ICS 13.110
CCS J 09

中华人民共和国国家标准

GB/T 41118—2021

机械安全　安全控制系统设计指南

Safety of machinery—Guideline for the design of safety control systems

2021-12-31 发布　　2022-07-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 1
5　迭代设计过程 …… 2
6　设计准备 …… 3
6.1　风险评估 …… 3
6.2　识别安全功能 …… 3
6.3　规定安全功能的特征 …… 3
6.4　确定所需性能等级 …… 4
6.5　编制安全需求说明 …… 5
7　安全控制系统的设计 …… 6
7.1　概述 …… 6
7.2　编制安全设计说明 …… 7
7.3　设计硬件系统 …… 7
7.4　开发安全相关软件 …… 11
7.5　验证安全功能的 PL …… 12
7.6　形成设计文件 …… 12
8　确认 …… 13
8.1　确认原则 …… 13
8.2　分析 …… 13
8.3　测试 …… 13
8.4　归档 …… 13
附录 A（资料性）　压力机安全控制系统设计及验证示例 …… 14
附录 B（资料性）　木工圆锯机安全控制系统设计及验证示例 …… 19
附录 C（资料性）　码垛机安全控制系统设计及验证示例 …… 22
参考文献 …… 25

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国机械安全标准化技术委员会(SAC/TC 208)提出并归口。

本文件起草单位：皮尔磁电子(常州)有限公司、上海辰竹仪表有限公司、合肥磐石自动化科技有限公司、深圳国技仪器有限公司、十一维度(厦门)网络科技有限公司、漳州科晖专用汽车制造有限公司、焙之道食品(福建)有限公司、漳州佳龙科技股份有限公司、浙江武精机器制造有限公司、浙江佛尔泰智能设备有限公司、安士能电器(上海)有限公司、台州龙江化工机械科技有限公司、南京理工大学、中机生产力促进中心、四川蜀兴优创安全科技有限公司、泰瑞机器股份有限公司、奥煌检测技术服务(上海)有限公司、北京机械工业自动化研究所有限公司、广东康鑫新材料有限公司、南京林业大学、惠州学院、巨力自动化设备(浙江)有限公司、苏州安高智能安全科技有限公司、江苏省特种设备安全监督检验研究院、佛山市南海旋旖机械设备有限公司、广东利英智能科技有限公司、江苏长虹智能装备股份有限公司、佛山市定中机械有限公司、西安凯益金电子科技有限公司、中汽认证中心有限公司、东莞市雄大机械有限公司、西安立贝安智能科技有限公司、江苏强凯检测有限公司、西安宁康特数据服务有限公司、广东全伟工业科技有限公司、上海彩琪信息科技服务中心、平湖李挺机械制造有限公司、山东佐耀智能装备股份有限公司、枣庄市慧天美亚保温节能建材有限公司、广东雪莹电器有限公司、义乌市粤鑫模具科技有限公司、黎明职业大学。

本文件主要起草人：赵彬、项楠、熊从贵、舒玉恒、黄之炯、周婷、朱平、余海箭、吴建伟、薛从福、蔡松华、赵阳、徐志坚、黄剑锋、居里锴、刘治永、陆晓光、秦培均、黄飞、徐文超、魏建鸿、章日平、宋小宁、陈卓贤、庞艳、袁超群、仇云杰、李勤、钟耀华、向梅、吴向亮、程红兵、居荣华、倪燎勇、皮玉林、沈海波、王哲维、付卉青、赖秀珍、李挺、黄勇、沈德红、王洪伟、宋光升、陈小全、颜国霖、林通、王明华、李立言、李忠、钟云山、姜涛、张晓飞。

引　言

机械领域安全标准体系由以下几类标准构成：

——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)，涉及在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，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(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。

根据 GB/T 15706，本文件属于 B 类标准。

本文件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文件的起草。

此外，本文件预定用于起草 C 类标准的标准化机构。

本文件规定的要求可由 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。

急停装置、联锁装置、双手操纵装置等安全防护装置安全功能的实现依赖于安全控制系统。GB/T 16855.1给出了安全控制系统的设计原则，本文件的目的是指导设计人员如何根据GB/T 16855.1设计安全控制系统。

本文件的附录 A、附录 B 和附录 C 分别给出了压力机、木工圆锯机及码垛机安全控制系统的设计及验证示例。

机械安全　安全控制系统设计指南

1　范围

本文件给出了安全控制系统的设计迭代过程、设计准备、设计实施以及确认的指南。

本文件适用于GB/T 15706—2012界定的机械的安全控制系统的设计及升级。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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

GB/T 16855.1—2018　机械安全　控制系统安全相关部件　第1部分：设计通则

3　术语和定义

GB/T 15706—2012和GB/T 16855.1—2018界定的以及下列术语和定义适用于本文件。

3.1

安全控制系统　safety control system

执行规定的安全功能，以控制或维持某一受控设备的安全状态，并通过其自身或其他控制系统，以及外部风险减小措施而实现所需性能等级(PL_r)的特定控制系统。

3.2

平均危险失效周期数　mean cycles to dangerous failure

B_{10D}

直到10%的元件发生危险失效时的平均循环次数。

注：元件通常指机械元件、机电元件、气动元件或液压元件。

4　缩略语

下列缩略语适用于本文件。

AOPD：有源光电保护装置(Active Optoelectronic Protective Device)

CCF：共因失效(Common Cause Failure)

DC：诊断覆盖率(Diagnostic Coverage)

FMEA：失效模式及影响分析(Failure Mode and Effects Analysis)

$MTTF_D$：平均危险失效间隔时间(Mean Time to Dangerous Failure)

PFH_D：每小时平均危险失效概率(Average Probability of Dangerous Failure Per Hour)

PL：性能等级(Performance Level)

RFID：射频识别(Radio Frequency IDentification)

SF：安全功能(Safety Function)

SRASW：安全相关应用软件(Safety-related Application Software)
SRESW：安全相关嵌入式软件(Safety-related Embedded Software)
SRP/CS：控制系统安全相关部件(Safety-related Part of a Control System)

5 迭代设计过程

安全控制系统的设计和确认宜充分考虑GB/T 15706—2012中图1的风险评估方法和GB/T 16855.1—2018中图1给出的风险评估/风险减小概况，并按本文件的图1所示流程实现其预定安全功能。

