ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 45111—2024

保护层分析(LOPA)、安全完整性等级(SIL)定级和验证质量控制导则

Quality control guidelines for layer of protection analysis(LOPA), safety integrity levels(SIL)determination and verification

2024-12-31 发布　　2025-07-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

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、中国石油集团安全环保技术研究院有限公司、国能(连江)港电有限公司、上海燃气工程设计研究有限公司、中国电力工程顾问集团华北电力设计院有限公司、梅思安(中国)安全设备有限公司、中控技术股份有限公司、辽宁美卓伦检测技术有限公司、上海歌略软件科技有限公司。

本文件主要起草人：刘瑶、帅冰、徐德腾、史学玲、黄步余、董秀娟、朱明露、魏振强、唐彬、吕峰、陈小华、范咏峰、施隋靖、俞文光、朱旭营、李秋娟、李旺、王巨洪、孙勇、孙永康、严晓生、孙舒、周卫、张作本、谢亚莲、于世恒、马铁量、李玉明、马云鹏、钱福群、杨敏文、张雪、王晓鹏、曹欣宜、周力、聂中文、马欣欣、赵焱、孙文勇、史威、刁宇、姜志成、吕智嘉、熊文泽、雷柏伟、朱杰、赵俊丹、杜康、魏娟、相桂生、靳江红、姜念琛、孙炜、孟邹清、杨柳、朱弘毅、陈祖志、闫炳均、任军民、陈军松、张益南、刘东、李志勇、杨绍军。

引　言

随着GB/T 20438(所有部分)和GB/T 21109(所有部分)的广泛应用,功能安全概念得到有效普及。在石油、天然气、化工、电力等行业,功能安全研究的是如何确保包括安全仪表系统(SIS)在内的保护层实现足够的风险管控能力。SIS执行安全仪表功能(SIF)的可信性用安全完整性表示,其安全完整性能力用安全完整性等级(SIL)表征。

本文件中提到的危险与风险分析,其目的是全面识别系统中潜在的危险及操作性问题,一般为定性分析,在基本工艺流程设计完成后即可开展。常见的分析方法有:危险与可操作性分析(HAZOP)、故障树分析(FTA)、检查表、失效模式和影响分析(FMEA)。

在工程实践中,对于危险与风险分析中识别出的高风险点和重要控制点一般需开展进一步的半定量分析,以确认设置有足够的保护层,保护层分析(LOPA)即为常用的半定量风险分析方法,在LOPA工作过程中,将针对风险场景识别已设置或应设置的保护层分配降险能力,若涉及SIF,则需为SIF确定相应的SIL要求,此过程即为SIL定级。

SIL验证的目的是通过定量计算及必要时的定性分析,从硬件安全完整性和系统性安全完整性两方面确认SIF配置满足SIL定级提出的SIL要求,常见的SIL验证方法有:可靠性框图法、故障树法、马尔可夫法等。一般在完成SIS设计后开展SIL验证,以确保SIS配置满足安全要求。

在操作和维护阶段需要通过定期的功能安全评估(包括危险与风险分析、SIL定级、SIL验证等)确认SIS执行的SIF可维持相应的SIL能力。

通过本文件的制定,为各行业开展LOPA工作、SIL定级和验证工作提供审查依据,指导企业对LOPA工作、SIL定级和验证过程实现质量控制,提升运行风险管控水平。

保护层分析(LOPA)、安全完整性等级(SIL)定级和验证质量控制导则

1 范围

本文件明确了保护层分析(LOPA)与安全完整性等级(SIL)定级、SIL 验证间的关系,规定了 LOPA 工作、SIL 定级和 SIL 验证的质量控制要素、质量控制要求和质量控制审查要求。

注:本文件中 SIL 定级特指使用 LOPA 方法开展的 SIL 定级工作。

本文件适用于 LOPA、SIL 定级和验证的质量控制。

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 20438(所有部分) 电气/电子/可编程电子安全相关系统的功能安全

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

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

GB/T 21109(所有部分) 过程工业领域安全仪表系统的功能安全

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

GB/T 32857—2016 保护层分析(LOPA)应用指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

场景 scenario

可能导致不期望后果的一种事件或事件序列。

[来源:GB/T 32857—2016,3.1.9]

3.2

初始事件 initial event

使事故序列开始扩展所需的失效或错误的最小组合。

注:一般由一个单独的初始原因、多个原因或有使能条件的初始原因组成。有些情况下初始事件也可能是由同一时间发生的两种不同初始原因构成的。

3.3

中间事件 intermediate event

初始事件发展成后果之前的关键事件。

注:通常是一个能被检测到的事件,如某压力容器压力高、某储罐液位高。需要指出的是,特殊场景可能由初始事件直接发展成为不良后果,不存在中间事件。