保护层分析（LOPA）及风险图表法在 SIL 定级中的应用

鲁毅[1]，袁小军[1]，冯双虎[1]

（[1]北京华清国诚安全技术有限公司，北京 100025）

摘要：目前，安全完整性等级（SIL）作为安全仪表功能（SIF）的主要性能指标已被广泛应用。IEC 61511 列举了一系列基于风险的分析方法以确定 SIS 系统的安全完整性等级。

目前，SIL 定级中应用最为广泛的为保护层分析（LOPA）及风险图表法。保护层分析（LOPA）作为一种半定量的分析方法，综合考虑保护层、可接受标准及初始事件概率等因素影响，相对风险图表法更加量化，其分析结果也更加准确。

风险图表法作为一种更加简洁易懂的分析方法，可对大量的场景进行快速的梳理，因此适用于安全仪表回路的初步筛选。对风险图表法识别出的 SIL 等级较高的回路可使用 LOPA 方法进行再次分析确认。

本文旨在阐述 LOPA 及风险图表法的用途，通过分析 LOPA 及风险图表法之间的区别以及优缺点，以明确其不同的适用范围。

关键词：安全完整性等级（SIL）；安全仪表功能（SIF）；保护层分析（LOPA）；风险图表法

Application of LOPA and Risk Graphs for SIL determination

LU Yi[1]，YUAN Xiaojun[1] ，FENG Shuanghu[1]

([1]*Industry risk control，Beijing* 10025，*China*)

Abstract：Safety Integrity Level (SIL), as defined in IEC 61511, is a widely used safety performance measure for safety instrumented functions. The standard IEC 61511 suggests several methods for SIL determination, ranging from fully quantitative methods to fully qualitative methods.

Two widely used methods in the process industry for SIL determination are Layer of Protection Analysis (LOPA) and Risk Graphs. Each of these methods has their own advantages and disadvantages. LOPA allows the required risk reduction to be incorporated into the SIL values with higher precision. This enables a more detailed consideration of the available protection layers and leaves an objective traceable record of the decision-making process.

This paper seeks to explore the differences between LOPA and Risks graphs and to investigate the combination of Risk Graphs and LOPA method to provide the same level of SIL determination rigor as LOPA with high efficiency.

Key words：Safety Integrity Level（SIL）；Safety Instrument Function（SIF）；Layers of Protection Analysis（LOPA）；Risk Graph

2015-00-00 收到初稿，2015-00-00 收到修改稿。

联系人：安佰芳。**第一作者**：冯双虎（1986—），男，学士，工程师。

Received date: 2015-00-00.

Corresponding author: Feng Shuanghu, shuanghu.feng@irc-risk.com

引　言

一个典型的化工过程包含各种保护层，如本质安全设计、基本过程控制系统（BPCS）、报警与人员干预、安全仪表功能（SIF）、物理保护（安全阀等）、释放后保护设施、工厂应急响应和社区应急响应等。这些保护层降低了事故发生的频率。在开展化工过程工艺危害分析时，保护层是否足够，能否有效防止事故的发生是分析人员最为关注的一个问题。

安全完整性等级（SIL）是 IEC61508 和 IEC61511 中提出的一个重要概念。安全完整性等级是一种离散的级别，用于规定分配给安全仪表系统的安全仪表功能（SIF）的安全完整性要求。安全完整性等级分为 4 个等级，安全完整性等级随数字增大而提高，1 为最低，4 为最高。需要注意的是，安全完整性等级并不是对过程风险的衡量，也不是某个系统或元件的性质，而是对安全仪表系统的安全仪表功能水平的衡量。

确定 SIL 等级的方法很多，IEC61511 附录 B~F 列举了一系列的方法。这些方法的应用主要取决于以下诸多因素，其中包括：

（1）场景的复杂程度；

（2）与企业相关的应用指南；

（3）风险特性及所需要的风险降低；

（4）工作人员的经验及技能；

（5）关于风险的参数的可用信息。

本文主要讲述了保护层分析法（LOPA）与风险图表法在工程实践中如何使用，并总结了各自的优缺点，以帮助读者更好的把握其不同的应用场景。

1 相关标准要求

2000 年，国际电工委员会（International Electrotechnical Commission）发布了 IEC61508 标准《电气/电子/可编程电子安全相关系统（E/E/PES）的功能安全》，明确提出了安全相关系统的功能安全问题，即如何确保安全相关系统在危险发生时有效执行其安全功能。

