

内容简介

《现代电力通信网架构与关键技术》是一部系统阐述智能电网时代背景下电力通信网络发展脉络、体系架构与核心技术的专业著作。本书立足国家“双碳”战略和新型电力系统建设需求，全面梳理了电力通信网从传统支撑型通道向智能化、泛在化数字基础设施演进的历史进程，深入剖析其在保障电网安全稳定运行、支撑源网荷储协同互动、赋能能源互联网建设中的关键作用。

全书共分十章。第一章概述现代电力通信网的发展背景、功能定位与演进趋势；第二章系统介绍国际与国内主流技术标准体系，重点解析 IEC、ITU-T、IEEE 及我国电力企业标准在通信协议、接口规范与安全要求方面的关键内容；第三章至第五章聚焦逻辑与物理架构，分别阐述承载网、业务网与支撑网的三层逻辑模型，“云-管-边-端”一体化新架构，以及骨干传输网、配电通信网和无线接入网构成的多层次异构物理网络；第六章深入剖析软件定义网络（SDN）、网络功能虚拟化（NFV）、5G 网络切片、无源光网络（PON）等关键技术 在电力场景中的适配机制与部署策略；第七章围绕服务质量（QoS）保障，详解流量监管、令牌桶算法、优先级调度等机制如何支撑继电保护、精准负荷控制等高实时性业务；第八章专论网络安全，构建“分区、分级、纵深防御”的安全体系，涵盖边界防护、加密认证、安全审计与零信任架构；第九章系统介绍电力通信网应急响应体系，包括组织机制、预案制定与备份恢复、业务连续性保障、攻击溯源取证等技术手段；第十章展望未来发展趋势，探讨空天地一体化通信、人工智能驱动的智能运维、通感算一体融合等前沿方向。

本书突出“业务驱动、安全优先、标准引领、技术融合”四大特色，不仅详述了光纤复合架空地线（OPGW）、电力线载波（PLC）、微波、卫星等多种传输介质的工程适用性，更紧密结合调度自动化、配电自动化、高级量测体系（AMI）、分布式能源接入等典型业务场景，阐明通信技术选型与网络设计的内在逻辑。书中大量引用国家电网、南方电网等企业标准与技术规范，体现了理论与工程实践的高度统一。本书既可作为高等院校电气工程、信息通信等相关专业研究生和高年级本科生的教材或参考书，也可 为电力系统科研人员、规划设计工程师及运维管理人员提供权威、系统的知识支撑与技术指南。

现代电力通信网架构与关键技术
Architecture and Key Technologies of Modern Power Communication Networks

陈雅琳 著



PRICE: \$60.00

Architecture and Key Technologies of Modern Power Communication Networks

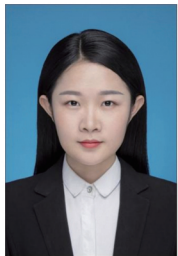
现代电力通信网架构与关键技术

陈雅琳 著



International
Union of Scientific and
Technological Scholars

作者简介

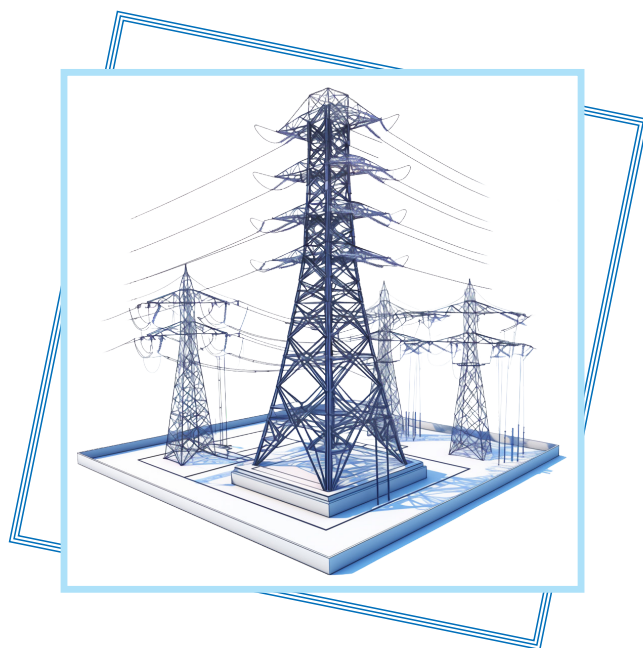


陈雅琳，出生于 1994.11 月，女，汉族，硕士研究生，工程师，河北沧州市人，从事电力信息通信研究，2019 年至今任职于国网冀北电力有限公司信息通信分公司，负责通信运维检修相关工作。

Architecture and Key Technologies of Modern Power Communication Networks

现代电力通信网架构与关键技术

陈雅琳 著



International
Union of Scientific and
Technological Scholars

CIP INFORMATION

Title: Architecture and Key Technologies of Modern Power Communication Networks

题目：现代电力通信网架构与关键技术

Author: Yalin Chen

作者：陈雅琳

ISBN: 979-8-90040-018-1

Publisher: CYPEDIA INTERNATIONAL UNION OF SCIENTIFIC AND
TECHNOLOGICAL SCHOLARS

Price: \$60.00

定价：60 美金



**International
Union of Scientific and
Technological Scholars**

Architecture and Key Technologies of Modern Power Communication Networks

现代电力通信网架构与关键技术

Address: 100 N Howard St Ste R, Spokane, Wa, 99201. United States

Tel: +888-754-5177

Email: contact@cypedia.net

Format: 170mmx240mm 1/16 Sheets: 16.5

Word Counts: 200.000

Edition: First edition in December 2025

Printing: First printing in December 2025

CYPEDIA INTERNATIONAL UNION OF SCIENTIFIC AND TECHNOLOGICAL SCHOLARS

非开放获取·电子版请联络出版社购买·版权归出版社所有·侵权必究

Not Open Access. For the electronic version, please contact the publisher for purchase. The copyright belongs to the publisher. Infringement will be prosecuted.

前言

PREFACE



随着“双碳”目标的深入推进和以新能源为主体的新型电力系统加速构建，电网正经历一场深刻的技术革命与形态重塑。高比例可再生能源接入、海量分布式资源聚合、源网荷储深度互动等新特征，对电力系统的灵活性、韧性与智能化水平提出了前所未有的挑战。在此背景下，作为电网运行的“神经系统”和数字化转型的基石，电力通信网的战略地位日益凸显——它已不再是传统意义上被动的信息传输通道，而是深度融入感知、控制、决策全链条，成为支撑电网安全、高效、绿色、智能运行的核心数字基础设施。

正是基于这一时代背景，笔者深感有必要系统梳理现代电力通信网的发展脉络、技术体系与未来方向，为行业同仁提供一部兼具理论深度与实践价值的专著。《现代电力通信网架构与关键技术》的撰写，旨在回应三个核心关切：其一，如何构建一张高可靠、低时延、广覆盖的通信网络，以满足继电保护、差动保护等生产控制类业务毫秒级响应的严苛要求？其二，如何在开放融合的趋势下，有效平衡业务承载能力提升与网络安全风险防控之间的矛盾？其三，如何通过标准体系与技术创新的双轮驱动，走出一条具有中国特色的电力通信发展道路？

本书的构思源于笔者多年参与电力通信规划、标准制定与重大工程实践的深切体会。我们看到，一方面，5G、SDN/NFV、人工智能等 ICT 前沿技术日新月异，为电力通信注入强大动能；另一方面，电力业务对确定性、安全性的极致追求，又要求技术引入必须审慎、稳健、可管可控。因此，本书特别强调“业务导向”原则，所有技术讨论均围绕具体电力应用场景展开。例如，在分析 5G 网络切片时，重点阐述其如何为差动保护提供端到端硬隔离通道；在介绍流量整形技术时，明确指出其在防止高速骨干网向低速终端设备突发冲击中的关键作用。

同时，本书高度重视我国电力通信标准体系的独特价值。从国家标准、行业标准到国家电网、南方电网等企业标准，一个“基础—设备—业务—管理”四位一体、覆盖全生命周期的标准化框架，不仅保障了全国电力通信网的互联互通与安全稳定，更成为推动自主创新、培育产业生态的重要引擎。书中专门章节对此进行了系统归纳，以期为读者理解中国电力通信发展的制度优势提供窗口。

此外，面对日益严峻的网络安全形势，本书将安全理念贯穿始终。电力通信网承载着关乎国计民生的关键业务，其安全防护绝非简单的技术叠加，而需构建涵盖物理层、网络层、应用层的纵深防御体系。书中详细解读了“安全分区、网络专用、横向隔离、纵向认证”的十六字方针及其在新一代通信架构中的落地路径。

需要指出的是，电力通信技术正处于快速迭代之中，本书虽力求反映最新进展，但仍可能滞后于某些前沿探索。未来，随着 6G、量子通信、通感一体等技术的成熟，电力通信网必将迎来更深刻的变革。笔者期待本书能成为一块铺路石，激发更多同行投身于这一关乎国家能源安全与数字经济发展的重点领域。

限于作者水平，书中难免存在疏漏及不妥之处，敬请读者批评指正。

—— 陈雅琳

CONTENTS ◀ | 目录

第一章 电力通信网概述	1
第一节 电力通信网发展历程	1
第二节 电力通信网基本概念与特点	6
第三节 电力通信网体系结构	10
第四节 电力通信网技术标准	17
第二章 电力通信网基础理论	23
第一节 通信系统基本原理	23
第二节 信号传输与调制技术	28
第三节 信道编码与纠错技术	34
第四节 多址接入技术	38
第三章 电力通信传输技术	43
第一节 光纤通信技术	43
第二节 无线通信技术	48
第三节 电力线载波通信	54
第四节 卫星通信技术	60
第五节 混合传输技术	63
第四章 电力通信网络架构	69
第一节 骨干通信网络	69
第二节 接入通信网络	74
第三节 终端通信网络	79
第四节 网络拓扑结构	85
第五节 网络分层模型	90

第五章 电力通信协议体系	97
第一节 通信协议基础	97
第二节 电力专用协议	100
第三节 国际标准协议	106
第四节 协议转换技术	112
第五节 协议安全机制	116
第六章 电力通信网络安全	121
第一节 网络安全威胁分析	121
第二节 加密与认证技术	125
第三节 访问控制机制	130
第四节 安全监测与防护	137
第五节 应急响应体系	141
第七章 电力通信网管理技术	147
第一节 网络管理系统	147
第二节 性能监测技术	152
第三节 故障诊断与处理	156
第四节 资源配置优化	162
第五节 服务质量保障	168
第八章 智能电网通信技术	175
第一节 智能电网通信需求	175
第二节 高级计量架构	181
第三节 配电自动化通信	186
第四节 分布式能源通信	191
第五节 电动汽车通信	196
第九章 电力通信新技术应用	201
第一节 5G 通信技术	201
第二节 物联网技术	206
第三节 边缘计算技术	211

第四节 人工智能应用	215
第五节 区块链技术	219
第十章 电力通信网发展展望	225
第一节 技术发展趋势	225
第二节 标准化进程	230
第三节 产业化前景	235
第四节 挑战与对策	241
第五节 未来发展方向	247
参考文献	253

第一章 电力通信网概述

第一节 电力通信网发展历程

一、早期电力通信阶段

电力系统发展初期，通信手段比较落后，基本上是依靠物理线路完成简单的信号传递，主要目的是实现调度指令的传达、变电站之间的联系。该时期的通信网络结构比较扁平，覆盖面小，技术上以模拟信号为主，功能单一，但为后来专业网络的建立积累了宝贵的运行经验和基础设施资源。

（一）电力线载波通信的诞生与应用

电力线载波通信是电力系统特有的通信方式，它利用已有的高压输电线路作传输媒介，实现电力流和信息流的同路传输。20 世纪初，高压电网发展起来以后，长距离调度通信问题日渐突出，专门敷设通信线路既费钱又难于维护。通过研制出阻波器、耦合电容器来把高频的通信信号叠加到工频电力线上。这项技术大大降低了变电站与调度中心之间建设成本，使二者间可以建立比较稳定的语音联络和运动信号传输通道。

载波通信的使用范围并不只限于语音服务，在继电保护领域也起到了不可替代的作用。用电力线传输的高频闭锁信号，故障发生后可以毫秒级的速度告诉对侧断路器及时动作，大大提高电网的运行稳定性。虽然受到线路噪声、电晕干扰、阻抗匹配等影响，通信质量在恶劣天气下会有一定的波动，但它在物资匮乏、技术落后的年代里是电力通信的“定海神针”。为解决长距离传输信号衰减的问题，中继技术也应运而生，沿途变电站设增音机来完成跨区域的调度指挥。

那时的载波设备大多使用模拟调制技术，频谱利用率不高，一般只能支持几路语音和低速数据通道。设备体积大，电子管以及早期的晶体管电路耗电量大，散热问题严重。而正是由于这种依托于强大的电力网络架构的通信方式，才奠定了电力专用通信网“伴生”于一次系统的基本形态，也为后来专用网络的独立化、专业化发展提供了逻辑基础。

（二）微波通信在电力系统中的初步探索

电网规模扩大以后，仅靠电力线载波已经不能满足不断增长的通道需求。跨越复杂地形或者不适合载波通信的区域时，微波通信作为一种无线视距传输方式被应用到电力系统中。微波通信利用特高频无线电波在视距范围内直线传播的特性，通过设置微波接力站，逐站中继将信号传送到远方。它不受地面线路故障的影响，有较强的抗灾能力，是载波通信的补充。

微波频段资源比较充足，相较于载波通信而言可以提供更宽的电路通道，承载更多的电话线路以及更复杂的数据远动。崇山峻岭之中架设实体线路十分困难，微波通信依靠“空中架桥”解决了偏远变电站、水电站之间的互联问题。技术人员要保证传输质量就得准确算出传输路径的非涅尔区，绕过山体和建筑物的遮挡，在高山上搭建无人值守的中继站。

早期的模拟微波系统提高了通信容量，但是多径衰落、雨衰等问题也随之而来。暴雨或者大气层结不稳定的时候，信号会遭遇非常严重的误码，乃至中断。为了解决以上问题，分集接收技术应运而生，利用空间分集或者频率分集技术来抑制信号波动。尽管高山台站的供电与防雷工作量大，但微波通信在当时还是为电力系统搭建起了一条重要备用的线路，形成了载波和微波相辅相成的早期网络。

（三）早期通信网络的功能与局限性

早期电力通信网主要是为了满足电网调度的实时性要求而建立起来的。其功能主要是语音调度、远动数据采集和一些继电保护信号的传送。网络结构大多是点对点或简单的链状、星状拓扑，缺少复杂的网状互联能力。从逻辑上讲，这样的结构简单直接，便于故障排除，但共享和网络生存性上有着天生的不足。一旦中心节点或者关键链路出现问题，就会造成大面积通信中断，没有迂回路由的保护。

技术在体制上是以模拟通信为主。这就意味着信号在传输时很容易受到电磁干扰的叠加影响，而且噪声不能像数字信号那样通过再生中继完全消除。传输距离越远，信噪比越小，网络的覆盖半径也就越小。模拟设备难以实现高度集成，各个厂家设备的接口标准不一样，互连互通非常困难，造成严重的“烟囱式”建设。

业务支持能力单一化成了当时的瓶颈。除了传统的调度电话、低速遥测遥信数据之外，网络很难承载行政办公、视频监控等宽带业务。频谱资源稀缺，每一次新业务的增加都需要投入大量资金改造设备或者申请频谱。随着电网自动化水

平的提高，上述缺点越来越明显，因此迫切需要一场从模拟到数字、从窄带到宽带的技术革命。

早期电力通信方式特点对比表

通信方式	传输介质	主要特点	优点	局限性
电力线载波	高压输电线路	利用现有电力线传输高频信号	成本低、无需新建线路、调度和继保双重作用	易受干扰、传输容量小、质量波动
微波通信	无线电波（视距）	无线视距传输、中继	传输容量大、抗灾能力强、适应复杂地形	易受天气影响、需建设中继站、维护工作量大

早期电力通信方式的特点与局限性，如上表所示。

二、现代电力通信网形成阶段

20 世纪 80 年代中期以后，全球信息技术浪潮一日千里，电力通信网也迎来了转折点。光纤通信技术成熟以后，彻底突破了传输带宽的瓶颈；数字化技术全面普及以后，又重塑了网络交换和复用的方式。电力通信网从辅助手段一跃成为现代信息高速公路，可以同时承载各种业务。

（一）光纤通信技术的引入与普及

光纤通信问世以后，电力通信发展史上就出现了一件里程碑式的事件。光纤由于传输损耗小、频带宽、抗电磁干扰能力强等天然的优势，与电力系统强电磁环境下通信需求十分吻合。光纤复合架空地线技术的发明，把光纤单元设置在输电线路地线里，既给予防雷保护，又创建起高速光通信通道，不必额外申请线路和架设杆塔，明显缩减了建设难度和成本。

1. 骨干网上，电力系统开始大范围铺设光缆，开始慢慢取代微波干线。长距离、大容量的光传输系统使跨省、跨区电力调度数据可以无损、实时地进行交换。单模光纤得到广泛的应用，中继距离由原来的几十公里增加到上百公里，中继站的数目大大减少，系统的可靠性大大提高。

2. 在城域网以及配电网方面，光纤复合相线和全介质自承式光缆被采用，从而让光纤网络深入到城市里的每一个角落以及边远变电站之中。光纤有良好的绝缘性，能安全地穿过高压区，克服了传统铜缆不能进入高压室的困难，给变电站内部设备的监视和综合自动化创造了条件。

3. 光通信设备的国产化进程在这个时期也明显加快。从最初进口散件组装到现在的自主研发,国内光传输设备制造能力的提升大大降低了建网成本,推动了光纤到变电站、光纤到户的普及。光纤网络形成以后,带宽限制的年代终于在电力通信史上告一段落。

(二) 数字化与网络化转型

传输介质革命把信号处理技术由模拟变成数字。脉冲编码调制技术把模拟信号转换成数字信号,克服噪声累积的难题的同时使信号存储、处理、交换都变得灵活起来。同步数字体系技术的出现标志着传输网络进入了新的时代,一个标准化和智能化并存的时代。用统一的帧结构和接口标准实现了不同速率、不同厂家的设备间无缝连接。

数字化转型除了使信号质量得到改善之外,也可以视作是网络结构的一场大变革。采用时分复用技术的数字程控交换机代替了老式的步进制、纵横制交换机,可以实现呼叫连接的瞬间建立和各种增值业务功能。网络拓扑结构开始出现环网、网状网。自愈环技术的使用,使网络在光缆断开或者节点失效的时候,能够在几十毫秒内自动将业务切换到备用路径上,极大地提高了通信系统生存能力,满足了电网“N-1”甚至“N-2”的安全标准。

这时网络管理系统也从无到有,由散而聚。通过标准的网管接口,运维人员可以在远程网管中心对全网设备进行远程监控、远程配置下发和远程故障定位。数字信号处理技术还产生了会议电视、继电保护专用数字接口等新的业务,电力通信网开始同时担负生产和管理两种功能,成为企业信息化建设的主要血脉。

(三) 综合业务数字网的建设

随着数字传输和交换网络完善,单一专用网络无法满足多样化业务需求,建设综合业务数字网成行业共识。综合业务数字网是通过标准用户接口提供语音、数据、图像等多种通信业务的“一线通”综合数字网。在电力系统,调度电话、行政办公等业务可在一个物理网络统一承载、管理。

窄带综合业务数字网建成后承担调度和行政电话数字化任务,提供简单电路交换数据业务。宽带技术出现后,异步传输模式的宽带综合业务数字网技术在核心节点试用,以统计复用满足突发数据流量承载需求。虽异步传输模式被互联网协议技术取代,但它引入的机制和概念为后续多业务融合网络流量工程设计提供思路。

同时，电力数据通信网独立组网，用专用数据网络连接各级调度中心和变电站，为能量管理系统提供数据通道。因大量非生产性业务出现，通信网络带宽需求大增。综合业务数字网出现后，电力通信部门从全局规划网络资源，打破各业务独立建网局面，实现通信资源集约化利用，为全网化发展奠基。

三、智能化发展阶段

迈入 21 世纪之后，智能电网的概念被提出，给电力通信网带来了前所未有的挑战与机遇。通信网已经不再是单纯的信息传输通道，它已经进入到智能电网的感知层、控制层、决策层当中，成为智能电网的第二张网络。此阶段通信技术同信息技术深度融合，云计算、物联网、大数据这些新兴技术在电力通信网里被普遍应用，促使电网从泛在化、宽带化向着智能化实现迅速跃进。

（一）面向智能电网的通信需求升级

智能电网要实现发电、输电、变电、配电、用电、调度各个环节的全面感知和双向交互，通信网络的覆盖范围、带宽容量、传输时延要求就极高。在配用电侧，有大量的智能电表、分布式电源、电动汽车充电桩需要接入网络，所以通信网络必须要有很强的接入能力以及扩展性。

传统骨干通信网功能强大，但是配电通信网一直就是其薄弱环节。为了支持配电自动化及高级量测系统，电力通信网向末端不断延伸，构成了覆盖中低压电网的庞大的神经末梢。除了要解决最后一段的接入问题外，还要应对各种复杂多变的现场环境。业务流量的流向也随之发生改变，从原来的一对一、一对多变成多点对多点的网状交互模式。数据具有更强的突发性、实时性，精准负荷控制业务通信时延要控制在毫秒级。

实现电网运行状态的全方位可视化要依靠高清视频监控，输变电设备的状态监测传感器等技术来支持，上行带宽需求随之大幅上升。传统的下行流量为主、非对称的网络架构要进行重构。同时伴随着电力市场化交易的推进，用户侧和电网侧之间的信息交互越来越多，数据的安全性以及隐私性成为了电力通信网需要解决的问题。因此网络要保证通畅，还要懂业务，具备按照业务感知的智能调度和质量保障能力。

（二）新兴信息通信技术的融合应用

为了满足智能电网越来越复杂的需求，电力通信网积极吸收和融合了当前最

先进的信息通信技术，形成了异构融合、云边协同的新型技术架构。

1. 第五代移动通信技术的出现，给电力物联网的发展提供了必要的支持。其低时延、高可靠、大连接的特性，正好符合差动保护、无人机巡检、海量仪表采集等典型的电力业务场景。利用网络切片技术，运营商网络可以为电力业务提供隔离的虚拟专网，在保证安全的前提下，也减少了自建基地的投入。

2. 工业互联网标识解析体系在电力行业的应用，给每一个电力设备赋予独一无二的数字身份证，实现了电力设备全生命周期可追溯管理。无源光网络技术由于具有无源、点对多点的拓扑优势，在配电自动化以及电力光纤到户的建设中得到了大规模的应用，为宽带接入提供了一种经济高效的方案。

3. 软件定义网络、网络功能虚拟化技术的使用，使网络架构更灵活敏捷。控制层和转发层的分离使得网络资源分配可以用软件编程来完成，新业务上线的速度大大加快。数据中心互联的时候，跨区域算力调度和数据备份就像流水一样简单。

第二节 电力通信网基本概念与特点

一、电力通信网的定义与内涵

（一）电力通信网的定义

电力通信网是为保证电力系统安全稳定运行而产生的，是电网调度自动化、网络运营市场化、管理现代化的基础。电力系统的专用通信网络，用有线、无线、卫星等多种通信方式建立起发电、输电、变电、配电、用电、调度等各个环节的信息传输通道。该网络承载着电网继电保护、安全自动装置、调度自动化等重要的生产控制业务，也承载着企业管理信息系统、视频会议、办公自动化等管理信息业务。可以说，电力通信网是电网不可分割的一部分，也是电网智能化、数字化转型的神经系统。

电力通信网内涵不断增大，在现代能源体系中也日益重要。它不再只是服务于传统的电力生产，正在向支撑泛在电力物联网、能源互联网的方向发展，深入挖掘先进的信息通信技术。电力通信网正在建设全时空、全方位的电力信息感知和交流体系。这种定义上的变化也体现了通信技术与电力技术相互融合的发展方

向，这意味着电力通信网正从以前的单纯的辅助支撑体系，向着重要的价值创造体系转变。它的网络覆盖范围已经从原来的骨干网延伸到了配电网的末端，用户端，形成全域、全业务、全覆盖的通信体系。

（二）电力通信网的核心构成要素

构成电力通信网的要素很多，各种要素相互配合，共同保证信息的准确传递。物理层和逻辑层一起构成庞大的网络结构。为了更好的分析它的内部结构，可以将它的主要构成要素归纳如下表所示

电力通信网核心构成要素表

要素类别	主要组成	关键作用 / 特点
传输介质和线路设施	光纤复合架空地线、全介质自承式光缆、微波、卫星、电力线载波、无线公网	电力通信网的“血管”，依托电力杆塔资源架设，高可靠性，构成立体传输物理层
传输与交换设备	同步数字体系、光传送网、分组传送网（PTN/MPLS）设备；程控交换机、软交换设备、IP 路由器	电力通信网的“心脏”，实现信号复用、交叉连接、路由选择、转发，保障数据高效传输
通信支撑系统	通信电源系统、同步网系统、通信管理系统	网络运行的“免疫系统”，提供不间断供电、全网时钟同步、实时监控、配置管理与故障告警
业务接入终端	远动终端、继电保护接口装置、配电自动化终端、智能电表集中器、行政办公终端	网络的“手脚”，实现物理信号与通信信号的转换，是通信网与电力业务系统的直接接口

像核心构成要素表那样，各个要素不是孤立存在的，而是通过标准化的接口和协议相互耦合在一起的。传输介质建立物理连通性，传输设备完成逻辑通道的划分，支撑系统保证运行环境的稳定，接入终端完成业务数据的落地。正因为有这样精密的系统配合，才能使电力通信网在复杂的电磁和地理环境中长时间稳定高效地运转。

（三）与公用通信网的区别与联系

电力通信网是专用网，不同于电信运营商建立的公用通信网，但两者之间又存在着千丝万缕的联系。两者的技术体制遵照相同的国际标准，但是建设目的，服务对象，网络架构以及运维模式却大相径庭。公用网追求广覆盖、大容量、经济效益最大化，服务对象为全体民众，业务种类主要是语音和互联网接入。电力通信网的主要目标就是保障电网安全，经济效益服从于安全效益。

在服务的对象和服务的业务上,二者存在着巨大的差异。公用网用户数量多,分布分散,业务流量突发性、随机性较强,公用网网络一般采用统计复用提高网络利用率。电力通信网主要是为电力企业内部服务,它的核心业务如继电保护、调度指令等有很高的确定性、实时性要求,一般采用刚性管道或者高优先级传输方式,以保证在电网发生故障等极端情况下通信不中断。即使在网络拥塞的情况下,电力通信网也要保证生产控制类业务的传输,这种由于电力系统事故造成的通信高峰,和公用网的节假日高峰流量模型有天壤之别。

但是两者之间也存在着互补、合作的联系。从技术上讲,电力通信网大部分借鉴了公用网成熟的同步数字体系、光传送网、IP/MPLS 等技术,并根据电力行业的需要做了相应的修改。从资源利用的角度来说,电力通信网可以利用自身丰富的电力杆塔资源来架设光缆,既可以满足自身的通信需求,又可以为公用网提供路由资源;在电力通信覆盖盲区或者应急通信的情况下,电力系统也会租用公用网的链路或者利用公用无线网络进行末端接入。既相互独立又相互依存的关系,就是国家整体信息通信基础设施发展状况的真实写照。

二、电力通信网的主要特点

(一) 高可靠性与高安全性要求

电力通信网可靠性影响电网安全,任何一点通信中断或者误码都会造成电网事故扩大,甚至导致大面积停电。所以高可靠性是电力通信网的本质特征。可靠性并不单单是靠设备平均无故障时间来体现,在网络架构设计中也被充分的体现出来。电力通信骨干网一般采用环形、网孔型等高生存性拓扑结构,严格遵守 N-1 或 N-2 安全原则,即任一节点、链路故障时业务能无缝倒换保证不中断。核心调度业务一般都会配置物理路由完全隔离的双通道,甚至采用不同技术体制的异构备份方案,从而最大程度上降低共模故障的风险。

从安全角度来说,电力通信网存在物理和网络两种安全问题。从物理上来说,通信设施大多处于野外的高压输电线路或变电站里,所以需要具备强大的抗电磁干扰能力、耐高压绝缘性能、抵抗雷击、冰灾等自然灾害的能力。从网络逻辑安全角度而言,电力通信网实行严格的分区管理,对生产控制大区和管理信息大区实施逻辑或者物理隔离,采用专用的安全设备部署纵向加密认证网关、横向隔离装置等,构建起牢不可破的防御体系。

对于电力通信网来说，安全不单是要防范外部入侵，还要防范内部人员由于误操作造成的威胁。网络管理系统具有较好的权限控制以及操作审计功能，对一些关键的配置更改要经过严格的核准手续。近乎苛刻的安全标准是由电力生产“产供销瞬间完成”的特性决定的，通信网必须像电网本身一样具有很高的鲁棒性、抗毁性，在任何极端环境下都必须成为电网可以信赖的神经中枢。

（二）业务多样性与强实时性并存

电力通信网需要承载的业务种类繁多，从毫秒级的电网控制信号到大带宽的视频监控数据都有，具有很强的多样性以及差异性。除数据格式和传输速率不同外，服务质量指标的要求也不同。像对时延非常敏感的继电保护业务，它的端到端时延一般要控制在 10 毫秒之内；像对数据完整性要求非常高的电量计费业务；还有对吞吐量要求比较高的远程视频巡检业务。怎样在一个物理网络上满足这些完全不同的业务需求，就成了电力通信网技术设计中的一个难题。

为了克服这一难题，电力通信网使用了细粒度的业务分类和映射方式，具体如下业务分类与特点表所示：

电力通信网业务分类与特点表

业务类别	典型业务	核心特点	QoS 保障策略
生产控制类	继电保护、安稳装置信息、调度自动化实时数据	数据量小，实时性、抖动和可靠性要求极高	分配固定时隙或最高优先级逻辑通道，使用刚性管道技术，保障零阻塞、低延迟
生产管理类	配网自动化、故障录波远传、EMS 非实时数据	对实时性要求相对不高，数据量大，需强数据吞吐及突发流量处理能力	保证数据吞吐量与突发处理能力，优先级高于行政办公类
行政办公和信息化类	OA 办公、视频会议、企业 ERP 系统	具备互联网应用特点，带宽需求大	采用统计复用传输，网络资源紧张时优先级低于生产类业务

由上表可知，不同的业务在同一个网络里同时存在，所以通信设备要具备较强的多业务接入和调度能力。现代电力通信网通过服务质量保障、流量整形、硬切片等技术对业务进行逻辑隔离，提供不同的服务。强实时性业务独占快车道，大颗粒业务使用宽车道，这样一种“各行其道、有条不紊”的运行模式，是电力通信网区别于一般企业网的重要特点，也是保证电网生产与管理高效协同的重要因素。

（三）与电力系统物理拓扑的强关联性

电力通信网的建立和分布,很大程度上是依附于电力系统的物理网架结构的,而紧密的依存关系就是其最明显的空间特性。电力光缆一般沿着高压输电线路铺设,光纤复合架空地线直接架设在输电铁塔顶端作地线使用,全介质自承式光缆架设在输电线路下面。变电站既是电能传输的节点,又是通信网的骨干节点;发电厂既是电能的源头,又是重要的通信终端局站。电力通信网的物理拓扑和电网重合,所以其覆盖范围与电网基本一致,因此又称为电网通。

这种强相关性既有建设的优势,也有运维的困难。优势在于,电力通信网不需要像公用网那样大规模征地、建基站、铺设管线,建设成本低、周期短,可以充分利用电力线路走廊天然的路由优势。但是这也意味着通信网运行状态会受到一次电网运行状况的影响。当输电线路检修或者发生倒塔、断线故障时,挂在输电线路上的通信光缆也会受到影响,从而出现“电网故障导致通信中断,通信中断又反过来影响电网事故处理”的困境。

根据这一特点,在规划和设计电力通信网的时候,必须考虑到电网的物理走向。为防止单一输电走廊的风险,核心骨干通信网一般会采用异路由建设,即尽量避免主备路由同塔架设。配电通信网侧的通信节点分布与配电变压器、开关站的分布完全一致。和电力拓扑的深度绑定还表现在网络保护策略上,通信路由迂回策略一般要参照电网潮流流向及重要断面,在电网发生“N-1”故障的时候能够提供有效的支撑路径,而不是成为电网运行的薄弱环节。深刻认识这种拓扑关联性,对开展电力通信网的规划、隐患排查和应急演练有着非常重要的指导意义。

第三节 电力通信网体系结构

一、电力通信网的分层结构

（一）骨干层、汇聚层与接入层划分

骨干层处于电力通信网核心位置,主要是各级调度中心、大型发电厂、超高压变电站等重要节点之间进行联系,负责全网的跨区域、大颗粒业务流量的传输工作。这一层主要是由覆盖省内外各城市的光缆线路组成环形或者网状拓扑,其可靠性及传输容量极高。骨干节点数量虽然很少,但是地位十分重要,网络拓

扑设计普遍采用多重路由备份机制，在极端的灾害情况下也能保证核心业务的连续性。

汇聚层处于骨干层和接入层之间，起着承上启下的作用。它主要负责把各个接入节点的业务流量进行汇聚、收敛后上送到骨干网络，再把骨干网下发的控制指令分发给各个接入点。汇聚层节点分布较多，在地区供电局、大部分变电站和部分重要配电点都有分布。本层建设重点是提高网络的覆盖密度，提高业务调度的灵活程度，一般采用环网和链形相结合的混合拓扑结构，既可以提高传输效率，又可以适应各个区域电网发展需求的不同。

接入层就是电力通信网最后一公里，直接面向成千上万的电力终端设备，比如配电变压器、智能电表、分布式电源、微网控制器等。节点数量很多，分散性大，所处环境复杂多变。接入层建设的主要目的就是实现广覆盖、大连接，消除通信盲区。根据不同的应用场景，可以选择有线或者无线通信方式，构成星型、树型或者网状网络结构，保证各种末端感知数据的实时采集以及控制指令的准确下达。

（二）各层功能定位与关键技术

骨干层的主要功能就是提供超大带宽、超长距离、极低时延的信息传输通道，保证跨区域电网调度指令和广域相量测量数据的实时交互。因此光传送网技术得到了广泛的应用，特别是密集波分复用技术，一根光纤就可以实现太比特级的传输容量。随着业务颗粒度更加精细化，分组增强型光传送网技术逐渐占据了主流，它把光层的传输优势和数据层的灵活调度能力有机地融合在一起，可以有效地承载大容量的电路交换、分组交换业务。

汇聚层主要是对业务流量进行汇聚、转发和初步处理，需要具有很强的多业务适配能力和高网络生存性。本层核心使用分组传送网技术，分组传送网技术在保留传统同步数字体系保护倒换、操作维护特性的同时，加入了面向连接的分组交换方式，可以较好地处理突发数据流量。为应对以后业务云化迁移的趋势，部分汇聚节点已经开始使用路由交换技术，利用灵活的三层路由网络来实现业务流量的就近转发和智能选路，进而有效地减轻骨干网的传输压力。

接入层的主要功能就是提供泛在、异构、低成本的终端接入能力来满足海量物联网设备的连接需求。无源光网络技术由于具有无源、抗干扰性好、维护成本低等特点，已经成为配电通信网主流的有线接入技术。光缆不能到达的地方，无线公网、电力无线专网、微功率无线通信技术起着重要的补充作用。随着 5G 移

动通信技术的成熟应用，5G 的低时延、高可靠、大连接特性正在慢慢改变接入层的技术生态，在精准负荷控制、配网差动保护等业务上有着巨大的应用前景。

（三）分层结构的优势与挑战

分层结构设置使电力通信网有显著的管理优势和很强的扩展性。经过网络分层以后，运维人员就根据不同层的特性来制订差别化的运维策略，骨干层以光缆路径安全为主，接入层则是以设备的在线率以及覆盖范围为主。网络需要扩展或者技术升级的时候，分层架构可以实现局部的技术更新，而不会给整个网络架构带来巨大的冲击。这样模块化的发展方式大大降低网络创建的复杂性以及投资风险。

但是伴随电网业务数字化、智能化转型的不断深入，传统分层结构也面临前所未有的挑战。分布式能源大量接入引起电力流与信息流双向互动，原以纵向汇聚为主的流量模型发生了根本变化，横向流量剧增给汇聚层、骨干层跨域调度能力带来巨大压力。大量异构终端接入造成接入层网络边界越来越模糊，安全防护也变得越发复杂困难。怎样在维持分层架构清晰性的同时，打穿层级壁垒，达成端到端的业务快速开通与协同保障，成了当下电力通信网架构演进进程中必须面对的难题。

二、电力通信网的域间划分

（一）调度通信域与行政通信域

1. 调度通信域：属于电力通信网中安全等级最高的区域，专门为电网生产控制类业务服务。此区域担负着继电保护、安全自动装置、调度自动化、广域相量测量等诸多重要业务，这些业务对于通信时延、抖动、可靠性等指标有着很高的要求。为保证电网运行绝对安全，调度通信域一般采取物理隔离或者逻辑强隔离的方式，建立独立传输线路和交换网络，严禁和外部公共网络直接相连，从而形成封闭受控的高安全通信环境。

2. 行政通信域：主要为电力企业的日常经营管理和办公自动化服务，它所承载的业务有视频会议、企业资源计划系统、办公邮件、营销服务等。行政通信域业务流量大、突发性强，实时性要求不高，但是对带宽扩展性、应用层功能丰富性有较高要求。该区域网络一般会存在受控的互联网接口，使用通用的互联网协议技术栈，有利于信息的快速共享和跨部门协作，利于企业数字化转型和管理创新。

(二) 发电、输电、变电、配电、用电通信域

通信域	主要业务 / 功能	通信特点 / 需求	关键技术 / 介质
发电通信域	实时监测与调节：逆变器状态、风机转速、光伏板温度等；发电量上报；源网协调控制	高频数据采集、指令下达；满足电网侧频率调节、电压支撑要求	专网通信、工业以太网、光纤
输电通信域	输电线路及附属设备状态监测：覆冰、舞动、杆塔倾斜等；无人机巡检；分布式传感	长距离传输、低功耗；地理环境恶劣、供电困难；空地一体化立体通信	光纤复合架空地线、微波、卫星通信、无线传感网
变电通信域	站内保护装置、测控单元和监控后台高速、低时延通信；站内全景数据上传	高速、低时延通信；满足智能变电站过程层 / 站控层信息交互；数据汇总	光纤以太网、IEC 61850 规约、同步数字体系
配电通信域	中低压配电网自动化与智能化：配电开关监控、故障定位隔离；供电可靠性提升	节点数量最多、拓扑变化最频繁；复杂网络结构；广覆盖、可靠性高	光纤、无线通信（4G/5G、LoRa）、配电自动化规约
用电通信域	智能用电采集、双向互动服务、电动汽车充电桩管理；需求侧响应、虚拟电厂	终端分散、数据并发量大、单点流量小；海量小数据包快速传输、拥塞控制；用户隐私安全	蜂窝网络、电力线载波、微功率无线、智能抄表规约

发电通信域主要涵盖各种规模的火电、水电、核电厂以及新兴的新能源场站。由于新能源装机比例的上升，该领域的通信需求也由原来的发电量上报转变为对逆变器状态、风机转速、光伏板温度等大量参数的实时监测和调节。通信系统要满足高频数据采集、指令下达给电网侧频率调节、电压支撑的要求，保证源网协调运行。

输电通信域就是对输电线路和其辅助设备状态进行监测。本区域的通信节点大多数沿高压输电走廊呈链式分布，地理环境比较复杂，供电条件比较艰苦。因此通信技术需要具有长距离传输、低功耗等特点，光纤复合架空地线是主要的传输介质。随着无人机巡检和分布式传感技术的使用，输电通信域也开始形成空地一体化的立体式通信网，对线路覆冰、舞动、杆塔倾斜等隐患进行实时感知。

变电通信域主要位于变电站内，起骨干网和接入网连接的作用。在智能变电站架构下，站内通信网络已经从原来的电缆连接变成了现在的光纤以太网，过程层和站控层的划分使得二次设备间的信息交换更加高效。该域通信的重点就是保证站内保护装置、测控单元和监控后台之间高速低延迟的通信，及时将站内汇总的全景数据传送到上级调度中心和运维主站。

配电通信域的节点数量最多、拓扑变化最快。此域主要为中低压配电网自动化和智能化服务，如配电开关监控、故障定位隔离等。配电网的网络结构比较复杂，一般用光纤和无线混合的方式进行通信。该域的建设水平直接决定着供电可靠性和电压质量，是现阶段电力通信网投资建设的重点。

用电通信域直接面向最终的电力用户，包含智能用电采集、双向互动服务、电动汽车充电桩管理等业务。该域通信的特点是终端分散，数据并发量大，但是单点流量小。通信系统要处理海量小数据包的快速传输以及拥塞控制的问题，同时还要注重用户隐私数据的安全。电力市场化改革不断推进之后，用电通信域已经成为电网和用户之间数字化的桥梁，支撑着需求侧响应、虚拟电厂等新业务的发展。

（三）各通信域的业务特点与互联需求

上表中各个通信领域在地理上、服务对象上存在差异，但是业务运转越来越紧密。调度域要实时从发、输、变三个域获取运行数据来进行状态估计和安全分析，还要把控制指令穿透到配电域乃至用电域的分布式资源。这种跨越式的业务链条，就要求通信网络要打破以前的信息孤岛，建立统一的数据交换准则和连接接口。源网荷储协同互动，电网侧需要实现分钟级甚至秒级的调整用户侧的空调或者储能设备，这就要求跨域通信的时延稳定性和指令执行的确定性达到很高的要求。

各个通信域的业务流量特性大相径庭。发电和变电领域以持续稳定、有规律的周期性数据为主，流量模型容易预测；配电和用电领域具有明显的突发性、随机性，受用户行为、环境因素影响较大。行政域主要是尽力而为的大带宽数据流。域间互联的时候，要部署高性能的网关设备以及流量整形策略，避免低优先级业务的突发流量对高优先级业务通道造成冲击。并且要形成纵深防御体系以应对跨域网络安全风险，把防火墙、正反向隔离装置以及入侵检测系统部署到各个安全域之间，保证数据流传输时不被泄露、不被篡改，可以正常访问。

三、电力通信网的逻辑功能架构

逻辑功能架构冲破了物理设备具体形态的束缚，从信息处理以及网络控制的角度出发，对电力通信网展开抽象并重新构建。它规定了网络中各种不同的逻辑实体的职责划分以及相互关系，是实现网络智能化管理以及业务敏捷编排的重要基础。现代电力通信网的逻辑结构正朝着控制和转发相分离、管理和业务相融合

的趋势发展。

（一）承载网、业务网与支撑网

逻辑网	功能定位	组成部分 / 技术	主要特点 / 作用
承载网	透明传输和交换比特流； 为上层业务提供统一接口 和 QoS 承诺	光缆、微波、载波等 传输介质；光传输设 备、路由器、交换机	坚强、灵活、泛在的物理管道； 具备网络切片能力，提供逻辑 隔离的专用网络
业务网	直接为各种电力应用提供 通信服务；管理会话、寻 址、业务逻辑	电话交换网、调度数 据网、综合数据网、 视频会议系统	调度数据网独立于行政网；综 合数据网承载管理信息流；与 电力业务流程紧密契合
支撑网	辅助承载网、业务网正常 工作；提供统一时间 / 频 率基准、传输控制信息	同步网、信令网	确保数字通信网络无滑码传输； 保证电网相量测量数据时间精确 对齐；网络智能化的神经中枢

承载网是电力通信系统的基础，对比特流进行透明传输和交换。它由光缆、微波、载波等传输介质和光传输设备、路由器、交换机等网络单元组成。承载网的设计目的就是建立一个坚强、灵活、泛在的物理管道网络，屏蔽底层传输介质的差别，给上层业务提供统一的服务接口和质量承诺。伴随着技术的发展，承载网已经逐步具备了网络切片的能力，可以在同一物理设施上虚拟出多个逻辑上相互隔离的专用网络，从而满足不同业务对于服务质量多样化的需要。

业务网是在承载网基础上，面向各种电力应用提供通信服务的网。它一般由电话交换网、调度数据网、综合数据网、视频会议系统等组成。业务网主要研究的是会话的建立、路由寻址和业务逻辑的实现。调度数据网用专用虚拟局域网技术，在逻辑上建立了一个独立于行政办公网络的平面，专门给实时生产控制业务服务；综合数据网用多协议标记交换技术来承载各种管理信息流。业务网的形成要同电力业务流程相契合，保证通信服务可以同生产管理流程无缝对接。

支撑网是保证承载网、业务网正常工作的辅助网络，主要有同步网和信令网。如上表所示，同步网为全网设备提供统一的高精度时间、频率基准，保证数字通信网络无滑码传输、电网相量测量数据时间精确对齐。信令网传输的主要为网络控制信息，如呼叫建立信令、路由更新信令等，是网络智能化的“大脑”。虽然支撑网不直接承载用户数据，但是支撑网的运行状况会直接影响整个通信网络的稳定性和可靠性。

（二）网络管理、同步与信令系统

网络管理系统是电力通信网的“大脑”，可以对全网资源实施集中监控、配

置、分析、优化。现代电力通信管理系统已经从原来的单一设备级管理发展为网络级、业务级管理，并且对不同的厂商、不同的技术都有统一的纳管能力。采用人工智能，大数据分析技术以后，系统可以开展故障预知性保养工作，而且还能做到告警信息自动关联起来进行分析，并且把网络流量平均分配出去，以此来提高运营效率。同时为了适应软件定义网络技术的应用，管理系统正向网络控制器演进，可以利用软件编程的方式对网络拓扑及流量策略进行动态调整。

同步系统在电力通信网中有特殊重要的地位。它既可以为通信设备提供时钟同步，也可以为电网一次设备提供高精度授时。智能变电站、广域保护投入使用以后，时间同步的精度要求就达到了微秒甚至纳秒。目前的同步网络主要以北斗卫星导航系统为主，地面光纤时间同步网络为辅，用时间协议在光传送网中传递时间信息，解决了卫星信号易受干扰、室内覆盖不足的问题，形成了天地一体、互为备份的高可靠时间同步体系。

信令系统是网络控制信息的载体，其结构的好坏直接影响连接建立速度及网络的可扩展性。传统的电路交换网，七号信令系统为主。全 IP 网络发展过程中会话发起协议、直径协议等软交换和融合通信信令系统也越来越流行。基于 IP 的信令协议更开放灵活，可以支持多媒体业务融合和跨域漫游。尤其是对电力无线专网来说，有效的信令交互方式成了大量终端快速接入和移动性管理的基础。

（三）“云-管-边-端”一体化架构

云-管-边-端一体化架构，是为满足能源互联网发展需求而产生的新型逻辑形态，它不再把通信网仅仅看作传输通道，而是将其提升为计算、通信、存储一体化的数字化基础设施。

1. “云”层，也就是中枢大脑，把全网的数据收归己有，并且布置强大的计算集群以及大数据分析平台。主要处理电网规划优化、电力市场交易分析等全局性、长时间跨度、非紧急的复杂决策事务。

2. “管”层：即通信网络，既是连接通道，又具有算力调度能力，可以实现数据在云、边、端之间的快速传输。

3. 边层：在网络的边缘，靠近数据源头的地方布置了边缘计算节点。它担负着实时性高、数据量大的局部业务处理工作，像配网故障就地研判、视频监控智能分析之类，这样就很好地缓解了云端的压力以及传输时延。

4. “端”层指的是各种各样的感知、执行终端，具有一定的信息采集和初步

处理的能力，是物理世界和数字世界的交汇点。

一体化架构结合了软件定义网络、网络功能虚拟化这些先进技术，把计算资源和通信资源深度融合起来一起调度。实际运行时，端侧采集的数据根据业务需要可以在本地进行处理，也可以上传到边缘节点进行清洗，还可以直接上传到云端进行分析。这样的结构大大提高电力通信网对新兴业务响应速度与处理能力，给构建万物互联、人机智能互动现代能源体系奠定坚实的技术基础。云边协同之后，算法模型可以云端下发给边缘做推理，边缘的样本数据也可以上传到云端做模型训练，如此便形成了一个不断改进的智能闭环。

第四节 电力通信网技术标准

一、国际标准组织与体系

（一）IEC、ITU-T、IEEE 等主要组织

国际电工委员会在电力自动化和通信领域中处于领导地位，该协会下的第57技术委员会是专门从事电力系统控制以及相关通信标准的制定。TC57制订的一系列标准涵盖了从调度中心到变电站、再到配电网整个通信网络和系统的规范，其中变电站通信网络和系统规范最为人所熟知。该组织致力于电力系统各个层次的信息模型的统一，保证不同的应用系统之间传输的数据能够被正确理解。IEC体系重视语义互操作性，用抽象通信服务接口来定义，使应用功能和底层通信技术解耦，电力系统可以灵活地使用不断发展的通信技术，不需要频繁重构应用层。

国际电信联盟电信标准化部门主要是就底层通信传输技术进行标准化。制定了一系列重要的同步数字体系和光传送网标准，对光接口参数、帧结构、复用映射方式、网络管理功能都作了详细的说明。对于电力线载波通信，国际电信联盟电信标准化部门也发布了有关窄带和宽带电力线通信的建议书，对在电力线上进行数据传输的物理层和数据链路层机制做出了规定。其标准一般都很严格并且具有普遍性，给电力通信骨干网和接入网的物理通道创建赋予了强有力的保证，保障了全世界通信设备在物理层面相互连接。

电气电子工程师学会在局域网、城域网、无线通信技术上做出重大贡献，它制定的以太网标准系列在电力通信网中应用最广，是链路层协议。IEEE 802系

列标准对以太网的物理介质、帧格式以及介质访问控制方式做了规定，成为变电站站控层和过程层网络的基础。电气电子工程师学会为无线通信所制定的 Wi-Fi、ZigBee 等标准，在配用电通信网“最后一公里”接入中同样起着非常重要的作用。电气电子工程师学会也制定了些电力系统特殊需求的标准，比如精确时间同步协议、同步相量测量通信标准。这些建立起来的标准对于开展广域测量系统、电网实时动态监测起了很好的促进作用。

（二）国际标准在电力通信中的应用

国际标准在电力通信里被普遍应用到发、输、变、配、用各个部分，进而形成起全方位多层次的标准化通信环境。变电站自动化当中，IEC 61850 标准成了全球通行的标准。此标准不但规定了站内智能电子设备之间通信行为，而且还用面向对象的建模技术将变电站的一次设备、二次功能抽象为逻辑节点。变电站内保护、测控、计量等各种功能可以借助于统一以太网平台来共享信息。智能变电站的建设大多采用 IEC61850 标准的过程层网络来取代传统的二次电缆，用 GOOSE 和 SV 报文，大大减少现场接线的工作量，提高系统维护性以及拓展性。

广域通信网采用国际电信联盟电信标准化部门标准的 OTN 技术建立电力骨干传输网。电力系统调度数据、继电保护信号、视频监控业务对传输时延、抖动、可靠性有不同的严格要求。OTN 技术把电信级运维管理能力同波分复用的大带宽结合起来，可以做到刚性管道、物理隔离，保证关键生产业务的安全传输。应用这些国际标准之后，电力通信网就形成了连接省、地、县三级调度中心的传输大动脉，进而达成跨区域资源调配和故障协同处理。

配用电通信网络大量使用电气电子工程师学会系列标准来实现海量终端的灵活接入。配电自动化系统中工业以太网交换机按照 IEEE 802.3 标准构建环网或者树形网络，把柱上开关和环网柜终端连接起来，从而实现对故障的快速识别并将其隔离。以 IEEE 802.15.4 无线传感器网络技术为载体，在智能用电环节开展智能电表数据采集、家庭能源管理。这样就可使电力通信网深入每一个千家万户，实现双向互动的智能用电服务模式，进而达到分布式能源消纳和需求侧响应的目的。

（三）国际标准化最新进展

伴随着能源互联网、数字化转型的发展，国际标准化组织会提高电力通信标准效率、安全性、智能性。国际电工委员会 TC57 正在努力将 IEC 61850 标准从

变电站内部扩展到变电站之间以及配电网,研究基于广域网的保护控制通信机制。国际电工委员会正努力把 CIM 模型和分布式能源接入所产生的大量数据融合起来,从而实现整个网络语义的统一建模,消除各个业务系统之间存在的信息孤岛,使跨域数据可以自由流通。

由于通信技术的更替,底层传输标准也在不断更新,时间敏感网络成了当下国际化的热点。电气电子工程师学会正在制定一系列时间敏感网络标准,以太网为基础提供确定性的时延、零丢包的传输能力,这对满足电力系统对于实时控制的极致要求有着极其重要的意义。时间敏感网络技术可以同时承载不同优先级的业务,可以保证继电保护等重要业务的实时性,也能满足视频等大流量业务的带宽需求,给电力通信网融合架构提供了一种新的技术途径。

无线通信上,以 3GPP 为首的 5G 标准已经同电力垂直行业深度对接。国际标准化组织对于 5G 网络切片、低时延高可靠通信、海量机器类通信在智能电网中应用的研究工作正在进行。使用电力专用网络切片模板和服务质量参数,国际标准解决公网承载电力业务的安全性、隔离性问题,促进 5G 技术在配网差动保护、无人机巡检、精准负荷控制等场景的应用。

二、国内标准体系

我国的电力通信标准体系是以国际标准为基础,结合我国电网的调度体制、管理方式和技术特点来建立完善的。这套体系既接轨国际,又具有中国特色,支撑起世界上最大的电网安全稳定运行和智能化发展。

国内电力通信标准层级对比表

标准层级	发布机构	性质	主要范围 / 特点
国家标准	国家标准化管理委员会	强制性 / 推荐性	核心技术领域, 与国际主流技术路线接轨, 提供统一研发依据。例如: 变电站通信网络。
行业标准	国家能源局 / 相关行业协会	推荐性, 具体化	补充国家标准, 聚焦电力行业特有通信技术及业务规范。例如: 电力线载波、电力光纤到户。
企业标准	国家电网、南方电网等大型企业	内部规定, 要求更高	高于国标和行标, 新技术落地先行先试, 工程建设和物资采购的具体指导。例如: 物联网架构、设备技术规范。

如上表所示,我国电力通信标准体系分为国家标准、行业标准和企业标准三个层级。

（一）国家标准、行业标准

国家标准属于我国电力通信技术领域内最高层级的规范，由国家标准化委员会发布，具有强制性或者推荐性。在电力通信方面，GB/T 系列标准基本都是对核心国际标准的等同采用或修改采用，使得国内的技术路线与国际主流接轨。我国对于变电站通信网络及系统有国家标准，详细规定了通信网络结构、数据模型、一致性测试方法。这些国家标准的选定为国内的电力设备制造企业提供统一的研发标准，避免出现因为标准不一样而造成市场的碎片化、资源浪费的现象。

