安全仪表系统设计概述

蔡桥路*
河北铭威工程设计有限公司　河北　石家庄　050000

摘　要：文中先对 SIS 系统设计目标、设计原则、安全性和可用性之间的关系进行了分析，最后总结了 SIS 系统的设计步骤。

关键词：安全仪表；安全完整性等级；

DOI：https://doi.org/10.37155/2717-5189-0309-29

引言

当前，我国在石油化工企业的生产过程中涉及大量使用甲类、乙类危险化学品物质，工艺设备及管道不可避免的会存在危险性因素，在新闻报道当中出现的石油化工企业爆炸事故屡见不鲜，造成了巨大的社会影响。政府监管部门和石油化工从业人员不得不深刻反思安全事故，探索如何提高石油化工生产的安全性。

2014年11月原国家安全监管总局出台《国家安全监管总局关于加强化工安全仪表系统管理的指导意见》【安监总管(2014)116号】文件，文件中要求从2018年1月1日起，所有新建涉及“两重点一重大”的化工装置和危险化学品储存设施要设计符合要求的安全仪表系统。其他新建化工装置、危险化学品储存设施安全仪表系统，从2020年1月1日起，应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。

安全仪表系统SIS是指能执行安全功能的仪表系统，是一个相对宽泛概念，包括紧急停车系统ESD、燃烧器管理系统BMS、高完整性压力保护系统HIPPS、火灾报警及气体检测系统F&GS等。

1 安全性与可用性

1.1 安全仪表系统的安全性

安全仪表系统的安全性是指任何潜在危险发生时，安全仪表系统保证使过程处于安全状态的能力。不同安全仪表系统的安全性是不一样的，安全仪表系统自身的故障无法使过程处于安全状态的概率越低，则其安全性越高。安全仪表系统自身的故障有两种类型。

（1）安全故障

当此类故障发生时，不管过程有无危险，系统均使过程处于安全状态。此类故障称为安全故障。对于按故障安全原则(正常时励磁、闭合) 设计的系统而言，回路上的任何断路故障是安全故障。

（2）危险故障

当此类故障存在时，系统即丧失使过程处于安全状态的能力。此类故障称为危险故障。对于按故障安全原则设计的系统而言，回路上任何可断开触点的短路故障均是危险故障。换言之，一个系统内发生危险故障的概率越低，则其安全性越高。

1.2 安全仪表系统的可用性

安全仪表系统的可用性是指系统在冗余配置的条件下，当某一个系统发生故障时，冗余系统在保证安全功能的条件下，仍能保证生产过程不中断的能力。与可用性比较接近的一个概念是系统的容错能力。一个系统具有高可用性或

高容错能力不能以降低安全性作为代价，丧失安全性的可用性是没有意义的。严格地讲，可用性应满足以下几个条件。

（1）系统是冗余的；

（2）系统产生故障时，不丧失其预先定义的功能；

*通讯作者：蔡桥路，1985.10，汉，男，河北石家庄长安区十里铺村，河北铭威工程设计有限公司，自控仪表设计工程师，中级工程师，本科，研究方向：石油化工企业自控仪表工程设计。

（3）系统产生故障时，不影响正常的工艺过程。

1.3 安全性与可用性之间的关系

从某种意义上说，安全性与可用性是矛盾的两个方面。某些措施会提高安全性，但会导致可用性的下降，反之亦然。例如，冗余系统采用二取二逻辑，则可用性提高，安全性下降；若采用二取一逻辑，则相反。采用故障安全原则设计的系统安全性高，采用非故障安全原则设计的系统可用性好。安全性与可用性是衡量一个安全仪表系统的重要指标，无论是安全性低、还是可用性低，都会使损失的概率提高。因此，在设计安全仪表系统时，要兼顾安全性和可用性。安全性是前提，可用性必须服从安全性;可用性是基础，没有高可用性的安全性是不现实的。

2 安全仪表系统的设计目标

安全仪表系统设计的目标，首先是要满足装置的安全度等级要求，衡量标准在于它能否达到要求平均故障概率PFDaverage，即要求下的设备失效的可能性。为了达到装置的安全度等级，系统必须具有高的安全性。但是，系统的安全性越高，必然使设备停车次数越多，维修时间延长，降低了系统的可用性。而在石化等行业的现实应用当中，设备停车可能造成重大的经济损失，这就要求系统既具有高安全性，又具有高可用性。安全仪表系统的设计并不是安全性越高越好，要寻求的是一种最优配置，即在达到安全度等级的前提下，合理配置经济实用的系统。

因此，在设计安全仪表系统时，首先要进行风险分析，确定必要的风险降低指标；然后确定 SIL 等级并进行风险分配，以确定安全仪表系统应承担的风险降低指标;最后，综合考虑系统的安全性与可用性，对系统的结构进行合理配置。

3 安全仪表系统的设计原则

3.1 基本原则

SIL设计的基本原则之一，是应根据E/E/PES安全要求规范进行设计。分析确定SIL的方法，确定的SIL 就是E/E/PES设计时要求实现的安全完整性目标。

SIL设计的基本原则之二，是采取一切必要的技术与措施保证要求的安全完整性。为了实现安全完整性，必须同时满足E/E/PES的随机安全完整性要求与系统安全完整性要求，因为随机失效主要是硬件的随机失效。因此，分析时，随机安全完整性就简化为硬件安全完整性。故障检测会影响系统的行为，因此，它与硬件以及系统的安全完整性都相关。

