煤矿网络安全等级保护建设规划分析

钟兆华 刘清涛

矿山智能化建设大幅提升了煤矿生产的自动化、现代化及智能化水平，人工智能、工业物联网、云计算、大数据、机器人、智能装备等与煤矿生产的深度融合，形成了全面感知、实时互联、分析决策、自主学习、动态预测、协同控制的智能系统，可实现煤矿采掘、运输、通风、分选、安全保障、经营管理等过程的智能化运行，对提升煤矿安全生产水平、保障煤炭稳定供应具有重要意义。但同时新技术的应用带来了新的安全风险，且随着工业化、信息化的快速发展，煤矿工业互联网建设加速，煤矿生产网络越来越开放，隔离被打破，给煤炭企业网络安全防护带来了挑战。

中煤华利能源控股有限公司荣欣公司（以下简称荣欣公司）矿井位于山西省吕梁市，设计产能为90万t/a。矿井目前建设了办公网络、煤炭专网、工业以太环网等，已经建成三级信息化矿井，建设信息化系统项目35项。荣欣公司基于现有网络基础，建设了内部业务应用系统、行政办公网络、井下通信、视频监控等，给日常办公及矿井自动化带来诸多便利，但也带来了安全隐患。目前，荣欣公司的网络系统缺少必要的安全设备，网络、主机、应用均存在安全风险。另外，国家加强了对网络安全工作的监管，网络安全已上升至法律层面。2017年6月，《中华人民共和国网络安全法》颁布施行，第21条明确规定国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护（图1）制度的要求，履行安全保护义务。2019年12月，等级保护2.0正式实施，这是网络安全的一次重大升级，保护对象范围在传统系统的基础上扩大了云计算、移动互联、物联网、工业控制系统等场景的同时，对等级保护2.0的建设提出了新的

什么是等级保护

根据信息和信息系统在国家安全、经济建设、社会生活中的重要程度，以及遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度，将信息系统划分为不同的安全保护等级，并对其实施不同的保护和监管

