 或类别 4 的 SRP/CS 中的两个通道，在规范、设计和编码中采用相异技术时，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 IEC 61508-7:2000 等。

注 2：对于类别 3 或类别 4 的 SRP/CS 使用的元件，在 SRESW 设计和编码中采用相异技术时，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。

对于没有满足 SRESW 要求的元件，例如制造商的 PLC 没有安全等级，下列任一情况下可以使用：

——SRP/CS 限制为 PL=a 或 PL=b，且使用类别 B、类别 2 或类别 3；

——SRP/CS 限制为 PL=c 或 PL=d，且类别 2 或类别 3 的两个通道中可能使用多个元件。双通道中的元件采用相异技术。

4.6.3 安全相关的应用软件(SRASW)

软件安全全生命周期(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 FVL 编写，则还应满足用于 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 PL 不同的几种安全功能，则应采用与最高 PL 有关的安全要求。用于 PL_r为 a～e 的元件的 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 SRASW，需要采用或推荐采用以下提高效率的附加措施(影响较低的用于 PL_r=c，影响中等的用于 PL_r=d，影响较高的用于 PL_r=e)。

a) 应复查安全相关软件的技术规范(也可见附录 J)，向生命周期内涉及的所有人员开放此规范，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) 性能指标，例如：响应时间；

3) 具有外部信号接口的硬件架构，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：对于使用一个元件及其工具达到 PL=e 的情况，该工具应满足适当的安全标准；如果使用了不同的工具的两种不同组件，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、动态存储分配不明确、调用接口不完整、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，或者至少指导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块(FB)库——无论是工具制造商提供的安全相关 FB 库(强烈推荐用于 PL=e)，还是符合本部分且用途已被确认的特定 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：功能块图、梯形图)。

c) 软件设计的特征应是：

1) 半形式化方法描述数据和控制流，例如：状态图或程序流程图；

2) 主要由源自经安全相关确认的功能块库的功能块实现模块化和结构化编程；

3) 限制编码大小的功能块；

4) 编码在功能块内执行，功能块宜有一个入口和一个出口点；

5) 三个阶段的架构模型，输入⇒处理⇒输出(见图 7 和附录 J)；

6) 仅在一个程序位置分配安全输出；

7) 使用检测外部失效的技术和将输入、处理和输出模块导向安全状态的防御性编程技术。

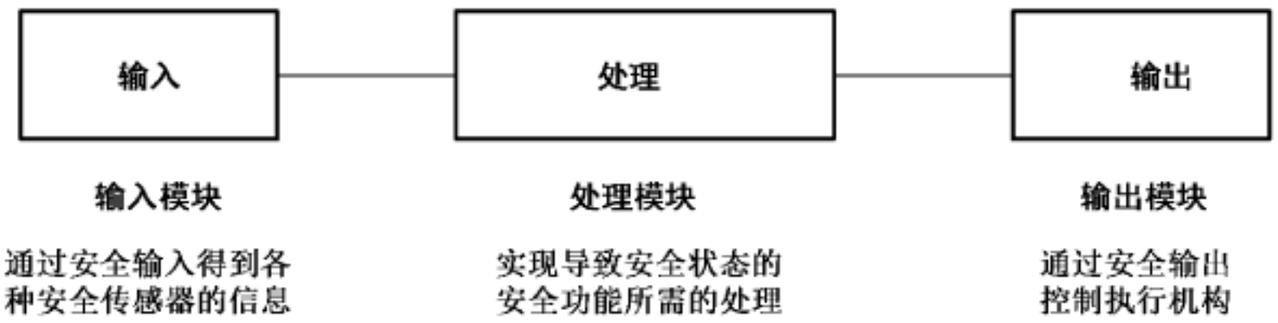


图 7 软件的一般架构模型

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) 不应存在非安全相关数据和安全相关数据的逻辑组合，因为这可导致安全相关信号的完整性下降。例如：输出控制安全相关信号的地方采用逻辑“或”组合安全相关和非安全相关的信号。

e) 软件执行/编码：

1) 代码应可读、可理解及可测试，为此宜使用符号变量(而不是显式硬件地址)；

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(防御性编程)可用的数据完整性和真实性检查(例如：范围检查)；

4) 代码宜开展仿真测试；

5) PL=d 或 PL=e 时，宜通过控制流和数据流分析检验。

f) 测试：

1) 合适的确认方法是对功能性行为和性能指标(例如：时序性能)的黑盒测试；

2) PL=d 或 PL=e 时，推荐由分析边界值开始执行测试用例；

3) 建议制定测试计划，且宜包括具有通过准则和所需工具的测试用例；

4) I/O 测试应保证在 SRASW 内正确使用安全相关信号。

g) 文件：

1) 应对所有生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/语句及声明中足够的注释。

h) 验证[1)]。

示例：复查、检查、遍查或其他的合适活动。

i) 配置管理：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配置。

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全生命周期内的活动。

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。

应控制修改访问权限且应归档修改历史。

注：修改不会影响已在使用的系统。

4.6.4 基于软件的参数化

应考虑把基于软件的安全相关数据参数化，并作为 SRP/CS 设计的一个安全相关方面在软件安全要求规范中进行描述。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；

——控制来自参数传输进程错误的影响；

——控制不完整参数传输的影响，以及

——控制参数化所用工具硬件和软件的故障和失效的影响。

参数化工具应满足本部分中对 SRP/CS 的所有要求，或者也可以使用特殊流程设定安全相关参数。该流程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；

——确认参数完整性的其他合适方式。

以及随后的确认，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：使用不是专门预定用于该目的的装置进行参数化(例如：个人电脑或相当的装置)，这一点尤其重要。

用于传输/转发过程编码/译码的软件模块以及用户用于安全相关参数可视化的软件模块，应至少在功能方面采用相异技术以避免系统性失效。

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：

——检验每个安全相关参数的正确设置(最小值、最大值和典型值)；

——检验安全相关参数是否进行了合理性检查，例如：使用无效值等；

——检验是否防止了安全相关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：使用不是专门预定用于该目的的装置进行参数化(例如：个人电脑或相当的装置)，这一点尤其重要。

4.7 验证达到的 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性能等级(PL_r)。

4.8 人类功效学方面的设计

操作者与 SRP/CS 之间的界面的设计和实现应使得机器所有预定使用和可预见的误用过程中没有人员有危险(也可见 GB/T 15706、EN 614-1、ISO 9355-1、ISO 9355-2、ISO 9355-3、EN 1005-3、GB 5226.1—2008 中第 10 章、GB/T 4205 和 GB/T 18209)。

人类工效学原则的使用应使得机器和控制系统，包括安全相关部件都容易使用，从而使得操作者不会尝试以危险方式进行操作。

GB/T 15706—2012 中 6.2.8 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 安全功能规范

本章给出了SRP/CS可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(或制定C类标准)时应包括该清单中的必要功能。

示例：安全相关停止功能、防止意外启动、手动复位功能、抑制功能、保持—运行功能。

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)也可以是安全功能，但是这只能在对机械进行了完整的风险评估后才能确定。

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和安全相关参数，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)应保证满足表中列出的有关安全功能所适用的全部要求。

本章给出了某些安全功能特征的附加要求。

必要时，特征与安全功能的要求应针对不同能量源进行适配。

表8和表9中列出的标准大部分与电气方面相关，如果是其他技术(例如：液压、气动)，则应满足相应的要求。

表8 一些适用于典型机器安全功能及其某些特征的标准

安全功能/特征	要求		附加信息，见：
	本部分	GB/T 15706—2012	
由安全防护装置触发的安全相关停止功能[a]	5.2.1	3.28.8、6.2.11.3	GB 5226.1—2008 中 9.2.2、9.2.5.3、9.2.5.5 GB/T 18831 GB/T 19876
手动复位功能	5.2.2	—	GB 5226.1—2008 中 9.2.5.3、9.2.5.4
启动/重启功能	5.2.3	6.2.11.3、6.2.11.4	GB 5226.1—2008 中 9.2.1、9.2.5.1、9.2.5.1、9.2.6
现场控制功能	5.2.4	6.2.11.8、6.2.11.10	GB 5226.1—2008 中 10.1.5
抑制功能	5.2.5	—	GB/T 29483—2013 中 5.5
保持—运行功能		6.2.11.8 b)	GB 5226.1—2008 中 9.2.6.1
使能装置功能		—	GB 5226.1—2008 中 9.2.6.3、10.9
防止意外启动	—	6.2.11.4	GB/T 19670 GB 5226.1—2008 中 5.4
被困人员的撤离和救援	—	6.3.5.3	—
隔离和能量耗散功能	—	6.3.5.4	GB/T 19670 GB 5226.1—2008 中 5.3、6.3.1
控制模式和模式选择	—	6.2.11.8、6.2.11.10	GB 5226.1—2008 中 9.2.3、9.2.4
控制系统不同安全相关部件之间的相互作用	—	6.2.11.1 (最后一句)	GB 5226.1—2008 中 9.3.4
安全相关输入值参数化监控	4.6.4	—	—
急停功能[b]	—	6.3.5.2	GB/T 16754 GB 5226.1—2008 中 9.2.5.4

[a] 包括联锁防护装置和限定装置(例如：超速、超温、超压等)。

[b] 补充保护措施，见GB/T 15706—2012。

表 9　一些给出某些安全功能和安全相关参数要求的标准

安全功能/安全相关参数	要求		附加信息，见：
	本部分	GB/T 15706—2012	
响应时间	5.2.6	—	GB/T 19876—2005 中 3.2、A.3、A.4
安全相关参数，例如：速度、温度或压力	5.2.7	6.2.11.8 e)	GB 5226.1—2008 中 7.1、9.3.2、9.3.4
能量源的波动、损失和恢复	5.2.8	6.2.11.8 e)	GB 5226.1—2008 中 4.3、7.1、7.5
指示和警告	—	6.2.8	GB/T 1251.1 GB/T 1251.2 GB/T 1251.3 GB/T 15969 GB/T 18209.1 GB 5226.1—2008 中 10.3、10.4 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况的风险评估结果。

b)　机器的操作特征，包括：

——机器的预定使用(包括可合理预见的误用)；

——操作模式(例如：现场模式、自动模式、与机器区域或部件有关的模式)；

——周期时间；

——响应时间。

c)　紧急操作。

d)　不同工作过程和手动活动(修理、调整、清洗、故障查找等)交互作用的描述。

e)　安全功能预定实现或防止的机器动作。

f)　失能后机器的动作(见 5.2.8)。

注：在某些情况下，可能需要考虑失能后机器的动作。例如：有必要保持住纵轴以防止因重力导致的坠落。这需要两个独立的安全功能：得能情况下及失能情况下。

g)　机器能工作或不能工作的条件(例如：工作模式)。

h)　操作频率。

i)　可同时激活并导致冲突动作的功能的优先次序。

5.2　安全功能详述

5.2.1　安全相关的停止功能

除了表 8 中的要求外，还应包括下列要求：

安全相关的停止功能(例如：由安全防护装置触发)触发后，一旦有必要，应使机器尽快进入安全状态。这种停止功能应优先于由操作原因引起的停止。

当一组机器协同工作时，应设置信号发送装置，将停止状况传输至管理控制系统和/或其他机器。

注：安全相关的停止功能可导致操作问题和重启困难，如：电弧焊。为了减小废弃这种停止功能的可能性，可在此停止功能前增加由操作原因引起的停止，完成实际操作并准备好从停止位置轻易且快速地重启（例如不对生产造成破坏）。一种解决方法就是使用带防护锁定的联锁装置，当循环到达某指定位置时，防护锁定释放，可轻易重启。

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：

安全防护装置发出停止指令后，停止状态应保持到出现具备重启的安全条件为止。

通过复位安全防护装置的安全功能的重新恢复，会解除停止指令。如果风险评估显示可行，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。

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安全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况；

——慎重操作；

——使控制系统能接受独立的启动指令；

——在复位触发装置从其接通（ON）位置脱开后才能被接受。

提供手动复位功能的安全相关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需要的安全水平。

复位触发装置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，需要特殊的复位程序。

注：一种解决办法是采用第二个复位触发装置。复位功能由处于危险区内的第一个复位触发装置和处于危险区外的第二个复位触发装置（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之前的有限时间内实现。

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：

只有危险状况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—2012 中 6.3.3.2.5。

启动和重启的这些要求也应适用于可遥控的机器。

注：传感器反馈给控制系统的信号可触发自动重启。

示例：在机器的自动操作中，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，不应准许遥控重启。控制系统提供的防止意外启动的作用取决于风险评估的结果。

5.2.4 现场控制功能

除了表 8 中的要求外，还应包括下列要求：

当机器通过便携式控制装置或悬挂式操纵装置等进行现场控制时，应满足以下要求：

——选用现场控制的设施应位于危险区之外；

——现场控制应只有在风险评估规定的区域才有可能触发危险状态；

——现场控制和主要控制之间的切换不应产生危险状况。

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。抑制期间安全状态应由其他方式提供。

抑制结束时，SRP/CS 的所有安全功能都应恢复。

提供抑制功能的安全相关部件选择的性能等级应使得抑制功能不会削弱相关安全功能需要的安全水平。

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：

如果风险评估显示有必要，则应确定 SRP/CS 的响应时间(也可见第 11 章)。

注：控制系统的响应时间是机器总响应时间的一部分。所需的机器总响应时间能够影响安全相关部件的设计，例如：需要提供制动系统。

5.2.7 安全相关参数

除了表 9 中的要求外，还应包括下列要求：

当安全相关参数，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安全相关数据手动输入错误能够导致危险状况，则应在控制系统安全相关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：

当能量水平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 类别及其与 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。

类别是用作达到特定 PL 的基本参数。类别根据第 4 章中描述的设计考虑，规定了 SRP/CS 在耐受故障方面所要求的性能。

类别 B 是基本的类别。出现故障可导致安全功能丧失。类别 1 主要通过选择和应用合适的元件来改进耐受故障的能力。类别 2、类别 3 和类别 4 主要是通过改进 SRP/CS 的结构来提高指定安全功能的性能。其中，类别 2 是通过定期检查正在执行的指定安全功能来实现；类别 3 和类别 4 是通过保证单一故障不会导致安全功能丧失来实现。对于类别 4 以及合理可行时的类别 3，这类故障会被检测到。类别 4 应规定耐受累积故障的能力。

表 10 中给出了 SRP/CS 的各个类别、要求和故障情况下的系统性能。

就某些元件的失效原因而论，某些故障是可以排除的(见第 7 章)。

具体 SRP/CS 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；

——所需性能等级(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；
——平均危险失效间隔时间($MTTF_D$)；
——诊断覆盖率(DC)；
——类别 2、类别 3 和类别 4 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 6.2.3～6.2.7。

以下的典型架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架构。通常可能偏离这些架构，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、故障树分析)证明其是合理的，从而证明该系统满足所需性能等级(PL_r)。

指定架构不能当作电路图，也不能当作逻辑图。对于类别 3 和类别 4，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会导致安全功能的丧失。

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 指定架构

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某一种类别。每种类别都能够用安全相关方框图进行典型表示。这些典型表示称为指定架构并在以下对每种类别的描述中列出。

图 5 中给出的取决于类别、每个通道的 $MTTF_D$ 和 DC_{avg} 的 PL 是以指定架构为基础的，这一点很重要。如果用图 5 估计 PL，则宜证明 SRP/CS 的架构其与所声称类别的指定架构是等效的。满足各类别特征的设计通常与该类别对应的指定架构是等效的。

6.2.3 类别 B

SRP/CS 应根据相关标准进行设计、构造、选择、装配和组合，并且运用使用于具体应用的基本安全原则，以耐受：

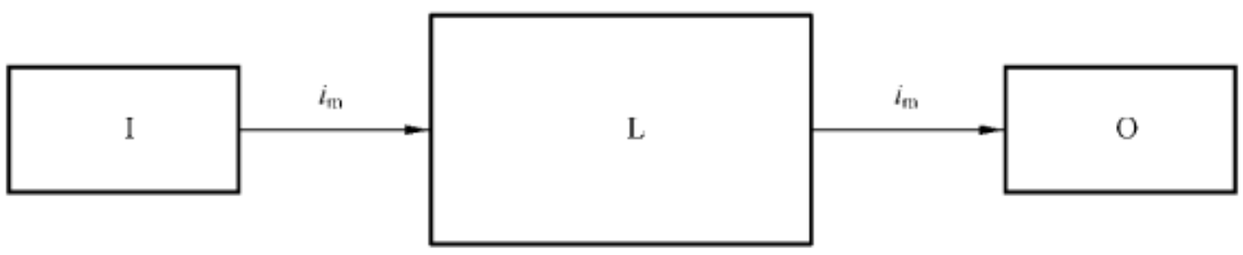
——预期的运行负荷，例如：与分断能力和频率有关的可靠性；
——工艺物料的影响，例如：清洗机的洗涤剂；
——其他相关的外部影响，例如：机械振动、电磁影响、动力源中断或扰动。

