ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 32857—2025
代替 GB/T 32857—2016

保护层分析(LOPA)应用导则

Application directives for layer of protection analysis(LOPA)

2025-12-02 发布　　2026-07-01 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。

本文件代替GB/T 32857—2016《保护层分析（LOPA）应用指南》，与GB/T 32857—2016相比，除结构调整和编辑性改动外，主要技术变化如下：

——增加了条件修正因子（见3.2）、原始风险（见3.5）、中间事件（见3.7）、残余风险（见3.12）、风险点（见3.13）、风险降低因子（见3.14）、复合场景（见3.16）、安全仪表功能（见3.17）、（SIF的）运行模式（见3.20）、安全关键动作（见3.21）等10个术语和定义；

——更改了基本过程控制系统（见3.1，2016年版的3.1.2）、使能事件或使能条件（见3.4，2016年版的3.1.12）、初始事件（见3.6，2016年版的3.1.5）、保护层分析（见3.8，2016年版的3.1.1）、保护层（见3.9，2016年版的3.1.3）、独立保护层（见3.10，2016年版的3.1.7）、安全完整性等级（见3.18，2016年版的3.1.11）、安全仪表系统（见3.19，2016年版的3.1.13）、可容忍风险（见3.22，2016年版的3.1.18）等9个术语和定义；

——删除了事件（见2016年版的3.1.4）、频率（见2016年版的3.1.6）、共因失效（见2016年版的3.1.14）等3个术语和定义；

——增加了保护层分析（LOPA）的基本要求（见5.2）、应用范围（见5.3）、人员要求（见5.4）；

——增加了在工程实践中LOPA可选择单一场景分析法或复合场景分析法的描述及适用情况（见第6章）；

——增加了风险点识别的来源（见7.1）；

——更改了场景识别的来源（见7.2.2，2016年版的6.1.2）、场景筛选的规则（见7.2.3，2016年版的6.1.3）；

——增加了场景补充要求（见7.2.4）；

——更改了后果及严重性评估的要求（见7.3，2016年版的6.2）；

——更改了初始事件分类（见表1，2016年版的表2）；

——增加了初始事件频率确认依据（见7.4.3）；

——增加了使能条件确认要求（见7.5）；

——增加了条件修正因子确认要求（见7.6）；

——更改了独立保护层识别要求（见7.7.1，2016年版的6.4.3）和独立保护层PFD的确认要求（7.7.2，2016年版的6.4.4）；

——更改了单一场景分析法后果频率的计算（见7.8，2016年版的6.5）；

——增加了复合场景分析法后果频率的计算（见7.9）；

——更改了风险评估与建议的内容（见7.10，2016年版的6.6）。

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、中石化国家石化项目风险评估技术中心有限公司、中国寰球工程有限公司、南京南瑞继保工程技术有限公司、中科合成油技术有限公司、北京风

控工程技术股份有限公司、天津保泰安全技术服务有限公司、北京联合普肯工程技术股份有限公司。

本文件主要起草人：刘瑶、帅冰、王建伟、王雪梅、范咏峰、袁小军、孙舒、朱明露、施隋靖、娄清辉、肖松青、乔靖玉、史学玲、程泱、包伟华、张少华、刘飞舟、姜巍巍、张武涛、葛春涛、徐德腾、孙勇、吕峰、马欣欣、妥少辉、韩占武、杨柳、李秋娟、刁宇、朱旭营、王杰、张炜、赵俊丹、赵焱、薛永刚、张雪、朱弘毅、王哲蓓、刘万里、孙爱、熊文泽。

本文件及其所代替文件的历次版本发布情况为：

——2016 年首次发布为 GB/T 32857—2016；

——本次为第一次修订。

引　言

本文件的目的是描述保护层分析(LOPA)的原理和分析过程,为应用 LOPA 方法开展危险分析与风险评估提供适当的指南和参考。保护层分析方法是一种半定量的风险评估方法,它通过分析保护层的要求时危险失效概率来判断现有保护层是否可以将特定场景下的风险降低到可容忍风险标准所要求的水平。它的优点如下。

- 与定性方法相比较,LOPA 可提供相对量化的风险决策依据,避免主观因素对风险控制决策的影响。
- 虽然没有定量风险分析那么精确,但其过程简便。在定量分析工作之前,可应用 LOPA 方法对风险相对较高的场景进行筛选,从而提高整个风险分析的工作的效率,节约分析工作的成本。
- LOPA 是安全完整性等级(SIL)的重要评估工具,与图表法相比较,LOPA 可提供更加准确的结果。
- 通过 LOPA,可了解不同独立保护层在降低风险过程中的贡献,在此基础上,可选择更加经济合理的保护措施来降低风险。
- LOPA 通常采用表格的形式记录评估的过程,记录过程符合通常的思维习惯,文件易读易用。

通过 LOPA,可发现可行方案,如增设其他保护层、改变工艺等,从而选择最经济有效的降低危险性的措施。

LOPA 方法,作为一种简化的半定量的风险评估方法,使得对场景的分析比其他定量风险分析方法更省时间和精力,更重要的是,它提供了识别场景风险的方法,并且将其与可容忍风险比较,以确定现有的安全措施是否合适,是否需要增加新的安全措施。LOPA 通过展开分析场景的全过程,能很好地识别中间事件、安全措施和事故后果,帮助分析人员全面了解、认识特定的场景。

LOPA 也存在其不足之处。与定性分析方法相比较,它每次只是针对一起特定的场景进行分析,不能反映各种场景之间相互影响。此外,初始事件的发生频率及独立保护层的要求时危险失效概率等数据对 LOPA 的结果有很大的影响,需要付出很多努力和积累才能获取这些数据。

这种半定量的风险评估方法既可以减少定性分析方法的主观性,又较定量分析方法更容易实行,在风险评估中越来越广泛地被应用。

保护层分析(LOPA)应用导则

1 范围

本文件规定了保护层分析(LOPA)的一般要求、基本程序、分析过程以及文档要求。

本文件适用于指导各行业开展保护层分析工作。

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 20438.4—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

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

3 术语和定义

GB/T 20438.4—2017 和 GB/T 21109.1—2022 界定的以及下列术语和定义适用于本文件。

3.1

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通常支持执行多种功能,如过程控制功能、监视、报警。

[来源:GB/T 21109.1—2022,3.2.3]

3.2

条件修正因子 conditional modifiers

场景风险计算时使用的可能性概率之一。

注:通常表现为影响后果(例如:人员伤亡、点火概率、致死率)而不是主要损失事件后果(例如:泄漏、容器破裂)时使用。

3.3

后果 consequence

某一特定事件的结果。

注:通常包括人员伤亡、财产损失、环境污染、声誉影响等。

3.4

使能事件或使能条件 enable event/enable condition

不直接导致场景后果发生的事件或条件。

注:是使初始事件转变为场景后果的某种必要的操作状态或条件。