WILEY

Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis

保护层分析：使能条件与修正因子导则

[美] 化工过程安全中心（CCPS） 著

鲁 毅 冯双虎
刘昳蓉 孔令仪 译

袁小军 校

化学工业出版社

Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis

保护层分析：使能条件与修正因子导则

[美] 化工过程安全中心（CCPS） 著

鲁 毅 冯双虎
刘昳蓉 孔令仪 译

袁小军 校

化学工业出版社

·北京·

自 IEC61508/IEC61511 这两个功能安全相关标准在 2000 年及 2003 年发布后，以工艺危害分析为基础的 SIL 评估已经成为流程工业的一个重要技术风险管理手段。本书不是简单地给出了功能安全仪表的工程规定，而是积累比对各大国际石油公司或化工公司的相关 SIL 评估规则，通过对使能条件与修正因子的分类，在更高的层次上梳理了如何去合理地应用规则。

本书能够帮助业主单位编制更符合本公司风险管理策略的 SIL 评估执行程序，亦能够帮助工程公司及咨询评估单位更加细致准确地把握 LOPA 分析中的规则。

图书在版编目(CIP)数据

保护层分析：使能条件与修正因子导则/[美] 化工过程安全中心（CCPS）著；鲁毅等译．—北京：化学工业出版社，2015.4

书名原文：Guidelines for enabling conditions and conditional modifiers in layer of protection analysis

ISBN 978-7-122-22973-1

Ⅰ.①保… Ⅱ.①化… ②鲁… Ⅲ.①化工过程-风险分析 Ⅳ.①TQ02

中国版本图书馆 CIP 数据核字（2015）第 026380 号

Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis by Center for Chemical Process Safety.

ISBN 978-1-118-77793-0

北京市版权局著作权合同登记号：01-2014-1273

责任编辑：赵玉清　　文字编辑：徐雪华
责任校对：王　静　　装帧设计：关　飞

出版发行：化学工业出版社（北京市东城区青年湖南街 13 号　邮政编码 100011）
印　　刷：北京永鑫印刷有限责任公司
装　　订：三河市胜利装订厂
710mm×1000mm　1/16　印张 7½　字数 87 千字
2015 年 6 月北京第 1 版第 1 次印刷

购书咨询：010-64518888（传真：010-64519686）　售后服务：010-64518899
网　　址：http://www.cip.com.cn
凡购买本书，如有缺损质量问题，本社销售中心负责调换。

定　价：50.00 元

译者前言

自 IEC61508/IEC61511 这两个功能安全相关标准在 2000 年及 2003 年发布后，以工艺危害分析为基础的 SIL 评估已经成为流程工业的一个重要技术风险管理手段。本书的译者们在过去十年中为大量流程工业新建与在役装置提供了 SIL 定级、验算、认证等服务。译者发现工程公司、业主单位、设备供应商，甚至每个评估人员在 SIL 定级中，对规则的理解与把握都可能大相径庭，以至于带来完全不同的 SIL 定级与评估结果。

译者通过不断积累比对各大国际石油公司或化工公司的相关 SIL 评估规则，并关注其在过去十年中的变化，看到了整个流程工业为提高安全性与可用性所做出的努力。但是这些规则之间的差异甚至是矛盾，有时也会给评估人员带来困扰。

2013 年年底，CCPS 预告将发布一个与 LOPA 保护层规则相关的新导则，风控工程第一时间引进了这个导则。经过一年时间的翻译，《保护层分析：使能条件与修正因子导则》一书终于完成。本书不是简单地给出了功能安全仪表的工程规定，而是通过对使能条件与修正因子的分类，在更高的层次上梳理了如何去合理地应用规则。

译者在本书的作者名单中还发现了来自雪佛龙菲利普斯化工公司的熟悉名字，某些章节的内容仿佛把译者带回了几年前执行 HAZOP/LOPA 分析的那段有趣日子。

希望本书能够帮助业主单位编制更符合本公司风险管理策略的 SIL 评估执行程序，亦能够帮助工程公司及咨询评估单位更加细致准确地把握 LOPA 分析中的规则。

这些规则虽然拗口且不易理解，但它带来了国际石油与化工公司的

多年经验积累，这让我们这些从业者更加坚信我们是走在一条正确的道路上。

感谢风控工程的译者们，你们在繁忙的工作之余，投入自己的时间和热情。安佰芳、江琦良、朱海奇、宫业青、陈维东等都对本书的翻译做出了贡献。时光荏苒你们已经或正在成为行业中的佼佼者，与你们成为同事我深感荣幸。

