ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 21109.1—2022/IEC 61511-1:2016
代替 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、硬件和应用编程要求

Functional safety of safety instrumented systems in the process industry sector—Part 1:Framework, definitions, system, hardware and application programming requirements

(IEC 61511-1:2016, Functional safety—Safety instrumented systems for the process industry sector—Part 1:Framework, definitions, system, hardware and application programming requirements, IDT)

2022-10-12 发布　　2023-05-01 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 …… Ⅳ
引言 …… Ⅵ
1　范围 …… 1
2　规范性引用文件 …… 3
3　术语和定义及缩略语 …… 3
3.1　术语 …… 3
3.2　术语和定义 …… 4
3.3　缩略语 …… 19
4　与本文件的符合性 …… 21
5　功能安全管理 …… 21
5.1　目的 …… 21
5.2　要求 …… 21
6　安全生命周期要求 …… 24
6.1　目的 …… 24
6.2　要求 …… 26
6.3　应用程序 SIS 安全生命周期要求 …… 27
7　验证 …… 30
7.1　目的 …… 30
7.2　要求 …… 30
8　过程危险和风险评估 …… 31
8.1　目的 …… 31
8.2　要求 …… 31
9　给保护层分配安全功能 …… 32
9.1　目的 …… 32
9.2　分配过程要求 …… 32
9.3　基本过程控制系统作为保护层的要求 …… 34
9.4　防止共因、共模和相关失效的要求 …… 35
10　SIS 安全要求规范(SRS) …… 35
10.1　目的 …… 35
10.2　一般要求 …… 35
10.3　SIS 安全要求 …… 35
11　SIS 设计和工程 …… 37
11.1　目的 …… 37
11.2　一般要求 …… 37
11.3　检测到故障时的系统行为要求 …… 38

11.4 硬件故障裕度 …… 39
11.5 关于设备选择的要求 …… 40
11.6 现场设备 …… 42
11.7 接口 …… 42
11.8 维护或测试设计要求 …… 43
11.9 随机失效的量化 …… 44
12 SIS应用程序开发 …… 45
12.1 目的 …… 45
12.2 一般要求 …… 45
12.3 应用程序设计 …… 46
12.4 应用程序的实现 …… 47
12.5 应用程序验证要求(审查和测试) …… 48
12.6 应用程序方法和工具的要求 …… 48
13 工厂验收测试(FAT) …… 49
13.1 目的 …… 49
13.2 建议 …… 49
14 SIS安装和调试 …… 50
14.1 目的 …… 50
14.2 要求 …… 50
15 SIS安全确认 …… 51
15.1 目的 …… 51
15.2 要求 …… 51
16 SIS操作和维护 …… 53
16.1 目的 …… 53
16.2 要求 …… 53
16.3 检验测试及检查 …… 55
17 SIS修改 …… 56
17.1 目的 …… 56
17.2 要求 …… 56
18 SIS停用 …… 57
18.1 目的 …… 57
18.2 要求 …… 57
19 信息和文档要求 …… 57
19.1 目的 …… 57
19.2 要求 …… 57
参考文献 …… 59

图1 GB/T 21109的整体框架 …… Ⅶ
图2 IEC 61508与IEC 61511间的关系 …… 2

图 3　IEC 61511 和 IEC 61508 间的详细关系 …… 2
图 4　安全仪表功能和其他功能的关系 …… 3
图 5　可编程电子系统(PES):结构和术语 …… 13
图 6　包含三个 SIS 子系统的 SIS 架构示例 …… 15
图 7　安全生命周期阶段和功能安全评估阶段 …… 25
图 8　应用程序安全生命周期及其与 SIS 安全生命周期的关系 …… 28
图 9　典型保护层和风险降低方法 …… 34

表 1　IEC 61511 中使用的缩略语…… 20
表 2　SIS 安全生命周期一览表…… 26
表 3　应用程序安全生命周期:一览表 …… 26
表 4　安全完整性要求:PFD_{avg} …… 32
表 5　安全完整性等级:SIF 的危险失效平均频率 …… 33
表 6　不同 SIL 对应的最小 HFT 要求 …… 39

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。

本文件是GB/T 21109《过程工业领域安全仪表系统的功能安全》的第1部分。GB/T 21109已经发布了以下部分:

——第1部分:框架、定义、系统、硬件和应用编程要求;

——第2部分:GB/T 21109.1的应用指南;

——第3部分:确定要求的安全完整性等级的指南。

本文件代替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》,与GB/T 21109.1—2007相比,除结构调整和编辑性改动外,主要技术变化如下:

——增加了功能安全管理中对人员的管理要求(见5.2.2.3);

——增加了功能安全管理系统的要求(见5.2.5.2);

——增加了根据本文件发布前的规范、标准或实践设计和实施的SIS,对用户提出了要求(见5.2.5.4);

——增加了功能安全评估、审核和修订的新要求(见5.2.6);

——增加了安全生命周期结构和计划要求(见6.2);

——增加了应用程序SIS安全生命周期要求(见6.3);

——增加了验证要求(见7.2);

——增加了对SIS开展安防风险评估的要求(见8.2.4);

——删除了“安全完整性等级4的附加要求”,增加风险降低要求>10 000或危险失效平均频率<10^{-8}/h的审查要求和保护层分配要求;

——增加了BPCS不准备符合本文件时,保护层分配的要求(见9.3.4);

——增加了应用程序安全要求规范相关要求(见10.3.3～10.3.6);

——增加了SIS设计和工程要求中的安全手册要求和SIF通信要求(见11.2);

——增加了SIS旁路情况下的相关要求(见16.2.3、16.2.4、16.2.7、16.2.11);

——增加了SIS备件的相关要求(见16.2.12);

——增加了负责执行操作和维护的人员关于危险和风险分析、分配和设计的审查要求(见16.2.13);

——更改了失电情况下SIS的行为要求,将其扩充为动力源(包括电源、空气、液动源或气动源)丢失情况下SIS的行为要求(见11.2.11,2007年版的11.2.11);

——更改了检测到故障时的系统行为要求(见11.3,2007年版的11.3);

——更改了硬件故障裕度要求(见11.4,2007年版的11.4);

——更改了设备选择要求(见11.5,2007年版的11.5);

——更改了SIF的失效概率,将其改为随机失效的量化并补充了随机失效量化相关要求(见11.9,2007年版的11.9);

——更改了应用软件要求,已改为SIS应用程序开发,并明确应用程序设计、实施、验证要求及方法工具要求(见第12章,2007年版的第12章)。

本文件等同采用IEC 61511-1:2016《功能安全　过程工业领域安全仪表系统　第1部分:框架、定义、系统、硬件和应用编程要求》。

本文件做了下列最小限度的编辑性改动:

——将标准名称修改为《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、硬件和应用编程要求》；

——将规范性引用的IEC 61511(所有部分)列入第2章；

——纳入了IEC 61511-1:2016/AMD1:2017的修正内容，所涉及的条款的外侧页边空白位置用垂直双线(‖)进行了标示。

本文件由中国机械工业联合会提出。

本文件由全国工业过程测量控制和自动化标准化技术委员会归口(SAC/TC 124)。

本文件起草单位：机械工业仪器仪表综合技术经济研究所、中石化安全工程研究院有限公司、国能智深控制技术有限公司、浙江中控技术股份有限公司、国家管网集团北方管道有限责任公司、杭州盘古自动化系统有限公司、上海辰竹仪表有限公司、北京龙鼎源科技股份有限公司、上海工业自动化仪表研究院有限公司、北京市科学技术研究院城市安全与环境科学研究所、绵阳市维博电子有限责任公司、福建顺昌虹润精密仪器有限公司、北京京仪集团有限责任公司、重庆宇通系统软件有限公司、南京优倍电气有限公司、西安东风机电股份有限公司、北京维盛新仪科技有限公司、深圳市特安电子有限公司、安徽天康(集团)股份有限公司、汉威科技集团股份有限公司、西门子(中国)有限公司。

本文件主要起草人：史学玲、刘瑶、李玉明、裘坤、周有铮、俞文光、朱明露、田雨聪、张韬、靳江红、钱福群、沈玉富、阮赐元、岳周、王玥、朱杰、姜巍巍、张卫华、张艾森、魏海洋、帅冰、张新国、张刚、杨柳、施隋靖、左新、马欣欣、周婷、卜志军、姜荣怀、张鹏、朱爱松、王莉、陈志扬、董健、王毅、李传友、牛小民、史威、熊文泽、孙炜、张萍、魏振强、皮英霞、孙舒、韩占武、陈祖志、李佳、曹德舜、李荣强。

本文件及其所代替文件的历次版本发布情况：

——2007年首次发布为GB/T 21109.1—2007；

——本次为第一次修订。

引　言

在过程工业中，用来执行安全仪表功能的安全仪表系统已应用多年。要使仪表能有效地用于安全仪表功能，最重要的是该仪表需达到某些最低标准和性能水平。

GB/T 21109 阐述了过程工业安全仪表系统的应用。GB/T 21109 还强调要执行一次过程危险和风险评估(H&RA)，使之能导出安全仪表系统的规范。仅在与安全仪表系统的性能要求相关时，才考虑其他安全系统的贡献。安全仪表系统包括执行安全仪表功能所必要的从传感器到最终元件的所有设备。

GB/T 21109 包括以下几部分。

——第 1 部分：框架、定义、系统、硬件和应用编程要求。目的是提出安全仪表系统(SIS)的规范、设计、安装、运行和维护要求，以确保该系统能使过程达到或保持安全状态。

——第 2 部分：GB/T 21109.1 的应用指南。目的是提供按 GB/T 21109.1 中定义的安全仪表功能及其相关的安全仪表系统的规范、设计、安装、操作和维护的指南。

——第 3 部分：确定要求的安全完整性等级的指南。目的是确定安全仪表功能的安全完整性等级的各种不同方法。

GB/T 21109 包含了作为应用基础的两个概念：安全生命周期和安全完整性等级。

GB/T 21109 针对基于使用电气(E)/电子(E)/可编程电子(PE)技术的安全仪表系统。在逻辑解算器使用其他技术的情况下，需应用 GB/T 21109 的基本原则来确保实现功能安全要求。GB/T 21109 还涉及安全仪表系统的传感器和最终元件，不管它们用了何种技术。GB/T 21109 在 GB/T 20438 的框架范围内专用于过程领域。

为达到上述最低原则，GB/T 21109 提出了 SIS 安全生命周期活动的方法。采纳此种方法以便使用合理和一致的技术策略。

在大多数情况下，固有安全过程设计就能很好地实现安全性。但是在某些情况下，这是不可能或不切实际的。必要时，还可结合一个或一些保护系统来降低已发现的残余风险。保护系统可依靠不同的技术(化学的、机械的、液压的、气动的、电气的、电子的、可编程电子的)。为促成该方法，GB/T 21109 要求：

——执行危险和风险评估以便确定整体安全要求；

——给安全仪表系统分配安全要求；

——在一个框架内工作，该框架适用于实现功能安全的所有仪表类措施；

——详述了如何使用某些活动(如安全管理)，这些活动适用于实现功能安全的所有方法。

针对过程工业的安全仪表系统的 GB/T 21109：

——包括从初始概念、设计、实现、运行和维护直到停用的所有 SIS 安全生命周期阶段；

——能使现有的或新的国家专用的过程工业标准同 GB/T 21109 协调一致。

GB/T 21109 致力于在过程工业领域达到高度一致(如基本原则、术语、信息等)。这将带来安全和经济两方面的好处。GB/T 21109 的整体框架见图 1。

在权限方面，在管理当局(如国家的、省的、自治区的等)已建立过程安全设计、过程安全管理或其他规定的情况下，这些要求需比 GB/T 21109 中定义的要求优先考虑。

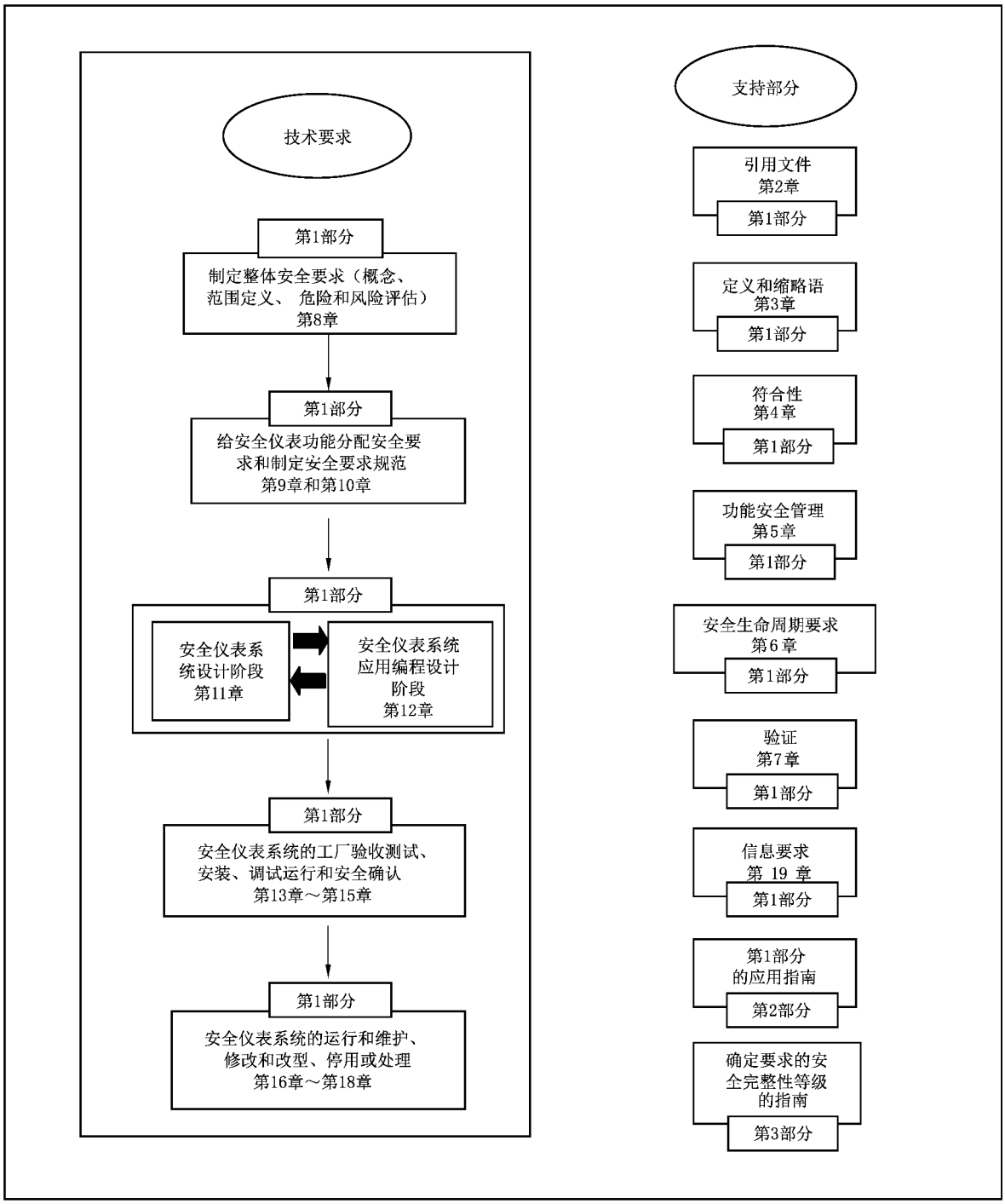


图 1　GB/T 21109 的整体框架

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、硬件和应用编程要求

1 范围

本文件给出了安全仪表系统(SIS)的规范、设计、安装、运行和维护要求,以确保该系统能使过程达到或保持安全状态。本文件是GB/T 20438(所有部分)在过程领域的应用标准。

本文件:

a) 规定了实现功能安全的要求,但未规定执行这些要求的责任方(如:设计方、供应商、业主/运行公司、承包商)。根据安全计划、项目计划和管理以及国家规定将责任分配给不同各方。

b) 适用于把满足GB/T 20438.1~20438.3—2017或本文件中11.5要求的设备集成到用于过程领域应用的整体系统中,但不适用于希望声明设备适用于过程领域的SIS的制造商(见GB/T 20438.2—2017和GB/T 20438.3—2017)。

c) 定义了IEC 61511和IEC 61508的关系(见图2和图3)。

d) 适用于为具有有限可变语言的系统开发应用程序,或使用固定程序语言设备的情况,但不适用于开发嵌入式软件(系统软件)或使用全可变语言的制造商、SIS设计方、集成商和用户(见GB/T 20438.3—2017)。

e) 适用于过程领域的多个行业,例如,化工、石油和天然气、造纸、制药、食品与饮料及非核能发电。

注1:过程领域中的某些应用可能还需满足一些附加的要求。

f) 描述了SIF与其他仪表功能间的关系(见图4);

g) 在考虑了通过其他方法实现的风险降低后,辨识出SIF的功能要求和安全完整性要求;

h) 规定了系统架构和硬件配置、应用编程以及系统集成的生命周期要求;

i) 规定了SIS用户和集成商的应用编程要求;

j) 适用于为保护人员、公众、环境,使用单个或多个SIF实现功能安全的情况;

k) 可适用于非安全应用,例如,资产保护;

l) 定义了SIF的实施要求,SIF是实现功能安全的整体部署的一部分;

m) 使用了SIS安全生命周期(见图7),并定义了确定SIS功能要求和安全完整性要求所必须的一系列活动;

n) 规定了定义每个SIF的安全功能要求和安全完整性等级(SIL)时应开展危险与风险评估;

注2:图9概述了风险降低措施。

o) 建立了SIL对应的要求时失效平均概率(要求模式)和危险失效平均频率(要求模式和连续模式)的目标值;

p) 规定了硬件故障裕度(HFT)的最低要求;

q) 规定了实现特定SIL所要求的措施和技术;

r) 定义了根据本文件实施一个SIF时所能实现的最高功能安全性能等级(SIL4);

s) 定义了最低的功能安全性能等级(SIL1),低于这个等级则本文件不适用;

t) 提供了一个确定SIL的框架,但未规定特定应用所要求的SIL(应基于特定应用的了解和整体风险降低目标来确定);

u） 规定了 SIS 从传感器到最终元件所有部分的要求；
v） 定义了 SIS 安全生命周期中需要的信息；
w） 规定了 SIS 设计需考虑人员因素；
x） 未对操作和维护人员个体提出直接要求。

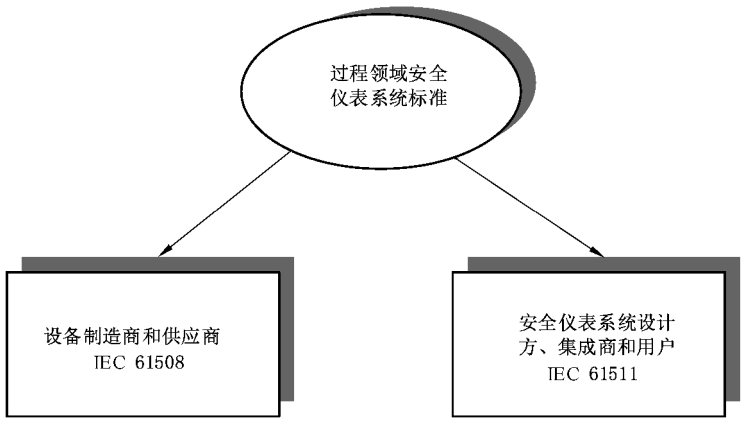


图 2 IEC 61508 与 IEC 61511 间的关系

注 3：对于 IEC 61511 中引用 IEC 61508 的内容，安全仪表设计方、集成商和用户还需使用 IEC 61508。

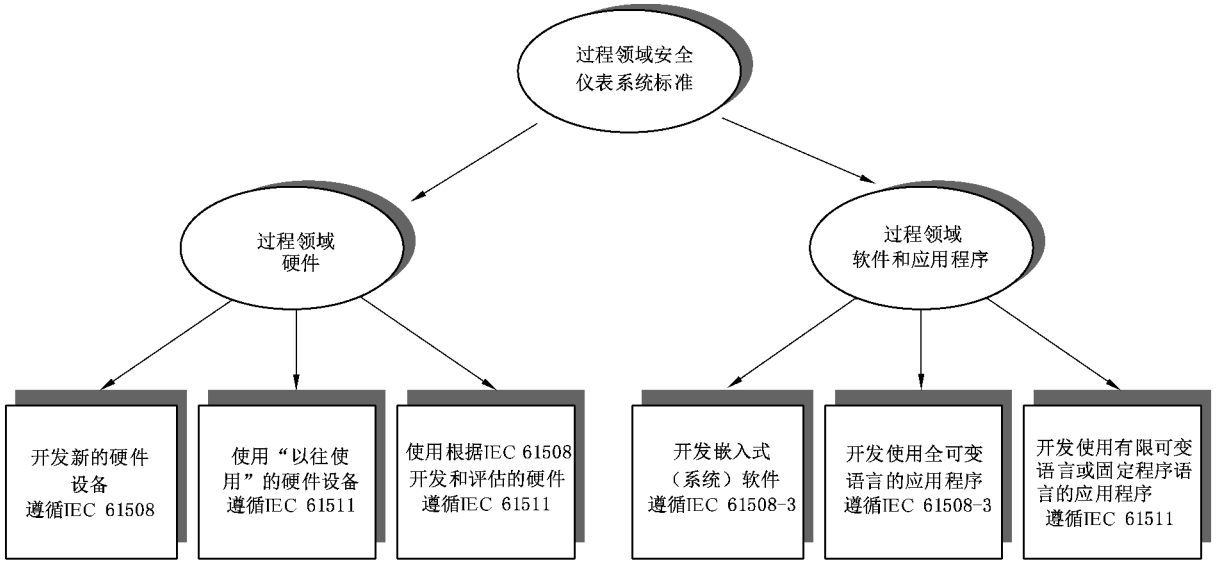


图 3 IEC 61511 和 IEC 61508 间的详细关系

注 4：当系统中包含遵循其他标准（如机械、燃烧器等）的子系统时，指南见本文件和 IEC 61511-2:2016 中 A.7.2.2。

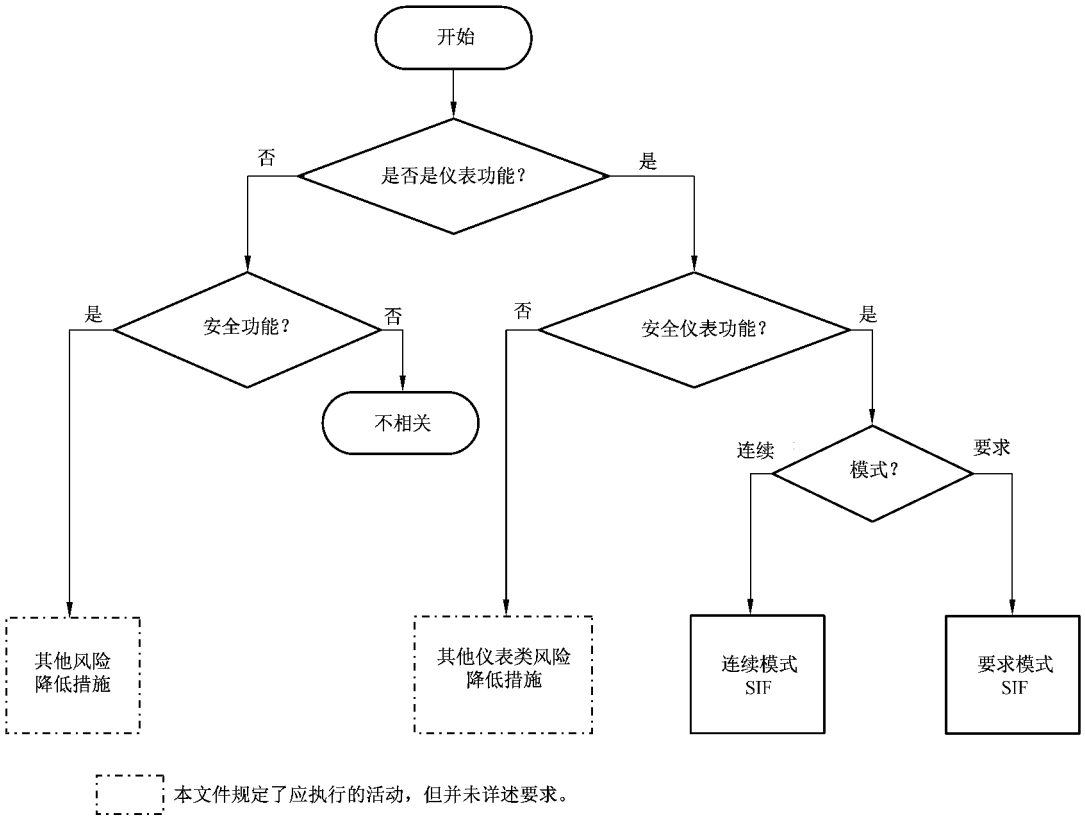


图 4　安全仪表功能和其他功能的关系

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。

IEC 61511(所有部分)　功能安全　过程工业领域安全仪表系统(Functional safety—Safety instrumented systems for the process industry sector)

