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

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。

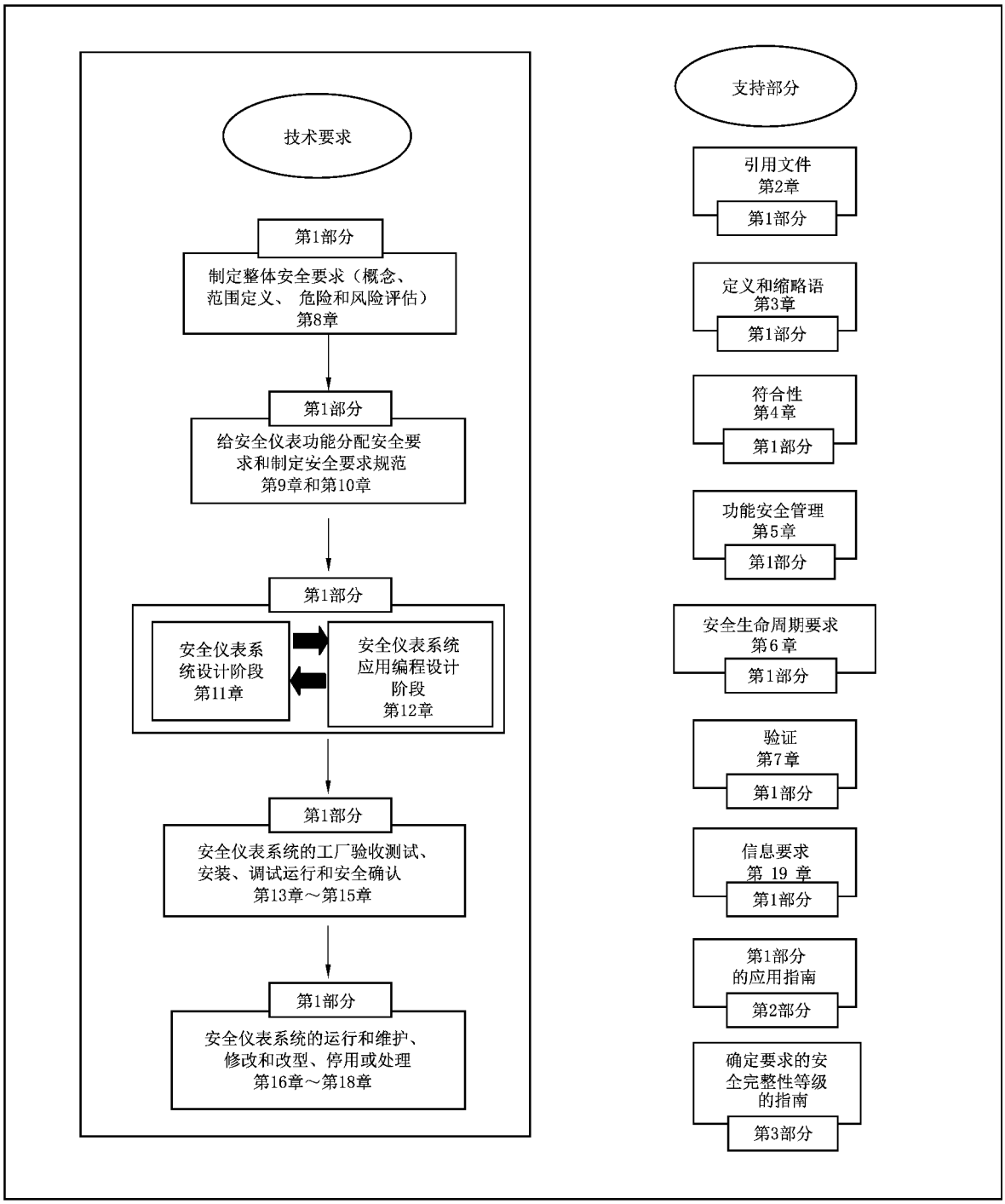


图 1　GB/T 21109 的整体框架

# 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);