

# 基于 5G+智慧矿山行业应用全场景一站式安全评估体系研究与应用

张育慧,郝力群,王文静,李天松,刘 博

(中国移动通信集团内蒙古有限公司,内蒙古 呼和浩特 010020)

**摘要:**当前全球网络安全形势极其严峻复杂,工业企业互联网频繁遭受到黑客攻击、勒索,甚至发生服务中断、停产等严重安全事故。随着 5G+垂直行业应用的快速发展,垂直行业信息化发展驶入快车道,但智慧矿山等垂直行业应用场景下的安全风险评估工作相对滞后,在缺少行业应用安全基线、安全管理制度体系及安全风险评估最佳实践的情况下,5G+智慧矿山行业应用保障能力分散,传统风险与不可靠的边缘环境风险叠加,面临的网络安全风险更加复杂。本文面向 5G+智慧矿山行业应用,通过建立安全评估框架、细化安全评估指标、梳理安全评估流程、整合安全评估工具,构建“全场景、一站式”的安全评估体系。同时针对井工矿和露天矿两大矿业类型的九大类典型业务场景开展安全评估实践,为 5G+智慧矿山行业安全稳定运营、高质量发展提供坚实的基础和保障。

**关键词:**5G+智慧矿山;风险识别;安全评估;行业应用安全

**中图分类号:**TP311

**文献标识码:**A

**文章编号:**2096-9759(2023)06-0205-07

## 1 引言

当前网络安全形势极其严峻,工业企业互联网频繁遭受到黑客的攻击和勒索,甚至发生服务中断、停产等严重安全事故。但随着 5G+智慧行业应用的快速发展,智慧矿山等垂直行业应用场景下的安全风险评估工作相对滞后,在缺少行业应用安全基线、安全管理制度及安全风险评估最佳实践的情况下,5G+智慧矿山行业应用保障能力分散,传统风险与不可靠的边缘环境风险叠加,面临的网络安全风险更加复杂。

本文围绕 5G+智慧矿山行业应用业务场景和特点,深入分析行业应用现状和安全需求,使用威胁建模方法识别安全风险,建立面向 5G+智慧矿山行业应用的安全评估框架、安全评估指标、安全评估流程,整合多个自研、商用和开源安全检测工具,构建“全场景、一站式”的安全评估体系。遵循该评估体系,按照评估流程,推动将安全评估服务嵌入到业务的全生命周期,为 5G 业务安全运行提供安全需求分析、基础设施安全、安全应用开发及测试及系统上线后的持续化安全评估与漏洞闭环管理,为 5G+智慧矿山行业安全稳定运营、高质量发展提供坚实的基础和保障。

## 2 5G+智慧矿山行业应用现状及安全需求分析

### 2.1 5G+智慧矿山行业现状

(1)内蒙古矿山产业规模巨大,战略意义重大

中国矿产资源丰富,占全球矿业总产值的 17%,排名第一。其中煤炭资源分为内蒙古、山西、陕西、新疆四大煤炭生产区,占全国煤炭产量 81.2%。

2020 年,中国煤炭产量达到 38.4 亿吨,其中内蒙古煤炭产量 10.06 亿吨,占全国煤炭总产量的四分之一,创内蒙古煤炭生产历史新高。内蒙古现有煤矿 532 座,生产矿井 516 座,规模 12.27 亿吨/年,申请核准煤矿 16 处、规模 1.09 亿吨/年,其中井工矿 276 座,规模 6.48 亿吨/年,露天矿 241 座,规模 5.79 亿吨/年。

(2)国家高度重视,持续推进矿山行业智能化水平不断发展

2020 年 3 月 2 日,八部委联合印发《关于推进煤矿智能化发展的指导意见》,强调推广新一代信息技术应用,分级建设

智能化平台。

2020 年 5 月,内蒙古自治区能源局等部门联合印发《关于加快煤矿智能化发展的指导意见》提出要促进煤炭工业高质量发展,提升我区煤矿智能化水平,圈地 34 家智能化建设项目清单。

2020 年 6 月,内蒙古自治区九部门联合印发了《关于加快全区煤矿智能化建设的实施意见》,提出到 2021 年,建成 50 个智能工作面。

2020 年 12 月,国家能源局、国家煤矿安全监察局发布《关于开展首批智能化示范煤矿建设的通知》,提出审核确定内蒙古乌海能源老石旦煤矿等 71 处煤矿,作为国家首批智能化示范建设煤矿,内蒙古自治区内占 12 座。

2021 年 1 月,内蒙古自治区能源局发布《内蒙古自治区推进煤矿智能化建设三年行动实施方案》,提出 2023 年 12 月底前,所有正常生产煤矿全部实现智能化,全面完成智能化建设三年行动工作任务。