2003 年发布的 IEC61511 标准《过程工业领域安全仪表系统的功能安全》则是基于 IEC61508 的框架针对过程工业中的 SIS 的细化。其中 IEC61511-3（确定要求的安全完整等级的指南）中明确了 SIL 定级的主要方法，例如安全层矩阵法、风险图、保护层分析（LOPA）等。

根据 IEC61508 的定义，安全功能（safety function）是由 E/E/PE 安全相关系统或其他风险降低措施实现的，用于针对特定危险事件使受控设备（Equipment Under Control）达到或保持安全状态的功能。

根据上述定义，安全功能的执行并不局限于安全仪表系统（SIS），并且安全功能具有针对性，着眼于特定的危险事件。危险事件的评估主要基于风险的概念。风险是针对一个特定危险事件发生频率和后果的综合度量。常见的各类风险描述如下：

（1）工艺风险：工艺过程中特定危害性事件的风险，确认工艺风险时不考虑其他安全保护因素的影响，如基本工艺控制系统及相关的人为因素；

（2）可接受风险（工艺安全目标等级）：基于当前的社会价值特定环境下的可以被接受的风险；

（3）剩余风险：危害性事件在考虑所有保护层之后的风险。

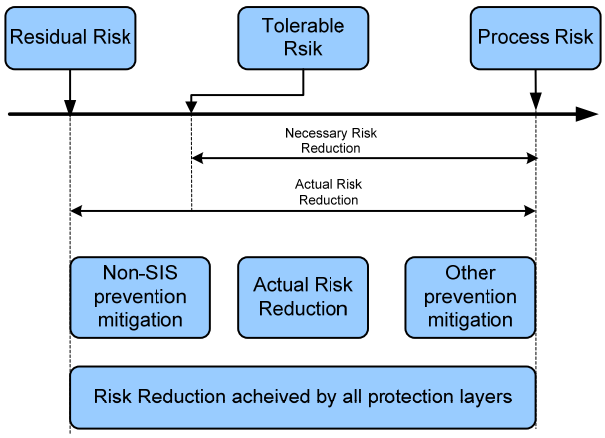

图 1 风险削减

Fig.1 Risk reduce

如图 1 所示，安全功能的作用在于降低风险。然而无限制的降低风险是不现实的。在实践中，人们往往是按照 ALARP（As Low As Reasonably Practicable）的原则，将风险降低到可接受的程度，保证受控设备或过程处于足够安全的状态。因此，要设计合理有效的安全功能，就需要对受控对象进行准确充分的危险辨识和风险分析。随后基于可接受风险的标准确定风险降低的要求。在确定了必要的风险降低要求之后，如现有保护层无法提供足够的风险削减，则需要安全仪表系统能够正确地降低风险。这种对风险削减进行分析的过程，即为 SIL 定级。

安全完整性等级（SIL）是 IEC61508 和 IEC61511 中提出的一个重要概念。安全仪表系统（SIS）的使用目的在于必要时可通过执行安全功能，将化工过程的风险降低到可接受的

水平。

SIL 定级的目的就是对安全仪表功能（SIF）回路进行分析，以确定其风险削减所需要的安全完整性等级（SIL）。

本文通过介绍 SIL 定级中两种不同方法的优缺点，以阐述其不同的应用场景，为本项目后期 SIL 定级工作的顺利开展提供指导意见。

2 SIL 定级方法

IEC61511 及 IEC61508 提出了一系列的风险定级的方法，这些既包括定性的分析方法也包括半定量及定量的分析方法。采用完全定量分析方法（QRA）对场景进行分析时，需要大量的资源，并且需要考虑多种因素的影响，因此其分析成果的精度较高，例如，定量风险评估（IEC61508-5 中附件 D）。但是由于这种方法评估周期较长，所需资料及影响因素较多，因此在项目概念设计阶段进行 SIL 定级时，宜采用 LOPA、风险图表法及安全矩阵法进行分析。以下对 SIL 定级的几种常见方法进行简单介绍。

2.1 保护层分析（LOPA）

LOPA 是一种半定量分析方法，可被用于识别能够满足独立保护层要求（依据 IEC61511 Part3，附件 F）的安全仪表系统。

在 LOPA 中，需要对提出或提供的独立防护层的有效性进行分析验证。这些保护层综合的效果将会与可接受风险的标准进行比对。如果满足企业的风险可接受标准则不需要提供额外的风险降低措施。如果其不符合风险可接受标准则需要增加额外的风险降低措施。这种额外的风险降低可以通过提高安全联锁系统的 SIL 等级或是增加更多的保护层来达到。

