文章编号:1671-251X(2023)S1-0032-05

# 基于白名单的煤矿网络“白环境”构建研究

杭成宝

(国能北电胜利能源有限公司,内蒙古 锡林浩特 026000)

**摘要**:为保障煤矿智能化建设,做好煤矿网络安全防护,以国能北电胜利能源有限公司为例,通过鱼骨图剖析了煤矿企业被动式防御的网络安全现状、问题及其原因,提出基于白名单构建煤矿网络“白环境”,实现主动防御。首先,在区分黑名单和白名单机制的基础上,基于白名单化繁为简的可靠技术特性,采用沙漏模型分析了将白名单机制转变白名单理念贯穿于网络安全架构中的必要性;其次,基于白名单理念,参考网络安全等级保护 2.0 的防护标准,设计了基于白名单技术的网络“白环境”架构,实现纵深防御、监测预警与协同防御的目标。最后,采用 PDCA 理论开展网络“白环境”安全运营闭环管理,为企业发展持续提供可靠的网络安全防护。

**关键词**:煤矿智能化;网络安全;主动防护;白名单;白环境

中图分类号:TD67　　文献标志码:A

# Research on the construction of "white environment" in coal mine network based on white list

HANG Chengbao

(CHN Energy Beidian Shengli Energy Co., Ltd., Xilinhot 026000, China)

## 0 引言

随着云计算、5G、虚拟化及人工智能(Artificial Intelligence,AI)等信息技术的快速发展与应用,在“四个革命、一个合作”能源安全新战略和“碳达峰、碳中和”绿色发展战略引导下,深入开展煤炭行业供给侧结构性改革,不断推进煤炭高质量发展,进一步将煤矿传统工艺与信息技术深度融合,实现煤矿数字化转型,发展煤矿智能化,成为煤矿发展的必由之路。2020 年 3 月 8 部委发布《关于加快煤矿智能化发展的指导意见》以来,基于“减人、增安、降本、提效”的智能化发展理念,在各煤矿生产工艺环节,各类智能化应用呈井喷式涌现,尤其是煤矿智能掘进、无人驾驶运输、无人破碎、无人装车、智能选煤、煤矿机器人等智能化生产应用系统得到加速发展与推进,加快了煤矿智能化发展的进程[1]。而以计算机为核心的信息技术是把双刃剑,自从 1987 年发现了全世界首例计算机病毒 c-brain 以来,病毒不断困扰着涉及计算机领域的各个行业,随着煤矿企业智能化水平迅速提高,其面临的网络安全问题更多,工控系统受控基础设施将受到破坏,网络安全问题会演变成现实物理安全问题,其安全风险是灾难性的,建设相对可靠完善的网络安全防御是煤矿智能化建设中适应新时代网络安全问题的需求。

当网络互联互通时,恶意代码、木马病毒或者异常攻击的流通也会变得更加方便,针对该问题,世界各大安全厂商、专家学者都在不懈努力。孟令强等[2]、汪锋等[3]提出了白名单主动防御系统的设计理念,在网络环境下建设白名单可信应用程序子系统,从而在根源上制止恶意软件的运行和传播,实现计算机系统启动、加载和运行全生命周期的安全保证。接着有专家提出基于白名单构建访问控制模型、开展异常违规行为监测的新技术思路[4-5]。2014 年白名单机制开始用于办公系统,2015 年白环境管理开始应用于安全运维中,2017 年白名单机制开始应用于工业控制入侵检测中,以提升工控网络的各种攻击和异常检测率[6-10],2019 年白名单被应用于视频监控网中实现主动防护,之后白名单技术在 Web 应用、主机防病毒等安全防护中得到应用[11-13]。在煤矿智能化建设过程中,从工控生产到办公经营决策涉及各类信息化系统,变被动防御为主动防护亟待进一步研究。

