



中华人民共和国国家标准

GB/T 21109.2—2023/IEC 61511-2:2016

代替 GB/T 21109.2—2007

过程工业领域安全仪表系统的功能安全 第2部分:GB/T 21109.1—2022的 应用指南

Functional safety of safety instrumented systems for the process industry sector—
Part 2: Guidelines for the application of GB/T 21109.1—2022

(IEC 61511-2:2016, Functional Safety—Safety instrumented
systems for the process industry sector—Part 2: Guidelines for
the application of IEC 61511-1:2016, IDT)

2023-03-17 发布

2023-10-01 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	IX
引言	XI
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
附录 A (资料性) GB/T 21109.1—2022 的指南	2
A.1 范围	2
A.2 规范性引用文件	2
A.3 术语和定义及缩略语	2
A.4 与 GB/T 21109.1—2022 的符合性	2
A.5 功能安全管理	2
A.5.1 目的	2
A.5.2 “要求”指南	2
A.6 安全生命周期要求	9
A.6.1 目的	9
A.6.2 “要求”指南	9
A.6.3 “应用程序 SIS 安全生命周期要求”指南	9
A.7 验证	11
A.7.1 目的	11
A.7.2 “要求”指南	11
A.8 过程危险和风险评估	12
A.8.1 目的	12
A.8.2 “要求”指南	12
A.9 给保护层分配安全功能	14
A.9.1 目的	14
A.9.2 “分配过程要求”指南	14
A.9.3 “基本过程控制系统作为保护层的要求”指南	16
A.9.4 “防止共因失效、共模失效和相关失效的要求”指南	17
A.10 安全要求规范(SRS)	18
A.10.1 目的	18
A.10.2 “一般要求”指南	18
A.10.3 “SIS 安全要求”指南	18
A.11 SIS 设计和工程	22
A.11.1 目的	22
A.11.2 “一般要求”指南	22
A.11.3 “检测到故障时的系统行为要求”指南	27
A.11.4 “硬件故障裕度”指南	27

A.11.5	“设备选择的要求”指南	29
A.11.6	现场设备	31
A.11.7	接口	31
A.11.8	“维护或测试设计要求”指南	33
A.11.9	“随机失效的量化”指南	34
A.12	SIS 应用程序开发	38
A.12.1	目的	38
A.12.2	“一般要求”指南	39
A.12.3	“应用程序设计”指南	39
A.12.4	“应用程序的实现”指南	42
A.12.5	“应用程序验证(审核和测试)要求”指南	42
A.12.6	“应用程序方法和工具的要求”指南	45
A.13	工厂验收测试(FAT)	46
A.13.1	目的	46
A.13.2	“建议”指南	47
A.14	SIS 安装和调试	47
A.14.1	目的	47
A.14.2	“要求”指南	47
A.15	SIS 安全确认	47
A.15.1	目的	47
A.15.2	“要求”指南	47
A.16	SIS 操作和维护	48
A.16.1	目的	48
A.16.2	“要求”指南	48
A.16.3	检验测试及检查	49
A.17	SIS 变更	51
A.17.1	目的	51
A.17.2	“要求”指南	51
A.18	SIS 停用	51
A.18.1	目的	51
A.18.2	“要求”指南	51
A.19	信息和文档要求	52
A.19.1	目的	52
A.19.2	“要求”指南	52
附录 B (资料性)	使用可靠性框图开发 SIS 逻辑解算器应用程序的示例	53
B.1	概述	53
B.2	应用程序开发和确认原理	54
B.3	应用描述	54
B.3.1	概述	54
B.3.2	过程描述	54
B.3.3	安全仪表功能	54
B.3.4	风险降低和多米诺效应影响	56
B.4	应用程序安全生命周期执行	56

