

石油化工装置何时设置安全仪表系统

关于安全仪表系统 (SIS) 设置及工程执行的几个重要问题探讨——石油化工装置具有易燃、易爆、高温、高压、有毒、有害的特点,对于安全提出了很高的要求,确定是否需要设置安全仪表系统 (SIS) 以及设计符合要求的安全仪表系统 (SIS) 是工程设计的重要内容。国家和地方的很多文件都提到了安全仪表系统 (SIS), 体现了其重要性, 包括: 安监总管三〔2014〕116 号《加强化工安全仪表系统管理的指导意见》、安监总管三〔2017〕121 号《化工和危险化学品生产经营单位重大生产安全事故隐患判定标准 (试行)》和应急〔2019〕78 号《危险化学品企业安全风险隐患排查治理导则》等。本文从安全仪表系统 (SIS) 的概念和风险减低原则等方面探讨石油化工装置何时需要设置安全仪表系统 (SIS), 以及工程设计中应注意的问题。

PROCESS-Tip

* 更多信息请扫描二维码:



chem.vogel.com.cn

* 反馈编码: A211124

文 / 范咏峰 王云 曾德智

安全仪表系统 (SIS) 概念

SIS 是 safety instrumented system 的缩写。

安全仪表系统 (SIS) 的定义是: 用来实现一个或几个仪表安全功能 (SIF) 的仪表系统。

仪表安全功能 (SIF) 是指具有某个特定安全完整性等级 (SIL1、SIL2、SIL3) 的, 用以达到防止、减少危险事件发生或保持过程安全状态的安全保护功能或安全控制功能。

安全仪表系统 (SIS) 可以由传感器 (Sensor)、逻辑解算器 (Logic Solver) 和最终元件 (Final Element) 的任何组合组成, 典型的安全仪表系统 (SIS) 如图 1 所示。

传感器也称为测量仪表, 逻辑解算器也称为逻辑控制器。

何时需要设置安全仪表系统

当石油化工装置具有 SIL1 及以上的仪表安全功能 (SIF) 时, 应设置安全仪表系统, 反之, 不具有 SIL1 及以上的仪表安全功能 (SIF) 时, 原则上不需要设置安全仪表系统。

仪表安全功能 (SIF) 的安全完整性等级宜通过安全风险评估确定, 安监总管三〔2014〕116 号《加强化工安全仪表系统管理的指导意见》要求: 设计安全仪表系统之

前要明确安全仪表系统过程安全要求、设计意图和依据。要通过过程危险分析, 充分辨识危险与危险事件, 科学确定必要的安全仪表功能, 并根据国家法律法规和标准规范对安全风险进行评估, 确定必要的风险降低要求。根据所有安全仪表功能的功能性和完整性要求, 编制安全仪表系统安全要求技术文件。

工程执行原则

实际工程中, 可以按照以下原则确定是否需要设置安全仪表系统:

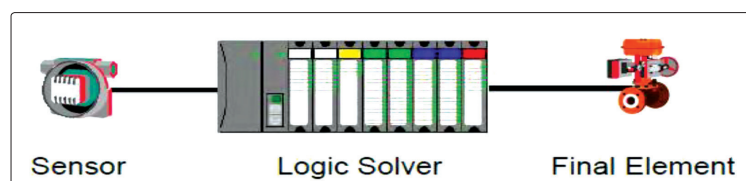


图 1 安全仪表系统 (SIS) 示意

本文作者范咏峰、曾德智供职于中科合成油工程有限公司; 王云供职于山东济炼石化工程有限公司。

1. 有管辖权的部门根据经验和主观意志确定。此时,即使没有 SIL1 及以上的仪表安全功能(SIF),也可以设置安全仪表系统。

2. 标准规范的要求和规定、安全要求、IPL 方法论、SIL 评估确定。上一章节“何时需要设置安全仪表系统”中给出的原则,属于此类。

3. 经济评价确定(前提是满足安全基本要求),比如 ALARP(as low as reasonably practicable)分析。注:ALARP 的采用应符合法律法规标准规范以及企业的要求,比如有些文件和企业规定要求如果涉及人身伤亡,通常不允许采用 ALARP。举例:某个场景只涉及经济损失后果,并且如果设置安全仪表系统,并不能带来满足预期的经济回报(比如设置 SIS 的投资大于不设置 SIS 带来的经济损失),这时根据具体情况分析,可以不设置 SIS。