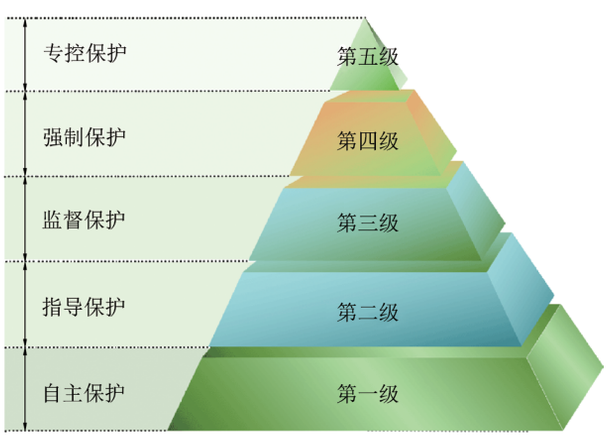

图1 网络安全等级保护

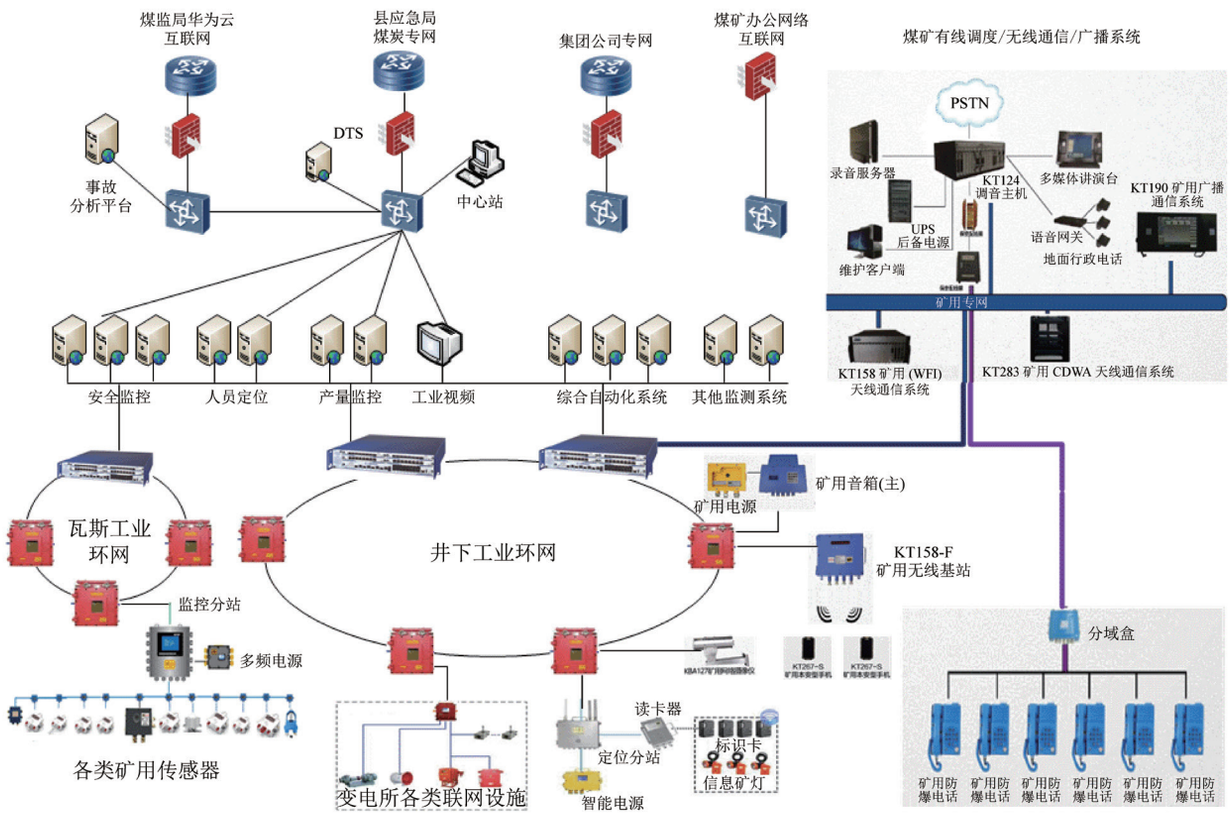

图2 荣欣公司网络安全架构现状

要求。2021年3月，山西省能源局等部门联合印发了《煤炭企业网络安全等级保护工作管理办法》《煤矿企业贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的工作实施方案》，文件明确要求落实并实施国家网络安全等级保护制度，科学开展安全建设整改。基于上述背景，荣欣公司决定进行安全等级保护建设，提升自身安全防护能力，保证本单位网络系统安全稳定运行且合法合规。

网络信息系统安全现状分析

为全面梳理煤炭企业网络信息系统安全保护现状，以及为如何开展网络安全等级保护定级工作提供指导意见，对荣欣公司网络系统进行了调研，网络安全架构现状如图2所示。

荣欣公司的网络环境分为煤炭专网、煤监局事故分析平台网、集团专网、煤矿办公网络与井下工业环网5类。

1）煤炭专网上联应急局，通过DTS采集井下瓦斯、人员定位、产量监控数据，同时将工业视频上传到上级监管部门。目前通过1台路由器上联煤炭专网，通过1台防火墙下联煤炭专网交换机，三大系统及工业视频通过双网卡配置双地址连接煤炭专网与工业环网。

2）煤监局事故分析平台所在网络（互联网）单独通过交换机-防火墙-4G路由器连接互联网，通过VPN的方式将煤炭专网DTS采集的瓦斯浓度、人员信息等数据上传至本地事故分析平台（煤矿信息化综合监控系统平台），再上传至华为公有云事故分析平台，事故分析平台网络通过交换机与煤炭专网交换机进行互联，通过路由实现互通。