行业标准（DL/T）是由国家能源局或者行业协会来制定的，主要是对电力行业具体使用情况的细化和补充。电力行业的标准中包含了电力特有的一些通信技术以及业务规范，例如电力线载波通信、电力光纤到户、电力应急通信等。行业标准具有很强的操作性，对设备技术参数、功能要求、试验方法、运行维护流程等都做了详细的说明。电力系统继电保护通信接口、调度数据网技术体制等各方面行业标准起着至关重要的规范作用，保证了通信系统与一次系统、二次保护系统相互配合。

1. 标准化转化的深度与广度：我国在引进国际标准的时候，并不是简单地照搬翻译，而是根据国内电网高电压、长距离、大容量的特点进行了适应性改造。在超高压电网继电保护通信标准中，对于长距离光纤传输特性提出了具体指标要求。

2. 自主标准的创新突破，按照我国电力业务的特点，如大规模集中抄表的需求等，我国制定了相应的低压电力线载波通信标准，对物理层的调制方式以及组网协议做出规定，促进了国内芯片、设备的发展。

（二）电力企业标准与技术规范

电力企业所使用标准一般为国家电网、南方电网等大型国有企业制定的，技术指标比国家标准和行业标准要高些，以满足更高的供电可靠性要求。企业标准是新技术落地应用的前哨，在国家标准还没有出台的新兴技术领域，企业标准常常先行先试，填补空白。电力物联网建设之初，两大电网公司都发布了自身单位的物联网架构标准、终端接入协议和边缘计算技术需求等指导文件，推动了很多试点项目的实现。

技术规范属于企业标准的补充，通常用在具体的工程建设以及物资采购过程

当中。电网公司每一期集中招标采购都会发布设备技术规范书，对通信设备的硬件配置、软件功能、环境适应性、售后服务等做出具体的规定。这些规范有很强的约束力，直接决定入网设备的质量水平。以动态修订技术规范促进供应商技术，比如近年要求光传输设备要支持最新的加密等级的算法，交换机要有一定的抗电磁干扰的能力。

电力企业的标准中，对于系统集成和运行管理的标准化有特别的强调。对于通信管理系统，企业标准明文规定了北向接口规范，不同的厂家网管系统都可以通过北向接口接入到统一的综合监管平台，对全网通信资源实施集中监视、集中调度。配用电通信领域的企业所制定的标准对通信模块的物理尺寸、引脚定义作出规定，使通信模块可以即插即用、互相替换，大大降低现场运维的工作难度和备品备件的费用。

（三）国内标准体系的构成与特点

国内电力通信标准体系是“基础标准打根基、设备标准做支撑、业务标准导向、管理标准保运行”的立体结构。基础标准规定术语定义、电磁兼容、环境条件等通用要求，给整个体系提供底层逻辑支撑。设备标准对光传输、程控交换、数据网、无线接入等各种具体的设备都有详细的技术要求。业务标准主要是对调度自动化、继电保护、营销计量等具体业务所要求的通信通道的时延、带宽、误码率等提出的要求，体现的是通信为电网生产服务的本质。

该体系最大的特点就是全生命周期的标准化管理。从规划设计、工程建设、竣工验收、运行维护、退役报废等各个阶段都有相应的标准可以参照。设计规范对通信网的拓扑结构、路由迂回方式、电源配置等提出要求，保证网络物理结构的健壮性；验收规范对测试项目和合格判据做出详细规定，严控工程质量；运行规程对巡视检查、故障处理、检修作业等实行标准化流程，保证网络运行连续稳定。

国内标准体系还有很强的安全导向性。由于电力通信网是“第二张实体电网”，安全防护标准被提到了很高的优先级。体系里包含了很多关于电力监控系统安全防护、通信网网络安全接入、数据加密认证等强制性的规范。要求建立纵深防御体系，实行分区、分级、隔离管理，严防外部网络攻击对核心控制系统造成影响。用安全优先的标准设计思想来应对日益复杂的网络安全威胁，保障国家能源基础设施的信息安全。

国家标准、行业标准、企业标准三者有机结合、互相补充，构成国内电力通信标准体系动态演进的闭环。工程实践中出现的经验教训被及时总结，转化为企业的标准，在经过实践检验后，再上升为行业标准或者国家标准，反过来又指导着更多的工程实践。此种机制使标准体系具有了生机，可以迅速适应能源革命与数字革命所带来新技术的挑战。

第二章 电力通信网基础理论

第一节 通信系统基本原理

一、通信系统模型

（一）信源、信道与信宿

信源是消息的产生地，主要功能就是把各种形式的原始信息转化成电信号。在电力通信场景中，信源种类繁多，既有变电站各种传感器采集的模拟电压电流数据，又有调度中心发出的数字控制指令。非电或电物理量经转换之后，就成了后面环节可以处理的基带信号，为信息的远距离传输在形态上做好了准备。

信道是信号传输的物理媒介，把发送端和接收端连接起来，是通信系统里最复杂的部分。电力通信网充分利用了电力特有的资源，光纤复合架空地线、电力线载波等各种信道形式都存在。光纤信道因为其宽频带和低损耗而被选作骨干网；电力线载波利用已经存在的输配电线路来传输数据，覆盖面广，但是需要面对恶劣的噪声环境和阻抗变化。信道物理特性会影响信号传输距离、传输速度，在系统设计时要把信道的物理特性作为重要的约束条件来考虑。

信宿是传输过程的终点，它把接收到的电信号还原成接收者能理解的消息。无论是电网调度员面前的监控大屏，还是自动化装置内部的逻辑处理器，信宿都要将信源发出的原始意图完整无缺地还原出来。本质上就是信源变换的反过程，它的正确性完全取决于信号在传输过程中保持的完整性。如果信道中掺杂过多的畸变因素，信宿的还原工作就会变得很困难，甚至会出现错误的操作指令，在电力系统中这是不允许的。

（二）发送与接收设备

发送设备处在信源与信道之间，它要对基带信号实施必要的加工，使之契合信道的传输特性。一般的过程分为编码、调制这两个步骤。信源编码是去除冗余信息以提高传输效率，或者增加冗余位来提高抗干扰能力；调制就是将基带信号搬移到适合信道传输的高频载波上。在电力微波通信或者无线专网中，发送设备

必须具有高精度的频率合成和功率放大能力,才能使信号越过地理障碍,稳定地传送到远端。

接收设备的功能和发送设备正好相反,它要从信道中取出微弱的有用信号,然后进行解调、解码,最终恢复出原始的基带信号。信号在传输的过程中不可避免地要受到衰减和噪声的影响,所以接收设备一般都配备性能较好的滤波器和放大器。现代数字通信系统中,接收机还带有复杂的均衡算法以及同步技术,用来补偿信道造成的频率选择性衰减和时延抖动。电力系统继电保护通道接收设备处理的速度会影响故障切除的时间,所以要求硬件有很好的实时处理能力。

随着现代通信技术的发展,发送设备和接收设备越来越集成化、智能化。软件无线电技术出现以后,可以通过软件定义的方式改变设备的功能,使系统更加灵活。智能变电站的通信接口设备不仅要完成物理层信号的收发,还要完成链路层甚至网络层的协议解析,是一次设备和站控层网络之间的重要节点。集成度越来越高,虽然简化了硬件设计,但是给设备的散热设计和电磁兼容性提出了新的挑战。

(三) 噪声与干扰

通信系统运行的背景不可能是真空般的干净,一定会受到各种噪声和干扰。噪声是影响通信系统性能的主要因素,它既可以是系统内部电子器件产生的热噪声、散粒噪声,也可以是外部环境的电磁干扰。在电力通信环境下,高压开关操作产生的瞬时脉冲、输电线路电晕放电、雷击电磁脉冲等都是具有很强行业特征的强干扰源。这些干扰信号叠加在有用信号上,会使接收端做决策时产生偏差,从而造成误码。为了对抗噪声,工程师们设计出了各种各样的信道编码方案以及扩频技术,妄图在噪声的背景中开辟出一条路来。

二、信息与信号度量

(一) 信息的度量: 熵

信息在通信理论中是有统计学意义的,信息就是消息中的不确定性。一个事件发生的概率越小,那么这个事件发生所包含的信息量就越大。为了度量各种消息所含信息的多少,提出了熵的概念。熵是信源输出的消息平均信息量的度量,从统计平均的意义上反映了信源整体的特性。二进制数字通信中信息量的单位一般用比特,一个比特就是两个等概率事件中发生一个所消除的不确定性。

对于连续变化的模拟信源，熵的概念就要发展到微分熵。虽然微分熵不再直接代表信息量，但是它还是可以表征信号取值的随机性。电力系统监测时，大量的数据一般都会有很强的时空相关性，即数据中有很多是冗余的。根据信源熵的计算结果，可以知道数据压缩的理论极限，从而设计出高效的编码算法。在广域相量测量系统中，对高频采样的同步相量数据进行熵编码，可以大幅度降低传输带宽的需求，从而减轻骨干网的流量压力。

信息的度量与消息本身的意义完全无关。不论跳闸指令是紧急的还是普通的，只要它们的统计概率特征相同，在通信理论里它们的信息量就一样。不考虑语义层面的度量方法，使通信工程师可以把注意力集中在底层的传输问题上，不需要关心上层应用的具体逻辑。就是在这个理论的基础上，通用的通信网络才可以承载各种各样的电力业务，底层的资源共享、复用才得以实现。

（二）模拟信号与数字信号

信号是信息的物理载体，根据参量取值是连续还是离散，可以分为模拟信号和数字信号两种。两种信号形态同存在电力通信网络里，各自发挥作用、各尽职守。

1. 模拟信号是时间上连续、幅度上也连续的信号。传统的载波电话、早些时候的远动遥测系统多用模拟信号来传送信息。模拟信号可以直接反映物理量变化的过程，波形的每一点都含有特定的信息。但是模拟信号在传输过程中抗干扰能力较弱，噪声叠加后很难去除，随着传输距离的增大，噪声不断积累，信号质量迅速下降。不过，模拟信号在实时性要求高、传输距离短的模拟量采集回路中仍然起着不可替代的作用。

2. 数字信号是时间上离散、幅值量化的信号。经过抽样、量化、编码这三步就可以把模拟信号变成数字信号。数字信号的抗干扰能力强，用再生中继技术可以消除传输过程中噪声的累积，从而实现长距离高质量传输。数字信号便于加密、压缩和差错控制，很适合于电力通信网对安全性、可靠性有严格要求。由于数字信号处理芯片性能的飞速发展，电力通信网已经全面走向数字化，从变电站内部的过程层网络到跨地区的骨干传输网，数字信号已经成为信息交流的主要方式。

（三）信号带宽与频谱

任何实际的信号在频域上都存在一定的宽度，称为信号的带宽。信号的频谱结构可以反映出信号能量在频率轴上分布的情况，它是认识信号传输特性的重要角度。按照傅里叶变换理论，时间有限的信号在频域必然无限延伸，但在工程中

一般只关心包含大部分能量的主瓣宽度。电力通信中基带数字信号的带宽和传输速率成正比，速率越高占用频带就越多。

信道带宽资源是有限的，在有限带宽内传输更多的信息成为通信技术不断追求的目标。电力线载波通信可用频谱资源由国家无线电管理机构严格划分，受到线路阻抗特性的限制，一般只用在几十千赫到几百千赫范围内。为了在这么窄的频带内实现高速的数据传输，正交频分复用等高频谱利用率的技术被广泛使用。这些技术把高速的数据流分成许多低速的子流，然后在多个互相垂直的子载波上分别传送，这样就大大提高了频谱效率。

信号的带宽还会对其通过信道时所受到的失真产生影响。如果信号的带宽大于信道本身的相干带宽就会造成频率选择性衰减、波形畸变、产生码间干扰。因此，在设计电力通信链路的时候，必须使信号带宽和信道带宽相匹配。光纤通信虽然光纤本身具有巨大的潜在带宽，但是实际可以利用的带宽受到色散、非线性效应的限制。采用波分复用的技术可以同时在一个光纤内传输不同频率的光信号，信道带宽可提升好几个数量级来满足电网大数据的传输要求。

三、通信系统性能指标

（一）有效性：传输速率与频带利用率

有效性主要是通信系统传输信息的速度和资源利用的效率。模拟通信系统用有效传输频带来衡量它的有效性，数字通信系统则用码元传输速率和信息传输速率来表示。码元传输速率，也就是波特率，表示的是每秒传输的码元符号个数，码元传输速率反映的是信号波形变换的速度；信息传输速率，也就是比特率，表示的是每秒传输的平均信息量。多进制调制中，一个码元传送多个比特信息，所以比特率大于波特率。

频带利用率又称为带宽利用率，即单位频带宽度内所能实现的传输速率。它直接体现出系统对宝贵的频谱资源的利用程度。电力无线专网建设中频谱资源非常有限，提高频带利用率就是指在相同的频宽内，可以接入更多的终端或者提供更大的业务带宽。为提高该指标，高阶调制技术被广泛应用，但是也增大了系统实现的难度以及对信道环境的敏感性。

伴随着智能电网业务的发展，对通信系统的有效性要求也越来越高。配电自动化“三遥”业务需要通信网低时延、高吞吐量，视频监控、巡检机器人等宽带

业务需要传输速率达到吉比特级。因此下一代电力通信网必须在物理层技术上进行持续创新,采用毫米波、大规模天线阵列等新技术,大幅度提高系统传输容量以及频谱利用率,以满足以后全域物联网接入需求。

（二）可靠性：误码率与误帧率

可靠性是通信系统正确无误的传送信息的能力,在电力系统中,可靠性比有效性更加重要。模拟系统的可靠性一般用接收端输出信噪比来度量,数字系统用误码率、误帧率来度量最为直接。误码率就是接收错误码元个数和总传输码元个数之比,用来衡量系统在统计意义上的准确性。在电力调度数据网中,因为传输的是关系到电网安全的控制指令,所以对误码率的要求非常高,一般要求小于十的负九次方或者更低。

而误帧率是从数据链路层来考察可靠性的。一个数据帧只要出现一个比特出错,就会把整个数据帧丢弃或要求重传。恶劣的电磁环境会引发突发性干扰产生成串的误码,造成大量的丢帧。为了保证通信的可靠性,在电力通信协议中都加入了循环冗余校验及自动重传请求。当出现错误的时候,接收端就会要求发送端重新发送数据,直到接收正确为止。虽然这会牺牲一部分传输效率,增加时延,但是可以保证数据的最终正确性,对非实时但是要求高可靠性的业务来说非常重要。

（三）有效性与可靠性的权衡

通信系统有效性与可靠性是一对受物理规律限制的矛盾统一体。信噪比一定的情况下,香农公式给出了信道容量的极限。提高传输速率(即提高有效性)一般采用更高阶的调制方式或者减少纠错编码冗余度,但是信号点在星座图中会变得更密集,两个信号点间欧氏距离变小,在同样的噪声干扰下容易产生判断错误,从而造成误码率增大(即降低了可靠性)。相反要得到很低的误码率需要增大发射功率、减小传输速度或增加冗余编码,但会破坏系统的有效性。

在电力通信网的工程实践过程中,必须根据具体业务需求找到两者之间的最佳平衡。

通信系统性能权衡表

指标	继电保护通道	变电站视频监控	智能抄表数据
可靠性要求	极高（万无一失）	中等（可接受偶尔马赛克）	高（数据完整性）
有效性要求	低速（可牺牲带宽）	高速（画面流畅清晰）	中速（周期性传输）
时延要求	极低（毫秒级）	中等（秒级可接受）	较高（分钟级可接受）
典型技术选择	低速、强抗干扰编码	高压缩比、高传输速率	窄带、高效组网

继电保护通道的可靠性和实时性是压倒一切的要求，因此宁可牺牲带宽，采用低速但抗干扰能力强的编码方式，也要保证跳闸指令万无一失。变电站视频监控业务偶尔出现的马赛克、丢帧等现象并不会造成严重后果，因此可以采用较高的压缩比、传输速率来保证画面的流畅、清晰。智能抄表等周期性数据对实时性要求不高，但是对数据完整性要求较高，可以使用窄带、低功耗但是有重传机制的通信技术。

权衡在网络架构的设计中也有体现。为了提高可靠性，电力通信网一般采用双路由、双设备热备的方式，甚至采用迂回路由很多的环形或网状拓扑。冗余配置虽然会降低网络整体的资源利用率（有效性），但是它给电网安全筑起了坚固的防线。未来技术发展希望可以接近香农极限工作，在香农极限附近使用最新的信道编码技术，比如极化码、低密度奇偶校验码等，传输速率很高，但是误码率依然很低，在高层次上实现了有效性与可靠性。这既是通信理论研究的前沿，又是现代电力通信网演进必然走向。

第二节 信号传输与调制技术

一、模拟调制技术

（一）幅度调制

幅度调制是用基带信号来控制载波的振幅，使载波的振幅随基带信号的变化而变化。早期电力线载波通信由于解调结构简单，线性幅度调制方式被广泛使用。标准幅度调制信号的频谱由载波分量和上下两个边带组成，两个边带携带相同的信息。但是载波本身不携带信息却占用了大部分的发射功率，使得这种方式的功

率利用率较低。

提高传输效率的方法就是采用 DSB-SC 双边带抑制载波调制技术。该技术消除了不携带信息的载波分量,把全部功率用于携带边带信息,从而大大提高了功率效率。但是接收端必须和发送端同频同相的本地载波同步解调,这就大大增加了系统的复杂性。更进一步发展的 SSB(单边带)调制,是在双边带的基础上只保留一个边带,既节省了一半的传输带宽,又节约了发射功率。对带宽资源紧张的电力线信道来说,SSB 技术就显得非常珍贵。远距离话音通信、窄带数据传输中用得很多,能有效地规避频带内的窄带干扰,大大提高通信链路的可靠性。

(二) 频率调制与相位调制

频率调制和相位调制统称为角度调制,都属于非线性调制。与幅度调制不同的是,它们是用载波的频率或相位来传递信息,载波的幅度保持不变。由于包络恒定,在非线性放大器中所受失真影响小,特别适合于对功率放大器效率要求较高的电力微波通信系统。频率调制把基带信号的幅度变化转变成载波的频率偏移,它的明显优点就是抗噪声能力强。增大调频指数,用更宽的传输带宽换得解调后信噪比大幅提高,这对信噪比普遍偏低的电力线环境来说非常关键。

相位调制是用基带信号直接控制载波的瞬时相位。虽然在模拟通信时代,它主要被看作是频率调制的过渡形式或者用于特殊用途,但是它的基本原理却是现代数字调制技术的重要基础。接收端一般用鉴频器或者鉴相器进行解调,对信道中幅度衰落的影响有较好的抵抗能力。信道中若存在脉冲干扰时,由于干扰主要表现为大幅尖峰,限幅器很容易将这些幅度变化切除掉,并且不破坏寄存在频率或者相位中的有用信息。因此角度调制对电力开关操作产生的瞬态脉冲干扰有很强的抵抗力,经常被用作关键保护信号的传输链路。

(三) 模拟调制的性能比较

选择电力通信系统调制方式的时候要综合考虑带宽效率、功率效率和设备复杂度这三个主要因素。各类模拟调制方式在这几项指标上表现出截然不同的特点,因此适用的业务也不同。

模拟调制技术特性比较

特性	标准幅度调制	双边带抑制载波	单边带调制	频率调制	相位调制
功率效率	低 (载波消耗大部分功率)	高 (全部用于信息)	高 (全部用于信息)	恒定包络 (效率高)	恒定包络 (效率高)
带宽利用率	2 倍基带带宽	2 倍基带带宽	1 倍基带带宽 (最优)	数倍基带带宽 (宽带 FM)	数倍基带带宽 (与 FM 类似)
抗噪声能力	最差	较差	较好	最佳 (宽带 FM)	较好 (角度调制共性)
设备复杂度	最简单 (非相干解调)	较高 (需同步解调)	较高 (需同步解调)	中等	中等
典型应用场景	早期电力线载波	(较少单独使用)	远距离语音 , 窄带数据	电力微波通信	关键保护信号传输

从上表可见，不同模拟调制技术在性能上各有侧重，其选择应依据具体的通信需求和环境条件。

1. 抗噪声性能上，宽带频率调制最好，用带宽换取更高的信噪比，单边带调制次之，标准幅度调制最差。电力线噪声较大的频段中，调频方式通常可以获得比调幅方式更好的话音质量。

2. 频带利用率：单边带调制占有绝对优势，占用的传输带宽只是基带信号带宽，适合于频谱资源紧张的电力载波频段。相反地，宽带频率调制为了获得高的信噪比而占用数倍于基带带宽，是功率受限系统里最好的选择。

3. 设备复杂度：标准幅度调制非相干解调最简单，造价低。而抑制载波的双边带调制和单边带调制都需要复杂的同步电路，成本比较高。频率调制系统处于两者之间，但是随着集成电路技术的发展，其实现难度大大降低。

二、数字基带传输

(一) 常用数字基带信号码型

数字基带信号码型设计要考虑直流分量抑制、定时信息提取和频谱结构优化等各方面。最基本的单极性不归零码虽然实现简单，但是存在严重的直流分量，不能通过变压器耦合的交流信道；在连续传输“0”或“1”的时候，也不能有效地提取同步时钟。双极性码用正负电平表示二进制数据，在 0 和 1 等概率出现时没有直流分量，抗干扰性能好。

电力通信光传输设备接口中使用较多的是 CMI 码（传号反转码）。信息码

中用“1”交替编码为正负电平，用“0”固定编码为某方向的电平跳变。编码方式中没有直流分量，定时信息丰富，利于接收端恢复时钟。虽然它占用的传输带宽是原来信号的两倍，但是对于带宽资源充足的光纤链路来说，并不是主要瓶颈，它的传输稳定性才是最大的优点。

常用的码型有HDB3码(三阶高密度双极性码)。它的目的就是克服AMI码(传号交替反转码)由于出现长串的“0”而造成的定时提取困难的问题。HDB3码用破坏点来消除长串“0”，既保持了无直流分量的特点，又实现了较小的传输带宽。在早期电力载波机和PCM设备中，由于HDB3码频谱能量主要集中在低频段，带宽增益要求不高，所以成为接口标准的首选码型，很好地保证了变电站之间继电保护信号的可靠传输。

(二) 基带传输的码间串扰与奈奎斯特准则

实际的电力通信信道中，由于传输介质(双绞线、同轴电缆等)的带宽总是有限的，因此信号经过系统时不可能不产生波形失真。这样就使前后码元的波形在时间上变宽，相互重叠，造成码间串扰。当码间串扰达到一定程度的时候，在接收端做判断的时候很难分清当前码元是0还是1，造成误码率剧增，甚至造成通信中断。这就是数字基带传输速率提升遇到的物理极限。

为了消除码间串扰必须满足奈奎斯特第一准则。准则认为，如果传输系统的频域传输函数满足一定的对称性要求的话，则在接收端可以实现无码间干扰。理论上理想低通滤波器可以实现这一目的，可以达到最高的频带利用率，即每赫兹带宽传输2个比特。但是理想低通滤波器的冲激响应在时域上拖尾很长，不能在物理上实现，而且对定时误差非常敏感。

一般用升余弦滚降滤波器近似满足奈奎斯特准则。引入滚降系数之后，系统传输特性边缘变缓。虽然会稍微降低频带利用率，但是时域波形拖尾的快速衰减得到了保证。折中的设计大大减小了定时精度对于系统的影响，在电力环境抖动、漂移等复杂的条件下也能保证系统的稳定传输。

(三) 眼图与均衡技术

眼图是实验室和工程现场用来直观、有效地检测数字基带传输质量的方法。用示波器的余辉功能把随机信号序列按位周期重叠起来显示，图形酷似人眼。眼图的“眼睛”张开越大，信号质量就越好，码间串扰和噪声的影响就越小。眼图最好的时候，就是眼睛张得最大的地方，眼图的斜率表示系统对时延误差的敏感

程度。电力通信设备入网检测中必须进行眼图分析,眼图分析是评价设备抗干扰能力、信道适应能力的重要手段。

当信道特性恶化导致眼图闭合时,单纯依靠滤波器已不足以满足要求,此时便需要引入均衡技术。

1. 线性均衡器是最简单的均衡器,使用横向滤波器结构,用改变抽头系数的办法补偿信道的幅频、相频特性来校正畸变的脉冲。此法虽然简单有效,但是当信道存在深度衰落点时,在该频点上放大了噪声,降低了信噪比。

2. 判决反馈均衡器:它利用已经做出的判断来消除后向的码间串扰。由于反馈的是判决后的净信号,所以不会引入新的噪声。电力线载波这样频率选择性衰落比较严重的信道中,采用判决反馈均衡技术可以明显改善接收性能,保证恶劣信道环境下数据的完整性。

三、数字调制技术

(一) 幅度键控、频移键控与相移键控

最基本的二进制数字调制方式为幅度键控、频移键控和相移键控。二进制幅度键控用载波的存在与否来表示“1”和“0”,实现最简单,常用于成本非常敏感、速率要求不高、电力遥测系统中。但是因为其抗噪声能力差,判决门限随信道增益变化,所以在现代主干网中很少单独使用。

二进制频移键控用两个不同的频率来代表“0”和“1”。该调制方式具有恒定包络的特点,可以采用非线性功放,并且可以使用非相干解调,使得接收机的结构较为简单。低速电力线载波通信以及早期的无线数传电台都使用 2FSK,因为 2FSK 的稳健性很强。

二进制相移键控用载波相位的 0 度、180 度变化来携带信息。在所有的二进制调制方式中,2PSK 的抗噪声性能最好,相同误码率要求下需要的信噪比最小。由于接收端存在相位模糊的问题,工程上一般采用相对相移键控,即用前后码元的相位差来传递信息。虽然差分编码机制会降低一定的信噪比性能,但是它可以完全消除相位模糊,因此成为电力系统继电保护复用通道的主要调制方式之一。

(二) 正交幅度调制

由于智能电网对数据吞吐量的要求越来越高,单个参数的调制方式在带宽效率上已经趋于极限。正交幅度调制把输入的比特流分组映射到复平面上二维的星

座点，很好地利用了幅度和相位这两个参数。16 阶正交幅度调制每个符号可以携带 4 个比特的信息，星座图上就有 16 个离散的点。此种调制方式极大提高了频带的利用率，在有限的电力专用频谱资源下做高清视频监控、大容量用电信息采集数据传输变得可行。

但是 QAM 的代价是要求信道线性度和信噪比更高。星座点越多，星座点之间的欧氏距离就越小，系统对幅度、相位误差的容忍度就越低。电力无线专网 (LTE230 系统) 当实时检测到信道质量之后会根据情况改变调制阶数。当信道状况好时，系统就使用 64 阶或者更高阶的调制方式来提高速率；但是当检测到恶劣天气或者强干扰的时候，它会自动退回到低阶调制方式，以保证连接的稳定性。自适应机制很好地体现了现代电力通信网络智能化的特点。

（三）现代高阶调制技术

为了满足对极高传输速率的需求，现代电力通信网络已经普遍使用高阶调制技术以及多载波复用方式。正交频分复用技术虽然经常被看作一种复用技术，但它的本质是把高速数据串并变换后，调制到大量的正交子载波上，每个子载波一般采用高阶调制。该技术对于电力线信道所固有的多径效应、频率选择性衰落等具有很好的对抗作用。OFDM 技术在符号之间插入循环前缀后，可以有效地消除码间串扰，使原来复杂的单频点均衡简化成频域的“一键式”处理。

高压电力线宽带载波通信、新一代电力 5G 切片网络中，256 阶或者 1024 阶的超高阶调制技术已经步入实用化试验阶段。这些技术一般是把前向纠错编码和调制相结合，例如网格编码调制，可以在不增加带宽的情况下获得较大的编码增益。为了实现这么高的调制阶数，收发信机必须使用高精度的时钟同步技术、非线性预失真技术去消除功率放大器的非线性。虽然实现难度很大，但是它带来的频谱效率飞跃，给未来全景感知、实时互动的数字电网赋予了坚实的物理层通道支撑。随着芯片算力的提升，这些过去只存在于理论层面的高级波形技术，也正在逐步在变电站巡检机器人、分布式能源调控等实际场合里得到应用。

第三节 信道编码与纠错技术

一、信道编码基本原理

(一) 编码增益与冗余度

编码增益是度量信道编码性能好坏的指标。它直观地表明了相同的误码率要求下,使用编码技术比不编码时可以节省的信噪比。电力通信系统中编码增益越大,说明同样的发射功率可以覆盖的范围就越远,同样的传输距离所能容忍的背景噪声就越大。实现增益的基础就是引入冗余度,在原始信息位之外加上校验位。虽然这些额外的比特并不直接携带用户数据,但是它们却包含了数据位之间逻辑约束的关系,正是这种关系给接收端提供检错和纠错的依据。

冗余度的选择要传输效率和可靠性之间求得一个最佳点。冗余度过大,虽然可以提供很强的纠错能力,但是会导致有效数据的传输速率大大降低,造成频谱资源的浪费。在电力无线专网等带宽受限的场合,设计者常常根据信道的实时情况来灵活调节码率,也就是自适应地改变冗余度。信道质量较好时减少冗余提高吞吐量,信道变坏,比如遇到雷雨天气或者大型设备启停产生的脉冲干扰的时候,就增加冗余来保证连接的稳定。动态平衡机制,也就是现代高效编码方案设计的中心思想。

(二) 差错控制的基本方式: 检错重发与前向纠错

差错控制技术主要有两种: 检错重发和前向纠错。这两种技术在电力通信不同的业务中各有优势。检错重发机制即接收端只对收到的数据有无错误进行检测,发现错误就请发送端重新发送。设备计算量小,在信道质量好时传输效率高。电力用电信息采集系统等对实时性要求不高,但数据量大的业务中,检错重发被广泛使用。它可以以较低的成本保证电表数据的正确性,即使多次重传也不会对系统整体运行造成致命影响。

前向纠错机制却采用了完全不同的办法。发送端在发送数据的时候就加入了足够的冗余信息,使得接收端不仅可以发现错误,还可以对一定范围内的错误进行自动纠正,不需要反向信道请求重传。单向纠错能力对电力调度自动化、继电保护等业务来说十分重要。通信时延的确定性是首先要考虑的,重传造成的时延抖动是不能容忍的。尽管前向纠错会增大处理复杂度以及带宽消耗,但是它保证

数据流连续性及实时性的同时，在恶劣的信道环境里维持稳定的单向传输链路，因此前向纠错成为关键控制业务的主要选择。

（三）电力通信信道特性分析

电力通信信道具有很大的复杂性和特殊性，主要是由于电力线、变电站等环境不是为通信而设计的。电力线载波通信的信道阻抗由于负载变化很大，而且存在严重的频率选择性衰落。除了常见的高斯白噪声，还有电网开关动作、变频器工作产生的脉冲噪声和窄带干扰等。这些非高斯噪声具有突发性、幅度大的特点，很容易就将普通的通信信号淹没，造成连续的突发误码，这对传统的信道编码方案提出了严峻的挑战。

无线通信在变电站的环境中也遇到了严峻的考验。变电站内部金属结构很多，形成很多反射面，多径效应严重，信号传播中会出现深度衰落。高压设备产生的工频电磁场、开关动作时产生的瞬态电磁干扰都会使无线频段的噪声底噪变大。这时信道就不再平稳了，是快时变、强干扰的信道。因此电力系统所用的信道编码技术必须具有很强的抗突发错误的能力，单纯用来纠正随机错误的编码方法很难胜任。一般要结合交织技术，把突发错误分散成随机错误，才能在如此恶劣的物理环境下建立起可靠的数字通道。

二、常用纠错码

随着通信理论不断发展，纠错码也从最初的简单方法发展到代数构造、概率迭代译码。电力通信网络的各个层面都有不同的纠错码配合使用，共同构成多层次的差错控制系统。理解各种常用码型的原理和特性是提高电力通信链路性能的前提。

常见的纠错码及其特性可见下方的对比表。

常用纠错码特性对比表

码型	主要纠错能力	编码复杂度	译码复杂度	典型应用场景
汉明码	单比特随机错误检测与纠正	低	低	板级通信、简单遥测终端
BCH 码 (循环码)	多比特随机错误纠正	中	中	电力线载波帧头保护、存储系统
卷积码	随机错误纠正、连续数据流	中	中 (维特比译码)	电力无线专网、语音、流媒体视频
Turbo 码	接近香农极限、随机错误	高	高 (迭代译码)	卫星通信、应急通信、深空探测
LDPC 码	接近香农极限、随机错误、低误码平层	高	高(置信传播,可并行)	5G 电力切片、无线物联网、宽带载波
RS 码	突发错误纠正	中高	中高	光盘存储、二维码、电力线载波外码

(一) 线性分组码：汉明码、循环码

线性分组码是最早应用的纠错码，它是按严格的代数理论构造的。其中最基本的一种就是汉明码，它利用奇偶校验位的巧妙组合来确定单个比特错误的位置。虽然纠错能力较弱，但是编解码电路简单，处理时延小，仍被用于电力系统内部板级通信以及对可靠性要求不高、成本敏感的简单遥测终端中。接收端利用计算出的校正子可以很快判断数据块是否存在错误、定位错误，确定性的逻辑运算使汉明码成为学习纠错编码的基础。

循环码在此基础上又增加了循环移位的特点，编解码器可以利用移位寄存器快速完成。CRC 循环冗余校验大多数是用在电力通信协议帧结构完整性的检验上。它虽然主要用来检错，但是它的代数结构与具有纠错能力的 BCH 码有共同的渊源。BCH 码是循环码的一个子类，它具有很强的多比特纠错能力，适合用来纠正随机独立错误。在早期的电力线载波通信标准中，BCH 码经常被用来保护重要的控制帧头，这样即使在噪声干扰的情况下，接收端也能正确的识别出帧的开始以及帧的属性，从而为后面的数据解调做好铺垫。

(二) 卷积码及其译码算法

卷积码和分组码不一样，卷积码有“记忆”。输出码字同当前时刻输入的比特有关系，同前面一段时间内输入的比特也有关系。这种前后相关的特性，使卷积码处理连续数据流有优势。在电力无线专网中，卷积码因为良好的随机错误纠

正能力被大量使用。用状态转移图或者网格图来表示它的编码过程，可以清楚地表现信息序列在时间轴上的发展轨迹。非常适合传输语音、流式监控视频等对连续性有较高要求的电力业务数据。

卷积码的解码一般用维特比算法，它是一种最大似然准则下的动态规划算法。维特比算法在网格图中找一条与接收序列距离最小的路径，这条路径对应的输入序列就是最有可能的发送信息。尽管计算量随着约束长度呈指数增长，但是现代数字信号处理器已经能够轻松应对。在电力通信低信噪比的环境下，使用维特比译码可以充分利用信号能量，将误码率大幅度地减小。为了克服电力信道上常见的长串突发错误，通常把卷积码和交织技术结合起来使用，把长串错误打散成随机错误，从而充分发挥卷积码的纠错能力。

（三）Turbo 码与 LDPC 码

随着宽带通信时代到来的同时，Turbo 码和 LDPC 码由于能接近香农极限的性能而彻底地改变了高可靠通信的局面。Turbo 码通过并行级联两个分量码，在接收端用迭代译码结构实现。它用软判决信息在两个译码器之间反复传递和更新，逐渐逼近真实值。在电力应急通信车卫星链路或者远距离微波传输中，Turbo 码可以在信噪比较低的情况下维持链路同步，保证灾害现场高清视频以及大量感知数据可以顺利传送到指挥中心。

LDPC 码，即低密度奇偶校验码，用稀疏的校验矩阵以及图论置信传播算法，具有比 Turbo 码更好的错误平层性能和更强的并行处理能力。这就意味着当要求达到极低的误码率标准时，LDPC 码会更加稳定，也更适合采用硬件并行的方式去实现，进而达到极高的吞吐量。在最新的电力无线物联网以及 5G 电力切片应用当中，LDPC 码被选作数据信道的主要编码方式。它可以做到毫秒级的超低时延传输，而且数据是绝对可靠的，完全满足智能电网对精准控制和海量并发接入的双重需求。

第四节 多址接入技术

一、多址接入技术概述

（一）多址接入的基本概念

多址接入的主要目的就是解决多用户共享信道时信号区分的问题。无线通信环境中频谱资源是有限的，如果每个电力终端占用固定频段全天候通信，将会造成巨大的资源浪费。多址技术利用在频率、时间、码域或者空间等各个方面引入正交性或准正交性，把物理信道划分成若干逻辑信道供不同的用户使用。这样一种资源划分方式，使得接收端可以从混合信号中正确分离出期望的用户信号，并且可以有效地抑制其它用户的干扰。

多址接入设计对于电力通信场景来说也要考虑业务特性不同。配电自动化业务对时延要求很高，对可靠性要求很高，用电信息采集业务节点数量多，数据包小且具有突发性。因此选择恰当的多址方式不但是通信效率的问题，也是关系到电网控制指令能否准确下达的问题。基本的多址协议分为固定分配多址和随机分配多址。前者有频分、时分等，适合于业务量比较稳定的场合；后者适合于突发性比较强的业务。现代通信系统常常会把几种办法联合起来使用，这样可以应对电磁环境复杂多变、业务种类繁多的情况。

（二）频分多址

频分多址技术是通信史上最早出现，并且应用最广泛的多址技术。基本原理就是把整个可用频带划分成若干个互不重叠的子频带，每个子频带作为一个独立的通信信道，供一个用户独占使用。通话或者数据传输时，该用户独占此频段资源，其它用户不能使用。为了防止相邻信道信号频谱混叠产生邻道干扰，各个子频带之间必须留有一定的频率间隔，即保护频带。

这项技术的优点是实现简单，不需要复杂的定时同步系统，基站和终端的信号处理过程比较直观。由于每个用户独占频率，信道估计和均衡比较容易，通信过程连续，不需要复杂的缓存控制。早期电力无线专网建设时，频分方式被广泛用来做语音调度、低速数据传输等业务，它所具有的稳定连接特性给关键业务提供物理隔离。

但是该技术也有明显的不足，频谱利用率低，这是该技术最大的缺点，保护

频带的存在直接造成了频谱资源的浪费。网络中的用户数量增加,就需要开辟新的频段,系统的扩容受到可用总带宽的限制。电力物联网中的传感器节点有成千上万个,如果用频分方式分配的话需要的频谱资源将是天文数字,在实际应用中是不现实的。同时由于固定分配方式缺乏灵活性,即使某个用户处于静默状态,它所占用的频率资源也不能供其它用户使用,造成资源利用率低。

(三) 时分多址

时分多址技术把时间分成周期性的帧,每一帧又分成若干个时间片。每个用户被赋予一个固定的时隙序号,只能在指定的时隙内发送或接收信号,在其他的时隙内要么静默要么接收。在时间轴上对信号做正交分布,使多用户可以共享同一个频率,但轮流使用。接收端只需要根据时隙同步信息,在对应的时隙时间窗口内打开接收门限,就可以将不同的用户信号分开。

该技术可以大大提高频谱传输效率,因为所有用户都使用整个频段,因此不需要很多的保护频带。突发式传输方式适合于智能电表定时上报等非连续性数据业务。由于发射机不是连续工作的,有利于移动终端的功耗管理,同时可以方便地测量出周围基站的信号强度,从而实现平滑越区切换。

虽然时分技术提高了容量,但是它对全网的时间同步提出了非常严格的要求。如果终端和基站的时间不同步,就会造成传输数据包在时间上出现重叠,产生符号间干扰。因此系统必须采用复杂的同步机制以及保护间隔,才能容忍由于传输时延所造成的误差。由于终端和基站的距离各不相同,在广覆盖的电力无线网络中传输时延也不一样,这就需要系统具有精准的定时提前量调节能力,从而增加了系统的设计复杂度。

二、码分多址与正交频分多址

随着数字信号处理能力不断加强,利用扩频和多载波调制技术实现多址的方案也越来越受欢迎。该类技术并不仅仅是单纯的时间和频率的划分,在复杂的空间上用数学编码和正交变换完成资源复用,极大地提高了系统的抗干扰能力以及频谱效率。

(一) 码分多址原理与特点

码分多址技术根据扩频通信原理,给每一个用户分配一个唯一的、伪随机的扩频码序列。在发送端,用户数据信号与这个扩频码相运算,把信号的频谱扩展

到比原来信号带宽更大的范围内。在接收端，用相同的扩频码与接收到的宽带信号做相关运算，依靠码序列自相关性强、互相关性弱的特性，把期望信号还原成窄带信号，把其他用户信号还原成宽带噪声，实现信号分离。

这项技术最显著的特点就是所有的用户可以同时、同频地进行通信，即频率和时间都是完全共享的。因为信号扩展到了很宽的频带上，所以它的功率谱密度很低，甚至可能被噪声淹没，因此它具有很强的隐蔽性、抗截获能力。对于电力系统来说，这就意味着数据传输具有天然的物理层安全屏障，难以被外部的恶意侦听或者干扰。

同时由于扩频增益的存在，系统具有很强的抗窄带干扰能力、抗多径衰落能力。变电站的电磁环境比较复杂多变，脉冲噪声和多径反射都比较严重，码分技术可以有效地抑制这些干扰，保证通信链路的稳定。系统还具有软切换的功能，即终端在切换基站的时候先建立新的连接，再关闭原来的连接，这对维持电力应急通信车辆在移动过程中业务的连续性十分关键。

（二）正交频分多址原理与优势

正交频分多址技术是将正交频分复用和多址接入结合起来的一种技术。它把高速数据流进行串并转换，分解成多个正交子载波并行传送。和传统的频分技术不同，正交频分多址的子载波在频谱上重叠，但是它们之间满足正交性条件，接收端利用快速傅里叶变换可以无损地分离出各个子载波上的数据。从多址接入的角度来讲，系统把子载波和时间符号组成资源块，这些资源块成为分配给不同用户的最小调度单位。

该技术最大的优点就是频谱利用率高。因为子载波之间不需要保护间隔，所以频谱资源被最大程度地压缩利用。在频率选择性衰落信道中，系统根据信道质量信息，把用户调度到信道质量好的子载波上进行传输，从而获得频率分集增益和多用户分集增益。

正交频分多址技术还很灵活。系统可以根据电力业务需求，随时改变分配给各个终端的子载波数目以及调制编码方式。以视频监控这种大带宽业务分配较多的资源块，遥信这种小数据业务分配较少的资源块。其精细的资源调度颗粒度大幅度地提高了系统并发承载多业务的能力，因此成为第四、第五代移动通信技术的核心技术。

（三）CDMA 与 OFDMA 在电力无线通信中的应用

在电力无线通信系统的实际部署中，码分多址和正交频分多址两种技术并不是相互取代的关系，而是各自支撑着不同的发展阶段、不同的应用场景下的业务需求。

码分技术一直以来都是中国电力无线专网的支撑技术，在 230MHz 等低频段的专网建设中，有较好的表现。由于它具有很好的覆盖能力和抗干扰能力，被广泛地用于偏远地区的配电终端接入。在安全性要求非常高的场合，例如负荷控制指令下发电路中，码分扩频方式给安全余度提供重要的保障。即使信号受到多径效应的影响而使质量下降，利用接收机技术也能把分散的信号能量集中起来，保证控制指令能正确到达。

正交频分技术才是构成宽带电力无线专网的核心。伴随着智能电网向信息化、视频化方向发展，输电线路无人机巡检、变电站机器人巡检等业务产生了大量的高清视频、图像数据回传需求。正交频分技术由于具有高吞吐量、带宽分配灵活等特点，可以很好地支持这些大带宽业务。在基于 LTE 或者 5G 架构的电力专网当中，它完成了成千上万个智能电表的并发接入任务，凭借细致的资源调度算法，在保证关键业务低时延的同时，也没有忽视普通业务的传输速度。利用多天线技术，也可以改善无线信号在复杂的工业环境中所达到的深度以及传输速率。

第三章 电力通信传输技术

第一节 光纤通信技术

一、光纤通信基本原理

（一）光纤的导光原理与类型

光纤由纤芯、包层和涂覆层组成，它的导光原理是全反射。纤芯的折射率稍大于包层，当光线以大于临界角的角度射向纤芯和包层的界面时，就不可能折射出包层，而会被全部反射回纤芯内。这样就形成了连续的全反射，使光信号被限制在纤芯中，可以传输很远的距离。根据折射率分布的不同，光纤可以分为阶跃折射率光纤和渐变折射率光纤。阶跃光纤的纤芯折射率是均匀分布的，在界面处突变；而渐变光纤的折射率是从中心向外呈抛物线递减，可以充分利用自聚焦效应减小模间色散，提高传输带宽。

按照传输模式数量的不同，光纤还可以分为多模光纤和单模光纤。多模光纤的纤芯直径大，可以传输几百个光模式，但是各模式传播速度不一样，存在严重的模间色散，因此限制了传输距离和带宽，一般用在短距离局域网。单模光纤的纤芯直径很小，在给定的工作波长下只能传输基模，完全消除了模间色散，具有很宽的频带和很小的传输损耗，是电力通信骨干网首选的介质。在实际运用当中，为了适应不同的环境需求，电力特种光纤如光纤复合架空地线、全介质自承式光纤等被广泛应用。这些特种光纤将电力线路架设的特点结合在一起，既能起到地线或者支撑的作用，又能提供通信通道，表现出电力通信特有的物理层结构。

光纤的损耗特性、色散特性是决定传输质量好坏的两个主要参数。损耗主要是材料吸收、散射和弯曲辐射造成的，损耗的大小决定了中继距离的长短。目前石英光纤在 1550nm 波长处损耗很小，可以进行远距离通信。色散会使光脉冲在传输中展宽，产生码间干扰，从而限制系统传输速率。色散包括材料色散、波导色散、偏振模色散。高速率传输系统必须使用色散补偿技术或者用色散位移光纤、非零色散位移光纤等新型光纤来保证信号的完整性。

（二）光源与光检测器

光源是光纤通信系统中的核心部件,主要的功能就是把电信号转变为光信号。电力通信中常用的是发光二极管、半导体激光器。发光二极管通过半导体材料中载流子的自发辐射发光,结构简单、成本低、可靠性高,但是输出功率小、谱线宽、调制速率低,适用于短距离、低速率通信系统。半导体激光器是基于受激辐射,利用光学谐振腔实现光放大而产生的相干性好、谱线窄、方向性强、输出功率大的激光。

1. 半导体激光器具有阈值特性,只有当注入电流超过阈值电流时才会产生受激辐射而发出稳定的激光。随着温度的增加,阈值电流增大,输出功率变小。因此,在实际使用中,常常需要加上自动温度控制、自动功率控制电路,保证光源稳定工作。分布反馈激光器在有源区附近加入光栅结构,能够实现单纵模工作,适合高速、长距离的波分复用系统。

2. 光检测器处在接收端,它把微弱的光信号转变成电信号。其主要的性能指标有响应度、响应速度、暗电流。PIN 光电二极管是在 P 型和 N 型半导体之间加入一层本征半导体,使耗尽层变宽,从而提高量子效率和响应速度。它的工作电压低、电路简单,在各种速率的通信系统中都有应用。雪崩光电二极管利用雪崩倍增效应,在强电场的作用下使光生载流子碰撞电离,获得内部增益,大大提高探测灵敏度,尤其适合微弱信号的检测。

光检测器工作时产生的噪声有量子噪声、暗电流噪声和热噪声。噪声会使得系统信噪比变小,误码率增大。为了获得最佳的接收性能,除了选用高性能的检测器之外,接收机电路前置放大器的设计也十分重要,一般会采用高阻抗型或者跨阻抗型放大器来满足低噪声、宽带宽的要求。电力系统恶劣的电磁环境对光器件的封装、屏蔽设计有很高的要求,必须保证它有足够的抗干扰能力。

（三）光纤通信系统的基本组成

光纤通信系统是由光发射机、光纤线路、光接收机和中继器等设备组成的完整的链路。光发射机是将复用设备输出的电信号进行编码、调制后,驱动光源发出相应的光信号送入光纤的设备。调制方式有直接调制和外调制两种,直接调制通过改变注入电流来控制光源强度,简单经济,但是载流子密度变化会引起频率啁啾;外调制在光源输出恒定光功率的前提下,利用电光效应或者声光效应,在光波上加载调制信号,可以实现极高的调制速率和优良的光谱特性,是超高速长距离系统的标准配置。

光纤线路作为传输通道,除了光缆本身以外,还有光纤连接器、光衰减器、光隔离器等无源器件。连接器是光纤与设备、光纤与光纤之间的活动连接装置,要求插入损耗小、回波损耗大。光隔离器可以保证光只能按一个方向传播,从而避免反射光对光源的影响。因为光纤损耗,所以进行长距离传输的时候,光信号就会慢慢变弱。信号幅度小于接收灵敏度的时候,要加装中继器。传统的光电再生中继器要完成光电光转换,结构复杂,系统透明性受到限制。而掺铒光纤放大器的出现,给通信技术带来了革命性的变化,它可以对光信号进行直接放大,具有高增益、宽带宽、低噪声等优点,实现了全光中继,大大促进了多波长复用技术的发展。

光接收机的主要作用就是检测微弱的光信号,将其转换成电信号,再经过放大、整形、再生等处理,恢复出原始的数字信号。其核心部件是光检测器和判断电路。在时钟信号的控制下,均衡后的信号被判决电路采样判决,根据设定的阈值来判断码元是1还是0。为了对系统进行监控,接收机一般都具有告警和性能监视的功能,可以实时上报信号丢失、帧失步等故障信息。在电力通信专网中,为了保证业务的高可靠性,一般采用双路由或者环网保护方式,系统需要具备快速自动倒换的功能,在光缆中断或者设备出现故障的时候可以保证业务的连续性。

二、光网络与传输技术

(一) 同步数字体系与光传送网

同步数字体系就是对数字信号进行同步复用、传输和交换的一套标准化体制。彻底解决了准同步数字体系因为标准不统一、复用方式复杂等而存在的问题。同步数字体系采用统一的帧结构,把低速支路信号映射到固定位置的容器中,利用指针调整技术解决了网络中频率、相位偏差问题,实现了从高速信号中直接上下低速支路信号的功能,极大地简化了复用设备,使网络拓扑更加灵活,便于实现分插复用和数字交叉连接。其帧结构中包含很多开销字节,用作段层和通道层的运行、管理、维护,给网络赋予了强大的自愈能力和监控手段。

1. 同步数字体系给网络节点之间的接口规定了标准,使不同厂商的设备可以互相连接。基本模块信号是同步传送模块的第一级,速率为155.52兆比特每秒,更高级的模块信号是用字节间插复用的方式组成的,速率是四倍的递增。严格的同步复用结构保证了信号的时序关系,但是承载分组业务时带宽利用率不高。

2. 由于 IP 业务迅速发展, 因此诞生了光传输网。光传送网在光域上完成客户信号的封装、传输、复用、路由、监控, 它把同步数字体系的运行维护能力与波分复用的大容量传输结合起来。它使用光通道数据单元、光通道传送单元等层次结构来组织, 而且采用数字包封技术, 可以透明地传输以太网、存储区域网等各种客户信号, 不受信号格式和速率的限制。

常见光传送网信号封装格式

格式名称	主要用途	优点	缺点
GFP	透明承载各种客户信号	灵活、支持多业务	帧开销相对较大
LAPS	承载分组业务到 SDH	利用 SDH 网络资源	无法直接承载 IP 数据包
PPP	点对点通信链路	简单、广泛使用	不支持多点连接

3. 光传送网最突出的特点就是采用了前向纠错技术。通过在发送端增加冗余纠错码, 接收端用解码算法来检测和纠正错误, 可以大大减小线路误码率, 增大光传输距离, 并且对光信噪比的要求也就相对较低了。对长跨距的电力通信线路来说尤其重要。光传输网可以进行多级串联的监视, 能分段监控跨运营商或者跨管理域的网络性能, 给电力通信网精细化经营管理提供有力的工具。

(二) 波分复用技术

波分复用技术就是让不同的光信号在一条光纤上同时传输, 最大限度地使用光纤带宽。它把光纤的低损耗窗口分成若干个信道, 每一个信道传输一路独立的光信号。发送端用光合波器将不同波长的信号合在一起, 接收端用光分波器将它们分开。这项技术使得传输容量得到了成倍的提高, 并且具有较好的透明性, 各个波长通道可以独立地传输不同速率、不同格式的信号, 互不干扰, 就好像是在光纤里面建立起了许多个虚拟的光纤。

波分复用分为稀疏波分复用和密集波分复用。稀疏波分复用的波长间隔较大, 对光源和滤波器的要求不高, 成本低, 适合城域网边缘层。密集波分复用的波长间隔很小, 一般为 0.8 纳米或更小, 可以在一根光纤中复用几十甚至上百个波长, 是骨干网扩容的关键技术。为了实现长距离传输, 密集波分复用系统一般使用掺铒光纤放大器, 能对所有波长的信号一次性进行放大, 不需要对每个波长单独进行电中继。但是多波长信号在非线性介质中传播时, 会因为四波混频、受激布里渊散射等非线性效应产生信道间串扰和功率波动, 需要通过合理的色散管理、功率控制来抑制。

波分复用技术用在电力通信网络里，一方面可以有效解决光纤资源不足的问题，另一方面也可以实现多种保护机制。除线路保护外，可以实现光通道保护，即发送端并发双发，接收端选优接收或中间节点用光分插复用器上下波长，构造高生存性光环网。随着可重构光分插复用器的出现，波分复用网络由原来的点对点的静态链路变成了动态可配置的光联网，根据业务流量变化做波长连接的实时调整，极大提高了网络的灵活性和资源利用率。

（三）自动交换光网络技术

自动交换光网络是光网络智能化发展必然走向。它在传统传送网的基础上增加了控制平面，可以实现光连接动态建立和拆除。传统的光网络连接配置一般是通过人工方式在网管系统里做静态配置，耗时又低效，不能及时应对突然出现的业务需求或者网络故障。自动交换光网络依靠控制平面的信令协议、路由协议、链路管理协议来赋予网络节点智能感知、自动协商的能力，使得网络能够像电话网一样实现即时的带宽预订、按需带宽分配。

自动交换光网络的体系结构由传送平面、控制平面、管理平面三大部分组成。传送平面是光信号的物理传送和交换平台；管理平面是对网络资源和配置进行宏观管理的平面；控制平面是重要部分，它依靠邻居发现功能自动获取网络拓扑信息，依靠路由协议计算最佳路径，依靠信令协议驱动传送平面建立交叉连接。分布式的控制方式降低了对于某一个网管系统的过度依赖，提高了网络的抗毁性。网络发生故障的时候，控制平面能很快计算出恢复路径，建立新的连接，实现毫秒级的业务恢复，比人工调度快得多。