注：GB/T 21109(所有部分)　过程工业领域安全仪表系统的功能安全[IEC 61511(所有部分)]

GB/T 20438.1—2017　电气/电子/可编程电子安全相关系统的功能安全　第 1 部分：一般要求(IEC 61508-1:2010，IDT)

GB/T 20438.2—2017　电气/电子/可编程电子安全相关系统的功能安全　第 2 部分：电气/电子/可编程电子安全相关系统的要求(IEC 61508-2:2010，IDT)

GB/T 20438.3—2017　电气/电子/可编程电子安全相关系统的功能安全　第 3 部分：软件要求(IEC 61508-3:2010，IDT)

3　术语和定义及缩略语

3.1　术语

术语按照字母顺序在 3.2 中列出。

3.2 术语和定义

下列术语和定义适用于本文件。

某些定义可能和 GB/T 20438.4—2017 中相同术语的定义不同，造成不同的原因可能是这些术语用于过程领域，也可能是为了与其他相关权威引用文件匹配（如 IEC 60050，ISO/IEC Guide 51:2014）。然而，除非另有声明，这些定义的技术含义和 GB/T 20438.4—2017 中相同的术语完全一样。

3.2.1

架构 architecture

配置 configuration

系统中硬件和软件组件的特定配置。

注：在 IEC 61511 系列中可以指，例如，SIS 子系统的布局、SIS 子系统的内部结构或 SIS 应用程序的内部结构。

3.2.2

资产保护 asset protection

分配给一个系统的功能，为防止资产损失或破坏而设计。

3.2.3

基本过程控制系统 basic process control system；BPCS

对来自过程及其相关设备、其他可编程系统和/或操作员的输入信号作出响应并生成输出信号使过程及其相关设备按照期望的方式运行的系统，但它不执行任何 SIF。

注 1：BPCS 包括确保过程以期望的方式运行的所有必要设备。

注 2：BPCS 通常可执行多种功能，如过程控制功能、监视、报警。

3.2.4

旁路 bypass

阻止全部或部分 SIS 功能执行的行为或设施。

注 1：旁路的例子包括：

- 阻断跳闸逻辑的输入信号，但仍然显示输入参数并向操作员报警；
- 使跳闸逻辑发送给最终元件的输出信号保持在正常状态，以阻止最终元件动作；
- 在最终元件周围设置的物理旁路；
- 预选输入状态（如开/关输入）或通过一种工程工具（如在应用程序里）强制设置。

注 2：其他术语也可用于代指旁路，如超驰、阻止、禁用、强制、抑制或屏蔽。

3.2.5

通道 channel

独立执行某个特定功能的单个设备或一组设备。

注 1：通道中的设备可包括输入/输出（I/O）设备、逻辑解算器、传感器以及最终元件。

注 2：双通道（即两个通道）配置是指拥有执行相同功能的两个独立通道的配置。两个通道可以完全相同也可以不同。

注 3：本术语可用来描述一个完整系统或系统的一部分（如传感器或最终元件）。

注 4：通道描述了 SIS 硬件架构特征，通常用此特征来满足硬件故障裕度要求。

3.2.6

共因 common cause

3.2.6.1

共因失效 common cause failures

由单一事件引起的不同设备的并发失效，并且这些失效间不互为因果。

注 1：由一个共因引起的所有失效未必恰好在同一时间发生，因此在 SIF 实际失效前有一定时间来检测共因的发生。

注 2：共因失效也可能导致共模失效。

注 3：共因失效的可能性降低了系统冗余或故障裕度的效果(如增加了多通道系统中两个或更多通道的失效概率)。

注 4：共因失效是相关失效，可能由外部事件(如温度、湿度、过电压、火灾、腐蚀)、系统性故障(如设计的、组装的或安装的错误、缺陷)、人为错误(如误用)等引起。

注 5：单个共因失效是属于一组并发失效中的一个失效。

3.2.6.2

共模失效　common mode failures

不同设备的并发失效，这些失效具有相同的失效模式(即相同故障)。

注 1：共模失效可能由不同的原因引起。

注 2：共模失效也可能是共因失效(3.2.6.1)的结果。

注 3：共模失效的可能性降低了系统冗余和故障裕度的效果(如两个或更多通道以相同的方式失效，引起相同的错误结果)。

注 4：单个共模失效是属于一组并发失效中的一个失效。

3.2.7

补偿措施　compensating measure

在维护或过程运行中，发现 SIS 性能降级时，临时采取用来管理风险的方法(这些方法是计划内的并且文档化)。

3.2.8

组件　component

执行某一特定功能的系统、SIS 子系统或设备的组成部分。

注：组件也可能包括软件。

3.2.9

配置管理　configuration management

迭代系统中组件识别和布置的规则，为了在生命周期全过程中管控组件变更，保持系统连续性和变更的可追溯性。

3.2.9.1

保守方式　conservative approach

开展分析和计算时使用的谨慎方式。

注：在安全领域，每次分析、假设或计算时(关于模型、输入数据、计算等)都选择这种方式以确保产生保守结果。

3.2.10

控制系统　control system

对来自过程和/或操作员的输入信号进行响应，并产生使过程以期望的方式运行的输出信号的系统。

注：控制系统包括传感器和最终元件，可能是 BPCS，可能是 SIS，也可能是两者的结合。

3.2.11

危险失效　dangerous failure

使给定的安全动作受阻或无法执行的失效。

注 1：只有在针对一个给定的 SIF 时，才可以说某个失效是“危险”的。

注 2：实施了故障裕度时，一个危险失效可导致：

- SIF 降级，这种情况下可执行安全动作，但是会有更高的 PFD 或 PFH，或
- SIF 失效，这种情况下完全无法执行安全动作或已经诱发了危险事件。

注 3：没有实施故障裕度时，所有的危险失效都会导致 SIF 失效。

3.2.12

相关失效　dependent failure

概率不能表示为引起失效的独立事件的无条件概率的简单乘积的失效。

注 1：两个事件 A 和 B，如果 A 和 B 同时发生的概率 $P(A \& B)$ 大于 $P(A) \times P(B)$，则 A 和 B 是相关的。

注 2：保护层间相关失效的考虑参见 9.4.2 和 IEC 61511-3:2016 中附录 J。

注 3：相关失效包括共因失效。

3.2.13

检测到的 detected

揭露出的 revealed

显性的 overt

硬件和软件相关的一类失效或故障，它们自身发出通知或可通过正常操作或专用检测方法发现。

注 1：使用这些术语有以下差异：

- “显性的”是用于发生时（如由于状态改变）会自己发出通知的失效或故障。这样的失效可以在一发生时就开始维修。
- “检测到的”是用于发生时自己不会发出通知，保持隐藏直至被一些方法（例如，诊断测试、检验测试、操作员介入如物理检查和人工测试）检测到的失效或故障。只有当这些失效被揭露后才能对其进行维修。IEC 61511 中此术语的具体运用见注 2。
- “揭露出的”是用于由于是显性的或被检测到而被发现的失效或故障。

注 2：在 IEC 61511 中，除非上下文提及了其他含义，否则术语“危险的检测到的失效/故障”均指通过诊断测试检测到的危险失效。

注 3：若检测非常及时（例如，通过诊断测试），则检测到的失效或故障可作为显性的失效或故障考虑。若检测不是非常及时（例如，通过检验测试），则在提出安全完整性等级时，检测到的失效或故障不能作为显性的失效或故障考虑。

注 4：一个揭露出的危险失效只有在足够短时间内能够自动或人工采取有效措施以确保过程安全的情况下才能当作一个安全失效。

3.2.14

设备 device

能实现某一特定功能的硬件或含有软件的硬件。

注：例如，传感器、逻辑解算器、最终元件、操作员接口和现场配线。

3.2.14.1

现场设备 field device

直接与过程连接或位置非常靠近过程的 SIS 或 BPCS 设备。

注：例如，传感器、最终元件和手动开关。

3.2.15

诊断 diagnostics

揭露故障的频繁（相对于过程安全时间）自动测试。

3.2.15.1

诊断覆盖率 diagnostic coverage；DC

被诊断检测到的危险失效率的占比。不包括任何被检验测试检测到的故障。

注 1：诊断覆盖率通常应用于 SIS 设备或 SIS 子系统。如通常为传感器、最终元件或逻辑解算器确定诊断覆盖率。

注 2：对安全应用，诊断覆盖率通常应用于 SIS 设备或 SIS 子系统的危险失效。例如，一个设备的危险失效的诊断覆盖率为 $DC=\lambda_{DD}/\lambda_{DT}$，式中 λ_{DD} 是检测到的危险失效率，λ_{DT} 是总的危险失效率。对于一个具有内部冗余的 SIS 子系统，DC 与时间有关：$DC(t)=\lambda_{DD}(t)/\lambda_{DT}(t)$。

注 3：当给出诊断覆盖率（DC）和总的危险失效率（λ_{DT}），检测到的危险失效率（λ_{DD}）和未检测到的危险失效率（λ_{DU}）可以按照如下计算：$\lambda_{DD}=DC\times\lambda_{DT}$，$\lambda_{DU}=(1-DC)\times\lambda_{DT}$。

3.2.16

多样性 diversity

执行一个要求的功能的不同方式。

注：可以通过不同的物理方法、不同的编程技术或者不同的设计方式来实现多样性。

3.2.17

误差　error

计算出的、观测到的或测量到的值或条件，和真实的、规定的或理论上正确的值或条件之间的差异。

[来源：GB/T 2900.99—2016，192-03-02]

3.2.18

失效　failure

失去按要求执行的能力。

注 1：设备失效是导致设备出现某种故障状态的事件。

注 2：如果能力的丧失是由一个潜在故障引起，一旦特定的一组条件出现，则失效发生。

注 3：执行要求的功能必定会排除某些行为，把某些功能定义为要避免出现的行为，这些行为的出现就是失效。

注 4：失效是随机的或系统性的(见 3.2.59 和 3.2.81)。

[来源：GB/T 2900.99—2016，192-03-01，有修改]

3.2.18.1

失效模式　failure mode

失效发生的方式。

注：失效模式可以由功能丧失或状态转变来定义。

[来源：GB/T 2900.99—2016，192-03-17]

3.2.19

故障　fault

由于某个内部状态，无能力按要求执行。

注 1：故障可能由部件本身的失效引发，也可能由生命周期早先阶段(如规范、设计、制造或维护)的缺陷引发。

注 2：当一组特定的情况出现时，设备的一个故障会导致一个失效。

[来源：GB/T 2900.99—2016，192-04-01，有修改]

3.2.20

故障避免　fault avoidance

在 SIS 安全生命周期的任何阶段，使用技术和规程避免引入故障。

3.2.20.1

故障排除　fault exclusion

通过进一步分析排除由不太可能发生的失效模式引发的故障。

注 1：关于故障排除的进一步信息可参见 ISO 13849-1 和 ISO 13849-2。根据这些标准，故障排除可以基于：

- 技术上不太可能发生的故障；
- 独立于应用的普遍接受的技术经验；
- 与应用和特定危险有关的技术要求。

注 2：对于执行安全功能的设备识别出的失效模式，当其相关危险失效率相对于安全功能的目标失效量足够低时，此失效模式可以排除。也就是说，对于已声明故障排除的所有设备的失效模式，其危险失效率之和通常不可超过目标失效量的 1%。

3.2.21

故障裕度　fault tolerance

出现故障或错误时，功能单元能够继续执行要求的功能或操作的能力。

3.2.22

最终元件　final element

BPCS 或 SIS 的一部分，为达到或保持安全状态执行必要的物理动作。

注：例如，阀门、开关设备以及电机，包括他们辅助的元件(如电磁阀和用来驱动阀门的执行机构)。

3.2.23

功能安全　functional safety

与过程和 BPCS 有关的整体安全的一部分，它取决于 SIS 和其他保护层的正确工作。

3.2.24

功能安全评估　functional safety assessment；FSA

基于证据的调查，以评判一个或多个 SIS 和/或其他保护层所实现的功能安全。

3.2.25

功能安全审核　functional safety audit

对于按计划安排的功能安全要求专用的程序是否有效地执行并满意地达到规定目的进行系统地、独立的检查。

注：功能安全审核可以作为 FSA 的一部分。

3.2.26

硬件安全完整性　hardware safety integrity

在危险失效模式中，与随机硬件失效有关的 SIS 安全完整性的一部分。

注 1：与本术语有关的两个失效参数是危险失效平均频率和要求时失效平均概率。

注 2：见 3.2.82。

注 3：本定义与 GB/T 20438.4—2017 中的定义有差别，从而反映出过程领域术语的差异。

3.2.27

伤害　harm

对人体健康的损伤或损害，或对财产或环境的损害。

[来源：ISO/IEC Guide 51：2014，3.1]

3.2.27.1

伤害事件　harmful event

引起伤害的危险事件。

注：一个危险事件是否会导致伤害取决于人员、财产或环境是否暴露于危险情况中，以及对于人员伤害来说，暴露的人员是否能在事件发生后避免事件后果。造成伤害的危险事件才叫伤害事件。

3.2.28

危险　hazard

伤害的潜在根源。

注：本术语包括短时内发生的对人员的危害（如着火或爆炸），以及对人体健康长时间有影响的那些危害（如有毒物质或放射性释放）。

[来源：ISO/IEC Guide 51：2014，3.2，有修改]

3.2.28.1

危险事件　hazardous event

可能导致伤害的事件。

注：一个危险事件是否会导致伤害取决于人员、财产或环境是否暴露于危险情况中，以及如果会对人员造成伤害，这些暴露的人员是否能在事件发生后避免后果发生。

[来源：ISO/IEC Guide 51：2014，3.3，有修改]

3.2.28.2

危险情况　hazardous situation

人员、财产或环境暴露在一个或多个危险中的情况。

[来源：ISO/IEC Guide 51：2014，3.4]

3.2.29

人为错误　human error

引发不当结果的有意识或无意识的人的动作或不动作。

注 1：失误、疏漏、过失都是人为错误的例子。

注 2：这里不包括蓄意行为。

3.2.30

影响分析　impact analysis

确定一个功能或组件的改变对该系统和其他系统中其他功能或组件的影响的活动。

3.2.31

独立组织　independent organization

通过管理和其他资源，在进行安全评估或确认的 SIS 安全生命周期的特定阶段中，同负责活动的组织分开且为不同的组织。

3.2.32

独立人员 independent person

在进行安全评估或确认的 SIS 安全生命周期的特定阶段中，同所发生活动分开且不同的人员，这些人员对那些活动不负有直接责任。

3.2.33

输入功能　input function

为了给逻辑解算器提供输入信息，监视过程及其相关设备的功能。

注：输入功能可以是手动功能。

3.2.34

仪表　instrument

在执行某个动作中使用的仪器（典型的参见仪表系统）。

3.2.34.1

仪表系统　instrumented system

由传感器（如压力、流量、温度变送器）、逻辑解算器（如可编程控制器、分布式控制系统、离散控制器）和最终元件（如控制阀门、电机控制回路）组成的系统。

注：仪表系统执行仪表功能，包括控制、监视、报警和保护功能。仪表系统可以是 SIS（见 3.2.67）或 BPCS（见 3.2.3）。

3.2.35

逻辑功能　logic function

在输入信息（由一个或几个输入功能提供）和输出信息（由一个或几个输出功能使用）之间执行变换的功能。

注 1：逻辑功能将一个或几个输入功能转换为一个或几个输出功能。

注 2：进一步信息参见 IEC 61131-3:2013 和 IEC 60617-12:1997。

3.2.36

逻辑解算器　logic solver

BPCS 或 SIS 的一部分，它执行一个或多个逻辑功能。

注 1：在 IEC 61511 中，针对逻辑解算器使用了以下术语：

- 机电技术的电气逻辑系统；
- 电子技术的电子逻辑系统；
- 可编程电子系统的可编程电子逻辑系统。

注 2：例如，电气系统、电子系统、可编程电子系统、气动系统和液压系统。传感器和最终元件不是逻辑解算器的组成部分。

3.2.36.1

安全配置的可编程电子逻辑解算器　safety configured PE logic solver

专门配置用于安全应用的通用型工业级 PE 逻辑解算器。

注：进一步信息参见 11.5。

3.2.37

维护/工程接口　maintenance/engineering interface

为能正确维护或修改 SIS 所提供的硬件和软件。

注：维护/工程接口可能包括：在软件中可能含有的指令和诊断程序、具有适当通信协议的编程终端、诊断工具、指示器、旁路设备、测试设备和校准设备。

3.2.37.1

平均维修时间 mean repair time；MRT

预期的整体维修时间。

注：MRT 包含 MTTR 时间中的时间段(b)、(c)和(d)(见 3.2.37.2)。

3.2.37.2

平均恢复时间　mean time to restoration：MTTR

预期的完全恢复的时间。

注：MTTR 包含：

- 检测失效的时间(a)；
- 开始维修前的时间(b)；
- 实际的维修时间(c)；
- 组件恢复运行前的时间(d)。

(b)的开始时间是(a)的结束点；(c)的开始时间是(b)的结束点；(d)的开始时间是(c)的结束点。

3.2.37.3

最大允许维修时间　maximum permitted repair time；MPRT

检测到失效后允许的最长维修时间。

注 1：MRT 可用作 MPRT，但是定义 MPRT 时可以不考虑 MRT。

- 可选择小于 MRT 的 MPRT 来降低危险事件的可能性。
- 如果可以放宽对危险事件可能性的约束，则可选择大于 MRT 的 MPRT。

注 2：如果定义了 MPRT，在计算随机硬件失效概率时可使用 MPRT 取代 MRT。

3.2.38

减轻　mitigation

降低危险事件后果的行动。

注：例如，检测到火灾或气体泄漏时紧急减压或关闭风门，或检测到火灾时开启消防水。

3.2.39

(SIF 的)运行模式　mode of operation (of a SIF)

SIF 的运行方式，低要求模式、高要求模式或连续模式。

a) 低要求模式：在这种运行模式下，SIF 只有在要求时才动作，以将过程导入一个特定的安全状态，并且要求的频率不大于一年一次。

b) 高要求模式：在这种运行模式下，SIF 只有在要求时才动作，以将过程导入一个特定的安全状态，并且要求的频率大于一年一次。

c) 连续模式：在这种运行模式下，SIF 作为正常运行的一部分保持过程处于一种安全状态。

3.2.39.1

要求模式 SIF　demand mode SIF

在低要求模式[3.2.39 a)]或高要求模式[3.2.39 b)]下运行的 SIF。

注 1：SIF 发生危险失效时，危险事件只会在下列情况下发生：

- 失效未被检测到并且在下次检验测试前发生要求；
- 诊断测试检测到失效，但是相应过程及其有关设备没有在要求发生前进入安全状态。

注 2：在高要求模式下，通常使用连续模式标准是合适的。

注 3：表 4 和表 5 定义了在要求模式下运行的 SIF 安全完整性等级。

3.2.39.2

SIF 连续模式　continuous mode SIF

在连续模式[3.2.39 c)]下运行的 SIF。

注 1：SIF 发生危险失效时，除非在过程安全时间内采取预防措施，否则无需进一步失效就将发生危险事件。

注 2：连续模式涵盖执行连续控制以保持功能安全的 SIF。

注 3：表 5 定义了在连续模式下运行的 SIF 安全完整性等级。

3.2.40

模块　module

SIS 应用程序中的独立部分(可以嵌入一个或一组程序)，用来执行某个特定功能(例如，最终元件的启动、停止、测试序列，SIF 内部的应用特定序列)。

注 1：在 IEC 61131-3:2013 中，一个软件模块就是一个功能或功能块。

注 2：大多数模块会在一个应用程序中重复使用。

3.2.41

MooN

“N”个独立通道构成的 SIS 或其部分，其中“M”个通道足以执行 SIF。

3.2.42

必要的风险降低　necessary risk reduction

为确保风险不超过可容忍风险，由 SIS 和/或其他保护层实现的风险降低。

3.2.43

非可编程系统　non-programmable system

(NP)系统　(NP)　system

基于非计算机技术的系统(即不基于可编程电子或软件的系统)。

注：例如，硬接线电气或电子系统，机械、液压或气动系统。

3.2.44

运行环境　operating environment

设备安装的固有条件，这些条件会对设备的功能和安全完整性造成潜在影响。例如：

- 外部环境，如防冻需求、危险区域划分；
- 过程运行条件，如温度、压力、振动极限；
- 过程组分，如固体、盐、腐蚀物；
- 过程接口；
- 与工厂维护和运行管理系统的集成情况；
- 通信吞吐能力，如电磁干扰；及
- 动力源质量情况，如电源、空气、液压。

