ICS 号
中国标准文献分类号

团　体　标　准

T/CASEI XXX—XXXX

起重机械安全相关电气、电子和可编程电子控制系统的功能安全

Lifting appliances—Functional safety of safety-related electrical,electronic and programmable electronic control systems

（征求意见稿）

xxxx-xx-xx 发布　　xxxx-xx-xx 实施

中国特种设备检验协会 发布

目　次

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。

本文件由中国特种设备检验协会提出并归口。

本文件起草单位：略

本文件主要起草人：略

本文件为首次发布。

引 言

本文件采用 GB/T 15706、GB/T 28526 和 GB/T 20438.2 中提及的风险评估、安全相关控制系统的设计和确认方法,参考GB 16855 和ISO 13482 中的功能安全规范要求,制定了相关技术内容。

本文件涵盖起重机械安全相关控制系统的危害、危害情况或危害事件的描述。危害的数量和类型直接与起重机械应用的场景、制造及施工质量以及日常维护保养的水平相关。这些危害相关的风险随起重机械的使用和本身用途的类型以及设计、安装、操作和维护的方式而变化。

起重机械安全相关电气、电子和可编程电子控制系统的功能安全

1 范围

本文件规定了起重机械控制系统的功能安全评估要求及流程、危害识别与风险评估、功能安全管理、安全相关控制功能（以下简称 SRCF）规范要求、安全相关控制系统（以下简称 SRCS）要求、SRCS 设计与整合、检验和确认等内容；旨在降低人员直接接近或操作起重机械时，发生人身伤害或财产损失风险的功能安全相关要求。

本文件适用于单机运行起重机械相关控制系统的功能安全评估；协同作业的无人起重机群组的功能安全评估，可参照本文件执行。

本文件不适用于以下范畴：一是其他标准或法规针对人身与财产防护所提出的全部要求（如防护措施、非电气联锁或非电气控制相关要求）；二是电气控制设备自身引发的电气危害（如电击，参见 GB 5226.1）。

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 5226.1 机械电气安全 机械电气设备 第1部分:通用技术条件

GB/T 15706-2012 机械安全 设计通则 风险评估与风险减小

GB/T 15969.3 可编程序控制器 第3部分:编程语言

GB/T 16754 机械安全 急停 设计原则

GB/T 16855.1-2018 机械安全 控制系统有关安全部件 第1部分:设计通则GB/T16855.2机械安全 控制系统安全相关部件 第 2 部分:确认

GB/T 20438 电气/电子/可编程电子安全相关系统的功能安全

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

GB/T 45374-2025 起重机械 危险源辨识

T/CASEI 62001-2019 起重机械 安全状况评估

3 术语和定义

GB/T 20438.4-2017界定的以及下列术语和定义适用于本文件。

3.1.1

安全相关控制系统 safety-related control system

其失效可能导致风险立即增加的控制系统。

注：SRCS包括由电气、电子、可编程电子控制电路等组成的全部控制系统,其失效可能导致功能安全的降低或丧失。

3.1.2

起重机械功能安全 Lifting appliances functional safety

起重机械控制系统的安全部分,取决于 SRCS 的正确功能、其他技术安全相关系统和外部风险降低设施。

注 1:改写 GB/T 20438.4-2017,定义3.1.12。

注 2:仅考虑起重机械控制系统中取决于 SRCS 正确功能的功能安全

3.1.3

安全相关控制功能 safety-related control function

由具有规定的完整性等级的 SRCS 执行的控制功能,预期用于保持机器的安全状况或防止风险立即增加。

3.1.4

SRCS 诊断功能 SRCS diagnostic function

预期用于检测 SRCS 故障,并在检测出故障时产生特定输出信息或动作的功能。

注：该功能预期用于检测可能导致 SRCF 危险失效并引发特定故障反应功能。

3.1.5

SRCS 故障反应功能 SRCS fault reaction function

当 SRCS 范围内的故障被 SRCS 诊断功能检测出时，所触发的功能。

3.1.6

每小时危险失效概率 probability of dangerous failure per hour

1小时内危险失效平均概率。

注：PFH_D不应与要求失效概率(PF)相混淆

3.1.7

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

预期的危险失效平均时间。

3.1.8

安全相关软件safety-related software

在安全相关系统中，用于实现 SRCF 的软件。

3.1.9

性能等级 performance level PL

在可预期条件下，用于规定 SRP/CS 执行安全功能的离散等级。

3.1.10

安全完整性等级 safety integrity level SIL

一种离散的等级，用于规定分配给SRCS安全相关控制功能的安全完整性要求。

3.1.11

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

控制系统中响应有关安全输入信号并产生有关安全输出信号的部件。

注1:SRP/CS的组成,以有关安全的输入信号被触发为起始点(例如:行程限位开关等),以控制文件的动力输出(例如:接触器的主触点等)为终止点。

注2: 如果监测系统用于诊断，也可认为它们是 SRP/CS。

3.2 符号及缩略语

下列缩略语适用于本文件

CCF：共因失效(Common cause failure)

DC：诊断覆盖率(Diagnostic converage)

DCavg：平均诊断覆盖率(Average diagnostic converage)

E/E/PES：电气/电子/可编程电子系统(Electrical/Electronic/Programmable System)

FB：功能块(Function block)

I/O：输入/输出(Input/Output)

LVL：有限可变语言(Limited variability language)

$MTTF_d$：平均危险失效时间(Mean time to dangerous failure)

PFH_D：每小时危险失效概率(Probability of dangerous failure per hour)
PL：性能等级(Performance level)
PL_r:所需的性能等级(Requirement of performance lever)
SIL：安全完整性等级(Safety integrity level)
SRASw：有关安全的应用软件(Security-related applications software)
SRCF：安全相关控制功能(Safety-related control function)
SRCS：安全相关控制系统(Safety-related control system)
SRESW：有关安全的嵌人式软件(Security-related embedded software)
SRP/CS：控制系统有关安全部件(Safety-related part of a control system)
SRS：安全相关软件(Safety-related software)

4 一般要求

4.1 人员要求

为评估起重机械SRCS是否达到功能安全要求，应组建一个符合T/CASEI 62001-2019要求的评估组,此外，该评估组宜配备具备不同学科知识、多种经验和专业技能的专家，包括下列人员:

——能回答关于起重机械设计和功能方面技术问题的人员；
——具备起重机械操作、调试、保养、维修等实际经验的人员；
——了解类起重机械事故历史的人员；
——熟悉有关法规、标准,包括 GB/T 15706-2012 以及与所评估起重机械有关的具体安全问题的人员；
——长期从事起重机械检验的检验师或以上人员。

不同的人员针对相似的情况的分析所形成的详细结果若存在差异，应尽量完善评估组的知识和专业技能,提高该风险评估结果的可信度。

4.2 评估范围

应对起重机械整体安全生命周期、电子 / 电气 / 可编程电子（E/E/PE）系统安全生命周期及软件安全生命周期的全阶段开展功能安全评估。评估过程中，需考量各安全生命周期每个阶段所开展的活动及形成的输出，并判定其是否符合第 7 章至第 9 章的相关要求。

功能安全评估应贯穿上述三个安全生命周期的全过程，既可在单个安全生命周期阶段结束后开展，也可在多个阶段完成后开展，但核心前提为必须在已确定的危险发生前完成至少一次功能安全评估。

4.3 评估内容

4.3.1 功能安全评估应考虑如下内容:

——先前所做的功能安全评估工作(一般包括以前的安全生命周期阶段)；
——对整体安全生命周期、E/E/PE 安全生命周期或软件安全生命周期进一步执行功能安全评估的计划；
——对先前的功能安全评估的建议以及已做更改的程度。

4.3.2 对于起重机械整体安全生命周期、E/E/PE 安全生命周期或软件安全生命周期不同阶段的功能安全评估应制定计划并保持一致。

4.3.3 功能安全评估活动计划应规定:

——承担功能安全评估的各方；
——每次功能安全评估的输出；
——功能安全评估的范围；
——要求的资源；
——承担功能安全评估各方的独立水平；
——与应用相关的承担功能安全评估各方的能力。

