文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

基于等保 2.0 的石油化工行业工业控制网络安全防护体系

赵迪　赵越　杨飞
中国石油化工股份有限公司西北油田分公司
DOI:10.32629/acair.v4i1.19372

[摘　要] 在现代工业4.0工业化革命战略不断发展的背景下,原本封闭的传统工业控制系统也逐渐开放,随之而来的网络黑客、木马、病毒、勒索软件等对工业控制系统造成了攻击,对现代工业行业造成了严重威胁。本文以石油化工行业为例,基于等保2.0标准分析了工业控制网络安全防护体系,保证石化行业工业控制网络运行的安全性。
[关键词] 工业网络；石油化工；安全防护；网络安全
中图分类号：TU276.7　文献标识码：A

Industrial Control Network Security Protection System for the Petrochemical Industry Based on the Classified Protection 2.0 Standard

Di Zhao　Yue Zhao　Fei Yang
China Petroleum & Chemical Corporation (Sinopec) Northwest Oilfield Company
[Abstract] Against the backdrop of the continuous development of the modern Industry 4.0 revolution strategy, traditional industrial control systems, which were originally closed, have gradually opened up. This has led to attacks on industrial control systems by network hackers, trojans, viruses, ransomware, and other threats, posing serious risks to modern industries. This paper takes the petrochemical industry as an example and analyzes the industrial control network security protection system based on the Classified Protection 2.0 standard to ensure the operational security of industrial control networks in the petrochemical industry.
[Key words] Industrial Network; Petrochemical Industry; Security Protection; Network Security

网络安全等级保护2.0标准(简称等保2.0)主要工作就是保证网络与数据的安全性,可以覆盖石油化工行业的全网络安全工作。等保2.0在建设整改、原有备案、监督检查与等级测评基础上,增加了安全评估、监测、通报预警等功能,增强石油化工行业网络安全的定期检查效果,及时防范可能会出现的网络攻击行为,增强系统的完整性、保密性,对行业网络整体环境进行改善,还增强了企业网络管控效果,提高企业网络安全管理水平[1]。所以,本文在研究中以等保2.0标准要求设计石油化工行业工控网络安全防护体系,更好的抵御网络病毒、黑客等风险,保证石油化工行业工控网络运行的稳定性、安全性[1]。

1 石化行业工业控制网络安全防护体系的部署

石油化工行业工业控制网络是控制技术与现代信息技术的融合,被广泛应用在工业自动化领域中,用于连接传感器、现场设备、监控系统与控制器,实现过程控制、数据采集、信息集成等功能。工控网络要兼顾石油化工行业的控制管理、应用管理,优先保证业务连续性与系统可用性,导致部分成熟信息技术系统安全产品无法在工业现场直接应用,提高了工业控制网络的安全风险发生率。创建了基于等保2.0的安全通信网络、区域边界一体化安全防护体系,实现了事前预防、事中响应、事后审计功能。

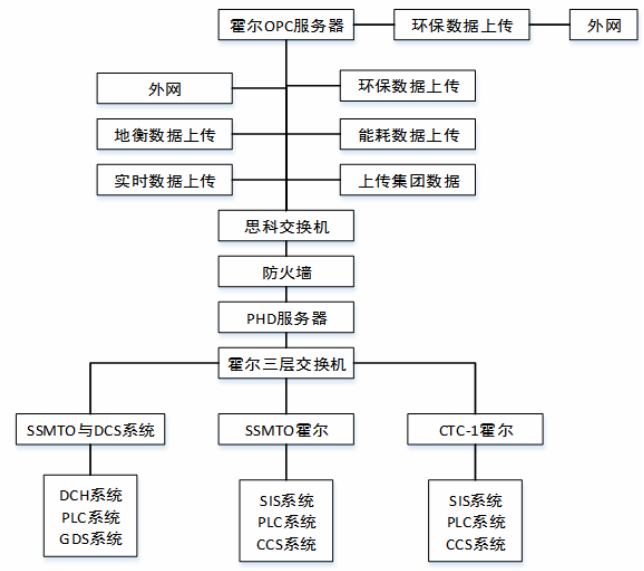

图1　安全系统的部署结构

根据石油化工行业工控网络的架构,将安全防护体系划分为多个层次,分别为办公网络、生产管理、现场控制等。通过核心交换机与防火墙隔离其他网络,保证工业控制网络的安全性。以国家认证加密技术传输跨域数据,保证系统的访问控制与数据安全性,图1为安全系统的部署结构。

