ICS 35.030
CCS L 80

团　　体　　标　　准

T/CNCA 109—2025

智能化煤矿网络安全技术要求

Technical requirements for intelligent coal mine network security

2025-04-07 发布　　2025-06-30 实施

中国煤炭工业协会　发布
中国标准出版社　出版

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国煤炭工业协会提出。

本文件由中国煤炭工业协会科技发展部归口。

本文件起草单位：陕西陕煤榆北煤业有限公司榆林信息化运维分公司、北京珞安科技有限责任公司。

本文件主要起草人：齐景锋、赵洪辉、王珀、刘厚荣、崔含、王鹏飞、李耀龙、冯向谊、马朝远、苏兴旺、许一健、冯栋、肖智中、申荣鹏、何兴红。

智能化煤矿网络安全技术要求

1 范围

本文件规定了煤矿生产企业网络安全技术、安全管理及安全运营服务的要求。

本文件适用于煤矿生产企业工控网生产信息系统、企业网信息化系统的网络安全防护。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

网络安全 network security

对网络环境下存储、传输和处理的信息的保密性、完整性和可用性的保持。

[来源:GB/T 25069—2022,3.616]

3.2

身份认证 identity authentication

在计算机及计算机网络系统中确认操作者身份的过程。

3.3

安全审计 security audit

获取、记录、存储、分析关键事件活动和行为信息,为事后安全事件分析提供线索和取证。

3.4

物联网 internet of things

将感知节点设备通过互联网等网络连接起来构成的系统。

[来源:GB/T 22239—2019,3.15]

3.5

资产 property

对企业具有价值的信息或资源,是安全策略保护的对象。

3.6

脆弱性 vulnerability

计算机或网络系统在软件、硬件、协议和安全策略方面的固有缺陷。

3.7

威胁 threaten

网络或系统存在被窃听、重传、伪造、篡改、非授权访问、拒绝服务攻击等不利动作或活动。

3.8

风险 risk

利用系统存在的漏洞和脆弱性,导致系统关键信息丢失、损坏或破坏的可能性。

4 缩略语

下列缩略语适用于本文件。

ABAC：基于属性的访问控制（Attribute-Based Access Control）

CA：证书授权（Certificate Authority）

DDoS：分布式拒绝服务攻击（Distributed Denial of Service Attack）

DLP：数据防泄漏（Data Loss Prevention）

DMZ：非军事化区（Demilitarized Zone）

HMI：人机界面（Human Machine Interface）

HTTPS：超文本传输安全协议（Hypertext Transfer Protocol Secure）

IP：防护等级（Ingress Protection）

NDA：保密协议（Non-Disclosure Agreement）

OPC：用于过程控制的 OLE（OLE for Process Control）

OWASP：开放式 Web 应用程序安全项目（Open Web Application Security Project）

PAM：特权访问管理（Privileged Access Management）

PII：个人身份信息（Personally Identifiable Information）

PLC：可编程序控制器（Programmable Logic Controller）

RBAC：基于角色的访问控制（Role-Based Access Control）

SCADA：监视控制与数据采集系统（Supervisory Control and Data Acquisition）

SQL：结构化查询语言（Structured Query Language）

SSH：安全外壳协议（Secure Shell）

TLS：传输层安全性协议（Transport Layer Security）

UPS：不间断电源（Uninterruptible Power Supply）

VPN：虚拟专用网络（Virtual Private Network）

5 安全防护模型

基于煤矿生产企业网络安全现状与业务特性，从安全技术、安全管理及安全运营三个维度构建标准化的网络安全要求，形成技术防护、管理闭环、服务支撑三位一体的网络安全防护模型，推动煤矿生产企业网络安全生态体系的良性发展，防护模型如图 1 所示。

煤矿生产企业网络安全防护架构见附录 A。

煤矿生产企业安全防护设备部署见附录 B。设备功能介绍见附录 C。

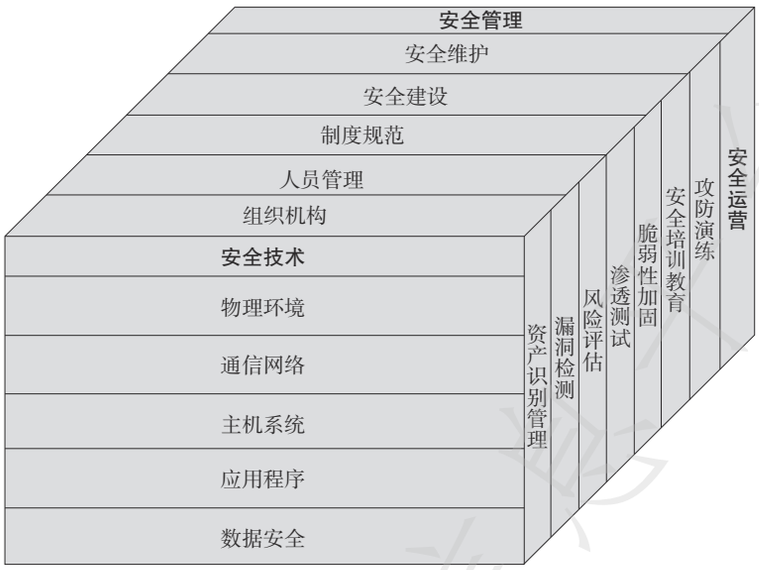

图1　安全防护模型

6　系统等级评定防护

按照煤矿生产企业工控网生产信息系统、企业网信息化系统被攻击后的影响范围、程度及对生产安全影响，遵循自主定级的原则，评定为一般系统、重要系统、关键系统，并组织专家开展定级评审，确认系统最终等级；在对应防护等级上，依次对应初级、中级、高级三个防护等级，形成分等级、分重点的防护模式，对应关系见表1。系统定级评审表参照附录D。

表1　系统级别及防护等级

级别	描述	防护等级
一般系统	系统受到破坏后，会损害公民、法人和其他组织的合法权益，对社会秩序和公共利益造成损害，对安全生产无直接影响或影响较小，破坏后影响范围有限，可快速恢复	初级防护
重要系统	系统受到破坏后，会严重损害公民、法人和其他组织的合法权益，对社会秩序和公共利益造成严重损害，甚至可能对国家安全造成轻微损害，间接影响生产安全，中断可能导致生产停滞或安全隐患	中级防护
关键系统	系统受到破坏后，会特别损害公民、法人和其他组织的合法权益，对社会秩序和公共利益造成特别损害，甚至可能对国家安全造成特别损害，直接影响煤矿安全生产，可能导致重大安全事故或人员伤亡	高级防护