5 流程

在进行起重机械安全相关控制系统功能安全评估过程中,应符合图1所示流程。

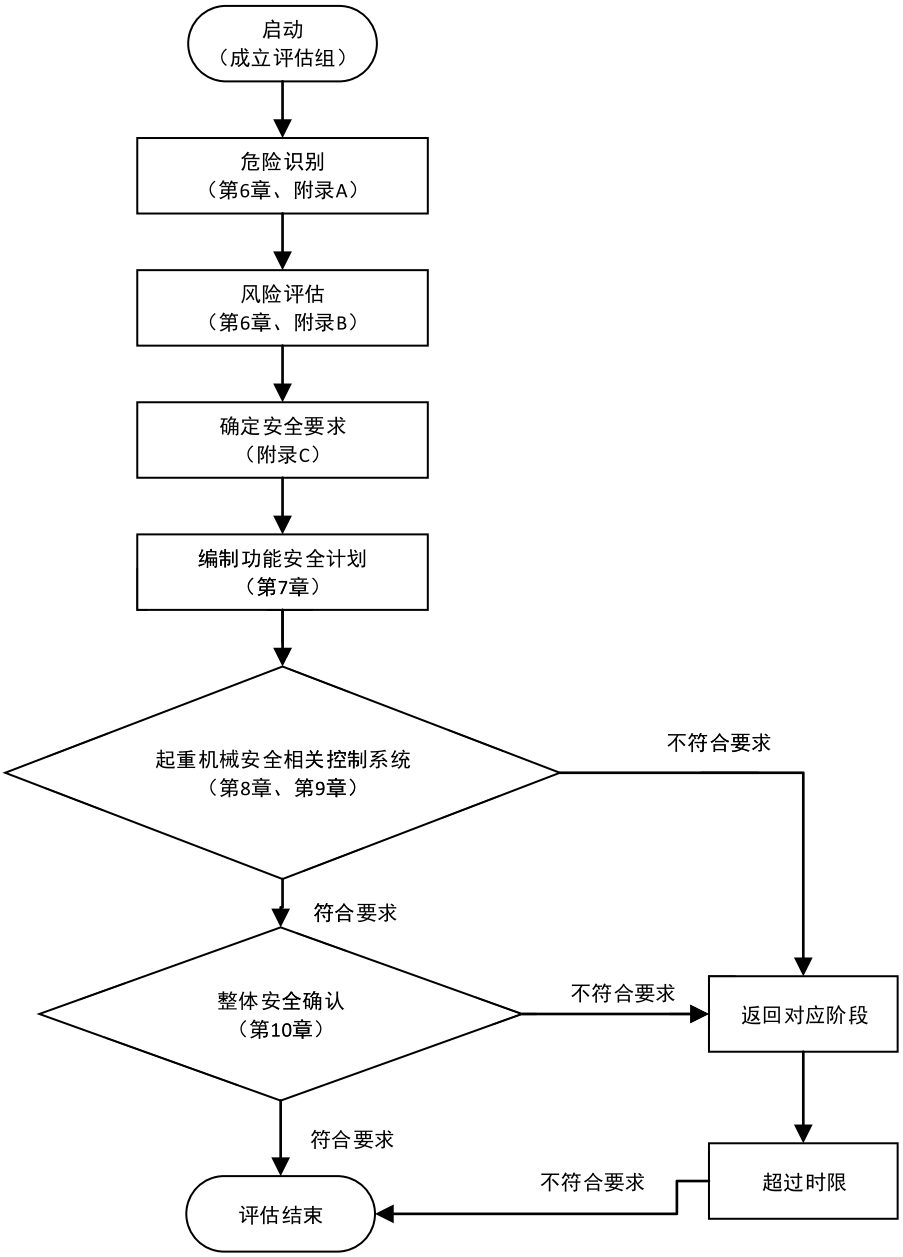


图1 起重机械功能安全评估流程图

6 危险识别和风险评估

6.1 危险识别

危险识别应能够识别起重机械中可能出现的任何危险。附录A包含了一份典型的危险清单（参考GB/T 45374-2025）,这些危险均为起重机械电气系统可能出现的危险。当然,这一列表未包含所有的危险可能性，如:

a) 起重机械系统可能因为其特殊需求设计具有的其他危险；

b） 使用造成的其他危险；
c） 可合理预见的误用。

6.2 风险评估

风险评估应考虑起重机械在整个安全生命周期中所处的危险环境,并仔细注意在各种情况下, 可能会与起重机械发生接触的物体。风险评估过程见图2。

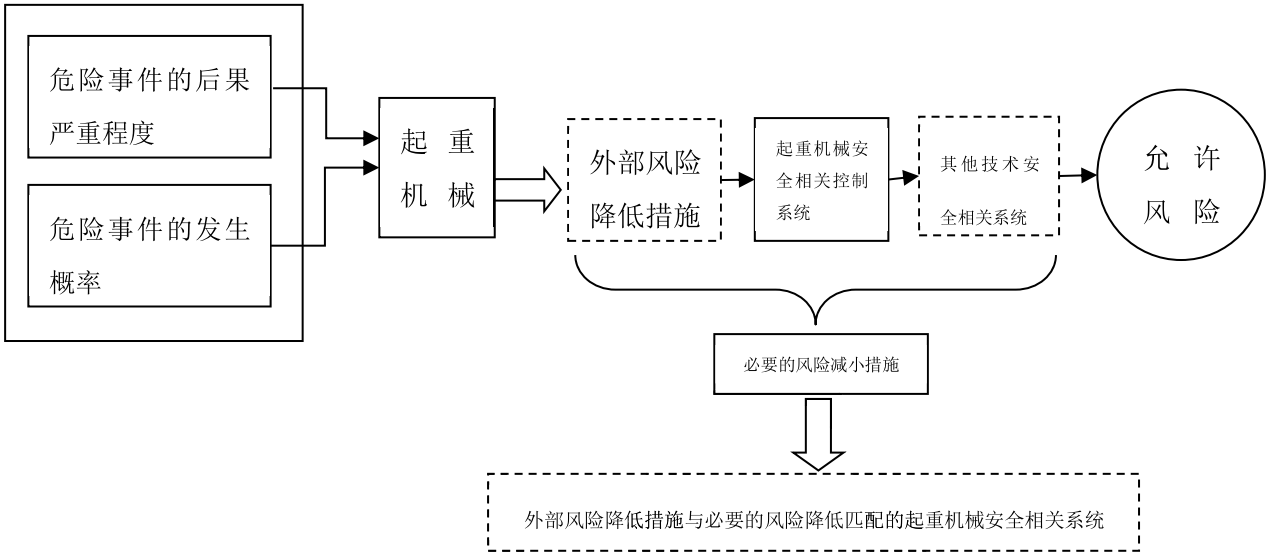


图2 起重机械风险评估过程

在采用所有安全设计和保护措施以后,其他风险对于起重机械,应被评估并证明它已被降至可接受的水平。

应根据具体情况,设计适当的风险评估方法，附录B给出了基于风险图法的示例，其他评估方法可以参考T/CASEI 62001-2019中5.8以及GB 28526-2012的附录A。如果使用其他方法的风险参数用于风险评估,那么应检验其是否恰当。评估的最终结果的应当是不会造成任何不可接受的风险。

7 功能安全管理

7.1 目的

本章规定了为达到 SRCS 所要求的功能安全所必需的管理和技术工作。

7.2 要求

7.2.1 起草功能安全计划

对于每个 SRCS 设计项目,都应起草功能安全计划,并形成文档,必要时,应及时更新。该计划应包括第 6 章~第 10 章规定的运行控制程序。

功能安全计划内容应根据具体情况而定,其中包括:

a） 起重机复杂程度（吨位、高度、自主运行等）；
b） 设计和技术新颖程度；
c） 设计特点标准化程度；
d） 如果失效可能的后果。

起草功能安全计划时应注意:

a) 确定第 8 章~第 10 章规定的有关活动。
b) 描述为满足规定的功能安全要求而采取的方针和策略。
c) 描述为实现应用软件、开发、集成、检验和确认的功能安全的措施。
d) 确定第8章~第10章中规定对执行和检查各项工作负责的人员、部门或者其他单位和资源
e) 确定或建立相关程序和资源以便记录和维护同 SRCS 功能安全相关的信息(参见附录 D),如:
1）危险识别和风险评估的结果;
2）用于安全相关功能及其安全要求的设备;
3）负责维护功能安全的部门;
4）达到和保持功能安全(包括 SRCS 修改)所需的程序。
f) 描述考虑相关机构问题时的配置管理(参见附录 E)策略。
g) 建立检验计划，应包括:
1) 进行检验的细节;
2)执行检验的人员、部门或单位的详细情况并设立相应的负责人;
3）检验策略和技术的选择;
4）检验仪器设备的选择和使用;
5）检验活动的选择;
6）验收准则;
7）用于评估检验结果的方法。
h) 建立确认计划,其中包括:
1) 进行确认的细节;
2）操作有关模式(如正常操作、设置)的确定;
3)参照受检验的 SRCS 的要求;
4)适用于确认的技术策略，例如:分析方法或统计试验;
5)验收准则;
6)出现失效时采取的行动，以满足验收要求。
注: 确认计划应指出 SRCS 及其子系统是否进行常规测试、形式测试和(或)抽样测试。