B.4.1	概述	56
B.4.2	应用程序 SRS 开发的输入	56
B.4.3	应用程序设计和开发	59
B.4.4	应用程序的生成	70
B.4.5	应用程序验证和测试	71
B.4.6	确认	71
附录 C (资料性)	从 NP 技术转换为 PE 技术时的注意事项	72
附录 D (资料性)	如何从管道与仪表图(P&ID)演变成应用程序的示例	73
附录 E (资料性)	用于应用编程的方法和工具	76
E.1	用于应用编程的典型工具集	76
E.2	应用程序设计的规定和约束条件	77
E.3	用于应用编程的规则和约束条件	77
附录 F (资料性)	通过 SIS 项目示例针对使用继电器梯形图语言开发的应用程序的安全生命 周期每个阶段进行说明	79
F.1	概述	79
F.2	项目定义	79
F.2.1	概述	79
F.2.2	概念性计划	79
F.2.3	过程危险分析	80
F.3	简化工艺过程描述	80
F.4	初步设计	82
F.5	IEC 61511 应用	82
F.5.1	概述	82
F.5.2	第 F.1 步:危险和风险评估	85
F.5.3	危险识别	86
F.5.4	初步危险评价	86
F.5.5	事故历史	86
F.6	初步工艺过程设计的安全考虑	88
F.7	识别出的过程危险	88
F.8	工艺过程设计定义策略	89
F.9	初步危险评估	91
F.9.1	概述	91
F.9.2	步骤 F.2:安全功能分配	94
F.10	SIF 安全完整性等级确定	94
F.11	保护层分析(LOPA)应用实例	94
F.12	可容忍风险准则	96
F.13	步骤 F.3:SIS 安全要求规范	98
F.13.1	概述	98
F.13.2	输入要求	98
F.13.3	安全功能要求	98
F.13.4	安全完整性要求	100
F.14	功能描述和概念设计	100

F.14.1	反应器系统逻辑的说明	100
F.15	SIL 验证计算	101
F.16	应用程序要求	108
F.17	步骤 F.4: SIS 安全生命周期	115
F.18	技术和设备选择	115
F.18.1	概述	115
F.18.2	逻辑解算器	115
F.18.3	传感器	115
F.18.4	最终元件	116
F.18.5	电磁阀	116
F.18.6	紧急排放阀	116
F.18.7	调节阀	117
F.18.8	旁路阀	117
F.18.9	人机界面(HMI)	117
F.18.10	隔离	118
F.19	共因和系统性失效	118
F.19.1	概述	118
F.19.2	多样性	118
F.19.3	规格书错误	118
F.19.4	硬件设计错误	119
F.19.5	软件设计错误	119
F.19.6	环境过度应力	119
F.19.7	温度	119
F.19.8	湿度	119
F.19.9	污染物	120
F.19.10	振动	120
F.19.11	接地	120
F.19.12	电源线路调节	120
F.19.13	电磁兼容性(EMC)	120
F.19.14	动力源	121
F.19.15	传感器	121
F.19.16	工艺腐蚀或污垢	121
F.19.17	维护	121
F.19.18	误操作敏感性	121
F.19.19	SIS 架构	121
F.20	SIS 应用程序设计特性	123
F.21	配线实践	123
F.22	安防	123
F.23	步骤 F.5: SIS 安装、调试、确认	124
F.24	安装	124
F.25	调试	125
F.26	文档	125
F.27	确认	126

F.28	测试	126
F.29	步骤 F.6: SIS 操作和维护	137
F.30	步骤 F.7: SIS 变更	139
F.31	步骤 F.8: SIS 停用	139
F.32	步骤 F.9: SIS 验证	139
F.33	步骤 F.10: 功能安全管理和 SIS FSA	140
F.34	功能安全管理	140
F.34.1	概述	140
F.34.2	人员能力	140
F.35	功能安全评估	141
附录 G(资料性)	应用程序开发实践的指南	142
G.1	目的	142
G.2	一般安全应用编程属性	142
G.3	可靠性	142
G.3.1	概述	142
G.3.2	内存使用的可预测性	143
G.3.3	控制流的可预测性	143
G.3.4	考虑准确度和精度	145
G.3.5	时间特性的可预测性	146
G.4	数学或逻辑结果的可预测性	147
G.5	鲁棒性	147
G.5.1	概述	147
G.5.2	控制多样性的使用	147
G.5.3	控制异常处理的使用	149
G.5.4	检查输入和输出	149
G.6	可追溯性	150
G.6.1	概述	150
G.6.2	控制内置函数的使用	150
G.6.3	控制编译库的使用	150
G.7	可维护性	150
G.7.1	概述	150
G.7.2	可读性	151
G.7.3	数据抽象	153
G.7.4	功能内聚性	154
G.7.5	延展性	154
G.7.6	可移植性	154
参考文献		156
图 1	GB/T 21109 的整体框架	XII
图 A.1	应用程序 V 模型	10
图 A.2	BPCS 保护层和 BPCS 触发原因的独立性	17
图 A.3	分配给 BPCS 的两个保护层的独立性	17
图 A.4	系统、SIS 硬件和 SIS 应用程序的关系	21