7　安全技术要求

7.1　初级防护要求

7.1.1　物理环境安全

7.1.1.1　场地选择

具体要求如下：

a）　煤矿工控网、企业网地面机房应避免设在建筑物的高层、地下室及用水设备的下层或隔壁；

b） 地面机房位置应避开存放腐蚀、易燃、易爆物品及有害气体等危险区域；
c） 地面机房位置应避开低洼、潮湿、地震频繁、强噪声及强电磁场的区域；
d） 井下安全设备宜安装在硐室内，硐室过道应保持畅通，硐室内设备与墙壁、设备之间应留出60 cm以上的通道；
e） 井下硐室内不应存放汽油、煤油、绝缘油和其他易燃物品；
f） 井下硐室内应采取防水措施，不应滴水或积水；
g） 井下安全设备所用的机箱、配电柜应具备IP防护等级、防爆认证资质。

7.1.1.2 防破坏、盗窃

具体要求如下：
地面机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。

7.1.1.3 防水、防静电、防雷击

具体要求如下：
a） 应在机房地面、吊顶设防水层，并有漏水检查装置；
b） 应在机房易产生静电的地方采用静电消除装置；
c） 应将机房机柜、设施和设备等通过接地系统安全接地。

7.1.1.4 供电系统

具体要求如下：
a） 机房应具备可靠的双路供电冗余，以确保电力的不间断供应；
b） 机房应配备足够容量的UPS系统，为设备提供短时间的应急电力支持。

7.1.1.5 火灾报警及消防

具体要求如下：
a） 应在机房装有灭火装置；
b） 不应使用水、干粉或泡沫等易产生二次破坏的灭火剂。

7.1.1.6 温、湿度控制

应设置温、湿度自动调节设施，温度控制在20 ℃～24 ℃之间，相对湿度保持在45%～65% 范围内。

7.1.2 通信网络安全

7.1.2.1 架构设计

具体要求如下：
a） 将用户规模、网络带宽、网络延时、数据处理需求等作为网络设计的主要指标，应满足后续业务扩容需求；
b） 网络架构、设备选型、业务模块等应具备可扩展性；
c） 工控网煤矿生产信息系统所在的通信网络应采用环形组网方式。

7.1.2.2 安全分区

具体要求如下：
a） 应根据系统业务属性、功能、实时性要求区分系统类别，并划分至对应区域；
b） 孤立的网络系统，不严格要求形成区域的概念，但应具备相应的安全防护措施。

7.1.2.3 边界防护

具体要求如下：

a） 应对系统和网络边界部署防护类设备，能够对常规的攻击行为拦截并告警；应对4G/5G、虚拟化等接入边界设置合理的屏蔽、检测措施；

b） 应在工控网与企业网之间应采用物理隔离技术手段，不准许不同网络大区之间非安全互联互通。

7.1.2.4 安全监测

具体要求如下：

a） 应具备对网络流量和日志的攻击监测、入侵分析、行为审计、恶意代码检测的能力，及时发现网络中的恶意攻击、违规操作、非法接入等异常行为；

b） 应提供详细的网络安全审计记录，至少包含事件日期、事件类型、事件级别、访问源IP、访问目标IP、是否成功等，且留存时长不少于180 d。

7.1.3 主机系统安全

7.1.3.1 系统加固

具体要求如下：

a） 关闭煤矿工控网生产信息系统、企业网信息化系统高危端口和服务，修改默认配置，收敛资产暴露面；

b） 对工控网生产信息系统、企业网信息化系统的默认账户实施重命名、删除或禁用操作；应采用字母、数字、下划线组合且长度不小于8位的复杂口令，不准许空口令、证件号、工号、联系方式等作为口令使用；同步部署口令周期性更换策略，每90 d完成一次口令更新；

c） 对煤矿工控网生产信息系统、企业网信息化系统安全日志、系统日志有合理的第三方配置；

d） 及时更新系统、数据库、规则库、病毒库及漏洞补丁信息；对系统的策略配置、安全规则及时更新、优化和变更调整，并确保配置结果生效；

e） 涉及煤矿生产信息系统生产区工程师站、操作员站，应关闭或封堵外设接口，并通过严格的物理或技术措施严加管控；不准许开启多网卡配置，互访不同网络；

f） 通过白名单防护机制对煤矿生产信息系统生产区工程师站、操作员站进行防护，防止恶意软件或程序破坏现场终端。

7.1.3.2 漏洞管理

具体要求如下：

a） 以60 d为检测周期，对煤矿生产信息系统、信息化系统开展系统漏洞专项检查，并做好安全评估及整改工作；

b） 及时关注官方发布的与系统软、硬件相关的漏洞，及时追踪补丁信息，并一定时间内（原则上不超过3 d）完成补丁修复；涉及煤矿生产信息系统在补丁修复前，应在模拟环境运行测试，验证补丁安全和稳定性。

7.1.3.3 操作审计

应对煤矿生产信息系统、信息化系统的登录注销、服务启动关闭、文件修改、程序使用等系统交互活动实时审计记录，并对日志信息进行第三方的安全备份，时长不少于180 d。

7.1.3.4 集中管理

应对网络设备、安全设备或安全组件集中管控，对设备运行状况、安全状态、安全策略、恶意代码、补

丁升级等进行集中配置和控制。

7.1.4 应用程序安全

7.1.4.1 应用识别

基于协议、流量行为、应用指纹、负载特征、机器模型、威胁情报等识别程序流量，推断应用类型，并对最终应用进行分类。

7.1.4.2 应用访问

具体要求如下：

a） 应通过口令、生物识别、硬件令牌等两种或两种以上因素组合技术验证访问者真实身份；

b） 应通过网络层、应用层、数据层设置对应用的访问控制策略；

c） 应设定会话超时、登录次数限定、自动退出等技术措施。

7.1.4.3 应用防护

应部署应用安全防护和审计类设备，实现常规攻击防护、检测与审计。

7.1.4.4 应用审计

具体要求如下：

a） 应具备精准识别对煤矿生产信息系统、信息化系统的漏洞探测、弱口令通信、文件上传/下载、命令注入、SQL注入、跨站脚本、跨站请求伪造、信息泄漏等常规漏洞利用的技术措施；