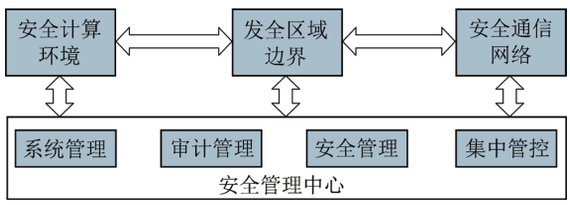

图3 等保“一个中心、三重防护”体系

3）集团专网上联集团，为独立网络。煤矿办公网络通过1台路由器连接互联网，实现煤矿端通过路由器地址转换上网，为独立网络。

4）井下工业环网主要负责对井下自动化和监测类系统进行数据采集、展示、监控，由瓦斯环网与工控环网组成，瓦斯环网只负责瓦斯数据采集并上传至瓦斯服务器，工控环网负责井下除瓦斯系统以外的其他自动化及监测类系统。

荣欣公司信息系统的不同网络和区域之间存在一定程度的信息共享需求，在各物理网络边界及重要业务服务器区域的边界上没有严格的控制手段，一旦遭到网络攻击就会造成大面积的网络瘫痪，仅靠防火墙设备无法防护各类变形攻击行为，同时也会波及到其他网络。

矿端事故分析平台网出口只采用了1台路由器上联，下联通过防火墙、交换机均未能实现设备级和链路级冗余，设备或链路发生故障时无法在最短时间内恢复使用。网络内网终端如果感染病毒，则无法对网络内部进行病毒查杀或隔离。路由器、交换机及重要业务服务器等设备的日志信息未实现集中存储及审计分析。

安全等级保护改造需求分析

企业各业务系统基本部署于工业环网，由三大系统及工业视频连接到煤炭专网，通过集团进行数据及视频上传至监管部门。目前，荣欣公司网络安全防护措施匮乏且防护设备单一，未形成系统化及立体化防护体系，如防火墙等仅有的安全防护设备从首次部署至今，几乎从未做过配置更新及升级工作，漏洞修复、打补丁等工作同样从未实施。此外，网内电脑未安装杀毒软件，导致安全保障的难度大幅增加。

安全等级保护整改建设按照完善“一个中心、三重防护”体系（图3）的原则，并最终达到等保合规、业务安全的目的。

需求分析具体主要分为外部的安全物理环境需求分析和系统内部的安全通信网络需求分析、安全区域边界需求分析、安全计算环境需求分析、安全管理中心需求分析等方面。

安全物理环境需求分析

煤矿企业机房应具备基本的有效管控措施，以保障网络及信息化系统的物理环境安全规范。需要解决的主要问题包括以下5点：

1）机房出入口未配置电子门禁系统，无法控制、鉴别和记录进入的人员。

2）未完善机房防盗报警系统或设置有专人值守的视频监控系统。

3）未将各类机柜、设施和设备等通过接地系统安全接地。

4）未采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。

5）主要设备未采用必要的接地防静电措施，机房应补齐防静电地板。

安全的物理环境作为网络安全外部需求，可自行建设整改，不做重点讨论。

安全通信网络需求分析

经过调研，煤矿企业在通信网络方面基础一般，煤炭事故分析平台网络并未实现设备及链路级冗余，一旦出现网络设备硬件故障，网络将发生瘫痪，造成业务应用服务停止。不同网络间未采取可靠的技术隔离手段，一经连通，网络间即处于不设防的危险状态。不同网络区域与其他网络区域之间未采取可靠的访问控制手段，可能造成跨网非法应

用访问及数据泄露。网络中未进行安全分区分域保护，所有业务应用均处于整体网络中，所有终端可访问网络内所有网络设备及服务器主机设备。需要解决的主要问题包括以下6点：

1）未提供关键网络设备冗余，无法保障系统的可用性。

2）网络带宽未能够满足业务高峰时期数据交换需求，未合理地划分网段和VLAN。

3）不同物理网络间未采取物理隔离装置，难以实现隔离。

4）未划分不同的网络区域，重要网络区域与其他网络区域之间未采取可靠的技术隔离手段。

5）未采用校验技术或密码技术保证通信过程中数据的完整性和保密性。

6）未提供有效的网络安全审计能力，包括日志审计、数据库审计及运维审计等方面，不利于事后追溯。

安全区域边界需求分析

在区域及网络边界方面的基础较为薄弱，网络之间连接错综复杂，未在网络区域之间根据访问控制策略设置访问控制规则，网络边界的访问控制配置不当且未及时更新。在关键网络节点处没有任何技术手段用来检测、防止或限制从外部或内部发起的网络攻击行为，缺乏恶意代码检测和清除技术手段。需要解决的主要问题包括以下4点：

