案例 1

北京威努特技术有限公司

石油销售公司油库生产系统网络安全能力升级改造项目

基于“行为白名单”的油库生产系统安全防护技术

引言：

石油销售公司下辖油库均采取炼厂直输进库，管道、铁路、公路出库的“一进三出”方式，是中国石油在多省份成品油资源的重要集散地，承担着保障油库所在地区的后路畅通和成品油市场稳定供应的重任，配送范围覆盖半个中国。经过“十五”以来近十五年信息化建设，实现了从“集中”到“集成”的飞跃，促进了“两化”的深度融合。目前，销售信息化已完成大规模全局性信息系统建设和系统集成，逐渐完成系统提升与集成应用工作，正在迈向商业智能、决策支持方向发展，提高信息利用与共享能力，通过信息化建设促进油库主营业务转型升级。原来相对分散、独立的装置通过内部网络连接到一起，数据耦合程度增加，使得来自于外部和内部的网络安全风险增加，油库生产系统的网络安全建设迫在眉睫。

本方案结合相关国家标准、行业要求，采用“白环境” 的纵深防御安全防护技术体系架构，积极开展网络安全升级改造建设，提升自身网络安全防护能力。

一、项目概况

石油销售公司借鉴相关安全管理规定，参照等级保护以及指导方案要求，结合部署在总部数据中心系统和部署在库站系统的实际，制定了基于“行为白名单”的“纵深安全防御”技术方案，满足等保 2.0“一个中心、三重防护”以及中石

油信息处规划总院的《销售工控系统安全防护指导方案》要求，进而构筑油库生产系统“安全可信环境”，达到“只有可信任的设备，才能接入控制网络”、“只有可信任的消息，才能在网络上传输”、“只有可信任的软件，才允许被执行”的防护效果。并且在此项目中创新应用基于“行为白名单”建立的面向工控 PLC 设备的行为模型固化技术，结合油库生产系统业务流程，利用智能技术，以时间周期维度作为判断，发现工控指令隐藏的多重复杂周期模式，建立工控指令复杂周期场景指纹模型。通过该模型对工控指令和生产工艺行为进行更加精细化的解析和管控，解决“传统白名单”只能静态对工业控制协议指令识别的劣势，避免因指令时间错误引起异常，有效识别误操作、网络攻击、恶意操作等，保证工控业务稳定运行。

项目建设完成后全面提升了油库生产系统的整体安全性，确保设备、系统、网络的高效运行，减少运维人员的工作量，提高了安全生产管理水平、工作效率以及管理效率。并且此项目在国内石油销售板块具有“标杆”意义，能够在国内其它销售公司进行广泛推广。

1. 项目背景

油库是国家重要的能源基础设施，应做为安全防护的重点对象。由于燃油的易燃、易爆特性，在其储存及运输的过程中面临着诸多风险，一旦管理不当，将有可能引发重大安全事故，其中因油库生产控制系统异常所导致的安全事故已屡见不鲜。攻击者基于对目标系统所使用的工控协议及工业流程的深入了解，通过更改控制命令，导致安全事件的发生，甚至影响到广大人民群众的生命财产安全。比如，恶意下发非法工控指令，控制油库压力升高、停止发油业务等。

油库生产系统在销售系统的应用流程中属于关键业务模块，通过油库中库级系统与工控系统集成，共同协作完成进销存自动管理。在油库生产场景中，石油销售公司生产系统的主要威胁来自于上位机和下位机的通信，因为上位机就是普通的计算机，由人操作，很容易感染病毒、木马入侵或人为恶意破坏，形成恶劣影响。在勒索病毒爆发时，石油销售公司部分油库库级系统出现不同程度病毒感染，导致生产系统无法正常运行。因此需要依据网络安全法、等保 2.0 以及中石油公司下发的指导方案要求积极开展网络安全升级改造建设，提升自身网络安全防护能力。

2. 项目简介

石油销售公司油库库级生产系统与工控系统集成，完成油库进销存的自动管理。油库一般以专线方式接入到广域网，目前大部分油库与广域网边界无安全防护措施，信息网与工控网之间未作有效隔离，工控主机无有效安全防护措施，工控软件及操作系统存在漏洞，设备联网机制缺乏安全保障，业务及用户行为无有效审计手段，组网混乱。因此需开展油库生产系统网络安全改造推广项目，削弱或根除安全风险，提高油库生产系统的网络安全防护能力。

