5G行业应用安全风险评估报告

**应用名称：神华国华广投（北海）发电有限责任公司5G专网项目**

**中国移动通信集团广西有限公司**

**2023年8月**

**目录**

[1 行业应用基本情况介绍 3](#_Toc144073317)

[1.1 应用名称 3](#_Toc144073318)

[1.2 应用内容简介 3](#_Toc144073319)

[1.3 所属行业 3](#_Toc144073320)

[1.4 业务场景 3](#_Toc144073321)

[1.5 应用规模 4](#_Toc144073322)

[1.6 应用类型 4](#_Toc144073323)

[1.7 行业用户身份认证情况 4](#_Toc144073324)

[1.8 设备及网络部署位置 5](#_Toc144073325)

[1.9 切片类型 7](#_Toc144073326)

[1.10 专网模式 7](#_Toc144073327)

[1.11 对公共安全的影响 7](#_Toc144073328)

[2 安全评估情况 7](#_Toc144073329)

[2.1 评估工作情况概述 7](#_Toc144073330)

[2.2 评估人员组成 8](#_Toc144073331)

[2.3 评估实施流程及时间 8](#_Toc144073332)

[2.4 评估结果 9](#_Toc144073333)

[2.4.1 5G典型应用场景安全 9](#_Toc144073334)

[2.4.2 5G应用通用安全 11](#_Toc144073335)

[2.4.3 5G专网安全 17](#_Toc144073336)

[2.4.4 5G关键技术安全 31](#_Toc144073337)

[2.4.5 5G行业应用安全保障 47](#_Toc144073338)

[2.4.6 5G行业应用数据安全 59](#_Toc144073339)

[3 整改建议及落实情况 78](#_Toc144073340)

[3.1 整改建议 78](#_Toc144073341)

[3.2 整改落实情况 79](#_Toc144073342)

[4 评估结果签字确认 80](#_Toc144073343)

# 行业应用基本情况介绍

## 应用名称

神华国华广投（北海）发电有限责任公司5G专网项目

## 应用内容简介

神华国华广投北海神华电厂是国家能源集团下属企业，计划在北海市北海神华厂区区进行厂区二期扩建工程，按照客户规划拟将北海神华电厂打造为国华智能电站建设示范项目。

以5G专网、高度自动化、智能化设备为基础，采用先进管控策略和信息处理手段，保证设备动作灵活可靠、状态实时感知、各工况自动适应，实现全过程自动控制、全系统信息融合，全生命周期高效管理；以“减少运行人员、提高机组效率、提升管理安全水平”为主线，通过大数据平台对生产数据整理、分析，形成高价值的数据资源和标准化的业务流程，促进“运行规范化、检修标准化、专业纵深化”，推动安全风险预控管理体系完善、落地，最终实现北海神华电厂智能生产，同时为国华电力提供重要业务及生产数据，最终为国华电力实现智慧企业添砖加瓦。

目前厂内的无线、有线网络已无法满足日后智慧电厂的应用实际需求，鉴于5G技术在工业互联网领域的应用，以及国家层面所倡导的“新基建”、“5G+工业互联网”的要求，北海神华电厂提出了5G专网的建设需求，我司拟在电厂内实现5G专网覆盖，以满足厂内智能应用的需求，提升日常工作效率，保障生产安全。

## 所属行业

能源电力

## 业务场景

属于增强移动宽带（eMBB）场景。

1.5G+AI视频安防：基于可见光、红外摄像头等视频监控设备，实时采集视频监控画面，通过5G网络回传至视频监控平台，可进行图像自主识别，重点针对发电厂内人、机、料、法、环生产五要素进行安全管控，降低企业生产安全风险。

利用5G网络的高清视频回传、数据实时采集、以及AI智能分析检测，及时发现厂内设备及管线的故障（例如冒烟、漏气、失火等等），收到危险或破损预警后可及时安排专业人员前往解决，提高生产效率、降低人员安全风险。

5G高清相机+AI，增加特征识别点，提高AI识别的距离和灵敏度，更有效的识别工人的规范操作，实时识别风险，通过大喇叭、对讲机、人员调度等方式，及时纠正和处理。

2.5G+AI设备在线点检和维护：工作中的良好维护和正确维护，可以使设备运行时间增加，减少故障，确保工厂设备的可靠性。系统通过周期、运行时间、事件和测量等预防性维护策略，进行定期维修、维护，分解维修计划，通过检修路径的设置实现5G在线设备检测和AI预测性维护，并能自动生成预防性维修工单，为需要计划维护的设备建立详细的维护计划策略，提高设备维护维修中的预见性和计划性，将电厂职员尤其是生产人员从庞大的紧急性维修的工作重担下解放出来。