b） 应提供详细的安全审计记录，至少包含事件日期、事件类型、事件级别、访问源IP、访问目标IP、是否成功等，为事后溯源审计提供审查依据；

c） 应保证应用审计记录的留存时长不少于180 d。

7.1.4.5 应用评估

具体要求如下：

a） 以60 d为检测周期，对应用程序开展漏洞专项检查，并做好安全评估及整改工作；

b） 在新应用投入使用前，应进行业务功能和安全漏洞的测试，确认在无安全隐患的前提下，才能上线使用。

7.1.5 数据安全治理

具体要求如下：

a） 根据数据敏感性和业务重要性（核心业务数据、用户隐私数据）划分备份优先级；

b） 数据备份应采用1-1-1备份规则：1份数据、1种介质、1份异地；

c） 对煤矿生产信息系统、信息化系统的关键数据保存时长不少于180 d。

7.2 中级防护要求

7.2.1 物理环境安全

7.2.1.1 场地选择

具体要求如下：

遵守7.1.1.1场地选择要求。

7.2.1.2 防破坏、盗窃

具体要求如下：

遵守 7.1.1.2 防破坏、盗窃要求，并增加：

对机房采取设备固定、安装防盗报警系统等措施。

7.2.1.3 防水、防静电、防雷击

具体要求如下：

遵守 7.1.1.3 防水、防静电、防雷击要求。

7.2.1.4 供电系统

具体要求如下：

遵守 7.1.1.4 供电系统要求，并增加：

机房应配备足够容量的 UPS 系统，为设备提供不少于 2 h 的应急电力支持。

7.2.1.5 火灾报警及消防

具体要求如下：

遵守 7.1.1.5 火灾报警及消防要求，并增加：

应在机房地板、吊顶、空调管道及易燃物附近设有烟、温感探测器。

7.2.1.6 温、湿度控制

具体要求如下：

遵守 7.1.1.6 温、湿度控制要求。

7.2.1.7 电磁防护

具体要求如下：

机房应对关键设备通信线路实施电磁屏蔽措施。

7.2.1.8 防静电

具体要求如下：

a） 机房应采用防静电地板或采用其他防静电措施；

b） 机房应采用静电消除器、佩戴防静电手环等措施，以防止产生静电。

7.2.1.9 内部装修

具体要求如下：

a） 机房装修材料应符合难燃材料或非燃材料特性，应能防潮、吸音、不起尘、抗静电等；

b） 机房活动地板应平整、光洁、防潮、防尘，且有稳定的抗静电性能和承载能力，具备耐磨、耐腐蚀等特性。

7.2.2 通信网络安全

7.2.2.1 架构设计

具体要求如下：

遵守 7.1.2.1 架构设计要求，并增加：

应提供关键通信线路、主机设备、网络设备、控制组件的冗余，保证业务的高可靠性。

7.2.2.2 安全分区

具体要求如下：

遵守 7.1.2.2 安全分区要求。

7.2.2.3 边界防护

具体要求如下：

a) 应对系统和网络边界部署行为管理类、准入类设备，能够对常规的攻击行为拦截并告警，对内外部网络连接、请求行为进行监管；

b) 应在工控网与企业网之间应采用物理隔离技术手段，不准许不同网络大区之间非安全互联互通。

7.2.2.4 安全监测

具体要求如下：

遵守 7.1.2.4 安全监测要求。

7.2.2.5 通信传输

具体要求如下：

a) 应采用HTTPS、SSH等安全通信协议来保障数据传输，防止通信过程被窃听、篡改或劫持；

b) 应使用VPN或其他加密技术建立安全可信的通信链路，对敏感信息字段或整个报文进行加密。

7.2.3 主机系统安全

7.2.3.1 系统加固

具体要求如下：

遵守 7.1.3.1 系统加固要求。

7.2.3.2 准入控制

具体要求如下：

a) 对煤矿生产信息系统、信息化系统的访问账户设置细粒度的访问控制权限，使用最小特权，实现账户权限分离；

b) 煤矿生产信息系统、信息化系统应具备登录控制、登录错误锁定、连接超时退出等技术措施；

c) 应对系统访问源严格执行准入认证机制，仅允许已授权的主体访问；

d) 系统生产厂商或其他外部人员，非安全或未经过认证的远程工具不能连接内部系统及设备。

7.2.3.3 漏洞管理

具体要求如下：

a) 以45 d为检测周期，对煤矿生产信息系统、信息化系统开展系统漏洞专项检查，并做好安全评估及整改工作；

b) 及时关注官方发布的与系统软、硬件相关的漏洞，及时追踪补丁信息，并一定时间内（原则上不超过3 d）完成补丁修复；涉及煤矿生产信息系统在补丁修复前，应在模拟环境运行测试，验证补