3. 项目目标

油库是协调原油生产、原油加工、成品油供应及运输的纽带，是国家石油储备和供应的基地，它对于保障国防和促进国民经济高速发展具有相当重要的意义。本次油库网络安全改造推广项目旨在全面提升石油销售公司油库生产系统的整体安全防护水平，保障设备、系统、网络的可靠性及稳定性，提高安全生产管理水平和工作效率，满足我国等级保护相应等级的防护要求及国家相关政策法规、标准要求，从而实现以下项目目标：

首先，按照生产系统重要程度，按照不同流程规划不同安全区域，通过技术手段实现安全区域边界的“白环境”，实现访问控制白名单固化、工业协议白名单固化、业务白名单固化；其次，针对油库生产系统的安全计算环境载体实现应用锁定、系统锁定、外设锁定、网络锁定，建立工控主机的安全管理中心、安全状态监测中心；再次，通过监测生产系统内关键网络节点的业务流量，实现工控网络异常流量监测、异常事件监测。

在油库过程监控层建设工业安全运营中心，实现工业资产的主动发现、漏洞无损扫描、网络攻击检测、安全运维、日志记录。通过统一安全管理平台实现工控网络安全产品的统一策略下发，提高运维效率，降低维护成本，构建“一个中心、三重防护”的安全体系架构。

二、项目实施概况

本项目采用“行为白名单”核心技术，结合石油销售公司油库生产系统业务流程，建立精准的安全防护模型，实现了办公网与生产网物理隔离、主机加固及

防护等，最终通过项目验收，达到预期防护效果。

1. 项目总体架构和主要内容

项目以 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》、工信部信软〔2016〕338 号《工业控制系统信息安全防护指南》等国家标准为依据，采用“行为白名单”的纵深防御安全防护技术体系，从“一个中心、三重防护”的角度出发对油库生产系统进行统一规划、统一建设，进而构筑油库生产控制系统安全“可信环境”，确保：