(3)智慧矿山等行业应用面临着新的挑战

随着信息化、智能化与行业应用的不断融合,黑客的攻击和勒索频繁发生,重要工控系统极易被破坏发生服务中断、信息泄露等严重的网络安全事件,网络安全形势极其严峻,智慧矿山等行业应用面临新的安全挑战。

### 2.2 安全需求分析

随着 5G+垂直行业应用的发展,单一主体网络向多主体网络转变,面向人的连接向面向机器连接转变,NFV、网络切片、边缘计算、能力开放等新技术泛使用,行业应用越来越多样化、复杂化。在 5G+智慧矿山规划、建设、运营中要全面考虑网络安全、物理环境安全、硬件设备安全、应用安全、SDN/NFV 安全、网络切片安全、MEC 安全、数据安全、管理安全等方面,以确保行业应用安全稳定运营。

“5G+智慧矿山”行业应用需求呈快速增长,5G+智慧矿山等特定行业应用场景下的安全风险评估体系建设相对滞后,缺少业务应用安全最佳实践,行业应用安全评估需求迫切。

## 3 5G+智慧矿山行业应用场景

5G+智慧矿山将人工智能、工业物联网、云计算、大数据、

收稿日期:2023-03-20

**作者简介:**张育慧(1979-),男,内蒙古人,大学本科,主要从事网络与信息安全管理;郝力群(1985-),女,内蒙古人,硕士研究生,主要从事网络与信息安全管理;王文静(1998-),女,内蒙古人,大学本科,主要从事网络与信息安全管理;李天松(1995-),男,内蒙古人,硕士研究生,主要从事网络与信息安全管理;刘博(1987-),男,内蒙古人,大学本科,主要从事网络与信息安全管理。

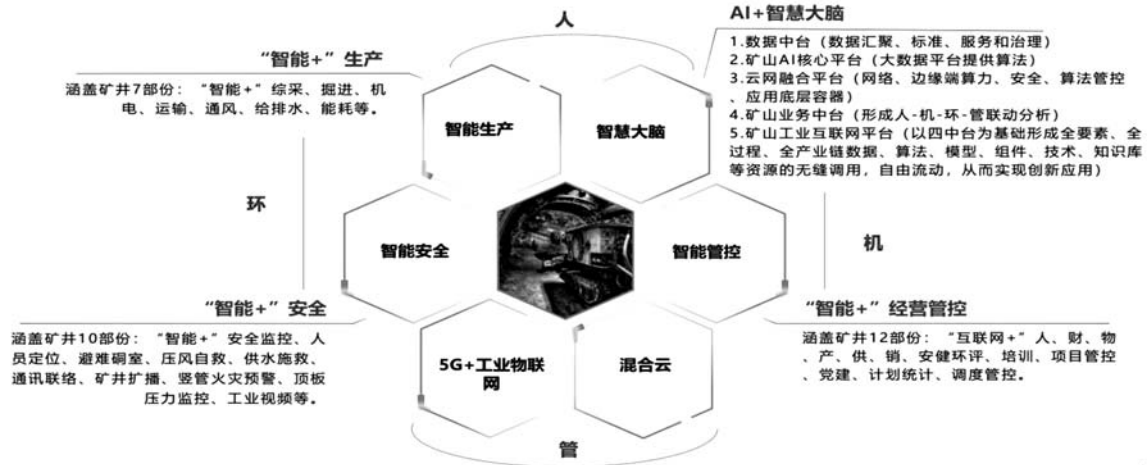


图 1 5G+智慧矿山建设方案

机器人化装备等与现代煤炭开发利用深度融合, 形成智能系统, 实现智能化运行。

安全评估需要结合 5G+智慧矿山整体的技术架构, 在应用层, 安全评估需要根据不同业务场景适配不同的评估内容, 覆盖井下融合组网、高清视频监控、矿用无人驾驶、矿用机械远程控制、无人化采掘等多个应用场景; 在平台层, 评估工业互联网平台、AI 智能分析平台、全景工作面等平台的安全性, 以及各矿山与平台之间的 API 接口安全、数据安全等; 在网络层, 评估 5G 基站安全、露天移动专网安全、井下融合专网安全、边缘计算安全等; 在终端层, 评估摄像头、雷达、传感器、网关、采煤机、皮带机、通风掘进机、矿车等 IOT 安全, 以及手机、智能单兵装置等终端安全。



图 2 5G+智慧矿山技术方案

#### 4 基于威胁建模的风险识别

按照《5G 网络建设与应用安全实施指南(2021)》《中国移动 5G 网络与业务安全基准测评规范》《中国移动 5G 网络安全技术规范(发布版)》《5G 垂直行业应用安全指南-印发版》《5G 新技术新业务安全评估总体要求-印发版》《5G 新技术新业务安全评估参考指标-印发版》《中国移动网络云安全运维技术要求(发布版)》《中国移动网络数据安全管理办法(2020 版)》《中国移动边缘计算网络安全技术要求》《5G 行业应用安全风险动态评估要素》等规范标准, 全面收集 5G+智慧矿山业务情况, 运用 STRIDE 威胁建模方法对 5G+智慧矿山井下部分(井工), 井上部分(露天), MEC(边缘计算)及 5GC(核心网部分)等应用场景进行威胁建模, 实现对两大类矿山九大类典型业务场