1）在网络边界和区域之间未根据访问控制策略设置访问控制规则，未合理配置访问控制，以及未随业务发展及时更新。

2）未采取措施在关键网络节点处检测、防止或限制从外部或内部发起的网络攻击行为。

3）未采取措施在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的更新。

4）未采取措施在网络边界、重要网络节点进行安全审计，以及对重要的用户行为和重要安全事件进行审计。

安全计算环境需求分析

在计算环境方面基础相当薄弱，网络设备、安全设备及主机设备存在大量弱口令及相同口令。设备鉴别信息缺乏防窃听措施或手段，且未采用多种身份鉴别技术。缺乏有效的安全审计措施，对重要用户行为和重要安全事件进行追溯审计。需要解决的主要问题包括以下8点：

1）网络设备、安全设备及主机设备存在大量弱口令及相同口令，未对登录的用户进行身份识别和鉴别，身份鉴别信息复杂度不符合要求且未定期更换。

2）设备鉴别信息缺乏防窃听措施或手段，且未采用多种身份鉴别技术，未采取必要措施防止鉴别信息在网络传输过程中被窃听。

3）缺乏有效的安全审计措施，未对重要的用户行为和安全事件进行追溯审计。

4）设备存在开启不需要的系统服务、默认共享及高危端口。

5）未采取任何设备管理终端准入管控等限制措施。

6）缺乏主机恶意代码防范措施。

7）缺乏对重要数据传输完整性的保护措施。

8）缺乏数据备份措施。

安全管理中心需求分析

在管理中心方面未采取任何措施及手段，未采取任何运行监控措施及安全事件发现处置措施。需要解决的主要问题包括以下3点：

1）缺乏运行监控措施。

2）缺乏安全事件发现处置措施。

3）未对分散的审计数据进行汇总及集中分析。

网络安全建设目标

为全面推进煤矿企业网络安全防范管理、监测预警、应急处置等各项工作，积极构建良好的网

(a) 技术要求　　(b) 管理要求

图4 等级保护2.0（三级）基本要求框架

络安全保护生态，提升安全综合防护能力，深入贯彻落实国家网络安全等级保护制度和关键信息基础设施安全保护制度，健全完善网络安全综合防控体系，荣欣公司的网络安全建设工作需实现以下4个目标：

1）全面满足网络安全等级保护2.0第三级标准（图4）及关键信息基础设施安全保护制度的能力要求。

2）进行云计算服务器虚拟架构建设，使煤矿数据中心从单独的、割裂的物理形态向云化转变，为建设智能矿山及煤矿大数据打下良好基础。

3）建设有效的数据安全防护，在数据安全治理、数据备份恢复、数据监督管理及大数据协同安全等方面有效提高数据安全防护能力，重点加强矿端业务数据资产安全管控，具备数据资产分析、数据安全管控以及数据安全监测等防护措施。

4）落实网络安全态势感知监测预警措施，部署网络安全威胁分析设备，对网络运行状态、网络流量、用户行为、网络安全案件等进行监测分析，对网络攻击事件的分析和处置能够从事前监测、事中防御、事后审计等方面进行监测。

网络安全建设内容

为全面提升信息安全整体水平，实现智能化矿井要求，根据《山西省煤矿企业信息化建设等级评估评分细则》《煤炭企业网络安全等级保护工作管理办法》等文件要求，确定以下6项具体建设内容：

1）根据网络安全等级保护2.0第三级标准及关键信息基础设施安全保护制度的能力要求，煤矿企业需制定安全建设整改方案，落实建设整改措施，消除安全风险隐患，建立立体化、动态化的安全技术防护体系，以保证信息系统具备整体安全保护能力。

2）煤矿企业数据中心采用云计算服务器虚拟架构，实现数据中心计算、存储、网络及安全资源弹性扩展，提升数据中心及业务应用的一体化、集约化能力。

3）根据《煤矿企业贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的工作实施方案》的要求，实施重要业务数据的安全防护，重点加强矿端业务数据资产安全管控，提供数据资