注：一些过程应用可能有特殊的运行环境要求以确保在重大事故事件中保持正常。例如，一些设备需要特殊的罩壳、吹扫或火灾防护。

3.2.45

操作模式　operating mode

过程操作模式　process operating mode

过程操作的所有计划状态，包括的模式有：检修或紧急停车后的开车、正常操作和停车、临时操作、紧急操作和停车等。

3.2.46

操作员接口　operator interface

在操作人员和 SIS 之间进行信息交换的手段（如显示界面、指示灯、按钮、喇叭、报警器）。

注：操作员接口有时又叫人机界面（HMI）。

3.2.47

输出功能　output function

根据来自逻辑功能的输出信息，控制过程及其相关设备的功能。

3.2.48

性能　performance

对照规范和 IEC 61511 系列，完成给定动作或任务的能力。

3.2.49

阶段　phase

发生 IEC 61511 中描述活动的 SIS 安全生命周期中的某个时段。

3.2.50

预防　prevention

降低危险事件发生可能性的行动。

3.2.51

以往使用　prior use

基于以前在类似运行环境的运行经验，由用户开展的文档化评估，以证明某个设备适用于 SIS 并且能达到所需的功能和安全完整性要求。

注 1：为了基于以往使用证明一个 SIS 设备可用，用户需文档说明设备能在类似的运行环境中实现满意的性能。为高度确定计划的设计、检查、测试、维护和操作具有充分的实践，必需了解在运行环境中设备如何运转。

注 2：经使用证明是基于设备制造商的设计基础（即温度极限、振动极限、腐蚀极限、需要的维护支持）。以往使用在处理设备的安全性能时，设备只能在某个过程领域工厂场地内运行，而这些场地往往不同于制造商的设计基础。

3.2.52

过程风险　process risk

由异常事件（包括 BPCS 故障）引起的过程条件产生的风险。

注 1：本文件中的风险与使用 SIS 提供必要的风险降低的特定危险事件有关（即与功能安全相关的风险）。

注 2：IEC 61511-3:2016 中描述了过程风险分析。确定过程风险的主要目的是给风险（不考虑保护层）建立一个参考点。

注 3：过程风险的评估包括相关人员因素问题。

注 4：本术语相当于 GB/T 20438.4—2017 中的“受控设备（EUC）风险”。

3.2.52.1

过程安全时间　process safety time

如果 SIF 未执行，从过程失效或基本过程控制系统失效（潜在的增加危险事件的可能性）到危险事件发生之间的时间段。

注：这只是过程的一个属性。SIF 需在考虑过程延迟（如容器冷却）的情况下足够快的检测到失效并且完成动作以防止危险事件发生。

3.2.53

可编程电子　programmable electronics;PE

基于计算机技术的部件,可能由硬件、软件以及输入和/或输出单元组成。

注:本术语覆盖基于一个或多个中央处理单元(CPU)及相关的存储器的微电子设备。过程领域可编程电子的例子包括:

——智能传感器和最终元件;

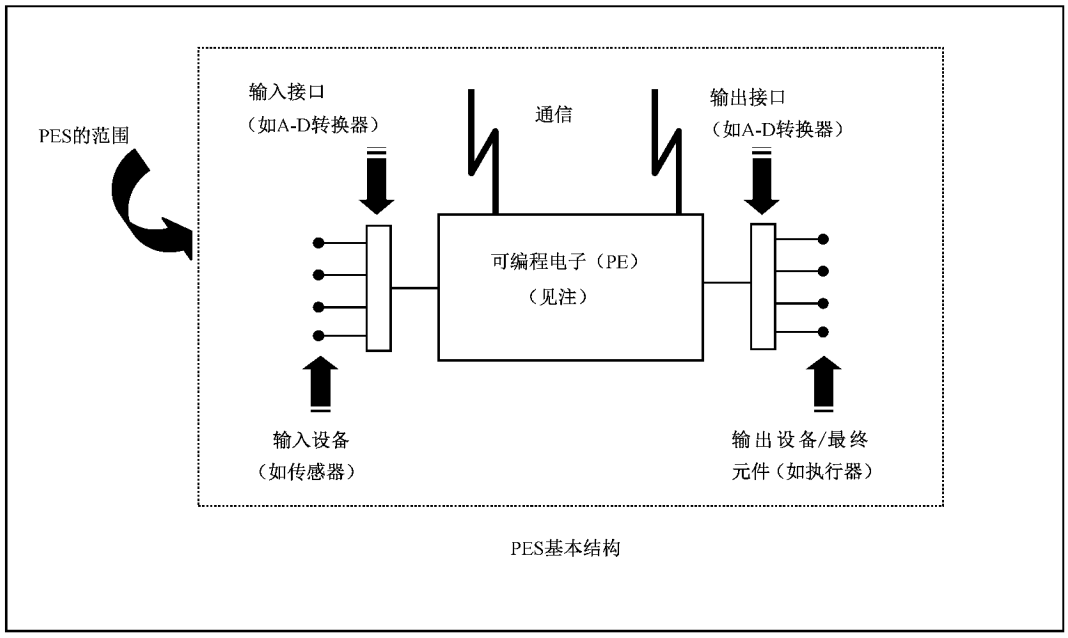
——可编程电子逻辑解算器,包括:

- 可编程控制器;
- 可编程逻辑控制器;
- 回路控制器。

3.2.54

可编程电子系统　programmable electronic system;PES

基于一个或多个可编程电子设备的,用于控制、防护或监视的系统,包括系统中所有的设备,如电源、传感器和其他输入设备、数据总线和其他通信途径、以及执行器和其他输出设备(见图 5)。



注:PE 画在本图的中心位置,但可存在于 PES 中多个位置。

图 5　可编程电子系统(PES):结构和术语

3.2.55

编程　programming

编码　coding

为解决某个问题或处理数据而设计、编写和测试一组指令的过程。

注:IEC 61511 中,编程通常与可编程电子(PE)相关。

3.2.56

检验测试　proof test

为检测出 SIS 中隐藏的危险失效而执行的周期性测试,以期在必要时通过维修使系统恢复如新或尽可能"如新"。

3.2.57

保护层　protection layer

通过控制、预防或减轻以降低风险的任何独立机制。

注：它可能是过程工程机制(如装危险化学品的容器尺寸)、也可能是机械工程机制(如安全阀)、或者 SIS、或者是管理规程(如应对紧急危险的应急计划)。可以自动启动或手动启动这些响应机制(见图 9)。

3.2.58

质量　quality

一个实体满足指明的和隐含需要的性能总和。

注：详见 ISO 9000。

3.2.59

随机硬件失效　random hardware failure

由一种或多种可能的退化机理引起的，硬件在某个随机时间发生的失效。

注 1：在不同部件中存在以不同速率发生的许多退化机理。因为在工作不同的时间之后，由于这些机理，制造公差会引起部件失效，所以某个包含许多部件的整体设备的失效将以可预见的速率发生，但发生的时间是不可预见的(即随机的)。

注 2：随机硬件失效和系统性失效的 2 个主要差别：

- 随机硬件失效只涉及系统本身(某个故障)，而系统性失效涉及系统本身和某个特定的条件(见 3.2.81)，因此，随机硬件失效仅由一个单独的可靠性参数(即失效率)表征，而系统性失效由两个可靠性参数(即已有故障的可能性和某个特定条件的危险率)表征。
- 系统性失效可在检测到后消除而随机硬件失效不能。

这意味着随机硬件失效的可靠性参数可以通过现场反馈来估计，而对系统性失效很难做到。系统性失效更适合通过定性方法来评估。

3.2.60

冗余　redundancy

存在不止一种途径来执行要求的功能或表示信息。

注 1：例如，使用重复设备和附加校验位。

注 2：冗余主要用来提高可靠性或可用性。

[来源：GB/T 20438.4—2017，3.4.6]

3.2.61

风险　risk

伤害发生可能性与该伤害严重性的组合。

注：发生可能性包括暴露于危险情况的概率、危险事件的发生概率和避免或限制伤害的可能性。

[来源：ISO/IEC Guide 51:2014，3.8]

3.2.62

安全失效　safe failure

可能触发某个给定的安全动作的失效。

注 1：一个失效是“安全的”只是对于某个给定的安全功能来说。

注 2：当实施了故障裕度时，安全失效会导致：

- 在安全功能可用的情况下继续运行，但是有更高的要求时成功率或者更低的危险事件发生可能性；
- 触发安全功能误动作。

注 3：当未实施故障裕度时，不论过程条件如何，安全失效将触发安全功能。这也称为误动作。

注 4：误动作就给定的安全功能来说是安全的，但是对其他安全功能来说可能是危险的。

注 5：误动作可能会对过程的生产可用性造成不利影响。

3.2.63

安全状态　safe state

达到安全时的过程状态。

注 1：一些状态比其他状态更安全。从某个危险条件到最终的安全状态，或者从安全条件到某个危险条件的过程中，过程可能必须经过几个中间安全状态。

注 2：在有些情况下，仅当过程处于连续控制时才存在安全状态。这样的连续控制可能是短时间的或是不确定的时段。

注 3：一个状态对于一个给定的安全功能来说是安全的，而对于其他给定的安全功能可能会增加危险事件的可能性。在这种情况下，第一个功能的最大允许平均误动作率（见 10.3.2）宜考虑其他功能相关的潜在风险的增加。

注 4：本定义同 GB/T 20438.4—2017 中的定义有差别，从而反映出过程领域术语中的差异。

3.2.64

安全　safety

不存在不可容忍的风险。

注：根据 ISO/IEC Guide 51，术语“可接受风险”和“可容忍风险”被考虑为同义词。

[来源：ISO/IEC Guide 51:2014，3.14，有修改]

3.2.65

安全功能　safety function

针对特定的危险事件，为达到或保持过程的安全状态，由一个或多个保护层实现的功能。

3.2.66

安全仪表功能　safety instrumented function；SIF

由安全仪表系统（SIS）实现的安全功能。

注：SIF 设计用来达到一个要求的 SIL，SIL 由其他参与降低相同风险的保护层决定。

3.2.67

安全仪表系统 safety instrumented system；SIS

用来实现一个或多个 SIF 的仪表系统。

注 1：SIS 由任意组合的传感器、逻辑解算器及最终元件组成（见图 6）。它也包括通信和辅助设备（如电缆、管道、电源、取压管、伴热）。

注 2：SIS 可以包括软件。

注 3：SIS 可以包括人为动作作为 SIF 的一部分（见 ISA TR 84.00.04:2015，第 1 部分）。

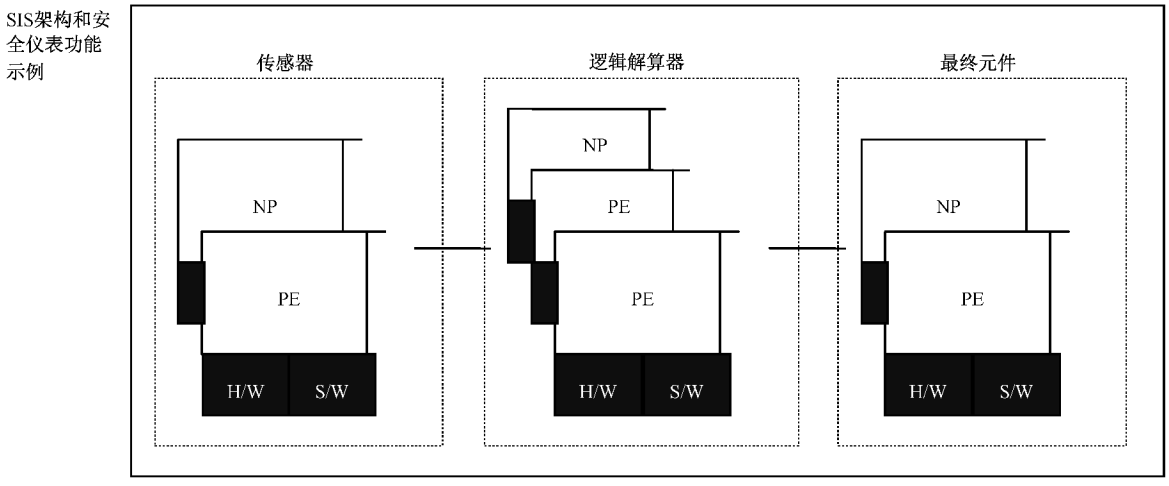


图 6　包含三个 SIS 子系统的 SIS 架构示例

3.2.68

安全完整性　safety integrity

在要求时执行所需 SIF 的 SIS 能力。

注 1：对于要求的 SIF，此定义等同于 SIS 的可信性。可信性常被理解为经济概念而不是安全概念，为了避免混淆，没有使用“可信性”。

注 2：能力包括功能响应(如在规定时间内关闭某个特定的阀门)和 SIS 能按要求动作的可能性。

注 3：在确定安全完整性时，需包括导致非安全状态的随机硬件和系统性失效的所有原因(如硬件失效、软件导致的失效和电气干扰引起的失效)。这些类型中的某些失效，特别是随机硬件失效，可以使用危险失效平均频率或者要求时的失效概率等参数来量化。然而，安全完整性还取决于许多系统因素，它们不能精确量化，通常在生命周期中定性考虑。系统性失效导致 SIS 危险失效的可能性可以通过硬件故障裕度(见 11.4)或其他方法和技术来降低。

注 4：安全完整性包含硬件安全完整性(见 3.2.26)和系统性安全完整性(见 3.2.82)，但也需考虑硬件和系统相互影响共同引发的复杂失效。

3.2.69

安全完整性等级　safety integrity level;SIL

为规定 SIS 应达到的安全完整性要求而分配给 SIF 的离散等级(4 个等级中的一个)。

注 1：SIL 等级越高，期望的 PFD_{avg} 越低，或者导致危险事件的危险失效平均频率越低。

注 2：目标失效量和 SIL 间的关系见表 4 和表 5。

注 3：SIL4 是安全完整性的最高等级，SIL1 是最低等级。

注 4：此定义和 GB/T 20438.4—2017 中的定义有差别，从而反应过程领域术语中的差异。

3.2.69.1

安全完整性要求　safety integrity requirements

为某个 SIF 声明一个给定的 SIL，实现这个 SIF 的 SIS 必须满足的一组 IEC 61511 的要求。

注：SIL 等级越高，相关的安全完整性要求越高。

3.2.70

SIS 安全生命周期　SIS safety life-cycle

从项目概念阶段开始到所有的 SIF 停用为止所发生的、包含在 SIF 实现中的必要活动。

注 1：严格地讲，术语“功能安全生命周期”更为准确，但从 IEC 61511 上下文来看可不必考虑形容词“功能(的)”。

注 2：IEC 61511 中使用的安全生命周期模型见图 7。

3.2.71

安全手册　safety manual

功能安全手册　functional safety manual

定义如何安全应用 SIS 设备、子系统或系统的信息。

注 1：安全手册可能包括来自制造商和用户的信息。

注 2：对于遵循 IEC 61508 的设备，来自制造商的信息就是安全手册。

注 3：这可能是一份独立文档，也可能是一份文档集。

注 4：此定义和 GB/T 20438.4—2017 中的定义有差别，从而反应过程领域术语中的差异。

3.2.72

安全要求规范　safety requirements specification;SRS

包含安全仪表功能和相关安全完整性等级的功能要求的规范。

注：在一些行业也称安全要求规格书。

[来源：GB/T 20438.4—2017，3.5.11，有修改]

3.2.73

传感器　sensor

BPCS 或 SIS 的一部分，用来测量或检测过程条件。

注：例如，变送器、转换器、过程开关以及位置开关。

3.2.74

软件　software

程序、进程、数据、规则和关于数据处理系统操作的相关文档。

注 1：软件与记录它的媒体无关。

注 2：不同类型软件的例子见 3.2.75 和 3.2.76。

3.2.75

应用编程语言　application programming languages

3.2.75.1

固定程序语言　fixed program language;FPL

在这种类型语言里，用户只能调整几个预先定义好的固定的参数组。

注：使用 FPL 的设备的典型例子是：智能传感器（如不带控制运算的压力变送器）、智能最终元件（如不带控制运算的阀门）、事件时序记录器、专用智能报警盒的设定点。FPL 的使用通常被称为“设备配置”。

3.2.75.2

有限可变语言　limited variability language;LVL

用于商业或工业可编程电子控制器的编程语言，其能力仅限于在相关安全手册中定义的应用。这种语言的记法可能是文本或图形或二者皆有。

注 1：这种语言用户容易理解，并可提供组合预定义的、应用专用的库函数的能力以实现 SRS。LVL 可提供一种与应用所要求的功能几乎一致的功能。

注 2：IEC 61511 认为实现安全属性必要的约束需综合以下情况：安全手册，应用编程人员定义过程控制算法所需要的功能与语言的契合度，逻辑解算器提供的嵌入到逻辑解算系统程序和逻辑解算器开发环境中的编译和运行时检查，在认证报告和安全手册定义的这些约束可以确保满足 GB/T 20438.3—2017 中的相关要求。

注 3：IEC 61511 里提到应用程序时，LVL 是最普遍使用的语言。

3.2.75.3

全可变语言　full variability language;FVL

计算机编程者易于理解，并可提供实现各种各样功能和应用的能力的一种语言。

注 1：使用 FVL 的系统的典型例子是通用型计算机。

注 2：在过程领域，嵌入式软件可能使用 FVL，而应用程序编程则很少使用 FVL。

注 3：FVL 的例子包括：Ada、C、Pascal、指令表、汇编程序语言、C＋＋、Java 和 SQL。

3.2.76

软件和程序类型　software & program types

3.2.76.1

应用程序　application program

专用于用户应用的程序。通常，它包含为达到 SIS 功能要求而必要的控制输入、输出、计算和决策的逻辑顺序、许可、限制和表达式。

3.2.76.2

嵌入式软件　embedded software

作为系统组成部分由制造商提供的软件，最终用户不能对其进行修改访问。

注：嵌入式软件也被称作固件或系统软件。见 3.2.75.3 全可变语言。

3.2.76.3

工具软件　utility software

用来创建、修改和编写应用程序的软件工具。

注：SIS 运行并不需要这些软件工具。

3.2.77

应用程序生命周期　application program life-cycle

从开始构思应用程序到永久性停用应用程序期间发生的活动。

注 1：一个典型的应用程序生命周期包括需求、开发、测试、集成、安装和修改等阶段。

注 2：软件（包括应用程序）不能被维护，但可以被修改。

3.2.78

SIS 子系统　SIS subsystem

SIS 的独立部分，它的危险失效将导致 SIS 的危险失效。

注 1：图 6 阐述了 SIS 由三个 SIS 子系统构成。

注 2：从割集的角度看（见 IEC 61025），SIS 子系统的最小割集也是整个 SIS 的最小割集。因此 SIS 里 SIF 的实施完全取决于 SIS 的 SIS 子系统（即 SIS 子系统失效，则相关的 SIF 也失效）。

3.2.79

系统　system

根据某个规则相互作用的一组设备。

注 1：人可以是系统的一部分。

注 2：本定义和 IEC 61508 中的定义有差别，从而反映出过程领域术语里的差异。

3.2.80

系统性能力　systematic capability

当设备根据安全手册规定的说明进行应用时，设备的系统性安全完整性达到规定 SIL 要求的置信度的度量（表示为 SC 1 到 SC 4），其与特定的安全功能有关。

注 1：系统性能力参照 GB/T 20438.2—2017 和 GB/T 20438.3—2017 中系统性故障的避免和控制要求确定。

注 2：系统性失效机制取决于设备的特性。对于只由硬件组成的设备，只考虑硬件失效机制。对于由硬件和软件组成的设备，则需要考虑硬件和软件失效机制间的相互影响。

注 3：某设备 SC N 的系统性能力是指当设备按照安全手册规定的 SC N 要求应用时，此设备达到了 SC N 的系统性安全完整性。

3.2.81

系统性失效　systematic failure

与已有故障有关的失效，这种失效会在特定条件下发生，只有对设计、制造过程、操作规程、文档或其他相关因素进行修改以去除故障，才能消除这种失效。

注 1：软件的系统性失效的起因也被称为 Bug。

注 2：仅凭矫正性维护而不做修改通常不能消除涉及特定条件下的失效的原因。

注 3：系统性失效可在完全相同条件的应用下重复产生，虽然不是所有重复失效都是系统性的。

注 4：导致系统性失效的故障实例包括发生于下列各项的人为错误：

- 安全要求规范；
- 硬件的设计、制造、安装和运维；
- 软件（包括应用程序）的设计或实现。

注 5：以相同方式设计、安装、操作、实施或维护的相似设备可能包含相同的故障。因此，在特定条件发生时，它们就是共因失效。

3.2.82

系统性安全完整性　systematic safety integrity

在失效的危险模式中与系统性失效有关的 SIS 的安全完整性的一部分。

注 1：系统性安全完整性通常无法量化（不同于硬件安全完整性）。

注 2：另见 3.2.26。

3.2.83

目标失效量　target failure measure

SIF 要求的性能，既可规定为在要求运行模式下要求时执行 SIF 的平均失效概率，也可规定为在连续运行模式时执行 SIF 的危险失效平均频率。

注：表 4 和表 5 给出了 SIL 和目标失效量之间的关系。

3.2.84

可容忍风险　tolerable risk

根据社会的当前水平，在给定范围内能够接受的风险。

注：见 IEC 61511-3:2016 中附录 A。

[来源：ISO/IEC Guide 51:2014，3.15]

