基于业务与安全融合的智慧煤矿主动防御技术与实践*

王许培，王伟刚
（国家能源投资集团信息公司网络与信息安全中心，北京 100011）

摘　要：针对当前智慧煤矿多系统高集成、低耦合等问题，充分运用“云大物智移”等新型信息技术，以“安全融入业务”的网络安全建设思路，满足实际生产和管理中的网络安全建设需求。在“一个中心，三重防护”的基础上，以“四网”融合的网络布局，采用网络安全纵深防御和网络欺骗技术实现主动式防御，多维手段联防联控，构建融合智慧煤矿 IT、OT、IIoT 及安全监控系统的多维协同纵深防护安全体系。以场景化、协同化的安全防护能力，让网络安全、数据安全、业务安全的防护形成合力，更大化保障煤炭企业的安全生产和运营管理。研究成果和体系规范在一些重保活动中得到实践应用，效果良好。

关键词：智慧煤矿；业务安全；主动防御；数据安全
中图分类号：TP393　　文献标识码：A　　DOI：10.19358/j.issn.2097-1788.2022.06.003
引用格式：王许培，王伟刚. 基于业务与安全融合的智慧煤矿主动防御技术与实践[J].网络安全与数据治理，2022，41(6)：17-24，33.

Active defense technology and practice of smart coal mine based on business and security integration

Wang Xupei, Wang Weigang
(Network and Information Security Center, CHNENERGY Investment Group Co., Ltd., Beijing 100011, China)

Abstract: Aiming at the problems of high integration and low coupling of multiple systems in smart coal mines, new information technologies such as “cloud computing, big data, IoT, mobile Internet, AI” are fully used to meet the needs of network security construction in actual production and management with the idea of “integrating security with business”. On the basis of “one center, three layers of protection”, with the network layout of “four networks” integration, the network security defense in depth and network fraud technologies are used to achieve active defense. Multi-dimensional means of joint prevention and control are used to build a multi-dimensional collaborative deep protection safety system integrating intelligent coal mine IT, OT, IIoT and security monitoring system. With scenario-based and collaborative security protection capabilities, the protections of network security, data security and business security form a resultant force to great ensure the safety production and operation management of coal enterprises. The research results and system specifications have been applied in some major project security activities with good results.

Key words: smart coal mine; business security; active defense; data security

0 引言

2020 年国家发改委、国家能源等 8 部委联合印发《关于加快煤矿智能化发展的指导意见》[1]（以下简称《意见》），明确提出要加快对网络安全技术与煤矿生产业务深入融合的关键性技术研究。为深入贯彻执行《意见》，国投集团信息中心基于煤矿生产业务与网络安全、数据安全深度融合，从当前煤矿行业以安全合规建设、单点防护为主导的传统安全向基于“三化六防”策略的主动防御转变，开展煤矿网络安全的主动防御技术的实践研究与应用，构建煤矿基础资源数据化、安全业务体系化、智能对抗引擎化和安全决策智慧化的主动防御体系，全面提升煤矿主动防御能力，对行业的安全建设、运营等有一定的参考借鉴价值。

* 基金项目：国家能源集团信息化项目“煤炭企业工业控制系统网络安全防护规范”（T20042G2001F）

1 智慧煤矿网络安全建设难点分析

智慧煤矿物联网感知设备异构多样且动态变化，尤其是“云大物智移”技术与环境感知、视频监控、定位导航、广播调度等应用系统深度融合，彻底改变传统的安全管控模式，加剧了感知设备的恶意接入、攻击渗透、数据泄密等风险，数据安全和网络安全融合的安全服务成为煤矿业务安全的重要保障。

智能系统低耦合增加安全处置协同的难度。智能系统“积木式堆叠”[2]，造成海量“数据烟囱”“采而无用”问题，增加了井下、井上生产作业过程真正智能化协同和安全处置联动的难度。

智慧煤矿行业安全规范有待提高。智能系统堆砌式集成，行业并未形成整体成套的技术供给能力，导致针对煤矿的网络安全规划与建设难以形成行业的可执行标准与规范。

2 业务与安全融合的主动防御关键技术分析

智慧煤矿业务高度流程化，稍有干扰就会影响业务的连续性，同时针对能源行业的攻击呈上升态势，一定程度上加剧了目前仍以合规建设为主导的煤矿网络攻击风险。智慧煤矿的网络安全主动防御建设必须在等级保护建设的基础上，围绕“一个中心，三重防护”，结合煤矿“四网融合”的应用场景，以威胁感知为核心，以威胁数据为驱动，融合包含边界隔离、访问控制、入侵监测、安全审计等防护手段，引入诱捕、SOAR、UEBA、XDR 等主动防护技术，聚合安全数据，整体规划协同防护建设策略，构建多维协同的纵深防护安全体系。以场景化、协同化的安全防护能力，让网络安全防护形成合力，以“三化六防”思维保障煤炭企业的安全生产和运营管理。

2.1 基于业务与安全融合的安全防护技术

智慧煤矿的核心是实现安全信息主动化感知、生产系统智能化管理、数据信息高效化处理、调度决策智能化控制等，与之相适应的网络安全建设也必须与业务耦合，对网络资源异常行为准确及时预警和应急响应，保障应用系统的安全稳定运行提供安全支撑。

