石 油 化 工 自 动 化, 2007, 2 :18
AUTOMATION IN PETRO-CHEMICAL INDUSTRY

# 石油化工装置安全仪表系统的设计

李胜利,卢金芳
(中国石油天然气华东勘察设计研究院,山东 青岛 266071)

**摘要**: 通过对安全仪表系统的发展过程、安全等级的判定方法、安全仪表系统的设计等内容的阐述,明确安全仪表系统的相关知识及工程设计原则。

**关键词**: 安全仪表系统;安全度等级;显性故障;隐性故障;可靠性;可用性
**中图分类号**: TP273 **文献标识码**: B **文章编号**: 1007-7324(2007)02-0018-05

**The Design of Safety Instrumented System for the Petrochemical Plant**

Li Shengli, Lu Jinfang
(China Petroleum EastChina Design Institute, CNPC, Qingdao, 266071, China)

**Abstract:** The development of safety instrumented system, determination of safety integrity level and design of safety instrumented system is described. Above mentioned content could be used to improve the knowledge and design principle about safety instrumented system.

**Keyword:** safety instrumented system; safety integrity level; overt fault; covert fault; reliability; availability

近年来,生产事故的频发使得安全生产受到越来越多的关注,为确保工厂生产过程的安全,安全仪表系统已越来越多地得到重视并应用。本文通过安全仪表系统在石油化工领域的应用,详细介绍安全仪表的发展过程、安全概念、安全等级及确定、安全仪表系统的设计等内容。

## 1 安全仪表系统的概念和发展过程

安全仪表系统执行必要的安全功能,以使被控对象达到或保持在安全状态,并使所要求的安全功能达到必需的安全完整性。它可以防止危险事件的发生和减少危险事件的影响(有关安全相关系统本身的故障或失效也导致危险事件)。当发生危险事件时,安全仪表系统将采取适当的动作和措施,防止被控对象进入危险状态,避免危及人身安全和损伤设备。在结构上,安全仪表系统由传感器测量元件、控制级设备和最终执行元件等构成。

20 世纪 70 年代中期以前,相关安全系统的控制设备均由电磁继电器组成,部分也采用固态集成电路构成。20 世纪 80 年代开始采用可编程序控制器(PLC)。随着对设备安全、人身安全和环境保护的要求越来越严格,各工业企业和仪表自动化行业对过程安全功能,即有关安全系统的功能安全给予了极大的关注。20 世纪 80 年代中期以后,伴随着微电子技术和控制系统可靠性技术的发展,专门用于有关安全系统的控制器系统、安全型 PLC 和安全解决方案得到迅速发展和推广。

为了促进和规范安全相关的控制和保护系统的设计、制造和应用,国外一直致力于制定相关的标准。欧洲国家处于领先地位,最早的安全相关系统的标准于 20 世纪 70 年代诞生在德国,是有关锅炉/燃烧器启停控制的。此后,随着仪表控制技术和控制系统可靠性技术的发展,为适应各种工业部门对安全相关系统性能要求的不断提高,有关安全相关系统的标准也不断更新和完善,目前国际上常见的标准有:

a) IEC61508 Functional safety of electrical/electronic/programmable electronic safety-related systems;

b) IEC61511 Functional safety: Safety instrumented systems for the process industry sector;

c) ANSI/ISA-84.01 Application of safety

收稿日期: 2006-09-05;修改稿收到日期: 2006-11-21

作者简介: 李胜利(1972—),男,山东单县人,1994 年毕业于西南石油学院计算机专业,工学学士,注册自动化系统工程师(ASE),现就职于中国石油华东设计院,从事石油化工自动化工程设计工作,已发表论文 3 篇。

instrumented systems for the process industries;

d) DIN V 19250 Programmable safety system;

e) NFPA-85 Boiler and combustion systems hazards code (2001)。

其中,ANSI/ ISA-84.01 已经被美国 OSHA (Occupational safety and health administration ——职业安全和健康管理局) 接受,广泛应用于北美。IEC61508 已于 2002 年 8 月份正式成为欧洲标准。中国是 IEC 的重要成员,全国工业过程测量和控制标准委员会也在研究是否将 IEC61508作为中国的国家标准。