3.2.85

未检测到的　undetected

未揭露出的　unrevealed

隐藏的　covert

没有检测到的或没有揭露出的或未显露的。

注：在 IEC 61511 中，除非上下文有其他意思，术语“未检测到的危险失效/故障”与未被诊断测试检测到的危险失效/故障有关。

3.2.86

确认　validation

通过检查和提供客观证据，证实用于某个规定用途的特定要求得到了满足。

注：在 IEC 61511 系列中这是指证明安装后的 SIF 和 SIS 在各方面满足 SRS。

3.2.87

验证　verification

通过检查和客观证据证实要求已满足。

注 1：在 IEC 61511 中，这是指在相关 SIS 安全生命周期的每个阶段，通过分析和/或测试，证明对于特定的输入，输出在各方面满足为该特定阶段所设置的目标和要求的活动。

注 2：验证活动的例子包括：

- 为确保符合某阶段的目标和要求，考虑该阶段的特定输入，对输出（来自安全生命周期所有阶段的文档）进行审查；
- 设计审查；
- 对设计的产品进行测试，以确保它们按规范工作；
- 在系统各个部分分步组装到一起后进行集成测试，并进行环境性能试验以确保所有部分能按规定方式一起工作。

3.2.88

看门狗　watchdog

用来监视可编程电子设备正确运行，并能在检测到不正确运行时采取动作的诊断设备和输出设备（典型如开关）的组合。

注 1：通过由软件控制的输出设备对外部设备（如硬件电子看门狗定时器）定期复位，看门狗可证实软件系统正确运行。

注 2：当检测到危险失效时，为使过程进入某个安全状态，看门狗可用于断开一组安全输出。看门狗用于提高 PE 逻辑解算器的在线诊断覆盖率（见 3.2.13 和 3.2.15）。

3.3　缩略语

IEC 61511 中使用的缩略语如表 1 所示。还包括了过程领域功能安全相关的一些通用缩略语。

表 1　IEC 61511 中使用的缩略语

缩略语	全称	解释
AC/DC	Alternating current/direct current	交流/直流
AIChE	American institute of chemical engineers	美国化工工程研究所
ALARP	As low as reasonably practicable	最低合理可行
ANSI	American National Standards Institute	美国国家标准研究所
AP	Aplication program	应用程序
BPCS	Basic process control system	基本过程控制系统
CCPS	Centre for chemical process safety	化工过程安全中心
DC	Diagnostic coverage	诊断覆盖率
E/E/PE	Electrical/electronic/programmable electronic	电气/电子/可编程电子
EMC	Electro-magnetic compatibility	电磁兼容
FAT	Factory acceptance testing	工厂验收测试
FPL	Fixed program language	固定程序语言
FSA	Functional safety assessment	功能安全评估
FSMS	Functional safety management system	功能安全管理体系
FTA	Fault tree analysis	故障树分析
FVL	Full variability language	全可变语言
HFT	Hardware fault tolerance	硬件故障裕度
H&RA	Hazard & risk assessment	危险和风险评估
HMI	Human Machine Interface	人机界面
IEC	International Electrotechnical Commission	国际电工委员会
IEV	International Electrotechnical Vocabulary	国际电工词汇
ISA	International Society of Automation	国际自动化协会
ISO	International Organization for Standardization	国际标准化组织
LVL	Limited variability language	有限可变语言
MooN	“M” out of “N” channel architecture	“N”取“M”通道架构
MPRT	Maximum permitted repair time	最大允许维修时间
MRT	Mean repair time	平均维修时间
MTTR	Mean time to restoration	平均恢复时间
NFPA	National Fire Protection Agency (US)	美国消防协会
NP	Non-programmable	非可编程
OEM	Original Equipment Manufacturer	原始设备制造商
PE	Programmable electronics	可编程电子
PES	Programmable electronic system	可编程电子系统
PFD	Probability of dangerous failure on demand	要求时危险失效概率

表 1　IEC 61511 中使用的缩略语（续）

缩略语	全称	解释
PFD_{avg}	Average probability of dangerous failure on demand	要求时危险失效平均概率
PFH	Probability (average frequency of dangerous failures) of failure per hour	每小时的失效概率(危险失效平均频率)
pl	Plural	复数形式
PLC	Programmable logic controller	可编程逻辑控制器
SAT	Site acceptance test	现场验收测试
SC	Systematic capability	系统性能力
SIF	Safety instrumented function	安全仪表功能
SIL	Safety integrity level	安全完整性等级
SIS	Safety instrumented system	安全仪表系统
SRS	Safety requirement specification	安全要求规范

4　与本文件的符合性

为符合本文件，应满足第 5 章～第 19 章中列出的各项要求。

5　功能安全管理

5.1　目的

第 5 章要求的目的是确定为确保实现功能安全目的而必需开展的管理活动。

注：本章的目的在于达到和保持 SIS 的功能安全，不同于为达到工作场所安全所需的通用健康和安全措施。

5.2　要求

5.2.1　概述

应确定达到功能安全的政策和策略以及实现它们的评价方法，并应在组织范围内进行交流。

5.2.2　组织和资源

5.2.2.1　应确定负责执行和审查每个 SIS 安全生命周期阶段的人员、部门、组织或其他单位，并告知它们应承担的职责。

5.2.2.2　参与 SIS 安全生命周期活动的人员、部门或组织应能胜任执行他们所负责的活动。当考虑 SIS 安全生命周期活动中涉及的人员、部门、组织或其他单位的胜任能力时，应处理和文档化以下各项：

a)　过程应用相关的工程知识、培训和经验；

b)　所使用应用技术相关的工程知识、培训和经验(如电气、电子或可编程电子)；

c)　所使用传感器和最终元件相关的工程知识、培训和经验；

d)　安全工程知识(如过程安全分析)；

e)　功能安全要求相关的法律法规知识；

f)　与他们在 SIS 安全生命周期中角色相称的管理和领导技能；

g) 对事件潜在后果的理解；
h) SIF 的 SIL；
i) 应用和技术的新颖性和复杂性。

5.2.2.3 应制定规程以管理所有参与 SIS 生命周期的人员的能力。应定期进行评估，以记录人员能力与其执行的活动是否匹配，以及人员在某一角色内的表现情况。

5.2.3 风险评价和风险管理

应按照第 8 章识别危险、评价风险和确定必要的风险降低。

注：出于经济原因，还可以考虑潜在的经济损失。

5.2.4 编制安全计划

应编制安全计划以确定要求执行的活动以及负责执行这些活动的人员、部门、组织或其他单位。在整个 SIS 安全生命周期当中，安全计划（见第 6 章）应按需更新，编制安全计划的详细程度应与个人或组织在 SIS 安全生命周期中所扮演的角色相称。

注：安全计划可包括在：

——质量计划中“SIS 安全生命周期计划”章节；或
——名为“SIS 安全生命周期计划”的单独文档；或
——包含公司规程或工作实践的若干文件。

5.2.5 执行和监视

5.2.5.1 应执行规程以确保及时跟踪 SIS 有关的建议得到满意解决，这些建议来源于：

a) 危险分析和风险评估；
b) 质量保证活动；
c) 验证活动；
d) 确认活动；
e) 功能安全评估；
f) 功能安全审核；
g) 事件后的和事故后的活动。

5.2.5.2 任何给全权负责 SIS 安全生命周期一个或几个阶段的组织提供产品或服务的供应商，应按该组织的规定提供产品或服务，并应拥有质量管理系统。应制定规程以证明质量管理体系的充分性。

如果一个供应商为产品或服务做了任何的功能安全声明，这个声明被组织用来证明对 IEC 61511 的符合性，这个供应商应有功能安全管理体系。为了建立恰当的功能安全管理体系，规程应设置到位。

功能安全管理体系应满足 GB/T 20438.1—2017 中第 6 章的要求，或功能安全声明符合的 IEC 61508衍生标准的功能安全管理要求。

5.2.5.3 应制定规程，根据 SIS 的安全要求评价 SIS 的性能，以：

——识别和预防可能危及安全的系统性失效；
——监测和评估 SIS 的失效率参数是否符合设计中的假定值；
——定义失效率大于设计中的假定值时所必要的校正动作；
——对比实际运行中 SIF 的要求率与风险评估中在确定 SIL 要求时所做的假设。

5.2.5.4 对于根据本文件发布前的规范、标准或实践设计和实施的 SIS，用户应确定设备的设计、维护、检查、测试和操作是以安全的方式进行。

5.2.6 评估、审核和修改

5.2.6.1 功能安全评估

5.2.6.1.1 应为功能安全评估制定规程并严格执行，以对 SIS 的各 SIF 实现的功能安全及安全完整性

做出评判。该规程应要求任命一个评估小组，包括特定应用所需的技术、应用和操作专家。

5.2.6.1.2 评估小组应至少包括一位与项目设计团队(阶段1，阶段2和阶段3)无关或不参与SIS运行和维护(阶段4和阶段5)的具有高级资质的人员。

5.2.6.1.3 在编制功能安全评估计划时，应考虑：

a) 功能安全评估的范围；
b) 参加功能安全评估的人员；
c) 功能安全评估小组的技能、职责和权限；
d) 功能安全评估活动所产生的信息；
e) 参与评估的其他安全机构；
f) 完成功能安全评估活动所需的资源；
g) 评估小组的独立水平；
h) 修改后，重新确认功能安全评估所使用的方法。

注：当评估组很大时，可考虑在组内包含多位与项目组无关的高级资质人员。

5.2.6.1.4 FSA团队应审查当前评估覆盖阶段以前的安全生命周期各阶段开展的，且未被之前FSA覆盖的工作。如果之前开展过FSA，FSA小组需考虑之前评估的结论和建议。开展FSA活动所在的SIS安全生命周期阶段应在安全计划中列出。

注1：在识别出新的危险时，或修改后，或运行期间，可增加额外的FSA活动。

注2：可考虑在以下阶段(见图7)开展FSA活动：

——阶段1：在已执行危险和风险评估、已确定要求的保护层和已制定安全要求规范之后；
——阶段2：在完成SIS设计之后；
——阶段3：在完成SIS安装、预调试和最终确认，以及制定好操作和维护规程之后；
——阶段4：在取得操作和维护经验之后；
——阶段5：在对SIS进行修改之后和停用之前。

注3：FSA活动的次数、规模和范围取决于特定的情况。其决定因素可能包括：

a) 项目规模；
b) 复杂程度；
c) SIL；
d) 项目持续时间；
e) 失效后果；
f) 设计特征的标准化程度；
g) 安全规章制度的要求；
h) 相似设计经验；
i) 考虑相关因素，例如：
- 运行时间；
- 运行时变更的数量和范围；
- 检验测试频率。

5.2.6.1.5 危险出现之前FSA小组应执行FSA并确认：

a) 已开展危险和风险评估(见8.1)；
b) 已执行或解决由危险和风险评估提出的适用于SIS的建议；
c) 项目设计变更规程已到位并已经正确执行；
d) 已解决所有功能安全评估提出的建议；
e) 根据安全要求规范设计、实施和安装SIS，已确认和解决任何差异；
f) 与SIS有关的安全、操作、维护和紧急规程都已到位；
g) SIS确认计划编制是合适的并已完成确认活动；
h) 人员培训已完成，有关SIS的相应信息已提供给维护和操作人员；
i) 实现进一步功能安全评估的计划或策略已经就位。

5.2.6.1.6 应针对SIS安全生命周期活动中使用的设计、开发和生产工具评估以证明它们不会对SIS

产生任何不利影响，或者应由验证规程确认这些工具的输出物。

注 1：对这些工具的重视程度，取决于它们对所要达到的风险水平的影响。

注 2：开发和生产工具的实例包括：仿真和建模工具、测量设备、测试设备、维护活动中使用的设备和配置管理工具。

注 3：工具的质量保证包括（但不限于）：校准标准、操作历史和缺陷列表的可追溯性。

5.2.6.1.7 应提供功能安全评估的结果以及通过该评估提出的建议。

5.2.6.1.8 在必要时，所有相关信息都应根据要求提供给功能安全评估小组。

5.2.6.1.9 如果因为修改而开展功能安全评估，则评估需考虑对拟修改工作开展影响分析，确认修改工作符合 IEC 61511 的要求。

注：SIS 修改相关的安全生命周期（包括 FSA）要求见 17.2.3。

5.2.6.1.10 在运行和维护阶段，应定期开展 FSA 以保证维护和操作的执行符合设计预期，并满足 IEC 61511中安全管理和验证的有关要求。

5.2.6.2 功能安全审核和修订

5.2.6.2.1 审核的目的是审查信息文件和记录，以确定 FSMS 是否到位、更新并遵循。一旦发现差距，就会提出改进建议。

5.2.6.2.2 所有安全生命周期活动中制定的必要规程都应接受安全审核。

5.2.6.2.3 功能安全审核应由不参与 SIS 工作的独立人员开展。应为审核制定规程并严格执行，并应符合以下要求：

——功能安全审核活动的频率；

——执行操作活动的人员、部门、组织或其他单位和执行功能安全审核活动的人员、部门、组织或其他单位之间的独立程度；

——记录和跟踪活动。

5.2.6.2.4 除非同类替换（即同等替换，元件的精确复制或已批准的替换，而不需要对已安装的 SIS 进行修改），否则为启动、文档化、审查、实施和批准 SIS 的变更所需的变更管理规程应到位。

5.2.6.2.5 变更管理规程应到位，识别出影响 SIS 要求的变更（如 BPCS 的再设计，某个区域人员配备的变更）。

5.2.7 SIS 配置管理

5.2.7.1 在任何 SIS 安全生命周期阶段，应编制 SIS 配置管理规程。

注：尤其需要规定：

——实施正式配置管理的阶段；

——用于唯一标识 SIS 或 SIS 子系统的全部组件（如设备、应用程序）的规程；

——防止未授权设备进入服务的规程。

5.2.7.2 开发和执行应用程序所使用的 SIS 软件、硬件和规程应纳入配置管理，并应保持版本控制。

注：SIS 软件包括应用程序（如逻辑解算器中的）、嵌入式软件（如传感器、逻辑解算器、最终元件中的）、工具软件（工具）。

6 安全生命周期要求

6.1 目的

本章的目的是：

——定义 SIS 安全生命周期活动的各个阶段及要求；

——定义和组织 SIS 安全生命周期内的技术活动；

——确保已有（或制定）适当的计划，以确保 SIS 满足安全要求。

注 1：图 7 示出了本文件的整体方案。此方案只是用来说明并指出从初始概念一直到停用的典型 SIS 安全生命周期活动。

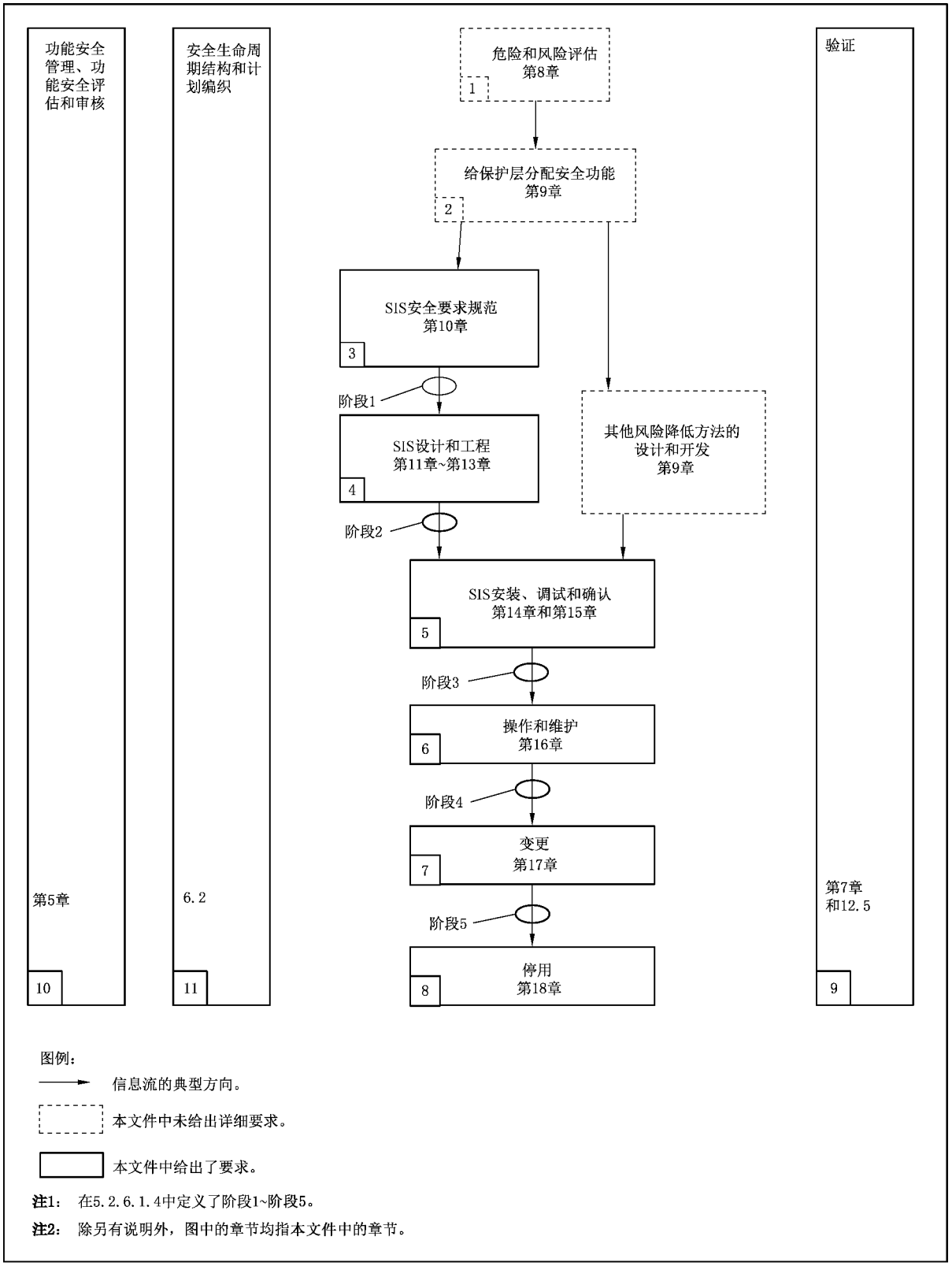


图 7　安全生命周期阶段和功能安全评估阶段

注 2：图 7 中的信息可能从运行和维护流向早期的生命周期阶段，以反映对事件和失效的追踪以及验证工程假设。

6.2 要求

6.2.1 在编制安全计划时,应定义一个结合了本文件要求的SIS安全生命周期。安全生命周期还应包括应用编程(见6.3.1)。

6.2.2 应根据它的输入、输出和验证活动来定义SIS安全生命周期的每个阶段(见表2)。

表2 SIS安全生命周期一览表

安全生命周期阶段或活动		目的	要求所在章节	输入	输出
图7方框号	标题				
1	危险和风险评估	确定过程及相关设备的危险和危险事件、导致危险事件的事件后果、与危险事件相关的过程风险、风险降低要求和要达到必要的风险降低所需要的安全功能	8	过程设计、布局、人员配备安排、安全目标	关于危险、要求的安全功能和相关风险降低的描述
2	给保护层分配安全功能	将安全功能分配到保护层,并为每个SIF分配相应的SIL	9	要求的SIF和相关安全完整性要求的描述	关于安全要求分配的描述(见第9章)
3	SIS安全要求规范	为了达到要求的功能安全,根据要求的SIF及其相应的安全完整性规定每个SIS的要求	10	关于安全要求分配的描述(见第9章)	SIS安全要求 应用程序安全要求
4	SIS设计和工程	设计SIS以满足SIF及其相应的安全完整性的要求	11,12	SIS安全要求; 应用程序安全要求	符合SIS安全要求的SIS设计 SIS集成测试计划
5	SIS安装、调试和确认	集成和测试SIS; 根据要求的SIF及其相应的安全完整性,确认SIS在各方面都满足安全要求	14,15	SIS设计 SIS集成测试计划 SIS安全要求 SIS安全确认计划	符合SIS安全要求的功能齐全的SIS SIS集成测试的结果 安装、调试和确认活动的结果
6	SIS操作和维护	确保在操作和维护期间保持SIS的功能安全	16	SIS安全要求 SIS设计 SIS操作和维护计划	操作和维护活动的结果
7	SIS变更	对SIS进行校正、增强或改造以确保达到和保持要求的SIL	17	修改后的SIS安全要求	SIS修改结果
8	停用	保证正确审查、部门组织确保SIF(继续恰当保留); 确保适当的审查,部门组织,并确保SIF适当保留	18	竣工安全要求和过程信息	停用的SIF

表 2　SIS 安全生命周期一览表（续）

安全生命周期阶段或活动		目的	要求所在章节	输入	输出
图 7 方框号	标题				
9	SIS 验证	测试和评估给定阶段的输出，以确保作为该阶段输入的产品和标准的正确性和一致性	7、12.5	每个阶段 SIS 的验证计划	每个阶段 SIS 验证的结果
10	SIS 功能安全评估	对 SIS 所达到的功能安全进行调查并做出判断	5	SIS 功能安全评估计划编制 SIS 安全要求	SIS 功能安全评估结果
11	安全生命周期结构和计划	确立如何完成生命周期各步骤	6.2	不适用	安全计划