图 A.5	可靠性参数的不确定度说明	37
图 A.6	70%置信度上限的图解	37
图 A.7	根据蒙特卡罗模拟得出的目标结果的典型概率分布	38
图 B.1	SIF 02.01 工艺流程图	55
图 B.2	SIF 06.02 工艺流程图	55
图 B.3	SIF02.01 和 SIF 06.02 的功能规范	57
图 B.4	SIF 02.01 硬件功能架构	57
图 B.5	SIF 06.02 硬件功能架构	58
图 B.6	从管道和仪表图中提取 SOV 的硬件规范	58
图 B.7	SIF 02.01 硬件物理架构	59
图 B.8	SIF 06.02 硬件物理架构	59
图 B.9	模型集成的层级结构	63
图 B.10	包括安全特性模型和 BPCS 逻辑模型的模型集成的层级结构	64
图 B.11	状态转换图	65
图 B.12	SOV 典型逻辑框图	66
图 B.13	SOV 典型逻辑模块框图	67
图 B.14	典型逻辑模块框图实现——BPCS 部分	68
图 B.15	SOV 应用程序典型逻辑模块实现——SIS 部分	69
图 B.16	用于最终实现模型检查的完整模型	70
图 D.1	油气分离器的 P&ID 示例	73
图 D.2	(一部分)ESD 因果图(C&E)的示例	74
图 D.3	安全 PLC 功能块编程中(一部分)应用程序的示例	75
图 F.1	简化流程图:PVC 工艺过程	81
图 F.2	SIS 安全生命周期阶段和 FSA 阶段	83
图 F.3	用于 PVC 反应器单元的初步 P&ID 示例	90
图 F.4	显示每个 SIS 设备 PFD_{avg} 的 SIF S-1 气泡图	103
图 F.5	S-1 故障树	104
图 F.6	显示每个 SIS 设备 PFD_{avg} 的 SIF S-2 气泡图	105
图 F.7	SIF S-2 故障树	106
图 F.8	显示每个 SIS 设备 PFD_{avg} 的 SIF S-3 气泡图	107
图 F.9	SIF S-3 故障树	108
图 F.10	PVC 反应器单元 SIF 的 P&ID	109
图 F.11	图例(第 1 页/共 5 页)	110
图 F.11	图例(第 2 页/共 5 页)	111
图 F.11	图例(第 3 页/共 5 页)	112
图 F.11	图例(第 4 页/共 5 页)	113
图 F.11	图例(第 5 页/共 5 页)	114
图 F.12	VCM 反应器的 SIS	122
表 B.1	操作模式规范	60
表 B.2	状态转换表	65
表 F.1	SIS 安全生命周期概述	84
表 F.2	SIS 安全生命周期——方框 1	85

表 F.3	氯乙烯的一些物理特性	87
表 F.4	假设分析/检查表	91
表 F.5	HAZOP	92
表 F.6	用于制定 SIF 策略的部分危险评估汇总	93
表 F.7	SIS 安全生命周期——方框 2	94
表 F.8	容许风险分级	96
表 F.9	VCM 反应器示例:基于完整性等级的 LOPA	96
表 F.10	SIS 安全生命周期——方框 3	98
表 F.11	安全仪表功能和 SIL	98
表 F.12	SIF 的 I/O 功能关系	99
表 F.13	SIS 传感器、正常运行范围 & 跳闸点	99
表 F.14	因果图	101
表 F.15	SIS 设备的 MTTFd	102
表 F.16	SIS 安全生命周期——方框 4	115
表 F.17	SIS 安全生命周期——方框 5	124
表 F.18	仪表类型及所使用的测试规程一览表	127
表 F.19	联锁检查规程旁路/模拟检查表	136
表 F.20	SIS 安全生命周期——方框 6	137
表 F.21	SIS 跳闸日志	137
表 F.22	SIS 设备失效日志	137
表 F.23	SIS 安全生命周期——方框 7	139
表 F.24	SIS 安全生命周期——方框 8	139
表 F.25	SIS 安全生命周期——方框 9	139
表 F.26	SIS 安全生命周期——方框 10	140