景的全覆盖, 识别安全威胁共计 163 项。

表 1 5G+智慧矿山全场景风险点示例

分类说明	出现次数
篡改	46
攻击者可能会篡改传输皮带并从中提取密钥材料	1
攻击者可能会篡改矿用 5G 智能矿帽并从中提取密钥材料	1
...	...
否认	6
攻击者可以否认恶意行为并消除导致拒绝问题的攻击足迹	1
攻击者可以拒绝对 API 的恶意行为导致拒绝问题	3
由于缺乏审计, 攻击者可以拒绝对数据库采取行动	2
拒绝服务	6
攻击者可能会通过拒绝服务攻击来阻止对托管在智能调度平台上的应用程序或 API 的访问	1
攻击者可能会通过拒绝服务攻击来阻止访问托管在 API 上的应用程序或 API	1
...	...
欺骗	16
攻击者可能会欺骗 API 并获得对 Web API 的访问权限	1
攻击者可能会欺骗 API 并获得对 Web 应用程序的访问权限	1
...	...
特权提升	76
攻击者可能会获得矿用隔爆兼本安型无线通信器(5G CPE) (Service Bus Technologies)的特权	5
攻击者可能会获得矿用隔爆型 BBU(Service Bus Technologies)的提升权限	1
...	...
信息泄露	12
攻击者可以从日志文件中访问敏感数据	1
攻击者可以从移动设备获取敏感数据	1
...	...
总计	163

根据上述威胁建模统计分析,总结出 8 大类 5G 智慧矿山行业应用需要重点关注的网络安全威胁:

(1) 网络服务安全威胁: 业务接入设备类型多数量大, 多种安全域并存, 安全风险点增加, 同时恶意代码入侵、缓冲区溢出等传统网络攻击威胁仍然存在。

(2) 硬件环境安全威胁: 边缘计算节点部署在无人值守机房、矿区机房或人迹罕至的极寒之地, 防护与安保措施相对薄弱, 存在因自然灾害而引发的设备断电、网络断链或遭受物理接触等安全风险。

(3) 虚拟化安全威胁: 容器或虚拟机面临篡改镜像、漏洞攻击、DDoS 攻击、逃逸攻击等威胁;

(4) 边缘计算平台安全威胁: 基于虚拟化基础设施部署的边缘计算平台 MEP 面临服务接口非授权访问, 窃取、篡改和删除敏感隐私数据的威胁。

(5) 应用安全威胁: 边缘计算节点连接海量的异构终端、部署大量第三方矿山 APP, 多样化的通信协议面临利用通信协议漏洞攻击的威胁, APP 之间的非法访问以及第三方 APP 恶意消耗 MEC 系统资源等安全威胁同样存在。

(6) 能力开放安全威胁: 开放的 API 如果缺少有效的认证和鉴权手段, 或安全性没有得到充分的测试和验证, 存在仿冒终端接入、漏洞攻击、侧信道攻击等安全威胁。

(7) 管理安全威胁: 边缘节点在矿区分布式部署, 依赖远程管理和运维, 如果升级和补丁修复不及时, 攻击者可利用漏洞进行攻击;

(8) 数据安全威胁: 5G+智慧矿山边缘计算平台可收集、存储与其连接设备的数据, 包括应用数据、用户数据等。其数据面临数据损毁风险、数据泄露风险等安全风险。

## 5 5G+智慧矿山行业应用全场景一站式安全评估体系

结合威胁建模所识别的安全风险, 通过对现有 5G 安全标准和规范的梳理以及适用性匹配, 经整合归并, 最终形成面向 5G+智慧矿山行业应用的安全评估框架和具体评估内容。

表 2 威胁建模和现行规范标准与 5G 智慧矿山场景适配情况

对标项目	梳理结果	适配结果
5G+智慧矿山威胁建模	163 个风险点	重点关注 8 类安全风险
《中国移动 5G 网络与业务安全基准测评规范》	针对 5G 业务安全评估要求 105 项	适用 85 项
《边缘计算白皮书》	针对边缘计算安全防护要求 66 项	适用 64 项
《中国移动 5G 垂直行业应用安全指南》	5G 垂直行业应用安全场景 109 个	适用 11 个安全场景, 涉及安全要求 39 项
《5G 新技术新业务安全总体要求》	5G 业务通用安全措施 63 项	适用 63 项
《5G 新技术新业务安全评估参考指标》	5G 安全评估指标 77 项	适用 37 项
《5G 行业应用安全风险动态评估要素》	5G 安全评估项和参考指标 28 项	适用 27 项
结合以往的安全评估经验, 对 5G+智慧矿山场景下的安全评估内容进行补充和完善		补充 6 项