智慧煤矿分为井上办公网、煤矿工业环网、井下生产控制网、安全环境监测环网及 5G 基站内网等。尤其是井下监测系统、生产控制系统拓扑结构复杂多变，网络噪声信号突出，同时井上监控智能系统频繁与井下控制网络传输程序或调整工艺参数、收集控制网络的业务运行数据，导致井上 IT 系统的威胁很容易渗透到井下控制系统，增加了井下 OT系统的安全风险。另外，井下 OT 系统很容易被内置一些隐蔽威胁，在外部恶意引擎触发后会快速演变且难以捕捉，而针对 PLC、RTU 等一些恶意软件也会采用命令与控制信号更加隐蔽地潜入 OT 系统，对控制器进行间隙式指令干扰而引起系统不稳定、智能化业务的工作流程中断而导致煤矿事故发生，因此如何实时、精准感知井下 OT 系统的异常行为是智慧煤矿安全建设的重点。从智慧煤矿的内生需求出发，基于 PPDAR(策略、防护、检测、分析、响应)安全防护模型，从“设备安全、控制安全、网络安全、应用安全和数据安全”五大角度，构建煤矿纵深安全防御体系、形成《工业控制系统信息安全防护能力成熟度模型》的“综合协同能力”是关键。

具体举措有：(1)对多源告警数据基于大数据 AI 分析与融合、基于规则的快速检测、全资产动态管控、事件化分析和处置等技术手段，从根因分析、关联分析、事件化分析等维度准确监测网络攻击活动，提高威胁检测和响应速度和精确度，提升整体网络安全防护能力；(2)以基于 SOAR 技术的自动化操作快速应对各类繁琐枯燥的安全任务；(3)基于大数据 AI 的多源异常行为分析精准预警，并多设备策略联防联控；(4)基于工单闭环机制的快速应急处置等。

针对井下 OT 系统的网络安全与业务融合最为关键的任务是利用多维感知技术和大数据 AI 融合技术侦探 OT 系统过程状态中的可疑攻击活动，尤其是针对控制工业协议的恶意渐进式数据载荷增量、工控协议的挟持篡改、通信过程中的数据投毒等[3-4]。实际上，井下 OT 生产控制网内的控制流程是周期性的、且相互之间的通信链接是相对固定的，OT 系统内的任何扰动均会体现在控制内网流量的异常波动、控制器端口流量的异常变化、设备之间的访问关系异常、设备 CPU、内存等占有率的异常变化、控制系统输出的偶发波动等。因此，针对 OT 系统的可疑攻击活动的网络监测可以采用基于协议载荷 DPI、基于流量 DFI 的实时监测，并结合基于业务过程的工控可疑活动侦探综合分析与预判。针对业务过程的监测有基于控制逻辑监测和基于过程状态监测，其中基于控制逻辑监测的任务是实时感知任务调度的时间序列和控制程序的异常，基

于过程状态侦探的任务是实时分析流程变量的残差和临界状态。基于网络安全与业务安全融合的关键任务就是如何利用大数据 AI 分析技术关联网络监测与业务过程监测的异常行为、预判攻击行为并精准预警、调度应急策略、阻止攻击行为等。

在业务与网络安全融合的过程中，最为重要的是需要精准辨识网络攻击与业务偶发故障等，并根据辨识结果启动相应的应急处置程序，否则就会发生误动作而导致不可挽回的损失。网络攻击不同阶段的网络异常行为导致业务异常的程度存在一定的差异，在网络侦察的初始阶段，对业务影响是较小的，而在初步入侵、C&C(命令与控制)阶段，对业务便开始有显性影响，因此，为防止网络攻击势态的进一步蔓延，就必须在网络攻击的最初始阶段就能精准感知并实时预警、启动应急流程。基于此，网络安全感知系统必须与自动化设备状态综合监测实时交互状态数据，以此弥补网络安全感知数据稀疏难以实时辨识安全威胁的问题，增强实时感知、辨识可疑活动的颗粒度和精准度。井上指挥系统可以根据感知的可疑活动出现时所依赖的网络环境要素、基于时序的控制输入/输出等偏移控制基线的排列熵累积，利用 OT 系统从正常状态到异常状态的临界点作为特征参考，实时评估网络攻击、设备偶发故障等征兆，进行实时预警与启动相应的应急措施，辨识流程如图 1 所示。

2.2 攻击诱捕验证技术

井下 OT 系统采用工业物联网架构，使用大量网络化传感设备，通过诸如 5G 等无线通信技术形成各自的传感器网络，相关信号一旦被恶意干扰，有可能造成诸如采掘业务、安监业务、调度业务等干扰，甚至业务中断等故障，或者恶意窃取、篡改远程控制信号以控制井下的生产、监控装置而引发煤矿事故。由于井下生产作业环境的特殊性，保障控制信号在井上、井下传输过程中的完整性、可用性、连续性成为智慧煤矿安全生产保障的关键。有效的防护措施是在井上调度中心区旁路部署基于 DPI、DFI 的工控协议安全审计设备，对流经生产综合监控系统的网络流量进行审计，并对上位机与下位机之间的工业协议识别和深度解析，对违规操作、误操作以及关键操作(如下载、上传、组态变更以及 CPU 启