不论采用哪种方式,都以满足法律法规、标准规范为最低要求。

国家安监总局令第 40 号《危险化学品重大危险源监督管理暂行规定》第十三条规定:涉及毒性气体、液化气体、剧毒液体的一级或者二级重大危险源,应配备独立的安全仪表系统;意味着,只要属于涉及毒性气体、液化气体、剧毒液体的一级或者二级重大危险源,不论相关仪表安全功能(SIF)的安全完整性等级是否达到 SIL1 或者以上,都要求配备独立的安全仪表系统,即使 SIL 评估确定所有的 SIF 都没有达到 SIL1 或者以上,也需要配备独立的安全仪表系统。此条要求属于前面提到的确定是否需要设置安全仪表系统工程执行原则中的第 1

条原则:有管辖权的部门根据经验和主观意志确定。

SIL 评估是确定石油化工装置是否需要设置安全仪表系统的最常见的方法,SIL 评估和分级宜采用保护层分析法(LOPA)。

如何降低风险

风险是伤害发生的概率与该伤害严重程度组合,降低风险可以从严重性和可能性两个维度考虑,选择合适的风险降低措施。降低危险事件发生的可能性属于预防措施,降低后果严重性属于减轻措施,预防和减轻措施对风险的影响如图 2 所示。

BPCS(DCS)、报警系统和 SIS 等属于预防措施,防火堤、围堰和消防等属于减轻措施。

独立保护层(IPL)

IPL 是 Independent protection layer 的缩写。

独立保护层(IPL)的定义为:一种设备、系统或行动,有效地防止场景向不期望的后果发展,它与场景的初始事件或其他保护层的行动无关。独立性表示保护层的执行能力不受到初始事件或其他保护层失效的影响。独立保

护层的有效性和独立性可以被审查。

只有具备以下特性才能被确定为独立保护层:

1. 有效性:按照设计的功能发挥作用,应有效地防止后果发生。

2. 独立性:独立于初始事件和任何其他已经被认为是同一场景的独立保护层的构成元件。

3. 可审查性:对于阻止后果的有效性和要求时危险失效概率(PFD)应以某种方式(通过记录、审查、测试等)进行验证。

SIS 与 IPL 的关系

风险降低措施通常通过独立保护层实现,一些常见的独立保护层(IPL)的举例:基本过程控制系统(BPCS)、报警及响应、SIF(SIS)、安全阀以及防火堤等。

安全仪表系统是众多独立保护层(IPL)中的一个独立保护层(IPL),所有的环节均应满足相关法律法规标准的要求。风险降低措施如图 3 所示,安全阀同时具有预防措施和减缓措施 2 种属性。

通常只有在其他独立保护层(IPL)不能将初始风险降低到可接受风险时,才考虑设置安全仪表系统。

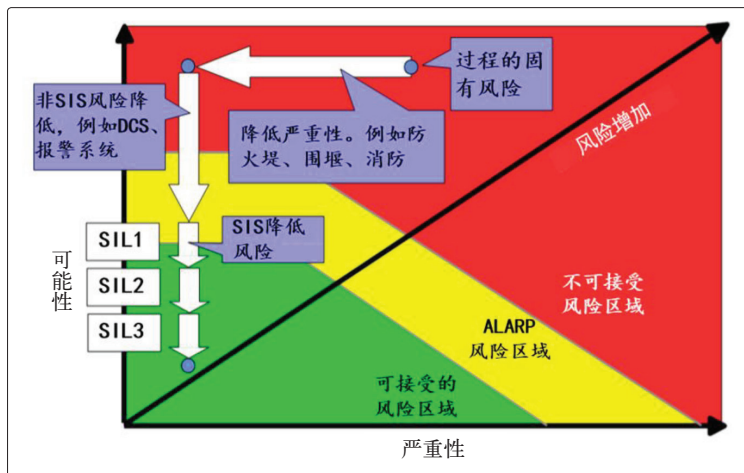


图 2 预防和减轻措施对风险的影响

IPL 响应顺序和 IPL 选择顺序不同

行业内有如下争论：有观点认为 SIS 是用于消除 BPCS、安全阀、爆破片等独立保护层所未能消除的残余风险。另外一种观点提出的不同意见，提出 SIS 不能消除安全阀和爆破片未能消除的残余风险，此观点认为洋葱模型中 SIS 相对于安全阀和爆破片在内层，外层消除内层未能消除的残余风险，而不是反过来。

以上两种观点出发点不一样，阐述问题的角度不同，都具有正确的一面，应注意：IPL 响应顺序和 IPL 选择顺序不同。IPL 的响应顺序基本上是按照洋葱模型从内到外的顺序进行的，IPL 的选择顺序却不是按照洋葱模型的从内到外的顺序来选择。

石油化工装置典型多保护层结构如图 4 所示，机械的保护（比如安全阀和爆破片）通常作为阻止危险事件实际发生的最后一道防线。安全阀和爆破片等的设置通常是依据法律法规标准规范要求确定的。

