

石油化工行业整体安全探讨

石油化工企业的安全设计和运维——过去的这些年，社会经济的不断发展使得过程工业的规模越来越大，带来的整体系统所面临的风险也随之增加，以石油天然气开采运输、石油以及化工等为代表的过程工业，在为我国的经济生产建设发挥重要作用的同时，其本身面临的安全形势也十分严峻。一旦发生事故，不但会使企业蒙受重大的经济损失，也会给社会带来不稳定的因素。因此，石油化工企业的安全设计和运维尤其重要，本文从全生命周期管理和独立保护层设计两个维度，探讨石油化工行业整体安全考虑的内容。

文 / 边文艺

整体安全的定义

整体安全贯穿于工厂规划、设计、建设、试车、投产和运行维护的全生命周期。

设计阶段对安全问题进行科学周密的考虑，通过基于严格机理的工艺过程模拟，可以从源头消除隐患，化解风险，避免设计上的“先天不足”，对于工艺设计不能消除的固有风险，需要做预先危险性分析，有效识别危险事件，了解危险事件的原因和后果，在此基础上设置必要的独立保护层，将过程风险降低到可接受的水平，独立保护层包含过程控制层、安全控制层、主动保护层、被动保护层和应急响应层。运行维护阶段对各个保护层状态的检测和维护可以确保每个保护层能够按照预期实现其风险降低能力。

随着信息化和工业化融合的不断深入，工业控制系统从单机走向互联，从封闭走向开放，从自动化走向智能化。在生产效率显著提高的同时，工业控制系统面临着日益严峻的网络安全威胁。在当前技术环境下，单纯的物理隔离和外部硬件防火墙已经不足以保障工业系统的网络安全，必须实施更有效的信息安全升级方案在各个层面上应对来自系统外部和内部的威胁。同时，网络安全防护系统必须进行持续审查和评估。

整体安全设计是石化安全生产中至为重要的环节，对石化安全生产具有决定性的作用。整体安全关注的内容如图1所示。

行业自身的性质，使得其存在很多的安全隐患。所以，作为石油化工生产中最为首要的任务就是合理的规划、设计整个工艺流程，为后续的安全生产奠定基础。而所谓技术上的石油化工工艺设计，其主要内容是通过工艺计算等方法绘制工艺流程图，包括设备布置、工艺流程设计、电气仪表设计以及管道布置等内容。需要各个部门相互配合，相互协作，共同完成石油化工工艺设计的工作。

PROCESS-Tip

* 更多信息请扫描二维码：



chem.vogel.com.cn

* 反馈编码：A202125

本文作者供职于施耐德电气（中国）有限公司。

一体化安全设计

由于石油化工

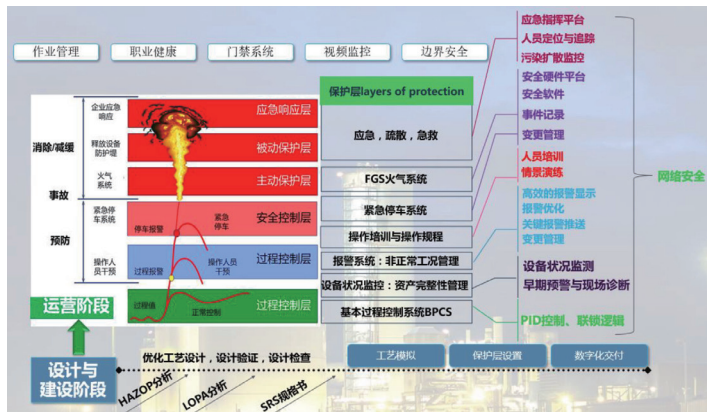


图1 整体安全概览

施耐德电气的 UDE 一体化设计平台,可以实现多专业多用户协同工作, UDE 一体化设计平台包含了工艺仿真计算 (PRO/II)、P&ID 设计 (Diagrams)、电气仪表系统设计 (Electrical & Instrumentation) 和多专业三维布置设计 (PDMS/E3D) 等功能,可以实现:同一项目环境下进行集成管理;用户随时从不同的应产品中访问数据;异地协同设计;由数据标准驱动的管理。