(1)工业防火墙。使用专利4s深度防护与白名单技术分析工控协议,并过滤异常命令提高设备与网络安全性。另外,工业防火墙还可以通过实时控制工控协议满足工作现场需求。在复杂工作现场,利用专业硬件平台提高网络运行可靠性。

(2)入侵检测系统(IDS)。利用协议解析使网络IP地址与资源定位仪统一,收集网络元数据模拟化工执行载荷,对存在的威胁进行实时分析。另外,入侵检测系统还可利用反病毒事件库识别网络中存在的已知威胁,并分析未知威胁,保证系统安全性。

(3)工业网络安全审计监测系统。利用深度检测技术对石化行业工业控制网络中的工控协议进行分析,保证网络完整性。通过系统中不同的工业协议满足网络不断变化的需求,并实时监测异常警报通信,保证业务连续性[2]。

2 石化行业工业控制网络安全防护体系的安全机制

由于现代工业控制网络环境比较复杂,传统防护措施已经无法满足实际需求。所以,本文提出以下多重安全防护机制:

2.1终端访问控制

(1)切片接入认证。通过移动管理功能(AMF)认证合法网络终端,通过授权、切片签约的功能阻止未授权切片的访问,降低网络终端安全风险。

(2)终端入网二次认证。石化企业启动二次认证,自主控制终端接入5G专网,利用专线对接核心网,对终端身份认证后触发会话管理功能(SMF),在AAA认证中传输终端身份信息并使其入网,二次认证的部署结构详见图2。

(3)终端电子围栏。如果将固定终端部署在物理位置,可以通过以下方式创建电子围栏:方法一,利用AMF规划跟踪区域标识(TAC)企业与终端绑定关系,保证特定终端才可以进入到指定企业网络,避免企业数据泄露;方法二,利用策略控制功能(PCF),在用户接入位置发生改变时,可以通过实际位置对网络接入的允许范围进行判断。终端电子围栏可以避免非法访问,增强无线终端安全性。

(4)机卡绑定设置。石化行业工业生产网络需要通过特定的号码、终端才能够连接专网,利用AAA绑定用户和设备识别码,避免机卡恶意插拔[3]。

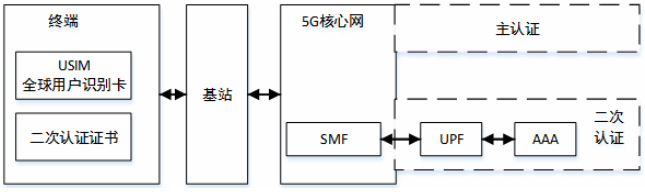

图2　二次认证的部署方式

2.2数据传输加解密

在工业控制网络中,通过数据加解密保证石化企业的信息与客户隐私安全性,避免数据被恶意篡改或者未经授权的访问。图3为数据的加解密过程,对称加密算法(AES算法)可在大规模数据加密中应用,利用相同密钥进行加解密,但是密钥比较复杂。非对称加密算法(ECC、RSA加密)通过私钥与公钥实现加解密,提高密钥管理的灵活性与安全性,被广泛应用在数字签名与身份认证方面。

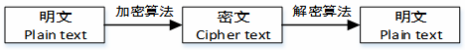

图3　数据的加解密过程

将数据加密应用在工业控制网络中,不仅能够保护行业中用户信息的隐私,还能够保证网络环境下数据的安全性、完整性。在网络终端添加交易数据,并对数据进行加密处理,避免数据传输、存储中被恶意篡改。结合数据加密技术能够提高数据的安全性,保证智能合约数据的完整性。利用此方案,可以实现安全、高效的数据加解密机制,提高网络安全防护体系的可靠性[4]。

2.3网络安全的纵深防御

由过程监控层、现场控制层、企业资源层与生产管理层构成,以分区分域思想在不同防区安装安全防护设备,利用工业网络协议阻断黑客攻击,从而抵御内外网的网络攻击行为,主要包括:

(1)企业资源层。包括服务器集群与办公网络,主要功能为避免内部网络违规操作与互联网入侵。办公网络中的终端计算机可能会发生弱口令、系统漏洞等风险,服务器集群存在应用业务漏洞、服务器高危漏洞等风险。所以,本文部署了表1建筑设备防线,使用网络层入侵检测、漏洞扫描、入侵诱捕等设备对企业资源层重点防护。