7.2.2 实施功能安全计划

实施功能安全计划,应确保立即跟踪,并完满地解决由于下列原因造成的 SRCS 相关的问题:
——第 8 章~第 10 章规定的活动;
——检验活动;
——确认活动。

8 安全相关控制功能(SRCF)要求

8.1 目的

本章规定由 SRCS 执行 SRCF 的要求。

8.2 SRCF 要求规范

8.2.1 概述

8.2.1.1 减少风险的措施

依据附录 C 中提出的风险降低策略,安全功能的任何需要应被确定。因此,应主要采用以下两种保护措施减少风险:
——减少在电气元件级的故障概率。其目的为减少影响安全功能的故障或失效的可能性。可通过增加元件可靠性来实现,例如:为了把致命故障或失效减到最少或排除故障(见 GB/T 16855.2),选用经检验的零件和(或)应用经检验的安全原则。
——改善控制系统有关安全部件(SRP/CS)的结构,其目的为避免故障的危害影响。一些故障可以检测到,而且需要冗余和(或)监测结构。

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

8.2.1.2 一般要求

如果被选择的安全功能由 SRCS 执行(全部或部分地),那么,应规定相关 SRCF。

各SRCF 规范应包括:

——功能要求规范(见 8.2.3)；

——安全完整性要求规范(见 8.2.4)。

上述项目应在安全相关软件(SRS)中形成文件。

注1：当非申气设备结合电气手段执行安全功能时,本文件将不考虑应用于非电气设备的目标失效值。电气手段涵盖了所有依据电气原理操作的装置和系统，包括:

——机电装置；

——非可编程电子装置；

——可编程电子装置。

注2：SRS 需要按照版本控制,作为配置管理程序的一部分(参见附录 E)。

安全要求规范应经过检验确保在预期应用中的一致性和完整性。

注3：例如:它可以通过检验、分析、核对表获得。参见GB/T 20438.7-2017 中 B.2.6。

8.2.2 可用信息

应使用下列信息制定各 SRCF 功能要求规范和安全完整性要求规范:

——起重机械风险评价结果应包括针对各种特定危害的风险降低过程所必需的所有安全功能。

——起重机械操作特性,包括:

- 操作模式（人工/自动）；
- 工作循环时间；
- 工作环境条件；
- 人机交互(例如：操作指令、触摸屏等)；维护(例如：维修等)。

——所有和 SRCF 相关的信息,都可能影响 SRCS 的设计,例如:

- SRCF 预期实现或防止的机器行为的描述；
- SRCF 之间以及 SRCF 与任何其他功能(无论机器内外)之间的所有界面；
- SRCF 要求的故障反应功能。

8.2.3 SRCF 功能要求规范

8.2.3.1 SRCF 功能要求规范应描述各个需要执行的 SRCF 的细节,包括

——SRCF 应激活或禁用的条件(例如:操作模式)；

——可能同时激活,但会造成冲突动作的那些功能之间的优先权；

——各 SRCF 的工作频率；

——各 SRCF 要求的响应时间；

——SRCF 同其他起重机械功能之间的接口;

——要求的响应时间(例如:输入输出装置);

——各 SRCF 的描述;

——故障反应功能以及起重机械重新启动或继续运转等操作的各种限制的描述,以防初始故障即导致机器停止运行；

——工作环境描述(例如:温度、湿度、气体环境、化学物质、机械振动和冲击)；

——试验以及各种相关设施(例如:试验设备、试验接入端口)；

——预期用于 SRCF 机电装置的操作循环周期、工作循环周期和(或)使用类别。

8.2.4 SRCF 的安全完整性要求规范

8.2.4.1 每个标准安全完整性要求应来自风险评估，以确保达到必要的风险降低。本文件安全完整性要求表示为标准安全完整性要求每小时危害失效概率的目标失效值。

8.2.4.2 每个 SRCF 的安全完整性要求应按照 GB 28526 依照 SIL 规定并形成文档。当要求的SRCF安全完整性低于SIL1时,应符合GB/T 16855.1最低要求的B类。

8.3 SRCS的要求

8.3.1 要求的安全性能

通过控制系统执行保护措施的安全性能应符合本章要求。起重机械控制系统功能的性能等级(PL)要求或安全完整性等级(SIL)要求应通过 9.3.1 或6.2 确定,并应符合 GB/T 16855.1 的要求。该过程应含检验和确认。

表1给出了基于每小时平均危险失效概率的PL和SIL之间的关系。

表1 基于每小时平均危险失效概率的PL和SIL之间的关系

性能等级（PL）	每小时平均危险失效概率（1/h）	安全完整性等级（SIL）
a	$\geqslant 10^{-5}$～$<10^{-4}$	无特殊的安全要求
b	$\geqslant 3\times 10^{-6}$～$<10^{-5}$	1
c	$\geqslant 10^{-6}$～$<10^{-6}$	1
d	$\geqslant 10^{-7}$～$<10^{-6}$	2
e	$\geqslant 10^{-8}$～$<10^{-7}$	3

在采用T/CASEI 62001-2019进行安全状况评估时，性能等级(PL)可与T/CASEI 62001-2019中表8中安全状况等级对应。

8.3.2 停止功能

自主运行的起重机械遇到障碍物、人等,应具备停止功能；制动性能(减速)满足安全要求,不会产生对障碍物、人等造成伤害的撞击或发生其他危害。在设计时应考虑安全停止,确保在任意速度下的故意制动,不会发生失控或者起重机零部件和载荷的落下等产生危险的情形。停止状态可以根据起重机工作工况由制造商决定。

8.3.3 安全相关的速度控制

通过风险评估确定起重机械机构工作速度的限值,超过该限值可能产生的危害。

对于自动运行的起重机械只有经授权人员允许将速度才能调整最大。且速度应根据起重机械工作工况的不同,设定不同的速度限值。改变速度限值应基于风险评估起重机械的速度应确保其运动部件的速度不会超过安全相关的速度要求。

8.3.4 急停

任何情况下，急停功能均应保持可用且处于可操作状态。在起重机械的各类运行工况中，该功能的优先级应高于其他所有功能，且不得削弱为解救陷入危险人员所设计的各类便捷措施的效用。急停功能不得用于替代安全防护措施及其他安全功能，而应作为补充防护措施进行设计。急停装置触发后，应能以合适的方式终止起重机械的危险运行与操作，且不会产生附加风险，同时无需人员进行进一步干预。

合适的方式可包括:

——选择最合适的减速率;

——应用预定的停机顺序。

急停功能的设计需确保起重机械操作人员决定使用急停装置时，无需考虑该操作带来的后果。

8.3.5 用户界面的设计

当控制设备(例如:操纵手柄、无线遥控器、操作控制面板以及其他设备)用于控制起重机械时,它们在操作过程中应具有适当的可靠性。

该命令装置固定或不固定在起重机械上,其对起重机械的电气连接应不会造成危险。

8.3.6 运行模式

起重机械应设计为只能在一个特定模式下运行操作。若风险评估表明自动/手动模式切换存在潜在危害，则起重机械应在模式切换前立即执行停机功能。该模式不得自行切换，且不应引发其他危害。对于所有运行模式，均应明确界定可用及禁用的安全功能范围。