## 2　安全仪表系统的安全度等级

安全度等级是用于描述安全仪表系统安全综合评价的等级,指在规定的条件下、规定的时间内,安全系统成功实现所要求的安全功能的概率。安全仪表系统的安全度等级越高,安全系统实现所要求的安全功能失败的可能性就越低。IEC61508 标准根据安全系统满足安全要求的程度将安全系统分为 4 个等级: SIL1～SIL4,SIL1 最低,SIL4 最高。德国 TUV 标准将安全度等级分为 8 个等级: AK1～AK8,AK1 最低,AK8 最高。ANSI/ ISA-84.01 将安全系统分为 3 个等级: SIL1～SIL3,SIL1 最低,SIL3 最高。以 IEC61508 标准为例,安全度等级以故障危险的平均概率 (*PFD*avg) 来表述的,对应关系如下。

SIL1　*PFD*avg = 0.1～0.01
SIL2　*PFD*avg = 0.01～0.001
SIL3　*PFD*avg = 0.001～0.000 1
SIL4　*PFD*avg = 0.000 1～0.000 01

这一定义着重于安全仪表系统执行安全功能的可靠性。在确定安全完整性过程中,应包括所有导致非安全状态的因素,如随机的硬件失效,软件导致的失效以及由电气干扰引起的失效,这些失效的形式,尤其是硬件失效的形式可用测量方法来定量描述。依照 IEC61508 的规定[1],安全仪表系统的可靠性由安全度等级来确定。安全度等级的认定是一个复杂的过程,它要以受控设备 (ECU) 的安全现状评价为基础。IEC61508 对于安全仪表系统安全度的认定也举例列举了认定方法。在设计过程中,这些方法对于安全仪表系统的安全度等级的认定具有借鉴、指导意义。本文介绍其中的一种定性的安全度认定方法: 风险图示法。

风险图示法基于式 (1) 来进行。

$$R = fC \tag{1}$$

式中　$R$ ——在没有安全有关系统时的风险;
　　$f$ ——在没有安全有关系统时危险事件发生的频率;
　　$C$ ——危险事件的后果 (指在健康、安全或者环境危害有关的后果)。

$f$ 由以下 3 个因素确定: 在危险区域发生的危险持续时间和频率;避免危险事件发生的可能性;在没有任何安全有关系统时,危险事件发生的可能性,即意外发生的可能性。这里共引出了下列 4 个风险概念参数 ($C$, $F$, $P$, $W$)。

a) 危险事件的后果 ($C$)。在风险图示中,它被定义为下列 4 种类型: $C1$ ——轻微的伤害; $C2$ ——对 1 人或 1 人以上造成严重的持久的伤害,甚至导致 1 人死亡; $C3$ ——导致数人死亡; $C4$ ——导致很多人死亡的灾难性后果。

b) 在危险区域发生的危险持续时间和频率 ($F$)。在风险图示中,它被定义为下列 2 种类型: $F1$ ——不常发生; $F2$ ——经常、持久地发生。

c) 避免危险事件的可能性 ($P$)。在风险图示中,它被定义为下列 2 种类型: $P1$ ——在一定条件下能避免; $P2$ ——几乎不可避免。

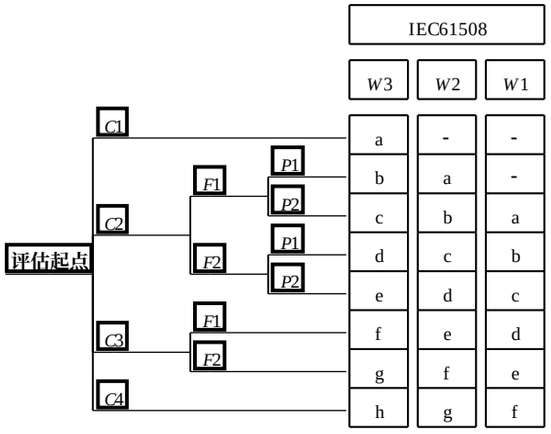
d) 意外事件发生的可能性 ($W$)。在风险图示中,它被定义为下列 3 种类型: $W1$ ——可能性极小,且发生的意外事件具有类似性; $W2$ ——可能性小,且发生的意外事件很少有类似性; $W3$ ——可能性相对高,发生的意外事件具有类似性。

通过上述 4 个参数,依照图 1 便能确定受控设备 (ECU) 的安全仪表系统的安全度要求。

根据上述的风险图示法,例如,现在某炼油装置的 4 种风险参数分别为: $C3$, $F1$, $P1$, $W1$ 根据图 1 导出降低风险必需的最小等级是 d,根据图 1 中的对照表,得出该装置安全仪表系统的安全度等级为 SIL 2。当然,该方法中用到的 4 种风险评估参数 ($C$, $F$, $P$, $W$) 的确定应依据专门的安全评价机构出具的安全评估报告完成。