丁安全和稳定性。

7.2.3.4 操作审计

具体要求如下：

遵守 7.1.3.3 操作审计要求。

7.2.3.5 集中管理

具体要求如下：

遵守 7.1.3.4 集中管理要求，并增加：

应通过身份认证、授权、管理等操作实现系统流程化的管控和运维，并对操作过程留有审计记录。

7.2.4 应用程序安全

7.2.4.1 应用识别

具体要求如下：

遵守 7.1.4.1 应用识别要求。

7.2.4.2 应用访问

具体要求如下：

遵守 7.1.4.2 应用访问要求，并增加：

应采用 RBAC、ABAC、PAM 实现对应用的权限分配管理。

7.2.4.3 应用防护

应部署应用安全防护、防篡改和审计类设备，实现常规攻击的防护、检测与审计。

7.2.4.4 应用审计

具体要求如下：

遵守 7.1.4.4 应用审计要求。

7.2.4.5 应用评估

具体要求如下：

a) 以 45 d 为检测周期，对应用程序开展漏洞专项检查，并做好安全评估及整改工作；

b) 在新应用投入使用前，应进行业务功能和安全漏洞的测试，确认在无安全隐患的前提下，才能上线使用。

7.2.5 数据安全治理

7.2.5.1 数据采集

具体要求如下：

a) 明确数据采集目的、数据类型、存储期限及共享范围，对敏感个人信息（生物识别、健康信息），需用户主动勾选同意；

b) 采集煤矿生产信息系统、PII财务数据、商业秘密，需严格限制采集范围和权限，仅收集与业务功能直接相关的最小数据集。

7.2.5.2 数据传输

具体要求如下：

a） 建立数据通信加密隧道，提供端到端的加密服务，防止数据明文泄露；

b） 使用TLS证书（由可信CA签发）验证通信双方身份，防止中间人攻击。

7.2.5.3 数据备份

具体要求如下：

a） 根据数据敏感性和业务重要性（核心业务数据、用户隐私数据）划分备份优先级；

b） 数据备份应采用3-2-1备份规则：3份数据、2种介质、1份异地；

c） 对煤矿生产信息系统、信息化系统的关键数据保存时长不少于180 d。

7.3 高级防护要求

7.3.1 物理环境安全

7.3.1.1 场地选择

具体要求如下：

遵守 7.1.1.1 场地选择要求。

7.3.1.2 防破坏、盗窃

具体要求如下：

遵守 7.1.1.2 防破坏、盗窃要求，并增加：

对机房采取设备固定、安装防盗报警系统等措施。

7.3.1.3 防水、防静电、防雷击

具体要求如下：

遵守 7.1.1.3 防水、防静电、防雷击要求。

7.3.1.4 供电系统

具体要求如下：

遵守 7.1.1.4 供电系统要求，并增加：

机房应配备足够容量的 UPS 系统，为设备提供不少于 4 h 的应急电力支持。

7.3.1.5 火灾报警及消防

具体要求如下：

遵守 7.1.1.5 火灾报警及消防要求，并增加：

应在机房地板、吊顶、空调管道及易燃物附近设有烟、温感探测器。

7.3.1.6 温、湿度控制

具体要求如下：

遵守 7.1.1.6 温、湿度控制要求。

7.3.1.7 电磁防护

具体要求如下：

遵守 7.2.1.7 电磁防护要求。

7.3.1.8 防静电

具体要求如下：

遵守 7.2.1.8 防静电要求。

7.3.1.9 内部装修

具体要求如下：

遵守 7.2.1.9 内部装修要求。

7.3.2 通信网络安全

7.3.2.1 架构设计

具体要求如下：

遵守 7.1.2.1 架构设计要求，并增加：

应提供关键通信线路、主机设备、网络设备、控制组件的冗余，保证业务的高可靠性。

7.3.2.2 安全分区

具体要求如下：

遵守 7.1.2.2 安全分区要求。

7.3.2.3 边界防护

具体要求如下：

a） 应对系统和网络边界部署行为管理类、准入类设备，能够对常规的攻击行为拦截并告警，对内外部网络连接、请求行为进行监管；

b） 应在工控网与企业网之间应采用物理隔离技术手段，不准许不同网络大区之间非安全互联互通。

7.3.2.4 安全监测

具体要求如下：

遵守 7.1.2.4 安全监测要求，并增加：

应具备对高级威胁检测，威胁情报等分析识别检测的能力。

7.3.2.5 通信传输

具体要求如下：

遵守 7.2.2.5 通信传输要求。

7.3.3 主机系统安全

7.3.3.1 系统加固

具体要求如下：

遵守 7.1.3.1 系统加固要求。

7.3.3.2 准入控制

具体要求如下：

遵守 7.2.3.2 准入控制要求，并增加：

远程访问应建立身份鉴别、认证、授权、审计等流程化访问流程，接入账户实行专人专号，定期审计接入账户操作记录。

7.3.3.3 漏洞管理

具体要求如下：

a) 以30 d为检测周期，对煤矿生产信息系统、信息化系统开展系统漏洞专项检查，并做好安全评估及整改工作；

b) 及时关注官方发布的与系统软、硬件相关的漏洞，及时追踪补丁信息，并一定时间内（原则上不超过3 d）完成补丁修复；涉及煤矿生产信息系统在补丁修复前，应在模拟环境运行测试，验证补丁安全和稳定性。

7.3.3.4 操作审计

具体要求如下：

遵守 7.1.3.3 操作审计要求。

7.3.3.5 集中管理

具体要求如下：

遵守 7.1.3.4 集中管理要求，并增加：

a) 应通过身份认证、授权、管理等操作实现系统流程化的管控和运维，并对操作过程留有审计记录；

b) 应能够对业务安全告警及流量数据风险可视化，关联预测，实现统一分析与运营。

7.3.4 应用程序安全

7.3.4.1 应用识别

具体要求如下：

遵守 7.1.4.1 应用识别要求。

7.3.4.2 应用访问

具体要求如下：

遵守 7.1.4.2 应用访问要求，并增加：

应采用 RBAC、ABAC、PAM 实现对应用的权限分配管理。

7.3.4.3 应用防护

具体要求如下：

遵守 7.2.4.3 应用防护要求。

7.3.4.4 应用审计

具体要求如下：

遵守 7.1.4.4 应用审计要求。

7.3.4.5 应用评估

具体要求如下：

a） 以30 d为检测周期，对应用程序开展漏洞专项检查，并做好安全评估及整改工作；
b） 在新应用投入使用前，应进行业务功能和安全漏洞的测试，确认在无安全隐患的前提下，才能上线使用。

7.3.5 数据安全治理

7.3.5.1 数据采集

具体要求如下：
遵守 7.2.5.1 数据采集要求。

7.3.5.2 数据传输

具体要求如下：
遵守 7.2.5.2 数据传输要求，并增加：
a） 使用AES-GCM、ECDHE密钥交换，避免RC4、DES等弱加密算法；
b） 传输前后对数据计算哈希值，对比确保请求来源可信；
c） 可通过DLP系统监控证件号、手机号等敏感数据的传输。

7.3.5.3 数据备份

具体要求如下：
遵守 7.2.5.3 数据备份要求。

7.3.5.4 数据销毁

采用逻辑或物理销毁手段，确保数据被彻底、不可逆删除。

8 安全管理要求

8.1 组织机构

具体要求如下：
a） 应设立网络安全管理组织或机构，负责日常的网络安全组织管理和协调监督；
b） 应设立网络安全领导小组，企业负责人为网络安全第一责任人，落实煤矿生产信息系统、信息化系统专责人的网络安全责任，贯彻“谁主管谁负责、谁运营谁负责”的原则。

8.2 岗位人员

具体要求如下：
a） 网络安全组织或机构应设立职能岗位，并在各个岗位配备有一定技术积累的技术人员；
b） 应建立内部、外部人员对煤矿生产信息系统、信息化系统访问制度或规范，签订保密协议；
c） 应建立网络安全人员入岗、在岗、离岗等规章制度和流程；
d） 应定期对在岗人员开展网络安全技能和意识培训，并制定培训管理考核办法。

