ICS 13.110
J 09

中华人民共和国国家标准

GB/T 16855.2—2015/ISO 13849-2:2012
代替 GB/T 16855.2—2007

机械安全　控制系统安全相关部件
第 2 部分:确认

Safety of machinery—Safety-related parts of control systems—
Part 2:Validation

(ISO 13849-2:2012,IDT)

2015-12-10 发布　　2016-07-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 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2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 16855.2—2007《机械安全　控制系统有关安全部件　第2部分：确认》。与GB/T 16855.2—2007相比，除编辑性修改外主要技术变化如下：

——在范围中增加了适用于对性能等级的确认(见第1章，2007年版的第1章)；

——增加了安全功能的安全要求规范的确认(见第7章)；

——增加了性能等级及其相关参数($MTTF_d$、DC_{avg}和CCF)、安全相关软件的确认(见第9章，2007年版的第1章)；

——增加了技术文件和使用信息的确认(见第12章)；

——增加了故障特性确认及诊断措施示例(见附录E)。

本部分使用翻译法等同采用ISO 13849-2:2012《机械安全　控制系统安全相关部件　第2部分：确认》(英文版)。

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：如皋市包装食品机械有限公司、国家机床质量监督检验中心、南京理工大学、欧姆龙自动化(中国)有限公司、中机生产力促进中心、南京林业大学光机电仪工程研究所、皮尔磁工业自动化贸易(上海)有限公司、ABB(中国)有限公司、西门子(中国)有限公司。

本部分主要起草人：史传明、居里锴、赵钦志、张晓飞、李勤、宁燕、居荣华、李立言、褚卫中、张天强、罗广、程红兵、刘英、陈能玉、黄之炯、张亚荣、宋小宁、吴健、王正、付卉青、刘治永、姜涛、于恒。

本部分所代替标准的历次版本发布情况为：

——GB/T 16855.2—2007。

引　言

机械领域安全标准的结构如下：

——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 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 类标准(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。

根据 GB/T 15706，本标准属于 B1 类标准。

C 类标准可补充或修改本标准中的要求。

对于 C 类标准范围内的机器，如果已按照该标准设计与制造，则优先采用该 C 类标准中的要求。

本部分规定了控制系统安全相关部件的安全功能、类别和性能等级的确认过程。本部分认识到通过分析(见第 5 章)和测试(见第 6 章)的组合可实现控制系统安全相关部件的确认，并规定了试验的特殊环境条件。

本部分规定的大多数程序和条件都是基于一种假设，即采用了 GB/T 16855.1—2008 中 4.5.4 规定的估计性能等级(PL)的简化程序。本部分没有给出采用其他程序(例如：马尔科夫建模)的指南，这种情况下，本部分的某些条款不再适用，并且有必要满足附加的要求。

无论控制系统安全相关部件采用了何种技术(电气、液压、气动、机械等)，其设计通则(见 GB/T 15706)的指南都在 GB/T 16855.1 中给出。这包括一些典型安全功能的描述，所需的性能等级的确定，以及类别和性能等级的通用要求。

本部分给出的一部分确认要求是通用性的，而其他确认要求则是专门针对所采用的技术类型。

机械安全　控制系统安全相关部件
第2部分:确认

1　范围

本部分规定了通过分析和测试确认以下参数时需遵循的程序和条件:

——规定的安全功能;

——按照GB/T 16855.1设计的控制系统安全相关部件(SRP/CS)达到的类别;

——按照GB/T 16855.1设计的控制系统安全相关部件(SRP/CS)达到的性能等级。

注:可编程电子系统(包括嵌入式软件)的附加要求在GB/T 16855.1—2008的4.6和GB/T 20438中给出。

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 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 16855.1—2008　机械安全　控制系统有关安全部件　第1部分:设计通则(ISO 13849-1:2006,IDT)

3　术语和定义

GB/T 15706—2012和GB/T 16855.1—2008界定的术语和定义适用于本文件。

4　确认过程

4.1　确认原则

确认过程的目的是为了确定SRP/CS的设计是否支持机械的所有安全要求规范。

确认应证明每个SRP/CS满足GB/T 16855.1的要求,特别是:

a)　设计原理提出的,由该部件所提供的安全功能的规定安全特性。

b)　规定的性能等级的要求(见GB/T 16855.1—2008中4.5):

　1)　规定的类别的要求(见GB/T 16855.1—2008中6.2);

　2)　控制和避免系统性失效的措施(见GB/T 16855.1—2008中附录G);

　3)　适用时,软件的要求(见GB/T 16855.1—2008中4.6);

　4)　在预期环境条件下执行安全功能的能力。

c)　操作者界面的人类工效学设计,例如,不会因此诱使操作者采用危险的操作方式,如废弃SRP/CS(见GB/T 16855.1—2008中4.8)。

宜由独立于SRP/CS设计的人员进行确认。

注:"独立人员"并不意味着需要第三方测试。

确认包括分析确认(见第5章),以及按照确认计划在可预见的条件下进行的功能测试(见第6章)。图1给出了确认过程。分析与测试之间的平衡取决于安全相关部件所采用的技术和所需的性能等级。

对于 2 类、3 类和 4 类，安全功能的确认还应包括故障条件下的测试。

宜尽可能早地启动分析工作，并与设计过程同时进行，以便能尽早在问题还相对容易解决的时候解决，即在“安全功能的设计和技术实现”和“评估性能等级 PL”这两步之间（GB/T 16855.1—2008 中图 3 第四个方框与第五个方框之间）。部分分析工作有必要推迟到设计完成后进行。

由于控制系统的规模、复杂性或者集成到（机器的）控制系统中产生的效果，在必要时，宜作如下的专门安排：

——在集成前单独对 SRP/CS 进行确认，包括模拟相应的输入和输出信号；

——确认安全相关部件与控制系统内其余部分的集成效果。

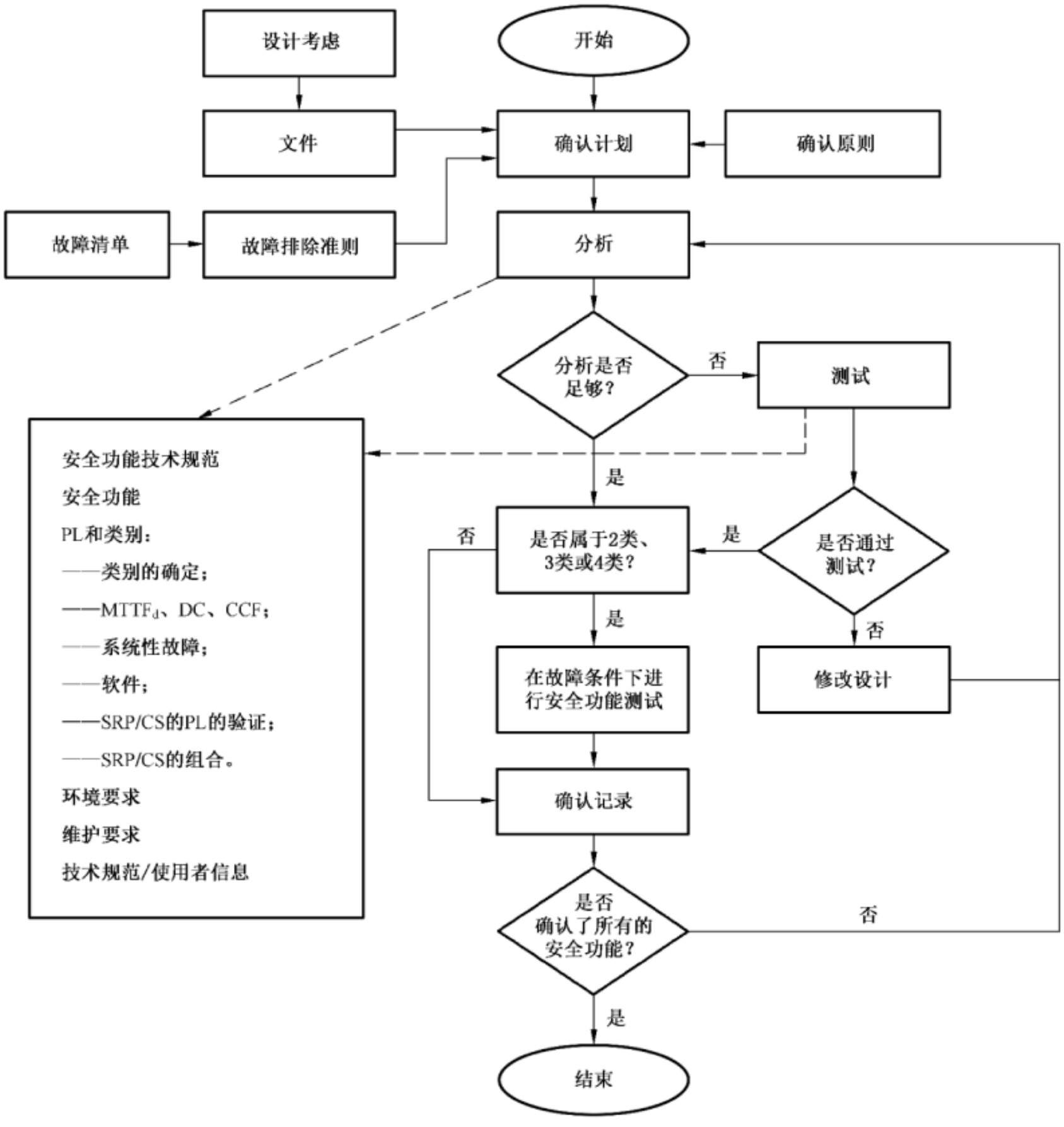


图 1　确认过程

图 1 中的“修改设计”是指设计过程。如果无法成功完成确认，则有必要改变设计。然后，还宜对修改后的安全相关部件重新进行确认。宜重复此过程，直到所有安全功能的安全相关部件均已成功完成确认。

4.2　确认计划

确认计划应识别和描述对规定的安全功能及其类别和性能等级进行确认过程的要求。

确认计划还应识别用于确认规定安全功能、类别和性能等级的方法。适当时，应规定以下内容：

a) 识别技术规范文件；

b) 测试过程中的操作和环境条件；

c) 需要进行的分析和测试；

d) 适用的测试标准；

e) 确认过程中每一步骤的负责人或单位。

此前已按相同技术规范确认过的安全相关部件只需要引用此前的确认即可。

4.3 一般故障清单

确认过程包括考虑 SRP/CS 在所有考虑的故障条件下的性能。故障考虑的基础是附录 A～附录 D 中根据经验以表格形式给出的故障清单。这些表格包括：

——元件/组件，如导线/电缆(见附录 D)；

——故障，如导体间短路；

——允许的故障排除，考虑环境、操作和应用等因素；

——备注栏，给出故障排除的理由。

故障清单仅考虑永久性故障。

4.4 特殊故障清单

如有必要，应创建一个特殊的产品相关故障清单，作为安全相关部件确认过程的参考文件。此清单可以以附录中相应的一般故障清单为基础。

对于基于一般故障清单的特殊的产品相关故障清单，应规定以下内容：

a) 一般故障清单列出的故障；

b) 一般故障清单没有列出的其他相关故障(例如，共因失效)；

c) 一般故障清单中列出的，并且在满足一般故障清单中给出的准则(见 GB/T 16855.1—2008 中 7.3)的前提下可能可以排除的故障；

特殊情况下，还应包括：

d) 一般故障清单不允许排除的，但给出了排除理由和原理(见 GB/T 16855.1—2008 中 7.3)的其他故障。

对于不是基于一般故障清单的故障清单，设计者应给出故障排除的原理。

4.5 确认信息

随着所采用的技术、待证实的类别和性能等级、系统设计原理以及 SRP/CS 对风险减小的作用的变化，确认所需要的信息也将随之改变。在确认过程中应包括含有以下足够信息的文件，以证实安全相关部件执行规定安全功能能达到所需的的性能等级和类别：

a) 每种安全功能所需特征的技术规范，以及其所需的类别和性能等级；

b) 图样和技术文件，例如，机械、液压和气动部件、印刷线路板、装配面板、内部布线、外壳、材料和安装的图样和技术文件；

c) 带功能描述框的框图；

d) 电路图，包括接口/连接；

e) 电路图的功能描述；

f) 开关元件的时序图、安全相关的信号；

g) 已确认元件相关特性的描述；

h) 对于在 g)中没有列出的安全相关部件，列出名称、额定值、允差、相关的操作力、型号规格、失

效率数据、元件制造商以及其他安全相关数据的元件清单；

i) 所有相关故障的分析(也可见 4.3 和 4.4)，例如：附录 A～附录 D 的表格中列出的故障，包括所有已排除故障的理由；

j) 被加工材料影响的分析；

k) 使用信息，如安装和操作手册/说明书。

如果软件与安全功能相关，则软件的文件应包括：

——明确无误的技术规范，并规定软件需要达到的安全性能；

——软件的设计能达到所需的性能等级的证据(见 9.5)；

——用于证明达到了所需的性能等级的试验的细节(尤其是试验报告)。

注：软件的要求见 GB/T 16855.1—2008 中 4.6.2 和 4.6.3。

应提供如何确定性能等级以及每小时危险失效平均概率的信息。可量化因素的文件应包括：

——安全相关的模块图(见 GB/T 16855.1—2008 中附录 B)或者指定结构(见 GB/T 16855.1—2008 中 6.2)；

——$MTTF_d$、DC_{avg}以及 CCF 的确定；

——类别的确定(见表 1)。

应提供关于 SRP/CS 系统方面的文件信息。

应提供如何将若干 SRP/CS 组合来达到所需要的性能等级的信息。

表 1 与性能等级有关的类别的文件要求

文件要求	需要文件的类别				
	B	1	2	3	4
基本安全原则	×	×	×	×	×
预期操作力	×	×	×	×	×
被加工材料的影响	×	×	×	×	×
受其他相关外部影响时的性能	×	×	×	×	×
经验证的元件	—	×	—	—	—
经验证的安全原则	—	×	×	×	×
各通道平均危险失效时间($MTTF_d$)	×	×	×	×	×
安全功能的检查程序	—	—	×	—	—
执行的诊断措施，包括故障反应	—	—	×	×	×
检查间隔，如有规定	—	—	×	×	×
诊断覆盖率(DC_{avg})	—	—	×	×	×
设计时考虑的可预见单一故障和采用的检测方法	—	—	×	×	×
已识别的共因失效(CCF)及预防方法	—	—	×	×	×
可预见的单一故障排除	—	—	—	×	×
待检测的故障	—	—	×	×	×
每种故障条件下如何保持安全功能	—	—	—	×	×
每种组合故障条件下如何保持安全功能	—	—	—	—	×
防止系统性故障的措施	×	×	×	×	×
防止软件故障的措施	×	—	×	×	×
× ——需要文件； — ——不需要文件。					
注：类别是指 GB/T 16855.1—2008 中给出的类别。					

4.6 确认记录

应记录通过分析和测试进行的确认。记录应反映各项安全要求的确认过程。如果以前的确认记录有效,也可以引用。

对于确认过程中未通过确认的安全相关部件,确认记录应描述哪些组件没有通过分析/测试确认。应确保在修改后所有安全相关部件均已重新确认。

5 分析确认

5.1 一般要求

应通过分析对 SRP/CS 进行确认。分析的输入包括:

——风险分析识别出的安全功能及其特征,以及所需的性能等级(见 GB/T 16855.1—2008 中图 1 和图 3);

——可量化指标($MTTF_d$、DC_{avg}和 CCF);

——系统结构(如指定结构)(见 GB/T 16855.1—2008 中第 6 章);

——影响系统性能的不可量化的定性指标(适用时,包括软件);

——确定性论据。

相对于测试,通过分析来确认安全功能需要形成确定性论据。

注 1:确定性论据是基于定性指标(如制造质量、使用经验)的论据。这一方法取决于具体应用,并受到各种因素的影响。

注 2:确定性论据与其他证据的区别在于,它们表明所需的系统特征是根据系统模型进行逻辑推导得出的。此类论据可建立在简单易懂的概念基础上。

5.2 分析方法

分析方法的选择取决于具体目标。目前有如下两种基本方法:

a) 自上而下(演绎)的方法,适合于确定可导致顶事件的起始事件,并通过起始事件的概率计算顶事件的概率。该方法也可用于研究已识别的多重故障的因果关系。

示例:故障树分析(FTA,见 GB/T 7829)和事件树分析(ETA)。

b) 自下而上(归纳)的方法,适合于研究已识别的单一故障的因果关系。

示例:失效模式和影响分析(FMEA,见 GB/T 7826)和失效模式、影响及危害性分析(FMECA)。

6 测试确认

6.1 一般要求

在分析确认没有形成结论时,应通过测试来完成确认。测试往往是分析的补充,通常情况下也是必要的。

测试确认的计划和实施应遵循逻辑方法,尤其是:

a) 在开始测试之前应制定测试计划,包括:

1) 试验规范;

2) 符合规范所需的试验结果;

3) 试验的时间顺序。

b) 应形成测试记录,包括:

1) 测试人员的姓名;

2） 环境条件(见第 10 章)；

3） 测试程序和所使用的设备；

4） 测试日期；

5） 测试结果。

c） 应将测试记录和测试计划进行对比，以确保达到了规定的功能和性能目标。

试验样品应尽可能在与最终运行条件相似的条件下运行，即连接上所有的外围装置和外罩。

测试可由人工完成，也可自动完成，例如，通过计算机。

实际应用时，应向 SRP/CS 施加各种组合的输入信号来完成安全功能的测试确认。应将输出端的响应结果与相应规定的输出结果进行比较。

建议向控制系统和机器系统地施加这些组合输入信号，例如，电源接通、启动、操作、方向改变、重新启动。必要时，为了观察 SRP/CS 在反常或不正常的情况下的响应，应扩展输入数据的范围。此类输入数据的组合应考虑可预见的误操作。

测试目标决定了测试的环境条件。环境条件可以是以下一种：

——预定使用的环境条件；

——特殊的特定条件；

——给定的条件范围(如果存在漂移)。

宜由操作者与负责进行测试的人员协商确定可以认为是稳定的且测试有效的条件范围，并做记录。

6.2 测量精度

通过测试进行确认的过程中，测量精度应与试验相适应。一般情况下，应保证温度的测量精度在 5 ℃ 以内，并保证以下参数的测量精度在 5%以内：

a） 时间；

b） 压力；

c） 力；

d） 电气参数；

e） 相对湿度；

f） 线性。

如果与上述测量精度有偏差，应说明理由。

6.3 更严格的要求

如果随行文件对 SRP/CS 提出的要求高于本部分规定的要求，则应采用更严格的要求。

注：如果控制系统不得不经受特别恶劣的工作条件时，如野蛮操作、湿度影响、水解、环境温度变化、化学制剂影响、腐蚀、因靠近发射装置造成的高强度电磁场等，则可采用更严格的要求。

6.4 试验样品数量

除非另有规定，否则安全相关部件的测试应采用单个产品样品进行。

不应修改测试过程中的安全相关部件。

某些测试可使某些元件的性能发生永久的改变。如果元件的永久性改变使得安全相关部件不能满足后续测试的要求时，应采用新的样品进行后续测试。

如果某一特定测试为破坏性试验，且通过对 SRP/CS 的部件进行单独测试可得到相同的结果，则为了得到测试结果，可采用该部件的样品来代替安全相关部件进行测试。只有分析表明，对安全相关部件的测试已足以证明执行安全功能的整个安全相关部件的安全性能，才能使用这种方法。

7 安全功能的安全要求规范的确认

在确认提供安全功能的 SRP/CS 或 SRP/CS 组合的设计之前，应先验证安全功能的安全要求规范是否能确保其预定用途的一致性和完整性。

由于安全要求是其他活动的基础，因此在开始设计之前宜分析安全要求规范。

应确保对机器控制系统所有安全功能的要求都编制了文件。

为了确认这些规范，应采用相应措施防止系统性故障(错误、疏漏或不一致)。

可以通过审查和检查 SRP/CS 的安全要求和设计规范来完成确认，特别是证明已考虑了以下各个方面：

——预定用途的要求和安全需求；

——操作条件和环境条件，以及可能的人为错误(如误用)。

如果产品标准规定了设计 SRP/CS 的安全要求(如适用于集成制造系统的 GB 16655 或适用于双手操纵装置的 GB/T 19671)，也应考虑这些标准。

8 安全功能的确认

安全功能的确认应证明提供安全功能的 SRP/CS 或 SRP/CS 组合符合所规定的特征。

注 1：不存在硬件故障时，设计和集成阶段造成的错误(如对安全功能特征错误的理解、逻辑设计错误、硬件装配错误、软件代码输入错误等)导致的系统性故障可使安全功能丧失。这些系统性故障中的一部分将在设计阶段暴露出来，而其他系统性故障将在确认过程暴露，或者还是没有被发现。此外，确认过程也可能发生错误(如没有检查到某些特性)。

应采用以下列出的相应措施确认安全功能的规定特征：

——图表功能分析、软件审查(见 9.5)；

注 2：如果机器的安全功能很复杂或数量众多，分析能够减少所需功能试验的数量。

——模拟；

——检查安装在机器上的硬件元件，以及相关软件的详细资料，以确定其与文件的一致性(如制造、类型、版本)；

——在机器所有操作模式下对安全功能进行功能测试，以确定其是否满足规定特征(某些典型安全功能的技术规范，见 GB/T 16855.1—2008 中第 5 章)，功能测试应保证在整个范围内实现了所有安全相关的输出，并按照技术规范的要求响应安全相关输入，测试案例通常来源于技术规范，但某些案例也有可能来源于对图表或软件的分析；