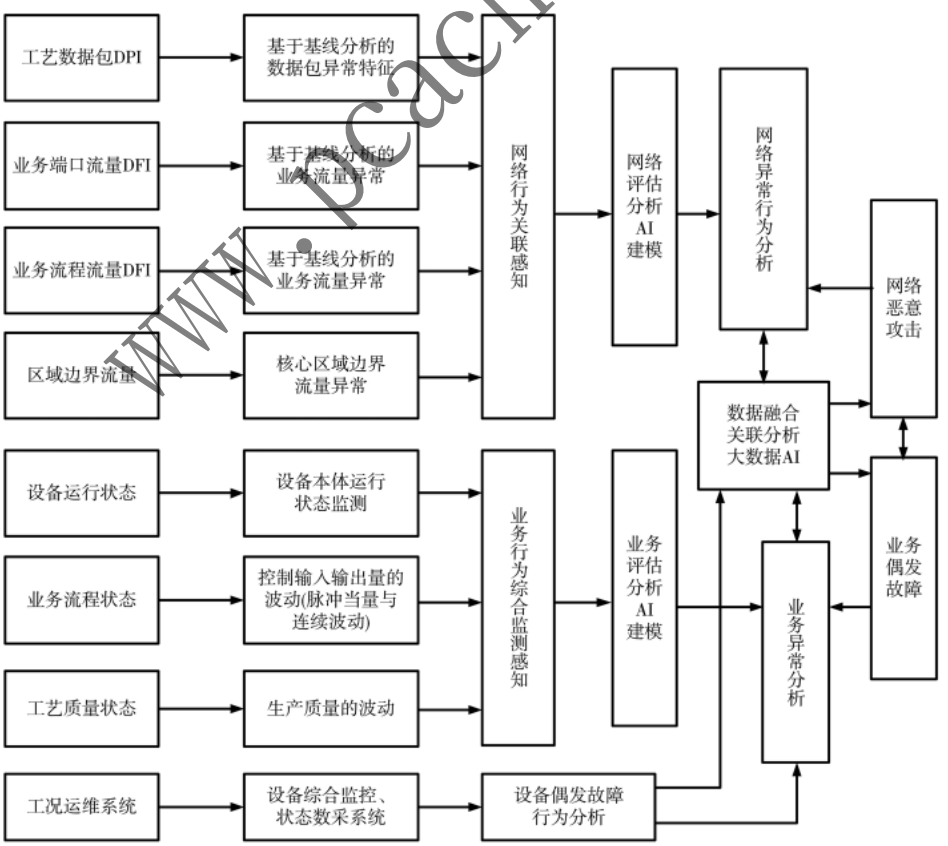

图 1 基于业务与网络安全融合的智能流程图

停)等进行监测,实时了解生产网络的安全状态,为事后追溯、定位提供证据。为进一步防范井上网络威胁对井下系统的渗透、弥补基于特征的安全手段难以防范 0Day 对井下系统的攻击,通过在井下工控系统的关键位置部署入侵诱捕装置,并接受井上指挥中心的策略分发系统的指令动态调整诱骗策略以诱捕攻击者,以深度交互的方式获取详细的攻击步骤,为联控与溯源提供决策。考虑到井下生产系统诱捕系统实施部署的难度及不同区域保护的需求差异性,同时兼顾蜜罐伪装性和防御安全性,在井上运营系统入口处部署中高交互性蜜罐而在井下生产系统入口处部署中高交互性工控蜜罐,且井上与井下的蜜罐装置协同,情报共享,在纵深防御上协同捕获隐蔽攻击行为,一定程度上提升了井上、井下系统的安全协同防御能力,也保障了生产系统的安全生产。诱捕策略与蜜罐部署如图 2 所示。

为进一步提升井下工控蜜罐的诱捕能力,其必须高度仿真井下实际生产控制系统,具体设计为:在其 OS 内核载入数采系统的网卡、磁盘、固态驱动器、I/O 控制、数采程序等多个虚拟功能,并利用动态欺骗策略诱导恶意程序进入蜜罐陷阱。为进一步发挥蜜罐的情报作用,提升多安全设备协同能力,具体设计为井上蜜罐与入口的 IPS、流量审计协同,井下蜜罐与不同作业系统的边界防护控制、区域流量分析审计等协同,井上、井下蜜罐与指挥中心策略分发系统、情报中心形成策略联动和协同,生产不同策略的诱饵分阶段步骤诱捕攻击者,形成多维度的纵深、横向的安全防护能力,保障生产系统安全稳定运行。

2.3 实战化的网络攻击联动防御技术

基于实战化的网络攻击防御联控是在安全技术、调度流程、指挥平台协同的基础上,通过网络与业务异常行为监测协同的智能分析、载荷编排SOAR、定向防御三大引擎协同达到动态智能防御的目的,实现对网络安全态势的精准感知、安全威胁的智能分析、预警信息的自动分发、响应措施的联动处置,构建集“威胁检测、实时防护、动态响应、态势预测、应急指挥”为一体的智能网络安全主动防御体系。

面向实战化的联防战术中,首要任务是在全域重点系统风险评估的基础上,与自动化设备维护系统实施对接自控设备偶发故障的监测信息,构建与部署以策略联动机制为核心的整体网络安全防护策略与设施,以提升攻击监测和防护的效率为目的,动态优化“边界防护策略联控、蜜罐诱饵策略调度、流量监测颗粒度动态调优、威胁情报动态分发”等整体防控策略,基于实战化的主动防御策略动态调优过程如图 3 所示。三个关键步骤:(1)优化日志分析,采用事件分析法、时间分析法以及流量包样本分析法等方式,在大量异构数据中捕获关键信息、感知异常行为、关注重点事件;(2)及时处置设备误报、拉通业务侧沟通渠道,核实能否快速对业务代码逻辑进行修改,解决业务误拦问题;(3)优化平台