鲁　毅

风控（北京）工程技术有限公司　www. irc-risk. com

2014 年 12 月

本书是化工过程安全中心出版的过程安全导则概念系列图书中的一本，其他书籍名单可登陆 www. wiley. com/go/ccps 进行查看。

我们真诚地希望这本书中所涉及的内容，能够在整个化工行业安全领域留下浓墨重彩的一笔。美国化学工程师协会和化工过程安全中心技术委员会及附属委员会成员、其所有员工和相关承包商，均为本书的编制提供了直接或间接的帮助。他们的工作提高了本书的准确度和清晰度。美国化学工程师学会，其顾问——CCPS 技术指导委员会及其分委员会的委员，这些委员的雇主——高级管理人员和董事，或 Unwin 公司及其雇员均不担保或代表本书内容的准确性或正确性。本书的用户对本书的使用或滥用所产生的任何后果承担法律责任。

缩　写

AEGL　Acute Exposure Guideline Level 急性暴露指导浓度

AIChE　American Institute of Chemical Engineers 美国化学工程师协会

AIHA　American Industrial Hygiene Association 美国工业卫生协会

API　American Petroleum Institute 美国石油协会

BPCS　Basic Process Control System 基本工艺控制系统

CCPS　AIChE Center for Chemical Process Safety 美国化学工程师协会化工过程安全中心

CPI　Chemical Process Industry 化工行业

CPQRA　Chemical Process Quantitative Risk Analysis 化工过程定量风险分析

DDT　Deflagration-to-detonation Transition 爆燃转爆轰过程

DTL　Dangerous Toxic Load 危险毒性荷载终点指标

EPA　U. S. Environmental Protection Agency 美国环境保护局

ERPG　Emergency Response Planning Guideline 应急响应预案导则

ETA　Event Tree Analysis 事件树分析

FMEA　Failure Modes and Effects Analysis 失效模式及影响分析

FMECA　Failure Modes, Effects, and Criticality Analysis 失效模式、影响与关键性分析

FTA　Failure Tree Analysis 故障树分析

HAZOP　Hazard and Operability [Study] 危险及可操作性分析

IDLH　Immediately Dangerous to Life and Health 立即危害生命和

健康终点指标

IPL Independent Protection Layer 独立保护层

LC_{LO} Lethal Concentration, Low 最小致死浓度

LC_{50} Lethal Concentration, 50%mortality 半数致死浓度

LOPA Layer of-Protection Analysis 保护层分析

LOPC Loss of Primary Containment 主要存储设施损失

MAWP Maximum Allowable Working Pressure 最大许可工作压力

NFPA National Fire Protection Association 美国国家消防协会

P Probability (Dimensionless) 概率（无量纲）

PFD Probability of Failure on Demand 需求时失效概率

PSV Pressure Safety Valve 安全阀

RV Relief Valve 泄压阀

SIF Safety Instrumented Function 安全仪表功能

SIS Safety instrumented system 安全仪表系统

SLOD Significant Likelihood of Death 显著死亡概率

SLOT Specified Level of Toxicity 特定毒性水平

U. K. United Kingdom 英国

U. S. United States 美国

名词解释

异常工况：装置运行中可能导致工艺偏离其正常工况的一个或一系列扰动。在危害评估程序中，与偏离含义一致。

管理控制：指导和/或检查与装置操作相关的工程系统或操作人员绩效的程序要求。

可审核性：可通过检查相关信息、文件以及程序来确认其设计、检验、维护、测试以及操作实践可以实现其核心功能的充分性及一致性。

自燃点：一种可燃物/氧化剂的混合物，在不存在其他点火源的情况下，在某一指定测试条件下自发燃烧的最低温度。

基本工艺控制系统（BPCS）：根据来自工艺信息及其相关设备、其他编程系统的输入信号，和/或来自操作人员提供的输入信号进行响应（逻辑解算），产生相应的输出信号，并在正常生产终点指标内对工艺及其相关设备进行操作调整，使其满足设计要求的控制系统。