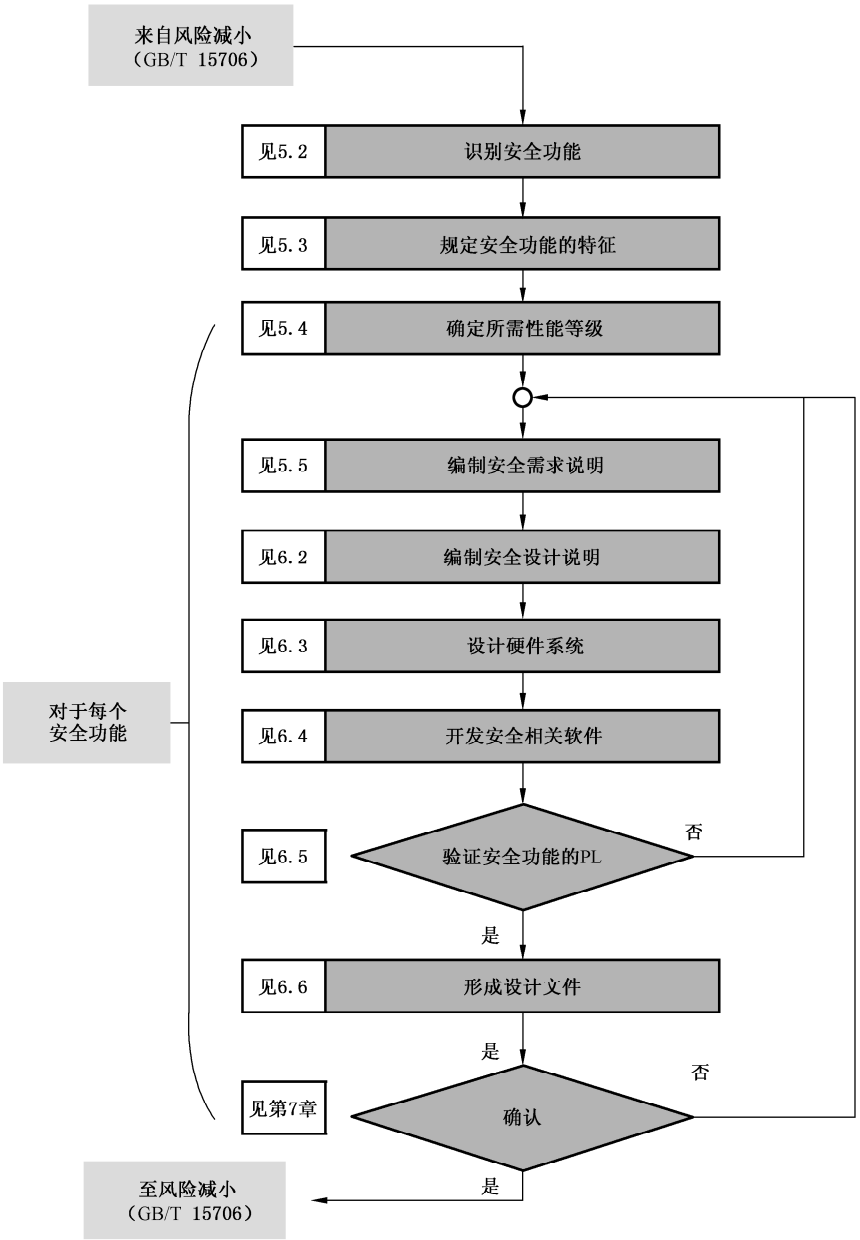


图1 安全控制系统的迭代设计过程

6 设计准备

6.1 风险评估

在设计安全控制系统之前，宜对机械进行风险评估。如果风险评估结果发现存在不可接受的风险，宜通过 GB/T 15706—2012 中图 1 给出的风险减小过程迭代三步法消除危险或者尽可能减小风险。通常，只有在通过安全防护措施无法经济合理地减小风险的情况下，才可以通过使用信息（包括组织措施）减小风险。因此，在大多数情况下宜采用安全防护措施减小风险，而安全控制系统是实现风险减小的重要措施之一。

注：风险评估和风险减小的策略见 GB/T 15706—2012。

6.2 识别安全功能

通过安全控制系统进行风险减小的起点是识别安全功能，即定义由安全控制系统执行的一个或多个安全功能（SF），以实现风险减小。识别安全功能的主要目的就是确定通过控制系统实现的保护措施。通过控制系统实现的保护措施，即为进行风险减小的安全功能。例如，联锁装置可实现安全联锁这一个安全功能，但不带联锁装置的活动式防护装置无法实现这一安全功能。

6.3 规定安全功能的特征

宜根据应用场合和具体危险规定安全功能需具备的特征。例如，如果存在抛射物，采用光幕就不合适，可以采用活动式防护装置。如果 C 类标准没有相关规定，安全功能可由机器设计者定义，如：

a） 运动的受控停止以及在静止位置宜使用固定抱闸；

b） 防止轴/气缸在设定模式下掉落；

c） 人员进入机械臂危险区之前机械臂能主动降速；

d） 防止人员被困；

e） 人员操作压力机时，如有其他人员在危险区内，通过光幕检测来阻止压力机危险运动的触发。

表 1 根据 GB/T 16855.1—2018 的表 8 对主要安全功能进行了总结，并增加了各种可能应用的示例。

表 1 典型安全功能及应用示例

安全功能	应用示例
由安全防护装置触发的安全相关停止功能	由安全转矩关断（STO）、安全停止 1（SS1）或安全停止 2（SS2）响应防护装置的触发
手动复位功能	确认已离开防护装置保护区域
启动/重启功能	带启动功能的联锁防护装置允许重启
本地控制功能	从危险区内的某个位置控制机器运动
抑制功能	保护装置临时性暂停，如材料输送过程中
保持-运行功能	从危险区内的某个位置控制机器运动，如设定过程中
防止意外启动	操作者在危险区进行人为干预

表 1　典型安全功能及应用示例（续）

安全功能	应用示例
受困人员的撤离和营救	在危险区触发联锁装置的紧急逃生装置
能源隔离和耗散功能	打开液压阀门释放压力
控制模式和模式选择	通过操作模式选择开关激活安全功能
急停功能	由安全转矩关断(STO)或安全停止 1(SS1)响应急停装置的致动

6.4　确定所需性能等级

各安全功能要求的风险减小程度会有差别。在 GB/T 16855.1—2018 中，风险减小的程度由性能等级(PL)确定。安全控制系统实现的安全功能的安全性能评估通过 5 个性能等级(PL)表示，每一级性能等级对应一个每小时危险失效概率(PFH_D)范围，PL 与 PFH_D 的对应关系见表 2。

表 2　PL 与 PFH_D 的对应关系

性能等级(PL)	平均每小时危险失效概率(PFH_D) h^{-1}
a	$10^{-5} \leqslant PFH_D < 10^{-4}$
b	$3\times10^{-6} \leqslant PFH_D < 10^{-5}$
c	$10^{-6} \leqslant PFH_D < 3\times10^{-6}$
d	$10^{-7} \leqslant PFH_D << 10^{-6}$
e	$PFH_D < 10^{-7}$

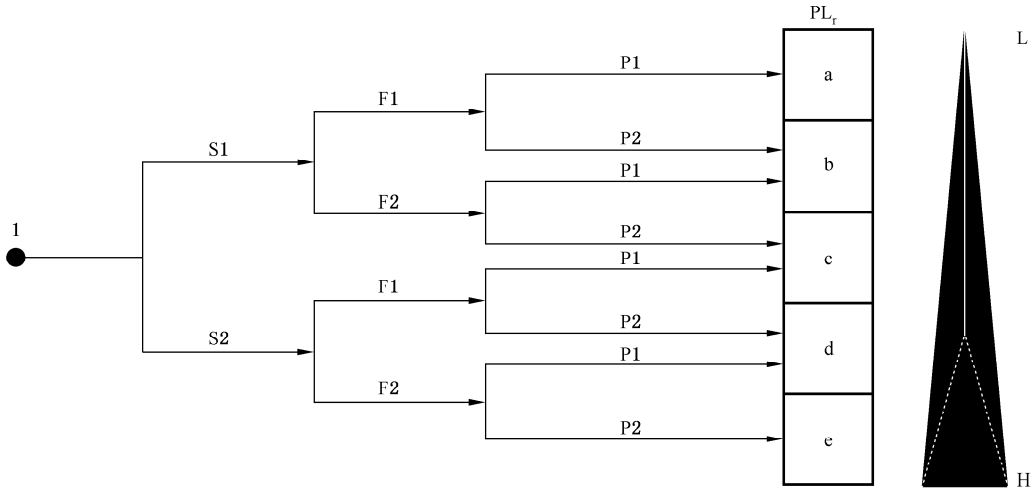
宜给每一个预定安全功能规定所需性能等级(PL_r)，即技术目标值。

宜优先按照 C 类标准确定安全功能的 PL_r，如注塑设备的 C 类标准中规定合模区操作侧的安全联锁功能的 PL 需要达到 e，即 $PL_r = e$。

如果没有合适的 C 类标准，可根据图 2 直接得出 PL_r。

注：具体参数的选择见 GB/T 16855.1—2018 的附录 A。

每个安全功能都宜根据图 2 确定 PL_r。



标引序号说明：

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；

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)；

F1 ——很少-不常和/或暴露时间短(通常是累计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/次)；

F2 ——频繁-连续和/或暴露时间长(不符合 F1 的情况)；

P1 ——在特定条件下可能(见 GB/T 16855.1—2018 的 A.2.3)；

P2 ——几乎不可能(见 GB/T 16855.1—2018 的 A.2.3)。

图 2 用于确定安全功能 PL_r 的风险图

6.5 编制安全需求说明

编制安全需求说明是安全控制系统设计的必要步骤。安全需求说明宜通过文档的方式，识别出实现安全功能的各个安全控制子系统，并对相应的安全功能加以阐述。安全需求说明宜详细说明机器安全控制系统中包含的各个安全功能，包括每个安全功能需要达到的 PL_r、实现每个安全功能所需的安全控制子系统(包括相关的输入、逻辑和输出)以及各安全控制子系统之间的逻辑关系。

安全需求说明宜包含以下内容：

a) 文档状态：
   1) 文档编号；
   2) 模板版本管理；
   3) 项目版本管理；
b) 术语；
c) 安全控制系统设计责任约定；
d) 系统概览：
   1) 安全功能定义；
   2) 功能名称；
   3) 功能描述；

4） 涉及的安全控制子系统；

5） 所需性能等级；

6） 信号处理(如果存在)。

在编制安全需求说明时，即使用于实现安全功能的安全控制子系统都相同，这些安全功能也宜分开定义。因为，其中的逻辑处理可能不同，例如一个安全功能需要断电延时切断执行机构，而另一个则需要瞬时切断执行机构。与之相类似，如果使用相同的逻辑实现不同的安全功能，也宜将安全功能分开描述。因为用于实现安全功能的安全控制子系统可能不同，从而导致安全功能可靠性存在差异。