（1）只有可信任的设备，才能接入系统网络；

（2）只有可信任的消息，才能在系统网络上传输；

（3）只有可信任的软件，才允许被执行。

项目总体架构设计图如下所示：

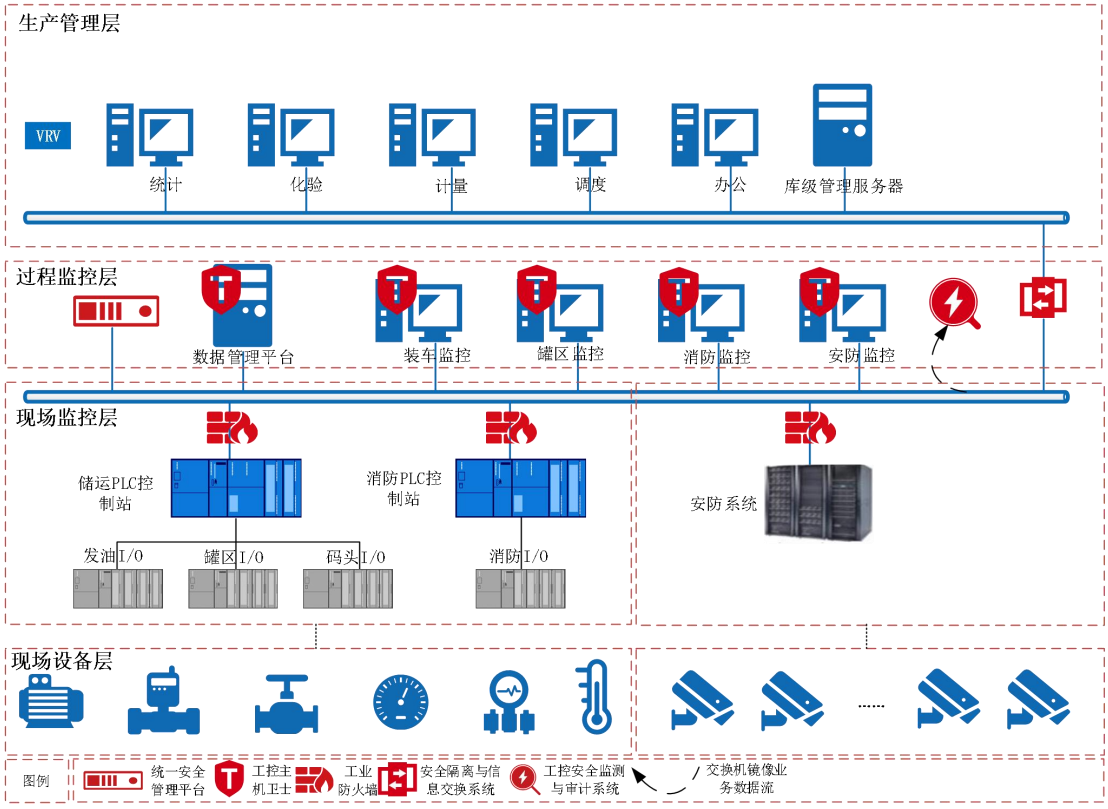

图 2-1 项目总体架构设计

项目主要建设内容涉及以下方面：

✓ 构建区域边界“白环境”，在油库现场设备层和现场监控层之间部署工业防火墙，建立访问控制白名单和工业协议白名单，实现“值域级”的细粒度访

问控制；在过程监控层和生产管理层部署安全隔离与信息交换系统，实现油库生产网环境中不同安全级别网络之间数据安全交换的隔离，防止内部机密信息的泄露，实现网间安全隔离和信息交换；

✓ 构建通信网络“白环境”，在油库生产系统关键网络节点处部署工控安全监测与审计系统，建立全流量行为模型，实现工业网络异常流量监测、工业网络关键事件监测、工控协议规约检测、工控网络通信记录回溯等；

✓ 构建主机业务“白环境”，在油库装车监控主机、罐区监控主机、消防监控主机、安全监控主机以及数据管理平台服务器部署工控主机卫士，利用非法外联、网络白名单、双因子认证、访问控制、安全基线、程序白名单和外设管理等功能，有效阻止工控恶意程序或代码在工控主机上的感染、执行和扩散；

✓ 构建安全管理中心，实时对采集到的不同类型日志信息进行标准化处理和实时关联分析，帮助用户满足安全审计的合规要求；制定严格的资源访问策略，并采用强身份认证手段，全面保障系统资源安全；安全设备集中管理，对安全策略集中管控、安全事件集中分析，为油库生产系统网络安全状态监控、故障快速定位等提供技术支撑。

2. 具体应用场景和安全应用模式

具体应用场景：采用“行为白名单”技术形成“三重固化、三种防护模式”下的纵深防御安全防护技术体系架构，适用于油库控制系统和油库综合自动化系统的安全防护，保障泵站监控系统，罐区（库区）监控系统，装车系统、油品检验系统的高效、稳定运行。亦可为石油石化、电力、轨道交通、烟草、市政、智能制造、冶金及军工等国家重点工控行业构筑工控系统的网络安全防护体系，保障工控系统平稳、高效运行。

安全应用模式： 现场控制层核心控制设备的正常运行对整个生产控制系统起到关键性的作用，因此在核心控制设备前端部署工业防火墙，采用白名单机制确保只有可信的消息才允许传输；在过程监控层，对工程师站、操作站、服务器等工控主机上部署工控主机卫士，采用程序白名单确保有可信的程序才允许运行；在生产管理层边界部署工业防火墙，利用防火墙的访问控制功能，提高生产控制系统的边界防护能力；在生产管理层建立安全管理中心，通过统一安全管理平台

实现对所有安全设备的集中管控、安全事件的集中分析以及全网安全态势的可视化展示，从而实现一体化的安全防护体系。

3. 安全及可靠性

项目从区域边界安全、通信网络安全、计算环境安全以及安全管理中心（简称一个中心、三重防护），4 个方面为油库生产系统提供安全防护，从而保障业务系统的高可靠性。

计算环境安全：基于“白名单”防护方式的工控主机卫士，具备非法外联检测功能，可检测非法网络连接，日志记录和告警；具备网络白名单功能，只允许工业主机与特定服务器进行通信；具备双因子认证功能，提供 USB-key 的组合认证，提升工业主机登录安全；具备访问控制功能，提供强制访问控制模型，保护注册表、系统文件、关键进程；具备安全基线功能，提供安全基线检查和加固功能，提升操作系统安全等级；具备程序白名单功能，可自动扫描、跟踪软件安装及升级生成可执行程序白名单；具备外设管理功能，只允许经过认证的特定 USB 设备才在工业主机上运行。通过以上主机卫士 7 大核心安全功能，构成了安全计算环节的基石，进而保障工控业务系统的高效、稳定运行。

通信网络安全：采用“白环境”为核心技术的工业防火墙，可有效解决传统“黑名单”技术在解决工控网络安全问题时存在的兼容性、易用性、日常工作量大等问题，同时可对工控网络中的工业协议进行深度识别及有效管控，从而提升整个工控系统网络环境的安全性，保障业务运行的可靠性。