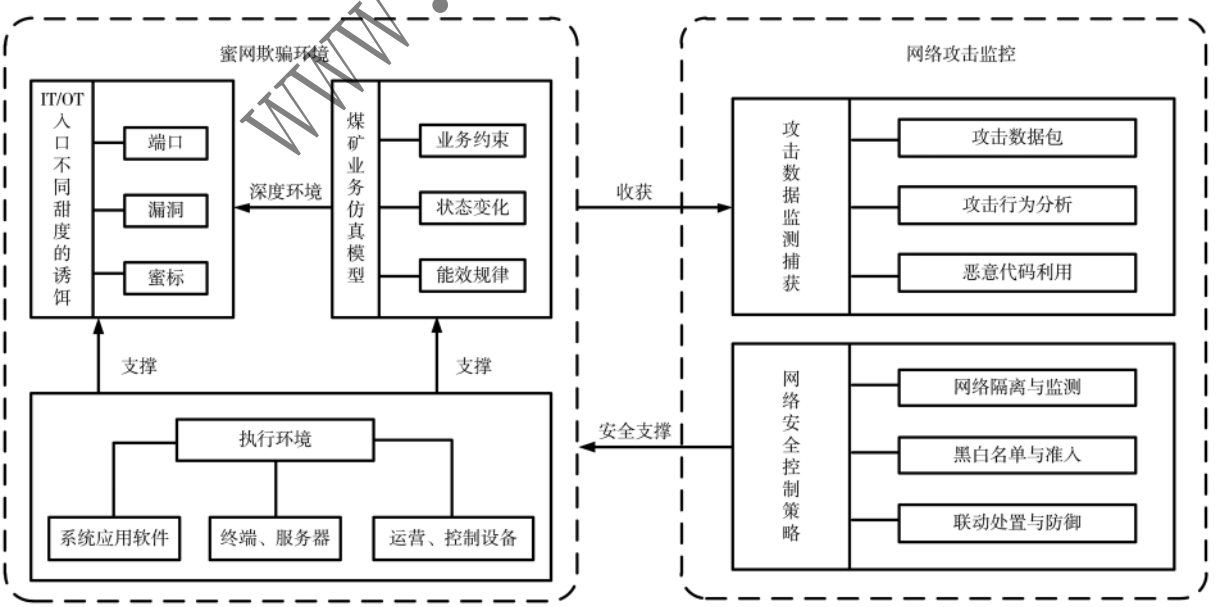

图 2 诱捕策略与蜜罐部署

和设备策略，根据日志分析及误报处理的结果，对网络设备策略、安全设备策略、主机策略等进行进一步调整和优化。

在针对智慧煤矿的主动防御设计时，注重设备联动、情报共享、策略分发、分层控制与动态调优等，系统性的关键防护策略如下：

(1)第 1 道防线：在核心安全域部署基于 AI 的防火墙，并与蜜罐、情报中心联控，实时动态调整封堵策略，最大限度收敛资产暴露面、最小化网络访问控制。

(2)第 2 道防线：在基于业务安全保障的分域分区的基础上，部署 WAF、IDS、工业防火墙等，与井上指挥中心联动进行动态策略调优，提升边界动态的防护能力、监测和防护南北向流量。

(3)第 3 道防线：在区域核心汇聚处部署全流量分析设备进行攻击行为监测，提升内网和重点系统的安全防护能力，监测东西向流量。

(4)第 4 道防线：针对核心区域的防护，与井上指挥中心策略分发系统联控，通过旁路阻断实现一键封堵功能，提升快速应急响应处置能力，支撑集中化处置。

(5)第 5 道防线：井上、井下、数据中心出入口部署策略蜜网，与情报中心、策略分发系统联动，提供威胁动态感知、攻击诱捕、行为分析和溯源取证能力，精准定位攻击源头，提升核心系统免受攻击的能力。

(6)第 6 道防线：通过对流量、告警、日志等元数据利用大数据 AI 分析能力和机器学习算法，进行集中化、范式化分析，结合攻击链模型从海量告警事件中快速定位，重点关注和处理核心资产安全状态、重要安全事件，提升井上智能安全联防指挥中心的综合预警、智能决策、快速联控、精准调度等能力。

3 智慧煤矿数据分类分级及其安全防护技术

针对智慧煤矿的数据安全防护，不仅需要实施分级管控、加强对重要和核心数据的流转范围及其风险的管控，更需要针对生产控制数据的完整性、实时性和有效性等进行重点保护，因为攻击者可通过多种方式对诸如开/闭控制器、读/写寄存器、上传/下载控制程序等操作命令注入恶意数据，甚至篡改环境温度、压力等传感器数据，以此破坏包括控制命令、载荷数据等在内的数据完整性，干扰工控系统的业务连续流程，造成系统性干扰与控制扰动。因此，针对智慧煤矿数据安全而言，运行数据、