LOPA 分析的工作流程如图 2 所示：

Init. Eve.		Conq.		Enab. Fac.			UEF	Safe'd (incl. non_IPLs)	IPLs			MEF		SIL Req.	HAZOP Rec.	LOPA Rec.		Note
Descr.	Freq.	Cat.	S	Type	Descr.	Freq.			Type	Descr.	PFD	Freq.	Residual Risk			Descr.	Resp.	
		S		Equip. Usage Dur.					1.Process Design									
				Expo. Prob.					2.BPCS									
				Ign. Prob.					3.Alarms & Ops Interv.									
				Fat. Prob.					4.Other SIF									
									5.Physical Prot.									
									6.Post-Release Prot.									
									7.Others									

图 2 LOPA 工作表

Fig.2 LOPA Worksheet

（1）初始原因

如表 1 所示，针对每一个影响事件，在记录表中列出其所有初始原因。影响事件可能有多个初始原因，列出每一个初始原因对 LOPA 分析来说是非常重要的。每一个初始原因（原因）应来自 HAZOP 分析结果。从人员安全、财产损失、环境影响三个方面的后果考虑确定严重程度等级。表 1 为后果严重度等级的示例：

表 1 后果严重性

Table 1 Consequences severity

Consequences

Severity	People	Asset Production/ Property	Environmental Effect	Reputation
Catastrophic (5)	Multiple fatalities	Loss > $50M	Spill > 100,000 bbl OR Tier 3 OR International assistance	International TV International papers
Major (4)	Multiple LWDC OR one or more Permanent Disability OR 1 Fatality	Loss between $5M – $50M	Spill > 10,000 bbl OR Tier 2 OR Regional assistance	National TV National papers
Serious (3)	Single LWDC OR multiple RWDC	Loss between $100K – $5M	Spill > 1,000 bbl OR Tier 1 OR Localised effect	Local TV Local written media
Moderate (2)	MTC OR Single RWDC	Loss between $10K - $100K	Spill > 1 bbl OR Moderate effect	Local media interest
Minor (1)	Minor injury with First Aid	Loss < $10K	Spill < 1 bb OR Spill in containment OR Minor effect	No Reaction

（2）初始原因频率

初始原因导致事件发生的每年的频率值基于 CCPS 及 OREADA 数据库确定。在决定初始原因频率时，LOPA 分析团队的经验是非常重要的。

（3）初始事件减轻因子

初始事件经过人员暴露概率，设备使用频率等不同初始事件减轻因子削减初始风险。

（4）保护层失效需求概率

每一个保护层包含设备和/或管理控制，具备和其他保护层一起控制或减缓工艺风险的功能。具有较高程度可靠性（能实现其功能）的保护层才具备作为独立保护层（IPL）的可能性。

当初始原因出现后，合理的工艺设计可以用来降低影响事件的发生几率。例如，管道或容器的夹套可以在主体管道或设备完整性失效的情况下防止工艺物料的泄露。

如记录表中的基础工艺控制系统（BPCS）。如果一个 BPCS 的控制回路在初始原因发生后可以防止影响事件的发生，则基于该控制回路的 PFD（要求时的平均失效概率）的置信度将会在 LOPA 分析中被考虑。

2.2 风险图表法

风险图表法是一种定性的分析方法，该方法的合理使用，取决于完整性管理者对系统了解、经验及风险因素的识别。该方法最初在 DIN V19250 及 VDI/VDE2180 中应用，此后被德国过程工业和机械部分所接受。

风险图表法基于风险与危险事件的后果及频率成正比的原理。首先假设不存在安全仪表系统以及 BPCS 等典型非安全仪表系统的安装符合标准要求。其后果需要考虑人员、财产及环境的影响。图 3 为典型风险图表法。