起重机械的运行模式包括：手动控制模式、半自主模式（远程监护）、自主模式和维护模式。

8.3.7 手动控制

在手动控制的起重机械工作时,手动控制装置和操作界面应设计有醒目的中文标签。

8.3.8 其他

以上未提及的起重机械 SRCS 的要求,但在进行风险评估中被确认需要执行的 SRCS 的要求,应根据制造商或使用者的具体需求设计实现。

9 安全相关控制系统(SRCS)设计与整合

9.1 目的

SRCS 设计或选择要求,以满足安全要求规范中规定的功能和安全完整性要求。

9.2 一般要求

按 GB/T16855.1 的规定,起重机械SRCS 的选择或设计(包括总体硬件、软件体系结构、传感器、工作机构、可编程电子器件、嵌入式软件,应用软件等)均应符合下列要求:

a) 识别 SRCS 执行的每种安全功能所需要的 PL,见附录 A。

b) 每种安全功能技术实现的要求：

1）硬件系统要求；

2）软件系统要求；

3）系统确认。

c) 在设计和集成时,应考虑可维护性和可测试性,以便执行 SRCS 的这些特性。SRCS 设计,包括诊断和故障反应功能，应形成文件，文件应满足以下要求：

1）精确、完整、简明；

2）适合预期目的；

3）可存取、可维护；

4）版本可以控制。

d) 在 SRCS 设计、开发和执行期间,执行的工作结果应在适当阶段验证。

9.3 每种安全功能技术实现的要求

9.3.1 硬件要求(性能等级)

起重机械执行安全相关控制系统中安全相关功能的技术为液压、机电、可编程电子等,起重机械 SRCS 的有关安全部件完成安全功能的能力通过确定 PL 表示。对于所选的完成安全功能的每个 SRCS 和(或)SRCS 的组合,都应完成其 PL 的估计。

应通过估计以下参数确定 SRP/CS 的 PL:

——单个元件 $MTTF_d$的值；

——DC；

——CCF;

——结构;

——安全功能在故障条件下的性能；

——有关安全的软件；

——系统性失效；

——预期环境条件下,完成安全功能的能力。

图 3 给出了与每个通道的 $MTTF_d$组合的类别以及为了达到安全功能要求的 PL 的 DC_{avg}的选择。

对于 PL 的估计,图 3 给出了与 DC_{avg}一起的类别(水平轴)和每个通道的 $MTTF_d$(柱形图)。图中的

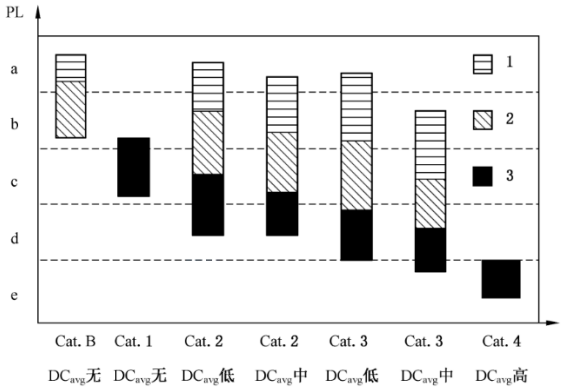
阴影代表了每个通道的 $MTTF_d$ 的 3 个范围(低、中、高).它可选择用于达到要求的 PL。

使用图 3 中的简单方法应确定 SRCS 的类别以及每个通道的 DC_{avg} 和 $MTTF_d$。

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。

考虑到这些参数,图 3 提供了确定由 SRCS 实现的 PL 的方法图解。类别(包括共因失效)和 DC_{avg} 的组合确定选择图 3 中的那一列。根据每个通道的 $MTTF_d$ 应选出有关直方柱的 3 个不同阴影区域中的一个。

这些区域的纵向位置确定能在竖轴上读出的要求的 PL,如果该区域有两种或三种可能的 PL,表 1 中给出了所达到的 PL。数字更精确的 PL 的选择取决于每个通道 $MTTF_d$ 的精确值。



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3 PL 和每个通道的类别、DC_{avg} 和 $MTTF_d$ 的关系

表 2 估计由 SRCS 达到的 PL 的简单程序

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

对于采用复杂控制电路的自主运行的起重机械SRCS，可按 GB28526-2012 中的第6章，确定性能等级所对应的安全完整性等级。

9.3.2 软件要求

9.3.2.1 一般要求

有关 SRCS 的嵌入式软件或应用软件的所有生命周期内的活动，应主要考虑避免软件生命周期内出现的故障(见图 4)。以下要求的主要目标为易读、易理解、可测试及可维护的软件。

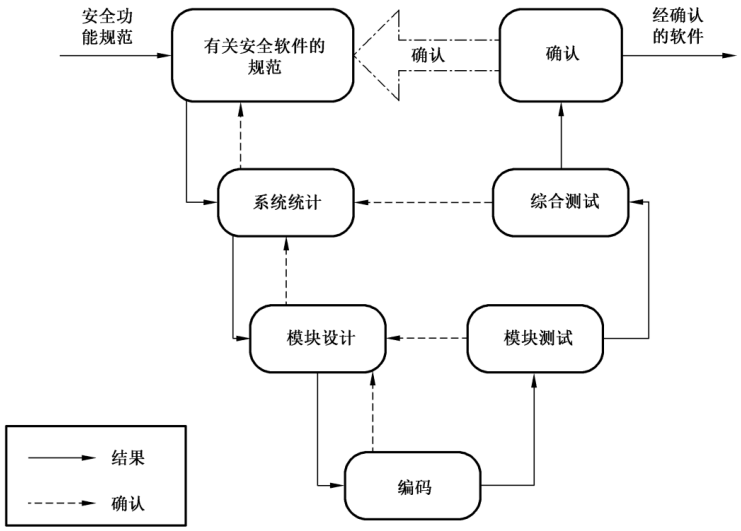


图4　软件安全生命周期的简单 V 模型

9.3.2.2　有关安全的嵌入式软件(SRESW)

对于用于 PL，为 a~d 的元件的 SRESW,应采用以下基本方法:

——对软件安全生命周期内的活动进行检验和确认，见图 4;

——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;

——使用基于软件方法用于诊断随机的硬件失效时,正确执行的检验功能测试,例如:黑盒子测试;

——修改后,合适的软件安全生命周期内的活动。

9.3.2.3　有关安全的应用软件(SRASW)

软件安全生命周期(见图 4)适用于 SRASW。

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

——对开发周期进行检查和确认，见图 4;

——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,应采用或推荐采用以下提高效率的附加措施(较低效率用于 PL_r 为 c,中等效率用于 PL_r 为 d,较高效率用于 PL_r 为 e):

a) 应复查有关安全软件的技术规范,使生命周期内涉及的所有人员可得到该规范,且应包括以下内容的描述:

1) 具有要求的 PL 的安全功能以及相关的工作模式;

2) 性能准则，例如:响应时间;

3) 具有外部信号界面的硬件结构。

b) 工具、库和语言应选择:

1) 适用且可安全使用的工具要求：对于性能等级（PL）达到 e 级的元件及其配套工具，该工具应符合相应安全标准；若采用两款不同零件且各配套不同工具，则该组合可安全使用。所采用的技术特征应能检测可能导致系统性错误的情形（如数据类型不匹配

等）。相关检查应主要在编译阶段开展，不得仅依赖运行阶段完成。工具宜强化语言子集与编码指南，或至少对开发者使用上述内容起到督促、引导作用。

2） 只要合理可行，宜采用经确认的功能模块(FB)库-工具制造商提供的有关安全的功能模块(FB)库(PL=e),或符合本文件且用途已被确认的详细功能模块(FB)库。

3） 宜采用合理的适用于模块化方法的 LVL-子集,可包括 GB/T 15969.3 中认可的语言子集。推荐采用图示语言(例如：功能模块图、梯形图)。

c） 软件设计的特征应为:

1） 半正式的方法描述数据和控制流，例如:状态图或程序流程图;

2） 主要由源自有关安全的经确认的功能模块库的功能模块实现模块化和结构化设计;

3） 限制了编码大小的功能模块;

4） 编码在功能模块内执行,功能模块宜有一个入口和一个出口点;

5） 三个阶段的结构模型,输入处理-输出(见图 5);

6） 在唯一一个程序位置安全输出的安排;

7） 使用用于检测外部失效的技术和用于在输入、处理和输出模块内置于安全状态的预防性编程技术。

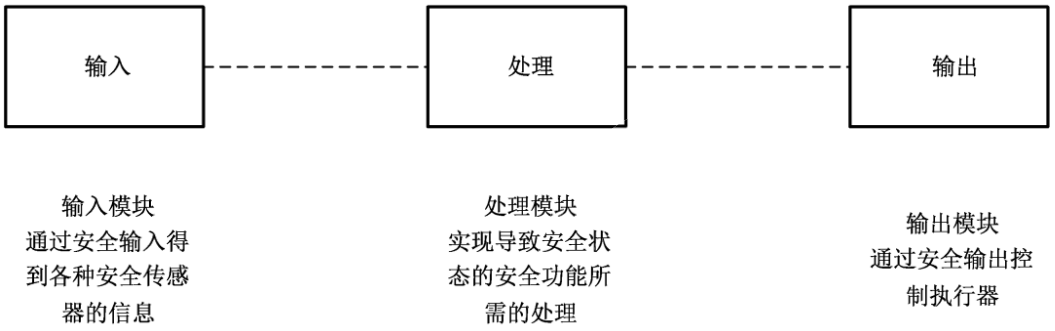


图5 软件的一般结构模型

d） 当 SRASW 和非 SRASW 组合在一个元件中时：

1） SRASW 和非 SRASW 应在与有明确定义的数据链接的不同 FB 中编码;