8.3 制度规范

具体要求如下：
a） 应建立人员管理、资产管理、运维管理、设备管理、机房管理、应急管理、变更管理、事件管理和培训教育的制度或规范；

b） 应由特定人员定期对安全管理制度或规范进行制定、发布和更新。

8.4 安全建设

8.4.1 选择服务商

具体要求如下：

a） 煤矿生产信息系统、信息化系统建设维护部门选用的软、硬件系统及专用网络安全设备，应优先选用国产化；

b） 在开展网络规划、安全建设、安全运维和安全评估时，宜优先考虑有类似项目经验的服务商，并要求提供安全合同、业绩案例、验收报告等证明材料；

c） 与服务商签订保密协议，明确各方应履行的网络安全责任和义务。

8.4.2 系统软件开发管理

具体要求如下：

a） 将安全融入开发流程，明确功能外的网络安全需求，在架构设计、编码规范、安全配置等进行合理的优化；

b） 新系统软件应对其进行风险评估、漏洞扫描等系统性的安全测试，确保系统功能和安全不存在隐患的前提下，才能正式投入使用；

c） 与开发人员签订保密协议，对开发过程中涉及的系统信息、软件资源、源代码等进行保密；系统建设部门应及时回收各类管理权限，并将开发记录归档。

8.4.3 项目验收与交付

具体要求如下：

a） 确认网络安全信息化项目成果与技术指标要求的完成情况，并作为验收的前提条件；

b） 对项目核心交付文档内容进行确认、清查盘点，并组织专家审核，规范项目验收流程，直至项目完全验收合格。

8.4.4 等级保护建设管理

具体要求如下：

a） 应按照监管部门要求，对部分煤矿生产信息系统、信息化系统开展系统等级保护建设，完成系统定级、备案、建设、测评和监督审查流程；

b） 已定级备案的煤矿生产信息系统、信息化系统，应开展对应安全防护能力的复测，三级系统1次/年、二级系统1次/2年，不符合等级保护标准要求的，应及时整改。

8.5 安全维护

8.5.1 运维环境管理

具体要求如下：

a） 机房应划分核心区、操作区，进入运维场地提前申请报备、登记，严格限制非授权人员进入；

b） 定义运维角色，实现账户与权限分离，临时权限申请应审批并设置自动回收时间；

c） 划分VLAN隔离不同网段，不准许跨网段直接通信；

d） 运维操作应经过身份识别、认证授权、单点登录，并记录运维过程中操作记录与指令日志；

e） 第三方运维人员应签署保密协议，操作受内部审计；

f） 运维环境应保持整齐清洁，并具备对风量、温度、湿度、洁净度等各种性能指标检测手段。

8.5.2 存储介质管控

具体要求如下：

a） 对移动存储介质分类标识(绝密、机密、内部、公开)，识别其用途与敏感级别(如标注机密级—财务数据)；

b） 敏感介质存放于带锁柜体或保险箱，仅授权人员可接触；

c） 新介质入库时应登记编号、型号、密级，并初始化加密；

d） 定期检测移动介质健康状态，进行可读性验证；

e） 移动存储介质实行专网专用，不准许在工控网、企业网交叉使用；

f） 在移动介质接入前开展病毒查杀，检测交换传输内容的安全状态。

8.5.3 恶意代码防范

具体要求如下：

a） 区分恶意代码类别及传播途径(病毒——邮件附件、U盘，蠕虫——网络共享、系统漏洞)；

b） 通过部署安全设备、防护软件或采用白名单安全防护模式，实现网络或终端设备的安全防护；

c） 已运行的恶意代码，应详细记录受灾时间、受灾位置、代码种类、具体功能、破坏情况等，并对受灾区域第一时间进行隔离；

d） 强化人员安全意识，不准许点击未知链接、恶意附件、钓鱼邮件。

8.5.4 网络事件处置

具体要求如下：

a） 建立网络和系统的安全事件识别评估、分析上报、处理响应流程，在出现网络安全事件后，及时隔离受影响的系统或网络，并进行取证分析，追踪事件来源，形成事件处理报告；

b） 建立安全设备之间的协同处理机制，实现安全事件自动化分析研判、响应和处理。

8.5.5 变更规范管理

具体要求如下：

a） 制定网络安全变更规范，形成变更闭环，确保变更操作能够有效跟踪和控制；

b） 对重大变更或影响系统稳定性的变更，进行充分的风险评估和测试，保障变更操作的安全性；

c） 在变更操作引发问题时，应立即采取回滚措施，将系统恢复到变更前的状态；

d） 对变更操作进行详细记录，包括变更内容、变更责任人、变更时间、变更结果等信息，便于后续跟踪和审计。

8.5.6 备份恢复管理

具体要求如下：

a） 制定完整的备份恢复计划，定期对关键业务数据进行备份，并进行备份数据恢复测试；

b） 通过技术和管理手段加强数据备份介质的安全管控。

9 安全运营要求

9.1 资产识别管理

具体要求如下：

a） 建立硬件资产、软件资产、数据资产、服务资产、人员资产及影子资产的分类分级、标识管理，确保资产看得见、理得清、管得住；
b） 定期对资产开展安全巡检和评估，审计资产使用记录、运行状态等，确保资产可核查，关停和下线无效或不在网资产；
c） 当涉及资产信息变更时，应及时更新资产清单。

9.2 漏洞检测

具体要求如下：
a） 通过安全评估工具对煤矿生产信息系统、信息化系统开展周期性的安全检测，识别目标系统存在的漏洞，并出具漏洞评估及验证报告；
b） 检测周期为：关键系统1次/30 d，重要系统1次/45 d，一般系统1次/60 d。

9.3 风险评估

具体要求如下：
a） 定期对煤矿生产信息系统、信息化系统组织网络安全风险评估，从评估目标、范围、工作计划、依据、内容、结果等方面建立评估流程，完善评估方案；
b） 建立硬件资产、软件资产、数据资产、服务资产、人员资产及影子资产清单；
c） 通过物理环境、软硬件故障、人为操作、网络攻击、管理制度识别煤矿生产信息系统、信息化系统面临的威胁名称、种类、来源、动机及出现的频率等，形成威胁列表；
d） 从安全技术、安全管理与安全运营等方面，识别煤矿生产信息系统、信息化系统面临的威胁和可能被利用的弱点，形成脆弱性列表；
e） 对煤矿生产信息系统、信息化系统安全防护措施进行识别确认，包括设备名称、设备类型、设备功能、安全规则、运行策略及实施效果等，形成安全措施清单；
f） 可使用扫描工具、渗透测试工具、安全审计工具、拓扑发现工具等作为煤矿生产信息系统、信息化系统风险评估过程中的辅助手段。