## 3　安全仪表系统的设计[2]

安全度的确定为安全仪表系统的设计奠定了基础,安全仪表系统的运行模式分为两种: 故障-安全模式和故障-运行模式。故障-安全模式: 系统出现故障,系统将停止运行,装置相关设备进入安全停车状态。故障-运行模式: 系统出现故障,系统将继续运行。




| 降低风险必需的最小等级 | 安全度等级(SIL) |
|---|---|
| - | 无安全性要求 |
| a | 无专门安全性要求 |
| b , c | SIL1 |
| d | SIL2 |
| e , f | SIL3 |
| g | SIL4 |
| h | 一套 E/ E/ PE 安全电子系统不能满足要求 |

图 1 安全度等级评估

石油化工装置安全仪表系统应采用故障-安全模式,安全仪表系统内任一环节的故障,都将使得受控装置停车处于安全状态。正常情况下,安全仪表系统是处于静态的,它"静静"地监视着装置的运行,不需要人为干预,仅在生产装置出现异常情况危及安全时,它才"迅速出手",按照预先设计的方案使装置安全停车。只要装置在运行时,它就必须"在线",不允许被旁路或取代。

这引入了故障的概念,故障分为显性故障(overt fault)和隐性故障(covert fault)。显性故障是指能够显示自身存在的故障,如系统断电、安全 PLC 的卡件故障等,故障会立即被检测出并产生状态报警,在经预设判断确定不能保证完成安全功能时,系统会执行停车动作,使装置处于安全状态。隐性故障是指不能显示自身存在的故障,是不对危险产生报警,并允许危险发展的故障,是一种危险的故障。隐性故障一旦出现,系统因故障的存在而无法动作,使生产装置甚至整个工厂陷入危险的境地。例如系统因常闭触点"粘连"不能正确打开、执行元件如球阀处于"抱死"状态不能关闭,安全仪表系统联锁停车时却动作不了,对生产装置的危害十分严重,后果不堪设想。

显性故障不影响安全仪表系统安全性,但影响系统的可用性。隐性故障影响系统的安全性但不影响可用性。安全仪表系统的设计目标就是使得系统具有零隐性故障,并且尽可能少的影响可用性的显性故障。

3.1 安全仪表系统的可靠性和可用性设计

安全仪表系统应理解为一个系统概念,它包括安全 PLC 及接口设备、检测元件、执行元件。

系统的可靠性是指在一定的时间间隔内,发生故障的概率。整个系统的可靠性 $R_0(t)$ 是由组成系统的各单元可靠性($R_1(t)$, $R_2(t)$, $R_3(t)$ …)的乘积,即

$$R_0(t) = R_1(t)\,R_2(t)\,R_3(t)\,\cdots$$

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。人们通常对于安全 PLC 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。

系统的可用性是指系统可以使用工作时间的概率。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。

安全仪表系统的可靠性和可用性看起来似乎是一对矛盾体。从工厂所有者的角度看,只要安全仪表系统能够满足设计要求的安全等级就可以了,在此基础上,可用性是系统最主要指标,高的可用性减少了装置无谓的停车,提高生产效率。从维护者角度看,安全仪表系统发生任何故障时,那么系统就需要维修,就存在系统失效导致装置停车的危险,这时系统的低故障率是强调的重点,现场检测仪表、执行元件的冗余配置、PLC 的三重化、四重化等结构可能会成为选择。从设计的角度看,安全仪表系统的可靠性、可用性是相互依存的,没有必要也不能使其分开。确定系统的安全等级后,设计人员应根据装置的具体特点、危险性、危害性等确定 PLC 采用何种结构(如二重化、三重化、四重化等),确定系统现场仪表的设置,这个问题甚至可以和业主进行交流,充分了解业主的要求。至于可用性,较高的可用性是生产管理者、维护者和设计者共同的目标,也应该是评价整个系统最基本的指标。

3.1.1　安全 PLC

a) 可靠性。PLC 的可靠性首先应满足安全仪表系统的安全度等级(SIL 1～4 或 AK 1～8),在此基础上,世界上各著名的安全仪表系统制造商均推出了不同结构的系统,有非冗余的、冗余的、冗余容错的、三重化结构(TMR)、四重化结构(QMR),这些系统都取得了 TUV 认证达到相应的安全等级。原则上只要能经认证,并够达到装置要求的安全等级,那么该 PLC 就能应用在该装置上,执行安全保护功能。