——进行延伸功能测试，以检查是否存在来自输入端的可预见的异常信号或信号组合，包括动力中断和恢复，以及不正确的操作；

——检查操作者-SRP/CS 界面是否符合人类工效学原则(见 GB/T 16855.1—2008 中 4.8)。

注 3：防止系统性失效的其他措施在 9.4 中给出(如多样性、通过自动测试检测失效)，这些措施也有助于检测功能故障。

9 性能等级和类别的确认

9.1 分析和测试

对于提供安全功能的 SRP/CS 或 SRP/CS 组合，其确认应证明满足了安全要求规范中的所需的性能等级(PL_r)和类别。原则上，这需要采用电路图进行失效分析(见第 5 章)，并且在失效分析无法得到

结果时，应：

——在实际电路上进行故障插入试验，并对实际元件进行故障触发试验，尤其是系统中对失效分析所获得的结果存在疑问的元件（见第 6 章）；

——模拟控制系统发生故障时的工况，如采用硬件和/或软件模型。

在某些应用中，可能有必要把相连的安全相关部件分为几个功能组，并对这些功能组及其接口进行故障模拟试验。

通过测试进行确认时，根据实际情况，试验宜包括以下内容：

——对产品样品进行故障插入试验；

——对硬件模型进行故障插入试验；

——故障的软件模拟；

——子系统失效，如动力源。

将故障插入到系统的准确时刻非常关键。应通过分析确定故障插入的最坏影响，并在此关键时刻插入故障。

9.2 类别规范的确认

9.2.1 B 类

B 类 SRP/CS 的确认应根据基本安全原则（见表 A.1、表 B.1、表 C.1 和表 D.1）证明元件的规范、设计、制造和选择符合 GB/T 16855.1—2008 中 6.2.3 的要求。应证明通道的 $MTTF_d$ 至少为 3 年。这可以通过检查 SRP/CS 是否符合确认文件中提出的相应规范来实现（见 4.5）。环境条件的确认见 6.1。

注：特殊情况下，可要求更高的 $MTTF_d$ 值，如当 $PL_r = b$ 时。

9.2.2 1 类

1 类 SRP/CS 的确认应证明：

a) 它们满足 B 类的要求；

b) 如果元件至少满足下列条件之一，则说明元件是经验证的（见表 A.3 和表 D.3）：

1) 在类似使用条件下已有广泛成功的应用；

2) 元件的制造和验证采用了证明其与安全相关的应用相适应并且可靠的原则；

c) 已经正确实施经验证的安全原则（适当时，见表 A.2、表 B.2、表 C.2 和表 D.2），并且如果采用了新制定的原则，则应对以下内容进行确认：

1) 如何避免预期的失效模式；

2) 故障是如何避免的，或如何降低其发生概率。

可以利用相关的元件标准来证明与此条款的符合性（见表 A.3 和表 D.3）。应证明通道的 $MTTF_d$ 至少为 30 年。

9.2.3 2 类

2 类 SRP/CS 的确认应证明：

a) 它们符合 B 类的要求；

b) 所采用的经验证的安全原则（如果适用）满足 9.2.2c）的要求；

c) 在设备检查过程中，逐一检测所有相关故障并产生合适的控制动作，该动作：

1) 触发安全状态；

2) 或者在不可能触发安全状态时，提供对危险的警告；

d) 设备检查本身不会造成不安全状态；

e) 开始进行检查的时间是：

1) 在机器启动时或在触发危险状态之前；

2) 如果风险评估和操作类型表明有必要，则在运行期间按照设计规范定期进行检查；

注 1：在操作期间进行检查的需求和程度由设计者的风险评估和必要的操作类型确定。

f) 功能通道($MTTF_{d,L}$)的 $MTTF_d$ 至少为 3 年；

g) $MTTF_{d,TE}$ 大于 $MTTF_{d,L}$ 的一半；

h) 检测频率大于或等于预期要求频率的 100 倍；

i) DC_{avg} 至少为 60%；

j) 已充分减小共因失效(见 GB/T 16855.1—2008 中附录 F)。

注 2：特殊情况下，可要求更高的 $MTTF_d$ 和/或 DC_{avg}，如由于 PL_r 较高时。

9.2.4 3 类

3 类 SRP/CS 的确认应证明：

a) 它们符合 B 类的要求；

b) 所使用经验证的安全原则(如果适用)满足 9.2.2c)的要求；

c) 单一故障不会造成安全功能的丧失；

d) 单一故障(包括共因故障)按照设计原理和所使用的技术进行检测；

e) 各通道的 $MTTF_d$ 至少为 3 年；

f) DC_{avg} 至少为 60%；

g) 已充分减小共因失效(见 GB/T 16855.1—2008 中附录 F)。

注：特殊情况下，可要求更高的 $MTTF_d$ 和/或 DC_{avg}，如由于 PL_r 值较高时。

9.2.5 4 类

4 类 SRP/CS 的确认应证明：

a) 它们符合 B 类的要求；

b) 所使用经验证的安全原则(如果适用)满足 9.2.2c)的要求；

c) 单一故障(包括共模故障)不会造成安全功能的丧失；

d) 单一故障在下一次要求安全功能时或在下一次要求安全功能之前被检测到，这可通过 DC_{avg} 至少为 99%来实现；

e) 如果 DC_{avg} 至少为 99%时不能检测到单一故障，则故障的累积不会导致安全功能的丧失，且故障的累积程度符合设计原理；

f) 各通道的 $MTTF_d$ 至少为 30 年；

g) 已充分减小共因失效(见 GB/T 16855.1—2008 中附录 F)。

9.3 $MTTF_d$、DC_{avg} 和 CCF 的确认

$MTTF_d$、DC_{avg} 和 CCF 的确认通常通过分析和目视检查来完成。

应检查元件的 $MTTF_d$(包括 B_{10d}，T_{10d} 和 n_{op})的真实性(例如：是否符合 GB/T 16855.1—2008 中附录 C)。例如：将供应商数据表中给出的值与 GB/T 16855.1—2008 的附录 C 进行对比。当故障排除声明表明特殊元件不影响通道 $MTTF_d$ 值时，则应检查故障排除的可信度。

注 1：能够故障排除意味着元件的 $MTTF_d$ 无限大；因此，该元件将不影响通道 $MTTF_d$ 的计算。

注 2：对于 B_{10d} 的确定，见 GB 14048.4—2010 中附录 K 等。

应检查 SRP/CS 各通道 $MTTF_d$ 的计算是否正确，包括对不相似的冗余通道采用对称公式(见 GB/T 16855.1—2008 中附录 D)计算得出的 $MTTF_d$。应确保在采用对称公式计算之前，单个通道的

$MTTF_d$ 已严格限制在不超过 100 年。

应检查元件和/或逻辑模块 DC 值的真实性(例如:是否违背 GB/T 16855.1—2008 中附录 E 给出的措施)。应在典型的使用环境条件下,通过测试来确认是否正确实施检查和诊断(硬件和软件),包括相应的故障反应。

应检查 SRP/CS 的 DC_{avg} 计算是否正确。

应确认是否采用了足够的措施来防止共因失效(例如,是否符合 GB/T 16855.1—2008 中附录 F)。典型确认措施是在环境条件下进行的静态硬件分析和功能性测试。

注 3:对于电子元件 $MTTF_d$ 的计算,环境温度取+40 ℃作为基准。确认过程中,确保满足基准环境和功能条件(特别是温度)对于 $MTTF_d$ 是很重要的。当设备或元件的工作温度明显高于(如超过 15 ℃)规定的+40 ℃时,则有必要采用较高环境温度的 $MTTF_d$ 值。

9.4 与 SRP/CS 性能等级和类别相关的系统性失效防止措施的确认

与 SRP/CS 性能等级和类别相关系统性失效(定义见 GB/T 16855.1—2008 中 3.1.7)的防止措施的确认通常可采用以下方式:

a) 检查设计文件,以确定:
   1) 是否应用基本的和经验证的安全原则(见附录 A~附录 D);
   2) 是否采取进一步措施避免系统性失效(见 GB/T 16855.1—2008 中 G.3);
   3) 是否采取进一步措施控制系统性失效,如硬件多样性(见 GB/T 16855.1—2008 中附录 G)、防修改保护或失效断言编程;
b) 失效分析(如 FMEA);
c) 故障插入试验/故障触发;
d) 如果使用了数据通讯,则进行检查和测试;
e) 检查质量管理体系是否能够在生产过程中避免系统性失效。

9.5 安全相关软件的确认

安全相关嵌入式软件(SRESW)和安全相关应用软件(SRASW)的确认应包括:

——软件在目标硬件上执行时规定的功能动作和性能准则(如定时性能);

——验证采用软件措施是否足以达到安全功能规定的 PL_r;

——软件开发过程中为避免系统性软件故障所采取的措施和行动。

首先应检查是否对安全相关软件的技术规范和设计文件进行文件编制,并审查这些文件的完整性,且不存在错误理解、疏漏或矛盾。

注:对于小程序,利用软件的文件(控制流程图、模块或块的源代码、I/O 或变量分配表、对照表)通过控制流程或程序的审查或走查进行分析就足够了。

一般来说,软件可看作是“黑盒子”或“灰盒子”(见 GB/T 16855.1—2008 中 4.6.2),并可分别用黑盒子或灰盒子试验来确认。

根据 PL_r[GB/T 16855.1—2008 中 4.6.2(针对 SRESW)和 4.6.3(针对 SRASW)],试验宜包括:

——功能动作和性能(如定时性能)的黑盒子试验;

——基于限值分析的附加延伸试验项目,推荐用于 PLd 或 PLe;

——I/O 试验,以确保安全相关输入和输出信号的正确使用;

——模拟事先通过分析方法确定的故障以及预期响应的试验项目,其目的是为了评价基于软件的失效控制措施是否充分。

已确认过的单独软件功能不需要再次确认,但是,如果针对具体项目而将这里多个此类安全功能块组合在一起时,则应确认最终的总体安全功能。

应检查软件的文件，以确定是否按照简化的 V 模型(GB/T 16855.1—2008 中图 6)采取足够的措施和行动来防止系统性软件故障。

应检查针对软件采取的符合 GB/T 16855.1—2008 中 4.6.2(针对 SRESW)和 4.6.3(针对 SRASW)的措施是否得到正确实施，这些措施取决于需要达到的 PL。

如果其后对安全相关软件进行了修改，应在相应的范围内进行再次确认。

9.6 性能等级的确认和验证

采用简化程序按照 GB/T 16855.1—2008 中 4.5.4，以及 GB/T 16855.1—2008 中附录 B～附录 F 和附录 K 估计 SRP/CS 的 PL 时，应进行以下验证和确认：

——检查根据类别、DC_{avg} 和 $MTTF_d$ 确定的 PL 是否正确(按照 GB/T 16855.1—2008 中 4.5.4 和附录 K)；

——验证 SRP/CS 达到的 PL 是否满足机械的安全要求规范所需的性能等级(PL_r)，即：$PL \geqslant PL_r$。

基于估计的平均每小时危险失效概率，采用其他方法来评价达到的 PL 时，确认过程应考虑：

——各元件的 $MTTF_d$ 值；

——DC；

——CCF；

——结构；

——检查文件、应用、计算是否正确。

9.7 安全相关部件组合的确认

如果安全功能由两个或两个以上的安全相关部件实现，则应通过分析和必要的测试对该组合进行确认，确保该组合满足设计规定的性能。可以考虑采用已有的安全相关部件的确认记录结果。应进行以下确认步骤：

——检查描述总体安全功能的设计文件；

——检查根据每个单独的安全相关部件确定的 SRP/CS 组合总体 PL(按照 GB/T 16855.1—2008 中 6.3)是否正确；

注：所有组合的 SRP/CS 的每小时平均危险失效率的总和可代替 GB/T 16855.1—2008 的表 11。检查系统、结构和 CCF 方面的不可量化限制是很重要的，因为这些不可量化限制可把总体性能等级限制在较低的值。

——接口特征的考虑，如电压、电流、压力、信息的数据格式、信号电平；

——与组合/集成相关的失效分析，如通过 FMEA；

——针对冗余系统，组合/集成相关的故障插入试验。

10 环境要求的确认

设计中规定的 SRP/CS 性能应在控制系统规定的环境条件下进行确认。

确认应通过分析和必要的测试来完成。分析和测试的范围取决于安全相关部件及其安装所在的系统，所采用的技术，以及需要确认的环境条件。采用系统或其元件的运行可靠性数据，或者确定是否符合相应的环境标准(如防水、防振)，可有助于确认过程。

适当时，确认应针对：

——因冲击、振动、污染物进入产生的预期机械应力；

——机械耐久性；

——额定电功率以及动力源；

——气候条件(温度和湿度);

——电磁兼容性(抗扰度)。

当需要通过试验来确定是否符合环境要求时,则应遵循相关标准规定的,以及具体应用要求的程序进行。

通过测试完成确认之后,安全功能应仍然符合安全要求的技术规范,或者 SRP/CS 应能提供安全状态的输出信号。

11 维护要求的确认

确认过程应证明已满足了 GB/T 16855.1—2008 中第 9 章第二段规定的维护要求。

维护要求的确认应包括:

a) 使用信息的审查,以确认:

1) 维护手册的内容是否完整[包括程序、需要的工具、检查的频率、更换磨损元件的时间间隔(T_{10d})等],且容易理解;

2) 适当时,是否存在只能由技能熟练的维护人员完成维护的要求;

b) 检查是否采用了便于维护的措施(如提供诊断工具来帮助故障查找和修理)。

此外,适用时,还应包括以下措施:

——防止维护过程中发生错误的措施(如通过真实性检查检测错误的输入数据);

——防止篡改的措施(如设置密码防止未经授权人员进入程序)。

12 技术文件和使用信息的确认

确认过程应证明满足了 GB/T 16855.1—2008 中第 10 章规定的技术文件要求,以及 GB/T 16855.1—2008 中第 11 章规定的使用信息要求。

附 录 A
（资料性附录）
机械系统的确认工具

当机械系统与其他技术结合使用时，还宜考虑附录 A。

表 A.1 和表 A.2 列出了基本安全原则和经验证的安全原则。

表 A.3 列出了适用于安全相关应用的经验证的元件，这些元件采用了经验证的安全原则和/或符合特殊用途的标准。某些应用中的经验证元件可能不适用于其他应用。

表 A.4 和表 A.5 列出了故障排除及其原理。更多故障排除见 4.4。

发生故障的精确时刻很关键（见 9.1）。

表 A.1 基本安全原则

基本安全原则	备 注
采用合适的材料以及适当的加工	材料、加工方法和处理方式的选择与应力、耐久性、弹性、摩擦、磨损、腐蚀、温度等有关
正确的尺寸和外形	考虑应力、张力、疲劳、表面粗糙度、公差、黏性、制造等因素
元件/系统的正确选择、组合、布置、装配和安装	使用制造商的操作说明书，如目录表、安装说明、技术规范和在类似元件/系统的成功应用实例等
失能原则的使用	通过能量释放得到安全状态。有关停止的主要操作见 GB/T 15706—2012 中 6.2.11.3。 提供的能量用于启动机构的运动。有关启动的主要操作见 GB/T 15706—2012 中 6.2.11.3。 考虑不同的模式，如操作模式、维修模式。 **重要——失去能量可能产生危险时无需遵循此原则，如失去夹持力时导致工件被释放**
正确的紧固	采用螺钉锁紧时，考虑制造商的操作说明书。 使用适当的扭矩加载技术可以避免过载，并实现充分防松
力及类似参数的产生和/或传输限制	例如安全销、安全片、扭矩限制离合器。 **重要——元件的持续完整性是保持所需控制水平的关键时，无需遵循此原则**
环境参数范围的限制	例如安装位置的温度、湿度、污染等。见第 10 章并考虑厂商的操作说明书
速度及类似参数的限制	考虑应用所需要的速度、加速、减速等
正确的反应时间	考虑弹簧疲劳度、摩擦、润滑、温度、加速和减速过程中的惯性、组合公差等
防止意外启动	考虑不同模式（操作模式、维护模式等）下，由于储能或恢复动力源引起的意外启动。 有必要通过特殊装置来释放储能。 在特殊应用中，如夹持装置或保证一定位置需要保持的能量，需要单独考虑
简化	避免安全相关系统中不必要的元件
分离	安全相关功能与其他功能分开
正确的润滑	考虑是否需要润滑装置，以及关于润滑剂和润滑间隔的信息
流体和灰尘进入的正确防护	考虑 IP 等级（见 GB 4208）

表 A.2　经验证的安全原则

经验证的安全原则	备　　注
采用经仔细选择的材料和制造方法	选择与应用相关的合适材料、适当的制造方法和和处理方法
使用具有定向失效模式的元件	事先知道元件的主要失效模式，并且失效模式通常是相同的，见 GB/T 15706—2012 中 6.2.12.3
裕量/安全系数	安全系数由标准给出或由安全相关良好经验得出
安全位置	元件的可移动部分通过机械方式（仅靠摩擦是不够的）保持在安全位置。需要施加力才能从安全位置移开
加大关闭力	获得安全位置/状态通过增大的关闭力实现，所谓增大是相对于打开力而言的
仔细选择、组合、布置、装配以及安装与应用相关的元件/系统	—
仔细选择与应用相关的紧固	避免仅靠摩擦力
直接机械动作	为实现直接机械动作，需要执行安全功能的所有运动的机械元件和与之相连的元件一起运动，例如，通过凸轮直接断开电气开关的触点，而不是依靠弹簧。见 GB/T 15706—2012 中 6.2.5
多重部件	通过并行的多重部件来降低故障的影响，例如，几个弹簧中的一个弹簧失效不会导致危险的状态
使用经验证的弹簧（也可见表 A.3）	经验证的弹簧要求： ——采用经仔细选择的材料、制造方法（如使用前的预调整和循环）和处理（例如轧制和喷丸硬化）； ——弹簧有足够的导向力； ——对于疲劳应力有足够的安全系数（即发生断裂的概率不大）。 也可能按以下要求设计成经验证的压簧： ——使用经仔细选择的材料、制造方法（如使用前的预调整和循环）和处理（例如碾压和喷丸硬化）； ——弹簧有足够的引导力； ——空载时，两圈间的空隙要小于弹簧丝直径； ——断裂后还保留足够的作用力（即断裂不会导致危险状态）。 **注**：首选压簧。
力及类似参数的限制范围	确定与经验和应用相关的必要限制。例如：安全销、安全片和扭矩限制离合器。 **重要——元件的持续完整性是保持所需控制水平的关键时，无需遵循此原则**
速度及类似参数的限制范围	确定与经验和应用相关的必要限制。例如，离心调速器、速度的安全监控、有限的位移
环境参数的限制范围	确定必要的限制。例如，安装位置的温度、湿度、污染。见第 10 章并考虑制造商的应用说明
反应时间的限制范围、有限的滞后	确定必要的限制。 考虑弹簧疲劳度、摩擦、润滑、温度、加速和减速过程中的惯性、组合公差等

表 A.3　经验证的元件

经验证的元件	“经验证的”条件	标准或技术规范
螺钉	考虑了所有影响螺钉连接的因素和应用。见表 A.2	机械连接所用的螺钉、螺母、垫圈、铆钉、销、螺栓等都是标准的
弹簧	见表 A.2,“使用经验证的弹簧”	ISO 4960 中给出了弹簧钢和其他特殊应用的技术规范
凸轮	考虑了所有影响凸轮布置(如联锁装置的部件)的因素。 见表 A.2	见 GB/T 18831(联锁装置)
安全销	考虑了所有影响应用的因素。见表 A.2	—

表 A.4　故障及故障排除——机械装置、元件及组件
(例如,凸轮、从动件、链条、离合器、刹车、轴、螺钉、销、导向装置、轴承)

故障	故障排除	备注
磨损/腐蚀	根据规定的使用寿命,在仔细选择材料、尺寸(裕量)、制造过程、处理方法和正确润滑的条件下,故障可排除(也可见表 A.2)	见 GB/T 16855.1—2008 中 7.3
泄漏/松动	根据规定的使用寿命,在仔细选择材料、制造过程、锁紧方法和处理方法的条件下,故障可排除(也可见表 A.2)	
断裂	根据规定的使用寿命,在仔细选择材料、尺寸(裕量)、制造过程、处理方法和正确润滑的条件下,故障可排除(也可见表 A.2)	
由过度应力引起的变形	根据规定的使用寿命,在仔细选择材料、尺寸(裕量)、处理方法和制造过程的条件下,故障可排除(也可见表 A.2)	
僵硬/粘连	根据规定的使用寿命,在仔细选择材料、尺寸(裕量)、制造过程、处理方法和正确润滑条件下,故障可排除(也可见表 A.2)	

表 A.5　故障及故障排除——压簧

故障	故障排除	备注
磨损/腐蚀	采用经验证的弹簧和仔细选择紧固件的条件下,故障可排除(见表 A.2)	见 GB/T 16855.1—2008 中 7.3
安装和断裂引起的压力减少		
断裂		
僵硬/粘连		
松动		
由过度应力引起的变形		