类别 B 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。

类别 B 可实现的 PL 最大值为 PL＝b。

注：故障发生时可导致安全功能丧失。

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/T 12668.3。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。



说明：

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　类别 B 的指定架构

6.2.4　类别 1

对于类别 1，应满足 6.2.3 中类别 B 的要求和以下要求。

属于类别 1 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)。

安全相关的应用中，“经验证的元件”是满足下列条件之一：

a)　在过去类似的应用中广泛应用并取得成功效果的元件；

b)　在安全相关的应用中，采用已证明其适用性和可靠性的原则制造并验证的元件。

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

决定是否接受某特定元件作为“经验证的”元件取决于用途。

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 $MTTF_D$ 应为高。

类别 1 可达到的最大 PL 为 PL＝c。

注 2：类别 1 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：故障的发生可导致安全功能的丧失。然而，类别 1 中每个通道的 $MTTF_D$ 比类别 B 中的高。因此，安全功能的丧失的可能性小一些。

明确区别“经验证的”和“故障排除”(见第 7 章)很重要。一个元件能否当作经验证的元件取决于其用途。例如：带强制断开触点的位置开关用于机床可认为是经验证的元件，但却不适合用于食品工业——奶业，如在几个月后乳酸可造成该位置开关损坏。故障排除可产生很高的 PL，但应在装置全生命周期内都应采用准许该故障排除的适当措施。为了确保这一点，可能需要控制系统以外的附加措施。对于位置开关，这些措施的示例包括：

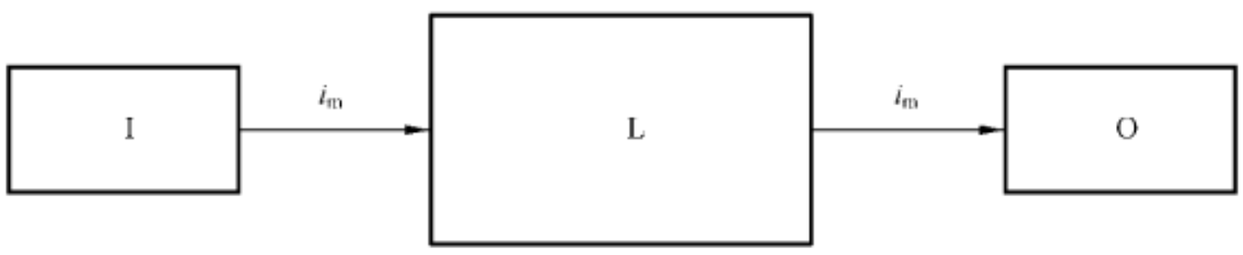
——在开关调整后确保其固定牢固的措施；

——确保凸轮固定牢固的措施；

——确保凸轮横向稳定性的措施；

——避免位置开关超行程的措施，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措施。



说明：

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 类别 1 的指定架构

6.2.5 类别 2

对于类别 2，应满足 6.2.3 中类别 B 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。

类别 2 的 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；

——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、需要安全功能的瞬时和/或如果风险评估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，准许运行；

——如果检测到故障，产生触发适当控制动作的输出(OTE)。

若 $PL_r=d$，输出(OTE)应产生一个安全状态，此安全状态应保持到排除故障为止。

对于 $PL_r=c$ 及以下的 PL_r，在可行的时候输出(OTE)应产生一个安全状态，并应保持到故障清除为止。当无法产生安全状态时(例如：最后的切换装置中的触点熔焊)，测试设备的输出 OTE 发出警告即可。

对于类别 2 的指定架构，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 OTE)。

整个 SRP/CS 的诊断覆盖率(DC_{avg})宜至少为低。每个通道的 $MTTF_D$ 应由低到高，取决于所需性能等级(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)。测试设备和提供安全功能的安全相关部件可以是一体的或是分离的。

类别 2 可达到的最大 PL 为 PL=d。

注 1：因为安全功能的检查不能适用于所有元件，所以某些情况下类别 2 不适用。

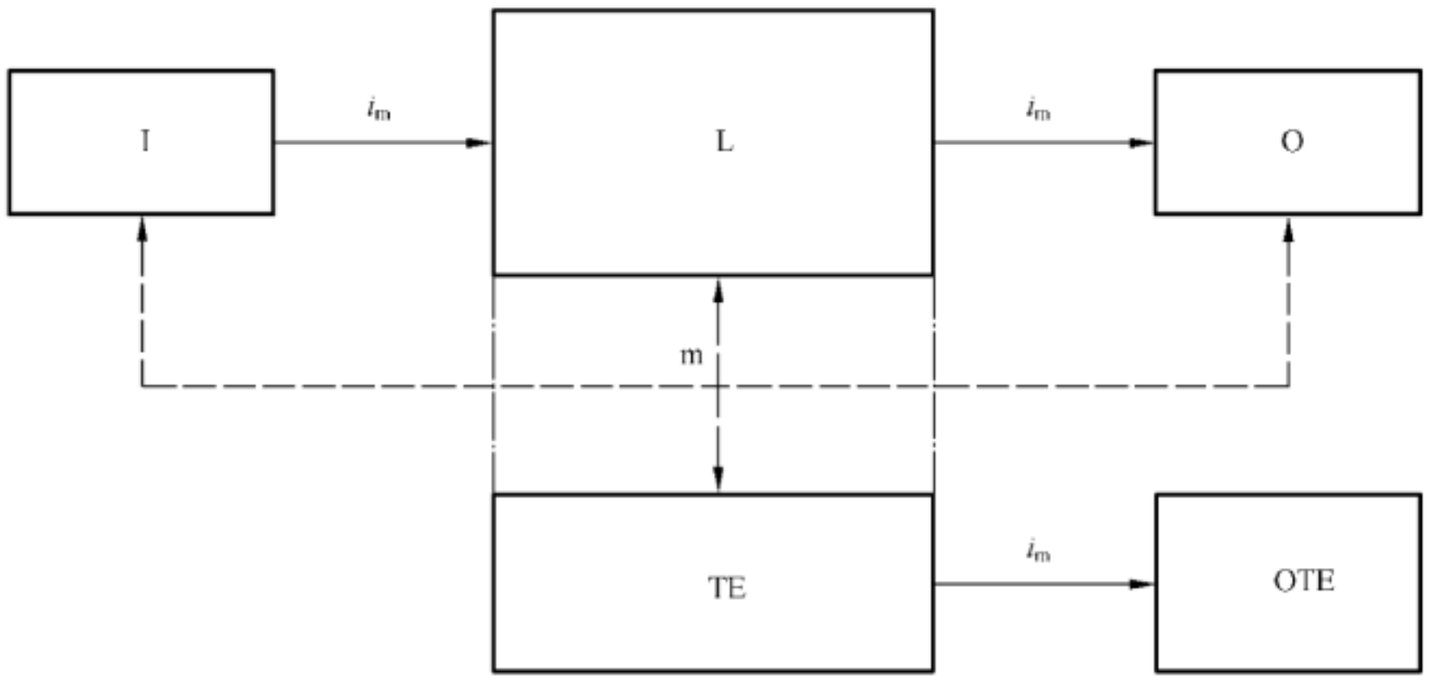
注 2：类别 2 系统特征为：

——出现故障可导致两次检查之间安全功能的丧失；

——通过检查可检测到安全功能的丧失。

注 3：支持类别 2 功能有效性的原则是所采用的技术条件，例如：检查频率的选择能够降低危险状况发生的概率。

注 4：基于指定架构的简化方法的应用，可参照 4.5.4 的说明。



说明：

i_m ——连接方式；

I ——输入装置，例如：传感器；

L ——逻辑模块；

m ——监控；

O ——输出装置，例如：主接触器；

TE ——测试设备；

OTE——TE 的输出。

虚线代表合理可行的故障检测。

图 10 类别 2 的指定架构

6.2.6 类别 3

对于类别 3，应满足 6.2.3 中类别 B 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。

类别 3 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，单一故障应在下一次要求安全功能时或之前被检测出。

整个 SRP/CS 的诊断覆盖率(DC_{avg})应至少为低。每个冗余通道的 $MTTF_D$ 应由低到高，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被检测出。因此，未发现的故障的累积能够导致意外输出并使机器处于危险状况。用于故障检测的合理可行措施的典型示例，就是利用机械导向的继电器触点的反馈和冗余电气输出进行监控。

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。

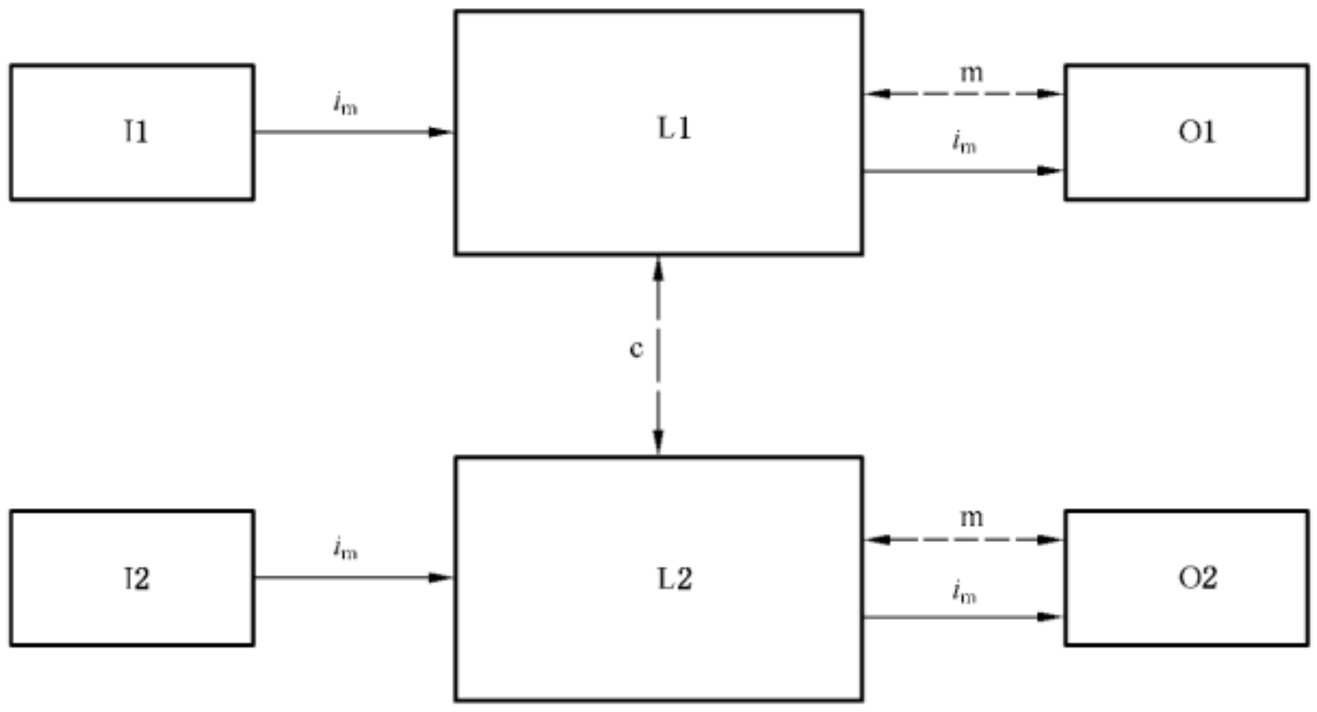
注 3：类别 3 系统特征为：

——单一故障出现时安全功能继续执行；

——检测到一些故障，但不是所有的故障；

——未检测到的故障的累积可能导致安全功能的丧失。

注 4：所采用的技术可能会影响故障检测的实施。



说明：

i_m ——连接方式；

c ——交叉监控；

I1、I2 ——输入装置，例如：传感器；

L1、L2 ——逻辑模块；

m ——监控；

O1、O2——输出装置，例如：主接触器。

虚线代表合理可行的故障检测。

图 11 类别 3 的指定架构

6.2.7 类别 4

对于类别 4，应满足 6.2.3 中类别 B 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。

类别 4 的 SRP/CS 的设计应使得：

——在这些安全相关部件中的任一部件的单一故障都不会导致安全功能的丧失；

——单一故障在下一次要求安全功能时或之前被检测到，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，那么未发现的故障的累积也不应导致安全功能的丧失。

整个 SRP/CS 的诊断覆盖率(DC_{avg})应为高，包括故障的累积。每个冗余通道的 $MTTF_D$ 应为高。应采取防止 CCF 的措施(见附录 F)。

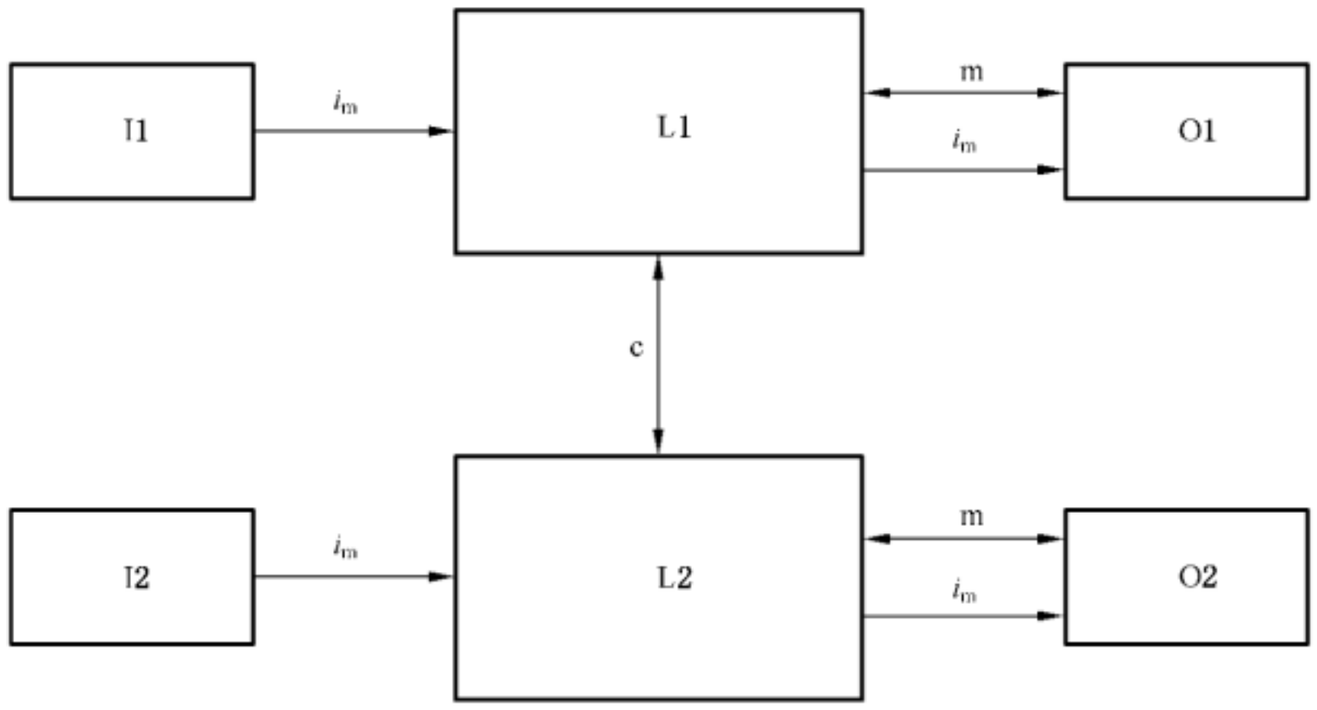
注 1：类别 4 系统特征为：

——单一故障出现时安全功能继续执行；

——及时检测到故障以防安全功能丧失；

——考虑了未检测到的故障的累积。

注 2：类别 3 和类别 4 之间的差别是类别 4 中的 DC_{avg} 更高，并且每个通道所需的 $MTTF_D$ 仅为“高”。实际应用中，考虑两种故障的组合可能就足够了。



说明：

i_m ——连接方式；

c ——交叉监控；

I1、I2 ——输入装置，例如：传感器；

L1、L2 ——逻辑模块；

m ——监控；

O1、O2——输出装置，例如：主接触器。

用于监控的实线代表诊断覆盖率，该诊断覆盖率大于类别 3 中指定架构的诊断覆盖率。

图 12 类别 4 的指定架构

表 10　类别要求摘要

类别	要求摘要	系统行为	用于实现安全的原则	每个通道的 $MTTF_D$	DC_{avg}	CCF
B （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	发生故障可导致安全功能的丧失	主要特征是元件的选择	低～中	无	无关
1 （见 6.2.4）	应采用类别 B 的要求。应使用经验证的元件和经验证的安全原则	发生故障可导致安全功能的丧失，但发生的概率低于类别 B 的概率	主要特征是元件的选择	高	无	无关
2 （见 6.2.5）	应采用类别 B 的要求和经验证的安全原则。 应通过机器控制系统以适当的时间间隔检查安全功能（见 4.5.4）	发生故障可导致两次检查之间安全功能的丧失。 通过检查来检测安全功能的丧失	主要以结构为特征	低～高	低～中	见附录 F
3 （见 6.2.6）	应采用类别 B 的要求和经验证的安全原则。 安全相关部件的设计应使： ——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丧失； ——只要合理可行，单一故障都可被检测到	发生单一故障时，安全功能总是有效。 会检测到某些但不是全部故障。 未检测到的故障的累积可导致安全功能的丧失	主要以结构为特征	低～高	低～中	见附录 F
4 （见 6.2.7）	应采用类别 B 的要求和经验证的安全原则。 安全相关部件的设计应使： ——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丧失； ——单一故障在下一次要求安全功能时或之前检测到。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丧失	发生单一故障时，安全功能总是有效。 故障的累积的检测降低了安全功能丧失的概率（高 DC）。 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（包括故障的累积）	见附录 F
注：全部要求见第 6 章。						