自动交换光网络支持不同的业务等级协议，给重要程度不一样的业务提供不同的保护、恢复方案。例如对继电保护等重要业务采用 1+1 备份，对一般数据业务采用恢复时间较长但是资源占用较少的重路由恢复。不同的服务等级对应不同的服务能力，可以为各种电网业务提供经济高效的承载方式。自动交换光网络具有软永久连接、交换连接两种模式，在保持传统网管配置的确定性的同时又具有动态信令配置的灵活性，为电力通信网向全光网平滑过渡提供了一条技术途径，符合智能电网对高可靠、大带宽、低时延通信的严格要求。

第二节 无线通信技术

一、无线通信基本原理

(一) 无线电波传播特性

无线电波在空间中传播并不是直线运动，会受到周围环境的影响。当电磁波从发射源发出以后，就会碰到扩散、反射、折射、绕射和散射等种种物理现象。在理想的自由空间中，电波的能量随着距离的增加而按平方反比规律下降，这种基本的损耗叫做路径损耗。但是实际电力通信环境中的电波传播路径比自由空间要复杂得多，不论是城市里一栋栋的配电房，还是山丘起伏间分布的变电站，电波的传播途径都比自由空间要复杂得多。建筑物、植被、地表起伏等都会阻挡电波，使信号强度急剧下降，这就是所谓的阴影效应。

电波的波长直接决定了它绕过障碍物的能力，波长越长，绕射能力就越强，覆盖范围也就越广。低频段的信号穿透墙壁，覆盖地下室方面表现良好，适合安装在深处的电表或者开关柜的通信上。高频信号虽然可以携带更多的信息，提供更宽带宽，但是绕射能力较差，容易受到树木、建筑等的阻挡。除了宏观上由于路径损耗和阴影效应造成的影响之外，在传播过程中还会由于多径效应产生复杂的干扰。

发射信号到达接收端不同的路径，传输时间和相位都不一样。各种不同的反射波、散射波在接收天线处集中在一起，有的会互相加强信号，有的则互相抵消，造成信号的深度衰减。信号强度的剧烈波动，在很短的时间段内，短时间内频繁出现，是无线通信所要面对的一个巨大难题。为了减小这些传播特性带来的不利影响，在现代通信系统的设计过程中就必须充分考虑频段的选取、链路预算以及传播模型的校正等工作，保证在复杂的物理环境中通信链路是稳定的可靠的。

(二) 无线信道的衰落与抗衰落技术

无线信道是通信系统中难以控制的环节之一，信道质量的好坏直接影响通信的可靠性。信号在传输过程中遇到的衰落一般分为大尺度衰落和小尺度衰落。大尺度衰落主要是由于路径损耗和阴影效应所造成的，大尺度衰落所表现的是信号强度随着距离增大而降低的宏观趋势。小尺度衰落是由多径传播、多普勒频移引起的，表现为接收信号的幅度、相位在很短的时间、很短的距离内发生急剧的变

化。当移动台处于驻波场内时,信号幅度会服从瑞利分布或者莱斯分布,由于信道条件变化很快,很容易导致误码。

为了对抗这些衰落,改善通信质量,在工程中采用了各种抗衰落技术。分集技术就是其中一种最有效的手段,它的基本思想就是让接收端接收到多路相互独立衰落的信号,再进行合并,这样就能大大降低深衰落出现的概率。常用的分集方式有空间分集、频率分集、时间分集、极化分集。双天线接收就是电力无线终端中常见的空间分集应用,即在空间上隔开一定距离的两个天线来接收信号,只要其中一路信号质量好,系统就能够正常解调。

信道均衡技术主要是用来消除多径效应造成码间干扰。在接收端插入一个频率特性与信道相反的滤波器,就可以补偿信道的畸变,恢复原来的信号波形。数字信号处理能力提高之后,自适应均衡器可以实时跟踪信道变化,不断调整系数,在高速移动或者环境较差的情况下也能保持较好的性能。信道编码技术就是在发送数据时加上一些冗余的校验位或者纠错位,这样即使接收方出现一定的误码率,也可以通过这些冗余信息进行错误纠正,从而得到正确的数据。交织技术可以将突发连续的错误分散开来,再用纠错编码配合使用,从而提高系统抗干扰能力。

(三) 天线基本原理与类型

天线是无线通信系统里将射频信号与电磁波互相转换的关键器件。发射天线把发射机输出的高频电流转换成向空间辐射的电磁波,接收天线把截获的电磁波能量转换成高频电流送到接收机。天线性能的好坏直接关系到通信距离及通信质量,主要的技术参数有增益、方向性图、极化方式、输入阻抗、工作带宽等。增益体现的是天线把能量集中辐射到某个方向上的能力,增益越大,通信距离就越远,不过波束宽度越小,对准精度的要求也就越高。

在电力通信中,根据具体应用场景的不同,各类天线发挥着各自独特的优势,详情可见下表:

电力通信常用天线类型概览表

天线类型	特点	主要应用场景
全向天线	水平面均匀辐射，垂直面有一定波束宽度	点对多点通信中心站，全方位覆盖（如杆塔集中器接收四面八方终端信号）
定向天线	能量集中辐射到特定方向或窄扇区	点对点通信链路，扇区覆盖（如电力线路巡检、远距离变电站数据回传使用抛物面或对数周期天线）
智能天线	天线阵列与数字信号处理结合，形成多波束，自动跟踪用户，抑制干扰	新型电力无线专网（如波束赋形技术），大幅提高频谱利用率，增加系统容量，降低邻区干扰，尤其适用于密集物联网节点

新型电力无线专网中，智能天线技术（波束赋形）被广泛使用，可以大大提高频谱利用率，增加系统容量，减少邻区干扰，对密集布置的电力物联网节点来说尤为重要。

二、电力无线专网技术

（一）230MHz 数传电台

230MHz 频段是国家无线电管理委员会为电力、水利等行业遥测、遥控、数据传输而划定的专用频率。该频段上的数传电台是电力行业最早使用，应用最广的一种无线通信方式。传统的 230MHz 数传电台大多使用频分复用的方法，以 25kHz 窄带传输低速数据。其技术体制比较简单，一般采用 MSK 或者 GMSK 等恒包络调制方式，设备成本低、抗干扰能力强、绕射性能好、覆盖距离远。

由于工作频率低，230MHz 信号对地形、建筑物的穿透能力强，适合在地形复杂偏远地区或者建筑密集的城市配电网中使用。早期的负荷管理系统和配电自动化系统中，数传电台起到了举足轻重的作用，成功地实现了对专变用户的远程抄表和负荷控制。但是由于带宽很小，传输速率一般只有几千比特每秒，不能承载图像、视频或者高频次大数据量的采集业务。传统电台大多采用轮询的方式，因此系统的容量较小，实时性也较差。但是，在那些带宽要求不高但覆盖面大、建设成本低的应用场景中，230MHz 数传电台还在使用，而且正朝着采用更高效的调制解调技术的窄带高速化方向发展。

（二）LTE-G/LTE-230 电力专网

为了克服传统的 230MHz 技术带宽不足、时延大、容量小的问题，电力行业引入了 4G LTE 技术，利用 230MHz 离散频谱的特点，研发出了 LTE-G（又称为

LTE-230) 电力无线专网系统。这并不只是 LTE 系统的简单移植到 230MHz 频段, 而是在电力行业特殊的频谱环境下做出的定制。由于 230MHz 频段是离散的窄带频谱资源, 不像公网那样有连续的宽带频谱, 所以 LTE-230 采用了载波聚合技术, 把多个离散的 25kHz 窄带频点聚合起来, 形成一个等效的宽带信道, 从而大大提高了数据传输速率。

LTE230 系统使用正交频分复用技术, 可以对抗频率选择性衰落, 提高频谱利用率。

1. 物理层优化, 由于配电自动化三遥业务需要的时延小于一毫秒, 所以在帧结构、信令过程等方面做了一些减少不必要的消耗的工作, 使得端到端时延变小。

2. 深度覆盖、大容量, 230MHz 频段有优良的传播特性, 单个基站的覆盖半径可达数公里到几十公里, 大大降低了基站的部署数量。同时使用自适应调制编码和多天线技术, 系统容量可以呈指数增长, 可以同时接入几千个智能终端。

3. 安全可控 LTE-230 为定制化深度的专网, 采用双向鉴权、空口加密等安全手段, 保证数据不出专网, 完全由电力企业掌控, 从根本上杜绝了公网遭受外部攻击、数据泄露的风险。

(三) WiMAX 等宽带无线接入技术

WiMAX (全球微波互联接入) 是以 IEEE802.16 标准为基础设计的宽带无线城域网技术。WiMAX 曾是电力通信中解决“最后一公里”接入问题有力竞争者。以正交频分复用和正交频分多址接入为主要技术, 可实现非视距传输, 在宽频段上提供几十兆比特每秒的数据吞吐量。WiMAX 网络结构简单灵活, 支持点对点、点到多点、网状网等多种组网方式, 部署灵活性高。

在电力应急通信、变电站视频监控等场合, WiMAX 技术就表现出它的价值。采用 WiMAX 基站可以快速在事故现场建立宽带通信链路, 将现场高清视频、采集数据实时传回指挥中心。其强大的服务质量机制可以给不同的业务流提供不同的服务保证, 保证语音、视频等实时业务的流畅传输。虽然 WiMAX 技术的发展受到了蜂窝移动通讯技术如 LTE 的激烈竞争, 产业链趋于萎缩, 但是专网频段 (1.8GHz 或 5.8GHz 免执照频段) 中, 采用 WiMAX 或者其衍生技术建立宽带电力微波接入网, 仍可以成为光纤难以覆盖地区的一种有效的补充方式。此类技术经常被用在变电站之间的中继链路备份上, 也可以作为通信接入网汇聚层的一种无线回传方式, 成功解决了有线资源匮乏地区宽带通信的问题。

三、公网无线通信技术

（一）4G/5G 技术在电网中的应用

由于第四代移动通信技术已经有了成熟的产业链和广泛的覆盖面，所以已经成为电力公网应用的主力军。它承载着大量的用电信息采集业务，在电动汽车充电桩运营、分布式光伏监控等各方面起着重要的作用。4G 网络的高带宽使以前难以实现的移动作业应用成为可能，电力营销移动作业终端、输电线路无人机巡检图像回传等都得以实现，大大提高了一线作业的效率和信息化水平。

第五代移动通信技术商用以后，给电力通信带来革命性的机遇。5G 技术有超高速率、超低时延高可靠、海量机器类通信这三大特点，而智能电网的三大典型场景，大带宽视频巡检、精准负荷控制 / 配电自动化、海量物联采集，也正与之契合。

就控制类业务而言，5G 空口授时精度加上毫秒级的端到端时延，使得利用无线网络承载配网差动保护变得可行。差动保护对通信时延和抖动的容忍度非常小，过去只能依靠光纤。5G 超低时延高可靠切片技术出现以后，配网自动化创建费用降低。

5G 网络切片可以把一个物理网络分割成多个逻辑上隔离、虚拟化的子网络。电力行业可以根据自身业务需要创建自己的专属业务切片，以达到硬件隔离、独占资源等目的，从根源上杜绝公网应用的安全隐患以及资源被抢占的问题。此种公网专用模式既能得到公网的广覆盖优势，又能达到近似专网的性能保证。

（二）NB-IoT/eMTC 等物联网技术

伴随着万物互联时代到来，电力系统所要连接的终端数目呈指数级增长。许多终端分布在地下室、管井等信号难以到达的地方，大部分采用电池供电，功耗十分敏感。传统的 2G、3G、4G 网络无法同时满足广覆盖、低功耗、低成本这三个要求。窄带物联网、增强型机器类型通信都是为物联网设计的蜂窝通信技术，一经推出就迅速在电力行业得到广泛应用。

窄带物联网使用的是蜂窝网络技术，其占用的带宽是 180kHz，可以直接建立于现有的 GSM、UMTS 或 LTE 网络上，降低安装费用，实现平滑升级。它有四个明显的优势，一是覆盖范围广，窄带物联网提供了改进的室内覆盖，在相同的频段下，网络增益比现有的网络高 20dB，覆盖面积可以增大 100 倍，可以穿

透井盖、厚墙等障碍物，很好地解决了智能电表在恶劣环境下深覆盖的问题；二是支持海量连接，一个窄带物联网扇区可以支持 10 万个连接，非常适合高密度的电力感知节点接入；三是更省电，窄带物联网终端模块的待机时间可达 10 年，解决了难以供电区域设备的维护问题；四是模块价格低，有利于大范围推广和应用。增强型机器类型通信技术的速率比窄带物联网高，移动性更好，支持语音，因此更适合于需要位置移动或者一定数据吞吐量的电力物联网应用，例如移动式电力物资追踪或者带有语音交互功能的智能终端。

（三）公网融合通信模式

电网业务的多样性和变化性，使得单一的专网或者公网都不能一劳永逸地解决所有的问题。专网在核心区域、关键控制业务上起着不可替代的作用，但是在广大农村地区或者非关键业务上，建设全覆盖专网的投入产出比过低。公网虽然覆盖范围广、成本低，但是在极端灾害下容易断电，在网络拥塞的时候业务稳定性容易受到影响。因此，建立公网互补、协同工作的融合通信方式成为必然。

公网融合不是简单的物理叠加，它牵涉到网络架构设计、终端模组研发、业务智能调度等许多复杂的方面。终端侧双模或者多模通信模块可以支持专网频段和公网频段，可以智能感知网络信号质量。当专网信号好时，终端会锁定专网进行关键控制指令的传输，保证安全和实时性；当专网出现盲区或者发生拥塞的时候，终端可以无缝切换到公网链路，进行非关键数据的传输或者作为备份通道。在网络侧，可以使用云管平台对公网连接和专网连接进行统一管理、统一认证、统一调度。虚拟专用拨号网络、专用接入点名称技术应用，在公网中建立了一个安全的专用数据隧道，把公网流量安全地引入到企业内网中。该种融合模式极大地提高了电力通信网的鲁棒性、经济性，并且成功实现了关键业务用专网、普适业务用公网、应急场景双备份的科学组网模式。

第三节 电力线载波通信

一、电力线载波通信原理

（一）电力线信道特性分析

电力线不是为通信而设计的，它的信道环境非常复杂且时变性很强，给载波通信带来了严峻的挑战。输入阻抗剧烈波动就是它的主要特点之一。电力线上连接的负载种类繁多且随机投切，使得线路阻抗在不同的时间、不同的地方存在巨大的差别。阻抗失配会引起信号反射、多径效应，还会造成发射机功率传输效率下降。多径传播会带来信号的频率选择性的衰减，造成某一特定频率的分量在经过传输之后严重衰减或者完全消失，从而极大影响通信品质。为了克服这个问题，一般会使用具有抗多径干扰能力的调制解调技术，比如正交频分复用技术，利用多个子载波并行传输数据，把频率选择性衰落的影响分散开来。

噪声干扰是电力线信道所遇到的又一难题。电力线上的噪声来源很多，既有电网本身产生的工频谐波噪声，又有各种用电设备产生的脉冲噪声和背景噪声。背景噪声的功率谱密度比较小，并且随着频率慢慢改变，脉冲噪声具有突然出现、幅度大、持续时间短等特点。大功率变频设备、开关电源、接触器通断等都会在电力线上产生强烈的脉冲干扰。非高斯分布的噪声很容易造成突发性误码，单纯提高发射功率是行不通的。这时，需要用到前向纠错编码、交织技术以及自动重传请求机制，从编码层面提高系统抗噪声能力，保证恶劣噪声环境下数据可以完整无缺地传输。

信号的衰减特性也不能忽略，高频载波信号在电力线上传输，距离越远衰减就越严重。衰减同传输距离有关，还同信号频率密切相关。频率越高，线路的趋肤效应就越明显，信号衰减也越剧烈。电力线路的分支结构、接头接触电阻、绝缘老化等都会增加信号损耗。长距离传输时要合理布置中继节点，对信号进行放大再生，使接收端信噪比达到解调的要求。不同的电压等级的电力线其衰减特性也存在着差别，低压配电网由于分支多，负载复杂，因此其信号衰减要比中压配电网严重得多。

（二）耦合与滤波技术

耦合电路是连接通信设备和高压电力线路的接口，主要作用是将高频载波信

号耦合到电力线中,并将电力线上的工频高压与通信设备隔离。电容耦合是最常用的一种方法,利用高压电容器对工频电流高阻抗、对高频信号低阻抗的特性来实现信号通路和强电隔离。耦合电容的选择要满足承受电力线路额定电压和雷电流冲击的能力,高频下效果好,通过载波信号时损耗小。一般还会串联一个结合滤波器,与耦合电容一起构成带通滤波器,进一步滤除工频电流及谐波,只允许特定频率的载波信号通过,提高信号注入效率,保护后端低压电路。

滤波技术在电力线载波通信里属于净化频谱、压制干扰的重要部分。阻波器是串接在电力线路两端的装置,它对高频载波信号呈高阻抗,阻止载波信号泄露到非通信区或流向变压器等低阻抗设备,把信号能量限制在指定的通信线路范围内。阻波器一般由电感线圈及调谐元件组成,其谐振频率精确调节后,在载波频段呈现极高的阻抗,在工频下阻抗很小,不影响电能的输送。它具有通低频、阻高频的特点,可以减小载波信号的无谓损耗,增大通信距离,提高可靠性。

除了线路侧的阻波器以外,接收机前端的滤波电路也不能少。信号进入解调芯片之前,先用模拟前端滤波器去掉带外噪声和干扰信号。由于电力线噪声的频带很宽,因此设计高性能的带通滤波器对提高系统信噪比来说非常重要。现代的载波通信系统大多采用有源滤波器和无源滤波器相结合的方式,既可达到滤波精度的要求,又可以满足宽动态范围的目的。对于宽带载波通信,占用的频带较宽,因此滤波器的设计也更加复杂,除了考虑通带平坦度外,还要考虑群时延平坦度,防止信号波形发生畸变。良好的耦合和滤波设计,为建立稳定的电力线载波通信链路物理连接打下基础。

（三）电力线载波通信系统构成

电力线载波通信系统是一个包含调制解调、信号耦合、网络控制、应用接口等众多功能的系统。它的核心部件就是载波调制解调模块,把终端设备的数据流转换成适合在电力线上传输的高频模拟信号。发送端数字信号经过编码、交织、映射处理后,由数模转换器变成模拟波形,再经功率放大器放大到足够大的电平,驱动耦合电路。在接收端,微弱的载波信号经过耦合电路提取、低噪声放大、滤波、模数转换后,进入数字信号处理器进行解调、解码,最后得到原始数据。现代载波模块大部分采用了集成度很高的片上系统结构,集成了高性能的微处理器和专用的数字信号处理单元,可以实时适应信道的变化,根据信道的好坏,实时的调整调制方式和编码速率。

1. 主站与从站设备

通信网络一般是以主站设备为中心的星型结构。主站设备一般设置在配电变压器低压侧或变电站内，是整个子网的控制中心，负责建立和维护网络、选择路由、同上层网络相连。从站设备分布在各个用户端或者监测点，例如智能电表、采集终端等，响应主站的指令并上传数据。主站需要有较强的处理能力、存储空间，可以同时接入大量的从站节点，对数据进行汇聚。

2. 中继设备

由于电力线信道衰减，长距离通信要采用中继器进行中继。中继器接收源节点发出的微弱信号，经过解调、纠错、重新编码、调制后，以一定的功率转发给下一个节点。中继方式有物理层中继和链路层中继两种。前者只是放大整形信号，延迟小，但是噪声也会被放大；后者是对整个数据包进行处理，可靠性高，但是延迟大。智能组网技术让网络里的普通节点也能充当中继，依靠自动路由发现算法来创建多跳通信路径，这样就增进了网络的覆盖范围。

3. 网络管理系统

为了保证通信系统能够稳定地运行，需要有一套完善的管理系统。此系统针对网络中的各个节点的工作状态，信道情况，通信流量等参数实施监视，给用户提供配置管理，故障诊断以及性能剖析等服务。运维人员通过图形化界面就能清楚看到网络拓扑结构，很快找到通信故障点。当信道拥塞或者受到严重干扰的时候，网管系统能远程调节通信参数，改变工作频段、减少通信速率等来保证最基本的通信联系。

二、中压与低压载波技术

（一）中压配电网载波

中压配电网载波通信主要应用于 10kV 或者 35kV 的架空线或者电缆线路，是配电自动化系统中的一种重要通信方式。该层次的通信环境比低压侧更好，负载变化小，噪声水平低，但是对通信的可靠性、实时性要求很高。中压载波系统一般担负着传输开关状态信息、故障指示信息、遥控指令的任务，通信中断或者延时都会影响配电网的故障隔离和恢复速度。中压线路一般呈辐射状或者环状，很长，信号在传输过程中要经过很多分段开关、联络开关，所以对载波设备的跨距传输能力以及穿透力要求很高。

架空线路和地下电缆的信道特性相差很大,中压载波技术要适合于两种不同的传输介质。架空线路的波阻抗大,信号衰减小,但是容易受到雷电、无线电干扰、树木触碰等的影响。电缆线路的波阻抗小、分布电容大,高频信号在电缆线路中衰减比在架空线上要大得多,而且接头反射复杂。电缆线路一般用较低的载波频段,或者利用电缆屏蔽层做回流通道来减小衰减。混合线路中阻抗不匹配点处反射大,设计时应做阻抗匹配计算,在节点处加阻抗匹配器消除驻波,保证信号能量的传输。

为了提高中压载波的可靠性,目前大多数系统都采用了自适应频率捷变、多载波技术。当某一工作频点受到外界强干扰的时候,系统可以自动检测并且迅速跳转到干净的频点进行通信。多载波技术把数据分散到不同的子信道里进行传输,即使某一个子信道受到了干扰,也能用纠错编码恢复原来的数据。由于中压设备安装在高压带电体旁侧,中压设备的绝缘以及电磁兼容性设计十分重要。耦合装置需要满足严格的耐压标准,通信终端需要有很强的抗电磁干扰能力,以防止高压开关动作时产生的强电磁脉冲导致设备死机或者损坏。中压载波设备一般用感应式耦合的方式安装,不需要断开一次线路,给工程实施和维护带来了极大的便利。

(二) 低压用户集抄载波

低压电力线载波通信主要工作在 380V/220V 电压等级的用户侧,是实现智能电表远程集中抄表的主要技术。低压电网的拓扑结构很繁杂,有树状、星状和混合型,而且会因用户接入或者退出而发生变化。每个台区的变压器下面接了数百个计量节点,信号传输路径交织错综。最难的是,在低压电网里有很多家用电器、工业设备,它们既是负载又是噪声源。变频空调、LED 驱动电源、电动汽车充电桩等设备在工作的时候会大量产生高次谐波和脉冲干扰,低压电力线已经成为公认的最恶劣的通信信道。

为了解决低压信道复杂性的问题,自动路由组网技术成为低压载波系统必需的技术。由于节点数量多且信道状态不稳定,点对点直接通信不能覆盖所有的用户。通过构造动态的网状网络,每一个电表节点既是终端也是中继器。集中器发出组网指令,各节点通过接收信号强度和链路质量自动选取最佳路径,从而形成多级中继结构。当一条路径被阻断中断的时候,网络会马上启动路由恢复程序,另辟蹊径找到新路保证数据能够顺利到达目的地。抄表系统自愈合之后抄表的成

功率达到了 100%，可以在低压台区复杂的环境下实现全覆盖。

随着智能用电业务的拓展，低压载波技术也由原来的单向抄表发展为现在的双向互动。系统除了上传电量数据外还要下发费率参数、控制指令、实时电价信息。这就使载波通信的带宽与时延要求更高了。为了克服最后一公里的通信瓶颈，相位识别、台区识别等技术也被广泛应用。利用载波信号在不同相线上的过零点不同来判断电表所处的相别，为三相负荷平衡调节提供依据。在载波信号里嵌入特设的台区特征码，能很好地避免相邻台区产生串扰、信号误读的现象，很好地解决了高密度住宅区存在的台区档案混乱问题，从而提高了精细化管理的水平。

（三）宽带与窄带电力线载波技术

窄带电力线载波技术就是工作在 3kHz 到 500kHz 之间的一种载波通信技术。频率低，信号可以在电力线上传输比较远的距离，对于线路阻抗的变化不敏感，穿透性好。早期的窄带技术大多采用频移键控、相移键控等单载波调制方式，电路结构简单、成本低、功耗极低。其数据传输速率一般为几百 bps 到几千 bps，对于抄表、路灯控制等数据量小、实时性要求不高的场合已经足够。随着技术的发展，基于正交频分复用的窄带高速技术逐渐成为主流，它既保持了窄带传输距离的优势，又可以利用多载波并行传输大幅度提高频谱利用率、抗干扰能力，速率可以达到几十 kbps，能够较好地支持费控、事件上报等业务。

宽带电力线载波技术所处的工作频段为 2MHz-30MHz 或者更高，其可用带宽明显比窄带技术要宽。宽带载波利用高频段信道特性相对平坦、背景噪声小的特点，可达到数 Mbps 到数百 Mbps 的物理层传输速率。因此电力线不仅可以传输控制指令，还可以传输语音、图像、视频流等多媒体业务。宽带载波可以把室内电力线变成高速局域网，连接计算机、智能电视、网络存储设备，不需要重新布线就可以实现全屋网络覆盖。宽带载波给工业互联网场景下的设备状态监测、远程固件升级等大数据传送提供强有力的支撑。

宽带与窄带电力线载波技术特点对比表

特性	宽带电力线载波技术	窄带电力线载波技术
工作频率	2MHz ~ 30MHz 甚至更高	3kHz ~ 500kHz
数据传输速率	数 Mbps ~ 数百 Mbps	数百 bps ~ 几十 kbps
传输距离	几百米（受线路分支、阻抗影响大）	远距离、大覆盖
抗衰减能力	较弱（高频衰减快）	较强
系统功耗与成本	较高（需强运算能力处理器）	较低
适用业务类型	多媒体业务（语音、视频），大数据传输，高速局域网	低速控制网络（抄表、路灯控制、费控、事件上报）
中继节点需求	更多	较少

1. 技术特点对比

从上表可知，宽带技术速率高，但是高频信号在电力线上的衰减很快，传输距离一般只有几百米，受线路分支、阻抗失配影响较大，需要更多的中继节点。窄带技术速率低，但是传输距离远、覆盖面积大、抗衰减能力强，适合长距离、大覆盖的低速控制网络。宽带系统一般要求处理器运算能力强，耗能大，价格高；窄带系统经济实惠，便于大规模使用。

2. 应用场景互补

宽带和窄带技术并不是对立的，它们在实际的电力通信网建设中是互相补充的。高频次、大数据量的台区，例如需要实时采集电压电流波形做电能质量分析的场合，最适宜使用宽带载波。在广大农村地区或者线路老化的旧城区，窄带载波由于具有稳定的传输性能和低成本的特点而仍占主导地位。双模通信技术正在兴起，即在一个通信模块中同时集成了宽带和窄带（或者射频无线）两种模式，根据信道环境自动切换，既能保证在恶劣环境下的基本通信能力，又能在条件允许的时候提供高速数据服务。

3. 标准化与互操作性

随着技术的发展，宽带和窄带载波都有了相应的国际和国家标准。窄带领域有 PRIME、G3-PLC 等国际标准以及国内的电力行业标准，对物理层和数据链路层的协议细节作出规定。宽带领域有 HomePlug 系列、G.hn 等标准。统一标准打破了各个厂家设备之间的壁垒，实现了互相勾通，从而大大促进了产业链的发展。物联网技术深入发展时，电力线载波会和无线通信、光纤通信一起发展，共同形成泛在、异构、高效的能源互联网通信架构。

第四节 卫星通信技术

一、卫星通信系统概述

(一) 卫星通信系统的组成与特点

卫星通信系统由空间分段、地面分段、用户分段三大部分构成。空间分段即通信卫星，在系统中充当空中中继站的角色，主要由卫星平台和有效载荷两部分组成。当中有效载荷指的是转发器加天线系统，它直接影响到卫星的通信能力及其所能覆盖的区域。地面分段一般是指卫星测控站、主站，对卫星进行跟踪、遥测、指令控制、网络资源调度管理，保证卫星始终处于正确的轨道位置，良好的工作状态。用户分段指的是分布在全国各地的各种地球站，包括固定站、车载站、便携站、手持终端等，它们是电力业务数据接入卫星网络的直接入口。

卫星通信技术覆盖范围广、通信距离远，并且通信成本与距离无关。理论上的一颗地球静止轨道卫星可以覆盖地球表面大约三分之一的面积，三颗卫星联网就可以实现全球无缝覆盖。对跨越数千公里的特高压电网来说，这种特性具有天然的适应性。卫星通信不受地理地形的限制，无论是崇山峻岭、浩瀚海洋还是茫茫戈壁，只要视线不受阻碍，就可以建立链路，给偏远地区的电力设施接入带来了极大的方便。该技术还具有灵活性好、部署方便的特点，当地面网络由于故障而停电时，可以迅速搭建起应急通信线路，保证电力系统指挥调度工作连续性。卫星信道具有广播的特性，有利于实现点对多点的组播业务，加快电力系统信息的分发。

虽然卫星通信具有明显的优势，但是它也存在传输时延大、链路损耗高、易受雨雪天气影响等固有的特性。对于地球静止轨道卫星来说，电磁波往返传播时间大约为半秒，这对一些实时性要求比较高的差动保护业务来说是不小的考验。频率越高，信号穿透大气层时受到的雨衰影响就越大，因此系统设计时需要预留足够的链路余量，或者采用自适应编码调制技术来抵消其影响。

(二) 卫星轨道与频率划分

按照高度和运行周期不同，卫星轨道分为低地球轨道、中地球轨道、地球静止轨道。不同种类的卫星在电力通信上应用范围各有不同，其频率资源的分布也会对通信系统的容量以及抗干扰能力造成影响。

卫星轨道与频段特性对照表

特性	地球静止轨道	低地球轨道	L/S 频段	C 频段	Ku 频段	Ka 频段
高度 / 频率	约 36000 km	500-2000 km	1-4 GHz	4-8 GHz	12-18 GHz	26-40 GHz
运行周期	与地球自转同步	90-120 分钟	N/A	N/A	N/A	N/A
时延	约 0.5 秒	极低	低	中	高	很高
覆盖范围	单星覆盖 1/3 地球表面	需星座实现连续覆盖	广	广	广	广
雨衰影响	较小	较小	极小	小	较大	很大
终端设备	大, 固定	复杂, 需跟踪	小型化	中型	小型化, 便携	需大口径天线 / 抗雨衰
电力应用	调度电话、数据回传	实时物联网、低时延业务	手持终端、移动资产	核心骨干通信、数据备份	应急通信、便携站	高清视频监控、大带宽业务

如上表所示，在频率划分上，电力卫星通信涉及 L 频段、S 频段、C 频段、Ku 频段以及 Ka 频段。

L 频段和 S 频段频率低，雨衰影响小，终端设备小型化程度高，常用于手持卫星电话和移动资产管理；C 频段抗雨衰能力强，传输性能稳定，是电力核心骨干通信的重要频段，常用于重要变电站的数据备份；Ku 频段可用带宽较宽，终端天线口径相对较小，便于携带和部署，目前是电力应急通信车和便携站的主流选择；Ka 频段作为高通量卫星的主要工作频段，具有极大的带宽资源，可以支持高清视频监控等大速率业务，但是受气象条件的影响最大，一般需要配合抗雨衰措施使用。

二、卫星通信在电力系统的应用

（一）应急通信与偏远地区通信

当地震、台风、冰灾等严重自然灾害发生时，地面的光缆、基站等通信设施往往先遭袭击，很容易被破坏造成通信中断，形成一个个信息孤岛。此时，由于卫星通信具有不依赖地面基础设施的特点，它就成为了恢复电力指挥系统、传递灾情的生命线。电力应急通信车上搭载的动中通或者静中通卫星天线，在到达灾区现场之后几分钟之内就能迅速入网，从而建立起现场指挥部与后方调度中心之间的高速数据通道，可以及时将现场的受灾照片、视频以及抢修进度回传到后方，保证调度指令能够准确传达。

我国西部广大地区、高山峡谷、海岛等恶劣环境下铺设光纤网络施工难度大、建设费用高、维护困难,造成许多变电站、水电站、输电线路长期处于通信盲区。卫星通信技术是解决最后一公里接入问题最经济、最可行的办法。在偏远站点上建小型卫星地面站,就可以用低成本实时采集并传输运行数据,使偏远电网设备可以被统一的管理系统来监督。

此种应用模式不仅可以解决基本的连接问题,还可以较好地支持无人值守变电站的远程运维。运维人员依靠卫星链路,可以在远端对设备的状态进行监视、参数进行设置、故障进行诊断,从而很大程度上减少人工巡检的次数和风险。伴随低轨道卫星互联网发展,未来偏远地区电力物联网终端可以直接使用更低功耗、更小体积的设备接入卫星网络,对配电变压器、分布式能源站点进行广域覆盖,提升农村、边疆电网智能化程度和供电服务质量。

（二）电网巡检与视频监控

输电线路一般会穿行于崇山峻岭之间,传统的人工巡检效率低、危险性大。无人机巡检技术的使用大大提高了工作效率,但是当无人机超出视距范围时,测控以及图像回传就成为限制因素。由卫星通信技术支撑的超视距无人机巡检依靠的是高带宽的卫星链路,无人机能够实时把高清可见光、红外热成像视频传回控制中心。运维人员无需到现场,就可以了解线路覆冰、异物悬挂、绝缘子破损等情况,真正做到了千里之外的运筹帷幄。

在输电线路可视化监控方面,安装在铁塔上的视频监控装置依靠卫星通道,对外界容易引起山火、滑坡、外力破坏等危险地段进行全天候监控。当前端装置利用图像识别算法发现异常情况的时候,可以立即通过卫星链路发起报警,上传现场快照或者短视频,有效弥补了山区公网信号覆盖不足的短板,形成电网安全的立体防护网。

海上风电场等离岸电力设施地面公网不能覆盖,海底光缆铺设和维修成本高、有断缆风险。卫星通信是海上风电运维船只、升压站平台与陆地集控中心之间最可靠的联系纽带,可以传输 SCADA 数据、进行语音通话、视频监控作业,保证海上绿色能源稳定输出。

第五节 混合传输技术

一、混合传输网络概念

（一）混合传输的驱动力与优势

电力系统业务形态正在发生深刻的变化，由原来的单向数据采集变为双向交互、实时控制。不但要保证通信网络有高带宽、低时延，更对它的灵活性、泛在性提出了严峻的考验。广大的农村地区或者地形复杂的山区，铺设光纤成本高、维护难度大，无线通信技术因为部署灵活、建设周期短的特点正好可以弥补有线网络的不足。城市中心区对通信可靠性要求很高，单纯依靠无线网络易受频谱资源干扰、建筑物遮挡等因素的影响，这时有线网络的稳定性就显得格外重要。

混合传输架构的主要动力就是实现技术和经济性两者的平衡。依靠骨干网络高速稳定的光纤以及接入层无线网络广覆盖、灵活便捷的特点，在保证业务服务质量的前提下，可以大大降低企业的网络建设与维护投入。该架构具有很强的抗毁性和生存能力，在某一传输链路发生故障的时候，它可以依靠异构网络的冗余路由机制，立即切换到另一种传输介质上，保证关键业务的连续性。自然灾害频发区域，混合传输网络所具有的多路径保障特性，成为提升电力通信网应急通信能力的重要因素。

（二）有线与无线混合传输模式

有线和无线混合传输模式是电力通信网中目前使用最多的架构形式，核心是以光纤作为流量回传的主干，用无线技术作为延伸到末梢的毛细血管。变电站、供电所等核心节点一般都通过 OPGW 或者 ADSS 光缆实现了光纤互联，形成了牢固可靠的骨干传输环网。节点既是数据汇聚点，又是无线接入网关的部署点，完成协议转换与数据分发。

从接入侧来看，对于配电自动化终端、智能电表、分布式能源站点等来说，由于点多面广且分散，光纤铺设的“最后一公里”问题一直困扰着行业。此时采用工业级无线路由器、微波设备或者无线公网模块，把分散的终端数据汇聚到最近的光纤接入点上，就形成了光纤和无线相结合的混合传输链路。该模式既能保持光纤网络的高带宽特性，又能发挥无线网络的接入便利性，很好地解决了配电环节的通信覆盖盲区问题。需要指出的是，随着技术的发展，混合已经不是简

单的物理连接，而是在链路上的智能调度，即根据业务的优先级以及链路的实时质量来决定使用有线传输、无线传输还是双路并发，从而达到传输效率的最大化。

（三）不同技术体制的融合

混合传输网络的搭建过程，实质上就是多种异构技术体制互相碰撞、融合的过程。在电力通信网中一直存在着以 TDM 技术为基础的同步数字体系网络和以分组交换为基础的 IP 网络。前者有严格的时延控制和电路仿真，可以带继电保护、生产控制这类高优先级业务；后者带宽利用率高、组网灵活，可以带管理信息系统、视频监控这类业务。混合传输架构中这两种体制不是孤立存在的，而是通过多业务传送平台或者分组增强型光传送网设备进行统一承载。

在无线领域，融合同样在加速进行：

1. 公网和专网的体制性并存，电力无线专网、电力无线 4G 和 5G 的安全性强，隔离性好、时延小、适合承载控制类业务；运营商公网（4G、5G）覆盖面广，产业链成熟，适合承载采集类和非实时业务。利用多模通信模组或者融合网关，终端可以支持各种专用网和公网制式，能够智能地实现“平时走专网、繁忙时溢出到公网”的切换。

2. 宽带与窄带互补融合：对于图像、视频巡检等高带宽业务使用宽带无线技术；智能电表读数、传感器状态上报等小数据量、低功耗业务则用窄带物联网技术或者微功率无线技术。混合传输网络在一个架构内可以同时支持各种不同的速率、不同的制式的通信协议，利用边缘计算节点对数据做预处理、协议解析，从而减轻核心网的传输压力。

3. 天地一体化融合：在地面网络不能覆盖的无人区或者深海等地方，卫星通信作为一种特殊的天基无线方式，正在和地面光纤以及无线网络相融合。利用卫星、4G/5G 和光纤组合起来形成立体化的通信网络，从而达到对电力通信网络进行全方位、全天候的覆盖，在任何极端环境下都可以实现对电力设施的可视、可测、可控。

二、典型混合传输方案

针对电力系统各种业务的不同特性以及地理分布，业界已经探索出了许多成熟的混合传输组网方式。这些方案不是固定不变的，会根据实际情况做出调整，目的在于解决具体的通信难题，提高整个网络的工作效率和安全水平。

典型混合传输方案概述

方案名称	主要构成	应用场景	核心优势
以光纤为主、无线为辅的骨干网延伸方案	光纤主路由 + 大容量微波 / 卫星通信作为备份或支链	地质灾害频发区、跨江河湖海或高山峡谷，偏远变电站 / 水电站接入	提高骨干网抗毁与扩展能力，应对极端情况，实现成本效益最优
“光纤 + 无线”的配电网“最后一公里”接入方案	光纤（推进至汇聚点）+ 短距离无线或 4G/5G/ 专网模块	配电网“最后一公里”接入，节点分散、环境复杂区域，老旧城区改造	解决末端接入难题，兼顾高带宽与灵活接入，高效覆盖配电自动化业务
“公网 + 专网”互为备份的通信保障方案	电力无线专网 + 运营商无线公网（双卡 / 双模组，APN/VPDN 安全隧道）	业务可靠性要求极高场景（如精准负荷控制），极端天气 / 灾害下的应急通信	显著提升业务可靠性，提供双重保障，增强极端条件下的感知和控制能力

上述典型混合传输方案的详细介绍如下：

（一）以光纤为主、无线为辅的骨干网延伸方案

在电力通信骨干网的建设过程中，由于光纤传输具有很大的传输容量以及很强的抗干扰能力，一直占据主导地位。但地质灾害频发地区、跨越江河湖海或者高山峡谷的地方，光缆的架设及维护存在很大的技术难题和经济负担。此时采用大容量微波或者卫星通信作为光纤链路的备份或延伸，是较为经济的一种解决方式。一般在枢纽变电站或者骨干节点之间建设光纤主路由，担负大部分生产调度数据以及管理信息数据的传输任务。

当发生地震、泥石流等自然灾害造成光缆中断或者进行光缆检修时，系统可以毫秒级地切至备用的微波链路。虽然微波传输的带宽比光纤小，但是它“视距传播”的特点可以跨越物理障碍，快速建立应急通信链路，保证调度电话、远动数据等重要业务的最低限度传输。对于一些偏远的小型变电站或水电站，如果离主干光缆较远且架线施工难度大，则可以采用微波接力的方式直接接入骨干网，形成光纤环网 + 微波支链的拓扑。保证骨干网的稳固性的同时大大提高了网络的扩展能力、抗毁能力，是电网在极端情况下的主要手段。

（二）“光纤 + 无线”的配电网“最后一公里”接入方案

配电通信网联结着配电站、环网柜、柱上开关、智能电表等大量的节点，节点数量多、分布广、现场环境复杂。完全依靠光纤接入，投资大、施工协调难度高，在老旧城区改造时经常遇到无孔可入、无管可穿的情况。“光纤 + 无线”的混合接入方案给破解配电网“最后一公里”接入难题赋予了一把金钥匙。

该方案一般把光纤引到配电房、小区开闭所或者一级汇聚节点，使用工业级以太网交换机或 EPON/GPON 光线路终端来实现重要节点高速接入。分散在周围的柱上开关、故障指示器、智能电表等终端设备用无线方式进行连接。

具体点说，可用 ZigBee、Wi-SUN、LoRa 这些短距离无线技术，以光纤节点做中心，创建无线微网，把传感器产生的数据先收集起来，再经由光纤回传。远离主干线、位置独立的配电终端可以直接加装 4G、5G 通信模块或电力无线专网终端，利用运营商基站或者自建基站进行数据上传。

本方案用光纤大带宽、稳定等特点解决汇聚层数据拥塞问题，并用无线技术灵活、方便的优点解决末端接入施工难的问题，达到高效覆盖配电自动化业务的目的。

（三）“公网 + 专网”互为备份的通信保障方案

由于电力业务对于通信安全可靠性的要求越来越高，仅仅依靠单一网络来承载的风险越来越明显。特别是当网络承载着精确负荷控制、配电自动化三遥等重要业务的时候，一旦通信中断，会造成电网故障扩大，甚至引起大面积停电事故。因此，建立公网和专网互相备份的通信保障机制，就成为提高业务可靠性的有效手段。

电力终端设备一般都配备双卡槽或双模组，可以同时接入电力无线专网和运营商无线公网。业务数据一般情况下采用电力无线专网进行传输。电力无线专网采用专用频段、专用设备建立起来的网络，具有网络独享、干扰小、安全等级高等特点，可以保证生产控制类业务的服务质量。

当电力无线专网信号弱、基站故障或者网络拥塞的时候，终端设备就会自动察觉链路情况，然后平稳地转到运营商公网通道。为了保证公网传输的安全性，在公网的一端设置专用的 APN 或者 VPDN 隧道，叠加国密算法加密，建立穿越公网的虚拟安全隧道。

互为备份机制相当于给电力通信加了双重保险。即使遭遇台风、冰灾等恶劣天气时，只要某个网络被破坏，其它的网络还保留有部分通信功能，从而大幅提高了电力系统在极端环境下的感知与控制能力。

三、混合传输网络的关键技术

（一）多协议标签交换技术

多协议标签交换技术是一种实现混合传输网络中业务智能调度的技术。电力通信中各种业务共存，它们对于带宽、时延、抖动、丢包率的要求千差万别。传统的 IP 路由技术是逐跳转发目的地址，不能保证重要业务的服务质量，也不能有效地避免网络拥塞。多协议标签交换技术把复杂的路由查找简化成了简单的标签交换，在数据包前面加一个很短的固定长度标签，使数据转发速度得到了大幅度提高。

混合传输网络当中，多协议标签交换技术的流量工程功能十分重要。它会按照业务需求以及网络资源的实时情况，预先创建好从源节点到目的节点的标签交换路径。

对继电保护差动信号等时延要求极高的业务，多协议标签交换-TE 可以为它规划一条走光纤网络、跳数最少、带宽独占的最优路径。对视频监控、办公自动化等对带宽要求较高但是对时延没有太多要求的业务，可将其调度至备用路径或者无线传输链路之中，达到网络资源负载均衡的目的。

多协议标签交换支持快速重路由，当有线或者无线混合网络中某一段链路出现故障时，可以在 50 毫秒之内把流量转向事先算好的保护路径，从而保证业务不断。借助标签精确控制的能力，混合网络就可以像单一物理网络一样给应用提供确定的服务质量保证。

（二）分组传送网技术

分组传送网技术是把光通信技术与 IP 分组技术结合在一起发展起来的新技术，主要服务于电力通信网的由 TDM 向全 IP 化的转变。混合传输架构里保存了同步数字体系技术的电信级可靠性特性，拥有丰富的 OAM（操作，维护，管理）功能，而且具备 IP 技术统计复用，灵活扩展的优点，成为有线骨干网和无线接入网的主要承载平台。

分组传送网技术是采用面向连接的分组交换方式，对突发性数据流量有较好的处理效果，适合于承载配网自动化、用电信息采集等有潮汐效应的电力业务。在混合组网的情况下，分组传送网设备作为汇聚节点，提供 TDM 接口、以太网接口、ATM 接口等多种接口，可以无缝接入各种老的设备和新的智能终端，实现不同技术代际共存。

分组传送网还有一个优势就是同步技术。电力系统中很多控制业务，例如相量测量单元 PMU 都需要非常高的时间同步精度。分组传送网网络支持 IEEE 1588v2 精确时间同步协议，利用地面光纤网络可以做到微秒级甚至纳秒级的时间传递，代替传统 GPS 授时方案，解决了卫星信号在室内或者地下变电站不能覆盖的问题。全网高精度同步对智能电网稳定运行有不可替代的作用。

（三）统一网管与业务调度

随着混合传输网络规模变大、技术体制变得越发复杂，传统的分专业管理方式已经不能适应越来越复杂的运维需求。光纤传输设备、无线基站、数通路由设备大多来自不同的厂家，各自拥有独立的网络管理系统，容易造成故障界定的难度增大、业务开通效率降低。因此，构建起跨越地域、层级、厂商的统一网管和业务调度平台，就成了实现混合网络智能运维的关键。

统一网管平台采用标准北向接口（CORBA、XML、Restful API）从底层各个异构网络采集告警数据、性能数据、配置数据，形成全网统一的资源数据库和拓扑视图。

1. 端到端业务开通，运维人员只需要在统一的界面输入业务的源宿节点、QoS 需求，系统就会自动计算出从光纤骨干网、分组传送网汇聚层到无线接入网的最优路径，然后自动下发配置指令，把人工配置几天的工作量减少到几分钟内。

2. 智能故障诊断利用大数据分析、人工智能算法对大量的告警信息做相关性分析。当混合网络出现故障的时候，系统可以立即找出是光缆断开、无线干扰还是设备断电造成的，并准确找到故障根本原因，从而减少无效的派单。

3. 平台对全网的流量流向加以监控，找出网络的瓶颈。重大活动保电、迎峰度夏时期，依据预案对业务优先级进行动态调节，将非关键业务的带宽限制在一定范围内，保证指挥调度业务的通畅。

集中化、智能化管理之后，混合传输网络就不再是孤立的个体，而是一个有机的整体，具有自感知、自优化、自愈合的能力，为智能电网高质量发展打下了坚实的通信基础。

第四章 电力通信网络架构

第一节 骨干通信网络

一、骨干网的功能与定位

（一）连接各级调度中心与枢纽变电站

骨干通信网的第一个主要功能就是把国家级、区域级、省级调度中心、大型枢纽变电站、换流站紧密地连接起来。这不是简单的物理相通，而是有层次、有逻辑的信息交换网络。在实际运行当中，骨干网要跨越数千公里的地理距离，经过各种各样的地形地貌，把散布在各地的电力中枢紧密联系起来。利用超长距离的光传输技术，国家电网或者南方电网总调可以对边远地区的特高压线路实时掌握。

各级调度中心依靠骨干网来下达调度指令，保证全网的频率和电压的稳定。枢纽变电站作为电网能量节点，会产生大量的运行数据，也需要通过骨干网上传到决策中心。骨干网覆盖范围决定电网调度控制半径，带宽能力决定信息交流深浅、宽窄。为了配合电网扁平化管理的推进，骨干网的连接触角正向末端更重要的节点延伸，形成更加密集、响应更加迅速的连接网格，为全网一体化协调控制打下坚实的物理基础。

在特高压交直流混联电网结构下，骨干网还要承担换流站间进行跨区直流输电的通信任务。这些站点之间相隔千里，对通信时延和同步性有非常严格的要求。骨干网采用直接光路，中间跳数最少，保证控制信号瞬间到达，保证跨区能源传输安全。

（二）承载核心生产控制业务

电力系统的生产控制业务是骨干网承载内容的重中之重，它们直接影响电网安全，属于生命线业务。

1. 继电保护信号传输属于骨干网中一个非常重要的工作。电网发生故障时，保护装置要以几毫秒为时间基准交换状态信息、切除故障，这就需要骨干网提供超低时延、超低抖动的传输通道。

2. 调度自动化系统数据和广域相量测量系统数据，要通过骨干网进行实时汇聚。数据流就像电网的血液一样，不断地给调度中心的大屏输送数据，给运行人员提供态势感知和决策的依据。

3. 调度电话作为应急指挥的最后一道防线，它的语音信号高保真、无阻塞传输也依赖于骨干网的专用通道资源。

除生产控制大区(I区、II区)业务外，骨干网还要保证管理信息大区高速互联。企业资源管理、营销数据汇聚、视频会议等业务对实时性的要求不高，但是数据的吞吐量很大。骨干网采用严格逻辑隔离，在一条物理光缆上为不同的安全级别划分出各自的传输管道，保证核心控制业务的优先权，并且满足不断增长的管理数据传输需求，实现业务承载多样化但安全标准统一。

(三) 对网络可靠性的极致要求

电力生产要求骨干通信网具备极高的可靠性、不能中断。任何一个瞬间的中断都会造成连锁性的电网事故。骨干网的设计标准比公用通信网络高得多，在自然灾害或者设备故障等极端情况下也必须保证核心功能正常运行。网络架构的每一个环节都力求做到极致，光缆路由的选择、传输设备的配置无一例外都遵循冗余备份的原则。

物理上骨干网一般采用三路由或者四路由的物理路径，单向光缆断路不会造成站点孤立。在设备上关键板卡、电源模块、交叉时钟单元都实行了热备份，可以实现故障无间断转换。对于承载特别重要业务的通道，还会使用异路由双发选收的方式，即相同业务信号在两条完全独立的线路上同时发送，接收端实时选择最佳接收路径，把传输中断概率降到最低。

骨干网的可靠性也同全天候网管监视、智能化故障诊断系统密切相关。当网络的光功率衰减或者误码率增大等出现细微的性能下降情况时，监控系统就会立即发出警告，调度人员可以及时进行处理。该种主动防御、快速反应的机制使得骨干网能承受地震、冰灾等各种恶劣环境的影响，是电网中坚韧不拔的脊梁，保证能源连续安全流动。网络可用率一般设置在小数点后多个九的级别上，体现的是电力通信人对安全责任的坚守。

二、骨干网拓扑结构

（一）环型拓扑结构及其保护机制

环型拓扑结构是电力骨干网早期及部分区域网络最常用的结构形式，用光纤把各个节点首尾相连，构成闭合环路。该结构最大的优点就是天然具有保护功能和节省光纤资源的特点。环型网络中，任一节点与其他节点之间都存在顺时针和逆时针两种传输路径。当环上某处光缆断开或者节点设备出现故障的时候，业务流可以自动倒换到另一条备用路径上，从而达到业务迅速恢复的目的。

保护方式主要依靠的是同步数字体系中复用段保护或通道保护。复用段共享保护环在光纤断裂时，利用环两端节点倒换，将业务绕行到环的另一侧，倒换时间一般控制在 50 毫秒以内，可以满足大部分电力控制业务的要求。通道保护环更直接简单，采用并发选收方式，不需要复杂的协议交互，可靠性高。

随着骨干网规模增大，单一环网结构已经不能满足要求，因此出现复杂的多环相交、相切的环网结构。跨环业务调度成了新的难题，节点瓶颈也越来越明显。但是环型拓扑由于其结构简单、保护倒换快、成熟可靠等优点，在省级骨干网和地市级汇聚层仍然占据重要位置，是保证局部区域网络生存的有效手段。

（二）网状拓扑结构及其路由策略

得益于光传送网技术的发展和业务流量流向的变化，网状拓扑已逐渐成为国家和区域骨干网主要的选择。网状网结构就是节点之间有多条直接或者间接的连接路径，形成一种类似渔网般复杂交错的关系。网状网比环型网连接度更高，任意两点之间一般都有三条以上的独立路由，提高了网络的抗毁性以及带宽利用率。

网状拓扑中路由策略就变得十分重要。根据当前网络的拓扑结构、各处资源的占用情况来生成业务的最佳路由路径。主路由发生问题的时候，系统会从中选取最佳的恢复路径，把业务重新导向。虽然恢复时间比环网倒换长一点，但是它不再受预留保护带宽的限制，从而提高了全网络资源共享的效率。

网状网可以实行比较灵活的业务调度策略。可以给不同的业务设置不同的路由约束条件，继电保护业务必须使用最短物理路径以减小时延，一般管理业务则可以采用跳数多、带宽大的路径。这种不同的路由策略可以使骨干网对不同的电力业务做出细致的匹配，使网络中的各种资源的能力发挥到极致，形成具有高自愈能力的智能光网络。

（三）国家电网/南方电网骨干网典型架构

我国两大电网公司的骨干通信网经过多年建设发展，已形成了各自特色、极其坚固的网络格局。

1. 国家电网公司骨干网是“三纵四横”的主体结构。宏大的网络布局 and 特高压电网建设路径不谋而合，一纵一横，从北到南，从西到东，铺展在广袤的大地上。核心层用大容量光传送网设备组网，形成多层网状结构，可以保证跨区电网控制信号的高速直达。各个区域网根据地理特点分别采用格状或者环状结构加以补充，就形成了层级分明、覆盖面广的立体网络。

2. 南方电网公司骨干网以“八交十直”西电东送大通道为架构。主干网为典型的高连通度网状结构，可以有力支撑西电东送战略。在台风多发地区，南方电网为提高抗灾能力特意增加通信路由迂回能力。

