5G电力行业应用安全需求与架构白皮书

IMT-2020(5G)推进组

2022年11月

目录

1 引言

近年来，在人工智能、物联网等数字技术支持下，我国电力行业不断取得突破进展，智能电网建设初见成效。5G与智慧电网的结合将产生强大的化学反应，加速电力行业数字化转型，赋能电力行业精准、高效、安全地运维，促使其走出一条数字经济和能源经济融合发展之路，这无疑给电力上下游企业取得新一轮增长注入了新动能。

电网是关系国计民生的国家重要基础设施，如果发生大规模电力事故，将可能导致数以百万计的人受到影响，造成严重的经济损失和人员伤害。因此安全是智能电网压倒一切的根本性需求，需加强电力监控系统的信息安全管理，防范黑客及恶意代码等对电力监控系统的攻击及侵害，保障电力系统的安全稳定运行。我国国家发展与改革委员会于2014 年发布了《电力监控系统安全防护规定》（国家发展改革委员会 2014 年第14 号令），规定中指出电力监控系统安全防护工作应当落实国家信息安全等级保护制度，按照国家信息安全等级保护的有关要求，坚持“安全分区、网络专用、横向隔离、纵向认证”的原则，保障电力监控系统的安全；国家能源局于 2015 年发布了《电力监控系统安全防护总体方案》（国能安全[2015]36 号），方案确定了电力监控系统安全防护体系的总体框架，细化了电力监控系统安全防护总体原则，定义了通用和专用的安全防护技术与设备，提出了各级调度中心、发电厂、变电站、配电等的电力监控系统安全防护方案及电力监控系统安全防护评估规范。

电力系统对安全要求高，故障需要实时快速响应，对通信系统要求更为严格， 5G网络切片具有高强度隔离承载特性，可实现不同分区电力切片间互不影响、业务公平调度、质量可保障；5G端到端网络传输时延小于10毫秒，基于5G网络的精准时延控制、微秒级高精度网络授时能力，能满足配网差动保护等生产控制类业务的严苛通信需求，可实现故障精确定位和快速隔离。不过，5G网络原生的安全能力对于电力行业而言不能拿来就用，还需要网络设备商、集成商、解决方案提供商、芯片模组厂商等产业各方的共同配合，根据电力业务特点为适配电网安全稳定运行而作出革新改变，共同建成“具有电力特色的5G安全防护体系”。本白皮书通过对智能电网的安全政策和对5G网络切片安全需求的研究，提出适用于智能电网的5G网络安全参考架构，并对5G智能电网网络安全提出后续发展建议。

2 5G 电力行业应用概述

2.1 5G 智能电网概述

智能电网是以物理电网为基础，将现代先进的传感测量技术、通信技术、信息技术、计算机技术和控制技术与物理电网高度集成而形成的新型电网。智能电网从电厂到用户整个配输电过程中，感知所有节点之间的信息和电能的双向流动，在一定程度上对国家电网在效率、减排以及提高鲁棒性和安全性方面产生积极影响。

随着国内5G基站和网络部署的日趋完善，5G三大场景具备的超高带宽、超低时延、超大链接的技术特点在电力信息系统中发挥着至关重要的作用，可更好地促进资源优化配置。通过5G切片技术满足资源保障、安全性、可靠性/可用性等多方面的隔离需求，具体到电力应用场景，可以支持多种不同的资源隔离与共享方式，以适配不同等级的性能、功能以及隔离要求。

在电力系统生产控制大区、管理信息大区、互联网大区业务类型繁多，生产、控制、管控新业务的持续涌入，使得其对时延、抖动、带宽等网络性能要求不同，且对安全隔离和安全管控的需求度增高。电力通信网作为支撑智能电网发展的重要基础设施，需满足各类电力业务的安全性、实时性、准确性和可靠性要求。构建大容量、安全可靠的光纤骨干通信网，以及多业务灵活可信接入的配电通信网，是电力通信网络建设的两个重要组成部分。在骨干通信网侧，经过多年建设，35kV以上的主网通信网已具备完善的全光纤骨干网络和可靠高效数据网络，光纤资源已实现35kV及以上厂站、自有物业办公场所/营业所全覆盖。在配电通信网侧，由于点多面广，海量设备需要实时监测或控制，信息双向交互频繁，且现有光纤覆盖建设成本高、运维难度大，公网承载能力有限，难以有效支撑配电网各类终端可观可测可控。随着大规模配电网自动化、高级计量、分布式能源接入、用户双向互动等业务快速发展，各类电网设备、电力终端、用电客户的通信需求爆发式增长。

为应对日益多样化的电力需求和丰富的电力场景及应用条件，满足电力行业不同业务场景信息流、能量流及业务流的贯通、促进电力系统整体高效协调运行，电力行业的5G多元化应用场景应运而生。5G技术在以下场景具有优势：新能源及储能并网，输变电运行监控，配电网调控保护，用户负荷感知与调控，协同调度及稳定控制，在跨区域送受端协调控制，提

升电网供电可靠性，提升电力在尖峰负荷时期的运行可靠性和安全性，低延时传输和多参量数据融合处理，提高电网优化配置资源效率等。

2.2 5G 电力典型应用概述

5G在电力行业主要有四大应用场景，分别为控制类业务、采集类业务、移动应用类业务、以及以多站融合为代表的电网新型业务。在控制类业务中，5G技术将优化能源配置，避免大面积停电从而影响企业和居民用电，同时也将满足配电网实时动态数据的在线监测应用；在采集类业务中，5G将推动收集和提供整个系统的原始用电信息；在移动应用类业务中，5G预防安全事故和环境污染，减少人工巡检工作量，在未来可进行简单的带电操作；在多站融合业务中，5G技术将推进平台型、共享型企业建设。

(1)生产控制类业务

控制类业务中，典型的业务有精准负荷控制业务、智能分布式配电自动化业务、配网差动保护业务。

精准负荷控制业务场景，解决电网故障初期频率快速跌落、主干通道潮流越限、省际联络线功率超用、电网旋转备用不足等问题，根据不同控制要求，分为实现快速负荷控制的毫秒级控制系统和更加友好互动的秒级及分钟级控制系统。

