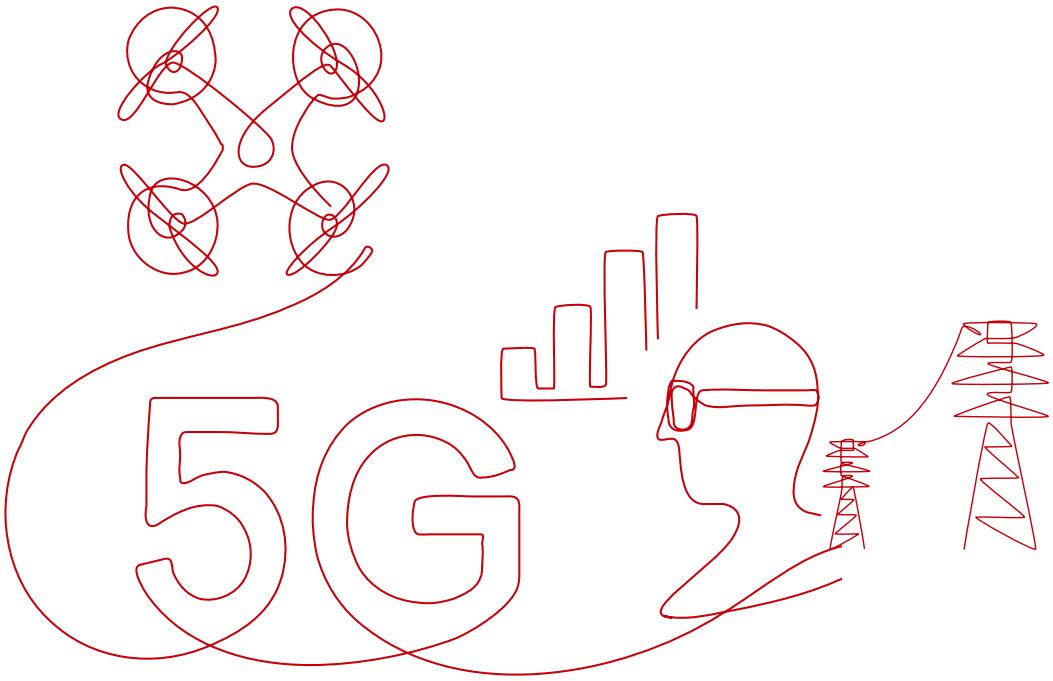
5GAIA 5G应用产业方阵 5G Applications Industry Array

5G DNA Deterministic Networking Alliance 确定性网络产业联盟

5G 电力虚拟专网网络安全白皮书



2022 年 3 月

目 录

前 言

5G 技术与电力行业深度融合，能够有效提升电力数字化、智能化水平，为构建清洁低碳、安全高效的电力体系提供有力支撑。网络安全是未来 5G 在电力行业规模化应用的先决条件，是 5G 赋能电力行业数字化转型的基础保障面，对电力行业“安全分区、网络专用、横向隔离、纵向认证”的安全防护原则要求，亟需设计兼顾 5G 传输性能与安全保障的网络安全防护体系。

2021 年 4 月，5G 应用产业方阵（5GAIA）及 5G 确定性网络产业联盟（5GDNA）共同立项了《5G 电力虚拟专网网络安全白皮书》，该白皮书由中国南方电网电力调度控制中心牵头，联合电力相关企业和运营商，以及通信设备和终端模组芯片厂家、网络安全产品及服务商，对 5G 电力虚拟专网网络安全方案进行了充分讨论及完善，并经 5GAIA 及 5GDNA 评审后，共同发布。

本白皮书也是 5GDNA 联盟继《5G 确定性网络 @ 电力系列白皮书 I：需求、技术与实践》（2020 年）、《5G 确定性网络 @ 电力系列白皮书 II：5G 电力虚拟专网建网模式》（2021 年）后发布的第 3 本系列化白皮书：《5G 确定性网络 @ 电力系列白皮书 III：5G 电力虚拟专网网络安全白皮书》，旨在将理论与实践相结合，分析 5G 网络应用于电力业务的安全需求及风险，从技术视角分析 5G 网络的安全能力并构建安全参考模型，从安全隔离、多层次认证、安全防护及监测等维度，提出可用、可信的 5G 电力虚拟专网安全参考方案，给出广域及局域的典型安全应用案例，并展望 5G 电力虚拟专网安全的发展趋势。

本白皮书主要编写单位及人员（以下排名不分先后）：中国南方电网电力调度控制中心的洪丹轲、陶文伟、曹扬、张国翊、朱海龙、林旭斌、胡飞飞，南方电网科学研究院有限责任公司的匡晓云、陈立明、索思亮，中国电力科学研究院有限公司的汪洋、丁慧霞、王智慧、马宝娟、孟萨出拉、朱思成，国网福建省电力有限公司的陈斌、陈端云、苏素燕、陈锦山、夏炳森、李源灏，中国信息通信研究院的杜加懂、王琦、侯伟彬、周洁，广东电网有限责任公司广州供电局的王莉、孙磊、王维，国网河南省电力公司信息通信公司的王文革、申京、赵豫京、杨莹、闫丽景，国网浙江省电力有限公司信息通信分公司的周鹏、陈逍潇、杨帆，中国移动通信集团有限公司的杨鹏、邱勤、周茉、崔旭升、吴沛喆、宋月、王荣，中国电信集团有限公司的沈军、刘亚天、呼博文、薄明霞、夏旭，中国联合网络通信集团有限公司的陈丹、王常玲、肖羽、蒋小燕，范勇杰，祝少波、蔡庆宇、赵元、李先达，华为技术有限公司的余晓光、余滢鑫、杨晓华、郝晶晶、阳陈锦剑，中兴通讯股份有限公司的滕志猛、冯岩、陈永波，广东省电信规划设计院有限公司的王劲、袁引，紫光展锐科技有限公司的张伟强、陈定云、朱勇旭，许继集团有限公司的徐涛，南京南瑞信息通信科技有限公司的胡阳、 张影、龚亮亮、李洋。

