Journal of Oil and Gas Technology 石油天然气学报, 2020, 42(4), 274-279
Published Online December 2020 in Hans. http://www.hanspub.org/journal/jogt
https://doi.org/10.12677/jogt.2020.424143

Hans汉斯

SIL and Redundancy Requirement of Safety Instrumented System

Shaoqing Shan, Yishan Guan, Yuewang Ma

China Petroleum Pipeline Engineering Co., Ltd. International, Langfang Hebei
Email: 1073340745@qq.com

Received: Oct. 10th, 2020; accepted: Nov. 20th, 2020; published: Dec. 15th, 2020

Abstract

Safety instrumented system is the system to prevent and reduce the occurrence of dangerous events in oil and gas pipelines or to maintain process safe status, and realize safe protection or safe control. Safety integrity level (SIL) is a classification method to quantify the expected or required safety level of safety instrumented system. The average probability of failure on demand of danger is an important index to measure the safety integrity level, and the hardware failure tolerance is determined by the safety integrity level. The domestic common specifications have made requirements on the logic controller redundancy of safety instrument system for each safety integrity level. The redundancy setting and safety integrity level requirements of logic control module of emergency shutdown (ESD) system of ARAMCO are significantly higher than the requirements of domestic specifications.

Keywords

Safety Instrumented System, Safety Integrity Level, Average Probability of Failure, Hardware Failure Tolerance, Redundancy

文章引用: 单少卿, 关沂山, 马岳旺. 安全仪表系统的 SIL 等级和冗余要求[J]. 石油天然气学报, 2020, 42(4): 274-279.
DOI: 10.12677/jogt.2020.424143

安全仪表系统的SIL等级和冗余要求

单少卿，关沂山，马岳旺

中国石油管道局工程有限公司国际事业部，河北 廊坊
Email: 1073340745@qq.com

收稿日期：2020年10月10日；录用日期：2020年11月20日；发布日期：2020年12月15日

摘 要

安全仪表系统是为防止、减少油气管道危险事件发生或保持过程安全状态，实现安全保护或安全控制的控制系统，安全完整性等级(SIL)是一种量化安全仪表系统预期或要求的安全水平的分级方式，平均失效概率是衡量安全完整性等级的重要指标，相应的安全完整性等级对应着相应的硬件故障裕度，国内常用规范对各个安全完整性等级的安全仪表系统逻辑控制器冗余做了相应要求，阿美公司的紧急停车(ESD)系统逻辑控制模块冗余设置和安全完整性等级要求明显高于国内规范要求。

关键词

安全仪表系统，安全完整性等级，平均失效概率，硬件故障裕度，冗余

1. 引言

2019 年 12 月 9 日，国家石油天然气管网集团有限公司(简称国家管网公司)在北京正式成立，预计国内油气管网建设将再次掀起建设高峰。目前我国累计建设的油气长输管道里程已经达 13.6 万公里，油气管道总里程在 2020 年将超过 15 万公里。随着我国油气管道里程的不断增长，油气管道的安全运行也越来越受到国家的重视，目前，油气管道建设上普遍采用安全仪表系统实现安全保护功能或安全控制功能，安全仪表系统的设计也已经实现规范化，其中，安全完整性等级(SIL)是安全仪表系统的一个重要指标[1]。

中国于 2007 年依据 IEC 61508 和 IEC 61511 发布了 GB/T 20438-2006《电气/电子/可编程电子安全相关系统的功能安全》和 GB/T 21109-2007《过程工业领域安全仪表系统的功能安全》，是国内安全仪表系统 SIL 评估工作的依据[2]。近年来，石油化工行业通常要求对工艺仪表流程图进行 HAZOP (危险与可操作性分析 Hazard and Operability Study)定性分析和 LOPA (保护层分析 Layer of Protection Analysis)半定量分析，从而确定重大风险的 SIL 等级，然后选择设备，选择子系统的冗余结构，验证 SIL 等级是否符合要求，完成仪表 SIL 等级设计[3]。

同时，国内标准 GB/T50770-2013《石油化工安全仪表系统设计规范》，GB/T32202-2015《油气管道安全仪表系统的功能安全评估规范》，GB/T32203-2015《油气管道安全仪表系统的功能安全验收规范》，对于安全仪表系统的设计、评价有着非常重要的指导作用[4]，这些标准对安全仪表系统不同 SIL 等级的