表2 精准负荷控制场景5G通信需求

业务类别	业务名称	通信需求				
		时延	带宽	可靠性	安全隔离	连接数
控制类业务	精准负荷控制	≤50ms	≤2Mbps	99.999%	安全生产Ⅰ区	X*10 个/km2

智能分布式配电自动化业务场景，配电自动化终端和主站的通信采用104或101规约，实现了电能召唤、时间同步、遥测、遥信和遥控等功能，向用户提供安全可靠的电力供应和优质高效的供电服务，同时也将满足于配电网实时动态数据的在线监测应用。

表3 分布式配电自动化场景5G通信需求

业务类别	业务名称	通信需求				
		时延	带宽	可靠性	安全隔离	连接数
控制类业务	分布式配电自动化	≤50ms	≤2Mbps	99.999%	安全生产Ⅰ区	X*10 个/km2

配网差动保护业务场景中，配电自动化终端定期给同一条配网线路上的其它终端发送电流矢量值（Sv采样值），DTU终端通过比较两端或多端同时刻的电流矢量值，并根据电流差值执行对应的差动保护动作。配网差动保护终端应支持通过5G网络给同一条配网线路上的其它终端发送电流矢量值。配网差动保护通过5G高精度授时技术可实现精准的同步对时。

表4 配网差动保护场景5G通信需求

业务类别	业务名称	通信需求					
		时延	带宽	可靠性	授时	安全隔离	连接数
控制类业务	配网差动保护	≤15ms	≥2Mbps	99.999%	us 级	安全生产Ⅰ区	X*10 个/km2

(2)电网采集类业务

电网采集类业务中，对通信需求的典型特征是点多面广，有线通信方式覆盖难度大，对通信时延要求不高，适合5G技术体制下的mMTC应用场景，典型的业务有用电信息采集等。

用电信息采集业务场景可实现用电信息的自动采集、计量异常监测、电能质量监测、用电分析和管理等功能，用电信息采集系统由主站、远程及本地通道、集中器和采集器/电表组成，用电信息采集的数据流向包括上行和下行两类。上行数据流是指低压工商业、居民用户和公配变用户的电能表数据经过采集器（可选）上传到集中器，集中器经上行通信通道传到用电信息采集系统主站；专变用户电能表的数据上传到专变终端，专变终端经上行通道传到用电信息采集系统主站。

表5 用电信息采集场景5G通信需求

业务类别	业务名称	通信需求					
		时延	带宽	可靠性	定位	安全隔离	连接数
采集类业务	用电信息采集	5s	800kbps	99.9%	支持	管理信息Ⅲ区	X*100 个/km2

（3）移动应用类业务

移动应用类业务对通信需求的典型特征是通信带宽要求高，安全性要求高，适合5G技术体制下的eMBB应用场景，典型的业务有移动巡检类业务和输电线路在线监测。

电力行业智能巡检业务场景包括电厂智能巡检、输电线路无人机巡检、变电站巡检机器人三类场景。传统的人工巡检或非智能巡检方式，经常出现漏巡、代巡、错检，以及巡检质量不高、信息反馈滞后等问题，通过引入北斗定位技术、5G定位技术方式，巡检机器人或电力巡检无人机等智能巡检有助于及时发现电力设备的故障隐患，为电力信息系统的安全生产起到重要的保障作用。电力巡检机器人或电力巡检无人机按照规划的路径自动运行，通过对无人机航迹规划并利用电力北斗地面增强站的精准导航，并在设置的巡检点自动监测和智能感知发电设备的运行状态（包括温度、速度、压力、震动、电压、电流等）及周围环境等信息，通过应用智能化数字设备完成信息图片等采集上传，对发电设备缺陷、违规和危及发电安全的隐患进行判别和预测，配合智能数据分析，通过巡检机器人的内外部巡视以及后台监测，以便及时消除缺陷，保证巡检过程线路安全和电力系统稳定。

表6 输电线路高清视频及无人机巡检场景5G通信需求

业务类别	业务名称	通信需求				
		时延	带宽	可靠性	定位	安全隔离
移动应用类	输电线路高清视频及无人机巡检	≦100ms	最大上行30Mbps	>99.9%	支持	管理信息III区

特高压线路途经重覆冰、舞动、山火、雷害、风害易发区，目前已规划逐塔安装视频监拍及在线监测装置，充分利用智能化手段应对极端自然灾害，要求通信技术手段传输带宽大。电线路在线监测后，汇聚节点与后台之间实现大带宽低延时数据通讯，每个感知终端都可以安装5G模组，直接传输到后台。

表7 输电线路在线监测场景5G通信需求

业务类别	业务名称	通信需求			
		时延	带宽	可靠性	安全隔离
移动应用类	输电线路在线监测	≦1s	最大上行35Mbps	>99%	管理信息III区

（4）电网新型业务

电网新型业务是随着智能电网和电力物联网的深入建设而出现的一类业务，这类业务个性化通信需求较多，缺乏存量业务前期的通信积累，而5G技术的出现，能更好地与传统通信方式结合，满足各种电网新型业务的个性化通信需求。典型的业务有多站融合业务等。

多站融合业务充分利用变电站、新能源场站、储能站、电动汽车充电站、供电营业厅所、抽水蓄能电站等场地环境建设不同等级和应用场景的数据中心站。数据中心站提供变电站数据的本地存储与边缘计算能力，网络边缘计算作为云计算的延伸，通过把云计算平台及其能力迁移到变电站、新能源场站等网络边缘，具备对高带宽、低时延、本地化业务的更强支撑功能，向社会提供资源共享服务。

2.3 5G 智能电网网络架构

对于电力行业专网业务，根据电力行业关于安全区的划分涉及业务隔离的要求，使用切片技术划分电力行业专用切片用于为配网PMU、配网差动保护和配电自动化三遥等电力行业生产控制类业务提供服务，划分电力行业通用切片用于为智能化巡检、智能配电房等管理信息类业务和其它业务提供服务。两类切片面向不同的电力行业终端，在无线网通过RB资源预留，在传输网和核心网通过资源物理隔离满足电力行业不同业务类别之间的隔离需求。

