烟草商业企业工控系统网络安全防护建设研究

王　晔[1]，万佳蓉[1]，荆　琛[1]，钟湘琼[2]
（1. 中国电子信息产业集团有限公司第六研究所，北京　100083；
2. 湖南省烟草公司衡阳市公司，湖南　衡阳　421001）

摘　要：随着商烟企业工业化和信息化水平的不断发展，物流配送和烟叶复烤使用了大量的工业控制系统，就如何将商烟工控系统的网络安全防护建设落地，首先分析了商烟哪些系统是工控系统，给出工控系统的类别，然后从“分层分区、安全组网、边界防护、综合管控”层面提出网络安全防护建设要点，并给出了安全建设示例，为商烟企业工控系统网络安全防护建设提供思路。

关键词：烟草商业；工业控制系统；网络安全防护
中图分类号：TP309　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2025.08.003
引用格式：王晔，万佳蓉，荆琛，等. 烟草商业企业工控系统网络安全防护建设研究［J］. 网络安全与数据治理，2025，44(8)：17-23.

Research on the construction of network security protection for industrial control system of tobacco commercial enterprises

Wang Ye[1], Wan Jiarong[1], Jing Chen[1], Zhong Xiangqiong[2]
(1. The 6th Recearch Institute of China Electronics Corporation, Beijing 100083, China;
2. Hengyang Branch of Hunan Tobacco Company, Hengyang 421001, China)

Abstract: With the continuous development of industrialization and informatization levels of tobacco commercial enterprises, a large number of industrial control systems are used in logistics distribution and tobacco leaf reroasting. This paper aims to implement the construction of network security protection for tobacco commercial industrial control systems. Firstly, it analyzes which systems are industrial control systems of tobacco commercial and gives the categories of industrial control systems. Then, the key points of network security protection construction are put forward from the level of "layered zoning, secure networking, boundary protection, and comprehensive control". Finally, the example of network security protection construction is given to provide ideas for the network security protection construction of industrial control system of tobacco commercial enterprises.

Key words: tobacco commercial; industrial control system; network security protection

0　引言

近年来，我国发布了一系列网络安全相关的法律法规、标准指南，如《中华人民共和国网络安全法》、等保2.0系列标准、《工业控制系统网络安全防护指南》等，烟草行业也制订了《烟草行业工业企业生产区与管理区网络互联安全规范》《烟草行业工业控制系统网络安全基线技术规范》等行业标准指导烟草行业工控系统网络安全建设，但是这些标准对于商烟工控系统的网络安全防护建设缺少针对性，无法解决商烟企业工控系统网络安全防护建设如何落地的问题，比如工控系统界定不清，工控系统安全防护的资产范畴不明[1]；部分企业工控网和信息网在早期建设时未分离[2]，工控系统现场设备层设备存在混网传输情况等。本文在调研了某省商烟实际需求和安全防护现状的基础上，结合商烟工控系统特点，给出了网络安全防护建设思路。

1　商烟工控系统的类别划分

以某省烟草商业企业为例，该企业主要负责全省烟叶种植、收购、调拨和卷烟的销售，下设烟叶复烤公司，负责烟叶复烤加工。商烟企业工控系统主要分布在烟草公司物流配送中心、烟叶复烤公司的复烤厂，物流配送中心主要业务包括卷烟的采购业务、入库业务、仓储业

务、分拣业务、出库业务和配送业务[3]等，复烤厂主要业务包括原烟出入库、选后烟出入库、成品片烟出入库和打叶复烤加工等。

商烟企业日常运行的信息系统众多，需要明确哪些系统属于工控系统。根据商烟企业开展的业务类别进行分类，烟草公司物流配送中心工控系统是物流分拣类，烟叶复烤公司工控系统是烟叶复烤类[4]，每个业务类别中不可根据生产环节和组成架构特点划分为多个工控系统类别，如表1所示。

表1　商烟工控系统分类

业务类别	工控系统类别	主要业务功能
物流分拣	卷烟仓储	卷烟出入库、仓储、备货等业务环节
	卷烟分拣	分为不同分拣线，对条烟进行分拣、打扫码、包装、贴标等
烟叶复烤	烟叶物流	原烟出入库、选后烟出入库、成品片烟出入库等业务环节
	复烤生产加工	预处理、真空回潮、打叶、复烤、打包、除尘等生产加工环节