原因：在危害评估程序中，与初始事件含义一致。

共因失效：由单一事件或特定工况导致两个或两个以上的失效场景同时发生。

（条件）修正因子：一种或几种在场景风险计算时使用的可能性概率，通常在风险可接受标准表现为影响后果时（例如：人身伤亡）而不是主要损失事件后果（例如：泄漏、管道破裂）时使用。修正因子包括但不仅限于：危险环境概率，点火概率，爆炸概率，人员暴露概率，伤亡概率，以及设备损坏或其他经济损失概率。

后果：某一特定事件的结果。在定性危害评估程序中，后果是指由

初始事件导致的影响，包括损失事件，有些时候甚至包括损失事件造成的影响。在定量风险分析中，后果指的是损失事件造成的物理性影响，通常包括火灾、爆炸，或者是有毒/腐蚀性物料泄漏。

后果分析：独立于频率或概率分析的可预期事故后果影响分析。

泄漏防护措施：通过主要工艺设施、基本工艺控制系统、操作程序及培训等措施，将工艺流程中的物料和能量保持在工艺设施内，并且使工艺流程处于设计和运行的安全范围内，从而避免发生异常工况和泄漏事件及其可能导致的损失、破坏和人员伤亡。

化工过程定量风险分析（CPQRA）：首先对工艺过程中的危害进行辨识，然后定量评估事故发生的可能性及后果的严重性，对化工行业来说，经常将可能性及严重性组合成风险进行度量。CPQRA 特别适用于偶然事件。它类似于核工业上常用的定量方法——概率风险评估（PRA），但是不尽相同。

偏离：操作条件超出了设计条件范围、安全操作条件范围或标准操作程序的要求。

使能条件：某个并不是失效、错误或者保护层但却是将事故序列转变为最终结果的必须条件。它是由一个不直接导致事故场景的条件或者操作阶段组成，但是它是事故场景转变为损失事件的必要条件；表示为无量纲的概率。

使能事件：使能条件的另一个专业名称。一般来说“使能条件”的名称较为恰当，因为使能条件通常指的不是事件，而更接近于一种条件状态。

终点指标：在 LOPA 或 QRA 中考虑的事故场景的最大范围。根据所采用分析方法的不同，终点指标可以用一种物料或能源的泄放量、定性的潜在损失和危害影响类别、带有/无修正因子的量化影响等级，或者全定量的损失和危害影响来表示。

偶然事件：一段时限内发生的非预期事件，通常与事故有关。

非连续泄漏：一段时限内的泄漏，通常与事故有关。

事件：由设备性能或人员操作或外部事件导致的与工艺相关的场景。事件包括初始事件、损失事件以及保护措施成功或失效。

事件序列：见事故序列。

事件树：一种通过图形的方式来表示事故序列里事件和环境的逻辑相关性，常用来分析事故形成过程。

外部事件：外部事件包括：（1）自然灾害，例如地震、洪水、龙卷风、极端环境温度、闪电等；（2）人为事故，例如飞机失事、导弹、附近工业事故、火灾、恶意损坏等；（3）公用工程中断，例如电力或工厂风。

失效：系统预期性能与实际性能间的不可接受的差距。

失效模式：可用来识别设备失效的事件或条件。失效模式包括安全功能失效、安全功能动作过早或误动作（多余动作）、超过设计终点指标或者某种物理状态（如检验时发现泄漏）。

失效模式与影响分析（FMEA）：一种系统的、表格式的分析方法，用来评估和记录设备部件各种类型的失效造成的影响。

失效模式、影响与关键性分析（FMECA）：FMEA 的一个变种，包括失效模式的潜在严重性后果的评估。

故障树：一种图形化的逻辑模型，用来描述可能导致某个特定的主要失效或事件（顶上事件）的多个失效事件组合及其逻辑关系。

频率：在指定单位时间内，某一事件发生或预期发生的次数。

危害：可能对人员、财产和/或环境造成潜在损害的一种物理或化学状态。

危险与可操作性分析（HAZOP）：一种基于场景的危险评估程序，在一个团队里使用一系列引导词来识别设计或程序操作时可能出现的偏差，然后审查偏差可能导致的潜在的后果以及确保目前存在足够的安全