本白皮书参与编写单位及人员（以下排名不分先后）：中国移动通信集团广东有限公司的刘钢庭、王丹弘、任若冰，中国移动通信集团福建有限公司的魏颖强、孙柏宁，北京智芯微电子科技有限公司的贾强，深圳市广和通无线股份有限公司的李许安，国网山东省电力公司电力科学研究院的马雷、刘新、刘冬兰、王睿、张昊，国网山东省电力公司青岛供电公司的徐群、刘明峰、李坤、孟建、侯路，四川中电启明星信息技术有限公司的张立堃、曾山、王瑞祥等。

引 言

电力行业属于国家基础设施行业，关系国计民生，其包括电网企业和发电企业等，对业务分类、安全管控的总体要求基本一致。随着智能电网多样化应用场景的出现，以网络切片和 Multi-access Edge Computing (MEC) 多接入边缘计算为核心的 5G 网络在电力的发、输、变、配、用各环节逐渐得到规模应用，形成 5G 电力虚拟专网。

5G 电力虚拟专网是“在电信运营商的 5G 网络中，基于网络切片、 MEC、能力开放等技术，在无线、承载、核心网等环节虚拟出一张面向电力行业的专用网络，并与电力通信专网跨域融合，实现端到端的电力业务承载、高强度安全隔离以及资源管理。”

5G 电力虚拟专网的典型业务承载需求如下表所示：

业务类型	典型应用场景	承载现状	未来承载需求
基础类	智能分布式配电自动化、智能配电网微型同步相量测量、用电负荷需求侧响应、高级计量、分布式能源调控、充电桩、应急通信等	已有较成熟承载方案。 1、连接模式：子站 / 主站模式，主站集中 2、采集频次较低 3、控制能力相对粗放	1、连接模式：主站下沉，本地就近控制 2、采集频次提升（计量分钟级） 3、精准控制（毫秒级别，节点级）
扩展类	巡检机器人、输电线路无人机巡检、基于物联网的状态监测、智能营业厅、仓储管理、智能家居等	处于蓬勃发展及不断优化阶段。采集内容以基础数据、图像为主，单终端带宽为 100k~2Mbps，采集连接数有限	1、物联网技术广泛应用，连接数大幅增长 2、高清视频类业务大量应用，带宽需求爆发 3、融合采集与工业精准控制应用结合 4、结合 AI 进行深层次应用探索
特殊场景类	智慧园区、智慧电厂、地下厂房深度覆盖、三维空间定位、可视化运维、智能诊断、网源协调、决策支持等	处于起步探索和发展阶段	1、特殊环境下深度覆盖、空间定位需求迫切 2、海量传感器等物联网应用需求爆发 3、基于人工智能、大数据的网元协同，智能诊断和决策支持

面向上述需求，5G 电力虚拟专网能够为电网不同分区业务提供高可靠安全隔离解决方案，基于软件定义网络 (SDN, Software Defined Network) 和网络功能虚拟化 (NFV, Network Function Virtualization)、服务化架构 (SBA, Service-based Architecture) 等新技术提供物理资源、虚拟逻辑资源等不同层次的安全隔离能力。

但由于 5G 电力虚拟专网处于起步阶段，其安全体系方面仍需进一步完善，例如细化网络切片的安全隔离方案、终端二次认证的场景及流程等；同时随着能源大数据、综合能源服务等新兴业务不断涌现，电力业务环境更加开放、生态更加复杂、数据共享更加频繁，电力业务的承载网络安全架构也随之多样化，电力业务安全、数据安全等面临着安全防护手段与业务系统不匹配的严峻挑战，迫切需要对 5G 电力虚拟专网的网络安全防护进行探讨，并与电力业务安全防护体系进行融合集成，进一步提升 5G 电力虚拟专网的安全水平，为智能电网业务承载提供更好的通信安全保障。

本白皮书旨在从技术视角分析 5G 电力虚拟专网的安全需求，给出网络安全参考模型及架构，探索形成 5G 电力虚拟专网安全解决方案，并给出典型的 5G 电力虚拟专网安全应用案例。

02 5G 电力虚拟专网安全需求与风险分析

本章对 5G 电力虚拟专网承载电力业务的安全需求与应用风险威胁进行分析。

2.1 电力业务安全需求分析

根据《电力监控系统安全防护规定》(国家发改委 2014 年第 14 号)、国家能源局《关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范的通知》(国能安全 [2015] 36 号文)等相关规定要求，电力监控系统安全防护需满足“安全分区、网络专用、横向隔离、纵向认证”的原则。本章从电力业务安全需求出发，提出三类业务安全模式：高安全业务、中安全业务、通用安全业务。

高安全业务是指与电力调度生产直接相关的生产控制类业务，通常部署在生产控制大区涉及实时控制类及感知采集类业务，如安全自动控制系统、电能量计量系统等。高安全业务安全防护需求高，需通过无线虚拟专网和防火墙接入信息内网，再经过安全接入区(含正反向隔离、前置机、安全接入网关等)接入业务主站。

中安全业务是指管理信息大区的相关业务，其安全等级仅次于高安全区业务，涉及到智能电网生产管理、办公自动化，与生产或管理类的个人桌面计算机相关，如电力调度运行管理系统、资产管理系统等业务。中安全业务分布广泛，人机互动频繁，安全防护需求较高，需通过无线虚拟专网和防火墙接入信息内网，再通过安全接入平台接入业务主站。

通用安全业务是指互联网大区业务，其安全等级相对最低。主要面向互联网应用，以移动应用为主，如即时通信软件、培训教育等业务。该类业务安全防护需求不高，通过互联网通道实现接入。