附 录 B
（资料性附录）
气动系统的确认工具

当气动系统与其他技术结合使用时，还宜考虑附录 B。气动元件为电气连接/控制时，宜考虑附录 D 中相应的故障清单。

注：国家相关法律法规中规定了附加要求。

表 B.1 和表 B.2 列出了基本安全原则和经验证的安全原则。

附录 B 未给出经验证的元件清单。“经验证的”状态主要取决于具体应用。如果元件满足 GB/T 16855.1—2008 中 6.2.2 和 ISO 4414:2010 中第 5 章～第 7 章的要求，则可认为是“经验证的”。某些应用中的经验证元件可能不适用于其他应用。

表 B.3～表 B.18 列出了故障排除及其原理。更多故障排除见 4.4。

发生故障的精确时刻是关键（见 9.1）。

表 B.1 基本安全原则

基本安全原则	备 注
采用合适的材料以及适当的加工	材料、加工方法和处理方式的选择与应力、耐久性、弹性、摩擦、磨损、腐蚀、温度等因素有关
正确的尺寸和外形	考虑应力、张力、疲劳、表面粗糙度、公差、加工等因素
元件/系统的正确选择、组合、布置、装配及安装	使用制造商的操作说明书，如目录表、安装说明、规范和在类似元件/系统的成功应用实例等
失能原则的使用	通过能量释放得到安全状态。有关停止的主要动作见 GB/T 15706—2012 中 6.2.11.3。 提供的能量用于启动机构的运动。有关启动的主要动作，见 GB/T 15706—2012 中 6.2.11.3。 考虑不同的模式，如操作模式、维修模式。 在某些应用中，此原则不适用，例如，气压损失将产生附加危险的场合
正确的紧固	采用锁紧螺钉、连接件、胶合、锁紧圈等进行紧固时，考虑制造商的操作说明书。 使用适当的扭矩加载技术可以避免过载
压力限制	例如：压力安全阀、泄压阀/控制阀
速度限制/速度降低	例如：通过流量阀和节流阀限制活塞速度
充分避免流体污染	考虑流体中固体微粒和水的过滤和分离
适当的转换时间范围	考虑管道长度、压力、排放能力、力、弹簧疲劳度、摩擦、润滑、温度、加速和减速过程中的惯性以及组合公差等
耐环境条件	在所有预期的环境和在任何可预见的不利条件下，如温度、湿度、振动、污染，所设计的装置都能工作。见第 10 章并考虑制造商的规范/操作说明书
防止意外启动	考虑不同模式下，例如，操作、维修模式，由于储能或恢复动力源引起的意外启动。 有必要通过特殊装置来释放储能（见 GB/T 19670—2005 中 5.3.1.3）。 对于特殊应用（例如夹持装置或保证一定位置需要保持的能量），需要单独考虑
简化	避免安全相关系统中不必要的元件
合适的温度范围	考虑整个系统
分离	安全相关功能与其他功能分开（如逻辑分离）

表 B.2　经验证的安全原则

经验证的安全原则	备　　注
裕量/安全系数	安全系数在标准中给出或由安全相关的良好经验得出
安全位置	元件的可移动部分通过机械方式(仅靠摩擦是不够的)保持在安全位置。 需要施加力才能从安全位置移开
加大关闭力	一种解决方案是滑阀移动到安全位置(关闭位置)的面积比明显大于滑阀移动到打开位置的面积比(安全系数)
通过载荷压力关闭阀门	通常是座阀,例如,提升阀、球阀。 考虑如何施加载荷压力,实现即使闭阀弹簧断裂,阀门依然关闭
直接机械动作	直接机械动作适用于气动装置内部的运动部分。也可见表 A.2
多重部件	见表 A.2
采用经验证的弹簧	见表 A.2
通过规定流量的控制来限速/减速	例如:固定的孔、固定的节流阀
力的限制/力的减小	可以通过一个经验证的泄压阀来实现,该泄压阀配备了尺寸合理并经正确选择的经验证的弹簧等
工作条件的合理范围	工作条件的限制,例如,宜考虑压力范围、流量和温度范围
正确避免流体污染	考虑流体中的固体颗粒与水是否需要高水平的过滤与分离
在滑阀中充分的正重叠	正重叠是确保停止功能和防止未经允许的移动
有限的滞后	例如,增加摩擦或组合公差将增加滞后

表 B.3　故障及故障排除——方向控制阀

故障	故障排除	备注
转换时间改变	只要驱动力足够大,且运动元件为直接机械动作,故障可排除(见表 A.2)	—
无转换(粘连在末端或零位置)或不完全转换(粘连在任意中间位置)	只要驱动力足够大,且运动元件为直接机械动作,故障可排除(见表 A.2)	
初始转换位置自发改变(没有输入信号)	只要保持力足够大,且运动元件为直接机械动作(见表 A.2),故障可排除;如果使用了经验证的弹簧(见表 A.2)并在正常安装和工作条件下使用(见备注),故障可排除;或者滑阀带弹性密封,且在正常的安装和工作条件下使用(见备注),故障可排除	满足以下条件即为在正常安装和工作条件下使用: ——考虑了制造商规定的条件; ——运动元件的重量不影响安全(如水平安装); ——没有反向惯性力作用到运动元件(如阀门运动方向考虑惯性力的大小和方向); ——没有产生极限振动和冲击应力
泄漏	只要表明带弹性密封的滑阀有足够的正重叠[见备注 1)],在正常的工作条件下使用,并且提供了足够的压缩空气处理和过滤方法,故障可排除;或者对于座阀,只要在正常的工作条件下使用[见备注 2)],并且对压缩空气做了充分处理和过滤,故障可排除	1)　在使用带弹性密封的滑阀的情况下,通常可排除因泄露产生的故障。然而,在长期使用后可能会发生少量的泄漏。 2)　满足制造商规定的条件即为在正常的工作条件下使用

表 B.3（续）

故障	故障排除	备注
长期使用后，因泄漏导致的流量改变	无	—
阀套爆裂或运动元件损坏，以及支架或压紧螺钉损坏/破裂	如果结构、尺寸和安装与良好的工程实践一致，故障可排除	
对于伺服阀和比例阀，引起不可控运动的气动故障	如果由于其设计和结构原因，伺服阀和比例方向阀从技术安全的角度可评估为常规的方向控制阀，故障可排除	—
注：如果控制功能是通过很多单一功能的阀门来实现，则宜对每个阀门进行故障分析。先导阀也宜按照与此相同的步骤进行。		

表 B.4 故障与故障排除——停止（关闭）阀/单向阀（止回）阀/速动通风阀/往复阀等

故障	故障排除	备注
转换时间改变	无	—
不能打开、不能完全打开、不能关闭或不能完全关闭（粘连在末端或任意的中间位置）	运动元件的导向系统是按照与不带阻尼系统非控制球座阀（见备注）类似的方式设计的，并且采用了经验证的弹簧（见表 A.2），故障可排除	对于不带阻尼系统的非控制球座阀，其导向系统的设计通常使得运动元件不可能发生粘连
初始转换位置自发改变（无输入信号）	在正常安装和工作条件（见备注）下，如果其提供的压力和面积使得关闭力足够，故障可排除	满足以下条件时，即为正常安装和工作条件： ——满足制造商规定的条件； ——没有特殊的惯性力影响运动元件，例如：运动的方向考虑了机器运动部件的运动方向； ——没有极限振动和冲击力产生
对于往复阀，两个输入的连接同时断开	如果运动元件的结构和设计使得不可能同时断开，故障可排除	—
泄漏	如果在正常工作条件下使用（见备注），对压缩空气做了充分处理和过滤，故障可排除	满足制造商规定的条件即为在正常的工作条件使用
长期使用后，因泄漏导致的流量改变	无	—
阀套爆裂或运动元件损坏，以及支架或压紧螺钉损坏/破裂	如果结构、尺寸和安装与良好的工程实践一致，故障可排除	

表 B.5　故障与故障排除——流量阀

故障	故障排除	备注
设定装置没有修改任何设定的情况下流量发生改变	对于不带运动元件[见备注 1)]的流量控制阀，如节流阀，如果在正常工作条件下使用[见备注 2)]，并且对压缩空气做了充分处理和过滤，故障可排除	1) 设定装置并不是运动元件。因为压差改变而引起的流量变化在这类阀门中受到物理上的限制，不属于此假定故障。 2) 满足制造商规定的条件即为在正常工作条件下使用
使用不可调节的圆孔和喷嘴时，流量发生改变	如果直径大于或等于 0.8 mm，在正常工作条件下使用[见备注 2)]，并且对压缩空气做了充分处理和过滤，故障可排除	
对于比例流量阀：由于意外改变设定值而引起流量变化	无	—
设定装置自发改变	如果根据技术安全规范在特定应用中对设定装置设置了有效保护，故障可排除	
设定装置的操作组件意外松开(旋松)	如果采用防止松开(旋松)的强制锁紧装置，故障可排除	
阀套爆裂或运动元件损坏，以及支架或压紧螺钉损坏/破裂	如果结构、尺寸和安装与良好的工程实践一致，故障可排除	

表 B.6　故障与故障排除——压力阀

故障	故障排除	备注
超过设定压力时，不能打开或打开不足(运动元件粘连或运动缓慢)[见备注 1)]	如果满足以下条件，则故障可排除： ——运动元件的导向系统与非控制球座阀或膜片阀的引导系统类似[见备注 2)]，例如带二级泄压的泄压阀； ——安装的弹簧是经验证的(见表 A.2)	1) 此故障只适用于用作施加力的压力阀，如夹紧； 此故障不适用于在气动系统中压力阀的正常功能，如压力限制、压力下降。 2) 对于非控制球座阀或膜片阀，导向系统的设计通常使得运动元件不可能粘连
压力降至设定值以下时，不能打开或打开不足(运动元件粘连或运动缓慢)[见备注 1)]		
设定装置没有修改设定的情况下，压力控制动作发生改变	对于直接驱动的压力限制阀和压力转换阀，如果安装的弹簧是经验证的，故障可排除(见表 A.2)	
对于比例压力阀：由于设定值的意外改变而引起压力控制动作改变[见备注 1)]	无	
设定装置自发改变	在满足应用要求的条件下，如果对设定装置进行有效保护，如铅封，故障可排除	—
设定装置的操作组件意外旋松	如果采用防止旋松的强制锁紧装置，故障可排除	
泄漏	在正常工作条件(见备注)下，对于座阀、膜片阀和带弹性密封的滑阀，如果对压缩空气做了充分处理和过滤，故障可排除	满足制造商规定的条件即为在正常工作条件下使用
长期使用后，泄漏流量改变	无	—
阀套爆裂或运动元件损坏，以及支架或压紧螺钉损坏/破裂	如果结构、尺寸和安装与良好的工程实践一致，故障可排除	

表 B.7　故障与故障排除——管道

故障	故障排除	备注
爆裂和泄漏	如果尺寸、材料的选择以及固定方式与良好的工程实践一致(见备注),故障可排除	使用塑料管时,有必要考虑制造商的数据,尤其是工作环境的影响,例如,热影响、化学影响或辐射影响。使用未经抗腐蚀处理的钢管时,提供充分干燥的压缩空气尤其重要
接头失效(如:开裂、泄漏)	如果采用咬入式管件或者螺纹管(即钢制接头、钢管),并且尺寸、材料的选择、制造、结构和固定方式与良好的工程实践一致,故障可排除	—
堵塞(阻塞)	对于动力回路中的管道,故障可排除。 对于控制和测量管道,如果公称直径大于或等于 2 mm,故障可排除	
小公称直径塑料管的弯结	如果采用合理的保护和安装并考虑了相关的制造商数据,例如最小弯曲半径,故障可排除	

表 B.8　故障与故障排除——软管总成

故障	故障排除	备注
泄露以及连接附件的爆裂、磨损	如果软管总成采用了按照 GB/T 15329.1 制造的软管,或者采用了带有相应软管附件的类似软管(见备注),故障可排除	以下情况下不能排除故障: ——预期寿命过期; ——强化措施产生疲劳; ——无法避免外部损伤
堵塞(阻塞)	对于动力回路中的软管总成,故障可排除。 对于用于控制和测量的软管总成,如果公称直径大于或等于 2 mm,故障可排除	—

表 B.9　故障与故障排除——连接器件

故障	故障排除	备注
螺钉破裂、断裂或者螺纹齿折断	如果尺寸、材料的选择、结构,以及与管道和/或管道/软管附件的连接与良好的工程实践一致,故障可排除	—
泄露(气密损失)	无	由于磨损、老化、弹性退化等原因,长期使用后不可能排除故障。假定不会发生重大的突发性气密失效
堵塞(阻塞)	对于动力回路中的连接器件,故障可排除。 对于用于控制和测量的连接器件,如果公称直径大于或等于 2 mm,故障可排除	—

表 B.10　故障与故障排除——压力变送器和介质压力传感器

故障	故障排除	备注
压力舱气密性/油密性的损失或改变	无	—
压力舱爆裂，以及附件和外壳用螺钉的破裂	如果尺寸、材料的选择、结构和附件与良好的工程实践一致，故障可排除	

表 B.11　故障与故障排除——压缩空气处理——过滤器

故障	故障排除	备注
过滤器组件堵塞	无	—
过滤器组件破裂或部分破裂	如果过滤器组件足够耐压，故障可排除	
过滤器状态指示器或监控器失效	无	
过滤器壳体爆裂，或者外罩或连接组件破裂	如果尺寸、材料的选择和在系统中的布置，以及固定方式与良好的工程实践一致，故障可排除	

表 B.12　故障与故障排除——压缩空气处理——注油器

故障	故障排除	备注
设定装置没有修改设定的情况下，设定值(单位时间的油量)发生改变	无	—
设定装置的自发改变	如果针对特殊情况，为设定装置提供有效保护，故障可排除	
设定装置操作组件意外旋松	如果采用防止旋松的强制锁紧装置，故障可排除	
壳体爆裂，或者外罩、固定或连接组件破裂	如果尺寸、材料的选择和在系统中的布置，以及固定方式与良好的工程实践一致，故障可排除	

表 B.13　故障与故障排除——压缩空气处理——消音器

故障	故障排除	备注
消音器阻塞(堵塞)	如果消音器组件的设计与结构满足备注的要求，故障可排除	如果消音器的直径大小适当，并且其设计满足工作条件，则消音器组件的堵塞和/或排气回压的增加不可能超过临界值

表 B.14　故障与故障排除——储压器和压力容器

故障	故障排除	备注
储压器/压力容器或连接器破裂/爆裂，或者固定用螺钉的螺纹断裂	如果结构、设备的选择、材料的选择，以及在系统中布置与良好的工程实践一致，故障可排除	—

表 B.15　故障与故障排除——传感器

故障	故障排除	备注
传感器有缺陷(见备注)	无	本表中的传感器包括信号采集、处理和输出，尤其是用于压力、流量、温度等的传感器
检测或输出特性改变	无	—

表 B.16　故障与故障排除——信息处理——逻辑元件

故障	故障排除	备注
由于转换时间改变、未能转换、不完全转换等导致逻辑元件有缺陷(如“与”组件、“或”组件、逻辑存储组件)	相应的故障假设和故障排除，见表 B.3、表 B.4 和表 B.5 及相关的元件	—

表 B.17　故障与故障排除——信息处理——延时装置

故障	故障排除	备注
有缺陷的延时装置，如气动、气动/机械计时和计数组件	对于不带运动元件的延时装置，如固定电阻，如果在正常工作条件下使用(见备注)，并且对压缩空气做了充分处理和过滤，故障可排除	满足制造商规定的条件即为在正常工作条件下使用
检测或输出特性改变		
壳体爆裂或者外罩或固定组件破裂	如果结构、尺寸和安装与良好的工程实践一致，故障可排除	—

表 B.18　故障与故障排除——信息处理——变换器

故障	故障排除	备注
有缺陷的变换器[见备注 1)]	对于不带运动元件的变换器，如反射式喷嘴，如果在正常工作条件下使用[见备注 2)]，并且对压缩空气做了充分处理和过滤，故障可排除	1) 这包括气动信号变换为电信号、位置检测(气缸开关、反射式喷嘴)、气动信号放大等。 2) 满足制造商规定的条件即为在正常工作条件下使用
检测或输出特性改变		
壳体爆裂或者外罩或固定组件破裂	如果结构、尺寸和安装与良好的工程实践一致，故障可排除	—

附 录 C
（资料性附录）
液压系统的确认工具

当液压系统与其他技术结合使用时，还宜考虑附录 C。液压元件为电气连接/控制时，宜考虑附录 D 中相应的故障清单。

注：国家相关法律法规中规定了附加要求。

表 C.1 和表 C.2 列出了基本安全原则和经验证的安全原则。宜避免液压流体中的气泡和气穴现象，因为它们会产生附加危险，如非预期的运动。

附录 C 未给出经验证的元件清单。“经验证的”状态主要取决于具体应用。如果元件满足 GB/T 16855.1—2008 中 6.2.2 和 ISO 4413:2010 中第 5 章～第 7 章的要求，则可认为是“经验证的”。某些应用中的经验证元件可能不适用于其他应用。

表 C.3～表 C.12 列出了故障排除及其原理。更多故障排除见 4.4。

发生故障的精确时刻是关键（见 9.1）。

表 C.1 基本安全原则

基本安全原则	备 注
采用合适的材料以及适当的加工	材料、加工方法和处理方式的选择与应力、耐久性、弹性、摩擦、磨损、腐蚀、温度、液压流体等因素有关
正确的尺寸和外形	考虑应力、张力、疲劳、表面粗糙度、公差、加工等因素
元件/系统的正确选择、组合、布置、装配及安装	使用制造商的操作说明书，如目录表、安装说明、规范和在类似元件/系统的成功应用实例等
失能原则的使用	通过能量释放得到安全状态。有关停止的主要动作见 GB/T 15706—2012 中 6.2.11.3。 提供的能量用于启动机构的运动。有关启动的主要操作，见 GB/T 15706—2012 中 6.2.11.3。 考虑不同的模式，如操作模式、维修模式。 在某些应用中，此原则不适用，例如，气压损失将产生附加危险的场合
正确的紧固	采用锁紧螺钉、连接件、胶合、锁紧圈等进行紧固时，考虑制造商的操作说明书。 使用适当的扭矩加载技术可以避免过载
压力限制	例如：压力安全阀、泄压阀/控制阀
速度限制/速度降低	例如：通过流量阀和节流阀限制活塞速度
充分避免流体污染	考虑流体中固体微粒和水的过滤和分离。 还考虑设置过滤是否需要维护的状态指示
适当的转换时间范围	考虑管道长度、压力、卸压能力、力、弹簧疲劳度、摩擦、润滑、温度/黏度、加速和减速过程中的惯性以及组合公差等
耐环境条件	在所有预期的环境和在任何可预见的不利条件下，如温度、湿度、振动、污染，所设计的装置都能工作。见第 10 章并考虑制造商的规范/操作说明书
防止意外启动	考虑不同模式下，例如，操作、维修模式，由于储能或恢复动力源引起的意外启动。 有必要通过特殊装置来释放储能。 对于特殊应用（例如夹持装置或保证一定位置需要保持的能量），需要单独考虑
简化	避免安全相关系统中不必要的元件
合适的温度范围	考虑整个系统
分离	安全相关功能与其他功能分离

表 C.2　经验证的安全原则

经验证的安全原则	备　　注
裕量/安全系数	安全系数在标准中给出或由安全相关的良好经验得出
安全位置	元件的可移动部分通过机械方式(仅靠摩擦是不够的)保持在安全位置。 需要施加力才能从安全位置移开
加大关闭力	一种解决方案是滑阀移动到安全位置(关闭位置)的面积比明显大于滑阀移动到打开位置的面积比(安全系数)
通过载荷压力关闭阀门	示例有座阀、插装阀。 考虑如何施加载荷压力,实现即使闭阀弹簧断裂,阀门依然关闭
直接机械动作	直接机械动作适用于气动装置内部的运动部分。也可见表 A.2
多重部件	见表 A.2
采用经验证的弹簧	见表 A.2
通过规定流量的控制来限速/减速	例如:固定的孔、固定的节流阀
力的限制/力的减小	可以通过一个经验证的泄压阀来实现,该泄压阀配备了尺寸合理并经正确选择的经验证的弹簧等
工作条件的合理范围	工作条件的限制,例如:宜考虑压力范围、流量和温度范围
监控流体的状态	考虑流体中的固体颗粒与水是否需要高水平的过滤与分离。还需考虑流体的化学/物理状态。还考虑设置过滤是否需要维护的状态指示
在滑阀中充分的正重叠	正重叠是确保停止功能和防止未经允许的移动
有限的滞后	例如:增加摩擦将增加滞后。组合公差也会影响滞后

