基于等保 2.0 的重点行业工控系统网络安全防护策略研究

张 悦[1],荆 琛[2],衣 然[2]

(1.国能信息技术有限公司,北京 100080;2.华北计算机系统工程研究所,北京 100083)

摘 要:在两化融合的工业建设大背景下,工控系统的互联互通性逐步加强,系统所面临的网络安全风险也越来越大。针对工控系统网络安全现状,依据等级保护 2.0 相关标准,提出了一种可实现隔离、监测、预警、审计等功能的工控网络安全防护策略,并以烟草行业为例,完成了应用部署与安全验证,为工控系统网络安全建设提供了实践参考。

关键词:等保 2.0;工控系统;网络安全

中图分类号:TP393 **文献标识码**:A DOI:10.19358/j.issn.2096-5133.2021.09.009

引用格式:张悦,荆琛,衣然. 基于等保 2.0 的重点行业工控系统网络安全防护策略研究[J].信息技术与网络安全,2021,40(9):54-57,76.

Research on the security protection strategy of industrial control network in key industries based on classified security protection standard 2.0

Zhang Yue[1], Jing Chen[2], Yi Ran[2]

(1.Guoneng Information and Technology Limited Company, Beijing 100080, China;
2.National Computer System Engineering Research Institute of China, Beijing 100083, China)

Abstract: In the context of the integration of industrialization and information in industrial construction, the interconnection and interoperability of the industrial control system has gradually strengthened, and the network security risks faced by the system have also become greater. Aiming at the current status of industrial control network security, this paper proposes an industrial control network security protection strategy that can realize the functions of isolation, monitoring, early warning, and auditing based on classified security protection standard 2.0. Taking the tobacco industry as an example, the application deployment and security verification have been completed, which provides a practical reference for the construction of industrial control system network security.

Key words: classified security protection standard 2.0; industrial control system; cyber security

0 引言

随着信息通信技术的高速发展,信息化与工业化深度融合,工控系统从封闭走向开放。在提高生产力的同时,工控系统由于自身的脆弱性和系统漏洞,给黑客入侵工控网络提供了通道,并且,各种网络病毒等也都潜在威胁着工业安全[1-5]。在两化融合的大背景下,工控网络的安全防护正面临着严峻的挑战。

1 工控系统网络安全现状

工控系统在建设之初,主要考虑实用性和可靠性,网络中几乎没有任何针对外部攻击和病毒感染的发现、防御手段[6-7],当各种病毒、木马等外部威胁进入厂区管理网、办公网后,就可以直达现场控制层网络,直接威胁到工业生产安全。

工控网络目前主要面临的安全风险有[8-12]:

(1)黑客攻击风险

随着网络攻击自动化、组织化、规模化的发展,掌握黑客技术的人员数量不断增加,各类攻击手段、策略和工具层出不穷,造成了网络黑客的泛滥。

(2)网络病毒传播风险

网络病毒是影响计算机网络安全的威胁。目前,计算机网络病毒的种类繁多,如 2017 年爆发的

“永恒之蓝”病毒等。黑客技术的发展，使得病毒的种类增加、破坏性增强。若工控网络不具备病毒防护能力，会遭受网络病毒的危害，可能造成信息被篡改、破坏和盗取等，甚至可能会造成网络瘫痪，严重影响工控行业的发展。

我国《网络安全法》第 21 条、59 条明确了等级保护的必要性和重要性，网络安全保障不力需要运营单位和个人承担相应责任和处罚措施，落实等级保护制度已经上升到法律层面。同时国家相关部门对工控企业工控系统信息安全的重视程度不断提高。烟草行业作为国民经济的支柱产业之一，其卷烟厂在制丝、卷包、物流、动力能源等各个车间中大量使用工控系统，是重点工控行业[13]。以烟草行业为例，卷烟厂工控系统受到破坏后，轻则网络瘫痪、停产停业，重则威胁到操作员的人身安全，会对社会秩序和公共利益造成严重损害。按等保 2.0[14]中的三级防护能力要求对如图 1 所示的某卷烟厂工控网络进行安全评估，发现其风险等级为高，即网络环境脆弱，存在高风险威胁，一旦发生网络入侵将对企业产生较大的经济影响，在一定范围内给组织的经营和信誉造成损害。主要安全问题如下：