**收稿日期**:2023-07-11;**责任编辑**:胡娴。

**作者简介**:杭成宝(1979—),男,山东滨州人,高级工程师,硕士,主要研究方向为露天煤矿网络安全与基础通信建设,E-mail:hchbao@qq.com。

本文以国能北电胜利能源有限公司(以下简称胜利能源)为例,通过鱼骨图剖析了煤矿企业网络被动式防御的现状、问题及其原因,以煤矿办公网、工控网、智能化系统等作为防护对象,按照网络安全等级保护 2.0(简称等保 2.0)的防护标准,提出摒弃传统网络安全防护理念,基于白名单构建网络“白环境”,实现主动防御。

## 1　煤矿智能化建设中存在的网络安全问题

2013 年以来,国家信息安全漏洞共享平台收录的安全漏洞每年平均增长率达 12.7%[14]。2021 年以来,网络安全态势有了新的变化,移动终端恶意程序数量上升速度较快,高危零日漏洞和事件性漏洞数量上升,网络攻击呈现出有组织、有针对性、攻击工具专业化、攻击手段多样化、趋向智能化、技术门槛降低的趋势,网络安全威胁逐渐增大。如何开展并做好攻击面管理、数据安全平台、软件定义边界安全访问技术、AI 安全运营成为研究热点。

煤矿企业需要意识到,基于网络的连通性智能化系统一旦受控,将面临“一点突破,全面受控”的危险。2016 年张涛[15]就提出电网信息安全的四大核心问题是生产管理人员部到位、计算机管理不到位、网络隔离不严以及人员安全意识淡薄。结合当前网络安全态势,在煤矿智能化发展过程中,以胜利能源为例,除了以上网络安全问题,主要还体现在以下方面:① 虽然实现了办公、视频监控和工控网三网隔离,部署了部分安全设备,但公司网络安全防护属于被动式防护,被动式的运维和管理,设备单一,缺乏实时性网络监测预警,无法满足主动式网络安全防护攻击溯源分析。② 在集团统建互联网出口、VPN 办公和公司自建网络准入、入侵监测等防护基础上,办公网仍存在内部攻击缺乏感知联动分析、缺乏攻击情报支撑等问题;工控网存在网络未细化分区、区域边界缺少监测、计算环境账号混用、主机系统裸奔等问题;运维管理存在人才欠缺、传统运维服务效率低等问题。

网络安全问题鱼骨图如图 1 所示。运用鱼骨图分析网络安全问题涉及安全意识、组织管理、技术人才、安全分区、设备策略、安全运营 6 个方面,包括网络安全意识差、组织协调难、专业技术人才发展认可不足、专业人员少、专业性差距大、安全设备种类单一、安全设备策略粗放、网络安全分区整体规划简单、网络安全运营处于被动式防护且缺乏周期性更新运营等 18 个原因。要保证煤矿智能化顺利发展,必须针对这些问题有针对性地统筹考虑。本文结合这些问题提出基于白名单构建煤矿网络“白环境”,实现主动网络安全防御。

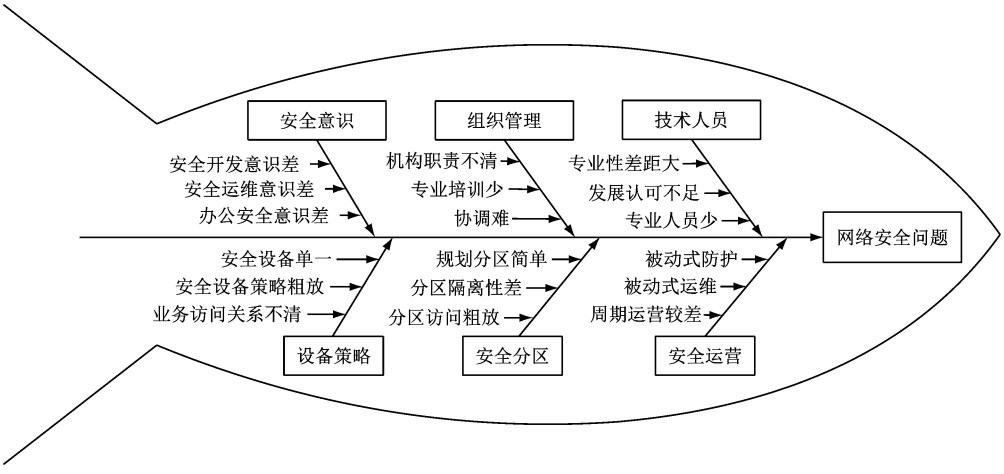


图 1　网络安全问题鱼骨图

## 2　基于白名单的网络“白环境”构建

在智能化建设发展过程中,煤矿企业要遵循网络安全“三同步”的原则,综合考虑网络态势现状,预防零日漏洞、多样化网络攻击,要高起点摒弃传统网络安全防护的理念,转变为主动式防护、主动式运维与监测,以推动网络“白环境”构建,实现网络安全主动防御。