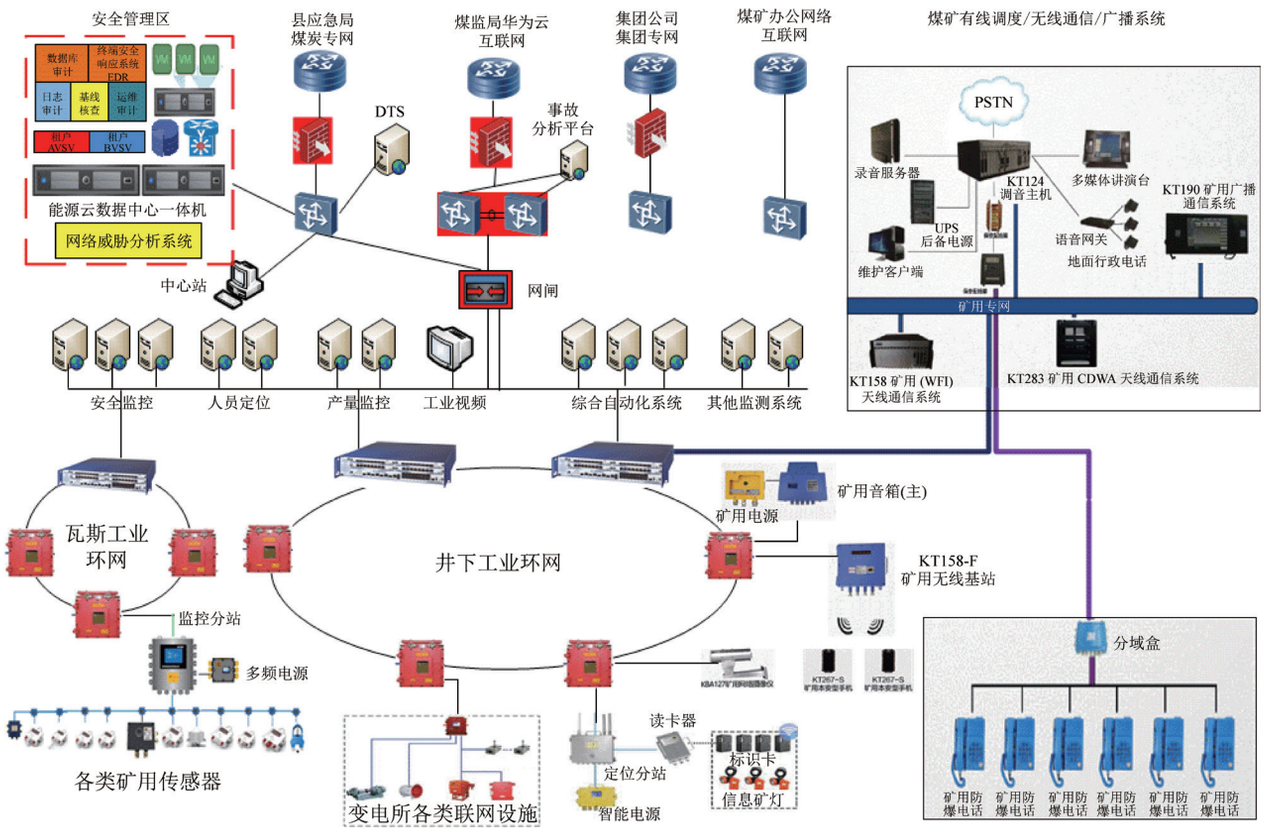

图5 荣欣公司网络等级保护整改拓扑

产分析，数据安全管控以及数据安全监测等防护措施。

4）根据《煤矿企业贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的工作实施方案》要求，落实网络安全态势感知监测预警措施，部署网络安全威胁分析设备，对网络运行状态、网络流量、用户行为、网络安全事件等进行监测分析。

5）建立网络安全管理组织机构及安全管理制度，成立信息安全工作组，设立安全责任人，制定实施信息系统安全等级保护的具体方案，并制定相应的岗位责任制，确保信息安全等级保护工作顺利实施。

