

工控系统

石化行业工控系统信息安全的纵深防御

文 | 青岛海天炜业自动化控制系统有限公司

纵观中国工业、能源、交通、水利以及市政等国家关键基础设施建设，DCS、PLC 等工业控制系统得以广泛应用，随着中国两化融合的深入发展，信息化的快速发展大大提高了公司的运营效率，但 TCP/IP、Ethernet 等通用技术和通用产品被大量引入工业领域，也将越来越多的信息安全问题摆在了企业面前。

另一方面，长久以来，企业更多关

注的是物理安全，信息化发展所需的信息安全防护技术却相对滞后，近几年来，因控制系统感染病毒而引起装置停车和其他风险事故的案例屡有发生，给企业造成了巨大的经济损失。Stuxnet 病毒的爆发更是给企业和组织敲响了警钟，工信部协 [2011]451 号通知明确指出要切实加强工业控制系统信息安全管理的要求。

本文以石化行业为例，就工业控制

系统信息安全存在的隐患，及其纵深防御架构体系进行简要探讨。

工业控制系统面临的信息安全漏洞

工业控制系统面临的信息安全漏洞包括：通信协议漏洞、操作系统漏洞、杀毒软件漏洞、应用软件漏洞和安全策略和管理流程漏洞。

通信协议漏洞

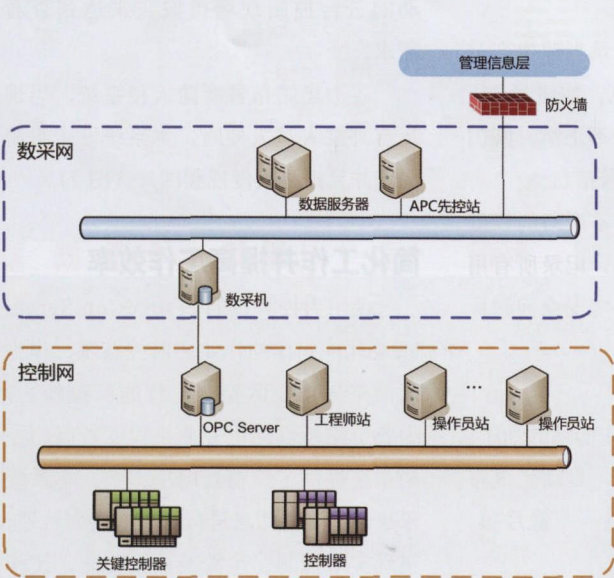


图 1 石化行业工控系统网络结构

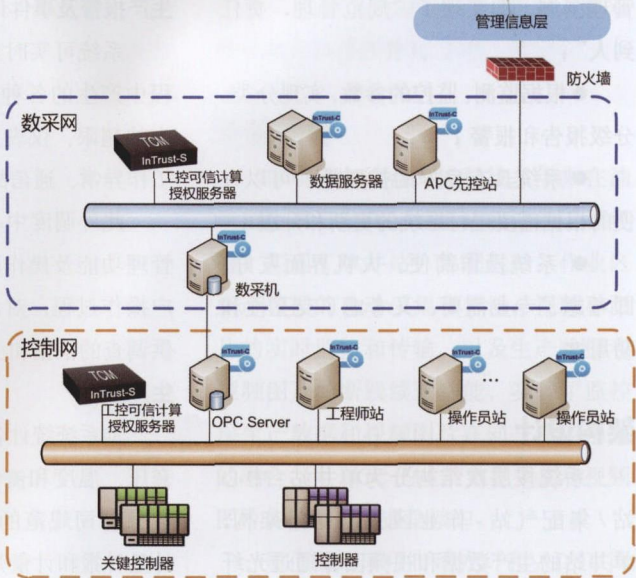


图 2 采用海天炜业 InTrust 工控可信计算安全平台提高工控系统终端安全的部署示意图

两化融合和物联网的发展使得 TCP/IP 协议和 OPC 协议等通用协议越来越广泛地应用在工业控制网络中,随之而来的通信协议漏洞问题也日益突出。

例如, OPC Classic 协议 (OPC DA、OPC HAD 和 OPC A&E) 基于微软的 DCOM 协议, DCOM 协议是在网络安全问题被广泛认识之前设计的,极易受到攻击,并且 OPC 通信采用不固定的动态端口号,在通信过程中可能会用到 1024-65535 中的任一端口,这就导致使用传统基于端口或 IP 地址的 IT 防火墙无法确保其安全性。因此确保使用 OPC 通信协议的工业控制系统的安全性和可靠性成为工程师的一个安全技术难题。

操作系统漏洞