针对电力行业的配网PMU、配网差动保护和配电自动化三遥等电力生产控制大区业务场景，为保障业务的高可用性运行对网络的低时延和高可靠性等需求，规划行业专用切片用于实现生产控制类业务的网络专属保障，并可进一步划分不同切片分别为配网PMU、配网差动保护和配电自动化三遥等业务提供网络切片服务，满足业务间隔离需求。针对电力行业智能化巡检和智能配电房等管理信息大区业务场景，为满足业务的大上行带宽，规划行业专用切片用于实现检测或监控数据采集类业务的网络保障，并可进一步划分不同切片分别为智能化巡检、智能配电房等业务提供网络切片服务，满足业务间隔离需求。

5G智能电网网络架构如图1所示：

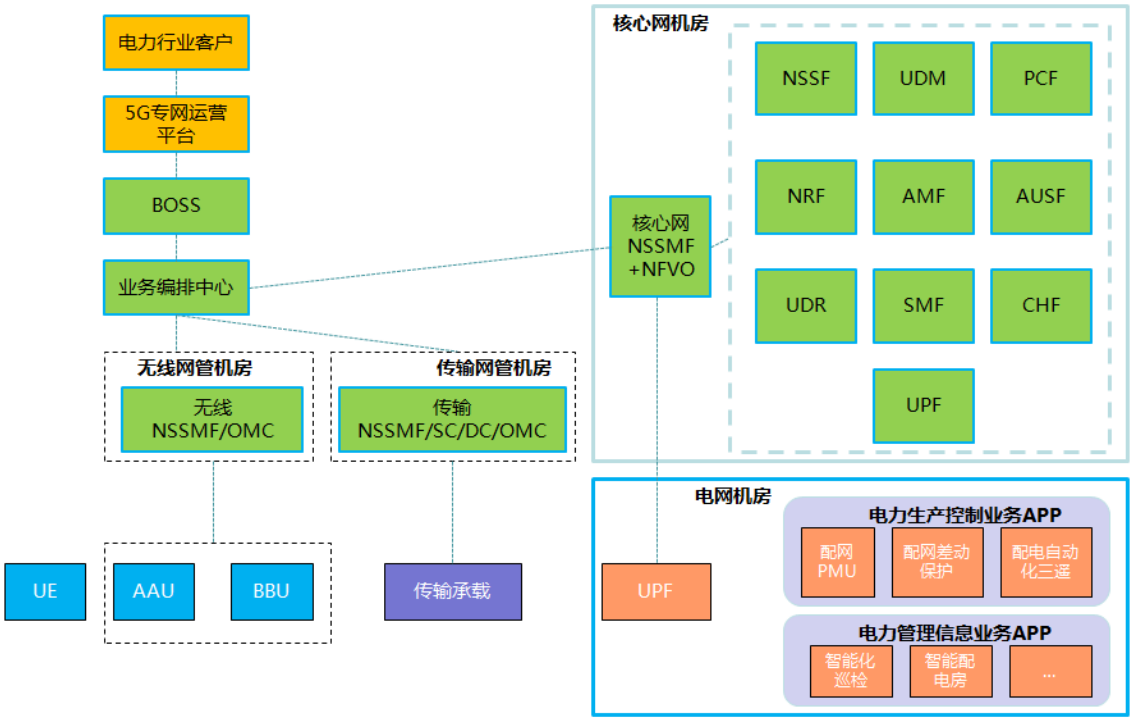

图 1 5G 智能电网网络架构

（1）行业专用切片开通

电力行业客户通过5G专网运营平台进行电力行业专用切片订购，BOSS发送业务表单到业务编排中心，携带切片业务标识(S-NSSAI)，切片签约省份、切片是否跨省、切片类型和切片SLA指标等。业务编排中心生成网元部署信息和切片初始配置信息。

网元部署信息包括无线模板(输入AMF列表、接入UPF列表、覆盖基站信息列表和IP地址等)、传输模板(基站侧VLAN ID、UPF侧VLAN ID等)和核心网模板(新建UPF信息、新建UPF数量、UPF主机名、N4接口地址和端口等)信息。

初始配置信息包括无线配置信息(切片用户组ID、用户组内PRB资源预留比例分配、帧结构和带宽等)、传输配置信息(传输隔离要求、VPN业务参数和基站侧VLAN ID等)和核心网局数据(切片AMF配置信息、切片SMF配置信息、切片UPF配置信息和DNN等)。

业务编排中心将网元部署信息和切片初始配置信息发送至无线、传输和核心网进行部署和配置。

（2）行业专用切片用户签约

电力行业用户签约，通过物联网BOSS发送用户的5G切片签约数据到数据网元HSS/UDM。用户5GC的切片签约信息包含S-NSSAI数据和DNN数据；S-NSSAI数据中定义了用户签约的所有S-NSSAI，其中default属性取值为true的为默认S-NSSAI，最大允许定义8个默认S-NSSAI。单

个S-NSSAI中最大允许包含50个DNN数据，其中最多只有一个缺省DNN。所有S-NSSAI下包含的DNN数据总数不超过50个。

（3）切片QoS保障

针对电力行业专用切片配置对应的QoS参数，核心网支持根据用户签约和业务信息配置各切片QoS保障数据，并下发至终端和无线侧。终端和无线侧支持按照规则将业务流匹配到QoS流。

终端、无线和核心网支持通过MBR、UE-AMBR等参数实现最高速率上限差异化保障。其中，核心网和终端应支持根据Session-AMBR等参数实现最高速率上限；无线和核心网应支持根据MFBR等参数实现限速；核心网支持根据UE-AMBR进行限速，以及根据运营商要求，逐业务进行速率上限控制。

终端、无线和核心网应支持通过GBR等参数配置实现绝对速率的下限保障。其中无线还应支持根据PBR、MinBR等参数实现绝对速率下限保障。

终端、无线和核心网应支持3GPP协议中规定的标准ARP配置，且无线支持根据ARP进行接纳优先级控制。

终端、无线和核心网应支持3GPP协议中定义的标准5QI，针对电力低时延控制类业务、大带宽数据类业务，切片可配置不同5QI，电力行业切片5QI取值一般为6，具体5QI配置情况需根据公司相关规定配置。