2　商烟工控系统网络安全需求

商烟业务涉及从烟叶种植、收购、调拨、烟叶复烤加工到卷烟的销售配送等一系列流程，其工控系统具体的安全需求如下：

（1）为更好地界定工控系统的防护范围，商烟工控系统需按照IEC/TS62443-1-1功能层次划分，进行分层分区的安全防护建设。

（2）工控系统需采用内网专线，并使用独立的网络设备内网核心交换机组网；商烟工控内网设备的运维需通过虚拟专用网络（Virtual Private Network，VPN）进行远程访问，远程运维终端进行接入限制；无线网络组网管控以及无线准入控制。

（3）工控系统边界防护包括各层之间、各区域之间边界安全防护，以防止攻击者跨区进行攻击，减少攻击发生时危害的蔓延。

（4）监测预警，实时监测异常的网络流量和网络攻击等，做到安全事件事中的及时告警，事后的溯源分析和取证，甚至事前的安全预警。

（5）在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户；对重要的用户行为和重要安全事件进行审计。

（6）在工控监控主机、现场操作站、服务器等设备安装主机安全卫士，监测随意的U盘插拔、文件拷贝、无线上网等违规行为，并通过统一安全管理平台对终端主机安全卫士进行统一管理。

（7）划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行集中管控；对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；对安全策略、恶意代码、补丁升级等安全相关事件进行集中管理等。

3　商烟工控系统网络安全防护建设

针对商烟工控系统网络安全防护建设，本文按照网络安全等级保护有关要求，结合IEC/TS62443-1-1工控系统功能层次划分，从“分层分区、安全组网、边界防护、综合管控”[5]几个层面进行工控系统网络安全防护建设。整体建设框架如图1所示[6]。

3.1　分层分区

分层分区是工控系统安全防护的结构基础，参照《信息安全技术　网络安全等级保护安全设计技术要求》（GB/T 25070—2019），典型工控系统采用分层、分区的架构，根据工控系统的业务特点和业务模块的重要程度，合理划分安全区域，重点保护工控系统核心业务的安全。纵向上0～3层为工控系统安全防护建设框架覆盖的区域，第0层：现场设备层；第1层：现场控制层；第2层：过程监控层；第3层：生产管理层。其中0～2层属于工控生产网，第3层属于工控管理网。横向上对工控生产网工控系统根据业务范围、资产属性等进行安全区域的划分。

3.1.1　纵向分层

第3层生产管理层，负责生产任务的分解下达和生产数据的采集。资产主要包括支撑业务功能的服务器、工作站等。

第2层过程监控层，负责接收、下发生产任务并转化为具体操作指令，并且获取执行结果的反馈。资产主要包括电控系统、控制服务器、操作站等。

第1层现场控制层，负责根据操作指令指挥各个执行器件完成具体动作。资产主要包括PLC控制器、分布式I/O模块、HMI等。

第0层现场设备层，包括完成生产业务等具体动作的各种执行器件，如电机、AGV小车、扫描器、打码机等。

3.1.2　横向分区

工控管理网（第3层）主要包括生产管理层，按照业务功能逻辑划分为服务器区域、调度管理区域、安全管理中心区域等。

工控生产网（第0～2层）主要包括当前及未来有控

制功能的业务系统或模块，按照以下原则横向划分为不同的安全区域：将具备相同功能和安全要求的业务系统置于同一个安全区域内，并按照方便管理和控制的原则为各安全区域分配网段地址。尽可能将业务系统完整置于一个安全区域内[7]，当业务系统的某些功能模块与此业务系统不属于同一个安全区域内时，可以将其功能模块分置于相应的安全区域中，经过安全区域之间的安全隔离设施进行通信。

根据工控现场实际业务情况，分区方式包括但不限于：第 0 ~ 2 层组成一个安全区域，第 0 ~ 1 层组成一个安全区域等。物流分拣类和烟叶复烤类工控生产网横向分区方式示例如图 2、图 3 所示。

