文章编号：1007-757X(2019)03-0112-04

区块链技术在烟草系统工控安全中的应用

徐元清，　卓蔚

（上海烟草集团有限责任公司 信息中心，上海 200082）

摘　要：设计了适用于烟草行业的工业控制系统的安全防护系统。针对现有烟草行业工控系统的实际安全问题，提出了包括信息技术(IT)和操作技术(OT)在内的全方位防护系统。烟草行业现有的安全防护体系主要部署在信息系统内部以及和工业现场的边界，从边界防护、漏洞检测、运维审计、全面监控等方面进行风险的监控和攻击的检测。在现有网络安全系统的基础上，提出一个基于区块链技术的新的解决方案，利用区块链技术的集体维护、可靠数据库、不可篡改等特点，针对可能受到的威胁和攻击进行防护和修复，实现从信息管理层到现场控制和设备层的安全身份认证，以及文件和数据的不可篡改等，从而实现对现有安全系统的补充和加强，提高整个工控系统的安全性和生产的安全防护水平。

关键词：区块链；安全防护；工业控制系统；身份认证；数据安全

中图分类号：TP311　　文献标志码：A

Application of Blockchain Technology in Cyber Security for Industrial Control Systems in Tobacco Industry

XU Yuanqing, ZHUO Wei

(Information Center of Shanghai Tobacco Group Co., Ltd., Shanghai, 200082)

Abstract: This paper presents a cyber security approach that has multiple layers of protection for industrial control systems in the tobacco production. Based on the cyber security challenges and solutions of current tobacco industrial control systems, it proposes a new approach that includes a full coverage of both information technology and operation technology. The existing security protection system of the tobacco industry is mainly to focus on the information network, and on the boundary of the information network and industrial control network. It carries out risk monitoring and attack detection by boundary protection, intrusion detection, operation and maintenance audit, and comprehensive monitoring etc. The new solution proposed in this paper is based on blockchain technology and utilizes the characteristics of blockchain technology, such as consensus driven, reliable database, and immutability etc., to protect, reduce and repair the possible threats and attacks. This approach realizes the security identity authentication and the tamper-proof of documents and data, and intensively integrates the information network and the industry control network, so as to effectively improve the security level of the current industrial control system, and to ensure the security protection of production.

Key words: Blockchain; Cyber security; Industry control system; Security identity; Data security

0　引言

工业控制系统(ICS)，是指用于操作、控制、辅助自动化工业生产运行、过程控制与监控的由各种自动化控制组件(包括设备、系统、网络以及控制器)的集合[1,2]。工业控制系统主要包括监控和数据采集系统(SCADA)，分布式控制系统(DCS)和可编程逻辑控制器(PLC)。在我国的烟草行业中已经广泛使用到各类工业控制系统，其中主要的是 SCADA 和 PLC 两类。这些工业控制系统的网络结构主要分为管理协同层、生产执行层、过程监控层、现场控制层和现场设备层[3]。管理协同层和生产执行层组成管理网，过程监控层、现场控制层和现场设备层组成工控网，两网之间存在较多的信息交互，联系紧密。从业务角度考虑，管理网和工控网必须互联，以交换命令和数据；但从安全角度考虑，管理网网络复杂，并和互联网相连，两网互联造成了管理网风险引入工控网。所以，信息技术在推动工业化快速发展的过程中，也给工业系统的安全运行带来了巨大的风险。

近年来，随着两化融合的不断推进，工业互联网深入发展，传统的互联网与工业网不断的加速对接和融合，工业网的安全问题也引起了更加广泛的关注和研究[4]。对工控系统网络安全防护体系的研究和分析已经成为当今社会关注的重点之一[5]。然而，现有的工业安全防护系统都是针对过程监控层及以上的信息技术网络部分，以及从信息网络到工控网络之间的边界部分。从现场控制层和现场设备层所在的操作技术网络来看，各种可编程逻辑控制器(PLC)以及某些现场设备，以及工控交换机都存在着传统的网络通信端口