(1)区域边界方面

①各生产车间网络边界缺乏安全隔离和边界防护。

②缺乏网络攻击监测手段，不能及时发现工控系统网络内存在的安全隐患，以及病毒、木马、DDoS、扫描、SQL 注入、XSS、缓冲区溢出、欺骗劫持等攻击行为。

(2)计算环境方面

①主机设备缺乏移动介质管控措施，存在接入移动介质(如 U 盘、移动硬盘、智能手机、光盘等)引入病毒、木马的风险。

②主机系统安全漏洞难以修复，由于工业控制系统高可用性的特点，主机设备升级需要进行兼容性测试，未经测试升级可能会导致业务端口冲突，造成系统运行故障，故工控系统不能轻易进行更新，存在大量漏洞。

(3)管理中心方面

①缺乏集中运维与监管，不能对所有工控安全防护设备及系统的运行状况、安全策略、恶意代码、补丁升级、安全审计等进行集中式的分析与管控。

②缺乏设备行为的审计措施，不能对各类工控安全设备、工控网络设备、主机、数据库等系统设备的运行日志、操作记录进行收集、分析，在发生事故

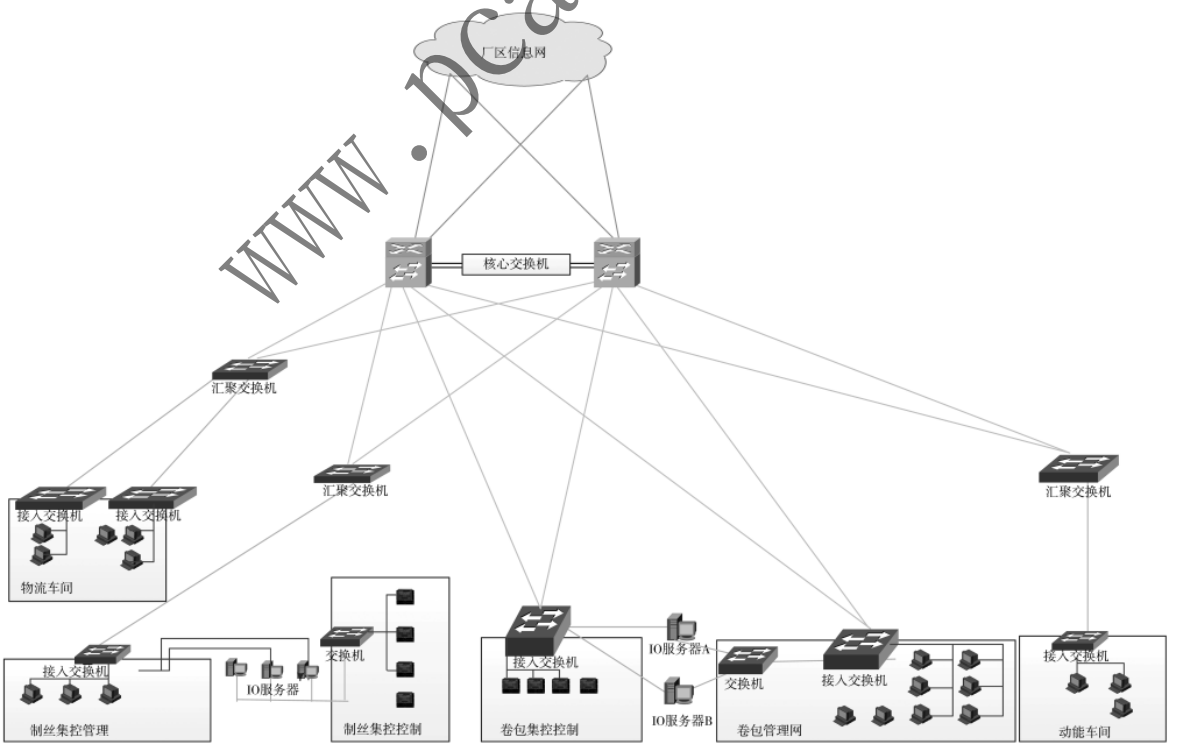

图 1 某卷烟厂工控网络拓扑图

后，难以实现事故分析和原因追溯。

2 安全防护策略设计

2.1 安全防护策略核心思想

针对工控系统缺乏技术防护手段应对网络攻击这一问题，本文提出了一种防护策略，其核心思想如下：

(1)区域隔离：通过工业防火墙进行区域隔离，对不同系统网段的访问通信进行细粒度设置，通过策略最小化设置限制生产网横向的非预期通信。

(2)监测预警：对生产网络中的流量进行特征匹配，及时发现异常流量并进行预警。

(3)终端加固：应用白名单技术，在系统正常运行阶段进行机器学习，形成进程运行的白名单，限制其他非预期的程序运行，同时可以修改主机注册表，限制移动介质的识别与自启动，防止移动介质的摆渡攻击。