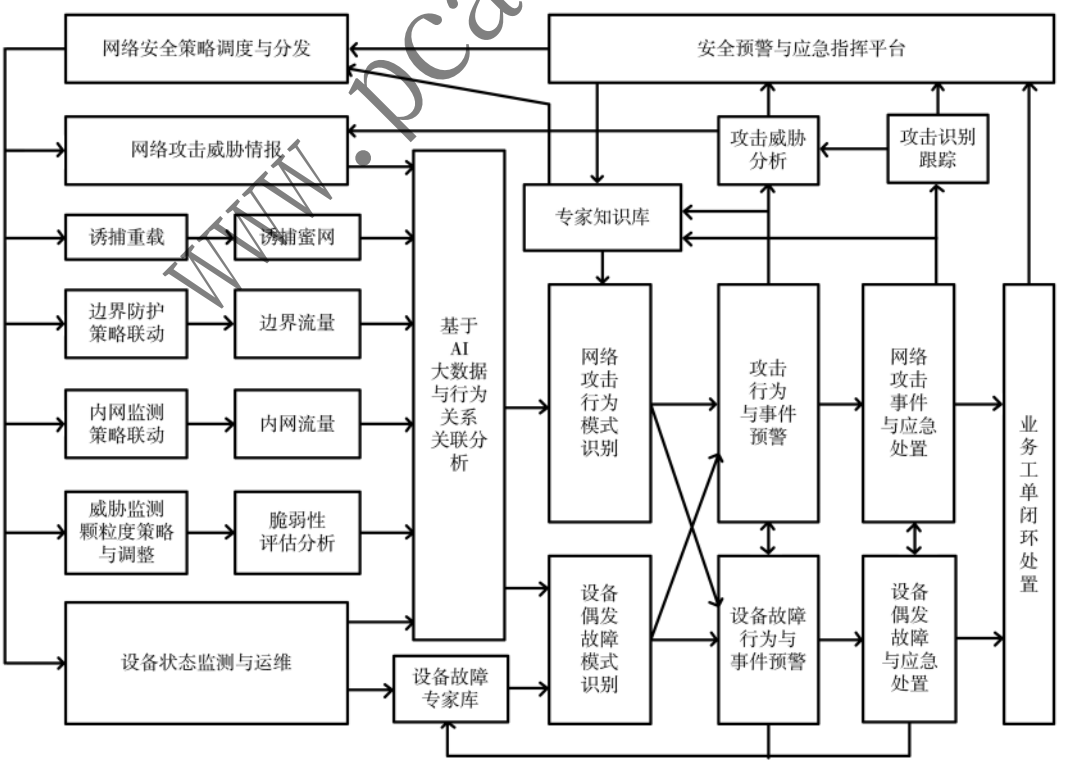

图 3 基于实战化的主动网络安全防御策略动态调优过程

控制数据、生产数据等保护成为关键。但当前智慧煤矿的相关系统高集成、弱耦合等现实缺点导致数据要素产生源头极其分散、采集环境恶劣、流转途径多样、业务场景复杂、处理环节非规范化等,且各自系统的数据在实时性、时序性、稳定性、连续性、结构化等方面存在较大差异,给数据分类分级、安全防护与治理等带来极大的困境。

3.1 数据分类

智慧煤矿的生产数据主要指生产控制过程产生的数据:包括采、掘、机、运、通、穿、爆等各种生产系统监测数据、运行的实时数据;安全数据分为安全监测及安全管理两类,其中安全监测是指井下的瓦斯、顶板、水文、火灾以及设备的运行情况等实时监测数据;安全管理是指企业的“双重”预防管理、安全生产管理、应急救援管理等类型的管理数据。针对煤矿的数据分类,结合智慧煤矿的生产系统、系统集成、运营管理等属性考虑,参考《信息安全技术 网络数据分类分级要求》等规范,按照“组织经营”维度进行分类,将生产数据分为用户数据(内部员工、协作单位人员、第三方监管人员、第三方运维人员以及客户、供应商等)、业务数据(采掘、运输、机电、安监、调度等)、经营管理数据(系统设备资产信息、客户与产品信息、产品供应链数据、业务统计数据等)、系统运行(控制信息、工况状态、工艺参数、系统日志等)、安全数据(安全设备、安全配置策略、网络拓扑、基线管理、安全接口数据等)、业务流程数据(流程与控制工艺、控制程序等)、监管数据(与上级监管部门、其他主体共享的数据等)、研发数据(研发设计数据、开发测试数据等)、运维数据(物流数据、产品售后服务数据等)等。

3.2 数据分级

依据煤矿数据遭篡改、破坏、泄露或非法利用后对煤矿生产经营和上级部门监管监察产生的影响制定数据分级定级规范,包括分级原则、分级依据、定级要素、定级方法等内容。结合智慧煤矿数据“流转、共享、安全”等方面均衡考虑,根据“影响范围、持续时间、可恢复性、数据敏感度”等维度,从数据泄露、数据篡改以及数据不可用等层面评估分析数据流转各要素的安全威胁,将慧煤矿数据划分为一般、重要与核心三个级别。针对不同级别的数据采用适度的安全措施,在数据流转等过程通过最小共享和泛化、共享(提取)自动化审批、最小使用范围、责任传递、定期稽核等方式保障其安全性[5]。在煤矿数据生命周期管理过程中,针对重要数据、核心数据、经过综合分析后提炼出的二次数据、一般数据经过二次组合或通过数据聚合分析形成更有价值的衍生敏感数据等,需要根据数据的适用范围、责权以及风险等,有针对性进行动态分级修正。煤矿的数据分类分级建设如图 4 所示。

3.3 数据防护

参考《工业与信息化领域数据安全管理办法》《信息安全技术 数据安全能力成熟度模型》等规范,针对煤矿数据全流程:数据采集安全、传输安全、存储安全、处理安全、交换安全、销毁安全等,首先需要确定全域的数据安全管理的组织架构及职责,保障数据的完整性、保密性、安全性和合规使用。其次需要对采集、传输、存储、交换的数据安全过程,从组织建设、制度流程、技术工具、人员能力等方面对数据安全进行规范操作,如:(1)在数据采集、流转、使用、存储、提炼等过程中,遵循权限最小环原则;(2)运用商密进行轻量级加密,以期降低