区域边界安全：结合业务系统的类型及其重要性，开展业务系统区域划分，不同业务系统区域边界采用工业防火墙进行有效的管控。防火墙具备传统下一代防火墙 IPS、AV 等功能的同时，亦可对工控协议进行深度识别以及有效管控，从而保障了区域边界的安全性，提升业务系统的稳定性。

安全管理中心：部署统一安全管理平台，满足等保标准中“一个中心”的防护建设要求，同时解决了安全日志和时间管理分散、难以掌控全局风险等问题。实现了对工业网络中的安全产品及安全事件进行统一管理的软硬件一体化，通过对控制网络中的边界隔离、网络监测、主机防护等安全产品进行集中管理，实现对全网中各安全设备、系统及主机的统一配置、全面监控、实时告警、流量分析

等，降低运维成本、提高事件响应效率。

4. 其他亮点

（1）针对工控领域的隐蔽攻击发现问题，本项目采用了基于多视角报警融合的隐蔽攻击发现技术。

研究网络流和物理流信息提取算法，从工控网络中，一方面提取资产信息、漏洞信息、拓扑信息等信息流特征，上述特征均是采用主被动结合的方式探测到的；另一方面提取控制流程、能量信息、业务信息等物理流特征，上述特征是从控制程序和现场传感器获取的。

基于协作式学习模型和标准正则化模型，研究多视角学习算法，从信息流和物理流特征中挖掘其中隐含的依存关系。工控环境由各个不同的组件（HMI、PLC、SCADA 等）协作完成某个具体业务流程，且组件内也存在多个服务共同完成某个具体任务。因此，在物理流和信息流中必然隐含着某种符合自然规律的依存关系，挖掘其中隐含的依存关系，从异常检测报警数据中发现隐蔽式攻击。

基于异常检测报警数据，采用数据挖掘算法提取攻击时间、攻击序列、攻击属性等特征，并依据上述特征构建工控网络攻击树，从攻击树中建立物理流与信息流映射关系。若从异常检测报警数据中实时提取的物理流与信息流间的映射关系，与历史的物理流与信息流内在依存关系存在冲突，且前者的特征符合威胁情报的某类特征，则表示发现了隐蔽攻击。

（2）项目中使用的安全防护类产品均设计有多种防护模式，结合业务实际需求可调整至不同的应用模式。

✓ 学习模式：安全防护类设备初次接入工控系统网络时，默认安全应用模式为学习模式，处于该模式下可通过智能学习建立 3 类白名单（访问控制白名单、工业协议白名单以及业务白名单），实现访问控制白名单固化、工业协议白名单固化、业务白名单固化（简称三重固化）。学习模式下的安全防护设备只具备学习功能，无告警及防护功能；

✓ 告警模式：告警模式下可针对违法白名单异常操作行为实时告警，同时安全运维人员可针对异常告警行为进行识别、结合实际业务情况对白名单防护规则进行优化调整；

✓ 防护模式：经过学习模式、告警模式后，进入防护模式。处于防护模式下的安全防护设备可对违反白名单异常操作进行实时阻断并产生告警，从而保障业务的高效、稳定运行。

三、下一步实施计划

优化提升：不断优化提升项目中所采用的新技术、新方法，结合工控领域各行业不同工控系统业务流程，建立工控系统精准防护模型，对工控指令和生产工艺行为进行更加精细化的解析和管控，解决当下工控系统安全防护技术的困境。建立油库生产系统工控网络安全态势感知平台，整合各油库内部设备资产、网络流量、安全漏洞、安全配置、安全日志、设备运行状态、业务故障日志等信息，通过智能关联分析获取油库生产系统的安全风险和态势，指导安全告警的事件处置工作。

复制推广：在我国工业向数字化、网络化和智能化转型升级的大环境下，在我国高举“核心技术是国之重器”的旗帜下，推荐其他石油销售公司借鉴本案例的经验，加强油库生产系统的安全防护能力。

四、项目创新点和实施效果

1. 项目创新点

项目通过建立可信任网络“白环境”和“白名单”防护理念，以自主可控的核心技术投入，以完全符合工业企业的产品设计，为工业企业构筑“安全白环境”整体防护体系，保护工业企业设施的稳定运行。