无线应支持通过MinBR/PBR实现最低速率保障，通过调度级别参数配置实现相对调度优先级保障，以及根据5QI按需开启专门的时延保障增强功能和可靠性保障功能。比如，针对低时延保障场景，基站需支持按5QI开关预调度、调整SR周期、开关DRX、开关保守调度（使用或不用低MCS配置表）、开关mini slot功能等；针对高可靠性要求场景，无线侧支持针对特定5QI承载配置更低码率的MCS策略、支持PDCP重复、支持mini-slot aggregation /repetition等。5QI映射指标表如表2-1所示：

表 2-1 5QI 映射指标表

5QI Value	Resource Type	Default Priority Level	Packet Delay Budget	Packet Error Rate	Default Maximum Data Burst Volume	Default Averaging Window
1	GBR	20	100 ms	10-2	N/A	2000 ms

2		40	150 ms	10-3	N/A	2000 ms
3		30	50 ms	10-3	N/A	2000 ms
4		50	300 ms	10-6	N/A	2000 ms
5	Non-GBR	10	100 ms	10-6	N/A	N/A
6		60	300 ms	10-6	N/A	N/A
7		70	100 ms	10-3	N/A	N/A
8		80	300 ms	10-6	N/A	N/A
9		90	300 ms	10-6	N/A	N/A

针对同一5QI，核心网支持为传输和承载配置不同DSCP，支持自配置5QI与DSCP、VLAN Pri的映射关系。承载应支持根据核心网、无线映射的DSCP等参数进行QoS调度。传输应支持根据核心网、无线映射的VLAN Pri、DSCP等参数进行QoS调度。

3 电力行业应用安全政策和标准

3.1 安全政策

电网安全是电力的基础，随着智能电网的高速发展，通信技术越来越多的应用于电力系统中，虽然新技术极大地提升生了电网系统的运营效率，但是其带来便捷的同时也存在潜在的安全问题，该问题已成为电力公司的关注焦点。关于智能电网安全与网络安全、通信设备与电网安全的关系备受关注，智能电网的安全发展成为了国际社会关注的热点问题，为了进一步推动智能电网的建设和发展，各国纷纷颁布相关法规和政策文件。

总体来看，多数国家均由政府负责智能电网的发展战略及5G智能电网发展安全，部分国家较为关注5G智能电网中新技术带来的安全隐患，但相关的5G智能电网安全政策和标准有待进一步完善。美国、日本和欧盟等国家与地区都在推动智能电网发展，进行了相关的战略部署并建立了政策支持，进一步促进智能电网发展的同时强化智能电网安全。美国由于其能源独立战略和旧电力设备升级的需求，大力发展智能电网。2007年，美国颁布《能源独立和安全法案》（EISA2007），该法案首次提出在美国建设智能电网计划，并指定美国能源部负责智能电网的总体工作。2009年5月21日，美国众议院能源和商业委员会通过《美国清洁能源和安全法案》，这个法案第一章就明确规定，美国要发展智能电网，提高电力传输效果。该法案的颁布意味着美国将智能电网提升到了美国国家战略层面；日本智能电网发展的驱动来

自于其国家能源安全的需求，从21世纪初开始着手投资智能电网，2003年以来，接连开展了一系列包括微电网、智慧城市在内的智能电网安全示范工程；欧洲各国发展智能电网的根本驱动力是实现可再生能源发展和节能减排目标，十九世纪末到二十世纪初，欧盟第五框架计划明确提出：欧洲电网中可再生能源和分布式发电整合。2005年，智能电网欧洲技术论坛成立，其目标是将当前的电网转换成一个用户和运营者互动的服务网，以提高欧洲输配电系统的效率、安全性及可靠性，2006到2008年，分别发布了《未来的欧洲电网——远景和策略》、《未来的欧洲电网——战略性研究议程》和《未来的欧洲电网——战略部署文件》等计划和政策方针。2009年，欧盟委员会成立了智能电网小组。2019年初，欧盟各国将根据颁布的清洁能源一揽子法令制定本国相应法律，鼓励信息通信、智能技术在电网中的运用。

2015年7月6日，我国国家发改委和国家能源局联合发布《关于促进智能电网发展的指导意见》，要求编制智能电网战略规划，提高输出电网智能化水平，与此同时，加强发展智能配电网，鼓励分布式电源和微网建设，促进能源就地消纳，到2020年，初步建设智能电网体系。该指导意见明确指出，发展智能电网，有利于进一步提高电网接纳和优化配置多种能源的能力，实现能源生产和消费的综合调配；有利于推动清洁能源、分布式能源的科学利用，从而全面构建安全、高效、清洁的现代能源保障体系。2016年2月29日，国家发改委发布《关于推进“互联网+”智慧能源发展的指导意见》，该意见中指出，应着眼能源产业全局和长远发展需求，以改革创新为核心，以“互联网+”为手段，以智能化为基础，紧紧围绕构建绿色低碳、安全高效的现代能源体系，推动能源互联网新技术，为实现我国从能源大国向能源强国转变和经济提质增效升级奠定坚实基础。2016年11月7日，国家能源局发布《电力发展“十三五”规划》，着力调整电力结构，着力优化能源布局，着力升级配电网，着力增强电网系统调节能力，着力提高电力系统效率，推进体制改革和机制创新，加快调整优化，转型升级，构建清洁低碳、安全高效的现代电力工业体系，惠及广大电力用户。2016年12月26日，国家发改委和国家能源局发布《“十三五”能源规划》，规划中提出，要贯彻落实五大发展理念，主动适应、把握和引领新常态，遵循能源发展“四个革命、一个合作”的战略思想，努力构建清洁低碳、安全高效的现代能源体系，描绘了“十三五”能源发展蓝图，明确了发展目标、重点任务和措施。

目前，我国在5G智能电网相关技术领域开展了大量的研究和实践，输电技术已达到国际领先水平，配用电领域的应用研究也在积极探索中。2007年，启动了智能互动电网可行性研究项目，为了提升电网安全稳定运行能力，同时启动了高级调度中心和统一信息平台等智能