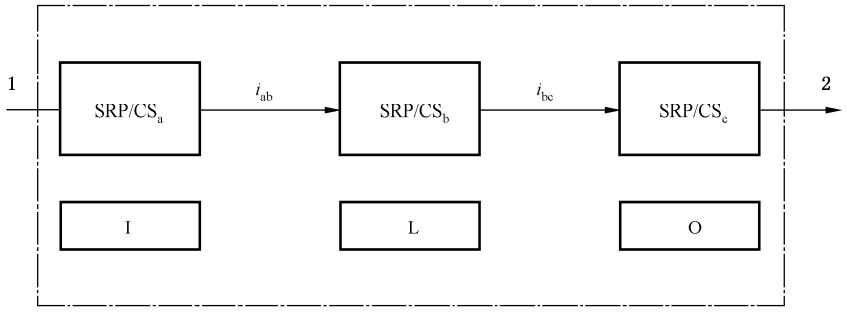
安全控制系统软件、硬件设计以及安全功能验证等后续步骤均需根据安全需求说明的内容实施。

7 安全控制系统的设计

7.1 概述

一旦定义了确切的安全功能、所要求的风险减小以及 PL_r，宜确定执行安全功能的安全相关部件，如选择安全光幕作为输入子系统、安全可编程控制器作为逻辑/处理子系统、接触器作为输出/动力子系统以及相互连接方式。

典型安全控制系统如图 3 所示。



标引序号说明：

SRP/CS$_a$、SRP/CS$_b$、SRP/CS$_c$ ——安全控制子系统；

I ——输入(例如：限位开关、传感器、AOPD)；

L ——逻辑(例如：安全继电器、安全可编程控制器)；

O ——输出(例如：阀、接触器)；

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)；

i_{ab}、i_{bc} ——相互连接方式(例如：电气连接)。

图 3 实现安全功能的典型安全控制系统示意图

进一步的安全控制系统设计包括定性设计和定量设计两方面。在定性设计阶段，主要考虑安全控制系统的架构类别。系统架构类别共有 5 种(由低到高分为 B、1、2、3 和 4)，架构的类别越高，则安全控制系统越容易实现更高的性能等级。在定量设计阶段，需分别考虑元器件的平均危险失效间隔时间($MTTF_D$)、平均诊断覆盖率(DC_{avg})以及系统共因失效三个因素。此外，还宜采取合理措施避免系统性失效。如果安全控制系统包含软件设计，则还宜遵循安全相关软件设计规范。

宜确定控制系统中实现安全功能的所有安全相关部件，将其纳入安全控制系统之中，并在安全设计说明中明确安全功能。

基于确定的安全功能以及 PL_r，选择安全相关部件，构成安全控制系统，通常需要考虑以下因素：

——安全功能实现的途径，如：

- 实现安全联锁输入，可以采用机械式、非接触式、RFID 等；
- 实现逻辑控制，可以采用安全继电器、安全可编程控制器等；
- 实现输出控制，可以采用阀、伺服控制器等。

——安全相关部件的安全特性，宜考虑：

- 部件可以实现的 PL；
- 部件可以构建的类别。

确定所有安全相关部件后，可以考虑以下因素评估安全控制系统的性能等级 PL：

——系统架构类别；

——$MTTF_D$；

——DC；

——CCF；

——系统性失效；

——安全相关部件的软件（如果有）；

——预期环境条件下，执行安全功能的能力。

根据上述因素进行系统设计后，可确定实际系统的 PL。对于每个安全功能，宜评估实际 PL 是否达到或超过 PL_r。若是，则说明该安全功能设计达到要求。反之，则需重新考虑上述设计因素，需改进设计以达到要求。

7.2 编制安全设计说明

宜根据安全需求说明编制安全设计说明。安全设计说明宜通过文档的方式，识别出实现安全功能的安全控制子系统在设计时需考虑的内容，包括：

——每个安全功能中涉及的安全相关部件的品牌型号、数量；

——安全相关部件符合的标准；

——安全相关部件的参数（$MTTF_D$、B_{10D}、PFH_D 等）；

——安全相关部件初始状态；

——安全相关部件电气编号；

——安全功能的触发频率；

——各安全控制子系统之间的逻辑关系（包括反馈、复位、延时、监控阈值等信息）。

安全设计说明可以独立于安全需求说明，也可以与安全需求说明相互补充并且整合在一个文档之中。

7.3 设计硬件系统

7.3.1 概述

每一个安全功能可通过几个安全控制子系统的组合来实现：输入子系统、逻辑/处理子系统、输出/动力子系统。硬件系统设计的主要目标是确定每个安全功能的实际 PL，以判断是否达到 PL_r。由于 PL 对应每小时危险失效概率（PFH_D），因此，确定每一个安全功能的安全控制系统的每小时危险失效概率 PFH_D，是完成硬件系统设计的主要目标。

常规的安全控制系统有输入子系统（输入装置，“I”）、逻辑/处理子系统（逻辑，“L”）和输出/动力子系统（输出装置，“O”）三部分组成（见图 3）。有两种方式可以获得各个子系统的 PFH_D：

——安全相关部件的生产厂家提供，如制造商一般可以提供安全继电器的 PFH_D 值；

——通过确定类别、$MTTF_D$ 和 DC_{avg} 后，根据 GB/T 16855.1—2018 的表 K.1 得出。

宜以子系统为单位，分别确定各个子系统的 PFH_D，再进行累加，得出整个安全控制系统的 PFH_D。

如图 4 所示，一个安全功能由 N 个安全控制子系统的组合来实现时，每一个安全控制子系统对应各自的 PL，即为 PFH_{DN}。所有实现这个安全功能的安全控制子系统的 PFH_{DN} 的总和，即为此安全功能的总的 PFH_D，然后根据 GB/T 16855.1—2018 的表 K.1，即可以得出对应的 PL。

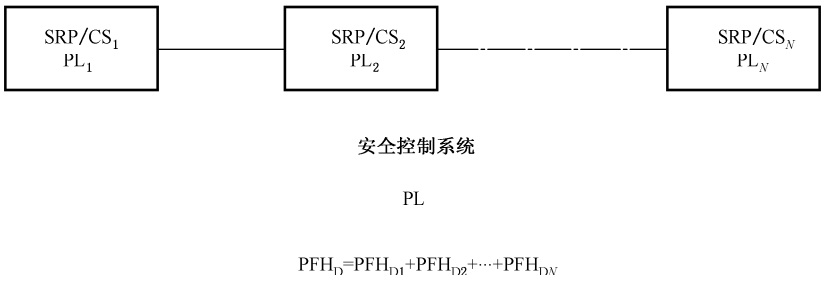


图 4　实现总 PL 的安全控制子系统组合

7.3.2　指定架构/类别

安全控制系统的架构决定其容错能力，并且是其他所有可量化指标的基础，以此得到安全控制系统的 PL。类别是指将安全控制系统按照其故障耐受能力及故障条件下的后续行为，以部件的可靠性和/或结构布置为基础进行的分类。评价由安全控制系统达到的 PL 的简化程序见表 3。故障耐受能力越高，风险减小的可能性越大。类别与五种基本架构形式之间存在对应关系，称为指定架构。

表 3　评价由安全控制系统达到的 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

宜按照输入子系统（输入装置，“I”）、逻辑/处理子系统（逻辑，“L”）和输出/动力子系统（输出装置，“O”）进行“垂直”划分进行架构和类别的设计。

GB/T 16855.1—2018 定义了五种架构作为类别。GB/T 16855.1—2018 采用对平均危险失效间隔时间（$MTTF_D$）、平均诊断覆盖率（DC_{avg}）以及防止共因失效（CCF）能力的量化要求对此前的类别定义进行补充。

基于所需性能等级 PL_r，可以根据表 3 进行指定架构的预设，如：

——PL_r = a 或 b，类别选择 B；

——PL_r = c，类别宜选择 1 或 2，但对类别 1 有高的可靠性要求；

——PL_r = d，类别宜选择 3；

——PL_r = e，类别宜选择 4。

以上选择仅通过简化程序给出预期的指定架构。结合对应 $MTTF_D$ 及 DC_{avg}，可进行安全相关部件的选择。但是，最终所实现的 PL 还需要通过计算 PFH_D 所得出。

类别 B 为基本类别，所有其他类别都需要满足类别 B 的要求。类别 B 和类别 1 主要通过选择和使用合适的元件实现故障耐受能力。发生一个故障就可使安全功能失效。由于使用了特殊元件和经验证的安全原则，类别 1 的抗共因失效能力要高于类别 B。