### 2.1　黑名单与白名单机制的区别

传统的煤矿网络安全防护中主要采用的是黑名单机制,就是对照已有的应用程序、安全规则或已知的木马病毒样本进行监测拦截,禁止特定的 IP 地址、域名、MAC 地址、用户或应用程序等实体访问或操作网络资源,未被禁止的则完全允许访问或操作,黑名单机制需要不断更新黑名单规则库,以应对新的安全威胁,无法及时监测拦截未知威胁。

白名单机制与黑名单机制相对应,主要是指只允许指定的 IP 地址、端口、MAC 地址、用户或应用程序等被授权的实体访问或操作网络资源,而其他未被授权的实体则被禁止访问或操作。白名单与黑

名单机制相比，由于只有被授权的实体才能访问或操作网络资源，所以更加安全可靠，可以更加有效地防止网络攻击、恶意软件和其他安全威胁，提高网络的安全性和稳定性。

### 2.2 白名单理念

胜利能源在煤矿智能化建设过程中，以办公网、工控网、智能信息化系统作为防护对象，充分利用白名单网络安全技术，并将其转换为一种白名单理念，如图 2 所示。运用沙漏模型化繁为简，将白名单理念贯穿于技术、管理、培训、运维服务之中，实现由被动防护转变为主动防御。

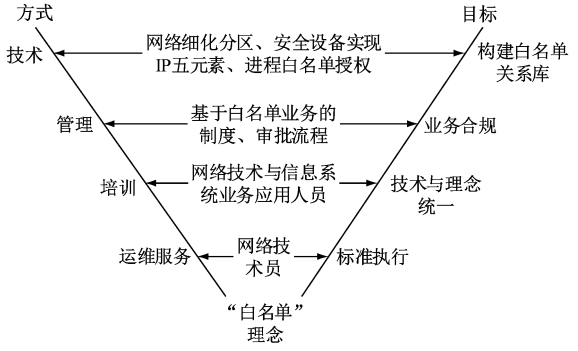


图 2 网络白名单理念沙漏模型

1）技术上，主要通过防火墙、网闸、安全态势感知、威胁情报、工控主机卫士等安全设备实现白名单理念。在做好网络细化分区基础防护的前提下，基于白名单明确业务访问关系和网络连通访问方向，以及可放行的 IP 五元素、进程等授权实体，从而将复杂的网络进一步梳理细化，构建自有的白名单关系库，以白名单独特的安全机制，有效解决零日漏洞、未知木马病毒等安全威胁，解决工控网内病毒库、安全设备规则库无法及时更新等问题，实现主动防御。结合态势感知异常流量监测技术，可开展异常流量溯源追踪分析，也可从攻击者的角度开展攻击路径分析，展示当前威胁攻击的所处阶段和攻击链，进而及时阻断，进一步提升主动防御能力。

2）管理上，企业要制定有关白名单网络安全制度，从制度上保障有组织机构和具备相关技术能力的人员，能够按业务审批流程开展相关服务，保障有资金来源，可购置并部署相关设备，开展相关业务。无论是管理制度制定还是资产上线管控、业务基线检测、策略部署、业务开通审批，全部基于白名单理念，实现依规审批，业务开通标准一致。

3）培训上，要实现网络白名单理念落地，构建网络“白环境”。要形成统一的网络安全意识，将白名单理念贯穿到网络安全培训过程中，尤其是对网络技术人员和信息系统业务应用人员，从白名单技术、管理制度、流程审批等方面定期开展培训，为更好地开展白名单业务奠定基础。