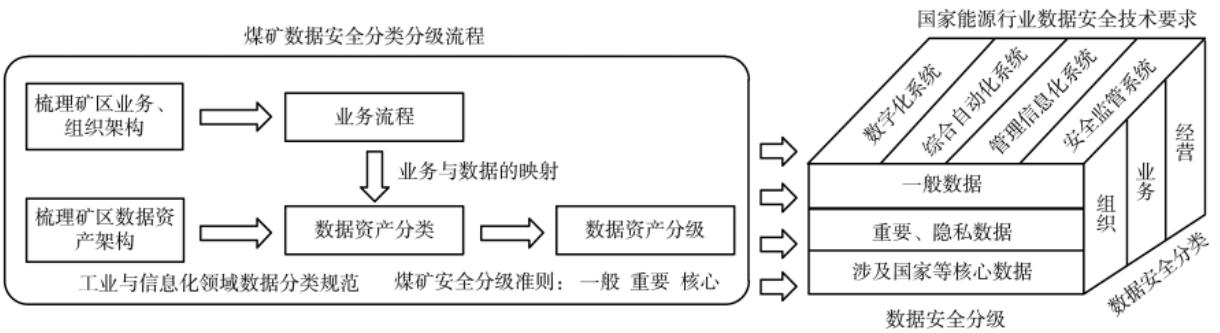

图 4 智慧煤矿的数据分类分级建设

加解密过程对数据实时性的影响；(3)监测重要、核心、二次、衍生等数据的分布及其流转过程中的泄密风险；(4)采用数据资产采集探针、网络流量分析、数据库审计等手段，融合数据资产识别引擎、数据及文件内容识别引擎、分类分级引擎、敏感数据分布引擎、威胁分析引擎等微服务搭建数据安全一体化监控平台，以“数据资产梳理、违规泄露发现、数据流转监测、数据安全审计”为核心，为煤矿提供一体化的数据安全监测、预警、应急与防御等服务；(5)通过风险处置及工单功能，实现从数据资产监测、风险识别、统一管控、事件响应和工单处理记录的数据安全运营能力。数据安全与治理过程如图 5 所示。

4 业务与安全融合的主动防御技术应用与实践

基于业务与安全融合的一体化运营能力建设以安全治理为核心、风险管控为导向、安全合规为基础，结合组织安全能力，满足安全运营的系统性、动态性和实战性需求，在人、技术、过程层面构建一体化的网络安全纵深防御、监测预警和应急处置体系。

首先，建立矿区级一体化的基于大数据 AI 分析监测平台和智能指挥中心，实现对矿区所有联网矿场的资产状态与安全状态监控、全域安全信息收集、配置与策略统一管理，并与威胁情报融合，提高矿区安全识别、安全处置、安全调度、安全上报等预警及处理、保障能力。针对行业监管数据，如安全监测监控、微震监测、水文监测、冲击地压监测、视频监测等，建设矿区统一数据池，通过 VPN、身份认证和数据加密技术统一上传出口，防止因数据上传出现非法外联、数据篡改、非法控制等安全隐患。

其次，根据《关键信息基础设施安全保护条例》的相关规定，参考《工业控制系统安全防护能力成熟度模型》的要求，结合煤矿业务安全的实际需求，将煤矿的网络安全防御能力建设确定为“四级：综合协同级”：统筹考虑安全风险需求，建立多级协同的安全管理体系，并通过态势感知、统一管控等技术手段实现综合决策、协调防护的安全能力，实现煤矿的纵深防御。“综合协同级防护能力”建设过程不仅需要实时精准发现网络中的网络攻击，更要深挖通过供应链或网络摆渡攻击潜入煤矿内网，针对特定目标实施非传统攻击手段的安全威胁综合分析和识别；同时建立以情报驱动为核心，协同“研判分析、溯源反制、应急响应、运营支持”安全防护能力，实现“一点发现，全面风险闭环”的联防联控机制，构建“云网边端”一体化安全保障体系，并结合网络攻防演练工作发现的问题及时纠正相关的措施与策略。