类别 2、类别 3 和类别 4 主要通过结构措施实现更好的安全功能表现。类别 2 的安全功能表现通常由技术检测设备(TE)通过自检定期自动检查。如果两次检测中间发生故障,安全功能就可能失败。通过选择适当的测试间隔,应用类别 2 可实现合适的风险减小。类别 3 和类别 4 发生单一故障不会导致安全功能丧失。类别 4 可自动检测到此类故障。在合理可行的情况下,类别 3 也能自动检测到此类故障。另外,类别 4 还具备抵抗未检测故障累积的能力。

注:有关指定构架示意图和类别要求总结见 GB/T 16855.1—2018 的 6.2。

7.3.3 平均危险失效间隔时间($MTTF_D$)

在确定 $MTTF_D$ 之前,宜选定安全控制系统中的相关部件。

无论是单个元件,如晶体管、阀门或接触器,还是模块、通道及安全控制系统作为一个整体,都有 $MTTF_D$。安全控制系统总的 $MTTF_D$ 可根据组成系统的所有元件的 $MTTF_D$,按照 GB/T 16855.1—2018 的附录 D 给出的简化方法计算得出。

单个元件的 $MTTF_D$ 宜通过以下顺序获得:

a) 制造商给出的 $MTTF_D$;

b) 根据制造商给出的 B_{10D} 按照 GB/T 16855.1—2018 的附录 C 通过计算得出;

c) 如果无可获得的数据,则选为 10 年。

宜分别估算各个子系统的 $MTTF_D$。如子系统采用类别 3 或类别 4 的构架,则需要考虑并联通道的平衡[见 GB/T 16855.1—2018 的公式(D.2)]。

7.3.4 诊断覆盖率(DC)

对 PL 有重要影响的另一个变量是安全控制系统的(自我)检测和监控措施。例如,有效的检测可以对元件的可靠性进行一定补偿。GB/T 16855.1—2018 采用诊断覆盖率 DC 来衡量检测质量。基准量可以是一个元件、一个模块或者整个安全控制系统。对于整个安全控制系统,DC 为平均诊断覆盖率 DC_{avg}。DC 的值分 4 级,见表 4。

表 4 诊断覆盖率(DC)

指标	范围
无	DC<60%
低	60%≤DC<90%
中	90%≤DC<99%
高	DC≥99%

有两种方法可以计算 DC_{avg},一种更精确,但更复杂;另一种则较简单。

精确但复杂的方法涉及失效模式和影响分析(FMEA),且以 DC 定义为基础。这种情况下,需要确定各元件的可检测的危险(dd)失效类型和不可检测的危险(du)失效类型,以及它们占元件总失效率的比例。最后,对这一比例进行求和并列式运算后,得出所考虑单元的 DC 值,见公式(1):

$$DC=\frac{\sum_{i=1}^{n}\lambda_{ddi}}{\sum_{i=1}^{n}\lambda_{ddi}+\sum_{i=1}^{n}\lambda_{dui}}=\frac{\sum_{i=1}^{n}\lambda_{ddi}}{\sum_{i=1}^{n}\lambda_{di}} \quad \cdots\cdots(1)$$

式中:

λ_{ddi}——组成安全功能的每个元件的可检测的危险失效率;

λ_{dui}——组成安全功能的每个元件的不可检测的危险失效率;

λ_{di}——组成安全功能的每个元件的危险失效率。

DC_{avg}的计算宜采用第二种简单的方法，这种方法基于直接对元件或模块层的DC进行合理保守的估算，然后再采用平均公式利用各DC值计算DC_{avg}。许多措施都可以按照典型标准措施进行分类，GB/T 16855.1—2018的附录E列出了各类措施的DC估计值。这些数值采用有四个分值(0%、60%、90%和99%)组成的粗略系统进行分类。常用的DC估计如下：

a) 类别B和1的架构，DC为0；

b) 针对输入装置，采用双通道但无法检测到短路故障，DC为90%；

c) 针对输入装置，采用双通道可检测短路故障，DC为99%；

d) 针对输出装置，如接触器，采用双通道且对接触器安全相关触点进行直接监控(通过机械连接触点元件监控)，DC为99%。

一旦知道了所有元件的DC值，就可以采用近似计算公式(2)计算系统的DC_{avg}值。此公式适合用于采用不同DC值的冗余通道的子系统的DC_{avg}估计。

$$DC_{avg}=\frac{\frac{DC_1}{MTTF_{d1}}+\frac{DC_2}{MTTF_{d2}}+\cdots+\frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}}+\frac{1}{MTTF_{d2}}+\cdots+\frac{1}{MTTF_{dN}}} \quad \cdots\cdots(2)$$

对于类别2，宜注意检测频率和检测可靠性。检测频率至少为安全功能平均要求率的100倍。如果要求安全功能后检测执行的很快，并且能够在危险发生前达到安全状态，则检测频率没有任何要求。整个检测通道的$MTTF_D$值不宜低于功能通道$MTTF_D$值的一半。

7.3.5 确定PL

确定类别、$MTTF_D$、DC_{avg}之后，可以确定安全控制系统中安全功能的PL。

实现安全功能的安全控制系统由不同的子系统组成。这些子系统采用不同的技术和/或实现不同的类别/性能等级。不同的子系统可通过线性(串联)或冗余(并联)方式连接，实现安全控制系统中的安全功能。宜采用以下步骤进行PL的确定：

a) 按照输入系统、信号处理单元和输出系统进行分类，构成独立的子系统。

b) 确定每一个子系统的PFH_D：

——如子系统直接给出PFH_D，可以直接使用，如安全光幕、安全可编程控制器；

——对于未直接给出PFH_D的子系统，宜根据每一个子系统类别、$MTTF_D$、DC_{avg}来确定该子系统的PFH_D。

c) 将所有子系统的PFH_D数值相加，通过求和得出整体PL的相关数值，见公式(3)：

$$PFH=\sum_{i=1}^{N}PFH_{Di}=PFH_{D1}+PFH_{D2}+\cdots+PFH_{DN} \quad \cdots\cdots(3)$$

式中：

N ——安全功能所使用子系统的数量；

PFH_{Di}——第i个子系统的平均每小时危险失效概率。

此处需特别注意子系统之间的接口：

——所有连接(如导体或总线系统实现的数据通信)需已在某个子系统的PL中考虑，或者连接故障已经排除或可以忽略不计；

——串联布置的安全子系统接口宜兼容，即发出要求安全功能信号的子系统的各输出状态能够触发下游子系统安全状态。

d) 根据GB/T 16855.1—2018的表K.1，对照总的PFH_D数值，确定对应的PL，即得出安全功能的性能等级。

7.3.6 防止共因失效(CCF)的措施

共因失效(CCF)为冗余安全控制系统两个通道都发生的因相同原因造成的相关危险失效。在实现

PL≥PL_r 的基础上，且采用类别 2、类别 3 和类别 4 的构架下，宜采取措施防止共因失效。GB/T 16855.1—2018 的附录 F 给出了一个包含 8 种重要防范措施的检查清单。这 8 种措施分别被赋予了 5～25 不等的分值：

a) 不同通道的信号路径之间的物理隔离(15 分)；
b) 技术相异，通道的设计结构或物理原理相异(20 分)；
c) 防止可能发生的过电压、过电流、过压力、过热等(15 分)以及采用经验证的元件(5 分)；
d) 开发过程中进行失效模式和影响分析，识别可能发生的共因失效(5 分)；
e) 就 CCF 及如何避免对设计者/维护者进行培训(5 分)；
f) 防止污染(机械或流体系统)以及电磁干扰(电气系统)触发共因失效(25 分)；
g) 防止不利环境条件触发共因失效(10 分)。

对于以上每种措施，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。

足够防止 CCF 的措施要求最低得分为 65 分。

7.3.7 故障考虑和故障排除

宜考虑以下的故障判别准则：

a) 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发生的所有故障宜一起视为单一故障；
b) 由共同原因造成的两个或两个以上单独的故障宜视为单一故障，即通常所说的共因失效；
c) 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；
d) 在技术上不大可能发生的某些故障；
e) 普遍认可的、独立于所考虑的应用的技术经验；
f) 与应用和特定危险有关的技术要求。

