

文章编号:1671-251X(2022)S2-0079-03

面向矿山智能化的工控数据安全保障体系

吴昊天

(国能信息技术有限公司, 北京 100011)

摘要:数据是矿山企业数字化转型和智能化生产的“生命线”。在矿山智能化升级过程中,数字化链接引发网络仿冒和数据窃取风险,智能化控制加剧网络安全管控需求,数据的规模化、价值化带来更大的网络安全风险,且数据管理措施失位现象较严重。基于以合规为指引、以风险为导向、以防护为基本、以业务为目标的防护原则,提出了智能矿山工控数据安全保障体系,从生产监控与管理大区、生产信息化大区、管理信息化大区3个业务区,阐述了工控数据安全防护措施,以保障矿山生产监测数据的完整性及工控管理、企业经营过程中的数据机密性。

关键词:智能矿山; 工控数据安全; 安全防护; 管理信息化; 生产信息化; 生产监控与管理

中图分类号:TD67 文献标志码:A

Security assurance system of industrial control data for intelligent mine

WU Haotian

(CHN Energy Information Technology Co., Ltd., Beijing 100011, China)

0 引言

随着矿山数字化、智能化技术快速发展,矿山生产设备之间互联互通,控制系统协同运行,极大地提高了矿山生产效率。但连接触发风险,实现网络互联与数据互通需考虑数据安全问题。数据是矿山企业数字化转型和智能化生产的“生命线”,需受到加倍重视和全方位防护。本文从矿山企业工控数据安全态势、防护措施等方面,阐述智能矿山工控数据安全保障体系建设。

1 矿山企业工控数据安全需求分析

在矿山智能化升级过程中,互联互通、数据汇聚会引发更多的安全风险,具体如下。

(1) 数字化链接引发网络仿冒和数据窃取风险。智能矿山建设使得分散的生产控制设备实现了联通和协同,导致潜在的网络攻击风险,如设备仿冒、数据窃取等。因此,需考虑互联互通的安全防护。

(2) 智能化控制加剧了网络安全管控需求。工控数据多呈现格式简单、种类繁多、高频交互、报文小等特征,监测数据和管理指令的完整可信关乎生

产安全,因此需建设有别于传统安全的防护机制,实现对工控数据的专用防护。

(3) 数据的规模化、价值化带来更大的网络安全风险。智能化建设转变了传统工业数据的使用模式,从单一静态向多维协同转变,包含数据资源池、云计算中心、一体化智能管控、智能生产应用、数据协同和决策支持等,实现了对数据的多方汇聚分析和数据价值挖掘。数据的规模化、价值化带来较大的安全风险,需从全局出发进行顶层设计,综合考虑数据平台的各类应用特性和外联方式,构建以数据为中心的安全防护体系,在挖掘数据价值的同时,保护矿山企业的核心商业秘密和生产经营数据。

除上述技术风险外,目前管理措施失位的现象较严重。安全是“三分技术,七分管理”。缺乏完善的安全技术使用规程和管理制度可能会造成更严重的危害,甚至引发连锁反应。因此,需加快制度修订编制,建立分级分类制度,加强培训,结合技术工具完善数据的统一管理。

2 智能矿山工控数据安全保障体系设计

结合智能矿山发展现状和信息化、智能化建设趋势,基于以合规为指引、以风险为导向、以防护为

收稿日期:2022-08-25;责任编辑:李明。

作者简介:吴昊天(1995—),男,北京人,主要从事网络与信息安全防护工作,E-mail:20035110@chnenergy.com.cn。

基本、以业务为目标的防护原则,提出智能矿山工控数据安全保障体系,如图 1 所示。该体系包括生产监控与管理大区、生产信息化大区、管理信息化大区,分为生产控制层、过程监控层、生产管理层的企