目前大多数工业控制系统的工程师站/操作站/HMI 都是基于 Windows 平台的,为保证过程控制系统的相对独立性,同时考虑到系统的稳定运行,通常现场工程师在系统开车后不会对 Windows 平台安装任何补丁,这样导致了操作系统存在被攻击的可能,从而埋下了安全隐患。

杀毒软件漏洞

为了保证工控应用软件的可用性,许多工控系统操作站通常不会安装杀毒软件。即使安装了杀毒软件,在使用过程中也有很大的局限性,原因在于使用杀毒软件很关键的一点是,其病毒库需要不定期的经常更新,这一要求尤其不适合于工业控制环境。而且杀毒软件对新病毒的处理总是滞后的,导致每年都会爆发大规模的病毒攻击,特别是新病毒。

应用软件漏洞

由于应用软件多种多样,很难形成统一的防护规范以应对安全问题;另外当软件面向网络应用时,就必须开放其网络端口。因此,常规的 IT 防火墙等安全设备很难保障其安全性。互联网攻击者很有可能会利用一些大型工程自动化软件的安全漏洞获取诸如污水处理厂、天然气管道以及其他大型设备的控制权,

一旦这些控制权被不良意图黑客所掌握,那么后果不堪设想。

安全策略和管理流程漏洞

追求可用性而牺牲安全,是工业控制系统存在的普遍现象,工业控制系统中移动存储介质包括笔记本电脑、U 盘等设备的使用缺乏完整有效的安全策略与管理流程也给工业控制系统信息安全带来了一定的威胁。

控制系统信息安全现状分析

目前,实时数据库系统在石化企业生产经营管理中得到越来越广泛的应用,通用通信协议和操作系统也几乎覆盖了所有的工业控制系统。根据业务功能的不同,石化行业工控系统网络一般分为三部分:控制层、数采层和管理信息层,如图 1 所示。

在信息安全方面,石化企业工控系统目前存在的安全问题主要有:

系统终端自身免疫力不足

系统终端自身免疫力不足。目前工业计算机操作系统大多采用 Windows 操作系统,一般不允许安装操作系统的安全补丁和防病毒软件,这些先天限制,使得工业计算机的操作系统存在很多已知或未知的漏洞无法解决,一旦发生针对性的网络攻击或病毒感染则会造成无法想象的后果;即便安装杀毒软件也仅能对部分病毒或攻击有所抑制,但病毒库存在滞后,也不能从根本上进行防护。另一方面,项目实施和后期维护中频繁使用 U 盘、笔记本电脑等外置设备,并且是在整个系统开车情况下实施,也存

