

浅谈在 BPCS 和 SIS 系统中的共享设备的信号连接方法

袁汉福 付卫红

中化化工科学技术研究总院有限公司

摘要：本文探讨了在确保 SIS（Safety Instrumented System，安全仪表系统）的安全完整性等级，并遵守 SIS 系统的安全生命周期标准的前提下，如何实现 SIS 与 BPCS（Basic Process Control System，基本过程控制系统）共用同一台阀门、电动机泵或传感器。当 SIS 和 BPCS 共享设备导致操作模式从较低需求转变为持续运行模式时，文中强调了相关组件的维护程序和策略必须相应调整的重要性。并进一步分析了在不同场景下 SIS 与 BPCS 共享设备的几种可行配置方案，并通过实例展示了信号连接的具体方法。

关键词：SIS 安全仪表系统；SIL 安全完整性等；SIF 安全仪表功能；BPCS 基本过程控制系统

在石油化工及煤化工行业中，大多数生产装置的控制与安全保护采用的是 BPCS 基本过程控制系统（以下 BPCS 全部使用“DCS”代替）和 Safety Instrumented System 安全仪表系统（以下简称“SIS”）。有时，一个过程信号需同时应用于 DCS 和 SIS 系统中，某些设备也需要被这两个系统共同使用，比如切断阀。在这种情况下，DCS 的顺序控制和 SIS 的联锁保护都需作用于同一台切断阀上，这意味着切断阀必须能够接受来自 DCS 和 SIS 两个系统的独立控制指令。

为了妥善处理这些信号关系，确保既符合 DCS 控制和 SIS 联锁的需求，又满足 SIS 系统的安全标准，必须采取有效的措施来降低控制功能与安全功能同时失效的风险。这通常涉及到精心设计的信号优先级、故障检测机制以及冗余配置等方面的技术手段，以保障系统的整体安全性与稳定性。

1 DCS 和 SIS 系统的区别

DCS 系统是过程控制系统，是动态

的。它始终对过程变量连续进行检测、运算和控制，对生产过程进行动态控制，确保产品的质量和产量，用于日常生产控制运行，需要人工频繁地干预，执行生产功能、实时控制。

SIS 系统是静态的，正常工况时，它始终监视生产装置的运行，系统输出不变，对生产过程不产生影响，非正常工况下时，它将按照预先的设计进行逻辑运算，进行联锁动作，保证人员和生产装置安全。一般情况下不需要人为干预。SIS 系统要求严格、可靠。SIS 系统比 DCS 系统在可靠性、可用性上要求更严格，所以 SIS 系统应独立于 DCS 系统，并独立完成安全仪表功能。

需要强调的是 SIS 系统独立设置原则：Safety Integrity Level。安全完整性等级（以下简称“SIL”）1 级逻辑运算器宜与 DCS 分开，SIL2 级逻辑运算器应与 DCS 分开，SIL3 级逻辑运算器必须与 DCS 分开，即只有在 SIL1 和没有 SIL 等级要求的情况下，同时满足国家相关法令的条件，可以考虑控制、联锁功能在 DCS 系统中完成。

2 DCS 和 SIS 共用元件(设备)的条件

在确定控制方案前，必须确保该方案符合化工装置风险识别、危险与可操作性分析（HAZOP）、重大危险源辨识以及安全仪表功能评估报告等文件的要求。此外，还需遵循涉及“两重点一重大”（即重点监管的危险化学品、重点监管的危险工艺和重大危险源）装置的相关政策、规范及国家法律法规的要求。例如，根据安监总局 40 号令的规定，对于涉及毒性气体、液化气体、剧毒液体的一级或二级重大危险源，必须配备独立的安全仪表系统（SIS），在这种情况下，则不应采用共用元件的方案。

DCS 和 SIS 共用元件必须满足以下要求：

- 1) 必须符合安全全生命周期的所有要求，必须有完善的确认、验证和记录。
- 2) DCS 和 SIS 共用元件会引起操作模式的改变，由低要求模式变为连续模式，相关元件的维护规程和策略均应相应改变。
- 3) SIS 和 DCS 共用元件（变送