3.2 逻辑设计原则

①可靠性原则

整个系统的可靠性 R0 (t) 是由组成系统的各单元可靠性(R1 (t) , R2 (t) ,R3 (t)) 的乘积，即 R0 (t) = R1 (t) R2 (t) R3 (t) 。任何一个环节可靠性的下降都会导致整个系统可靠性的下降。人们通常对于逻辑控制系统的可靠性十分重视，往往忽视检测元件和执行元件的可靠性，使得整套安全仪表系统可靠性低，达不到降低受控设备风险的要求。可靠性决定系统的安全性。

②可用性原则

可用性不影响系统的安全性,但系统的可用性低可能会导致装置或工厂无法

进行正常的生产。可用性常用下面公式表示：

$$A = MTBF/(MTBF + MTTR)\ [1]$$

式中 A ——可用度；

MTBF ——平均故障间隔时间；

MTTR ——平均修复时间。

而对于安全仪表系统对工艺过程的认知过程,还应当重视系统的可用性，正确地判断过程事故,尽量减少装置的非正常停工,减少开、停工造成的经济损失。

③故障安全原则

当安全仪表系统的元件、设备、环节或能源发生故障或失效时,系统设计应

当使工艺过程能够趋向安全运行或安全状态。这就是系统设计的故障安全型原则。能否实现“故障安全”取决于工艺过程及安全仪表系统的设置。

④过程适应原则

安全仪表系统的设置必须根据工艺过程的运行规律,为工艺过程在正常运行和非正常运行时服务。正常时安全仪表系统不能影响过程运行,在工艺过程发生危险情况时安全仪表系统要发挥作用，保证工艺装置的安全。这就是系统设计的过程适应原则。

3.3 回路配置原则

为保证系统的安全性和可靠性，以下 2 个原则在回路配置时应当加以注意。

①独立设置原则

用于 SIS 和 BPCS(基本过程控制系统)的信号检测应各自采用检测元件。在SIL3 级时，BPCS 的控制阀不能用作 SIS 仅有的最终元件；在 SIL1 级与 2 级时可以 使用，但要做安全性检查。

②中间环节最少原则

一个回路中仪表越多可靠性越差，典型情况是本安回路的应用。在石化装置中，防爆区域在 0 区的情况很少。因此可尽量采用隔爆型仪表，减少由于安全栅 而产生的故障源，减少误停车。

4 完整的安全仪表回路设计

在系统设计选型时，很容易只要求控制器部分的安全性，忽略了现场仪表的安全要求，实际上安全仪表系统包括了传感单元、逻辑控制单元和最终执行单元，其故障失效率的计算方法如下：

$$PFDSYS = PFDS + PFDL + PFDFE \ [1]$$

式中：PFDSYS — E/E/PE 安全相关系统的安全功能在要求时的平均失效概率

PFDS — 传感器子系统要求的平均失效概率

PFDL — 逻辑子系统要求的平均失效概率

PFDFE — 最终元件子系统要求的平均失效概率

图1 回路子单元结构

5 安全仪表系统的设计步骤

按照安全生命周期的内容，一套完整的 SIS 的设计主要包含以下步骤:

（1）过程系统初步设计,包括系统定义、系统描述和总体目标确认。

（2）执行过程系统危险分析和风险评价。

（3）论证采用非安全控制保护方案能否防止识别出的危险或降低风险。

（4）判断是否需要设计安全控制系统 SIS，如果需要则转第（5）步，否则按常规 控制系统设计。

（5）依据 IEC61508 确定对象的安全度等级 SIL。

（6）确定安全要求技术规范 SRS 。

（7）完成 SIS 初步设计并检验是否符合 SRS。

（8）完成 SIS 详细设计。

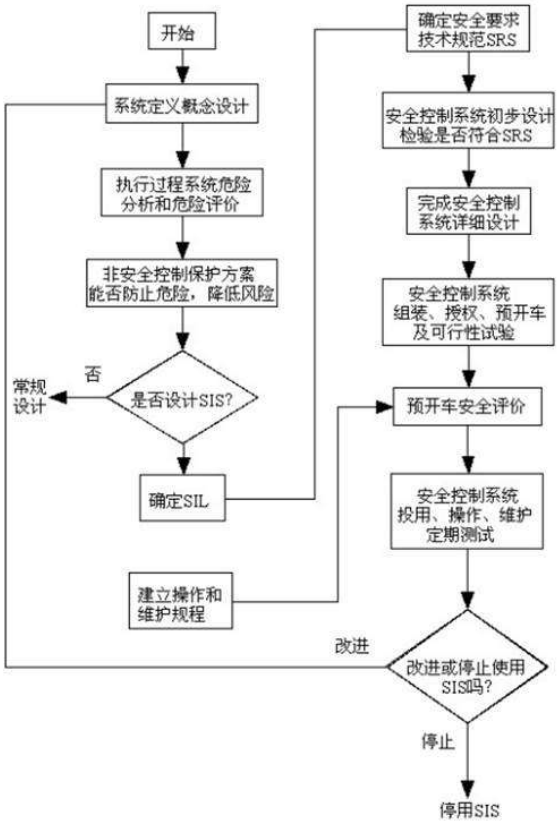
（9）SIS 组装、授权、预开车及可行性试验。

（10）在建立操作和维护规程的基础上，完成预开车安全评价。

（11）SIS 正式投用，操作、维护及定期进行功能测试。

（12）当原工艺流程被改造或在生产实践中发现安全控制系统不完善时，判断安 全控制系统是否停用或改进。

（13）如果需要改进，则转至第(2)步进入新的过程安全生命周期设计。



完整的 SIS 设计的步骤

图2 SIS系统设计步骤

6 结束语

通过以上论述，简单介绍了安全仪表系统的设计步骤，通过这样的设计，能满足安全监管部门对于石油化工企业本质安全设计要求。

参考文献：

[1]《SIL定级与验证》中国石化出版社 朱东利 主编