4）运维服务上，将网络白名单理念贯穿到运维服务中，使得运维服务更加安全、高效、标准，如通过堡垒机等统一的运维平台进行设备的访问操作，实现运维操作白名单化，非授权人员严禁登陆操作核心网络设备、安全设备及重要业务系统。要开展网络安全风险评估、网络安全攻防演练、网络渗透、网络漏洞检测等安全监测与应急响应服务，评估网络中白名单技术的网络安全隐患，并制定对应技术措施。

### 2.3 网络“白环境”架构设计

网络“白环境”设计需要从互联网侧、广域网侧、办公网侧和工控网侧分别考虑，做好 4 个区域的边界防护与内部动态实时监测、告警分析、攻击阻断。大型集团企业一般在互联网侧和广域网侧按统一的标准、要求、规划进行统一管控和防护。胜利能源作为子公司，其办公网和工控网侧的网络“白环境”架构如图 3 所示。

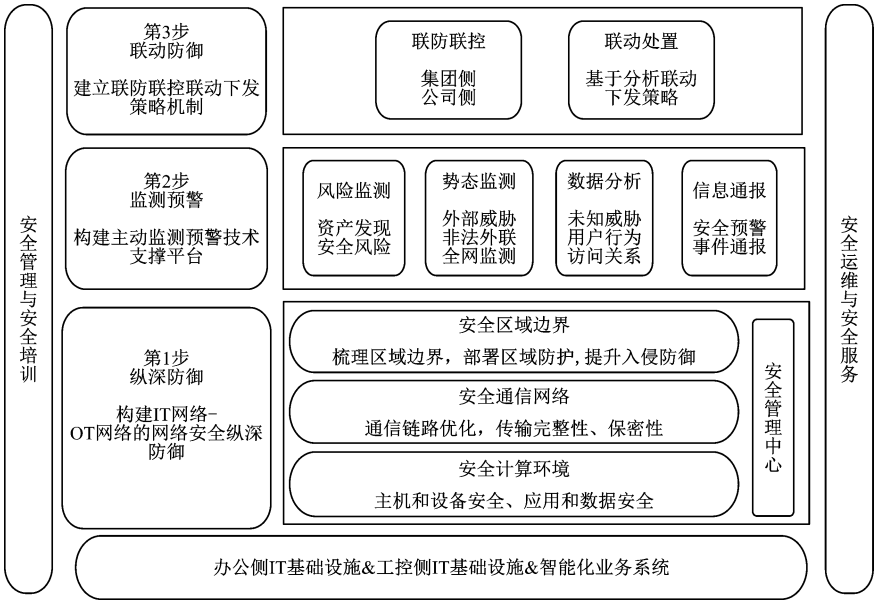


图 3 网络“白环境”架构

1) 以等保 2.0“一个中心、三重防护”的标准,进行公司顶层网络规划设计,部署网络集中管理平台、网闸、防火墙、工控主机卫士等基础安全防护设备。基于白名单梳理所有业务系统访问关系,建立业务系统行为基线,部署并优化白名单访问策略,实现安全管理中心统一管理,具备边界区域入侵防护能力,保障通信网络可靠,计算环境安全,实现从办公 IT 网络到工业 OT 网络的纵深防御。

2) 构建主动监测预警技术支撑平台,通过部署态势感知、流量探针、安全审计等新型安全监测设备,加强安全风险及安全势态监测能力;实现云-边协同监测,云端由集团统建,做好互联网侧和广域网侧监测。边端由煤矿自建,做好办公网、工控网监测,建立煤矿与集团公司的网络安全信息通报机制,提升网络主动监测预警能力。

3) 建立联防联控联动下发策略机制,通过主动监测平台的 AI 告警分析,包括未知威胁分析、用户行为分析、访问关系分析和异常流量分析等,分析攻击链路,追溯攻击源,由平台提供智能防护建议,自动/手动进行联动策略下发防护。

4) 在以白名单网络安全技术为主实现主动防御、监测告警分析及策略联动下发防护后,遵循网络白名单理念,配套开展网络安全管理、网络安全培训、网络安全运维和网络安全服务的建设,为网络“白环境”安全运营闭环管理提供支撑。