2.2 5G 电力虚拟专网安全风险分析

当前，受限于 5G 电力行业应用产业链的成熟度，5G 电力虚拟专网存在着一定安全风险，尤其是在终端和模组方面，厂家较少、价格较高、形式单一、业务适配度较差，无法完全满足电力业务应用需求。应用层面，电力行业应用的业务相关系统中的服务器会生成、处理存储大量用户敏感信息，包括个人身份信息、用户隐私信息等，业务系统如果存在用户标识安全性、数据完整性与机密性等安全问题，遭到黑客攻击，容易造成用户数据泄露，用户隐私将受到威胁，造成较大的社会影响。此外，在复杂的电力场景下，5G 网络建设存在遭受电磁干扰的风险。

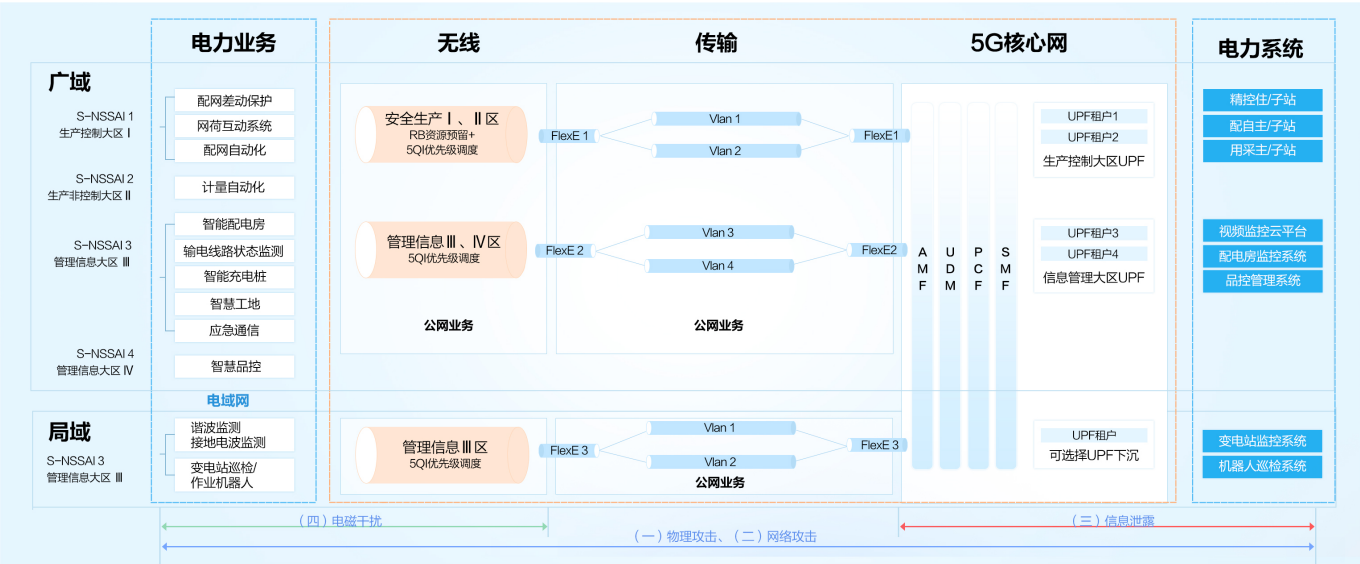


图 2.1 5G 电力虚拟专网面临的四类风险威胁点

如图 2.1 分析，5G 电力虚拟专网承载电力业务时可能存在物理攻击、网络攻击、信息泄露、电磁干扰四类风险威胁点，具体风险如表 2.1：

表 2.1 5G 电力虚拟专网风险威胁分类及举例

风险威胁	未来承载需求
（一）物理攻击	• 定向网络攻击基础设施信息系统，干扰物理系统运行，造成设备损坏和系统瘫痪，如网络攻击 + 物理破坏导致全国停电。 • MEC、UPF 节点被物理破坏：通过破坏物理防护措施或利用管理漏洞对 MEC、UPF 设备进行破坏、非授权访问，导致设备损坏、通信中断等风险。
（二）网络攻击	• 网络入侵、计算机病毒等网络空间攻击，导致电网的信息系统故障，如蠕虫网络攻击。 • 身份仿冒，通过截获合法用户身份信息并假冒该合法用户的身份访问网络 • 篡改，通过非法截获数据包等方式恶意篡改用户数据信息。 • 非法访问，对切片内的资源可能被其他切片中的网络节点非法访问，导致切片内部的故障和错误，影响可能其他切片的工作。 • 拒绝服务，利用 DDOS 攻击目标服务器或网络基础设施，导致业务服务不可用 • 设备版本破坏风险，版本文件（包括软件版本文件（.set）以及补丁文件（.pkg））和固件文件，从发布直到现场进行文件的安装升级，整个过程存在文件被篡改以及损坏的风险。
（三）信息泄露	• 数据泄露，核心网中数据库存在 SQL 注入、默认账户口令、数据库平台漏洞、滥用合法权限、非法提权等风险。 • 在 5G 环境下，用户隐私信息涉及用户标识、移动模式、位置信息、数据使用模式等内容。攻击者可通过多种手段获取这些用户隐私信息。
（四）电磁干扰	• 干扰无线工作频段，通过无线发射器等可干扰无线信道，使通信中断，导致业务终端“致盲”，脱离管控。