器、阀门)对 Safety Instrumented Function, 安全仪表功能(以下简称“SIF”)的要求都有影响。只有满足共用元件的要求时危险失效平均概率足够低,相关 SIF 经验证满足其安全完整性等级要求,符合安全生命周期的所有要求、充分考虑了 DCS 操作维护等对 SIS 的影响,以及按照功能安全标准要求编制相关检测及维护规程等前提条件后才能共用。如果 BPCS 和 SIS 共用元件,DCS 为独立保护层,共用元件应该同时担负原来 DCS 和 SIS 各自独立的保护层职责。

3 信号共用处理方法

3.1 一个信号源分别送给 DCS 和 SIS 系统

在工程设计中,我们经常遇到需要将同一个过程参数的信号同时输入到 SIS 和 DCS 系统的情况。当安全级别要求较高时,建议分别安装 2 台变送器,各自配备独立的取源部件,信号分别接入 SIS 和 DCS,以确保系统的独立性和可靠性。

然而,在安全要求相对较低且符合相关规范和国家法律法规的情况下,可以考虑使用单台变送器。此时,可以通过特定的连接方式,如图 1 所示,将信号同时传输至 SIS 和 DCS 系统。这种方式不仅简化了系统结构,而且减少了设备数量,同时也降低了成本,但前提是必须保证不会影响系统的整体安全性和功能性。

一台现场变送器信号直接硬接线连接到 SIS 系统,变送器的供电由 SIS 提供。若是本安回路,可以通过安装在 SIS 系统机柜的一进两出的安全栅实现该信号分给 DCS 系统。若是一般隔爆回路,可以通过安装在 SIS 系统机柜的一进两出的隔离器将实现该信号分给 DCS 系统。输送给 DCS 的信号通过一进两出的安全栅或隔离器的出口硬接线连接实现,并没有涉及到 SIS 系统的 I/O 卡件。

这个信号可以用于 DCS 信号显示、控制、联锁等用途。

规范规定:“当使用单独的 SIS 传感器时,通过适当的隔离器把信号转发给 DCS 是有好处的”^[1],所以变送器应具有安全功能要求和自诊断功能,确保变送器的可靠和安全,以及 SIS 系统能在要求的时间内把过程置于某个安全状态。

一台现场变送器信号直接硬接线连接到 SIS 系统, SIS 系统通过通讯将该信号连接到 DCS 系统,这个信号用于 DCS 信号显示,不能用作控制、联锁等用途。

3.2 控制阀门阀位开关信号的连接

SIS 系统的被控对象输出的辅助信号可以连接到 DCS 系统。例如, SIS 系统切断阀的阀位信号,如果不需要参与 SIS 的联锁逻辑,则可以直接接入 DCS 系统;若需要参与联锁,则应首先接入 SIS 系统。在某些情况下,即使阀位信号不参与联锁,也可以先接入 SIS 系统,再由 SIS 系统通过通信接口将信号传递给 DCS 系统。这样做的好处是,即便阀位信号仅用于操作员监控和报警,也不必经过复杂的信号路由,但如果阀位信号需要参与到联锁或其他关键安全功能中,直接接入 SIS 系统是必不可少的。至于调节阀的控制信号,则通常由 DCS 系统负责实现。

如图 2 所示,调节阀参加 SIS 联锁,调节阀需要设置阀位开关(不参加联锁的调节阀不需要设置阀位开关)。参加联锁的调节阀的阀位开关只设置联锁位置的阀位开关。切断阀和调节阀的阀位信号全部接入到 DCS 系统,这样做便