9.4 渗透测试

具体要求如下：
a） 签署授权协议，利用非破坏性质的测试手段对煤矿生产信息系统、信息化系统进行攻击测试，确定漏洞情况，测试内容至少包含OWASP Top 10漏洞类别；
b） 应包含信息收集、漏洞探测、漏洞验证、权限提升、内网渗透、信息整理、痕迹清理、输出报告等步骤；
c） 涉及煤矿生产信息系统的渗透测试，优先提供仿真测试环境，避免与测试目标直连，对系统业务产生影响；
d） 与渗透人员签订保密协议，不应向第三方及社会公众披露与企业煤矿生产信息系统、信息化系统的网络架构、业务数据、安全漏洞等相关信息。

9.5 脆弱性加固

具体要求如下：
a） 对操作系统的加固：文件权限、人员登录、口令设置、登录策略、共享设置、环境变量、日志配置、端口服务等；
b） 对应用程序的加固：口令强度及更改周期、目录和文件访问权限、IP连接、超时限制、加密设置、日志配置等；

c） 对网络通信设备的加固：账号权限、口令策略、登录策略、VLAN、端口服务、系统日志等；
d） 对安全设备的加固：账号权限、口令策略、访问策略、日志配置、管理IP、规则更新等；
e） 对工控设备的加固：服务端口、网卡配置等；
f） 对数据库的加固：口令策略、管理IP、审核策略、日志配置、连接超时等。

9.6 安全培训教育

具体要求如下：

a） 平衡各部门、岗位人员具体网络安全需求，制定月度、季度、年度的网络安全培训计划；
b） 基于岗位人员基本需求，开展法律法规、安全技术、岗位操作规程的培训，并对培训内容和结果记录归档；
c） 设立培训考核机制，明确网络安全奖励与违规处罚机制，不应无故缺席。

9.7 攻防演练

具体要求如下：

a） 为保障煤矿生产信息系统、信息化系统及运营网络的安全稳定，每年应最少开展一次网络安全攻防演习活动，对演练过程中发现的网络问题及时整改处置，确保安全隐患及时清零；
b） 应制定网络安全应急管理预案，完善应急处理机制保障应急渠道，在关键时间节点及重要敏感时期应安排人员实行7×24 h值守。

附 录 A
（资料性）
煤矿生产企业网络安全防护示意图

结合煤矿生产企业不同级别系统防护能力的要求，采用分层和分区的设计理念，将煤矿生产企业的网络分为多个逻辑区域，每个区域配备相应的安全防护设备，覆盖网络边界、终端、系统、数据、应用等多个领域，形成多层次、多维度的安全防护体系，见图A.1。

图A.1 煤矿生产企业网络安全防护示意图

附 录 B
（资料性）
安全防护设备部署清单

基于防护示意图，对不同网络区域内的各类安全防护设备、其部署位置、单位数量以及防护等级进行说明阐述，见表B.1。

表 B.1 设备部署表

序号	网络	设备名称	部署区域	单位	数量（仅参考）	防护等级		
						初级	中级	高级
1	工控网	工业防火墙	调度中心区	台	1	☑	☑	☑
2		工业主机加固		套	1	☑	☑	☑
3		网络准入系统		台	1		☑	☑
4		工业防火墙	业务通信环网区（井上、井下）	台	2	☑	☑	☑
5		工控安全审计		台	1	☑	☑	☑
6		工业主机加固		套	1	☑	☑	☑
7		工业防火墙	安全监测环网区	台	1	☑	☑	☑
8		工控安全审计		台	1	☑	☑	☑
9		工业主机加固		套	1	☑	☑	☑
10		工业防火墙	视频环网区	台	1	☑	☑	☑
11		主机安全加固		套	1	☑	☑	☑
12		视频安全防护		台	1	建议	建议	建议
13		工业防火墙	专线接入区	台	1	☑	☑	☑
14		应用防火墙	数据应用区	台	1	☑	☑	☑
15		工业主机加固		套	1	☑	☑	☑
16		云防护系统		套	1		☑	☑
17		下一代防火墙	物联网接入区	台	1	☑	☑	☑
18		网络准入系统		台	1		☑	☑
19		运维审计系统	安全运维管理区	台	1		☑	☑
20		工控入侵检测		台	1	☑	☑	☑
21		工控漏洞扫描		台	1			☑
22		高级威胁检测		台	1	建议	建议	建议
23		外设管理系统		台	1			☑
24		工控日志审计		台	1	☑	☑	☑
25		数据库审计		台	1		☑	☑
26		数据备份系统		台	1	☑	☑	☑

表 B.1　设备部署表（续）

序号	网络	设备名称	部署区域	单位	数量（仅参考）	防护等级		
						初级	中级	高级
27	工控网	集中安全平台	安全运维管理区	台	1	☑	☑	☑
28		工业态势感知		台	1			☑
29		安全隔离网闸	隔离区	台	1	☑	☑	☑
30	企业网	网络准入系统	办公区	台	1		☑	☑
31		终端防护系统		套	1	☑	☑	☑
32		无线安全网关		台	1			☑
33		下一代防火墙	外联区	台	1	☑	☑	☑
34		入侵防御系统		台	1	☑	☑	☑
35		DDoS防御系统		台	1			☑
36		负载均衡系统		台	1	建议	建议	建议
37		上网行为管理		台	1		☑	☑
38		网络诱捕系统		台	1	建议	建议	建议
39		应用防火墙	DMZ区	台	1	☑	☑	☑
40		防篡改系统		套	1		☑	☑
41		邮件安全网关		台	1	建议	建议	建议
42		应用防火墙	数据应用区	台	1	☑	☑	☑
43		数据库防火墙		台	1	建议	建议	建议
44		DLP系统		台	1	建议	建议	建议
45		防篡改系统		套	1		☑	☑
46		数据安全管理平台		台	1	建议	建议	建议
47		数据库安全评估		台	1			☑
48		云防护系统		套	1		☑	☑
49		下一代防火墙	专线接入区	台	1	☑	☑	☑
50		下一代防火墙	物联网接入区	台	1	☑	☑	☑
51		网络准入系统		台	1		☑	☑
52		运维审计系统	安全运维管理区	台	1		☑	☑
53		入侵检测系统		台	1	☑	☑	☑
54		漏洞扫描系统		台	1		☑	☑
55		高级威胁检测		台	1	建议	建议	建议
56		外设管理系统		台	1			☑
57		日志审计系统		台	1	☑	☑	☑

表 B.1　设备部署表（续）

序号	网络	设备名称	部署区域	单位	数量（仅参考）	防护等级		
						初级	中级	高级
58	企业网	数据库审计	安全运维管理区	台	1		☑	☑
59		数据备份系统		台	1	☑	☑	☑
60		安全态势感知		台	1			☑