6.3 实现总的 PL 的 SRP/CS 组合

安全功能可通过几个 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 可以指定同一个或多个不同的类别。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 应根据本章中所描述的方法来确定。这种情况下，需要对 SRP/CS 的组合进行确认（见图 3）。

根据 6.2，组合的控制系统安全相关部件起始于安全相关信号的触发点，终止于动力控制元件的输出。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。所有部件各自的性能等级（PL）都已算出时，为了避免对组合 SRP/CS 实现的 PL 重新进行复杂的估算，可按以下方法对串联组合的 SRP/CS 进行估算。

假设 N 个单独的 SRP/CS_i 串联组合执行一个安全功能，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）。

如果所有 SRP/CS_i 的 PFH_D 已知，那么组合 SRP/CS 的 PFH_D 为所有 N 个单独 SRP/CS_i 全部 PFH_D 值的和。组合 SRP/CS 的 PL 受到以下限制：

——参与执行安全功能的单独 SRP/CS_i 的最低 PL 值（因为 PL 也由不可定量因素决定），以及

——根据表 2，与组合 SRP/CS 的 PFH_D 相对应的 PL。

注：此方法的示例参见附录 H 及 ISO/TR 23849 的 8.2.6。

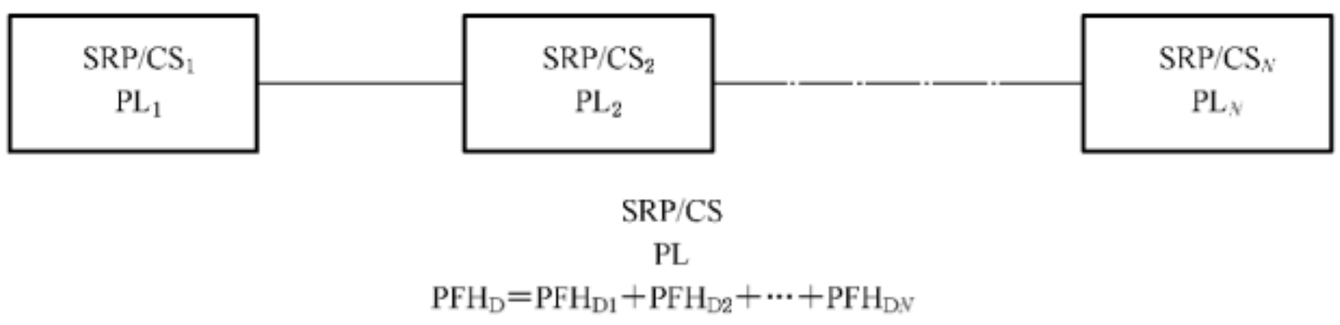


图 13 实现总的 PL 的 SRP/CS 组合

如果所有单独的 SRP/CS_i 的 PFH_D 未知，那么作为上述方法的最差情形，执行安全功能的 SRP/CS 组合的 PL 可采用表 11 按以下进行计算：

a) 识别最低的 PL_i：此为 PL_{low}；

b) 识别 $PL_i = PL_{low}$ 的 SRP/CS_i 的数量 N_{low}，$N_{low} \leqslant N$；

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，不准许
	$\leqslant 3$	⇒	a
b	>2	⇒	a
	$\leqslant 2$	⇒	b
c	>2	⇒	b
	$\leqslant 2$	⇒	c
d	>3	⇒	c
	$\leqslant 3$	⇒	d
e	>3	⇒	d
	$\leqslant 3$	⇒	e
注：本查询表中用于计算的值基于每个 PL 中值的可靠性值。			

7 故障考虑和故障排除

7.1 一般要求

根据所选的类别，安全相关部件的设计应达到所需性能等级(PL_r)。应评估耐受故障的能力。

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。故障清单并非穷举清单，必要时应考虑和列出附加的故障。此时，也宜明确描述评价的方法。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所有故障应一起视为单一故障；

——由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，则未必能评价 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。

8 确认

应对 SRP/CS 的设计进行确认(见图 3)。确认应证明提供每种安全功能的 SRP/CS 组合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

为了保持安全相关部件的规定性能，预防性或修复性维护通常是必要的。随着时间的推移，会与规定的性能发生偏离，并可导致安全性能恶化甚至导致危险状况。SRP/CS 的使用信息应包括 SRP/CS 的维护说明(包括定期检查)。

控制系统安全相关部件的维护应遵循 GB/T 15706—2012 中 6.2.7 规定的原则。维护的全部信息应符合 GB/T 15706—2012 中 6.4.5.1 e)的要求。

10 技术文件

设计 SRP/CS 时，设计者应至少对以下与安全相关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；
——安全相关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：一般情况下，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—2012 中 6.4.5.2 的原则和其他相关标准(例如：GB 5226.1—2008 中第 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：

——安全相关部件对类别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)，如果保持所选类别和安全性能是必需的，应给出适当的信息(例如：改进、维护和维修的信息)，以保证故障排除持续合理；
——偏离规定性能对安全功能的影响；
——SRP/CS 与保护装置的接口的明确阐述；
——响应时间；
——使用限制(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；
——内部元件的易接近性和可换性；
——方便、安全的故障查找方式；
——阐述应用相关架构类别时所参考依据的信息；
——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：

——对本部分注日期的引用(即："GB/T 16855.1—2018")；
——类别：B、1、2、3 或 4；
——性能等级：a、b、c、d 或 e。

示例：符合 GB/T 16855.1 本版本中类别 B 和性能等级为 a 的 SRP/CS，其表示方法如下：

GB/T 16855.1—2018　类别 B　PL=a

附 录 A
（资料性附录）
所需性能等级（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安全相关部件对风险减小的作用。这里给出的方法只是所需风险减小的一种估计方法，目的是仅作为设计者和标准制定者在确定由 SRP/CS 执行的每种必需的安全功能的 PL_r时的指南。

注：本 PL_r估计方法不是强制性的。它是一个常规方法，假定了最坏情况下发生危险事件的可能性（即事件发生的概率为 100%）。在估计 PL_r时可适当使用其他特定类型机器的风险估计方法，并应考虑处理类似机器/风险时的成功经验。因此，C 类标准要求的 PL 可以不同于图 A.1 中常规方法给出的结果。

图 A.1 中的图示基于的是提供预期安全功能之前的情形（见 GB/T 35081—2018）：在确定预期安全功能的 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估（也可见图 2）。

伤害的严重度（用 S 表示）仅是粗略估计（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）；

——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：使用直梯。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要求，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大于每年一次。

暴露于危险的持续时间宜根据能预见的与设备使用总时间有关的平均值来估计。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。如果没有其他判定依据，若频率高于每 15 min 1 次，则宜选择 F2。

如果累积的暴露时间不超过总运行时间的 1/20 且频率不超过每 15 min 1 次，则可以选择 F1。

A.2.3 避免危险事件的可能性 P1 和 P2 及发生概率

避免危险的概率及危险事件发生的概率共同组合成参数 P。当危险状况发生时，只有存在实际的机会来避免危险或显著降低其影响时才宜选择 P1，否则宜选择 P2。危险事件发生的概率可判定为低时，PL_r可以降低一个等级，见 A.2.3.2 危险事件发生的概率。

A.2.3.1 避免危险的可能性

重要的是要知道：在导致伤害之前，能否识别和避免危险状况。例如：是否能直接通过物理特征来识别暴露的危险，或者只能通过技术手段（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：

——产生危险的速度（例如：迅速或缓慢）；

——避免危险的可能性（例如：通过逃生）；

——与过程有关的实际安全经验；

——是否由经过培训且合适的人员操作；

——操作有无监控。

A.2.3.2 危险事件发生的概率

危险事件发生的概率取决于人的行为或技术失效，但多数情况下无法或难以准确确定。估计危险事件发生的概率宜依据的因素包括：

——可靠性数据；

——具有可比性的机器的以往事故。

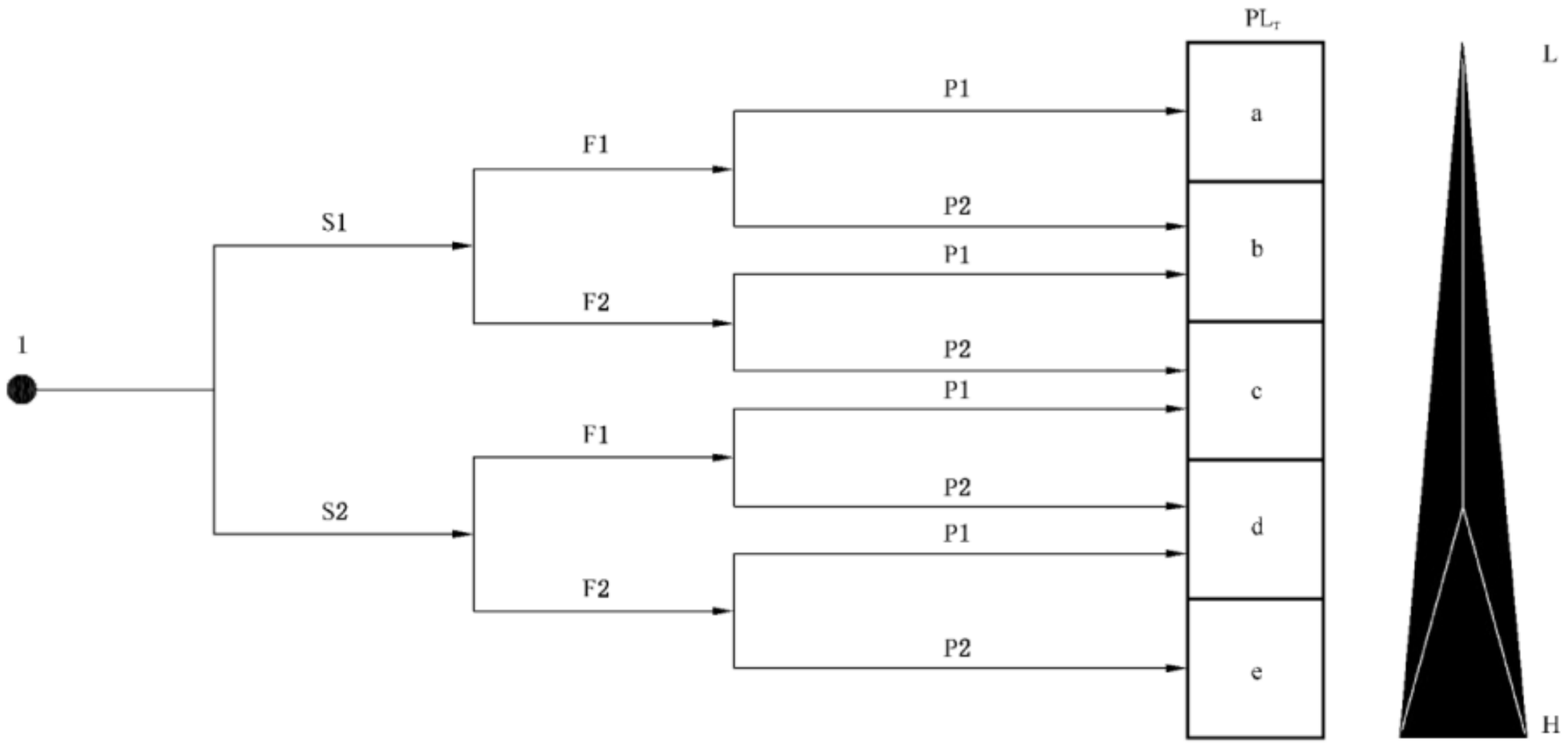
注：事故数量低并不意味着危险状况发生的少，而是意味着机器上采取了充分的安全措施。

可比的机器：

——包含相关安全功能预定降低的相同风险；

——需要相同的流程及操作动作；

——采用导致危险的相同技术。



说明：

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 ——所需性能等级。

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 ——在特定条件下可能；

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

图 A.1 给出了根据整台机器的风险评估确定安全相关 PL_r 的指南。该风险评估方法基于 GB/T 15706(见图 1 及 GB/T 35081)。每个安全功能都宜考虑本图。

A.3 重叠危险

使用本部分时，所有危险都作为一个特定危险或危险状况。为了量化风险，每个危险均可单独评价。

如果存在显著的、总是同时发生的直接关联危险的组合，则在风险估计时宜将它们组合。

进行机器风险评估时宜考虑确定危险是否宜单独考虑或进行组合。

示例 1：一个连续焊接机器人会产生多种同时存在的危险状况，比如由运动造成的挤压以及由于焊接过程导致的灼伤。这可作为一个直接关联危险的组合。

示例 2：不同的机器人在一个机器人站内工作，每个机器人分别考虑。

示例 3：作为风险评估的结果，对带有夹持设备的旋转台，每个夹持设备分别考虑可能就足够了。

附 录 B
（资料性附录）
模块法和安全相关模块图

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：

——模块宜代表与执行安全功能相关的 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——在指定架构中每个通道 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，准许通过归属于该模块的硬件单元的 $MTTF_D$，来计算该模块的 $MTTF_D$（例如：通过失效模式和影响分析或部件计数法，见 D.1）。

——仅用于诊断（例如：测试设备）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 安全相关的模块图

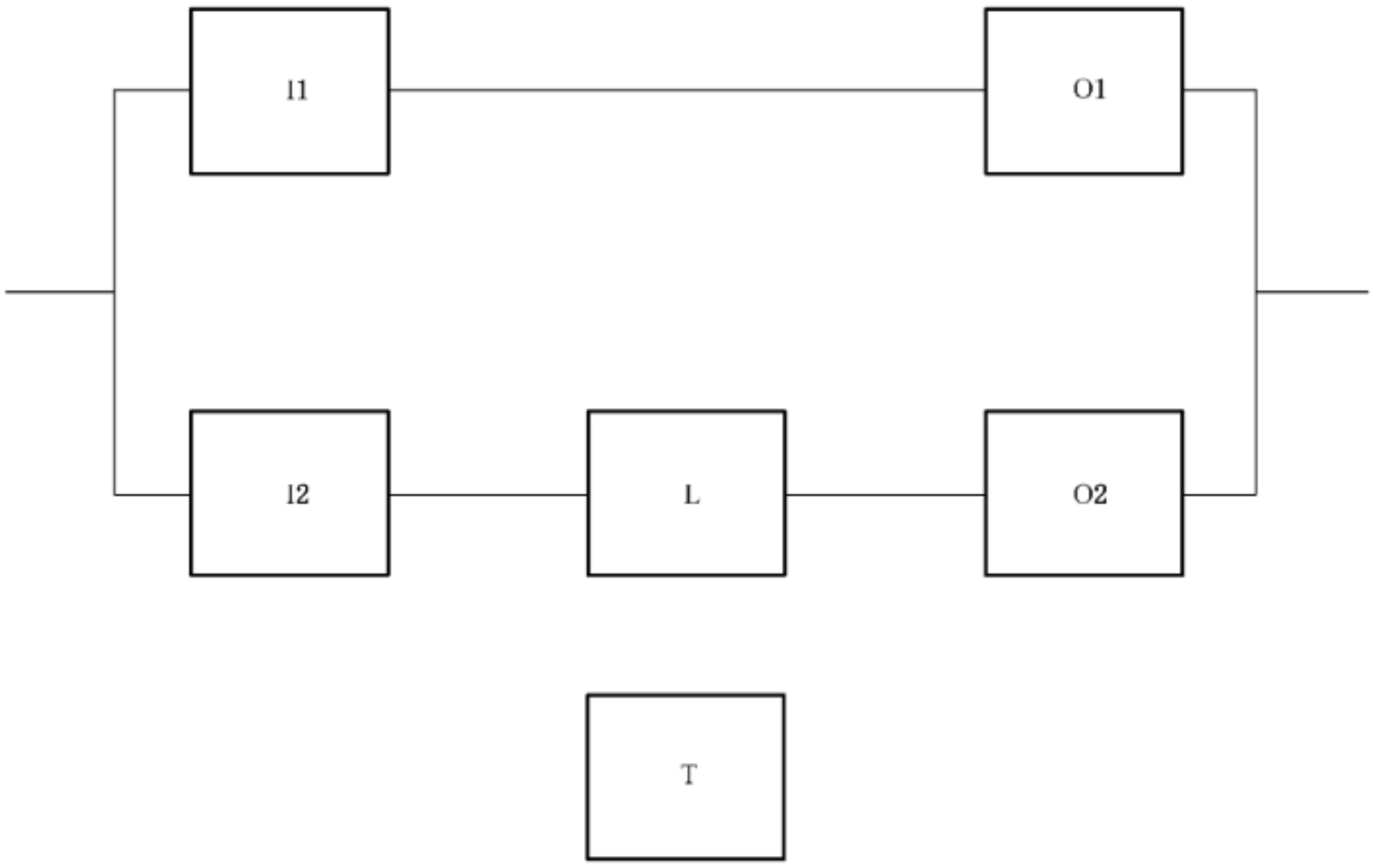
由模块法定义的模块可在安全相关的模块图中用图形方式表示 SRP/CS 的逻辑结构。对于这种图形表示，下列内容可作为指南：