✓ **基于“硬件级”的安全设备配置文件保护强化防护能力**

面对复杂的网络安全威胁与多样的攻击方式，在对油库生产业务系统构建边界安全的同时，也要考虑安全设备配置文件级的安全防护，避免由于突破边界防线，或内部攻击导致的配置文件修改，对工业控制系统实施破坏，造成不可预计的危险、损失等。本项目选用威努特自主研发的工业防火墙系列产品自带硬件级安全策略写保护功能，一旦设备完成策略配置投产运行，在开启本地硬件配置写

保护功能后，将会阻断一切非法配置修改请求。极端情况下，即使统一安全管理平被“攻破”，通过集中管理平台也无法修改工业防火墙的现行配置策略。

✓ **基于“硬件级”的单向流量接收消除潜在安全隐患**

工业控制系统的安全建设要考虑到接入的设备对当前系统零影响，保证油库生产业务系统平稳运行，本项目选用威努特自主研发工控安全监测与审计系列产品，具备独创的基于硬件级的仅单向接收镜像工控网络通信流量，设备采用纯物理单向设计，从网卡芯片级对数据发送进行阉割处理，所以设备仅接收流量不会发送任何通信信息，真正做到对油库生产控制系统无影响。极端情况，管理平台被攻陷也不会通过设备影响控制网。

✓ **基于“行为白名单”建立的面向工控 PLC 设备的行为模型固化技术**

为快速适用油库生产业务系统的安全防护需求，解决传统白名单使用中面临的问题，本项目采用了基于“行为白名单”的“三重固化”技术。针对工控设备的属性及行为进行描述，通过分析和抽象工控设备自身属性、行为及与其它设备的交互特征，构建工控设备行为模型描述框架，实现行为白名单的识别与固化；通过分析和抽象工控协议的状态机及交互特征，构建工控协议行为特征解码引擎，实现协议白名单的识别与固化；结合油库生产系统实际业务访问需求，创建并实现访问控制白名单的固化。

✓ **基于时间维度判定的智能复杂周期模型检测技术**

在传统白名单技术的基础上，结合油库生产系统业务流程，利用智能技术，以时间周期维度作为判断，发现工控指令隐藏的多重复杂周期模式，建立工控指令复杂周期场景指纹模型。通过该模型对工控指令和生产工艺行为进行更加精细化的解析和管控，解决传统白名单只能静态对工业控制协议指令识别劣势，避免因指令时间错误引起的异常，有效识别误操作、网络故障、恶意操作等引起的工控指令异常，保证工控业务的安全正常运行。

2. 实施效果

（1）经济效益

1）安全建设周期缩短，业务运行稳定保障：

相比传统 IT 安全项目建设周期，本次基于工业白环境理念的纵深防御安全防护建设项目由于采用“白名单”的相关技术原理，其不过度依赖于黑名单类型

的规则库、病毒库等，其上线周期相比传统安全建设项目缩短，业务系统安全风险同比建设初期降低，间接避免整体生产经济损失。

2）安全能力自动化，人力运维效率提升大：

通过采用自动化的统一运维管理平台以及配套产品自身的安全可视化管理界面，为人为管理相关安全设备提供便捷。相比与以往人工手动运维和故障排查的方式，运维效率提升，进而人员结构优化带来的经济效益表现为人力成本节约，企业整体运转效率得到提升。

3）被动+主动的立体安全模式，避免大额勒索事件经济损失：

2017 年勒索病毒 Wannacry 爆发至今，全球仍然每年会有不少制造企业遭受其勒索大额赎金，就已知的大额赎金事件当中，最高的可达千万美元级别。本次建设项目所提供的白环境技术理念以及配套专业设备，在针对工业安全场景勒索事件的防护上具备健壮的防护能力，可帮助企业避免百万美元级别的损失，每年帮助企业挽回间接的经济损失。

（2）社会效益

1）树立工业互联网企业网络安全建设的风向标：

本次基于工业白环境理念的纵深防御安全防护建设项目所采用的的白环境技术理念，是贴合工业场景高可靠、低时延等相关特点设计和研发的技术体系，开创了有别于传统黑名单机制网络防护手段的工业安全防护体系，同时也彰显了该石油销售公司社会主角的担当。

2）促进工业互联网领域安全建设氛围的形成：

石油销售油库工业安全相关建设的落地，将首先在其所属石油石化行业针对工业互联网企业安全分类分级建设起到示范作用，为其相关行业的其他工业互联网企业提供安全建设的宝贵经验，也将在整个工业互联网领域形成企业网络安全建设的良好氛围，以促进更多工业互联网企业（含 232 家联网工业企业、平台企业、标识解析企业试点单位）贯彻落实《中华人民共和国网络安全法》等相关法律法规和政策要求。