7.4 开发安全相关软件

安全软件包括安全相关应用软件(SRASW)及安全相关嵌入式软件(SRESW)。在安全控制系统设计中，通常是进行安全相关应用软件(SRASW)的开发。

对于安全控制系统中的安全相关应用软件(SRASW)的开发，一般要求参照“V”模型。如图 5 所示。

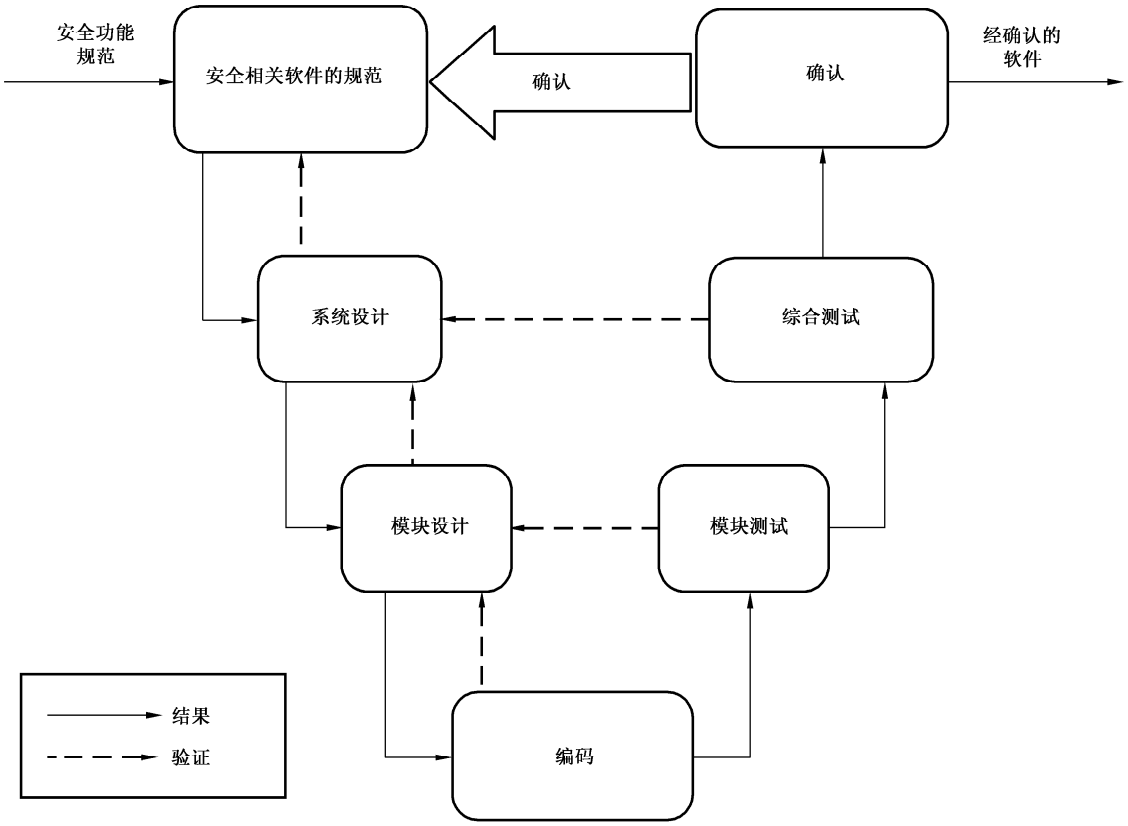


图 5　安全相关软件开发用简化 V 模型

在开发安全相关应用软件(SRASW)的过程中,安全设计说明可视为安全功能规范。

宜严格参照安全设计说明,进行系统、模块设计及程序编写。宜将安全相关应用程序和非安全相关应用程序分开编写。

编写安全相关应用程序时,为了避免错误,需要考虑以下几个方面:

——宜采用经过认证的编程软件;

——使用经认证的编程软件编写安全相关程序时,宜采用编程软件中经认证的安全软件功能块,如急停、安全联锁、安全光幕、安全速度监控等;

——采用经认证的安全软件功能块时,功能块的配置需满足 PL_r;

——避免采用任何非安全相关信号旁路安全相关信号;

——代码宜清晰易懂,便于后期的测试和无故障修改。

安全相关软件设计完成后,宜安排非本项目开发人员通过软件仿真执行测试工作。测试完成后,需验证安全相关应用软件(SRASW)满足安全相关软件规范。

注:关于安全相关软件设计的更多信息,见 GB/T 16855.1。

7.5　验证安全功能的 PL

对于每种单独的安全功能,有关的 SRP/CS 的 PL 宜与 PL_r 匹配。因此,需要将此 PL 与 PL_r 进行比较。如果某项安全功能实现的 PL 小于 PL_r,则需要采用 GB/T 16855.1—2018 的图 3 中描述的迭代过程进行设计改进(如使用 $MTTF_D$ 更优的其他元件),直到满足 $PL \geqslant PL_r$。

7.6　形成设计文件

验证和确认行为要求提供详细的文件资料。这些文件资料已经在开发过程中形成,根据所用技术

不同会有差别。宜充分考虑以下内容：

a) 提出对安全功能以及执行这些安全功能的安全控制系统全部要求的规范文件、性能指标、全部操作模式的列表、全面的功能描述、过程描述；

b) 适用标准的工作和环境条件，以及预定应用涉及的强度（额定数据）；

c) 安全控制系统的设计描述（包括所采用机械、电气、电子、液压和气动元件的细节）、布线图以及接头和接口描述、电路图、装配图、元件的技术数据和额定数据，适用的数据表；

d) 所有相关故障的分析，如以 FMEA（失效模式和影响分析）形式，并引用涉及的故障列表；

e) 确定 PL 的数据（量化文件）；

f) 全部软件文件；

g) 设计和实施遵循的质量保证准则，如模拟和数字电路设计准则、编程指南；

h) 已经完成测试的元件、模块或安全控制系统的测试证书。

文件资料宜完整，内容不相互抵触，结构具有逻辑性，容易理解，能够验证。

8 确认

8.1 确认原则

完成验证之后，宜对 SRP/CS 的设计进行确认，确认每个安全功能的要求均得到满足，对不满足要求的安全功能，则按照图 1 进行迭代设计，直至完成所有安全控制系统中所有安全功能的确认。

确认工作宜由独立于安全控制系统设计工作的人员来完成。确认包括分析，以及必要时按确认计划进行的测试。分析和测试之间的平衡取决于使用的技术。以下对确认程序一些最重要的内容进行了简要的说明。

注：确认的详细要求见 GB/T 16855.2。

8.2 分析

宜通过分析对安全控制系统进行评价。分析的目的是为了通过审查文件或适当时可采用分析工具，如静态和动态软件分析工具或 FMEA 工具来确定是否满足规定的要求。

$MTTF_D$、DC 以及 CCF 可以通过所提供的文件进行评价。

8.3 测试

如果仅通过分析进行评价还不够，则需要进行测试来证明能够满足要求。测试宜系统规划并合理实施，通常与实际开发过程同步，如原型阶段、功能模型阶段或软件/代码阶段。

测试所采用的配置宜尽可能接近预定使用的配置。

进行测试的环境条件宜事先确定。

测试可手动完成，也可以自动完成。

8.4 归档

所有分析和测试宜形成文件并记录最终结果（合格或不合格）。

如果安全控制系统规范规定的要求未全部满足，此时需要返回设计和实施过程的适当阶段。否则，则宜结束确认过程，评价是否已经对全部安全功能进行分析。如果全部分析过，则按照 GB/T 16855.1—2018 完成安全控制系统的评估。否则，继续对仍未完成确认的安全功能进行测试。

附 录 A
（资料性）
压力机安全控制系统设计及验证示例

A.1 风险评估

A.1.1 机器限制

使用限制：压力机由接受过专业培训的操作人员，每天 16 h 进行持续生产操作。由专业的维修人员进行日常保养和维修。操作人员仅使用双手模式进行生产，但维修人员根据具体的问题，会使用寸动模式、连续模式等其他操作模式。每一小时需要进入到压机背后，进行取废料及润滑操作，操作时间为 4 min。

空间限制：滑块行程为 800 mm，合模力为 250 t，每次循环时间大约为 8 s。操作人员需要手动将原料放置在模具上，并按下双手按钮启动压机。完成冲压作业后，操作人员需要手动将加工完成的工件取出。

A.1.2 危险识别

由于滑块的上下移动产生的模具夹紧点，造成的上肢挤压危险。

A.1.3 风险评价

由于滑块的上下移动产生对人员双手造成的挤压危险，最严重时可能造成操作员手臂截肢甚至是死亡，并且人员在 16 h 内会持续暴露在该风险之下。因此，在不使用任何防护措施的情况下，该风险是不可接受的。

A.2 识别安全功能

需考虑通过安全防护，如联锁装置、安全光幕和双手操纵装置作为安全功能进行风险减小。

A.3 规定安全功能特征

在危险区增加一个带有安全联锁的活动式防护装置，确保活动式防护装置打开时，危险运动停止。在上料部位增加安全光幕，确保人员在危险区域内的时候，安全光幕被触发。增加双手操纵装置，确保滑块下落时，操作人员的双手不在危险区域内。