### 5.1 安全评估体系框架

5G+智慧矿山安全评估体系框架包含物理环境安全、网络和基础设施安全、应用安全、数据安全、终端安全、业务场景安全、5G 关键技术安全、演练与应急、容灾与备份、安全管理及其他安全等 11 个安全模块, 共 69 个评估项, 132 个安全评估指标。

### 5.2 安全评估方法及流程

#### (1) 安全评估方法

评估人员对业务相关人员进行现场及远程调研, 通过人员访谈、文档查阅、演示查验、测试验证等多种方式对业务风险及企业安全保障能力进行核实验证。

人员访谈: 对照评估指标, 评估人员通过对企业网络与信息安全人员、业务主管以及业务平台技术合作方进行访谈与讨论。

文档查阅: 对照评估指标, 评估人员查阅业务安全保障相关的制度文件。

演示查验: 对照评估指标, 评估人员对业务系统平台的日志记录、内容安全保障技术手段进行查验核实。



图 4 5G+智慧矿山安全评估体系框架



图 5 安全评估流程图

测试验证: 对照评估指标, 评估人员对已采用的安全保障措施落实情况进行核实验证。

### (2) 安全评估流程

5G+智慧矿山安全评估流程分为准备阶段、预评测阶段、执行评测阶段、结束评测阶段。

### (3) 安全评估工具

自动生成评估表格降低难度: 评估前根据评估对象选择 5G 智慧矿山对应的应用场景, 自动生成评估模块、所需文档、技术测试点, 辅助评估人员迅速确定评估内容, 便于不同角色的评估专家同时开展评估, 增加评估易用性。

5G+智慧矿山基本信息填写			
基本情况	评估基本情况	评估单位	内蒙古移动
		评估时间	2021年5月
		评估人员及联系方式	XXXXXX
	5G+智慧矿山基本情况	矿山所属单位	XXX煤矿
		矿山类型	井工
		组网方式	4/5G融合组网
	5G+智慧矿山业务场景	数据是否出园	否
		是否接入智慧矿山工业互联网平台	否
		矿卡远程驾驶	否
	5G+智慧矿山业务场景	电铲远程操控	否
		全方位立体监控	否
		井下监控及AI智能识别	是
		井下远程控制类	否
		远程驾驶	否
		传感器信息采集类	否
	5G+智慧矿山业务场景	井下定位	是
		井下人员通信	是

图 6 5G+智慧矿山信息调研表

工作流程图:



图 7 5G+智慧矿山评估工作流程图

规范评估流程保障安全: 为了避免在评估过程中引入新的安全风险, 充分考虑行业应用情况, 制定详细的智慧矿山安全评估实施操作流程, 并配套风险规避措施和应急处置文档, 有效降低评估风险, 规范人员操作, 提高评估安全性。

安全评估过程文档模板目录:

### 01 5G+智慧矿山安全评估流程

#### 01-1 评估流程

#### 01-2 技术测试风险操作 checklist 确认-评估前

#### 01-3 技术测试风险操作 checklist 确认-评估中

#### 01-4 技术测试风险操作 checklist 确认-评估后

#### 01-5 免技术测试设备申请单

### 02 提供材料统计

#### 02-1 管理制度及技术文档登记表

### 03 漏洞扫描

#### 03-1 安全扫描工作申请单

#### 03-2 漏洞扫描风险提示

#### 03-3 安全评估-漏洞扫描配置流程及策略说明

#### 03-4 安全扫描作业规范

#### 03-5 安全扫描异常情况处置记录

#### 03-6 安全扫描报告模板

### 04 配置核查

#### 04-1 配置检查申请单

#### 04-2 配置检查风险提示

#### 04-3 安全评估-配置核查配置流程及策略说明

#### 04-4 配置检查作业规范

#### 04-5 配置检查异常情况处置记录

#### 04-6 配置检查报告模板

### 05 渗透测试

#### 05-1 渗透测试授权书

#### 05-2 渗透测试实施风险说明

#### 05-3 WEB 渗透测试用例

#### 05-4 XX 系统渗透测试过程记录报告

#### 05-5 XX 系统安全渗透测试报告模板

### 06 应急预案

#### 06-1 风险评估应急预案

### 07 文档输出统计

#### 07-1 安全检查输出文档

自动化工具增强适用性: 在实验环境或风险人为可控的情况下, 进行主动测试, 如漏洞扫描、渗透测试等; 在生产环境中, 进行被动测试, 如使用工控评估工具、监测平台等。