两个骨干网的架构并不仅仅是把物理光缆简单的叠加在一起，它也是先进的通信技术和电网运行特点深度融合的结果。它们都采用了分层分域的管理模式，把庞大的网络分成核心骨干层、区域汇聚层等不同的逻辑层次，既可以实现全网的统一调度，又可以给区域网络留出一定的自治空间。骨干网上不断涌现出超高速传输技术以及智能管控系统，正向着全光网迈进，给创建世界一流电网提供强大的信息支撑。

三、骨干网关键技术

（一）基于 SDH/OTN 的光传输网

同步数字体系长时间控制着电力骨干网，有着严格的同步特性以及很强的管理运维能力。SDH 技术时隙固定不变，给每一条业务提供刚性管道，这一特点正好满足了电力调度业务对时延确定性、安全隔离的高要求。对于 2Mbit/s 颗粒度的业务调度，SDH 有无法比拟的优势，目前仍然有很多（继电保护等）重要的业务使用它作为承载载体。

但是随着视频监控、数据中心互联等大带宽业务的爆发式增长，SDH 的容量扩展性不足的问题也越来越突出。光传送网技术出现以后，SDH 的电信级 OAM（操作、管理和维护）特性与波分复用的超大传输容量被结合到一起。OTN 利用光层交叉、电层处理，实现波长级和子波长级的大颗粒业务调度。

在现代电力骨干网中，SDH 和 OTN 是融合共存的。底层用 OTN 来构建超

大带宽的基础传送平面，单波长速率可以达到 100G 或更高，一根光纤总容量可以达到 Tbit 级别。上层则通过 EOS（以太网 over SDH）或者 SDH 接口卡继续兼容现有的低速调度业务。OTN 为主骨、SDH 为肉的技术组合，既可以保证传统核心业务的平稳运行，也可以给新型数据化业务提供无限带宽池，是目前电力骨干传输网主流的技术形态。

（二）基于 MPLS-VPN 的多业务承载

为了应对电力数据通信网中多样的业务种类和不同的服务质量要求，MPLS 叠加 VPN 成了骨干数据网的主要业务方案。MPLS 给数据包头部加上了很短的标签，使核心路由器只要根据标签快速转发，不需要做复杂的 IP 路由查找，大大提高了数据转发的效率。

基于 MPLS 的三层 VPN 技术，可以基于同一个物理网络，在不同的部门、不同的业务系统之间建立逻辑上完全独立的虚拟专用网。

MPLS-VPN 在电力业务中的应用

VPN 类型	承载业务	特性
实时 VPN	生产控制大区 I 区业务（如继电保护）	高优先级、低时延、保证带宽
非实时 VPN	生产控制大区 II 区业务（如 SCADA/EMS）	较高优先级、保证带宽
管理 VPN	企业资源管理、营销数据、视频会议	相对低优先级、高吞吐量
办公 VPN	不同城市办公网络互联	透明连接、如同一个局域网

如上表所示，调度数据网用 MPLS-VPN 把其分成实时 VPN、非实时 VPN，分别承载生产控制大区 I 区、II 区的业务。采用流量工程技术对实时 VPN 预留带宽资源，设置高优先级的转发队列，保证在网络拥塞的时候关键的遥测、遥控指令依然能够畅通。二层 MPLS VPN 技术，也就是 VPLS 技术，用来打通各个城市的办公网络之间透明的通道，把分散的网络当作一个局域网。MPLS-VPN 技术还支持快速重路由，在链路发生故障的时候，可以在 50 毫秒内把流量切到备份路线上去，它的可靠程度接近 SDH。该项技术使得电力骨干数据网具有了电信级的承载能力，可以实现业务的融合承载以及差异化服务。

（三）网络生存性技术

网络生存性就是指网络在遭遇各种故障或者攻击的时候，仍可以维持可接受的服务水平。生存性技术对于电力骨干网来说是保证电网安全运行的最后一道防线，分物理层、传输层和逻辑层三个方面的全方位防护和恢复。

传统的保护技术依靠硬件冗余和预留资源。线性复用段保护、环网保护等利用预先分配好的备用通道，当信号丢失时硬件自动完成倒换。该方法简单可靠，恢复快，但是资源利用率低。随着智能光网络的出现，基于控制平面的恢复技术也开始被使用。自动交换光网络可以在网络发生多点故障或者预设保护路径失效时，实时计算一条新的临时线路来恢复业务，大幅度提高了灾难情况下网络的生存概率。

除了传输层的生存性技术，业务层生存性技术也不可轻视。IP 网络中的快速重路由，虚拟路由器冗余协议等技术可以保证路由器节点发生故障的时候数据业务不会中断。对于极其重要的电力业务还会使用跨层协同的生存策略，例如在光传输层倒换的时候及时通知上层的数据设备调整路由，避免多层保护机制之间互相冲突、震荡。这样一种立体的生存技术体系，使得电力骨干网具有了很强的自愈能力，在地震、洪水等不可抗力面前，也能顽强地守护着能源信息的流动。

第二节 接入通信网络

一、接入网的功能与定位

（一）连接骨干网与终端设备

接入网的主要任务之一就是建立高速的信息通道，将骨干网与大量的终端设备连接在一起，使得数据流的双向透明传输、汇聚。电力通信系统中骨干网主要承担大容量、长距离的数据传输，终端设备数量很多、分布很分散、接口多种多样。接入网通过设置汇聚节点和接入节点，把分布各地的智能电表、配电终端、传感器等感知层产生的微小数据流进行汇聚，再通过高速上行链路送往骨干节点。这里不只是物理链路的连接，还有协议转换、流量整形、信令匹配等一系列复杂的逻辑处理，保证不同的设备、不同的标准可以接入同一个网络。

为了满足终端设备不断增加的带宽和实时性要求，接入网在连接层面上大量使用了光纤通信、无线公网、电力线载波等技术来构造起有线无线结合的网络。从物理上来说，接入设备要具备抗干扰、高温、低温、高湿度等恶劣环境正常工作能力，保证连接的稳定性。链路层利用动态带宽分配、QoS（服务质量）保证的方式，接入网按照业务优先级智能分配网络资源，保证重要的控制指令优先传输，普通监测数据上传不干扰。使得本来通信就不太方便的终端可以有效的加入

到网络中，形成畅通的联系。

随着物联网技术的广泛应用，接入网的连接对象也由原来的电力设备扩展到了分布式电源、电动汽车充电桩、用户侧智能家居设备等，这就对接入网的泛在连接、海量地址管理能力提出了更高的要求。连接的功能不再只是点对点的传输，而是向多点对多点、网状互联方向发展。在接入层配置边缘计算节点，把部分数据处理与分析任务从骨干网、云端下放到边缘节点上，极大减轻了骨干网传输的压力以及云端的计算压力。因此连接就不再只是物理上的导通，而是算力和智能的延伸。

（二）覆盖 110kV 及以下变电站、开闭所

接入网的地理覆盖范围和电压等级有关，主要对 110kV 及以下的变电站、配电室、开闭所、环网柜、柱上开关等配电网节点进行服务。接入网服务站点数量远远多于骨干网覆盖的 220kV 及以上核心枢纽变电站，分布非常分散，涉及城市中心、工业园区、农村等各个地区。广泛覆盖的需求使接入网在规划建设的时候要考虑地域差异、资源禀赋，选择合适的建设策略来满足全面覆盖、业务均衡的要求。

城市核心区域的 110kV 变电站、开闭所多建于地下或者建筑物内，占用空间小，管孔资源缺乏。因此接入网的建设大多依靠已有的光纤沟道资源和紧凑型设备，用高密度光缆网对密集站点实现全面覆盖。而在农村以及偏远地区，由于站点相距较远，铺设光纤的成本很高并且维护也不方便，这时接入网的覆盖更多地依靠无线专网或者公网资源，利用无线信号的广域覆盖特性来解决“最后一公里”的接入问题。接入网依据各电压等级站点所给定的接入带宽和接口类型来保证，无论是 110kV 变电站综合自动化系统还是 10kV 开闭所简单的监测设备都能够获得相应的通信资源。

完成对 110kV 及以下站点的全部覆盖，是使配电网由被动应对转向主动管理的物理载体。电力公司在站点上装设光线路终端、光网络单元或者无线通信模块之后，便可以对中低压电网的运行状况实施实时掌控，迅速察觉并隔离故障，供电可靠性及电压质量因而得到明显提升。深度网络覆盖为分布式能源接入创造了必要的通信条件，分散在配电网各处的太阳能、风能等可再生能源能被有效监测和调度，有利于能源结构的改善以及绿色电网的建设，也充分体现接入网对电网形态演变的支撑作用。

（三）承载配电自动化、营销等业务

接入网是电力业务的承载平台，需要同时满足生产控制类业务与管理信息类业务的不同要求，其中配网自动化和电力营销业务是代表性最强的两种应用。配电自动化业务主要包括配电 SCADA、故障定位与隔离、电压无功优化等内容，这类业务对通信网络的可靠度、时延和抖动要求非常高。配网故障发生之后，通信网络要毫秒级地把故障信息上传到主站，迅速下发切除指令，任何通信中断或者延迟都会造成停电范围的扩大，严重影响供电质量。因此，在承载配电自动化业务时，接入网一般使用工业级以太网或者无源光网络技术，并且构建环网保护或者双路由备份的方式来保证业务通道的高可用性。

电力营销业务有用电信息采集、远程费控、双向互动服务等，特点是节点多、单点数据小、并发率高。智能电表全面铺开之后，接入网每天需要处理大量的计量数据采集工作，对网络的并发处理能力和数据吞吐量提出了巨大的考验。营销业务包含用户隐私数据及费用结算，所以数据的安全性、完整性也需要保证。接入网通过身份认证、数据加密、访问控制，搭建起一道安全屏障，保证信息不泄露，不被篡改，使电力交易公平公正。

除了上述两类核心业务，接入网还承担着日益丰富的增值业务与新兴业务：

1. 无人值守变电站、开闭所的高清视频监控数据需要接入网络实现实时回传，便于运维人员远程查看现场的情况；温湿度、烟感、水浸等环境数据也需要接入网上传，因此对带宽的要求比较高。

2. 电动汽车充电设施通信，随着充电桩的大规模建设，对充电桩的运行状态监测、计费信息交换、有序充电控制等业务的相互对接入网需求越来越大，使接入网越来越趋向于物联网架构。

二、接入网组网模式

接入网的组网方式影响网络的拓扑结构、资源利用效率和抗毁能力，属于网络规划时必须考虑的设计因素。根据不同的地理环境、业务需求和光缆资源分布情况来确定电力接入网组网方式，实现技术、经济的最佳平衡。

接入网组网模式对比表

组网模式	核心特点	主要优势	主要劣势	适用场景
星型	所有终端直连中心节点	逻辑清晰，故障隔离容易	光纤资源消耗大，中心节点压力大	站点集中、对可靠性要求高的局部区域
树型	基于光分路器级联，逐级分支	节省主干光缆资源，覆盖范围广	单点故障风险，可靠性相对较弱	用户分布呈带状或片状的配电小区、商业楼宇
链型	多个节点串联，形成长链	与电力线路走向吻合，施工成本低	脆弱性高，易受中间节点故障影响	狭长地带，沿公路/铁路分布的电力设施
混合型	综合多种拓扑结构	灵活性高，适应复杂多变环境	运维管理难度大，需智能化网管	供电区域复杂多样，需兼顾可靠性与成本

各类组网模式的特点与适用场景，可参见上表。

（一）星型/树型组网模式

星型和树型组网模式属于电力接入网里常用的拓扑结构，无源光网络技术体系中常常采用这两种模式。网络以汇聚节点为中心，用光分路器把光信号逐级分发给各个用户终端，形成点对多点的放射状结构。星型结构中所有终端都通过独立链路直接接入中心节点，逻辑简单，易于故障隔离，任意一条链路的故障都不会影响其它节点。但是由于其光纤资源消耗较大，随着节点数量的增加，中心节点的端口压力和布线复杂度都会急剧上升。

树型组网模式为星型结构的延伸和优化，它依靠光分路器级联的方式，在光缆沿线根据用户分布情况灵活引出分支，极大节约了主干光缆资源。该模式适合于用户呈带状或者片状分布的配电小区、商业楼宇。通过合理的规划分光比和分光级数，在满足业务带宽需求的情况下，用最少的光缆投入获得最大的覆盖范围。以 EPON、GPON 为例，这二种技术就是采用树型拓扑结构，才能实现一根光纤接入几十甚至上百个终端。

尽管星型、树型网络模式在资源利用和建设成本上有优势，但是可靠性比较弱。由于网络结构存在单点故障的风险，一旦上联主干光纤或者核心分光器出现故障，就会造成与之相连的所有子节点的通信被切断。为克服这一不足，在关键业务场景中一般采用“手拉手”保护或者双归属保护的方式，也就是建立两条不同的路由链路，把树型网络的末端连接到不同的汇聚节点上。当主链路出现故障的时候，业务可以毫秒级地切换到备用链路上，这样既保持了拓扑的简洁性，又提高了系统的生存能力。

（二）链型组网模式

链型组网模式用通信链路把多个节点串联起来,形成一条长链,在早期基于SDH/MSTP技术建设的通信网,以及基于电力线载波的低压集抄系统中较为常见。链型组网最大的优点就是其组网方式与电力线路走向几乎完全吻合,电力线一般是呈线状延伸的,在沿途的杆塔和配变台区上就有很多。采用链型组网可以沿着电力线通道或者同杆架设的光缆顺势布设,最大限度地降低施工难度和建设成本,特别适合于狭长地带或者沿公路、铁路沿线分布的电力设施接入。

链型结构下,数据流需要经过中间节点逐级转发才能到达端点或者汇聚中心,越靠近汇聚节点的链路承载的流量越大,越容易形成网络瓶颈。为了解决这个问题,一般要在链首或者重要节点设置高带宽设备,采用流量汇聚和收敛技术。链型组网的另一特性就是脆弱性,由于节点间是串联的关系,任何一个中间节点掉电或者链路断开,都会造成下游所有节点通信中断,出现“断链”现象。因此链型组网时一般限制级联节点数量,防止链路过长造成可靠性大幅度下降。

为了提高链型组网的可用性,在现代电力接入网中常使用带旁路功能或者自愈能力的设备。在工业以太网交换机构成的链型网络中,可以使用光旁路保护器实现:当某个节点设备出现故障断电的时候,光信号可以直接通过物理旁路向下传递,保证链路的连通性。这些技术改进使链型组网在线性地理环境中依然有很强的生命力,是星型、树型组网的有力补充。链型组网由于施工方便,在配电线路自动化改造中得到了广泛的使用。

（三）混合组网模式

实际的电力通信网建设中,由于供电区域的复杂性、多样性,单一的组网模式很难适应所有场合,于是产生了混合组网模式。混合组网就是在一个接入网络中把星型、树型、链型、环型等多种拓扑结构综合使用,在不同的区域根据负荷密度、光缆资源状况、业务重要等级等因素进行组合。在变电站密集、光缆资源丰富的核心城区,可以采用光纤环网作为接入层,保证核心业务的高可靠性,在环网节点处采用树型或者星型结构延伸到周围的配电房和智能电表,形成主干环网、分支树型的复合架构。

混合组网模式很好地体现出接入网设计所具有的灵活性和实用主义。新建区域与老旧城区改造并存的复杂环境里,可以使得设计人员依照现场实际状况“量体裁衣”。对于由于地理环境限制不能布设光纤的孤立站点,可将其作为树型网

络的末端，使用无线微波或者 4G/5G 网络接入；对于沿线路状分布的配电自动化终端，则可以局部使用链型结构串接，接入到附近的骨干节点。它打破了僵硬的拓扑限制，把有线、无线、光纤、载波、环网和链型有机地融合在一起。

混合组网模式提高了网络的适应性和覆盖率，但是也加大了网络的运维管理难度。复杂的拓扑结构会增大故障定位和路由管理的难度，对网管系统的智能化水平提出了更高的要求。为更好地对复杂的网络结构加以管理，电力通信运营商采用软件定义网络等先进思想，集中控制平面，达到异构拓扑的统一视图以及自动调度。在网络混合组网结构下，网络不再是一个静止不变的物理连接，而是一个可以感知业务需求、并根据业务需求动态调整逻辑结构的弹性系统，这就成为未来电力接入网向智能化、融合化发展的必然趋势。

第三节 终端通信网络

一、终端通信网的概念与范围

（一）面向配电侧、用电侧的末端网络

终端通信网络从架构上来说属于电力通信网的末端接入层，是骨干通信网向配电台区以及用户内部的自然延伸和毛细渗透。它不再只局限于传统的变电站之间的高速互联，而是深入到低压配电变压器以下广阔的空间里，覆盖了从配电房、箱式变电站到居民住宅、工商业楼宇乃至分布式能源站点的物理空间。该网络层级要和配电网的拓扑结构相适应，必须能够适应复杂的地理环境、多样的安装条件，还要适应配电网频繁变化的拓扑结构和运行方式，具有高度分散、广覆盖的特点。

从功能逻辑上来说，配电侧和用电侧末端网络就是能源流与信息流的交汇点。配电侧实时上传配电线路的电气量参数、开关状态、环境监测数据给配电自动化系统做决策依据，实现故障快速定位和隔离；用电侧深入到用户内部的能效管理系统中，支持智能家居、电动汽车有序充电、需求侧响应等新型业务。终端通信网要具有很强的环境适应性和组网灵活性，才能在各种复杂的电磁环境和物理障碍下建立起稳定的、可靠的數據傳輸通道，打破傳統電網“盲調盲管”的局面，實現對電網末梢的全景感知。

因此，终端通信网络的创建，不是通信线路的简单布置，而是包含网络架构扁平化，接入手段多样化的一场技术革新。打破传统的垂直调度控制模式，把边缘计算能力推向网络末端。末端网络节点上配置计算资源之后，很多对实时性要求高、数据量存在冗余的业务就可以在本地处理，有效地减轻了上层主站的负担。同时，面向终端的网络架构给分布式光伏、分散式风电等新能源即插即用提供通信支撑，使电网可以像互联网一样接受大量生产者，促进能源消费方式的深刻变革，是建设清洁低碳、安全高效能源体系的坚实基础。

（二）连接智能电表、传感器、控制器等

终端通信网所连接的对象具有极其多样、零散的特点，是电力系统里数量最多的感知层、执行层单元，构成一个巨大的物联网生态。

1. 智能电表是终端通信网中最基本的、数量最多的接入节点。智能电表作为用户和电网互动的接口，除了要完成电能计量的法定义务外，还是一个能对电压电流进行监测、电能品质进行分析并及时上报停电事件的综合性感知单元。高频的数据采集上传，给电网负荷预测、线损分析、反窃电监测提供大量的第一手数据。

2. 各种环境及电气传感器成为终端通信网灵敏的触角。配电房、电缆隧道内温度湿度、烟感、水浸等环境传感器对设备运行环境进行监测；架空线路上的故障指示器、微气象监测装置对线路状态及气象实时监测。这些传感器所产生数据虽然单一，但是汇总起来能够对电网设备的健康状况做出准确的描述，推动电网由“事后维修”向“状态检修”转变。

3. 控制器类设备是电网执行精确控制的“手脚”。配电自动化终端（DTU、FTU）、智能断路器、无功补偿装置、用户侧空调负荷控制器、电动汽车充电桩控制器等，都需要通过终端通信网接收主站或边缘计算节点发出的控制指令。指令下发要具有高度的可靠性和实时性，通信延时或者丢包都会造成控制失败，从而影响电网的稳定运行。

4. 新型电力系统建立后，分布式电源逆变器、储能变流器也逐渐成为重要的接入设备。这些电力电子装置既要把发电量以及储能情况上传，又得遵照电网的调配命令，参加频率调节和电压支撑。终端通信网要采用标准化的接口协议，把各种品牌、各种通信规约的设备接入网络，实现源网荷储各个环节的互联互通。

（三）承载海量、低速率、低时延业务

终端通信网承载的业务流量特征与传统互联网存在显著差别，主要是连接节

点数目众多、单个节点的数据传输速率较低，但是对通信时延和可靠性有着很高的要求。

就终端通信网接入的设备数量级而言，一般是骨干网的成百上千倍。中等城市的终端节点数量可以达几百万，对网络地址管理能力、并发接入能力、拥塞控制能力有很高的要求。海量节点同时在线且周期上传数据，虽然单个数据包只有几百字节，但是汇聚之后产生的瞬时流量高峰很容易造成信令风暴。因此网络架构要设计出高效的随机接入算法和资源调度方案，在网络出现拥塞的时候，保证重要的业务数据仍然可以优先发送，不会被丢弃或者导致系统崩溃。

大部分终端业务为低速业务。智能电表的抄表数据、传感器状态监测数据一般只有文本或者简单的数值信息，不需要像视频流那样的高带宽。这就决定了终端通信网在技术选型的时候，更倾向于选择窄带通信技术或者低功耗广域网技术，从而获得更大的覆盖范围和更低的功耗成本。但低速率并不等于低性能，反而“小数据”传输往往具有很高的业务价值。例如一个只有几个字节的跳闸告警信号，不能及时到达的话，可能会造成大面积停电事故的扩大。所以，在有限的带宽资源下保证高价值信息的完整性，就成了终端通信网设计的一个主要难点。

时延敏感性属于终端通信网络业务的特征之一，对于配电自动化保护、控制等业务来说是特别的。当配电线路发生短路故障时，保护装置必须在毫秒级的时间内完成故障信息的交换和切除动作，如果通信时延超过了一定的限度就会造成保护失效。即使是非实时计量业务，在并发抄表量大或者即时费控指令下发时，也需要网络有秒级响应速度。终端通信网要采用扁平化的网络层级、改良的路由协议、边缘计算技术，大量减少数据传输路线上中间的环节，从而满足不同业务场景的差异化时延需求，保证电网控制指令的“即发即达”、状态感知的“实时在线”。

二、终端通信接入技术

根据终端通信网覆盖范围广、环境复杂、节点多等特点，电力行业根据实际情况采取了有线、无线相结合、宽带、窄带相融合的复合型接入方式。各种终端通信接入技术的特点对比如下表所示。

终端通信接入技术对比表

技术类型	传输介质	主要特点	优势	局限性 / 挑战	典型应用场景
低压电力线载波	低压配电线	有电即通信，无需专用线路；高速 PLC 基于 OFDM，频谱效率高，抗噪性强；支持自动组网、自愈合。	建设成本低，施工难度小，解决“最后一百米”接入难题，兼具感知能力。	信道环境恶劣（噪声、阻抗变化），信号衰减大，传输距离短。	居民小区、农村台区自动抄表，台区识别，线损分析，相位识别。
微功率无线	无线电波 (ISM, Sub-GHz)	部署灵活，不受物理线路限制；Mesh 网状网架构，自愈能力强；低功耗、远距离；采用 FHSS、国密算法保障安全性。	组网灵活，穿透力强，适合复杂地形和老旧区域改造；低功耗，覆盖范围广，安全性高。	开放空间易受干扰，需抗干扰技术；单跳带宽相对有限。	远距离抄表，分散设备连接，复杂环境（农村、老旧小区），电力控制类业务。
有线工业通信（工业总线 / 以太网）	双绞线，光纤 / 铜缆（工业以太网，PON）	RS-485 接口简单、成本低、抗共模干扰；工业以太网高带宽、IP 化、抗恶劣环境；PON 抗电磁干扰、雷击，超长距离无中继，高带宽。	确定性传输，高可靠性，抗干扰能力强；易于设备挂载；支持高带宽业务，满足低时延要求。	RS-485 速率和吞吐量有限；光纤专网建设成本较高。	配电房内部监测，智能电表集中器下行通信，配电自动化终端（DTU/FTU），视频监控，智能配电房，电动汽车充电站，配网差动保护。

（一）低压电力线载波

低压电力线载波通信技术是指以现有的低压配电线为传输介质，进行数据传输的一种通信方式，是目前电力终端通信网中应用最广的一种主流技术。

它的优点是**有电即通讯**，不需要专用线路，大大降低了建设和施工难度和费用。电力线已经通到每一个用户那里，用其来传输数据，可以解决“最后一百米”接入的问题。早期窄带电力线载波技术由于传输速率低、抗干扰能力差等原因，被用在低频次的自动抄表业务上。随着技术的发展，以正交频分复用为基础的高速电力线载波成了主流。HPLC 技术利用在较宽带宽内经过大量子载波并行传输数据的特点，具有很高的频谱利用率和抗噪性，可以自适应克服电力线信道里经常出现的脉冲干扰和频率选择性衰落，物理层速率可达兆比特级别，可以支持停

电上报、费控、台区识别等多种业务。

虽然电力线载波通信具有无需布线的先天优势，但是也面临着电力线信道环境非常恶劣的挑战。低压电网连接着各种家用电器、工业设备，变频器、开关电源等会产出大量的高频谐波噪声，很容易淹没通信信号。而且，电力线阻抗随负荷变化很大、信号衰减大、传输距离短。为此现代载波通信系统中普遍采用自动路由组网技术。通信模块可以自动检测网络拓扑结构，自动形成多跳传输网络。某条路径受到强干扰而中断时，可以很快更换路线，把临近的节点做中继转发。由于具有自组织、自愈合的特性，在复杂的低压台区中，电力线载波技术具有很强的生命力。

低压电力线载波技术除了抄表以外正向全网感知方向发展。利用电力线传输的载波信号可以实现相位识别、户变关系核对、线损细粒度分析等任务。利用载波信号过零点的特点可以判断用户所处的相位，通过比较台区总表和各个分表载波模块的时钟是否同步、信号强度等，可以自动理清复杂台区的拓扑结构，有效整治乱接线问题。这样的通信与感知一体化的走向，使电力线载波技术不再是简单的数据通道，而是电网精细治理的数字化眼睛。

（二）微功率无线

微功率无线通信技术主要工作在不需要许可的 ISM 频段上，依靠无线电波在空气中传输数据。由于它具有部署灵活，不受电力线拓扑限制的特点，所以成为终端通信网的重要补充方式。

1. 微功率无线技术组网的灵活性非常高。和电力线载波依靠物理线路不同的是，无线信号可以穿过墙壁和障碍物，实现跨台区、跨楼层的设备连接。对于一些电力线老化严重、噪声干扰严重导致载波通信难以正常工作的区域，微功率无线技术就可以很好地发挥它的优势。一般采用 Mesh 网状网架构，网络中的每一个节点既是终端又是路由器。新设备接入时可以自动搜索邻节点并加入网络，原有路径中断后也可以自寻替代路径，具备很强的自愈能力。它的这些特点使其适合于设备分散，地形复杂的农村地区或者老旧小区改造的场景。

2. 技术发展趋势是功耗越来越低，传输距离越来越远。传统的 ZigBee 等技术虽然成熟，但是穿透力和覆盖范围小。近几年，以 470MHz、230MHz 电力专用频段为代表的 Sub-GHz 无线技术开始成为主流。低频信号绕射能力好、传输距离远、单跳可覆盖几公里甚至十几公里的区域，能够有效减少中继节点数量。

采用扩频调制技术,如 LoRa 或者电力专用无线传输协议,接收机的接收灵敏度大幅度提高,在信噪比较低的情况下也能解调出有效的信号,使得通信更加可靠。

3. 抗干扰能力以及安全性同样属于微功率无线技术应用时的考虑因素。工作在开放空间中的无线信号很容易受到同频段其他设备干扰。因此微功率无线系统中大量使用了跳频扩频技术,通信频率在各个信道间随机跳变,有效地避免了定频干扰。就安全性来说,由于无线信道容易被窃听,采用国密算法为链路层数据加密和认证,使得每帧数据都得到严密的保护,防止恶意节点的入侵和篡改。采用“跳频+加密”的双重保护方式,给微功率无线在电力控制类业务的应用建立了一道安全防线。

(三) 工业总线与以太网

对于通信速率高、可靠性高、抗干扰能力强等一些特定场合,工业总线、以太网技术因具有确定的传输特性,在终端通信网中仍然是不可缺少的高端接入方式。

RS-485 总线是最早被广泛使用的工业串行通信标准,由于接口简单、成本低、抗共模干扰能力强等优点,在配电房内部监测、智能电表集中器下行通信中仍被大量使用。它使用差分信号传输,对抗工业环境电磁噪声效果好,在双绞线上可以实现千米级的通信距离。尽管其半双工的通信方式以及较低的波特率限制了数据吞吐量,但是对数据量小、节点相对固定的环境监测传感器和仪表读取而言,RS485 是一种性价比非常高的方案。利用 Modbus 等标准规约,不同厂家生产的设备可以方便地挂接在同一个总线上,成为构成配电物联网最基本的有线连接层。

工业以太网是终端通信网向宽带化、IP 化发展的代表。由于配电自动化终端(DTU、FTU)功能增强以及视频监控等高带宽业务的加入,传统低速总线已经不能满足需求。工业以太网沿用了商用以太网的高带宽和通用性,并且对电力工业环境加以加固。工业级光电转换器件、交换芯片可在高温、高湿、强电磁干扰等恶劣环境下长期稳定地工作。通过 VLAN 划分、QoS 优先级保证以及 ERPS 环网冗余协议,可以实现毫秒级的链路故障切换来保证保护控制指令的确定性传输。

光纤专网技术,尤其是无源光网络(PON, EPON/GPON),把工业以太网的性能提升到了新的高度。用光纤作传输介质,完全解决了电磁干扰、雷击等难题,实现了超长距离无中继传输。在智能配电房、电动汽车大型充电站这些关键节点,光纤接入可以做到吉比特级的上下行带宽。OLT 设备放置在变电站内,用

无源分光器连接各个配电终端的 ONU，构成一张高可靠性的树型全光网。延迟小，无源特性不需要中间链路供电，大大降低了运维难度。建设成本较高，但是因为供电可靠性的要求高，核心城市区域终端通信网中光纤以太网已经成为首选方案，支撑配网差动保护等高级业务的规模化应用。

由于技术的不断融合，工业总线和以太网领域正在向着“光进铜退”、以太网 IP 化方向发展。原本用 RS485 连接的设备逐渐用串口服务器改为以太网接口，并接入到统一的 IP 网络架构中。全 IP 化之后，终端通信网可以无缝对接上层云平台，实现端到端透明访问、统一管理，为软件定义配电网的发展打下了良好的物理基础。

第四节 网络拓扑结构

一、基本拓扑结构

基本拓扑结构是建立复杂通信网络的基石单元，每一个结构都有不同的几何形状以及传输特性。对这些基本结构的运行机制以及优点和缺点有充分的认识，是建立一个高效的、稳定的电力通信系统的必要前提。

常见电力通信网络基本拓扑结构特点

拓扑类型	主要特点	优点	缺点	电力通信应用示例
总线型	所有节点共享一条公共传输总线	布线简单，电缆用量少；初期成本低	单点故障（总线），冲突概率高，扩展性差	早期局部网络、小型工业控制
星型	所有节点通过独立链路连接到中央节点	便于管理维护，故障隔离容易；易于扩展	中央节点是单点故障；布线量大，成本高	电力调度数据网、行政电话网接入层
环型	节点首尾相连形成闭环，数据单向或双向传输	自愈能力强，可靠性高；传输效率高	节点增删配置复杂；一个节点故障影响整个环路（无保护时）	骨干传输网（如 SDH/OTN），继电保护
树型	层次化结构，根节点向下辐射分支	易于扩展，故障排查有方向性；适合分级管理	上层节点故障影响所有下级节点；根节点是单点故障	配电通信网、用电信息采集
网状型	节点间有多条路径相连（全网状/部分网状）	极高可靠性、冗余度；低时延；抗毁性强	布线和端口成本高；路由算法复杂	省级骨干网核心层、重要数据中心互联

（一）总线型、星型、环型、树型结构

总线型拓扑结构是一种以广播信道为基础的多节点连接方式，所有站点的硬件接口都直接与一条公共传输介质相连，这条传输介质称为总线。在电力通信的早期应用或者一些局域网中，由于布线简单、电缆用量少，总线型结构得到了人们的青睐。节点发数据时，信号向总线两端传播，其它节点通过地址匹配来接收数据。但是，总线型结构的主要缺点是总线是网络的瓶颈，一旦主干线断开，整个网络就会瘫痪。节点数量增多，总线负载加重，冲突概率增大，传输效率随之急剧降低，在现代大型电力骨干网中很少作为核心架构单独使用。

星型拓扑结构是以中心节点为枢纽，所有其他的外围节点都是通过独立的点对点连接方式接到中心节点上。电力调度数据网、行政电话网中星型结构应用较多。其结构优势在于易于管理、维护，单个外围节点故障不会影响其它节点的通信，故障隔离也较容易。但是中央节点在完成全网的数据交换和控制任务的时候，也是可能的单点故障源，一旦中央设备出问题，全网就会瘫痪。大型星型网络覆盖范围广时需要敷设大量的线缆，随着面积增大造价成倍增加。

环型拓扑结构把所有的节点用点对点链路连接成一个闭环，数据信号沿着环路按照一定方向逐站转发。电力通信传输网，尤其是以光纤通信为主的同步数字体系或者光传送网普遍使用环型结构，双向自愈环最为常见。该结构最大的优点是自愈能力强，当环路上某段光缆断或者某个节点出现故障时，业务流可以自动切换至备用保护通道或反向传输，保证通信不中断。环型结构空间利用率高，适合承载对可靠性要求很高的继电保护、自动化业务。虽然节点增删时所须的配置调整较为繁杂，但其带来的高生存性使其成为电力骨干传输网的首选之一。

树型拓扑结构是星型拓扑结构的扩展与延伸，有明显的层次性，一般由根节点、分支节点、叶节点组成。配电通信网以及用电信息采集系统大多使用树形结构。根节点一般设置在变电站或者汇聚中心，利用分支线路向下辐射的方式与众多配电终端、智能电表等相连。该结构与电力线载波通信或者无源光网络的物理结构高度契合，具有较好的扩展性，可以用较低成本覆盖大面积地理区域。树形结构的层级性使得故障排查方向清晰，但是也继承了对上层的依赖性，即根节点或者主干分支出现故障时，其下属的所有子节点都将失去连接。

（二）网状结构

网状结构，又叫网格结构，是电力通信网中一个非常重要的拓扑形态，其核

心特征就是网络中的各节点之间有多条传输路径,从而形成错综复杂的连接关系。

1. 全网状拓扑是网状结构的一种极端情况,每一个节点都和网络中其它所有的节点直接相连。这种连接方式理论上具有最高的可靠性和冗余度,即使某一个链路或者某个节点出问题了,也能找到其他的路径来通畅地通信,因此不会造成网络中断。核心调度节点或者极其重要的数据中心之间的互联采用全网状结构,可以保证无阻塞的数据交换,时延很低。

2. 但是工程中由于全网状结构的连接数与节点数的平方成正比,布线成本以及设备端口开销都非常昂贵。因此,通常出现部分网状结构。这种折中方案根据实际的业务流量和地理分布,在重要的节点之间建立多条互联,在非重要的节点之间建立单链路或者双链路。既可以保证核心业务生存的能力,又可以有效控制建设成本。

3. 网状结构对路由选择算法、网络控制协议有更高的要求。因为存在多种路径可以选择,网络要在传输过程中选择最好的路径,避开拥塞或者故障的地方。现代电力通信网采用智能光网络、软件定义网络等新技术,就是希望对网状拓扑的流量调度和故障恢复进行更好的管理,从而发挥网状拓扑多路径并行的优点。

(三) 混合型拓扑结构

在现实大型电力通信网络的建设过程中,单一的拓扑结构很难同时满足覆盖范围、可靠性、带宽和成本等各方面的严格限制,于是混合型拓扑结构应运而生,并且已经占据了主流地位。

混合型拓扑结构并不是简单地把各种基本结构拼凑在一起,而是根据分层分区的网络设计理念,把星型、环型、总线型、网状型结构有机地结合在一起。一般电力通信网骨干层采用网状或环型结构,以保证核心业务高速传输和强大自愈能力;接入层或末端配用电环节使用星型或者树型结构,实现广泛覆盖和低成本接入。省级骨干网一般会形成复杂的网状结构,地市级网络一般是由多个相切的环网组成的,而深入到居民小区的用电信息采集网一般呈树型分布。这种组合方式既发挥出各种基础拓扑的优点,又避免了各自的缺点。

混合型结构给网络赋予极大的灵活性以及扩展性。随着智能电网架构的不断发展以及新业务的出现,设计人员可以针对某一地区的特性有目的性地进行拓扑结构调整,不需要对整个电网结构做彻底改造。对地形复杂或者负荷分散的地区来说,有时还会把无线通信技术融合进去,形成灵活的星型发散结构,并且同光

纤环网相互联通。该架构可以适应电力业务点多面广的特点，又能对不同的电压等级、不同的重要程度的站点提供不同的通信保障服务，最终达到技术经济效益的最佳结合。

二、电力通信网拓扑选择原则

（一）可靠性与生存性要求

电力系统对于通信网络的可靠性要求非常高，一旦出现通信中断，很可能会造成电网保护失效，从而引发大范围停电事故。

可靠性是拓扑结构选择的重要原则，即网络结构必须具有抵御各种故障的能力。设计核心骨干网拓扑时一般都按照 N-1 甚至 N-2 的安全标准来进行，即网络中任意一个或者两个节点、链路发生故障时业务仍可以正常运行。这就决定了在关键层面上，只能采用具有多路由迂回能力的环状或网状结构，而不能采用无保护的单链或树状结构。承载继电保护信号的通道，在逻辑拓扑上实现冗余的基础上，物理路由上还要严格执行三路由或者双路由配置，保证物理路径的异构性，从而有效防止因同一地点施工破坏导致主备通道同时失效。

生存性指网络在遭遇地震、冰灾等极端情况发生破坏之后，仍能维持最基本的关键通信服务的能力。拓扑结构的选择一定要考虑到极端环境下脆弱的一面。拿容易遭遇冰灾的高寒山区来说，简单的链型结构很容易因为断线变成“孤岛”，但是多重连接的网状结构可以给网络的生存留下更多的机会。设计者要评价不同的拓扑在节点大规模瘫痪时所能保持的连通度，优先选择那些在网络破碎化的情况下，仍能让某个局部区域内的站点彼此联通的拓扑形式。极端生存能力要求，是电力专用通信网和普通公共网络最明显的一个区别。

（二）成本与可扩展性考量

电力通信网的建设涉及巨大的资金投入与长期的运维支出，经济性评估是拓扑决策中不可或缺的一环。

1. 建设成本主要是光缆铺设费、设备端口购置费和站房建设费等。全网状结构虽然性能优异，但是其线缆长度和端口数量呈指数级增长，对覆盖范围广泛的电力网络来说，要实现全网覆盖是不现实的，也是不必要的。设计者要在性能和造价二者之间找到一个契合点，在非核心区域把环型结构代替网状结构，既保证了通信需求，又大大削减了光缆资源。运维成本也会随着拓扑的复杂程度发生变

化，拓扑越复杂，故障排查起来就越麻烦，需要的人力培训成本也就越高。在保证业务需求的基础上，应该尽可能的简化网络的层次及连接关系。

2. 可扩展性是网络的生命周期和未来发展可能性的度量。伴随着智能电网的发展，新能源站点接入、电动汽车充电桩增多等将会带来新的通信节点需求。拓扑设计要留出足够的扩展接口和容量余量。树型或者星型结构在新增节点时具备天然的优势，只需要在末端新增即可；而环型结构在扩展的时候或许要实施环路拆分或者波道重新配置，操作起来比较繁杂。因此在规划阶段就需要对未来五年到十年的节点增长做出准确的预测，选择容易平滑扩容、不易频繁割接的拓扑结构，以实现投资效益的最大化。

（三）业务流向与流量特征

电力通信网业务流向具有很强的行业特征，与互联网业务无规则的突发访问模式不同，电力业务呈现明显的汇聚型、垂直型流向。

调度自动化、配网自动化、用电信息采集等核心业务的数据流向主要是各末端站点向地调、省调或者数据中心汇聚，即典型的“点对多点”或者“多点对一点”的模式。垂直型流量模型决定网络拓扑必须要有很强的汇聚能力。如果盲目采用扁平化的对等网状结构，会造成核心汇聚节点入度链路过多，造成资源浪费、效率低下。相反地，采取分层分级的汇聚型拓扑结构，比如多级星形、环形加树形等，更符合业务流量走向，层层收敛流量，从而减轻核心层的工作压力。

伴随着能源互联网的发展，变电站间横向的互动业务（站间联锁、区域协同控制）也越来越多。这种业务需要站点间有低时延的直达路径。单纯的树型结构会造成横向流量只能经过上层节点绕行，从而加大了传输时延，加重了骨干链路的压力。因此，在需要频繁进行横向数据交换的区域局部引入网状或者环型互联，可以形成适应混合流向的拓扑结构。根据各种业务对带宽、实时性和并发概率的需求来设计拓扑结构的几何连通性，使得拓扑结构符合实际物理流量的分布特性，是提高网络利用率、消除拥塞瓶颈的根本所在。设计者需要用流量仿真模型来检验不同拓扑下链路负载是否平衡，防止出现某个路径负载很重而其它路径没有利用的情况。

第五节 网络分层模型

一、OSI 七层参考模型

(一) 物理层、数据链路层、网络层

物理层处在参考模型的最下层,是构成通信网络的物理基础,它的主要工作就是实现传输介质上比特流的透明传输。这一层主要研究信号的电气、光学特性以及机械接口规范,比如电压等级、光波长、线缆引脚排列等。电力通信网络中,光纤复合架空地线等特种光缆成为物理层主要的传输介质。用光电转换技术将数字信号调制为光脉冲后再进行传输。物理层不关心比特流代表的具体含义,其主要任务就是保证发送端发出的每一个比特都能被接收端正确识别,从而为上层协议提供可靠的物理连接通道。

数据链路层处在物理层之上,它把不可靠的物理线路转变为逻辑上的无差错数据链路。该层把比特流整理成帧,用帧定界符标明数据的起止之处,采用循环冗余校验之类差错检测码找出传输时可能出错的码字。一旦发现错误,数据链路层就丢弃出错的帧或者要求重新发送。介质访问控制属于数据链路层的功能之一,对共享介质网络来说,需要使用某种算法协调各个节点对信道的访问,防止出现数据冲突的情况。以太网里,物理地址(也就是 MAC 地址)就是在这层定义并加以识别的,保证数据帧能正确地从一个节点传送到相邻的下一个节点。

网络层是通信子网的最高一层,它的主要任务是在复杂的网络结构中做数据包的路由选择和转发。不同于数据链路层只关心相邻节点间的传输,网络层主要实现源主机和目的主机之间端到端的路径选择。它使用 IP 地址这样的逻辑地址来标识网络中的每一个设备,通过路由协议动态地收集网络拓扑信息,找到最优的传输路径。网络发生拥塞的时候,网络层就要实施流量控制策略。对于过大不能直接传输的数据包,还要进行分片和重组来满足各个链路最大传输单元的要求。在跨越不同网络进行通信的时候,网络层起着很重要的作用,它掩盖了底层传输技术的差异。

(二) 传输层、会话层、表示层、应用层

传输层在分层模型中起着承上启下的作用,它是资源子网和通信子网的接口,为上层应用提供端到端的、可靠且与网络无关的数据传输服务。该层用端口号区

分同一台主机上运行的不同应用软件，实现复用和分用的功能。根据业务需求的不同，传输层可以提供面向连接的可靠服务，保证数据不丢失、不乱序；也可以提供无连接的尽力而为服务，满足对实时性要求高、对丢包不敏感的业务需求。流量控制和拥塞控制属于传输层的两种重要机制。流量控制是为了防止发送方速度太快而使接收方的缓冲区溢出，拥塞控制是为了防止网络中存在太多的数据而造成性能下降。

会话层的功能就是建立、管理、终止应用程序之间的会话连接，它是用户进程间对话的协调者。该层可以由通信双方协商确定通信模式，设置同步点，使在出现故障时能从断点处继续传送数据，不需要从头开始。尽管现代互联网协议栈中会话层的功能被应用层协议吸收了，但是在某些分布式系统或者远程过程调用里，独立的会话管理仍然有着重要的意义，它可以保证长时间运行的业务流程状态的一致性和连续性。

表示层主要解决用户信息的语法表示问题，保证一个系统应用层发送的信息能够被另一个系统的应用层正确读取。由于各个计算机系统之间在字符编码、数据格式、浮点数的表示等各个方面都存在着差别，因此需要提供数据转换的服务，例如将 EBCDIC 编码转换为 ASCII 编码。数据加密解密、压缩解压都属于表示层的功能。电力系统中存在大量的敏感信息传输，在表示层上加密可以有效地防止信息的泄露，使用数据压缩可以节省带宽资源，提高传输效率。

应用层是开放系统互连环境的最上层，直接面对用户的应用程序，为应用程序提供网络服务接口。这一层不关心数据传输方式，只关心数据的处理与利用方式，来完成具体的业务逻辑。从文件传输、电子邮件到远程登录等等，应用层协议都给进程间交换信息的格式、时序作出了规定。电力行业应用层包含从 SCADA 系统实时监控数据采集、继电保护信号传输到办公自动化系统日常通信等各个方面的内容，是网络技术和电力业务直接结合的最直接体现。

（三）OSI 模型的理论指导意义

尽管 OSI 七层模型在实际网络部署中显得过于繁琐，并且某些功能在不同的层次间有重复之处，但是它所具有的理论指导意义却是无法估量的。它依靠严格的分层思想，把复杂的网络通信问题分解成七个相对简单的子问题，使网络协议的设计、分析、教学有章可循。

1. 该模型定义了各层功能边界和服务原语，给不同厂商设备之间互操作性提

供理论基础，从而利于开放系统的形成。

2. 即使后来占据主导地位的 TCP/IP 模型在描述物理层和数据链路层功能的时候，大量借用 OSI 模型的术语和概念。

3. 在故障排查以及网络优化的时候，OSI 模型给予了明晰的逻辑步骤，工程师可以从物理层入手，依照层次逐层排查，效率非常高。

二、TCP/IP 四层 / 五层模型

（一）网络接口层、网络层、传输层、应用层

网络接口层对应的是 OSI 模型的物理层和数据链路层，在 TCP/IP 模型中，它主要处理和物理传输介质有关的所有内容。TCP/IP 这一层并没有规定具体采用什么样的硬件标准，但它支持目前所有的网络标准，包括以太网、令牌环、光纤分布式数据接口、各种无线通信标准等。其主要功能就是接收上层 IP 数据包，把它们封装成特定网络技术所要求的帧格式，再通过物理线路发出去；反之，它从线路上接收到帧，剥掉帧头、帧尾，再把数据上交给网络层。IP 网络对底层技术具有很强的包容性，可以工作在各种传输媒体上。

网络层在 TCP/IP 协议栈中处于核心地位，它的名称中包含“互联网协议”这四个字就表明该层起到实现异构网络互联互通的作用。它使用无连接的数据报服务方式，每个数据包分别路由，不保证到达顺序，也不保证不丢失。这种方式大大减轻了网络设备的工作负担，可以专心高速转发。网络层给整个网络分配唯一的 IP 地址，使全球的设备可以互相寻址。路由器属于网络层设备，依照 IP 包头里的目的地址，查询路由表来找出下一跳路径，于是就形成了互联网那庞大的网状骨架。

TCP/IP 模型中传输层也承担端到端通信的任务，它主要依靠两个性质完全不同的协议来完成这项工作，即传输控制协议和用户数据报协议。传输层处于网络层之上，它使用网络层提供的不可靠服务，为应用层提供需要的通信质量保证。它给应用程序供应套接字接口，把底层网络的繁杂之处隐藏起来，让程序员可以像读写文件那样开展网络编程。无论是网页浏览所需要的可靠流传输，还是视频会议所需要的实时数据报传输，传输层都能给出相应的解决方案。

TCP/IP 模型中应用层除了具有 OSI 模型中应用层的功能之外，还包含着表示层、会话层一部分的功能。由于大部分互联网应用不需要独立的会话管理或者

复杂的语法转换，扁平化的设计可以降低处理开销、提高通信效率。常见的应用层协议如 HTTP、FTP、SMTP 等，都是直接使用在传输层之上的。电力通信中以 IP 为载体的应用层协议正在逐渐代替传统通信规约，使业务系统更趋于标准和开放。

（二）TCP/IP 协议栈核心协议

TCP/IP 不是单一的协议，而是一个协议族，其中 IP 协议和 TCP 协议无疑是最重要的两个协议。IP 协议规定了数据包的格式，包括版本号、首部长度的、服务类型、总长度等等主要部分，同时还要有源地址和目的地址。并且规定了分片重组的手段，用以适应各种 MTU 的网络。为了配合 IP 协议，互联网控制消息协议 ICMP 用于在主机和路由器之间传递控制信息，网络不可达、主机不可达、回显请求等都是其中类型，是网络诊断的有力工具。地址解析协议解决的是将 IP 地址映射到物理 MAC 地址的过程，可以使得逻辑寻址过程能通过物理层进行实际的传送。

传输控制协议是面向连接、可靠的数据传输协议，它是一种字节流传输协议。它靠“三次握手”来创建联系，保证双方都已就绪；靠序列号和确认应答，保证数据无差错、有序到达；靠滑动窗口做流量控制，按照接收方的接收能力灵活调节发送速度；靠慢启动、拥塞避免这些拥塞控制算法，感知网络是否拥堵，主动减慢发送速度，保证网络稳定。与此相反，用户数据报协议是一种不可靠的、面向数据报的、更简单的协议。它没有重传、排序机制，头部开销小，因此很适合对实时性要求高、能容忍少量丢包的电力自动化业务，比如同步相量测量数据的传输。

（三）TCP/IP 模型的广泛应用

TCP/IP 模型取得巨大成功，就在于它强大的适应性以及可扩展性。它既形成了世界上最大的互联网络，又全面地改变了各个行业的通信手段。它与 OSI 模型的主要对应关系和功能概述见下表。

OSI 与 TCP/IP 模型对比及功能概述表

层级	OSI 七层模型	TCP/IP 四 / 五层模型	主要功能
第 7 层	应用层	应用层	为用户应用程序提供网络服务，实现特定业务逻辑
第 6 层	表示层	(部分融合)	数据格式转换、加密解密、压缩解压
第 5 层	会话层	(部分融合)	建立、管理和终止会话连接，同步数据
第 4 层	传输层	传输层	端到端的数据传输服务，流量控制与拥塞控制
第 3 层	网络层	网络层	路由选择、数据包转发、逻辑寻址
第 2 层	数据链路层	网络接口层	将物理线路变为无差错链路，帧处理、MAC 寻址
第 1 层	物理层	网络接口层	传输比特流，定义电气、光学和机械特性

在电力系统中，伴随智能电网建设进程的加快，通信网络正加速向 IP 化方向转变。

1. 从调度中心生产管理系统到变电站内综合自动化系统，TCP/IP 协议已经成为主要的通信语言。
2. 以 IP 为依托的统一通信平台建立之后，电力企业可以承载数据、语音、视频等各种业务，从而大幅降低网络建设及运维成本。
3. 利用 IP 网络天然的路由灵活性及自愈特性，可以建构出可靠的电力通信骨干网。当某条链路出现故障的时候，路由协议可以迅速收敛，自动切换到备用路径，保证控制指令能够连续地下达到控制终端。

三、电力通信网的分层实现

(一) 电力通信网对分层模型的映射

电力通信网的物理层一般是由坚强的光传输网络组成。光纤复合架空地线、全介质自承式光缆都是利用高压输电线路塔架的资源来搭建物理传输网络。该层使用同步数字体系和光传送网技术，带宽容量大，硬件倒换保护速度快，可以对原始光信号进行数字化比特流的处理。利用物理层有效的补充，即采用配电网末端用载波通信和无线专网作为接入最后 1 公里的方式。

在电力通信中，数据链路层和网络层的融合倾向比较突出，尤其 MPLS 技术出现之后更加明显。骨干传输网络上一般会建立基于 SDH/MSTP 或者 PTN/IP-MPLS 的逻辑网络。对实时性要求极高的生产控制大区业务一般映射到二层网络服务上，用虚电路或隧道技术建立点对点的刚性通道，以减少路由查找造成的时

间抖动。但是管理信息大区的业务更多时候是映射到三层 IP 网络，采用动态路由实现灵活的互联互通和资源共享。不同的映射策略，保障了重要的业务在网络拥塞的时候有确定的传输保证。

应用层是电力通信网最富特色的部分。这里运行着 IEC 61850、IEC 60870-5-104、DL/T 634 等电力专用规约。这些规约在标准的应用层之上，还要定义一些特定的应用服务元素及对象模型来描述断路器、变压器等电力设备的属性和操作。IEC 61850 标准利用抽象通信服务接口，把具体的通信映射与抽象的业务逻辑相分离，从而使变电站自动化系统可以脱离底层网络技术独立发展，充分体现了高超的分层设计智慧。

（二）各层关键协议与技术选型

电力通信网的物理层和数据链路层一般会选取确定性时延的技术。虽然以太网成本低、带宽高，但是它的传统冲突检测和退避机制不能满足继电保护的时间同步需求。因此电力通信网使用了工业以太网、同步以太网等增强型技术。采用高精度时钟同步协议以及流量整形手段之后，以太网就具备了硬实时性。为了进一步增加链路的可靠性，链路层大多使用环网保护协议，在链路出现故障以后 50 毫秒之内可以完成自愈。

网络层和传输层上的 IPv6 技术已经开始使用。随着智能电表、分布式电源等大量的终端接入，IPv4 地址枯竭问题越来越严重。IPv6 不但可以提供几乎无限的地址空间，而且通过流标签等手段加强了服务质量的管理，非常适合智能电网的差异化服务需求。在选择传输层协议时，遥测、遥信这类周期性上报的数据一般使用 UDP 协议来降低开销，遥控、遥调这类重要的指令完全依靠 TCP 协议的可靠传输机制。为了抵御网络攻击，还会使用 IPSec 等安全协议创建加密隧道，来保证调度数据网中控制指令不被篡改。

应用层协议选择主要看互操作性和可扩展性。制造报文规范曾经是电力自动化的主要应用层协议，但是由于它的复杂性，已经被更加现代的架构所取代。目前以 Web 服务为主的面向服务架构已经应用在电力信息集成领域，用 XML、SOAP 等标准技术来实现异构系统之间的数据交换。变电站内部，通用变电站对象事件和采样值协议直接映射到以太网链路层，跳过网络层和传输层，用最简单的协议栈完成保护跳闸信号的极速传输，这就是电力通信对标准分层模型的大胆优化。

（三）分层模型的简化与定制

电力通信网对于分层模型的简化，主要是实时性要求非常高的情况。标准的七层或者五层模型功能虽然齐全，但是每一层的封装、解封装都会带来额外处理时延。智能变电站继电保护中，因为要控制故障切除时间在毫秒以内，通信协议栈被大量压缩。像 IEC 61850 里的 GOOSE 报文就不使用 TCP/IP 协议栈，而是把应用数据直接打包到以太网帧里进行发送。虽然“跨层设计”牺牲了一定的路由灵活性，但是得到了极致的传输速度，完全符合电力系统“安全第一”的基本原则。