2）不应存在非有关安全数据和有关安全数据的逻辑组合,因为这可导致有关安全信号的完整性下降。例如:结构控制有关安全信号的地方采用逻辑“非”组合有关安全和非有关安全的信号。

e） 软件执行/编码:

1） 代码宜易读、易懂及可测试,为此宜使用符号变量(代替显式硬件地址);

2） 应使用合理的或公认的编码指南;

3） 宜使用应用层(预防性编程)可用的数据完整性和真实性检查(例如:范围检查);

4） 代码宜接受仿真测试;

5） PL=d或 PL=e 时,宜通过控制和数据流分析检验。

f） 测试：

1）合适的确认方法为功能性行为和性能准则(例如:时序性能)的黑盒子测试;

2）PL=d 或 PL=e 时,推荐由分析边界值开始进行试验;

3） 宜制定试验计划，且宜包括具有完成准则和所需工具的试验用例;

4） I/O 测试应保证在 SRASW 内正确使用有关安全信号。

g） 文件：

1） 应对所有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/声明及公告中足够的注释。

h） 验证:如复查、检查、遍查或其他的合适活动。

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

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

注：修改不影响已在使用的系统。

k） 验证仅针对专用代码，对于经验证的库函数则不必重复验证。

9.3.2.4 基于软件的参数化

应考虑把基于软件的有关各参数进行参数化,作为软件安全要求规范中要描述的 SRCS 设计的一个方面。采用 SRCS 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：

——控制有输入的范围；

——传输前控制数据损坏；

——从参数传输进程中控制错误的影响；

——控制完整参数传输的影响；

——控制参数化所用工具的硬件和软件故障和失效的影响。

参数化工具应符合对 SRCS 的所有要求,可使用特别的程序设定有关安全参数。该程序应包括通过以下两种方式之一确认 SRP/CS 的输入参数:

——修改后的参数重新发送至参数工具；

——确认参数完整性的其他合适方式。

包括随后的确认,例如:通过合适的技术熟练人员确认、通过参数化具自动检查的方式确认等。

注1：采用非专用装置开展参数化工作时，在数据传输与转发流程中，编码 / 译码软件模块及用户侧安全参数可视化软件模块，应至少实现功能层面的多样性设计，以此规避系统性失效风险。

注2：基于软件参数化的文件显示所用数据、识别与 SRCS 相关参数所需的必要信息、参数化实施人员信息，以及其他相关信息（如参数化日期），均应完整留存 / 记录。

注3：对基于参数化的软件进行以下的检验:

——检验每个有关安全参数的正确设置(最小值、最大值和典型值)；

——检验有关安全参数是否进行了合理性检查；

——检验是否防止了有关安全参数未经授权的修改；

——检验参数化数据/信号的生成与处理过程，是否能够确保不造成安全功能的丧失。

9.3.3 系统确认

9.3.3.1 概述

确认SRCS有关安全部件提供的安全功能是否符合其规定特性,根据技术规范要求,确认与安全相关的输出信号的正确性,以及与输入信号的逻辑相关性。应确认 9.3.3.2~9.3.3.9 的试验项目。

9.3.3.2 有关安全停止功能

有关安全的停止功能(例如:由安全保护装置触发)制动后，一旦有必要,应使起重机械进入安全状态。这种停止功能应优先于由操作原因引起的停止。

起重机械一般包含速度控制、超速停止功能、运行方向控制、限位开关停止功能、吊具避障停止功能（限自主运行起重机）、超载荷（力矩）停止功能，紧急停止功能等紧急停止功能测试，具体测试方法如下:

a） 速度测试:在手动/自动控制模式下,使起重机械以正常速度、最大速度运行，测试起重机械的正常速度与最大速度。

b） 超速测试:短接超速开关，测试起重机械是否会停止运行。

c） 运行方向测试：发出操作指令，测试起重机械实际运行方向与指令是否一致。

d） 限位开关功能测试：在手动/自动控制模式下,低速度运行起重机械后接触限位开关,起重机应紧急停止向危险方向运行,并保持停止状态但能向反向运行。

e） 吊具避障停止功能测试： 自主运行的起重机在自动控制模式下,避障停止功能测试为起重机在直线轨迹上以规定速度自动运行,通过障碍物触发避障传感器(激光/超声波等),引起起重机械保护性停止，测试从停止位置到障碍物位置的距离。

f）超载荷（力矩）停止功能：慢速起升载荷，当实际起重量超过实际幅度所对应的起重量额定值，但小于 110%起重量额定值时，超载限制器/起重力矩限制器应当起作用，此时应自动切断向不安全方向(如上升、幅度增大、臂架外伸或这些动作的组合)的动力源，但允许机构作安全方向的运动，并且发出禁止性报警信。

g）紧急停止功能测试:根据 GB/T 16855.1-2018 中表8的规定,急停功能应按GB/T 16754 规定检测,急停功能在任何时间都应可用和可操作,在起重机的各种运行模式/工况中，该功能应优先于所有其他功能,并且不应削弱为解脱陷入危险人员而设计的任何便利性。直到急停功能手动复位以前,任何启动指令(预定的、非预定的或意外的)应无效。

9.3.3.3 手动复位功能

安全保护装置发出停止指令后,停止状态应保持到有安全重启状态为止,通过复位防护装置,解除停止指令,再重新恢复安全功能。

手动复位功能应:

——通过 SRCS 内的一个独立的手动操作装置提供;

——只有所有安全功能和防护装置处于工作状态时才能实现复位;

——自身不能引起移动或危险状态;

——谨慎操作;

——使控制系统能接受独立的启动指令。

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

9.3.3.4 启动/重启功能

自主运行的起重机不宜具有自动启动/重启功能，危险状态不可能存在的情况下除外。

启动和重启的规定也适用于能够遥控的起重机械。

9.3.3.5 局部控制功能

当自主运行起重机通过诸如便携式遥控装置或有线操纵装置进行局部控制运行时,应符合以下要求：

——选用的局部控制应位于危险区之外;

——局部控制应只有在风险评价定义的区域才有可能触发危险状态;

——局部控制和主要控制之间的切换不应产生危险状态。

9.3.3.6 响应时间

SRCS 的响应时间为起重机械全部响应时间的一部分。必需的全部响应时间能够影响有关安全部件的设计,测试方法为按压起重机械的急停按钮或者触发起重机械限位开关,测试起重机械 SRCS 停止运动所需的时间（不同机构应分开测试）。

9.3.3.7 有关安全的安全参数

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

如果 SRCS 中有关安全数据手动输入错误能够导致危险状态,那么应在 SRP/CS 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。

9.3.3.8 电源的波动、损失和恢复

当电源电压的波动超出了设计工作范围时(包括能量供应损失),SRCS 应连续提供或触发能使起重机械系统其他部件保持安全状态的输出信号。

10 检验和确认

10.1 概述

在降低风险的过程中,所有与安全有关的起重机械性能值都应检验,包括在附录 C 中提到的有关控制系统需要的性能。

所有安全要求均应根据其相关检验标准进行检验，检验和检验方法的详细信息如下：

——A 检查：检查起重机械结构的状况；

——B 实际测试：在正常和异常情况下测试起重机械，功能测试(如故障注入测试)、循环测试(如可靠性测试)性能测试(如制动性能测试)；

——C 测量：将起重机械性能的真实值与特定的极限值进行比较；

——D 在操作过程中观察：(如方法 A)在正常和异常情况下检查起重机械的功能,如额定载荷、过载情况和影响条件；

——E 检查原理图:通过原理图的设计(如电气、气动、液压)和相关规范检查；

——F 软件检查:结构化检查,或通过软件代码的设计和相关的规范(代码检查或测试软件代码应该遵循的)；

——G 审查任务风险评估：结构审查或通过风险分析、风险评估和相关文件；

——H 检查图纸及相关文件:电气布置设计图纸和相关文件。

10.2 SRCS 确认

10.2.1 目的

用于 SRCS 的确认程序的要求,包括:检查和 SRCS 测试,以保证达到安全要求规范中陈述的要求 SRCS 确认可形成适用于起重机械设计的确认活动的一部分。

10.2.2 一般要求

应按照预定计划执行 SRCS 确认。

注1：有些情况,安全确认只能在安装后才能完成(例如:应用软件开发在安装后才能确定)。

注2：可编程序的 SRCS 确认由硬件、软件要求确认组成。软件确认要求包括在 9.3.2 中SRCS 要求规范(见 8.2)中规定的各 SRCF、所有 SRCS 操作和维护程序应通过试验和(或)分析进行确认。