常见的 PLC 结构有下列几种方式,均采用故障时性能递减的工作方式。

2-1-0 双重化结构:双重化到单系统,到完全失效(联锁停车)的双通道控制器。

3-2-0 三重化结构:三重化到双重化到完全失效(联锁停车)的三通道控制器。

4-2-0 四重化结构:四重化到双重化到完全失效(联锁停车)的冗余双通道控制器。

在很多文章中针对每种结构的 PLC 及不同的表决方式的可靠性,都有详细定性的分析,本文就不再赘述。

b) 可用性。系统的可用性是系统的基本指标,容错是系统提高可用性的重要手段,容错是指控制器或系统在出现故障时仍能正常工作同时又能查出故障的能力。它需要一定的冗余,I/O 模块、电源、通讯模块等的冗余配置是容错实施的基本条件。容错包括 3 种不同的功能:1) 故障检测——对 PLC 各部件进行诊断确定是否发生了故障;2) 故障鉴别——确定故障来源;3) 故障隔离——PLC 按预设的程序隔离故障,从而在发生故障时能继续工作。

提高系统的诊断覆盖率水平,大大增加了系统的可用率,诊断覆盖率数据一般没有明确的规定值,但它可作为不同系统的对比参数。

为了降低系统的平均修复时间(*MTTR*),提高可用性,安全仪表系统应具有足够数量的备品备件和专门的维护工具等,操作维护人员的技术素养等外部因素也是保证系统可用性的外部条件。

重化、冗余、容错结构的系统配置在提高了系统可靠性的同时,也提高了系统可用性。系统低可靠性时却要求较高的可用性时会造成系统的高成本。在安全仪表系统设计时,任何可靠性及可用性的定性分析结果都不能简单地作为认定某种结构的 PLC 可靠性及可用性高或低的依据,应仔细分析装置对安全仪表系统可用性及可靠性的要求,综合考虑各种因素,选择结构合适的 PLC,并合理进行系统配置。

3.1.2　安全仪表系统检测、执行元件

作为整个安全仪表系统的主要组成部分,检测、执行元件的可靠性及可用性往往得不到充分的考虑,尤其在设计阶段。统计显示,安全仪表系统的故障率分布大致为:检测元件的故障率约为 35 %,PLC 的故障率约为 15 %,执行元件的故障率约为 50 %。从上述统计结果看提高检测元件和执行元件的可靠性是进行安全仪表系统设计的重要环节,对于提高整个安全仪表系统的可靠性有重要意义。

a) 检测元件。为减少检测元件自身的故障率,安全仪表系统的检测元件应选用高性能高质量的产品,特别是智能产品、安全水平认证产品。近来世界著名的自动化公司都推出了具有安全水平认证的变送器产品,相关产品达到了 IEC61508 SIL1～4 安全等级并获得 TUV 认证。使得部分检测元件产品的安全等级(可靠性)有了明确的认定。

在检测元件的设置上,国内外相关的标准规范也对此有明确的描述。在 SH/T 3018-2003 中,分别描述了传感器的独立及冗余原则,SIL2 以上等级的安全仪表系统宜采用独立或冗余配置的检测元件。传感器的冗余配置能够极大地降低系统的故障率,提高系统的可用性,常见的冗余方式有下列 2 种。1) 双重冗余方式。配置 2 套完全相同的检测元件。当重点考虑系统的安全性时,冗余传感器信号在 PLC 内应采用“或”的逻辑运算,即任一检测元件达到安全临界条件均启动安全保护程序;当在安全性满足要求的情况下,重点考虑系统的可用性时,冗余传感器信号在 PLC 内应采用“与”的逻辑运算,即在 2 个检测元件同时达到安全临界条件时才能启动安全保护程序。2) 三重冗余方式。配置 3 套完全相同的检测元件。当检测位置的安全性和可用性均需要保障时,宜采用这种模式设置检测元件,冗余传感器信号在 PLC 内应采用“3 取 2”(2 out of 3)的逻辑运算,即在 3 个检测元件中有 2 个检测元件达到安全临界条件时才能启动安全保护程序。