电网试点工程。2008年，开始进行智能电网相关的研究和建设，致力于打造智能调度体系，搭建智能电网信息架构，为建设安全智能电网奠定基础。同时，相关高校相继成立了5G智能电网研究机构，对智能电网安全稳定运行进行研究和探索。除此之外，特高压交流试验示范工程和特高压直流输电工程相继投入运行，实现了我国大容量、长距离特征的高压核心技术上的突破，为智能电网的建设奠定了基础。智能电网5G通信业务总体上可分为控制类业务、采集类业务、移动应用类业务、多站融合为代表的电网新型业务。在 “十四五”建设期，智能电网将迎来快速发展智能电网在常规电网的基础上发展而来，通过融合自动化、信息化、5G、人工智能、大数据等技术，可以大大提升电网的整体运行及安全水平。

2018年，中国南方电网联合中国移动、华为发布了《5G助力智能电网应用白皮书》，针对当前智能电网的发展趋势和挑战，提结合 5G 网络切片关键技术研究与分析，制定出了5G智能电网安全体系整体政策要求，其中包括管侧安全方案及端侧安全方案；2020年完成一键顺控、变电巡检机器人、配电自动化三遥、配网 PMU等15类业务5G连通性测试，维护5G+智能电网安全；2021年3月，确定性网络联盟发布《5G确定性网络@电力系列白皮书 I：需求、技术及实践》，针对5G电网安全域进行了分析，提出了5G电网终端及网络安全解决方案，明确了对终端自身的安全防护和接入网络时对终端的保护及电力行业切片的网络安全包括切片自身的安全和用户使用切片的安全。

不过，目前我国5G智能电网安全领域相关的法律法规制度和政策等方面尚不成熟，需要进一步明确和完善5G智能电网的网络和信息安全相关制度和政策，推动5G智能电网信息安全和网络安全建设。

3.2 安全标准

智能电网的国际化安全标准主要涉及国际电工委员会（IEC）、国际电信联盟（ITU-T）、国际标准化组织（ISO）和电信标准化顾问组（TSAG）等。2000年5月，IEC发布了《电气/电子/可编程电子安全系统的功能安全》，即IEC 61508标准，该标准针对由电气/电子/可编程电子部件构成的、起安全作用的电气/电子/可编程电子系统(E/E/PE)的整体安全生命周期，建立了一个基础的评价方法。目的是要针对以电子为基础的安全系统提出一个一致的、合理的技术方案，统筹考虑单独系统(如传感器、通信系统、控制装置、执行器等)中元件与安全系统组合的问题。2003年，IEC发布《流程工业领域安全仪表系统的功能安全》，即IEC61511标准，针对基于使用电气/电子/可编程电子（E/E/PE）技术的仪表安全系统，规定

了逻辑解算器在设计和使用过程中，须采用的基本原则，以及构成仪表安全系统的传感器和最终元件所应达到的最低标准，并提出了达到这些最低标准的安全生命周期活动的方法，即，对过程工业中安全仪表系统的规范、设计、安装、运行和维护的要求进行了标准化；对安全仪表系统的系统、硬件、软件提出要求；在应用和安全整体级别的确定方面提供了相当多的指导。2005年4月，IEC发布《电力系统管理和相关信息交换 - 数据和通信安全》，即IEC62351标准，其中考虑智能电网的通信安全，包括安全访问控制、密钥管理和安全体系结构。通过对通信报文进行加密，可以规避通信设备从中间截获报文，即使通信设备被网络攻击，两端的设备在应用层仍能保障通信控制信息不会被篡改，从而保障电网安全。2010年5月，ITU-T接受了TSAG的建议，建立了新的标准制订小组，以推动智能电网标准工作的进程，该小组聚焦对相关国家标准进行分析比较，尽力避免新标准技术复杂，以推动产品尽力做到低能耗、低成本、高性能、高可靠性和安全性。

智能电网安全国家标准相关工作主要在全国信息安全标准化技术委员会（TC260）开展。目前发布了GB/T 20438《电气/电子/可编程电子安全相关系统的功能安全》国家标准，针对由电气和/或电子和/或可编程电子（E/E/PE）组件构成的，用来执行安全功能的系统安全生命周期的所有活动，提出了一个通用的方法。GB/T 21109《过程工业领域安全仪表系统的功能安全》国家标准，提出了达到最低标准的安全生命周期活动的方法。

2014年8月，国家发改委发布《电力监控系统安全防护规定》，该规定为加强电力监控系统的信息安全管理，防范黑客及恶意代码等对电力监控系统攻击及侵害，保障电力系统的安全稳定运行，根据《电力监管条例》《中华人民共和国计算机信息系统安全保护条例》等，制定了关于建立“安全分区、网络专用、横向隔离、纵向认证”的安全防护体系指导建议。2019年6月，国家标准化管理委员会公布“关于推广国家技术标准创新基地（智能电网）建设经验做法”的通知，旨在建设智能电网领域国家技术标准创新基地，促进科技、标准、产业同步发展，推进国家技术标准创新基地（智能电网）建设和运行。实践表明，通过对网络安全顶层设计，结合规范化的网络安全标准规范和立体纵深、分区分级的网络安全防护措施，结合现代通信和电力物联网技术，可以建立坚强智能电网系统，维持电网系统的安全稳定运行。

2017年以来，我国开展了大量的5G确定性网络使能智能电网技术安全的可行性验证，并取得一定的阶段性成果：2022年3月，5G应用产业方阵联合确定性网络产业联盟发表《5G电力虚拟专网网络安全白皮书》，针对5G电力虚拟专网安全的需求和风险进行分析，提出了5G

电力虚拟专网安全参考方案，分别针对5G电力广域虚拟和局域虚拟专网进行了案例应用分析；2020年7月，由中国电信牵头、联合南方电网、国家电网、中国移动、中国电信、华为以及VDF等欧洲运营商和政府机构等28家单位在3GPP R18成功立项5G智能电网需求框架，首次为5G在电力行业的应用构筑了体系化的安全标准平台。该标准的立项成功离不开5GDNA联盟中南方电网、国家电网等产业PoC样板项目的输入，依托本次立项，5GDNA会持续加强与3GPP、IEEE、5G-ACIA、CIGRE等国际标准组的合作，确保5G+智能电网项目在3GPP等国际标准的工作持续健康发展。