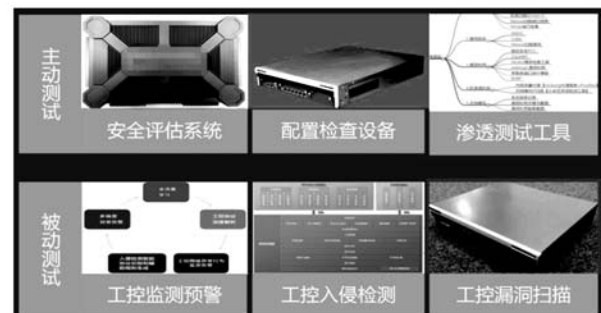


图 9 5G+智慧矿山安全评估检查工具

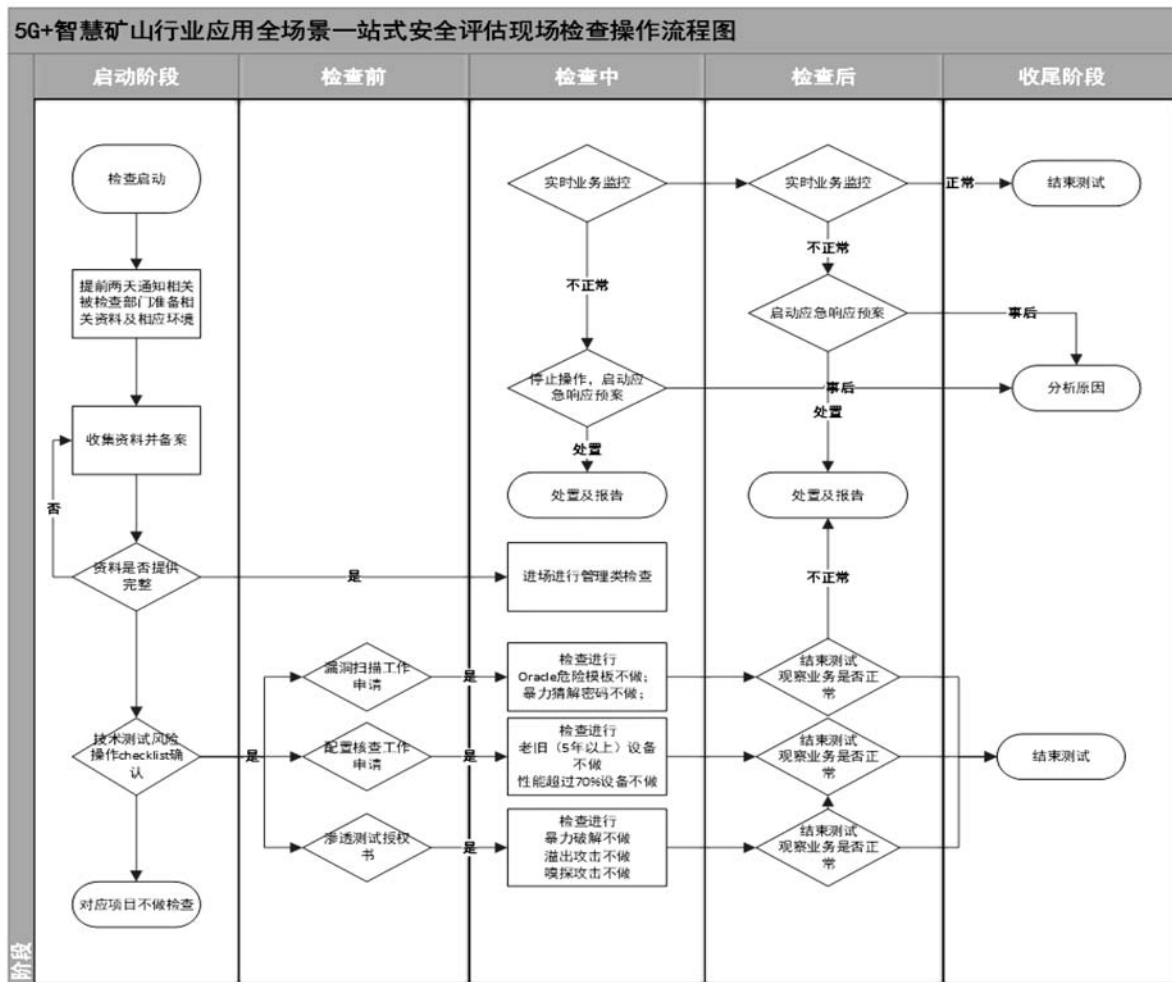


图 8 5G+智慧矿山安全评估现场检查操作流程

### 5.3 安全评估管理机制

参考新技术新业务安全评估机制,将安全风险评估机制纳入 5G+行业应用工作流程,并建立针对 5G+智慧矿山的安全评估机制,包括:上线前安全评估机制、定期核查动态核验机制。