根据生产设备的运维需求，5G+AI设备在线点检和维护功能实现集团/分公司一体化部署，对各厂区关键设备加装有线或无线振动温度传感器，并可通过工业协议接入设备的运行工况等数据。通过生产设备的在线监测和监测数据的多端存储，达到集团化的统一管理，从而实现设备的智慧运维和故障诊断。

3.5G智慧终端巡检：巡检是电厂运行的第一要务，巡检能够及时发现设备的异常情况，避免系统停车和事故的发生。巡检需要查看运行状况和仪表的状态显示（压力、温度、油位等）、运转噪声、运转振动，以及设备的跑冒滴漏情况。当前巡检多数为人工记录结果，巡检过程难以管理，结果难以应用。智能巡检采用5G通信技术实现产品跟踪，保障巡检信息实时传输，无需人工整理，提高工作效率、杜绝数据造假；还能高效监督巡检工作执行情况，避免漏检；同时确保中控中心与巡检人员信息互通。基于5G巡检仪，可以满足企业巡检数据不出园区的诉求，并支持视频对讲，提升沟通效率。

4.5G无人机智能巡检：5G无人机可借助激光雷达生成三维地图，并按照预设航线，借助可见光、红外摄像头等硬件设备，采集预设点位的可见光图像、红外图像数据信息，自主生成巡检报告，同时通过5G网络回传至巡检平台。通过5G+无人机的高速率回传、低延时控制针对空旷区域实现智能巡检，实现自主识别及告警，及时发现发电厂内不规范行为及设备管线故障等，降低人员日常工作检查量，加大巡检范围，提升巡检效率，提升整个厂区的安全性。

5.5G机器人巡检：巡检机器人可按照预定路线，借助可见光、红外摄像头、传感器等硬件设备，采集重点区域（如：升压站/主变区、配电房、输煤皮带等）内预设点位的图像、声音等数据信息，通过5G网络回传至巡检平台，实现自主巡检、自动避障、自主识别及告警，满足支持设备的跑冒滴漏检测、外观缺陷检测、关键部位红外测温、断路器及隔离开关的分合状态检测、变压器等充油设备的油位计检测、SF6气体压力等表计读数等内容的多种巡检需求，降低人工巡检安全隐患，提升巡检效率。

6.5G智能燃料:5G智能燃料管理平台借助5G、物联网、RFID、GPRS等技术将煤、煤场、运输、设备、人通过系统有机集合，实现燃料全方位智能高效管理。

智能燃料管控涵盖智能化应用、设备物联两个层面。在设备物联层面实现计量设备、采样设备、制样设备、化验设备、煤场设备、样品设备的集成，保证燃料数据的连贯和完整；在智能化应用层面支持汽车运煤、火车运煤、轮船运煤、汽车运水泥、场外车辆调度及与车联网集成，保证燃料数据的真实和可靠。

## 应用规模

宏站无线设备包括1台华为BBU，5台华为AAU，3台APP服务器。终端包括80台CPE，20台5G高清摄像机，共计开通100张物联网卡。

## 应用类型

包括视频监控类应用。辅以配备机器学习行为模型进行实时识别。本项目共需要进行3种行为训练，分别位“安全帽+工作服检测”、吸烟行为、睡岗行为，每个模型采集500-1000张图片进行AI训练，在系统中建立行为模型，当系统捕捉到违规行为时，可自动识别，系统弹框预警。