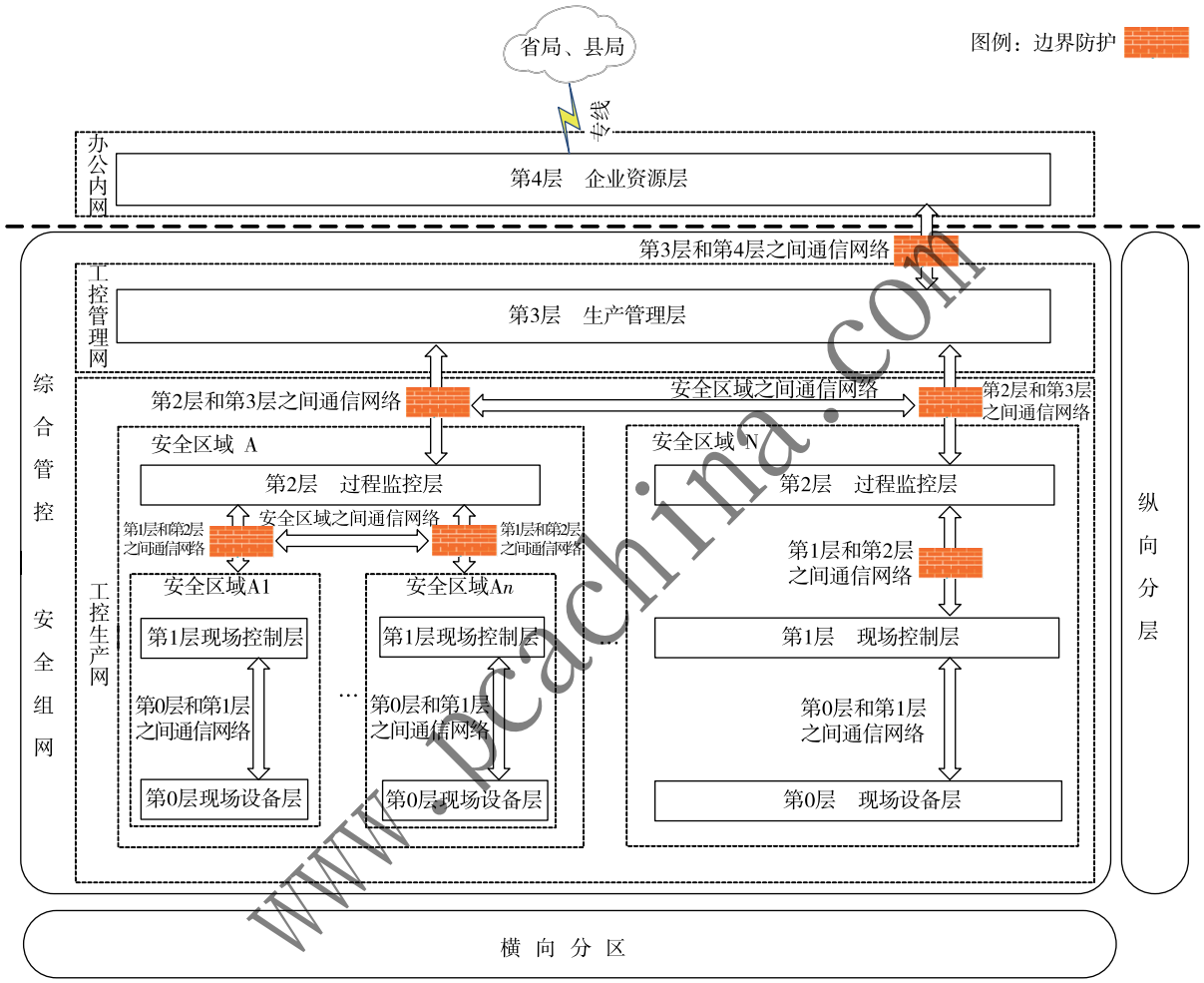

图 1　整体建设框架

物流分拣类						
分区方式示例 1	第 2 层	安全区域 A – 卷烟分拣			安全区域 B – 卷烟仓储	
	第 1 层 第 0 层	安全区域 A1 – 分拣线 1	安全区域 A2 – 分拣线 2	安全区域 A3 – 分拣线 3	安全区域 B1 – 仓储系统 1	安全区域 B2 – 仓储系统 2
分区方式示例 2	第 2 层	安全区域 A				
	第 1 层 第 0 层	安全区域 A1 – 分拣线 1	安全区域 A2 – 分拣线 2	安全区域 A3 – 分拣线 3	安全区域 A4 – 仓储系统 1	安全区域 A5 – 仓储系统 2
分区方式示例 3	第 2 层 第 1 层 第 0 层	安全区域 A – 分拣线 1	安全区域 B – 分拣线 2	安全区域 C – 分拣线 3	安全区域 D – 仓储系统 1	安全区域 E – 仓储系统 2