安全设计数字化交付

随着信息技术和互联网技术的飞速发展,数字化转型已成为企业提升竞争力的必然选择。国家住建部 2018 年 9 月颁发了 GB/T51296-2018《石油化工工程数字化交付标准》,数字化交付是建设数字化工厂的核心基础,可以确保实现设计、采购、施工和调试及运维等工程全生命周期各个阶段的数据信息共享,安全管理作为工厂运行维护的核心内容,安全设计资料的完整交付是运行期间安全维护的基础。施耐德电气的 AVEVA NET 数字化交付平台可承载和管理数字化交付信息,与多种工程软件集成并兼容多种文件格式的信息,提供可视化的展示工具,方便查看包含安全相关设计、施工以及安全数据移交的细节等。数字化交付过程如图 2 所示。

独立保护层

过程控制层

1. 基本过程控制系统

基本过程控制系统一般由 DCS 或 PLC 实现,实现基本的过程控制,以保证生产过程的工艺参量接近给定值或保持在给定范围内。控制系统的控制水平决定了基本过程控制系统作为独立保护层的风险降低能力。

施耐德电气用于控制性能优化的控制顾问 (Control Advisor) 可以实时监测控制回路,诊断回路存在问题,如回路振荡、PID 参数设置或仪表以及阀门问题等等,可以帮助改进控制水平和操作水平,减少波动、提高 PID 控制效果,如减小偏差、缩短响应时间等,由此提高自控率,降低操作风险,提升装置安全性。

2 设备状态检测

以往由于缺乏准确的方法来判断设备失效的确切时间,设备维护运营者不得不面临冒着发生故障停机的风险使其寿命最大化,或者提前更换正常部件以最大限度保障设备正常运行。预测性维护技术能够确保设备使用寿命最大化的同时,又能有效避免发生非计划停机。预测性维护技术旨在通过大数据分析,提前预测关键设备的健康状态,避免发生意外停机或缩短停机时间,最大限度地提高生产效率和生产安全性。

施耐德电气强大的 PRiSM 设备状态预测解决方案,首先建立不同设备的故障识别模型,然后灌入历史数据,进行机器学习,实时监测关键设备健康状况以及表现效

率,在设备出现故障之前提前进行预判。可以减少非计划停机;降低维护成本;延长设备使用寿命;识别可能影响设备绩效下降的因素;提高生产安全。

3 报警管理

实时监控报警是在生产工况发生异常时对操作人员进行第一时间提醒的重要工具,设置过程报警和系统报警的目的是为了确保设备的完好性以及工厂生产的连续性。一般情况下,在 DCS 中几乎每一个组态点都设置有个报警,一个 PID 回路通常包括回路完整性报警、高量程报警、设定点偏差报警和许多的其他报警。

实际使用过程中,有时报警太多会有碍操作人员正常操作,太少又不利于及时发现生产问题。普遍情况下,DCS 画面满盘数据闪烁,报警框不停闪烁,不仅影响正常操作与监控,而且造成操作人员的麻痹思想,熟视无睹,甚至直接关闭声光报警设备。此外,操作人员在短时间只能关注和处理一定数量的报警。

采用先进的 DCS 报警管理技术能够有效地剔除不必要的干扰,让操作人员能够更好地处理装置操作中产生的问题,有效提高装置的稳定性和安全性。

施耐德电气的报警管理系统 (System Advisor) 是一套用于建立完整报警系统的解决方案。报警管理系统软件的设计和解决方案的实施符合 EEMUA 191 与 ISA-18.2 国际标准,旨在建立一套有效的报警管理系统,提高操作员对异常状况的响应效率和能力,从而提升工厂的安全性。

4 人员培训和应急演练

操作员对过程报警的处理作为保护层设计的一部分,并不代

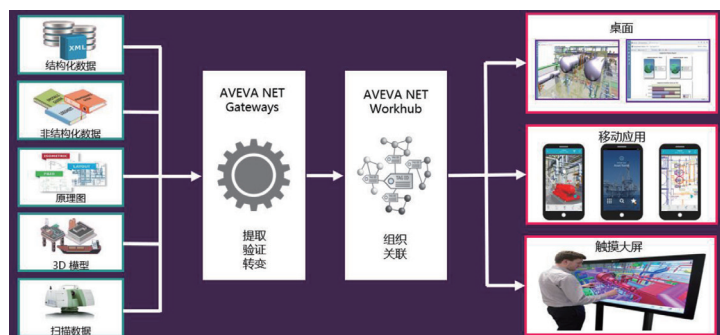


图 2 数字化交付

表设置了操作员就一定能够达到期望的风险降低能力, 操作员操作水平的高低决定了其风险降低能力的高低,

现代工厂的工艺过程和控制策略越来越复杂, 对装置工程师、生产操作员来说提出了很大挑战, 他们必须学习掌握这些新的、先进的控制系统, 熟悉调节控制的方法, 全面掌握和了解工艺过程中本身的原理及其动态特性等等。他们的工艺知识、经验和技能水平是工厂安全、顺利开工的前提, 也是保持平稳生产和安全生产的必要条件。