表1　企业资源层防线

防线	设备部署	功能	防护作用
企业资源层	防火墙	网络访问控制与隔离	实现互联网内外部的隔离
	入侵检测系统	对攻击流量监测	及时发现网络入侵情况
	高级威胁检测	分析网络流量	
	蜜罐	分析攻击流量	
	漏洞扫描系统	漏洞扫描	主动监测行业资产风险
	堡垒机	运维安全	统一管理设备、服务器
	日志审计系统	日志统一审计、管理	异常行为追溯、审计
	端点准入	接入网络端点	终端入网监测
	主机安全卫士	保证主机安全	主机安全监控、病毒防护

(2)过程监控层。重点对操作员、工程师站上位机等设备的防护,存在网络病毒、非授权操作、漏洞等风险。在主机设备中安装主机安全卫士防护系统,启动白名单防护机制预防未知威胁。实时扫描工业主机,包括设备运行路径、进程名等进程信息与设备类别、标识、名称等外设信息,利用电子签名机制创建白名单库。接入白名单内的外部设备,有效防护违规软件、木马病毒等威胁。

通过工业防火墙隔离，避免未授权的访问，保证作业区内生产的安全性，还能够阻绝威胁扩散，利用分域隔离避免网络中威胁的进一步蔓延[5]。

(3)生产管理层。和办公网络连接，对办公网络的跳板攻击、网络病毒与未授权网络的访问进行有效防护。利用办公网络隔离防护、入侵检测的功能建立安全管理中心，从而实现漏洞扫描、主机防护、入侵检测、日志审计。以细粒度访问控制对工业协议进行识别，避免工控网、办公网的非授权交互，实时监测黑客攻击、病毒传播，避免办公网络遭到入侵行为。

利用工业防火墙隔离网络安全与访问控制，根据工业堡垒机对石化行业账号、操作审计、认证等功能进行管理，使工作人员可以远程控制工业资源。在安全管理中心部署日志设计设备，接管除了流量审计、主机卫士外其他安全设备的日志接入，根据规则进行筛选过滤后，将安全设备数据传输在工业态势感知平台。通过日志审计系统的部署实时管理工控网内日志，协助工控安全管理人员获悉工控系统的安全运行状况，并保存全网日志，从而深入分析问题，为调查取证提供可追溯的数据依据。

(4)现场控制层。由于石化行业的分布范围广泛，所以选择无线数据、远程控制两种部署模式。但是，在现场控制设备管理过程中，会发生工程师站操作风险，设备运行中存在漏洞。为了解决以上问题，将现场控制设备作为主要防护对象，利用安全接入网认证用户的身份，下达唯一生产指令，使用密码算法对所传输的数据、身份进行加密、认证，避免出现数据被篡改的问题。在企业资源层中设计综合管控平台，接收安全设备运行中的日志信息，包括入侵监测网络、工业流量、主机安全防护与防火墙等信息。根据实际资产情况对工控安全数据进行感知，并实时监测、分析网络安全状态，管理人员以网络安全感知与预测信息制定网络安全防护方案。其次，通过设备联动的方法在防火墙中发送阻断指令，增强系统应急响应功能[6]。

3 结束语

在社会经济不断发展的过程中，保证石化行业工业控制网络的安全性具有重要意义。因此，本文基于石化行业网络业务的特点，以纵深防御设计思想设计了基于等保2.0的工控网络防护体系，对石化行业工控网络进行态势感知、入侵检测、主机防护、身份认证，实时监控生产数据流，防范恶意软件传播与定向攻击，实时告警潜在威胁，保证了石油化工行业网络的安全性。

[参考文献]

[1]李鹏.石油化工自控仪表系统的优化设计与实现[J].中国石油和化工标准与质量,2025,45(19):100-102.

[2]陈磊.石油化工企业“5G+工业互联网”网络安全威胁及对策[J].安全、健康和环境,2025,25(06):75-79.

[3]孙红斌.基于数字化转型的石油化工智能工厂安全管理体系建设[J].中国石油和化工,2025,(05):99-101.

[4]雍鲁秦,彭清明.石油化工行业网络安全运营探讨[J].中国石油和化工标准与质量,2024,44(16):81-83.

[5]李全.数字孪生技术在石油化工安全生产的应用现状及挑战[J].中国石油和化工标准与质量,2024,44(02):34-36.

[6]霍朝宾,武蕊.石化行业工控系统网络安全防护体系建设探析[J].网络安全与数据治理,2022,41(08):55-60.

作者简介：

赵迪(1984--),男,汉族,新疆乌鲁木齐市人,中石化西北油田分公司科技与信息管理部主管。学士学位,工程师,先后从事网络系统管理、IT硬件与运维管理,信息系统项目管理工作。