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 2 部分。GB/T 21109 已经发布了以下几个部分：

- 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—2022 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 21109.2—2007《过程工业领域安全仪表系统的功能安全 第 2 部分：GB/T 21109.1 的应用指南》，与 GB/T 21109.2—2007 相比，主要变化如下：

- 更改了原 GB/T 21109.2 的章、条号，在与 GB/T 21109.1 中对应的章、条号一致的前提下，前面加有符号“A”（见附录 A，更改了旧版的第 1 章～第 19 章）；
- 更改了 A.12 的内容，将原来应用软件要求，包括工具软件的选择准则更改为 SIS 应用程序开发的内容（见附录 A.12，2007 年版的第 12 章）；
- 删除了原附录 A 计算一个仪表安全功能要求时的失效概率的技术示例（见 2007 年版的附录 A）；
- 更改了附录 B 的内容，将原来附录 B 典型的 SIS 结构开发更改为使用可靠性框图开发 SIS 逻辑解算器应用程序的示例（见附录 B，2007 年版的附录 B）；
- 更改了附录 C 的内容，将原来附录 C 安全 PLC 的应用特征更改为从 NP 技术转换为 PE 技术时的注意事项（见附录 C，2007 年版的附录 C）；
- 更改了附录 D 的内容，将原来附录 D SIS 逻辑解算器应用软件开发方法的示例更改为如何从管道与仪表图（P&ID）演变成应用程序的示例（见附录 D，2007 年版的附录 D）；
- 更改了附录 E 的内容，将原来附录 E 开发安全配置的 PE 逻辑解算器的外配诊断程序的示例更改为用于应用编程的方法和工具（见附录 E，2007 年版的附录 E）；
- 增加了附录 F：SIS 项目示例说明使用继电器梯形图语言开发应用程序的安全生命周期每个阶段（见附录 F）；
- 增加了附录 G：应用程序开发实践的指南（见附录 G）。

本文件等同采用 IEC 61511-2:2016《功能安全 过程工业领域安全仪表系统 第 2 部分：IEC 61511-1:2016 的应用指南》。

本文件做了下列最小限度的编辑性改动：

- 将标准名称改为《过程工业领域安全仪表系统的功能安全 第 2 部分：GB/T 21109.1—2022 的应用指南》。

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(SAC/TC 124)归口。

本文件起草单位：机械工业仪器仪表综合技术经济研究所、国家管网集团西南管道有限责任公司、中国石油集团安全环保技术研究院有限公司、北京龙鼎源科技股份有限公司、上海辰竹仪表有限公司、北京京仪集团有限责任公司、杭州盘古自动化系统有限公司、北京联合普肯工程技术股份有限公司、济南市长清计算机应用公司、济南宁通自动化技术有限公司。

GB/T 21109.2—2023/IEC 61511-2:2016

本文件主要起草人：刘瑶、史学玲、周有铮、李玉明、徐德腾、张韬、张建国、朱明露、裘坤、熊文泽、张艾森、魏振强、陈小华、孙文勇、吴祚祥、靳江红、王玥、张新国、沈玉富、杨柳、姜荣怀、钱福群、周婷、韩占武、马欣欣、帅冰、王莉、张洪、俞文光、程相国、左新、朱弘毅、聂中文、田雨聪、李秋娟、施隋靖、朱旭营、陈红新。

本文件及其所代替文件的历次版本发布情况为：

——2007年首次发布为 GB/T 21109.2—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 拟包括以下几部分:

- 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—2022 的应用指南。目的是提供按 GB/T 21109.1—2022 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。