——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）；

——那些仅用于测试目的且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。



说明：

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 ——测试装置。

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 仅用于测试。

图 B.1 安全相关功能模块图示例

附 录 C
（资料性附录）
单个元件 $MTTF_D$ 值的计算或评估

C.1 概述

本附录给出几种用于计算或评估单个元件 $MTTF_D$ 值的方法：C.2 中给出的方法建立在不同种类元件的良好工程实践基础上；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 列出了电气元件的 $MTTF_D$ 值。

C.2 良好工程实践方法

如果满足以下准则，则可根据表 C.1 估计用于元件的 $MTTF_D$ 值和 B_{10D} 值：

a) 元件是根据 GB/T 16855.2—2015 中基本的和经验证的安全原则或相关的元件设计标准（见表 C.1）制造的（元件数据表中确认的）。

注：该信息可在元件制造商的数据表中找到。

b) 元件制造商为 SRP/CS 的设计者规定了适当的应用和操作条件。

c) SRP/CS 的设计满足 GB/T 16855.2—2015 中针对元件实施和操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）的 $MTTF_D$ 值可估计为 150 年：

a) 液压元件是根据 GB/T 16855.2—2015 中针对液压元件设计的表 C.1 和表 C.2 中基本的和经验证的安全原则制造的（元件数据表中确认的）。

注：该信息可在元件制造商的数据表中找到。

b) 液压元件制造商为 SRP/CS 的设计者规定了适当的应用和操作条件。SRP/CS 的设计者宜提供其职责相关的信息，以证明其针对液压元件的实施和操作符合 GB/T 16855.2—2015，表 C.1 和表 C.2 中的基本的和经验证的安全原则。

如果满足 C.4 的要求，则单个液压元件（例如：阀）的 $MTTF_D$ 值可以估计为 150 年。如果全年的平均操作次数（n_{op}）低于 1 000 000 次，则见表 C.1，其 $MTTF_D$ 值可以被估计得更高。

如果不能达到 a)或 b)的要求，制造商需给出单个液压元件的 $MTTF_D$ 值。如果制造商能提供数据，则针对气动、机械、机电以及液压元件的 $MTTF_D$，可采用 B_{10D} 的概念，而无需采用上述固定的 $MTTF_D$ 值。

表 C.1 元件 $MTTF_D$ 或 B_{10D} 的相关标准

	符合 GB/T 16855.2—2015 的基本的和经验证的安全原则	相关标准	典型值： $MTTF_D$（年） B_{10D}（周期）
机械元件	表 A.1 和表 A.2	—	$MTTF_D$＝150
n_{op}≥1 000 000 次每年的液压元件	表 C.1 和表 C.2	GB/T 3766	$MTTF_D$＝150

表 C.1（续）

	符合 GB/T 16855.2—2015 的基本的和经验证的安全原则	相关标准	典型值： $MTTF_D$（年） B_{10D}（周期）
1 000 000＞n_{op}≥500 000 次每年的液压元件	表 C.1 和表 C.2	GB/T 3766	$MTTF_D$＝300
500 000＞n_{op}≥250 000 次每年的液压元件	表 C.1 和表 C.2	GB/T 3766	$MTTF_D$＝600
n_{op}＜250 000 次每年的液压元件	表 C.1 和表 C.2	GB/T 3766	$MTTF_D$＝1 200
气动元件	表 B.1 和表 B.2	GB/T 7932	B_{10D}＝20 000 000
小载荷继电器和接触式继电器	表 D.1 和表 D.2	GB/T 21711 GB/T 14048 EN 50205	B_{10D}＝20 000 000
额定载荷继电器和接触式继电器	表 D.1 和表 D.2	GB/T 21711 GB/T 14048 EN 50205	B_{10D}＝400 000
小载荷接近开关	表 D.1 和表 D.2	GB/T 14048 GB/T 18831	B_{10D}＝20 000 000
额定载荷接近开关	表 D.1 和表 D.2	GB/T 14048 GB/T 18831	B_{10D}＝400 000
小载荷接触器	表 D.1 和表 D.2	GB/T 14048	B_{10D}＝20 000 000
额定载荷接触器	表 D.1 和表 D.2	GB/T 14048	B_{10D}＝1 300 000（见注 1）
位置开关[a]	表 D.1 和表 D.2	GB/T 14048 GB/T 18831	B_{10D}＝20 000 000
位置开关（带有独立的执行器，防护锁定）[a]	表 D.1 和表 D.2	GB/T 14048 GB/T 18831	B_{10D}＝2 000 000
急停装置[a]	表 D.1 和表 D.2	GB/T 14048 GB/T 16754	B_{10D}＝100 000

B_{10D}的定义和用法见 C.4。

注 1：如果没有其他信息（例如：产品标准），则 B_{10D}估计为 B_{10}的二倍（50％的危险失效率）。

注 2："额定载荷"或"小载荷"宜考虑 GB/T 16855.2 中描述的安全原则，比如超过额定工作电流。"小载荷"是指，例如：20％。

注 3：根据电气输出触点的数量以及后续 SRP/CS 的故障检测，符合 GB/T 14048.14 和 GB/T 16754 的急停装置以及符合 GB/T 14048.20 的使能开关可以估计为一个类别 1、类别 3 或者类别 4 的子系统。每个触点组件（包括机械驱动）可以被考虑为一条具有各自 B_{10D}值的通道。对于符合 GB/T 14048.20 的使能开关，这意味着通过按压或者释放实现的打开功能。有些情况下，考虑到装置的特定应用及环境条件，机器制造商可根据 GB/T 16855.2—2015 中表 D.8 进行故障排除。

[a] 假如直接断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、机械和机电元件(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间隔时间(元件的 $MTTF_D$)。多数时候,这类元件的制造商只给出直至 10%的元件发生危险失效时的平均周期数(B_{10D})。本章给出了通过制造商给出的与操作次数密切相关的 B_{10D}或 T(寿命)来计算元件 $MTTF_D$的方法。

假如满足以下所有准则,则可根据 C.4.2 估计单个气动、机电或机械元件的 $MTTF_D$值:

a) 元件是根据 GB/T 16855.2—2015 中表 A.1、表 B.1 或表 D.1 的基本的和经验证的原则设计及制造的。

注:该信息可在元件制造商的数据表中找到。

b) 用于类别 1、类别 2、类别 3 或类别 4 的元件是根据 GB/T 16855.2—2015 中表 A.2、表 B.2 或表 D.2 的基本的和经验证的原则设计及制造的。

注:该信息可在元件制造商的数据表中找到。

c) 元件制造商为 SRP/CS 的设计者规定了适当的应用和工作条件。SRP/CS 的设计者宜提供其职责相关的信息,该信息用于证明其采用的元件符合 GB/T 16855.2—2015 中表 B.1 或表 D.1 中基本安全原则。对于类别 1、类别 2、类别 3 或类别 4,还需告知使用者其有责任使实施和操作的元件满足 GB/T 16855.2—2015 中表 B.2 或表 D.2 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:GB/T 14048.5、GB/T 21711 和 ISO 19973 等)来确定 10%的元件发生危险失效时的平均周期数(B_{10D})[2)]。需规定元件的危险失效模式,例如:在终端阻塞或切换时间改变。如果不是所有的元件都在测试过程中发生危险失效(例如:被测试的 7 个元件只有 5 个元件发生危险失效),则宜对没有发生危险失效的元件进行分析。

通过 B_{10D}和年平均操作次数 n_{op},可计算出元件的 $MTTF_D$:

$$MTTF_D = \frac{B_{10D}}{0.1 \times n_{op}} \quad \cdots\cdots (C.1)$$

式中:

$$n_{op} = \frac{d_{op} \times h_{op} \times 3\,600\ s/h}{t_{cycle}} \quad \cdots\cdots (C.2)$$

元件应用时做以下的假设:

h_{op} ——平均工作时间,单位为小时每天(h/d);

d_{op} ——平均工作时间,单位为天每年(d/年);

t_{cycle} ——元件两个相继周期起始点(例如:阀的切换)之间的平均操作时间,单位为秒每周期(s/周期);

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:

$$T_{10D} = \frac{B_{10D}}{n_{op}} \quad \cdots\cdots (C.3)$$

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}可转变为 10%的元件发生危险失效时的平均时间 T_{10D}:

2) 如果没有给出 B_{10}的危险分数(例如:由制造商给出),则可使用 B_{10}的 50%,因此推荐采用 $B_{10D} = 2B_{10}$。

$$T_{10D}=\frac{B_{10D}}{n_{op}} \qquad \cdots\cdots(C.4)$$

在本部分中，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，更有可能是威布尔分布。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(λ_D)可估计为：

$$\lambda_D \approx \frac{0.1}{T_{10D}}=\frac{0.1\times n_{op}}{B_{10D}} \qquad \cdots\cdots(C.5)$$

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：

$$F(T_{10D})=1-\exp(-\lambda_D T_{10D})=10\%，即：\lambda_D=-\frac{\ln(0.9)}{T_{10D}}=\frac{0.105\ 36}{T_{10D}}\approx\frac{0.1}{T_{10D}} \qquad \cdots\cdots(C.6)$$

对于指数分布，由于$MTTF_D=1/\lambda_D$，代入后得：

$$MTTF_D=\frac{T_{10D}}{0.1}=\frac{B_{10D}}{0.1\times n_{op}} \qquad \cdots\cdots(C.7)$$

注：公式中的所有变量是以数值与测量单位乘积表示的物理量。正确使用式(C.5)、(C.6)及$MTTF_D=1/\lambda_D$等公式需要按照1年等于8 760 h将单位“年”转换为单位“小时”。

C.4.3 示例

对于气动阀，制造商确定以6×10^7个周期的平均值作为B_{10D}。该阀在一年中工作220 d，每天两班。该阀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：

——$d_{op}=220$ d/年；

——$h_{op}=16$ h/d；

——$t_{cycle}=5$ s/周期；

——$B_{10D}=6\times10^7$个周期。

把这些值代入下列方程式进行计算：

$$n_{op}=\frac{220\times16\times3\ 600}{5}=2.53\times10^6\ 周期/年 \qquad \cdots\cdots(C.8)$$

$$T_{10D}=\frac{60\times10^6}{2.53\times10^6}=23.7\ 年 \qquad \cdots\cdots(C.9)$$

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

根据表4可给出该元件的$MTTF_D$为“高”。对于该阀，上述假设在23.7年的限定操作时间内有效。

C.5 电气元件的$MTTF_D$数据

C.5.1 概述

表C.2～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。所有数据均为普通类型。各种不同的数据库(见参考文献列出的非穷举清单)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，则强烈推荐采用专用数据。

表C.2～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。

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 典型值	备注
双极型	TO18、TO92、SOT23	38 052	76 104	危险失效概率50%
双极型、低功率	TO5、TO39	5 708	11 416	危险失效概率50%
双极型、功率	TO3、TO220、D-Pack	1 903	3 806	危险失效概率50%
FET	MOS交叉点	22 831	45 662	危险失效概率50%
MOS、功率	TO3、TO220、D-Pack	1 903	3 806	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 典型值	备注
一般用途	—	114 155	228 311	危险失效概率50%
干扰抑制器	—	16 308	32 616	危险失效概率50%
齐纳二极管$P_{tot}<1$ W	—	114 155	228 311	危险失效概率50%
整流二极管	—	57 078	114 155	危险失效概率50%
桥式整流器	—	11 415	22 831	危险失效概率50%
闸流晶体管	—	2 283	4 566	危险失效概率50%
双向三极管开关、二端交流开关	—	1 522	3 044	危险失效概率50%
集成电路(可编程序的和不可编程序的)	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 典型值	备注
标准无源电容	KS、KP、KC、KT、MKT、MKC、MKP、MKU、MP、MKV	57 078	114 155	危险失效概率 50%
陶瓷电容	—	22 831	45 662	危险失效概率 50%
铝电解质电容	非固态电解质	22 831	45 662	危险失效概率 50%
铝电解质电容	固态电解质	38 052	76 104	危险失效概率 50%
钽电解质电容	非固态电解质	11 415	22 831	危险失效概率 50%
钽电解质电容	固态电解质	114 155	228 311	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 典型值	备注
碳膜	—	114 155	228 311	危险失效概率 50%
金属膜	—	570 776	1 141 552	危险失效概率 50%
金属氧化物和线绕电阻	—	22 831	45 662	危险失效概率 50%
可变电阻	—	3 805	7 618	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 典型值	备注
MC 应用	—	38 052	76 104	危险失效概率 50%
低频感应器和变压器	—	22 831	45 662	危险失效概率 50%
主变压器、开关变压器和电源变压器	—	11 415	22 831	危险失效概率 50%

表 C.7　光耦合器

光耦合器	示例	元件的 MTTF 年	元件的 $MTTF_D$ 年 典型值	备注
双极输出	SFH 610	7 610	15 220	危险失效概率 50%
FET 输出	LH 1 056	2 854	5 708	危险失效概率 50%

附 录 D
（资料性附录）
估算各通道 $MTTF_D$ 的简化方法

D.1 部件计算法

“部件计数法”可用于分别估算每个通道的 $MTTF_D$。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：

$$\frac{1}{MTTF_D}=\sum_{i=1}^{N}\frac{1}{MTTF_{Di}}=\sum_{j=1}^{N}\frac{n_j}{MTTF_{Dj}} \qquad \cdots\cdots(D.1)$$

式中：

$MTTF_D$ ——针对整个通道；

$MTTF_{Di}$、$MTTF_{Dj}$ ——组成安全功能的每个元件的 $MTTF_D$。

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 22.4 年，根据表 4，该示例中通道的 $MTTF_D$ 为“中”。

表 D.1 电路板的元件表示例

j	元件	元件数 n_j	$MTTF_{Dj}$（年）典型值	$1/MTTF_{Dj}$（1/年）典型值	$n_j/MTTF_{Dj}$（1/年）典型值
1	晶体管、双极型、低功率（见表 C.2）	2	11 416	0.000 087 6	0.000 175 2
2	电阻、碳膜（见表 C.5）	5	228 311	0.000 004 4	0.000 021 9
3	电容、标准、无功率（见表 C.4）	4	114 115	0.000 008 8	0.000 035 0
4	继电器，数值由制造商给出（B_{10D}=20 000 000 周期、n_{op}=633 600周期/年）	4	315.7	0.003 167 6	0.012 670 3
5	接触器（制造商提供数值）（B_{10D}=2 000 000 周期、n_{op}=633 600周期/年）	1	31.6	0.031 645 6	0.031 645 6
$\sum(n_j/MTTF_{Dj})$					0.044 548 0
$MTTF_D=1/\sum(n_j/MTTF_{Dj})$[年]					22.4

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 中的 $MTTF_D$ 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。在于该示例应用中，假定 d_{op}=220 d/年，h_{op}=8 h/d 以及 t_{cycle}=10 s/周期，得出 n_{op}=633 600 周期/年。通常，采用制造商提供的 $MTTF_D$ 和 B_{10D} 值将会产生的更好的结果，即该通道的 $MTTF_D$ 更高。

3） 部件计数法通常是一种稳妥的近似方法。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。

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

6.2 中的指定架构假设：对于冗余 SRP/CS 中的不同通道，每个通道的 $MTTF_D$值是相同的。每个通道的 $MTTF_D$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；

——可以用公式(D.2)来估算一个值来代替每个通道的 $MTTF_D$：

$$MTTF_D = \frac{2}{3}\left[MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}}\right] \quad \cdots\cdots\cdots (D.2)$$

在式(D.2)应用前，$MTTF_{DC1}$和 $MTTF_{DC2}$是两个不同的冗余通道的 $MTTF_D$值，各限定为最大值 100 年(类别 B、类别 1、类别 2 和类别 3)或 2 500 年(类别 4)。

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 $MTTF_D$均为 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，可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图 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）
功能和模块诊断覆盖率(DC)的估计