6.2.3　应编制面向安全生命周期所有阶段的安全计划，定义活动、准则、技术、措施、规程和负责组织/人员，以：

——确保在过程的所有相关模式下都能达到 SIS 安全要求；这包括功能和安全完整性两个方面的要求；

——确保 SIS 正确安装和调试；

——确保安装后 SIF 的安全完整性；

——在运行过程中保持安全完整性（如检验测试、失效分析）；

——在 SIS 的维护活动期间管理过程危险。

6.2.4　如果在安全生命周期的任何阶段，需要进行与之前生命周期阶段有关的变更，则之前 SIS 安全生命周期阶段和随后的阶段都应再次检查，按需改变并重新验证。

6.3　应用程序 SIS 安全生命周期要求

6.3.1　应根据应用程序安全生命周期（见图 8）每个阶段的基本活动、目的、要求的输入信息和输出结果、验证要求（见表 3）来定义这些阶段。

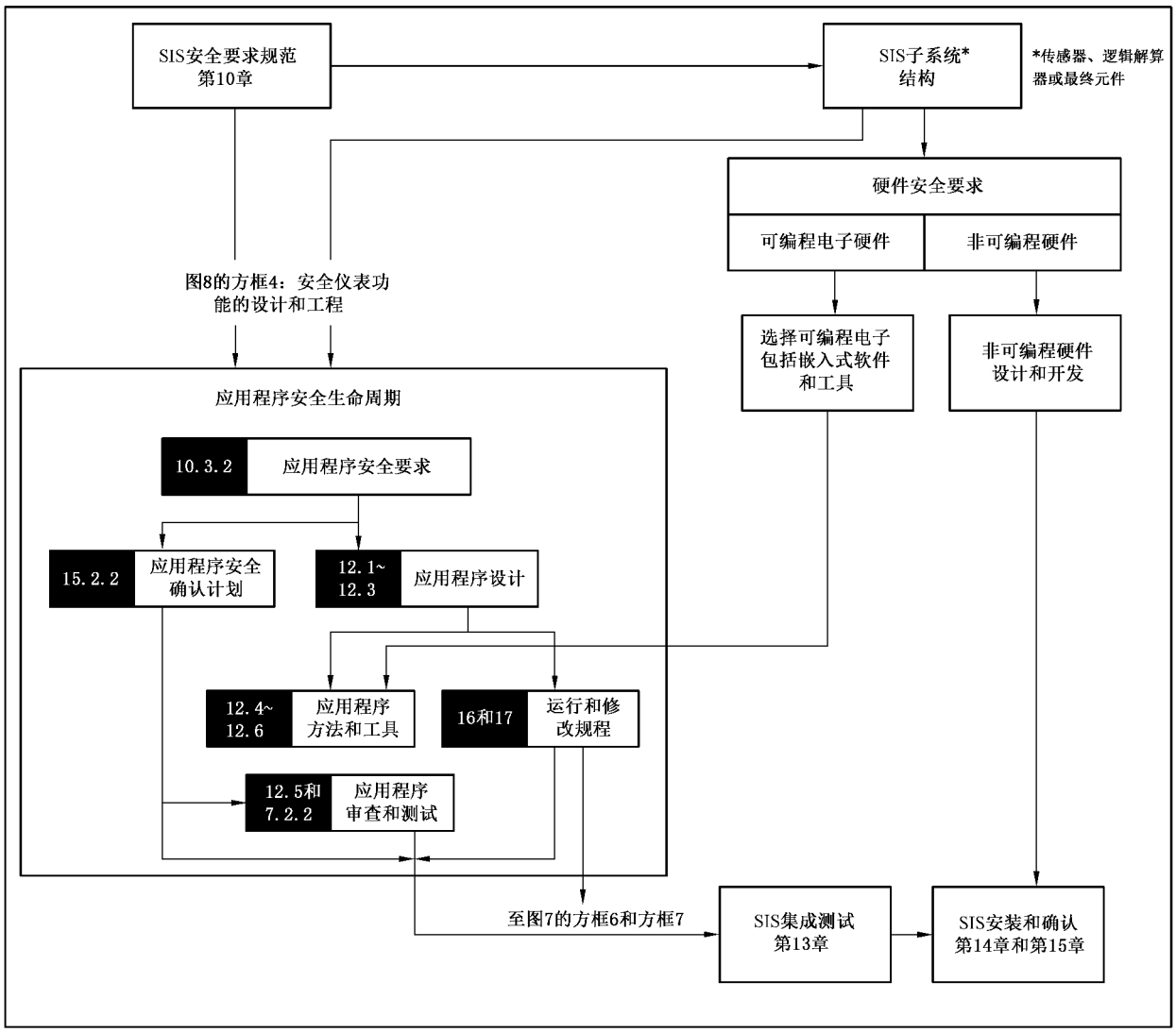


图 8　应用程序安全生命周期及其与 SIS 安全生命周期的关系

表 3　应用程序安全生命周期：一览表

安全生命周期阶段		目的	要求所在章节	输入	输出
图 8 方框号	标题				
10.3.2	应用程序安全要求	为实现要求的 SIF 所需的各 SIS 明确应用程序安全要求 明确分配给该 SIS 的各 SIF 的应用程序要求	10.3 11.5	SIS 安全要求 所选 SIS 的安全手册 SIS 结构	SIS 应用程序安全要求规范 验证信息
15.2.2	应用程序安全确认计划编制	编制确认应用程序的计划	15.2.2 15.2.5	SIS 应用程序安全要求	SIS 安全确认计划 验证信息

表 3　应用程序安全生命周期:一览表（续）

安全生命周期阶段		目的	要求所在章节	输入	输出
图 8 方框号	标题				
12.1～12.3	应用程序开发	结构 创建能满足规定的应用程序安全要求的应用程序架构 审查和评价 SIS 硬件架构对应用程序的要求 明确开发应用程序的规程	12.3 (10.3, 12.2)	SIS 应用程序安全要求 SIS 硬件架构设计的约束条件	架构设计描述,例如将应用程序分离为相关的过程子系统和 SIL,例如辩别像泵或阀序列这类通用应用程序模块 应用程序架构和子系统集成测试要求 验证信息
12.1～12.3	应用程序开发设计	进行应用程序设计 在应用程序的安全生命周期内,确定一组合适的组态、库、管理、模拟和测试工具	12.3	SIS 应用程序安全要求 架构设计描述 SIS 手册 所选的 SIS 逻辑解算器的安全手册	应用程序设计 编程过程中使用的规程 验证信息
12.4 12.6	应用程序实现	应用程序开发和应用程序模块开发 实现能满足规定的应用程序安全要求的应用程序 使用合适的支持工具和编程语言	12.4 12.3.4 12.6	设计描述 逻辑解算器手册和规程列表(配合应用程序使用)	1)应用程序(例如功能块图、梯形逻辑) 2)应用程序仿真和集成测试 3)特殊目的应用程序的安全要求 4)验证信息
12.5 7.2.2	应用程序验证	验证达到了针对应用程序安全的要求 显示所有的 SIS 应用程序可正确地相互作用,从而执行它们的预定功能而不执行非预定的功能	12.5 7.2.2	应用程序仿真和集成测试要求(基于结构的测试) 应用程序结构集成测试要求	应用程序测试结果 经验证和测试过的应用程序系统 验证信息
13	SIS 集成测试	将应用程序集成到目标逻辑解算器上,包括与现场设备和/或模拟器的交互。	13	应用程序和逻辑解算器集成测试要求	应用程序和逻辑解算器集成测试结果

6.3.2 应根据 12.6.2 的要求，为各生命周期阶段选择方法、技术和工具。

6.3.3 应对 SIS 安全生命周期的每个阶段进行验证(见第 7 章)，验证结果应按照第 19 章的描述提供。

7 验证

7.1 目的

本章目的是通过审查、分析和/或测试，来证明要求的输出能满足在验证计划编制确定的安全生命周期的适当阶段(图 7)定义的要求。

7.2 要求

7.2.1 验证计划编制应贯穿整个 SIS 安全生命周期，并应确定安全生命周期适当阶段所需的所有活动(图 7)，包括应用程序。验证计划编制应通过解决以下问题来符合 IEC 61511：

a) 验证活动；
b) 验证所使用的规程、措施和技术，包括执行和解决所产生的建议；
c) 何时进行这些活动；
d) 负责这些活动的人员、部门和组织，包括它们的独立水平；
e) 确定要验证的项目；
f) 确定验证依据的信息；
g) 输出是否足以满足该阶段的要求；
h) 数据的正确性；
i) 如何处理不符合项；
j) 工具和支持分析；
k) SIS 实施的完整性和要求的可追溯性；
l) 文件的可读性和可审核性；
m) 设计的可测试性。

7.2.2 当验证包括测试时，验证计划还应包括下列内容：

a) 应用程序和硬件以及现场设备的集成策略，包括应符合其他标准(如机械、燃烧器)的子系统的集成；
b) 测试范围(描述测试设备和包括硬件及编程设备在内要进行的测试类型)；
c) 测试用例和测试数据(具有相应数据的特定场景)；
d) 要进行的测试类型；
e) 测试环境，包括工具、硬件、所有软件和需要的配置；
f) 评估测试结果所依据的测试准则(如通过/失败准则)；
g) 针对测试失败的纠正措施的规程；
h) 地点(如工厂或现场)；
i) 与外部功能的相关性；
j) 合适的人员；
k) 变更管理；
l) 不符合项。

7.2.3 与安全功能集成在一起的非安全功能，应验证其不干扰安全功能。

7.2.4 应根据验证计划进行验证。

7.2.5 在测试时，任何修改都应进行安全影响分析，以确定所有被影响的 SIS 组件及必要的重新验证活动。

7.2.6 应提供验证过程的结果(见第 19 章),包括是否达到测试的目的和准则。

注 1:验证过程中所使用的技术、措施及独立水平的选择取决于一系列因素,包括复杂程度、设计的新颖性、技术的新颖性和要求的 SIL 等。

注 2:验证活动的例子包括设计审查、工具和技术的使用(包括软件验证工具和基于计算机的设计分析工具)。

8 过程危险和风险评估

8.1 目的

本章目的是确定:

a) 过程及其相关设备的危险和危险事件;

b) 导致危险事件的事件序列;

c) 与危险事件对应的过程风险;

d) 风险降低的要求;

e) 达到必要的风险降低所要求的安全功能;

f) 某些安全功能是否是 SIF。

注 1:第 8 章针对过程工程师、危险和风险专家、安全管理人员及仪表工程师。它的目的是识别确定 SIF 通常需要的多学科方法。

注 2:在合理可行的情况下,将过程设计成固有安全。如果做不到,就需要其他保护层(见图 9)。在一些应用中,工业标准可能会规定特殊保护层的使用。

注 3:风险降低可能通过多个保护层实现(见第 9 章)。

8.2 要求

8.2.1 对物料、过程及设备应进行危险和风险评估。其结果应是:

a) 识别出的每个危险事件及其起因的描述;

b) 危险事件可能性和后果的描述;

c) 过程操作模式考虑,如正常操作、开车、停车、维护、过程扰动、紧急停车;

d) 确定为达到要求的功能安全所需的附加风险降低;

e) 降低或消除危险和风险所采取的措施的描述或引用信息;

f) 在风险分析中对保护层的要求率和触发源的危险失效平均频率所做的假设的详细描述,以及赋予操作约束或人为干预的可信度的详细描述;

g) 识别 SIF。

注 1:在确定安全完整性要求时,需考虑产生要求的系统和被设计用来响应这些要求的保护系统之间共同原因的影响。例如,控制系统失效提出了(保护)要求,保护层中使用的设备同控制系统中使用的设备类似或相同。在这种情况下,当一个共同原因使保护系统中的类似设备变得无效时,BPCS 中设备的一次失效产生的(保护)要求可能就得不到有效地响应。因为在最初确定危险和分析风险的过程中,保护系统的设计未必就已完成,在这样早的一个阶段中还不可能辨别出共同原因问题。在这种情况下,只要完成了 SIS 和其他保护层的设计,就有必要重新考虑安全完整性要求和 SIF 要求。在确定过程和保护层整体设计是否满足要求时,需要考虑共同原因失效。

注 2:在 IEC 61511-3:2016 中展示了用于确定 SIS 所要求的 SIL 的技术的例子。

8.2.2 BPCS 危险失效作为触发源对保护层提出要求时,其危险失效平均频率不应被假设小于 $10^{-5}/h$。

8.2.3 应记录危险和风险评估,使以上各项之间的关系清楚和可追溯。

注 1:上述要求并不强制安全完整性要求一定要赋数值。也可以使用定性或半定量方法(见 IEC 61511-3:2016 中附件 C、附录 D、附录 E)。

注 2:安全完整性要求根据应用与国家法规要求的不同而有所不同。一个为多个国家所接受的原则是:采取附加的风险降低措施,直到成本投入同实现的安全完整性提高不成比例为止。

8.2.4 应开展安防风险评估以识别 SIS 的安防漏洞。评估应得出：

a) 该风险评估所覆盖的设备的描述(如 SIS、BPCS 或任何其他与 SIS 连接的识别)；

b) 识别出的威胁描述，这些威胁可能利用漏洞并造成安防事件(包括对硬件、应用程序和相关软件的蓄意攻击，以及人为错误导致的非蓄意事件)；

c) 安防事件导致的潜在后果以及这些事件发生的可能性描述；

d) 各阶段的考虑，如设计、实现、调试、运行和维护；

e) 附加风险降低要求的确定；

f) 对减少或消除威胁而采取的措施的描述或信息的引用。

注 1：SIS 安防相关导则见 ISA TR 84.00.09，ISO/IEC 27001:2013 和 IEC 62443-2-1:2010。

注 2：安防风险评估所需的边界条件信息和控制通常与设施的业主/运营公司有关，与供应商无关。这种情况下，设备的业主/运营公司有责任遵守本条款。

注 3：SIS 安防风险评估可包括在整体过程自动化安防风险评估中。

注 4：SIS 安防风险评估的范围可以从单个的 SIF 到公司内的所有 SIS。

9 给保护层分配安全功能

9.1 目的

本章目的是：

——给保护层分配安全功能；

——确定要求的 SIF；

——为各 SIF 确定相应的安全完整性要求。

注 1：在分配过程中可考虑其他行业标准或规程。

注 2：各 SIF 的完整性要求可能包括相关的风险降低、PFD、PFH 或 SIL。

9.2 分配过程要求

9.2.1 分配过程应导出以下结果：

——给用来实现必要风险降低的特定保护层分配安全功能；

——给 SIF 分配风险降低或危险失效平均频率。

注：法规要求或其他行业规范可能影响分配过程。

9.2.2 通过考虑 SIF 提供的 PFD 或 PFH 要求，可推导出该功能要求的 SIL。

注：进一步指南见 IEC 61511-3:2016。

9.2.3 在要求模式下运行的每个 SIF 所需要的 SIL，应根据表 4 或表 5 来确定。

9.2.4 在连续模式下运行的每个 SIF 所需要的 SIL，应根据表 5 来确定。

表 4 安全完整性要求：PFD_{avg}

要求运行模式		
安全完整性等级(SIL)	PFD_{avg}	要求的风险降低
4	10^{-5}～$<10^{-4}$	>10 000～100 000
3	10^{-4}～$<10^{-3}$	>1 000～10 000
2	10^{-3}～$<10^{-2}$	>100～1000
1	10^{-2}～$<10^{-1}$	>10～100

表 5　安全完整性等级:SIF 的危险失效平均频率

连续运行模式或要求运行模式	
安全完整性等级(SIL)	危险失效平均频率(每小时失效)
4	10^{-9}～<10^{-8}
3	10^{-8}～<10^{-7}
2	10^{-7}～<10^{-6}
1	10^{-6}～<10^{-5}

注 1:运行模式的进一步解释见 3.1.39。

注 2:用数值定义 SIL 是为了为不同设计和解决方案的对比提供一个客观的度量。然而,人们认识到,在当前的知识水平下,失效的许多系统性原因还只能进行定性评估。

注 3:对于连续模式或要求模式下的一个 SIF 所要求的危险失效平均频率,是通过把在连续模式或要求模式下操作的 SIF 失效所产生的风险,连同在考虑到其他保护层的贡献时导致同一风险的其他设备的失效率一并考虑来确定的。

9.2.5　当分配过程出现对单个或多个 SIS 或 SIS 与 BPCS 保护层的协同风险降低要求>10 000 或危险失效平均频率<10^{-8}/h 时,应重新考虑该应用(如过程或其他保护层)以确定是否可通过修改某些风险参数来避免出现风险降低要求>10 000 或危险失效平均评频率<10^{-8}/h。审查需考虑是否:

——可修改过程或容器/管道以从源头消除或降低危险;

——可采用额外的非仪表安全相关系统或其他风险降低措施;

——可降低后果严重性,如减少危险物料的数量;

——可降低特定后果的可能性,如降低危险事件触发源的可能性。

注:尽量避免要求通过单个 SIF 实现风险降低>10 000 或危险失效平均频率<10^{-8}/h 的应用,因为很难在 SIS 安全生命周期中达到和保持如此高水平的性能。当要求某个 SIF 实现风险降低>10 000 或危险失效平均频率<10^{-8}/h时,所有工厂验收测试、验证测试、验证和确认活动均要求高水平的能力和覆盖率。

9.2.6　如果进一步考虑后证实仍需某个风险较低要求>10 000 或危险失效平均频率<10^{-8}/h 时,则应考虑使用多个较低风险降低要求的保护层(如 SIS 或 BPCS)来实现该安全完整性要求。如果该风险降低被分配到多个保护层,则这些保护层应彼此独立,不独立时应进行评估以表明其影响与风险降低要求相比足够低,评估时需考虑下列因素。

——SIS 共因失效和要求的原因。

注 1:当失效会导致一个要求时,共因的范围可以通过考虑设备的多样性来评估,要考虑的设备包括失效会导致一个要求的所有设备以及 BPCS 保护层和/或用来降低风险的 SIS 的所有设备。

注 2:SIS 和要求原因共因的一个例子就是,传感器故障或失效引起过程失控会导致一个要求,并且控制用的传感器和 SIS 用的传感器是相同类型。

——与提供风险降低的其他保护层间的共因失效。

注 3:共因的程度可以通过考虑 BPCS 保护层和/或用于实现风险降低要求的 SIS 的所有设备的多样性来评估。

注 4:提供风险降低的 SIS 间共因的一个例子就是,如果不同测量设备和逻辑解算器的两个分开独立的 SIS 来提供风险降低,但是最终执行设备是两个同类型的截断阀或共用单个截断阀。

——共用操作、维护、检查或测试活动或共用检验测试规程和检验测试时间可能引入的所有相关性。

注 5:即使保护层不同,同时开展检验测试也会减弱整体风险降低,这可能是妨碍针对危险事件的必要风险降低的一个重要因素。

注 6：当需要高等级的风险降低，并且根据注 5 检验测试没有同时开展，即使使用多个独立保护层来降低风险，主导因素通常仍是共因失效。针对为同一危险事件提供风险降低的保护层内和保护层间的相关性开展评估并证明其足够低。

9.2.7 如果要实现＞10 000 或危险失效平均频率＜10^{-8}/h 的风险降低要求，无论是分配给单独的 SIS 或多个 SIS 或 SIS 与 BPCS 协同的保护层，应使用定量方法来开展进一步的风险评估以确认达到了安全完整性要求。方法需考虑 SIS 与下述设备的相关性和共因失效：

——任何其他保护层，其失效将对它提出要求；

——降低危险事件可能性的其他 SIS；

——降低危险事件可能性的其他风险降低方法（如安全报警）。

9.2.8 如果某个危险事件所需的风险降低被分配给单个 SIS 中的多个 SIF，则该 SIS 应满足总体风险降低要求。

9.2.9 应记录分配过程的结果，从而用过程的功能性需求和安全完整性要求来描述分配给 SIS 的安全功能，如要采取的行动、设定点、响应时间、延迟、故障处理、阀门密闭要求。

注：描述需有清晰的逻辑格式，并且可作为过程要求规范或安全描述引用。描述应明晰分配过程的目的和使用的方法。过程要求规范是 SRS（见第 10 章）输入信息，需足够详细以确保对 SIS 及其设备有足够的要求，例如，描述包括传感器设定点、可用于响应的过程安全时间以及阀门密闭要求。

9.3 基本过程控制系统作为保护层的要求

9.3.1 如图 9 所示，基本过程控制系统可能被声明为保护层。

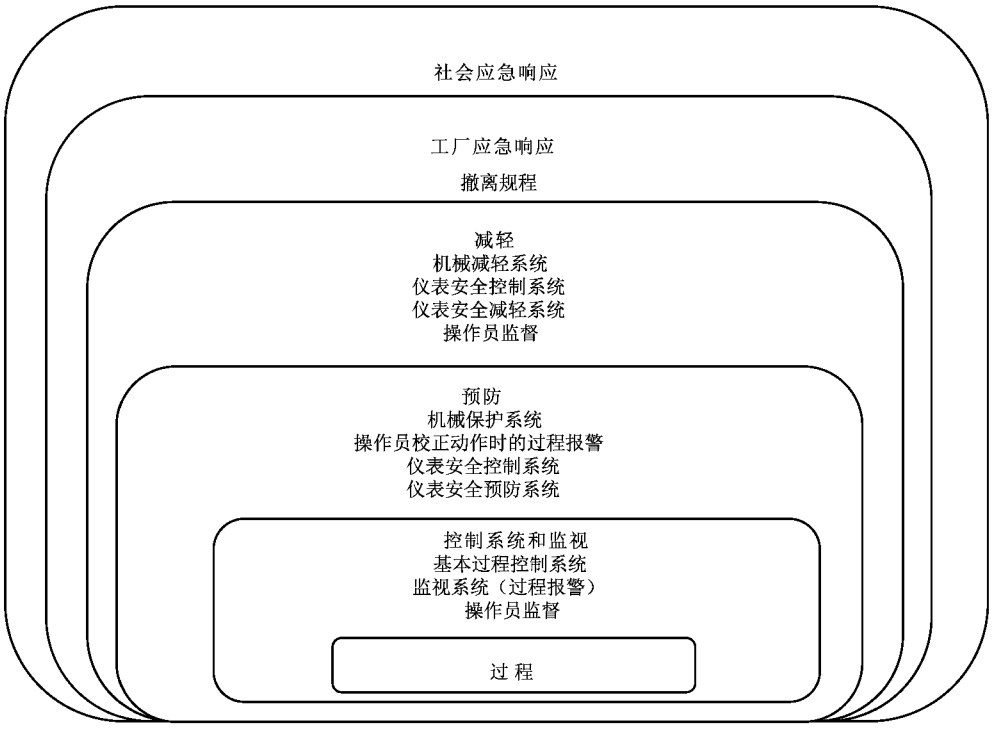


图 9 典型保护层和风险降低方法

9.3.2 BPCS 保护层声明的风险降低应≤10。

注：可考虑到这样一个事实，即 BPCS 可以是对保护层提出要求的触发源。

9.3.3 如果 BPCS 声明风险降低大于 10，则应按 IEC 61511 中的要求对 BPCS 进行设计和管理。

9.3.4 如果 BPCS 不准备符合 IEC 61511，则：

——导致危险事件的同一事件链中，当 BPCS 是对保护层提出要求的触发源时，声明的 BPCS 保护层不能多于一个；或

——导致危险事件的同一事件链中，当 BPCS 不是要求的触发源时，声明的 BPCS 保护层不能多于两个。

注：识别出的 BPCS 保护层可能由一个作为触发源的 BPCS 和第二个独立的 BPCS 保护层（见 9.3.2 和 9.3.3）或两个独立的 BPCS 保护层（当触发源与 BPCS 失效无关时）构成。