2.3 5G 电力虚拟专网安全需求分析

根据三种电力业务安全模式及 5G 电力虚拟专网风险分析情况，结合 5G 通信技术特性，提出 5G 电力虚拟专网承载电力业务的安全需求，具体如下：

表 2-2 5G 电力虚拟专网承载电力业务安全需求

序号	安全风险	安全需求	安全模式		
			高	中	通用
1	物理攻击	监测 + 响应	端到端设备全天候全方位的安全监测、制定安全管理策略、更新漏洞及补丁	端到端设备全天候全方位的安全监测、制定安全管理策略、更新漏洞及补丁	电力设备的安全监测、制定安全管理策略、更新漏洞及补丁
2	网络攻击	隔离 + 加密	物理隔离、电力专用安全加密算法及专用加密认证装置、多层次认证、增强认证的5G电力通信终端、网络异常监测	强逻辑隔离或物理隔离、电力专用安全加密算法及专用加密认证装置、多层次认证	逻辑隔离、电力专用安全加密算法、5G 网络主认证与切片认证
3	信息泄露	加密 + 认证	电力专用安全加密算法及专用加密认证装置、多层次认证、增强认证的 5G 电力通信终端	电力专用安全加密算法及专用加密认证装置、多层次认证	电力专用安全加密算法、5G 网络主认证与切片认证
4	电磁干扰	监测	电磁环境在线监测	电磁环境在线监测	电磁环境在线监测

03 5G 电力虚拟专网安全参考模型和架构

本章节重点从隔离、认证、安全监测与响应等应用方面，对高安全业务、中安全业务、通用安全业务三种模式的电力业务开展需求匹配，有针对性地提出 5G 电力虚拟专网的安全参考模型和架构。

3.1 5G 承载电力业务的安全模型

基于 5G 网络通信能力，以高安全业务、中安全业务、通用安全业务三种模式电力业务为维度，构建了包括隔离、加密、认证、监测、响应等五个方面的安全模型，如下图所示：

图 3-1 5G 电力虚拟专网安全模型

模型中的隔离指对接入网资源（包括基站处理资源和无线频谱资源）、承载网资源以及核心网资源，按照不同切片方案进行划分，可包括硬隔离和软隔离。

a. 硬隔离

硬隔离接近于物理隔离强度，也称为类物理隔离。例如为实现生产控制类业务和生产管理类业务的隔离，在无线侧使用独立频谱、RB 资源预留等方式，提供不同无线资源，在传输侧使用传输设备承载信令和用户面数据，并支持 FlexE 硬切片，在核心网侧新建业务专用的边缘 UPF，控制面建设独立的专用功能单元，通过安全接入区接入站内的自有业务平台。

b. 软隔离

软隔离接近于逻辑隔离强度。例如不同大区区域内部，根据业务需求进行分类，不同分类采用不同的 S-NSSAI 实现隔离。在无线侧采用不同业务共享 RB 预留资源以及 5QI 优先级调度，在传输侧支持基于 VPN 等技术，在核心网侧可以根据业务需要，用户面采用专用的或共享 UPF，控制面采用部分网元专用或全部网元共享方式，满足不同电力业务对于安全隔离的需求。根据传输侧是否采用 VPN 加密技术、核心网侧是否采用专用网元情况，将软隔离方式分为强逻辑隔离和普通逻辑隔离两种方式。

模型中的数据隐私保护主要包括终端数据加密存储，通信过程中的数据加密传输。

模型中的安全认证是指终端身份认证，终端数据与系统授权访问。

模型中的网络安全感知和监测是通过对 5G 整体网络进行监测来识别突发的恶意行为。

模型中的安全事件响应指对监测到的攻击行为进行告警及处置，包括接收、处理所使用产品或解决方案相关的安全漏洞，以及针对物理攻击、电磁干扰等事件的处置等。

3.1.1 高安全业务应用安全模型

高安全业务需采用电力专用通信网络进行加密传输和身份认证，并与其他安全等级的业务在通信网络上实现类物理隔离的安全防护能力。同一业务内处于低等级安全防护能力的设备和网络，应当通过必要的安全隔离措施实现与高等级安全防护能力的设备和网络互联。高安全业务应在满足其高实时、密集接入的前提下提供高性能等级的监测能力，并能在网络故障、受入侵等情况下提供相应业务能力要求的响应恢复能力。

3.1.2 中安全业务应用安全模型

中安全业务可与因特网互联，但应采取强逻辑隔离或类物理隔离措施，以及必要的认证、加密、访问控制措施，防止来自互联网侧的网络攻击，保证业务系统柜接入的可信性。中安全业务应特别强调满足视频监控类业务的安全防护要求。

3.1.3 通用安全业务应用安全模型

通用安全业务可采用因特网通信或 VPN 网络进行传输和身份认证，应能监测来自互联网的攻击行为，提供与业务相适应的安全防护能力。

3.2 5G 电力虚拟专网总体安全参考架构

5G 电力虚拟专网在支撑智能电网应用发展过程中，首先需要遵循国家能源局关于电网安全防护“安全分区、网络专用、横向隔离、纵向认证”的基本原则，其安全架构包括“云、管、端”三大层级，涉及终端安全、管道安全和平台安全和安全管理四个方面，如图 3-2 所示。

图 3-2 5G 电力虚拟专网总体安全参考架构

上图中的 5G 电力虚拟专网总体安全参考架构，其核心在于针对 5G 安全风险威胁构建终端、管道、平台等层面的安全防护能力以及 5G 电力虚拟专网的安全管理能力，以此来满足不同安全等级的电力业务的需求。

1、终端安全：可集成电力定制化安全模块，支持基于国密算法的非对称加密技术进行终端加密，实现主站对终端的身份鉴别和报文完整性保护。对重要终端，可采用双向认证、数据加密和零信任等接入访问控制技术。此外，对于特定的重要业务，还可以采用机卡绑定、终端 DNN 与网络切片绑定等安全策略。

2、管道安全：重点是利用 5G 高强度安全隔离的网络切片技术和可定制切片管理，为不同安全等级电力业务制定不同的切片策略，提供不同的专网安全保障服务。

3、平台安全：针对不同的电力业务设置不同安全服务区，服务区之间部署防火墙等防护措施防止跨应用攻击；部署二次认证 AAA 服务器和边界网管，防止非法终端接入和恶意攻击入侵。