(4)集中管控，联防联控：通过入侵监测、预警、审计，实现对安全事件的集中分析，结合应急方案形成快速处置方法，联合工控防火墙、主机白名单等安全防护措施进行联动，控制安全事件的发生与蔓延[15]。

(5)审计溯源：通过收集、分析各类工控设备、主机、数据库等的日志记录，实现异常报警、事故分析和原因追溯。

2.2 安全防护政策部署——以某卷烟厂为例

通过部署工业防火墙、工控入侵检测系统、工控监测分析预警系统、工控日志审计系统、工控数据库审计系统、工控主机加固软件、工控运维审计系统，实现各车间网络的区域分离、监测预警、终端加固、审计溯源、集中管控、联防联控，完善工控系统安全体系框架，提高工控网络的安全系数。以上文提到的某卷烟厂工控网络为例，图 2 为其完成安全防护策略实际应用部署的示意图，详细部署如下。

2.2.1 区域边界方面

(1)区域隔离

在制丝、卷包、物流、动力能源等各个车间的接入交换机与汇聚交换机之间部署工控防火墙，实现生产网络各区域的安全逻辑隔离和边界防护，避免生产区域之间的越权访问，防止病毒、蠕虫等恶意代码扩散和入侵攻击。通过部署、调试工控防火墙，根据业务需求进行策略最小化配置，用于分区分域，过滤非授权访问，保证只有授权的通信链接才允许通过。