定制化表现在管理平面的独立创建上。通用分层模型一般只考虑数据平面传输，电力通信网建立独立同步网和网管网。同步网给各个层次的设备提供统一的高精度时钟基准，这是 SDH、TDM 业务正常工作的前提。网管网通过使用 SNMP 等协议来采集各层设备的资料，来实现对于整个网络进行监控与调度。带外管理的设计使运维人员可以远程诊断故障、恢复网络，即使在业务网络瘫痪的时候也可以对通信网络进行有效的管理。

对标准分层模型进行灵活剪裁并加以功能增强，就得到了电力通信网的一种高效架构。这种架构既开放标准又有自己的行业特点。既保证了目前庞大电网的安全稳定运行，也给未来能源互联网中大量微网的接入、源网荷储的协同配合留有足够多的发展空间。

第五章 电力通信协议体系

第一节 通信协议基础

一、协议的概念与要素

（一）语法、语义与时序

通信协议的内部构造可解构为三个基本维度，它们共同定义了信息交互的完整范式。

1. 语法规定了通信数据的形式和编码，就像语言文法一样，规定了信号电平、数据块格式和物理传输特性。电力通信当中，语法表明了比特流怎样形成帧、包或者报文，保证接收方可以正确地把物理信号所承载的数字信息解析出来。

2. 语义是对信息以及错误处理的解释，也就是“说什么”。它规定何时发出何种控制信号，执行何种动作，作出何种反应。调度指令传输时，语义使二进制序列成为断路器合闸指令或者系统故障报警，给数据流赋予了实际的业务价值。

3. 时序主要解决通信双方速度同步以及事件顺序的问题，也就是“什么时候说”。它对事件发生次序以及速度匹配作出规定，保证发送方与接收方时间轴一致。电网保护业务中时序特别重要，毫秒级的误差也会造成保护装置误动作或拒动作，所以协议要具备严格的时间同步和序列控制能力。

（二）协议的分层思想

由于电力通信网络业务日趋复杂以及硬件环境异构化，单一的、大一统协议已不能满足日益复杂的要求，分层思想随之出现。通过将复杂的通信过程分成几个独立的层次，每一层只做一项工作，给上层提供标准的服务，把下层实现的细节隐藏起来。模块化设计的思想使系统具有很强的灵活性和扩展性。当某一层的某项技术发生革新的时候，只要它对外接口保持不变，就不会影响其他层次的正常运行，对生命周期较长的电力基础设施来说十分重要。

分层结构可以使不同网络的设备相互配合。物理层传输比特流，链路层完成相邻节点之间的可靠传输，网络层解决路由寻址问题，传输层和应用层分别完成

端到端的连接以及业务逻辑。这样各司其职的架构既可以兼容传统的串行通信设备，又可以与最新的光网络技术、无线传感网络无缝对接，形成一条又宽又韧的信息高速公路。

（三）协议数据单元与服务数据单元

在分层协议体系当中，数据的传递并不是简单的搬运，而是不断进行封装和解封装的动态过程，这个过程是通过协议数据单元和服务数据单元之间的传递实现的。服务数据单元将上层逻辑所传递的净荷信息传给下层。第 $N+1$ 层将服务数据单元传给第 N 层时，第 N 层认为它是待传输的数据实体，而不管它的内容。

为了完成传输任务，第 N 层在服务数据单元上加上本层控制信息，两者合称第 N 层协议数据单元。就像包裹的层层包装，每层都把自己封装了一层标签以及控制指令。数据到达接收端的时候，过程正好相反，各层剥离对应的头部信息，把还原后的服务数据单元逐层向上提交。因此各个协议层之间互不干扰，各自运行自己的协议逻辑，从而可以有条不紊地组织和拆解复杂通信中的各个处理环节。

二、协议的分类与功能

（一）面向连接与无连接协议

根据数据传输前是否需要建立逻辑通路，通信协议可以分为面向连接和无连接两种，这两种通信方式在电力业务中都有广泛的应用。面向连接的协议在数据传输之前，首先要经过建立连接、数据传送、释放连接这三个阶段。这种方式就像是拨打电话一样，通信双方在整个交互过程中一直存在着逻辑上的联系。最大的优势就是可以预先给数据流预留资源，提供更好的服务质量，特别适合对于时延抖动敏感并且持续时间较长的业务，调度电话、视频会议系统等。

无连接协议相当于传统的邮寄服务，每个数据包都带有完整的地址信息，在网络中独立寻径到达目的地。发送方不需要和接收方先握手，数据包的发送是突发的、即时的。这种机制极大地降低了通信建立的时延和开销，很灵活且鲁棒。在智能电网配电自动化场合中，大多数状态监测数据都是短小、偶发的，无连接协议可以很好地利用零散的小批量数据，减少了频繁建立连接带来的开销，从而提高了带宽利用率。

（二）可靠与不可靠协议

根据对数据交付是否进行确认，协议可以分为可靠协议和不可靠协议，直接决定了业务数据的安全性和实时性之间的平衡。可靠协议依靠确认机制，超时重传，流量控制等方法，保证数据无差错，不丢失，不重复，按序到达。在电网计费信息、继电保护定值修改等重要业务中，数据的准确性非常重要，一个比特的错误就会造成严重的经济损失或安全事故，因此需要使用可靠的协议，即使牺牲一定的传输效率也要保证数据的完整性。

但是不可靠协议也有其特殊的作用。此类协议只提供尽力而为的服务，不保证数据一定送达，也不做复杂的错误恢复。看起来存在一定的风险，但在实时变电站视频监控、高频采样同步相量测量等场合中，最新的数据比陈旧但是准确的数据更有价值。如果因为纠正上一帧错误而导致下一帧画面停滞，就会影响画面的连续性。不可靠协议去掉了繁琐的确认步骤，提高数据吞吐量和实时响应速度，满足海量流媒体传输的需求。

通信协议的常见分类及其特点，可参考下表：

电力通信协议常见分类与特性表

分类维度	协议类型	连接机制	可靠性保障	主要特点	典型应用场景
连接模式	面向连接协议	数据传输前需建立逻辑连接，维护状态。	较高	资源预留，服务质量可控，适合持续性传输。	调度电话、视频会议、文件传输
	无连接协议	每个数据包独立寻径，无需事先建立连接。	较低（尽力而为）	灵活高效，开销小，适合突发性、零散数据。	智能电网状态监测数据、配电自动化遥信
数据交付	可靠协议	采用确认、重传、流量控制等机制。	极高	保证数据无差错、不丢失、不重复、按序抵达。	电网计费信息、继电保护定值修改、远程控制
	不可靠协议	尽力而为传输，不保证送达，无复杂错误恢复。	较低	吞吐量大，实时性强，开销低。	实时视频监控、高频采样同步相量测量

（三）协议在通信过程中的作用

协议在通信的全过程中既是规则的执行者又是秩序的维护者，它在信息从产生源端到消费宿端的过程中一直存在。

1. 建立通信双方的握手。数据交换开始之前，协议利用特定的信令交换来协

商双方的通信参数，即缓冲区大小、最大报文长度、加密算法等，以保证双方处于兼容的工作状态。

2. 监控协议数据传输的完整性以及安全性。协议在传输过程中不断对流经的数据进行校验，一旦发现由于传输介质的噪声干扰造成的误码，就立即启动纠错算法或者重传请求，从而建立起抵御物理层干扰的逻辑防线。

3. 管理网络资源分配和释放。通信任务结束后依照规则关闭连接、释放占用的资源，防止网络拥塞。

经过这些细密而有力的控制，通信协议就把一团乱麻的物理信号变成了一条条有条不紊、容易明白的业务信息，于是庞大的电力系统神经中枢就能这样运转起来。

第二节 电力专用协议

一、远动通信协议

（一）IEC 60870-5 系列标准

IEC 60870-5 系列标准对电力系统的远动控制做了规定，主要应用于调度中心和变电站、发电厂之间。该系列标准定义了一个分层参考模型的通信体系，重点对物理层、链路层、应用层和用户进程做了规定。实际工程中使用最多的是 IEC 60870-5-101 和 IEC 60870-5-104。101 标准主要用在低速串行链路上，采用非平衡传输方式，在噪声干扰较大的模拟信道上，数据的完整性依靠严格的帧格式校验和重传来保证。

随着电力通信网光纤化、IP 化的快速发展，IEC 60870-5-104 标准也随之产生。它把 101 标准应用层的数据单元用 TCP/IP 协议包进行封装，利用以太网高带宽的优势来实现数据高速吞吐。104 协议简化了通道的配置，加入了流量控制、超时控制，使广域网通信效率大大提高。在应用服务数据单元 ASDU 设计上，该协议具有很强的灵活性，可以设计单点信息、双点信息、测量值、带时标事件记录等各种信息对象来满足电网实时监控的精细化需求。

为了保证不同厂商的设备可以相互配合，该系列标准还给出了互操作性表，要求设备制造商标明所支持的功能选项。该种设计理念很好地消除了由于不同的

实现所造成的通信障碍，使得异构系统之间的集成更为顺畅。早期版本的协议安全性比较差，在后续的更新中，添加了 IEC 60870-5-104 安全扩展来弥补身份认证、数据加密等各方面的缺陷。

（二）IEC 61850 标准体系

IEC 61850 标准体系是变电站自动化技术的一次飞跃，它不单是通信协议，还提出了一套变电站配置语言 SCL 和抽象通信服务接口 ACSI。本标准用面向对象的建模技术把变电站的一次设备、二次设备抽象成逻辑节点，用数据对象、数据属性来表达设备行为和状态。自我描述能力使智能电子设备 IED 之间可以实现“即插即用”的互操作，消除了传统私有协议造成的各个自动化孤岛。

IEC 61850 中引入了面向通用对象的变电站事件 GOOSE 以及采样值 SV 传送方式：

1. GOOSE 机制：专为满足保护跳闸等关键业务的毫秒级时间要求而设计。它跳过 TCP/IP 协议栈的繁琐处理，直接映射到以太网链路层，采用多播发布、订阅方式，保证闭锁、启动、跳闸信号的快速可靠传输，同时还具备心跳检测功能，可以实时监测链路状态。

2. SV 采样值传输：实现了电子式互感器输出的数字化。传统的模拟电压电流信号被转换成高精度的数字采样流，通过过程层网络共享给测控、保护、计量装置，大大简化了二次回路接线，解决了传统互感器饱和、绝缘等问题。

该标准将变电站通信网络分为站控层、间隔层、过程层，利用制造报文规范 MMS 实现站控层和间隔层之间非实时数据交换，例如定值修改、录波文件调阅等。IEC 61850 的推行不但改善了变电站的结构，也促使智能电网向数字化、网络化方向发展，目前已经向配电网、发电厂扩展。

（三）DNP3.0 协议

分布式网络协议 DNP3.0 起源于北美，专门为 SCADA 系统设计的开放性通信协议，很适合于要求数据传输可靠、环境恶劣的地方。DNP3.0 采用增强性能架构 EPA 模型，简化了 OSI 七层模型，只保留了物理层、数据链路层和应用层，增加了一个伪传输层。DNP3.0 的一个特点是伪传输层，它可以对长报文进行分片重组，从而使得协议能够适应各种长度限制的底层传输通道，无论是无线电台还是光纤网络都游刃有余。

该协议在数据链路层采用了严格的 CRC 校验和确认机制，支持点对点、多

点共线、分层网络等不同的通信模式。DNP3.0 支持轮询和主动上报两种数据获取方式，提出了“类”的数据概念，按照数据变化的频率以及重要程度把数据划分成不同的等级，使主站优先得到重要的变位信息，从而节约宝贵的带宽资源。DNP3.0 为了保障电力系统控制操作的安全，使用了选择、操作两步控制的模式来避免误操作。内建的安全认证功能利用挑战 / 响应机制来验证主站和子站的身份，给关键基础设施提供了必要的安全屏障。

常用电力远动通信协议对比

特性	IEC 60870-5-101	IEC 60870-5-104	IEC 61850	DNP3.0
应用场景	低速串行链路远动	IP 网络远动	变电站内自动化	SCADA 系统，恶劣环境
传输介质	串行口	以太网	以太网	各种（伪传输层）
协议栈	分层模型	TCP/IP 封装 101 应用层	自定义，面向对象	简化 OSI，伪传输层
主要特点	简单、可靠性高	高带宽、流量控制	互操作、即插即用、GOOSE/SV	可靠性强、分片重组、类数据
安全性	早期版本较弱，后有安全扩展	早期版本较弱，后有安全扩展	早期版本较弱，后有安全扩展	内置安全认证
主要缺陷	传输速率低，不适应 IP 化	对传统 101 升级，灵活性一般	复杂，初期实施成本高	协议较重，适用于特定场景

从上表可以看出，不同的远动通信协议各有侧重，以满足电力系统多样化的应用需求。

二、电力信息管理协议

（一）电力负荷管理协议

电力负荷管理协议主要是连接负荷管理主站和终端设备，用来监测和控制用户用电负荷，属于需求侧管理的重要技术手段。本协议设计之初就考虑到广域覆盖的通信需求，支持 230MHz 无线专网、GPRS/CDMA 公网、光纤等通信方式。协议中对远距离指令帧做了规定，帧起始符、控制域、地址域、链路用户数据、帧校验序列。

从业务功能上看，除了可以对功率、电量、电压等常规遥测数据进行上传外，还具有很强的控制逻辑。主站通过协议下发功率定值、电量定值或者直接的跳闸控制指令，终端收到指令后会做严格的权限验证和逻辑判断。为了应对日趋严重

的信息安全问题，现代负荷管理协议在应用层上加入了密码算法，给重要的控制报文和参数设置报文加上了加密，用消息认证码 MAC 来验证，以防止攻击者篡改指令或者非法控制用户的负荷。

该协议还有透明转发的功能，主站可以利用负荷管理终端和下端通道相接的电表来进行通讯。此设计大大扩大了系统覆盖面，使负荷管理系统在一定程度上具备了电能信息采集功能，从而达到投资效益最大化的目的。并且协议本身具备较好的事件记录和主动上报功能，当终端出现过负荷、篡改接线、设备故障等异常情况时，能通过突发传输方式向主站发出告警。

（二）电能信息采集与管理系统协议

电能信息采集和管理系统协议是智能电网“最后一公里”的数据桥梁，主要是规定采集主站、集中器、采集器、智能电表之间的通信行为。该领域的标准体系比较复杂，分为上行通信主站到集中器和下行通信集中器到电表两部分。上行通信协议一般为 TCP/IP 或者 UDP，根据 Q/GDW1376.1 标准使用面向连接的通信方式，具有心跳保持、断点续传等功能，可以保证大量的计量数据完整的上传到数据中心。

下行通信协议更多的是考虑物理层的多样性、低功耗，如电力线载波、微功率无线等。协议在应用层对数据标识 DI 做了丰富的多种编码，用树形结构对电能、需量、瞬时量、冻结量等各种数据进行了准确的编码。

1. 数据冻结，协议中的一大亮点，有日冻结、月冻结、整点冻结等模式。所有的终端同时锁定数据，实现全网电量统计的同时性，给线损分析提供准确的数据。

2. 事件上报和费控交互，协议中对于电表失压、断相、开盖等异常事件编码上报有规定。支持远程充值、参数下发、余额报警功能，实行先付费后用电的现代管理方式。

该类协议具有较强的通信并发处理能力以及自适应组网能力，在低压电力线载波通信中支持自动中继、路由发现，可以对低压台区线路阻抗变化大、噪声干扰强的情况做出动态响应，保证抄表成功率。

（三）电力企业内部信息系统接口协议

电力企业内部信息系统接口协议，就是冲破调度、生产、营销等部门之间形成的信息孤岛，做到企业内部的大融合。该领域核心就是根据 IEC 61968/61970

系列标准定义的通用信息模型 CIM。CIM 给各个厂家 EMS、DMS、GIS 系统提供了一个抽象的、与实现无关的语义模型，统一了全网络设备、拓扑、量测数据的命名规则及类继承关系，使得各个厂家系统可以理解彼此的数据含义。

电力企业为了实现系统之间松耦合的集成，大多采用企业服务总线 ESB。接口协议采用 XML、RDF 等标准格式打包数据，通过 Web Services 或者 JMS 消息中间件进行传输。因此各个业务系统可以采用发布者 / 订阅者或者请求者 / 响应者的方式灵活交换信息：营销系统能实时获得调度系统的停电计划，从而精准通知受影响用户；生产管理系统可以从资产管理系统获取设备台账，辅助检修决策。

SVG 普遍用作图形数据交换的标准载体，和 CIM/G 标准相结合实现电网接线图在各个系统之间无损转换。这就避免了以前人工反复画图的麻烦，保证了各个系统视图一致。接口协议的落实，给电力企业创建起了数据中台底座，给大数据分析以及人工智能的运用赋予了标准的数据养料。

三、新兴业务相关协议

（一）电动汽车充电通信协议

电动汽车充电通信协议是新能源汽车与充电桩供电设备之间的桥梁，它影响到新能源汽车的充电安全和计费准确性。以 GB/T 27930 为代表的标准体系，规定了基于 CAN 总线的物理层与数据链路层，也给出了详细的应用层报文定义。充电时车辆电池管理系统 BMS 和充电机之间要频繁地交换高频次的数据，协议把充电过程分成握手阶段、参数设置阶段、充电阶段、充电结束阶段。

握手和配置阶段双方交换版本信息、电池类型、额定容量、最高允许电压等重要参数来保证硬件匹配。充电阶段中 BMS 把电池的电压、电流、温度和 SOC 的需要信息传递给充电机，充电机按需求来调整输出功率并反馈自己所对应的状态。协议中设置了严格的超时判定及错误处理逻辑，如果出现通信中断或者数据异常，充电装置在毫秒级之内就会切断输出以防止电池过充或者热失控。

除了底层的控制交互之外，上层的运营管理协议也越来越重要。充电桩按照开放充电协议 OCPP 等标准，同云端运营平台交换用户鉴权信息、计量计费数据和设备状态的心跳。分层结构保证充电设施能够安全进行物理充电，也可以接入物联网生态系统提供扫码充电、即插即充等服务。

（二）分布式能源并网通信协议

分布式能源并网通信协议主要是解决光伏、风电等分散电源接入配电网之后，对分布式能源的可观测、可测量、可控问题。该类协议一般由逆变器通信协议和并网调度协议两部分组成。设备层利用 Modbus TCP、SunSpec 等协议从逆变器中获得发电功率、电压、频率和故障码等各种信息。这些协议结构简单，成本低，可以嵌入到各种微型控制器当中。

为适应高渗透率分布式电源给电网稳定带来的影响，在并网交互上使用 IEEE 1547 以及 IEC 61850-7-420 等高级标准，支持：

1. 有功 / 无功调节：协议允许调度主站给分布式电源下发有功缩减或者无功支持指令，使分布式电源参与电网调峰调频。

2. 孤岛检测与保护：依靠快速的信息交流，协议保证电网出现故障时，分布式电源可以正确地判断出孤岛的情况，并按照事先制定的规则解列或者继续工作，保证维修人员的安全和部分地区的供电稳定。

该类协议正向着具有即插即用特点的方向发展，利用 Web 服务技术，分布式电源接入网络后会自动向管理系统注册自己的能力参数，大大降低了运维的复杂性。

（三）智能用电家居交互协议

智能用电家居交互协议把智能电网和家庭内部用电设备之间隔开的“最后一米”联系起来，成为居民侧需求响应的重要技术基础。该领域协议种类繁多，有 ZigBee Smart Energy、Wi-Fi、蓝牙 Mesh、电力线载波通信等。由于 ZigBee Smart Energy 具有低功耗、自组网的特点，所以在家庭能源管理系统 HEMS 中占据着很重要的地位。它定义了计量、计费、文本消息、负载控制等功能簇，使智能插座、温控器、家用电器可以与智能电表或者能源网关进行加密通信。

智能能源规范 SEP 2.0 又将协议 IP 化了，用 IPv6 技术使各种物理介质之间可以互相连接互通。协议支持复杂的定价方式，比如分时电价 TOU、实时电价 RTP、尖峰电价 CPP。电网公司经由协议向用户家庭发送即时电价信号或者紧急削峰指令，智能家电接收到指令之后，依照用户的预设策略自动改变运行模式，电价较高时，自动提升空调设定温度或者停止洗衣机工作。

开放自动需求响应 OpenADR 协议更多的用在电网和工商业、大型社区网关之间。采用标准客户端和服务端结构，对需求响应事件发布、确认作出规定。因

此被动家庭负荷就转变成可以灵活调节的柔性资源，既降低了用户用能成本，又提高了电网削峰填谷的能力。

第三节 国际标准协议

一、工业控制与以太网协议

随着工业自动化技术同信息通信技术的深入融合，工业以太网慢慢取代了传统的现场总线，成为电力工业控制领域里的主要通信手段。电网控制系统在保证高实时性、高可靠性的前提下，也获得了更宽的带宽以及更强的扩展性。工业控制协议采用以太网设计，其特别之处在于很好地解决了标准以太网存在的确定性及抗干扰问题，可以满足变电站自动化、配电网控制等高要求环境下的需求。

工业控制协议概述

协议名称	通信模式	核心优势
Modbus	主从式	开放性、简单、通用性强、成本低
PROFINET	实时以太网	强实时性（微秒级）、高可靠性、灵活拓扑
EtherNet/IP	生产者 / 消费者	兼容商用以太网硬件、高效带宽利用

（一）Modbus 协议族

Modbus 协议从诞生之日起，就因为其开放性、简单性以及广泛的适用性，在工业通信领域成为了一种通用语言。该协议采用主从式通信结构，网络中每个从节点都用唯一的设备地址来标识，主节点通过发送查询命令来读取或者写入从节点的数据。电力系统中 Modbus 被广泛用作智能仪表、可编程逻辑控制器以及各种传感器状态监测与参数设定。其数据模型，采用寄存器和线圈，可以正确的将电力设备的开关状态和模拟量数值进行映射。

Modbus 协议族有多种变体，可以适应不同的传输介质和应用场合。Modbus RTU 模式使用紧凑的二进制形式，数据传输效率高，主要用在串行链路通信上。尤其在带宽有限的传统的变电站二次设备中，仍然发挥着举足轻重的作用。Modbus TCP 模式把 Modbus 报文放到 TCP/IP 数据包里，用以太网的高速传输特性，使控制层和信息层顺利连接起来。虽然 Modbus TCP 的实时性比一些专用工业以太网协议要差，但是由于它在变电站辅助系统监控、配电终端数据采集等应用中表现出的性价比高、兼容性好等特点，它已经成为一个颇具吸引力的选择。

Modbus 协议本身就存在一些先天的安全缺陷。早期版本没有认证和加密,数据很容易被篡改或者遭受重放攻击。现代电力通信网络构建时,工程师们一般采用叠加虚拟专用网隧道、增设防火墙规则或者使用具有安全扩展功能的新的 Modbus 版本等方式来弥补上述不足,保证控制指令的真实性及完整性。

(二) PROFINET 协议

PROFINET 是一种基于工业以太网的自动化标准,具有很强的实时通信能力,在电力自动化领域中也有着广泛的应用。协议用不同的通信通道来实现多样化业务的需求。非实时数据采用标准的 TCP/IP 通道进行传输,保证与办公网络的互通性;继电保护跳闸指令、同步相量测量等对时延要求非常高的业务,则使用 PROFINET 的实时、等时同步实时通信机制。该机制很好地规避了标准以太网协议栈繁琐的处理流程,在链路层就完成了数据交换,取得了微秒级的同步精度,传输抖动较小。

智能变电站内部不仅可以用 PROFINET 协议来完成设备之间周期性的数据交换,而且具有很强的设备描述和诊断功能。工程师可以利用 GSD 文件方便地集成不同厂家智能电子设备来快速配置和调试系统。PROFINET 协议为模块化的,可以采用一根网线同时传输工业实时数据和标准以太网数据,极大地减少变电站的布线工作量,降低建设及维护的成本。

PROFINET 的另一个优势就是网络拓扑结构的灵活性。它支持线型、星型、树型、环型等许多种网络结构。使用介质冗余协议,PROFINET 可以在毫秒级的时间内完成故障的恢复,并且自动地恢复正常的工作,这对电力生产系统所要求的高可靠性来说十分重要。如上表工业控制协议概述所示,PROFINET 的实时性、可靠性最好。

(三) EtherNet/IP 协议

EtherNet/IP 协议是通用工业协议在以太网上的具体实现,把应用层的通用工业协议封装到标准的 TCP/IP 和以太网帧中。因此 EtherNet/IP 可以充分利用已有的商用以太网硬件,即交换机、路由器、线缆等,大大降低了电力通信网络的硬件部署成本。电力系统中的 EtherNet/IP 常用于发电厂辅助车间的控制、分布式能源接入和配网自动化中对实时性要求不高的地方。

该协议最大的一个特点就是使用了生产者/消费者模型,与传统上用源/目的模型不同。在该模型中,数据源即生产者将数据广播到网络中,所有需要这些

数据的节点即消费者都可以直接接收到，生产者不需要逐个向每个消费者发送数据。该机制大大提高了带宽利用率，在多点协同控制的复杂电力应用场景下能有效减少网络拥塞，从而提高整个系统的响应速度。

1. 通用工业协议为 EtherNet/IP 提供丰富的对象库和服务集，使电力设备可以以标准对象的形式在网络中表示出来，极大地方便了参数设置、故障诊断、状态监测。

2. 通过有效区分显式消息和隐式消息，EtherNet/IP 能对非实时性的配置、调试信息加以管理，又能有效地传输实时的输入输出控制信息，可以针对电力生产过程的各种不同的业务需求来进行相应的通信操作。

二、通用网络与传输协议

（一）TCP/IP 协议簇

TCP/IP 协议簇是现代通信网络的通用语言，分层结构给电力通信网络的异构融合打下了坚实的基础。电力数据网络当中，IP 协议担当着数据包在网络拓扑里寻址、路由的任务，从而保证调度指令以及电能量数据可以穿过若干个子网，到达指定的目的地址。不管使用光纤专网、无线公网还是电力线载波通信，TCP/IP 都可以通过适配层技术隐藏不同的物理层之间存在的差别，给上层应用程序提供一致的通信接口。

由于传输控制协议具有面向连接和传输可靠的特点，所以它被用作电力营销系统、计费数据传输和重要文件交换的首选。通过三次握手建立连接，并使用序列号确认、重传机制来保证每一个比特的电力数据都能够准确无误地传送。即便在网络出现拥塞或者链路不稳定的状况下，传输控制协议所采用的滑动窗口流量控制以及拥塞避免算法，也会对发送速度实施动态的调节，从而保证连接的稳定，不至于对电费结算以及历史数据的存档产生不良影响。

用户数据报协议在电力通信网络中除上述业务外，还有不可替代的作用。变电站视频监控、语音调度、高频采样数据流等业务，实时性要求比数据传输的绝对完整性要高得多。用户数据报协议省去了连接建立和确认等复杂的流程，用最小的数据包头来传送数据。尽力而为的传输方式最大程度地减小了传输时延，调度员可以及时得到现场的视听信息。虽然偶尔出现丢包是可以接受的，但是它所带来的低时延对于指挥决策来说是至关重要的。

（二）SNMP 网络管理协议

随着电力通信网络规模的不断扩大、网络设备数量的急剧增加，传统的依靠人工巡检、分散管理的运维模式已经不能满足不断增长的运维需求。SNMP 网络管理协议应运而生，它提供了一种系统化的方法来监控和管理网络中的各种设备，即路由器、交换机、服务器以及支持 SNMP 的电力专用通信设备。管理站通过发送 Get、Set 等操作原语，和运行在设备上的代理程序交换信息，达到查询设备状态、修改设备参数的目的。

管理信息库是 SNMP 的核心部分，用层次结构和属性对被管理的对象进行详细的描述。电力通信网络当中，各个设备厂商通常会提供标准的管理信息库以及自行扩展的部分，其中就包括端口流量，中央处理器占用率，链路误差比等各项指标。运维人员可以随时通过网管平台获取实时数据，根据流量走向画出网络拓扑图，快速发现性能瓶颈或者硬件故障。

SNMP 协议从 v1 发展到现在的 v3，其安全性也有很大程度的提升。v1 版本只用团体名做简单的认证，存在明文传输的安全隐患；而 v3 版本加入了基于用户用户安全模型和基于视图的访问控制模型，可以对管理报文进行 MD5 或者 SHA 认证，也可以进行 DES 或者 AES 加密。强制使用 SNMPv3 对于保障电网安全稳定运行的通信网络管理系统来说，已经成了保证网络控制命令安全、防止恶意入侵、杜绝非法配置不可缺少的环节。

（三）RTP/RTCP 实时传输协议

音视频流媒体业务在电力应急指挥、无人值守变电站巡检等场景中所起的作用也越来越明显。RTP/RTCP 协议是为互联网上实时数据传输而设计的，一般工作在用户数据报协议之上。RTP 是用来传输数字音频、数字视频等实时数据的，报文头部含有序列号、时间戳、同步源标识符等信息。时间戳机制可以保证接收端正确地重组数据包的播放顺序，并且进行抖动缓冲，消除由于网络传输造成的时间差抖动，使画面流畅、声音清晰。

RTCP 是 RTP 的控制协议，不传输媒体数据，只周期性交换控制包。这些控制包里面就包含着丢包率、网络时延、抖动这些传输品质的统计数据。电力多媒体调度系统根据 RTCP 反馈信息可以实时调节编码速率或者分辨率。当网络带宽紧张或者存在干扰的时候，发送端会自动降低视频的清晰度来保证流畅性，防止画面出现卡顿或者黑屏的现象，保证指挥中心可以一直掌握现场的重要情况。

这两协议一起使用，就解决了通用 IP 网络对于实时多媒体业务的服务质量保证问题。在电力通信网络中，RTP/RTCP 与 SIP 信令协议一起构成全网络软交换语音系统、视频会议系统。这就使得远端专家可以实时对故障现场进行指导，极大的提高了电力系统应急反应的速度以及解决问题的效率。

三、物联网相关协议

（一）MQTT 协议

MQTT 协议是一种基于发布 / 订阅模式的轻量级的通信协议，是专为低带宽、高延迟或者不可靠的网络环境而设计的。在电力物联网里，成千上万个智能传感器、采集终端不需要直接同应用服务器创建繁杂的连接，它们把数据发布到代理服务器的某个主题上。应用系统作为订阅者，只需关注自己感兴趣的领域，便可以实时得到自己想要的信息。解耦架构大大减轻了终端设备的计算负担和网络流量，可以很好地处理大量的并发连接。

MQTT 协议有三种不同的服务质量等级，用来满足电力业务数据可靠性不同的要求。0 级（最多一次），适合于高频环境温湿度监测等可以容忍少量数据丢失的场合；1 级（至少一次），保证控制指令或者告警信息至少能够到达一次，但是可能会有重复；2 级（只有一次），采用四次握手机制，保证数据只传输一次并且准确无误，适合于计费数据或者关键开关操作记录的传输。这样一种服务质量的机制，使系统的设计者可以在可靠性与资源消耗之间找到最合适的那一点。

MQTT 还有遗嘱、心跳保活的功能。当部署在偏远地区的监测终端由于网络故障意外断线的时候，代理服务器就会发出预设好的“遗嘱”信息，主动告知管理平台设备离线。心跳报文用很小的流量来保持长连接，使调度中心随时知道终端的在线情况。因此，MQTT 成为了配用电物联网中使用最广泛的协议之一，它支撑起一个庞大的、从台侧的智能融合终端到户用智能家居的感知网络。

（二）CoAP 协议

CoAP 协议是专门为资源受限的物联网设备设计的类 Web 协议，它把 RESTful 架构风格巧妙地搬到受限节点网络里。相比超文本传输协议庞大的头部开销，CoAP 使用紧凑型二进制头部并使用用户数据报协议进行通信，大大减小了通信开销。在电力线路在线监测装置或者微型能量收集传感器中，CoAP 使设备可以像浏览网页一样被访问和控制。每个传感器数值都被抽象成统一资源标识

符资源，上位机用 GET、PUT、POST 等标准方法来操作它。

该协议使用观察者模式，使客户端可以不用轮询的方式获取资源状态的实时变化。变压器油温超过阈值或者开关状态发生变化的时候，服务器端就会自动把消息推送给观察者。可以节省网络带宽，又可以保证状态更新及时。CoAP 支持块传输，可以将大固件升级包或者波形数据文件分成小块来传输，满足低最大传输单元的无线传感网络环境。

CoAP 的又一大优势是它和互联网标准之间无缝对接的能力。借助超文本传输协议 /CoAP 代理网关，传统的 Web 应用可以很容易地穿透到电力物联网深层的感知域，不需要对现有的信息技术系统进行大规模的改造。这样电力公司就可以使用成熟的 Web 开发技术、工具快速开发出可视化设备管理平台、移动运维应用，从而加快电力物联网业务的推广和落地。

（三）AMQP 协议

AMQP 协议是应用层标准高级消息队列协议，是提供统一消息服务的协议，在电力企业级系统集成、后台数据处理中起着核心作用。MQTT 相比 AMQP 更多的还是关注后端系统的消息传递、路由、排队等。定义了交换机、队列、绑定等基本概念，支持点对点、发布订阅、扇出等多种路由策略，可以适应电力营销、运检、调度等各种业务系统之间复杂的交互需求。

在电力大数据平台中，AMQP 一般被用作数据汇聚和分发的总线。各采集系统产生的大量实时数据首先进入消息队列，AMQP 保证数据写入数据库或者被分析引擎消费之前不丢失。即便后端处理服务暂时性宕机，消息也会被安全地保存到队列里，等下次再处理。其强大的事务支持功能可以保证在多个系统联动操作的时候，消息处理的原子性和一致性，防止由于某个系统出现故障造成数据不一致。

1. 安全性，AMQP 有 SASL 认证，安全套接字层加密等来保证电网核心业务数据机密性以及完整性。

2. 利用细粒度流量控制，AMQP 可以有效地防止突发的大批告警信息“冲垮”后端处理系统，起到削峰填谷的作用，保证电力信息系统稳定运行。

第四节 协议转换技术

一、协议转换的必要性与应用场景

（一）异构网络互联需求

电力通信网包含发、输、变、配、用、调等各个环节，各个环节根据业务特点和覆盖范围建设了各种类型的通信网络。骨干传输网一般采用光纤通信技术，遵循 SDH 或者 OTN 标准；配电通信网大量采用工业以太网、无线公网、电力线载波等技术；用电采集侧采用微功率无线、ZigBee 等短距离通信技术。这些异构网络在物理层接口、链路层控制方式、网络层寻址方式等方面存在着很大的不同。

为了保证端到端业务的顺利流通，需要在网络层次不同的地方配置协议转换设备。以配电自动化系统为例，智能终端采集的数据大部分是通过串口或者现场总线接口，而主站系统几乎都是采用 TCP/IP 协议。此时协议转换装置就要完成串行通信链路到以太网链路的物理适配，并把现场总线规约中的数据帧重新封装成符合 IP 网络传输要求的报文格式。转换不是简单的电平调整，而是对不同网络结构下数据包进行深层次的分析、重组，以保证数据跨越不同的网络介质的时候，数据的完整性、时序性不被破坏。

异构网络互联需求也表现在不同行业的标准之间。智能电网不仅有电力专网，还要同外网进行数据交换。当电力系统要接入分布式能源、电动汽车充电桩或与智慧城市平台对接的时候，就会遇到行业标准不统一的问题。外部系统可以采用 MQTT、CoAP 等物联网通用协议，但是电网内部的控制系统必须严格遵守 IEC 61850、IEC 60870-5-104 等电力专用标准。协议转换技术起到通用翻译器的作用，它可以掩盖异构网络之间的差异，使上层应用可以透明地访问到各个终端的数据，从而创建泛在互联的能源互联网生态。

（二）新旧系统并存问题

电力系统基础设施建设周期长、投资大，因此电网设备的更新换代要逐步进行。目前电网结构中既有刚投运不久、采用最先进的数字化技术的智能变电站，也有运行了十几年甚至几十年的传统变电站和调度系统。新旧系统并存在相当长的一段时间内都会是电力通信网所面临的情况。

老旧的设备大多只能支持早期的通信规约，比如 CDT、Modbus RTU 或者早期的私有协议等，这些规约都是基于低速串行通信的，功能比较简单，不能支持复杂的信息模型。新建智能系统大多使用基于面向对象建模技术的 IEC 61850 标准，具有自描述、高速并发通信的能力。如果为了统一标准而全部淘汰更换老旧设备，将会产生无法承受的经济成本和巨大的停电风险。

协议转换技术可以解决上述的矛盾，并且是一种经济有效的解决方案。在老旧设备与新系统间加装协议网关或者转换服务器，把传统规约里模拟量、开关量等点表数据，转成 IEC 61850 标准里的逻辑节点数据对象。如此转换，老旧设备在逻辑上就成了具有现代通信能力的智能节点，可以被新一代调度自动化系统轻松识别并接管。不但可以延长存量资产的使用寿命，保护既有投资，而且保证电网技术改造平稳过渡，避免大范围更换设备造成电网震荡。

（三）多源数据融合需求

随着大数据、人工智能技术在电力行业的应用，电网运行控制关注的电气量数据也不再只是以往的那些。气象信息、地理空间信息、用户用电行为特征信息、能源市场交易信息等非电气量信息正在不断加入到电力通信网中。数据来源广泛，产生方式不同，造成数据格式和传输协议非常多样化且碎片化。

气象监测站点通过文本文件或者特定的气象报文格式发布温度、湿度、风速、光照数据；地理信息系统使用矢量图形数据和空间数据库接口；电力市场交易平台用 Web 服务接口以 XML 或者 JSON 格式交换数据。如果来自不同数据源、不同类型的各种数据直接进入电网控制中枢，就会造成数据处理系统的高度混乱和低效。

协议转换技术起到的作用就是实现数据的标准化。它要有多强的多协议适配能力，可以同时连上各种非标的数据流，并且把它们拆解解析，清洗融合之后再转换成统一的格式，

1. 结构化程度较低的文本数据要经过关键词提取、格式清洗等步骤，再转成标准的结构化记录。

2. 复杂的空间地理数据：需要进行坐标系转换和对象属性提取，使其与电网拓扑模型相匹配。

3. 互联网风格的 JSON 或者 XML 数据：转换模块需要对它进行扁平化处理，并将其映射到电力系统的通用信息模型上。

这样深入的清洗并融会贯通之后,原来的分散多源的数据就变成了统一语义、统一格式的高质量数据资产。这就给电网开展高级分析应用赋予了较好的数据条件,有力支撑起全景状态感知和精准决策。

二、协议转换的关键技术

(一) 协议分析与映射技术

协议分析是转换过程的开始,它的主要工作就是正确地对输入数据流进行解码。现代电力协议转换装置一般都装有强大的协议解析引擎,协议解析引擎常常采用状态机模型构建,可以对通信会话状态的变化做实时追踪。当数据帧到达之后,解析引擎就会依照预先设置好的规约库,一层层地剥掉通信报文的头部信息,从链路层校验开始,到网络层路由,再到应用层的数据载荷。定长报文可以用位置偏移量直接获取关键信息,变长报文或者用 TLV 等表示的复杂报文需要引擎动态计算字段边界来保证解析正确。

解析之后就是映射技术,它把源协议的信息元素映射到目标协议的数据结构中。这个过程比简单的字段拷贝要复杂的多。源协议与目标协议一般会采用不同的寻址方式及数据组织方式。比如 Modbus 协议的寄存器地址要映射到 IEC 61850 的“逻辑设备 / 逻辑节点 / 数据对象 / 数据属性”这种分层结构,就需要很复杂的映射配置表。

为了使映射更加灵活通用,目前主流技术使用配置文件驱动加载的方式。用户不需要修改程序代码,只需要使用图形化工具定义源数据点和目标数据点的对应关系,以及数值变换规则(变比缩放、偏移量修正)。运行时系统将这些配置载入到内存中的哈希表或者查找树结构里,进而达到快速的键值匹配以及数据填充。对逻辑不同的协议,映射层还需要对控制序列的模拟执行、心跳报文的代理发送、断链重连机制的转换等加以处理,保证两端系统逻辑行为的一致性。

(二) 数据格式转换与语义保持

数据在物理存储与传递过程中会出现编码上的差别,格式转换属于最底层的,也是最容易产生错误的环节。最典型的就是字节序问题,不同的处理器架构(大端模式和小端模式),对多字节整数的存储顺序是完全相反的,转换程序必须严格按照通信双方的规范进行正确的字节翻转。浮点数表示标准、字符集编码方式(ASCII、UTF-8 等)、时间戳基准点和精度等也都要进行标准化。任何一

个比特位出错或者解释有误，都会引起严重的遥测数据错误，甚至造成保护装置的误动。

比格式转换更深一层的就是语义保持技术。不同的协议对于同一个物理量的模型定义不一定相同，简单的数值传递会使得上下文的语义丢失。像 IEC60870-5-104 协议中的一个遥信位只是表示一个开关的分合状态，在 IEC61850 中就会带有质量品质位、时间戳、触发缘由等信息。从复杂的协议转换成简单的协议时，必须要有合理的信息截断或者聚合的方法，这样才能保留主要的语义，并且尽可能地利用扩展字段、合成信号等方法来传递一些辅助的信息。

为克服语义鸿沟问题，以本体论为基础的语义转换技术正在成为新的研究领域。该技术用公共信息模型作为中间媒介，把所有的源协议数据映射到标准化的 CIM 模型对象上，再由 CIM 模型导出为目标协议格式。源协议、中间模型、目标协议三者之间存在两级转换结构，虽然增加了处理的开销，但是实现了语义的一致性以及转换逻辑的解耦。语义标注以及推理机，可以自动发现数据里的语义异常情况，例如单位不匹配，量程超限等，在转换的时候进行自动修正或发出警告，从而完成由语法级转换到语义级互操作的过程。

（三）实时性与可靠性保障

电力系统对通信时延的要求非常严格，在继电保护、精准负荷控制等场合，如果因为协议转换产生任何延迟，都会影响故障隔离的速度以及系统的稳定性。为了保证实时性，协议转换技术中大量使用软硬件协同加速方案。硬件方面一般使用 FPGA（现场可编程门阵列）或者网络处理器来减轻 CPU 的负载。用硬件逻辑来实现底层的帧校验、过滤和转发，使报文处理的时延缩到微秒级。

在软件方面就是零拷贝技术以及多核并行处理。传统的协议栈处理数据的时候，一般要经过内核空间和用户空间多次的内存拷贝，造成大量的总线带宽和 CPU 时间的浪费。使用 DPDK（数据平面开发套件）等技术之后，协议转换程序可以直接对接网卡队列，在用户态完成零拷贝的数据包收发，从而大大降低上下文切换的开销。采用流水线的方式将协议解析、转换、封装等步骤分别交给不同的 CPU 核心去并行处理，可以大大提高系统的吞吐量。

可靠性的保证主要是依靠异常处理和冗余设计来完成的。协议转换装置一般被安置于无人值守变电站或者户外机柜之中，于是便要求它要有很强的抗干扰性能以及自愈功能。软件设计时一般会采用看门狗机制、内存防泄漏管理、完整的

异常捕获逻辑等措施,来保证程序在遇到畸形报文或者网络风暴的时候不会崩溃。

协议转换的可靠性保障策略,见下表:

可靠性保障策略

系统级冗余	双机热备:两台转换装置实时同步会话状态,当主设备故障时,备用设备能在毫秒级内无缝接管业务,保证数据流不中断。
网络鲁棒性	缓冲队列与重传机制:针对网络抖动、丢包问题,转换层内部设有优先级的缓冲队列,确保控制指令、告警信息优先转发,并在应用层实现重传。
运行态监测	全链路健康检测:系统能及时感知各个接口的通信质量,当链路劣化时,能自动切换路由或降级运行,从而构建坚固的通信线路。

从上表可知,在工业恶劣环境下,用这些技术与手段构建的协议转换系统可以保证长时间稳定工作,符合电力系统对于可靠性的要求。

第五节 协议安全机制

一、协议安全威胁

电力通信网络环境下协议安全威胁是多样的、复杂的。威胁并不只来自于外部,也可能来自于协议本身设计上的缺陷或者实现上的漏洞。下表给出了主要的协议安全威胁类型及特点:

电力通信协议安全威胁类型概览

威胁类型	攻击方式举例	潜在危害	常见影响
窃听、重放、篡改与伪造	网络嗅探、中间人攻击、报文重发、身份冒充	核心信息泄露、数据失真、系统误操作、非法控制	保密性、完整性、真实性遭破坏
拒绝服务攻击	大量连接请求、畸形报文泛洪、GOOSE/SV 泛洪	系统资源耗尽、设备死机、服务中断、实时控制失效	系统可用性、实时性严重受损
协议漏洞利用	缓冲区溢出、模糊测试、利用设计规范模糊性	程序崩溃、恶意代码执行、系统失控、安全防线突破	系统稳定性、安全性、可靠性下降

(一) 窃听、重放、篡改与伪造攻击

电力系统中大部分传统的通信协议仍然采用明文传输的方式,这样使得攻击者可以很方便地使用网络嗅探工具来获取通信数据,得到电网拓扑、设备参数和实时运行信息。被动窃听攻击的隐蔽性很高,很难被及时发现,但是它所获取的情报却可以为后续的高级攻击提供精准的支持。重放、篡改和伪造这三种主动攻

击，对于电网控制系统所造成的危害更加直接。攻击者截获合法控制报文后，稍后时间再发送，会造成断路器误动作或系统状态混乱。

更糟糕的是中间人攻击，可以随时对传输过程中的测量值和控制指令进行拦截修改。将正常的电压数据篡改成越限值，诱导调度系统作出错误的调节决策；或者伪造主站的跳闸指令，从而引发大面积停电事故。伪造攻击对数据本身以及冒充通信实体身份都属于伪造攻击。攻击者会伪装成合法的调度主站或者终端设备，欺骗系统从而获得对关键基础设施的非法控制权。攻击手段混合使用会对电力通信数据的保密性、真实性、完整性造成很大破坏。

（二）拒绝服务攻击

拒绝服务攻击就是用尽目标系统计算资源、网络带宽或者协议栈的处理能力，使得合法用户无法得到正常的服务。电力通信网中该种攻击的危害性尤为严重，因为电网控制对实时性有很高的要求。攻击者可以利用协议握手漏洞，向重要的节点发送大量的连接请求，使通信服务器的连接表饱和，从而不能处理正常的调度指令。

对于某种协议机制的攻击也时有发生。对于面向连接的协议，攻击者可以发送大量的畸形报文，造成接收端协议栈解析错误，甚至造成设备死机或者重启。当过程层网络遭受 GOOSE 或 SV 报文泛洪攻击的时候，大量的网络带宽瞬间被占用，造成正常的保护跳闸信号延时或者丢包，直接导致继电保护失效。此类攻击不需要复杂的渗透技术，只需要拥有足够的流量生成能力就可以实施，因此对电力实时控制系统造成很大的可用性威胁。

（三）协议漏洞利用

通信协议在实现过程中会不可避免的包含各种软件缺陷，这些漏洞很容易被黑客利用。缓冲区溢出是最常见的一种，如果协议解析程序没有对输入数据的长度做严格校验，攻击者发送的超长报文就会溢出内存中的关键数据或者代码区，造成程序崩溃或者执行任意恶意代码。对长期运行在变电站等无人值守环境下使用的嵌入式设备来说，危害性是十分深远的。

电力专用协议设计规范中存在一些模糊不清的地方，造成不同厂家的实现方式不同，引发兼容性问题，进而产生安全漏洞。攻击者利用模糊测试等技术找出不公开的漏洞，针对特定的设备编写攻击脚本。因为电力设备的更新换代周期比较长，而且补丁安装和固件升级受到运行窗口的严格限制，很多已知漏洞在系统

中存在很长时间都没有被修复。这种带病运转的状态给利用协议漏洞进行定向攻击创造了条件，使电力监控系统的脆弱性大大增加。

二、协议安全加固技术

（一）认证与访问控制机制

构建起严密的身份认证体系，这才算是阻止非法接入的第一道屏障。电力通信网络里大多提倡双向认证机制，就是通信的双方面在形成联系之前，要借助数字证书或者预先共享的密钥来互相确认身份的真实情况。

1. 基于公钥基础设施的数字证书认证属于目前比较稳健的一种方案。设备出厂时即内置唯一身份证书，通信握手时使用非对称加密算法来验证证书的有效性，从而保证通信对端身份的真实性以及不可抵赖性，有效防止伪造主站或者终端的攻击。

2. 身份认证成功之后，就会触发细粒度的访问控制策略。根据设备功能以及操作人员权限等级控制对某个数据对象的写、读操作。像普通的监测终端只能读取状态数据，重要的控制指令必须通过授权的调度主机才能发出。最小权限原则大大地减少了内部越权操作或者账户泄露所造成风险。

（二）数据加密与完整性校验

为了防止数据在传输过程中被窃听、被篡改，应该使用加密、完整性校验等技术。根据电力系统对实时性的要求不同，采取不同的加密技术。对于对时延敏感度较低的管理数据或者文件传送等，通常可采用高强度非对称加密算法与对称加密算法混合使用的方法，以达到数据绝对保密的目的。

在完整性保护上使用比较多的是消息认证码和数字签名。发送端生成哈希摘要之后用私钥或者会话密钥对数据进行签名，接收端验证签名就能知道数据在传输过程中是否被篡改。这就为每一帧报文贴上了防伪标签，任何微小数据的变化都可以立即被检测出来。尤其是广域网传输环境，基于 IPsec 或者 TLS 协议建立安全隧道，能够给没有内置安全机制的传统协议提供一层透明的加密保护壳，从而有效地防范对传输链路的各种攻击。

（三）安全协议的集成

把安全机制嵌入通信协议栈，这是改善内生安全能力的关键途径。即在协议设计的标准化阶段就加入安全规范，或者在已有的协议栈中用中间件的形式加

入安全模块。现代电力通信协议架构倾向于采取模块化的方法实现安全功能，可以按照不同的业务场景和安全等级需求，灵活启用或者禁用某一具体的某个安全选项。

安全协议集成时需要考虑到安全性和通信效率两个因素。在资源有限的配电自动化终端中，会使用轻量级的加密算法以及认证过程，来减少 CPU 和内存的使用。同时为了满足跨域通信的需求，安全网关就成为协议转换、安全隔离的关键点，可以集成多种安全协议栈来清洗和加固非安全域与安全域之间的协议。通过集成方式可实现即插即用的协议安全防护层，异构网络的安全互联。

三、电力协议安全实践

（一）IEC 61850 的安全扩展

IEC 61850 是变电站自动化的核心标准，IEC 62351 是其安全扩展标准，对智能变电站通信安全给出详细的指导。按照该标准，MMS 协议通信应该启用双向认证，用 TLS 加密等手段来保障后台监控系统和间隔层设备间的通讯安全。同时部署一个密钥管理中心，可以对变电站内成百上千台智能电子设备进行证书的自动分配和更新。

针对实时性要求非常高的过程层 GOOSE、SV 协议，提出了一个可以在 4 毫秒的传输时限内完成认证的方案 IEC 62351。实践中一般用 HMAC（哈希消息认证码）来实施认证，在报文的末尾加上一个计算量小的认证码，保证报文的来源合法、内容完整，并且不增加过多加密解密延时。虽然为了性能考虑，过程层报文一般不会对整个报文进行加密，但是，在跨变电站的广域保护中，利用硬件加速卡实现的链路层加密技术正在推广使用中，这样既保证了低时延又实现了机密性。

（二）远动协议的安全认证机制

在行业内，被广泛使用在调度自动化系统中的 IEC 60870-5-104 和 DNP3 安全协议已经得到推广使用。这些实践主要是应用层安全加固，在原有的协议数据单元中插入认证数据对象。如，IEC104 协议所扩展使用的，有挑战 and 响应的认证流程。主站发送关键控制指令之前，先向终端发出认证挑战，终端验证通过之后才能执行操作，以此来有效防止重放攻击。

密钥管理属于远动协议安全实践里的一大难题。目前最好的办法就是使用预

先置入的主密钥和动态生成的会话密钥。会话密钥按照时间或者通信流量来更新，即使攻击者破解了当前的会话密钥，也无法解密之前的数据，更无法预测将来会通信什么。对于原有的设备可以设计外挂式的加密认证盒，通过把 RTU（远程终端单元）串联在通信线路上来达到安全加固的目的，从而大大地降低了改造老设备的安全升级成本。

（三）协议安全测试与评估

为了保证协议安全机制能够正常发挥作用，建立常态化的测试和评价体系是必不可少的。模糊测试被广泛地用于电力协议的健壮性测试中，是高效的漏洞挖掘方式。测试人员用专门的工具产生大量的畸形报文、边界值报文、逻辑乱序报文对目标设备进行高强度的轰击，检测协议栈是否会崩溃、死锁、资源泄露等。

除了健壮性测试之外，合规性测试属于安全实施的范围。专业的检测机构按照 IEC 62351 等标准逐项验收设备的安全功能，保证加密算法强度、密钥管理流程、认证机制实现等都符合规范的要求。系统投入使用以后，持续的渗透测试以及流量监测是找出潜藏危险的主要途径。通过工业级入侵检测系统实时分析通信流量中的协议字段，可以识别出异常指令序列或者非法操作行为，形成实验室检测、现网监测全生命周期的协议安全闭环管理。

第六章 电力通信网络安全

第一节 网络安全威胁分析

一、常见网络攻击类型

（一）被动攻击与主动攻击

被动攻击主要是对信息的窃听、监测、流量分析。攻击者不会改变系统资源，也不会破坏数据传输的状态，只是在通信链路上截取数据包来获得敏感信息。此类攻击手段具有很强的隐蔽性，一般不会被攻击者察觉到，就可以实现信息的窃取。电力通信网中的被动攻击会使核心调度指令、重要用户信息、关键基础设施拓扑结构被非法获取，给之后更严重的攻击提供便利。攻击者用网络嗅探工具长时间潜伏在网路边缘或者内部，对通信流量的规律和特点进行分析，不会造成网络中断，但是带来的隐私泄露风险不能小视。

主动攻击与被动攻击正好相反，它直接对数据流进行篡改、伪造、重放或者阻断。攻击者不再只是旁观者，而是直接加入到通信过程里去，试图改变系统的状态或者误导通信双方。重放攻击就是通过录下有效的数据包并反复发送，以此来欺骗系统执行未经授权的操作，或者伪装成合法实体发送虚假的控制指令。在电力控制环境里，主动攻击的后果十分严重，会使得开关误动、保护装置失效，造成大范围的停电。防御主动攻击要采取严格的身份认证以及完整性校验机制，保证每一条指令的真正来源以及没有被篡改，从而创建出不可抵赖的通信环境。