4、安全监测：通过运营商将 5G 网络安全能力共享给电力行业的应用，对终端、切片、MEC、专用 UPF、安全防护设备等进行统一监控，实现全天候全方位 5G 电力虚拟专网网络安全态势感知。

04 5G 电力虚拟专网安全参考方案

本章针对业务需求，根据 5G 电力虚拟专网需遵循的“安全分区、网络专用、横向隔离、纵向认证”基本防护策略要求，在端侧、管侧、云侧等维度，为不同安全等级的电力业务提供不同的安全能力组合及参考方案，具体如下：

4.1 端到端切片安全隔离，提供电力虚拟专用网络

根据电力业务要求，需在不同安全分区或同一安全分区不同业务之间采用不同强度的隔离手段，例如针对高安全业务采用达到或接近物理隔离的隔离强度，针对中安全业务采用接近物理隔离或强逻辑隔离的隔离强度，针对通用安全业务采用普通逻辑隔离的隔离强度等。由此需要在 5G 电力虚拟专网的接入网、传输网、核心网等环节采用不同的隔离手段来实现灵活的横向隔离。

4.1.1 接入网隔离

5G 接入网隔离调度方式主要通过 5QI（5G Quality Identifier，5G QoS 标识符）优先级和 RB（Resource Block，资源块）资源预留，其中 RB 资源预留是 5G 区别于 4G 的重要特性。

根据电网不同业务对隔离性的不同要求，可以采用三类隔离方案：

（1）完全共享模式，无线资源完全共享。每个切片不直接参与资源的调度，由一个公共的调度来负责。

（2）部分独占模式，无线资源主要由 5QI 根据优先级进行调度，并基于 PRB 资源预留技术承载独占切片业务。

（3）完全独占模式，无线接入网使用独立的硬件资源和频谱资源，具备最高的安全性，但是建网成本会大幅增加。

4.1.2 传输网隔离

5G 无线接入网和核心网之间的传输网络可通过网络切片进行业务隔离。不同切片网络的转发面彼此隔离，而隔离性取决于采用不同的转发面切片技术。切片技术分为硬隔离切片和软隔离切片。

硬隔离切片是在 L1 或光层，基于物理刚性管道的切片技术，如：FlexE 技术、OTN 技术、WDM 技术。

软隔离切片是在 L2 或以上，基于统计复用的切片技术，如：基于 SR、MPLS-TP 的隧道 / 伪线技术，基于 VPN、VLAN 等的虚拟化技术。

在实际应用中，也可以采用混合硬隔离切片、软隔离切片的方案，硬隔离切片方式保证业务的隔离安全、低时延等需求，软隔离切片方式支持业务的带宽复用。

4.1.3 核心网隔离

5G 核心网隔离方案有完全共享、部分独占和完全独占三种模式，可依据电网的不同业务类型进行选择：

（1）完全共享模式，与 2/3/4G 网络的“一条跑道、尽力而为”一致，适用于对安全无特殊要求的公众网普通消费者业务。

（2）部分独占模式，少量网元功能独占与大部分网元功能共享相结合，平衡了安全性与成本，主要适用于高、中两大类安全类型业务。

（3）完全独占模式，等同于建设一张完整的电力行业专用核心网，具有最高的安全性，建设和运营成本也最高，适用于需要超高安全隔离性而对成本不敏感的特殊业务。

在实际组网中，应根据不同业务安全等级和隔离要求来选择接入网、传输网、核心网的隔离方式。例如针对高安全隔离要求的应用，无线侧应采用 RB 资源预留，承载传输网侧应采用 FlexE 硬管道隔离，核心网采用部分独占模式、独占用户面网元 UPF 模式或将用户面网元 UPF、信令面网元 AMF/SMF 均独占的进行组网。针对低安全隔离要求的应用，无线侧可采用完全共享模式或 5QI 高优先级调度技术、承载网侧可采用 VPN 管道进行软隔离、核心网可采用完全共享模式，共用运营商边缘 UPF 进行组网。

4.2 多层次认证体系，满足纵向认证要求

根据电力业务要求，需采用认证、加密、访问控制等技术措施实现数据的远方安全传输以及纵向边界的安全防护。4G 网络中，各业务仅能通过 APN 名称及密码实现不同业务接入网络的认证，一旦认证信息泄露，则存在电力网络被非法接入的风险。由此需要 5G 电力虚拟专网能够提供终端接入认证、二次认证等纵向认证措施，以确保终端接入主站的合法性。