表 C.3　方向控制阀

故障	故障排除	备注
转换时间改变	只要驱动力足够大,且运动元件为直接机械动作(见表 A.2),故障可排除;或者对于和其他至少一个阀门一起用来控制流体主流量的特殊类型插装座阀不能打开[见备注 1)],故障可排除	1)　如果满足以下条件,即为插装座阀的特殊类型: ——触发安全相关转换运动的有效面积至少是运动元件(提升阀)总面积的 90%; ——有效面积上的有效控制压力可增加至与该座阀动作相符的最大工作压力(符合 GB/T 17446—2012 中 3.2.429); ——与最大工作压力相比,运动元件有效面的反面上的有效控制压力可降至非常小,如:使用泄压阀时的回压或者使用吸入/填充阀时的供压; ——运动元件(提升阀)带有外围平衡槽; ——座阀及其导向阀门设计成歧管块(即:这些阀门的连接无软管总成和管道)
无转换(粘连在末端或零位置)或不完全转换(粘连在任意中间位置)	只要驱动力足够大,且运动元件为直接机械动作(见表 A.2),故障可排除;或者对于和其他至少一个阀门一起用来控制流体主流量的特殊类型插装座阀不能打开[见备注 1)],故障可排除	

表 C.3（续）

故障	故障排除	备注
初始转换位置的自发改变（无输入信号的情况下）	只要驱动力足够大，且运动元件为直接机械动作（见表 A.2），故障可排除；如果采用了经验证的弹簧（见表 A.2），并且在正常安装和工作条件下使用[见备注 2)]，故障可排除；或者对于和其他至少一个阀门一起用来控制流体主流量的特殊类型插装座阀不能打开[见备注 1)]，并且在正常安装和工作条件下使用[见备注 2)]，故障可排除	2) 满足以下条件即为在正常安装和工作条件下使用： ——满足制造商规定的条件； ——运动元件的重量不影响安全，如水平安装； ——没有特别的惯性力影响运动元件，例如：运动方向要考虑运动机械部件的定向； ——没有产生极限振动和冲击应力
泄漏	对于座阀，如果在正常安装和工作条件下使用（见备注），并且提供了充分的过滤系统，故障可排除	满足制造商规定的条件即为在正常安装和工作条件下使用
长期使用后，因泄漏导致的流量改变	无	—
阀套爆裂或运动元件损坏，以及支架或压紧螺钉损坏/破裂	如果结构、尺寸和安装与成功的工程实践一致，故障可排除	
对于伺服阀和比例阀：引起不可控动作的液压故障	如果由于其设计和结构原因，伺服阀和比例方向阀从安全的角度可评估为常规的方向控制阀，故障可排除	
注：如果控制功能是通过很多单一功能的阀门来实现，则宜对每个阀门进行故障分析。先导阀也宜按照与此相同的步骤进行。		

表 C.4 故障与故障排除——停止（截止）阀/单向（止回）阀/往复阀等

故障	故障排除	备注
转换时间改变	无	—
不能打开、不能完全打开、不能关闭或不能完全关闭（粘连在末端或任意的中间位置）	运动元件的导向系统是按照与不带阻尼系统非控制球座阀（见备注）类似的方式设计的，并且采用了经验证的弹簧（见表 A.2），故障可排除	对于不带阻尼系统的非控制球座阀，其导向系统的设计通常使得运动元件不可能发生粘连
初始转换位置自发改变（无输入信号）	在正常安装和工作条件（见备注）下，如果其提供的压力和面积使得关闭力足够，故障可排除	满足以下条件时，即为正常安装和工作条件： ——满足制造商规定的条件； ——没有特殊的惯性力影响运动元件，例如：运动的方向考虑了机器运动部件的运动方向； ——没有极限振动和冲击力产生
对于往复阀：两个输入的连接同时断开	如果运动元件的结构和设计使得不可能同时断开，故障可排除	—

表 C.4（续）

故障	故障排除	备注
泄漏	如果在正常工作条件下使用(见备注)，并提供了足够的过滤系统，故障可排除	满足制造商规定的条件即为在正常的工作条件使用
长期使用后，因泄漏导致的流量改变	无	—
阀套爆裂或运动元件损坏，以及支架或压紧螺钉损坏/破裂	如果结构、尺寸和安装与良好的工程实践一致，故障可排除	

表 C.5 故障与故障排除——流量阀

故障	故障排除	备注
设定装置没有修改任何设定的情况下流量发生改变	对于不带运动元件[见备注 1)]的流量控制阀，如节流阀，如果在正常工作条件下使用[见备注 2)]，并且提供了足够的过滤系统[见备注 3)]，故障可排除	1) 设定装置并不是运动部件。因为压差和黏度改变而引起的流量变化在这类阀门中受到物理上的限制，不属于此假定故障。 2) 满足制造商规定的条件即为正常工作条件。 3) 单向阀集成到流量阀中，还需考虑单向阀的故障推定
使用不可调节的圆孔和喷嘴时，流量发生改变	如果直径大于 0.8 mm，在正常工作条件下使用[见备注 2)]，并且提供了足够的过滤系统，故障可排除	
对于比例流量阀：由于意外改变设定值而引起流量变化	无	—
设定装置自发改变	如果根据技术安全规范在特定应用中对设定装置设置了有效保护，故障可排除	
设定装置的操作组件意外松开(旋松)	如果采用防止松开(旋松)的强制锁紧装置，故障可排除	
阀套爆裂或运动元件损坏，以及支架或压紧螺钉损坏/破裂	如果结构、尺寸和安装与良好的工程实践一致，故障可排除	

表 C.6 故障与故障排除——压力阀

故障	故障排除	备注
超过设定压力时，不能打开或打开不足(运动元件粘连或运动缓慢)[见备注 1)]	对于和其他至少一个阀门一起用来控制表 C.3 中的流体主流量的特殊类型插装座阀不能打开[见备注 1)]，故障可排除；或者运动元件的导向系统与不带阻尼装置的非控制球座阀[见备注 2)]类似，并且采用了经验证的弹簧(见表 A.2)，故障可排除	1) 此故障只适用用作施加力的压力阀，如夹紧，以及用作控制危险运动的压力阀，如暂停载荷。此故障不适用于在液压系统中压力阀的正常功能，如，压力限制、压力下降。 2) 对于不带阻尼装置的非控制球座阀，导向系统的设计通常使得运动元件不可能粘连
压力降至设定值以下时，不能打开或打开不足(运动元件粘连或运动缓慢)[见备注 1)]		
设定装置没有修改设定的情况下，压力控制动作发生改变	对于直接驱动的泄压阀，如果安装的弹簧是经验证的，故障可排除(见表 A.2)	
对于比例压力阀：由于设定值的意外改变而引起压力控制动作改变[见备注 1)]	无	

表 C.6（续）

故障	故障排除	备注
设定装置自发改变	如果根据技术安全规范针对具体应用对设定装置进行有效保护，如铅封，故障可排除	—
设定装置的操作组件意外旋松	如果采用防止旋松的强制锁紧装置，故障可排除	
泄漏	对于座阀，如果在正常工作条件（见备注）下使用，并且提供了充分的过滤系统，故障可排除	满足制造商规定的条件即为在正常工作条件下使用
长期使用后，泄漏流量改变	无	—
阀套爆裂或运动元件损坏，以及支架或压紧螺钉损坏/破裂	如果结构、尺寸和安装与良好的工程实践一致，故障可排除	

表 C.7　故障与故障排除——金属管道

故障	故障排除	备注
爆裂和泄漏	如果尺寸、材料的选择和固定方式与良好的工程实践一致，故障可排除	—
接头失效（如：开裂、泄漏）	如果采用焊接式接头、焊接法兰或者扩口式管接头，并且尺寸、材料的选择、加工、结构和固定方式与良好的工程实践一致，故障可排除	
堵塞（阻塞）	对于动力回路中的管道，故障可排除。 对于控制和测量管道，如果公称直径大于或等于 3 mm，故障可排除	

表 C.8　故障与故障排除——软管总成

故障	故障排除	备注
泄露以及连接附件的爆裂、磨损	无	—
堵塞（阻塞）	对于动力回路中的软管总成，故障可排除。 对于用于控制和测量的软管总成，如果公称直径大于或等于 3 mm，故障可排除	

表 C.9　故障与故障排除——连接器件

故障	故障排除	备注
螺钉破裂、断裂或者螺纹齿折断	如果尺寸、材料的选择、结构，以及与管道和/或流体技术元件的连接与良好的工程实践一致，故障可排除	—
泄露（气密损失）	无（见备注）	由于磨损、老化、弹性退化等原因，长期使用后不可能排除故障。假定不会发生重大的突发性气密失效
堵塞（阻塞）	对于动力回路中的连接器件，故障可排除。 对于用于控制和测量的连接器件，如果公称直径大于或等于 3 mm，故障可排除	—

表 C.10　故障与故障排除——过滤器

故障	故障排除	备注
过滤器组件堵塞	无	—
过滤器组件破裂	如果过滤器元件足够耐压，并且提供了有效的旁通阀或有效的污物监测，故障可排除	
旁通阀失效	如果旁通阀引导系统的设计类似于不带阻尼装置的非控制球座阀（见表 C.4），并且采用了经验证的弹簧（见表 A.2），故障可排除	
污物指示器或污物监控器失效	无	
过滤器壳体爆裂、罩或连接元件破裂	如果尺寸、材料的选择、系统中的布置和固定方式与良好的工程实践一致，故障可排除	

表 C.11　故障与故障排除——蓄能

故障	故障排除	备注
蓄能容器、连接器或盖板的螺钉破裂/爆裂，以及螺钉螺纹折断	如果结构、设备的选择、材料的选择，以及在系统中的布置与良好的工程实践一致，故障可排除	—
气体和工作液体之间的隔离组件泄漏	无	
在气体和工作液体之间的隔离元件的失效/损坏	在气罐/汽缸存储的条件下（见备注），故障可排除	不考虑严重的突发泄漏
气体侧注入阀失效	如果注入阀的安装与良好的工程实践一致，并且针对外部影响，提供了足够的保护，故障可排除	—

表 C.12　故障与故障排除——传感器

故障	故障排除	备注
传感器有缺陷（见备注）	无	传感器的类型包括信号采集、处理和输出，尤其是用于压力、流量、温度等的传感器
检测或输出特性改变	无	—

附 录 D
（资料性附录）
电气系统的确认工具

D.1 概述

当电气系统与其他技术结合使用时，还宜考虑附录 D。

GB 5226.1 规定的环境条件适用于确认过程。如果规定了其他环境条件，还宜考虑这些条件。

表 D.1 和表 D.2 列出了基本安全原则和经验证的安全原则。

当表 D.3 中列出的元件满足 GB/T 16855.1—2008 中 6.2.4 的规定时，可认为是“经验证的”。表 D.3 中列出的标准可用于证明这些标准对特殊应用的适应性和可靠性。某些应用中的经验证元件可能不适用于其他应用。

注：复杂的电子元件，如可编程逻辑控制器(PLC)、微处理器、专用集成电路，不能认为等同于“经验证的”元件。

D.2 和表 D.4～表 D.21 列出了故障排除及其原理。更多故障排除见 4.4。

进行确认时，宜考虑永久性故障和瞬态干扰。

发生故障的精确时刻是关键(见 9.1)。

表 D.1 基本安全原则

基本安全原则	备 注
采用合适的材料和适当的加工	材料、加工方法和处理方式的选择与应力、耐久性、弹性、摩擦、磨损、腐蚀、温度、导电率、介电强度等因素有关
正确的尺寸和外形	考虑应力、张力、疲劳、表面粗糙度、公差、加工等因素
元件/系统的正确选择、组合、布置、装配和安装	使用制造商的操作说明书，如目录表、安装说明、规范和在类似元件/系统中成功应用的工程实例等
正确的保护接地	控制回路次级回路一侧接地，电磁驱动装置工作线圈的一个端子或者是其他电气装置的一个端子都连接到保护接地电路(GB 5226.1—2008 中 9.4.3.1)
绝缘监控	使用绝缘监控装置，用来显示接地故障，或者在发生接地故障后自动切断电路(见 GB 5226.1—2008 中 6.3.3)
失能原则的使用	安全状态通过使所有相关装置的失能来获得，例如，输入端(按钮和位置开关)采用常闭(NC)触点，继电器采用常开(NO)触点(也可见 GB/T 15706—2012 中 6.2.11.3)某些应用中会有例外，例如，失去电源将产生附加危险。可能有必要通过时间延迟功能来达到系统安全状态(见 GB 5226.1—2008 中 9.2.2)
瞬态抑制	使用抑制装置(RC、二极管、变阻器)与负载并联，但不与触点并联。 **注**：二极管增加了切断时间。
减小响应时间	尽可能减小开关元件失电的延迟
兼容性	采用与电压和电流兼容的元件
耐环境条件	设备的设计使其能在所有预期环境中工作，也能在任何可预见的不利环境中工作，例如：温度、湿度、振动和电磁干扰(EMI)(见第 10 章)

表 D.1（续）

基本安全原则	备　　注
牢固固定输入装置	牢固固定输入装置，如联锁开关、位置开关、限位开关、接近开关，使得在所有预期的条件下，如：振动、正常磨损、异物进入、温度，能够维持住位置、对齐和开关容隙。 见 ISO 14119:2013 中第 5 章
防止意外启动	防止意外启动，例如，恢复供电后（见 GB/T 15706—2012 中 6.2.11.4、GB/T 19670、GB 5226.1）
保护控制电路	控制电路的保护宜满足 GB 5226.1—2008 中 7.2 和 9.1.1
按序开关冗余信号串联触点的电路	为了避免两个触点熔焊引起的共模失效，两个触点不在同一时间断开和闭合，从而使得始终有一个触点无电流

表 D.2　经验证的安全原则

经验证的安全原则	备注
直接机械连接的触点	采用直接机械连接的触点，例如，用于 2 类、3 类和 4 类系统中的监控功能（见 GB 14048.4—2010 的附录 F、GB 14048.5—2008 的附录 L、EN 50205）
避免电缆中的故障	为避免两个相邻导线之间短路，可采取以下其中一种措施： ——每个单独导线采用带屏蔽的电缆连接到接地保护电路； ——在扁平电缆中，在每两个信号导线之间使用一个接地导线
隔离间距	在端子之间、元件和导线之间留有足够的间距，以避免意外的连接
限制能量	用电容器提供有限的能量，例如，应用在定时器中
限制电气参数	通过限制电压、电流、功率或者频率来限制运动，如使用扭距限制、带位移/时间限制的保持-运行装置、减速来避免产生不安全状态
无不确定状态	避免控制系统中的不确定状态。控制系统的设计和结构使得在正常工作条件下和所有可预计的工作条件下都能预测其状态，如控制系统的输出
直接动作的驱动模式	直接动作通过无弹性元件的外形（不是通过力）来传递，例如，不是通过执行器与触点之间的弹簧来动作（见 ISO 14119:2013 中的 5.4，GB/T 15706—2012 中的6.2.5）
失效模式定向	只要有可能，装置/电路宜为失效安全状态或条件
定向失效模式	宜尽可能采用定向失效模式的元件或系统（见 GB/T 15706—2012，6.2.12.3）
裕量	对安全回路中的元件降额使用，例如通过以下措施： ——流经切换触点的电流宜小于其额定电流的一半； ——元件的切换频率宜小于其额定值的一半； ——元件总预期切换操作次数宜不超过该装置电气耐用度的 10%。 **注**：额定值可依据设计基本原理来降低。
尽可能减小故障的可能性	将安全相关功能与其他功能分开
复杂/简单的平衡	宜平衡以下两者之间的关系： ——复杂：实现更好控制； ——简单：实现更高的可靠性

表 D.3　经验证的元件

经验证的元件	“经验证的”附加条件	标准或技术规范
直接打开动作的开关，如： ——按钮； ——位置开关； ——凸轮操作式选择开关，如，用于操作模式	—	GB 14048.5—2008 中附录 K
急停装置	—	GB 16754 GB/T 14048.14
熔断器	—	GB 13539.1
断路器	—	GB 14048.2
开关、隔离器	—	GB 14048.3
差动断路器/剩余电流装置(RCD)	—	GB 14048.2—2008 中附录 B
主接触器	只有满足以下条件才是经验证的： a)　考虑了其他影响，如振动； b)　通过适当的方法避免失效，如裕量(见表 D.2)； c)　通过热保护装置限制负载的电流； d)　通过保护装置防止电路过载。 **注**：故障不可能排除。	GB 14048.4
控制和保护开关电器设备(CPS)	—	GB 14048.9
辅助接触器(例如：接触器式继电器)	只有满足以下条件才是经验证的： a)　考虑了其他影响，如振动； b)　强制激励动作； c)　通过适当的方法避免失效，如裕量(见表 D.2)； d)　通过熔断器或断路器限制触点的电流，以避免触点熔焊； e)　用于监测时，触点为强制机械导向。 **注**：故障不可能排除。	GB 14048.5 GB 14048.4—2010 中附录 F EN 50205
继电器	只有满足以下条件才是经验证的： a)　考虑了其他影响，如振动； b)　强制激励动作； c)　通过适当的方法避免失效，如裕量(见表 D.2)； d)　通过熔断器或断路器限制触点的电流，以避免触点熔焊。 **注**：故障不可能排除。	GB/T 21711.1 IEC 61810-2
变压器	—	GB 19212
电缆	宜对电缆外壳进行保护，以防止机械损坏(包括振动或弯曲等)	GB 5226.1—2008 中第 12 章
插头和插座	—	预定用途可依照相关的电气标准。 对于联锁，也可见 GB/T 18831
温度开关	—	电气方面见 GB 14536.1
压力开关	—	电气方面见 GB 14048.5； 压力方面见附录 B 和附录 C
电磁阀	—	—

D.2 故障排除

D.2.1 概述

只有部件在其规定的额定值内工作时,故障排除才有效。

D.2.2 “锡须”

如果是无铅制程和无铅产品,则可发生因“锡须”生长引起的电气短路。对任何元件短路相关的故障排除时,宜评价并考虑这种可能性。例如:如果认为锡须生长为高风险,则“电阻器短路”的故障排除是无效的,这是因为不得不考虑电阻器触点之间的短路。

注 1:锡须生长是一种主要与纯净亮丽的锡抛光相关的现象。针状凸起的长度可生长几百微米并导致电气短路。流行的理论认为锡须是由镀锡层中逐步增长的压应力引起的。

注 2:参考文献[34]和[35]有助于评价这种现象。

注 3:目前还没有印刷电路板(PCB)上出现锡须的相关报道。走线通常由不带锡涂层的铜组成,焊盘可用锡合金涂层,但生产过程似乎不会刺激锡须的生长。

D.2.3 安装在 PCB 上的部件的短路

只有按照表 D.5 给出的“两个相邻走线/焊盘之间短路”进行故障排除,才能排除安装在 PCB 上的部件的短路。

D.2.4 故障排除与集成电路

因为不可能排除可造成集成电路失灵的故障(见表 D.20 和表 D.21),所以,单一故障可导致由单个集成电路执行的安全功能(包括其检查/试验)的丧失。因此,采用单个集成电路实现 2 类、3 类或 4 类中容错和/或故障检测所需的多通道功能,这几乎是不可能的,除非满足 IEC 61508-2:2010,附录 E 中的特殊结构要求。

表 D.4 故障与故障排除——导线/电缆

故障	故障排除	备注
任意两根导线之间短路	导线间的短路,可以: ——永久连接(固定)并防止外部损坏,例如,采用电缆管道、电缆外壳; ——单独的多芯电缆; ——在电气绝缘外壳的内部(见备注); 或者 ——分别进行接地保护	假设导线和外壳均满足相应的要求(见 GB 5226.1)
导线与裸露的带电部件、与地,或者与保护连接导线之间短路	导线和裸露的带电部件之间的短路在电气外壳内(见备注)	
导线开路	无	—

表 D.5　故障与故障排除——印刷电路板/印刷电路组件

故障	故障排除	备注
两个相邻走线/焊盘之间短路	相邻导线之间的短路符合备注，故障可排除	基材至少要采用满足 GB/T 1303.1 的 EP GC。 电气间隙和爬电距离至少符合 GB/T 16935.5 的要求(电气间隙大于 2 mm 时，符合 GB/T 16935.1 的要求)，且污染等级为 2/过电压类别为Ⅲ；如果两条走线由安全特低电压/保护特低电压(SELV/PELV)供电，则污染等级为 2/过电压类别为Ⅱ，且最小电气间隙为 0.1 mm。 印刷电路组件安装在能防止传导污染的外壳内，如至少为 IP54 的外壳，并且印刷面涂有防老化清漆或覆盖所有走线的保护层。 **注 1**：经验已表明阻焊膜是比较满意的保护层。 **注 2**：按照 GB/T 16935.3 进一步利用保护层保护，可减小爬电距离和电气间隙。
走线断路	无	—

表 D.6　故障与故障排除——接线盒

故障	故障排除	备注
相邻端子之间短路	相邻端子之间短路依照备注 1)或备注 2)	1)　按照 GB/T 14048.7 或 GB/T 14048.8 使用端子和连接，并满足 GB 5226.1—2008 中 13.1.1 的要求。 2)　自身的设计避免发生短路，如：在连接点添加热缩套管
独立端子断路	无	—

表 D.7　故障与故障排除——多针连接器

故障	故障排除	备注
相邻两针之间短路	相邻针之间短路依照备注。 如果连接器安装在 PCB 上，则考虑采用表 D.5 进行故障排除	对于多股金属线，采用套圈或其他方式。爬电距离、电气间隙和其他所有间隙的尺寸宜至少满足 GB/T 16935.1 过电压类别Ⅲ的要求
无机械方式保护时，插入连接器位置交替或不正确	无	—
与接地、带电部件或者保护导线相连导线(见备注)短路	无	电缆芯可认为是多针连接器的一部分
独立连接器的针断路	无	—