具体设计时应根据炼油装置或局部检测位置的安全重要程度来确定。对于开关量检测元件,应选用常闭触点的开关测量仪表。

b) 执行元件。在执行元件的设置上,SIL2 以上等级的安全仪表系统宜采用独立或冗余配置的

执行元件。1) 在独立单台执行元件和冗余元件两种方法都有效时,采用高可靠度执行元件通常比执行元件冗余更好,执行元件应优先选用符合 IEC61508 安全度等级并取得相关认证的产品(如电磁阀、智能阀门定位器等)。2) 执行元件采用冗余配置一般有下列两种方式:采用冗余的阀门,每套阀门配套冗余的电磁阀。对于切断回路执行设备应为串联安装的 2 台切断阀;对于放空回路执行设备应为并联安装的 2 台放空阀。执行元件的冗余设置提高了系统的可靠性和可用性,同时也增加了安全仪表系统的成本。工程设计时,应以满足系统可靠性为原则,合理进行执行元件的设计。3) 一般情况下,作为执行元件的电磁阀应采用正常通电方式。

### 3.2 安全仪表系统的逻辑设计[3]

安全仪表系统的逻辑运算是系统的"灵魂和精髓",一套好的安全仪表系统除了可靠合理的硬件配置外,逻辑设计对系统性能至关重要。

#### 3.2.1 输入输出逻辑设计

石油化工装置相关设备进入故障状态运行,这将会导致危险可能发生。因此,安全仪表系统逻辑应按故障-安全方式设计。顾名思义,"故障-安全"中的"故障"是指装置安全仪表系统相关设备发生故障,如前文所述,它分为两类:显性故障和隐性故障,安全仪表系统重要目标之一是减少隐性故障。检测元件、执行元件是隐性故障的重灾区,这对检测元件、执行元件的设计提出了明确的要求。

a) 输入逻辑信号,安全仪表系统的输入信号大部分为开关量信号。当检测元件故障时,其输出的联锁保护临界条件的开关量信号应是可变化的,甚至与检测到联锁保护临界条件成立时的输出信号一致,这样就会减少隐性故障的存在,显然,常开触点(NO)是很难做到这一点的,检测元件的常闭(NC)输出信号便成了安全仪表系统的首选输入信号。一般情况下,按下列原则设计:安全临界检测元件的开关量输出信号为常闭(NC)信号;紧急停车按钮应为常闭(NC)输入信号;检测元件的屏蔽、维护按钮为常开(NO)信号;联锁保护复位按钮为常开(NO)信号。

b) 逻辑输出信号。安全 PLC 的输出至执行元件(电磁阀或电气设备)之间的环节尽可能少。为了提高输出开关量触点的容量,或为了实现与电气设备的隔离,习惯做法是在 PLC 输出卡件后加继电器等,需要明确的是在 PLC 输出卡件满足要求的情况下,应尽可能减少中间环节。

如果执行元件为电磁阀,安全仪表系统输出至电磁阀的开关量信号一般应为常闭(NC)信号,使得电磁阀处于常带电(励磁)状态,保证故障时电磁阀失电(非励磁),相应安全保护动作执行,使受控设备处于安全状态。

逻辑设计时输入输出信号常开、常闭的选择应以减少故障、特别是减少隐性故障到最小为原则,应根据具体情况做出安全分析,合理确定输入输出的逻辑信号类型,不应一概而论。

#### 3.2.2 PLC 逻辑设计

合理使用冗余检测元件的运算逻辑,如前文描述的检测元件三重冗余配置的"3 取 2"、检测元件二重冗余配置的"2 取 1"或"2 取 2"等逻辑形式,以满足所要求的可靠性和可用性。

应采用触发器逻辑电路完成安全保护动作的触发、复位等,减少或避免使用自锁逻辑电路实现安全保护动作。

在工程设计中,逻辑设计的基本形式有逻辑框图、梯形图等形式。逻辑框图是最常用的一种形式,逻辑框图的功能图形符号应采用标准化的、国际通用的形式,最低应符合国家相关标准规范,逻辑框图的因果关系也应简洁明了,使得逻辑框图易懂、实效。

## 4 结束语

通过本文对安全仪表系统的发展过程、安全等级的判定方法、安全仪表系统的设计等内容,阐述了安全仪表系统的相关知识。对石油化工装置及相关领域的安全仪表的设置、应用提供了完整明确的思路,对于石油化工领域的安全生产必将产生促进作用。

**参考文献**:

1 IEC61508 (2000), Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-related Systems-Part 1～7

2 IEC61511 (2003), Functional safety-Safety instrumented systems for the process industry sector-Part 1～3

3 SH/ T 3018-2003,石油化工安全仪表系统设计规范