SRCS 安全确认的测试应形成恰当文档,对各 SRCF 应有下列陈述:

a) 安全确认计划使用的 SRCS 版本和试验的 SRCS 版本；

b) 在 SRCF 试验(或分析)中,在 SRCS 安全确认计划期间具体涉及规定的要求；

c) 使用的工具和设备连同校准数据；

d) 每次试验结果；

e) 期望结果和实际结果的差异。

产生差异时,必要时应进行纠正活动和重新测试,并形成文件。

10.3 SRCS 系统安全完整性确认

针对起重机械控制系统的复杂程度,若为复杂电子设计,同时需达到PL=d时,可使用GB28526-2012相关设计要求,具体内容见GB28526-2012第6章,同时需满足以下内容:

a) 在规范、设计和集成阶段暴露失效的功能测试,和在SRCS软件/硬件的确认期间应采用避免失效的功能测试。包括检验(例如通过检查或试验)以评估 SRCS 是否受到保护,防止有害环境的影响,并应符合安全要求规范。

b) 干扰抗扰度测试用以保证 SRCS 能够满足电磁兼容相关要求。对于 SRECS 子系统或子系统元件不必执行电磁干扰的抗扰度测试,SRCS 对它的预期应用有足够的抗扰度,通过分析可以表现出来。

c) 要求的安全失效系数(Safe failure fraction)大于或等于 90%时应执行故障插入测试,这些试c验应在 SRCS 硬件中引入或模拟故障,结果应形成文件。

此外，下列一个或多个考虑 SRCS 的复杂性和指定的 SIL 的分析技术组应适用:

a) 静态分析和失效分析；

b) 静态、动态分析和失效分析；

c) 模拟和失效分析。

此外，下列一个或多个考虑 SRCS 的复杂性和指定的SIL的测试技术组应适用:

a) 黑盒测试:在实际功能状态下开展动态行为试验，以暴露潜在失效问题，验证其是否符合SRCS 功能规范要求，并评定 SRCS 的有效性与鲁棒性。
b) 如果安全失效系数小于90%应执行故障插入(注入)测试。此类试验需在 SRCS 硬件中引入或模拟故障，试验结果应形成正式文件留存。
c) 应执行“最坏情况”测试,以评定用分析技术指定的极端(即最坏)情况;
d) 当数据通信用于执行一个安全功能时，应估算通信过程中的失效量（例如残余错误率），失效量的估算及必要的技术措施应符合GB/T 20438.2和GB/T 20438.3的要求。
e) 现场试验:使用来自不同应用的现场经验作为一种措施,以避免SRCS 确认期间出现故障。

附 录 A
（资料性）
起重机械常见危险源

风险评估的重要步骤之一为危险（源）辨识。表 A.1 提供了一份最低辨识危险源的建议参考清单。具体的产生原因和危险事件可以参考GB/T 45374或者T/CASEI 62001相关附录。

表A.1 起重机械常见危险源

类别	名称	危险源
1.1电气系统	1.系统硬件	1）各电器元件间连接接触不良
		2）电器、电子元件、传感器等失效（老化、性能下降等）
		3）线缆、传感器等选型错误
		4）线缆破损或绝缘失效
		5）带电回路对地绝缘失效
		6）电气元件及装置安装不规范（位置、减震措施、布线及安装质量等）
		7）操作按钮、手柄、软件界面等颜色标识不正确或中文标识缺失
		8）电磁兼容性不能满足要求
		9）急停按钮失效
		10）储能系统失效（如电磁铁蓄电池）
		11）未按规定布置照明或照明损坏
	2.控制系统	1）控制系统不能满足实际运行工况要求
		2）控制系统误动作时会危及起重机的安全运行
		3）远程控制通讯网络连接中断、延时或存在安全漏洞等
	3.接地与防雷	1）起重机本体金属结构与供电线路的保护导线未进行可靠接地
		2）司机室与起重机本体接地点之间无可靠连接
		3）电气设备外壳、金属导线管及其支架等未进行可靠接地
		4）用起重机械金属结构和接地线作为载流零线
		5）接地电阻不符合要求

附 录 B
（规范性）
确定 SIL--风险图

B.1 一般要求

本附录描述了一种风险图方法,目的为说明一般原理。这种定性方法可以通过对与受控设备和受控设备控制系统有关的风险因素的了解确定起重机械SRCS的SIL。当风险模型符合表B.1 中说明的内容时,这种方法尤为有效。

当采用定性方法时,为了简化问题,引用一些参数共同描述当起重机械SRCS失效或不可用时危险情况的性质。选择合适的参数,将这些参数结合起描述分配到SRCS的SIL。这此参数：

——允许对产生的风险进行合理的分级；

——包括关键风险评估因素。

B.2 危险事件分类

危险事件可参照附录A提供的示例,根据作业环境、吊运物等不同,起重机械可能立生的危险事件会有所变化,不局限于附录A所提供的内容,需与被测对象的制造单位、使用单位等共同确认。

通过对危险事件的不同参数分类及组合,可获得起重机械SRCS的SIL。对以下参数进行危险事件分类,具体内容见表A.1:

——危险事件的后果严重性 S:严重程度由低至高,分别为 S1、S2、S3；

——发生危险的概率 P:由低至高,分别为 P1、P2；

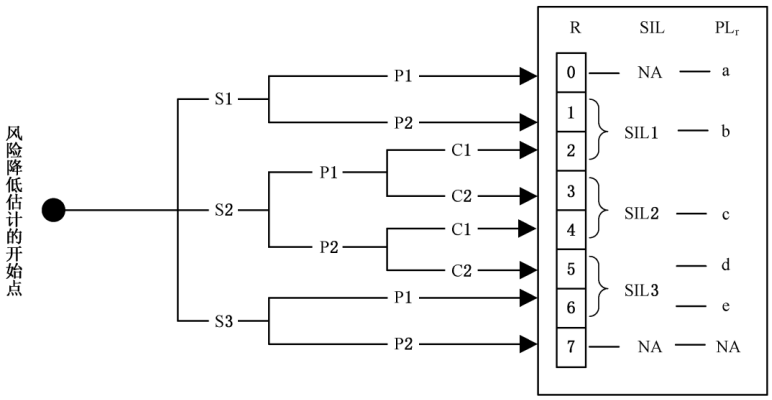
——危险事件的可控性 C:可控程度由低至高,分别为 C1、C2。

表B.1 风险参数说明

风险参数		分类	备注
危险事件后果严重性	S1	轻微伤害	应考虑危险事件能够实际发生的最严重（可信的最坏情况）的伤害。
	S2	较大伤害（如人员轻伤等）	
	S3	严重伤害（如人员死亡、设备倾覆等）	
危险事件的发生概率	P1	低概率（偶发）	连续运行时发生危险的概率
	P2	高概率（频繁发生）	
规避或减小伤害的可能性	C1	某些情况下可以控制	C1指通过控制系统或急停装置等在一定情况下可以控制危险事件的进行。
	C2	不可控	

B.3 风险图实现

风险图实现见图 B.1。



说明:R 表示风险等级,通过 0~7 表示风险的由低至高,NA 表示不适用

图B.1 风险图

附 录 C
（规范性）
安全要求

C.1 概述

起重机械应符合安全要求。如果出现第6章中描述的起重机械可能出现的危害,应确认安全要求、对应的 SIL 以及所要采取的相应措施,保护操作人员之外的人、设备或者其他安全相关物体不受任何伤害，确保操作人员的安全。