表 D.8　故障与故障排除——机电式位置开关、手动操作开关
（例如，按钮、复位执行器、DIP 开关、磁力触点、簧片开关、压力开关、温度开关）

故障	故障排除	备注
触点不能闭合	符合 GB/T 17454 的压敏保护装置	—
触点不能打开	满足 GB 14048.5—2008 中附录 K 的触点可打开	—
相互绝缘的相邻触点之间短路	对于满足 GB 14048.5 的开关，可以排除短路故障（见备注）	松动的带电部件宜不能在触点之间桥接绝缘
转换触点三个端子之间同时短路	对于满足 GB 14048.5 的开关，可以排除同时短路的故障（见备注）	
对于 PLe，不能排除机械（如执行器与触点组件之间的机械连接）和电气方面的故障。这种情况下，有必要采用冗余。对于符合 GB/T 14048.14 的急停装置，如果考虑了最大操作次数，则可排除机械方面的故障。		
注：机械方面的故障清单在附录 A 中列出。		

表 D.9　故障与故障排除——机电设备
（例如，继电器、接触器式继电器）

故障	故障排除	备注
当线圈失电时，所有触点保持在得电位置（例如：由于机械故障）	无	—
供电的时候，所有触点保持在失电位置（例如，由于机械故障、线圈电路开路）	无	
触点不能打开	无	
触点不能闭合	无	
转换触点三个端子之间同时短路	如果满足备注的要求，可排除同时短路的故障	电气间隙和爬电距离至少符合 GB/T 16935.1 的要求，且污染等级为 2/过电压类别为Ⅲ。 松动的带电部件不能在触点和线圈之间桥接绝缘
两对触点之间短路和/或触点与线圈端子之间短路	如果满足备注的要求，可以排除短路的故障	
常开触点和常闭触点同时闭合	如果满足备注的要求，可以排除同时闭合的故障	采用直接驱动（或机械连接）的触点（见 GB 14048.5—2008 中附录 L）

表 D.10　故障与故障排除——开关——接近开关

故障	故障排除	备注
输出端恒定低阻抗	无（见备注）	见 GB/T 14048.13
输出端恒定高阻抗	无（见备注）	宜描述防止故障的措施
电源中断	无	—
由于机械失效，开关无法操作	当满足备注时，由于机械失效导致的无法操作可以排除	开关的所有部件都宜充分良好地固定。机械方面，见附录 A
转换开关三个接线之间短路	无	—

表 D.11　故障与故障排除——开关——电磁阀

故障	故障排除	备注
不能得电	无	—
不能失电	无	
注：气动阀和液压阀机械方面的故障清单分别在附录 B 和附录 C 中给出。		

表 D.12　故障与故障排除——分离式电气元件——变压器

故障	故障排除	备注
独立的线圈断路	无	—
不同线圈之间短路	如果满足备注 1)和备注 2)，可排除不同线圈之间的短路故障	1) 宜满足 GB 19212 相关部分中的要求。 2) 不同线圈之间采用双重绝缘、强化绝缘或者保护屏。应根据 GB 19212.1—2008 的第 18 章进行测试。试验电压在 GB 19212.1—2008 中表 8a 给出。 线圈短路的故障需要采取适当的措施来避免，如： ——浸制线圈可以使单个线圈之间和线圈本体以及线圈铁芯的所有空隙都得以浸泡； ——采用的绕组导体远小于其绝缘和高温额定值。 3) 如果发生二次短路，不超过规定的工作温度
一个线圈短路	如果满足备注 1)，可排除一个线圈的短路故障	
有效匝数比改变	如果满足备注 1)，可排除有效匝数比改变的故障。也可见备注 3)	

表 D.13　故障与故障排除——分离式电气元件——电感器

故障	故障排除	备注
断路	无	—
短路	如果满足备注，可排除短路故障	线圈为单层，镀瓷或陶瓷，轴向连接和轴向安装
“$0.5L_N < L < L_N$＋公差”中的任意值，这里的 L_N 为感应系数的额定值	无	根据结构类型，可以考虑其他范围

表 D.14　故障与故障排除——分离式电气元件——电阻

故障	故障排除	备注
断路	无	—
短路	如果满足备注 1)和备注 2)，可排除短路故障	1) 电阻为膜片式、或线绕单层式电阻，并防止在破损时线圈开卷，轴向接线、轴向安装，且是浸渍过的。 2) 采用表面安装技术的电阻是金属薄片型，且封装类型为 MELF、迷你 MELF 或 μMELF。 3) 例如：如果认为锡须生长的风险为高，则对“电阻短路故障”进行故障排除是无效的，这是因为不得不考虑元件触点之间的故障

表 D.14（续）

故障	故障排除	备注
“$0.5R_N<R<2R_N$”中的任意值，这里的 R_N 为额定阻抗值[也可见备注 3)]	无	根据结构的类别，可以考虑其他范围

表 D.15　故障与故障排除——分离式电气元件——电阻网络

故障	故障排除	备注
断路	无	—
任意两个连接之间短路	无	
任意连接之间短路	无	
“$0.5R_N<R<2R_N$”中的任意值，这里的 R_N 为额定阻抗值	无	根据结构的类别，可以考虑其他范围

表 D.16　故障与故障排除——分离式电气元件——电位计

故障	故障排除	备注
单独连接断路	无	—
所有连接之间短路	无	
任意两个连接之间短路	无	
“$0.5R_p<R<2R_p$”中的任意值，这里的 R_p 为额定阻抗值	无	根据结构的类别，可以考虑其他范围

表 D.17　故障与故障排除——分离式电气元件——电容器

故障判定	故障排除	备注
开路	无	—
短路	无	
“$0.5C_N<C<C_N$＋公差”中的任意值，这里的 C_N 为额定容抗值	无	根据结构的类别，可以考虑其他范围
$\tan\delta$ 值改变	无	—

表 D.18　故障与故障排除——电子元件——分离式半导体
[例如，二极管、稳压二极管、晶体管、三端双向可控硅元件、稳压器、水晶振子、光电晶体管、发光二极管(LED)]

故障	故障排除	备注
任意连接断路	无	—
任意两个连接之间短路	无	
所有连接之间短路	无	
特性改变	无	

表 D.19　故障与故障排除——电子元件——光耦合器

故障	故障排除	备注
单独的连接断路	无	—
任意两个输入连接之间短路	无	
任意两个输出连接之间短路	无	
任意两个输入和输出连接之间短路	如果满足备注的要求，可以排除输入和输出之间的短路故障	光耦合器满足 GB/T 16935.1 规定的过电压类别Ⅲ。如果由 SELV/PELV 供电，则污染等级为 2/过电压类别为Ⅱ。 **注**：见表 D.5。 采取措施确保光耦合器的内部失效不会使绝缘材料温度过高

表 D.20　故障与故障排除——电子元件——不可编程集成电路

故障	故障排除	备注
每个独立的连接断路	无	—
任意两个连接之间短路	无	
固定型故障(即输入隔离或输出断开的高电平信号“1”和低电平信号“0”的短路)。所有输入和输出单独或同时出现静态高电平信号“1”和低电平信号“0”	无	
输出寄生振荡	无	
值改变(例如：模拟设备的输入/输出电压)	无	
注：在 GB/T 16855 的本部分中，少于 1 000 个门和/或少于 24 针的 ICs(集成电路)、运算放大器、移位寄存器和混合微膜组件可以认为是简单元件。这是一种主观定义。		

表 D.21　故障与故障排除——电子元件——可编程和/或复杂集成电路

故障	故障排除	备注
全部或部分功能出现的故障，包括软件故障	无	—
每个独立的连接断路	无	
任意两个连接之间短路	无	
固定型故障(即输入隔离或输出断开的高电平信号“1”和低电平信号“0”的短路)。所有输入和输出单独或同时出现静态高电平信号	无	

表 D.21（续）

故障	故障排除	备注
输出寄生振荡	无	—
值的改变，如：模拟设备的输入/输出电压	无	
由于集成电路的复杂性，硬件中被忽视的未检测到的故障	无	
分析宜识别附加故障，如果这些附加故障影响安全功能的运行，还宜考虑这些故障。		
注：在 GB/T 16855 的本部分中，如果一个 IC 由超过 1000 个门和/或超过 24 针组成就可认为是复杂的。这是一种主观定义。		

附 录 E
（资料性附录）
故障特性确认及诊断措施示例

E.1 概述

本附录是一种安全功能(SF 1)PL 的确认示例，但并没有给出关于 PL 以下几个方面的要求：

——$MTTF_d$；

——共因失效(CCF)；

——软件分析；

——系统性失效。

本示例并不包括以下几个方面的确认：

——安全要求规范(见第 7 章)；

——安全功能的特征(见第 8 章)；

——环境要求(见第 10 章)；

——维护要求(见第 11 章)；

——文件的要求(见第 12 章)。

本示例考虑了三种安全功能：SF 1、SF 2 和 SF 3。

SF 1 是一种由打开联锁防护装置触发的，四个独立的机器执行器的安全相关停止功能，并且这种安全功能可认为是每个执行器(SF 1.0、SF 1.1、SF 1.2、SF 1.3)的单独安全功能。为了减少示例的范围，只对 SF 1.0 和 SF 1.3 进行确认。

附录 A 给出了如何检查故障特性，以及回路提供的诊断覆盖率的指南。考虑到 GB/T 16855.1—2008 的附录 E，用于确定诊断覆盖率的方法是基于失效模式和影响分析(FMEA)的。

注：本示例并不包括 SRP/CS 的完整确认过程，特别是没有考虑 PLC 软件所必需的确认。安全相关软件的确认，见 9.5。

E.2 机器的描述

本示例基于一台手动加载和卸载工件的自动装配机。该机器预定执行两种按顺序的功能：插入球并通过螺钉固定到每个工件上。

该机器共有四个位置：加载位、卸载位，以及两个工位(见图 E.1)：第一个工位用于气动驱动插入球阶段，第二个工位用于气动驱动螺钉拧紧阶段。

电动旋转台将工件移动到四个位置中的每个位置。手动放置工件并手动将其从安装在旋转工作台上的工件夹持装置上移除。变频器控制的电机驱动一个行星齿轮和皮带传动系统使转台旋转。

在第一个工位，通过水平安装的气缸将一个球插入到工件中，气缸由单稳两位五通方向控制阀(1V1，见图 E.3)来控制。该气缸的基本位(阀门失能)是内缩位。球插入的深度由安装在气缸完全延伸位置的限位开关来监控，而所施加的压力则由气缸延伸用供气管路中的压力传感器来监控。

螺钉固定工位由竖直安装的无杆气缸组成，并通过气压驱动螺钉拧紧装置旋转。通过气缸使螺丝上升或下降，这个气缸由单稳两位五通方向控制阀(2V1，见图 E.3)来控制。该气缸的基本位(阀门失能)是螺钉拧紧装置上升后气缸的上面位置。此外，在气缸的低位连接处设置了一个先导控制单向阀(2V2)。

螺钉拧紧装置的旋转运动由气动马达驱动，该气动马达由单稳两位五通方向控制阀(3V1)控制。该气动马达的基本位(阀门失能)是OFF状态时的位置。螺钉拧紧装置提供的力矩由供气线中的压力传感器来监控。

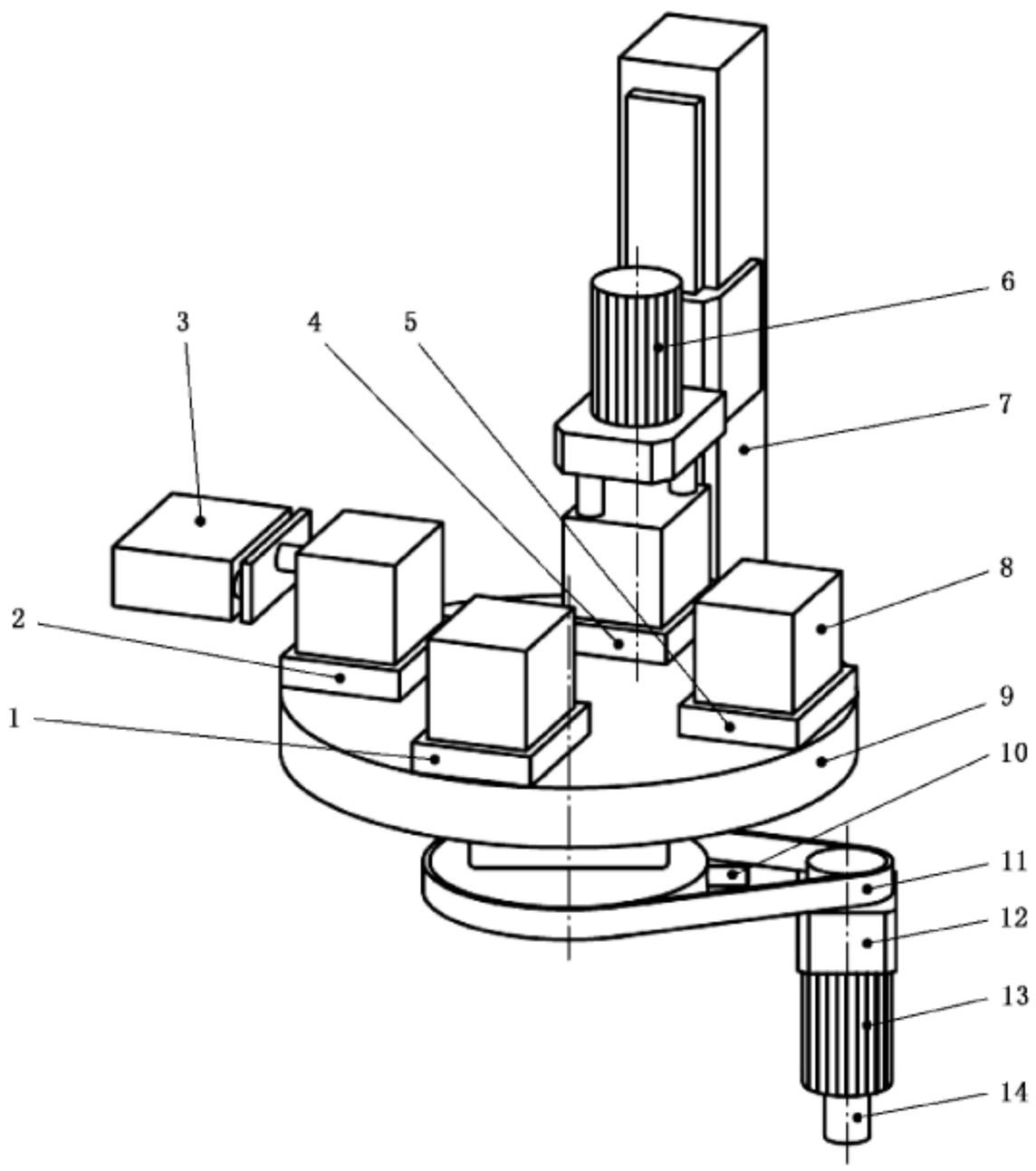
按下启动按钮，自动操作模式下的机器完成一个简单循环。在循环开始时，旋转台夹持住3个工件：(i)新加载一个工件；(ii)半成品工件(球已插入)；(iii)成品工件(球已插入且螺钉已拧紧)。在机器的每个循环内，旋转台旋转90°，与此同时，分别在新加载的工件上插入球，在半成品工件上拧紧螺钉。然后，机器功能停止，操作者打开联锁防护装置卸下成品工件并加载新工件。完成一个工件需要三个机器循环，旋转台从工件加载位置旋转至卸下位置，角度为270°。

提供了以下两种操作模式：

——手动加载和卸下的自动模式(联锁防护装置关闭后机器才能完全运动)；

——旋转台设定模式(联锁防护装置打开，且采用保持-运行控制装置控制旋转台的运动)。

该机械存在的危险是因气压驱动的执行器(在球插入和螺钉拧紧两个工位)和电气驱动旋转台运动引起的机械危险。正因为如此，除了联锁防护装置提供的进入加载区和卸下区(危险区)的入口之外，其余都通过固定式机械防护装置予以保护。



说明：

1——加载位；

2——球插入工位；

3——球插入气缸(A1)；

4——螺钉拧紧工位；

5——卸下位；

6——螺钉拧紧装置(A3)；

7——螺钉插入(竖直驱动)气缸(A2)；

8——工件；

9——旋转台；

10——脉冲传感器；

11——驱动带；

12——行星齿轮；

13——电机(M1)；

14——转动传感器(G1)。

图 E.1　示例中的机器：自动装配机

E.3 安全功能要求的描述

在自动操作模式下，通过以下安全功能防止危险运动：

SF 1——由打开联锁防护装置触发的安全相关停止功能，并且只要联锁防护装置打开，就防止意外启动。

在本示例中，可认为四个独立的机器执行器分别有各自的安全功能，见表 E.1：

——SF 1.0：旋转台的电机(M1)；

——SF 1.1：球插入气缸(A1)；

——SF 1.2：螺钉插入气缸(A2)；

——SF 1.3：螺钉拧紧装置的气动马达(A3)。

注 1：在本示例中，可认为安全相关停止功能和防止意外启动功能是一种安全功能，这是因为它们都是由同一个 SRP/CS 组合执行的功能。

在旋转台设定模式期间，而且联锁防护装置打开(通过气压驱动机器执行器被 SF 1.1、SF 1.2 和 SF 1.3 禁止)时，通过以下安全功能的组合实现旋转台运动的安全状态：

——SF 2：安全限速；

——SF 3：保持-运行模式。

表 E.1 各种操作模式下有效的安全功能

操作模式	安全功能					
	SF 1.0	SF 1.1	SF 1.2	SF 1.3	SF 2	SF 3
自动模式(联锁防护装置关闭)	×	×	×	×		
设定模式(联锁防护装置打开)		×	×	×	×	×
注：×表示安全功能有效。						

完成风险评估之后，各安全功能的 PL_r 值分别为：

——SF 1 为 PL_rd(安全相关停止以及防止意外启动)；

——SF 2 为 PL_rd(安全限速)；

——SF 3 为 PL_rc(保持-运行模式)。

注 2：为 SF 3 选择 PL_rc 时，考虑了与能够达到 PLd 的 SF 2 组合使用。

当执行 SF 1 时，触发以下功能：

——旋转台完成符合 GB 5226.1 中 2 类停机的受控停机；

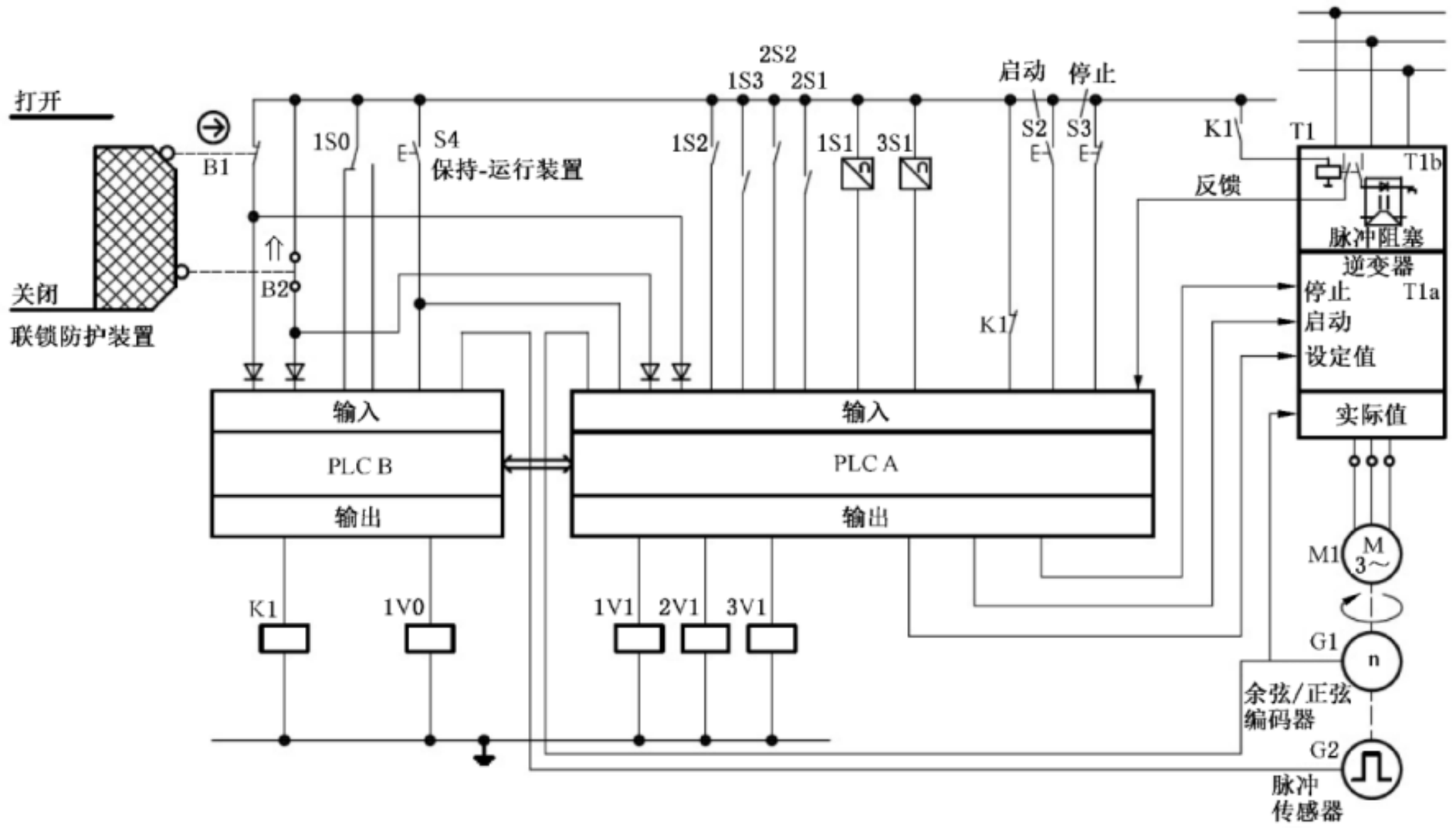
——球插入工位上水平安装的气缸(A1)以及螺钉拧紧工位上竖直安装的气缸(A2)回到和/或保持在其基本位(即分别是内缩位和上升位)；