4 5G 电力行业应用安全需求

4.1安全分区安全需求

电力系统分为生产控制大区和信息管理大区，其中生产控制大区又分为控制区(即安全I区)和非控制区(即安全Ⅱ区)，控制区和非控制区至少应逻辑隔离，生产控制大区与管理信息大区应实现物理级别隔离。

5G智能电网网络切片安全分区的具体安全需求包括：

a) 无线空口按切片为客户业务提供隔离；

b) 传输网按切片为客户业务提供生产控制大区业务和管理大区业务硬隔离；

c) 核心网按业务需求为客户提供通过切片，保证每个切片都能获得相对独立的物理资源；

d) UPF至电力业务系统主站通过专线连接；

e) 在终端接入5G网络的认证鉴权基础上，提供电力终端自主可控的次认证、切片鉴权服务，终端支持安全加密能力，满足电网行业安全需求。

4.2 网络专用安全需求

网络专用要求所使用的5G网络切片专网专用，不与其他业务混用。

智能电网网络切片专用的具体安全需求包括：

a) 无线空口为配电自动化业务提供资源预留，并支持业务数据机密性、完整性保护，保证空口数据安全；

b) 针对电力业务终端，支持接入双向认证机制，保证合法终端接入网络；

c） 传输网为生产控制大区业务提供隔离；

d） 核心网划分切片，保证每个切片都能获得相对独立的物理资源，在生产控制大区切片提供专用网元实现与安全接入区安全连接，实现网络专用；

e） 为电网切片与其他切片提供隔离，保证每个切片都能获得相对独立的物理资源；

f） 提供网络层的通信通道加密；

g） 向用户提供抗DDOS、防火墙、IDS/IPS、WAF等安全能力；

h） 管理面的接口都具备认证和鉴权，提供管理面的机密性和完整性保护；支持分权分域，防止越权运维；流程内的不同节点也支持指定相应的角色。

4.3横向隔离安全需求

隔离要有两个层级。第一，生产控制大区不同业务区域之间逻辑隔离；第二，生产控制大区I区和生产控制大区II区之间需物理隔离。

5G智能电网网络切片横向隔离的具体安全需求包括：

a） 生产和管理资源隔离：在5G SA端到端网络构建生产控制大区和管理信息大区两个切片所需专用承载网络资源，核心网采用专属UPF、SMF（可选），传输承载通过FlexE隔离，无线网根据业务特点灵活选择QoS及RB资源隔离方式，部分变电站、配电房场景需配置专属基站或小区。

b） 生产大区内部的I区和II区，应至少实现无线侧、传输侧和核心网侧的端到端网络的逻辑隔离。

c） 网络切片与外部数据网络应网络隔离，切片网元与外网设备间应做好边界防护，保护切片内网与外网间的安全。

d） 应实现切片之间故障隔离，切片的网络故障、网元业务故障、网元虚拟机故障等故障不能影响其他切片的正常运行。

4.4 纵向认证安全需求

纵向认证安全需求的目的是解决智能电网切片接入安全方面的问题，关注的是用户使用切片的安全。

5G智能电网网络切片纵向认证的具体安全需求包括：

a) 电力业务终端接入5G电力切片专网，应通过电信运营商核心网对接入网络切片的终端USIM/eSIM卡的主认证；

b) 电网行业用户应自主部署认证鉴权服务：当电力业务终端接入5G电力切片专网后，如需访问主站电力业务，应通过电网行业用户自主可控的次认证；

c) 电力终端和主站业务平台之间的通信，应采取端到端的加密保护；

d) 电力业务接入的5G终端应集成安全模块或安全芯片，支持通信数据加密；；

e) 应对控制命令和参数设置命令使用基于非对称加密算法的认证加密技术进行安全防护，实现配网终端对主站的身份鉴别与报文完整性保护；

f) 对电网主站进行安全防护。

5 5G 智能电网安全架构

5.1 5G 智能电网安全架构

根据电网安全生产控制大区业务及管理信息大区业务安全隔离需求，在5G SA端到端网络构建生产大区和管理大区两个切片所需专用承载网络资源，包含多个子域，并且涉及管理面、控制面和用户面，智能电网端到端切片安全架构如图2所示：

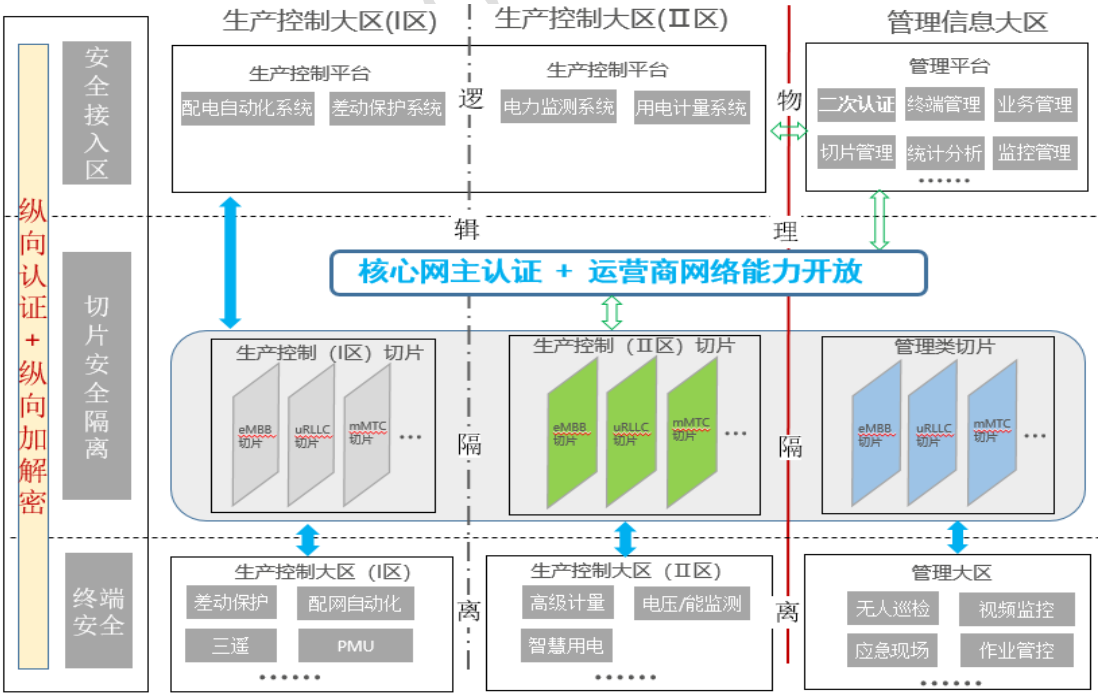

图2 5G智能电网网络安全架构

5G网络切片技术可以作为运营商助力智能电网建设的切入点，通过5G网络切片针对业务特点实现定制化网络，对网络进行分区以提供对电网的不同级别的访问，以启用精细的安全策略设置，满足智能电网各种特色业务的安全要求。