附 录 C
（资料性）
设备功能简述

C.1 工控网络区

C.1.1 工业防火墙

通过工控威胁特征识别、工业协议深度解析与可信白名单技术，完整检测数据包内容，及时阻断对工控系统网络攻击、非法操作和恶意破坏行为，为煤矿生产信息系统构建安全可信的运行环境。

C.1.2 工控安全审计

通过深度解析工控协议，黑白名单学习、自定义规则等，实时采集识别、分析动态监测网络中访问违规、异常流量和未知设备接入行为，记录网络会话和安全事件，为事后取证分析提供审计依据。

C.1.3 工业主机加固

通过白名单一键固化，全盘扫描可执行程序形成白名单库，实现对未知病毒和网络攻击免疫，结合身份认证、进程管理、移动存储设备管理等功能，为煤矿工控网工程师站、操作员站构建安全“白环境”。

C.1.4 视频安全防护

通过主动检查视频监控网络各级节点的链路状态，建立设备准入认证机制，及时发现非法接入的未知、违规、仿冒设备，并对接入及入侵攻击进行实时防护，告警和阻断。

C.1.5 网络准入系统

通过IP、802.1x细粒度的准入控制技术，能够对接入网络的设备进行严格管控，实现入网注册认证，解决“接入不可知、外联不可控、行为不可管”的问题，确保受信任的设备才能够接入到网络。

C.1.6 云防护系统

通过虚拟化微隔离防护技术，对云环境的安全状态实时分析监控，为企业云主机、云应用、云数据提供全面的安全运营解决方案，实现立体化的防护，保证虚拟化业务的安全稳定。

C.1.7 工控入侵检测

通过网络流量精准识别OPC、GOOSE、SV、IEC 104、MODBUS、DNP3等主流工控协议指纹特征，对未经授权访问、恶意软件、漏洞利用等异常活动过程有效检测，为事后取证溯源提供审查依据。

C.1.8 运维审计系统

通过单点登录、账号管理、身份认证、资源授权、访问控制和操作审计于一体，实现运维过程的“事前预防、事中控制、事后审计”运维目标，在简化运维操作的同时，提升运维管理水平。

C.1.9 工控漏洞扫描

集成工控漏洞检测规则，对SCADA、PLC、DCS、组态软件、HMI等多种工控系统开展漏洞评估，准确定位系统中存在的弱点，提供全面的安全检测报告，协助修补漏洞，提升工控系统的安全性。

C.1.10 高级威胁检测

通过威胁情报、行为模型、机器学习、虚拟沙箱和安全特征库等检测技术，对网络入侵、隐蔽信道、0day漏洞、变种病毒的APT攻击威胁提供检测关联、溯源手段，助力构筑安全、可信的网络环境。

C.1.11 外设管理系统

通过白名单接入管控机制，提供对移动存储设备使用前的病毒扫描、查杀与隔离，使用过程中的读写权限管控，使用后的文件操作日志审计，阻断病毒传播途径。

C.1.12 工控日志审计

对应用服务器、通信设备、安全设备、工控设备等所产生的运行日志、安全日志、操作日志等进行全面的标准化处理，存储、监控、审计、分析和响应，满足日志审计存储要求。

C.1.13 应用防火墙

通过识别SQL注入、XSS、Webshell上传、命令注入、非授权访问、爬虫防护等攻击类型，形成事前检查、事中防护、事后取证的安全流程，避免应用系统被恶意攻击入侵，保障安全稳定运行。

C.1.14 数据库审计

基于数据协议分析和SQL语言解析技术，实现对数据库访问行为的全程监控，高危操作的实时告警和安全事件的审计追溯，定位数据安全事件原因，生成合规报告，提高数据安全。

C.1.15 数据备份系统

通过设定备份计划，指定备份文件或目录并将其备份，防止原始数据丢失、损坏或被意外删除时，能够及时恢复数据，保护重要数据免受数据丢失。

C.1.16 集中安全平台

对工业防火墙、工控安全审计、主机加固系统等进行统一管理、配置、授权和响应，打破安全孤岛，解决设备各自运维而导致的信息不畅和事件处置效率低下的问题。

C.1.17 工业态势感知

通过采集煤矿工控网的设备资产、网络流量、安全事件、运行状态、网络拓扑等基础信息，全面监控工控网络攻击、系统/软件漏洞、木马和恶意代码的攻击行为，展现工控网可视化的安全风险和态势。

C.1.18 安全隔离网闸

在不同网络大区之间能够对信息流进行剥离还原重组，通过内容过滤、病毒查杀、安全审计等安全功能，实现两网间安全隔离和数据摆渡，完成数据、文件、视频的同步交换。

C.2 企业网络区

C.2.1 下一代防火墙

在传统防火墙功能的基础上，通过应用程序识别、身份验证、VPN、内容过滤等，深度检测阻断恶意网络流量，提供高级威胁防护功能，确保网络边界安全。

C.2.2 应用防火墙

通过识别SQL注入、XSS、Webshell上传、命令注入、非授权访问、爬虫防护等攻击类型，形成事前检查、事中防护、事后取证的安全流程，避免应用系统被恶意攻击入侵，保障安全稳定运行。

C.2.3 入侵防御系统

作为防火墙的补充，对漏洞利用攻击、蠕虫病毒、木马后门、溢出攻击、暴力破解等多种攻击行为防御，弥补网络层防护深层防御效果的不足，实现更深层级的防护。

C.2.4 DDoS防御系统

对SYN Flood、UDP Flood、ICMP Flood、IGMP Flood、ACK Flood等流量型攻击行为有效识别，并进行阻断，保障业务系统高可用。

C.2.5 云防护系统

通过虚拟化微隔离防护技术，对云环境的安全状态实时分析监控，为云主机、云应用、云数据提供全面的安全运营解决方案，实现立体化的防护，保证虚拟化业务的安全稳定。

C.2.6 无线安全网关

监测和控制无线网络传输的数据流量，检测潜在的安全威胁，阻止非授权用户访问无线网络、保护企业、组织和个人安全隐私。

C.2.7 上网行为管理

通过应用识别、应用控制、行为审计、身份认证、流量控制、网络业务优化等，控制和管理用户对互联网的使用，并为访问事后的审计和分析提供溯源手段。

C.2.8 终端防护系统

通过病毒查杀、网络管控、入侵防护、威胁响应、补丁管理、配置加固、威胁可视化等，有效防御各类对终端、服务器的威胁攻击行为，保障终端、服务器的安全。

C.2.9 网络准入系统

通过IP、802.1x细粒度的准入控制技术，能够对接入网络的设备进行严格管控，实现入网注册认证，解决“接入不可知、外联不可控、行为不可管”的问题，确保受信任的设备才能够接入到网络。