——螺钉拧紧装置(A3)立即停止。

注 3：在本示例中，风险评估确定因变频器失灵导致的旋转台减速不可控是可接受的，并且气缸 A1 和 A2 运动到基本位也是无危险的。

联锁防护装置与这些机器运动部件之间的最小距离根据机器的停机性能，按照 GB/T 19876 来确定。

机器还有其他安全功能，如急停、重新启动联锁、复位、操作模式选择等，但在本示例中不予考虑，因此，在图 E.2 和图 E.3 中并没有给出相关的元件。



说明：

⇑——驱动位置。

图 E.2　自动装配机——电路图

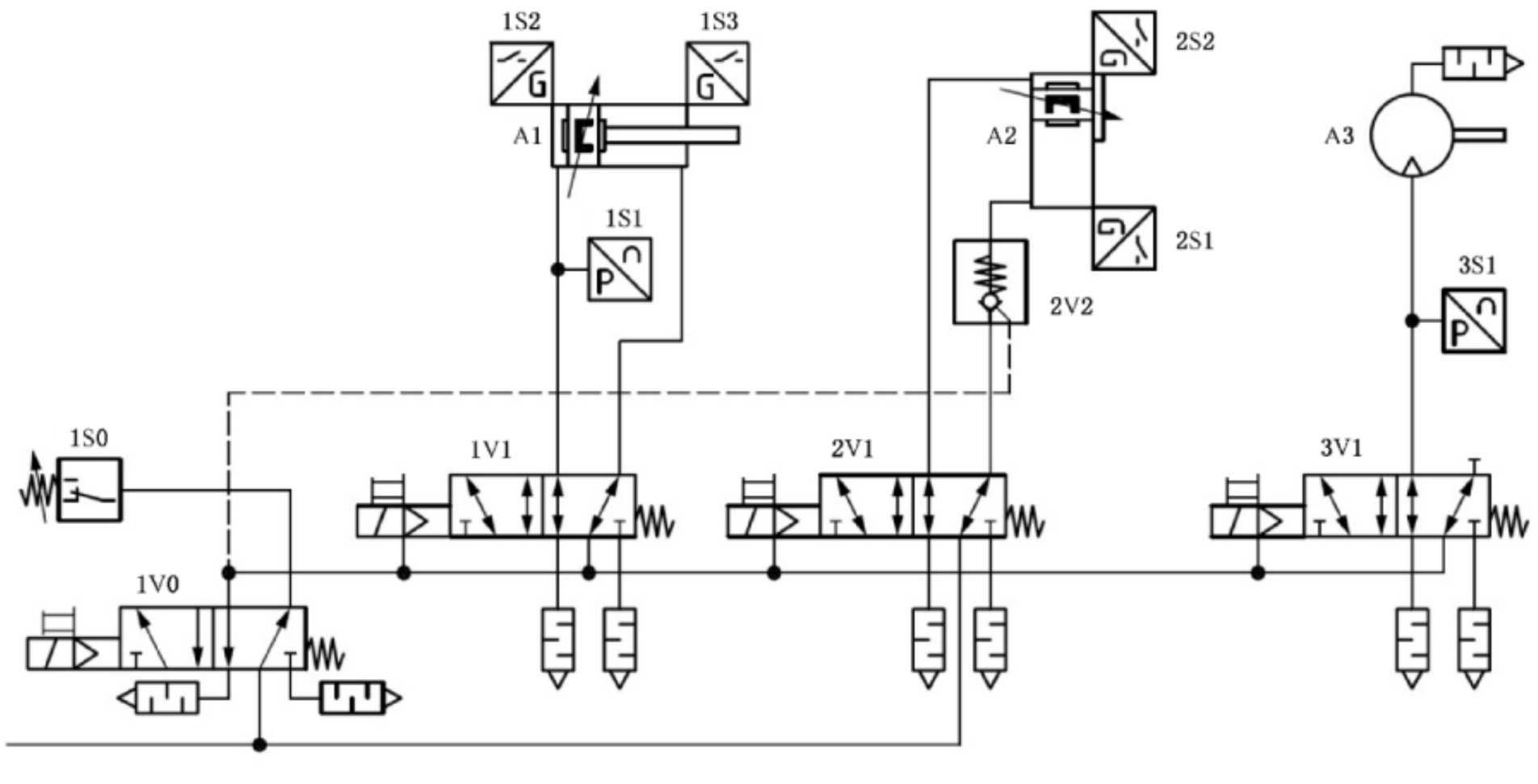


图 E.3　自动装配机——气动回路图

E.4　SRP/CS 的设计

E.4.1　概述

本示例中的控制系统综合采用了机电技术、电子技术和气动技术。

为了达到 SF 1 和 SF 2 的 PL_r，选择 3 类。因此，这些安全功能相关的所有电气和气动部件均采用了多样冗余和监控结构(见图 E.2 和图 E.3)。

为了达到 SF 3 的 PL_r，选择 2 类和 3 类的组合。

从传感器和控制执行器(联锁防护装置的位置开关、保持-运行按钮)传过来的信号被复制并传输至两个不同的 PLC(PLC A 和 PLC B 有着不同的硬件类型)，这两个不同的 PLC 通过专用软件功能模块(SRASW)处理这些信号。每个 PLC 还通过开关路径(独立于其他 PLC 开关路径)来控制旋转台变频器和气压驱动的机器执行器。

出于诊断(交叉监控)和同步的目的，两个 PLC 相互之间通过标准数据总线通信。

本示例中的特殊变频器有一项附加功能(内部延迟)使其功率半导体器件不能发出控制信号(脉冲阻塞)，这种功能可以认为是第二条关闭途径[满足 GB/T 12668.502 的安全扭矩停止(STO)]。

由于禁止马达的变频不能控制马达导致不可控制的减速，因此，这种脉冲阻塞特征不会使旋转马达快速停止。然而，在本示例中，脉冲阻塞仍能在操作者进入危险区之前使旋转台停止。因此，SF 1.0 不需要在脉冲阻塞之前通过受控制的减速直至停止这种特征。

在气动回路中，先导式电磁阀的单稳两位五通方向控制阀(1V1、2V1 和 3V1)控制每个机器执行器(A1、A2 和 A3)的气体供给。三个阀门的控制气体由相同类型的附加阀门(1V0)进行转换，这个附加阀门是一条控制的冗余通道。这个泄压阀的状态由压力开关(1S0)进行监控。A2 的气体供给来自主气源，而 A1 和 A3 的气体供给则来自控制气流供给(1V0)。

在球插入工件期间，也通过两个通道使得运动气缸 A1 的驱动室失能：

——通过在正常位置的转换，由 1V1 放气；

——通过在正常位置的转换，由 1V0 实现失能。

1V1 的状态由限位开关(1S2)监控。

先导控制单向阀(2V2)也从设置在 A2(竖直安装的无杆气缸)下部连接处的 1V0 获得控制。这为停止向下的运动并使机器执行器保持在其基本位(低位)提供了一条冗余通道。

2V1 的状态由限位开关(2S2)监控。

气动马达 A3(螺钉拧紧装置)的气体供应来自控制气流供给(1V0)，而不是主气流供给。这种采用 1V0 和 3V1 并联方式关闭 A3 气流供给的方式，为气动马达提供了一条控制冗余通道，从而确保 3V1 在得能位置失效时，A3 不能继续旋转。3V1 的状态由压力传感器(3S1)监控并提供模拟输出信号。

根据 3 类的要求，需满足基本安全原则和经验证的安全原则，以及 B 类的要求，尤其是还要满足 GB 5226.1 和 GB/T 7932 的要求。

实现 SRP/CS 的元件的特征在表 E.2 中详细给出。

表 E.2　实现 SRP/CS 的元件的特征(图 E.2 和图 E.3 的部件清单)

元件标号	功能	元件	特征	经验证的安全原则[a]	可能的故障排除
B1	监控联锁防护装置的位置	联锁开关	GB 14048.5—2008,包括满足 GB 14048.5—2008,附录 K 的直接打开动作	直接驱动模式	可排除操作时开关触点不能断开的故障。 由于 B1 为直接驱动模式,可排除电气故障
B2	监控联锁防护装置的位置	联锁开关	GB 14048.5—2008	无	无
S4	设定模式期间,产生保持-运行运动	常规打开按钮	—	无	无
PLC A PLC B	处理安全相关和非安全相关的信号	可编程逻辑控制器(PLC)	GB/T 15969.1 和 GB/T 15969.2	无	无
K1	在 PLC A 回路失效时,向变频器发出冗余 STOP 信号	继电器式接触器	GB 14048.5—2008,包括满足 GB 14048.5—2008,附录 L 和 EN 50205 的机械连接触点元件	机械连接触点	无
T1	驱动旋转台电子马达	变频器	变频器有采用脉冲阻塞的附加停止途径	带直接机械连接触点的阻塞继电器	无
G1	测量旋转台电子马达的速度	转动传感器(余弦/正弦)编码器	—	无	无
G2	监控旋转台的运动	脉冲传感器	—	无	无
1V0	控制方向控制阀 1V1、2V1、3V1 和单向阀 2V2 的先导气流	方向控制电磁阀	弹簧加载的阀、两位五通功能、先导操作、内部先导气流供给、带重叠的滑阀	表 B.2 中的“裕量/安全系数”、“安全位置”(采用经验证的弹簧)、“在滑阀中充分的正重叠”	卸压通道 5 处于正常位置时,通道 4 压力增大,因挤出导致的密封失效,无运行能量的情况下滑阀运动
1V1 2V1 3V1	控制球插入气缸 A1 控制螺钉旋入气缸 A2 控制螺钉拧紧装置(启动马达)A3	见 1V0	见 1V0	见 1V0	见 1V0

表 E.2（续）

元件标号	功能	元件	特征	经验证的安全原则[a]	可能的故障排除
2V2	防止螺钉拧紧装置竖直安装的螺钉旋入气缸(A2)坠落的装置	单向阀	先导单向阀、弹簧阀	表 B.2 中“通过载荷压力关闭阀门”	无先导气流打开
1S0	监控阀门 1V0 的状态	压力开关	固定开关点	监控不需要满足基本安全原则(无安全功能)	无
1S1 3S1	监控球插入过程施加的力 监控螺钉拧紧过程施加的力矩(压力)	压力传感器	模拟输出信号	监控不需要满足基本安全原则(无安全功能)	无
1S2、1S3 2S1、2S2	球插入气缸 A1 的限位开关 螺钉旋入气缸 A2 的限位开关	接近开关	磁力测量原则	监控不需要满足基本安全原则(无安全功能)	无
A1	球插入气缸	气缸	根据 GB/T 16855.1—2008 中 3.1.1，不在本部分的范围内		
A2	螺钉旋入气缸	带外部导向的无杆气缸	根据 GB/T 16855.1—2008 中 3.1.1，不在本部分的范围内		
A3	螺钉拧紧装置	气动马达	根据 GB/T 16855.1—2008 中 3.1.1，不在本部分的范围内		

[a] 设计元件时也考虑了基本安全原则(电气元件见表 D.1，气动元件见表 B.1)。

E.4.2 安全功能 SF 1——由打开联锁防护装置触发的安全相关停止功能，并且只要联锁防护装置打开，就防止意外启动

根据机器的技术规范，打开联锁防护装置必定触发四个机器执行器的停止：(i)旋转台(由变频器控制的马达驱动)；(ii)球插入气缸；(iii)螺钉旋入气缸；(iv)螺钉拧紧装置。因此，本功能可由图 E.4 进行标示。

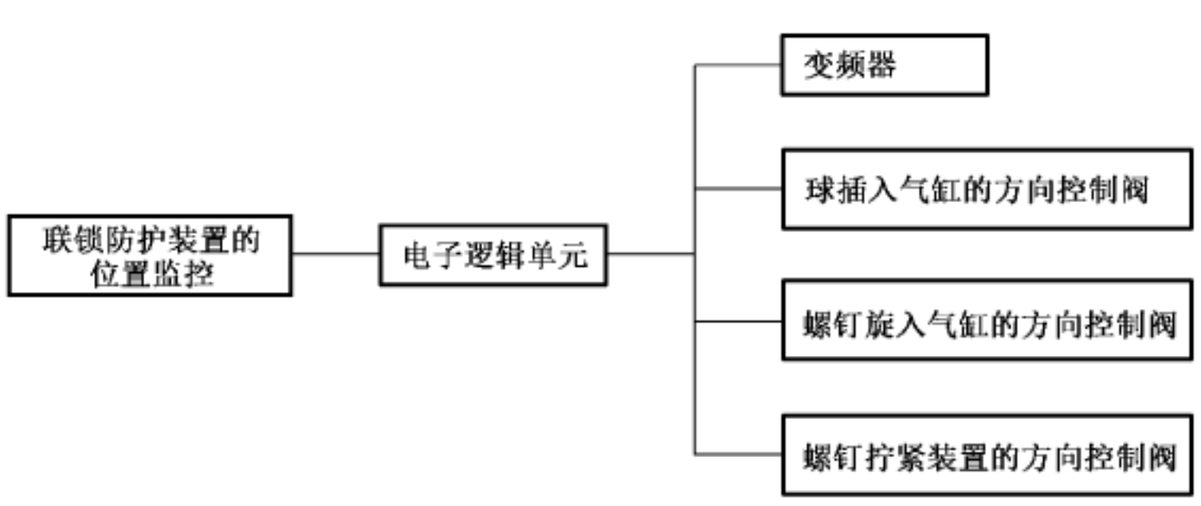


图 E.4 功能模块——SF 1.0、SF 1.1、SF 1.2 和 SF 1.3

当连锁防护装置打开时，PLC A 向变频器(T1a)发出停止信号，触发旋转台的停止。PLC B 监控旋转台通过 G2 减速的结果，并在检测到旋转台静止时，使 K1 失能，从而触发变频器(T1b)的脉冲阻塞。如果旋转台由于 T1a 或 PLC A 发生故障而不能停止时，PLC B 将检测到此故障并且仍然向变频器(T1b)发出自己的停止信号。这是停止功能的第二条独立通道。安全功能中与防止意外启动的那一部分安全功能也与此类似。

打开联锁防护装置使得 PLC A 通过 1V1、2V1 和 3V1 失能来触发球插入气缸、螺钉旋入气缸和螺钉拧紧装置的第一次停止。PLC B 通过 1V0 失能触发这三个执行器的第二次停止。

如果旋转台已经停止，但在联锁防护装置已打开的情况下，球插入和螺钉拧紧工位还在运行，则 PLC A 将立即使 1V1、2V1 和 3V1 失能，并且 PLC B 也将立即使 K1 失能。在一定的延迟后，PLC B 还将使 1V0 失能，以使球插入气缸(A1)完成行程并回到回缩位。

当联锁防护装置处于打开位置时，需要确保 PLC A 失能路径中的故障不会造成不受控的启动。为达到此目标，一旦旋转台马达静止，PLC B 就使 K1 失能，并且为了防止球插入气缸或螺钉旋入气缸的启动，还使 1V0 失能。

SRP/CS 执行 SF 1 的 PL 评估如下：

a) 识别安全相关部件

停止功能 SF 1.0 的安全相关部件及其在通道中的划分，可由安全相关的模块图图 E.5 给出。

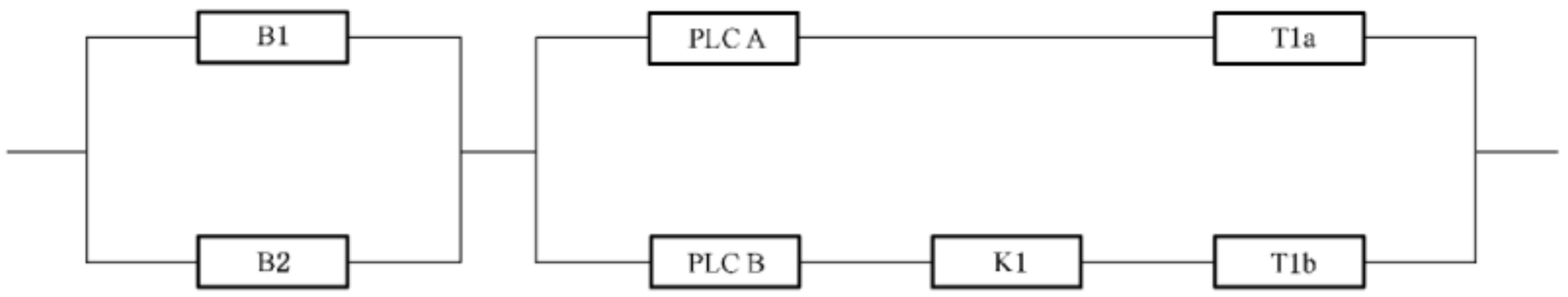
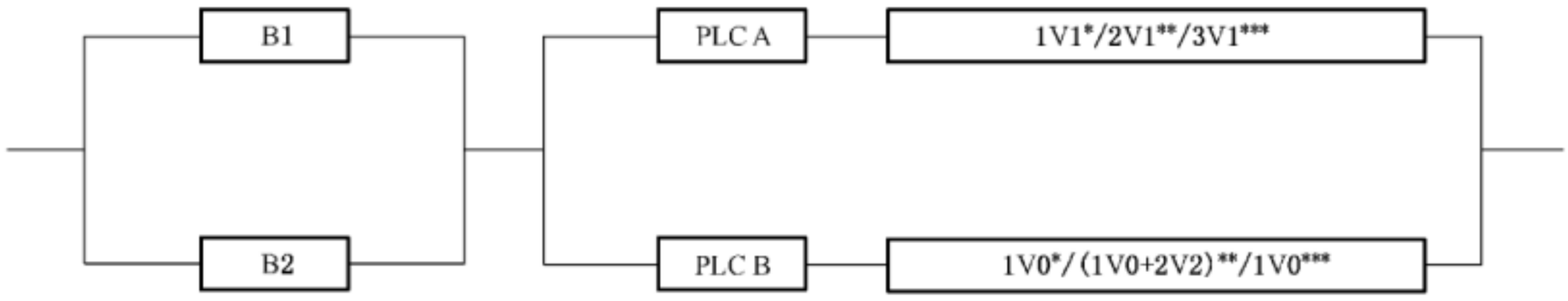


图 E.5 安全相关的模块图——SF 1.0

类似地，停止功能 SF 1.1、SF 1.2 和 SF 1.3 的安全相关部件及其在通道中的划分，可由安全相关的模块图图 E.6 给出。



说明：

* ——SF 1.1；

** ——SF 1.2；

*** ——SF 1.3。

图 E.6　安全相关的模块图——SF 1.1、SF 1.2、SF 1.3

根据图 E.5 和图 E.6，可分别绘制出各自的 3 类指定结构，因此，图 E.5 和图 E.6 可简化为两个 SRP/CS(输入、逻辑/输出)，如图 E.7 所示。

图 E.7　执行安全功能的 SRP/CS 组合

对于每个 SRP/CS，通过 GB/T 16855.1—2008 中 4.5.4 的简化程序估计出各自的 PL。

b)　估计每个通道的 $MTTF_d$

为了估计元件的 $MTTF_d$ 值，采用了制造商提供的可靠性数据。

为了估计通道的 $MTTF_d$，采用了部件计数法(见 GB/T 16855.1—2008 中附录 D)。多样冗余结构使得每个通道的 $MTTF_d$ 值不相同，通过采用对称公式，得出 SF 1.0、SF 1.1、SF 1.2 和 SF 1.3 的两个 SRP/CS_I 和 $SRP/CS_{L/O}$ 的每个通道的 $MTTF_d$ 平均值为 25 年(中)(见 GB/T 16855.1—2008 中 D.2)。

c)　估计 DC_{avg}

通过对不同元件进行的内部试验和监控措施得出的 DC，可计算出两个 SRP/CS 的 DC_{avg}。

根据 GB/T 16855.1—2008 的附录 E，通过 PLC A 和 PLC B 对防护锁定装置开关 B1 和 B2 进行真实性检查，得出 SF 1.0、SF 1.1、SF 1.2 和 SF 1.3 的 SRP/CS_I 的 DC_{avg} 为高(99%)。