措施。

危害评估：辨识某个系统中的个人危害，确定可能导致非预期事件的机理，并评估这些非预期事件在安全（包括公众安全）、环境及财产方面可能造成的影响。危害评估通常是以定性方法来判断装置设计及操作中可能导致事故的薄弱环节。

危害辨识：在事故发生时对可能造成非预期后果的物料、系统、工艺及装置特性的总结。

危害事件：见损失事件。

HAZOP/LOPA 分析：HAZOP/LOPA 分析是 HAZOP 分析的一种扩展，包括：选择 HAZOP 分析识别出的场景进行 LOPA 分析；评估初始事件频率，后果严重性以及独立保护层的有效性（通常表示为频率/后果消减因子）；在评估场景风险时考虑适当的使能条件和/或修正因子；将评估出的场景风险与风险可接受标准相比较以确定现有风险控制措施是否充分。

人员失误：任何超过系统定义的允许范围的人员行动（或行动缺失）。包括可能导致事故的设计人员、操作人员与管理人员失误。

影响：对失效事件最终损失及危害的衡量。影响可表现为受伤和/或死亡的人数，环境污染的范围和/或财产损失、物料泄漏、生产中断，市场份额损失和复原成本。

事故：会导致或可能导致不利影响的意外事件或事件序列。

事故序列：由初始事件和导致非预期后果的中间事件组成的一系列事件。

独立保护层（IPL）：能防止某个场景向非预期后果发展的一种设备、系统或行动，并且独立于指定场景的初始事件或其他任何保护层。

初始原因：在危害评估程序中，初始原因是事故序列中的首个事件，通常包括操作失误、机械故障或外部事件/影响等。初始原因标识了系统从正常状态向非正常状态的转变。

初始事件：使事故序列开始扩展所需的失效或错误的最小组合。它可以由一个单独的初始原因、多个原因或带有使能条件中的初始原因组成。（初始事件是保护层分析中的常用词，用来表示初始原因或初始原因及其造成直接影响的集合，比如“BPCS 失效导致的反应进料流量过高”。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，可参见附件 A 中关于特殊场景的讨论。）

中间事件：在事故序列中发生在初始事件之后、损失事件之前的事件。

保护层：依托于一套管理系统、能够阻止场景向非预期后果发展的设备、系统或行动。

保护层分析（LOPA）：保护层分析是一种同一时间对单一事故场景（原因-后果配对）进行分析的方法，使用预设的初始事件频率值，独立保护层失效概率以及后果严重性来评估场景的风险，再将场景风险与风险可接受标准进行比较，决定是否需要采取额外的风险消减措施或进一步分析。通常 LOPA 所分析的事故场景是通过基于场景的危害评估方法（例如 HAZOP 分析）来识别的。

可能性：对某一事件预期发生的概率或频率的衡量。可能性可以表现为事件频率（例如：事件年发生率）、指定时间间隔（例如：年度）内的发生概率或条件概率（例如：某一前置事件发生后特定事件的发生概率）。

损失事件：损失事件指的是发生了可能造成潜在的损失或伤害的不可逆物理事件时的异常情景。例如危险物料的泄漏，可燃气体或者可燃粉尘的点燃，和储罐/容器的超压破裂。一次事故可能包含多个损失事件。例如，第一损失事件是可燃液体溢出，然后可燃液体被点燃形成闪火和池火（即第二损失事件），火灾致使邻近的容器升温并破裂（第三损失事件）。通常情况下与“危险事件”意义相同。