作者简介：徐元清(1976-)，男，上海市，本科，研究方向：网络安全管理，信息化项目管理和信息化治理在企业的应用。

卓蔚(1978-)，男，上海市，本科，研究方向：工控安全和信息化项目建设在企业的应用。

和模块，同时这些设备本身存在的漏洞和威胁，都没有在现有工控安全解决方案的监控范围之内，很容易因为攻击而严重威胁工控系统的安全性。另外，工控网络中经常需要从管理层的 ERP(企业资源规划)和 MES(制造执行系统)向监控中心下发指令，以及从监控中心向 PLC 下发逻辑组态工程文件，该文件编译成功后即可运行。实际运用中这些指令和文件在下发过程中有可能遭到篡改或替换，导致文件编译失败或无法运行，严重时被植入恶意指令，后果不堪设想。同时，现场设备采集到的数据也需要向数据中心发送，保证这些数据的安全性和完备性也是非常重要而且必须的。而传统工控安全解决方案在工业大数据的应用背景下，越来越不能满足工业现场的安全需求。

基于工业现场的安全需求，以及工业现场设备、传感器和控制器的广泛分布并互联的特点，本论文提出了基于区块链技术的工业安全解决方案。区块链作为一个在数字货币中广泛使用的新技术，由于其去信任、去中心化、集体维护、可靠数据库等特点[6]，在工控安全领域，从设备安全接入的身份认证，增强指令、文件和数据完整性以及防篡改等方面来看，应用潜力很大。将区块链技术引入工控网安全应用中，将是一个非常具有前景的研究方向。目前，区块链在物联网中的应用已经引起了广泛的关注[7-9]，在工业互联网以及工控系统中的应用还有待进一步的研究。

1　基于区块链的关键技术

区块链的概念在 2008 年由中本聪第一次提出[10]，在随后的几年中，成为了电子货币的核心组成部分。简单来说，区块链是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案。该技术方案让参与系统中的任意多个节点，把一段时间系统内全部信息交流的数据，通过密码学相关算法计算和记录到一个数据块，并且生成该数据块的指纹用于链接下个数据块和校验，系统所有参与节点来共同认定记录是否为真。

区块链最主要的四个特征包括去中心化、去信任、集体维护、可靠数据库。去中心化保证了任意节点之间的权利和义务都是均等的，且任一个节点的损坏或者失去都会不影响整个系统的运作。因此也可以认为区块链系统具有极好的健壮性。去信任保证了参与整个系统中的每个节点之间进行数据交换是无需互相信任的，整个系统的运作规则是公开透明的，因此在系统指定的规则范围和时间范围内，节点之间是不能也无法欺骗其它节点。集体维护是指系统中的数据块由整个系统中所有具有维护功能的节点来共同维护的，而这些具有维护功能的节点是任何人都可以参与的。可靠数据库是指整个系统将通过分布式数据库的形式，让每个参与节点都能获得一份完整数据库的拷贝。除非能够同时控制整个系统中超过 51%的节点，否则单个节点上对数据库的修改是无效的，也无法影响其他节点上的数据内容，从而保证在节点之间交换的信息的不可篡改。

区块链的概念首次在中本聪的论文《比特币白皮书：一种点对点的电子现金系统》中提出，因此可以把比特币看成区块链的首个在金融支付领域中的应用。随着区块链技术的进一步发展，它在除了数字货币和金融以外的其他领域也都有了广泛的应用和探索。在万物互联的时代，区块链技术未来在工控网络也具有广阔的发展前景。工控网络相对比较封闭，通常处于企业内部网络运行，在企业内部建立小范围的私有区块链平台比较适合。私有区块链的成员共同建立有关成员资格，访问权和参与权的规则，包括授予和终止此类权利的标准。私有区块链通常将实施和执行此类规则的责任委托给管理员，并可授权管理员修改规则以应对不断变化的条件。除了成员资格，访问和参与权限之外，还可以划分网络上的数据的访问权限，以防止参与者有意或无意地访问其他参与者的敏感商业和客户数据。

图 1 是物流车间原料库的网络拓扑图。管理网主要体现在图 1 中的“服务器机房”标签位置处，部署了服务器及磁盘阵列、核心交换机等 IT 设备。工业网包含了厂区内的中控室、现场工业设备等，其关键节点为中控室内的工业交换机。该工业交换机连接了主 PLC、从 PLC 及盲节点服务器等，往下一级为现场人机交互接口 HMI 及其他工业设备。

从层级上来看，工业交换机往下层级主要采用工业协议，往上层级主要采用互联网协议(TCP/IP)。原料库整体网络结构具有较为明显的层级划分，是典型的工业网络环境，从网络安全的角度来看，缺少必要的边界隔离及访问控制等措施，也缺少必要的网络安全监控手段。