E.1 诊断覆盖率(DC)的示例

功能和模块诊断覆盖率(DC)的估计示例见表 E.1。

表 E.1 诊断覆盖率(DC)的估计

措施	DC
输入装置	
由输入信号的动态变化激励的循环测试	90%
合理性检查，例如：使用常开和常闭的机械连接触点	99%
对无动态测试的输入的交叉监控	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控(用于多路 I/O)	90%
对逻辑(L)中的输入信号和中间结果进行交叉监控、对程序流进行临时和逻辑软件监控、以及静态故障和短路的检测(用于多路 I/O)	99%
间接监控(例如：通过压力开关进行监控，通过执行机构的电气位置进行监控)	90%～99%，取决于实际应用
直接监控(例如：控制阀的电气位置监控，通过机械连接的触点组件监控机电装置)	99%
通过过程进行故障检测	0%～99%，取决于实际应用；单用本措施是达不到所需性能等级“e”
监控传感器的某些特征参数(响应时间、模拟信号的范围，例如：电阻、电容)	60%
逻辑	
间接监控(例如：通过压力开关进行监控，通过执行机构的电气位置进行监控)	90%～99%，取决于实际应用
直接监控(例如：控制阀的电气位置监控，通过机械连接的触点组件监控机电装置)	99%
逻辑模块的简单暂时时间监控[例如：定时器用作监测装置(如看门狗)，其触发点在逻辑模块程序内]	60%
由监测装置(看门狗)暂时对逻辑进行逻辑监控，由测试设备进行逻辑模块性能的真实性检查	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)

表 E.1（续）

措施	DC
由主通道在启动时，或在安全功能需要时，或在一个外部信号通过一个输入设备进行请求时，检查监测装置（如看门狗）的响应能力	90%
动态原则（要求安全功能时，逻辑模块的所有元件需要按 ON-OFF-ON 改变状态），例如：由继电器执行的联锁回路	99%
常量存储器：单字节信号（8 bit）	90%
常量存储器：双字节信号（16 bit）	99%
变量存储器：使用冗余数据进行 RAM 测试，例如：标记、标志、常量、定时器及这些数据的交叉比较	60%
变量存储器：检查存储器单元数据的可读性和可写性	60%
变量存储器：由改进的汉明码或 RAM 自检进行 RAM 监控（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%
通过过程进行故障检测	0%～99%，取决于实际应用；单独用本措施是达不到所需性能等级"e"
输出装置	
由一个通道对输出监控，无动态测试	0%～99%，取决于应用中信号改变的频率
无动态测试的输出的交叉监控	0%～99%，取决于应用中信号改变的频率
对输出信号交叉监控，有动态测试，无短路检测（用于多路/O）	90%
对逻辑（L）中输出信号和中间结果的交叉监控、对程序流进行临时和逻辑软件监控、以及对静态故障和短路的检测（用于多路 I/O）	99%
带有逻辑模块和测试设备监控的致动器的冗余关断路径	99%
间接监控（例如：通过压力开关进行监控，通过致动器的电气位置进行监控）	90%～99%，取决于实际应用
通过过程进行故障检测	0%～99%，取决于实际应用；单独用本措施是达不到所需性能等级"e"
直接监控（例如：控制阀的电气位置监控，通过机械连接触点元件监控机电装置）	99%

注 1：对于 DC 的附加估计，见 GB/T 20438.2—2017 中 A.2～A.15。

注 2：如果声明逻辑模块的 DC 为中或高时，需至少采用一种措施使变量存储器、常量存储器和处理单元的 DC 均达到 60%。除本表中列出的措施外，可能还用到其他措施。

注 3：对于 DC 范围给定的措施（例如通过过程进行故障检测），考虑所有的危险失效就能确定正确的 DC 值，然后决定对哪些危险失效需要通过 DC 措施进行检测。如仍不确定，宜根据 FMEA 估计 DC。

表 E.1 的应用示例如下。

示例 1:GB/T 16855.2—2015 中附录 E 给出了一个用于确认自动装配机器故障行为和诊断方法的完整样例(非常详细)。

示例 2:ISO/TR 24119 描述了一种基于串联联锁装置诊断覆盖率评估方法的实用渐进表。

示例 3:可能只有在安全相关元件参与生产过程的情况下,例如:将标准 PLC 或标准传感器用于工件加工以及作为执行安全功能的两个冗余功能通道之一,才能应用 DC 措施"通过过程进行故障检测"。DC 水平是否合适取决于共用资源的重合度(逻辑、输入/输出等),例如:如果印刷机上的旋转编码器的所有故障都会造成印刷过程显著中断,则用于检测安全限制速度的传感器的 DC 可估计为 90%～99%。

E.2 平均 DC(DC_{avg})的估计

在很多系统中,可能用到多种故障检测措施。这些措施可检查 SRP/CS 的不同部件且有不同的 DC。当根据图 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}:

$$DC_{avg}=\frac{\frac{DC_1}{MTTF_{D1}}+\frac{DC_2}{MTTF_{D2}}+\cdots+\frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}}+\frac{1}{MTTF_{D2}}+\cdots+\frac{1}{MTTF_{DN}}} \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(E.1)$$

式中,所有未经故障排除的 SRP/CS 元件都应考虑在内并求和。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 与被测试的元件有关,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 中附录 D 给出了传感器/执行器防止 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，但并不是所有的措施都适用于机械行业。本附录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 β 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。宜考虑控制系统安全相关部件的每个部件。

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，只能得满分或零分。如果只是部分满足某种措施，则该措施的得分为零。

表 F.1 防止 CCF 的措施的评分过程及量化

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： ——以配线/管路方式分离； ——在线路中通过动态测试检测出短路或开路； ——每个通道信号路径分别屏蔽； ——印刷电路板上足够的间隙和爬电距离	15
2	**相异**	
	采用不同的技术/设计或物理原则，例如： ——第一个通道为电子的或可编程电子的，第二个通道为机电硬接线的； ——每个通道采用不同的安全功能启动方式（例如：位置、压力、温度）；和/或 采用数字量和模拟量（例如：距离、压力或温度） 和/或 不同制造商制造的元件	20
3	**设计/应用/经验**	
3.1	防止过电压、过压力、过电流、过热等的保护	15
3.2	所用的元件是经验证的	5
4	**评估/分析**	
	为了避免共因失效，设计中对控制系统安全相关部件中每个部件进行了失效模式和影响分析并考虑其结果	5
5	**能力/培训**	

表 F.1（续）

编号	防止 CCF 的措施	得分
	设计者接受了培训，以了解共因失效的原因和后果	5
6	**环境**	
6.1	电气/电子系统：根据适当的标准（例如 IEC 61326-3-1），通过防止污染和电磁干扰（EMI）来防止 CCF。 流体系统：按照元件制造商关于传压介质净化的要求，过滤传压介质、防止污垢进入以及排放压缩空气。 **注**：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： 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	**最高可得 100**

总分	避免 CCF 的措施[a]
65 或 65 以上	满足要求
小于 65	不合格⇒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：

——采用失能法（见 GB/T 16855.2）

控制系统安全相关部件（SRP/CS）的设计宜使其在动力供应丧失时可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 可实现或保持机器的安全状态（也可见 GB 5226.1 和 IEC 61508-7:2000 中 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 GB/T 4208 等）。

——为了检测有缺陷的程序次序，包含软件的 SRP/CS 宜使用程序次序监测

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元素（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 IEC 61508-7:2000 中 A.9）。

——控制错误的影响或由任何数据通信过程引起的其他影响的措施（见 IEC 61508-2:2000 中 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：

——通过自动测试进行的失效检测；

——通过冗余硬件进行的测试；

——相异的硬件；

——强制模式的操作；

——机械连接的触点；

——直接断开动作；

——定向失效模式；

——当制造商可证明在适当的裕量增加的情况下，降额设计可提高可靠性时，通过适当的系数增加裕量，增加裕量的系数宜为 1.5 倍以上。

也可见 GB/T 16855.2—2015 中 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

根据应力、耐久力、弹性、摩擦、磨损、腐蚀、温度、传导率、电介质刚度等选择材料、制造方法和

处理方法。

——正确的外形和尺寸

应力、应变、疲劳、温度、表面粗糙度、公差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。

注 1：液压或气动阀等元件可能需要循环切换，以避免开关故障或不可接受的开关次数增加，在这种情况下，定期测试是必要的。

——经受规定环境条件的能力

SRP/CS 的设计应使其可在所有预期的环境和任何可预见的不利的条件下工作，例如：温度、湿度、振动和电磁干扰(EMI)(见 GB/T 16855.2—2015，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 IEC 61508-7:2000 中 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 IEC 61508-7:2000 中 B.3.7 和 B.3.8)。

——有仿真或分析能力的计算机辅助设计工具

系统的执行设计程序，并包括适当的能够获得的且已经过试验证明有效的自动构造单元(见 IEC 61508-7:2000 中 B.3.5)。

——模拟

同时从功能特征和构成 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 IEC 61508-7:2000 中 B.3.6)。

注 2：IEC 61508-2:2000 中附录 F 指出了在设计和开发专用集成电路(ASICs)、现场可编程门阵列(FPGAs)、可编程逻辑器件(PLDs)等时，避免系统性故障的方法和措施。

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）
控制系统安全相关部件组合的示例

图 H.1 是提供一种控制机器致动器功能的安全相关部件的示意图。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。

控制过程由电子控制逻辑和液压方向阀提供。风险由 AOPD 减小，AOPD 通过检测接近危险状况并在光束被遮断时阻止流体致动器的启动来减小风险。

提供安全功能的安全相关部件包括：AOPD、电子控制逻辑单元、液压方向阀和互连方式。

这些安全相关部件组合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危险运动。

安全相关部件的组合产生了一种证明基于第 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 中的安全相关部件可描述如下：

——对于电敏保护装置（光栅）：类别 2、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；

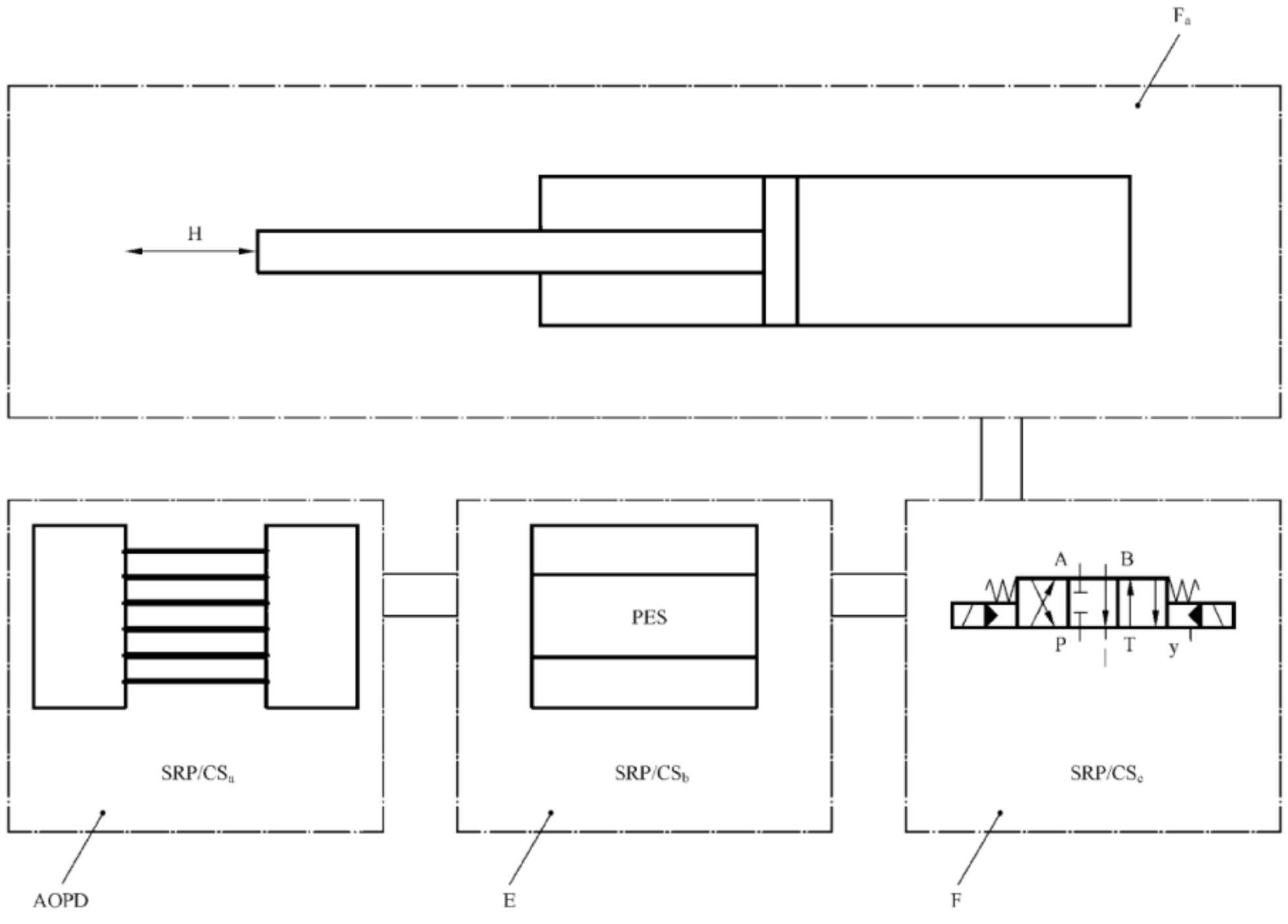
——对于电子控制逻辑单元：类别 3、PL＝d。为了提高该电子控制逻辑单元的安全性能等级，SRP/CS 的结构采用冗余结构，并采用几种能检测大多数单一故障的故障检测方法；

——对于液压方向阀：类别 1、PL＝c。经验证的情形主要是指具体应用。在本例中的阀可认为是经验证的。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：还需考虑连接方式的位置、尺寸和布局。

本组合 PL_{low}＝c 和 N_{low}＝2，其整体性能等级 PL＝c（见 6.3）。

注 2：如果图 H.2 中类别 1 或类别 2 部件发生一个故障，安全功能就可能丧失。



说明：

AOPD——有源光电保护装置(例如：光栅)，SRP/CS_a：类别 2、PL＝c；

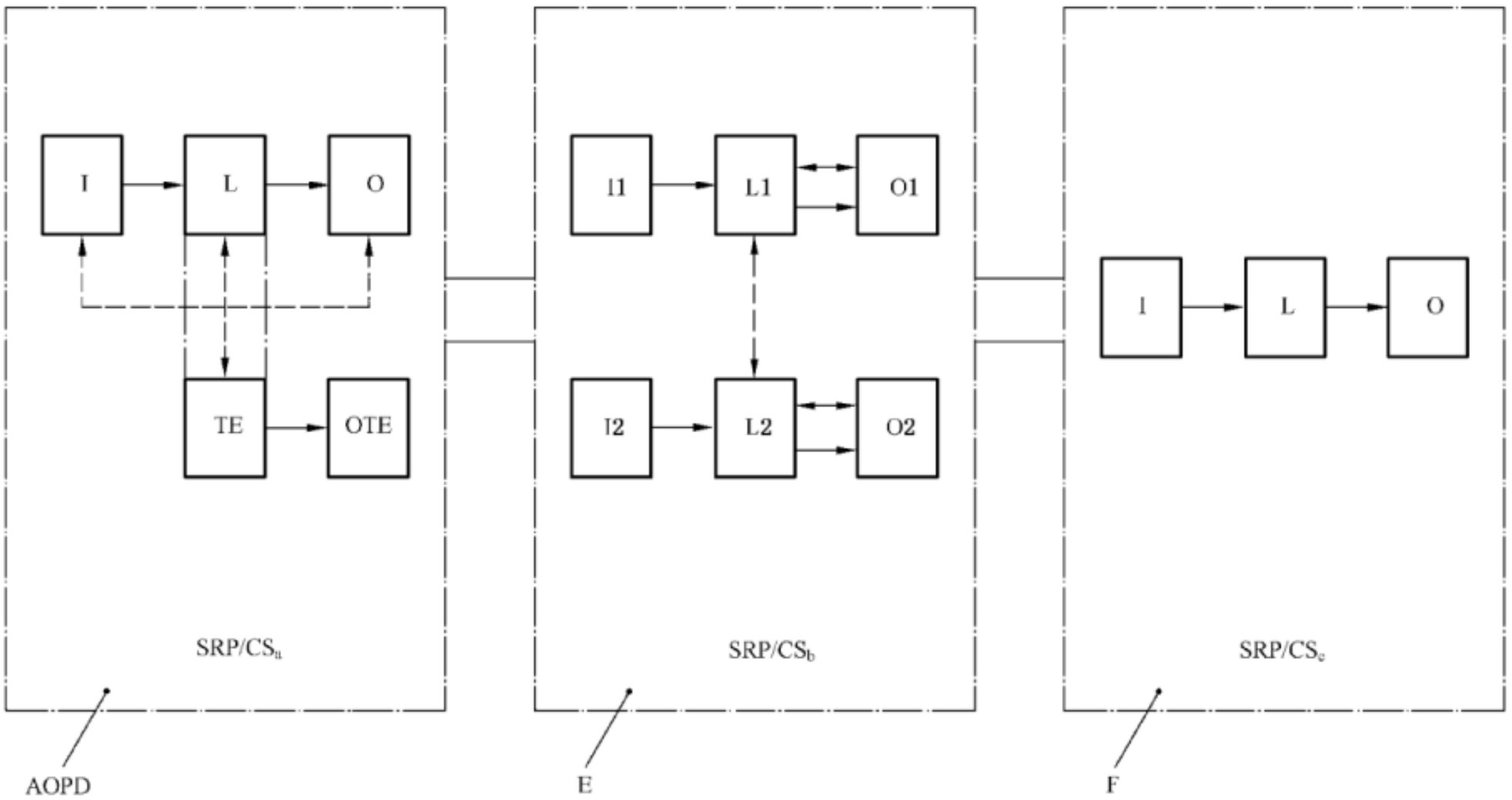
E——电子控制逻辑单元，SRP/CS_b：类别 3、PL＝d；

F——流体，SRP/CS_c：类别 1、PL＝c；

F_a——流体驱动器；

H——危险运动。

图 H.1　示例——说明 SRP/CS 组合的模块图



说明：

AOPD ——有源光电保护装置(例如：光栅)；

E ——电子控制逻辑单元；

F ——流体元件；

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 ——测试设备。

图 H.2 用指定架构替代图 H.1

附 录 I
（资料性附录）
示 例

I.1 概述

本附录举例说明了如何应用前面附录中给出的识别安全功能和确定 PL 的方法。给出了两种控制回路的量化方式，迭代过程见图 3 控制回路。

本附录分析了不同机器的控制回路的两个示例（A 和 B），见图 I.1 和图 I.3。两个示例都说明了防护门联锁的相同安全功能的性能，但由于用途不同，PL_r 也不同。第一个示例由具有中、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——由 $MTTF_D$ 中、高的元件组成，并采用适当的诊断测试。