根据 GB/T 20801.6-2020，符合下列情况的设备或管道系统，应设置安全泄放装置：

1. 设计压力小于外部压力源的压力，出口可能被关断或堵塞

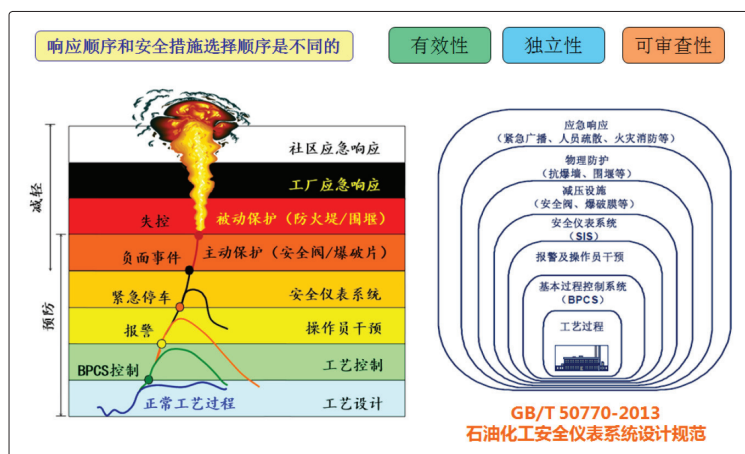


图 4 石油化工装置典型多保护层结构

的设备和管道系统。

2. 出口可能被关断的容积式泵和容积式压缩机出口管道系统。

3. 冷却水或回流中断、再沸器输入热量过多而引起超压的蒸馏塔顶气相管道系统等。

只要满足以上条件中的任何一条，不论是否设置了 SIS 系统，都需要设置安全泄放装置。GB/T 20801.6-2020 给出了安全泄放装置的定义：在非火灾或者火灾事故情况下，由进口静压力或进出口静压差的作用开启，泄放流体，以防止系统内压力超过预定安全值的装置，包括安全阀、爆破片装置及爆破针阀等。

自动控制仪表和报警联锁装置不得替代安全泄放装置作为系统的超压保护设施。当不允许排

放或不能安装安全泄放装置时，可通过过程危险源评价及分析所有的超压工况，采用系统设计方法，即本质安全设计或高完整性保护系统（HIPPS），消除系统的超压原因或者进行系统超压保护。

IPL 响应顺序和 IPL 选择顺序不同，通常只有在其他独立保护层（IPL）不能将初始风险降低到可接受风险时，才考虑设置安全仪表系统（SIS）。

LOPA 分析介绍

LOPA 是 Layer of Protection Analysis 的缩写。

石油化工装置中，LOPA 分析是 SIL 评估和确定 SIL 定级最常用的方法。

LOPA 分析是对事故场景风险进行半定量评估的一种系统方法，一次分析一个事故场景，使用初始事件频率、独立保护层失效概率和后果严重性的预定义值，将场景风险估计与风险标准进行比较，确定是否需要额外风险降低或更详细的分析。如需额外的风险降低并且是以仪表安全功能（SIF）的形式提供这种降低，LOPA 分析可以确定 SIF 的安全完

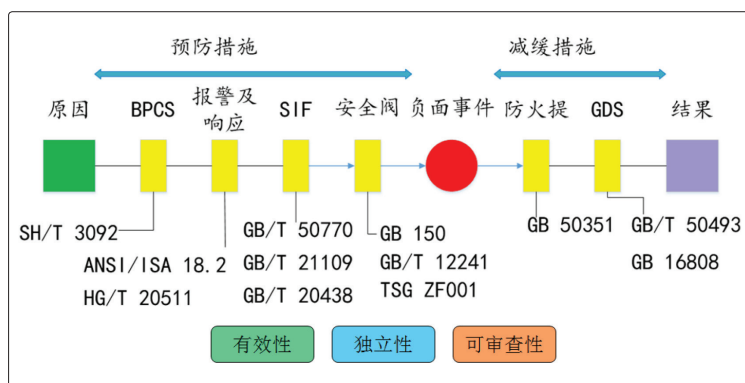


图 3 风险降低措施示意

整性等级 (SIL)。

LOPA 是在定性危险分析的基础上, 进一步对具体场景的风险进行相对量化的研究, 包括对场景的准确表述及识别已有的独立保护层, 从而判定该场景发生时系统所处的风险水平是否达到可容许风险标准的要求, 并根据需要增加适当的保护层, 以将风险降低至可容许风险标准所要求的水平。

LOPA 分析程序如图 5 所示, 其中, F_t 为后果可容忍频率, F_{np} 为不考虑 SIS 保护的后果发生频率 (考虑 SIS 以外的其他保护), 当 $F_t / F_{np} < 1$ 时需要进一步降低风险。