再次，在智慧煤矿的整体安全联防联控的过程

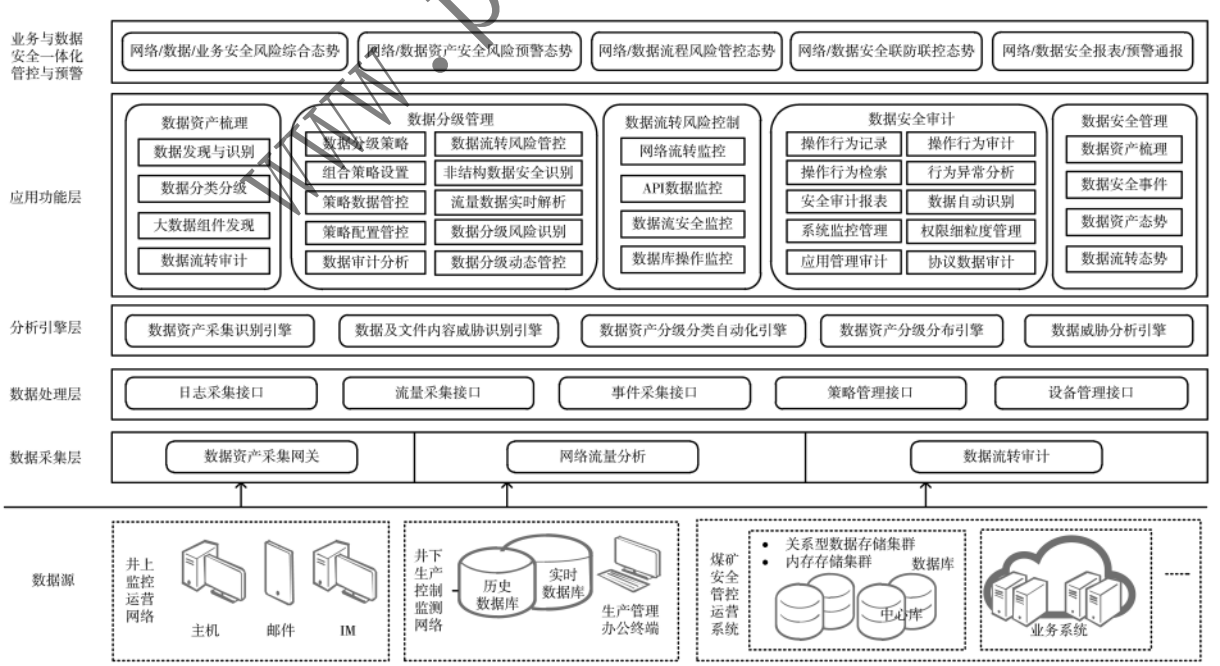

图 5 煤矿数据安全与治理过程

中,利用攻击链模型,逐层收敛告警信息,并以可视化的作战网格挂图进行预警与管控,提升攻击事件的监测准确率和网络安全日常运营工作效率,为面向实战化的网络安全保障提供有效监测处置手段。基于实战化策略构建网络安全纵深防御体系,提升防御的层数和智能封堵能力,以此增加攻击者的攻击难度,确保应用系统和数据资产安全。在全域网络行为感知基础上,重点增强对井下系统的设备接入网行为、网络访问行为、井上与井下访问、井下系统间的网络数据交换行为等感知与分析;加强对监控网络、生产网络、井下环网的非法外联、存储介质内外网交叉使用等行为感知与预警。针对井下生产控制系统的智能联动阻断、端口智能封堵等必须特别谨慎,必要时需要网络、安全与自动化控制的专家组人工参与研判,以防误判而引起的安全事故。智慧煤矿网络安全策略与实施部署如图 6 所示。

5 结论

通过对煤矿业务与网络安全技术深度融合的主动防御技术研究与实践应用,形成国投集团《煤炭企业工业控制系统网络安全建设规范》企标,并在国投集团"煤炭企业工业控制系统网络安全防护规范"信息化项目中应用实践,得到了有效验证,在诸如"重保"期间发挥了极大的作用。依赖平台系统强大的大数据 AI 分析能力、精准的预警能力、与安全设备之间的策略联动能力等,以及基于边界的智能化封堵联动、出入口蜜罐的诱捕作用、端口动态智能化封控及工单的快速闭环控制等,提高了矿区网络安全协同的工作效率、降低了网络安全管理与人员投入的成本、提高了安全人员整体的协同能力、完善了实战化的网络保障,实现了"工作流程化、过程可视化、工单电子化"等要求,确保智慧煤矿网络安全"零"事故,保证了煤矿的业务运营稳定运行。