本示例仅对联锁装置的安全功能加以分析。

A.4 确定所需性能等级（PL_r）

根据图 2，确定 S、F、P 的值，以确定 PL_r。

a) S——伤害的严重程度。

滑块的下落会对操作人员造成骨折甚至死亡的伤害，取值 S2。

b) F——暴露于危险的频率和时间。

人员累积的暴露时间为 64 min(4 min/h)，超过总运行时间的 1/20(48 min)，取值 F2。

c) P——规避危险或限制伤害的可能性。

滑块运动速度较快，惯性较大，因此发生危险情况时操作人员较难以回避，取值 P2。

根据图 2，得出实现该联锁功能的安全控制系统的所需性能等级 $PL_r=e$。

A.5 安全需求说明

安全功能名称：联锁装置（控制滑块运动）。

安全功能定义：安全防护装置，与活动式防护装置一同作为人员进入危险区域的保护措施，进行风险减小。

安全功能描述：联锁装置，通常采用安全门开关，安装在安全门上。当安全门打开的时候，触发安全门开关，开关输出可靠信号至安全控制系统，确保压力机滑块停止运动。

安全控制子系统：安全门开关为输入子系统，安全继电器为逻辑子系统，液压阀为输出子系统。

根据 A.4 的评估，所需求性能等级：PL_r＝e。

A.6 安全设计说明

压力机的安全设计说明示例见表 A.1。

表 A.1 安全设计说明内容示例

子系统	名称	电气标识符	品牌及型号	数量	安全参数	符合的标准	备注
输入	安全门开关	B1	本文件不做细化	1	B_{10D}＝2 000 000	GB/T 14048.5，直接断开	见 GB/T 16855.1—2018 的表 C.1，位置开关
		B2		1	B_{10D}＝1 000 000	GB/T 14048.5	制造商给出 B_{10D}
逻辑	安全继电器	K1		1	PFH_D＝2.31×10^{-9}	GB/T 16855.1—2018	制造商给出 PFH_D
输出	液压阀	YV1		1	$MTTF_D$＝150 年	GB/T 3766	见 GB/T 16855.1—2018 的表 C.1，液压元件
		YV2		1	$MTTF_D$＝150 年	GB/T 3766	见 GB/T 16855.1—2018 的表 C.1，液压元件
逻辑关系	安全门开关 B1 和安全门开关 B2 被触发，安全继电器 K1 断开液压阀 YV1，液压阀 YV2，并监控这两个阀的阀芯位置。						

A.7 指定构架/类别

根据表 3，如需要实现 PL_r＝e，选择类别 4 作为系统构架。针对三个子系统的构架构建如下：

a) 采用两个物理上分离的安全开关 B1 和安全开关 B2，采用双通道的方式由安全继电器 K1 监控，可以检测两个输入通道间的短路故障，电气回路图示例见图 A.1；

b) 选择满足 GB/T 16855.1—2018 的要求，可以实现类别 4 的安全继电器；

c) 输出采用液压阀 YV1 和液压阀 YV2 切断液压回路，阀芯位置信号反馈至安全继电器，液压回路图见图 A.2。

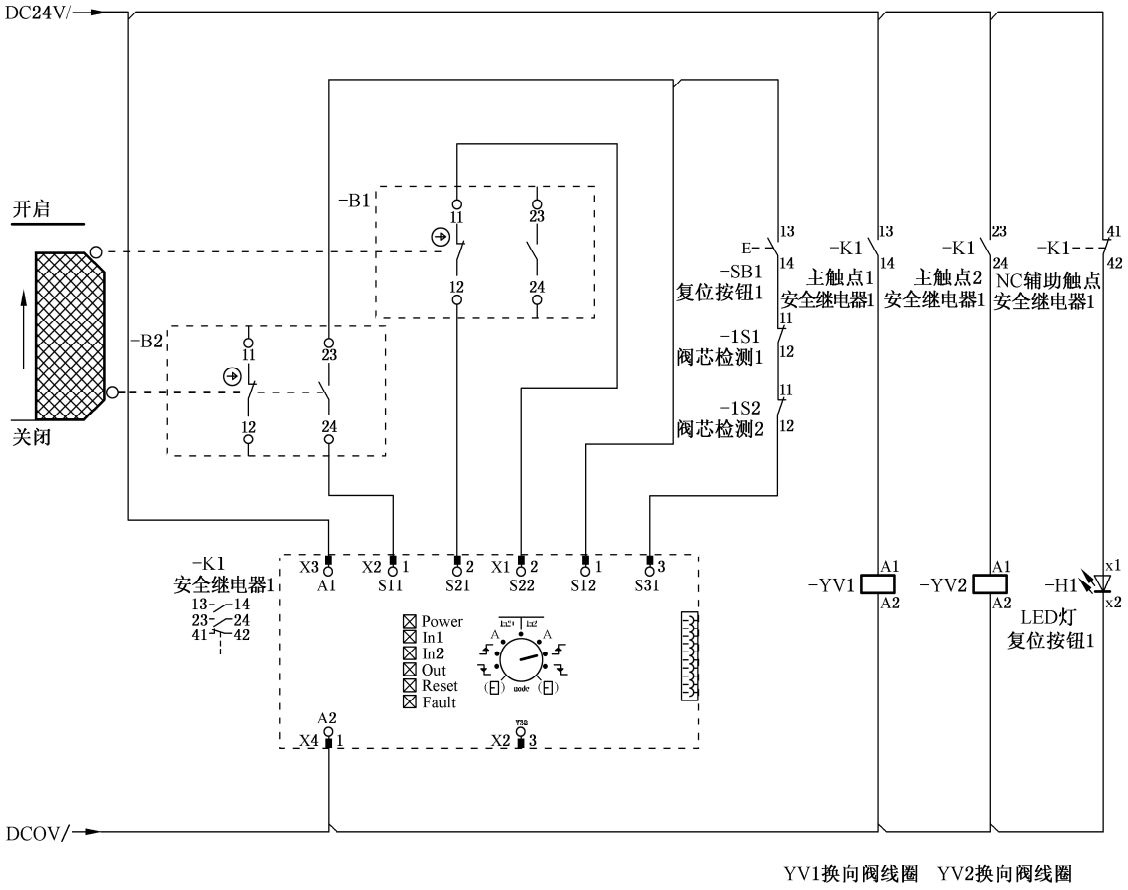


图 A.1 电气回路图示例

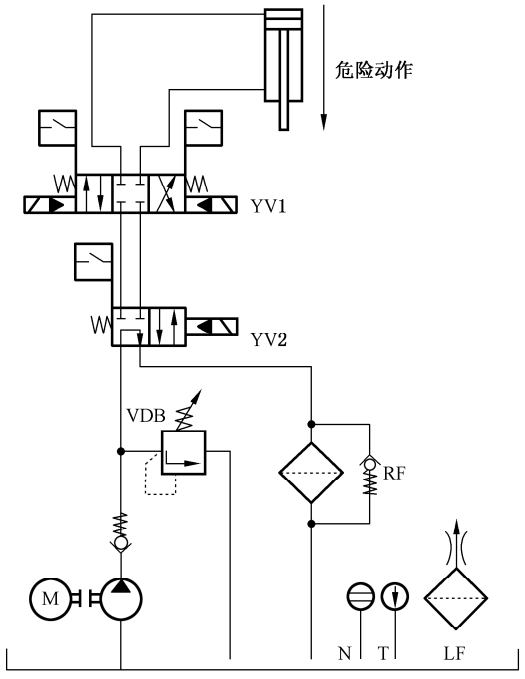


图 A.2 液压回路图示例

A.8 平均危险失效间隔时间($MTTF_D$)

按每年 365 个工作日、每天工作 16 h 以及每次安全门打开 1 h 的间隔时间,即:$d_{op}=365$,$h_{op}=16$,$t_{cycle}=3\ 600$,代入 GB/T 16855.1—2018 的公式(C.2),计算得出 $n_{op}=5\ 840$。

两个安全门开关的 B_{10D} 值分别为 2 000 000 和 1 000 000(见表 A.1),代入 GB/T 16855.1—2018 的公式(C.1),计算输入子系统各个通道的 $MTTF_D$ 值分别为:

——$MTTF_{D,B1}=3\ 424$ 年,取最大值 2 500 年;

——$MTTF_{D,B2}=1\ 712$ 年。

带直接断开操作的位置开关 B1 的电气触点可以进行故障排除。

根据 GB/T 16855.1—2018 的公式(D.2),计算输入子系统的 $MTTF_{D,I}$ 和 $MTTF_{D,O}$:

——$MTTF_{D,I}=2\ 130$ 年;