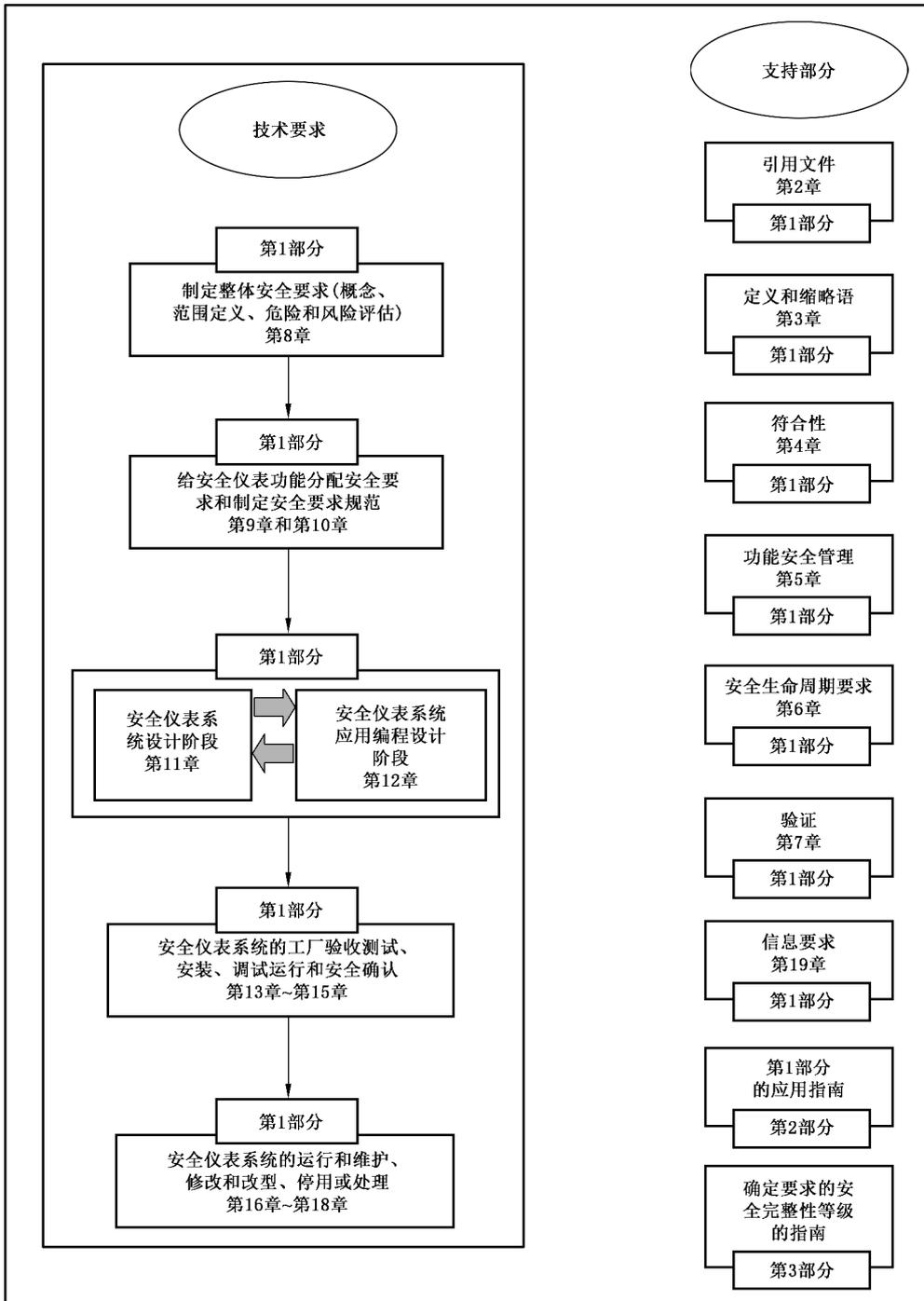


图 1 GB/T 21109 的整体框架

过程工业领域安全仪表系统的功能安全

第 2 部分:GB/T 21109.1—2022 的 应用指南

1 范围

本文件提供了按 GB/T 21109.1—2022 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。

注 1: 附录 A(资料性)已进行整理,其章条号除前面加有符号“A”外,其余与 GB/T 21109.1—2022 中对应的章、条号一致。

注 2: 附录 A 包含 GB/T 21109.2—2007 正文中的材料,这样做是为了防止出现标准正文均为资料性条款的情况,以符合标准编写规则。

注 3: 为了使本文件最大化利用:

——在使用特定条款指南时也需要同时回看所属章节指南(例如:当查看 5.2.6.1.3 的指南时,也要考虑 5.2.6 的指南);

——在特定条款无相关指南时(例如:未提供进一步指南),在适用时可考虑回看章节指南。

注 4: 本文件附录中给出的示例仅仅是在具体情况下实施 GB/T 21109 要求的特定例子,用户可根据自己的情况选择适用的方法和技术。

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 21109.1—2022 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(IEC 61511-1:2016, IDT)

3 术语、定义和缩略语

GB/T 21109.1—2022 界定的术语、定义和缩略语适用于本文件。