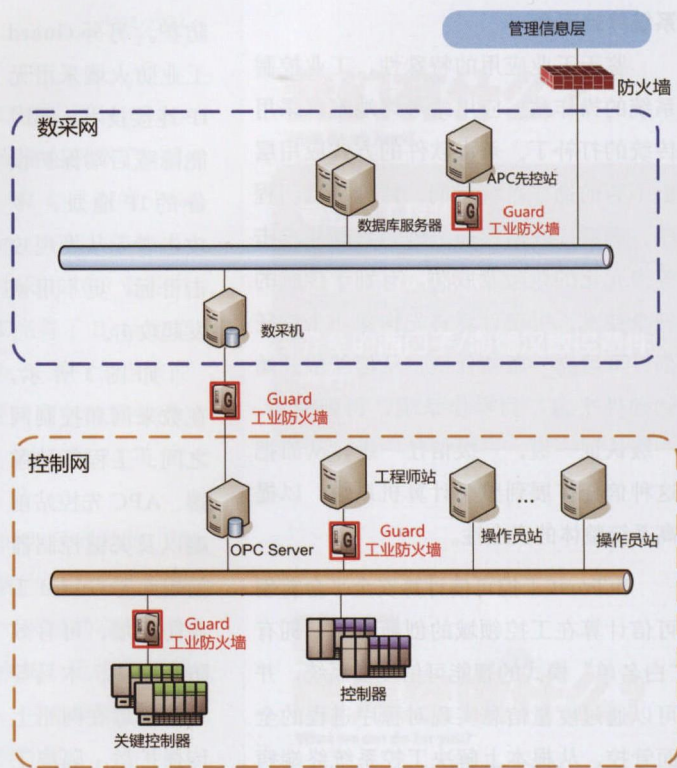


图 3 Guard 工业防火墙在石化行业工业网络安全防护中的应用

在较高的安全隐患。

工业网络扁平化现象突出

虽然大多数石化企业通过 Buffer 数采机或 OPC Server 的双网卡结构对数采网与控制网进行了隔离,部分恶意程序不能直接攻击到控制网络,但对于能够利用 Windows 系统漏洞的网络蠕虫及病毒等,这种配置并没有作用,病毒仍会在数采网和控制网之间互相传播。

系统缺乏信息安全监控措施,网络攻击事件无法追踪

现有网络如果遭受病毒和黑客攻击,维护人员无法进行故障点查询和原因分析,并采取应急响应措施,一些小的安全问题直至发展成大的安全事故才会被发现和解决。

基于纵深防御的工业控制系统信息安全解决方案

接下来将从终端安全、网络安全和智能审计记录分析三个方面,对基于纵深防御的工业控制系统信息安全解决方案进行分析。

系统终端安全

鉴于工业应用的特殊性，工业控制系统的操作站、应用站等终端难以采用传统的打补丁、杀毒软件的方式应用层出不穷的操作系统漏洞、计算机后门程序、病毒、数据扫描、密钥数据块攻击等多元化的风险及威胁。有别于传统的安全技术，可信计算首先构建一个信任根，再建立一条信任链，从信任根开始到硬件平台，到操作系统，再到应用，一级认证一级，一级信任一级，从而把这种信任扩展到整个计算机系统，以提高系统整体的安全性。

InTrust 工控可信计算安全平台首创可信计算在工控领域的创新应用，拥有“白名单”模式的智能可信度量系统，并可以通过度量信息实现对程序进程的全面管控，从根本上解决工控系统终端病毒感染、恶意代码进程启动、操作系统内核漏洞隐患。

网络安全

国际行业标准 ANSI/ISA-99、IEC62443 指出工业控制系统网络安全要点如表 1 所示：

参照国际行业标准，同时结合石化行业网络结构特点以及信息安全需要，可以将其工控网络划分为控制网、数采网、工程师站、APC 先控站、关键控制器等 5 个区域。

下一步就是实现区域之间网络通信的访问控制。工业防火墙是目前业界比较认可，市场应用最广的一种网络安全防护产品。以 Guard 工业防火墙为例，其采用工业协议深度包检查（DPI）技术，支持 OPC、Modbus TCP 等常见工业协议，远远超过了端口级别的访问控制，能提供更加有效的工业协议应用层

防护。另外 Guard 工业防火墙采用无 IP 连接技术，同时能隐藏后端保护设备的 IP 地址，令攻击者无从发现攻击目标，更不用谈发起攻击。

如图 3 所示，在数采网和控制网之间、工程师站前端、APC 先控站前端以及关键控制器前端部署 Guard 工业防火墙，可有效防止蠕虫、木马等非法病毒在网络上传播扩散；隔离工程师站，避免因工程师站感染而导致的病毒扩散；保护

