ICS 25.040
N 10

中华人民共和国国家标准

GB/T 32857—2016

保护层分析(LOPA)应用指南

Application guide for layer of protection analysis(LOPA)

2016-08-29 发布　　2017-03-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由中国机械工业联合会提出。

本标准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。

本标准起草单位:机械工业仪器仪表综合技术经济研究所、北京联合普肯工程技术有限公司、中国安全生产科学研究院、风控(北京)工程技术有限公司、中国石油天然气管道工程有限公司、中国石油天然气股份有限公司管道分公司、天津市居安企业管理咨询有限公司、中海油安全技术服务有限公司、上海撷果商务咨询有限公司。

本标准主要起草人:孟邹清、肖松青、俞文光、赵劲松、唐彬、袁小军、方来华、帅冰、聂中文、刘瑞、左信、张宝利、赵建民、刘瑶、程德发、游泽彬、许琛琛、史威、李秋娟、顾峥、周有铮、孙舒、靳江红。

引　言

本标准的目的是描述保护层分析(LOPA)的原理和分析过程,为应用 LOPA 分析方法开展风险分析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价方法,它通过评价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风险标准所要求的水平,它的优点是:

- 与定性分析相比较,LOPA 分析可以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,可以应用 LOPA 分析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 分析是安全完整性等级(SIL)的重要评估工具,与图表法相比较,LOPA 分析可以提供更加准确的结果。
- 通过 LOPA 分析,可以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,可以选择更加经济合理的保护措施来降低风险。
- LOPA 分析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。

通过保护层分析,可以发现可行方案,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 分析方法,作为一种简化的半定量的风险评价方法,使得对场景的分析和评价比其他定量风险评价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,并且将其与可容许风险比较,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 分析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 分析也存在其不足之处。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 分析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价方法可以减少定性评价方法的主观性,且较完全的定量评价方法容易实行,在风险评估中被越来越广泛地应用。

保护层分析(LOPA)应用指南

1 范围

本标准规定了LOPA分析的相关策略和细则,包括LOPA分析方法的技术性说明及开展LOPA分析时的组织工作的要求,如准备工作、分析会议、分析报告及建议项跟踪等环节的要求,并给出在过程工业中不同应用的示例。

本标准适用于过程工业开展的保护层分析,其他行业也可参照使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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 20002.4—2015 标准中特定内容的起草 第4部分:标准中涉及安全的内容

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

IEC 61508-4:2010 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(Functional safety of electrical/electronic/programmable electronic safety-realted systems—Part 4: Definitions and abbreviations)

3 术语和定义、缩略语

3.1 术语和定义

GB/T 20002.4、GB/T 21109.1和IEC 61508-4界定的以及下列术语和定义适用于本文件。

3.1.1

保护层分析 layer of protection analysis;LOPA

对降低不期望事件频率或后果严重性的独立保护层的有效性进行评估的一种过程方法或系统。

3.1.2

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

对来自过程的、系统相关设备的、其他可编程系统的和/或某个操作员的输入信号进行响应,并产生使过程和系统相关设备按要求方式运行的系统,但它并不执行任何具有被声明的SIL≥1的仪表安全功能。

注:对于过程领域而言,基本过程控制系统是一个全局性的术语。

3.1.3

保护层 layer of protect

用来防止不期望事件的发生或降低不期望事件后果严重性从而降低过程风险的设备、设施或方案。

3.1.4

事件 event

过程中发生的、可能由于设备能力或人员行动或影响风险控制系统的外部因素引起的过程事件。