图 2　物流分拣类工控系统横向分区示例

<table>
<tr><td colspan="5">烟叶复烤类</td></tr>
<tr><td rowspan="3">分区方式示例 1</td><td>第 2 层</td><td colspan="2">安全区域 A – 烟叶物流控制</td><td rowspan="3">安全区域 B – 复烤加工生产线</td></tr>
<tr><td>第 1 层</td><td rowspan="2">安全区域 A1 – 原烟库控制系统</td><td rowspan="2">安全区域 A2 – 成品库控制系统</td></tr>
<tr><td>第 0 层</td></tr>
<tr><td rowspan="3">分区方式示例 2</td><td>第 2 层</td><td rowspan="3">安全区域 A – 原烟库控制系统</td><td rowspan="3">安全区域 B – 成品库控制系统</td><td rowspan="3">安全区域 C – 复烤加工生产线</td></tr>
<tr><td>第 1 层</td></tr>
<tr><td>第 0 层</td></tr>
</table>

图 3　烟叶复烤类工控系统横向分区示例

3.2　安全组网

商烟企业可将网络划分为办公内网、工控管理网、工控生产网三部分[8]，如图 4 所示。典型工控系统区域覆盖工控管理网和工控生产网两部分，其中工控管理网包含生产管理层（第 3 层），工控生产网包含过程监控层、现场控制层以及现场设备层（0 ~ 2 层）。

工控生产网指为各生产单位生产业务服务的专用数据网络，承载过程监控层、现场控制层以及现场设备层的网络。工控生产网以及内部每个安全区域应采用独立的网络设备组网。现场控制层、现场设备层应采用业务需要的方式进行组网，如 PROFINET、PROFIBUS 等，网络设备应满足工控系统运行现场环境要求。

工控管理网承载生产管理层的网络，应采用独立的网络设备进行组网。划分不同的 VLAN，按照实际业务划分不同的区域，如服务器区域、调度管理区域、工控安全管理中心区域等。工控安全管理中心采用独立组网的管理方式，所有网络安全产品的策略下发、日志采集等动作不占用工控系统的网络带宽。

工控生产网和工控管理网通过互联接口连接，互联接口安全功能应符合《烟草工业企业生产网与管理网网络互联安全规范》（YC/T 494—2014）的要求，工控管理网与办公内网连接时要进行逻辑隔离。

3.3　边界防护

商烟工控系统的边界主要有：工控管理网和办公内网边界、工控生产网和工控管理网边界、工控管理网远程运维边界、无线网络边界等，具体边界防护策略如下：

（1）工控管理网与办公网边界

工控管理网和办公内网通信应采用隔离措施，如部署工业控制网络安全隔离和信息安全交换系统等，并采取冗余部署方式，工控管理网内部各安全区域通信应基于路由器、交换机的 ACL 规则、防火墙等进行逻辑隔离。

（2）工控生产网与工控管理网边界

工控生产网和工控管理网连接应采用安全措施进行隔离，隔离强度应当接近或达到物理隔离，如部署工业控制网络安全隔离和信息安全交换系统等，并采取冗余部署方式；工控生产网内部各安全区域之间通信、现场控制层 PLC 与过程监控层通信均应采用逻辑隔离措施，如部署工控系统专用防火墙等，并采取冗余部署方式。

（3）工控管理网远程运维边界

工控管理网远程运维采用 VPN，并设立安全接入区，采用安全措施进行隔离，如部署工控系统专用防火墙、工业控制网络安全隔离和信息安全交换系统等，并配置合理的访问控制策略。