子元件冗余设置做了对应要求，并在油气管道行业中得到越来越多的应用。

2. SIL 与平均失效概率

安全仪表系统是为防止、减少危险事件发生或保持过程安全状态，实现安全保护或安全控制的控制系统，安全仪表系统主要由测量仪表、逻辑控制器和最终元件三个子部分并配合相应的软件组成[5]。通常，各部分均应采用具有相应 SIL 等级认证的设备[6]。

SIL 等级是一种量化预期或要求的安全水平的分级方式，即在一定时间、一定条件下，安全相关系统执行期所规定的安全功能的可能性。选择安全完整性水平的目的是通过降低风险发生的概率，把系统的风险降低到可以接受的水平。国际标准中常由每小时发生的平均失效概率(PFDavg)来确定，共分为 SIL1 到 SIL4 这四个等级，SIL 等级级别越高要求其危险失效概率越低，系统的 SIL 等级可以通过 IEC61508 和 IEC61511 来进行 SIL 验证。其中，SIL 等级与平均失效概率之间的对应关系见表 1。

Table 1. Safety integrity level requirements in low requirement operation mode
表 1. SIL 等级与平均失效概率对应表

安全完整性等级(SIL)	平均失效概率(PFD_{avg})
4	$\geq 10^{-5}$ 且$\leq 10^{-4}$
3	$\geq 10^{-4}$ 且$\leq 10^{-3}$
2	$\geq 10^{-3}$ 且$\leq 10^{-2}$
1	$\geq 10^{-2}$ 且$\leq 10^{-1}$

安全仪表系统安全功能的平均失效概率，是通过计算和组合提供安全功能的所有子系统在要求时间的平均失效概率通过公式(1)中计算确定的，公式可以表示为：

$$PFD_{SYS} = PFDs + PFD_{L} + PFD_{FE} \tag{1}$$

式中：

PFD_{SYS}：安全仪表系统的安全功能在要求时的平均失效概率；

PFD_{S}：测量仪表子系统要求的平均失效概率；

PFD_{L}：逻辑控制器子系统要求的平均失效概率；

PFD_{FE}：最终元件子系统要求的平均失效概率[7]。

由此可以看出，安全仪表系统中某个安全仪表回路的 SIL 等级由各子部分 SIL 等级的最低级所限定，如果三个部分中最低的 SIL 等级为 SIL2，即使其他两个部分的 SIL 等级均为 SIL3，则整个回路的 SIL 等级是 SIL2 或甚至 SIL1。

需要注意的是，平均失效概率是安全仪表系统 SIL 等级的重要指标，但并不是唯一的衡量指标，对安全仪表系统的指标要求还有其他 3 个要求：硬件故障裕度要求、系统失效避免及控制要求和软件要求，需要也达到这 3 个要求，才能认为安全仪表回路满足了对应的 SIL 等级要求。

其中，系统失效避免及控制要求是一个原则性要求，要求安全仪表系统选用的设备具备对应的系统失效避免及控制方法[8]。系统失效是由其他原因而非性能自然退化导致的失效，系统失效起因可归结为 3 类：

1) 应力失效：元件在正常操作中超过了设计允许条件，导致应力超限的系统失效；

2) 设计失效：系统在投产之前的设计、生产、购买或安装中出现失误导致的系统失效；

3) 运行失效：系统在投产后，运行人员在设备保养维护、维修测试中，运行人员出现工作失误导致

的系统失效。

对于系统失效避免及控制要求，我们可以通过严守设计流程、选用带 SIL 认证设备、制定合理运维章程或提高人员工作水平来控制设计生产、购买安装、保养维护、维修测试等可能出现的问题，从而避免系统失效。

软件要求也是一个原则性要求，相对比较简单，需要软件的编译环境为对应 SIL 等级的编译程序的软件、固件，并对编译程序的管控、测试进行对应的强化。

安全仪表回路的这 2 种要求均为原则性指标，在本文中不再多加论述，下面将着重对硬件故障裕度要求进行探讨。

3. SIL 与硬件故障裕度要求

硬件故障裕度要求为半定量要求，取决于安全仪表回路的安全失效分数(SFF)，是对元件冗余的最低要求，即某回路的 PFD avg 符合该回路的 SIL 需求，但是如果组成该回路的硬件不能满足硬件故障裕度要求，该回路也不符合 SIL 的要求。IEC 61508-2-2010 中对逻辑控制器的硬件故障裕度要求见表 2 [9]。