## 3　网络“白环境”安全运营

在煤矿智能化网络安全防护建设中,需要特别关注的是,网络“白环境”建设不是一个项目,而是一个不断循环、持续发展的过程。从技术、管理、培训、运维服务 4 个方面运用 PDCA 戴明环管理理论,对网络“白环境”安全运营进行管理,为企业发展变化持续提供可靠的网络安全防护。PDCA 戴明环管理理论如图 4 所示。

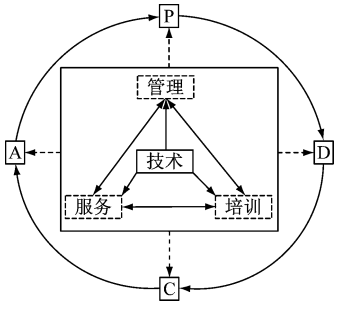


图 4　网络“白环境”PDCA 管理

1) 网络“白环境”的构建及后期的安全运营,需要将技术、管理、培训和运维服务有机融合,按照规划(Plan)、实施(Do)、检查(Check)、处置(Act)四个阶段闭环管理。如技术实施必须先按照网络“白环境”管理标准制定实施方案与实施计划,经审批通过后实施;执行过程中根据规划的控制点进行检查,发现策略部署不合理导致业务受影响时,要及时采取处理措施;实施后要开展培训,按统一的标准开展后续运维服务。

2) 管理、培训、运维服务之间虽然是相互独立的,但从网络“白环境”构建的角度看,三者也是相辅相成、相互补充的。网络“白环境”的构建要基于网络安全需求,部署支持白名单技术的安全设备,进而基于白名单开展网络业务关系梳理,部署并优化白名单策略。在企业内,需将白名单技术转换为白名单理念,使其贯穿于安全管理、安全培训和安全运维服务中,建立白名单业务体系,实现安全运营闭环管理。

## 4　结语

网络安全和信息化是相辅相成的,是信息化发展的基石。网络安全是煤矿智能化成功发展的保障与基础。以胜利能源为例,采用鱼骨图剖析了煤矿企业智能化发展过程中被动式防御的网络安全现状、问题及其原因,提出基于白名单构建一个“可信、可控、可管、可溯”的网络“白环境”。从技术、管理、培训、运维服务等方面,采用沙漏模型将白名单机制转变白名单理念,基于该理念,从办公网侧和工控网侧参照等保 2.0 的防护标准设计了网络“白环境”架构。最后分析了运用 PDCA 戴明环管理理论,对网络“白环境”安全运营进行管理,为企业发展持续做好网络安全防护。以白名单技术保障为基础、以管理运营为抓手、以监测预警为核心、以协同响应为目标设计的煤矿网络“白环境”实现了主动防御和网络安全数字化防护,但如何进一步实现网络安全全生命周期管理,开展网络与现实之间的映射关系及可视化展示,甚至开展“挂图作战”等,还有待进一步研究。

**参考文献:**

[1] 丁震,赵永峰,尤文顺,等. 国家能源集团煤矿智能化建设路径研究[J]. 中国煤炭,2020,46(10):35-39.

[2] 孟令强,关勇,张向红,等. 基于可信计算的应用程序白名单管理系统[J]. 计算机安全,2010(10):16-17,21.

[3] 汪锋,周大水. 白名单主动防御系统的设计与实现[J]. 计算机工程与设计,2011,32(7):2241-2244,2313.

[4] 章翔凌,王欢. 基于白名单技术构建主动防御体系[J]. 信息网络安全,2013(10):188-190.

(下转第 102 页)

行性。

**参考文献：**


[1] 闫凌，黄佳德. 矿用卡车无人驾驶系统研究[J]. 工矿自动化，2021，47(4)：19-29.

[2] GUO H，SHEN C，ZHANG H，et al. Simultaneous trajectory planning and tracking using a MPC method for cyber-physical systems：a case study of obstacle avoidance for an intelligent vehicle [J]. IEEE Transactions on Industrial Informatics，2018，14 (9)：4273-4283.

[3] LEE J，NAM Y Y，HONG S J. Random force based algorithm for local minima escape of potential filed method[C]. The 11th International Conference on Control Automation Robotics & Vision，Singapore，2010：827-832.