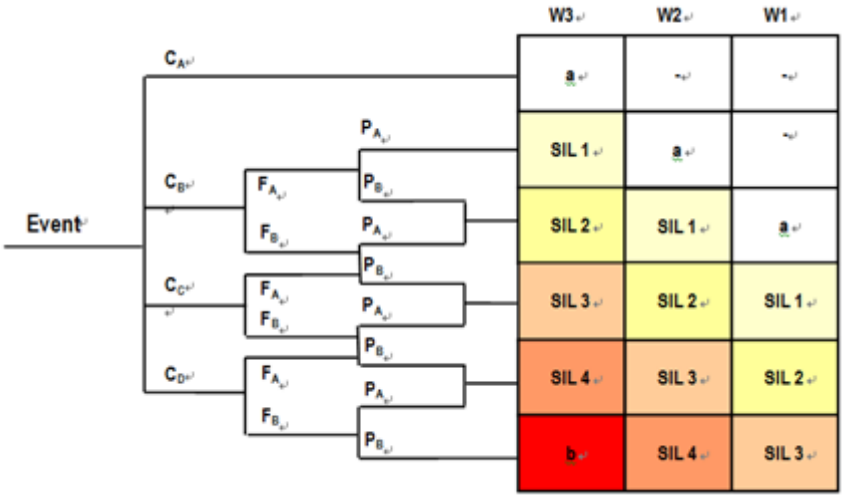

图 3 风险图表法

Fig.3 Risk Graph

后果发生的频率主要是以下几个因素的组合：

（1）出现在危险区域的频率及潜在的暴露时间

（2）避免危险事件的可能性

（3）安全仪表系统安装未到位时，发生危险事件的概率（不期望事件概率）

因此，产生了以下几个参数：

（1）危险事件的后果（C）

（2）出现在危险区域的频率与暴露时间的乘积（F）

（3）避免危险事件后果的可能性（P）

（4）不期望发生的概率（W）

当使用风险图方法时，首先考虑业主以及其他的部分风险要求，并且应以清楚且易于理解的措施来描述风险中每个分支的解释及评价，以确保方法应用时的一致性。另外，风险图标法应由各专业负责人共同确定。

3 LOPA 分析法及风险图表法优缺点

3.1 LOPA 分析法

LOPA 分析法，作为简化的半定量的风险评估方法，使得对事故场景的分析和评价比其他定量风险评价方法更节省时间和精力，主要具有以下优势：

（1）可以提供一种更为公开透明的 SIL 评估方法（分析不同保护层，可接受标准，概率基础等），并且 LOPA 分析方法的操作弹性允许其对一些使用风险图表法比较难以进行分析确定的因素进行分析考虑。

（2）由于 LOPA 分析会评估现有的所有安全保护层，因此与风险图表法相比，LOPA 分析方法不会过于保守（大多数情况下，风险图表法只将 PSV 视为一个保护层而忽略系统中得其他保护层）

（3）相对于风险图表法中使用的类似于“一个相对较高的可能性”，“一个较低的可能性”这些较为定性的描述，LOPA 分析方法则对初始事件、风险可接受标准、独立保护层的要求时失效概率（PFD）进行完全的量化分析，其分析结果也更加准确。

在 LOPA 分析过程中通常还会采用使能条件及修正因子（例如，使用率、人员暴露概率及点燃概率等）对场景后果进行修正，因此对场景的分析更加准确。

除了上述优点外，LOPA 分析法同样也存在一些局限性，如下所示：

（1）LOPA 不是识别危险场景的工具，LOPA 的正确执行取决于定性危险评价方法所得出的危险场景的准确性，包括初始事件和相关的安全措施是否正确和全面。

（2）当使用 LOPA 时，只有当择失效数据的方法相同并采用相同的风险标准时才能进行场景风险的对比。

（3）LOPA 是一种简化的方法，其计算结果并不是场景风险的精确值。

LOPA 分析法每次只针对一起特定的事故场景进行分析，不能反映各种事故场景之间的相互影响。由于 LOPA 分析的成果通常会受一些关键因素的制约，例如，风险可接受标准、初始事件以及独立保护层频率等，所以假如在分析中使用数据不同，则可能产生不同的结果。另外，LOPA 分析法中另外一个重要的缺点是无法对独立保护层之间的公因失效进行定量的分析。

3.2 风险图表法

风险图表法是一种非常简化的方法，易于操作，并且占用时间较短。这种可视的图形法，更加易于理解和掌握。

由于风险图表法是一种定性的方法，分析结果受主观因素的影响。因此分析团队的经验不同可能导致不同的结果，并且没有考虑使能条件以及修正因子的影响。而且分析中所使用的某些参数的很难确定，例如 F 值，需要综合考虑出现在危险区域的频率及暴露时间两个因数的影响。另外，某些参数的定义难以区别，例如“频率”及“可能性”的单位没有区别。如果采用校正的图标法进行分析，则需要制定合理的风险可接受标准，而且需要考虑所有设备风险才可提高分析的准确度。