SF 1.0、SF 1.1、SF 1.2 和 SF 1.3 的 $SRP/CS_{L/O}$ 提供了以下诊断措施：

——PLC A 通过 K1 触点的位置监控继电器式接触器 K1；

——PLC A 与 PLC B 之间交叉监控；

——PLC B 通过 G2 间接监控 T1a 和 PLC A；

——PLC A 自身通过 1S2、2S2、3S1 和 G1 间接监控其输出卡；

——通过 PLC A 和 PLC B 的内部看门狗监控程序次序；

——PLC A 通过 G1 间接监控 T1a；

——PLC A 通过脉冲阻塞继电器触点的位置监控 T1b；

——PLC A 通过 K1 触点的位置间接监控 PLC B；

——PLC B 自身通过 1S0 间接监控输出卡；

——PLC A 通过 1S2 间接监控 1V1；

——PLC A 通过 2S2 间接监控 2V1；

——PLC A 通过 3S1 间接监控 3V1；

——PLC B 通过 1S0 间接监控 1V0；

——通过过程观察检测 PLC A、T1a 和 1V1、2V1 和 3V1 的故障。

GB/T 16855.1—2008 的附录 E,这些诊断措施使 SF 1.0、SF 1.1、SF 1.2 和 SF 1.3 的 SRP/$CS_{L/O}$的 DC_{avg}达到中(90%)。

d) 估计防止共因失效(CCF)的措施

根据 GB/T 16855.1—2008 的附录 F,针对 SF 1.0、SF 1.1、SF 1.2 和 SF 1.3 的两个 SRP/CS 采取了足够的防止共因失效的措施(分离、差异性、过压保护、环境),每个 SRP/CS 的打分结果为 75 分。

e) 确定每个 SRP/CS 的 PL

每个 SRP/CS 的 PL 确定如下:

——SF 1.0、SF 1.1、SF 1.2 和 SF 1.3 的 SRP/CS_I:

——3 类;

——每个通道的 $MTTF_d$ 为中;

——DC_{avg}为高;

——防止 CCF 的措施为 75 分。

在 GB/T 16855.1—2008 的图 5 中代入这些值,但将 DC_{avg}限制为中(3 类),得出结果为 PLd。

——SF 1.0、SF 1.1、SF 1.2 和 SF 1.3 的 $SRP/CS_{L/O}$:

——3 类;

——每个通道的 $MTTF_d$ 为中;

——DC_{avg}为中;

——防止 CCF 的措施为 75 分。

在 GB/T 16855.1—2008 的图 5 中代入这些值,得出结果为 PLd。

f) 确定执行 SF 1.0、SF 1.1、SF 1.2 和 SF 1.3 的 SRP/CS 组合的 PL

根据 GB/T 16855.1—2008 的 6.3,并考虑 SF 1.0、SF 1.1、SF 1.2 和 SF 1.3 各自的 SRP/CS 具有相同的 PL,SF 1.0、SF 1.1、SF 1.2 和 SF 1.3 整个 SRP/CS 组合的 PL 确定如下:

——PL_{low}=d;

——N_{low}=2。

因此,每个 SF 1.0、SF 1.1、SF 1.2 和 SF 1.3 的 SRP/CS 组合后的 PL 为 PLd。

注:加上所有子系统的 PFH 值来计算得出的 PL 将更加准确。

g) 系统性失效

针对 SF 1.0、SF 1.1、SF 1.2 和 SF 1.3 的 SRP/CS,已根据 GB/T 16855.1—2008 的附录 G,采取了足够的防止系统性失效的措施。

E.4.3 安全功能 SF 2——安全限速(SLS)

当机器处于设定模式并且联锁防护装置处于打开位置时,旋转台只能以安全极限速度运动,该速度由 G1 和 G2 测量。PLC A 监控 G1 的信号,PLC B 则监控 G2 的信号,并且两个 PLC 各自完成期望速度/实际速度的比较。如果变频器 T1a 没有成功将速度降至极限值,则 PLC A 向变频器(T1a)发出停止信号,PLC B 则通过 K1 驱动变频器(T1a)的延迟脉冲阻塞。

a) 识别安全相关部件

安全功能 SF 2 的安全相关部件及其在通道中的划分,可由安全相关的模块图图 E.8 给出。

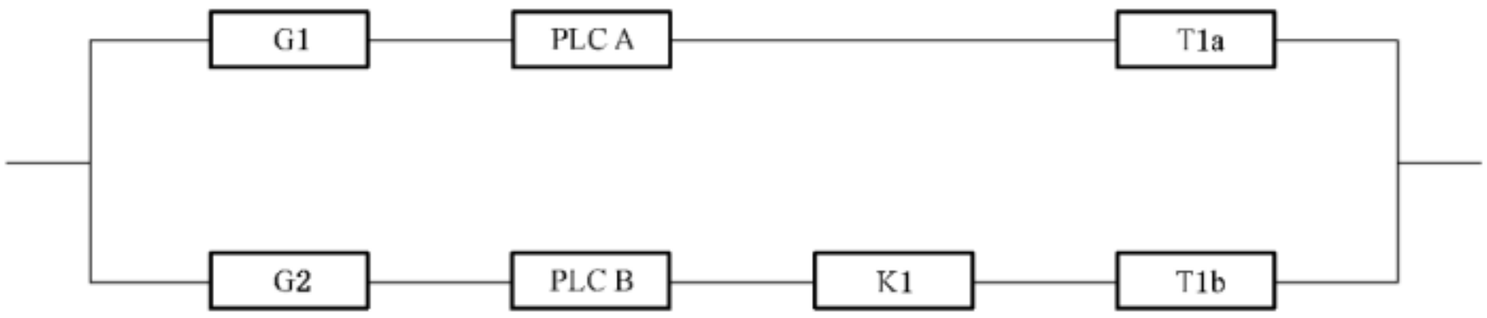


图 E.8 安全相关的模块图——SF 2

根据 GB/T 16855.1—2008 中 4.5.4 的简化程序，估计 SRP/CS 的 PL。

根据图 E.8，可绘制出 3 类指定结构，因此，安全功能由一个 SRP/CS 执行，如图 E.9 所示。

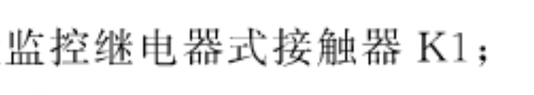


图 E.9　执行安全功能 SF 2 的 SRP/CS

根据 GB/T 16855.1—2008 中 4.5.4 的简化程序，估计 SRP/CS 的 PL。

b)　估计每个通道的 $MTTF_d$

为了估计元件的 $MTTF_d$ 值，采用了制造商提供的可靠性数据。

为了估计通道的 $MTTF_d$，采用了部件计数法（见 GB/T 16855.1—2008 中附录 D）。多样冗余结构使得每个通道的 $MTTF_d$ 值不相同，通过采用对称公式，得出 SRP/CS 每个通道的 $MTTF_d$ 平均值为 25 年（中）。

c)　估计 DC_{avg}

通过对不同元件进行的内部试验和监控措施得出的 DC，可计算出 SRP/CS 的 DC_{avg}。

SRP/CS 提供了以下诊断措施：

——PLC A 通过 K1 触点的位置监控继电器式接触器 K1；

——PLC A 与 PLC B 之间交叉监控；

——PLC B 通过 G2 间接监控 G1、T1a 和 PLC A；

——PLC A 通过脉冲阻塞继电器触点的位置监控 T1b；

——通过 PLC A 和 PLC B 的内部看门狗监控程序次序；

——PLC A 通过 K1 触点的位置间接监控 G2 和 PLC B；

——通过 PLC A 监控 G1；

——监控 G1 和 T1a（正弦/余弦信息的真实性）；

——通过 PLC B 监控 G2（按下 S4 后，PLC B 检查来自 G2 的脉冲；如果没有，则 PLC B 停止 T1b）。

GB/T 16855.1—2008 中附录 E，这些诊断措施使 SRP/CS 的 DC_{avg} 达到中（90%）。

d)　估计防止共因失效（CCF）的措施

根据 GB/T 16855.1—2008 的附录 F，针对 SRP/CS 采取了足够的防止共因失效的措施（分离、差异性、过压保护、环境），因此打分结果为 75 分。

e)　确定每个 SRP/CS 的 PL

SRP/CS 的 PL 确定如下：

——SF 1.0、SF 1.1、SF 1.2 和 SF 1.3 的 SRP/CS_I：

——3 类；

——每个通道的 $MTTF_d$ 为中；

——DC_{avg} 为中；

——防止 CCF 的措施为 75 分。

在 GB/T 16855.1—2008 的图 5 中代入这些值，但将 DC_{avg} 限制为中（3 类），得出结果为 PLd。

f)　系统性失效

针对 SRP/CS，已根据 GB/T 16855.1—2008 中附录 G，采取了足够的防止系统性失效的措施。

E.4.4　安全功能 SF 3——保持-运行模式

联锁防护装置打开时，按下按钮 S4 触发并保持旋转台的运动（以安全极限速度），并在释放按钮时

停止运动。当按钮处于释放位置时,必定能防止意外启动。两个 PLC 处理来自按钮 S4 的信号。

a) 识别安全相关部件

安全功能 SF 3 的安全相关部件及其在通道中的划分,可由安全相关的模块图图 E.10 给出。

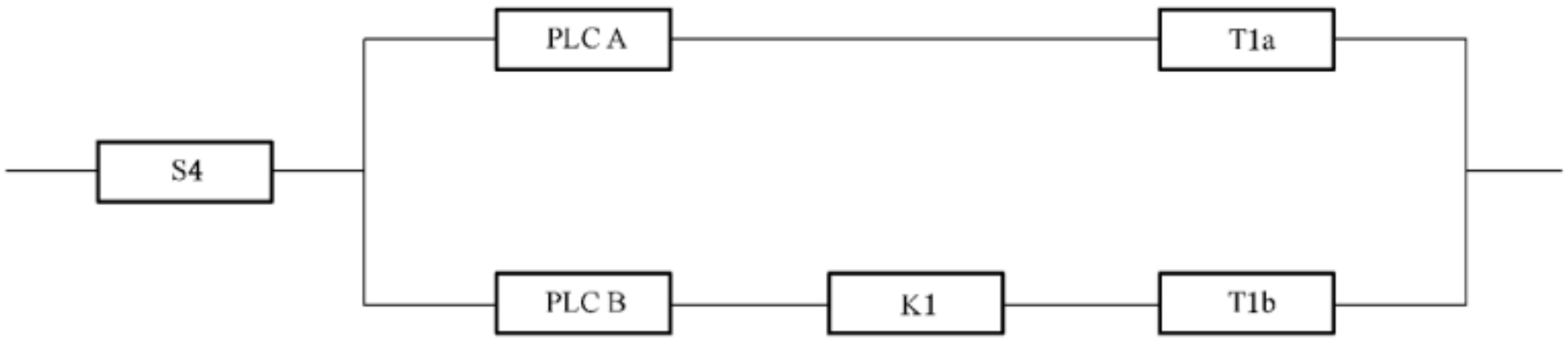


图 E.10 安全相关的模块图——SF 3

图 E.10 中的两部分可分别绘制出 1 类和 3 类指定结构,因此,图 E.10 可简化为两个 SRP/CS(输入、逻辑/输出),如图 E.11 所示。

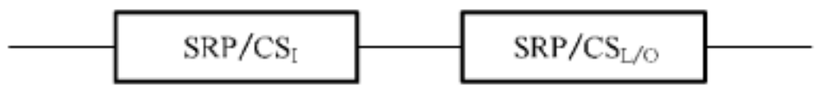


图 E.11 执行安全功能 SF 3 的 SRP/CS 组合

对于每个 SRP/CS,通过 GB/T 16855.1—2008 中 4.5.4 的简化程序估计出各自的 PL。

b) 估计每个通道的 $MTTF_d$

SRP/CS_I(保持-运行装置的按钮)的 $MTTF_d$ 通过制造商给出的 B_{10d} 计算得出,结果为 $MTTF_d$ 为高。

与 SF 1.0 的 $SRP/CS_{L/O}$ 一样,SF 3 的 $SRP/CS_{L/O}$ 每个通道的 $MTTF_d$(大于 25 年)平均值为 25 年(中)。

c) 估计 DC_{avg}

通过对不同元件进行的内部试验和监控措施得出的 DC,可计算出两个 SRP/CS 的 DC_{avg}。

根据 GB/T 16855.1—2008 的附录 E,PLC A 和 PLC B 对保持-运行按钮 S4 的监控(在一定时间范围内高低变化)使得 SRP/CS_I 的 DC_{avg} 为低(75%)。

SF 3 的 $SRP/CS_{L/O}$ 采用了与 SF 1.0 的每个 $SRP/CS_{L/O}$ 相同的监控措施,使得 $SRP/CS_{L/O}$ 的 DC_{avg} 为中(90%)。

d) 估计防止共因失效(CCF)的措施

根据 GB/T 16855.1—2008 的附录 F,针对每个 SRP/CS 采取了足够的防止共因失效的措施(分离、差异性、过压保护、环境),两个 SRP/CS 的打分结果为 75 分。

e) 确定每个 SRP/CS 的 PL

每个 SRP/CS 的 PL 确定如下:

——SRP/CS_I:

——1 类;

——通道的 $MTTF_d$ 为高。

在 GB/T 16855.1—2008 的图 5 中代入这些值,得出结果为 PLc。

——$SRP/CS_{L/O}$:

——3 类;

——每个通道的 $MTTF_d$ 为中;

——DC_{avg} 为中;

——防止 CCF 的措施为 75 分。

在 GB/T 16855.1—2008 的图 5 中代入这些值，得出结果为 PLd。

f) 确定执行 SF 3 的 SRP/CS 组合的 PL

根据 GB/T 16855.1—2008 的 6.3，并考虑 SF 3 的两个 SRP/CS，则整个 SRP/CS 组合的 PL 确定如下：

——$PL_{low}=c$；

——$N_{low}=1$。

因此，SF3 的 SRP/CS 组合的 PL 为 PLc。

g) 系统性失效

针对 SF 3 的 SRP/CS，已根据 GB/T 16855.1—2008 的附录 G，采取了足够的防止系统性失效的措施。

E.5 确认

E.5.1 概述

根据 E.1，本示例仅对安全功能 SF 1.0 和 SF 1.3 的故障状态和诊断措施进行确认。

根据 9.2 和 9.3，故障特性和诊断措施的确认通过审查设计文件、失效分析和补充性的故障插入试验来完成。

需要完成以下步骤：

a) 识别诊断措施以及他们测试/监控的单元(元件、模块)；

b) 对于特定单元，验证指派给每个诊断措施(DC)的 DC 值；

c) 分析系统的故障特性并确定试验实例；

d) 检查每个 SRP/CS 的 DC_{avg} 的计算是否正确；

e) 进行需要的试验，以确认 DC 值。

E.5.2 故障特性和 DC_{avg} 的确认

检查设计文件(SRP/CS 的安全相关模块图和诊断措施清单)，以确定在设计原理中假定的以下内容对于所有安全功能是否正确：

——安全相关模块图中的与每个 SRP/CS 相关的模块(元件)和 SRP/CS 组合；

——诊断措施和被监控单元。

采用 FMEA 检查指派给每个 SRP/CS 的每个被监控单元的 DC 值，以及系统的故障特性。

由于安全功能 SF 1 必须实现安全相关停止功能和后续的防止意外启动功能，因此，针对每一条要求分别在每一行针对每个相关的元件进行失效分析。

分析过程中，采用了附录 A、附录 B、附录 C 和附录 D 中相应的故障清单。

考虑了安全功能 SF 1.0 和 SF 1.3 的 FMEA，包括试验实例。

E.5.3 SF 1.0 和 SF 1.3 的 FMEA 和 DC_{avg}

E.5.3.1 SF 1.0

为了便于 SF 1.0 的分析，重新绘制了安全相关的模块图，如图 E.12 所示。

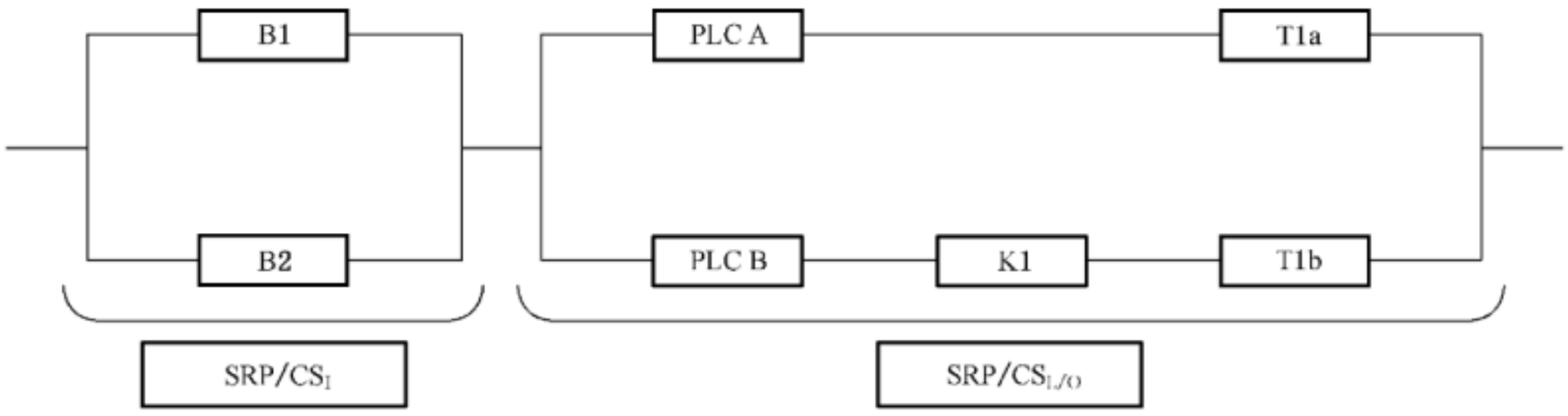


图 E.12　安全相关模块图——SF 1.0

见表 E.3 和表 E.4。

表 E.3　SF 1.0 的 SRP/CS$_I$ 元件的 FMEA 及 DC 的估计

	元件/单元	潜在故障	故障检测	效果/反应	试验确定
F1	联锁开关 B1	防护装置打开时触点不能断开(机械故障)[a]	当需要安全功能(联锁防护装置打开,真实性检查)时,PLC A 和 PLC B 通过 B2 信号的变化分别检测到故障	PLC A 通过 T1a,PLC B 通过 K1 和 T1b 使电机 M1 停止,并防止重新启动	在防护装置打开之前,在每个 PLC 的相关输入端施加静态高电平
F2		防护装置打开时无危险故障(故障排除)	—	—	—
PLC A 和 PLC B 对 B1 和 B2 进行的真实性检查使 B2 的 DC 为 99%(见 GB/T 16855.1—2008 中表 E.1)。					
F3	联锁开关 B2	防护装置打开时触点不能断开(电气或机械故障)	当需要安全功能(联锁防护装置打开,真实性检查)时,PLC A 和 PLC B 通过 B1 信号的变化分别检测到故障	PLC A 通过 T1a,PLC B 通过 K1 和 T1b 使电机 M1 停止,并防止重新启动	在防护装置打开之前,在每个 PLC 的相关输入端施加静态高电平
F4		防护装置打开时触点自发闭合(机械故障)	由于 B1 中没有相应的信号变换,PLC A 和 PLC B 分别立即检测到故障	PLC A 通过 T1a,PLC B 通过 K1 和 T1b 使电机 M1 停止,并防止重新启动	在防护装置打开时,在每个 PLC 的相关输入端施加静态高电平
PLC A 和 PLC B 对 B1 和 B2 进行的真实性检查使 B1 的 DC 为 99%(见 GB/T 16855.1—2008 中表 E.1)。					
注:故障分析并不包括导线,这是因为一般认为导线只有系统性原因才会失效。					
[a] 由于 B1 为直接驱动模式,因此可排除电气故障(见 GB 14048.5—2008 中附录 K)。					

通过分析可推断,SRP/CS$_I$ 中的任何单一故障将被立即检测到,或者在下一次需要安全功能之前被检测到。发生单一故障时,总是要执行安全功能并防止重新启动。

分析结果表明,设计过程假定的 B1 和 B2 的 DC 值(高)是足够的。由于两个元件的 DC 相等(99%),因此,SRP/CS$_I$ 的 DC$_{avg}$ 也为高(99%)。这与设计时的估计值是一致的。