#### (1) 上线前安全评估机制

在 5G+智慧矿山新应用投入运行前,按照 5G+智慧矿山安全评估体系、工作方法、工作流程进行安全评估,对发现的隐患问题及时进行整改和复测,确保新行业应用投入运行前安全可管、可控。

#### (2) 定期核查机制

行业应用运行期间定期开展安全评估,或在基础资源、技术实现方式、业务功能等方面发生较大变化时开展安全评估。

#### (3) 动态核验机制

行业应用运行期间,对行业应用安全保障能力措施手段进行动态核验,确保其保障能力持续动态有效,及时对发现有缺失、薄弱环节启动安全整改。

### 5.4 一站式安全评估要素

#### (1) 终端安全

具备防止终端被攻击或感染、身份鉴别与登录控制、终端安全审计、终端与 5G 网络双向认证、不同应用场景下认证及加解密方式按需选择、隐私数据加密传输等能力。

#### (2) 应用安全

具备业务应用层的用户身份鉴别与授权、防入侵、业务安全审计、应用数据安全存储、防接口被非法调用等能力。

#### (3) 数据安全

从数据生命周期各环节建立技术措施保证数据安全;具备敏感数据加密传输和存储、数据分权访问控制、数据脱敏、数据安全删除、数据备份与恢复、数据操作审计等机制或能力。

#### (4) 物理环境安全

边缘计算系统机房出入口应配置电子门禁系统,机柜应具备电子防拆封功能。边缘计算设备应是可信设备,具备防寒、防尘、防潮、防爆等安全措施。

#### (5) 网络和基础设施安全

网络具备安全认证、信令机密保护、信令完整性保护能力;关注安全域划分、物理/逻辑隔离、UPF 流量隔离、INTERNET 安全访问、矿区局域 MEC 场景下的安全域划分和通信隔离;操作系统、数据库、中间件、网络设备等要具备统一的系统安全配置要求,并按要求开展安全配置。

#### (6) 演练与应急

具备完善的应急管控要求及流程,制定完善的应急演练管理制度,定期开展针对 5G+智慧矿山业务场景的应急演练。

#### (7) 容灾与备份

具备路由器、交换机冗余机制;应具备网元级容灾管理要求及流程;应具备资源池级容灾管理要求及流程;应具备必要的备份恢复机制。

#### (8) 5G 关键技术安全

对 NFVI、业务通信系统、管理系统、网络架构安全、UPF 安全、MEC 平台安全、MEC 编排管理系统安全、MEC App 安

全、应用层、控制层、数据层以及南北向接口等进行安全防护;为每个切片定义不同的访问安全机制以及会话安全机制。

#### (9)业务场景安全

5G 相较于 4G,具有增强移动带宽(eMBB)、超高可靠低时延通信(uRLLC)和海量机器类通信(mMTC)的特点。增强移动带宽(eMBB)主要面向移动互联网流量爆炸式增长,为移动互联网用户提供更加极致的应用体验;超高可靠低时延通信(uRLLC)主要面向工业控制、远程控制、自动驾驶等对时延和可靠性具有极高要求的垂直行业应用需求;海量机器类通信(mMTC)主要面向环境监测等以传感和数据采集为目标的应用需求。

在 5G 智慧矿山中,凭借 5G 网络的增强移动带宽(eMBB)特点,可将矿用无人驾驶卡车及井下高清摄像头数据回传到调度平台,操作员只需在调度平台前即可掌握现场情况,实现矿用机械远程控制、无人化采掘等,在井工矿中也能更好实现井上井下协同运维和高清音视频通话;5G 网络的超高可靠低时延通信(uRLLC)特点,可以使矿用无人驾驶卡车、工业自动化系统的操作指令快速且稳定的传输;依靠海量机器类通信(mMTC)的特点矿区的车辆、工程设备、网络摄像头、以及矿用手机等数百个 5G 终端设备能够稳定的接入 5G 网络。

关于 eMBB、uRLLC、mMTC 三个业务类型,安全要求如下:

① eMBB:面向公众的 eMBB 业务应具备业务流量内容监控与识别能力;部署抗 DDoS 设备或具备抗 DDoS 攻击能力;及时升级现网防火墙、入侵检测系统等安全设备;部分场景下可采用二次认证和密钥管理机制;高安全要求业务场景可通过物理隔离或加密保护 5G 用户面保证网元之间用户数据传输安全性、核心网与 eMBB 业务服务平台之间可采用数据专线的方法保证用户业务数据传输安全性。

② uRLLC:部署抗 DDoS 设备或具备抗 DDoS 攻击能力;评估网络采用的安全机制对 uRLLC 业务时延、可靠性可能造成的影响;在部分场景下可以在用户终端及业务服务器之间建立应用层双向身份认证机制;应具备数据完整性保护、时间戳、序列号等机制。

③ mMTC:具备终端物联网卡违规滥用监测、终端安全风险监测能力;考虑网络负载能力,降低 DDoS 攻击的风险;应采用轻量级的安全算法、简单高效的安全协议来实现终端与网络间的双向认证、数据加密及完整性保护。