施耐德电气操作培训系统 (Operator Training System, OTS) 可以帮助运维人员获得全面的、全流程的和动态的工艺知识和操作体验, 并对控制方案深入了解和认识。在 OTS 中可以模拟设置多个场景, 基于 VR 和 AR 技术, 实现沉浸式应急演练培训。

安全控制层和主动保护层

安全仪表系统 (Safety Instrumented System, SIS) 作为独立保护层中最关键的部分, 是指用于实现一个或几个安全仪表功能的系统, 由传感器、逻辑控制器、最终元件及相关软件组成。安全控制层的紧急停车系统 (ESD) 和主动保护层的火灾报警和气体监测系统 (FGS) 都属于安全仪表系统的范畴。

安全仪表功能 (Safety Instrumented Function, SIF) 是指由安全仪表系统执行的安全功能, 安全仪表功能具有某个特定的 SIL, 同其他保护层一起参与风险的降低。安全仪表功能的管理可以确保安全仪表系统按照设计要求和预期工作, 达到相应的风险降低能力。

施耐德电气提供的 Triconex 安全仪表系统、报警与旁路管理工具 (Safety View)、安全应用逻辑自动测试工

具 (TSV) 和安全系统顾问 (System Advisor) 等获得了业界的高度认可, 如埃克森美孚、Reliance、雪佛龙以及利安德巴塞尔等很多国际能源巨头都选择了施耐德电气提供的 “SIF Manager” 平台作为安全仪表功能的管理工具来帮助他们自信地管理过程风险。图 3 是施耐德电气 Triconex 安全系统的系列产品。

被动保护层和应急响应层

被动保护层主要依靠前期设计的一些物理保护措施将已经发生的风险后果尽可能降到最低, 物理保护措施主要有压力泄放阀、火炬和罐区围堰等等

应急响应层承担事故应急响应调查及响应工作, 包含重大危险源管理、应急资源和应急预案数据库、应急响应联动处置、应急信息发布交换等内容

施耐德电气的 Wonderware 应急指挥平台, 提供应急预案数据库, 融合了应急指挥、人员定位与追踪、工业电视监控、门禁系统、作业管理、职业健康、环保在线监测和短信群发系统等模块, 可以协助安全管理执行团队最大程度将事故影响降至最低。

网络安全

工业控制系统网络安全防护是指, 通过实施技术和管理措施, 避免工业控制系统遭到非授权或意外的访问、篡改、破坏及损失。

首先从综合评价的角度, 运



图 3 Triconex 安全系统

用科学的方法和手段, 系统地分析和诊断工业控制系统所面临的威胁及其存在的脆弱性, 评估企业工业控制系统安全防护水平。提出有针对性的抵御威胁的防护对策和整改措施, 最大限度地保障工控系统网络安全, 防止工控系统的崩溃或瘫痪, 保障工控系统的安全稳定运行。

施耐德电气网络安全升级解决方案, 通过对工控系统实施安全分区、网络专用、横向隔离以及纵向认证等技术手段, 加强构筑工控系统边界安全防护网的同时, 也特别注重工控系统内部的安全防护能力, 采取身份认证、主机加固、病毒防护、入侵检测、系统恢复和安全审计/监测等措施, 进行多层面的信息安全防护, 最终形成完善的信息安全防护体系。

同时, 施耐德电气还提供各类丰富、专业的工业信息安全培训, 并在系统维护中, 持续改进安全方案、建立工控系统变更流程和应急预案, 提供全生命周期的工控系统网络安全服务。

结束语

风险永远不可能完全消除, 但风险可以更好地管理和降低, 重大危险事件很少是由单一原因造成的, 而是由多个保护措施同时失效造成的特殊事件, 因此, 优秀的整体安全工程设计和科学的管理维护, 可以保障装置的安全平稳生产, 实现企业可盈利运营。