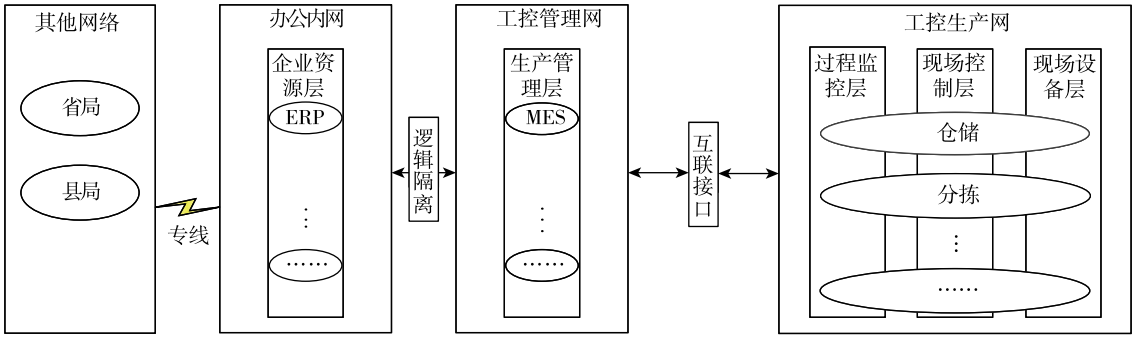

图 4　网络连接架构图

（4）无线网络边界

工控生产网无线网络接入有线网络应设立安全接入区，采用安全隔离、访问控制、认证加密等安全措施，如部署工控系统专用防火墙等。

3.4 综合管控

3.4.1 入侵防范

工控生产网各安全区域（如物流分拣类仓储区域、分拣线区域；烟叶复烤类生产区、仓储区）旁路部署工控入侵检测类设备，包括但不限于实现以下功能：

（1）实时获取数据包，并对数据包进行实时分析，发现网络攻击事件（包括端口扫描攻击、暴露攻击、强力攻击、木马后门攻击、DoS 攻击、缓存区溢出攻击、IP 碎片攻击、网络蠕虫等），并进行安全告警；

（2）识别基于现有工控协议以及主流的工控协议（如 S7、OPC、Modbus、IEC104 等）的事件，并深度解析；

（3）对工控协议的畸形报文和执行的高危指令（如写数据、逻辑下装、停机等）做到精准识别，实现对工控协议指令级的解析；

（4）实现对网络攻击特别是新型网络攻击行为的分析。

3.4.2 安全审计

在安全管理中心区域部署工控系统安全审计类产品，实现对工控系统网络中的重要安全事件的收集和审计，也可通过边界防护类设备、入侵检测类设备等获取网络安全事件；部署运维审计类系统，实现对运维人员维护过程中用户行为的追踪审计；部署工控数据库审计类系统，实现对数据库访问行为的审计；部署综合安全审计类设备，实现对工控系统所有安全事件和用户行为的统一审计。

3.4.3 工控主机安全

在工控主机中安装主机安全软件，使主机实现安全管控，主机安全软件应实现包括但不限于以下功能：

（1）有效防护病毒、木马等恶意程序，防止未授权应用程序和服务运行，识别非法外联、网络入侵和恶意软件并告警；

（2）在工控主机安全软件的选用上，应使用经过充分离线验证测试的防病毒软件或应用程序白名单软件，确保其不会对工控系统的正常运行造成影响；

（3）应定期对工控主机进行查杀，对临时接入设备使用前进行查杀，并做详细查杀记录；

（4）应实现网络内工控主机安全防护软件的统一管理，禁止从互联网直接升级。

3.4.4 控制设备安全

工控系统现场控制层（第 1 层）PLC 等控制设备自身应采取身份鉴别、访问控制、安全审计等控制措施，如受条件限制控制设备自身无法实现控制措施，应由其上位控制或管理设备实现同等功能或通过管理手段进行控制[9]。相关要求如下：

（1）控制设备上线前应对其进行安全性检测，控制设备固件中不存在恶意代码程序；

（2）应关闭或拆除控制设备的软盘驱动、光盘驱动、USB 接口、串行口或多余网口，确需保留的应通过相关的技术措施实施严格的监控管理；

（3）如条件允许，应逐步部署内嵌安全功能的控制设备，构建工控系统安全可信环境；

（4）应使用专用设备和专用软件对控制设备进行补丁更新、固件更新；

（5）关键控制设备应采用冗余机制以提高系统的高可用性；

（6）应定期备份控制设备配置文件，并定期验证备份恢复情况；

（7）控制设备现场运维调试，应对现场运维操作过程全程监督，保留工业控制设备上的相关访问日志，并对操作过程进行安全审计。

3.4.5 监测预警

在工控安全管理中心区域部署工控监测分析预警类平台（或工控安全态势感知平台）[10]，可利用工控管理网、工控生产网各生产线内部部署的安全设备作为监测预警设备探头，也可部署探针，通过自组网方式将日志信息统一发送至工控监测分析预警类平台，覆盖到现场控制设备、操作系统、网络设备、安全设备、网络行为、网络流量、业务审计、网络脆弱性、网络威胁态势等。