#### (10)安全管理

安全管理包含安全事件管理、用户行为管理、关键数据管理、生命周期管理、资产管理、平台基线管理、脆弱性管理、态势感知能力、安全运维、安全审计等内容。

#### (11)其他安全

包括信任模型和身份管理升级(多接入方式认证、多设备形态的身份管理等)、密钥和算法、隐私保护、高可用性、供应链安全等内容。

## 6 安全评估体系应用及实践

评估实践选取内蒙古某井工矿和某露天矿两大典型智慧矿山作为实地评估试点,其中井工矿包括 5G 网络、工业互联网平台、云平台等业务场景。露天矿包括 5G SA 专网+无人驾驶卡车等应用场景。

### 6.1 试点矿山安全评估概述

#### (1)井工矿

该煤矿包括 5G 网络、工业互联网平台、云平台等业务场景;

5G 网络:5G 网络主要用于井上和井下两部分。在这两个区域内 5G 网络均做到了全部覆盖,为各项应用的部署,提供数据“高速通道”的保障。

(1)井上部分:井上 5G 覆盖主要场景为办公楼、调度室、宿舍楼、锅炉房等,保障煤矿日常经营的数据回传和远程控制。

(2)井下部分:井下 5G 覆盖主要场景为副斜井、主斜井、2-2 煤运输大巷、2-2 煤辅运大巷、12203 辅运顺槽、12203 主运顺槽、12203 切面、12202 辅运顺槽、12202 主运输顺槽、3 煤层、3 煤辅运大巷、中央变电所、盘区变电所、避难硐室、机电硐室完成 5G 覆盖,支撑井下各类型的数据的回传和远程控制。

工业互联网平台:工业互联网平台完成煤矿瓦斯灾害防治系统、人员定位系统、束管监测系统、综采工作面监控系统、智能干选系统、视频监控系统、应急广播系统、人员车辆精准定位系统、无人值守电力系统、排水系统、锅炉房监控系统、通风系统、压风系统、污水处理系统等 14 个子系统的统一集成,支撑煤矿生产经营“一张表”。平台对各子系统的海量生产数据进行深度的挖掘、清洗、计算,对煤矿的决策提供数据支撑。

云平台:搭建云 610CV 算力和 160TB 存储的移动云平台,为煤矿的各个子系统正常运行提供算力和存储支持。云机房部署于运营商的 IDC 机房,免除了矿方传统的 DC 机房建设成本、安全运营成本、维护成本等,为矿方节省大量的资金投入。全部数据 IP 化,提供云桌面 97 台,为煤矿提供全局数据的统一接入,解决困扰煤矿多年的设备复杂、较多的局面。

结合以上煤矿的业务场景和特点,对 5G+智慧矿山安全风险研判表中各项指标进行判断,共计有 90 项评估指标适用。

#### (2)露天矿

内蒙古某露天矿,存在极寒的物理环境。该矿区的建设方案介绍:

①内部数据流经过 MEC 本地分流后直接在园区内闭环,不出公网;

②公网数据流经过 MEC 透传出园区,通过移动的地市核心网由公网取得数据;

③信令需与移动大区核心网互通,取得控制信息。信令只在用户终端附着或切换时产生交互,传递的是控制信令,与数据包无关。

④矿区包括无人驾驶场景,包含矿车、5G 手机、5G CPE 等终端。

结合该煤矿业务场景和特点,对 5G+智慧矿山安全风险研判表中各项指标进行判断,共计有 126 项评估指标使用。

### 6.2 安全评估结果及安全整改建议

遵照本文提出的安全评估体系,通过梳理业务场景,自动适配评估项,其中井工矿适配评估项共计 90 项,露天矿适配评估项 126 项。经现场进行访谈及技术测试评估,共计发现 43 大类安全风险(包含网络安全风险 90 多项)。

评估实践依据评估体系,围绕物理环境安全、网络和基础设施安全、应用安全、数据安全、终端安全、矿山场景安全、其他应用场景安全、5G 关键技术安全—网络切片安全、5G 关键技术安全—SDN 安全、5G 关键技术安全—虚拟化安全、5G 关键技术安全—容器安全、演练与应急、容灾与备份、安全管理及其他安全等方面开展,经评估其网络安全形势十分严峻,在终端安全、应用安全、数据安全、基础网络安全、虚拟化安全、矿山业务场景安全、网络安全管理、应急响应与容灾机制等方面存在一些问题和不足。





图 10 安全评估实践案例

主要体现在以下几个方面:

(1) 终端安全: 落实终端身份鉴别与登录控制, 具备防止终端被攻击或感染、终端安全审计、终端与 5G 网络双向认证、不同应用场景下认证及加解密方式按需选择、隐私数据加密传输等能力。