(2)监测预警

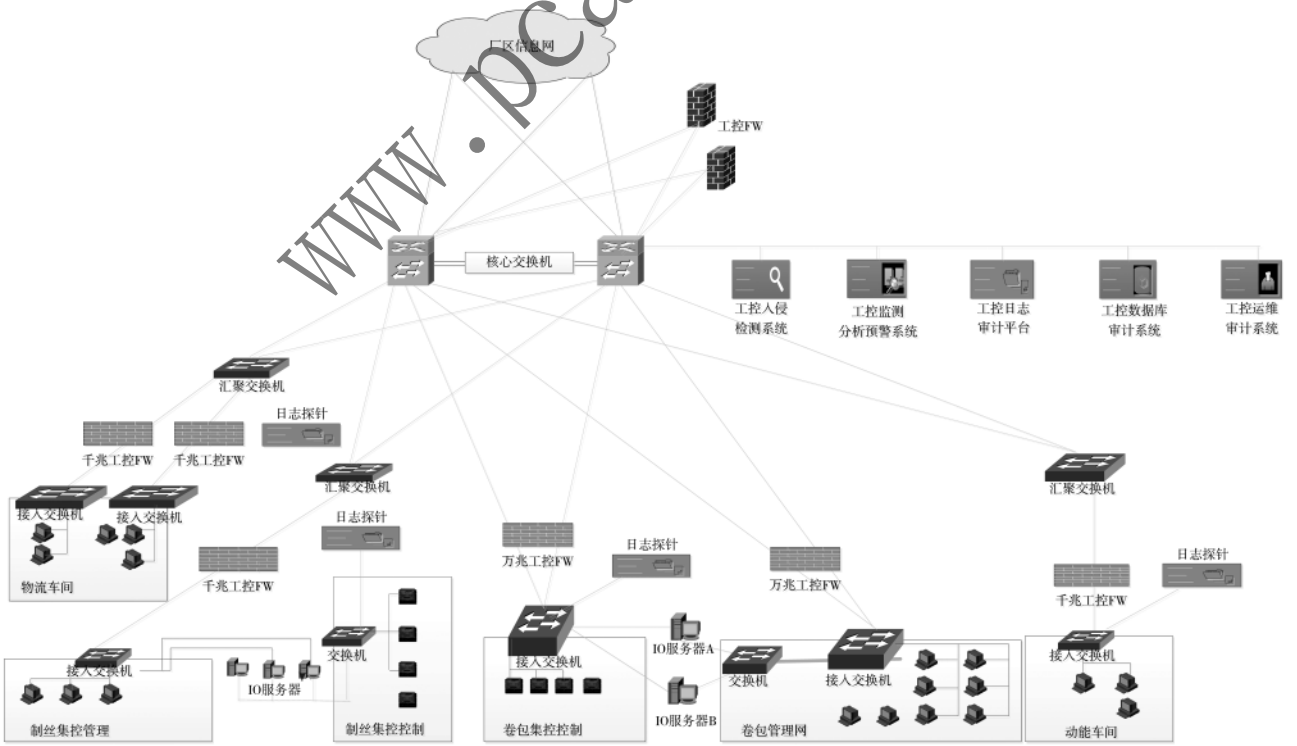

图 2 某卷烟厂工控网络安全防护策略示意图

监测类设备主要包括工控入侵检测系统、工控监测分析预警系统。监测工控网络异常流量,及时发现工控网络各层面安全隐患以及病毒、蠕虫、木马、DDoS、扫描、SQL 注入、XSS、缓冲区溢出、欺骗劫持等攻击行为,形成综合预警和态势感知的能力。

2.2.2 计算环境方面

工控主机加固软件既可防止终端被移动介质,如 U 盘、移动硬盘、智能手机、光盘等,带入的病毒木马入侵,还能通过在网络内部主机中依据程序特征建立操作系统运行的白环境,禁止非授信程序运行,解决操作系统因无法升级补丁带来的安全问题,保证系统的稳定运行。区别于传统的杀毒软件,计算环境的终端加固不依赖于特征库,不用频繁升级,适配于不能及时进行更新的工控环境。

(1)建立白名单库

通过快速磁盘检索机制全盘扫描筛选信任程序、快速建立白名单信任库,创建本地白名单信任库。

(2)启动防护

系统初始时扫描 exe 后缀的可执行程序,以及 dll、sys、ocx、bat、vbs 等所有 pe 格式的文件与脚本文件。采集这些文件的路径名称、数字证书信息、数字证书完整性、公司名称、版本信息、PE 头信息、文件的 SM3 哈希值。通过这些信息组合的条件校验这些文件是否可以被执行。

(3)外设防护

配置外设防护策略,检测移动外部设备的使用情况。支持 U 盘白名单设置,只允许指定的 U 盘插入并产生记录。

2.2.3 管理中心方面

(1)集中管理,联防联控

部署工控运维审计系统对所有工控安全防护设备及系统进行统一管理、分析,降低运维管理成本。开启互联网连接预警,在互联网连接状态发生改变时产生报警,可有效防止私自使用无线设备上网导致的信息外露事件。在监测类设备发现异常流量、入侵行为后,联合工控防火墙、主机白名单等安全防护措施设置相应策略,阻挡攻击行为,控制安全事件的发生与蔓延。

(2)审计溯源

审计类设备主要包括工控日志审计系统、工控数据库审计系统、工控运维审计系统以及制丝、卷包、物流、动力能源等各个车间部署的日志探针。收集各类工控安全设备、工控网络设备、主机、数据库等系统设备的运行日志、操作记录,分析和处理后及时通知管理人员,从而达到预防、事故分析和原因追溯的目的。

3 安全防护策略验证

对实现了工控网络安全防护策略实际应用部署的卷烟厂进行安全测评,其在技术层面的主要验证结果如下:

(1)区域边界防护验证

生产网通过部署工控防火墙,合理设置策略。通过办公网对生产网内系统进行渗透测试,发现仅在应用层面存在点击劫持、配置文件信息泄露两个低危漏洞,无法绕过工控防火墙对系统内部进行深入利用。

(2)终端加固验证

选择某台工作站关闭 USB 封闭功能,将恶意脚本拷入 U 盘中接入工作站,点击运行,发现恶意脚本无法执行,其进程无法启动,被白名单软件拦截。

(3)审计溯源验证

对系统进行配置更改,查询工控日志审计系统、工控运维审计系统,能够展示时间和日期、用户、操作详情等重要信息,形成审计记录,供审计员对安全事件进行分析与责任追溯。

(4)内网渗透验证

通过内部接入交换机进行网络扫描,入侵检测系统、工控监测分析预警系统形成告警日志,并提示网络安全员对事件及时处置。

完成系统的加固部署后,对生产系统再次按等保 2.0 中的三级防护能力要求进行安全评估,发现其风险等级由高降为低,不存在中高风险问题,证明了该安全防护策略的有效性。

4 结论

本文依据等保 2.0 相关标准,针对工控系统缺乏技术防护手段应对网络攻击行为这一问题,提出了可实现区域分离、监测预警、终端加固、审计溯源、集中管控、联防联控的整体防护策略,有助于管理人员及时发现安全事件,快速做出响应处置,提高工控系统网络安全防护能力。且已在某卷烟厂完成了实际应用部署、试运行及安全测评,证明了该防护策略的可用性、有效性,为工控系统提供了良好的安全防护案例。