——$MTTF_{D,O}=MTTF_{D,WV1}=MTTF_{D,WV2}=MTTF_{D,WV4}=150$ 年。

A.9 诊断覆盖率(DC)

针对输入子系统:双通道结构,且安全继电器 K1 对两个安全门开关状态的真实性监控,因此 B1 和 B2 的 DC 值取 99%。

针对输出子系统:液压阀取 DC 值 99%的依据是 K1 对两个液压阀开关状态的直接监控。

根据 7.3.4 中的公式(2),得出两个子系统的 DC_{avg} 都是 99%(“高”)。

A.10 确定 PL

a) 针对输入子系统:

——类别为 4;

——$MTTF_{D,I}=2\ 130$ 年;

——$DC_{avg,I}=99\%$(高)。

根据 GB/T 16855.1—2018 的表 K.1,$PFH_{D,I}=1.13\times10^{-9}$。

b) 针对输出子系统:

——类别为 4;

——$MTTF_{D,O}=150$ 年;

——$DC_{avg,O}=99\%$(高)。

根据 GB/T 16855.1—2018 的表 K.1,$PFH_{D,O}=1.61\times10^{-8}$。

c) 针对逻辑子系统:

根据安全继电器制造商给出的参数(见表 A.1),$PFH_{D,L}=2.31\times10^{-9}$。

d) 针对整个安全控制系统:

$PFH_D=PFH_{D,I}+PFH_{D,L}+PFH_{D,O}=1.13\times10^{-9}+2.31\times10^{-9}+1.61\times10^{-8}=1.954\times10^{-8}$

根据表 2,得出 PL=e。

A.11 防止共因失效(CCF)的措施

本示例采取的防止共因失效的措施包括:

——隔离(15);

——经验证元件(5);

——FMEA(5);

——过电压保护等(15);

——环境条件(25+10)。

根据 7.3.6，采取的措施总计得分为 75 分，满足防止 CCF 的措施要求最低得分为 65 分的要求。

A.12 故障考虑和故障排除

安全联锁功能的输入子系统由两个独立的开关组成，从物理上确保开关本身故障不会导致安全功能失效。

安全继电器分别采用两个安全触点分别控制两个液压阀，避免短路故障导致安全功能失效。

考虑到液压管路泄漏导致的安全功能失效，宜在液压回路中采用防爆阀，并定期保养检查。

A.13 验证安全功能的 PL

通过安全设计所构成的安全控制系统的 PL＝e，满足 PL≥PL_r。

附 录 B
（资料性）
木工圆锯机安全控制系统设计及验证示例

B.1 风险评估

B.1.1 机器限制

使用限制：该木工机械由接受过专业培训的操作人员，每天 8 h 进行间歇性的生产操作。由专业的维修人员进行日常保养和维修。操作人员在每个操作循环前，需手动打开防护罩，手工控制木材上下料进行切割，切割完成后将完成品取走。因此设备的主要仅有手动工作一种操作模式，根据加工零件的不同，单个零件加工时间约 0.5 min～1 min。

空间限制：大锯片直径 Φ40 mm、大锯切厚度 120 mm、机床外形尺寸 850 mm×500 mm×786 mm。电机功率 3 kW，主锯转数：4 000 r/min～6 000 r/min。

B.1.2 危险识别

当圆锯机在非工作状态时，锯片旋转造成的切割伤害。

B.1.3 风险评价

锯片旋转造成的切割伤害，最严重情况下可能造成人员截肢，因此在不使用任何防护措施的情况下，该风险是不可接受的。

B.2 识别安全功能

为了防止人员在非操作时误触及旋转的锯片，需考虑通过安全防护，如联锁装置作为安全功能进行风险减小。

B.3 规定安全功能特征

为防止圆锯机处于非工作状态时，锯片旋转对人员造成切割伤害。在大锯片处增加一个带有联锁的活动式防护装置，确保活动式防护打开时，锯片旋转运动停止并刹车。

B.4 确定所需性能等级

根据 ISO 19085-1：2017 中 5.3 的要求，得出实现该联锁功能的安全控制系统所需的性能等级 PL_r＝c。

B.5 安全需求说明

安全功能名称：联锁装置（控制锯片）

安全功能定义：安全防护装置，与活动式防护装置一同作为人员进入危险区域的安全防护措施，进行风险降低。

安全功能描述：联锁装置，通常采用安全开关，安装在活动式防护装置上。当活动式防护装置打开的时候，触发联锁装置，开关输出可靠信号至相关控制系统，确保锯片停止运动。

安全控制子系统：位置开关为输入子系统，接触器为输出子系统。

根据 B.4 的评估，所需求性能等级：PL_r＝c。

B.6 安全设计说明

木工圆锯机的全设计说明示例见表 B.1。

表 B.1 安全设计说明内容示例

子系统	名称	电气标识符	品牌及型号	数量	安全参数	符合的标准	备注
输入	位置开关	B1	本文件不做细化	1	B_{10D}=2 000 000	GB/T 14048.5，直接断开	参数由制造商给出
输出	接触器	Q1		1	B_{10D}=2 000 000	GB/T 14048.5	参数由制造商给出

B.7 指定构架/类别

根据表 3，如需要实现 PL_r=c，可以选择类别 1 作为系统构架。针对子系统的构架构建如下：

——采用一个工作在直接断开方式下的安全开关 B1；

——输出采用一个接触器 Q1 切断锯片电机供电。

电气控制回路图示例见图 B.1。

该设计遵守基本的安全原则，满足类别 B 架构的要求。采用断电安全原则作为基本安全原则，控制回路的接地可以被认为是一个经验证的安全原则。

位置开关 B1 是符合 GB/T 14048.5—2017 中附录 K 的直接断开动作位置开关，因此可认为是经验证的元件。当保护装置不在安全位置时，断开触点直接以机械方式切断电路。

接触器 Q1 符合 GB/T 16855.2—2015 中表 D.4 的附加条件，是一个经验证的元件。

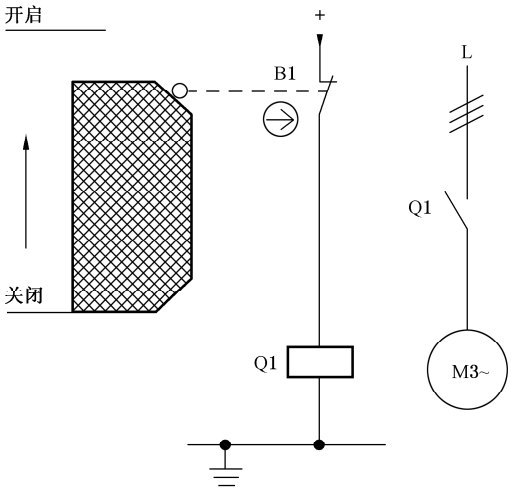


图 B.1 电气控制回路图示例

B.8 平均危险失效间隔时间($MTTF_D$)

按每年 200 个工作日、每天工作 8 h 以及每次防护罩打开 10 min 的间隔时间，即：d_{op}=200，h_{op}=8，t_{cycle}=600，根据 GB/T 16855.1—2018 的公式(C.2)，计算得到 n_{op}=9 600。

位置开关的 B_{10D} 值为 2 000 000(见表 B.1)，代入 GB/T 16855.1—2018 的公式(C.1)，计算输入子系统的 $MTTF_{D,B1}$：

$MTTF_{D,B1}$=2 083 年。

带直接断开操作的位置开关 B1 的电气触点可以进行故障排除。

类似的，输出子系统的 $MTTF_{D,Q1}=2\ 083$ 年。

B.9 诊断覆盖率(DC)的测试和检测措施

针对输入子系统：B1 无故障监控功能，因此 $DC_{avg}=0\%$。

针对输出子系统，Q1 无故障监控功能，因此 $DC_{avg}=0\%$。

B.10 确定 PL

a) 针对输入子系统：

——类别为 1；

——$MTTF_{D,I}=2\ 083$ 年；

——$DC_{avg,I}=0\%$(无)。

根据 GB/T 16855.1—2018 的表 K.1，$PFH_{D,I}=1.14\times10^{-6}$。

b) 针对输出子系统：

——类别为 1；

——$MTTF_{D,O}=2\ 083$ 年；

——$DC_{avg,O}=0\%$(无)。

根据 GB/T 16855.1—2018 的表 K.1，$PFH_{D,O}=1.14\times10^{-6}$。

c) 针对整个安全控制系统：

$PFH_D=PFH_{D,I}+PFH_{D,O}=1.14\times10^{-6}+1.14\times10^{-6}=2.28\times10^{-6}$