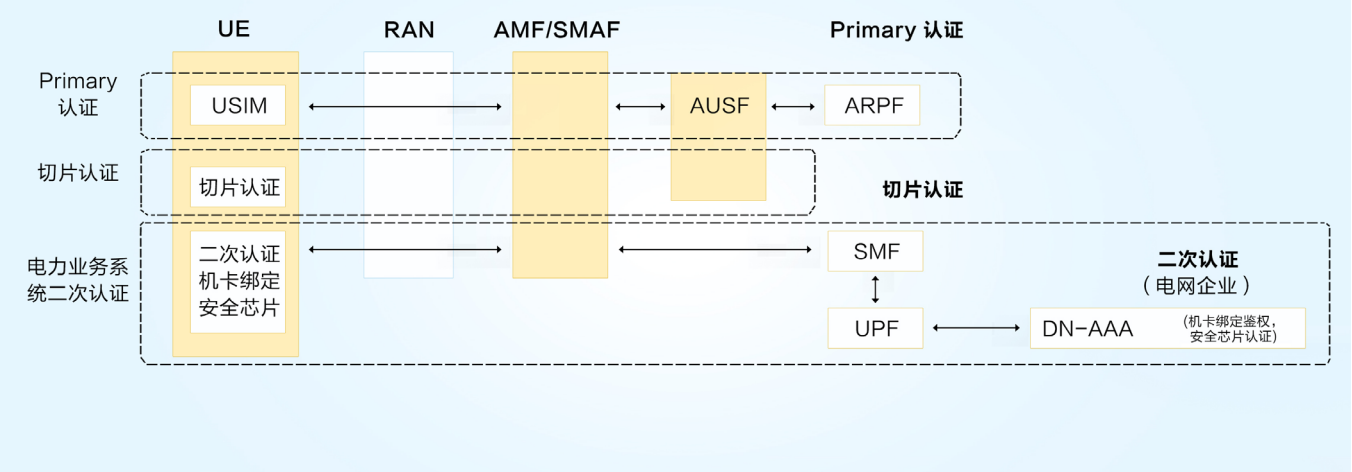


图 4.1 多层次鉴权认证

具体手段可包括：

机卡绑定：核心网侧将终端 USIM 卡的 IMSI 与设备 IMEI 进行绑定认证，如果二者不匹配则拒绝接入网络；

二次认证：基于 3GPP 二次认证架构及标准协议完成终端到 DN-AAA 服务器之间的终端二次鉴权认证，二次认证失败后则不允许终端访问电力业务；

安全模块认证：终端集成国密型号的安全模块，与中心侧 IPSec VPN 安全网关之间建立 VPN 数据传输通道，实现网络层双向身份认证。

在实际应用中，应根据不同业务安全等级和纵向认证要求来选择合适的隔离方式。尤其是在 5G 引入多层次鉴权认证体系的前提下，可视业务数据加密和身份认证需求，灵活使用相应的鉴权认证模式，简化传统基于硬件安全模块的通道加密及双向身份认证模式。

4.3 云边协同的安全应用，支撑安全防护及监测

针对云边协同的安全应用，需根据 5G 安全开放能力实现对 5G 电力虚拟专网的 MEC 安全防护、安全态势感知，并可针对部分业务开展 5G+ 区块链的安全认证模式探索。

4.3.1 基于基础设施和 APP 业务的 MEC 安全防护

电力 MEC 中包含连接（UPF，运营商可信域）与计算（MEP+ 第三方 APP，运营商不可信域）两部分，可采用如下手段提升电力 MEC 安全性。

1、针对 MEC 平台能力开放的特性，部署 vFW（虚拟防火墙）等虚拟化安全组件对来自边缘 APP 的访问进行过滤。APP 与 MEC 平台之间可按需进行访问控制及数据传输安全机制，如机密性、完整性保护及防重放攻击。通过漏洞及端口扫描手段来关闭 MEC 平台不必要的端口和服务。

2、提供 APP 全生命周期安全防护，保障业务及应用安全。对 APP 使用的资源进行隔离，对 APP 镜像和镜像仓库进行完整性和机密性、访问控制保护。另外，对 APP 提供包括身份安全、镜像安全、入侵检测等的安全防护。

4.3.2 全天候全方位的 5G 网络安全态势感知

电力企业通过部署网络安全态势感知系统，集成用户侧安全设备内置的安全探针、运营商安全能力开放平台开放的网络安全能力，下发安全策略，上报安全设备信息，可以缩短端到端 5G 电力虚拟网络的威胁发现时间，提供事前预防、事中隔离、事后回溯的能力，提升安全事件的响应速度，保障网络安全“规划、建设、运营”三同步。

4.3.3 5G+ 区块链的安全认证模式

5G 电力虚拟专网的融合性，以及 5G 边缘计算的分布性特征与区块链应用具有一定的匹配性。一方面，电力专用 UPF/MEC 既是电力客户用户面的专用网元，也同时受到运营商控制面的管理，是未来电力企业与运营商企业构建联盟链区块链的关键节点；另一方面，电力专用 UPF/MEC 的分布式部署、具有算力能力等特征，同样匹配区块链的去中心化应用特点。

因此，在 5G 系统自身的认证及数据加密的基础上，可通过 5G 能力开放、MEC 边缘计算等技术，叠加区块链技术，使 5G 电力虚拟专网跨域信息上链，尤其是基于电力企业、运营商企业的联盟链，在面向配电网终端可信接入、配电网差动保护的局域通信群组成员管理、需求侧响应、网荷互动、虚拟电厂、电力市场交易等场景，进一步提高融合信息的防篡改能力及安全可信度。

4.4 数据加密传输

针对 5G 电力虚拟专网的数据加密传输需求，可将 5G-CPE 终端与国密型号的安全模组一起实现 IPSec VPN 隧道，支撑终端安全接入认证及通信加密。对于重点防护的调度中心、发电厂、变电站，由于其数据的高度敏感性，应当设置经过国家指定部门检测认证的电力专用纵向加密认证装置或加密认证网关及相关设施，实现端到端的双向身份认证、数据加密和访问控制。加密认证网关除具有加密认证装置的全部功能外，还应实现电力系统数据通信应用层协议及报文的处理。

此外，5G 通信机制要求用户数据必须先经过 UPF 再进行转发，从而实现了从终端至基站至 UPF 的传输隧道，且不暴露在公网上，保障了用户通信数据安全。

针对 5G 电力虚拟专网的信令面数据加密传输要求，在如 N2、N3、N4 等信令面非服务化接口上需启用内置或外置 IPSec VPN 隧道对信令面数据传输过程中提供加密性保护和完整性保护，同时提供接口间的认证机制，防止攻击者仿冒网元对 5G 电力虚拟专网进行信令攻击。