为了提高工控系统的安全性，如图 1 和图 2 所示。

处于工控网内的各级服务器，交换机，PLC，甚至底层设备都可以作为参与节点接入区块链网络。区块链网络是个轻量级的网络，在进阶精简指令集机器架构 ARM(嵌入式系统芯片)上也可以运行。对于具有足够计算和存储能力的服务器、控制器和智能设备等，可以直接接入网络，在上面运行区块链相关协议。对于计算能力较弱或不方便直接修改的设备，可以用运行区块链协议的智能网关等作为代理，接入区块链网络。由于网络由参与节点共同维护，区块链网络具有高度的可扩展性，在实施中可以根据实际需求进行组网，例如，当管理层节点和工控层节点之间不能直接连接时，可以在各区内部分别组网。

2　区块链技术在工控系统中的应用

区块链网络是一个分散的点对点网络，因此它对故障具有弹性，没有单点故障。区块链本身在参与方达成共识后，无法更改或删除曾经记录在区块链上的交易。区块链网络中的所有交易都受到强加密的保护，而且透明性使其安全且可审计。这些特点都使其在工控安全中得到广泛的应用成为可能。下文讨论并给出区块链在工控系统中可能的应用场景。

2.1　工程文件防篡改

工控网络中经常需要从监控中心的工程师站向 PLC 下发逻辑组态工程文件，该文件编译成功后即可运行。实际运用中可能遇到文件在下发过程中遭到篡改或替换，导致文件无法运行，严重时被植入恶意指令，后果不堪设想。

为保证逻辑组态工程文件发布的正确性，可以建立工控网络区块链文件发布系统用于存储逻辑组态工程文件，该系统包括 2 层结构，底层由区块链数据库构建，上层是面向用户的工控网络区块链平台。如图 3 所示。