9.3.5 当 9.3.4 适用时，每个 BPCS 保护层应独立并且与触发源彼此分离，直至每个 BPCS 保护层声明足够的风险降低。

注 1：对分离和独立性评估可考虑实现风险降低的必要因素，如中央处理单元（CPU）、输入/输出模块、继电器、现场设备、应用编程、网络、数据库、工程工具、人机界面、旁路工具和其他设备。

注 2：热备控制器不被认为独立于主控制器，因为它会存在共因失效（例如，热备控制器有与主控制器和备用控制器相同的组件，例如，背板、固件、诊断、传输机制以及未检测到的危险失效）。

9.4 防止共因、共模和相关失效的要求

9.4.1 应对保护层的设计进行评估，以确保保护层之间、保护层同 BPCS 之间共因失效、共模失效和相关失效的可能性，同保护层的整体安全完整性要求相比足够低。这种评估可以是定性的也可以是定量的。除非 9.2.7 适用。

注：相关失效的定义见 3.2.12。

9.4.2 评估应考虑下列因素：

——保护层之间的独立性；

——保护层之间的多样性；

——不同保护层之间的物理分离；

——保护层之间、保护层同 BPCS 之间的共因失效。

注 1：解决过程的共因。泄放阀堵塞可能会产生与 SIS 传感器堵塞相同的问题。

注 2：实现独立和物理分离。人机界面、SIS/BPCS 网络或旁路可能会导致共因失效。

10 SIS 安全要求规范（SRS）

10.1 目的

本章目的是规定 SIS 的要求，包括应用程序和 SIS 架构。

10.2 一般要求

安全要求应从 SIF 分配和在危险及风险评估中确定的那些要求中推导出来。SIS 要求应以下述方法表达和构建：

——清楚、精确、可验证、可维护和切实可行；

——易于安全生命周期任何阶段有可能使用这些信息的人理解和解释。

10.3 SIS 安全要求

10.3.1 阐述制定 SIS 安全要求时需考虑的问题。

10.3.2 这些要求对设计 SIS 而言应是足够的，并且在编写 SIS 安全要求过程中应适当包括目的和应用方法的描述。

a) 达到要求的功能安全所必需的所有 SIF 的描述（如因果图、逻辑叙述）。

b) SIF 相关的现场输入和输出设备清单，它通过现场设备标识的方法清晰列出（如现场位号一览表）。

c) 识别和考虑共因失效的要求。

d) 每个 SIF 的过程安全状态的定义，例如，达到一个稳定的状态，并已避免或充分减轻特定的危险事件。

e) 若多个安全状态同时发生会产生一个单独的危险（如应急储存的过载、火炬系统的多次泄压），其中的每个安全状态要单独定义。

f) 每个 SIF 的假定触发源及要求频率。

g) 检验测试间隔相关要求。

h) 执行检验测试的相关要求。

i) 每个 SIF 在过程安全时间内，使过程进入安全状态的响应时间要求。

注：关于过程安全时间的进一步讨论见 IEC 61511-2:2016。

j) 每个 SIF 要求的 SIL 和运行模式（要求/连续）。

k) SIS 过程测量、范围、精度和它们跳闸点的描述。

l) SIF 过程输出动作和成功操作准则的描述，例如，阀门泄漏率。

m) 过程输入和输出之间的功能关系，包括每个 SIF 的逻辑、数学函数和任何要求的许可。

n) 每个 SIF 的手动停车要求。

o) 与得电或失电跳闸有关的要求。

p) 在停车后每个 SIF 的复位要求（如跳闸后的手动要求、半自动或全自动最终元件的复位要求）。

q) 每个 SIF 的最大允许误停车率。

r) 每个 SIF 的失效模式和要求的 SIS 响应（如报警、自动停车）。

s) 与启动和重新启动 SIS 规程有关的任何特殊要求。

t) SIS 和其他系统（包括 BPCS 和操作员）之间的所有接口。

u) 工厂操作模式的描述，以及每种操作模式下 SIF 要求的识别。

v) 10.3.3 中列出的应用程序安全要求。

w) 旁路要求，包括旁路状态时应用的书面规程，规程描述了如何管理控制旁路以及随后如何消除旁路。

x) 在检测到 SIS 中的故障事件时，达到和保持某个安全状态所必需的任何动作的规范。应考虑所有相关人员因素。

y) 在考虑到运输时间、地点、备件安装、服务合同、环境约束时，SIS 切实可行的平均维修时间。

z) 需要避免的 SIS 输出状态的危险组合的识别。

aa) 应识别 SIS 在运输、存储、安装及运行中可能遇到的所有极端环境条件。需考虑的有：温度、湿度、污染、接地、电磁干扰/射频干扰（EMI/RFI）、冲击/振动、静电放电、用电等级、水淹、雷电和其他有关因素。

bb) 应为整个工厂（如工厂开车）或单个设备的操作程序（如设备维护、传感器校准和/或修理）识别出正常和异常操作模式。可能需要额外设置 SIF 以支持这些操作模式。

cc) 必要时应为 SIF 定义承受一次重大意外事故的要求，例如，在一次火灾事故中阀门保持可操作性的时间要求。

10.3.3 应用程序安全要求应从 SRS 和 SIS 的架构（布局和内部结构）中推导。应用程序安全要求可以是 SRS 中的一部分，也可以是一个独立文档（如应用程序要求规范）。每个 SIS 子系统的应用程序安全要求输入信息应包括：

a) 每个 SIF 的详细安全要求，包括传感器表决等；
b) SIS 架构和安全手册提出的要求，如硬件和嵌入式软件的限制和约束；
c) 来自 5.2.4 的安全计划的要求。

10.3.4 应为实现要求的 SIF 所需的每个可编程 SIS 设备规定应用程序安全要求，应遵循 SIS 架构。

10.3.5 应用程序 SRS 应足够详细，以使设计和实施达到要求的功能安全，并能支撑开展功能安全评估。需考虑以下事项：

a) 该应用程序所支持的 SIF 及其 SIL；
b) 实时性能参数，如 CPU 容量、网络带宽、有故障时可接受的实时性能以及一个特定时间段内接收到的所有跳闸信号；
c) 程序次序和延时(如适用)；
d) 设备和操作员接口及其可操作性；
e) SRS 中规定的所有相关的过程操作模式；
f) 针对异常过程变量(如传感器值超量程、变化幅度过大、死值、检测到开路/短路)采取的动作；
g) 应用程序中执行的外部设备(如传感器和最终元件)进行检验测试和自动诊断测试的功能；
h) 应用程序自监测(例如，应用驱动的看门狗和数据范围确认)；
i) 对 SIS 中的其他设备(如传感器和最终元件)的监测；
j) 过程运行时定期测试 SIF 的相关要求；
k) 输入文档的参照(如 SIF 规范、SIS 配置和架构、SIS 硬件安全完整性要求)；
l) 通信接口的要求，包括限制它们使用的措施、数据确认以及接收和传输命令；
m) 应识别和避免由应用程序产生的过程危险状态(如同时关闭两个隔离气阀可能导致压力波动，从而导致危险状态)；
n) 应定义每个 SIF 过程变量的确认准则。

10.3.6 应通过以下方式表达和构建应用程序安全要求：

a) 描述支持应用程序安全要求的意图和方法；
b) 对 SIS 安全生命周期任何阶段将使用该文档的人员来说是清晰和易于理解的；这包括所有用户在使用术语和描述时不会有歧义并且能理解(如工厂操作人员、维护人员和应用编程人员)；
c) 可验证、可测试和可修改；
d) 可通过所有交付物追溯，包括详细设计文档、SRS 以及识别所需的 SIF 和 SIL 的过程危险分析。

11 SIS 设计和工程

11.1 目的

本章目的是设计一个或多个 SIS，以提供 SIF，并满足规定的完整性要求(如 SIL、相关风险降低、PFD 和/或 PFH)。

11.2 一般要求

11.2.1 应根据 SIS 安全要求规范，并考虑本章的所有要求来设计 SIS。

11.2.2 当 SIS 既执行 SIF 又执行非 SIF 时，在正常和故障条件下，对任何 SIF 有负面影响的所有硬件、嵌入式软件和应用程序均应被当成 SIS 的组成部分，并符合其可能影响的 SIF 中最高的 SIL 要求。

11.2.3 在 SIS 实现不同 SIL 的 SIF 时，共享或共用硬件、嵌入式软件和应用程序应符合最高 SIL。

注：如果能证明较低 SIL 的 SIF 对较高 SIL 的 SIF 没有负面影响，则不同 SIL 的嵌入式软件或应用程序可以在同一设备中共存。

11.2.4 如果不准备让 BPCS 符合 IEC 61511，SIS 应单独设计，并与 BPCS 分开，从而不影响 SIS 的安全完整性。

注 1：可交换操作信息但不能危及 SIS 的功能安全。

注 2：当证实 BPCS 的失效不会危害 SIS 的 SIF 时，SIS 的设备也可用于 BPCS 的功能。

11.2.5 应在 SIS 设计中给出可操作性、可维护性、诊断、检查和可测试性的要求，降低危险失效可能性。

11.2.6 SIS 设计应考虑人员的能力和局限性，并与分配给操作员和维护人员的任务相适应。操作员接口的设计应符合人员操作习惯并与操作员可能接受到的培训水平相适应。

注：例如，如果操作时要求经常进行限值数据输入或其他操作员输入，那么需要进行人因分析。

11.2.7 SIS 应被设计成一旦其将过程置于某个安全状态，除非 SRS 另有规定，过程应保持在该安全状态直至 SIS 被复位。

11.2.8 应设置与逻辑解算器无关的手动机制（如紧急停车按钮）来启动 SIS 最终元件，除非 SRS 另有规定。

11.2.9 SIS 设计应全面考虑 SIS 和 BPCS 之间，以及 SIS 和其他保护层之间的独立性和相关性。

11.2.10 一个设备用于 BPCS 时，不应同时用于 SIS，因为这个设备失效导致引发对 SIF 的要求和该 SIF 的危险失效。除非分析后可以确认整体风险是可接受的。

注：当 SIS 的一部分用于控制并且共用设备的一次危险失效可能引起对 SIS 所执行的功能提出一次要求时，则会引入新的风险。附加的风险与共用设备的危险失效率有关，这是因为当共用设备发生故障时，立即就会产生一个要求，而 SIS 对此要求无力做出响应。因此在这些情况下需要进行额外的分析以保证共用设备的危险失效率足够低。以传感器和阀门为例，经常需要考虑与 BPCS 的共用情况。

11.2.11 对动力源（如电源、空气、液动源或气动源）中断而不进入安全状态的所有 SIS 设备，应能对共用动力源丢失和 SIS 电路完整性进行检测和报警（如线路终端监视、供压测量、液压或气压检测）并根据 11.3 采取行动。

注 1：可通过使用辅助动力源（如备用电池、不间断电源、储气罐、液压蓄能器、第二气源）来提高动力源完整性。

注 2：动力源中断可能影响多个 SIF，甚至多个 SIS。因此需考虑多个 SIF 的共因失效。

11.2.12 SIS 的设计应针对识别出的安防风险提供必要的防护能力（见 8.2.4）。

注：SIS 安防相关导则见 ISA TR 84.00.09，ISO/IEC 27001:2013 和 IEC 62443-2-1:2010。

11.2.13 应提供安全手册，手册内容应涵盖在设备的预期配置和预期运行环境下，SIS 相关的运行、维护、故障检测和约束。

11.2.14 所有用于 SIF 的通信应使用适用于安全应用的技术，以满足要求的 SIL。

11.3 检测到故障时的系统行为要求

11.3.1 在 SIS 中检测（通过诊断测试、检验测试或其他方式）到一个危险故障时，应采取补偿措施来维持安全运行。如果不能维持安全运行，则应采取规定的动作来达到或保持过程的安全状态。如果补偿措施依赖于操作员执行规定动作来响应某个报警（如打开或关闭阀门），该报警则应作为 SIS 的组成部分。

注 1：可以在 SRS 中规定达到或保持过程的安全状态所需的特定动作（故障响应）（见 10.3.1）。它可以是过程的安全停车，也可以是依赖于该故障 SIS 降低风险过程的一部分。

注 2：维持安全运行所需的补偿措施取决于安全完整性要求、危险事件对应的可容忍风险、SIS 硬件故障裕度、预期的平均维修时间以及其他保护层的可用性。在某些情况下，只要采取动作确保在 PFD_{avg} 计算时假设的 MPRT 时间内完成危险失效的维修即可；但在其他情况下，可能需要提供其他措施来补偿缺失的风险降低直

至 SIS 完全恢复。还可参见 16.2.3。

11.3.2 当 SIS 的某个危险故障是通过某个报警来获得操作员注意时，应对该报警进行适当的检验测试和变更管理。

11.4 硬件故障裕度

11.4.1 对每个 SIF 而言，执行它的 SIS 应具有最低的 HFT。

注：这不排除在发生故障后系统运行期间的某一时刻 HFT 可能降低到最小要求以下的可能性。

11.4.2 当 SIS 可被分解成独立的 SIS 子系统（如传感器、逻辑解算器及最终元件）时，则 HFT 可在 SIS 子系统层级指定。

11.4.3 SIS 或 SIS 子系统的 HFT 应符合：

——11.4.5～11.4.9；

——GB/T 20438.2—2017 中 7.4.4.2（路线 1H）；

——GB/T 20438.2—2017 中 7.4.4.3（路线 2H）。

注：IEC 61511 中建立的路线源自 GB/T 20438.2—2017 中的路线 2H。

11.4.4 确定实现的 HFT 时，如果某些故障发生的可能性相较于安全完整性要求来说非常低，那么可以排除这些故障。这样的故障排除都应进行论证和记录。

注：关于故障排除的进一步信息可参见 ISO 13849-1:2006 和 ISO 13849-2:2012。

11.4.5 执行某个具有特定 SIL 的 SIF 的 SIS（或 SIS 子系统）的最小 HFT 应符合表 6，以及 11.4.6 和 11.4.7（如果适用）。

注：表 6 中的 HFT 要求表示最小的系统或 SIS 子系统冗余度。取决于具体应用、设备失效率和检验测试间隔，根据 11.9 要求，可能需要额外的冗余来满足 SIF 的 SIL 对应的失效量。

表 6 不同 SIL 对应的最小 HFT 要求

SIL	要求的最小 HFT
1（任何模式）	0
2（低要求模式）	0
2（高要求/连续模式）	1
3（任何模式）	1
4（任何模式）	2

11.4.6 对于未使用 FVL 或 LVL 可编程设备的 SIS 或 SIS 子系统，若表 6 规定的最小 HFT 导致额外故障并导致整体过程安全降级，则 HFT 可以减小。这种情况应开展论证并形成文档。论证时应有证据证明计划的架构符合预期目的并且满足安全完整性要求。

注：故障裕度是实现要求置信度（实现健壮的架构）的首选解决方案。当应用本条时，论证的目的是证明提议的替代架构提供了等效的或更好的解决方案。这可能取决于应用和/或使用的技术；如备用设置（例如，解析冗余，用其他传感器输出量的物理计算结果代替某个失效的传感器输出量）；使用同类技术的更可靠产品（如果有）；改用更可靠的技术；通过使用多样性技术减小共因失效的影响；提高设计余量；限制环境条件（例如，针对电子组件）；通过收集更多的现场反馈或专家判断减小可靠度的不确定性。

11.4.7 应用 11.4.6 时，如果得出某个故障裕度等于 0 的结果，11.4.6 中要求的论证应提供证据证明相关的危险失效模式可被排除（根据 11.4.4 要求，包括对系统性失效的可能性的考虑）。

11.4.8 FVL 和 LVL 可编程设备的诊断覆盖率不应小于 60%。

11.4.9 失效量计算中使用的可靠性数据应由不小于 70%的统计置信区间上限确定。

11.5 关于设备选择的要求

11.5.1 目的

本章目的是：

——规定组成 SIS 设备的选择要求；

——规定把设备集成到 SIS 架构中的要求；

——根据相关的 SIF 和安全完整性要求规定设备的验收准则。

11.5.2 一般要求

11.5.2.1 用于规定 SIL 的 SIS 的设备应符合 GB/T 20438.2—2017、GB/T 20438.3—2017 和/或 11.5.3～11.5.6 的规定。

11.5.2.2 应通过考虑制造商文件、SRS 的约束以及 11.9 假定的可靠性参数来确定所有设备适用于运行环境。所选设备的适用性应始终在特定运行环境中加以考虑。

注：基于不同运行环境和操作模式，设备可能表现出不同的失效率。从制造商获得的失效率数据可能不是在所有应用中都有效。例如，频繁使用的阀门和长期不动作的阀门失效率和失效模式分布可能不同。

11.5.3 根据“以往使用”选择设备的要求

11.5.3.1 应提供证明设备适用于 SIS 的适当证据。

注 1：以往使用评估的主要目的是：收集证据以证明与要求的安全完整性相比，危险系统性故障已被降至足够低的水平。

注 2：证据的详细程度取决于设备的复杂程度。

注 3：“以往使用”评估包括收集设备在类似运行环境下的性能表现的文档记录。“以往使用”证明设备的功能性和完整性，包括过程接口、完整的设备边界、通信和动力源。

注 4：如 11.9.3 所述，“以往使用”的数据可以放入用于计算硬件失效率的数据库。

11.5.3.2 适用性证据应包括：

——对制造商质量体系、管理体系和配置管理体系的考虑；

——设备的标识和规格书；

——在类似运行环境下设备性能的证明；

注 1：现场设备（例如，传感器和最终元件）在安全和非安全应用中的表现通常是相同的，因此，类似设备在非安全应用中的性能证据也可以用来满足此要求。

——运行经验的丰富程度。

注 2：对于现场设备而言，与运行经验有关的信息主要记录在用户设施的用户设备清单中，该清单的形成是基于设备在安全和非安全应用中成功运行时的大量历史记录并剔除不能成功执行功能的设备。倘若下列条件成立，现场设备清单可用来支持运行经验的声明：

- 清单是定期更新和监视的；
- 只有在获得足够的运行经验时，现场设备才可以加入该清单；
- 当现场设备的运行历史显示其性能不符合要求时，这些设备需从清单中移除；
- 清单中包含相关的运行环境信息。

注 3：运行环境会对设备性能造成明显影响，通常推荐基于充分的设备性能表现（通过多个现场的大量安装，并长时间运行而获得）来选择设备。获得的运行经验需允许足够时间来揭露早期失效，例如，那些和规格书、储存、安装和试车相关的早期失效。

注 4：用于获得可信的具有统计意义的可靠性数据而需要的运行经验通常远多于用于证明“以往使用”需要的运行经验。

11.5.3.3 所有基于“以往使用”选择的设备应通过规定的版本号进行识别，并受控于变更管理规程。当对这些设备做出变更时，应对“以往使用”的证据通过评估变更的影响论证是否继续有效。

11.5.4 根据“以往使用”选择 FPL 可编程设备（如现场设备）的要求

11.5.4.1 对于 SIL1、SIL2、SIL3，应符合 11.5.2、11.5.3 的要求以及以下条款。

11.5.4.2 所有可能影响安全的设备配置选项均应被识别并加以考虑。对于没有定义特定设置的，应确认设备的默认设置是否合适。设备未被使用的特性应在适用性证据中加以识别，并确定这些特性不太可能危害到 SIF。

11.5.4.3 对于设备的特定配置和运行环境，适用性证据应考虑：

——输入和输出信号的特性；

——使用的模式；

——使用的功能和配置；

——以往在类似运行环境中的使用情况。

11.5.4.4 对于 SIL 3 应用，还应对 FPL 设备进行评估以表明：

——FPL 设备能够执行要求的功能，并且以往使用表明当把该设备用作 SIS 的组成部分时，由于它的失效（既可能是硬件随机失效，也可能是硬件或软件中的系统性故障）可能导致危险事件的概率足够低；

——已经使用了针对硬件和软件的适当标准；

——FPL 设备已在可代表预期运行场景的配置中应用或测试过。

11.5.5 根据“以往使用”选择 LVL 可编程设备的要求

11.5.5.1 下面的要求适用于执行 SIL 1 或 SIL 2 的 SIF 的 SIS 中使用的 PE 设备。

11.5.5.2 11.5.4 要求均适用。

11.5.5.3 在设备以往使用的运行环境和当前 SIS 的运行环境存在任何差异时，应标明这些差异，适当时，应根据分析和测试进行评估，以表明用于当前 SIS 时，系统性故障的可能性足够低。

11.5.5.4 为论证某个设备的适用性所必需的运行经验应考虑以下因素来确定：

——SIF 的 SIL；

——设备的复杂程度和功能性。

11.5.5.5 倘若满足下列所有附加条款，则可在 SIL 1 或 SIL 2 应用中使用安全配置的一个 PE 逻辑解算器。

——了解非安全失效模式。

——针对识别出的失效模式使用安全配置技术。

——嵌入式软件在安全应用中有优良的使用历史。

——可提供针对未经授权或非预期修改的保护。

注：安全配置的 PE 逻辑解算器是指通用工业级 PE 逻辑解算器，由 OEM 厂商、系统工程师或终端用户专门配置以用于安全应用。

11.5.5.6 应对在 SIL 2 应用中使用的所有 PE 逻辑解算器进行正式评估（根据 5.2.6.1）以表明：

——PE 逻辑解算器能执行要求的功能并且以往使用表明当把该设备用作 SIS 的组成部分时，由于它的失效（既可能是硬件随机失效，也可能是硬件或软件中的系统性故障）可能导致危险事件的概率足够低。

——采取措施在程序执行时检测故障，并触发合理的响应。这些措施应包括以下所有内容：

- 程序顺序监视；
- 通过在线监测来检测失效或保护代码不被修改；
- 失效断言或多样化编程；
- 变量的范围检查，或者值的合理性检查；
- 模块化方法；
- 嵌入式软件和工具软件已使用合适的编码标准；
- 使用可代表预期运行场景的测试用例进行了典型配置的测试；
- 使用值得信赖的、经验证的软件模块和组件；
- 系统已经过动态分析和测试；
- 系统不使用人工智能，也不使用动态配置；
- 已执行文档化的故障插入测试(负面测试)。

11.5.6 选择 FVL 可编程设备的要求

当使用 FVL 对应用程序进行编程时，PE 设备应符合 GB/T 20438.2—2017 和 GB/T 20438.3—2017 的要求。

11.6 现场设备

11.6.1 现场设备的选择和安装应最大程度减小可能因运行环境条件导致信息不准确的失效。考虑的条件宜包括：腐蚀、物料在管道中冻凝、悬浮物、聚合、结焦、温度和压力极限，干式取压管中的冷凝，湿式取压管中的不充分冷凝。