（二）分布式拒绝服务攻击

分布式拒绝服务攻击使用大量的受控僵尸主机，向被攻击的目标系统发送海量的请求，目的是耗尽目标系统的网络带宽、连接数或者计算能力，使其不能响应正常的合法用户的请求。电力行业由于大量智能终端、分布式能源、物联网设备接入，若其自身防护能力不够，很容易被攻击者利用成为发起攻击的跳板。攻击者掌控着成千上万的被感染设备，向电力调度中心、数据中心或者重要的业务服务器发出大量的无用数据包，致使通信链路阻塞、业务处理迟缓甚至瘫痪。这

种攻击的流量很大，来源散乱，而且具有突发性，传统的单点防御很难应对。

电力通信网所遭遇的分布式拒绝服务攻击，一般具备较强的针对性以及策略性。攻击者会选择在电网负荷高峰期、重大活动保电时段或者系统升级维护时段发起攻击，以期造成最大的破坏，或者引发社会恐慌。为防范此类威胁，电力通信网要配置高性能流量清洗设备、协同防御机制。

1. 流量检测和清除是第一道防线，对网络流量特征进行实时采集，用行为分析算法识别并丢弃异常的数据包，保证正常的业务流量通过。

2. 协同防御机制就是需要创建跨区域、跨层级的威胁情报共享与应急响应体系，在攻击源被发现之后可以迅速联动各方面的资源进行阻止、追查，把攻击的影响降到最低。

（三）恶意代码与病毒

恶意代码、病毒是网络空间里最古老、最持久的威胁，它们以文件、脚本、宏或者无文件攻击的方式隐藏在系统里，窃取数据、破坏文件、加密勒索或者控制主机等。电力企业办公网和生产控制大区之间尽管有物理或者逻辑上的隔离，但是恶意代码仍然可以通过移动存储介质、运维终端、供应链植入等方式进入到核心区域。特洛伊木马会伪装成合法程序来欺骗用户去执行，在后台建立隐蔽通道让攻击者远程控制关键设备；勒索病毒用强加密算法来加密重要数据文件勒索赎金，严重威胁到电力业务数据的完整性和可用性。

随着高级持续性威胁的发展，专门针对电力行业定制的恶意代码也越来越多。恶意代码的针对性和隐蔽性都很强，可以识别出特定的工业控制协议、厂商设备或者硬件环境，专门针对电力监控系统或者继电保护装置实施破坏。有些蠕虫病毒会利用系统的漏洞，在内部网络内进行自动传播，能够迅速感染大量的计算机，造成大范围的网络瘫痪、业务中断。防范此类威胁要建立全生命周期的恶意代码治理体系，在终端准入控制、补丁统一管理、行为动态审计等各个环节层层设防，以确保恶意代码在电力通信网中无法立足、运行、扩散。

上述常见网络攻击类型的概览，可见下方常见网络攻击类型概览表。

常见网络攻击类型概览表

攻击类型	主要方式	攻击目的
被动攻击	窃听、流量分析、信息监测	获取敏感信息，为后续攻击提供情报
主动攻击	篡改、伪造、重放、阻断数据流	改变系统状态、误导通信双方
分布式拒绝服务	大量僵尸主机发出洪水般请求	耗尽目标系统资源，使其无法响应
恶意代码与病毒	植入病毒、木马、勒索软件、蠕虫	窃取数据、破坏系统、勒索、远程控制

二、电力通信网特有威胁

（一）对生产控制系统的攻击

生产控制系统是电网运行的中枢，直接控制着发、输、变、配、用各环节的物理设备。对于该系统的攻击不再是简单地窃取信息层面的数据，而是直接对物理世界展开攻击，试图达到破坏和瘫痪的目的。攻击者通过工业控制协议的漏洞下达错误的断路器分合命令、改变发电机组的运行参数、篡改保护定值、屏蔽告警信息等，都会造成设备物理损坏、电网频率震荡、系统解列。由于早期的工控系统在设计的时候主要考虑的是可用性而不是安全性，因此内置的安全机制较弱，通信协议大多采用明文传输并且认证机制不严格，给攻击者创造了可乘之机，一旦突破边界防护，就会很容易控制底层设备。

该类攻击一般要求攻击者具备丰富的电力专业知识以及工控网络知识。攻击者常常隐藏在网络之中，钻研业务流程和系统逻辑，寻找最薄弱的环节加以利用。震网病毒事件属于此类攻击的典型例子，体现出了在数字空间里破坏物理设施的可能性。电力系统中类似的攻击会引发连锁反应，造成单个变电站故障进而迅速蔓延到整个电网，造成严重的后果。

为了防御生产控制系统遭受的攻击，必须要使用纵深防御策略。除了传统的防火墙、入侵检测系统之外，还需要加上工业协议解析装置，检查传输指令语义逻辑是否合法。同时加强对工控主机白名单的管理，严格控制可以运行的进程、服务以及外设接口等，保证只有经过授权的操作才能被执行，最大限度地减少被恶意操控的风险。

（二）物理环境安全威胁

电力通信网的物理设施分布广泛，偏远山区的输电线路杆塔、城市中心的变电站通信机房等，巨大的地理覆盖范围给物理环境的安全带来严重挑战。通信

光缆是传输的主干血管，野外通信光缆很容易受到自然灾害、人为破坏、生物侵害等因素的影响。山火、泥石流、地震等自然灾害会造成光缆中断，造成大面积通信中断；蓄意的人为破坏，比如偷盗通讯线缆、非法破坏基站设备等都会对电力业务正常传送造成严重影响。变电站无人值守方式使入侵者有物理接触通信设备的可能，可以通过控制台接口直接修改配置，获取机密信息或者在硬件中植入后门。

环境因素也会影响到设备稳定运行。极端温度变化、高湿度、雷电、强电磁干扰都会导致通信设备发生故障、老化加快或者性能下降。高压变电站的环境中强大的电磁场会干扰通信信号，严重的会造成精密电子元器件的损坏，造成数据传输误码率提高。为了对抗物理环境的威胁，就要对通信设施进行物理加固和环境监控。布置全天候视频监控、电子围栏、红外报警等安防系统，对机房以及杆塔周围出现的任何异常情况做到实时监控，采用具有高等级防护的工业级通信设备，提高抗电磁干扰、防雷击、耐候性，在恶劣的自然环境和电磁环境下也能保证可靠的通信。

（三）供应链安全风险

供应链安全风险存在于电力通信设备设计、研发、制造、运输、安装、维护的所有环节里。由于全球化分工，电力通信网所采用的软硬件产品，常常是由不同国家、不同厂商的部件或者模块组成。任何一个环节如果植入了恶意逻辑、存在预置后门、使用了有漏洞的开源组件，都会成为埋伏在电网深处的一颗定时炸弹。芯片级后门、预装的恶意固件、开发工具中的污染代码，常规的安全检测手段很难发现，一旦被特定的指令触发，攻击者就可以绕过所有的外围防线，直接拿到系统的最高权限，进行窃密或者破坏。

电力行业对于供应链的依赖性非常大，核心路由器、交换机、光传输设备、智能电表等关键设备，其供应商数量很多，层级很复杂。供应商自身的安全水平参差不齐，部分小供应商安全意识差、防护能力不足，容易给攻击者造成可乘之机。攻击者可以对供应商内部网络发起攻击，修改即将发布的软件补丁或者固件更新包，在电力通信网各个节点发布带有的恶意代码的软件，造成供应链攻击事件。应对供应链安全风险要创建全流程的管控体系，创建安全可信的产业生态。

1. 在采购环节，就要严格审查供应商的安全性，对产品开展准入测试，让供应商给出详细的软件物料清单和安全承诺书，保证产品来源可追溯，安全可控，

还要深入进行代码审计和后门检测。

2. 在开发和生产的过程中保证关键核心技术的自主可控，减少对单一来源的依赖，在核心芯片、操作系统、数据库等关键领域加强国产化替代，提高自主研发能力，构建自主安全的技术体系。

3. 运维阶段要健全漏洞检测和应急响应机制，实时监测所使用的第三方组件或开源代码库的新漏洞，及时修复已发现的漏洞来减少供应链风险演变为安全事件。

第二节 加密与认证技术

一、对称加密与非对称加密

（一）DES/AES 对称加密算法

数据加密标准属于早期普遍应用的对称加密体制，长期以来掌控着电力远动通信。用 56 位密钥对 64 位的数据块实行复杂的置换和替换。虽然它的设计初衷是为了提高硬件实现效率，但是随着计算能力的飞速发展，56 位的密钥空间已经不能抵御暴力破解了。虽然在现代电力通信网络中还可以找到其踪迹，被用于非核心业务数据的简单防护，但是其安全隐患已经促使行业逐步淘汰并替换。

高级加密标准已经作为数据加密标准的一种替代品，现在已经成为电力通信网络数据链路层、网络层数据加密的主流选择。该算法使用分组密码体制，支持 128 位、192 位、256 位的密钥长度，可以抵御目前所有的已知密码分析攻击。在智能电表数据采集、配电自动化终端通讯等对实时性要求很高的情况下，由于高级加密标准的运算速度快、占用的资源少，可以保证大量的业务数据被加密。

电力系统对于实时控制有着很高的要求，而高级加密标准的硬件加速功能正好可以达到这个要求。在通信模块中嵌入专用加密芯片，可以保证通信的速度，实现数据的线速加密。根据不同的安全等级对数据进行加密，采用不同的密钥长度，可以对核心控制指令进行最高级别的保护，也可以满足普通监测数据的传输效率。对称加密技术由于具有灵活的配置方式，因此在电力通信网络的各个层次上都有所应用。

（二）RSA/ECC 非对称加密算法

与对称加密不同的是，非对称加密使用了公钥和私钥的概念，从根上解决了密钥分发的问题。其中基于大整数因子分解难解性而提出的 RSA 算法，是目前使用最广泛的非对称加密体制。电力通信网络当中，RSA 算法一般被用于创建安全传输通道之前的握手过程，还有关键操作的数字签名等情况。因为其安全性依赖于密钥长度，所以达到高级加密标准同等的安全强度时，RSA 算法必须使用非常长的密钥，从而造成运算开销过大，一般不直接用于大容量业务数据的加解密。

椭圆曲线密码算法使用椭圆曲线离散对数问题作为基础，比 RSA 使用更短密钥可以得到相同的安全强度。因此，它在计算能力、存储空间有限的电力终端设备上具有很大的优势。手持式运维终端、分布各地的传感器节点、部分老旧配电终端等，椭圆曲线算法由于计算量小可以完成高强度身份认证和密钥协商，大大拓宽了电力物联网边缘侧非对称加密技术的应用范围。

电力系统密钥管理中心与终端设备进行交互的时候，非对称加密起着核心的作用。当主站系统需要给数以万计的智能终端分配新的对称密钥时，一般会采用终端预先设置好的公钥进行加密封装。终端收到之后，使用自己严密保管的私钥来解密，得到会话密钥，进而开启后续的高速保密通信。这种混合加密模式发挥出非对称算法密钥管理方便、对称算法加密速度快这两种特性，二者共同组成了现代电力通信网络安全架构的骨干。

主要加密算法特性对比表

特性	对称加密（如 AES）	非对称加密（如 RSA/ECC）
密钥类型	单一共享密钥	公钥与私钥对
密钥管理	密钥分发困难	解决密钥分发问题
加密速度	极快	较慢
安全强度	密钥长度与算法	密钥长度与数学问题难度
主要应用	大数据量加解密、会话加密	密钥协商、数字签名、身份认证
典型场景	数据传输加密、存储加密	数字证书、SSL/TLS 握手

如上表所示，对称加密和非对称加密各有优势，在电力通信网络中互为补充。

（三）密钥管理技术

密钥全生命周期管理是密码技术发挥效用的重要环节，任何一个环节出了问

题都会造成整个加密体系的崩溃。电力通信网络覆盖面积大、设备数量多，所以建立一套自动化、标准化的密钥管理体系就显得尤为重要。

1. 密钥生成：必须采用国家密码管理局认证的物理随机数发生器，保证生成的密钥序列具有良好的随机性、不可预测性。电力调度中心的中心服务器一般采用专用硬件安全模块来实现该功能，避免软件实现所引入的伪随机性。

2. 密钥存储：密钥的存储要达到很高的物理和逻辑安全保护的要求。主站侧的根密钥存放在防拆卸、防探测的硬件加密机里；终端侧用安全芯片的安全存储区保存，这样即使设备被物理劫持，攻击者也无法通过读取内存或者侧信道攻击获取有效密钥。

3. 密钥更新与销毁要具备自动化功能以及应急响应能力。系统根据事先设定的安全策略来定期更换会话密钥，以防长时间用同一个密钥而造成的破解风险。一旦检测到设备入侵或者设备退役，就要立即启动密钥销毁程序，彻底清除存储介质中残留的信息，保证过去通信数据后向安全。

二、数字签名与证书

（一）数字签名原理与作用

数字签名技术用非对称加密算法的逆过程来实现。发送方用自己的私钥对数据摘要进行加密，得到签名，接收方用发送方的公钥解密签名，并与接收到的数据摘要进行比对。调度员发出的调度指令会有数字签名。当指令在传输过程中被恶意修改或者由入侵者伪造时，接收端会验签不过，从而拒绝执行这个高危操作，能够有效地防止虚假指令造成的电网事故。

这项技术最大的价值就是不能被否认。由于私钥只有发送方拥有，所以通过公钥可以验证的签名一定是发送方生成的。电力市场交易中发电企业与购电大户之间的电子合同的签署、即时报价数据的提交等都用到了数字签名技术。一旦发生交易纠纷，数字签名就会变成具有法律效力的电子证据，确定各方的责任，保证电力市场的公平、有序运行。

为了提高签名效率，实际应用中一般对消息的哈希值进行签名，而不是直接对消息本身进行签名。电力通信网络中大量使用国密系列哈希算法，把任意长度的业务数据压缩成固定长度的摘要。不但可以大幅度减少签名运算的计算量，还可以利用哈希函数的雪崩效应，即原始数据哪怕只有一位比特发生改变，其对应

的摘要也会发生剧烈变化，因此可以灵敏地察觉到任何破坏数据完整性的企图。

（二）公钥基础设施

公钥基础设施就是可以提供公钥加密、数字签名服务的平台，它是依靠第三方权威机构来管理用户身份与公钥的关联。在电力行业里，数字证书一般是由电力认证中心来完成其管理。

PKI 一般包括认证中心，注册机构、证书库、证书吊销列表等。认证中心是信任的源头，根密钥的安全是整个体系的基础，一般用物理隔离和多人分权的方式来保护。注册机构分布于各个区域或者业务部门，对用户的证书申请资格进行审核，保证证书持有者的真实身份与登记信息一致。分层管理结构符合电力系统分区分层的管理模式，根据需要可以方便部署证书服务，快速覆盖各个地区。

电力物联网的公钥基础设施正在向轻量化发展。对于大量计算能力较弱的感知终端，传统的证书验证过程就显得过于繁重。因此行业内开始研究基于标识密码技术的无证书公钥基础设施体系，把设备的身份标识直接当作公钥，免去了证书的传输与验证过程，缩减了网络带宽的耗费，保持必要的信任传递途径，给泛在电力物联网的可信互联赋予了新的解决方法。

（三）数字证书的申请与应用

数字证书是网络空间的电子身份证，把用户的公钥和身份信息关联起来，再用认证中心的数字签名固定，防止被篡改。调度员、运维人员、重要的服务器、网关等都必须申请并获得合法的数字证书。

1. 申请流程：从用户向注册机构发出身份证明文件和公钥请求文件开始。设备证书一般由运维人员在设备出厂或者入网调试的时候，通过安全通道导入或者在线申请。注册机构审核通过之后，请求会被转交给认证中心，认证中心使用根私钥签发证书，最后通过离线介质或者在线协议将证书发给申请者。

2. 证书的应用：证书被广泛地用在电力业务的各个方面。如在变电站做远程运维时，运维人员需插入带个人证书的智能密码钥匙，系统才会根据证书是否有效来决定允许执行什么操作。主站和终端之间用交换的设备证书完成双向认证，建立加密传输隧道。管理员在员工离职或者设备报废的时候，会把相应的证书放进吊销列表中，然后推送给全网的验证节点，立刻阻止非法访问。

三、身份认证技术

（一）口令认证与动态口令

传统的静态口令认证属于比较基础的身份认证方式，但是其安全性已经不能满足电力系统关键区域的要求。弱口令、口令复用、社会工程学攻击等都使静态口令很容易被获取。但是，在一些非关键的办公辅助系统或者作为多因素认证的一部分，静态口令仍然存在。为了提高系统的安全性，一般都会强制要求口令具有一定的复杂度，即必须同时包含大写字母、小写字母、数字、特殊字符，并且要定期更换。

动态口令技术通过时间同步或者事件触发实现“一次一密”。电力调度自动化系统远程登录时，运维人员要配合手持令牌完成动态口令的手动输入。令牌内部装着高精度时钟和种子密钥，每 60 秒产生一个新的 6 位数字密码。服务器端使用同样的算法和种子做同步计算，只有相等时才允许访问。彻底消除了重放攻击和网络嗅探的威胁，即使攻击者得到了当前口令，一分钟后该口令也会失效。

由于移动应用的普及，基于手机软件的软令牌也被用在电力移动作业终端上。软令牌比硬件令牌更便于分发、维护，且成本低。利用手机自带的指纹或者面部解锁功能，软令牌除了提供动态密码以外，在实质上就构成了隐性的双因子认证，提高了安全性又改善了作业人员的使用体验。

（二）生物特征识别

生物特征识别技术用人体固有的生理特征或者行为特征来鉴别身份，具有不可遗忘、难以伪造的特点。生物识别技术已经成了特高压变电站、电力调度大厅等重要场所的物理门禁和重要操作终端的标配。指纹识别技术已经比较成熟，可以比对采集到的指纹脊线特征来识别，已经广泛应用到手持巡检终端的登录解锁上。

人脸识别、虹膜识别具有更高的安全级别和非接触式的便利性。电力监控中心摄像装置能即时对操作员面相取样完成在职验证。当检测到未经授权人员靠近操作台或者操作员离开时，系统会自锁屏幕或者发出报警。虹膜识别因为具有很高的熵值以及稳定性，被应用到最高密级的数据机房门禁系统中，只有少数核心管理人员才能进入。

生物特征数据属于敏感的个人隐私信息。在电力通信网络中使用这些技术的

时候,必须遵守有关数据保护的法规。系统一般只保存生物特征的哈希摘要,而不保存原始图像,将这些数据加密保存在独立、安全的区域。采用端侧比对模式,即在采集端完成特征提取和比对工作之后,只将认证结果发送到后台,最大限度地防止了生物特征信息的泄露。

(三) 基于证书的强认证

数字证书强认证属于电力行业认为的最高等级的一种认证方式。它依靠公钥基础设施,用非对称加密算法的挑战应答方式来核实身份。当用户尝试接入的时候,服务端会发送一个随机数挑战,用户需要使用存放在硬件介质上的私钥对随机数进行签名然后返回。服务器用用户的公钥来验证签名,以确认用户拥有合法的私钥。

认证方式一般用智能卡或者 USB Key 来承载。在电力营销系统中,柜台操作员发起业务流程时必须将个人 USB Key 插入终端。硬件加 PIN 码的双因子认证模式,“所见即所得”+“人证合一”。即使电脑被植入木马,攻击者也因为没有物理介质而不能伪造身份。

设备同设备之间的机器通信领域也广泛地采用了基于证书的强认证。智能变电站的过程层设备,合并单元、智能终端等,采用预设的设备证书,在建立通信链路的时候进行双向认证。该种自动化的强认证方式去除了人工设置口令的麻烦与错误,给电网自动化系统即插即用、安全互联构筑起了可信的信任根基。利用安全套接层协议握手过程,通信双方不仅相互认证了身份,而且就今后使用怎样的会话密钥达成了协议,从而实现了认证和加密的有机结合。

第三节 访问控制机制

一、访问控制基本模型

创建电力通信网安全架构的时候,选取合适的访问控制模型属于制订安全策略的基本工作。不同的模型适用不同的安全需求场景,有灵活自管、严格强制性隔离、大规模组织的角色管理等范式,多种范式一起组成访问控制的理论基础和实践框架。三种基本模型的主要特性如下表所示:

访问控制基本模型对比表

特性维度	自主访问控制	强制访问控制	基于角色的访问控制
核心思想	资源拥有者自主授权	系统强制安全策略	基于职能分配权限
管理方式	访问控制列表	安全标签	角色 - 权限映射
权力中心	用户（资源拥有者）	系统管理员 / 安全策略	角色（组织结构）
灵活性	高	低	中高
安全性	较低（依赖用户意识）	极高（系统强制）	较高（基于最小权限）
复杂性	低（简单场景）	高（需要底层支持）	中高（大型组织）
适用场景	办公自动化、非核心业务	军事、核电、电力调度核心系统	大型企业、职能明确的系统
电力应用	日常行政办公文件共享	电力监控系统、核心调度数据网	调度员、运维工程师权限管理

（一）自主访问控制

自主访问控制一般被用作非核心业务区的权限控制策略，是一种灵活的权限控制策略。在该种模式下，资源（客体）的拥有者拥有很大的决定权，可以按照自己的意愿将访问权限授予系统中的其他用户。权限可以在用户之间自由流转，具有很高的灵活性和普适性，特别适合那些对信息流向控制要求不高，但是非常重视协作效率的办公自动化环境。电力企业日常行政办公网络当中，文件共享以及协同编辑业务常常采取这样的策略，从而推动部门之间的信息交流。

但是由于权限管理的权力分散到每一个用户身上，系统的整体安全性很大程度上依赖于用户自身的安全意识。一旦高权限用户账号遭到攻击，攻击者就可以凭借这个用户的授权去获取很多敏感资源的访问权限。DAC 一般是借助 ACL 来具体说明每一个主体对于客体所能进行的读、写、执行等操作。虽然 ACL 不能满足复杂的安全需求，但是由于其在低安全级别应用场合下无与伦比的便利性，所以仍然占据着一席之地。

为了弥补 DAC 在安全性上的缺陷，在现代实践中常把 DAC 和身份认证、审计结合起来使用。经过严格的验证保证操作者的真实，对所有的授权以及访问进行记录，在发生安全事件时可以有效地追查。此种结合策略维持了灵活性并改善了系统总体的安全程度，可较好地支撑电力通信网里的辅助业务系统。

（二）强制访问控制

强制性访问控制比较安全。它不再根据用户的个人意愿来确定访问权限，而

是由系统管理员或者安全策略制定者事先制订出严格的访问规则。系统给每一个主体和客体赋予唯一的安全标签，来表明它的安全级别和类别。主体对客体每一次访问请求都需要经过安全内核严格检验后才能完成。主体安全级别与客体安全级别符合预设的支配关系时才能获得访问权。

电力监控系统、核心调度数据网中使用 MAC 可以保证数据的保密性、完整性。按照安全策略，低安全级主体不能读取高安全级客体信息，以防机密外泄；反之，高安全级主体也不能向低安全级区域写入信息，从而避免高密级信息流出或者低密级信息被污染。这样的双向流向控制就形成了比较牢固的信息隔离壁垒，就算特权用户想越轨也难以逾越系统预先设置好的安全标准。

MAC 的实施一般需要操作系统的底层或者数据库管理系统底层的支持，主要依靠安全增强型操作系统内核来实现。对电力通信网中重要的节点如调度中心的主服务器、重要数据库等地方部署带有 MAC 功能的系统可以防止木马病毒窃取行为。即使恶意代码获得了运行权限，由于载体进程的安全标签限制，恶意代码也不能接触到系统中的高密级数据，把潜在的损失降到最低。

（三）基于角色的访问控制

由于电力企业信息化程度的不断提升，用户数量以及资源种类的增长呈指数级态势，直接管理用户和权限之间关系的工作变得越来越繁琐并且容易出错。于是就有了基于角色的访问控制。用中间概念“角色”来表示权限，将权限授予角色，再将角色分配给用户。这种间接授权的方式大大降低了权限管理的复杂性，安全策略的执行也更加的清晰明了，适合于大型电力企业。

1. RBAC 模型中的角色是依据企业内部职能划分定义的，例如调度员、运维工程师、审计员等。每个角色预先被赋予完成其职责所需的最小权限集。当员工入职或转岗时，管理员只需将其账号关联至相应角色，该员工便自动获得该角色所拥有的所有权限，无需逐一配置。

2. 引入角色层级关系可以进一步提高模型的表达能力。高级角色可以继承低级角色的权限，形成与企业组织结构相对应的权限继承树。高级运维主管除了具有普通运维人员的全部权限外，还具有审批和配置修改的高级权限。分层设计可以有效地减少重复配置，保证权限结构的统一性、可维护性。

3. RBAC 的重要特性之一就是责任分离原则。通过设置互斥角色，强制要求某些关键的操作必须由两个人来完成，并且不能由同一人同时担任两种会产生利

益冲突的角色。电力交易系统中为了防止内部欺诈，交易发起人和交易审核人必须是两个不同的角色。

二、网络边界访问控制

（一）防火墙技术

防火墙是网络边界最基础、最重要的访问控制设备，部署在电力通信网各个安全域的边界上。根据事先设定的规则表来对进出网络的数据包进行检查和过滤。规则一般是根据源地址、目的地址、端口号、协议类型等五元组信息来决定放行还是丢弃数据包。电力调度数据网与综合数据网之间的防火墙，形成了一道牢固的屏障，只允许被特许的数据流量在受到控制的状况下传输。

防火墙的核心功能之一就是状态检测技术。状态检测防火墙可以跟踪网络连接的会话状态，识别出属于同一个连接的数据流，而传统的包过滤防火墙不能做到这一点。只有已经建立合法连接的响应包才能够通过防火墙进入内网，任何外部没有请求过的连接请求都会被拒绝。该种机制大大提高了防火墙对于欺骗攻击、拒绝服务攻击的防御能力，给电力内网提供动态的安全防护。

因为应用层攻击越来越复杂，新一代防火墙具备了应用层代理、深度包检测等功能。它不再只是对网络层、传输层头部信息进行检查，而是直接对数据包的载荷内容进行检测，判断具体发送的是哪种应用协议类型、发送了什么指令。应用层防火墙对于在电力系统 Web 应用中，可以阻止对应用程序的 SQL 注入、跨站脚本等攻击，保证业务系统应用逻辑不会被恶意修改。经过细致的应用识别与控制之后，防火墙就实现了从网络连接到业务内容的全部访问控制。

（二）物理隔离与网闸

在电力系统安全防护体系中，生产控制大区与管理信息大区之间必须实现物理隔离或者逻辑强隔离，这是保证电网安全运行的底线要求。物理隔离就是指两个网络在物理链路上是完全断开的，不存在直接的电气连接，从而实现物理上的网络攻击。但是为了满足必要的业务数据交换需求（实时运行数据传送到管理系统进行分析），专用的隔离装置——网闸被广泛使用。

网闸的“双岛”结构是由内网处理单元、外网处理单元及中间隔离交换单元组成。工作原理是采用协议剥离和数据摆渡的方式，当数据从内网传到外网的时候，内网单元先剥离 TCP/IP 等通用网络协议，只把纯数据载荷写入中间存储介质，

然后断开内网连接，外网单元再与中间介质建立连接，读取数据并重新封装协议后发往外网。在整个数据交换过程中，内外网处理单元都不和中间介质同时连接，从而达到物理隔离而逻辑连通的目的。

完全切断了依靠网络协议进行的数据交换方式，完全切断了依靠网络协议进行的攻击途径，比如 TCP 会话劫持、恶意代码传播等等。按照电力二次系统安全防护的规定，正向隔离装置是生产区向管理区进行单向的数据传输，保证核心控制指令不会被外部所篡改；反向隔离装置是管理区向生产区进行极少量数的数据传输，并且需要经过严格的签名认证以及内容检查。物理隔离和网闸技术的应用，给电力关键设施提供最上层的保护。

（三）安全接入区设计

随着移动作业、分布式能源接入、智能电表等新业务的迅速发展，电力通信网要接入很多外部终端。为了在开放接入的同时保证内网安全，要专门划出一个安全接入区作为外部系统进入电力内网的缓冲区。安全接入区一般设于管理信息大区的边界处，并且配有多套安全防护装置，用以检测来自外部或第三方网络中的访问请求，防止潜在的威胁直接闯入到内部的网络的系统之中。

1. 安全接入网关是该区域的核心设备，它的主要功能就是创建安全加密通道，保证数据通过公共网络进行传输时保密和完整性。网关一般用高强度加密算法对传输的数据进行加密，即使数据被截获也不能被破解。同时网关也具有细粒度的访问控制功能，只有符合安全策略的终端才允许建立连接，并且对可以访问的业务进行严格的限制。

2. 安全接入区的前置服务器是业务代理。外部终端不能和内部服务器直接交互，只能同前置服务器交互。前置服务器会对外部提交的资料进行格式检验、内容过滤以及协议转换，确认没有问题之后，就会通过隔离装置把数据同步到内网当中。断链设计可以隐藏内网拓扑结构和核心资产，增大攻击者横向移动的难度。

3. 完善身份认证和终端安全检测机制，又成了安全接入区的一个重要支柱。终端接入前须利用数字证书、动态口令等很多种认证方式来判定用户身份的真假。系统会检测终端的安全状态，即装没装杀毒软件、病毒库是否更新及时、是否有违规外联等。只有身份合法、环境安全的终端才能接入网络，不安全因素被排除在安全接入区之外。

三、内网访问控制

（一）网络接入控制

网络接入控制解决的关键问题是谁可以接入到网络，连接后可以做些什么。电力企业办公网、生产网接入终端数量大。如果缺少有序的管理，私自接入无线路由器、非法外联等行为会给网络造成巨大的安全隐患。部署 NAC 可以利用 802.1x、MAC 地址绑定或者 Portal 认证等方式，在设备接入交换机端口的一瞬间就进行认证。只有通过认证的合法设备，交换机才会开放端口让它通过；否则端口将会被关闭或者划分到隔离 VLAN。

除身份认证外，NAC 还要做端点安全合规性检测。系统会联动终端的安全代理软件，对操作系统补丁安装情况、防病毒软件运行状况、违规软件进行扫描。对检测终端的安全漏洞进行检查，若不符合就采取访问控制措施只允许访问补丁服务器或者修复区。修复完毕之后，才可回归正常的网络使用状态。把网络接入权限同终端安全状态绑定起来，可以有效地避免带病终端成为内网病毒的传播源。

（二）虚拟专用网访问控制

VPN 技术在电力通信网中常用来创建贯穿广域网的安全通道。对分布在不同地理位置的变电站、供电所、营业厅等，可以采用 MPLS VPN 或者 IPSec VPN 技术，在公共通信基础设施上划分出逻辑上相互独立的专用网络。这就使电力业务流量和其他流量互不干扰，各个业务部门之间逻辑上相互隔离。调度自动化业务和营销业务分别在各自的 VPN 实例里运行，即使一个网络发生拥塞或者安全事件，对另一个网络不会有任何影响。

远程维护和移动办公人员可以使用 VPN 实现安全高效的接入。用户需要安装 VPN 客户端，通过内网的 VPN 网关建立加密隧道。系统在隧道建立的时候除了会验证用户的凭证，还会根据用户的角色以及网络环境动态地下发访问控制策略。如限制远程用户只能访问指定服务器端口，或者禁止用户在使用 VPN 连接时访问互联网。如此细的粒度来控制隧道内部的访问，可以避免远程接入通道被攻击者当作入侵内网的跳板。

VPN 技术一般采用冗余性高、可靠性好的设计。电力通信网的关键链路一般会设置主备 VPN 通道。主通道发生故障的时候，流量可以毫秒级地切换到备用通道上，保证业务的连续性。使用 VPN 流量加密封装来保证敏感业务数据在

传输过程中不被窃听、篡改，给电力数据远距离传输提供可靠的保密保障。集隔离、加密和访问控制于一身的这项技术，给构建弹性、安全的电力广域网打下了坚实的基础。

（三）数据库与应用系统访问控制

应用系统以及数据库是电力数据的最终承载者，也是访问控制的最后一环。应用层访问控制已经不满足于对 IP 地址和端口的控制了，而是更加细致入微地进入到具体业务功能的及数据字段上的控制之中。现代电力业务系统大多是分层架构的，Web 服务器、应用服务器和数据库服务器之间互相信任并且交互紧密。应用系统内部一般采用基于角色的权限控制，按照用户职能对菜单项、按钮乃至数据行设置可见性权限。在营销系统中，普通柜员只能看到自己办理的客户档案，不能看到全辖区的客户数据。

数据库层面的访问控制更底层、更细致。除了标准的数据库账号密码认证外，也可以通过视图、存储过程、触发器等方式对表做更详细的权限管理。通过精细定义权限策略来控制用户只可以读取指定的列（屏蔽身份证号、银行卡号等敏感字段）或者只能在某个时间段内对数据进行操作。为防止特权账号滥用，数据库审计系统会对全表扫描、批量删除等高风险操作指令进行记录，同时会实时告警。对于数据的操作行为进行深度的管理，可以很好的控制内部人员窃取、破坏数据的行为。

针对 SQL 注入等数据库攻击，应用系统在开发阶段就已经引入了参数化查询和输入验证机制，并且在运行的时候通过 Web 应用防火墙来实施动态拦截。为了防御高级持续性威胁，部分核心系统正在尝试将零信任架构运用到应用层面，即不再默认内部各个服务彼此之间互相信任，而是对每一个 API 请求都进行实时的身份认证和权限检查。持续验证机制可以减少攻击者突破应用边界以后可操作的余地，保证电力核心业务数据安全。

第四节 安全监测与防护

一、入侵检测与防御系统

（一）IDS/IPS 原理与部署

入侵检测系统主要是通过旁路监听网络流量，再对流量进行深入分析，从而发现入侵行为。它的主要功能就是使用镜像端口取得数据包，经过协议解析提取应用层信息，并与内部攻击特征库作比对。当系统检测到匹配的恶意行为的时候，就会立刻产生告警日志并上报给管理人员。IDS 一般不会直接阻止通信，以保证业务的连续性。该种被动监测方式很适合布置在调度数据网核心交换节点，可以实现对整个网络安全态势的全方位掌控。因为没有采用单点设计，所以即使某一台设备出现故障，也不会造成整个系统的整体失效，同时也为之后的安全审计和溯源工作积累了充分的数据基础。

入侵防御系统采用串行接入方式，直接部署在数据传输的必经之路。它不但具有检测的功能，还拥有实时的阻断能力。当系统检测到 SQL 注入、缓冲区溢出、恶意扫描等攻击行为时，立即丢弃相关数据包或者切断 TCP 连接，将威胁消灭在萌芽状态。部署 IPS 于电力信息网的互联网出口、核心服务器区，可有效防范外部的攻击威胁，保证 Web 服务和数据库的安全。为满足电力业务对实时性的严格要求，现代 IPS 设备使用硬件加速、零拷贝技术来提高深度包检测的性能，在保证能对网络流量做深度分析的基础上，使网络延时控制在微秒级，尽量减小对电力业务数据传输的影响。

（二）基于特征与基于异常的检测

特征检测技术目前最成熟、应用最广，它的原理与杀毒软件相似，依靠的是庞大的并且不断更新的攻击特征签名库。每一个已知的网络攻击方式，比如某个特定格式的蠕虫病毒代码段，某个异常的协议头部字段，某个特定的恶意网址，都会被当作唯一的数字指纹进行提取。网络流量当中数据片段如果和指纹完全一样，那就说明是攻击。这种方法准确率很高，误报率低，特别适合用来对付电力系统里常见的已知类型的攻击，可以很快地识别出大量爆发的普通病毒和木马。

1. 利用异常的检测技术依靠统计学和机器学习算法，用来发现未知的零日漏洞攻击、变种威胁等。该技术依靠长时间学习来创建电力通信网正常流量基线模

型, 流量大小、协议分布、访问频次、连接时长等各方面都会被纳入考虑。

2. 实时流量偏离预设的正常基线, 且偏离的程度超过预设阈值时, 系统就会发出告警。平日流量平稳的变电站终端突然发出大量的连接请求, 或者在非工作时间内大量敏感数据库的操作, 都被判定为异常行为。尽管会存在一定的误报情况, 但是对于新型高级持续性威胁的发现仍具有不可替代的作用, 一定程度上弥补了特征检测只能识别已知攻击的不足。

(三) 统一威胁管理

统一威胁管理设备将防火墙、入侵检测、防病毒、内容过滤、虚拟专用网等安全功能集到一起, 在一个硬件平台上运行。在电力通信网的配电通信接入网和边缘场站侧, 由于场站数量多且受物理环境限制不能部署多台独立的安全设备, 因此一体化解决方案有很高的应用价值。在统一硬件架构、操作系统下, 数据流经拆包重组之后可以同时进行多种安全扫描, 大大减小了处理延迟, 提高了整体吞吐效率。

UTM 设备可以简化网络拓扑结构、降低建设与维护成本, 也可以集中统一地进行安全策略的管理。管理员可以通过一个控制台对各个设备的访问控制规则、入侵防护策略以及内容过滤清单进行统一的发布, 从而避免出现由于各个设备的策略互相冲突所造成的安全漏洞。面对混合型攻击的时候, UTM 设备可以促使各个功能模块相互配合, 比如说一旦发现恶意邮件附件, 就会立刻触发防火墙去封禁发件人的地址, 而且还会更新入侵防御的规则, 以此来阻止之后的连接, 从而达到对复杂威胁的立体防护效果。该设备针对电力物联网终端接入场景, 对工业协议的识别、过滤能力进行了加强, 在开放的网络环境下保证电力业务数据的完整性、保密性, 为边缘计算节点提供轻量级、功能齐全的安全屏障。

二、终端与服务器安全

(一) 主机入侵防御系统

主机入侵防护系统直接安装在服务器或者工作站的操作系统上, 和网络层的防护设施互相补充。它潜入了系统内核, 对文件系统的访问, 注册表的修改, 进程的启动, 网络连接等所有底层操作都进行了严密的监视。与传统杀毒软件只分析文件的静态特征不同, HIPS 更多是对行为的动态分析与控制。当某个合法进程执行异常操作的时候, 比如记事本程序试图对系统关键进程进行代码注入, 或

者 Web 服务器进程试图修改系统启动项，HIPS 就会立刻拦截这个系统调用，阻止恶意代码取得系统控制权。

对于电力调度自动化系统来说，业务主机的稳定是十分重要的。HIPS 采取白名单机制，把系统内部合法的可执行程序以及动态链接库固定下来。不在白名单的代码不能执行，从源头上杜绝未知病毒、木马的发生。该系统可以防止内存溢出攻击，采用地址空间布局随机化、数据执行保护技术来加强防护，有效地阻止旧的电力业务软件漏洞被利用。对于不能及时打补丁的老旧操作系统，HIPS 可以提供行为层面的防护，给老系统加上虚拟补丁功能，不需要修改系统文件就可以阻断漏洞利用的途径，保证电力存量资产的安全运转。

（二）终端安全管理

终端安全管理平台能很好地解决电力企业很多终端的管理问题，对网络里的所有终端执行标准化的控制和合规性检测。采用在每台终端上安装轻量级代理软件的方式，获取各个硬件配置信息、软件版本信息、补丁安装情况信息、安全策略执行情况等信息。系统强制所有的终端接入内网时必须达到事先设定的安全基线，即必须安装防病毒软件并更新到最新病毒库、必须设置屏幕保护密码、必须禁用高危服务等。不符合要求的终端会被系统通过网络准入控制技术隔离到修复区，只有整改合格以后才能访问业务网络。

就移动存储介质而言，它会带来数据泄露与病毒的传播，所以终端安全管控十分严格地进行注册认证。只有经过加密处理并且注册授权的专用移动硬盘或者 U 盘才能在内网终端使用，系统会详细记录文件拷贝、删除、修改日志，实现数据流转全过程可追溯。系统会对内网终端对外联行为进行实时监控，禁止使用双网卡、无线网卡或手机热点等违规连接互联网的方式来建立内外网穿透通道。经过软硬件资产自动识别并且关联起来之后，管理员可以很快发现私接设备和硬件变动的情况，从而保证电力内网边界完整并处于控制之下。

（三）服务器加固与虚拟化安全

服务器加固是系统工程，其目的就是通过减少攻击面来提高操作系统的抗攻击性。关闭 FTP、Telnet 等不安全的协议，只保留业务必需的通信方式；严格控制超级管理员远程登录权限，采用基于角色的访问控制和多因素认证；定期审计系统日志和账户活动，及时清除长期不用的僵尸账号。对电力核心数据库服务器还要细分权限，使数据库管理员不能直接看到敏感业务数据的内容，达到管理权

和数据权分离的目的。

伴随着电力数据中心云化的推进，虚拟化安全成了新的研究焦点。Hypervisor 是虚拟化层的重中之重，它自身安全与否决定了所有运行在其上的虚拟机的安全。因此，必须保证 Hypervisor 及时更新，配置严格，防止攻击者用虚拟机逃逸技术突破隔离层进入物理主机。

虚拟化环境下内部网络流量（东西向流量）大部分不经过传统的物理防火墙。因此，必须使用虚拟防火墙或者微隔离技术来控制虚拟机之间的通信。每一个虚拟机都应该视作一个独立的防护单元，为每一个虚拟机赋予独立的、专属的安全策略，以此阻止一台虚拟机被攻破之后，攻击者利用它在虚拟网络内部随意横向移动，从而波及整个云资源池。为了更好的了解服务器加固的一些主要措施，可以参照下表。

服务器加固核心措施

减少攻击面	关闭不必要的服务与端口，卸载不必要的软件组件，确保操作系统精简运行。
强化身份认证	实施强密码策略，启用多因素认证，对特权账户进行严格管理和监控。
最小权限原则	用户和应用程序仅被授予执行其功能所需的最低权限，避免使用具有过高权限的账户。
补丁与更新管理	及时安装操作系统、应用程序和固件的安全补丁，修复已知漏洞。
安全配置基线	制定并实施符合行业标准（如 CIS Benchmark）和企业政策的安全配置基线，定期审计配置合规性。
日志审计与监控	启用详细的系统和应用日志，对异常登录、权限变更、关键文件访问等事件进行实时监控与告警，并定期进行日志分析。
数据保护	对敏感数据进行加密存储和传输，实施数据备份与恢复策略，确保数据的完整性、可用性和保密性。
网络隔离	利用防火墙、VLAN 等技术对服务器进行网络隔离，限制外部访问，并对服务器之间的通信进行严格控制。
安全软件部署	部署防病毒软件、入侵检测 / 防御系统（HIDS/HIPS）等安全工具，提供额外的保护层。
虚拟化安全	确保 Hypervisor 层安全，实施虚拟防火墙或微隔离，对虚拟机间通信进行控制，防止虚拟机逃逸。

第五节 应急响应体系

一、应急响应组织与流程

（一）应急响应小组组建

电力通信网络的应急响应工作中经常要跨部门、跨层级进行协作配合。因此建立一支高效的应急处理队伍，是取得成功的保证。该组一般由决策层、管理层和技术执行层构成，呈现出金字塔形的指挥调度架构。决策层一般由公司分管领导担任；管理层为通信职能部门的负责人；技术执行层为网络专家、系统管理员、安全分析师、设备厂商的技术支持人员，他们做具体的故障排查和恢复工作。人员选拔不能只看重技术能力，还要考虑心理素质和抗压能力，保证在紧急、高压的情况下仍能保持冷静的判断。

为了使应急响应小组实战中能迅速集合、有效发挥作用，日常的动态管理以及能力培养也不能忽视。组织内部应建立定期的队员信息更新制度，保证联络渠道畅通无阻，指定替代人员，以防重要人员缺席时出现响应链条中断。小组的成员需要定期参加模拟演练，通过红蓝对抗、桌面推演等方式来提高团队的配合默契程度，并掌握各种处置工具及平台。针对电力通信网络所具有的特性，还需要设置专门的技术小组，来负责继电保护通道、安全稳定控制系统等重要的业务，在涉及电网安全的关键业务受到损害的时候，可以获得最高优先级的技术资源支持。这对于全方位、立体化的应急响应人才队伍建设具有举足轻重的作用。

人员职责分工在组建之初就要明确，防止事故处理时互相推诿责任的情况发生。一般采取主岗负责、副岗协助的方式，每个关键技术岗位至少配备两人。发生突发的大规模网络瘫痪或者恶意攻击事件时，应急小组可以马上分成若干个职能小组，分别开展监测分析、抑制攻击、系统恢复以及对外通报等任务。模块化的组织方式提高应急处理的效率，从而保证了电力通信网络安全运行。

（二）应急响应预案制定

完备的应急预案是现场处置工作的行动指南，应急预案的制定要以全面认识电力通信网络潜在风险为基础。预案体系要包含自然灾害、人为破坏、设备故障、网络攻击等各类风险情景，还要按事件影响范围和危害程度来分等级分类。制定过程中要充分考虑电力生产业务的特殊性，把保证电网调度数据网、综合数据网

等核心业务的连续性放在第一位。预案内容除了要包含处置操作手册外，还要包含物资调配、后勤保障、舆情应对等辅助环节的预案，保证应急响应工作整体协同、系统联动。

针对不同类型的突发事件，预案应当具备高度的针对性与可操作性，通过细化场景来提升指导价值：

1、对于网络攻击类的事件，预案需要确定出攻击特征的辨识方式、流量清洗设备的分布方案、防火墙阻断规则的下达途径，在第一时间就阻止攻击源。

2、针对物理灾害类事件，预案要详细规划备用光缆路由的启用方案，应急通信车的布设地点，卫星通信链路的建立流程，保证极端情况下仍能保持通信畅通。

3、核心设备出现故障时，要准备好详细的备品备件清单，厂家技术支持的联系人和电话也要备齐，同型号设备的快速替换和配置恢复指南不能缺少，这样可以尽量减少业务中断的时间。

预案的生命力就在于不断的修编，一成不变的文档不能有效应对瞬息万变的安全威胁。电力企业要形成应急预案的动态演练和评价体系，在电网结构变动、新技术采用或者外部安全环境发生变化的时候，及时对预案加以修订。每次应急演练结束之后，都应当有专人开展复盘分析工作，认真分析演练过程中存在怎样的缺陷和不足，并及时对陈旧的处理程序以及联系信息做出更改。只有保持预案的实时性、鲜活性，才能保证应急响应人员在真正的危机来临时，能够根据预案做出最正确的判断和行动，将损失降到最低。

二、应急响应技术手段

在现代电力通信网络的应急处置中，面对的是海量的数据环境，已经不能像以前一样，单纯的依靠人工处置，必须借助先进的技术手段来辅助提高应急处置的效率。建立一个包含备份恢复、业务保障、溯源取证的综合技术支撑体系，是解决复杂的网络安全问题的唯一途径。

电力通信网络应急响应技术手段涵盖了多个方面，见下表所示：

电力通信网络应急响应技术手段概览

技术手段分类	主要技术 / 策略	主要目标 / 作用
系统备份与恢复	定期自动备份、全量 / 增量备份、物理隔离与异地存储、虚拟机快照、容器镜像、自动化恢复工具、持续数据保护、异地容灾中心	确保数据完整性与可用性；大幅缩短系统恢复时间目标
业务连续性保障	环网保护、双归属接入、路由热备份、物理路由分离、智能光网络、服务器集群、负载均衡、流量清洗与整形、微服务架构与容器化部署、降级服务策略、双路市电、不间断电源、柴油发电机、环境监控	保证核心业务最低限度运行；抗击局部故障与大规模攻击；保障不间断动力与环境支持
攻击溯源与取证	多源异构日志收集、大数据分析 & 关联挖掘、专业取证工具、威胁情报共享、外部合作机制、蜜罐与欺骗防御、可视化溯源图谱	查明攻击真相与路径；固定电子证据；完善防御策略；实现人员级归因；由被动响应转向主动侦察反制

（一）系统备份与快速恢复

系统备份与快速恢复技术属于电力通信网络抵抗灾难的最后一道壁垒，和数据资产能不能延续息息相关。电力行业的数据完整性、可用性是非常重要的，必须创建起一个多层次、多种策略的备份系统。对关键业务系统使用的操作系统、数据库、配置文件、应用日志等要实行定期的自动备份，采用全量备份与增量备份结合的方法，既能保证数据的完整性又能提高存储效率。存储介质要完成物理隔离并且存放到异地，防止本地机房一旦遭遇火灾、水灾或者受到勒索病毒攻击的时候，主备数据一起消失引发灾难性结果。随着虚拟化、云技术在电网中广泛使用，采用虚拟机快照、容器镜像等技术实现分钟级系统状态备份已经成为常态，大大缩短了备份窗口。

快速恢复能力的建设重点就是缩短恢复时间目标，即系统在业务中断之后能够最快地重建服务能力。这就需要使用自动化编排工具、一键恢复脚本等把繁琐的恢复过程转为标准化的、代码化的流程，从而大大降低由于人工操作造成的出错率和等待时间。对调度自动化、配电自动化等关键业务应该采用持续数据保护技术，在发生数据变动的时候实时捕获到数据变更并记录下来，系统可以回滚到任意时间点，这样极大的提高了抵抗勒索软件攻击和人为误操作的能力。实战演练时一定要检验备份数据能否正常运用，恢复脚本是否有效，避免出现“备份成功但是不能恢复”的尴尬局面。

异地容灾中心属于系统备份技术中比较高级的一种。它利用地理上分散布置

主备数据中心的方式，达到跨地域数据实时同步以及业务接管的目的。当主中心出现重大故障的时候，可以用全局负载均衡、域名切换等技术将业务流量无感知的转移到备用中心。尽管双活或多活数据中心架构的建设成本较高，但是对于支撑国家关键信息基础设施的电力通信网络来说，这是保证极端情况下业务不瘫痪的必要投入。不断改进数据同步算法、链路带宽管理可以有效地降低数据丢失的风险，保证电网神经中枢的安全。

（二）业务连续性保障

业务连续性保障技术，是指电力通信网络在局部发生故障或者受到攻击的时候，其核心业务仍能维持最低限度的运行水平，不会造成大面积的瘫痪。这就需要在网络结构，传输链路，应用交付等多方面做冗余设计以及优化。在网络层面广泛使用环网保护、双归属接入、路由热备份协议等方式，保证单节点或者链路出现故障时，不会产生网络孤岛。承载生产控制大区业务专线网络的物理路由隔离也十分严格，以防止由于同沟同缆造成共模风险。另外还可以使用智能光网络技术完成毫秒级的光层切换，保证继电保护等实时业务不发生延时。

为了应对应用层面的冲击，各种高可用性技术被集成到了电力业务系统当中，形成了很强的服务提供能力：

1、使用服务器集群以及负载均衡技术，把业务请求分发到多台计算节点上。当某一台服务器出现故障的时候，流量就会被自动剔除并重新定向，服务端对此一无所知。

2、当发生分布式拒绝服务攻击的时候，部署流量清洗和整形设备可以识别出恶意流量，优先处理和转发正常的业务报文。

3、用微服务架构和容器化部署实现故障域隔离及熔断。当非核心功能模块出现异常时，不会影响整个系统的稳定性，并能通过降级服务策略来优先保证核心功能的可用性。

业务连续性要控制好电力供应、环境监控、供应链安全这些外部依赖的资源。通信机房均设有双路市电引入、大容量 UPS 及柴油发电机作后备，保证通信设备有连续的动力供应。环境监控系统采集温湿度、烟感、水浸数据并联动精密空调、消防设备等来消除物理环境对设备的威胁。全方位的技术保障措施交织成一张严密的防护网，在狂风暴雨般的攻击和故障面前，保证电力通信网络能够挺立不倒，持续守护电网的跳动。

（三）攻击溯源与取证

应急响应过程中，攻击溯源、取证技术对于打击网络犯罪、完善防御策略有极其重要的作用，对重要信息基础设施所面临的大规模、长时间的网路攻击而言更是如此。因此需要建立全网视角的安全监测、日志留存体系，收集防火墙、入侵检测系统、主机审计、数据库审计等多源异构日志。运用大数据分析以及关联挖掘技术，从大量的碎片化信息当中重新拼凑出攻击链条，还原攻击者入侵的路径，内部网络横向移动的轨迹，以及具体的数据窃取操作等，给溯源工作赋予详实的数据支撑。

取证工作必须依照法律程序和技术规范，以保证提取的电子证据具有法律效力。技术人员要依靠专门的取证工具，对受侵害系统的内存镜像，硬盘数据和网络数据包实施固化提取，还要算出哈希值来保证数据的原始完整。对于易失性数据的获取只能争分夺秒，首先获取网络连接状态、进程列表、打开文件句柄等现场数据。同时威胁情报库和外部合作机制对捕获的恶意样本进行逆向分析，获取其通信特征码、控制域名等信息并与全球威胁态势关联，试图达到对攻击组织、来源和动机人员级的归因。

为了提高溯源的准确性，蜜罐以及欺骗防御技术被加入到电力通信网络的主动防御体系当中。在网络侧部署高仿真虚拟电力业务系统以及假数据，从而诱骗企图入侵的攻击者。一旦攻击者接触到蜜罐，系统就会对其所有的操作指令、工具指纹、惯用战术等进行全程记录。不仅可以有效地推迟攻击者对于真实目标进行探测的时间，也可以为防御方获取第一手的攻击情报。这种“请君入瓮”的办法，把原来的被动挨打局面变成主动出击的侦察，使应急响应由事后的补救变为事前的诱捕和反制，把电力通信网络在网络空间的防御能力提升到诱捕和反制的水平。通过可视化溯源图谱把晦涩的技术数据变成一目了然的攻击视图，让决策者可以快速认清威胁真面目，从而制定出更加精准的长期防御计划。

第七章 电力通信网管理技术

第一节 网络管理系统

一、网管系统功能架构

（一）性能管理、故障管理、配置管理、安全管理、计费管理

性能管理就是监测网络运行状态以及服务质量状况。它会一直收集网络里的流量，延迟，丢包率这些重要的性能指标数据，然后按照事先设定好的阈值来找出可能存在的性能瓶颈。监测数值如果超出正常范围就会立刻发出警报并形成性能趋势报告，给网络的改善与扩容给予科学的数据支撑，保证网络一直处在最好的工作状态。

故障管理的主要目的就是及时发现并消除网络中出现的异常情况。网络设备或者链路发生中断、误码率过高这样的状况时，故障管理模块马上会接到告警信息，然后通过关联分析技术对大量的告警信息进行过滤以及关联分析，从而找到最根本的故障原因。系统可以自动分发工单，甚至可以执行自动恢复操作，大大缩短故障修复时间，减少电力业务受影响的范围。