C.2 动力源的危害

起重机械应防范与它的动力源有关的所有危害发生。起重机械的电气和机械安全性能应按GB/T 5226.1和GB5226.32的相关要求以及起重机械的电气和机械安全标准,按照适用的标准设计任何暴露于起重机械周围的人都应受到保护,应防止其与起重机上的带电部分直接或间接的接触.应提供一种隔离任何危害能源的方法(如:电气、机械、液压、气动、化学和热)。这种危害的能源应被清楚地识别,并且如果重新连接将导致危害发生,隔离器应能够被锁定

对于上述危害,如果适用,应采用以下安全防护及补充保护措施:

1) 用于保护危险能量部件的防护装置或外壳,其设计应符合IEC 60529 定义的电气危险的适当IP等级,而其他由风险评估决定的危险,则应符合 ISO 13857 规定的安全距离;
2) 在出现过热的地方,应采用散热措施(例如:散热器、气流)。如果使用风扇，宜使用风扇控制装置。

C.3 系统起动和重新起动

起重机械在起动后,不得立即执行任何危险动作。起重机在系统起动和重新起动时电动机不会出现任何过放电现象,系统电路应保持足够安全几余,电容受潮或其他原因易导致系统起动或重起时起火爆炸。

C.4 电磁兼容

在工作场景中,起重机械正常工作所产生的骚扰电平不应妨碍其他设备按预定方式工作,其电子系统的抗电磁干扰能力,在正常可预见的所有可能的情况下不应出现有可能导致危害的异常运动和异常状态起重机械应符合 GB/T 37283 和 GB/T 37284 的规定

起重机械产生的电磁骚扰强度，不应超出其预期使用场合规定的允许限值。设备自身应具备足够的抗电磁干扰能力，以确保在预期使用环境中稳定、正确运行。

针对上述电磁危害，若适用，应采取下述安全防护或补充保护措施之一：通过对入射辐射实施电磁屏蔽，将相应风险降低至可接受水平。

C.5 对身心健康的影响

起重机械在工作时,不应对操作人员身心健康(身体和心理)造成影响。

与人有肢体接触的操纵装置其接触部位材质应避免使用过敏材料(如镍、铬和部分橡胶材料会使皮肤产生过敏反应),接触部位形状应符合人体工学设计要求。

与人的交互方式设计（如安全监控管理系统）,应尽量简单易用,利于人的理解,并避免因让使用者需经常性留意某些紧急或异常状态而导致的精神紧张以致疲劳等不适。

应通过风险评估,尽量消除起重机对人可能造成的心理负面影响。对于上述危害,如果适用,应采用以下安全防护及补充保护措施:

a)减震(悬挂)机制的使用;
b)使用姿势支撑物。

C.6 起重机械运动可能造成的危害

与安全相关部件接触的时候避免起重机械作危害运动,起重机械运行过程中或者停止时,具有足够的稳定性,避免因结构断裂、倾覆等造成人身或环境危害。对于上述危害，如果适用,应采用以下安全防护及补充保护措施:

a）符合要求的稳定性设计；

b）有监测稳定性的传感器或限位措施；

c）限制起重机械的速度；

d）防止超载的装置。

C.7 不正确的自主决策和行为造成的危害

具有自主决策和行为能力的起重机械,应避免因起重机决策信息不全面等因素导致的不正确决策或行为对人造成伤害后果,或对环境造成危害后果。

起重机械可通过提高其决策行为的可靠性(例如:采用更好的传感器等),或通过限定起重机的使用条件和环境，降低因起重机不够全面的甚至错误的行为决策所可能导致的对人或设备产生伤害的风险。

对于上述危害,如果适用,应采用以下安全防护及补充保护措施:

a） 传感器和传感算法的能力/可靠性应提高到一个没有不可接受的风险发生的水平。

b） 识别算法的设计方式,应能计算出某一决策为正确的概率并且可以被监视。对于具有高不确定性结果的决策,应使用替代方法和(或)附加信息进行重新评估。如果重新评估后,不确定依然不能接受,应寻求外部援助或启动保护停机。

c） 对导致危险状况的决策，应进行确定性检查。

d） 决策应由多个传感器加以验证。

C.8 使用者对起重机械缺乏认知

风险评估表明,操作人员对起重机缺乏认知具有危害性,需要采取措施降低风险。例如:在工作环境中,起重机械运行时会发出声音降低危害；起重机在自主运行过程中检测到人或其他障碍物时有自主停机避障,不用担心会撞到人或其他障碍物；动臂式起重机,在其动作的过程中需要与人及周围物体保持一定距离。

对于上述危害,如果适用,应采用以下安全防护及补充保护措施:

a）应提供声光发生器,以警告使用者潜在的危险情况；

b）应提供警告灯或其他光学装置,以警告使用者和第三方,有起重机械出现；

c）若有安全相关物体在其保护性停止空间内,则起重机械应停止,并在物体离开后继续执行其任务。

C.9 定位和导航方式

自主运行的起重机械应具有足够的准确导航、自主避障的能力,规划合理的运动路线,在运动时与安全相关部件碰撞时不会造成预见之外的危害。工作环境变化时,在定位和导航发生故障不会导致不可预期的危害。定位不确定时不会导致起重机本体或者起重机相关部件发生危害性运动，对于上述危害,如果适用,应采用以下安全防护及补充保护措施:

a)监测定位的稳定性和可信度,并在不稳定的定位时,进入安全状态；

b)不稳定定位时的补偿。

附 录 D
（资料性）
SRCS 使用信息

D.1 目的

应提供 SRCS 信息,使用户能够开发程序,以保证在起重机使用和维护期间保持SRCS所要求的功能安全。

D.2 安装、使用与维护文件

安装、使用与维护文件见 GB/T 15706-2012 中第6章提供的一般信息,起草随机文件时应予以考虑。文档应提供 SRCS 的安装、使用和维护信息，应包括:

a)设备、安装和装配的全面描述。

b)SRCS 预期使用的陈述和防止可预见的误用的必要措施。

c)实际工作环境信息(例如:照明、温度、气体环境)(适合时)。

d)起重机总图及主要部件图(适合时)。

e)电气原理图。

f)检验试验时间间隔或寿命。

g)SRCS 功能和机器电气控制系统功能之间的交互作用描述(包括互连接线图)。

h)必要措施描述,保证 SRCS 功能从机械电气控制系统功能中分离出来。

i)如果需要,暂停SRCF(例如:用于手工编程,程序检验),为保持安全所提供的防护和措描述。

j)有关编程信息。

k)适于 SRCS 维护要求的描述，包括:

1) 用于记录机器维护历史的日志。

2）为保持 SRCS 功能安全需要进行的日常维护活动,包括:有预定寿命的元件日常更换。

3）SRCS 中出现故障或失效时要遵循的维护程序。

4）维护、重新试运转必需的工具和适用于维护工具、设备的程序。

5）定期测试规范、预防维护和纠正维护规范。

注1：定期试验为确认正确操作和检测故障必要的功能试验。

注2：预防性维护为保持 SRCS 所需性能而采取的措施。

纠正维护包括将 SRCS 带回到设计状态的特定故障发生后采取的措施。

附 录 E
（资料性）
功能安全管理相关修改程序及文件要求

E.1 修改程序

在SRCS 设计、集成和确认期间(例如:SRCS 安装和试运行时)修改时,本附录规定的修改程序适用。

修改 SRCS 的要求源自于下列情况,例如:

——安全技术规范或标准的变化;

——实际使用条件;

——安全事件/事故经验 ;

——生产工艺变化;

——起重机械改造或其操作模式改变。

注：按照 SRCS 的使用信息(附录 D)或说明书对其进行的干预(例如:调整、设置、修理),本附录不考虑修改。

要求修改 SRCS 的原因应生成文件。要求的修改及其影响应进行分析,以建立 SRCS 的功能安全效果。修改的效果分析和其对 SRCS 功能安全影响的 分析应形成文件。以经过修订的文件为基础,在执行任何修改前应准备一个完整的行动计划,并形成文件。

E.2 配置管理程序

E.2.1 配置管理程序应按照功能安全计划(见 6.2.1)执行,应考虑下列因素:

a) 各修改过程的计划。

b) 决策过程和修改 SRCS 相关决定的文件。

c) 改变要求程序的按时间顺序排列的文档(例如:工作日志),包括:

1）识别可能受影响的危害;

2）改变要求(硬件或软件)的描述;

3）改变要求的原因;

4）每个决定的授权;

5）影响分析;

6）重新检验(对各阶段)和重新确定;