主工艺物料泄漏（LOPC）：主要工艺设施中物料的非预期或不可控泄漏，包括无毒性的和不可燃的物料（例如：水蒸气、蒸汽凝液、氮

气、压缩二氧化碳或压缩空气）。

减缓：减少损失事件的影响。

减缓措施：被设计为用来减少损失事件造成的影响的保护措施。

操作员：负责在系统进行生产活动时所必须的监控、控制和执行任务的人员。一般来说还包括执行所有种类任务的人员（例如：读数、校对、维护）。

工艺安全管理：一种为了确保工艺装置安全性而进行的包含了管理法则及分析技术应用的项目或活动。有时也称作“工艺危害管理”。

预防性保护措施：在特定初始事件发生后，能够避免相应特定损失事件的保护措施。例如，能够终止初始事件发展为损失事件这一事故链条的特定保护措施。（注：某种程度上来说，泄漏防护措施也可能预防初始事件的发生；然而在危害评估中，“预防性保护措施”特指本名词解释所指含义。）

主要工艺设施：直接与工艺物料接触，用于物料反应、存储或输送等目的的设施，如储罐、容器、管线、储运容器或设备。一般来说主要工艺设施在设计时会考虑泄漏防护措施，用来容纳或控制主要工艺设施的泄漏。泄漏防护措施包括但不限于储罐围堰、工艺设备外壳、连至油水分离系统的排污收集系统以及双重壁储罐的外壳。

概率：表示为一个事件或一个事件序列在一个事件间隔内发生的可能性或一个事件在测试/要求时成功或失效的可能性，为0～1的无量纲数字。

需求时失效概率（PFD）：系统在需要实施指定功能（如，紧急情况或手动触发）时失效的概率。

定量风险分析（QRA）：通过工程评估及模拟的方法来定量计算某装置或工艺过程中潜在事故的预期发生频率与后果严重性的系统分析方法。

可检出失效：某个可能立刻或马上引起报警/指示系统的故障。它

可以在相对较短的时间内导致矫正动作。

风险：一个或一组潜在事故的预期发生频率（年频率）和后果严重性的组合。

风险分析：通过识别潜在事故场景，然后将预期发生可能性及每个场景可能造成的后果影响进行评估和结合，来对场景、装置、工厂和/或公司风险进行预估。需要时可将各风险场景进行叠加来获取总体风险。

风险评估：风险评估指的是一种利用风险分析结果来进行风险消减策略决策的过程，可通过相对风险等级或对比风险目标的方式来进行评估。

风险控制措施：预期可降低损失事件发生可能性或减缓损失事件后果的工艺相关手段。

风险管理：风险管理指的是用于分析、评估及控制风险（为了保护人员、公众及环境安全，保护公司资产、避免生产中断）的管理政策、程序和操作实践等的系统应用。包括运用适当的设计和管理控制来降低风险的决策支持系统。

保护措施：初始事件发生后可能中断事件链的任何设施、系统或动作或可以减轻损失事件影响的措施。见“预防性保护措施”、“减缓保护措施”以及“防泄漏保护措施”。

安全系统：设计用于限制或终止一个事故序列的设备和/或程序，从而避免损失事件的发生或减轻它的后果。

场景：场景指的是会导致损失事件及影响的一个非预期事件或事故序列，包括事故序列中相关的保护措施是否失效。

泄漏源参数：指的是用来确定危险物料和/或能量泄漏至周边环境导致的最终损失事件后果的初始事件的相关泄漏参数（例如：量级、速率、时长、方向、温度）。对于气体扩散模型来说，泄漏源参数指的是扩散模型的输入条件，包括实际蒸气云的温度、气体组成、密度、大

小、速率和质量等条件。

顶上事件：在故障树“顶部”的损失事件或其他非预期事件，可以通过布尔逻辑门来分析其可能的原因，并向下追溯到基本事件。

未检出失效：未检出失效指的是无法在系统正常运行时被检测出来的失效，只能通过全面的诊断测试来检测。

故障假设分析：故障假设分析是一种基于场景的风险评估过程。使用头脑风暴的方法在一个熟悉待分析对象的团队中进行提问或考虑可能出现什么错误、会发生什么后果以及现有的安全措施是否足够。

故障假设/检查表分析：通过使用检查表或其他常用的列表来构建假设的一种故障假设分析方法。