6）制定煤矿网络业务应用系统应急预案。按可能出现问题的不同情形制定相应的应急措施，在网络系统出现故障和意外且无法短时间恢复的情况下，确保生产活动能够持续正常进行。

整改方案设计

通过对荣欣公司企业网络结构进行深入调研及重新设计（图5），对事故分析平台网、煤炭专网及若干工业环网进行边界厘清及安全隔离规划，在安全威胁可控的前提下实现数据跨网传输，具体规划内容为以下4点：

1）将煤矿企业纵向分为生产控制层、生产管理层、企业资源层3个主要层次。生产控制层主要包括地面工业环网、井下工业环网、安全监控工作环网、无线通信等系统，以及相关系统所需的PLC、传感器、分站、协议转换模块等相关生产设备；生产管理层主要包括过程监控区（常规情况下的过程监控层）、生产管理区（常规情况下的生产管理层）、调度中心、云安全中心及云数据中心；企业资源层主要包括煤矿企业互联网/煤炭专网出口相关链路及煤矿企业管理应用。

2）生产控制层主要包括井下数据，包含工业视频、安全监控、电力监控、无线通信、广播通信等系统，以及相关系统所需的PLC、传感器、分站、协议转换模块等相关生产设备。

3）生产管理层为本次设计的重点，其中为达到本次等保三级安全整改效果，需在煤炭专网建立安全管理中心，部署日志审计、防病毒系统、运维审计、数据库审计、基线核查、应用主机综合防护系统、安全采集探针等符合等保三级要求的安全能力。

4）在企业资源层，本次网络安全等级保护主要针对煤炭专网相关联的三大系统和工业视频及事故分析平台应用系统网络进行安全整改。煤炭专网防火墙更换为含入侵防御及防病毒能力的下一代防火墙，满足边界对病毒及入侵的防范。由于事故分析平台网承载等保三级业务应用系统，因此将事故分析平台网的接入交换设计为冗余链路及冗余设备，防火墙更换为含入侵防御及防病毒能力的下一代防火墙，事故分析平台服务器双链路连接2台交换机，保证事故分析平台网关键链路、网络及服务器链路的高可靠性及高可用性。同时在事故分析平台网与煤炭专网之间，煤炭专网与工业环网之间通过新增网闸，满足不同网络间物理隔离的需求，符合等保三级的要求。

结 语

随着近些年安全形势不断严峻，加强网络外部防护及内部管控，实现全面整体安全防护、检测、审计的全生命周期安全需求越来越迫切，煤矿作为国家定义的关键信息基础设施运营者，应当履行网络安全等级保护相关工作。同时，为了推进矿山智能化建设，更好地保障煤炭企业网络安全，煤矿网络安全建设工作的开展十分必要且具有重要意义。

■ 责任编辑：李金松

作者简介：
第一作者：钟兆华，高级工程师，主要从事机电技术管理工作。E-mail：2059783368@qq.com
作者单位：中煤华利能源控股有限公司

热点问答

矿井“一通三防”管理信息系统涉及的主要核心算法与实现功能有哪些?

主要核心算法：①通风网络图绘制及拓扑联动算法；②自动生成通风网络图算法；③通风网络模拟解算算法；④通风阻力计算算法；⑤瓦斯涌出预测模型；⑥事故树分析及其计算模型。

主要实现功能：①系统建立了完善的、符合煤炭行业规范的通风安全专业符号库，同时为用户提供了方便的图例制作和管理工具；②系统具有精美的地图显示效果，提供了强大的地图排版布局环境，支持打印预览和裁剪打印输出，并支持各种型号的打印机和绘图仪；③提供了全自动、交互式的通风网络图生成功能，方便地进行通风网络图的编辑和网络模拟解算；④在采掘工程平面图基础上绘制通风系统图、防尘系统图、避灾路线图、瓦斯防治系统图等；⑤基于采掘工程平面图或通风系统图自动生成通风网络图；⑥实现通风机数据的统一管理；⑦基于通风系统图巷道拓扑关系自动生成任意视角的通风立体图（巷道立体图）。

—— 来源：《中国煤矿智能化发展报告》（2020年）