Table 2. Safety integrity level requirements in low requirement operation mode
表 2. 逻辑控制器的硬件故障裕度要求

安全失效分数(SFF)	硬件故障裕度要求(FTmin)		
	0	1	2
60%	不允许	SIL1	SIL2
60%~90%	SIL1	SIL2	SIL3
90%~99%	SIL2	SIL3	SIL4
99%	SIL3	SIL4	SIL4

表 2 指明了安全仪表回路中逻辑控制器的硬件结构构成方式是否需要采用硬件冗余，根据逻辑控制器的安全失效分数，找到对应的行即可确定对应 SIL 等级的硬件故障裕度，即需要多少数量的冗余设备。

可以看出，相应的 SIL 等级的逻辑控制器对应着相应的硬件故障裕度，即相应的冗余设备数量，同时，增加安全仪表回路中某子部分的硬件故障裕度可以提升该子部分的 SIL 等级[10]-[16]。

4. 国内安全仪表系统逻辑控制器冗余要求

目前国内常用的 GB/T 50770-2013《石油化工安全仪表系统设计规范》，规定石油化工工厂或装置的 SIL 等级最高为 SIL3 级。规范中对逻辑控制器的冗余设置要求为：SIL1 级安全仪表功能，可采用冗余逻辑控制器；SIL2 级安全仪表功能，宜采用冗余逻辑控制器；SIL3 级安全仪表功能，应采用冗余逻辑控制器。

同时，在国内某管道行业设计单位的油气管道行业安全仪表系统技术规格书中，对逻辑控制单元的冗余设置的准则为：对于 SIL1 级安全仪表系统，可采用单一的逻辑控制单元；对于 SIL2 级安全仪表系统，宜采用冗余的逻辑控制单元。如采用可编程逻辑控制器，其中央处理单元、电源模块及通讯网络与接口等宜冗余设置；对于 SIL3 级安全仪表系统，应采用冗余的逻辑控制单元。如采用可编程序逻辑控制器，其中央处理单元、电源模块、输入/输出模块及通讯网络与接口等应冗余设置。

根据表 2，SIL1~SIL3 级的逻辑控制器冗余要求解释如下：

一般来说，逻辑控制器的 SFF 应为 90%~99%。SIL1 级要求的硬件故障裕度为 0，用 1 台逻辑控制器即可满足，所以技术规格书规定 SIL1 级的安全仪表回路可采用单一的逻辑控制器；即使逻辑控制器的

SFF < 90%，SIL1 级的安全仪表回路也可以采用单一的逻辑控制器。

SIL2 级要求的硬件故障裕度为 0，SIL2 级安全仪表回路可以用 1 台逻辑控制器，所以技术规格书规定 SIL2 级的安全仪表回路宜采用冗余的逻辑控制器，并没有强制要求逻辑控制器冗余。

SIL3 级要求的硬件故障裕度为 1，因此技术规格书规定 SIL3 级的安全仪表回路应采用冗余的逻辑控制器，在此处有强制要求逻辑控制器冗余。

5. 阿美公司 ESD 系统逻辑控制器冗余和 SIL 要求

阿美公司的 ESD 系统技术规格标准中，要求供应商制造的由模块、操作系统软件和固件组成的 ESD 设备应符合 IEC 61508 的 SIL3 等级要求，甚至通信介质(例如：光缆)应为物理和逻辑的专用设备，不得用于其他非 ESD 功能，且不可以包括其他非 ESD 网络的桥接、路由器或交换机，除非它们是 TUV 认证的 SIL3 安全通信网络的一部分。并且要求 ESD 系统必须使用冗余体系结构进行配置，即双模块冗余 DMR-ESD (1oo2D)表决架构或三模块冗余 TMR-ESD (2oo3)表决架构。

双模块冗余(1oo2D 配置)：ESD 系统使用两个单独的处理器，每个处理器具有自己的单独的 I/O 模块，总线结构，机箱，软件和电源，以 1oo2 布置对输入信号进行表决。