业资源层。不同层级的实时性、承载业务和防护重点不同。智能矿山工控数据安全保障体系以不同层级为界限,从数据全生命周期防护的各个环节出发,提供有针对性的安全设计。

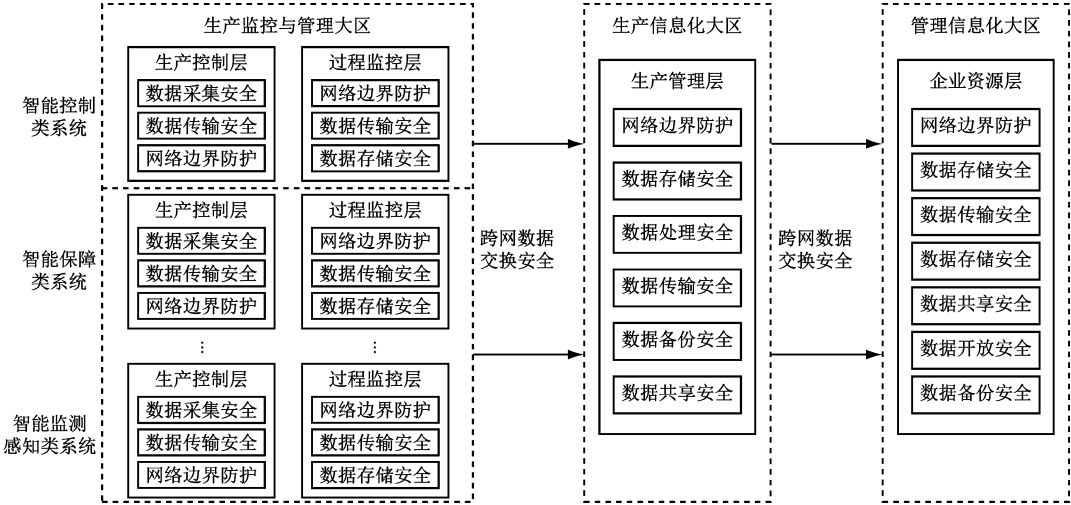


图 1 智能矿山工控数据安全保障体系

2.1 生产监控与管理大区

智能矿山各生产系统以过程监控层的管理设备对生产监控层的实时控制系统和生产设备进行管理,因此将生产控制层和过程监控层合并为生产监控与管理大区,对各生产系统进行数据安全设计。

智能控制类系统包括生产设备、自动化控制系统和智能化分析系统。生产设备将实时生产状态和监测数据上传至控制系统和分析系统中,控制系统按需下达控制指令。智能监测感知类系统包括针对矿山各类物理环境的监测监控系统、人员保护类系统等,环境参数采集设备将矿山各类实时信息回传至监控平台,视频监控系统实时回传监控视频图像,人员保护类系统将人员定位、通信和状态数据回传到管理平台。从安全考虑,需进行网络边界防护、数据采集安全、数据传输安全和数据存储安全等防护设计,构建工业生产最末端的第 1 层防护体系。

网络边界防护主要通过部署工业防火墙、入侵检测、工业审计、主机防护和运维管控,实现对终端与服务器的安全防护。考虑数据来源的可信度和监测数据上传及指令下达的安全传输需求,需部署接入认证设备,并对生产设备进行安全加固,保障数据源可信。此外,需关注管理控制系统及智能化分析系统中的数据存储安全,通过部署加密类和审计类设备,保障数据在存储和使用过程中的安全性。

2.2 生产信息化大区

生产信息化大区主要覆盖企业的生产管理层,部署了大量生产信息化系统,如 MES(Manufacturing Execution System,制造执行系统)、生产综合调度、三维采矿平台、智能预测预警等业务系统,对矿山各

生产环境提供集中管控、协同支撑、决策优化和健康监测等功能。生产信息化大区联通了各生产监控与管理大区的系统,汇聚多方数据,需进行网络边界防护、数据传输安全、数据存储安全、数据处理安全、数据备份安全和数据共享安全防护设计,形成对生产控制系统的第 2 层工业生产安全防护体系。

网络边界防护通过部署统一安全管理平台、日志收集与分析系统、运维审计系统、工业防火墙、入侵检测系统,实现对管理网络边界的综合防护;部署 VPN(Virtual Private Network,虚拟专网)安全网关,构建数据安全传输通道,并对接入设备进行可信度鉴别;部署数据加密系统和审计系统,对数据库、文件系统进行综合防护;部署身份认证模块,对业务处理行为进行鉴别和签名,实现数据处理的有效追溯;建设备份中心和安全备份通道,实现数据安全备份;建设数采单向设备和数据安全交换设备,支撑管理数据与相关第三方监管机构的数据上报和安全交互。

2.3 管理信息化大区

管理信息化大区主要覆盖企业资源层,部署日常办公类系统、市场营销类系统、经营管理类系统和决策支持系统等与企业生产经营相关的统建系统。鉴于矿山企业体系化、多层级的组织结构模式,需跳出单一的组织结构单元,从企业资源层全局出发,针对整体架构及各决策层级、各业务单元之间的业务与管理交互进行相应的数据安全体系规划设计。