C.2.10 负载均衡系统

通过将网络流量、数据请求、计算任务等分配到多台服务器之间均衡地分配处理，以便优化性能、提

高可靠性和增加可扩展性，避免单个服务器过载或故障导致的业务中断。

C.2.11 网络诱捕系统

通过提供与数据库、HTTP、FTP、SSH等与真正业务系统非常类似的服务，内置多种易被攻击工具识别安全漏洞，吸引黑客攻击，记录交互过程，还原攻击手段，并进行统一分析和处理。

C.2.12 防篡改系统

通过文件过滤驱动技术在事前阻止黑客对HTML代码、文本内容、媒体文件等的篡改，并在事中及时发送安全告警，保障网站和网页内容的安全和完整性。

C.2.13 邮件安全网关

通过对邮件内容深度检测，识别钓鱼邮件、病毒邮件、垃圾邮件内容并精准防护；此外，通过邮件白黑名单机制，实现对邮件外发自动加解密，确保敏感数据在可信范围内流转，防止核心数据外泄。

C.2.14 数据库防火墙

通过分析数据库通信协议中的SQL语句和语法特征，检测恶意行为、非授权访问敏感信息等，实时阻断和告警，避免数据库遭恶意访问，保障敏感数据不被外泄或窃取。

C.2.15 DLP系统

通过指纹识别、图像识别、关键字、数据标识符等对静态数据、动态数据、使用中的数据进行安全识别、监控和防护，对信息泄露事件做到事前预防、事中审计和事后溯源取证追责，保护数据资产安全。

C.2.16 数据安全管理平台

利用系统建模方法和大数据分析，对数据归集、处理、共享、交换场景下的数据风险进行全域治理和合规监管，对发现的数据安全风险进行及时预警和通报，建立数据动态流动的安全管控机制。

C.2.17 数据安全评估

及时发现数据库安全配置、风险代码、弱口令等问题，完成对数据安全动态评估，并提供数据安全状况监测评估报告，提升数据安全状态。

C.2.18 运维审计系统

通过单点登录、账号管理、身份认证、资源授权、访问控制和操作审计于一体，实现运维过程的“事前预防、事中控制、事后审计”运维目标，在简化运维操作的同时，提升运维管理水平。

C.2.19 入侵检测系统

基于攻击特征、行为基线、机器学习等技术手段，精确检测网络异常流量、用户行为和设备运行状态等信息，及时发现识别异常网络攻击行为，为事后提供调查和溯源依据。

C.2.20 漏洞扫描系统

针对主机系统、WEB应用、数据库进行扫描，发现漏洞后提供漏洞说明、漏洞影响、漏洞验证和漏洞修复建议等，并采取相应的措施加固整改，防患于未然。

C.2.21 日志审计系统

对应用服务器、通信设备、安全设备等所产生的运行日志、安全日志、操作日志等进行全面的标准化处理，存储、监控、审计、分析和响应，满足日志审计存储要求。

C.2.22 数据库审计

基于数据协议分析和SQL语言解析技术，实现对数据库访问行为的全程监控，高危操作的实时告警和安全事件的审计追溯，定位数据安全事件原因，生成合规报告，提高数据安全。

C.2.23 数据备份系统

通过设定备份计划，指定备份文件或目录并将其备份，防止原始数据丢失、损坏或被意外删除时，能够及时恢复数据，保护重要数据免受数据丢失。

C.2.24 高级威胁检测

通过威胁情报、行为模型、机器学习、虚拟沙箱和安全特征库等检测技术，对网络入侵、隐蔽信道、0day漏洞、变种病毒的APT攻击威胁提供检测关联、溯源手段，助力构筑安全、可信的网络环境。

C.2.25 外设管理系统

通过白名单接入管控机制，提供对移动存储设备使用前的病毒扫描、查杀与隔离，使用过程中的读写权限管控，使用后的文件操作日志审计，阻断病毒传播途径。

C.2.26 安全态势感知

通过网络流量、大数据、威胁情报、智能分析技术等，深度挖掘、采集和分析网络日志和安全信息，呈现以资产、事件、威胁、时间、空间、业务行为等多个维度的网络安全态势，并全方位地感知预测。

附 录 D
（资料性）
煤矿系统评审表

按煤矿生产信息系统、信息化系统被攻击后的影响范围及程度，遵循自主确认其系统等级，并组织专家开展系统定级评审的原则，形成系统评级认定表（表D.1）、系统评级专家意见表（表D.2），便于辅助系统定级落地。

表 D.1 系统评级认定表

年 月 日

企业名称	系统名称	系统类别	系统描述	主管部门	负责人/联系方式	职称/职务	被攻击影响对象范围及程度	部门拟定等级

表 D.2 系统评级专家意见表

年 月 日

企业名称				
注册地址				
煤矿智能化建设等级				
基本信息				
系统名称	系统类别	系统描述	被攻击影响对象范围及程度	部门拟定等级
专家评审				
单位名称	职称/职务	姓名/联系方式	评审意见	最终等级

参 考 文 献

[1] GB/T 20984—2022 信息安全技术 信息安全风险评估方法
[2] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[3] GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南
[4] GB/T 25069—2022 信息安全技术 术语
[5] 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
[6] GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求
[7] GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南
[8] GB/T 34679—2017 智慧矿山信息系统通用技术规范
[9] GB/T 36323—2018 信息安全技术 工业控制系统安全管理基本要求
[10] GB/T 36324—2018 信息安全技术 工业控制系统信息安全分级规范
[11] GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求
[12] GB/T 41400—2022 信息安全技术 工业控制系统信息安全防护能力成熟度模型
[13] GB/T 41479—2022 信息安全技术 网络数据处理安全要求
[14] GB 50215—2015 煤炭工业矿井设计规范
[15] GB/T 51272—2018 煤炭工业智能化矿井设计标准
[16] 智能化示范煤矿验收管理办法(试行)(国能发煤炭规〔2021〕69号)

中国煤炭工业协会
团 体 标 准
智能化煤矿网络安全技术要求
T/CNCA 109—2025

*

中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲2号(100029)

网址 www.spc.net.cn
总编室:(010)68533533　发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230　1/16　印张 2.25　字数 54 千字
2025年7月第1版　2025年7月第1次印刷

*

书号:155066·5-15546　定价　59.00 元