针对数据泄露、勒索攻击等数据安全威胁，可通过数据分级分类、敏感数据加密、流量监测等措施，提供覆盖数据存储、处理、交换等环节的一体化数据安全防护。

4.5 安全事件响应

智能电网业务及应用系统众多，对机密性、完整性、可用性、可靠性等方面要求高，而 5G 新技术多，参与方多，体系复杂，要保证电力业务安全可靠运行，预防各种网络安全事件的发生，需要 5G 电力虚拟专网提供高效的安全事件响应能力，有效实现各方协同联动，共同应对 5G+ 智能电网安全挑战。因此，电力企业可与运营商、供应商、行业协会、标准组织等业界伙伴合作构建生态合作体系，充分利用外部技术力量做好安全事件的预防、监控与处理。例如，建立安全事件响应流程与机制；扫描和接收来自企业内部、外部的网络安全事件或漏洞报告；确认事件或漏洞是否存在，确定严重级别、影响范围；分析其根本原因以及抑制、消除影响的方案；监控事件或漏洞方案实施进展情况；针对电磁干扰及物理破坏等开展监测并给出响应措施。

05 5G 电力虚拟专网安全应用

5.1 5G 电力广域虚拟专网应用案例

5G 电力广域虚拟专网应用方面，已应用案例按照 5G 电力虚拟专网顶层架构方案，基于 5G SA 切片网络，在某供电区域建设了涵盖发、输、配、变、用、综合 6 大类、51 个业务场景的 5G+ 智能电网应用示范区。

目前示范区内已经完成了变电设备在线监测、配电自动化、配网差动保护、配网 PMU 等生产控制类业务，以及输电线路状态在线监测及视频监控、巡检机器人、智能配电房等管理信息大区业务的试点运行。目前各业务试点整体运行情况良好，打造了广域环境下 5G 电力虚拟专网业务安全应用的创新模式。

1. 可靠的安全隔离性能。基于 5G 电力虚拟专网顶层架构，通过在无线侧空口 RB 资源预留、传输侧配置 FlexE 硬管道、核心网侧开通电力专用切片、部署电力专用的 UPF+MEC 设备，实现了电力业务与其它公众用户、行业用户业务的隔离，确保承载生产控制类业务的 5G 切片具备端到端隔离性能，改善了 4G 网络下只具备逻辑隔离条件的掣肘，充分满足电力业务承载的安全性要求。

2. 稳定的超低时延和精准授时性能。基于 5G 的超低时延和精准授时性能，满足了配网差动保护及配网同步相量测量业务的承载需求。根据在示范区的测试情况，广域条件下配网差动保护业务平均时延达到毫秒级，延时抖动导致的最大延时大幅降低，差动保护采样幅值误差均大幅减小，PMU 授时精度显著提升，充分满足了业务承载需求。

3. 完善的业务安全监视 / 态势感知性能。基于运营商网络能力开放，电力搭建了 5G 网络管理平台，实现了对电力 5G 业务、网络切片性能、电力终端的统一管理，解决电力 5G 应用场景丰富多样，网络组网架构复杂多变的背景下，对网络灵活管控的需求、网络通道管理的需求、海量终端监控的需求，降低网络运维复杂度，保障电力 5G 应用安全、高效、可靠运行。

5.2 5G 电力局域虚拟专网应用案例

5G 电力局域虚拟专网应用层面，已应用案例在火电厂、换流站等场景，通过共建共享等方式实现了 5G 网络全覆盖，提高智能化运维及管理水平。

火电厂应用案例内的 5G 电力虚拟专网全面采用了 uRLLC、mMTC、eMBB 三种 5G 网络切片，应用成果覆盖 5G+ 大型工业系统控制、5G+ 移动视频监视、5G+ 传感器接入、5G+ 人员安全管控、5G+ 智能巡检、5G+ 设备运维诊断、5G+ 安全应急等典型火电厂业务场景。运用 5G 网络融入了火电厂智能发电平台 ICS、智慧管理平台 IMS 的全业务领域，采用了如下电厂内 5G 专网安全应用模式，有效支撑了各项业务应用网络化、信息化、数字化、智能化。

1、高质量覆盖。通过 5 个室内外 5G 宏基站、37 个 5G 微基站，构建了厂级 5G 自组织网络，实现了火电厂区 0.28 平方公里 5G 信号的高质量无死角全覆盖。5G 网络下行速率 350Mbps, 上行速率 160Mbps，网络双向时延小于 15ms，支持 10 的 7 次方个终端 / 平方千米的连接密度，数据处理能力超过 10Gbps。

2、安全自主可控。基于 5G 网络 uRLLC 切片技术划分生产控制网络，并采用孤网运行、安全接入区、MEC、安全隔离、日志审计、态势感知、流量监测等技术措施，保证了网络安全自主可控。

3、业务融合应用。实现 5G 与火电分散控制系统 DCS 的融合应用，建设了全覆盖、全业务应用示范的 5G+ 智慧火电厂，实现了初级的全域感知、状态预警、多场协同、限域优化、精准控制、综合提效。

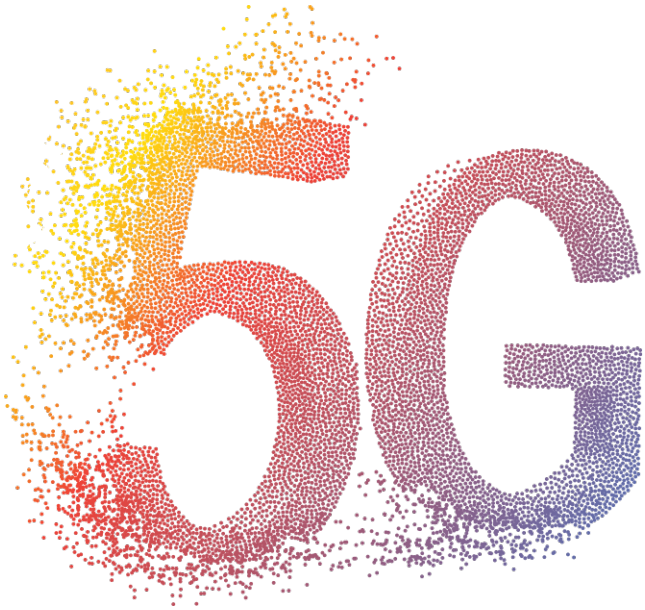
换流站应用案例内的 5G 电力虚拟专网主要为中安全业务和通用安全业务，例如：现场作业管控终端、设备移动监控、单兵作业终端、智能巡检机器人、灭火机器人、电力无人机等，为满足各类业务的安全接入与应用效果，采用了如下 5G 园区专网安全应用模式：