三重模块化冗余 ESD (TMR，2oo3 配置)：TMR 配置的 ESD 系统采用 3 个处理器，这些处理器与三重 I/O，总线结构，机箱和软件并行运行，每个处理器同时且独立地执行其各自的应用程序，验证数据，执行逻辑指令，控制计算，时钟和表决器/同步信号以及执行全面的系统诊断和差异监控。流程输出通过三重路径发送到输出模块，在此处对其进行表决(2oo3)，以确保逻辑和输出完整性。

因此，阿美公司 ESD 系统标准的控制模块冗余设置只有两种选择，即双模卡冗余和三重模块冗余，对比来讲，1oo2 结构可靠性最高，可用性最差，2oo3 结构可用性最好，可靠性较高，并且要求 ESD 系统相关设备均符合 SIL3 等级要求。

6. 结束语

我们可以看到，平均失效概率是衡量安全完整性等级的重要指标，相应的安全完整性等级对应着相应的硬件故障裕度，国内常用规范对相应 SIL 等级安全仪表系统的逻辑控制器冗余做了要求。

同时，阿美公司的 ESD 系统逻辑控制模块冗余和 SIL 等级要求明显是高于国内规范要求的，同时也高于国际标准要求，这固然提高了 ESD 系统的安全性，但也给工程建设带来了较高的成本，这需要国内工程承包商在承接阿美公司项目时，对 ESD 系统的 SIL 等级要求以及相关的冗余体系进行足够的重视和注意。

参考文献

[1] 沈学强, 白焰. 安全仪表系统的功能安全评估方法性能分析[J]. 化工自动化及仪表, 2012, 39(6): 703-706.

[2] 李宏浩. 储气库安全仪表系统 SIL 提升与安全维保优化研究[D]: [硕士学位论文]. 东营: 中国石油大学(华东), 2018.

[3] 李冬, 王孝民. HAZOP、LOPA 和 SIL 方法在设计中的应用[J]. 云南化工, 2019, 46(4): 113-114.

[4] 赵东风, 阚钰烽, 韩丰磊. 基于保护层分析法的安全完整性等级评估方法研究及应用[J]. 石油化工自动化, 2019, 55(1): 49-53.

[5] 黄步余, 叶向东, 等. GB/T50770-2013 石油化工安全仪表系统设计规范[S]. 北京: 中国计划出版社, 2013: 2.

[6] 聂中文, 邓东花, 等. SY/T6966-2013 输油气管道工程安全仪表系统设计规范[S]. 北京: 石油工业出版社, 2013: 24.

[7] IEC (2010) IEC61508-1-2010 Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems Part 1: General Requirements. IEC, Geneva.

[8] 田京山, 王长楠, 王贵波. 安全完整性等级衡量指标探讨[J]. 石油化工自动化, 2017, 53(5): 11-14.

[9] IEC (2010) IEC 61508-2-2010 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems Part 1: Requirements for Electrical/Electronic/Programmable Electronic Safety-Related Systems. IEC, Geneva.

[10] 高继实, 潘辉. 安全仪表系统 SIL 定级的意义[J]. 化工设计通讯, 2017, 43(9): 124.

[11] 宋蓓. 在役罐区安全仪表系统设计方案的研究[J]. 石油化工自动化, 2019, 55(5): 10-12+18.

[12] 杨永光, 金常青, 崔黎宁, 等. 安全仪表系统中传感器冗余配置方式的分析[J]. 石油化工自动化, 2014(1): 14-16.

[13] 周荣义, 钟岸, 任竟舟. 安全系统安全完整性等级确定方法比较研究[J]. 中国安全生产科学技术, 2014, 10(3): 67-73.

[14] 张永辉. 安全仪表系统(SIS)的 SIL 评估[J]. 化工管理, 2019(31): 181-182.

[15] 廖柯熹, 杨艺, 白国红, 等. 输气站场 ESD 系统的 SIL 定级与验证[J]. 中国安全生产科学技术, 2015(1): 161-165.

[16] 付建民, 李成美, 东静波, 等. 数据不确定条件下安全仪表系统SIL等级验证方法研究[J]. 中国石油大学学报(自然科学版), 2017, 41(3): 129-135.