(2) 应用安全: 严格落实用户身份鉴别机制, 加强权限控制措施, 对应用接口进行认证和访问控制、对应用平台进行上线前安全检测和加固、日常要对应用异常流量进行监测和安全事件应急处置, 提升各应用系统健壮性。

(3) 数据安全: 需建立数据安全管理制度, 明确数据在采集、传输、存储、处理、使用、销毁等环节的技术保护措施。

(4) 基础网络安全: 需根据业务类别和重要程度划分安全域、对安全域边界进行安全防护、核心区域建立冗余备份、严禁服务器使用双网卡和随身 WIFI、严格落实生产网与办公网物理隔离。需部署安全态势感知系统、入侵检测/防御系统、抗 DDoS 攻击系统、防病毒系统、僵尸蠕防恶意软件系统, 定期进行巡检和安全策略优化。

(5) 虚拟化安全: 需加强宿主机、镜像、容器等安全配置和防护, 覆盖整个生命周期。落实虚拟化资源隔离、权限控制等措施, 并支持对恶意流量和恶意行为的监控。

(6) 矿山业务场景安全: 对 5G 终端进行认证鉴权, 对无线设备在线情况和异常行为进行监测, 并能够进行远程下线等控制。

(7) 网络安全管理: 需建立网络安全管理制度、明确网络安全管理部门或机构、配备网络安全专职人员、细化网络安全职责、提升人员网络安全意识、强化网络安全规划、建设、运维管理, 提升网络安全应急响应管理。需落实网络安全三同步, 同步规划、同步建设、同步运行, 确保系统上线前各项网络安全技术管控措施规划到位、建设到位、运行到位。

(8) 应急响应及容灾机制: 制定涵盖常见安全事件的应急响应预案, 明确应急流程和应急联系人, 定期开展安全演练与数据恢复演练。

(9) 其他安全: 增加供应链(包括硬件设备供应商、应用软件合作商、业务合作商等)安全管控机制; 对关键设备自主可控, 需具备适配国产设备能力。

## 7 安全评估体系完善

在安全评估实践工作过程中, 发现在安全评估体系中还有需改进的方向, 一是安全测评工具及方式也应该与时俱进, 随着科技水平的发展, 网络系统及应用在不断翻新, 智能化应用及场景越来越复杂, 今后还应该加大对评估测评技术和方

式的研究应用, 在评估工具上不断改进, 以确保评估工作的高效开展。二是风险识别完成后应建立风险分级管控台账, 根据高、中、危风险级别建立涵盖风险识别、风险评估、风险管理等信息的风险分级管控台账, 促进风险信息的传递交流, 加快风险整改、加强风险规避, 同时能强化安全风险管控。

## 8 结语

目前 5G+智慧矿山行业正处于信息化、智能化快速发展阶段, 本研究构建的 5G+智慧矿山行业应用全场景一站式安全评估为智慧矿山的高质量发展提供了坚实的基石。评估实践证明, 本文提出的评估框架可针对 5G+智慧矿山规模、业务场景、组网方式、终端类型等方面进行灵活拓展和裁剪, 能够指导评估人员快速开展评估工作。

后续, 通过推动 5G+智慧矿山行业应用安全评估工作不断完善, 将为智慧矿山行业应用领域和及上下游产业的可持续、高质量发展注入新动能, 同时也为其他垂直行业项目提供安全评估实践思路。

## 参考文献:

- [1] 杨红梅.5G 边缘计算安全关键问题及标准研究[J].信息安全研究,2021.
- [2] 张滨.5G 边缘计算安全研究与应用[J].电信工程技术与标准化,2020.
- [3] 张滨.5G 数据安全防护技术研究[J].信息安全研究,2021.
- [4] 《未来已来 5G 行业研究报告》艾瑞咨询系列研究报告, 2020.
- [5] 《内蒙古自治区能源局内蒙古推进煤矿智能化建设三年行动实施方案》.2021 年.
- [6] 《工业和信息化部办公厅 5G 网络建设与应用安全实施指南》.2021 年.
- [7] 《工业和信息化部办公厅 5G 行业应用安全风险动态评估要素》.2022 年.
- [8] 《中国移动 5G 网络与业务安全基准测评规范》.2019 年.
- [9] 《中国移动 5G 垂直行业应用安全指南》.2020 年.
- [10] 《5G 新技术新业务安全评估总体要求》.2020 年.
- [11] 《5G 新技术新业务安全评估参考指标》.2020 年.
- [12] 《中国移动网络云安全运维技术要求》.2020 年.
- [13] 《中国移动网络数据安全管理办法》.2020 年.
- [14] 《中国移动边缘计算网络安全技术要求》.2020 年.
- [15] 《工业互联网产业联盟 5G 边缘计算白皮书》.2020 年.
- [16] 《中国移动 5G 网络安全技术规范》.2019 年.