因此，风险图表法由于过于保守的分析，通常会导致过度设计。高安全完整性（SIL）等级在仪表可靠性、冗余设置以及操作维护等方面的要求更高，因此也需要更多的资金投入。

因此良好的风险图表法通常需要考虑以下几点因素：

（1）选择正确的结构，并充分考虑评估中所需参数。

（2）对每个参数进行定义，可对风险进行充分评估。

（3）对结果进行合理修正。

4 总结与展望

上述所讲 SIL 定级的方法，由于其原理及方法不同，因此可分别应用于不同的场景分析。

定性的分析方法（如，风险图表法）其分析结果相对保守，并且其分析成果（SIL 等级）不精确。这些分析方法较为简单也易于操作，但是过于保守的分析可导致设计过度，增加投资，例如，增加一个 SIL 等级至少需要增加数万元的投入。因此从这个角度出发，使用相对量化的分析方法可以节省部分成本。定量分析的结果通常非常明确，完善的文档管理程序允许不同人员对分析中的每个环节进行跟踪，并且可以提供相对完整的生命周期管理程序，但往往需要投入较多的资源。对于较为简单场景可采用定性的方法进行初步筛选，对于需要高资金投入或对结果的精确度较高的场景，可采用半定量及定量的方法进行精确分析。

综合考虑以上因素，具体的 SIL 定级项目时，应分为两个阶段执行。对于安全功能回路数量较多的项目，可采用风险图表法通常作为初步筛选，对于筛选出的 SIL 等级较高的回路（通常考虑为 SIL2）可以采用 LOPA 分析法进一步分析。在 LOPA 分析过程中确定不同独立保护层的降低风险过程中的贡献值，则可以选择更加经济合理的方法来降低风险，既保证了可靠性又减少了因过度设计带来的成本投入。根据不同的场景选择更加合理可行的方法执

行。不但提高了 SIL 评估执行效率，而且有助于生命周期的完整性管理。

国家安全生产监督总局在 2014 年 11 月发布的 116 号文“加强化工安全仪表系统管理的指导意见”对安全仪表系统功能安全的评估、安全仪表系统管理制度落实、人员培训等提出了新的要求，预示着我国安全系统的功能安全设计已经逐渐走了规范化的道路，安全仪表系统的应用及发展必将为流程工业企业的生产运营提供一道新的保障。

References

[1] IEC 61508-2010, Functional Safety of Electrical/ Electronic/Programmable Electronic Safety-related Systems

[2] IEC 61511-2003, Functional Safety-Safety Instrumented Systems for the Process Industry Sector

[3] On the use of LOPA and risk graphs for SIL determination - as published mkopsc 2014

[4] GB/T 20438-2006 电气/电子/可编程电子安全相关系统的功能安全

[5] GB/T 21109-2007 过程工业领域安全仪表系统的功能安全

[6] AQT 3054-2015 保护层分析（LOPA）方法应用导则

[7] The Layer of Protection Analysis（LOPA）method. Anton A. Frederickson, Mr., (prepared answer) 01 April, 2002

[8] Introduction to layer of production analysis. Angela E. Summers, Ph.D., P.E, President, SIS-TECH Solutions, LP.To be presented at the Mary Kay O’Conner Process Safety Center Symposium, Texas A&M University, October 2002. Published in Journal of Hazardous Materials.

[9] Determination of Safety Integrity Level (SIL) using LOPA method in the Emergency Shutdown System (ESD) of Hydrogen unit. Iranian Journal of Health, Safety & Environment, Vol.1, No.4, pp 191-195.

[10] SIL DETERMINATION AND PROBLEMS WITH THE APPLICATION OF LOPA. Alan G King Hazard & Reliability Specialist, ABB Engineering Services, Bellingham, Cleveland UK. TS23,4YS.

[11] Instrumented Protective Systems - SIL Classification and Lifecycle Integrity Management to comply with BS EN 61508 / 61511.Jane Capewell and Lyn Fernie, AK EHS & Risk.

[12] Safety Integrity Level (SIL) Assessment as key element within the plant design. Tobias WALK, ILF consulting Engineers GmbH Germany.