配置管理做网络资源的初始化、变更和核查。保存有全部网络设备的配置信息数据库，包含端口参数、路由策略、电路交叉连接等等一些重要的信息。运维人员通过配置管理界面发出指令，就可以远程进行业务的开通、修改操作，不需要亲临现场。该模块还具有配置一致性校验的功能，可以有效地避免由于人为失误造成网络中断的情况。

安全管理、计费管理在电力专网中虽然侧重点不同，但是都必不可少。安全管理主要是对网管系统进行安全访问控制、操作日志审计、数据加密等工作，从而达到防止非法入侵和恶意篡改的目的。计费管理在电力内部市场化结算场景下使用，对各个业务部门占用的通信资源详细记录。尽管电力通信一般采用自有的专用网络，但是对资源占用率进行统计，仍然可以给分摊成本提供量化的依据。

（二）网管系统的层次化架构

电信管理网模型把管理功能自下而上分成网元管理层、网络管理层、业务管理层、商务管理层。电力通信领域将其简化具体化之后，就形成了层次化的管控结构。底层直接对接具体的物理设备，向上层隐藏硬件细节，给上层提供统一的逻辑视图。

网元管理层同通信设备存在直接交互，主要针对单个网元的配置，告警监视以及维护工作。它处理的数据粒度最细，一般由设备厂商提供专用网管软件。网络管理层从全局的角度去管理跨多网元的端到端连接，解决跨子网的路由和保护倒换等跨子网的问题，主要处理整个通信网络的拓扑结构和连通性。分层设计使得上层管理系统可以只做业务逻辑上的工作，不用去处理底层复杂的硬件指令。

（三）集中式与分布式网管

集中式网管架构把所有的管理功能都集中到高性能服务器集群上，用广域网把各个地市的被管设备连接起来。该架构的优点是数据集中，利于全网资源的统一调度和综合分析，运维人员在调度中心就可以掌握全省或者全网的通信情况。但由于数据汇聚在一点上，对大规模网络实时处理要求很高，一旦中心节点出现故障，全网的管用功能就会瘫痪。

分布式网管架构把管理功能分散部署到各个区域或层级节点上，采取化整为零的方法。各个分部网管各自负责本区域的网络监控，只把经过筛选的重要信息传给上级网管。有效地减轻了中心链路带宽的压力，提高了系统的容灾性以及扩展性。电力通信网当中，末端接入节点数目呈指数级增加之时，混合式架构，也就是把分散式的采集同集中式的展现融合起来的做法，便成了一个趋向。

1. 集中式管理适合骨干传输网，可以全局优化、快速开通端到端业务，有利于统一安全策略的实施。

2. 分布式管理更适用于配用电通信接入网，能很好地满足大量分散节点接入的要求，提高了边缘侧的故障响应速度。

二、网管接口与协议

网管接口和协议是管理系统同网络设备之间、不同层次的管理系统之间的信息交换的通道。标准化协议可以消除设备厂商之间的壁垒，达到异构网络互联互通的目的。由于电力通信网的发展，现已出现多种协议并存的现象，不同时期的、

不同技术体制的设备使用的协议也不一样。

网管接口协议特性对比表

协议名称	主要特点	应用场景	优点	缺点
SNMP	请求 - 响应模式； MIB；陷阱机制	IP 网络设备监控 与管理(路由器、 交换机、服务器)	简单易用；带宽占 用小；广泛支持； SNMPv3 提供安全	早期版本安全性差； MIB 结构复杂；对复 杂业务逻辑支持有限
TL1	面向人机交互； ASCII 文本；指 令清晰	SDH/MSTP 等传 输设备管理	直观易读；指令执 行效率高；响应结 构固定易解析	描述复杂数据结构能 力有限；主要用于命 令行交互
CORBA	面 向 对 象； IDL；透明通信	异构系统间集成； 复杂拓扑 / 告警 数据传输	跨平台、跨语言； 封装复杂业务逻辑； 支持复杂数据模型	技术门槛高；开发维 护复杂；性能开销相 对大

上表列出了常见网管接口协议的特性对比。

(一) SNMP 协议

简单网络管理协议目前是使用最广泛的网管协议，在数据通信领域占主导地位。它使用请求 - 响应的客户端服务器模式，管理站通过发送查询请求来获得代理进程中的管理信息库数据，代理进程也可以主动向管理站发陷阱消息报告异常事件。该协议简单易用，对网络带宽占用很小。

该协议经过不断的改进，功能也越来越完善。早期版本过于简单，存在先天的安全漏洞，明文传输的团体名很容易被截获。SNMPv3 版本中加入用户安全模型、视图访问控制模型等安全机制，有认证、加密传输等特点，安全性得到提高。在电力调度数据网、综合数据网的管理中，该协议被广泛地用于对路由器、交换机、服务器的状态进行监视，是实现 IP 网络可管理性的基础。

(二) TL1、CORBA 等北向接口

北向接口是指网元管理系统与上一级网络管理系统之间，实现跨厂商综合管理的接口。事务语言 1 是一种面向人机的事务操作语言，用 ASCII 码文本格式表示，具有很好的可读性。虽然属于较早的技术，在 SDH 传输设备管理中至今还有大量的应用。运维人员可以直接使用命令行和设备进行交互，其响应消息结构固定，容易上层软件解析。

公共对象请求代理体系结构属于面向对象技术体系里的关键接口技术。它用接口定义语言来定义对象的方法、属性，使得不同编程语言、不同操作系统下的应用程序可以透明地通信。在电力通信综合网管创建时，它在很长一段时期内都

是主流的北向接口标准，用来传输复杂拓扑数据和告警信息，达成异构系统之间的无缝对接。

1. TL1 接口以文本流为基础，指令清晰直观，适合执行单一、确定的维护操作，如查询光功率、复位单板等，解析效率高但描述复杂数据结构的能力有限。

2. CORBA 接口基于对象模型，能够封装复杂的业务逻辑与数据关系，适合处理网络拓扑同步、端到端电路配置等高层管理任务，但开发与维护的技术门槛相对较高。

（三）厂家私有协议与接口

虽然标准化组织制定了大量的通用协议，但是设备厂商为了提供不同的功能特性或者提高在某个场景下的性能，会开发出自己的管理协议和接口。私有协议一般能够对设备的底层寄存器进行深入的访问，可以完成标准协议所不能实现的高级诊断以及精细的控制。

私有接口的存在给电力通信网统一管理造成困难。为了把设备接入综合网管平台，开发人员必须为每种私有协议编写专门的适配器或者解析插件，从而增大系统建设的工作量以及后期维护的成本。电力公司对设备的选取以及网络管理系统的创建进行规划时，一般会要求厂家开放私有接口文档，或者给出标准化的中间件，以此来消除“信息孤岛”，保证全网管理的一致性、完整性。

三、电力通信综合网管

由于电力通信网中存在传输、交换、数据、接入等不同的技术体制，且存在多厂商设备混合组网的情况，因此建立一个统一的电力通信综合网管系统是必然的。该系统可以屏蔽底层网络的异构性，给调度员、运维人员提供一个全方位的网络视图，达到跨专业、跨区域协同管理的目的。

（一）多厂家、多技术网元统一管理

综合网管的第一个主要工作就是解决异构网络的接入问题。采用适配层技术之后，系统可以同时支持 SNMP、CORBA、Telnet 等南向接口协议，把各个厂商、各个型号设备所产生出来的原始数据转换成统一的内部数据模型。经过标准化之后，上层应用就不必考虑底层具体的实现方式，对华为、中兴、烽火等不同品牌的设备也能够进行统一管理。

综合网管对 SDH、OTN、PTN、IP/MPLS 等多种技术进行了融合管理。可

以跨越技术边界，建立起各个网络资源之间的联系。当发生光缆中断时，系统不单可以查出物理层断点位置，还能够自动地分析出受影响的传输电路和其所承载的业务通道，进而可以对故障原因做跨专业定位、业务受影响分析等。

（二）资源管理与拓扑呈现

资源管理是综合网管的主要模块，包含空间资源、物理资源、逻辑资源、业务资源等各方面的信息。系统建立详细的资源台账，对机房、机柜、板卡、端口、时隙、波道等网络要素的基本情况及占用情况做详细的记录。这些数据不仅可以做日常维护，也可以为网络规划、资产全生命周期管理提供准确的依据。

拓扑呈现功能用可视化技术把枯燥的数据转成直观的图形界面。系统可以分层、分域地显示拓扑图，用户可以从宏观的地理信息系统地图逐级下钻到微观的设备面板图。动态拓扑技术是根据网络的状态变化而不断对拓扑视图进行更新，链路的通断、流量的拥塞等情况用不同的颜色或者线条粗细来表示，使运维人员可以及时的了解网络的状态。

（三）与其他管理系统的集成

电力通信综合网管不能孤立存在，必须与电力企业的其他信息化系统融合，实现业务流程自动化流转。与调度管理系统互联之后，通信检修计划就可以和电网调度计划同步，从而防止通信中断干扰电网控制业务。和地理信息系统结合之后，给光缆线路的巡检、抢修工作提供准确的空间位置服务。

业务开通、故障处理过程中综合网管同 IT 服务管理系统、电子工单系统对接非常重要。网管发现严重故障后，会自动打开工单系统，产生抢修任务单，下发给对应的维护人员手持终端。维护人员处理完毕的反馈信息会回到网管系统的里面，形成闭环。这种跨系统的流程整合冲破了部门之间的壁垒，明显加快了电力通信运维的总体反应速率，而且很大程度上改善了精细管理的水平。

第二节 性能监测技术

一、性能指标体系

(一) 网络层性能指标

网络层性能指标主要用来反映通信链路上的传输质量以及连通情况，是评价基础网络是否健康的依据。电力通信网当中，传输时延属于最关键的指标之一，对于继电保护这类实时性要求非常高的业务而言，连毫秒级的时延抖动都不能接受，否则就会引发严重的电网事故。因此需要微秒级别的高精度测量端到端往返时延和单向传输时延。吞吐量体现的是网络带宽的利用情况，也是衡量当下链路承载业务流量的能力指标；当吞吐量过大时，就会占用很多网络带宽，很容易引发网络拥塞，所以要和链路容量一同进行实时监控并实施动态调度。

丢包率是网络层可靠性的一个方面。长距离光纤传输或者微波通信过程中，信号衰减、噪声干扰、设备缓存溢出等都会造成数据包丢失。电力调度数据网的丢包率需要区分突发性丢包和周期性丢包，从而可以判断链路质量下降是由瞬时干扰还是设备故障所导致。而误码率更多地被用来进行物理层和链路层的监测，它是通过单位时间内传输出错的比特数目来进行对光缆、电缆等传输介质的物理特性和光模块工作状态的检测。

除上述基本指标外，网络层的可用性指标也不能忽略。它是用来度量链路在一段时间里正常工作的时间占总时间的比例，从而反映出网络的稳定性。核心骨干网一般要达到五个9的可用性，即99.999%以上。为了实现上述目的，网络层性能监测还要包含路由收敛时间、保护倒换时间等动态指标，保证业务在网络拓扑发生变化或者出现故障的时候可以快速恢复，保证电力生产业务的连续性。

(二) 业务层性能指标

业务层性能指标直接关系到用户的最终体验和电力业务的执行效率，是衡量通信网服务质量好坏的标准。和数据包传送重视的网络层不一样，业务层更注重的是应用交互的响应速度和成功率。

1. 业务响应时间是衡量系统交互效率好坏的标准。电力营销系统中指的是客服坐席查询用户信息所耗费的时间；配电自动化系统中指的是主站下发指令到终端反馈执行结果的总时间。该指标受网络传输的影响，也和服务器处理能力、数

数据库查询效率有关，因此需要分段监测才能找到瓶颈所在。

2. 业务连接成功率可以体现系统服务的可靠性。当系统并发量很高的时候，大量的终端设备会同时进行连接请求，系统需要立刻统计握手成功的次数、握手失败的比率。连接成功率低，认证服务器忙，IP 不足或者开启了防火墙。对建立连接、保持连接、断开连接的全过程进行监测，可以评价业务系统承载极限和健壮性。

（三）设备层性能指标

设备层是电力通信网的基础，设备层的性能指标指的是路由器、交换机、光传输设备、服务器等硬件设备的运行状况。中央处理器利用率属于设备计算负载的关键参数，如果其数值偏高，可能会引发数据包处理延迟或者丢包，一般需要设置分层阈值来实施监测。内存使用率同样不能忽视，内存泄漏或者长时间占据高位会引发设备死机，尤其对于那些负责管理复杂路由表项或大量并发连接的核心节点来说，对内存进行监控就显得十分重要。

端口性能指标是设备层监测的主要内容，端口流量收发速率、端口错误包统计、端口丢弃包统计、端口光功率水平等都属于端口性能指标。对光传输设备来说，发光功率或者收光功率过小都会引起误码率上升，严重时还会引发链路断开。实时读取光模块的数字诊断监控信息，可获得电压、电流、温度等底层物理参数，可以提前发现光器件的老化趋势或者异常故障，在业务受到影响之前进行预防性维护。

设备的环境适应性指标，也是性能监测不可缺少的一部分。电力通信设备大多设置于变电站、配电房这样的地方，温度，湿度，电源电压，风扇转速这些环境参数都会对设备的寿命和稳定状态产生影响。高温会造成芯片降频或者烧毁，高湿度容易引发电路板短路。利用设备内部集成的传感器获取环境数据，与设备自身运行指标进行关联分析，可构建设备健康度画像，给运维人员提供改善设备运行环境的建议，使硬件设施长期稳定地在规定的环境范围内运行。

设备层性能指标还要包含板卡状态、冗余配置的检测。主控板、交换板、电源模块等重要部件一般都采用冗余备份的形式，监测系统必须随时对主备状态是否正常、倒换功能是否就绪进行确认。一旦发现备用板卡出现故障或者同步状态出现异常，就要立即发出告警信号，避免主用板卡出现故障时陷入“单点失效”的危险。这种深入的硬件级别的监测，就是通信网高可靠性物理基础。

电力通信网关键性能指标分类表

指标类型	关注层面	典型指标	关键作用
网络层	链路传输质量与连通性	传输时延、吞吐量、丢包率、误码率、可用性	衡量基础网络健康，保障数据传输稳定
业务层	用户体验与业务执行效率	业务响应时间、连接成功率	评估通信网服务质量，优化用户体验
设备层	硬件设备运行状态	CPU 利用率、内存利用率、端口流量、光功率、环境参数、板卡状态	监测硬件健康，预防设备故障与老化

从表中可以看出电力通信网性能指标体系是个多级、多维的综合性监测体系，用以全面保证电网业务运转的稳定性。

二、性能数据采集与处理

（一）主动探测与被动采集

主动探测技术通过模拟用户的操作行为或者注入测试流量的方式，来对网络端到端的性能进行检测。不需要依靠用户实际流量，可以在网络空闲的时候或者业务部署之前来评价网络质量。常用方法有发送互联网控制消息协议回显请求测量往返时延和丢包率，或者使用专门的性能测量协议做详细的抖动、单向时延测试。主动探测控制性强，可以对某一条特定路径或者某一类业务进行定向检测，但会消耗一定网络带宽资源，因此探测时应该合理设置探测频率、流量大小等，以避免对生产业务产生影响。

被动采集技术就是不干扰现有的网络流量，使用镜像端口、分光器或者设备自身统计功能来获取真实的业务数据。简单网络管理协议目前使用的最多的被动采集方式，管理站对设备代理进行轮询，得到接口流量、设备负载等标准管理信息库数据。网络规模扩大之后，基于流的技术开始受到人们的喜爱，它能提供会话级别的流量统计，诸如源地址、目的地址、应用协议类型以及流量特征等，给精细化的流量分析赋予了丰富的数据来源。

遥测技术是新的采集手段，正在慢慢取代传统的轮询。它采取推送形式，设备可以亚秒级频率主动把性能数据推送给采集器，极大减小了数据采集的时延，实现了接近实时的网络状态感知。软件定义网络架构里，遥测技术能够把带内网络遥测结合起来，把每一跳设备的转发时延、队列深度这些信息加入到数据包头

当中，这样就可以对每一个数据包在全网路径上的走向进行精确跟踪，并对其性能实施全方位的透视，这为解决微突发拥塞这种瞬时性的问题给予了强大的手段。

（二）性能数据的存储与压缩

电力通信网产生性能数据有明显的时间序列特征，并且数据量会随着监测颗粒度细化呈指数级增长。传统的关系型数据库处理海量高并发写入、范围查询时力不从心，所以高性能的时间序列数据库成为了存储性能数据的理想选择。时间戳索引的优化使每秒可以写入百万级的数据，并且数据的压缩率非常高。采用列式存储结构，把相同的指标数据连续存放起来，依靠数据的时间连续性和相似性，从而大量削减磁盘所占的空间。

为了降低存储成本，提高查询速度，在性能数据处理过程中，数据压缩算法起着至关重要的作用。无损压缩算法，例如游程编码、差分编码等，在去除数据中冗余信息的同时，并不会损失数据的精度。针对长期归档的历史数据，采用有损压缩或者降采样技术，在保证数据整体趋势以及关键特征点（最大值、最小值等）的前提下，将秒级数据聚合为分钟级或者小时级数据。可以满足近期故障排查时对高精度数据的需要，也可以满足长期趋势分析时对存储容量的需求。

（三）性能数据的可视化展示

把枯燥的性能数据变成直观的管理信息，这才叫可视化。运维人员通过图形界面可以对整个网络的运行状况有清晰的认识。拓扑视图是最基本的展现形式，它把地理信息系统和逻辑拓扑融合起来，在地图上清楚地显示出各个站点、链路之间的联系，而且用颜色编码（红、黄、绿）来实时渲染各个网元的性能状况。当某条链路负载过重或者出现中断的时候，拓扑图上对应的线条就会变色闪烁，从而让调度员快速定位到故障区域。

仪表盘视图主要是显示重要的性能指标。根据不同层级的管理者来定制不同的仪表盘。决策层关心整个网络的健康等级评分、核心业务系统可用率这样的宏观数据，技术层则更在意具体的设备 CPU 使用曲线、接口流量趋势图这种微观数据。热力图是一种形象的网络流量分布显示方式，用颜色的明暗程度来表示各个区域或者链路的负载状况，可以清楚地显示出网络中的热点及瓶颈所在，从而对网络进行扩容和流量均衡。

趋势图 and 对比图在性能分析中使用较多。通过将现时的性能曲线叠加在同期历史数据、基线数据上，就能发现性能突变、异常。用本周末流量模式和上周同

时间段的流量做对比，若某个时段流量突然增大，有可能存在违规接入或者病毒感染的风险。多维关联视图把网络性能与业务质量、设备环境等数据放在同一个时间轴上显示，使运维人员可以找到性能波动背后深层次的原因，例如温度上升是否会降低光功率、进而引起误码率上升等。

第三节 故障诊断与处理

一、故障管理流程

（一）故障发现、定位、排除、验证

电力通信网在正常工作时，故障的发生就是整个处理过程的开始，主要是网管系统实时监控和告警上报。当通信设备或者链路发生异常情况的时候，网管系统就会凭借声光报警，短信通知等方式，马上把警告传达给运维人员。用户因业务中断或者性能下降而发出的申诉，也是重要的发现途径。运维人员在收到故障信息之后，第一时间开展初步的判断，查看告警详情并分析业务受影响的范围，以此来判定故障是否真实存在以及紧急程度如何。这一阶段要求监控系统具有很高的灵敏度，可以发现误码率上升、光功率下降之类的细微异常，在业务彻底中断之前发出警告。

定位是最重要、最耗时的一步，要使用逻辑分析和物理测试的方法。运维人员按照网络拓扑结构，按照告警流向和相关性分析，将故障点一步步收敛到某个网元、某个板卡或者某个端口。对于复杂的故障，还要用到光时域反射仪、误码仪等仪器做分段测试或者环回测试判断故障位置。准确的位置可以防止盲目派单，大大提高抢修效率。找到故障根因之后，排除工作就紧跟着开展起来，更换硬件、熔接光缆、重启软件、回滚配置这些操作都是可能涉及的。

故障排除的验证环节不能轻视，它关乎故障排除的最终质量。运维人员要确认告警是否完全清除，各项性能指标是否恢复正常范围，与业务部门一起测试，保证电力调度数据、继电保护信号等重要业务传输的准确无误。只有业务稳定运行一段时间以后，才可以判断故障已经处理完成。整个过程要详细记录并归档，形成完备的故障处理日志，为后面复盘分析赋予丰富的数据支撑，保证每次故障处理都变成改进运维水平的财富。

（二）故障级别划分与上报机制

电力通信网所承载的业务重要性是有差别的，因而故障处理应实行分层分类的管理。一般将故障分为特别重大、重大、较大、一般四个等级，根据故障对电网安全生产造成的影响大小、业务中断范围、修复难易程度来判定。特别重大故障一般会干扰电网的正常调度，造成电网中断，属于最高级别的应急响应事件，需要调动全网的资源来进行抢修。一般故障只是对非核心设备或者局部的非重要业务造成影响，处理时限比较宽松。分级机制保证运维资源有限时，最重要的业务先得到保障。

上报机制则是故障信息在组织内部高效流转的保障，明确了不同级别故障的汇报路径与时限要求。

1. 一般故障在规定时间内上报给地市级通信调度部门，由其协调本地资源进行处理，并定期汇报进展情况。

2. 对于较大及以上级别的故障，必须立即上报，运维人员在发现故障后必须在极短的时间内，越级上报至省级或者国家级电力通信调度中心，并且通知同级安监、运检等有关部门。

3. 故障处理时要定时续报，保证各级指挥机构知晓抢修进程和现场状况，从而在需要的时候给予技术支持或者物资调配。

严格的上报机制打破了信息孤岛，使故障处理从“单打独斗”转变为系统协同作战。

（三）故障知识库管理

故障知识库是电力通信网运维的结晶，它把历史故障案例、典型处理方案、设备维护手册、专家经验以结构化的方式存起来、管起来。一个完善的知识库不能仅仅是文档的堆砌，而应该具备强大的检索和关联功能。当运维人员碰到不熟悉的或者复杂的故障现象时，只需要输入关键词或者故障代码，就可以很快从知识库中找到相应的故障案例及解决方法，从而大幅度地缩短故障排查的时间。知识库的建立是动态的，每一个新的故障处理结束之后，经过审核通过的标准化案例要立即加入到知识库中，不断充实知识库。

知识库的管理包括了对于隐性知识的挖掘和传承，资深运维人员的经验大多以个体知识的形式存在，而知识库的建立就使得这些知识成为组织的共有资源。系统可以对知识库里的数据执行统计分析，找出频繁出现的故障点，普遍存在的

问题，从而给设备选择，网络规划，人员培训等给予数据方面的支撑。利用知识库做模拟故障演练和培训，也是提高新员工技能水平的一种方式。经过长时间的积累和改进，故障知识库会成为智能运维系统重要的数据底座，为以后实现自动化诊断打下坚实的基础。

二、故障诊断技术

伴随着电力通信网规模的爆发式增长，传统的依靠人工经验的诊断方式已经不能满足时效性和准确性的需求。用算法和算力对大量的告警数据做深度的挖掘与智能分析，是提高网络运维智能化的必由之路。

下表对电力通信网中常见的故障诊断技术进行了详细对比：

常见故障诊断技术对比表

技术类型	核心原理	优势	局限性	适用场景
告警关联与压缩分析	基于拓扑、时间、层级关系，识别根因告警并过滤衍生告警	消除告警风暴，聚焦根因，大幅降低运维人员压力，提升定位效率	规则依赖预设，难以应对未知拓扑或新型故障	大规模、复杂电力通信网的日常告警管理，快速识别已知故障根源
基于专家系统的故障诊断	模拟专家知识与推理过程，通过“如果-那么”规则进行判断	解释性强，诊断逻辑清晰，处理标准化、规范化故障效率高且准确	知识获取困难，规则库维护成本高，难以处理未知或非典型故障	常见、规范化故障的快速诊断与处理，辅助经验传承
基于机器学习的智能诊断	从历史数据中自主学习故障模式与规律，进行预测与识别	能够处理复杂、非线性数据，发现潜在故障模式，实现早期预警和自进化	依赖大量高质量数据，模型训练与调优复杂，解释性相对较弱	复杂网络环境下的故障预测、早期预警、未知故障模式发现，以及自动化运维

（一）告警关联与压缩分析

大型电力通信网经常会出现由于单个网络故障而引发的“告警风暴”现象，即一个根源告警（光缆中断等）会导致下游大量网元出现信号丢失、帧失步、业务中断等衍生告警。成千上万条告警涌入网管系统，很容易淹没重要信息，使运维人员陷入数据迷雾中。告警关联与压缩分析技术就是为解决上述痛点而产生的，它用预设的拓扑规则和逻辑算法对原始告警流进行过滤、归并、根因推断。技术关键就是找出告警间的因果联系以及时间相关性，对某个时间段内、某个拓扑路径上的一连串衍生告警实施屏蔽或者折叠操作，只把最重要的根源告警呈现给运维人员。

分析技术主要包括时间窗关联、拓扑关联、层级关联这三个方面。时间窗相关关注极短时间内发生的告警序列，拓扑相关根据网络连接关系判断上下游设备告警的逻辑联系，层级相关在物理层、链路层和网络层之间建立映射，物理层的光路中断必然导致上层协议全部失效。经过多维度综合之后，此系统能够自行消除重复的信息，告警被压缩的比例可以达到 90% 以上。很大程度上减轻了监控人员的视觉疲劳，提高了故障定位的准确性，为之后的自动派单处理争取了时间。

（二）基于专家系统的故障诊断

专家系统是模拟人类专家解决复杂问题的计算机程序，它被广泛应用到电力通信网的故障诊断当中。它由知识库、推理机两部分组成。知识库中存有资深通信专家总结出的产生式规则，也就是“如果……那么……”的逻辑判断。当接收光功率低于阈值且误码率不断增大的时候，就判断为光路衰耗过大。推理机把实时采集的网络状态数据同规则库加以比对，经由正向或者反向的推理链条，自动生成故障原因并给出处理建议。

专家系统最大的优点就是解释性很强，可以很明确地告诉运维人员自己的判断理由，在面对常见的、规范的故障时，速度快、准确。可以实现全天候不间断工作，弥补人工值守由于疲劳、情绪变化等因素造成的不足。为了应对网络技术的不断更新，现代专家系统一般都加入了动态规则更新机制，可以使得运维人员自由地添加或者修改新的设备、新的特性所对应的规则。尽管专家系统对于未知的、非典型的故障不能很好地处理，但是它在标准化的运维场景中仍然起着不可替代的作用。

（三）基于机器学习的智能诊断

网络环境越来越复杂，简单的规则已经不能完全地刻画出故障模式了，于是基于机器学习的智能诊断技术应运而生。机器学习算法不同于专家系统那样依靠预先设定的规则，而是可以从大量的历史数据中自我学习，找到其中的规律。经过清洗并标注过去几年的告警日志和性能指标数据，就可以训练出能够识别故障特征的高维模型。监督学习算法（支持向量机、随机森林等）可以对已知故障样本进行分类，也可以对新的异常做出准确的判断；无监督学习算法（聚类分析等）可以发现未知的故障模式或者潜在的亚健康状态，从而实现故障的早期预警。

使用深度学习技术可以提高诊断智能化。神经网络可以对非结构化的日志文本以及时间序列数据进行处理，可以发现人类专家无法察觉的细微变化。用长短

期记忆网络来分析设备性能指标的时序波动,可以有效地预测光模块寿命的趋势,从而实现从事后抢修到事前预防的转变。机器学习模型还具有自我进化的特性,随着新数据的不断输入,其诊断准确率会越来越高。数据驱动的诊断范式正在深刻地改变电力通信网的运维模式,为自智网络提供强大的算法引擎。

三、故障恢复与自愈

(一) 故障恢复与保护倒换机制

保护倒换属于通信网络中最基本、最高效的恢复方式,一般借助硬件或者底层协议来实现,倒换时间被严格控制在 50 毫秒之内,以满足继电保护等实时业务的需求。光传输网络中常用线性复用段保护、环网保护、子网连接保护等几种方式。线性保护有 1+1 和 1:1 两种模式,1+1 保护采用双发选收模式,可靠性最高但是资源占用较大;1:1 保护在主用通道正常工作的时候,备用通道可以承载额外的业务,资源利用率较高。环网保护是用光纤组成环形网络,在环上某处断开时,业务会从反方向传输,形成新的通路。

除传统的同步数字体系保护之外,光传送网还引入了光通道、光复用段保护,可以在光层面上直接对波长进行倒换,不需要经过电层,时延更低。这些都是硬保护机制,由设备芯片直接触发,不需要上层网管系统参与,所以反应速度很快。配置保护策略的时候,一定要遵照业务等级划分准则,保证电网调度控制等一级业务安排最高级别双路由双设备保护,行政办公等非实时业务可以降低保护等级。完善的保护倒换测试在验收环节十分关键,必须定时开展倒换演练,以此来考查保护倒换逻辑是否有效及时延。

(二) 业务自动重路由

业务自动重路由技术主要用在智能光网络、分组交换网络等地方,它摒弃了传统的依靠预留备用路径的方式。当网络出现故障并且预设的保护路径也失效的时候,或者需要处理多点故障的时候,控制平面就会马上依照目前的网络拓扑以及资源占用状况,计算出一条新的最优路径。利用网状网高连接度的特点可以大大提高网络的可靠性,并且提高资源利用率。重路由恢复时间一般是秒级或者几分钟,但它具有较好的灵活性以及较大的恢复范围,比传统保护要强很多。

在实际运用当中,自动交换光网络或者通用多协议标签交换技术的控制平面,可以实时感知到整张网络的链路状况。当工作路径出现中断的时候,源节点就会

发出路径计算的请求，绕过故障的节点或者链路，重新建立起标签交换的路径或者光波长的通道。重路由算法一般可以带宽、时延、跳数、业务优先级等约束条件。

1. 高优先级业务将获得优先计算与资源抢占权，确保在网络资源拥塞时核心业务仍能畅通无阻。

2. 为了防止路由震荡，一般都会设置等待时间和回切策略：只有当故障存在的时间足够长时才对路径进行重路由操作；待原路径的故障被修复并且稳定之后再决定是否恢复使用原有的路径。

3. 利用智能化的恢复方式，使得电力通信网在遇到自然灾害造成大面积网络瘫痪的时候，仍可以依靠迂回线路维持核心架构的通信联系。

（三）网络自愈技术

网络的自愈技术就是网络生存性最高的体现。自愈网络有感知、诊断、决策、执行的闭环功能，可以自动对各种硬件及软件故障进行处理，不需要人工干预。真正的自愈不是单层面的恢复，而是光层、电层、分组层、业务层等多层次的协同。当光缆断开时，首先触发底层的光保护倒换；倒换不成功时再启动电层的子网连接保护；若资源不足，则由 IP 层的路由协议进行收敛和重路由。这样的纵向垂直协同机制，使得故障恢复的成功率和效率最大化。

未来的网络自愈将会走向意图驱动的自治网络。利用软件定义网络技术获得全网络全局视图，结合人工智能算法进行风险预测，可以在流量调优之前完成预判。一旦发生故障就可以自动重连，可以对全网流量进行智能再分配，不会出现重路由导致局部拥塞的情况。高度智能化的自愈能力，使电力通信网具有像生物体一样的强大的免疫力和再生能力，在极端恶劣的环境下也能顽强生存，给坚强智能电网的建设提供最可靠的信息通信保障。这项技术的不断进步将会使传统运维从以前被动地“救火”式工作转变为网络自动驾驶，网络自动驾驶的时代已经来临。

第四节 资源配置优化

一、网络资源管理

(一) 带宽资源、端口资源、IP 地址资源管理

带宽资源是电力通信网中最主要的传输要素，带宽资源的管理水平决定了业务通道是否畅通，服务质量的好坏。电力骨干传输网中光传送网技术应用较多，带宽管理主要是波长、时隙的分配。管理系统要随时跟踪光复用段的波长占用状况，保证核心节点的波长资源在主备路由之间平均分配，从而避免因为某一条链路带宽用尽引发的业务阻塞情况出现。对于使用时分复用的同步数字体系网络，带宽管理要细化到高阶和低阶虚容器的映射以及交叉配置，必须有效控制 VC-4 和 VC-12 虚容器的利用率，为继电保护等重要的生产业务预留足够的专用通道。分组传送网和数据通信网中带宽管理的动态性更强，管理员利用流量工程技术，给高优先级业务设置承诺接入速率和峰值信息速率，在保证高优先级业务独占带宽的情况下，让低优先级业务共享剩余带宽，可以大大提高整个链路的吞吐能力。

端口资源是指网络设备和终端业务之间物理连接的接口，端口资源管理就是对端口的物理特性、状态监测以及配线端口间连接关系的管理。电力通信机房内设备种类繁多，光口、电口、以太网口等物理接口数量以万计，精准的端口管理需要建立与现场完全一致的数字化端口台账。管理系统应当可以实时地显示出每一个板卡端口的占用、空闲、故障以及预占状态，从而防止因为台账更新不及时造成盲目跳线或者资源冲突。对于高密度接入区，端口管理还要结合综合配线架的跳纤关系做端到端链路关联，保证端口出现故障的时候，运维人员可以迅速定位到受影响的业务范围。由于设备集成度提高，虚拟端口管理也变得更重要，逻辑接口配置参数、物理端口绑定关系要严格控制版本，不能因为配置漂移而出现业务中断。

在电力物联网飞速发展的时代，IP 地址资源的管理就显得尤为重要。伴随着数以亿计的智能电表、配电自动化终端、微型传感器接入电网，对 IP 地址的需求量呈指数级增长，传统的 IPv4 地址空间已经严重不足。地址管理策略要兼顾公网地址和私网地址的映射关系，还要包含向 IPv6 过渡的演进方案。私网地址规划应该遵循分层化、可聚合的原则，按照电压等级、行政区域、业务类型来

划分独立的地址段，利用子网掩码、变长子网掩码技术提高地址利用率。从电力业务高安全性的要求出发，IP 地址管理要与网络准入控制体系结合起来，建立 IP 地址同 MAC 地址、交换机端口间的绑定关系，防止非法终端擅自接入或者篡改 IP 地址所造成的网络安全问题。自动化的地址管理工具可以对全网地址的存活情况进行实时的扫描，回收长时间不用的僵尸地址来保证地址池循环再生。

（二）资源生命周期管理

资源生命周期管理意在搭建起一个从“摇篮”到“坟墓”的电力通信资源全周期管控闭环，保证每一个资源无论处于哪个阶段都能被掌控。从规划设计阶段开始，设计人员根据电网发展规划和业务需求预测，制定出详细的资源建设方案，此时的资源还只是“设计态”，没有形成实体资产。工程建设阶段，设备到货验收、安装调试、入网测试，资源状态由设计态变为在建态，此时应该检查实物信息和设计图纸是否一致，保证序列号、软硬件版本等基本信息录入正确，为后续运维打牢基础。

1. 入网运行期间是资源生命周期中占据时间最长、也是管理最要紧的一段时期。这时资源处于在运态，管理重心向状态监察、变更维修、定时巡查转移。每一次业务开通、路由更改和板卡更换都会触发资源的更新，以此来保证系统中的数据同现实世界中物理对象之间保持一致。运维部门要建立严格的资源变更审批程序，用电子工单系统来记录每一次变更的操作人、操作时间和变更内容，从而实现资源变动全过程的可追溯。对长期运行的老旧设备还应进行健康状况评价，根据故障率、备品备件充足率、厂商技术支持状况来动态地制定维护策略，必要时可以降级使用或者限制新业务接入。

2. 报废阶段属于资源生命周期的终点。当通信设备达到规定使用年限，或者因为技术更新换代不能满足业务需要的时候，就要启动退役程序。资源状态变更为待报废，在经过资产评估和审批后，物理设备被拆除回收，系统中逻辑数据被归档或者逻辑删除，从而释放出机架位、端口、IP 地址等所占用的关联资源。该环节规范性管理可以防止占用了宝贵机房空间、系统数据库资源，从而达到资源循环使用，资产价值最大化的目的。

资源生命周期管理不是线性单向的流动过程，而是带有反馈机制的螺旋上升过程。运维阶段得到的故障数据和性能指标，要反馈给规划设计部门，作为以后设备选择和网络架构优化的参照。当某型号的光传输设备在运行过程中频繁出现

板卡故障的时候,资源管理系统应自动发出警告,提醒以后在工程的建设中谨慎选用该型号的设备。全生命周期的数据可以形成闭环反馈,从而使得电力通信网的建设质量以及运行水平不断得到提高,使资源管理不断得到优化。

(三) 资源利用率统计与分析

资源利用率统计分析,是发掘电力通信网潜力、提高投资效益的有效方法。运维人员通过大数据分析平台对全网海量资源数据进行多维、深层次的拆解。不仅要关注骨干链路带宽利用率,还要深入到汇聚层、接入层,关注边缘节点端口占用率、槽位占用率、设备 CPU 和内存的负载情况。全景式的统计视图可以清楚地看到网络资源的分配状况,找出资源富余、资源短缺的区域,在业务接入许可的时候做出更好的决策,将业务调度到资源充足的节点,避免局部拥塞的发生。

分析工作的核心是发现规律,预测趋势。对历史数据做长期追踪可以形成资源消耗的时间序列模型,进而发现电力业务流量潮汐效应和增长规律。通过对迎峰度夏期间的调度数据网流量峰值特征进行分析,可以为下一年保电工作提供带宽扩容的量化依据。另外,在资源利用率分析中需要注意“短板效应”,即主要排查利用率一直过高(超过 70%)的链路和利用率长期为零的资源。高风险链路系统自动产生扩容建议或者路由优化方案;对闲置资源做现场核查,决定是否僵尸业务占用或者规划预留不合理产生的闲置,并且及时释放或者重新规划。

为了使分析结果更加直观,方便使用,可视化展示技术被广泛使用。采用地理信息系统和逻辑拓扑图相结合的方式,把资源利用率以热力图的形式叠加在电网地图上,红色区域为资源紧张区,绿色区域为资源充足区,使决策者对全网资源情况一目了然。建立资源利用效率评价指标体系也是很重要的一个环节,以设定合理的阈值区间来量化考核各级运维单位的资源管理水平,促使运维单位主动开展资源整治、优化工作,提高电力通信网的投入产出比。

二、网络优化目标与方法

电力通信网的优化过程是复杂的多目标决策,其实质是在资源限制下,尽量提高网络综合性能。随着电网业务对通信系统的要求越来越高,通信系统优化的目标也从原来的简单的保证连通性,向高可靠、低时延、负载均衡、智能化的方向发展。为了达到上述目的,要综合应用理论分析、仿真建模、智能算法等许多种方法与手段。网络优化不但是对故障的被动反应,更是面向未来的主动架构调

整，目的是打造一个有强大的鲁棒性、自愈能力的弹性通信网络来应对自然灾害、外力破坏、突发性业务高峰等带来的挑战。

提高网络的可靠性，减少网络时延，均衡负载是电力通信网优化的三个主要目标。下表给出了三大主要的优化目标以及对应的优化策略和评价指标。

电力通信网核心优化目标及策略表

优化目标	目标描述	关键优化策略	衡量指标（示例）
提升可靠性	确保网络在故障情况下仍能持续提供服务，消除单点故障风险。	拓扑冗余（双路由、环网）、保护机制（线性复用段保护、子网连接保护、环网保护、自动交换光网络）、并发选收机制。	业务恢复时间、平均故障间隔时间、网络可用率。
降低时延	减少数据传输和处理的时间延迟，满足新型电力系统对精准控制的实时性要求。	简化网络层级、缩减业务跳跃次数、确定性网络技术（时间敏感网络）、光缆路由优化（裁弯取直）。	端到端时延、时延抖动、抖动率。
均衡负载	合理分配网络流量，避免局部拥塞和资源浪费，提高整体网络效率。	流量工程技术（多协议标签交换）、动态负载均衡策略、全网流量模型构建。	链路利用率、吞吐量、负载均衡度。

（一）提升网络可靠性、降低时延、均衡负载

提高网络的可靠性属于电力通信网优化的主要目标，同时这也是电网安全稳定的前提。优化策略主要是对拓扑结构加以完善，对保护机制加以加强。从物理拓扑上看，为了消除单点故障的风险，应该建设双路由、多路由、环网等结构，保证当某个节点或者链路出现问题的时候，业务依然有其他的可用路径。逻辑保护里常用到线性复用段保护、子网连接保护、环网保护等技术，也积极采用自动交换光网络技术来实现网状网的智能重路由，业务恢复时间一般不超过 50 毫秒。对核心调度业务采用并发选收方式，即把相同的数据分别通过两条完全独立的路径传送出去，接收端选取性能最好的那条路径，把链路故障给业务造成的影响降至最低。

降低时延属于对应新型电力系统精准控制需求的主要方式。随着配电自动化、准确负荷控制、差动保护等业务逐渐推广开来，毫秒级的时延抖动就会影响到电网动作的准确性。简化网络层、减少业务跳转次数、使用确定性网络技术。采用时间敏感网络标准，在交换设备上采用按时间片调度的方式，给高优先级的控制

指令开辟绿色通道,在网络拥塞时也能及时到达。同时优化光缆路由走向,裁弯取直,减小物理传输距离造成的光速延迟,也是降低端到端时延的物理方法。

均衡负载可以有效解决网络流量分布不均造成的局部拥塞、资源浪费问题。在实际运行过程中,经常会遇到主干链路长期满载,而备用链路空闲的情形。流量工程技术的引入,很好的解决了这一矛盾。建立全网流量模型,使用多协议标签交换技术显式规划业务路径,管理者可以将流量导向轻载链路上,实现全网流量的智能分流。动态负载均衡策略依据实时链路状况自适应地调节路由权值,在察觉某条路径发生拥塞的时候,便会把新增的流量挪到其它路径上,如此一来就能优化整个网络的吞吐量并加强抗冲击的能力,避免因局部过载而引发的连锁网络瘫痪状况出现。

(二) 基于仿真的网络优化

基于仿真的网络优化技术给复杂的电力通信网供应了一个低成本、低风险的试验场所。在真实的网络上大规模进行配置调整或者新技术验证,会带来业务中断的巨大风险,而仿真技术很好地解决了这个问题。利用 OPNET、NS-3 等专业的网络仿真软件可以创建出现实网络拓扑、设备参数、业务模型和现实网络相似的“数字孪生”网络。可以模拟各种网络协议运行情况,再现电力业务数据流向和交互过程,对网络性能瓶颈进行准确诊断。

1. 仿真技术在网络规划、扩容方案验证等各方面起着不可替代的作用。设计人员可以利用仿真平台,在开始建设之前先模拟各种建设方案,然后比较不同建设方案的带宽利用率、端到端时延和丢包率等主要指标。模拟 N-1 或者 N-2 个节点同时故障的情况(在网络中任意处发生 N 个设施中的 N-1 个或 N-2 个故障时的情况),观测网络的自我修复行为及业务受损情况来评价方案的可靠性。先仿真、后建设的模式可以避免规划设计中的盲目性、缺陷,保证投资的准确性、有效性。

2. 对突发流量、网络攻击的压力测试也是仿真优化的应用场景。电力通信网经常会出现由于大面积停电故障录波上传造成的流量冲击。仿真环境可以构造极端流量模型,检验网络拥塞控制机制的有效性,检验服务质量策略是否可以保证关键业务的优先转发。可以模拟分布式拒绝服务攻击等网络安全威胁,评价现有的安全防护体系防御能力的边界、薄弱环节,给网络安全加固提供量化的依据。经过多次的仿真迭代优化以及参数调整之后,可以得到网络配置的最优解,并且将安全的配置策略应用于物理网络当中。

（三）基于启发式算法的优化

随着电力通信网规模增大，网络路由寻径、波长分配、拓扑设计等问题已经变成了非常复杂的非线性组合优化问题。传统的数学规划方法由于计算量太大，很难在有限的时间内得到最优解。这时以生物进化、群体智能机理为灵感来源的启发式算法具有很强的求解能力。该类算法不需要依靠问题精确的数学解析式，模仿自然界中的进化、觅食过程，利用随机搜索和迭代进化，在可以接受的时间内找到全局近似最优解，很适合解决大规模通信网络的资源配置问题。

遗传算法是使用最广的启发式算法。在电力通信网路由优化中，将每一条可能的业务路径编码成一条染色体，用包含时延、带宽、跳数、可靠性等因子的适应度函数评价路径的好坏。算法模拟生物进化中选择、交叉、变异的过程，不断淘汰适应度低的路径，保留并优化优质路径。经过多代繁殖迭代，种群中最优的个体就代表了当前网络状态下最好的路由配置方案。这种方法对于多约束条件的路由选择很有效，可以很好地权衡时延最短、负载最轻、风险最小等互相矛盾的优化目标。

粒子群优化算法、蚁群算法在网络优化中有各自的应用。粒子群算法模仿的是鸟群的捕食行为，通过粒子自身的最优位置以及群体最优位置的交流，使得整个种群很快达到最优解区域，常用来设置连续变量的网络参数，如功率控制、缓冲区分大小等。蚁群算法模仿蚂蚁寻找食物时留下的信息素，利用正反馈机制使流量选择更好的路径，具有很强的分布式计算特性及鲁棒性，适用于动态变化的电力通信网路由寻优。当网络拓扑结构发生变化或者链路断开的时候，蚁群算法可以依靠残留的信息素来快速找到新的最优路径，具有很强的自适应性。将启发式算法嵌入到软件定义网络的控制器当中，就可以对电力通信网实施智能化的实时调度，使它具有类似生物体的自我感知和自我进化的能力。

第五节 服务质量保障

一、QoS 基本概念

(一) QoS 参数与指标

量化评价网络性能，需要有明确而具体的定义参数来构成服务质量的评价体系，影响业务在传输过程中实际体验的好坏。

带宽是最基本的一个，它指的就是网络链路在单位时间内能传输的最大数据量，直接影响视频监控、大文件传输等流量密集型业务的效率。电力系统当中，远程抄表，大数据分析这些业务对带宽有着极大的需求，这样才能保证海量的数据可以及时上传并进行处理。

延迟又叫做时延，是指从数据包从源端发出到目的端接收所消耗的总时间。一般由传输延迟、传播延迟、处理延迟和排队延迟组成。电力调度自动化系统当中，遥测、遥信信息的传输对于延迟非常敏感，哪怕只是延迟一点点，就会影响到调度中心对电网状态的正确判断。

抖动用来度量数据包到达目的端的时间间隔的变化情况，即延迟变化率。在语音通信、PMU 数据传输中，如果产生较大的抖动就会引起接收端缓冲区溢出或者欠载，使语音出现断续现象，数据解析出错，对业务造成干扰、破坏准确性和连续性。

丢包率就是数据包在传输过程中丢失的比例，一般由于网络拥塞、链路错误或者设备故障等原因造成。继电保护业务对于丢包率的要求几乎达到了极致，任何一条控制指令的丢失都可能造成故障切除失败，引发大面积停电，后果不堪设想。

可用性属于一项综合性指标，它代表了网络在一个给定时间段内处于可工作状态的概率，这也是电力通信网络作为电网“神经系统”必须遵守的最基本准则。

这些指标之间存在相互制约的关系，高带宽并不一定意味着低延迟，低丢包率也不能直接保证低抖动。因此，在设计电力通信网络 QoS 策略的时候要根据业务特性进行权衡。继电保护信号对延迟要求非常低，零丢包是必需的，即便要为此牺牲部分带宽利用率；而视频会议系统更看重要素充足的带宽以及稳定的抖动。网络管理者可以对上述参数进行细致的管理并予以持续监测，从而对网络的

健康状况有实时的了解,进而为不同优先级的业务赋予合适的资源,最终创建一个既高效又可靠的通信环境。

(二) DiffServ 与 IntServ 模型

集成服务模型和区分服务模型是两种完全不同的解决 QoS 问题的方法,在不同的网络环境和业务需求下各自有各自的优势,对电力通信网络流量设计产生了深远的影响。

1. 集成服务模型,它使用流式的资源预留。应用程序在发送数据之前,首先要向网络申请一定的服务质量。利用资源预留协议,网络中每一个路由器都要为每一个数据流保存状态信息,保证沿途每一条链路都留出足够的带宽和缓存空间。该模式可以给关键业务提供确定性的端到端质量保证,适合对实时性有极高要求的应用。但是由于大型骨干网络中数据流量的快速增长,路由器要维护的状态表项占用大量存储和处理资源,造成扩展性很差,所以在核心层的应用受到限制。

2. 区分服务模型和 IntServ 模型相反,DiffServ 模型放弃了对单一流进行复杂的状态管理,转而使用基于“类”的服务机制。在网络边缘,流量被分类并加上不同的标签(DSCP 值),核心路由器只根据数据包头部上的标签来执行相应的转发策略,比如快速转发、保证转发或尽力而为。该机制大大减轻了核心设备的负担,扩展性非常好,已经成为目前电力通信广域网以及骨干网的主流技术。它不能给所有的业务提供绝对的端到端保障,但是合理的带宽规划、策略配置完全可以满足大多数电力业务对性能的高要求。

需要说明的是,这二者并不是相互排斥的,在实际的电力通信网络架构中常常一起使用。在变电站局域网内部或者接入层,流量规模小、确定性要求高,局部可以采用集成服务思想或者利用时间敏感网络技术实现严格保障。而覆盖广大的电力传输骨干网上,由于区分服务模型的高效灵活,已经占据了主导地位。在接入边界上把 IntServ 请求映射成 DiffServ 代码点,从而达到端到端的服务质量协同的目的。既可以保证核心网良好的扩展性又能满足边缘层的某些业务严格要求。

(三) QoS 在电力通信中的重要性

电力通信网络属于智能电网运作的专用神经系统,其上承载着生产控制、企业管理、视频监控等诸多种类的业务。由于业务极其多样化、电网对于安全性的极致追求,QoS 机制在其中起着不可替代的作用。

电力系统的业务核心，比如继电保护、安全稳定控制等，是不能有丝毫妥协的即时性、不可中断性。当电网出现故障时，保护装置要以毫秒级的速度完成信息交换并切除故障，而这时网络正受到故障引起的突发性流量洪峰的冲击。若没有 QoS 保证，重要的保护信号会被大量的视频数据或者办公文件传输淹没，从而造成数据排队或者丢失。保护信号出现延迟或者消失，电网故障就无法被及时隔离，可能会造成设备损坏或者系统崩溃。QQoS 机制赋予生产控制业务最高优先级，在任何网络拥塞情况下，这些关系电网安全的重要数据都会被赋予绿色通道，优先转发，从而保证电网的安全防线不可攻破。

伴随着能源互联网的建设不断深入，大量的分布式电源、电动汽车充电桩、智能终端等新型设备接入电网，造成通信网络的流量模式越来越动态和不可预测。传统的尽力而为转发模式已经不能适应复杂多变的环境。用详细的 QoS 策略来调度网络资源。用电高峰期限制非生产性业务带宽占用，保证配电自动化、负荷控制指令及时下发，在日常运维时段给高清视频巡检赋予足够带宽，有效地改良运维效率。QQoS 不仅可以解决资源争用问题，还可以提高网络投资的价值，使有限的带宽产生最大的经济收益，有力支持电网向数字化、智能化转型。

二、QoS 实现技术

（一）流量分类与标记

流量分类和标记属于 QoS 实施的第一步，准确程度直接影响到后面策略执行的效果，同时也是区分不同业务身份的关键一步。

网络设备根据数据包报文头部的关键信息来判定业务类型。常用的分类标准有物理接口、源 IP 地址、目的 IP 地址、MAC 地址、TCP/UDP 端口号、IP 优先级等。电力通信网根据业务的重要性和实时性要求把流量分成不同的等级。继电保护、安稳控制业务属于最高优先级的关键控制类；调度自动化、同步相量测量业务属于高优先级的实时数据类；视频会议、视频监控属于多媒体类；办公自动化、文件传输等属于尽力而为类。

这些具体的电力业务 QoS 分类可见下表：

电力业务 QoS 分类表

业务类别	典型业务	优先级要求	关键特性	推荐保障等级
关键控制类	继电保护、安稳控制、调度指令	最高	极低延迟（毫秒级）、零丢包、高可靠性	严格保障（如 EF）
实时数据类	调度自动化、同步相量测量、SCADA	高	低延迟、低抖动、低丢包	优先保障（如 AF）
多媒体类	视频会议、视频监控、IP 电话	中	保证带宽、低抖动	一般保障（如 AF）
尽力而为类	办公自动化、文件传输、网页浏览	低	无严格要求	尽力而为（如 BE）

上表所列的复杂分类一般在网络的边缘设备，也就是接入层交换机或者路由器上完成，而不是在核心设备上执行，以此来防止核心设备处理能力被过度消耗。

分类完成后设备会对数据包进行标记，也就是将分类的结果写在数据包头部的指定位置，使网络中后续的设备可以快速识别并执行相应的服务策略。在二层以太网帧上一般用 802.1Q 标签中的优先级字段（即 802.1p），优先级范围为 0-7，共 8 个等级。三层 IP 报文中使用服务类型字段或者差分服务代码点字段来标记。DSCP 字段有 64 种编码组合，可以进行更细致的服务等级划分。

为了保证全网一致的服务质量策略，就需要在全网内制定出统一的映射规范。继电保护业务可标记为 EF(加速转发)类，对应最高 DSCP 值；视频业务标记为 AF(保证转发)类。数据包经过不同的网络域（比如从变电站层到骨干层）时，就需要重新标记数据包，使之适合每个网络段不同的 QoS 策略。用一次分类，处处识别的方法，网络可以形成一条条逻辑上独立的通道，保证各种业务各走各道，互不干扰。

（二）队列调度与拥塞避免

各类经过分类和标记的流量汇聚到网络出口处的时候，如果出口带宽小于总输入流量，拥塞就不可避免地会发生。这时队列调度算法就会起作用，决定这些数据包哪一个先发送，而拥塞避免则是在队列即将满载之前，如何主动丢弃一些报文。

严格优先级调度算法是电力通信网络中使用最广的调度方式之一，专门用于保证重要的控制业务。在此机制下，只要高优先级队列(存放继电保护信号的队列)里还有数据，设备就会绝对优先地发送高优先级队列里的数据，直到该队列为空

才会转而处理低优先级队列。该种方式可使重要业务的延迟和抖动降到最小。单独使用 SP 算法会导致低优先级的业务（办公数据）长期得不到服务，出现饿死现象。因此，在工程中常采用 SP+ 加权轮询或者加权公平队列。即，将继电保护等最重要的业务进行 SP 调度，将视频、办公等其他业务进行 WRR 或者 WFQ 调度，按照预设的权重分配剩余带宽，实现核心业务安全与其它业务公平的兼顾。