这些特征是 3 类的典型特征。设计(见 E.4.1)时为了满足 E.3 中给出的安全要求规范(PL$_r$)也选择了 3 类。

可通过表 E.3 最后一列给出的试验来检测诊断措施是否得到正确实施。

表 E.4　SF 1.0 的 SRP/$CS_{L/O}$元件的 FMEA 及 DC 的估计

	元件/单元	潜在故障	故障检测	效果/反应	试验确定
F1	PLC A	在输入/输出卡上的粘连故障，或者 CPU 中粘连、错误的译码或不执行，这些故障在防护装置打开之前或打开时，阻止 PLC A 向 T1a 发出停止指令	通过 PLC B 读取 G2 的信号并将其时间相关的信号与预期的转数变化进行比较，从而检测到故障。 某些故障是由 PLC A 在电机 M1 功能性停止时或在需要安全功能时通过读取 G1 的信号检测到的。 其他故障可由 PLC A 中的内部看门狗(WD[a])功能在早期检测到	防护装置打开时，在一定的时间延迟后，PLC B 通过 K1 和 T1b 使电机 M1 停止，并防止重新启动。 对于故障由 PLC A 在电机 M1 功能性停止时通过读取 G1 的信号检测到的情况，PLC A 通知 PLC B，其结果使电机 M1 停止并由 PLC B 防止重新启动。 对于故障由 WD 检测到的情况，PLC A 在需要安全功能之前或者在电机 M1 功能性停止之前，通过 T1a 使电机 M1 停止并防止重新启动，然后通知 PLC B	在防护装置打开之前，在 PLC A 的停止输出端施加静态高电平
F2		在输入/输出卡上的固定逻辑型故障，或者 CPU 中固定逻辑型、错误的译码或不执行，这些故障在防护装置打开时从 T1a 删除 PLC A 的停止指令	由于防护装置打开时电机由 PLC B 通过 K1 和 T1b 保持停止，通过 PLC B 读取 G2 的信号不能检测到故障。 某些故障是(如输出卡)在关闭防护装置时由 PLC A 通过读取 G1 的信号检测到的。 上述故障及附加故障由操作者在防护装置关闭时通过过程观察检测到，或者在下一次需要安全功能(打开防护装置)时，由 PLC B 检测到。 其他故障可由 PLC A 的 WD[a] 功能在早期检测到	防护装置打开时，由 PLC B 通过 K1 和 T1b 使电机 M1 保持停止。 对于故障由 PLC A 在防护装置关闭时通过读取 G1 的信号检测到的情况，PLC A 通知 PLC B，其结果使 PLC B 防止电机 M1 意外启动。 对于故障由 WD 检测到的情况，PLC A 使电机 M1 保持停止并通过 T1a 防止重新启动，然后通知 PLC B	在防护装置打开时，将启动信号传输至变频器
PLC B 通过 G2 间接监控 PLC A，PLC A 通过 G1 间接监控自己的输出卡，通过内部看门狗监控程序次序，以及通过过程观察检测故障，使得 PLC A 的 DC 达到 90%(见 GB/T 16855.1—2008 中表 E.1)。 可以认为上述措施与 GB/T 16855.1—2008 中表 E.1 的注 2 相关。					

表 E.4（续）

	元件/单元	潜在故障	故障检测	效果/反应	试验确定
F3	变频器 T1a	变频器控制和动力电子元件的粘连故障和其他复杂的内部故障，这些故障在防护装置打开之前或打开时，阻止 T1a 停止电机	在需要安全功能时，通过 PLC B 读取 G2 的信号检测到故障。 在电机 M1 功能性停止时或在需要安全功能时，通过 PLC A 读取 G1 的信号检测到故障	防护装置打开时，在一定的时间延迟后，PLC B 通过 K1 和 T1b 使电机 M1 停止，并防止重新启动。 在功能性停止期间检测到故障时，PLC A 通知 PLC B，其结果使 PLC B 停止并防止其重新启动	在防护装置打开之前或打开时，将变频器的停止输入设置为高电平
F4		变频器控制和动力电子元件的粘连故障和其他复杂的内部故障，这些故障在防护装置打开时，向 T1a 的功率半导体器件发出门信号	在防护装置打开时，由于 PLC B 通过 K1 和 T1b 使电机 M1 保持停止，因此，通过 PLC B 读取 G2 的信号不能检测到故障。 在防护装置关闭时，将由操作者通过过程观察来检测故障。 在防护装置关闭时，还能由 PLC A 通过读取 G1 的信号来检测故障	防护装置打开时，由 PLC B 通过 K1 和 T1b 使电机 M1 保持停止。 在防护装置关闭时，电机发生（不危险的）意外启动。 检测到故障时，PLC A 通知 PLC B，其结果使 PLC B 防止电机 M1 意外启动并防止其重新启动	在防护装置打开时，将启动信号传输至变频器
PLC B 通过 G2 间接监控 T1a，PLC A 通过 G1 间接监控 T1a，以及通过过程观察检测故障，使得 T1a 的 DC 达到 99%。					
F5	PLC B	在输入/输出卡上的粘连故障，或者 CPU 中粘连、错误的译码或不执行，这些故障在防护装置打开之前或打开时，阻止 PLC B 关闭 K1	需要安全功能时，通过 PLC A 监控 K1 的机械连接反馈触点来检测故障。 某些故障可由 PLC B 的 WD[a] 功能在早期检测到	防护装置打开时，PLC A 通过 T1a 使电机 M1 立即停止，并防止重新启动。 对于故障由 WG 检测的情况，PLC B 通知 PLC A，然后在需要安全功能之前，通过 T1b 使电机 M1 停止并防止重新启动	在防护装置打开时，使 K1 保持在得电位置
F6		在输入/输出卡上的粘连故障，或者 CPU 中粘连、错误的译码或不执行，这些故障在防护装置打开时从 K1 删除 PLC B 的停止指令	通过 PLC A 监控 K1 的机械连接反馈触点立即检测到故障。 某些故障可由 PLC B 的 WD[a] 功能在早期检测到	防护装置打开时，由 PLC A 通过 T1a 使电机 M1 保持停止，并防止重新启动。 对于故障由 WG 检测的情况，PLC B 通过 T1b 使电机 M1 停止并防止重新启动，并通知 PLC A	在防护装置打开时，打开 K1 至得电位置

表 E.4（续）

	元件/单元	潜在故障	故障检测	效果/反应	试验确定
PLC A 通过 K1 反馈触点的位置间接监控 PLC B，以及通过内部看门狗监控程序次序，使得 PLC B 的 DC 达到 90%。					
F7	继电器式接触器 K1	防护装置打开时，触点不能断开（电气故障，如触点熔焊）	在需要安全功能时，PLC A 通过监控 K1 的机械连接反馈触点来检测到故障	防护装置打开时，PLC A 通过 T1a 使电机 M1 立即停止，并防止重新启动	在防护装置打开时，使 K1 的触点保持在 ON 位置
F8		防护装置打开时无危险故障（故障排除）	—	—	—
PLC A 通过 K1 的机械连接反馈触点监控继电器式接触器 K1，使得 K1 的 DC 达到 99%。					
F9	变频器 T1b	防护装置打开时，内部继电器式触点不能断开	在需要安全功能时，PLC A 通过监控 T1b 的内部继电器的机械连接反馈触点来检测到故障	防护装置打开时，PLC A 通过 T1a 使电机 M1 立即停止，并防止重新启动	在防护装置打开时，使 T1b 中的阻塞继电器的线圈输出保持在高电平
F10		防护装置打开时无危险故障（故障排除）	—	—	—
PLC A 监控 T1b 的内部（脉冲阻塞）继电器，使得 T1b 的 DC 达到 99%。					
注：可以认为大多数 PLC 故障发生在输入/输出卡上，并且为固定逻辑型（所有 PLC 故障的 90%），但 PLC 的 WD 功能只能检测到某些影响程序次序的故障。					
[a] PLC 某些不会导致安全功能失效（如 PLC 无法向驱动或阀门发出停机指令，或者无法保持驱动或阀门的停机指令）的内部故障，可由 WD 功能检测到。					

通过分析可推断，SRP/CS_I 中的任何单一故障将被立即检测到，在电机 M1 功能性停止时被检测到，或者在下一次需要安全功能之前被检测到。发生单一故障时，通常能执行安全功能。如果 PLC A 和 PLC B 中存在未检测到的故障，只有一条通道可能重新启动。

分析结果表明，设计 SRP/$CS_{L/O}$ 时假定的 DC 值是足够的。根据 SRP/$CS_{L/O}$ 中采用的不同元件的 $MTTF_d$ 和 DC 的估计值，得出 DC_{avg} 为中（90%）。这与设计时的估计值是一致的。

这些特征是 3 类的典型特征。设计（见 E.4.1）时为了满足 E.3 中给出的安全要求规范（PL_r）也选择了 3 类。

可通过表 E.4 最后一列给出的试验来检测诊断措施是否得到正确实施。

E.5.3.2 SF 1.3

为了便于 SF 1.3 的分析，重新绘制了安全相关的模块图，如图 E.13 所示。

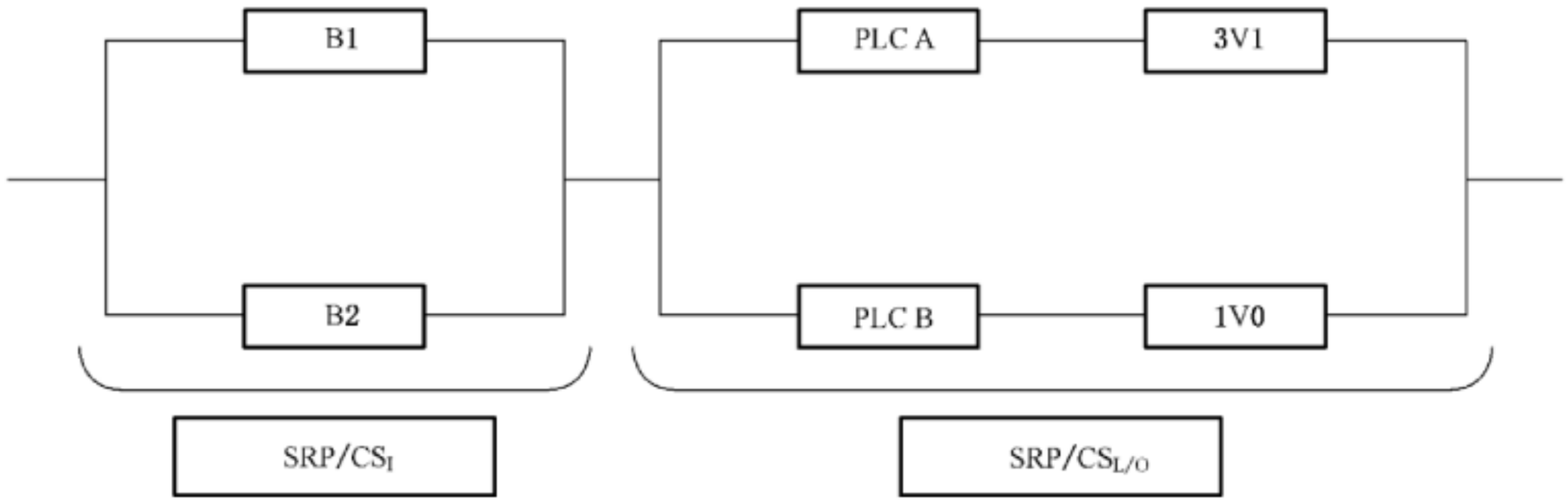


图 E.13　安全相关模块图——SF 1.3

对于 SF 1.3 的 SRP/CS$_I$，诊断措施和被测试/监控的单元与 SF 1.0 是一致的，因此，SRP/CS$_I$ 的 DC$_{avg}$ 也为高(99%)。

见表 E.5。

表 E.5　SF 1.3 的 SRP/CS$_{L/O}$的 FMEA

	元件/单元	潜在故障	故障检测	效果/反应	试验确定
F1	PLC A	在输入/输出卡上的粘连故障，或者 CPU 中粘连、错误的译码或不执行，这些故障在防护装置打开之前或打开时，阻止 PLC A 关闭 3V1	某些故障(如输出卡)是由 PLC A 在气动马达 A3 功能性停止时或在需要安全功能时通过读取压力传感器 3S1 的信号检测到的。 其他故障可由 PLC A 的 WD[a] 功能在早期检测到	防护装置打开时，在一定的时间延迟后，PLC B 通过 1V0 使气动马达 A3 停止。 对于故障由 PLC A 在气动马达 A3 功能性停止时通过读取 3S1 的信号检测到的情况，PLC A 通知 PLC B，其结果使 PLC B 通过 3V1 使气动马达 A3 停止，并防止重新启动。 对于故障由 WD 检测到的情况，PLC A 在需要安全功能之前或者在气动马达 A3 功能性停止之前，通过 3V1 使气动马达 A3 停止并防止重新启动，然后通知 PLC B	在防护装置打开之前，在 PLC A 的 3V1 输出端施加静态高电平
F2		在输入/输出卡上的粘连故障，或者 CPU 中粘连、错误的译码或不执行，这些故障在防护装置打开时，使 PLC A 打开 3V1	某些故障(如输出卡)是在防护装置关闭时，由 PLC A 通过读取压力传感器 3S1 的信号检测到的。 其他故障可由 PLC A 的 WD[a] 功能在早期检测到	防护装置打开时，由 PLC B 通过 1V0 使气动马达 A3 保持停止。 在关闭防护装置时，PLC B 使 1V0 储能，并且气动马达 A3 将重新启动(无危险)。 对于故障由 PLC A 在关闭防护装置时通过读取 3S1 的信号检测到的情况，PLC A 通知 PLC B，其结果使 PLC B 防止气动马达 A3 意外启动，并防止其重新启动。 对于故障由 WD 检测到的情况，PLC A 使气动马达 A3 保持停止并通过 3V1 防止重新启动，然后通知 PLC B	在防护装置打开时，将 PLC A 的 3V1 输出变为高电平

表 E.5（续）

	元件/单元	潜在故障	故障检测	效果/反应	试验确定
PLC A 通过 3S1 间接监控自己的输出卡，以及通过内部看门狗监控程序次序，使得 PLC A 的 DC 达到 90%。					
F3	方向控制电磁阀 3V1	在防护装置打开之前或打开时，无法打开（粘连在末端位置）、不完全打开（粘连在任意中间位置）或者打开时间改变	在需要安全功能时，或者在气动马达 A3 功能性停止时，由 PLC A 通过读取压力传感器 3S1 的信号检测到故障。 也可由操作者通过过程观察检测到故障	防护装置打开时，在一定的时间延迟后，PLC B 通过 1V0 使气动马达 A3 停止。 检测到故障时，PLC A 通知 PLC B，其结果使 PLC B 通过 1V0 使气动马达 A3 停止并防止其重新启动	在防护装置打开时，将 3V1 的电气和气动控制信号保持在高电平
F4		防护装置打开时，初始切换位置的自发改变（无输入信号）。 **注**：由于 3V1 采用了经验证的弹簧，并在在正常安装和操作条件下使用，因此，此故障可以排除	—	—	—
PLC A 通过 3S1 间接监控 3V1，以及通过过程观察检测故障，使得 3V1 的 DC 达到 99%。					
F5	PLC B	在输入/输出卡上的粘连故障，或者 CPU 中粘连、错误的译码或不执行，这些故障在防护装置打开之前或打开时，阻止 PLC B 关闭 1V0	某些故障（如输出卡）是由 PLC B 在需要安全功能时通过读取压力开关 1S0 的信号检测到的。 其他故障可由 PLC B 的 WD[a] 功能在早期检测到	防护装置打开时，PLC A 通过 3V1 使气动马达 A3 立即停止。 对于故障由 PLC B 通过读取压力开关 1S0 的信号检测到的情况，PLC B 通知 PLC A 并使 K1 保持释放，其结果使 PLC A 防止重新启动。 对于故障由 WD 检测到的情况，PLC B 通知 PLC A，然后在需要安全功能之前，通过 1V0 使气动马达 A3 停止并防止重新启动	在防护装置打开之前，在 PLC B 的 1V0 输出端施加静态高电平
F6		在输入/输出卡上的粘连故障，或者 CPU 中粘连、错误的译码或不执行，这些故障在防护装置打开时，使 PLC B 打开 1V0	某些故障（如输出卡）由 PLC B 通过读取压力开关 1S0 的信号立即检测到的。 其他故障可由 PLC B 的 WD[a] 功能在早期检测到	防护装置打开时，由 PLC A 通过 3V1 使气动马达 A3 保持停止。 对于故障由 PLC B 通过读取压力开关 1S0 的信号检测到的情况，PLC B 通知 PLC A 并使 K1 保持释放，其结果使 PLC A 防止重新启动。 对于故障由 WD 检测到的情况，PLC B 通知 PLC A，然后通过 1V0 使气动马达 A3 保持停止并防止重新启动	在防护装置打开时，将 PLC B 的 1V0 输出变为高电平

表 E.5（续）

	元件/单元	潜在故障	故障检测	效果/反应	试验确定
PLC B 通过 1S0 间接监控自己的输出卡，PLC A 通过 K1 的反馈触点的位置间接监控 PLC B，以及通过内部看门狗监控程序次序，使得 PLC B 的 DC 达到 90%。					
F7	方向控制电磁阀 1V0	在防护装置之前或打开时，无法打开（粘连在末端位置）、不完全打开（粘连在任意中间位置）或者打开时间改变	在需要安全功能时，由 PLC B 通过读取压力开关 1S0 的信号检测到故障	防护装置打开时，PLC A 通过 3V1 使气动马达 A3 立即停止。对于故障由 PLC B 通过读取压力开关 1S0 的信号检测到的情况，PLC B 通知 PLC A 并使 K1 保持释放，其结果使 PLC A 防止重新启动	在防护装置打开之前，在 PLC B 的 1V0 输出端施加静态高电平
F8	电磁阀 1V0	防护装置打开时，初始切换位置的自发改变（无输入信号）。 **注**：由于 1V0 采用了经验证的弹簧，并在正常安装和操作条件下使用，因此，此故障可以排除。	—	—	—
PLC B 通过 1S0 间接监控 1V0，使得 1V0 的 DC 达到 99%。					
注：可以认为大多数 PLC 故障发生在输入/输出卡上，并且为固定逻辑型（所有 PLC 故障的 90%），但 PLC 的 WD 功能只能检测到某些影响程序次序的故障。					
[a] PLC 某些不会导致安全功能失效（如 PLC 无法向驱动或阀门发出停机指令，或者无法保持驱动或阀门的停机指令）的内部故障，可由 WD 功能检测到。					

通过分析可推断，SRP/CS 中的大多数单一故障将被立即检测到，在电机 A3 功能性停止时被检测到，或者在下一次需要安全功能之前被检测到。发生单一故障时，通常能执行安全功能。只有未检测到 PLC A 和 PLC B 中有故障时，只有一条通道可能重新启动。

分析结果表明，设计 SRP/$CS_{L/O}$时假定的 DC 值是足够的。根据 SRP/$CS_{L/O}$中采用的不同元件的 $MTTF_d$ 和 DC 的估计值，得出 DC_{avg} 为中（90%）。这与设计时的估计值是一致的。

这些特征是 3 类的典型特征。设计（见 E.4.1）时为了满足 E.3 中给出的安全要求规范（PL_r）也选择了 3 类。

可通过表 E.5 最后一列给出的试验来检测诊断措施是否得到正确实施。

参 考 文 献

[1] GB/T 1303.1 电气用热固性树脂工业硬质层压板 第1部分:定义、分类和一般要求

[2] GB 4208 外壳防护等级(IP代码)

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

[4] GB/T 7826 系统可靠性分析技术 失效模式和影响分析(FMEA)程序

[5] GB/T 7829 故障树分析程序

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

[7] GB 13539.1 低压熔断器 第1部分:基本要求

[8] GB 14048(所有部分) 低压开关设备和控制设备

[9] GB 14536(所有部分) 家用和类似用途电自动控制器

[10] GB/T 15329.1 橡胶软管及软管组合件 织物增强液压型 第1部分:油基流体用

[11] GB/T 15969.1 可编程序控制器 第1部分:通用信息

[12] GB/T 15969.2 可编程序控制器 第2部分:设备要求和测试

[13] GB 16655 械械安全 集成制造系统 基本要求

[14] GB 16754 械械安全 急停 设计原则

[15] GB/T 16935(所有部分) 低压系统内设备的绝缘配合

[16] GB/T 17446—2012 流体传动系统及元件 词汇

[17] GB/T 17454(所有部分) 机械安全 压敏保护装置

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

[19] GB 19212(所有部分) 电力变压器、电源装置和类似产品的安全

[20] GB/T 19670—2005 械械安全 防止意外启动

[21] GB/T 19671 械械安全 双手操纵装置 功能状况及设计原则

[22] GB/T 19876 械械安全 与人体部位接近速度相关的安全防护装置的定位

[23] GB/T 21711.1 基础机电继电器 第1部分:总则与安全要求

[24] ISO 4413 Hydraulic fluid power—General rules and safety requirements for systems and their components

[25] ISO 4414 Pneumatic fluid power—General rules and safety requirements for systems and their components

[26] ISO 4960 Cold-reduced carbon steel strip with a mass fraction of carbon over 0.25%

[27] ISO 14119:2013 Safety of machinery—Interlocking devices associated with guards—Principles for design and selection

[28] IEC 61078 Analysis techniques for dependability—Reliability block diagram and boolean metheads

[29] IEC 61165 Application of Markov techniques

[30] IEC 61249(all parts) Materials for printed boards and other interconnecting structures

[31] IEC 61508-2:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 2:Requirements for electrical/electronic/programmable electronic safety-related systems

[32] EN 952 Safety of machinery—Safety requirements for fluid power systems and their components—Hydraulics

[33] EN 953 Safety of machinery—Safety requirements for fluid power systems and their components—Pneumatics

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

[35] JESD22A121.01 Test Method for Measuring Whisker Growth on Tin and Alloy Surfaces Finishes[1)]

[36] JESD201 Test Method for Measuring Whisker Growth on Tin and Alloy Surfaces Finishes[1)]

1) JEDEC Solid State Technology Association,2500 Wilson Boulevard,Arliington,VA 22201-3834,www.jedec.org/download/search/22a1121-01.pdf

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2部分:确认
GB/T 16855.2—2015/ISO 13849-2:2012
*
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.gb168.cn
服务热线:400-168-0010
010-68522006
2016年5月第一版
*
书号:155066·1-54017

GB/T 16855.2-2015