(下转第 76 页)

保密科学技术,2020(5):16-19.
[15] 刘冬,程曦,杨帅锋,等.加强我国工业信息安全的思考[J].信息安全与通信保密,2019(8):24-35.
[16] 钟欣.美国总统特朗普签署网络安全行政令[N].人民邮电报,2017-06-05.
[17] 工业和信息化部,国家标准化管理委员会.工业互联网综合标准化体系建设指南[R].2020.
[18] 尚文利.功能安全与信息安全相结合,实现工业系统的两安融合[J].自动化博览,2020,37(2):16-17.
[19] 安成飞,周玉刚.智能制造工业互联网的安全分析与防护[J].自动化博览,2021,38(1):82-85.
[20] 康帝.5G网络中工业互联网安全问题研究[J].电子元器件与信息技术,2020,4(6):22-23.
[21] 谢丰,伊胜伟,高洋.加强工业互联网风险分析与安全测评,保障"新基建"安全[J].中国信息安全,2020(7):36-38.
[22] 科技日报.5G面临风险大考:我国一半以上工控系统带毒运行[EB/OL].(2019-06-24).http://www.xinhuanet.com/ 2019-06/24/c_1124660796.htm.
[23] 赵丽莉,周彤.以CPS为核心的工业互联网安全风险及监管控制[J].北京科技大学学报(社会科学版),2021,37(1):48-55.
[24] 郭宾,雷曜,朱奕辉.浅谈工业互联网安全服务云建设思路[J].中小企业管理与科技(中旬刊),2020(5):128-129.

(收稿日期:2021-03-31)

作者简介:

肖泄栅(2000-),女,本科,主要研究方向:网络信息安全。

洪晟(1981-),男,博士,副教授,主要研究方向:网络信息安全、复杂系统安全运行状态监测与健康管理、复杂系统通用质量"六性"技术。

(上接第57页)

参考文献

[1] 陈晓兵,陈凯,徐震,等.面向工业控制网络的安全监管方案[J].信息网络安全,2016(7):61-70.
[2] 孟瑾,石怀忠,崔建华.基于烟草工控网络安全防护策略与应用[J].网络安全技术与应用,2019(12):158-161.
[3] 唐亮,唐树莺,杨帆.卷烟物流分拣工业控制系统网络安全防护体系设计[C]//中国烟草学会2017年学术年会,2017.
[4] 匡建华.烟草企业网络安全防护体系建设[J].电子技术与软件工程,2017(18):205-206.
[5] 曾瑜,郭金全.工业控制系统信息安全现状分析[J].信息网络安全,2016(9):169-172.
[6] 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.
[7] 耿欣.烟草行业工业控制系统安全保障体系研究[J].烟草科技,2017,50(12):99-105.
[8] 李愿军.省级烟草企业网络与信息安全的思考[J].电子技术与软件工程,2017(21):211-212.
[9] 张承亮,宁欣,郭军,等.烟草行业的数据防泄漏[J].电子技术与软件工程,2019(7):194-195.
[10] 朱洪波.烟草行业数据安全管理平台的研究[J].网络安全技术与应用,2019(6):93-95.
[11] 韩晓樱,冯明辉.浅谈福建中烟网络安全体系建设[J].网络安全技术与应用,2019(7):115-116.
[12] 王昱镔,陈思,程楠.工业控制系统信息安全防护研究[J].信息网络安全,2016(9):35-39.
[13] 樊金健,谢一飞.基于安全域划分的网络安全体系设计:保障烟草工业企业安全生产[J].工业技术创新,2019,6(2):59-65.
[14] GB/T 22239-2019 信息安全技术-网络安全等级保护基本要求[S].北京:中国标准出版社,2019.
[15] 陈兴毕,李源,殷耀华,等.基于烟草工控系统网络安全风险评估的研究与应用[J].信息技术与网络安全,2019,38(7):19-26.

(收稿日期:2021-06-25)

作者简介:

张悦(1990-),女,硕士,工程师,主要研究方向:网络安全。

荆琛(1994-),女,硕士,助理工程师,主要研究方向:网络安全。

衣然(1988-),男,硕士,工程师,主要研究方向:网络安全。

版权声明

经作者授权，本论文版权和信息网络传播权归属于《信息技术与网络安全》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《信息技术与网络安全》编辑部

中国电子信息产业集团有限公司第六研究所