11.6.2 应采取手段保证得电跳闸回路的电路和电源完整性。

注 1：线路终端监视器是上述手段的一个实例，通过连续监测一个辅助电流从而确保电路的连续性，而辅助电流的强度不会影响 I/O 的正常工作。

注 2：失电的附加要求参见 11.2.11。

11.6.3 除非经安全审查允许读写，智能传感器应设置写保护，以防止意外修改。

注：审查可考虑人员因素，例如，未遵守规程。

11.7 接口

11.7.1 概述

SIS 的接口包括但不限于：

——操作员接口；

——维护/工程接口；

——通信接口。

11.7.2 操作员接口要求

11.7.2.1 在 SIS 操作员接口是借助于 BPCS 操作员接口的情况下，需考虑在 BPCS 操作员接口中可能发生的可信失效。

注：这包括编制计划，使得在操作显示界面完全失效的情况下，有序地安全停车。

11.7.2.2 SIS 的设计应尽量减少需要操作员进行选择的选项，以及出现危险时旁路系统的需要。如果设计不要求使用操作员动作，则设计宜包含防止操作员错误的设施。

注：如果操作员不得不选择某个特殊选项，可设置证实步骤。

11.7.2.3 旁路开关或旁路手段应防止未经许可的使用(如加键锁或口令保护,连同有效管理控制)。

注:可考虑对旁路操作实施强制的时间限制,并限制每次可激活的旁路数量。

11.7.2.4 对于维护 SIF 至关重要的 SIS 状态信息应在操作员接口显示。这些信息包括:

——过程处于其流程中的哪个环节;

——已发生 SIS 保护动作的指示;

——旁路保护功能的指示;

——已发生某个自动动作(如表决降级和/或故障处理)的指示;

——传感器和最终元件的状态;

——影响安全的断电;

——诊断结果;

——支持 SIS 所需的环境调节设备的失效。

11.7.2.5 SIS 操作员接口的设计(见 11.7.2.7)应能防止改变 SIS 应用程序。

11.7.2.6 在需要将信息从 BPCS 传输给 SIS 时,应使用系统、设备或规程来证实传输了正确的信息,并且不会损害 SIS 的安全完整性。

注:使用的系统、设备或规程可包含针对从 BPCS 到特定 SIS 变量的选择性写入的控制。

11.7.2.7 SIS 操作员接口借助于 BPCS 操作员接口的设计应保证从 BPCS 到 SIS 的错误信息或数据不会损害安全性。

11.7.3 维护/工程接口要求

11.7.3.1 SIS 维护/工程接口的设计应确保此接口的任何失效都不会对 SIS 执行 SIF 的能力产生不利影响。这可能要求在 SIS 正常运行时断开维护/工程接口,如编程面板。

11.7.3.2 维护/工程接口应为下列功能提供访问安全防护:

——SIS 运行模式、程序、数据、屏蔽报警通信的方法、测试、旁路、维护;

——SIS 诊断、表决和故障处理服务;

——增加、删除或修改应用程序;

——排除 SIS 故障所需的数据;

——在需要旁路时,应使得报警和手动停车设施不会失效。

11.7.3.3 维护/工程接口不应用作操作员接口。

11.7.3.4 启用和禁止读-写访问功能应仅能通过配置管理流程来实现,使用具有适当文档和安防措施(如身份验证和用户安保通道)的维护/工程接口。

11.7.4 通信接口要求

11.7.4.1 SIS 通信接口的设计应确保通信接口的任何失效不会对 SIS 使过程达到或保持安全状态的能力产生不利影响。

11.7.4.2 当 SIS 能够与 BPCS 和外部设备进行通信时,通信接口、BPCS 或外部设备不应对 SIS 中的任何 SIF 产生不利影响。

11.7.4.3 通信接口应足够健壮以便能承受包括电源浪涌在内的电磁干扰而不会引起 SIS 的危险失效。

11.7.4.4 通信接口应适宜不同参考地电位的设备间的通信。

注:可以选择不同的媒介(如光纤)。

11.8 维护或测试设计要求

11.8.1 设计应允许以端-端或分段对 SIS 进行测试。在预定的过程停机时间之间的间隔大于检验测试

间隔的情况下,需要在线测试设施。

注:术语端-端意味着从传感器与过程流体的接触端到执行器与过程流体的接触端。

11.8.2 当需要在线检验测试时,测试设施应为 SIS 设计的必要组成部分。

11.8.3 当 SIS 包括测试或旁路设施时,它们应符合:

——应按 SRS 中定义的维护和测试要求设计 SIS;

——对 SIS 任何部分的旁路均应通过报警或操作规程警示操作员。

11.8.4 应确定在维持过程安全运行前提下,允许 SIS 处于旁路状态(维修或测试)的最大时间。

11.8.5 当 SIS 处于旁路状态(维修或测试)时,应按 11.3 的要求提供确保维持安全运行的补偿措施。

11.8.6 在 PE SIS 中,强制输入和输出不得用作应用程序、操作规程和维护的一部分(下述情况除外)。

除非设置有规程和访问安防,否则不准许在 SIS 不停止工作的情况下强制输入和输出。针对任何这种强制,应选用合适的方式通知或发出报警。

11.9 随机失效的量化

11.9.1 各 SIF 的计算失效量应等于或优于 SRS 中规定的 SIL 对应的目标失效量,这应由计算确定。

注:在复杂应用中,可用危险事件频率代替目标失效量(例如,不同的要求原因有不同的安全完整性要求时,或非独立 SIS 顺序动作时)。

11.9.2 SIF 随机失效的计算失效量需考虑下列所有因素:

a) 与每个 SIF 相关的 SIS 架构及 SIS 子系统的架构;

b) 估计的每个失效模式的失效率,它是由随机硬件失效产生的,这种失效可引起 SIS 危险失效且已被诊断测试检测到;

c) 估计的每个失效模式的失效率,它是由随机硬件失效产生的,这种失效可引起 SIS 危险失效但已被检验测试检测到;

d) 估计的每个失效模式的失效率,它是由随机硬件失效产生的,这种失效可引起 SIS 危险失效,既未被诊断测试检测到又未被检验测试检测到;

e) SIS 对检验测试本身引起的失效敏感度;

f) SIS 对共因失效的敏感度;

g) 任何定期的诊断测试的诊断覆盖率,相关的诊断测试间隔和诊断设施的失效概率;

h) 任何定期检验测试的覆盖率,相关的检验测试规程和检验测试设施和规程的可靠性;

i) 检测到的失效的维修时间和维修期间 SIS 的状态(在线或离线);

j) 在任何模式下可能引起 SIS 危险失效的任何通信过程的估计危险失效率(包括诊断测试检测到的和未检测到的两种情况);

k) 可能引起 SIS 危险失效的操作员响应的估计可能性(包括诊断测试检测到的和未检测到的两种情况);

l) SIS 所需动力源的可靠性。

注:有几种建模方法可用,最适用的方法取决于分析人员及具体情况。可用的方法包括(见 IEC 61508-6:2010 中附录 B):

——因果分析;

——可靠性框图;

——故障树分析;

——马尔可夫(Markov)模型;

——佩特里(Petri)网模型。

可能通过分析或数值模拟进行概率计算(如蒙特卡罗模拟)。

11.9.3 量化随机硬件失效的影响时使用的可靠性数据应可信、可追踪、有资料支持且经过论证，并且应基于在相似运行环境中相似设备的现场反馈。

注 1：上述可靠性数据包括：用户收集的数据，厂商/供应商/用户数据（从设备上收集到的数据的衍生数据），通用的现场反馈可靠性数据库中的数据等。在某些情况下，工程判断可用于评估缺失的可靠性数据，或评估在某个不同运行环境下收集到的可靠性数据的影响。

注 2：缺乏可反映运行环境的可靠性数据是概率计算时经常出现的问题。最终用户可按照 IEC 60300-3-2:2004 或 ISO 14224:2016 的要求组织相关设备可靠性数据收集，以提高 IEC 61511 的实施效果。

注 3：基于返修的供应商数据可能被限制在完全了解运行环境并完全按照 IEC 60300-3-2:2004 或 ISO 14224:2016 进行记录的设备样本。用户也可以记录其 SIF 的运行环境，并证明供应商的运行环境数据与其 SIF 的环境匹配。

11.9.4 在计算失效量时应评估和考虑可靠性数据的不确定度。

注 1：可靠性数据的不确定度可通过现场反馈的数量（越少的现场反馈意味着越大的不确定度）或/和运用专家判断来进行评价。已出版的标准（IEC 60605-4）、贝叶斯方法、工程判断技术等可被用于估计可靠性数据的不确定度。

注 2：下列技术可被用于计算失效量（详见 IEC 61511-2:2016）：

——对各输入的可靠性参数，采用 70%置信区间的上限值而不采用其平均值，以获得失效量的保守估计；

——利用输入的可靠性参数的概率分布函数，进行蒙特卡罗模拟得出可代表失效量分布的柱状图，并用此分布评估出一个保守值（例如，失效量真值有 90%的置信度优于计算值）。

11.9.5 对于某个特定设计，如果未能达到相关 SIF 的目标失效量，则：

a) 识别对失效量贡献最大的设备或者参数；

注：故障树的割集分析在此非常有效。

b) 评估可能的改进措施（例如，更可靠的设备、增加针对共模失效的防范措施、增加诊断或检验测试覆盖率、增加冗余、缩短检验测试间隔、交错测试等）对识别出的设备或参数的影响；

c) 选择并且实施改进措施以建立新的结果；

d) 对比新结果与目标失效量，并重复 a)～本步骤直至以保守的方式达到目标失效量。

12 SIS 应用程序开发

12.1 目的

本章目的是定义应用程序开发的要求。

12.2 一般要求

12.2.1 SIS 应用程序应符合应用程序安全要求（见 10.3.3）以及本章对 SIL1～SIL3（包括 SIL3）的所有要求。

12.2.2 应用程序员应审查 SRS 中的信息和应用程序安全要求，以确保要求是全面的、清晰的、易理解的和一致的。应识别并解决应用程序安全要求中的所有缺陷，如果对应用程序安全要求进行了修改，应进行影响分析。

12.2.3 IEC 61511 解决与 LVL 编程以及使用 FPL 的设备相关问题。IEC 61511 不关注与 FVL 以及 SIL4 应用程序编程相关的问题。如果某些功能块是用 FVL 编写的，那么这些功能块应按照 GB/T 20438.3—2017 进行开发和修改。

12.2.4 在 SIS 应用程序需同时实现安全和非安全功能的情况下，所有应用程序都应作为 SIS 的组成部分并且应符合本文件，此外，应通过评估和测试明确非安全功能不会影响安全功能。

12.2.5 应用程序应按如下方式设计：确保一旦 SIS 将过程置于安全状态，不论失电情况和恢复供电情况，过程将维持在安全状态，直到触发复位，除非 SRS 另有规定。

注 1：如果 SIF 没有复位功能，则宜有文档化的工程论证，以说明为什么无需复位所带来的安全延迟即可重启过程是可接受的。

注 2：更多信息可参见 11.2.7。

12.2.6 在 SIS 启动（或上电）期间，应用程序应确保安全输出保持在安全状态（通常为失电状态）直至被复位，除非 SRS 另有规定。

12.2.7 应用程序应被设计成：每一次应用程序扫描都会执行应用程序的所有部分，除非在安全手册中有特定替代要求。在确立应用程序扫描要求时，需考虑过程安全时间要求。

12.2.8 SIS 应用程序和数据应遵循变更、修订控制、版本管理、备份和恢复规程。

12.2.9 SIS 应用程序安全生命周期计划应涉及以下方面。

——在应用程序设计和开发过程中应用的 SIS 安全生命周期阶段和活动。这些要求包括为了避免应用程序中的错误和控制可能发生的失效而采用的措施和技术。

——传递给 SIS 集成实施组织的与应用程序确认有关的信息。

——为用户准备的其操作和维护 SIS 所需的信息和规程。

——执行应用程序修改的组织满足的规程和规范。

12.3 应用程序设计

12.3.1 应用程序设计应实现所有 SIS 逻辑，包括每个 SIF 的所有过程操作模式。

12.3.2 应用程序设计的输入应为 SRS，包括应用程序要求（见第 10 章）、SIS 架构（见第 11 章）以及进行应用程序设计的方法与工具（见 12.6）。应用程序设计应与 SRS 一致并可追溯回 SRS。

12.3.3 应用程序设计应能支撑功能安全评估的实施。

12.3.4 应用程序设计及其分解后的模块（如适用）应阐明要求是如何实现的，适用时包括以下内容：

——使过程达到或保持安全状态的功能；

——所有识别出的应用程序组件的规范，以及识别出的组件间的连接和交互的描述；

——应用程序功能相关的时序约束及其在程序中执行的扫描时间；

——所使用标准库模块（功能块）的详细描述；

——所使用专用模块（功能块）的详细描述；

——关于内存分配方式的描述；

——使用的全局变量的列表和保护其完整性的方法；

——识别应用程序中所有的非 SIF 和与非安全相关部分的接口，以确保它们不会影响任何 SIF 的正常运行；

——输入和输出接口的定义，包括位号列表及相关的数据类型；

——SIS 应用程序和操作员接口数据交互的详细说明；

——SIS 应用程序和 BPCS 及外设（例如，打印机、数据存储器等）之间数据交互的详细说明；

——如何处理和记录外部和内部诊断信息；

——操作和维护接口的实现方法的详细描述，包括报警的优先级划分、提示和确认；

——为实现要求的 SIL 而实施的应用层诊断的详细描述，例如，外部看门狗、应用数据完整性校验、传感器确认；

——系统组态检查，包括预期的硬件设备和软件模块是否存在并可访问；

——如何使应用程序设计复杂度最小化，例如，通过使用模块化设计和简单功能；

——与 SIS 子系统故障检测、警报和管理相关的功能；

——SIF 在线周期性测试相关的功能；

——SIF 离线周期性测试相关的功能；

——允许安全地进行 SIS 维护的功能；

——应用程序设计规范所引用的文档。

12.3.5 应用程序设计应确保：

——对于 SRS 及其预期目的的完备性；

——对于 SRS 及其预期目的的正确性；

——避免歧义，即对于那些在 SIS 安全生命周期任何阶段会使用该文件的人员来说要清晰；这包括使用对于设备操作人员、系统维护人员和应用程序编程人员能清楚并可理解的术语和描述；

——避免设计缺陷。

12.4 应用程序的实现

12.4.1 应用程序开发方法应符合 SIS PE 子系统制造商提供的开发工具和限制。

12.4.2 下列信息应包含在应用程序或相关文档中：

a) 应用程序的开发者；

b) 应用程序目的的描述；

c) 所使用的安全手册的版本；

d) 每个 SIF 对应用程序部分(模块)的依赖关系的标识；

e) 对应用程序 SRS 的追溯；

f) 每个 SIF 及其 SIL 的标识；

g) 所用符号的标识和描述，包括逻辑约定、标准库函数及应用库函数；

h) SIS 逻辑解算器的输入输出信号的标识；

i) SIS 使用通信的地方，都要有通信信息流的描述；

注：例如，某个 SIF 使用多个逻辑解算器的情况。

j) 对程序结构的描述，包括对输入/输出子系统的数据逻辑处理顺序的描述，以及对扫描时间带来的限制的描述；

k) 如果 SRS 有要求，还包括：

- 确保现场数据正确性的方法(例如，通过模拟量传感器之间的对比来提高诊断覆盖率)；
- 确保经通信链路发送的数据正确性的方法，例如，当从 HMI 发出通信时，在执行命令前发送“确认”；
- 确保通信安全的方法(例如，网络安全措施)；

l) 版本标识和修改历史。

12.4.3 如果设计使用了先前开发的应用程序库函数，应基于下列要求论证它们的适用性：

——符合 IEC 61508，如果对 FVL 进行了符合 GB/T 20438.3—2017 的“经使用证明”评估，应用程序库函数在其上运行的可编程设备也应根据 GB/T 20438.2—2017 进行“经使用证明”评估；或者

——当使用 FPL 或 LVL 时，需符合本文件“以往使用”的要求(见 11.5.4 或 11.5.5)；

——对于所有情况，证明未被使用的功能不会对应用程序造成不利影响。

12.4.4 应用程序应以结构化的方式编写，以实现：

——功能的模块化分解；

——将 SIF 应用程序的复杂度保持在与 SIF 的复杂度一致的最低限度；
——功能(包括容错特性)及应用程序内部结构的可测试性；
——应用功能和相关约束的追溯和说明；
——硬件架构和应用程序架构之间一一对应。

12.5 应用程序验证要求(审查和测试)

12.5.1 应按照第 7 章执行验证计划。

12.5.2 应用程序(包括其文档)应由某个未参与原始开发的具备资质的人员审查。应记录审查的方法和结果。

12.5.3 应用程序(适用时包括其分解成的模块)应通过审查、分析、仿真和测试技术使用书面程序和测试规范进行验证，以确认应用程序功能满足 SRS 且没有执行非预期功能，并且对 SIF 没有非预期影响。应包括以下内容：

a) 对应用程序设计规范、定义的方法和规程以及安全确认和测验计划的符合性；
b) 应用程序所有部分的测试；
c) 一系列典型数据条件的测试；
d) 失效情况的测试(即负面测试)；
e) 执行的时机和顺序；
f) SIS 的通信测试；
g) 将离线应用程序集成到逻辑解算器硬件和底层 PE 上；
h) 通过内部数据流检查来确认逻辑解算器按预期工作，而非仅仅看起来在工作；
i) 可能的话，将应用程序与第三方设备进行集成测试。

12.5.4 应验证 I/O 数据对应用程序的映射，包括数据类型和范围。

12.5.5 在测试中，对应用程序的修改应进行影响分析，以确定：
——所有受影响的应用程序部分；和
——必要的重新设计和重新验证活动。

12.5.6 应记录应用程序测试结果，包括以下内容：
——被测试的应用程序的版本以及其支持文件；
——配套软件和测试工具的版本；
——执行测试和审查的人员姓名以及日期；
——测试、审查和执行日期的描述；
——测试结果；
——测试的目标和准则是否达到；
——失效原因、失效分析以及纠正措施和复测要求(如果在测试中出现失效)。

12.6 应用程序方法和工具的要求

12.6.1 应用程序开发应遵循适用的安全手册中的约束。

注：使用安全手册时，如果特定应用需要，可执行附加程序对方法和工具使用进行限制。

12.6.2 应为生命周期每个阶段选择方法、技术和工具并予以应用，以达到：
——将在应用程序中引入故障的风险最小化；
——揭露并消除应用程序中已经存在的故障；
——在可行范围内确保应用程序中残留的故障不会导致不可接受的后果；

——在 SIS 的整个生命周期内，强化应用程序修改管理的手段；

——提供证据证明应用程序具备所要求的质量。

13 工厂验收测试（FAT）

13.1 目的

本章目的是测试 SIS 设备以确保其达到了 SRS 中规定的要求。

注 1：通过在安装前测试逻辑解算器以及相关的软件和硬件，能够较容易地识别和纠正错误。

注 2：FAT 有时又称为集成测试，并且可以是确认的一部分。

注 3：当运行中需要高可信性时（如海底应用），建议在最终安装前将现场元件和逻辑解算器结合在一起进行测试。

13.2 建议

13.2.1 在项目安全计划编制时应明确 FAT 的需求。

注 1：为了开展集成测试，可能需要逻辑解算器供应商和设计承包商之间紧密协作。

注 2：这些活动在设计和开发阶段之后，安装和调试运行之前进行。

注 3：这些活动适用于 SIS 子系统，无论有没有 PE。

注 4：FAT 通常是在现场安装和调试前于工厂环境下进行。

13.2.2 FAT 计划应明确以下内容：

——要执行的测试类型，包括黑盒系统功能性测试、性能测试、内部检查、环境测试、接口测试、在降级和/或故障情况下进行的测试、异常测试、电源故障情况下的安全响应测试（包括重新上电后的重启）以及 SIS 维护与操作手册的应用；

注 1：黑盒功能测试是一种将系统视为“黑盒”的测试设计方法，因此它无需使用其内部结构知识。黑盒测试设计通常专注于测试功能需求。黑盒测试的同义词包括行为测试、功能测试、不透明盒测试以及闭盒测试。

注 2：性能测试确定系统是否满足及时性、可靠性和可用性、完整性、安全性目标和约束。

注 3：环境测试包括 EMC、寿命和应力测试。

注 4：可进行内部数据流检查，以确保 SIS 按照规定处理输入数据并生成输出响应。

——测试用例、测试描述和测试数据；

注 5：落实谁负责开发测试用例、谁将负责执行测试和见证测试是非常重要的。

——对其他系统/接口的依赖性；

——测试环境和工具；

——逻辑解算器、传感器和最终元件的配置；

——判断测试完成的测试准则；

——针对测试失败的纠正措施程序；

——测试人员的资质；

——物理位置；

——测试造成的危险，特别是涉及储能时；

——清晰的测试配置图表；

——在进行测试时应予记录的测试、数据、结果和现象。

注 6：不能进行物理测试时，通常以正式的推理来说明为什么 SIS 达到了要求、目标或约束。

13.2.3 应在逻辑解算器的确定版本上进行 FAT。

13.2.4 应按照 FAT 计划进行 FAT。这些测试应显示所有逻辑均正确执行。

13.2.5 对于进行的每一项测试，应关注以下内容：

——所使用的测试计划的版本；

——所测试的 SIF 和性能特性；

——详细的测试规程和测试描述；

——按时间顺序编排的测试活动记录；

——使用的工具、设备和接口。

13.2.6 记录 FAT 的结果，应包括：

a) 测试用例；

b) 测试结果；

c) 目标和测试准则是否满足。

如果测试过程中出现失效，则应记录失效原因并进行分析，采取相应的改正动作。

13.2.7 在 FAT 过程中，任何修改或变更都应经过安全分析以确定：

a) 对每个 SIF 的影响程度；

b) 应定义和实施的测试和验证的范围。

注：根据 FAT 的结果，在采取改正动作的同时可进行调试。

14 SIS 安装和调试

14.1 目的

本章目的是：

——根据规范和图纸安装 SIS；

——调试 SIS 以便为最终的系统确认做好准备。

注：调试活动的目的是确保各 SIS 设备均已按设计做好运行准备。

14.2 要求

14.2.1 安装和调试计划应定义安装和调试所需的所有活动。计划应提供以下内容：

——安装和调试活动；

——安装和调试所使用的规程、措施和技术；

——应在何时进行这些活动；

——负责这些活动的人员、部门和组织。

适用时安装和调试计划可整合到整体项目计划中。

14.2.2 应按设计和安装计划正确安装 SIS 的所有设备。

14.2.3 应按照最终系统确认计划进行 SIS 调试。调试活动应包括(但不限于)对以下内容的证实：

——已正确接地；

——已正确接通动力源并可运行；

——已拆除运输固定材料和包装材料；

——无物理损伤；

——已正确校准和配置好所有的仪表；

——所有现场设备均可运行；

——逻辑解算器和输入/输出均可运行；

——与其他系统和外设的接口均可运行；

——远程 SIS 系统间的所有通信均可运行。

14.2.4 应形成适当的SIS调试记录,说明调试活动的结果以及是否满足设计阶段确定的目标和准则。如果出现失效,应记录失效的原因。

14.2.5 对于实际安装与设计资料不符的情况,应由有资质的人员对差异进行评估并确定差异对安全的影响。如果确定差异对安全没有影响,则应将设计资料更新为“竣工”状态;如果这种差异对安全有负面影响,则应对安装进行调整,以满足设计要求。