图 1 业务组网图

## 行业用户身份认证情况

该业务单位经营许可证如下。

图片包含 文本

AI 生成的内容可能不正确。

图 2 经营许可证

## 设备及网络部署位置

UPF与MEC部署在客户园区机房内，其余设备部署在大区。

图片包含 图形用户界面

AI 生成的内容可能不正确。

设备部署位置

## 切片类型

该项目未配置并使用特殊切片，故不涉及切片类型。

该项目通过配置独立专用DNN、专用的宏站及室分单元实现隔离和资源专享。

## 专网模式

该项目属于中国移动尊享模式行业专网，独立建设部署了专用的基站，通过数通设备接入大网共享型UPF。

属于混合共用模式。

## 对公共安全的影响

社会影响力：该项目专网只覆盖园区内，受到破坏后对国家安全、社会秩序、经济运行和公共利益基本无损害。

服务重要性：该项目专网使用终端较少且不涉及核心业务与生产，被破坏后对较少的用户造成影响、且仅对较小的地区造成影响。

规模和服务范围：该项目专网服务范围较小，服务用户数量较少，所提供的服务重要性较低，被破坏后对网络和业务运营商的合法权益损害较小。

综上所述，初步判断该项目对公共安全影响较小。

# 安全评估情况

## 评估工作情况概述

2023年7月21日-7月29日。本阶段工作内容包括成立评估组并确定小组人员，在对网络等环境调研的基础上，确定评估范围并梳理所需资料，如技术文档、管理文档、设备列表等；收集调研业务情况，结合业务特点，选择业务适用的安全评估指标，明确业务评估范围内已有的安全管理措施和技术保障措施。广西移动信息安全中心负责人，防城港分公司的集客部、网络部、客响中心以及技术合作方人员共同参与此次评估工作。

## 评估人员组成

|  |  |  |  |
| --- | --- | --- | --- |
| **姓名** | **部门** | **工作岗位** | **联系方式** |
| 黎峰 | 中国移动广西公司信息安全中心 | 网络安全主管 | 13617710924 |
| 谢晓刚 | 评估人员 | 评估人员 | 17376573131 |
| 宋涤非 | 评估人员 | 评估人员 | 19975261860 |

## 评估实施流程及时间

根据《5G行业应用安全评估规范》的相关要求，本次评估流程包括以下三个阶段：

**评估准备阶段：**2023年7月21日-7月23日。本阶段工作内容包括成立评估组并确定小组人员，在对网络等环境调研的基础上，确定评估范围并梳理所需资料，如技术文档、管理文档、设备列表等；收集调研业务情况，结合业务特点，选择业务适用的安全评估指标，明确业务评估范围内已有的安全管理措施和技术保障措施。

**组织实施阶段**：2023年7月23日-2023年7月26日。在前期准备的基础上，评估组成员通过人员访谈、文档查阅、演示核查、测试验证等方式对5G行业专网及其业务风险和保障能力作出验证：

* 人员访谈：对照评估指标，企业安排信息安全部、集团客户部、业务合作方的相关人员，对评估人员提出的问题进行回应与讨论。
* 文档查阅：对照评估指标，评估人员提出业务安全保障相关的制度文件需求，企业安排相关人员准备提供，评估人员进行查阅。
* 演示核查：对照评估指标，相关方安排相关人员，对目前已拥有的安全能力及系统中的相关技术手段等进行介绍展示，评估人员进行核实确认并保留截图记录。
* 测试验证：根据企业提供的测评环境和条件，评估人员根据具体的测试用例或技术手段，对企业已采用的安全保障措施落实情况进行核实验证。

在获取评估结果后，评估人员对照评估指标对结果进行综合分析，形成评估结论。

**评估总结阶段**：2023年7月27日-7月29日。针对安全评估结果及结论，提出后续建设中安全保障能力的改进方向和重点，并与相关方人员召开会议进行确认，对评估结果达成一致意见。根据评估情况，完成评估报告撰写及签字盖章。

## 评估结果

### 5G典型应用场景安全

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 评估模块 | 评估指标 | 评估内容 | 评估意见 | 研判依据 |
| 1.1  5G典型应用场景安全 | 1.1.1  增强型移动宽带（eMBB）场景 | a)应具备eMBB场景下的安全保障能力，应部署网络安全防护、入侵检测等安全技术手段以满足超大流量条件下的安全需求。 | 符合 | 该项目属于eMBB场景。该网络环境中共享UPF侧部署有防火墙设备，网络安全能力满足该流量等级下的正常运行和安全防护。其余安全能力复用大区公网安全资源池，提供流量清洗等安全能力，提升大流量下的安全处理能力。业务平台由用户自行建设，本次评估不涉及。 |
| b)针对eMBB场景下的高安全要求应用场景，应支持二次身份认证授权、加密、专线等安全加强措施以保障应用安全。 | 不涉及 | 该项目为基本的接入业务，且客户未提出较高安全需求，故此项暂不涉及。 |
| 1.1.2  超高可靠低时延（uRLLC）场景 | a)应具备uRLLC场景下的安全保障能力，部署相关技术措施，如优化业务接入认证、数据加解密安全机制以满足低时延场景的安全需求。 | 不涉及 | 该项目不涉及uRLLC应用场景。 |
| b)针对uRLLC场景下的高安全要求应用场景，企业应支持建立应用层双向身份认证、数据完整性保护等安全加强措施以保障业务安全。 | 不涉及 | 该项目不涉及uRLLC应用场景。 |
| 1.1.3  海量机器类通信（mMTC）场景 | a)应具备mMTC场景下的安全保障能力，部署相关技术措施，如面向海量机器类通信的安全监测处置模型、分布式身份管理、轻量级的认证和数据完整性保护等，以满足mMTC场景下海量终端接入、认证节点集中带来的安全风险。 | 不涉及 | 该项目不涉及mMTC应用场景。 |
| b)针对mMTC场景下的高安全要求应用场景，企业应支持终端二次认证、加密保护等能满足相关需求的安全加强措施。 | 不涉及 | 该项目不涉及mMTC应用场景。 |