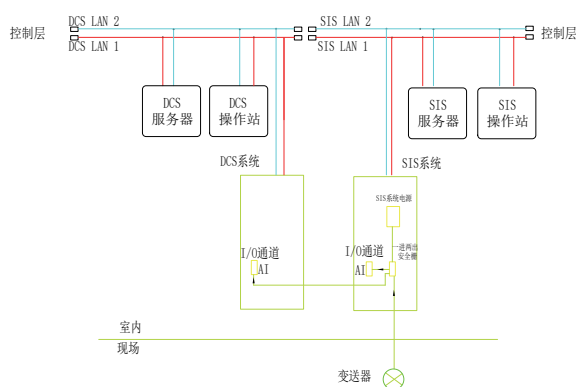


图 1 现场变送器供电和信号连接示意

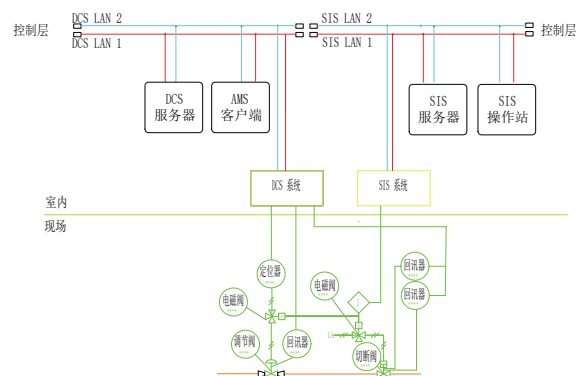


图 2 执行机构信号的连接示意

于操作人员的观察。

4 共用设备的信号连接方法

当 SIS 系统联锁一台机泵的启停动作,同时 DCS 系统的操作站也可以手动启停该机泵。有的操作是 DCS 通过通信的方式把动作命令传输给 SIS, DCS 命令通过硬接线传送到 SIS, 参加 SIS 系统的逻辑运算。规范规定:“基本过程控制系统不应介入安全仪表系统的运行或逻辑运算”^[1],所以 DCS 与 SIS 之间是不能使用通信传输这类动作命令的,也不可以通过硬接线传送动作命令信号。

解决方案:如果 SIS 的联锁回路的安全级别是 $\leq$ SIL 1 或没有 SIL 等级,且符合本文上述的所有要求,可以把整个联锁逻辑全部移到 DCS 中完成,否则 SIS 联锁逻辑依然在 SIS 实现,DCS 的启停命令直接输出到 MCC 去,不经过 SIS 实现,如图 3 所示,然后需要在电气的控制回路中增加一

个 DCS 的停车接口。

当一台切断阀既参加 SIS 的联锁,又参加 DCS 的顺序控制,同样是共享设备的问题。“当 DCS 和 SIS 功能使用单一阀门的情况下,设计应保证 SIS 动作超迟 DCS 动作,一般可以通过把 SIS 直接连接到一个电磁阀上来达到这个要求,电磁阀可以直接断开执行器的动力源,例如在阀门定位器和执行器之间”^[1]。

解决方案:如果 SIS 的联锁回路的安全级别及所有安全要求满足要求,可以把整个联锁逻辑全部移到 DCS 中完成,这样联锁和顺序控制均在 DCS 中实现。

如果 SIS 的联锁回路的安全级别要求高,可以使用 2 台切断阀实现,1 台作为 SIS 联锁用,1 台作为 DCS 顺序控制用。这样做需要增加设备,也可以使用 1 台切断阀,配置 2 台电磁阀,1 台电磁阀参加 SIS 联锁,另 1 台电磁阀参加 DCS 的顺序控制,这种方式要通过 PDF 计算以保证安全功能的要求,如图 4 所示。

当调节阀一方面要参加调解,另一方面需要参加联锁,同样是 DCS 和 SIS 两个系统共享一台设备的问题。如果安全级别要求比较高,联锁切断功能新设置一台切断来完成,但是当安全级别的要求不是很高的情况下,也可以在调节阀的气路上加装电磁阀,电磁阀的信号来自 SIS 系统,如图 5 所示。这种设置的安全要求比独立设置切断阀要低,比全部在 DCS 系统中实现调节和联锁要高,具体要求应当看联锁回路的安全功能 SIL 的要求,和国家有关法令法规的要求来确定。

在一条管线上,存在 DCS 的调节阀和 SIS 联锁用的切断阀,调节阀也参加 SIS 的联锁,当 SIS 的联锁触发时,切断阀动作,并要求 DCS 的调节阀同时动作到安全位置,指挥调节阀的阀门定位器输出到安全位置,不是通过在调节阀的气路上的电磁阀的动作完成,规范规定:“安全仪表系统不应介入或取代基本过程控制系统的工作”^[2]。按照