15 SIS安全确认

15.1 目的

本章目的是通过审查和测试来确认安装和调试好的SIS及相关的SIF达到了SRS中所声明的那些要求。

注:SIS安全确认有时被称为现场验收测试(SAT)。

15.2 要求

15.2.1 SIS确认计划编制应贯穿SIS安全生命周期,并应定义确认所需的所有活动和设备。活动项目应包括:

——确认活动,包括基于SRS对SIS进行确认以及由此产生的建议的实施和解决。

——对过程及其相关设备的所有操作模式进行确认,包括:

- 为使用所做的准备工作,包括设置和调整;
- 开车、自动、手动、半自动、稳定运行状态;
- 复位、停车、维护;
- 在SIS安全生命周期先前阶段识别出的其他模式。

——确认所使用的规程、措施和技术,包括如何在不将工厂和过程置于SIS防护的危险事件风险下,开展确认活动。

——何时进行这些活动。

——负责这些活动的人员、部门和组织,以及确认活动的独立性水平。

——执行确认活动所依据的引用信息(如因果图)。

——需要安装或提供的设备设施(如用于阀门测试的隔离阀和泄漏检测设备)。

注:确认活动的例子包括回路测试、逻辑测试、校准规程、应用程序仿真。

15.2.2 应用程序确认计划应包括:

a) 在开始调试前,识别针对过程各操作模式需确认的应用程序功能。

b) 确认的技术策略,包括:

- 手动和自动技术;
- 静态和动态技术;
- 分析和统计技术。

c) 根据b),将用于证实各SIF符合规定的安全要求和SIL的措施(技术)及规程。

d) 进行确认活动所要求的环境(例如,对于测试,包括校准过的工具和设备)。

e) 应用程序。

f) 为完成确认所需的通过/失败准则,包括:

- 要求的过程和操作员输入信号以及它们的顺序和值;
- 预期的输出信号以及它们的顺序和值;

- 其他验收准则，如内存使用率、时间和数值容差。

g) 评估确认结果（特别是失败）的策略和规程。

h) 确认所有文件（见第 19 章）以确保 SIF 的准确性、一致性和可追溯性（从 H&RA 开始到 SIF 最终安装）。

15.2.3 在要求把测量精度作为确认的一部分时，应对照一个可追溯到某个标准的规范，把用于此功能的仪表校准到适合该应用的某个不确定度范围内。如果这种校准不可行，则应使用一种替代方法并记录。

15.2.4 应根据 SIS 确认计划对 SIS 及其相关 SIF 进行确认。确认活动应包括（但不限于）：

a) 证实 SIS 在 SRS 定义的正常和异常过程操作模式（如开车、停车）下均可正常运行；

b) 证实 BPCS 和连接的其他系统间不良相互作用不会影响 SIS 的正常运行；

c) SIS 能与 BPCS 或任何其他系统或网络进行正常通信（如需要），包括在异常情况下，如数据过载；

d) 传感器、逻辑解算器和最终元件均按照 SRS 运行，包括所有冗余通道，包括数据过载等异常情况；

注：如果按第 13 章对逻辑解算器进行了 FAT，则可把 FAT 认作是对逻辑解算器的确认。在所有设备安装到工厂后，全回路确认将测试逻辑解算器的功能性和它与其他 SIS 子系统的连接。

e) SIS 设计文档与安装的系统一致；

f) 证实针对无效的过程变量值（例如，超出范围），SIF 按照规定运行；

g) 触发了正确的停车顺序；

h) SIS 提供了正确的警报和运行显示；

i) SIS 中所包含的计算不仅在期望的数值范围内是正确的，在限值和超过限值时也是正确的；

j) SIS 复位功能按 SRS 执行；

k) 旁路功能运行正确；

l) 启动超驰运行正确；

m) 手动停车系统运行正确；

n) 维护规程中的检验测试策略；

o) 诊断报警功能按要求执行；

p) 证实在动力源（如电源、空气、液动源）中断时，SIS 能按要求运行；并证实当动力源恢复时，SIS 能返回期望的状态；

q) 证实达到了 SRS 规定的 EMC 抗扰性（见 10.3）。

15.2.5 应用程序确认应确定：

a) 所有规定的应用程序安全要求（见 10.3.2）均被正确执行；

b) 在 SIS 故障情况或降级运行模式或 SIS 和 BPCS 之间的任何接口故障情况下，应用程序均不会危及安全要求；

c) 应用程序不会因执行“不使用的”软件功能（即未在规范中定义的功能）而危及安全要求；

d) 应提供确认活动的信息。

15.2.6 确认计划活动的结果应显示并覆盖整个 SIS 确认过程。SIS 确认文档应包括：

a) 所使用的 SIS 确认计划的版本；

b) 被测试（或分析）的 SIF，及其在 SIS 确认计划编制过程中识别出的要求；

c) 使用的工具和设备，及其校准数据；

d) 每次测试的结果；

e) 使用的测试规范的版本；
f) 完成的测试的验收准则；
g) 被测试 SIS 硬件、应用程序和其他软件的版本；
h) 实际结果和预期结果间的不符合项及解决办法；
i) 在出现不符合项的情况下，对不符合项所做的分析，以及对是否继续进行测试或是发布一个变更请求而做出的决定。

15.2.7 实际结果应对照预期结果进行验证。所有的不符合项都应进行分析，分析结果应作为确认文件的一部分。这应包括所做的分析和决定(关于是继续确认，还是发出变更要求并返回到生命周期的某个早期阶段)。

15.2.8 在 SIS 确认之后，识别出的危险出现之前，应开展以下活动：
——应返回所有旁路功能(如对 PE 逻辑解算器和 PE 传感器的强制、禁止报警)的正常位置；
——应按过程开车要求和规程设置所有的过程隔离阀；
——应清除所有的测试介质(如流体)；
——应清除所有的调试超驰和强制许可。

16 SIS 操作和维护

16.1 目的

本章目的是确保：
——每个 SIF 能在操作和维护过程中保持要求的 SIL；
——对 SIS 的操作和维护能维持要求的安全完整性。

16.2 要求

16.2.1 应编制 SIS 的操作和维护计划。计划应提供以下内容：
a) 例行的和异常的操作活动；
b) 检查、检验测试、预防性维护和故障维修活动；
c) 操作和维护使用的规程、措施和技术；
d) 对通过诊断、检查或检验测试检测出的故障和失效的操作响应；
e) 对操作和维护程序符合性的验证；
f) 何时进行这些活动；
g) 负责执行这些活动的人员、部门或组织；
h) SIS 维护计划。

注：SIS 维护计划可以阐述不同 SIL 等级的维护特点。

16.2.2 操作和维护规程应根据相关安全计划制定，规程应提供：
a) 为保持“同设计一样的”SIS 的功能安全所需执行的例行方法和程序；
b) 确保检验测试的质量和一致性的规程，以及确保设备更换后进行充分确认的规程；
c) 在维护或操作期间，为防止不安全状态和/或减小危险事件后果所必需的措施和约束(例如，为了测试或维护需要旁路一个系统时，需要实施哪些附加的风险降低)；
d) 用于测试诊断功能的方法和规程；
e) SIS 失效时需要保留的信息，以及 SIS 要求率的信息；
f) 与要求率和 SIS 可靠性参数有关的数据收集的规程；

注 1：收集和分析失效数据有很多好处，包括如果运行中的失效率明显低于设计时的预测，则有可能降低维护成本。新安装的实施成本也可能降低，因为新设计可基于不那么保守的失效率。

g） 需保留的表明 SIS 审核和测试结果的信息；

h） 当 SIS 发生故障或失效时应遵从的维护规程，包括：

- 故障诊断和维修规程；
- 重新确认规程；
- 维护报告要求；
- 跟踪维护性能的规程。

注 2：考虑的内容包括：

- 报告失效的规程；
- 分析系统失效的规程；
- 在 BPCS 失效时实现安全停车的动作；
- 确保测试设备进行适当的校准和维护。

16.2.3 操作规程应切实可行。在由于旁路（维修或测试）导致 SIS 被禁用或降级时，应在相应的操作限制下（持续时间、过程参数等）采取补偿措施以维持安全。应向操作员提供旁路前和旁路中适用的规程，旁路移除前应做什么，以及处于旁路状态的最大允许持续时间等信息。这些信息应定期复审。

注：操作和维护规程可包括检验测试后是否移除旁路的验证。

16.2.4 当某个 SIS 设备被旁路时，只有在危险分析确定已实施补偿措施且其提供了足够的风险降低的情况下，才允许过程继续运行。应制定相应的操作规程。

16.2.5 应根据相关规程进行操作和维护。

16.2.6 应对操作员进行关于其所在区域的 SIS 的功能和操作的培训，培训应确保他们理解：

——SIS 如何工作（跳闸点及 SIS 因此执行的动作）；

注 1：这也可能包括某个 SIS 动作对继续运行装置的影响。

——SIS 能防护的危险；

——所有旁路/超驰开关的正确操作和管理，以及在什么情况下使用这些旁路；

——手动开/停车开关的操作，以及何时激活这些手动开关；

注 2：也可包括“系统复位”和“系统重启”。

——出现诊断报警时应采取的动作（例如，当指示 SIS 存在某个问题的报警出现时，应采取什么动作）；

——对诊断功能的合理验证。

16.2.7 应在旁路日志里记录所有旁路的状态。所有旁路都需要授权和指示。

16.2.8 应按要求培训维护人员，以维持 SIS（硬件和软件）全部功能的性能，从而满足各 SIF 的目标 SIL。

16.2.9 应分析预计的和实际的 SIS 行为之间的差异，必要时应做修改以保持要求的安全。应包括监视以下内容：

——每个 SIF 的要求率（见 5.2.5.3）；

——对系统提出要求时采取的动作；

——构成 SIS 的设备的失效及失效模式，包括在正常运行、检查、测试或对 SIF 产生要求时识别出来的；

——提出要求的原因；

——误停车的原因和频率；

——补偿措施涉及的设备的失效。

16.2.10 操作和维护规程可能需要修订，有必要时应在修订后进行：

——功能安全审核；

——SIS 测试；

——来自正常或异常操作和维护事件的经验。

16.2.11 应为每个 SIF 编制书面的检验测试规程，以揭露未被诊断检测到的危险失效。这些书面的测试规程应描述需要执行的每个步骤并应包括：

——每个传感器和最终元件的正确操作；

——正确的逻辑动作；

——正确的报警和指示。

注：下列方法可用来确定需被测试的未检测到的失效：

——故障树检查；

——失效模式和影响分析；

——以可靠性为中心的维护。

16.2.12 应标识出 SIS 的备件并且保证其可用，从而将由于 SIS 某部件不可用而引起的旁路时间缩短至最小。

注：如果不是同型(完全相同)替换，则可按对 SIS 的修改进行管理。

16.2.13 负责操作和维护的人员应审查危险和风险分析、安全功能分配和 SIS 设计，以确保这些阶段所做的假设是有效的，例如，关于占用和防腐的假设。

16.3 检验测试及检查

16.3.1 检验测试

16.3.1.1 应使用书面的规程进行定期的检验测试以揭露未检测到的故障，这些故障阻碍 SIS 按照 SRS 运行。

注 1：特别要注意识别可能导致共因失效的失效原因。

注 2：功能测试规程还可强调对于避免引入共因失效的需求。

16.3.1.2 应对整个 SIS 进行测试，包括传感器、逻辑解算器和最终元件(如关断阀和电机)。

注：SIS 的测试可以以端到端的形式或以分段的形式进行(见 11.8.1)。

16.3.1.3 应根据 SRS 安排检验测试。SIF 在运行环境中安装后，SIF 的检验测试频率应根据 11.9 通过 PFD_{avg} 和 PFH 计算来确定。

注：SIS 的不同部分可能要求不同的测试间隔，例如，逻辑解算器的测试间隔可能与传感器或最终元件不同。

16.3.1.4 应以一种安全和及时的方式修复检验测试过程中发现的任何缺陷。在修复完成后应再进行一次检验测试。

16.3.1.5 应根据历史测试数据、工厂经验和硬件退化情况等各种因素，定期(周期由用户决定)重新评估测试频率。

注：用户可以根据这些数据和对测试频率原始基础的分析来调整测试频率。

16.3.1.6 对应用程序的任何变更都需要对受影响的 SIF 进行全面的确认和检验测试。如果对变更进行了适当的审查和部分测试，以确保变更是根据更新后的安全要求设计并正确实施的，则允许例外。

16.3.1.7 应使用适当的管理规程审查检验测试的延期，防止重大延迟。

16.3.2 检查

应对每个 SIS 进行定期目视检查，以保证不存在未经授权的修改和可观察到的缺损(如缺螺栓或仪表罩、固定架生锈、线断开、管道破裂、加热保温层破损、绝缘缺失)。

注：这些问题可能预示着故障频率的增加。

16.3.3 检验测试和检查的文档

用户应保存记录，证明检验测试和检查已按要求完成。这些记录至少应包括以下信息：

a) 所进行的测试和检查的说明，包括所使用的测试规程的标识；

b) 测试和检查的日期；

c) 执行测试和检查的人员姓名；

d) 被测系统的序列号或者其他唯一标识符（如回路号、位号、设备号和 SIF 号）；

e) 测试和检查的结果，包括“调整前（as-found）”状态、发现所有故障（包括故障模式）以及“调整后（as-left）”状态。

17 SIS 变更

17.1 目的

本章目的是：

——在对 SIS 进行变更之前应正确编制修改计划并对修改进行审查、批准和文档化；

——确保不管 SIS 作何改变都能保持所要求的 SIS 安全完整性。

注：对 BPCS、其他设备、过程和操作条件的修改均进行审查，以确定这些修改是否会对 SIS 的要求属性和频率造成影响。针对有不利影响的修改还需进一步考虑，以确定风险降低水平依然足够。

17.2 要求

17.2.1 在对 SIS 进行任何修改之前，应建立授权和控制变更的规程。

17.2.2 规程应包括明确的方法来识别和请求所要做的工作以及可能受到影响的危险。

17.2.3 在对 SIS（包括应用程序）进行任何修改之前，应进行分析，以确定拟进行的修改对功能安全的影响。当分析表明拟进行的修改可能影响安全时，则应返回 SIS 安全生命周期的第一个受影响的阶段。

17.2.4 修改和重新验证的安全计划应切实可行。修改和重新验证应按照计划执行。

17.2.5 修改影响到的所有文档都应更新。

17.2.6 符合 5.2.6.1.9 要求的功能安全评估未完成和未经正式授权，不得开始修改活动。

17.2.7 对 SIS 的所有更改都应保留相应的信息。这些信息包括：

a) 修改或更改的描述；

b) 变更原因；

c) 识别出的危险和可能受影响 SIF；

d) 对 SIS 的修改活动的影响分析；

e) 变更要求的所有审批；

f) 用于验证变更已正确实施以及 SIS 按要求执行的测试；

g) SIS 修改活动的详细信息（如修改日志）；

h) 相应的配置历史；

i) 用于验证变更没有对未修改的 SIS 部分产生不利影响的测试。

17.2.8 修改应由经过适当培训的合格人员进行。变更宜通知所有受影响的人员及其他相关的人员，并对其进行关于该变更的培训。

18 SIS 停用

18.1 目的

本章目的是确保：

——SIS 在停用之前要对它进行一次正确的复审，并应得到必要的授权；

——保证在停用活动过程中保持要求的 SIF 继续运行。

18.2 要求

18.2.1 在部分或全部 SIS 或 SIF 的停用实施之前，授权和控制变更的规程应到位。

18.2.2 规程应包括明确的方法来识别和请求所要做的工作以及可能受到影响的危险。

18.2.3 应就拟进行的停用活动对功能安全的影响进行分析评估。评估应包括对 H&RA 的更新，该更新应足以确定对 SIS 安全生命周期的影响范围。随后的 SIS 安全生命周期阶段应重新评估。评估还需考虑：

——在执行停用活动过程中的功能安全；

——停用 SIS 对相邻操作单元和设施的影响。

18.2.4 影响分析的结果应用于编制安全计划以重新实施 IEC 61511 相关要求，包括重新验证和重新确认。

18.2.5 没有适当的文档支撑和审批授权，不得开始停用活动。

19 信息和文档要求

19.1 目的

本章目的是确保提供必要的信息并把这些信息文档化，以便：

——能有效地执行安全生命周期的所有阶段；

——能有效地执行验证、确认和功能安全评估活动。

19.2 要求

19.2.1 应向负责实现本文件要求的人员提供本文件要求的文档。

19.2.2 文档应：

——描述安装、系统或设备及其使用；

——准确和保持最新；

——容易理解；

——适合它所预定的目的；

——以一种可访问和可维护的形式提供，以确保相关文档能便捷而准确的识别、定位、检索和修订。

注：在第 14 章、第 15 章包含有对信息的更详细的要求。

19.2.3 文档应有唯一的标记以应对引用不同部分的可能。

19.2.4 文档应有表明信息类型的名称。

19.2.5 文档应可追溯到本文件的要求，包括危险和风险评估。

19.2.6 文档应有修订索引(例如，版本号)，以便能够识别信息的不同版本。

19.2.7 文档的结构应便于检索相关信息。应能够识别文档的最新修订(版本)。

注：文档的物理结构取决于许多因素，如系统的大小、复杂程度和组织要求。

19.2.8 所有相关文档都应被修订、补充、审查和批准，并处于适当的信息控制计划的控制之下。

19.2.9 应维护与下列各项有关的当前文档：

a) 危险和风险评估的结果及相关假设；

b) 用于 SIF 的设备及其安全要求；

c) 负责保持功能安全的组织；

d) 为达到和保持 SIS 功能安全所需的规程；

e) 17.2.5 中定义的修改信息；

f) 安全手册；

g) 设计、实现、测试和确认。

注：在 12.4.2、第 14 章、第 15 章和 16.3.3 中有更详细的要求。

参 考 文 献

[1] GB/T 2900.99—2016 电工术语 可信性(IEC 60050-192:2015,IDT)

[2] GB/T 20438.4—2017 电气/电子/可编程电子安全相关系统的功能安全 第4部分:定义和缩略语(IEC 61508-4:2010,IDT)

[3] ISO 9000:2005 Quality management systems—Fundamentals and vocabulary

[4] ISO 9001:2008 Quality management systems—Requirements

[5] ISO 13849-1:2006 Safety of machinery—Safety related parts of control systems—Part 1: General principles for design

[6] ISO 13849-2:2012 Safety of machinery—Safety related parts of control systems—Part 2: Validation

[7] ISO 14224:2016 Petroleum, petrochemical and natural gas industries- Collection and exchange of reliability and maintenance of data for equipment

[8] IEC 60300-3-2:2004 Dependability management—Part 3-2: Application guide—Collection of dependability data from the field

[9] IEC 60605-4:2001 Equipment reliability testing—Part 4: Statistical procedures for exponential distribution—Point estimates, confidence intervals, prediction intervals and tolerance intervals

[10] IEC 60617-12:1997 Graphical symbols for diagrams—Part 12: Binary logic elements

[11] IEC 61000-1-2:2016 Electromagnetic compatibility (EMC)—Part 1-2: General—Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena

[12] IEC 61025 Fault tree analysis (FTA)

[13] IEC 61131-3:2013 Programmable controllers—Part 3: Programming language

[14] IEC 61131-6:2012 Programmable controllers—Part 6: Functional Safety

[15] IEC 61506:1997 Industrial-process measurement and control—Documentation of application software

[16] IEC 61508 Functional safety of electrical/electronic/programmable electronic safety—Related systems

[17] IEC 61508-6:2010 Functional safety of electrical/electronic/programmable electronic safety related systems—Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

[18] IEC 61511-2: 2016 Functional safety—Safety instrumented systems for the process industry sector—Part 2: Guidelines for the application of IEC 61511-1

[19] IEC 61511-3:2016 Functional safety—Safety instrumented systems for the process industry sector—Part 3: Guidance for the determination of the required safety integrity levels

[20] IEC 61784-3:2017 Industrial communication networks—Profiles—Part 3: Functional safety fieldbuses—General rules and profile definitions

[21] IEC 62443-2-1:2010 Industrial communication networks—Network and system security—Part 2-1: Establishing an industrial automation and control system security program

[22] IEC 62682:2014 Management of alarms for the process industry

[23] ISO/IEC Guide 51:2014 Safety aspects—Guidelines for their inclusion in standards

[24] ISO/IEC 2382:2015 Information technology—Vocabulary

[25] ISO/IEC 2382-1:1993 Information technology—Vocabulary—Part 1:Fundamental terms

[26] ISO/IEC 27001:2013 Information technology—Security techniques—Information security man-

agement systems—Requirements

[27] ISO/IEC/IEEE 90003:2018 Software engineering—Guidelines for the application of ISO 9001:2015 to computer software

[28] ISO TR 12489:2013 Petroleum, petrochemical and natural gas industries—Reliability modelling and calculation of safety systems

[29] ISA TR 84.00.04:2015 第1部分 Guidelines for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511)

[30] ISA TR 84.00.09 Cybersecurity Related to the Functional Safety Lifecycle