[4] 安林芳，陈涛，成艾国，等. 基于人工势场算法的智能车辆路径规划仿真[J]. 汽车工程，2017，39(12)：1451-1456.

[5] 修彩靖，陈慧. 基于改进人工势场法的无人驾驶车辆局部路径规划的研究[J]. 汽车工程，2013，35(9)：808-811.

[6] 唐志荣，冀杰，吴明阳，等. 基于改进人工势场法的车辆路径规划与跟踪[J]. 西南大学学报(自然科学版)，2018，40(6)：174-182.

[7] AKBRIPOUR H，MASEHIAN E. Semi-lazy probabilistic road-map：a parameter-tuned，resilient and robust path planning method for manipulator robots [J]. International Journal of Advanced Manufacturing Technology，2016，89(5-8)：1-30.

[8] TAHERI E，FERDOWSI M H，DANESH M. Fuzzy greedy RRT path planning algorithm in a complex configuration space [J]. International Journal of Control，Automation and Systems，2018，16 (6)：3026-3035.

[9] 宋晓琳，周南，黄正瑜，等. 改进 RRT 在汽车避障局部路径规划中的应用[J]. 湖南大学学报(自然科学版)，2017，44(4)：30-37.

[10] 杜明博，梅涛，陈佳佳，等. 复杂环境下基于 RRT 的智能车辆运动规划算法[J]. 机器人，2015，37(4)：443-450.

[11] 李梓欣，李军. 自动驾驶汽车路径规划算法研究[J]. 汽车工程师，2021，292(8)：11-14.

[12] 辛煜，梁华为，杜名博，等. 一种可搜索无限个邻域的改进 A* 算法[J]. 机器人，2014，36(5)：627-633.

[13] 齐尧，徐友春，李华，等. 一种基于改进混合 A* 的智能车路径规划算法[J]. 军事交通学院学报，2018，20(8)：85-90.

[14] 梁昭阳，蓝茂俊，陈正铭. A* 算法在 Shortest-Path 方面的优化研究[J]. 计算机系统应用，2018，27(7)：255-259.

[15] 赵鑫，胡广地. 平滑 ARA* 算法在智能车辆路径规划的应用[J]. 机械科学与技术，2017，36(8)：1272-1275.


(上接第 35 页)


[5] 石波，王红艳，郭旭东. 基于业务白名单的异常违规行为监测研究[J]. 信息网络安全，2015(9)：144-148.

[6] 尚文利，安攀峰，万明，等. 工业控制系统入侵检测技术的研究及发展综述[J]. 计算机应用研究，2017，34(2)：328-333，342.

[7] 胡海生. 一种基于白名单机制的电力监控主机恶意代码防御方案[J]. 计算机应用与软件，2017，34(9)：114-119.

[8] 陈万志，李东哲. 结合白名单过滤和神经网络的工业控制网络入侵检测方法[J]. 计算机应用，2018，38(2)：363-369.

[9] 严彪，尹丽波，应欢，等. 基于白名单机制的工控分级入侵检测算法[J]. 通信技术，2018，51(4)：907-912.

[10] 赵威，李光昱，安锐. 白环境管理在企业安全运维中的应用[J]. 电力信息与通信技术，2015，13(8)：115-118.

[11] 付宏涛，刘爱军. 基于业务白名单技术在视频监控网的设计与实现[J]. 信息系统工程，2019(4)：74-75.

[12] 黄长慧，胡光俊，李海威. 基于 URL 智能白名单的 Web 应用未知威胁阻断技术研究[J]. 信息网络安全，2021，21(3)：1-6.

[13] 李鹤，唐清弟，刘剑明. 基于“白名单”技术的主机防病毒研究与设计[J]. 水电站设计，2022，38(1)：69-71.

[14] 杭成宝，孙那斌，孙建荣. 基于平行理论的智能化煤矿平行安全非技术问题研究[J]. 煤矿安全，2022，53(2)：241-245.

[15] 张涛. 电网信息安全有四大核心问题[J]. 国家电网，2016(2)：25-26.