7）受改变要求活动影响的所有文件;

8）在改变过程中执行的所有活动和执行这些活动的人或实体。

d) 下列信息的文件，允许随后审查：

1）配置状况;

2）版本状态;

3）所有修改和批准的理由;

4）修改的细节。

E.2.2 适当改变控制过程的程序应考虑下列要求：

a) 为每个 SRCS 版本定义唯一的基线程序。

b) 基线的所有配置项目的定义。这至少应包括:

1)安全要求分析和规范;

2） 有关设计文件;

3） 硬件或软件模块;

4） 试验计划和结果;

5） 检验和确认报告;

6） 已存在的软件部分,这些软件部分将并入 SRCS;

7） 创建和试验用的开发环境;

8） 所有配置项有唯一标识的准确维护，保持 SRCS 的完整;

9） 改变控制程序;

10） 效果分析,应对每个改变要求进行评定。该评定应包括合适的危害分析,并应考虑 SERCS 其他所有修改活动;

11） 对 SERCS 所有可接受的修改,返回到 SERCS 的硬件和软件适当的设计阶段(例如:规范、设计、集成、安装);

12） 执行所有必要的操作，以证明已达到规定的安全完整性;

13） 对执行必要的改变要求活动的授权应取决于影响分析的结果。

E.3 文件

E.3.1 文件应:

——精确和简明，便于理解;

——适合其预期目的;

——容易获取和保持。

E.3.2 SRCS 的设计者应区别出用户相关的文件与设计和建造相关的文件。

E.3.3 文件应有标题和名称,指明其内容范围。

E.3.4 文件应有修订索引(版本号),从而能够区别文件的不同版本。

E.3.5 文件的修改应符合E.2.1的要求。

参 考 文 献

[1] TSG51-2023 起重机械安全技术规程
[2] 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
[3] GB/T 38260-2019 服务机器人功能安全评估
[4] GB/T 15969.6-2015 可编程序控制器 第6部分：功能安全
[5] GB 4943.1 信息技术设备 安全 第 1部分:通用要求
[6] GB/T 23821 机械安全 防止上下肢触及危险区的安全距离

中国特种设备检验协会团体标准

《起重机械安全相关电气、电子和可编程电子控制系统的功能安全》

编制说明

一、工作简况

1．任务来源

根据中国特种设备检验协会团体标准工作委员会文件《中国特种设备检验协会团体标准项目任务书》要求，本项目由中国特种设备检验协会团体标准工作委员会起重机械标准化工作组指导、监督和具体管理。项目由江苏省特种设备安全监督检验研究院牵头负责起草，联合南京理工大学、河南省特种设备安全检测研究院以及相关起重机制造单位、电气企业共同参与。本标准基于江苏省市场监管局科技项目《起重机械电气功能安全评估关键技术研究》(KJ204102)的研究成果。

2.主要工作过程

编制阶段：

1．2022年6-8月，完成前期调研，查阅相关标准及资料，确定标准编制的总体思路和框架搭建。

2.2022年8月25日，编制组在南京进行了第一次会议，会议研讨制定相应工作计划和责任分工，确立工作思路，制定了标准编制计划和实施时间表。

3.2022年11月26日，编制组召开了内部讨论会议，对标准草案逐条进行了讨论，根据正文内容增加两条术语定义，优化部分表格

格式。

4. 2023年2月6日，编制组召开了内部讨论会议，结合实际需求，优化调整了附录A中表格的内容。

5.2023年4月1日，编制组召开了内部讨论会议，按照标准格式进行了文本调整，优化部分细节内容。

6.2023年10月19日，编制组在南通召开会议，结合科研项目的进展情况对部分内容进行了优化。

7.2023年10月31日,编制组在南京对标准进行了进一步优化，形成了第一版的征求意见稿；

8.2023年11月-2024年8月，编制组前往山东、江苏、河南、重庆等地开展调研，交流标准内容，根据收集的信息，结合TSG51的内容要求对标准进行了相应调整，并在院内小范围征求意见。

8.2024年11月27日，编制组根据内部征求意见的结果对征求意见稿进行了修订，形成第二版征求意见稿。

8.2025年11月14日，编制组召开研讨会，对第二版征求意见稿进行了研讨，结合新发布的GB/T45374《起重机械 危险源辨识》，调整了流程图、附录资料等，形成第三版征求意见稿。

征求意见阶段:

编制组将讨论稿在内部公示审阅，根据反馈意见修订后形成《起重机械安全相关电气、电子和可编程电子控制系统的功能安全》(征求意见稿)及编制说明，报送至中特协团标委起重机械工作组秘书处。

二、 标准编制原则和主要内容论据

1. 标准编制原则

面向市场与技术创新结合:遵循“面向市场、服务产业、自主制定、适时推出”原则,紧密结合国际标准、科研项目和实际需求，统筹推进标准修订与产业应用协同发展。

适用性与可操作性:保证标准内容满足当前起重机的现状及今后智能化起重机的发展需求，为起重机械电气系统安全要求提供明确、具体的依据，确保内容表达科学准确、语言简洁精炼。

规范性与协调性:标准的结构和内容编排严格依据 GB/T1.1-2020，确保符合机械制造标准体系要求，与现行法规、标准保持协调一致。

2. 标准主要内容

本标准主要针对起重机械电气系统的安全要求,主要技术内容如下:

范围:明确了本文件适用于以单台方式使用的起重机械相关控制系统的功能安全,以协同方式共同工作的无人起重机群组的功能安全评估可参照此标准。

规范性引用文件: 给出了本文件编制中主要引用的标准。

术语和定义: 给出了起重机械功能安全、安全相关控制功能等术语，同时 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》界定的术语和定义适用于本文件。

符号及缩略语:因本文件涉及大量缩略语,因此在此处统一表述。一般要求: 给出了评估人员、范围和内容上的规定要求。

流程: 规程了起重机械功能安全评估流程图

危险识别和风险评估：给出了危险识别的一般要求和风险评估的流程。

功能安全管理：规定了达到安全相关控制系统（SRCS）所需要的管理和技术工作的要求。

安全相关控制功能规范要求：给出了由安全相关控制系统（SRCS）执行安全相关控制功能规范(SRCF)的要求。

安全相关控制系统设计与整合：给出了安全相关控制系统（SRCS）的设计或选择要求。

检验和确认：给出了安全相关控制系统（SRCS）的检验要求及方法。

附录A—附录E：给出了危险源、风险图法、起重机伤害等资料性附录。

3.解决的主要问题

近年来，随着起重机械不断向大型化、高参数和智能化等方向发展，因起重机械安全相关电气、电子和可编程电子控制系统失效而导致起重机械发生故障或事故的概率也逐渐增加，而目前起重机的相关检规或标准主要通过功能验证的方式来确认电气系统的完好性，难以满足当前和今后智能化起重机械电气功能安全评估需求。特别是《起重机械安全技术规程》（TSG51-2023）的发布，其内容上对电气系统的功能安全提出了相关要求，例如2.6.1条款，A6.4条款等。因此，制定《起重机械安全相关电气、电子和可编程电子控制系统的功能安全》标准，有利于提升设计制造过程中电气设备的本质安全，也有利

于进一步规范电气风险评估报告的统一性、完整性和可操作性。

四、标准中涉及专利的情况

本标准不涉及专利问题。

五、预期达到的社会效益等情况、对产业发展的作用等情况

提升安全规范性、促进行业标准化：统一起重机行业电气功能安全要求，确保行业内的一致性和规范性，消除行业内各单位在起重机电气安全设计、制造、检测和评估过程中的个性化差异，促进行业标准化进程。

六、与国际、国内对比情况

本标准的编写主要参考了国际标准 ISO 13849（对应国标 GB/T16855）和国际标准 IEC61508（对于国标 GB/T20438）系列标准以及 ISO 23849（对应国标 GB/T30175），结合起重机械形成在起重机中运用要求，制定过程中未查询到同类国际、国内标准。

七、与现行相关法律、法规、规章及相关标准，特别是强制性标准的协调性

国际标准 ISO 13849（对应国标 GB/T16855）和国际标准 IEC61508（对于国标 GB/T20438）系列标准协调一致。

八、重大分歧意见处理经过和依据

无。

九、贯彻标准的要求和措施建议

建议标准批准发布 3 个月后实施，实施前组织检验机构、起重机械整机制造单位、相关电气设计制造单位、使用单位开展培训。

十、其他应予说明的事项

无。