SIL 定级

按照图 6 所示进行风险分析, 比较 SIF 后果可容忍频率 (F_t) 和不考虑 SIS 保护的后果发生频率 (F_{np})。

如果风险降低尚未达到可容忍风险标准, 即 $F_t / F_{np} < 1$, 则需要进一步降低风险, 石油化工装置进一步的风险降低措施有: SILa、SIL1~3。

比较剩余风险与可容忍风险标准, 确定是否需要额外风险降低, 如需额外风险降低并且以 SIF

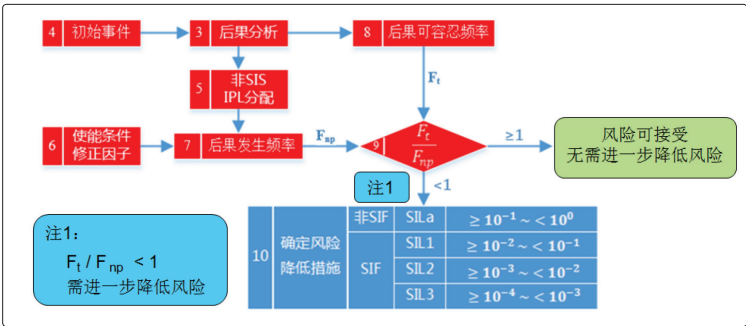


图 6 分析风险是否可接受 (F_t/F_{np}) 示意

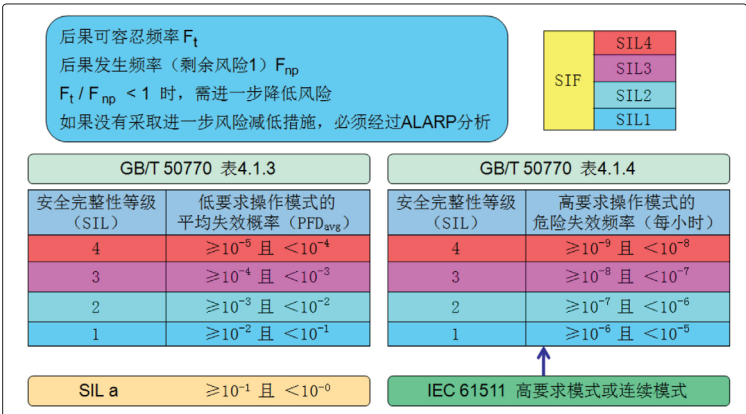


图 7 是否需要 SIS 及 SIL 定级示意

的形式提供, 那么需要设置 SIF, 可以根据图 7 确定 SIF 的 SIL 等级。

SIL1~3 需要满足 GB/T50770 和 GB/T21109 等标准, 应特别注意安全生命周期的要求。SILa 可以在 BPCS 或者 SIS 中实现, 不需要满足 GB/T50770 和 GB/T21109 等标准, 但需要满足其他相关标

准的要求, 比如 BPCS、报警管理等标准的要求。

总结

执行功能安全相关标准要求, 设计符合要求的安全仪表系统 (SIS) 是石油化工工程设计中的重要内容。安监总管三〔2014〕116 号《加强化工安全仪表系统管理的指导意见》是安全仪表系统的重要文件, 在实际工程设计中应切实的执行 116 号文的要求。正确理解安全仪表系统 (SIS) 的概念以及风险降低的方法论和认识论, 有助于合理的开展安全仪表系统 (SIS) 的工程设计, 实际工程中既要防止过设计, 也要防止欠设计。

希望通过本文可以有助于了解安全仪表系统 (SIS) 的设置原则和工程具备可执行性的原则。

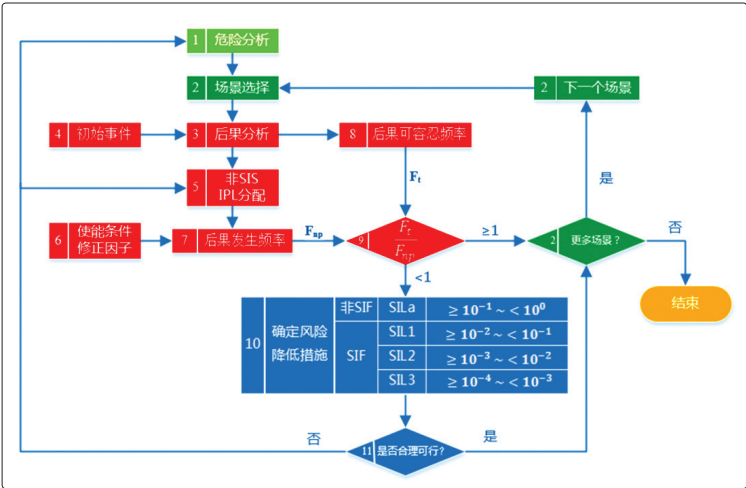


图 5 LOPA 分析程序