该5G行业应用涉及eMBB场景。

针对eMBB场景，拥有安全保障能力如下：

于共享型UPF边界处部署有防火墙，用于专网与行业网络的基本隔离，且可满足该流量等级下的正常运行和安全防护；复用大区公网安全资源池，提供流量清洗等安全能力，提升大流量下的安全处理能力。

### 5G应用通用安全

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 评估模块 | 评估指标 | 评估内容 | 评估意见 | 研判依据 |
| 2.1  应用基础安全 | 2.1.1  项目规模 | 应确定行业用户的应用规模情况，比如用户开卡数量。 | 符合 | 该项目用户规模清晰。 |
| 2.1.2  用户类型 | 应确认行业用户的应用类型情况，明确用户所属行业类型和行业终端类型。 | 符合 | 该项目用户类型清晰。 |
|
| 2.1.3  行业用户身份信息 | 应对行业用户身份信息进行认证登记，应留存行业用户单位有效证件（法人证书、经营许可证等）、责任人和经办人有效证件、责任人和经办人委托授权书以及经办人办理业务时的现场照片。 | 符合 | 该项目已留存用户法人信息与办理人身份信息。 |
|
|
| 2.1.4  设备及网络环境 | 应确认提供应用服务的设备及网络环境情况，如切片类型、专网模式（公网共用、混合共用和独立专用）、业务平台、MEC、5G 设备列表等。 | 符合 | 该项目的设备、切片模式、组网模式、业务平台情况均已掌握。 |
| 2.1.5  公共安全影响 | 应对行业应用是否会对公共安全造成影响进行评估。如果将对公共安全造成影响，需确定影响程度。 | 符合 | 经初步判断，该项目对公共安全造成的影响较小，该项目只覆盖校园范围内，且主要为利用现有5G网络建设情况，使用CPE转接WIFI信号，与原有网络基本一致，受到破坏后对国家安全、社会秩序、经济运行和公共利益基本无损害；该项目重点为提升校园5G网络体验，为5G智慧校园打下坚实基础，承载业务以ToC应用流量以及校园网为主，同时存在替代链路，故服务重要性一般；  该项目专网服务范围固定，规模不大，且存在替代链路，被破坏后对网络和业务运营商的合法权益损害较小。 |
| 2.2  应用平台安全 | 2.2.1  应用平台物理安全 | 当企业为行业用户提供了5G应用平台时，应明确应用服务器、机房、节点的地理位置，应具备一定的管理措施和技术措施确保其物理环境安全。 | 不涉及 | 该项目未向行业用户提供5G应用平台。 |
|
| 2.2.2  云计算/云服务安全 | 当应用平台采用了云计算技术或采购第三方云服务时，应确保计算存储资源/云服务安全。 | 不涉及 | 该项目未采用第三方云服务。 |
|
| 2.3  业务合作安全 | 2.3.1  合作方式合规性评估 | 应对合作方式进行合规性评估，确保应用合作模式符合行业经营管理相关规定。 | 不涉及 | 该项目不涉及第三方合作。 |
| 2.3.2  合作企业安全保障能力 | 应对合作企业的安全保障能力进行评估，确保其信息安全管理工作及保障措施可以满足相关法律法规要求，可以保障应用的信息安全。 | 不涉及 | 该项目不涉及第三方合作。 |
|
|

5G应用通用安全共有9个评估项，其中不涉及项4个，符合项5个，不符合项0个。

评估材料如下：

#### 应用基础安全

1. 应确定行业用户的应用规模情况，比如用户开卡数量。

**评估结果：符合。**

该项目开物联网卡6张，用于5G工业CPE。

b) 应确认行业用户的应用类型情况，明确用户所属行业类型和行业终端类型。

评估结果：符合。

该项目应用类型为设备接入，接入网关为5G工业CPE。

c) 应对行业用户身份信息进行认证登记，应留存行业用户单位有效证件（法人证书、经营许可证等）、责任人和经办人有效证件、责任人和经办人委托授权书以及经办人办理业务时的现场照片。

评估结果：符合。

手机屏幕截图

AI 生成的内容可能不正确。