I.2 安全功能和要求的性能等级（PL_r）

对于这两个示例，与防护门联锁相关的安全功能详细说明如下：

联锁防护门打开时，危险运动将停止（通过减速或切断电动机电源）。

注：对于示例 B，风险评估已确定由 SW2、CC 或 PLC 的故障导致电机减速失控是可以接受的。

联锁防护和机器运动部件之间的最小距离根据机器停止性能按照 GB/T 19876 确定。

对于示例 A，根据风险图解法确定下列风险参数（见图 A.1）：

——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。

这些参数决定了所需性能等级为 PL_r＝c。

首选类别的确定：通常，PL＝c 可通过相当可靠的单通道系统（类别 1）、经测试的单通道系统（类别 2）或冗余架构（类别 3）实现（见图 5 和第 6 章）。

对于示例 B，风险参数 S2 和 P1 相同，但暴露于危险的频率和/或时间，F＝F2，频繁至连续和/或暴露时间长。

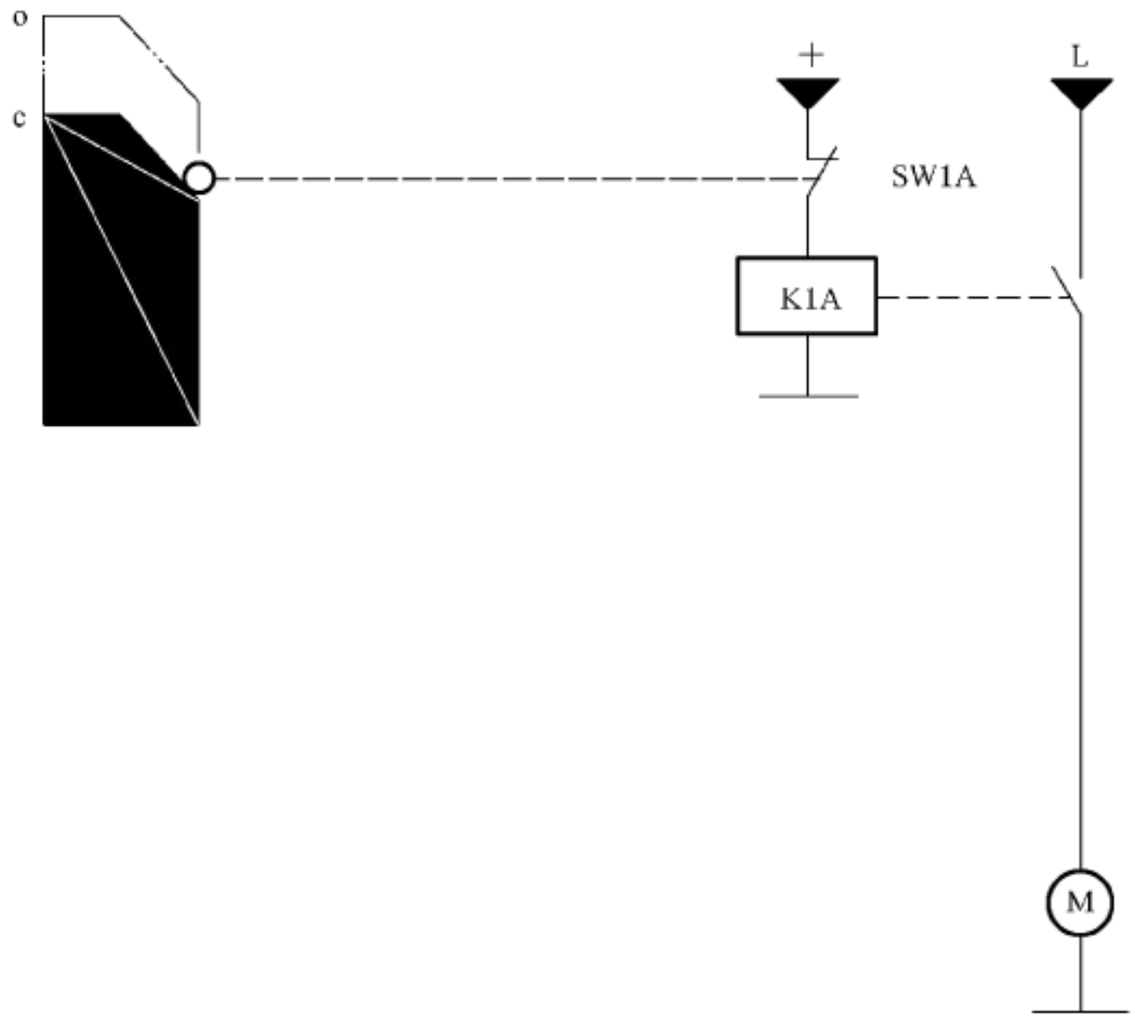
上述结论决定了所需性能等级为 PL_r＝d。

首选类别的确定：通常，性能等级 d 可通过冗余架构（类别 2 或 3）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

影响联锁防护装置安全功能的所有部件在图 I.1 中给出。为了简化，省略了不影响安全功能的元件（例如启动和停止开关）。



说明：

o ——联锁防护装置打开；

c ——联锁防护装置未打开；

M ——电动机；

K1A ——接触器式继电器；

SW1A ——位置开关(NC)。

图 I.1 执行安全功能的控制回路 A

本例中，采用直接断开动作并以强制致动模式工作的位置开关 SW1A，机械部件不能进行故障排除。位置开关连接到接触式继电器 K1A，该接触式继电器能切断电动机的电源。因此，这些安全相关部件的主要特征如下：

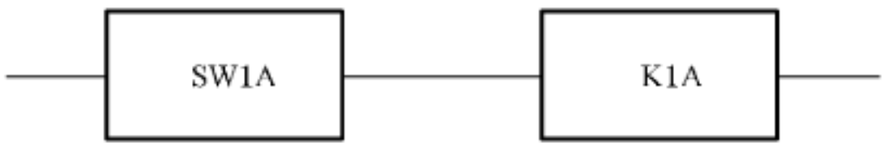
——机电元件的一个通道；

——位置开关 SW1A(NC)触点采用强制机械动作为高 B_{10D}；

——接触器式继电器 K1A 为高 B_{10D}。

根据 GB/T 16855.2，本例中的位置开关和接触式继电器都是经验证的元件。

可由图 I.2 中的安全相关模块图来表示安全相关部件。



说明：

K1A ——接触式继电器；

SW1A ——位置开关。

图 I.2 识别示例 A 中安全相关功能部件的安全相关模块图

I.3.2 $MTTF_D$、DC_{avg}、防止共因失效的措施、类别、以及 PL 的量化

假定 $MTTF_D$的值、DC_{avg}以及防止共因失效措施根据附录 C、附录 D、附录 E 和附录 F 来估计，或由制造商给出。类别根据 6.2 来估计。

——$MTTF_D$

接触式继电器 K1A 和位置开关 SW1A 对于单个通道的 $MTTF_D$ 有影响。假定制造商给出的值为 $B_{10D,SW1A}=20\ 000\ 000$ 次(位置开关不受负载影响)以及 $B_{10D,K1A}=400\ 000$ 个周期(接触器式继电器在最大负载下)。采用 C.4.2 的方法,取 220 d/年、每天工作 8 h 以及每次 60 min 的周期时间,得出 $MTTF_{D,SW1A}=113\ 636$ 年,$MTTF_{D,K1A}=2\ 273$ 年。根据 D.1 中的部件计数法,得出一个通道的 $MTTF_D$ 为:

$$\frac{1}{MTTF_D}=\frac{1}{MTTF_{D,SW1A}}+\frac{1}{MTTF_{D,K1A}}=\frac{1}{113\ 636\ 年}+\frac{1}{2\ 273\ 年}=\frac{0.000\ 45}{年} \quad \cdots\cdots(I.1)$$

由计算结果导出该通道的 $MTTF_D=2\ 222$ 年(限定为 100 年),或根据 4.5.2 中的表 4,该通道的 $MTTF_D$ 为“高”。

注:如果没有关于 SW1A 或 K1A 的 B_{10D} 信息,可根据 C.2 或 C.4 做出最坏情形的假设。

——T_{10D}

C.4.2 给出的方法得出的 $T_{10D,SW1A}$ 为 11 364 年,$T_{10D,K1A}$ 为 227 年,两者均超出 20 年的任务时间,因此不需要任何预防性更换。

——DC

由于控制回路 A 中未执行诊断测试,因此根据 4.5.3 中的表 5,DC=0 或“无”。

——CCF

由于只使用了一个通道,因此不考虑防止 CCF 的措施。

——类别

满足类别 1 的特征(基本的和经验证的原则,经验证的元件),包括要求该通道的 $MTTF_D$ 为“高”。

图 5 中的输入数据:该个通道的 $MTTF_D$ 为“高”(100 年),DC_{avg} 为“无”,类别为 1。

根据图 5,得出 PL=c。

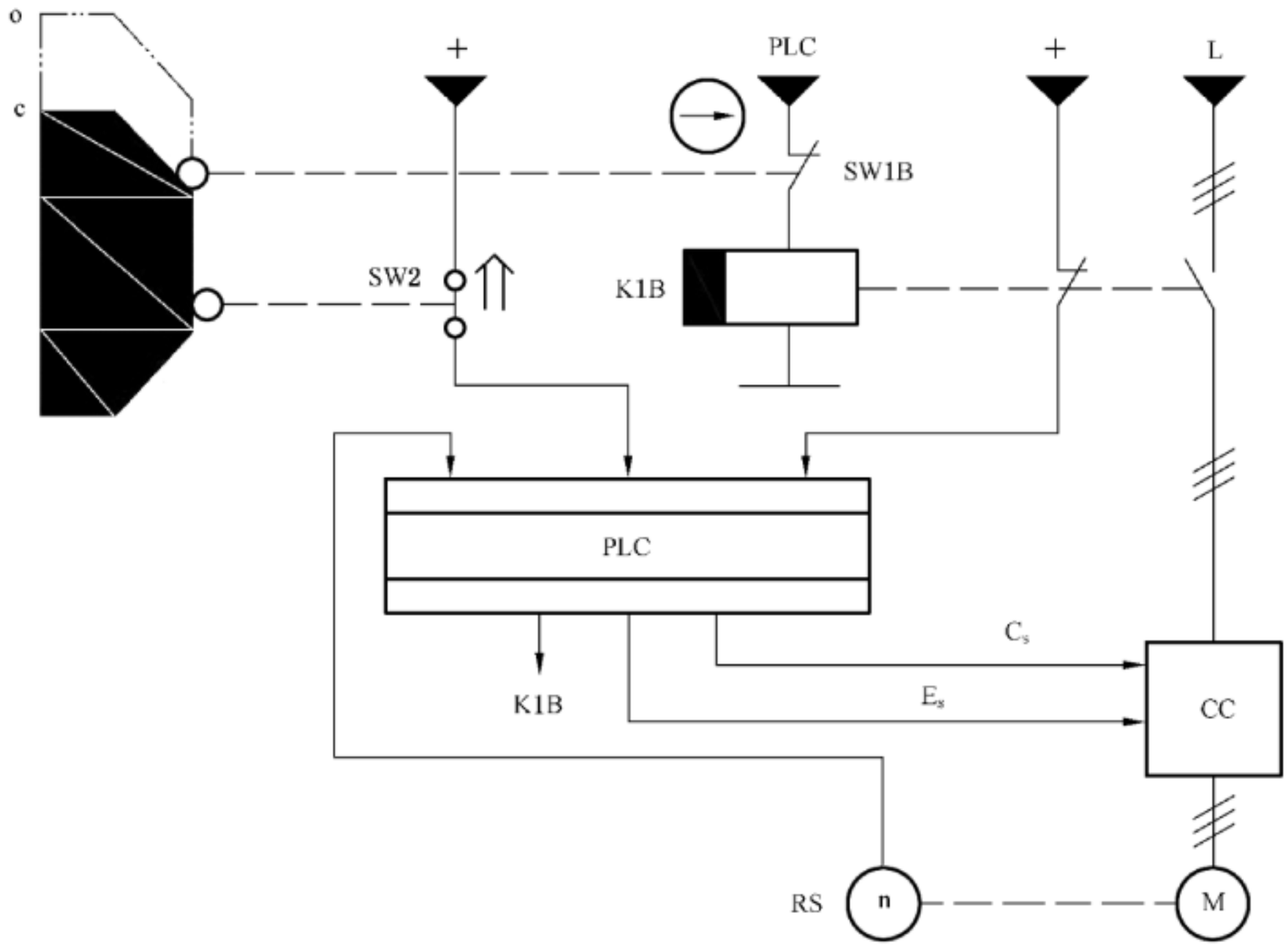
应用附录 K 得出每小时平均危险失效概率(PFH_D)为 1.14×10^{-6}/h 和 PL=c。

这个结果与 I.2 要求的性能等级 PL_r=c 匹配。因此,控制电路 A 满足 I.2 应用示例 A 的风险减小要求,具体为 S2、F1、P1 和 PL_r=c。

I.4 示例 B,冗余系统

I.4.1 安全相关部件的识别

所有影响联锁防护装置安全功能的部件在图 I.3 中给出。为了简化,省略了不影响安全功能的元件(例如启动和停止开关或 K1B 的延时开关)。



说明：

PLC ——可编程逻辑控制器；

CC ——换流器；

M ——电动机；

RS ——旋转传感器；

o ——联锁防护装置打开；

c ——联锁防护装置未打开；

C_s ——停止功能(标准的)；

E_s ——使能(标准的)；

K1B ——接触式继电器；

SW1B ——位置开关(NC)；

SW2 ——位置开关(NO)；

⇑ ——直接断开。

图 I.3 执行安全功能的控制回路 B

在本例中，采用双通道架构实现冗余。与示例 A 一样，第一个通道采用有直接断开动作的位置开关 SW1B，并以强制致动模式工作。这个位置开关与一个接触式继电器 K1B 相连，该接触式继电器可切断电动机的电源。在第二个通道中，采用了可编程序电子元件。第二个位置开关与可编程序控制器相连接，能够控制换流器 CC 切断电动机电源。因此，这些安全相关部件的主要特征如下：