这个规定, SIS 系统是不能给 DCS 传输这个信号,在有些国外工艺包中,类似情况 SIS 是通过通信方式传输给 DCS 的。

解决方案:将切断阀的阀位回讯接入 DCS 系统,在 DCS 中检查切断阀的阀位回讯信号如果在安全位置,DCS 调节器的输出也调整到安全位置,调节阀和切断阀的阀位回讯信号进行比对,不一致时进行报警。

5 结语

在工程设计前期,完成 SIF 安全功能评价是非常重要的。每个联锁回路应有明确的 SIL 等级要求,这为工程设计提供了依据。然而,有些工程项目并未进行安全功能评价。在这种情况下,自动化控制人员和工艺人员需要进行充分沟通,明确联锁的重要性的和一旦发生事故可能造成的危害程度,从而初步估算出一个 SIL 等级作为联锁回路设计的依据。

SIS 和 DCS 系统共享设备是一个要求极为严格的过程。只有在所有前提条件均得到满足的情况下,方可实施。这包括但不限于确保系统符合安全完整性等级要求、遵守安全生命周期管理标准、合理配置信号连接以及制定相应的维护策略。通过严格的管理和技术措施,可以确保系统既满足安全要求,又能够高效运行。

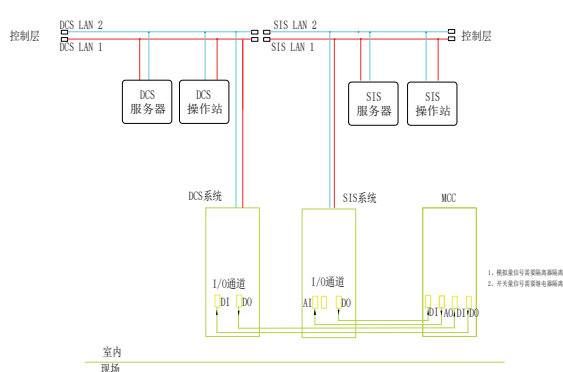


图3 控制系统与MCC的接线示意

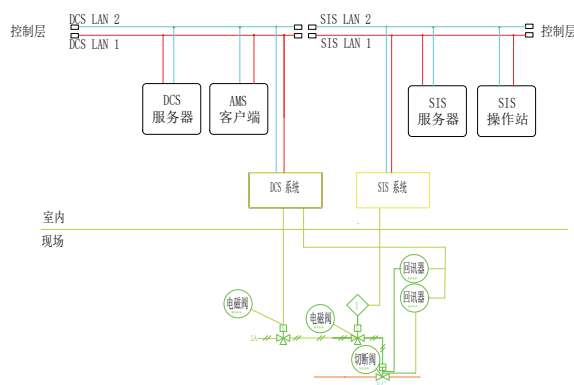


图4 双电磁阀信号连接示意

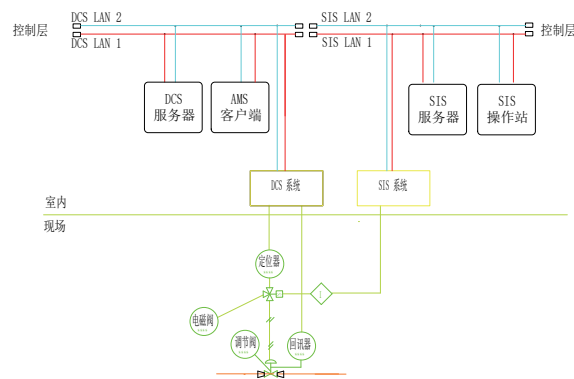


图5 执行机构信号连接示意

参考文献:

- [1] 全国工业过程测量控制和自动化标准化技术委员会 (SAC/TC124), 过程工业领域安全仪表系统的的功能安全: GB/T—21109.2—2007[S]. 北京: 国家市场监督管理总局、国家标准化委员会, 2007.
- [2] 中国石化工程建设有限公司, 石油化工安全仪表系统设计规范: GB/T 50700—2013[S]. 北京: 中国计划出版社, 2013.