根据表 2，PL=c。

B.11 防止共因失效(CCF)的措施

由于采用类别 1 的指定架构，此时无需考虑防止共因失效的措施。

B.12 故障考虑和故障排除

安装上采用位置开关进行位置监控。防护装置的稳定布置保证了位置开关的启动。位置开关的执行元件受到保护，不会发生位移。仅使用刚性机械部件连接(在执行器和触点之间没有弹簧元件)。

B.13 验证安全功能的 PL

通过安全设计所构成的安全控制系统的 PL=c，满足 $PL\geqslant PL_r$。

附 录 C
（资料性）
码垛机安全控制系统设计及验证示例

C.1 风险评估

C.1.1 机器限制

使用限制：该码垛机由接受过专业培训的操作人员，每天 24 h 进行持续生产操作。由于生产过程中的需求，操作人员需要偶尔进入码垛区域进行调节作业，整理箱子箱型或捡起掉落在地面的纸箱，但人员进入时，需要打开维护门才能进入。正常每 8 h，需要进入危险区域 2 次，每次 5 min。正常生产时，人员无需进入。

由专业的维修人员进行日常保养和维修。但维修人员进入危险区域前，会按照码垛机厂商的安全说明，对危险能源进行上锁挂牌，并针对存在重力坠落危险的机构使用安全插销进行机械方式锁定。

空间限制：码垛机在低位产品进料的情况下，最高速度为 300 层/h。

C.1.2 危险识别

由于码垛机构上下移动，推板的前后移动，以及输送带运动产生的夹紧点和卷入点，造成的人员上肢或身体的挤压或卷入危险。

C.1.3 风险评价

由于码垛机构上下移动产生对人员双手造成的挤压危险，最严重时可能造成操作员死亡，并且人员在每 4 h 就会进入码垛机内部，暴露在该风险之下，因此在不使用任何防护措施的情况下，该风险是不可接受的。

C.2 识别安全功能

考虑通过安全防护，如固定式防护装置、联锁装置和安全光幕作为安全功能进行风险减小。

C.3 规定安全功能特征

在危险区域四周增加固定式防护，针对需要物料进出的位置，增加带有屏蔽功能的安全光幕，当物料通过且正确触发屏蔽逻辑时，码垛机可保持运行状态，针对人员需要进入进行调节作业或维修的位置，增加带有安全联锁的活动式防护，确保活动式防护打开时，危险运动停止。

本示例仅对联锁装置的安全功能加以分析。

C.4 确定所需性能等级

根据图 2，确定 S、F、P 的值，以确定所需性能等级。

a） S——伤害的严重程度。

码垛机结构的移动会对操作人员造成骨折，截肢甚至死亡的伤害，取值 S2。

b） F——暴露于危险的频率和时间。

人员累积的暴露时间每个班次为 10 min，低于每个班次的运行时间的 1/20（24 min），取值 F1。

c） P——规避危险或限制伤害的可能性。

码垛机机构的运动速度较快，惯性较大，因此发生危险情况时操作人员较难以回避，取值 P2。

根据图 3，得出实现该联锁功能的安全控制系统所需的性能等级 PL_r＝d。

C.5 安全需求说明

安全功能名称：联锁装置（控制码垛机构运动）。

安全功能定义：安全防护装置，与活动式防护装置一同作为人员进入危险区域的安全防护措施，进行风险降低。

安全功能描述：联锁装置，通常采用安全门开关，安装在安全门上。当安全门打开的时候，触发安全门开关，开关输出可靠信号至安全控制系统，确保码垛机构停止运动。

安全控制子系统：安全门开关为输入子系统，安全 PLC 为逻辑子系统，控制码垛机构动作的变频器为输出子系统。

根据 C.4 的评估，所需求性能等级：PL_r＝d。

C.6 安全设计说明

码垛机的安全设计说明示例见表 C.1。

表 C.1 安全设计说明内容示例

子系统	名称	电气标识符	品牌及型号	数量	安全参数	符合的标准	备注
输入	安全门开关	B1	本文件不做细化	1	$PFH_d=2.62\times10^{-9}$	GB/T 18831—2017，4 型	参数由制造商给出
逻辑	安全 PLC	K1		1	$PFH_d=4.47\times10^{-10}$	GB/T 16855.1 PL＝e	参数由制造商给出
输出	变频器	Q1		1	$PFH_d=7.05\times10^{-8}$	STO 功能符合 GB/T 12668.502	参数由制造商给出

C.7 指定构架/类别

根据表 3，如果需要实现 PL_r＝d，可选择类别 3 作为系统构架。针对三个子系统的构架构建如下：

——根据设备制造商手册，安全门开关 B1 采用 RFID 原理，其两个通道符合类别 4 的要求；

——选择满足 GB/T 16855.1—2018 的要求，可以实现类别 4 的安全 PLC；

——变频器的安全转矩关断功能符合 GB/T 16855.1—2018 中类别 3 要求，并且该功能满足 GB/T 12668.502。

电气控制回路图示例见图 C.1。

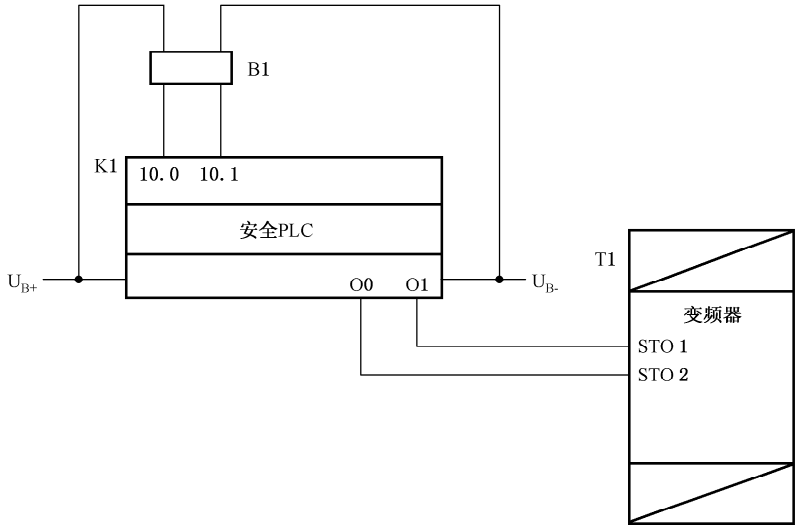


图 C.1 电气回路图示例

C.8 确定 PL

a) 针对输入子系统：根据制造商提供的参数(见表 C.1)，$PFH_{D,I}= 2.62\times10^{-9}$。

b) 针对逻辑子系统：根据制造商提供的参数(见表 C.1)，$PFH_{D,L}= 4.47\times10^{-10}$。

c) 针对输出子系统：根据制造商提供的参数(见表 C.1)，$PFH_{D,O}= 7.05\times10^{-8}$。

d) 针对整个安全控制系统：

$PFH_D=PFH_{D,I}+PFH_{D,L}+PFH_{D,O}=2.62\times10^{-9}+4.47\times10^{-10}+7.05\times10^{-8}=17.357\times10^{-8}$

根据表 2，PL＝d。

C.9 防止共因失效(CCF)的措施

本示例采取的防止共因失效措施包括：

——隔离(15)；

——经验证元件(5)；

——FMEA(5)；

——过电压保护等(15)；

——环境条件(25＋10)。

根据 7.3.6，采取的措施总计得分为 75 分，满足防止 CCF 的措施要求最低得分为 65 分的要求。

C.10 故障考虑和故障排除

安全门开关牢固安装，确保联锁装置正确动作。安全门开关的供电导线可以单独敷设，也可以采用防止机械损伤的保护措施。

安全 PLC 满足类别 4 和 PL＝e 的所有要求。安全相关软件(SRASW)按照 PL＝d 的要求和 7.4 的说明进行编程。安全 PLC 的每个输出都是由 PLC 的两个处理通道驱动。

针对伺服电机驱动的码垛机构，如存在重力坠落危险的，宜增加防坠落装置(如插销气缸)，并定期保养检查。

C.11 验证安全功能的 PL

通过安全设计所构成的安全控制系统的 PL＝d，满足 $PL\geqslant PL_r$。

参 考 文 献

[1] GB/T 3766 液压传动 系统及其元件的通用规则和安全要求

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

[3] GB/T 14048.5 低压开关设备和控制设备 第5-1部分:控制电路电器和开关元件 机电式控制电路电器

[4] GB/T 16855.2 机械安全 控制系统安全相关部件 第2部分:确认

[5] 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

[6] 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

[7] GB/T 35081—2018 机械安全 GB/T 16855.1与GB/T 15706的关系

[8] ISO 19085-1:2017 Woodworking machines—Safety—Part 1:Common requirements

[9] BGIA Report 2/2008e,Functional safety of machine controls—Application of EN ISO 13849