APC 先控站和关键控制器；从网络层面构建工控系统运行的安全环境。

智能审计记录分析

海天炜业工控安全管理平台 SMP 是专门针对工控网络行为审计记录的智能分析管理软件，具备强大的审计日志存储查询功能，可以对海量的审计数据进行实时监控和网络行为态势分析，使系统安全运维人员能够通过实时日志展示画面随时监控正在发生的不同级别审计日志和报警信息，也可以通过安全管理平台的条件查询、统计、筛选、图表展示和态势分析算法模型等强大的功能迅速得出网络健康状况，最终自动获得详细的统计分析报告和事件处置方式建议，实现系统安全运维管理的实时性、完整

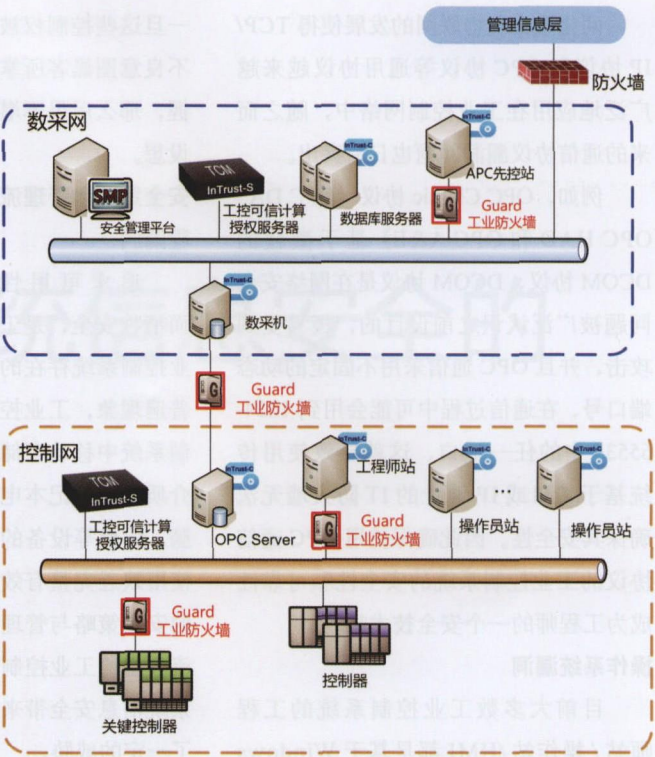


图 4 终端加固、网络安全、智能监控。海天炜业石化行业纵深防御工业控制系统信息安全防护架构

性、自动化、智能化。整体“纵深防御”工业控制系统信息安全部署结构如图 4 所示。

保障企业生产安全稳定运行

石油化工等关键基础设施和能源行业关系国计民生，在我国两化融合深入发展的同时，如何确保工控系统信息安全是石化行业信息化建设重要的一部分。

本文以纵深防御的工业信息安全防护理念为核心，在充分了解石化行业网络结构和安全现状的基础上，对石化行业工控系统信息安全需求进行了认真分析，从终端安全、网络安全和智能监控三方面出发，通过部署 InTrust 工控可信计算安全平台、Guard 工业防火墙以及工控安全管理平台 SMP，介绍了海天炜业工业控制系统信息安全的纵深防御在石化行业的应用，实现高效保护工控系统远离木马、蠕虫、黑客等各种威胁和攻击，保障企业生产安全稳定运行。

表 1 ANSI/ISA-99 指出的控制网络安全要点

要点名称	要点描述	达到目标
区域划分	具备相同功能和安全要求的设备在同一区域内	安全等级分区
管道建立	实现区域间执行管道通信	易于控制
通信管控	通过控制区域间管道中通信管理控制来实现设备保护	数据通信可控