——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；

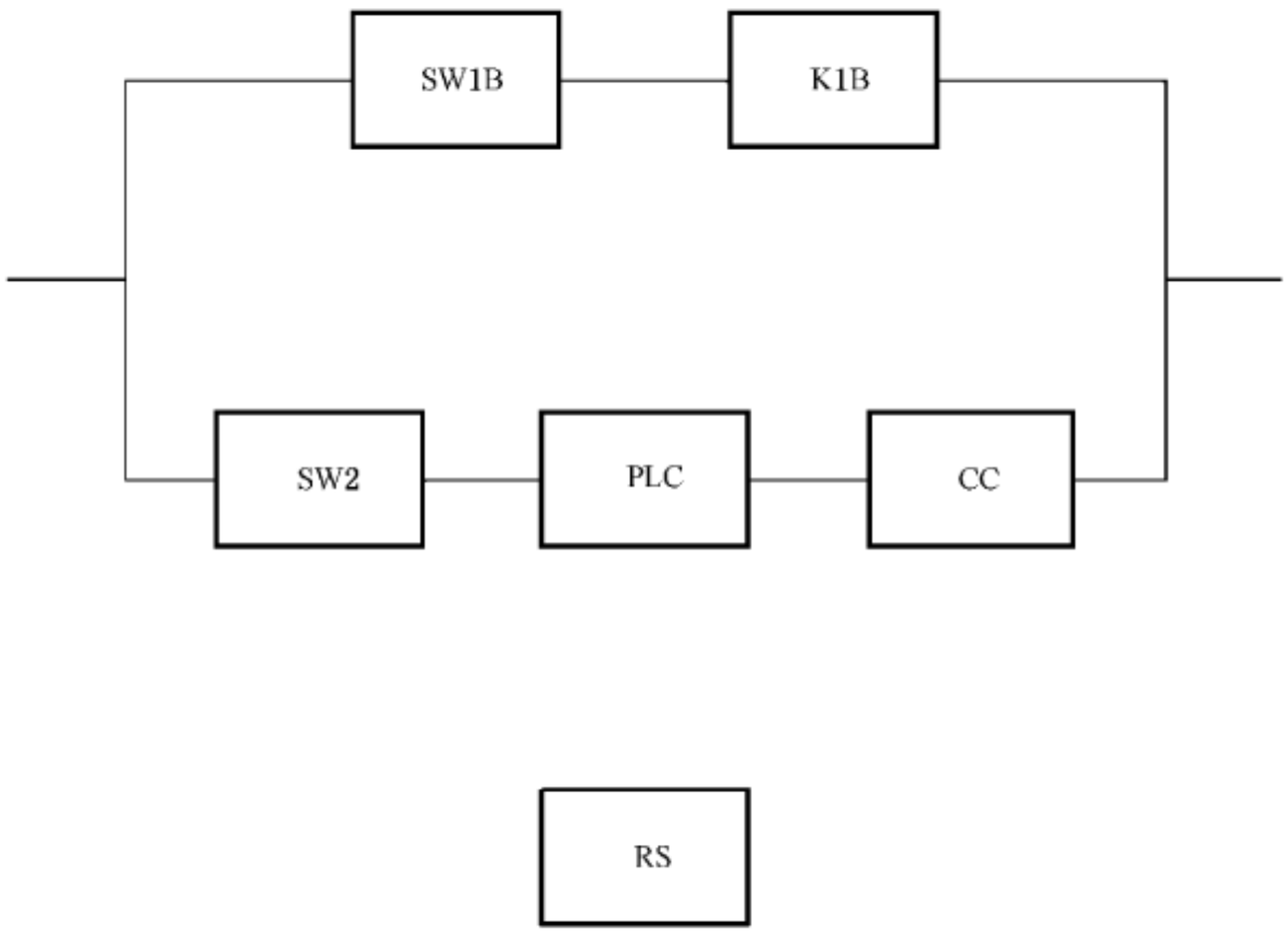
——只有位置开关 SW1B(NC)具有强制机械动作触点，但两个位置开关 SW1B 和 SW2 均具有高 B_{10D}；

——接触器式继电器 K1B 具有高 $MTTF_D$；

——电子元件 PLC 和 CC 具有中等 $MTTF_D$；

——PLC 的安全相关应用软件(SRASW)，例如软件与监控输入信号 SW2、K1B、RS 以及去往换流器的输出指令相关的部分，均按 4.6.3 进行说明、设计和验证，实现 $PL_r = d$。

安全相关部件及其通道的划分可由图 I.4 中的安全相关功能模块图来表示。因此，第一个通道由 SW1B 和 K1B 组成，第二个通道由 SW2、PLC 和 CC 组成，而 RS 只用于测试换流器。



说明：

SW1B ——位置开关；

K1B ——接触式继电器；

SW2 ——位置开关；

PLC ——可编程序控制器；

CC ——换流器；

RS ——旋转传感器。

图 I.4 识别示例 B 中安全相关部件的模块图

I.4.2 每个通道 $MTTF_D$、DC_{avg}、防止共因失效的措施、类别、以及 PL 的量化

假定每个通道 $MTTF_D$ 的值、DC_{avg} 以及防止共因失效的措施根据附录 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 具有直接断开动作并以强制致动模式工作，但机械部件未进行故障排除证明。

——$MTTF_D$

位置开关 SW1B 和接触式继电器 K1B 对于第一个通道的 $MTTF_{D,c1}$ 有影响。假定制造商给出的值为 $B_{10D,SW1B}$=20 000 000 次（位置开关不受负载影响）以及 $B_{10D,K1B}$=400 000 次（接触器式继电器在最大负载下）。采用 C.4.2 的方法，取工作 300 d/年、每天工作 16 h 以及每次 4 min 的周期时间，得出 $MTTF_{D,SW1B}$=2 778 年，$MTTF_{D,K1B}$=56 年。根据 D.1 中的部件计数法，得出第一个通道的 $MTTF_D$ 为：

$$\frac{1}{MTTF_{D,C1}}=\frac{1}{MTTF_{D,SW1B}}+\frac{1}{MTTF_{D,K1B}}=\frac{1}{2\ 778\ 年}+\frac{1}{56\ 年}=\frac{0.018\ 2}{年} \quad \cdots\cdots(I.2)$$

由计算结果导出该通道的 $MTTF_D$=55 年，根据 4.5.2 中的表 4，该通道的 $MTTF_D$ 为“高”。

在第二个通道中，SW2、PLC 和 CC 对 $MTTF_{D,C2}$ 有影响。假设制造商给出的 $B_{10D,SW2}$ 为 1 000 000 个周期。与第一个通道相同，采用 C.4.2 的方法，得出的 $MTTF_{D,SW2}$ 为 139 年。假设制造商给出的 PLC 和 CC 的 $MTTF_D$ 为 20 年。采用 D.1 中的部件计数法导出第二个通道的 $MTTF_{D,C2}$ 为：

$$\frac{1}{MTTF_{D,C2}}=\frac{1}{MTTF_{D,SW2}}+\frac{1}{MTTF_{D,PLC}}+\frac{1}{MTTF_{D,CC}}=\frac{1}{139\ 年}+\frac{1}{20\ 年}+\frac{1}{20\ 年}=\frac{0.010\ 7}{年} \quad \cdots\cdots(I.3)$$

由计算结果导出该通道的 $MTTF_D=9.3$ 年，根据 4.5.2，该通道的 $MTTF_D$ 为“低”。

注：如果没有关于 SW1B、SW2 或 K1B 的 B_{10D} 信息，可根据 C.2 或 C.4 做出最坏情形的假设。

由于这两个通道具有不同的 $MTTF_D$，式(D.2)可用来计算对称双通道系统的 $MTTF_D$ 的等效等同值。此公式计算出的 $MTTF_D=37$ 年，或根据 4.5.2 中的表 4，通道的 $MTTF_D$ 为“高”。

——T_{10D}

C.4.2 给出的方法得出的 $T_{10D,SW1B}$ 为 278 年、$T_{10D,K1B}$ 为 5.5 年、$T_{10D,SW2}$ 为 13.9 年，后两个低于 20 年的任务时间。因此，只有 K1B 在工作满 5.5 年之前更换，SW2 在工作满 13.9 年之前更换，PL 和 PFH 的估计才有效。

——DC

在控制电路 B 中，由 PLC 测试 5 个安全相关部件：SW1、SW2 和 K1B 的测试由 PLC 读回，CC 的测试则由 PLC 经由 RS 读回，PLC 执行自检。每个被测部件相关的 DC 为：

1) $DC_{SW1B}=DC_{SW2}=99\%$，“高”，由于真实性检查，见表 E.1(输入装置部分的第 2 行)；

2) $DC_{K1B}=99\%$，“高”，由于常开和常闭机械连接式触点，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”，由于由控制逻辑单元对致动器进行间接监测，见表 E.1(输入装置部分的第 6 行)——如果 PLC 监控到 CC 的失效，则可由使能装置(标准的)停止运动并断开接触器式继电器 K1B(附加的切断路径)。

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。

$$DC_{avg}=\frac{\frac{DC_{SW1B}}{MTTF_{D,SW1B}}+\frac{DC_{K1B}}{MTTF_{D,K1B}}+\frac{DC_{SW2}}{MTTF_{D,SW2}}+\frac{DC_{PLC}}{MTTF_{D,PLC}}+\frac{DC_{cc}}{MTTF_{D,CC}}}{\frac{1}{MTTF_{D,SW1B}}+\frac{1}{MTTF_{D,K1B}}+\frac{1}{MTTF_{D,SW2}}+\frac{1}{MTTF_{D,PLC}}+\frac{1}{MTTF_{D,CC}}}$$

$$=\frac{\frac{0.99}{2\,778\text{ 年}}+\frac{0.99}{56\text{ 年}}+\frac{0.99}{139\text{ 年}}+\frac{0.3}{20\text{ 年}}+\frac{0.9}{20\text{ 年}}}{\frac{1}{2\,778\text{ 年}}+\frac{1}{56\text{ 年}}+\frac{1}{139\text{ 年}}+\frac{1}{20\text{ 年}}+\frac{1}{20\text{ 年}}}=\frac{0.09}{0.13}=67.9\% \qquad \cdots\cdots(\text{I.4})$$

因此，根据 4.5.3 和表 5，得出 DC_{avg} 为“低”。

——CCF

根据 F.2 对控制电路 B 进行防止 CCF 措施估计的得分在表 I.1 中给出。

表 I.1　示例 B 中防止 CCF 方法的估计

编号	条目	控制回路的得分	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	**相异**		
	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、过压力、过电流、过热等的保护	15	15
3.2	所用的元件是经验证的	无(仅部分满足，见 F.2)	5

表 I.1（续）

编号	条目	控制回路的得分	最大可能得分
4	**评估/分析**		
	为了避免共因失效，设计中对控制系统安全相关部件每个部件进行了失效模式和影响分析并考虑其结果	无	5
5	**能力/培训**		
	设计者接受了培训，以理解共因失效的原因和结果	无	5
6	**环境**		
6.1	电气/电子系统：根据适当的标准（例如 IEC 61326-3-1），通过防止污染和电磁干扰（EMI）来防止 CCF	25	25
6.2	其他影响： 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	10
	总和	80	最大 100

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

满足类别 3 的特征，因为：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，单一故障能够在下一次要求安全功能时或之前被检测到；诊断覆盖率（DC_{avg}）为 60%～90%；防止 CCF 的措施足够且每个通道的等效 $MTTF_D$ 为“高”。

图 5 中的输入数据为：通道的 $MTTF_D$ 为“高”（37 年），DC_{avg} 为“低”，类别为 3。

根据图 5，得出 PL＝d。

应用附录 K（用 36 年）得出平均每小时危险失效概率（PFH_D）为 5.16×10^{-7}/h 和 PL＝d。

该结果与 I.2 中所需性能等级 PL_r＝d 匹配。因此，控制电路 B 满足 I.2 的应用示例 B 对风险减小的要求，具体为 S2、F2、P1 和 PL_r＝d。

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；

——用于操纵控制组件(满足安全要求)所需的处理；

——执行机构的控制。

本应用中，功能块层级上的 SRESW 的设计如图 J.1 所示。

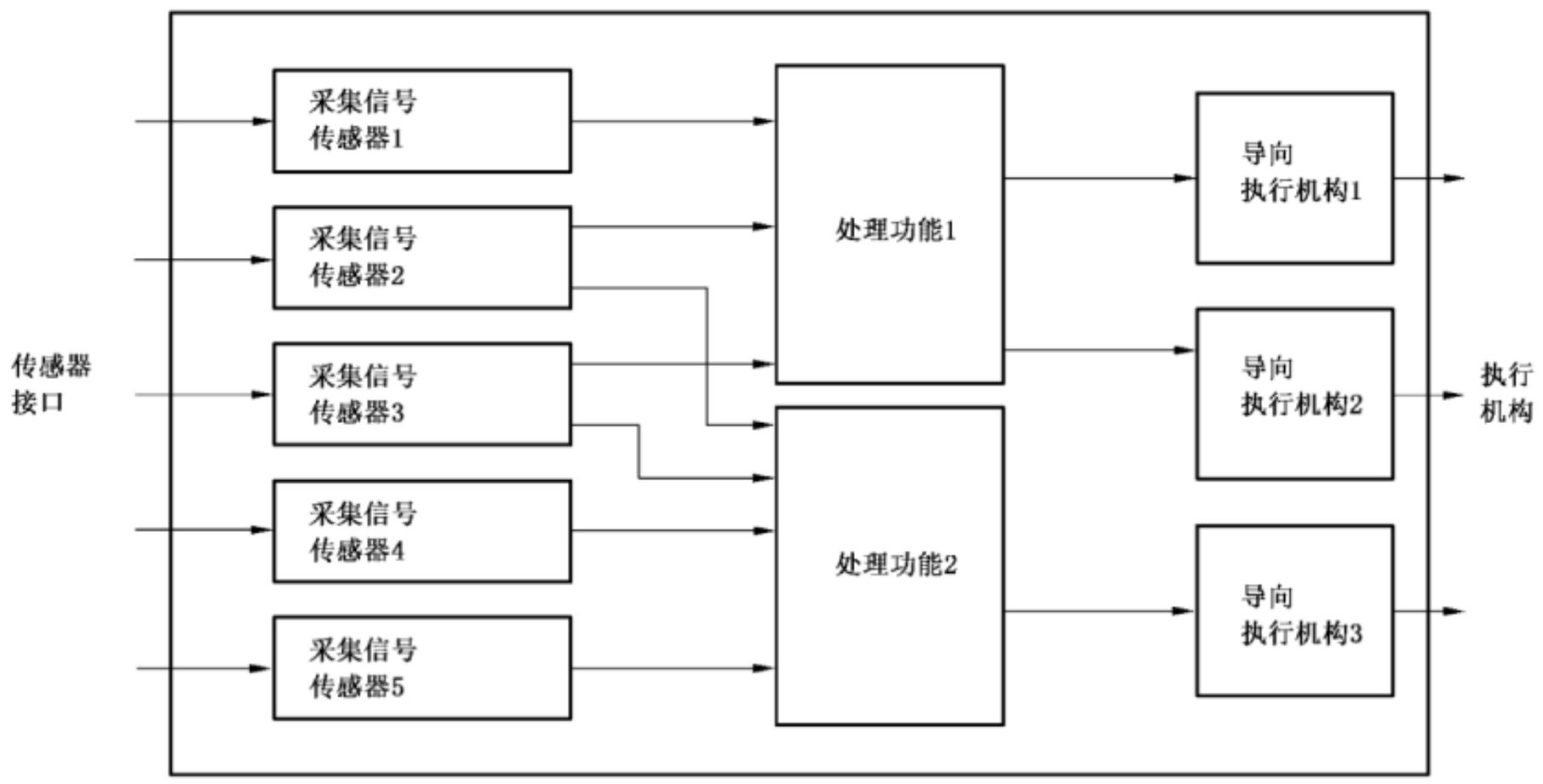


图 J.1 功能块层级的软件设计示例

J.2 软件安全生命周期 V 模型的应用

表 J.1 介绍了将软件安全生命周期 V 模型应用于机器控制方面的活动和文件的综合示例。

表 J.1 软件安全生命周期内的活动和文件

设计活动	验证活动	相关文件的提供
机器方面： 识别涉及 SRP/CS 的功能	识别安全相关功能	“用于机器控制的安全相关的技术规范”
架构方面： 确定带传感器和执行机构的控制架构	所选元件安全特征的评注	“控制架构的定义”

表 J.1（续）

设计活动	验证活动	相关文件的提供
软件技术规范方面： 将机器功能转换为软件功能	描述的重新读取(见 J.3)	“软件描述”
软件架构方面： 将各种功能细分到功能块中	确定关键模块，这些模块是重大的复审和确认工作的对象	“功能块建模”
编码方面： 根据编程规则编码(见 J.4)	代码的重新读取。功能和合规验证	“代码中的编码注释” “重新读取表的编码”
确认方面： 测试方案的制定： 功能的运行方面 失效的反应方面	测试范围的验证 测试结果的验证	“对应矩阵”：它交叉引用技术规范段落和测试结果 “测试表”：包括测试方案和对测试结果的注释

J.3 软件技术规范的验证

作为软件安全生命周期的一部分，软件技术规范层面上的验证活动在于，走读描述内容以验证其是否恰当地描述了所有的敏感点。在验证每种功能时，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导致 SPR/CS 产生预先未知行为的漏洞；