用户向区块链平台管理员申请发布逻辑组态工程文件，管理员审批通过后可将逻辑组态工程文件编译后的文件的

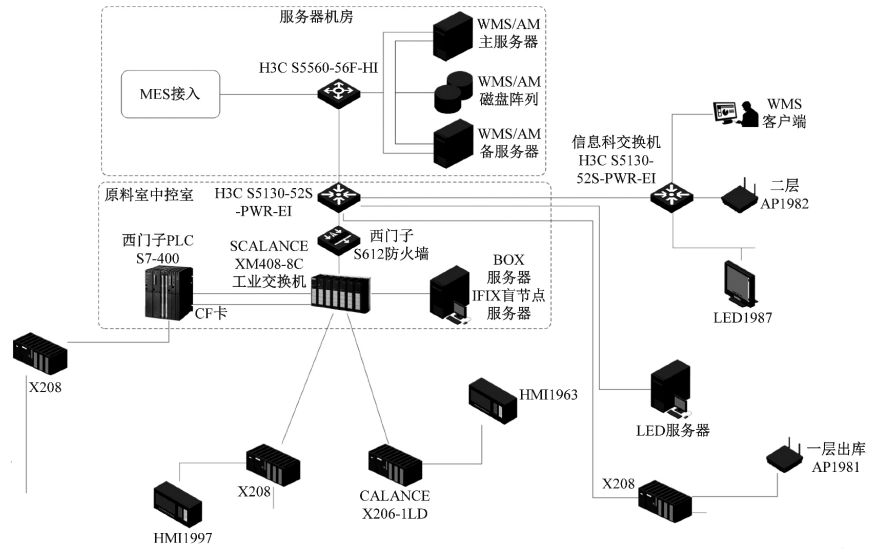

图 1　物流车间网络拓扑图

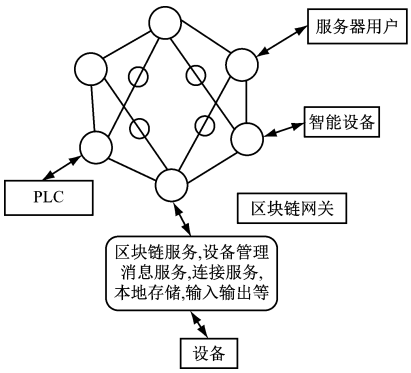

图 2　工控系统区块链网络示意图

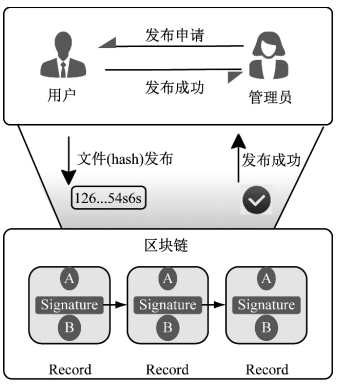

图 3　工控网络区块链文件发布系统

相关信息形成发布摘要信息存储到区块链上。发布摘要信息包括存储发布方 A(监控中心)和接收方 B(PLC)的地址，发布文件的哈希值等，并由区块链各节点共同盖上时间戳。发布摘要信息可以根据发布单号进行查询。PLC 下载逻辑组态工程文件后，根据发布单号将编译后的文件哈希值和区块链上的数据进行比较，如果不一致，说明文件遭到篡改并向监控中心报警。

通过逻辑组态工程文件区块链发布技术，实现了逻辑组态工控文件一旦发布就无法被篡改。攻击者即使在接收端修改组态文件，也会由于验证无法通过从而无法运行达到保护目的。该技术解决了传统逻辑组态工程文件易被第三方修改的问题。

除了逻辑组态工程文件，从管理层发往控制层的指令文件，以及从现场设备传往数据中心的相关数据，都可以通过区块链技术进行安全的分享和保护，防止被第三方篡改。

2.2　身份验证

不同于传统的工控安全采取的检测和监控可能受到的身份接入的攻击，区块链技术关注的是预防而不是检测。对于区块链网络而言，每个接入请求都要经过整个系统里节点的共识来进行认证。因此，即使是单个节点或部分节点受到攻击，整个系统的共识会阻止其他节点乃至整个系统被黑客攻击，因此可以实现持续连接。比如，被攻击的节点试图输入错误的密码和用户名，那么区块链的共识机制会拒绝该请求并且自我修复，不妨碍整个系统的正常连接和运行。因此，区块链技术涵盖了传统的工控安全系统提供的安全接入的部分功能，但传统工控安全系统更多的是检测此类行为而不是预防。

今天的工业正在经历转型变革，在现在的工业系统中，设备，人员和应用程序有更多的合作，共同交换数据，做出决策并采取行动。基于区块链的身份验证和身份管理可实现任意应用程序级的安全性和访问控制。管理员能够立即为设备，应用程序和人员创建安全组和策略，以实现安全的协作和数据交换。

对于烟草生产的工控系统而言，区块链技术不仅可以用于管理层的服务器，工程师站，数据中心，人机界面(HMI)等处的身份接入的认证，还可以直接用于现场智能设备和控制器的接入认证。随着工业互联网和工业云的发展，设备越来越智能化，数据和连接逐渐地向智能设备迁移，越来越多的智能设备以及 PLC 等可以直接接入到工控系统中。这样的扩展可以提高效率以及生产力等，但是同时也给整个公司的工业系统带来了安全挑战。在这种情况下，区块链的分布式架构非常适合提供智能设备标识、身份验证和无缝的安全数据传输。

在基于区块链的系统中，当用户尝试接入系统或访问受保护应用程序时，会收到来自受保护对象的身份验证请求。

用户将验证请求数据是否合法，受保护的应用是否是他们期望的对象。这可以通过使用公钥加密来完成。受保护的对象对请求进行签名，然后通过区块链对其进行公开验证。在验证此请求后，用户创建响应，发送登录信息并对其进行签名，然后将其发送回受保护对象上的指定路由。这个请求将使用受保护对象上的公钥加密来验证，验证通过后用户将登录。这个过程并不局限于某个应用或设备。如果用户不想使用特定应用来登录，则用户可以使用其公钥生成自己的签名并以表单形式提交，然后区块链网络将对其进行验证，如图 4 所示。

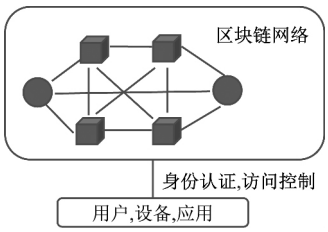

图 4　工控网络区块链身份认证

3　总结

本论文基于区块链技术，对烟草行业工业控制系统安全防护体系进行了升级设计，弥补了传统工控安全体系在工业控制系统(ICS)尤其是在操作技术领域的不足，为确保工控系统的稳定可靠运行和信息安全提供有力支撑和全面保障。区块链技术在工控系统安全领域的应用目前还处于起步阶段，本论文提出的安全防护体系的设计，未来在行业内具有一定的推广价值，在行业内可以起到应用示范的作用，可以进一步推动区块链新技术在其它行业的工控安全系统的深入研究和应用实践。