3.5 建设示例

为了更好地给商烟企业提供工控系统网络安全防护建设参考，本文给出了烟草商业企业工控系统网络安全防护建设示例图[11]，如图 5 所示。

在网络安全防护建设中，安全设备的合理部署至关重要。表 2 给出了安全设备部署的位置和实现的功能，供商烟企业工控系统网络安全建设时参考。

4 结束语

随着移动互联、云计算、物联网、5G 专网、人工智能[12]等新技术在商烟工控系统中的应用，工控系统接入设备的场景愈发复杂，面临着诸多安全挑战。本文依据网络安全等级保护的相关要求，结合商烟工控系统的网络安全需求，提出了切实可行的工控系统网络安全防护建设思路。未来商烟企业需要双管齐下：在技术层面，积极探索并应用前沿安全技术，如利用基于人工智能的数据挖掘技术，对工控系统产生的海量数据进行深度分

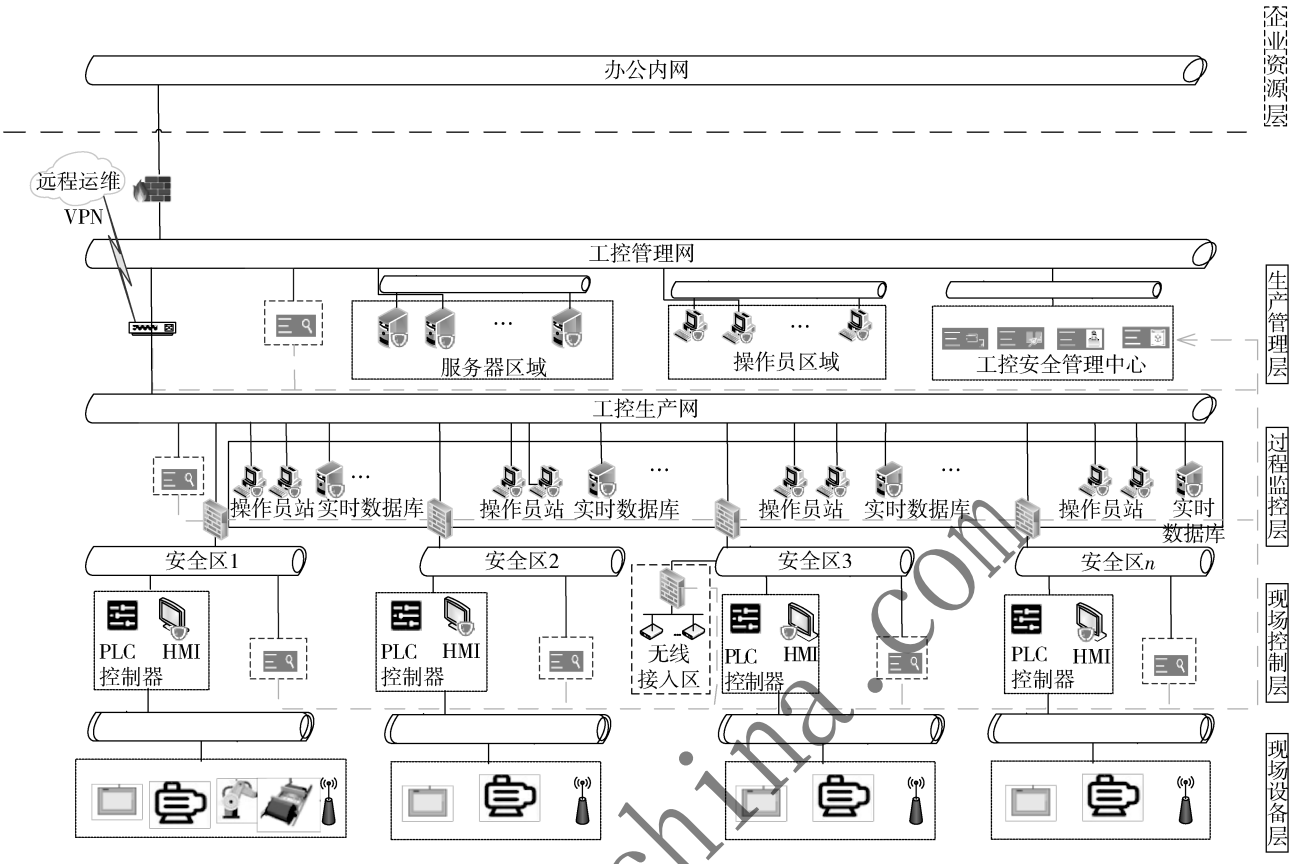

图 5　烟草商业企业工控系统网络安全防护建设示例图

表 2　安全设备部署说明表

序号	产品类型	安全设备部署位置	实现功能
1	防火墙	工控管理网与办公内网之间	边界防护－逻辑隔离
2	网络安全隔离与信息交换系统	工控生产网和工控管理网之间	边界防护－物理隔离
3	工业防火墙	现场控制层各安全区域边界	边界防护－逻辑隔离，对工控协议深度解析
4	工控入侵检测系统	现场控制层各安全区域边界	综合管控－入侵检测
5	工业信息安全日志平台	工控安全管理中心	综合管控－安全事件审计
6	工控数据库审计系统	工控安全管理中心	综合管控－数据库安全审计
7	工控运维审计系统	工控安全管理中心	综合管控－安全运维审计
8	工控监测预警分析平台	工控安全管理中心	综合管控－监测预警
9	工控主机加固系统	各操作站、工程师站、服务器	综合管控－工控主机安全

析，实时监测异常行为，提前预警潜在的安全威胁；引入量子加密技术，为数据传输与存储筑牢加密防线，有效抵御各类高级攻击手段。在管理方面，建立健全安全管理制度，制定严格的操作规范和权限管理机制，从人员层面降低安全风险；构建完善的应急响应机制[13]，确保在遭遇突发安全事故时，能够迅速响应、高效处置，最大程度保障业务的连续性。通过技术与管理的双轮驱动，推动商烟企业网络安全工作迈向高质量发展阶段。