——准确地规定用于激活和撤销(去活)功能的条件；

——明确的保证所有可能的情况都已处理；

——一致性测试；

——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，通常宜由作者、数据载入、版本和最新的存取类型来鉴别。关于编程规则，可作以下区分：

a) 程序结构层面上的编程规则

程序设计应结构化以能显示一个一致和易懂的通用框架，便于定位不同的处理。这意味着：

1) 对典型程序或功能块使用样板；

2) 为了识别对应于“输入”“处理”和“输出”的主要组成部分，将程序分段；

3) 对源程序中的每段程序进行注释，以便于修改后更新注释；

4) 调用一个功能块时，描述该模块的作用；

5) 宜使用单一种类数据类型的存储地址，并以唯一的标签加以标识；

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转地址，经授权的条件跳转。

b) 关于使用变量的编程规则

——任何输出的激活或撤销(去活)宜只发生一次(集中条件)；

——程序宜结构化以使更新一个变量的等式集中化；

——每个全局变量、输入或输出，应具有一个显式助记符名称，并应在源程序中通过一个注释对其进行描述。

c) 功能块层的编程规则

——推荐使用经 SRP/CS 供应商确认的功能块，检查这些经确认的模块假定工作条件是否符合程序的条件。

编码块的大小宜限制在以下指导值：

i) 参数——最大 8 个数字、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。

——功能块不宜改变全局变量。

——数字值宜相对于预设基准来控制，以保证有效范围。

——功能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故障。

——宜通过注释来描述故障检测后的故障代码和模块状态。

——宜通过注释来描述模块的复位或正常状态的恢复。

附 录 K
（资料性附录）
图 5 的数值表示

见表 K.1。

表 K.1 图 5 的数值表示

	平均每小时危险失效概率 PFH_D(1/h)及对应的性能等级 PL													
每个通道的 $MTTF_D$ 年	类别 B DC_{avg}＝无	PL	类别 1 DC_{avg}＝无	PL	类别 2 DC_{avg}＝低	PL	类别 2 DC_{avg}＝中	PL	类别 3 DC_{avg}＝低	PL	类别 3 DC_{avg}＝中	PL	类别 4 DC_{avg}＝高	PL
3	3.80×10^{-5}	a			2.58×10^{-5}	a	1.99×10^{-5}	a	1.26×10^{-5}	a	6.09×10^{-6}	b		
3.3	3.46×10^{-5}	a			2.33×10^{-5}	a	1.79×10^{-5}	a	1.13×10^{-5}	a	5.41×10^{-6}	b		
3.6	3.17×10^{-5}	a			2.13×10^{-5}	a	1.62×10^{-5}	a	1.03×10^{-5}	a	4.86×10^{-6}	b		
3.9	2.93×10^{-5}	a			1.95×10^{-5}	a	1.48×10^{-5}	a	9.37×10^{-6}	b	4.40×10^{-6}	b		
4.3	2.65×10^{-5}	a			1.76×10^{-5}	a	1.33×10^{-5}	a	8.39×10^{-6}	b	3.89×10^{-6}	b		
4.7	2.43×10^{-5}	a			1.60×10^{-5}	a	1.20×10^{-5}	a	7.58×10^{-6}	b	3.48×10^{-6}	b		
5.1	2.24×10^{-5}	a			1.47×10^{-5}	a	1.10×10^{-5}	a	6.91×10^{-6}	b	3.15×10^{-6}	b		
5.6	2.04×10^{-5}	a			1.33×10^{-5}	a	9.87×10^{-6}	b	6.21×10^{-6}	b	2.80×10^{-6}	c		
6.2	1.84×10^{-5}	a			1.19×10^{-5}	a	8.80×10^{-6}	b	5.53×10^{-6}	b	2.47×10^{-6}	c		
6.8	1.68×10^{-5}	a			1.08×10^{-5}	a	7.93×10^{-6}	b	4.98×10^{-6}	b	2.20×10^{-6}	c		
7.5	1.52×10^{-5}	a			9.75×10^{-6}	b	7.10×10^{-6}	b	4.45×10^{-6}	b	1.95×10^{-6}	c		
8.2	1.39×10^{-5}	a			8.87×10^{-6}	b	6.43×10^{-6}	b	4.02×10^{-6}	b	1.74×10^{-6}	c		
9.1	1.25×10^{-5}	a			7.94×10^{-6}	b	5.71×10^{-6}	b	3.57×10^{-6}	b	1.53×10^{-6}	c		
10	1.14×10^{-5}	a			7.18×10^{-6}	b	5.14×10^{-6}	b	3.21×10^{-6}	b	1.36×10^{-6}	c		
11	1.04×10^{-5}	a			6.44×10^{-6}	b	4.53×10^{-6}	b	2.81×10^{-6}	c	1.18×10^{-6}	c		
12	9.51×10^{-6}	b			5.84×10^{-6}	b	4.04×10^{-6}	b	2.49×10^{-6}	c	1.04×10^{-6}	c		

表 K.1（续）

每个通道的 $MTTF_D$	平均每小时危险失效概率 PFH_D(1/h)及对应的性能等级 PL											
	类别 B	PL	类别 1	PL	类别 2	PL	类别 2	PL	类别 3	PL	类别 3	PL	类别 4	PL
年	DC_{avg}＝无		DC_{avg}＝无		DC_{avg}＝低		DC_{avg}＝中		DC_{avg}＝低		DC_{avg}＝中		DC_{avg}＝高	
13	8.78×10^{-6}	b			5.33×10^{-6}	b	3.64×10^{-6}	b	2.23×10^{-6}	c	9.21×10^{-7}	d		
15	7.61×10^{-6}	b			4.53×10^{-6}	b	3.01×10^{-6}	b	1.82×10^{-6}	c	7.44×10^{-7}	d		
16	7.13×10^{-6}	b			4.21×10^{-6}	b	2.77×10^{-6}	c	1.67×10^{-6}	c	6.76×10^{-7}	d		
18	6.34×10^{-6}	b			3.68×10^{-6}	b	2.37×10^{-6}	c	1.41×10^{-6}	c	5.67×10^{-7}	d		
20	5.71×10^{-6}	b			3.26×10^{-6}	b	2.06×10^{-6}	c	1.22×10^{-6}	c	4.85×10^{-7}	d		
22	5.19×10^{-6}	b			2.93×10^{-6}	c	1.82×10^{-6}	c	1.07×10^{-6}	c	4.21×10^{-7}	d		
24	4.76×10^{-6}	b			2.65×10^{-6}	c	1.62×10^{-6}	c	9.47×10^{-7}	d	3.70×10^{-7}	d		
27	4.23×10^{-6}	b			2.32×10^{-6}	c	1.39×10^{-6}	c	8.04×10^{-7}	d	3.10×10^{-7}	d		
30			3.80×10^{-6}	b	2.06×10^{-6}	c	1.21×10^{-6}	c	6.94×10^{-7}	d	2.65×10^{-7}	d	9.54×10^{-8}	e
33			3.46×10^{-6}	b	1.85×10^{-6}	c	1.06×10^{-6}	c	5.94×10^{-7}	d	2.30×10^{-7}	d	8.57×10^{-8}	e
36			3.17×10^{-6}	b	1.67×10^{-6}	c	9.39×10^{-7}	d	5.16×10^{-7}	d	2.01×10^{-7}	d	7.77×10^{-8}	e
39			2.93×10^{-6}	c	1.53×10^{-6}	c	8.40×10^{-7}	d	4.53×10^{-7}	d	1.78×10^{-7}	d	7.11×10^{-8}	e
43			2.65×10^{-6}	c	1.37×10^{-6}	c	7.34×10^{-7}	d	3.87×10^{-7}	d	1.54×10^{-7}	d	6.37×10^{-8}	e
47			2.43×10^{-6}	c	1.24×10^{-6}	c	6.49×10^{-7}	d	3.35×10^{-7}	d	1.34×10^{-7}	d	5.76×10^{-8}	e
51			2.24×10^{-6}	c	1.13×10^{-6}	c	5.80×10^{-7}	d	2.93×10^{-7}	d	1.19×10^{-7}	d	5.26×10^{-8}	e
56			2.04×10^{-6}	c	1.02×10^{-6}	c	5.10×10^{-7}	d	2.52×10^{-7}	d	1.03×10^{-7}	d	4.73×10^{-8}	e
62			1.84×10^{-6}	c	9.06×10^{-7}	d	4.43×10^{-7}	d	2.13×10^{-7}	d	8.84×10^{-8}	e	4.22×10^{-8}	e
68			1.68×10^{-6}	c	8.17×10^{-7}	d	3.90×10^{-7}	d	1.84×10^{-7}	d	7.68×10^{-8}	e	3.80×10^{-8}	e
75			1.52×10^{-6}	c	7.31×10^{-7}	d	3.40×10^{-7}	d	1.57×10^{-7}	d	6.62×10^{-8}	e	3.41×10^{-8}	e
82			1.39×10^{-6}	c	6.61×10^{-7}	d	3.01×10^{-7}	d	1.35×10^{-7}	d	5.79×10^{-8}	e	3.08×10^{-8}	e
91			1.25×10^{-6}	c	5.88×10^{-7}	d	2.61×10^{-7}	d	1.14×10^{-7}	d	4.94×10^{-8}	e	2.74×10^{-8}	e
100			1.14×10^{-6}	c	5.28×10^{-7}	d	2.29×10^{-7}	d	1.01×10^{-7}	d	4.29×10^{-8}	e	2.47×10^{-8}	e

表 K.1（续）

	平均每小时危险失效概率 PFH_D(1/h)及对应的性能等级 PL						
每个通道的 $MTTF_D$ 年	类别 B PL DC_{avg}＝无	类别 1 PL DC_{avg}＝无	类别 2 PL DC_{avg}＝低	类别 2 PL DC_{avg}＝中	类别 3 PL DC_{avg}＝低	类别 3 PL DC_{avg}＝中	类别 4 PL DC_{avg}＝高
110							2.23×10^{-8} e
120							2.03×10^{-8} e
130							1.87×10^{-8} e
150							1.61×10^{-8} e
160							1.50×10^{-8} e
180							1.33×10^{-8} e
200							1.19×10^{-8} e
220							1.08×10^{-8} e
240							9.81×10^{-8} e
270							8.67×10^{-8} e
300							7.76×10^{-8} e
330							7.04×10^{-8} e
360							6.44×10^{-8} e
390							5.94×10^{-8} e
430							5.38×10^{-8} e
470							4.91×10^{-8} e
510							4.52×10^{-8} e
560							4.11×10^{-8} e
620							3.70×10^{-8} e
680							3.37×10^{-8} e
750							3.05×10^{-8} e
820							2.79×10^{-8} e

表 K.1（续）

	平均每小时危险失效概率 PFH_D(1/h)及对应的性能等级 PL						
每个通道的 $MTTF_D$ 年	类别 B PL DC_{avg}＝无	类别 1 PL DC_{avg}＝无	类别 2 PL DC_{avg}＝低	类别 2 PL DC_{avg}＝中	类别 3 PL DC_{avg}＝低	类别 3 PL DC_{avg}＝中	类别 4 PL DC_{avg}＝高
910							2.51×10^{-8} e
1 000							2.28×10^{-8} e
1 100							2.07×10^{-8} e
1 200							1.90×10^{-8} e
1 300							1.75×10^{-8} e
1 500							1.51×10^{-8} e
1 600							1.42×10^{-8} e
1 800							1.26×10^{-8} e
2 000							1.13×10^{-8} e
2 200							1.03×10^{-8} e
2 300							9.85×10^{-8} e
2 400							9.44×10^{-8} e
2 500							9.06×10^{-8} e

注 1：如果类别 2 的要求率小于或等于测试率的 1/25(见 4.5.4)，则表 K.1 所述类别 2 的 PFH_D值乘以 1.1 的系数用作最坏情况的估计值。

注 2：根据以下 DC_{avg}计算 PFH_D值：

——DC_{avg}＝低，用 60％计算；

——DC_{avg}＝中，用 90％计算；

——DC_{avg}＝高，用 99％计算。

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] IEC 61508-1:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 1:General requirements

[6] IEC 61508-2:2000 Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 2:Requirements for electrical/electronic/programmable electronic safety-related systems

[7] IEC 61508-4:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 4:Definitions and abbreviations

[8] IEC 61508-5:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 5:Examples of methods for the determination of sagety integrity levels

[9] IEC 61508-6:2000 Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 6:Guidelines on the application of IEC 61508-2 and IEC 61508-3

[10] IEC 61508-7:2000 Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 7:Overview of techniques and measures

[11] IEC 62061:2005 Safety of machinery—Functional safety of safety-related electrical,electronic and programmable electronic control systems

[12] GUIDELINES HSE Programmable Electronic Systems in Safety-related Application,Part 1 (ISBN 0 11 883906 0) and(ISBN 0 11 883906 3)

[13] CECR-184 Personal Safety in Mcroprocessor Control Systems(Elektronikcentralen,Denmark)

更多出版物

[14] GB 1251.1 人类工效学 公共场所和工作区域的险情信号 险情听觉信号

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

[16] GB 1251.3 人类工效学 险情和信息的视听信号体系

[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/T 4208 外壳防护等级(IP代码)

[20] GB 5226.1—2008 机械电气安全 机械电气设备 第1部分:通用技术条件

[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/T 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(所有部分) 可编程序控制器

[25] GB/T 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/T 18209(所有部分) 机械安全 指示、标志和操作

[30] GB/T 18831 机械安全 与防护装置相关的联锁装置 设计和选择原则

[31] GB/T 19001 质量管理体系 要求

[32] GB/T 19670 机械安全 防止意外启动

[33] GB/T 19671 机械安全 双手操纵装置 功能状况和设计原则

[34] 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

[35] GB/T 20438.2—2017 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

[36] 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

[37] GB 28526—2012 机械电气安全 安全相关电气、电子和可编程电子控制系统的功能安全

[38] ISO 9355-1 Ergonomic requirements for the design of displays and control actuators—Part 1:Human interactions with displays and control actuators

[39] ISO 9355-2 Ergonomic requirements for the design of displays and control actuators—Part 2:Displays

[40] ISO 9355-3 Ergonomic requirements for the design of displays and control actuators—Part 3:Control actuators

[41] ISO 19973(all parts) Pneumatic fluid power Assessment of component reliability by testing

[42] ISO/TR 24119 Safety of machinery—Evaluation of fault masking serial connection of interlocking devices associated with guards with potential free contacts

[43] IEC 60947(all parts) Low-voltage switchgear and controlgear

[44] IEC 61810(all parts) Electromagnetic elementary relays

[45] IEC 61300(all parts) Fibre optic interconnecting devices and passive components—Basic test and measurement procedures

[46] IEC 61326-3-1 Electrical equipment for measurement,control and laboratory use—EMC requirements—Part 3-1:Immunity requirements for safety-related systems and intended to perform safety-related functions(functional safety)—Generalindustrial applications

[47] EN 457 Safety of machinery—Auditory danger signals—General requirements,design and testing

[48] EN 614-1 Safety of machinery—Ergonomic design principls—Part 1:Terminology and general principles

[49] EN 982 Safety of machinery—Safety requirements for fluid power systems and their components—Hydraulic

[50] EN 983 Safety of machinery—Safety requirements for fluid power systems and their components—Pneumatic

[51] EN 1005-3 Safety of machinery—Human physical performance—Part 3:Recommended force limits for machinery operation

[52] EN 1088 Safety of machinery—Interlocking devices associated with guards—Principles for design and selection

[53] EN 50205 Relays with forcibly guided(mechanically linked) contacts

[54] SN 29500(all parts) Failure rates of components

[55] GOBLE W.M.Control systems—Evaluation and Rehability.2nd Edition.Instrument Society of America(ISA),North Carolina,1998

[56] BGIA-Report 2/2008e Functional safety of machine controls—Application of ISO 13849, German Social Accident Insurance(DGUV),June 2009,ISBN 978-3-88383-793-2,free download in the Internet:www.dguv.de/ifa/13849e

数据库

[57] SN 29500 Failure rates of components,Edition 1999-11,Siemens AG

[58] IEC/TR 62380 Reliability data handbook—Univeral model for reliability rediction of electronics components,PCBs and equipment[4)]

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

[60] Reliability Prediction Procedure for Electronic Equipment,Telcordia SR-332,Issue 01,May 2001(telecom-info.telcordia.com),Bellcore TR-332,Issue 06

[61] EPRD,Electronic Parts Reliability Data(RAC-STD-6100),Reliability Analysis Centre,201 Mill Street,Rome,NY 13440

[62] NPRD-95,Non-electronic Parts Reliability Data(RAC-STD-6200),Reliability Analysis Centre, 201 Mill Street,Rome,NY 13440

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

[64] 中国军用标准,GJB/z 299B

4) Identical to RDF 2000/Reliability Data Handbook,UTE C 80-810,Union Technique de I'Electricité et de la Communication.

中 华 人 民 共 和 国
国 家 标 准
机械安全 控制系统安全相关部件
第 1 部分:设计通则
GB/T 16855.1—2018/ISO 13849-1:2015
*
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(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2018 年 12 月第一版
*
书号:155066·1-61771

GB/T 16855.1-2018

GB/T 16855.1—2018/ISO 13849-1:2015