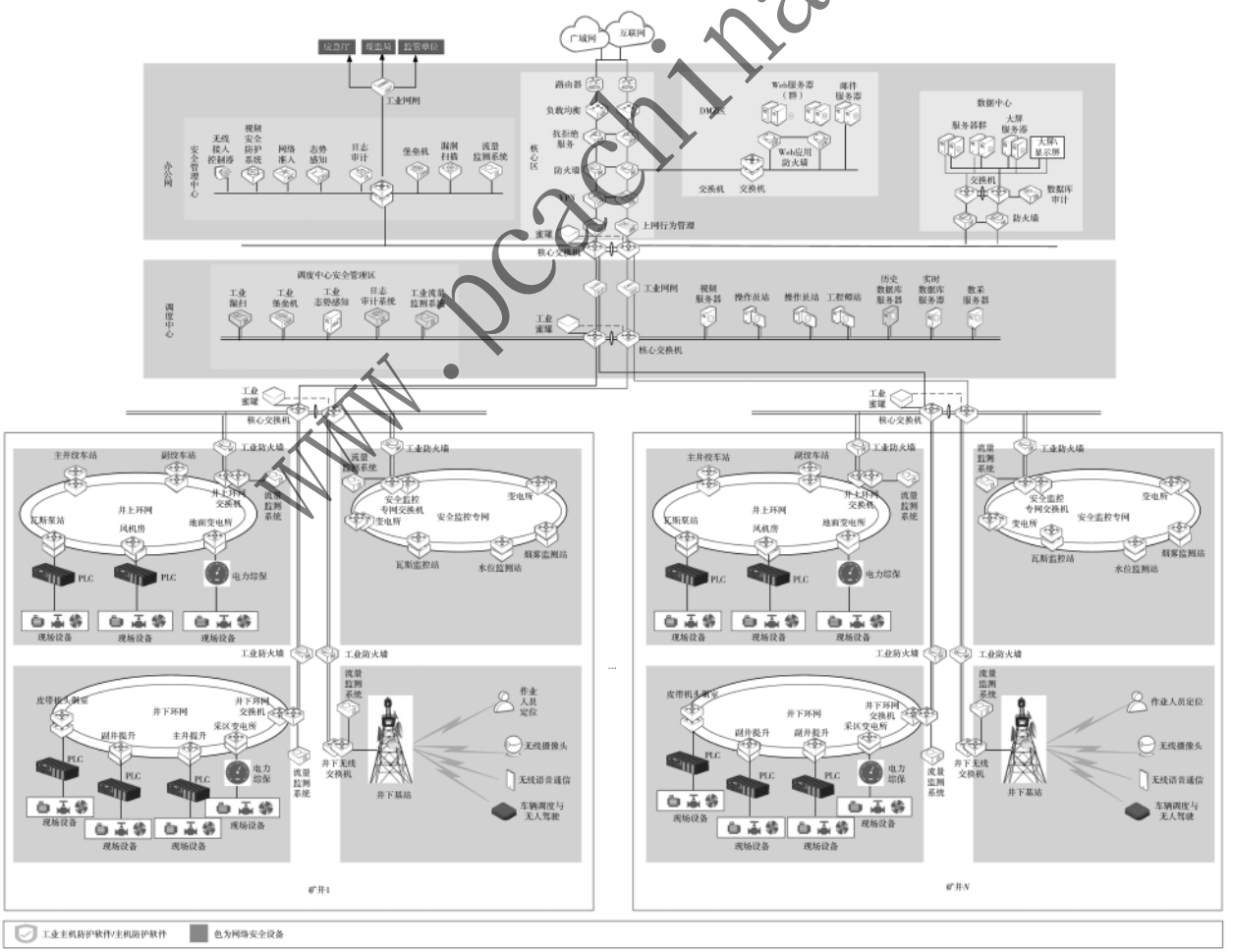

图 6 智慧煤矿的主动防御流程

(下转第 33 页)

(2016 年 4 月 19 日)[EB/OL].[2022-09-09].http://www.gov.cn/xinwen/2016-04/25/content_5067705.htm.
[7] 梁晴.绿盟科技战略解决方案系列介绍——金融行业供应链安全解决方案[Z/OL].[2022-09-09].https://mp.weixin.qq.com/s/Ms-3kxqQqEnFST6slGdlZA.
[8] 郭启全.认真落实网络安全等级保护制度,构建新时代国家网络安全综合防控体系[Z/OL].[2022-09-09].https://mp.weixin.qq.com/s?__biz=MzU1O-DM1Njc1Ng.
[9] 盘善海,裴华.高安全等级网络安全防护体系研究与设计[J].通信技术,2021,54(7):1715-1720.
[10] 魏昊.强化供应链安全保障工作,保护关键信息基础设施安全[EB/OL].[2022-09-09].http://www.cac.gov.cn/2021-08/31/c_1632032388356198.htm.

(收稿日期:2022-09-09)

作者简介:

庞彬彬(1985-),男,本科,高级安全顾问,主要研究方向:关键信息基础设施安全、云安全、数据安全。

(上接第 16 页)

研究[J].青岛大学学报(自然科学版),2015,28(4):72-76.
[12] 胡腾,郭曦鹏.机床空间误差完备建模方法与 NC 代码优化补偿技术[J].工程科学与技术,2019,51(6):190-199.
[13] 潘鋆,韩京辰,于丹,等.基于形式化模型的 NC 代码异常检测[J].微电子学与计算机,2021,38(11):81-87.
[14] 潘忠英.朴素贝叶斯中文文本分类器的设计与实现[J].电脑编程技巧与维护,2021(2):37-39.
[15] 国家标准化管理委员会.GB/T 25070-2019.信息安全技术 网络安全等级保护安全设计技术要求[S].2019-05-10.
[16] 国家标准化管理委员会.GA/T 1177-2014.信息安全技术 第二代防火墙安全技术要求[S].2014-07-24.

(收稿日期:2022-10-08)

作者简介:

王晓鹏(1979-),男,硕士研究生,高级工程师,主要研究方向:工业互联网安全、物联网安全、边缘计算安全、工业数据安全、智能制造安全。

张雄杰(1987-),男,本科,高级工程师,主要研究方向:工业互联网安全、物联网安全。

陈毅真(1982-),男,本科,高级工程师,主要研究方向:工业互联网安全、物联网安全。

(上接第 24 页)

参考文献

[1] 发改能源[2020]283 号文:《关于加快煤矿智能化发展的指导意见》[Z].2020.
[2] 王丹识,韩鹏军,王荣博,等.我国煤炭企业网络安全现状、问题分析研究与建议[J].中国煤炭,2022,48(7):34-40.
[3] ABDO H,KAOUK M,FLAUS J M,et al.A safety/security risk analysis approach of industrial control systems:a cyber bowtie-combining new version of attack tree with Bowtie analysis[J].Computers & Security,2018,72:175-195.
[4] SARKAR P,CHAKRABARTID,JORDAN M.Nonpara-metric link prediction in large scale dynamic networks[J].Electronic Journal of Statistics,2014,8(2):2022-2065.
[5] 张敏,魏伟,谭天怡,等.数据分类分级及其发展路径研究[J].网络安全与数据治理,2022,41(1):18-22,29.

(收稿日期:2022-10-25)

作者简介:

王许培(1989-),男,本科,助理工程师,主要研究方向:能源工业互联网安全、数据安全、物联网安全等。

王伟刚(1990-),男,本科,助理工程师,主要研究方向:能源工业互联网安全、移动互联网安全等。

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