建设总部级数据安全服务体系,作为集团数据安全服务的核心,保证全集团数据安全保障的整体性,同时为集团总部业务区的集团性企业信息

化应用提供本地化数据安全服务能力支撑;在企业内部各组织机构网络的互联网出口部署 VPN 安全网关,实现各组织机构跨广域网通信链路的机密性保护,保证企业内各组织机构间数据交互的机密性、完整性;各二、三级单位建设本地分支数据安全服务区,在集团总部数据安全服务中心的统一管理下,提高服务本地化业务应用的数据安全能力。

具体实践上,基于密码技术,通过信道加密方式或信源加密方式,实现企业业务平台各商业秘密数据传输的机密性、完整性保护,同时调用数据安全服务,针对业务平台本地存储的各种关键用户数据、业务数据进行加密存储,实现关键数据存储的机密性、完整性保护。

针对业务办公和数据处理,通过密钥认证方式,实现企业“互联网+”平台应用系统用户登录的可靠身份认证,实现平台应用可信访问;通过数字签名、时间戳等密码技术,确保用户后续操作的抗抵赖性防护。

针对数据共享和数据开放,通过数据安全交换平台,结合数据标签、安全多方计算等技术,实现数据多方的协同共享和安全交换;通过数据安全 API (Application Programming Interface,应用程序接口)网关,实现数据对外服务过程中的应用鉴别、安全传输和访问控制,保障授权应用访问权限内的数据集,避免数据开放引发数据外泄。

3 结语

工控环境有别于传统网络环境,其封闭、独立特

(上接第 73 页)

2 结语

煤矿智能化综合管控平台的技术应用是煤矿智能化建设中的重点,是煤矿各项智能化应用系统的底层基础。煤矿智能化是一项涉及多专业的复杂工程,而我国目前的煤矿智能化仅仅处于初级阶段,需要不断努力,有序开展各地区的煤矿智能化建设,从而更好地实现煤炭行业的智能化发展和转型。

参考文献:

[1] 田立贞. 煤矿智能化开采技术研究现状及展望[J]. 当

性决定了防护机制需从工控场景、工控协议和工控设备的特性出发,以数据安全保障体系为指导,研制有工控属性的数据安全防护产品。以矿山智能化转型为背景,以智能矿山作为工控防护场景,对生产监控与管理、生产信息化、管理信息化 3 个业务区进行梳理,从数据全生命周期角度设计了工控数据安全保障体系,以保护矿山生产监测数据的完整性及工控管理、企业经营过程中的数据机密性。

参考文献:

[1] 韩志磊,王治宇,苏军,等. GPS 智能巡检系统在尾矿库安全管理中的应用[J]. 有色金属(矿山部分),2018,70(4):6-11.

[2] 阮诗昆,黄玉锦,蓝先灵. 智能卡车调度系统在紫金山露天矿的应用[J]. 有色金属(矿山部分),2020,72(2):102-106.

[3] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求[S].

[4] 陆耿虹,冯冬芹. 基于改进 C-SVC 的工控网络安全态势感知[J]. 控制与决策,2017,32(7):1223-1228.

[5] 任圆. 工控网络多安全目标优化防护方法研究[D]. 哈尔滨:哈尔滨工程大学,2020.

[6] 崔文,李浩荡,丁震,等. 露天煤矿 5G 网络建设与网络安全研究[J]. 工矿自动化,2021,47(增刊 1):36-38.

[7] 张春坡. 黑岱沟露天煤矿工业控制网络安全防护技术研究与应用[J]. 煤炭工程,2021,53(增刊 1):144-148.

[8] 杨翔宇. 关于工控网络与非公开网络互联的数据安全保障分析[J]. 电子技术与软件工程,2020(20):247-248.

代化工研究,2020(23):13-14.

[2] 姜德义,魏立科,王翀,等. 智慧矿山边缘云协同计算技术架构与基础保障关键技术探讨[J]. 煤炭学报,2020,45(1):484-492.

[3] 汤海龙. 智慧矿山信息系统通用技术规范解读及关键技术探讨[J]. 煤炭科学技术,2018,46(增刊 2):157-160.

[4] 吴群英,蒋林,王国法,等. 智慧矿山顶层架构设计及其关键技术[J]. 煤炭科学技术,2020,48(7):80-91.

[5] 罗香玉,李嘉楠,郎丁. 智慧矿山基本内涵、核心问题与关键技术[J]. 工矿自动化,2019,45(9):61-64.