图2包含电网专用切片的一个三层组网方案，其中控制类切片承载电力生产业务，如差动保护、三遥和精准负荷控制，电力终端装置通过5G CPE接入5G网络，5G核心网出口交换机配置路由互通，连接配电自动化主站系统。控制类业务通过网络切片技术与信息采集类业务（电力III/IV区业务）、移动应用类业务形成端到端隔离。

纵向认证是智能电网网络切片安全需求和防护原则中关于切片接入安全的核心问题。智能电网切片用户的纵向认证与“安全分区、网络专用、横向隔离”等其他三项安全需求与防护原则之间构成相辅相成的关系，共同组成完整的智能电网网络切片的安全保障机制。

智能电网不同的业务场景下的服务功能和性能的差异化及不同电力终端业务的时延、带宽、可靠性等一对一服务水平协议技术指标，客观上不仅要求智能电网以分层切片架构来区分体现，并且要求分层切片架构从网络技术上保障智能电网的 “安全分区、网络专用、横向隔离、纵向认证”等安全需求和防护原则。对于智能电网的切片划分，对应5G系统中eMBB、uRLLC、mMTC三大业务场景，通常可横向分为生产大区I/II（eMBB和uRLLC）和管理大区III/IV（eMBB和mMTC），其中，生产大区I和II又各自包括切片1和切片5，以及切片2和切片6，不同的网络切片为智能电网各类典型业务提供不同的能力，不同网络切片服务可更有针对性地满足智能电网的通信需求。5G智能电网网络切片典型分层架构如图3所示：

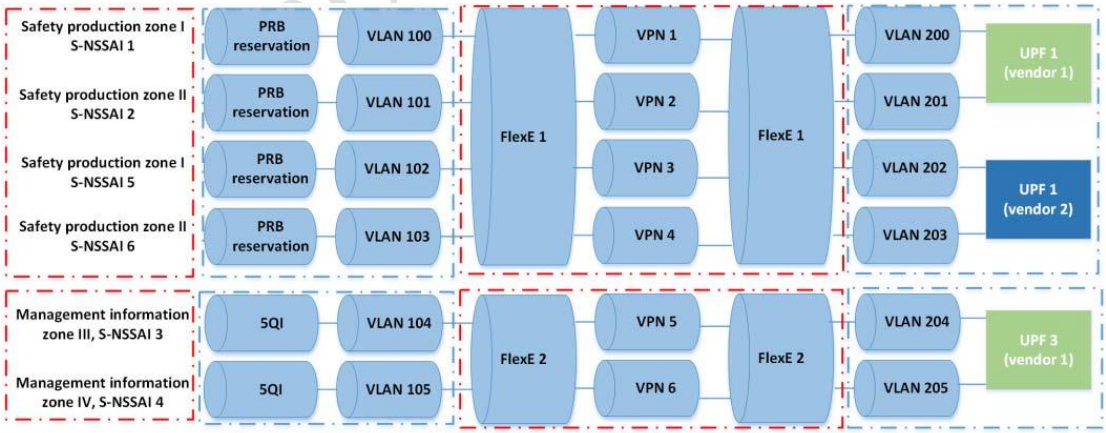

图 3 5G 智能电网网络切片典型分层架构

智能电网网络切片的分层架构给切片的管理和运维均带来一定程度的复杂性，复杂的分区和切片也带来较高的窜扰攻击风险，最终的安全问题落在如何正确使用智能电网网络切片上。就智能电网网络切片分层架构的安全需求而言，“安全分区、网络专用、横向隔离”的

目的是保证电网切片差异化的服务、质量与安全等级，关注的核心是智能电网切片的自身组成和安全，纵向认证安全需求实际上涵盖了用户接入切片安全和使用切片安全的全过程，包括无线空口的机密性和完整性保护、传输网的加密、核心网对终端的认证授权等过程。对于无线侧，应开启信令面和用户面的机密性和完整性保护，对接入网传输的隐私数据进行加密保护，确保未授权的站点无法从网络中截取数据；而对于传输网，可使用IPsec保障传输数据的安全，但基于性能和安全的平衡考虑，可暂不启用IPsec，而考虑应用层加密的方式保障数据传输的安全。

5.2 5G 智能电网安全技术

5.2.1安全分区技术

安全分区技术包括但不限于：

a) 无线空口按切片为客户业务提供高优先级QoS或RB无线空口资源预留进行隔离；

b) 传输网按切片为客户业务提供FlexE方式，实现生产控制大区业务和管理大区业务硬隔离；

c) 核心网按业务需求为客户提供通过VLAN/VXLAN划分切片，并在物理或虚拟网络边界部署硬件或虚拟防火墙来完成访问控制；

d) UPF至电力业务系统通过专线连接。

5.2.2网络专用及横向隔离技术

网络专用总体上实现专网专用，与公网隔离，达到“网关到网关”（甚至“终端到终端”）的专网水平，不与其他业务混用。具体技术包括但不限于：

1) 无线空口资源预留，并可开启业务数据面加密、完整性保护，保证空口数据安全；

2) 电力业务终端，采用接入双向认证机制（通过终端的NSSAI为终端选择正确的切片），保证合法终端接入网络；

3) 传输网为生产控制大区业务提供FlexE方式进行隔离；

4) 核心网通过VLAN/VXLAN划分切片，并在物理或虚拟网络边界部署硬件或虚拟防火墙来完成访问控制；

5） 传输加密技术；

6） 管理面的接口都具备认证和鉴权功能，管理面的传输通过TLS加密和完整性保护。

电力信息系统生产控制大区内部不同业务系统以及与外部区域之间实现隔离，隔离要有两个层级。第一、生产控制大区内部不同业务系统之间逻辑隔离；第二、大区和大区之间间需物理隔离。具体技术包括但不限于：