参考文献

[1] 胥强. 烟草行业工业网络安全解决方案［J］. 自动化博览，2019（12）：78－80.

[2] 陈斌. 烟草物流中心网络安全防御体系设计［J］. 工业信息安全，2024（5）：52－59.

[3] 蔡永长. 浅谈全方位保护邵阳烟草物流数据安全［J］. 计算机光盘软件与应用，2013，16（23）：161，163.

[4] 韩瀚. 基于等级保护标准的烟草商业企业工控系统网络安全自评估方法研究［J］. 软件，2021，42（11）：90－92.

[5] 罗晓峰. 打叶复烤企业工控安全现状及防控措施探讨［J］. 网络安全技术与应用，2019（12）：161－163.

[6] 信息安全技术 网络安全等级保护安全设计技术要求（GB/T 25070—2019）［S］. 2019.

[7] 烟草行业工业控制系统网络安全基线技术规范（YC/T

580—2019）［S］. 2019.
［8］烟草工业企业生产网与管理网网络互联安全规范（YC/T 494—2014）［S］. 2014.
［9］信息安全技术 网络安全等级保护基本要求（GB/T 22239—2019）［S］. 2019.
［10］何巍. 基于纵深防御的烟草行业工控安全解决方案［J］. 电子技术应用，2019，45（3）：88－91.
［11］李伟. 基于烟草商业物流工控系统安全风险评估研究［J］. 中国设备工程，2021（18）：135－136.
［12］吕晨阳，姜巍文，贾莉，等. 烟草行业数据安全体系建设与思考［J］. 价值工程，2024，43（34）：148－151.
［13］吴文权，吴君楠. 烟草行业网络安全及其防范措施研究［J］. 数字通信世界，2024（7）：46－48，75.

（收稿日期：2025－03－25）

作者简介：

王晔（1986－），女，硕士，高级工程师，主要研究方向：网络安全、工控安全。

万佳蓉（1996－），女，硕士，工程师，主要研究方向：网络安全、数据安全。

钟湘琼（1982－），通信作者，女，硕士，高级工程师，主要研究方向：信息化与网络安全。E-mail：26371759@qq.com。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部