参考文献

[1] 耿欣. 烟草行业工业控制系统安全保障体系构建[J]. 烟草科技，2017，50(12)：99-105.
[2] 张克伟，曹兴强，刘贵阳，等. 烟草工业控制系统安全防护分析与对策[J]. 科技论坛，2014(2)：144-145.
[3] 薛训明，杨波，汪飞，等. 烟草行业制丝生产线工业控制系统安全防护体系设计[J]. 科技展望，2016，26(14)：264-265.
[4] 陈亚亮，杨海军，姚钦锋，等. 工业控制系统网络安全防护体系研究[J]. 信息网络安全，2013(10)：57-59.
[5] 林枫. 工业控制系统网络安全防护体系的思考[J]. 信息通信，2017(5)：123-124.
[6] 中本聪(Satoshi Nakamoto). 比特币白皮书：一种点对点的电子现金系统[M/OL]. (2017-01-01) https://www.8btc.com/wiki/bitcoin-a-peer-to-peer-electronic-cash-system.
[7] Arshdeep Bahga, Vijay K Madisetti. Blockchain Platform for Industrial Internet of Things[J]. Journal of Software Engineering and Applications, 2016, 9(10)：533-546.
[8] 赵阔，邢永恒. 区块链技术驱动下的物联网安全研究综述[J]. 信息网络安全，2017(5)：1-6.
[9] 冯泽冰，方琳. 区块链技术增强物联网安全应用前景分析[J]. 电信网技术，2018(2)：1-5.
[10] Arind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Gold feder. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 2016.

(收稿日期：2018.12.12)

(上接第 106 页)

[5] Mayoral A, López V, de Dios O G, et al. Migration steps toward flexi-grid networks[J]. Journal of Optical Communications and Networking, 2014, 6(11): 988-996.
[6] 王峥瑜，宁帆，黄善国，等. Mixed-Line-Rate IP over OTN 网络中基于蚁群算法的路由和资源分配策略[J]. 光子学报，2014，43(S1)：35-38.
[7] 熊毅，郑睿. 面向智能电网的 OTN 网络规划及组网方案探讨[J]. 中国新通信，2014，16(17)：2-3.
[8] Eramo V, Listanti M, Lavacca F G, et al. Performance evaluation of integrated OTN/WDM metropolitan networks in static and dynamic traffic scenarios [J]. Journal of Optical Communications and Networking, 2015, 7(8): 761-775.
[9] Ye Y, Jiménez T, López V. Spectral, cost and energy efficiencies analysis in WDM MLR networks with OTN switching[J]. Photonic Network Communications, 2017, 34(3): 422-431.
[10] 赖俊森，汤瑞，李少晖，等. 400G WDM 系统关键参数测评方法研究[J]. 电信网技术，2015(4)：65-68.
[11] Kim D H, Bae H J, Han M K, et al. Direct admission to stroke centers reduces treatment delay and improves clinical outcome after intravenous thrombolysis [J]. Journal of Clinical Neuroscience, 2016, 27: 74-79.
[12] 刘爱军，杨育，李斐，等. 混沌模拟退火粒子群优化算法研究及应用[J]. 浙江大学学报(工学版)，2013，47(10)：1722-1730.
[13] 李中华，张泰山. 可拓聚类适应度共享小生境遗传算法研究[J]. 哈尔滨工业大学学报，2016，48(5)：178-183.
[14] 邝祝芳，陈志刚，刘蕙. 一种认知无线 Mesh 网络中负载均衡的组播路由算法[J]. 计算机学报，2013，36(3)：521-531.
[15] 李永林，叶春明，刘长平. 轮盘赌选择自适应和声搜索算法[J]. 计算机应用研究，2014，31(6)：1665-1668.
[16] 周聪海，黄智贤，邱挺，等. 随机搜索算法在换热网络优化中的应用进展[J]. 化工进展，2012，31(3)：495-501.
[17] 武兴亮，丁根宏. 改进小生境遗传算法求解多峰函数优化问题[J]. 信息技术，2013，37(1)：73-76.

(收稿日期：2018.03.08)