1） 生产和管理资源隔离；

2） 无线侧、传输侧和核心网侧的端到端网络的逻辑隔离；

3） 网络切片与外部数据网络网络隔离；

4） 切片之间故障隔离。

5.2.3 纵向认证技术

电力业务终端接入5G+智能电网满足国家能源局“纵向认证”的要求，且在通过电信运营商对5G虚拟专网的主认证之后，还需要根据电网系统的重要性实现对终端接入身份次认证的自主控制，具体技术包括但不限于：

a） 电力业务终端接入5G电力切片专网认证；

b） 电网用户自主部署认证鉴权服务器(如AAA)；

c） 电力终端和主站业务平台之间的通信端到端的加密保护；

d） 5G终端集成安全模块或安全芯片；

e） 电网主站安全防护设备。

6 建议及展望

5G商用进程快速推进，5G发展已进入落地应用的关键阶段，加快5G应用部署，赋能垂直行业，培育应用生态，成为当前业界关注的焦点；同时，由于5G与行业的深度融合打破了传统网络的封闭性，其带来的安全问题也受到高度重视。

随着电力行业逐渐成为5G应用发展的先行领域，5G的超大流量、超低延时和海量链接等特性在有效推动信息流与能量流融合，引领电网全流程、全区域业务变革的同时，新技术、新应用也带来了新的安全风险和挑战。目前，5G电力行业应用安全相关国际国内标准尚未完全成熟，需要产业链各环节（包括网络设备商、运营商、行业应用提供商、安全设备商、研

究机构）共同探索建立满足5G多样化需求的安全体系，共同应对5G网络安全风险，以便部署满足行业发展需求的安全可靠的5G网络，从而推动5G安全和5G产业同步规划、同步建设、同步发展。基于白皮书的研究成果，建议从以下3个方面重点推进：

一是出台5G电力应用安全相关政策指引性文件。建立主管部门加强协同联动和沟通衔接，联合发布跨部门、跨行业的指引性政策文件，明确5G电力应用安全要求及各方职责，共同构建并夯实5G融合应用安全责任体系。

二是制定5G电力应用安全相关行业标准。凝聚行业共识，系统推进5G电力行业应用安全标准研究，明确标准化重点方向，加强5G+电力基础共性标准、融合设备标准、解决方案标准的研制，加快标准化通用化进程，突破重点应用场景标准研究和制定，推动5G电力行业应用标准的迭代、评估和优化，促进相关标准在重点场景的应用落地。

三是开展5G电力应用安全测试验证及示范推广。加强5G电力应用安全测评能力建设，同步开展关键技术、标准及解决方案的测试验证，构建5G电力行业应用安全最佳实践案例，助力方案落地推广及试点示范，为全行业提供借鉴和参考。

5G作为实现万物互联的关键信息基础设施，是驱动国家经济社会数字化转型的重要力量。我国5G正式商用3年来，在各方共同努力下，我国5G创新发展取得积极进展，网络规模持续扩大，融合应用成效显著。安全是全面推进5G融合应用过程中保驾护航的核心力量，5G+垂直行业的快速发展，也给5G应用安全产业带来了难得的机遇。相信在产业各方的努力下，5G+电力行业应用安全相关政策、标准、产业将进一步健全完善，通信网络的安全能力与电力系统特殊的可靠性和安全性要求进一步适配，5G电力行业应用安全产品、及解决方案将进一步涌现，助力“5G+电力”大规模复制推广、 扬帆远航！

附录：缩略语

缩略语	英文名称	中文名称
3GPP	3rd Generation Partnership Project	第三代移动通信伙伴项目
5G	5th Generation Mobile Communication Technology	第五代移动通信技术
AAU	Active Antenna Unit	有源天线单元
AKA	Authentication and Key Agreement	身份验证和密钥协议
AMBR	Aggregated Maximum Bit Rate	聚合最大比特率
AUSF	Authentication Server Function	认证服务器功能
BBU	Building Base band Unit	室内基带处理单
CHF	CHarging Function	计费功能
DDoS	Distributed Denial-of-service Attack	分布式拒绝服务攻击
DNN	Data Network Name	数据网络名称
DRX	Discontinuous Reception	不连续的接收
DSCP	Differentiated Services Code Point	差分服务代码点
DTN	Data Transfer unit	无线传输终端
eMBB	Enhanced Mobile Broadband	增强移动宽带
GBR	Guaranteed Bit Rate	保证的比特速率
HSS	Home Subscriber Server	归属用户服务器
HTTPS	Hyper Text Transfer Protocol Secure	超文本传输安全协议
IDS	Intrusion Detection System	入侵检测系统
IPS	Intrusion Prevention System	入侵防御系统
IPsec	Internet Protocol Security	互联网安全协议
MEC	Multi-access Edge Computing	多接入边缘计算
MinBR	Minimum Bit Rate	最小比特速率
mMTC	massive Machine Type of Communication	海量机器类通信
NFVO	Network Functions Virtualisation Orchestrator	网络功能虚拟化编排器
NRF	Network Repository Function	网络存储库功能
NSSAI	Network Slice Selection Assistance Information	网络切片化辅助性信息筛选
NSSF	Network Slice Selection Function	网络切片选择功能

NSSMF	Network Slice Subnet Management Function	网络切片子网管理功能
PRB	Physical Resource Block	物理资源块
QoS	Quality of Service	服务质量
RB	Radio Beacon	无线电信标
SIM	Subscriber Identity Module	用户识别模块
SMF	Session Management Function	会话管理功能
UDM	Unified Data Management	统一数据管理
UDR	Unified Data Repository	统一数据存储库
UE	User Equipment	用户终端设备
UPF	User Plane Function	用户面功能
uRLLC	Ultra-reliable and Low Latency Communications	超可靠低时延通信
WAF	Web Application Firewall	网络应用防火墙

主要贡献单位