1. 灵活的业务可靠接入。换流站各种类型业务终端的相应系统一般部署在站内或者省电力公司，MEC 灵活的数据分流及转发卸载能力，解决了各类业务的灵活接入问题。通用安全业务的数据经 MEC 向公网分流，最终进入电力公司互联网大区；中安全业务系统部署于省电力公司时，终端数据经 MEC 分流后通过电力通信网传输至省电力公司接入相应系统；中安全业务系统部署于换流站时，终端数据经 MEC 本地卸载后接入站内服务器，经 MEC 分流后的业务数据进入管理信息大区需经过安全接入网关等安全防护设备。

2. 安全的数据隔离保障。换流站部署的 5G 基站与 MEC 均为电力专用，通过搭建 5G 局域虚拟专网，保证电力业务数据不出园区，达到了较高的安全隔离效果。同时业务数据传输过程采取机卡绑定、二次认证、安全模块认证等技术，实现终端和业务之间的安全传输，满足各类作业终端安全接入的防护要求。

3. 高性能的业务应用体验。5G 园区专网可灵活进行无线侧帧结构配置，保证上下行速率配比，提升网络 Qos 保障性能。换流站连续两年在年度检修工作中，利用 5G 大带宽能力保障现场作业管控、安全布控球等设备的实时传输，实现多个作业面、大量作业人员的实时安全管控，管控效率显著提升。根据站内测试情况，终端数据经 MEC 本地卸载后直接进入服务器的单向平均传输达到了超低时延的通信性能，机器人、无人机等终端的移动视频传输质量及音视频交互效果显著提升。

06 总结与展望



5G 是全球新一轮科技革命和产业变革的代表核心技术之一，“5G+ 数字电网”融合发展是电网数字化转型和新型电力系统建设的现实需求，将为双碳目标达成提供强有力的数字底座。

为深入贯彻习近平网络强国重要思想，服务新型电力系统建设和数字化转型，为电力行业“5G+ 数字电网”建设及规模化应用提供可靠的网络安全保障，5G 电力虚拟专网也需随着行业需求的发展不断提升切片的安全能力。

技术方面，随着 5G 技术的演进、业务需求的变化、攻防技术的发展，需不断丰富网络切片在无线、传输、核心网各个环节的安全保障手段，5G 电力虚拟专网将完善自身的安全管理，实现自主、安全、可控的目标。同时，5G 网络的切片安全也会不断向智能化方向发展，提供灵活、可定制的安全能力组合机制，方便垂直行业选择与业务需求匹配的安全能力、管理手段。

应用方面，5G 相关产业链上下游企业将持续支撑智能电网的发展需求，助力电力行业数字化发展，打造一批跨行业创新应用以及 5G 应用安全创新示范中心，并加强开放合作互信，共同应对 5G 安全风险、加快推进 5G 安全国际标准，凝聚全球共识建立 5G 安全国际评测认证体系，推动实现互信互认以及加强产业链上下游合作，提振 5G 安全信心。

附录 A：术语及缩略语

5GC:	5G Core 5G 核心网
5GDNA:	5G Deterministic Network Association 5G 确定性网络产业联盟
AMF:	Access and Mobility Management Function 接入和移动管理功能
AUSF:	Authentication Server Function 鉴权服务器功能
DTU:	Data Transfer Unit 数据传输单元
NSSF:	Network Slice Selection Function 网络切片选择功能
PCF:	Policy Control Function 策略控制功能
PMU:	Phasor Measurement Unit 相量测量装置
RB:	Resource Block 资源块
SMF:	Session Management Function 会话管理功能
UDM:	Unified Data Management 统一数据管理
UPF:	User Plane Function 用户平面功能

附录 B：参考文献

1. 南方电网 . 办总调 [2022]4 号《南方电网 5G 电力应用安全防护总体方案（试行）》.2022 年
2. 5G 确定性网络联盟 .《5G 确定性网络 @ 电力系列白皮书 II：5G 电力虚拟专网建网模式》. 2021 年
3. 3GPP TS 23.501 5G 系统架构 System Architecture for the 5G System
4. 3GPP TS 29.531 网络切片选择服务 Network Slice Selection Services
5. 国家能源局 . 国能安全 2015【36 号】《电力监控系统安全防护总体方案》. 2015 年
6. 5G 确定性网络联盟 .《5G 确定性网络 @ 电力系列白皮书 I：需求、技术及实践》. 2020 年
7. 5G 应用产业方阵 .《5G 行业虚拟专网网络架构白皮书》. 2020 年
8. 中国移动 .《中国移动 5G 行业专网技术白皮书》. 2020 年
9. 中国电信 .《中国电信 5G 定制网产品指导手册》. 2020 年
10. 中国联通 .《中国联通 5G 行业专网白皮书（2020）》. 2020 年
11. 国家电网 , 中国电信 , 华为 .《5G 网络切片使能智能电网产业报告》. 2018 年
12. 中国南方电网 , 中国移动 , 华为 .《5G 助力智能电网应用白皮书》. 2018 年
13. 中国信通院 , IMT-2020（5G）推进组 .《5G 安全报告》. 2020 年

版权声明