队列管理中传统的尾部丢弃策略，当队列满时把后续所有的报文都丢弃掉，会引起全局同步的现象：多个 TCP 连接同时检测到丢包然后减速，随后又同时加速，造成链路利用率的大幅波动。加权随机早期检测是一种主动的拥塞避免技术，很好地解决了以上问题。WRED 对队列的平均长度进行监视，当队列还没有完全填满的时候，就按照一定的概率随机丢弃报文。通常情况下，优先级低或者标记为丢弃优先级高的数据包被丢弃的几率大，而关键业务报文则设置成极小或者零丢弃概率。该机制能提前给发送端发送拥塞信号，通过隐含丢包通知来让源端平滑降低发送速率，避免网络陷入严重拥塞而保持流量的平稳流动。

（三）流量监管与整形

流量监管和整形都是对网络流量输入速率的控制，避免突发流量冲击网络核心资源，虽然目的相同，但是处理方式不同。

流量监管多使用于网络入口方向，给进入网络的流量加上速率限制。它一般使用令牌桶算法来判断流量是否超过了约定的规格。令牌桶会以固定的速率生成令牌，数据包在转发之前必须消耗掉相应数量的令牌。当桶内令牌充足时，数据包可以顺利通过；令牌不足时，就表示流量超速。对于超速报文，一般采用直接丢弃或者重新标记为低优先级后再转发的处理方式。流量监管可以控制非关键业务的带宽使用，防止其无限制地占用网络资源，可以控制恶意攻击或故障引起的广播风暴，避免网络的瘫痪。监管机制是即时生效的，能迅速阻断违规流量，有效保护网络边界。

流量整形主要是对网络出口进行处理，其主要目的是平滑突发流量，使其以相对均匀的速度发送出去。当流量速率大于设定的流量限制时，整形机制不会立即丢弃报文，而是把报文存到缓冲区排队，等待有足够的令牌的时候才发送出去。采用此种处理方式会引入额外延迟，但换来的是流量的平滑传输，能大大降低下游设备拥塞的情况。电力通信当中，数据流由高速骨干网流向低速接入网，或者接到处理能力比较弱的终端设备时，整形技术就显得格外重要。对数据进行整形，

防止给老的变电站终端一次性发送太多数据,使终端接收不过来而造成数据丢失。

1. 单速率三色标记算法属于流量监管中经常采用的算法。用两个令牌桶(承诺突发量和峰值突发量)把流量分为绿色(承诺速率以内)、黄色(超出承诺速率但在峰值以内)、红色(超出峰值)三类。该精细的评判机制使得网络在轻载的时候可以接受一部分突发的流量,在重载的时候优先丢弃红色、黄色报文从而达到灵活的带宽调节。

2. 配置流量整形的时候,缓冲区大小的设定很关键。缓冲区过小,整形效果不明显,仍会有很多丢包,缓冲区过大,延迟明显增加,实时业务性能受到影响。因此,一般要根据业务的延迟容忍度来仔细选择整形参数。在电力调度数据网中一般对骨干节点的非实时业务进行整形,而对实时业务只做监管或者直接转发,不引入不必要的时延。

采用监管与整形相结合的方法,能有效控制电力通信网络边界输入输出行为及形态,可以消除网络中出现的高流量尖峰。这就给电力通信网核心网络的 QoS 策略稳定执行营造出一种可以预知、可以控制的流量环境。

第八章 智能电网通信技术

第一节 智能电网通信需求

一、智能电网的典型特征

（一）信息化、自动化、互动化

信息化为智能电网高效运行打下基础，要对电网各个环节设备状态、环境状况、运行数据等信息进行实时、全面的采集，然后对采集到的信息进行数字化处理。海量数据的产生不再只是来自调度中心，而是来自于电网中的每一个末端感知节点，共同构成了电网运行的宏大全景图。数据不再是孤立的信息孤岛，统一了规范和模型架构之后可以实现部门间、区域间的数据共享、整合以及深度分析。

自动化程度的提高使电网的控制模式由人工辅助变为智能自控。先进的算法支持下，电网设备可以依靠实时的数据做出运行状态的判断，并且会自动去执行调节指令，完全不需要人工干预就可以实现故障隔离、负荷转供、电压无功优化等一整套复杂的操作。高度自动化机制提高了电网的反应速度，大大减少误操作可能，从而保证系统各种工况下都能稳定运行。

互动化使电网与用户间的关系彻底改变，电力流、信息流真正实现了双向互动。用户不再仅仅是电力消费者，而成为了深度参与电网调节的合作伙伴。通过智能终端及移动应用程序，用户可以随时掌握自身的用能状况与电价信息，进而灵活地安排用电计划。分布式电源、储能设备接入之后，用户就拥有了发用电一体化的双重身份，可以按照市场信号向电网反向送电，从而实现了源网荷储（发电侧、电网、负荷侧、储能）的友好互动与协同优化。

（二）坚强、自愈、兼容、经济

坚强性是智能电网面对极端挑战的物理保障，它要求电网架构有很强的结构强度和冗余度。面对特高压大容量输电造成的压力，自然灾害、外力破坏等突发事件造成的影响，电网的主体结构依然能保持完整，不会出现大面积停电事故。坚强性不能只在一次设备上体现出来，二次系统对故障的快速识别和准确切除才

能保证核心骨干网架不倒。

自愈能力是智能电网最具有智慧的特性之一，它给电网赋予了类似生物体免疫修复的本领。当系统某处出现故障的时候，智能控制系统会立即察觉到异常，依靠分布式智能逻辑迅速找到故障点。系统在毫秒级的时间内就可以快速地重新组织网络拓扑，隔离故障区域，通过其它通路给非故障区域供电，使故障影响范围最小化，甚至用户都察觉不到供电已经恢复。

兼容性就是智能电网包容万物的胸怀，打破了传统电网对于供电电源种类的限制。不管是集中式的火电、水电，还是分散式的风电、太阳能、微电网以及电动汽车等新型能源和设备，智能电网都能给予标准化的接口，愉快地接入，并且为整个系统提供服务。广泛的兼容性一方面利于清洁能源的大规模消纳，另一方面也利于各种新型用电设备的即插即用，进而推动能源消费方式多样化。

经济性存在于电网建设及运营的全部期间，其目的在于实现资源的最佳分配以及最大的社会效益。智能电网依靠细致的负荷经营以及全部生命阶段的资产运作，可以较好地减缓电网投入，改进设备利用情况，大幅削减输配电过程中的损失。随着电力市场的发展，价格信号成了引导资源流动的指挥棒，促使整个社会用最低的成本得到最好的电力服务，使得能源的价值得以最大程度地释放。

（三）清洁、高效

清洁能源大规模接入以及高效利用，是智能电网的核心任务，这就要求电网有很强的消纳能力和灵活的调节机制。通过准确的功率预测以及多种能源相互补充调度，可以较好地解决由于新能源发电自身存在的随机性、波动性所造成的弃风、弃光问题。推进能源结构的低碳转型，助力碳达峰、碳中和目标的同时，绿色电力也成为推动社会发展的清洁动力。

高效性体现在能源转换、传输、利用的各个环节都力求达到最佳的能效比。输电侧采用特高压技术以及柔性直流输电，大大减小了远距离输电的损耗；配用电侧的需求侧管理与能效分析，则使用户能够找到节能的机会，进而改善用能的方式。智能电网可以对全网潮流实施实时优化，大幅削减无效功率的流动，明显改善了整个系统能源利用的效能，因而用更少的能源耗费支撑起更多的经济产出。

二、智能电网对通信的新要求

（一）全覆盖、泛在化的连接需求

智能电网的触角伸向了电力系统每一个末梢，这就意味着通信网络必须完全消除覆盖盲区，做到对全域对象的无缝、泛在连接。

1. 首要的任务就是显著扩大覆盖面。传统通信一般只能到达变电站或者开闭所，智能电网要求信号能够深入到低压配电设备、表箱、甚至每一个智能插座。在偏远山区、地下管廊等信号难以到达的复杂环境里，通信网络要具备很强的穿透力和延伸能力，保证没有一个电力节点是信息孤岛，从而实现对电网运行状态的百分之百感知。

2. 连接对象泛在化，意味着连接范围的广泛普及。接入网络的既有传统的工业设备，又有数以亿计的传感器、智能电表、电动汽车充电桩、分布式能源控制器等各种终端。终端种类繁多、通信协议不一的时候，通信网络就要有很强的异构兼容性以及海量地址管理能力，实现即插即用的大规模并发接入，创建起万物互联的电力物联网生态。

3. 提高环境适应性也很重要。电力设备往往要在高电压，强电磁干扰，极端温湿度这些恶劣的环境下工作。所以通信设备要具备工业级的耐用性和优良的抗干扰性，在强电磁场中可以稳定传送信号，恶劣气候条件下仍可保持正常运转。全天候、全场景的适应能力，就是实现泛在连接、保证数据准确回传的物理基础。

（二）高可靠、低时延的控制需求

电网控制业务对于通信性能有着近乎苛刻的要求，任何通信故障或者时延都会造成无法挽回的损失，因此高可靠性、低时延是不可逾越的红线。

可靠性要求通信网络要达到电信级或者军用级的稳定程度，保证数据传输的误码率和丢包率处在极低的水平。对继电保护、安稳装置等重要业务，通信通道必须实行双路或多重冗余的设计方案，保证单个节点故障时可以无缝切换并且业务不受影响。通信网络的高可用性是电网安全运行的命脉，它必须保证在任何电网故障发生时，通信系统都能正确地将跳闸指令和状态信息传递出去。

时延特性直接决定电网故障处理的成败，对配电网自动化、精准负荷控制等业务来说，时延抖动哪怕是一毫秒都会造成控制失败。差动保护情况下，通信端到端时延一般要控制在几毫秒内，还要有严格的确定性，不能有太大波动。为了

实现这一目的, 通信网络架构要趋于扁平化, 缩减中间的转发节点, 而且要采用边缘计算技术把控制逻辑下沉到末端, 保证控制指令可以像光速一样快速抵达执行端, 从而达成电网动态的即时响应。

（三）大带宽、双向互动的业务需求

业务类型变得越发繁杂, 数据传输量也出现了指数级的增长, 大带宽以及双向交互特性成了智能电网新业务开展的重要条件。

输变电设备状态监测业务里, 很多高清视频、红外热成像等数据的使用, 给上行带宽造成了极大的压力。为了满足对变电站、输电线路实行全景式视频监控的需求, 通信网络须要兆比特甚至吉比特级别的接入速率, 才能实现多路高清视频的实时回传。基于图像识别的智能巡检技术要求原始图像数据实现高保真传输, 这样后台人工智能算法才能准确地识别出微小的缺陷, 完全改变了以前只传输窄带遥测数据的模式。

用电信息采集以及营销互动业务数据量大且具有双向性。智能电表高频采集造成大量负荷曲线数据, 须要大容量通道来汇聚上传。实时电价下发、费控指令、需求响应信号等都需要通过下行通道准确传送到用户侧。大量的双向数据交换, 通信网络必须要有对称的上下行传输能力, 不能因为带宽的配置不对等造成拥塞, 保证营销业务与客户服务的在线实时互动。

多媒体应急指挥、移动作业等业务的普及, 使人们对于带宽的需求越来越大。抢修现场作业人员要查阅大量的地理信息系统图纸、设备手册, 还要与指挥中心进行视频通话。无线通信网络要有广泛的覆盖范围, 在突发的大流量情况下也要保证稳定的吞吐量, 可以对现场态势进行实时直播, 并且支持远程专家的指导, 从而极大地提高了现场作业的效率 and 安全性。

三、智能电网通信业务模型

（一）发电、输电、变电、配电、用电、调度各环节业务

发电环节的通信业务主要是机组监控以及源网协调。传统电厂主要是机组运行参数实时上传和 AGC/AVC 指令的接收; 新能源场站除了功率预测数据上传外, 还有风机、光伏逆变器远程监测及快速频率响应控制等。该类业务一般都具有点多面广、实时性要求高的特点。

输变电环节的业务大致分为电网运行监视和设备状态检修两种。运行监视依

靠相量测量单元的同步相量数据高速传输来完成广域态势感知，状态检修包括变压器油色谱、避雷器泄漏电流、无人机巡检视频等非结构化数据的传输。这些业务对带宽的占用比较大，而且常常具有突发性，因此要求网络有较好的弹性吞吐能力。

配用电环节的业务最繁杂，它是万物的接口。配电自动化要和大量的开关站、环网柜的遥测、遥信、遥控（三遥）信息做实时交互，需要很低的时延来支持故障自愈功能；用电方面包括亿级数量的智能电表数据采集、电动汽车有序充电控制、智能家居能效管理等业务。该环节业务节点数量众多，数据包虽然小但是频率很高，给网络并发处理能力造成很大压力。

调度环节相当于电网的大脑，它把各个部分的重要运行数据汇集在一起。其业务包含实时调度指令下发，电网运行方式分析数据交互，继电保护故障信息处理等。调度业务属于安全防护的最高等级，对外部入侵、数据泄露有严格的要求，不能有丝毫的松懈，是通信安全防护中的重中之重。

（二）业务流量模型与 QoS 需求分析

业务流量模型存在明显的潮汐效应和突发性，必须做分层分级的细粒度建模。用电采集等周期性业务存在稳定的背景流量，故障录波、视频监控等事件触发型业务则会在某一刻产生大量的流量。因此在网络设计时不能只根据平均流量来确定带宽，应该留出足够的余量来应对极端情况下出现的流量高峰，避免重要的数据因为网络拥塞而丢失。

服务质量需求分析必须要按照业务的重要程度以及敏感度来进行区分定级。其具体需求如下表所示为智能电网通信业务 QoS 需求表。

智能电网通信业务 QoS 需求表

业务类别	典型应用	时延敏感度	抖动敏感度	带宽需求	优先级	丢包率要求
生产控制类	继电保护、 安稳控制	极高 （毫秒级）	极高	较低	最高	百万分之一 以下
管理信息类	办公自动化、 视频会议	较低	较低	较高	中等	较低
采集监控类	计量采集、 环境监测	一般	一般	较高	较低	一般

1. 生产控制类业务（继电保护、安稳控制等）对于这类通信的时延和抖动非常敏感，但是带宽需求不大。该类业务应该享有最高优先级，在网络设备中具有

绝对优先的排队、转发权利，即使在网络拥塞的时候也能畅通无阻，其丢包率要求一般在百万分之一以下。

2. 管理信息类业务（办公自动化、视频会议）属于第二类，带宽吞吐量大，但是对时延、抖动的容忍度高。此类业务可以采取尽力而为的传输方式，不过在网络空闲的时候应当能充分利用剩余的带宽来改善用户的感受。

3. 采集监控类业务（计量采集、环境监测）数据量大，但是对实时性要求不高。采用流量整形，错峰传输等方法平滑网络负载，比如将很多电表数据冻结后，统一安排在夜间网络空闲时分上传，以此来达到平衡全网流量，提升网络资源利用效率的效果。

（三）通信网络支撑体系

通信网络支撑体系是业务运行所依托的物理实体和逻辑结构的总称，要创建起“骨干加接入”、有线无线相融合的立体网络架构。骨干通信网络主要用光纤复合架空地线建立各级调度中心和高电压等级变电站之间的高速光传输环网。该网络层使用的是光传送网或者同步数字体系这样的硬管道技术，提供大容量、高可靠性的传输干线，像电网的主脉一样保证核心业务数据的无损传输。

接入通信网络存在点多面广的接入难题，要依照各地实际情况采用多种技术手段。在城市核心区以及新建小区可以采用光纤复合低压电缆来达到光纤到户的效果，提供极致的带宽体验；而在老旧城区和农村地区广泛使用工业以太网、电力线载波通信、无线公网或者专网技术来实现覆盖。尤其在 5G 技术日益成熟的情况下，它具有低时延、大连接的特点，所以成为了配用电接入层的好选择，从而形成了有线无线互补融合的接入结构。

支撑体系包含统一的网络管理系统以及安全防护系统。网管系统实现了对网络中所有的通信设备进行集中监控和智能运维，利用大数据分析技术实现提前预知设备故障、提高运维效率，构建出纵深防御体系，使用加密认证、流量清洗、入侵检测等手段保证了网络开放互联时信息的安全，给智能电网稳定运行打下坚实数字防线。

第二节 高级计量架构

一、AMI 系统组成

（一）智能电表

智能电表作为 AMI 系统中最基本的感知节点，功能也已经超越了传统的电能计量，发展成为具有边缘计算能力的一种智能终端。现代智能电表内置高精度计量芯片和高速微处理器，可以对电压、电流、频率、功率因数等几十种电力参数实行全方位实时监测。经过内部复杂的算法计算，可以实现分时段、分费率的计量，还有需量统计、电能质量分析、谐波监测等功能。为了满足双向互动需求，智能电表一般会带通断电控制继电器。电力公司根据用户的缴费情况或者电网紧急调控命令，可以远程实现对跳合闸的控制，使负荷管理更加灵活。

智能电表在硬件结构设计上采用模块化设计的思想，把计量模块和通信模块进行物理上的分离。该设计使得通信模块可以按不同的现场网络环境更换，无需拆下整个表体，大大降低设备全生命周期的成本。智能电表内部装有安全认证单元，用非对称加密算法对电量数据的采集、存储、传输全过程进行保护，来应对安全问题日趋严峻的现状。电表具有事件记录的功能，可以自动记录开盖、磁干扰、掉电等各种异常事件，是窃电稽查不可缺少的电子证据。

伴随着边缘计算技术的应用越来越深入，新一代的智能电表也正在向着非侵入式负荷辨识发展。采用高频采样的电表可以得到用户侧电器的特征电流波形，从而识别出用户正在使用的电器种类及能耗情况。不仅可以给用户提供详细的节能建议，也可以给电网企业提供准确的负荷预测以及高精度的需求侧管理数据。智能电表还留有多种本地接口，可以与水表、气表以及智能家居设备相连接，成为家庭智慧能源管理的网关。

（二）通信网络

AMI 通信网络形成了一条联结海量计量终端和控制中心的数据高速公路，一般分成广域网、邻域网、局域网这三层。广域网主要负责汇聚节点与主站系统之间的长距离数据回传，一般采用光纤专网或者运营商的移动通信网络。由于电力业务的安全性要求非常高，广域通信一般采用专用接入点或者虚拟专用网络方式隔离传输，保证业务数据不外传。光纤通信由于带宽高、时延小，成为骨干传

输的首选;在光纤不能到达的地方,4G、5G 公网就充分发挥其覆盖范围广的优势。

邻域网是 AMI 通信架构中最重要的也是最复杂的一块,主要是解决变压器台侧集中器与各个智能电表之间的“最后一公里”通信问题。这一层次存在节点数目众多、环境噪声繁杂、物理遮挡严重等诸多难题。为克服上述难题,邻域网经常使用电力线载波、微功率无线以及二者结合的混合组网方式。电力线载波利用已有的电力线资源,不需要重新布线,建设成本低;微功率无线通信利用空间射频信号传输,组网灵活,抗电力线噪声干扰能力强。实际部署时,一般会根据台区环境选择使用一种或者两种技术互补使用。

局域网处于用户侧内部,是智能电表和户内显示单元、智能插座及其它分布式能源装置之间短距离通信的网络。该层次的通信一般使用低功耗短距离无线技术,如蓝牙、ZigBee 等,目的是创建家庭能源局域网。用户可以利用局域网随时看到自己用电负荷曲线,收到电价通知,按照电网的峰谷时间自行调节大功率电器的开关时间。多层异构融合通信网络结构,保证 AMI 系统在各种复杂的地理环境以及电磁环境里都可以进行数据交互。

(三) 量测数据管理系统

量测数据管理系统担负着大量计量数据的清洗、存储、处理及分析工作,是 AMI 的“大脑”。该系统处于电力企业信息架构的中心位置,向上连接营销业务应用、配网调度系统和客户服务平台,向下管理大量的采集和通信基础设施。每天产生的亿级数据增量,用分布式存储加云计算架构来管理,保证数据处理的高并发、低时延。系统内建了强大的校验、估算、编辑引擎,可以自动识别采集时出现的畸变数据和缺失数据,并予以修正,保证入库数据的准确性及唯一性,为后面计费结算提供可靠的保证。

量测数据管理系统除了基本的数据管理外还有业务的深入分析。利用全网络计量数据的相关性分析能够精确地得到分台、分线路的线损率,并快速找到高损耗地区,有利于反窃电稽查。用大数据聚类算法,可以画出不同种类用户用电行为的画像,从而为实行差别电价策略给予决策支撑。发生停电时系统可以依据智能电表上报的掉电告警信息,结合网络拓扑结构快速判断出故障范围与类型并主动向抢修系统发单,由原来的被动报修转变为主动抢修。

随着数据资产价值越来越明显,量测数据管理系统正向开放平台发展。系统通过标准化的数据接口服务把脱敏的电力数据提供给政府部门、金融机构和第三

方能能源服务商。金融机构可以依据企业日用电曲线来判断企业的开工率以及经营状况，从而改善信贷风险控制。跨行业数据赋能既可以提升电力数据的社会价值，也可以催生出综合能源服务等新的商业模式。

二、AMI 通信技术

AMI 通信技术是实现智能电网全覆盖感知的基础，它的性能好坏直接影响计量数据采集的成功率和及时性。由于电力用户分布广，从城市高密度高层建筑到分散的农村山区，地理环境千差万别，一种通信技术很难满足所有地方的需求。因此 AMI 通信技术是多技术并存、互相补充。目前主流的技术有电力线有线通信技术和射频无线通信技术，将两者结合起来的混合组网技术正成为新的发展趋势。

AMI 通信技术种类繁多，其各自特点、优劣势及适用场景，可见下表：

AMI 通信技术对比表

技术类型	传输介质	传输特点	优点	缺点 / 挑战	适用场景
电力线载波	现有电力线	“有电通处即有通信”	无需布线，成本低；高带宽（宽带 PLC）	信道环境恶劣，时变性强；易受噪声干扰；跨变压器通信受限	城镇、密集区域；对布线成本敏感的场景
无线通信	空气介质	自愈性强，动态网络	不受电力线质量影响；组网灵活；低功耗；抗噪声	易受同频干扰、多径衰落；穿透力有限；易受物理遮挡	农村、分散区域；线路老化严重区域；物理遮挡少的场景
混合通信	电力线 + 空气	双模切换，智能选择	互补优势，高可靠性；适应性强；覆盖广	成本相对较高；技术复杂度稍高；协议融合挑战	复杂地理环境；新建及老旧小区改造；要求高可靠性的场景

（一）基于 PLC 的最后一公里通信

电力线载波通信技术使用遍布各地的电力线作为传输介质，可以实现“有电通处即有通信”，在 AMI 系统中应用最为广泛的是“最后一公里”接入方式之一。该技术将高频数据信号调制到工频电力线上，利用电力线路传输，接收端再解调还原出原始数据。早期的窄带载波技术由于传输速率低、抗干扰性差，不能满足高频次数据采集的需求。正交频分复用技术出现以后，高速窄带载波和宽带载波

技术应运而生。正交频分复用技术把高速数据流拆分成多个低速子数据流，然后在多个正交子载波上并行发送，这样就大大提高了频谱的利用率，而且具有很强的抗脉冲噪声能力。

宽带电力线载波技术的工作频率一般是 2 兆赫兹到 12 兆赫兹或更高，数据传输速率可达兆比特级。由于其带宽高，所以除了承载抄表等基本业务之外，还能支持远程固件升级、电能质量波形上传等大吞吐量业务。宽带载波采用自适应调制编码技术，可以随着信道质量的改变实时地改变调制阶数，从而保证在恶劣的信道环境里仍然能可靠通信。宽带载波网络具有自动路由、中继功能，节点间可以动态地建立多跳路径，很好地扩展了覆盖面，解决了长距离低压线路信号衰减的问题。

电力线载波技术虽然具有无需布线、维护方便的优点，但是信道环境恶劣，时变性大。电网中的各种开关电源、变频器产生的脉冲噪声，线路阻抗随着负载的改变而改变等特性，都会对载波通信的稳定造成影响。因此新一代载波技术使用了更高级的前向纠错编码和重传机制，并且还对算法进行改进以改善电网噪声模型。关于跨变压器通信技术的研究越来越深入，它的目的就是打破台区间的物理隔离，达到更大范围的网络互联互通的目的。

（二）基于 RF 的无线通信

基于微功率射频的无线通信技术依靠空气介质传送数据，不再受电力线路质量好坏的影响。此技术一般工作在免授权的 ISM 频段，采用网状网拓扑结构把节点连接起来，节点间可以自由连接，形成多路径动态网络。无线通信最大的优势就是独立性，不受电网谐波、脉冲噪声、线路通断等影响，适合线路老化较严重或者负荷特性复杂的台区。在农村地区，由于用户分布零散，电力线路长，分支多，使得载波信号衰减大，而无线通信可以利用空间的传播特性，一般具有较好的覆盖效果。

无线网状网技术具有很强的自愈能力。当网络中某个中继节点出现故障或者由于环境阻挡造成链路断开时，周围的节点会自动寻找新的路由路径，绕过故障点或者障碍物把数据传送到目的节点。该动态重组网机制大大提高系统的鲁棒性。为了应对无线信道里的同频干扰，多径衰落等状况，先进的无线抄表系统应用了扩频通信以及跳频技术。宽带内快速跳变工作频率可以避免受干扰的频点，保证数据可靠传输。低功耗也是无线通信的一大特点，很多电池供电的计量终端通过

无线技术可以达到几年不换电池的效果。

物联网标准统一以后, Wi-SUN 等国际标准就成了电力无线通信的主流标准。本标准对物理层和链路层技术体制做出规定, 保证各个厂商设备之间互操作性。基于 IPv6 协议栈的设计使得每一个无线智能电表都有唯一的 IP 地址, 可以无缝接入互联网。这便简化了网络的繁杂之处, 也为日后智慧城市的拓展留有余地, 利用电力无线网络传输路灯控制或者环境监测的数据。

(三) 混合通信组网方案

由于单一通信技术有局限, 所以双模混合组网方案, 即电力线载波和无线射频的结合, 已经成为解决复杂现场通信问题的有效途径。此方案在一个计量通信模块里把载波和无线两套物理层电路合二为一, 而且共用同一个介质访问控制层。双模模块在工作中可以实时检测出两个信道的信噪比、误码率等指标, 并且依据这些指标来选择最优的传输通路。该机制相当于给数据传输加了双保险, 使通信成功概率和稳定程度大大提高。

混合组网方案充分发挥载波和无线各自信道互相补充的特点。在地下室或者封闭表箱中, 无线信号很难穿透, 而电力线载波则能畅通无阻地沿线路传输; 反之, 当电力线路噪声较大或者断开的时候, 无线信号可以利用空间传输的优势, 保证数据链路的连续性。全天候、整个场景的适应性, 使双模技术在新建台区和老旧小区改造上都有了较大的应用价值。实测数据证明, 采用双模混合组网的台变, 一次抄表成功率比单一技术方案高很多, 大大减少运维人员现场补抄工作量。

从组网逻辑上来说, 混合通信技术做到了拓扑结构的混合。一个网络中可以有纯载波节点、纯无线节点, 双模节点则起到连接两种介质的作用。系统使用统一的路由协议, 可以利用不同的介质建立最好的路由树。某个节点可以利用载波把数据传给中继, 中继再通过无线方式把数据回传到集中器。这样灵活的异构组网方式, 很好地改善了网络资源的分配。随着芯片集成度不断增大、成本逐渐降低, 双模通信会成为智能电表的标配, 使 AMI 通信网络走向更为泛在、更为可靠、更为智能的未来。

第三节 配电自动化通信

一、配电自动化业务需求

(一) 馈线自动化通信

馈线自动化属于配电自动化的关键部分,可以及时而精准地找到线路中的故障点,并且将故障段隔离开来,使未出现故障的区域可以持续供电。该业务的实时性和可靠性要求较高,一般要求通信时延在毫秒级以内以保证保护动作正确。集中式馈线自动化模式中,各分段开关、联络开关的状态信息要实时上传到主站,控制命令也要快速下达,上行下行通道必须满足高吞吐量、低丢包率的要求。智能分布式馈线自动化模式中相邻的终端之间要互相进行对等通信,传递电流幅值、故障方向等关键信息,这就给通信模块横向互联的能力和逻辑处理的速度提出了更高的要求。

为了达到速动性要求,馈线自动化通信一般采用高优先级的传输方式。短路或者接地故障发生时,伴随的大电流、强电磁干扰会影响到通信链路,因此通信设备要具备强大的抗干扰能力以及电磁兼容性。对于差动保护等高级应用,除了需要数据传输速度快之外,还要求双向通道时延高度对称、抖动控制在微秒级以内,防止由于时钟不同步造成误动或拒动。在这种情况下,通信协议的帧结构要进行精简优化,去掉冗余开销,使故障报文可以以最短的路径、最快的速度穿透网络,直接到达决策节点。

配电网的拓扑结构变化很大,所以馈线自动化通信网络还要有自适应重构的能力。一次网架一旦出现转供或重组,通信路由就应该能够自动感知并重新规划,从而保证保护逻辑的连续性。这种动态适应性就要求通信设备内嵌智能路由协议,而且要和一次设备形成紧密的拓扑映射关系。对于重要的节点一般采用双通道冗余的方式进行配置,当主通道出现故障时,可以平滑的切换到备用通道,从而保证核心的保护业务数据通路不中断,在网络灾难来临时,将停电的范围控制到最小。

(二) 配电终端数据采集与监控

配电终端遍布开闭所、环网柜、柱上开关、配电变压器等处所,对电压、电流、有功功率、无功功率、开关位置等大量运行数据加以收集。数据采集和监控

业务具有节点数量多、单节点数据量小但是并发率高的特点。和馈线自动化不一样,这一类业务更多重视数据的完好性和历史可追溯性。通信系统要支持定时轮询和突发上报两种方式,在电网正常运行时周期性地上传遥测数据给状态估计,当出现异常情况时,立即触发告警上报,使调度人员可以及时掌握全网运行状况。

随着精益化管理需求的提升,配电终端的监测范围正从基本的电气量扩展至设备状态量。

1. 环境感知数据(柜内温湿度、水浸、烟感等非电学量数据)可以事先知道设备故障的可能性,把设备从计划检修变为状态检修。

2. 电能质量监测,包括谐波含量、电压暂降、三相不平衡度等指标的连续记录,这类数据一般采用统计压缩后传输的方式,需要通信链路具有突发大数据承载能力。

由于终端数量太多,通信架构承受着海量终端带来的地址和带宽压力,所以一般会使用分层分域的结构。汇聚节点属于中间层,主要对辖区内子终端数据进行汇聚,清洗打包之后再向主站上传,这样可以减少骨干网络的流量压力。数据传输时应按照电力监控系统安全防护的要求,对数据进行身份认证和加密。对公网通信要创建专门的虚拟专用网络隧道,并配合横向隔离装置来防止外来恶意入侵。终端设备需要具有远程固件升级、参数配置的功能,为了减少现场运维的人力成本,通信协议要具备断点续传、大文件传输的功能,保证维护作业的高效、安全。

(三) 分布式电源接入控制

在双碳目标的推动下,分布式光伏、分散式风电、储能装置大量接入配电网,使配电系统由原来的无源网络变成了有源网络。分布式电源接入控制业务要求通信系统对逆变器状态、发电功率、并网点电压进行实时监测,根据电网调度命令对有功和无功出力进行实时调整。由于可再生能源发电具有间歇性、波动性的特点,所以通信系统必须具有高频次的数据刷新能力,从而平抑功率波动,防止电压越限,保证局域电网的功率平衡和频率稳定。

当主网发生故障孤岛运行的时候,分布式电源的协调控制就显得尤为重要。通信系统要在毫秒级时间内把孤岛检测信号广播出去,并且把源荷匹配策略下发,这样才能保证微电网平稳切换、独立运行。该过程牵涉到源、网、荷、储等各个环节的协同作用,通信协议要具备良好的互操作性、可扩展性。对大量的户用光

伏系统来说，一般采用轻量化通信协议来满足基本的监控功能，降低通信模块的功耗、成本。

反向功率流的出现给继电保护逻辑带来了挑战，需要通信系统实时传输潮流方向信息，辅助保护装置判别故障性质。在电力市场化交易的背景下，分布式电源还需要参加辅助服务市场，通信接口除了要承载控制指令，还要传送计量计费 and 交易结算数据。此类数据的安全性以及防篡改能力要达到金融级水平，应用层应该使用高强度的数字签名、加密算法。通信网络的高可靠性在这里直接转化为经济价值，任何通信中断都会造成发电收益损失或者电网调节考核，因此，构建全覆盖、无盲区、高可靠的分布式电源接入通信网是实现源网荷储友好互动的技术基础。

二、配电通信组网方案

配电通信网建设要依照因地制宜、适度超前的原则，把区域地理环境，已有的光纤资源，业务的重要等级，投资效益等众多因素纳入考虑范围。单一的通信技术已经不能满足复杂的配电场景，目前主流的发展方向就是建设光纤和无线互补、专网和公网结合的混合组网方式。合适的组网方式，既可以保证核心业务的可靠运行，又可以兼顾边缘业务的覆盖范围和接入的方便程度，从而构建起一套层次分明、结构灵活、扩展性强的通信网络体系。不同组网方案的优劣及适用场合，见配电通信组网方案对比表。

配电通信组网方案对比表

方案类型	优点	缺点	适用场景
光纤通信	高带宽、低衰减、抗电磁干扰强、高可靠性、安全性高、扩展性强	建设成本高、施工周期长、管道资源要求高、入户困难	核心骨干网、高负荷密度区、重要用户供电线路、时延敏感业务
无线专网	广覆盖、大连接、低时延、部署灵活、建设速度快、维护量小、自主可控	频段资源有限、基站建设成本较高、易受环境遮挡	点多面广、分散布置的配电终端接入、区域覆盖、应急通信
载波与无线混合	无需布线、即插即用、低成本、高渗透率、自组织网络、自愈能力强	单一载波性能受限、信道特性复杂、跨相传输衰减大	配电网末端感知层、低压台区侧、海量末端节点接入

（一）光纤通信方案

光纤通信带宽大、衰减小、天然抗电磁干扰，是配网通信网络中可靠性最高

的传输介质，对时延和安全要求较高的核心区域和骨干节点来说更是如此。以太网无源光网络技术是目前配电光纤网的主流技术，点对多点的拓扑结构与配电网常见的树状或者辐射状分布模式相吻合。在变电站处设置光线路终端，在配电室或者环网柜处设置光网络单元，通过无源分光器完成链路分发，可以大大节省光纤和管道资源。

光纤通信的网络拓扑一般为手拉手环网或者双归属保护结构。当主链路出现断纤或者设备故障的时候，业务就可以立刻切换到备用链路上去，实现毫秒级的自愈恢复。差动保护这种对同步要求非常高的业务，光纤网可以提供纳秒级的时间同步。在建设过程中一般利用现有的 10kV 或者 35kV 电力线路杆塔资源同杆架设全介质自承式光缆或光纤复合架空相线，既降低了施工难度又保证了资产的权属可控。

虽然光纤方案性能优越，但是建设成本高、施工周期长，老旧城区或者地形复杂的偏远地区管道资源匮乏、入户困难。规划阶段要做好路由勘察，优先对核心商业区、高负荷密度区、重要用户供电线路实行全光纤覆盖。新建居住区、工业园区应执行电力光纤到户标准，通信管网和电力管网应与主体工程同时设计、同时施工。光纤网络除了承载配电自动化业务之外，还能为用电信息采集、多表合一以及电力物联网的新业务预留出足够的带宽裕度，是支撑坚强智能电网长远发展的战略性基础设施。

（二）无线专网方案

无线专网就是建立电力专用无线基站和核心网，使用授权频段进行数据传输，避免公网通信中存在的安全隐患和拥塞问题。基于长期演进技术的电力无线专网具备广覆盖、大连接、低时延的技术特点，适用于点多面广、分散布置的配电终端接入。无线专网相比光纤通信不需要铺设实体线缆，建设速度快、维护工作量小，可以适应配电网网架结构的调整和扩容。

无线专网工作在 230 兆赫兹或者 1.8 千兆赫兹等频段。230 兆赫兹的绕射性很好、覆盖范围大，在农村和郊区这样的广阔、低密度地区单站可以覆盖几十公里；1.8 千兆赫兹带宽容量大，适合于城市中心区域高密度数据并发的要求。采用正交频分复用、多输入多输出技术，无线专网在复杂城市建筑群或者变电站内部能提供稳定的连接质量。为了提高系统的抗毁性，无线专网核心网元一般采取异地容灾的方式进行部署，基站侧配置备用电源，保证在发生大面积停电或者自然灾

害的时候，通信网络仍能保持基本的运行状态，从而为指挥抢修力量提供保障。

安全性是无线专网的又一个主要竞争力。采用空口加密、双向鉴权、专用传输隧道的方式，构建出类似物理隔离的安全防护体系。与租用运营商公网不同，电力企业对于无线专网有完全的控制权，可以按照业务优先级随时对时隙进行分配和资源调度方案的调整，保证遥控指令等高优先级业务的畅通。网络规划时要依靠仿真软件做覆盖预估，合理安排基站站址，消除信号盲区。对地下室、屏蔽机房等信号较弱的区域，可以采用小微基站或者信号中继器的方式来补充深度覆盖，形成空地一体、立体覆盖的泛在通信网络。

（三）载波与无线混合方案

配电网末端感知层，特别是低压台侧节点数量成指数级增长，环境也越发复杂多变。单一的通信方式很难解决“最后一公里”接入难题，因此产生了载波与无线混合通信方案。该方案把高速电力线载波与微功率无线通信的双重优点融合起来，借助现有的低压电力线当作传输介质，再用无线射频信号来做空间补盲，进而达成无需布线、即插即用的灵活组网效果。

高速电力线载波技术使用正交频分复用调制，在强噪声、高衰减的电力线上也能达到兆比特级的数据传输速率。但是电力线信道特性随着负载变化很大，并且还存在跨相传输衰减大的问题。加入无线通信模块之后，当载波信道受阻时系统会自动切换至无线信道；而当无线信号受建筑物阻挡的时候，则采用电力线进行数据传输。双模异构通信机制使通信成功率和稳定性得到了极大的提高，在智能电表抄读、户变关系识别、低压拓扑自动生成等应用场景中效果明显。

混合组网一般使用自组织网络的网状拓扑结构。网络中的每一个节点既是终端节点又可以作为中继器，能自动发现临近节点构建多跳路径。某条路径一旦断开，网络算法就会自动找其他的路，自愈能力很强。双模通信模块可以嵌入到智能电表或者低压监测单元中，成本低，容易大规模推广。使用宽带载波技术可以识别台区内相位、对线损进行细部分析、对电动汽车进行有序充电。要达成互联互通，所涉及的通信协议得遵照统一的技术标准，从物理层到应用层全都得规范起来，消除不同厂家设备之间兼容性的问题。低成本、高渗透率的混合通信方式，很好地解决了配电物联网海量末端节点的连接瓶颈问题，打通了电网数据采集的微循环。

第四节 分布式能源通信

一、分布式能源并网通信需求

（一）分布式光伏、风电、储能监控

分布式光伏发电系统监控通信，主要是对逆变器状态、汇流箱数据、环境数据进行实时采集。逆变器是光伏系统的重要设备，它的输出功率、电压、电流、频率、故障代码等信息，对电网调度部门来说是决定光伏电站运行状况的重要参考。环境监测仪给出的太阳辐射强度、环境温度、组件温度等数据，对光伏功率预测系统来说也非常重要。大规模分布式光伏集群的通信网络要能承受高并发数据传输的压力，保证成千上万个节点运行数据可以同时上传到集控中心。屋顶光伏等分散式设施的通信模块一般集成在逆变器内，具有自动重新连接、断点续传功能，可以较好地抵抗复杂的电磁环境干扰。

风力发电系统监控通信比光伏复杂，机舱内有发电机组、齿轮箱、变桨系统、塔底主控制器等。风机转速、叶片角度、发电机定转子温度、振动数据等机械电气量要实时回传，方便运维人员远程做状态诊断和故障预警。风电场一般建在偏远或者地形复杂的地区，通信链路的不稳定问题比较突出。对于分散式风电接入，通信系统需要在恶劣的气象条件下依然保持较高的通信连通率，并可以对风机进行启动、停止、复位等指令操作。风功率预测对现场测风塔实时上传的风速、风向、气压等气象数据依赖很深，同样对上行通信带宽有具体指标要求。

储能系统属于调节电网波动的关键缓冲资源，它的通信需求大多表现在电池管理系统和能量管理系统之间高频通信上。BMS 要对电池簇内部单个电池的电压、电流、温度以及 SOC，SOH 等重要参数实施及时检测，刷新速度一般达到毫秒级或者微秒级。储能电站的热系统通信也不能小觑，空调、风机这些辅助设备的工作状态会影响到电池的安全与寿命。储能参与电网调频调峰服务时会收到调度中心发出的 AGC 指令，这就对通信网络提出了非常低的时延要求，一般要求端到端通信时延在秒级以内，保证功率响应及时准确。储能系统消防报警信号属于最高优先级的传输对象，任何时候都应该具有绝对的信道抢占权。

（二）并网点控制与调度

1. 公共连接点是分布式电源与大电网进行电气连接的物理接口，PCC 的电

气参数实时监测就是并网安全的第一道防线。通信系统需要实时把 PCC 处的电压偏差、频率偏差、谐波含量、三相不平衡度等电能质量数据传送到电网侧的电能质量治理装置,给电网侧的电能质量治理装置提供决策依据。调度主站根据实时数据,对并网接口装置发出有功功率削减或者无功功率补偿指令,保证局部电网电压、频率稳定。

2. 并网点通信的主要业务是有功功率、无功功率协调控制指令的传输。当电网负荷处于低谷或者出现拥塞的时候,调度中心通过通信网络向分布式电源发出弃光、弃风或者降功率运行的指令。对于具备 LVRT(低电压穿越)能力的机组,通信系统要上报穿越时的录波资料,事后可分析保护动作是否正确。控制指令一般采用 IEC 60870-5-104 或 Modbus TCP 等工业标准协议传输,通信链路必须非常可靠,加密认证也必须非常完善,否则就会有人擅自篡改或者误操作。

3. 孤岛检测以及防孤岛保护信号传输需要较高的通信速率。电网发生故障失压的时候,分布式电源要能立即发现孤岛情况,并断开连接,保证维修人员的安全。除了本地检测方法外,基于通信的传输跳闸方案被广泛应用,该方案要求变电站侧的跳闸信号能在几十毫秒内可靠传输至分布式电源侧的断路器控制器,任何通信延迟或丢包都可能导致严重的安全事故。

4. 继电保护信息的交换也属于并网点通信的内容。分布式电源渗透率提高之后,传统的配电网单向潮流变为双向潮流,保护配合就变得十分复杂。广域保护或差动保护方案需要相邻站点的 PMU 数据高速交换电流幅值、相位等相量测量信息,通信网络的同步授时精度和抖动指标要达到微秒级的苛刻要求。

(三) 微电网协调控制通信

微电网内部电源、负荷、储能等各要素之间,依靠高频通信来完成自主协调和优化运行。通信架构有集中式、分布式、分层式三种形式,各种形式对通信性能的要求也不一样。

孤岛工作模式时微电网的频率和电压稳定完全由内部控制策略来保证,主电源(一般是由储能或柴油机构成)和其他分布式电源之间的通信就显得尤为重要。为了保证功率平衡,通信网络要支持毫秒级功率分配指令传到现场,使各微源能很快地响应负荷的变化。如果采用对等控制方式,分布式电源控制器之间就要经常交换状态信息,以达到一致的控制目标。此种模式给通信网络的拓扑结构以及节点吞吐量带来考验,须要网络具备自组织、自愈合的特性,以防因单点故障致

使整个控制系统陷入瘫痪。

微电网由并网转为孤岛的平滑过渡（即预同步过程）很大程度上依靠通信系统实时性。切换瞬间，微网控制器要快速采集 PCC 点的电压幅值、频率、相位差，调节微网内电源的输出，直到两侧电气量满足同期条件。数据采样与指令的传送必须在极短的时间内完成，哪怕是一点点的迟缓都会造成切换的失败，并且会带来很大的冲击电流。

微电网与大电网之间需要互相通信才能发挥微电网的经济效益。微电网能量管理系统接受上级电网发来的电价信号、需求响应指令和辅助服务调度请求等输入信息，然后根据这些输入信息来优化内部运行策略。此类通信业务数据量小但安全等级高，一般用物理隔离装置或者纵向加密认证网关来完成跨区域传送，防止外部网络攻击穿透到微电网控制层面。

二、分布式能源通信方案

分布式能源点多面广、环境复杂、成本敏感，通信方案要按照覆盖范围、建设成本、运维难度、业务性能指标等各方面要求来选择合适的组网方式，一般采用有线无线结合、公网专网互补的混合组网架构。如下表所示为常见的分布式能源通信方案以及其特点和适用场合。

分布式能源常见通信方案对比

通信方案	关键特点 / 优势	主要挑战 / 劣势	典型应用场景
有线通信			
工业以太网	带宽高、时延低、抗电磁干扰强、技术成熟	部署成本高、施工难度大（尤其改造项目）	大型场站站内通信、保护装置互联
电力线载波	利用现有电力线、部署成本低、无需额外布线	信道环境差（噪声、衰减、阻抗变化），易受干扰	低压侧分布式光伏数据采集、计量
无线公网 / 专网			
4G/5G 公网	覆盖广、部署便捷、技术成熟	高并发时延抖动、安全性依赖运营商	分散式能源远程集控（非关键实时业务）
无线专网（如 LTE-230/1.8G）	安全性高、可控性强、广覆盖、深穿透	建设初期投入大、基站选址和频谱协调复杂	关键控制业务、偏远复杂地形风光电站
低功耗广域网	覆盖深、超低功耗、海量连接、成本低	时延较大（秒级）、不适用于高速移动与闭环控制	户用光伏监控、智能电表数据采集、环境传感器

续表

通信方案	关键特点 / 优势	主要挑战 / 劣势	典型应用场景
卫星通信	极端环境下通信可靠性高	带宽小、时延大、成本高昂	海上风电备用通信、偏远地区应急通信
物联网技术与架构			
边缘计算网关	本地数据处理、降低回传带宽与流量成本、缩短响应时间	网关算力与存储限制、部署维护复杂性	分布式能源站点侧数据清洗、聚合、初步分析
轻量级协议 (MQTT/CoAP)	发布 / 订阅模式、小报文头、支持 QoS、安全性高	协议选择与实现复杂性、不适用于高频控制	多业务系统数据推送、云端监控、异构设备接入

(一) 有线通信方案

工业以太网通信具有带宽高、时延低、技术成熟等优点，是大型分布式能源站站内通信的首选。场站内部常采用光纤或者双绞线组成环网或星型网，把各个发电设备的控制器、保护装置和监控后台连接起来。光纤通信具有很强的抗电磁干扰能力，远距离传输性能好，适合在高电压等级的升压站中使用。采用 IEC 61850 标准的通信结构，可以实现设备之间的互操作和信息共享，GOOSE、SV 报文高速传输，满足继电保护实时性要求。但是在既有建筑屋顶光伏等场合重新铺设光纤，施工难度大，成本高。

电力线载波通信技术采用现有的电力线作为传输介质，不需要额外布线，具有天生的物理连接优势，建设及维护成本较低。随着宽带载波技术的发展，其传输速率和稳定性都有了很大的提高，能够满足低压侧分布式光伏数据采集的基本需求。但电力线信道环境复杂，阻抗变化大、噪声强、衰减严重，逆变器开关频率附近存在的谐波干扰也会严重影响通信质量。一般要结合中继技术以及先进的调制解调算法（如 OFDM）才能有效提高通信的可靠性，使它适合于对实时性要求不高的计量和状态监测业务。

(二) 无线公网 / 专网方案

基于运营商蜂窝移动网络的公网通信方案，虽然不是最好的选择，但是由于其覆盖范围最广、部署最便捷，仍然被广泛应用。4G 网络技术已经很成熟，可以满足大部分分布式能源分钟级数据采集需求，但是在高并发情况下会因为基站拥塞而造成时延抖动。5G 网络由于大带宽、低时延、海量连接这三个特点，给分布式能源通信带来了革命性的变化。采用 5G 网络切片技术，在公网上虚拟出电力专用的逻辑网，实现端到端的资源隔离和服务质量保障，可以做到使用公网

广覆盖的同时,拥有接近专用网络的稳定、可预测的体验,非常适合分散式风电、光伏的远程集控。

无线专网方案一般采用 LTE-230、LTE-1.8G 等电力专用频段进行建设,全部由电力企业自行建设和运维,因此安全等级最高、可控性最好。LTE-230 系统采用电力行业已有的 230MHz 离散频谱资源,利用载波聚合、频谱感知等技术,实现广覆盖、深穿透,在地形复杂、偏远山区、地下室等信号盲区更加适用。无线专网刚建成时投入较高,基站选点和频谱协调工作繁杂,但是从长远角度来讲,其免流量费、自主可控的优点使其在重要控制业务中无法替代。LoRa、Wi-SUN 等非授权频段的无线专网技术也在微电网内部通信中有所应用,用以连接各个环境传感器以及智能电表。

海上风电等特殊场合的备用通信一般采用卫星通信。卫星通信带宽小、时延大,在极端天气导致地面网络中断的时候,可以保证最基本的状况监视和应急指令下达。由于低轨卫星互联网的发展,它的时延和带宽性能不断提高,将来有望成为分布式能源通信的一种补充方式。

（三）基于物联网的通信方案

1. LPWAN 技术, LPWAN 是低功耗广域网的英文缩写。NB-IoT、LoRa 等在分布式能源的分散式、非控制类数据采集上有着巨大的应用前景。NB-IoT 工作在授权频段上,深覆盖、低功耗、大连接的特性使其非常适合布置在地下室、管道井这些传统信号很难到达的地方,用来采集电表读数、设备温度这些少量的低频次小数据包。由于不支持高速移动、时延大(秒级),一般不用于闭环控制业务,但是对于海量分散、成本敏感的户用光伏监控来说,却是性价比极高的方案。

2. 边缘计算网关的出现使端到云的通信方式发生了变化,形成了一个新的“边缘云”协同结构。在分布式能源站点侧部署具备边缘计算能力的智能网关,可以在本地对数据进行清洗、聚合、存储和初步分析,只有处理后的关键信息或者告警才被上传到云端主站。不仅可以大大降低回传带宽的需求和流量成本,而且可以明显缩短本地控制策略的响应时间。边缘网关支持 Modbus、DL/T 645、IEC 104 等通信协议的转换和互通,很好地解决了底层设备接口标准不统一的问题,实现了异构设备的统一接入和管理。

3. 轻量级的通信协议 MQTT、CoAP 正在代替传统的复杂的工业协议,成为物联网领域主要的通信方式。MQTT 使用发布/订阅模式,使数据生产者和消费

者解耦，支持一对多的消息分发，非常适合分布式能源数据向多个业务系统（监控中心、运维 APP、大屏展示）推送。报文头很小，支持 QoS0、QoS1、QoS2 三种服务质量等级，在网络环境不稳定的情况下保证消息的可靠投递。协议一般在 TLS/SSL 加密层上运行，保证公网上传输数据的安全性、保密性和完整性。

第五节 电动汽车通信

一、电动汽车与电网互动通信需求

（一）充电桩状态监控与计费

充电基础设施的运行效率取决于对状态的及时、准确的监测。通信系统要不间断地对充电桩的电压、电流、功率因数、模块温度等物理参数进行采集，把模拟量转换成数字信号上传到云端平台。运营商利用远程监控界面可以实时了解设备运行状况，当出现过压、欠压或者绝缘故障的时候，系统必须在毫秒级的时间内做出反应，立即切断电源并给出故障代码。高频刷新的状态数据需要通信链路带宽充足、稳定，大量充电站并行充电的情况下并发数据流量呈指数增长。

计费系统的准确性是保证用户权益、保证运营商收入的基础。充电时的电能计量数据需要加密传输，防止人为篡改或者误传。通信协议要支持多费率计量模型，按照尖峰平谷等不同时段的电价策略，实时将计费参数下达到终端设备上。鉴权和计费流程包含用户身份识别、账户余额查询、预冻结金额和最终结算等各个交互环节。任何一个环节的通信超时或者丢包都会造成充值失败或者扣费错误，所以通信网络必须具有很高的可靠性和很低的延迟，保证支付指令和计量数据同步一致。

（二）充电负荷调度与控制

大规模电动汽车无序充电对配电网来说是巨大的冲击，变压器过载或者电压骤降。为了解决上面的问题，通信系统就要做到细粒度的负载调节以及有序充电。电网调度中心根据当前负荷预测以及配变容量，算出各个充电站点的最大可用功率限额，再经由广域通信网络把功率调节指令下达给站级控制器或者单桩。此过程需要通信链路支持双向调节，既可以下传控制指令，又可以上传执行结果和实时功率响应曲线，从而形成闭环控制回路。

基于价格信号的需求侧响应也是一种有效的负荷控制方法。通信网络把动态电价或者激励信号送进车主的移动端或者车载终端，以此来指引车主在电网低谷时候充电。电网频率越限或局部线路故障等紧急情况下，通信系统必须提供最高优先级的紧急断开或功率削减指令，并在几秒钟内完成负荷的减少。控制逻辑需要通信协议具有严格的优先级管理机制，保证在网络拥塞的时候关键的控制信号仍然可以优先传输。有序充电的实现要依靠车、桩、网三者之间的高效合作，任何一个环节的通信中断都会导致调度策略失效。

（三）V2G/V2H/V2B 双向互动

车网双向互动技术把电动汽车从电能的消费者转变为电网的产消者。电动汽车在 V2G 模式下是移动的储能单元，在电网高峰时段可以将电能回馈给电网，参与削峰填谷或者提供频率调节等辅助服务。此模式要求通信系统实时性和安全性很高，反向放电需要逆变器同电网保护配合完成。车辆电池管理系统要与充放电设备进行高频次的交互，及时得到电池剩余电量、最大放电功率、健康状态等信息，保证放电过程不会影响到电池寿命。

V2H、V2B 属于局域能源管理的重要部分。电动汽车同家庭或者楼宇能源管理系统之间互相通讯，配合光伏发电以及固定储能，从而达成微网内部能源的自平衡。通信协议要支持即插即用功能，车辆连接上之后就可以立即和本地能源网络建立联系，自动选择充放电策略。当检测到家庭负荷突增或者外部电网停电的时候，通信系统就要马上指示车辆转入放电模式，充当应急电源给重要的负载供电。这就要求通信架构具有很强的边缘计算能力以及本地自治能力，在广域网断开的情况下也能保证局域网内的交互可以继续。

二、电动汽车通信技术

（一）充电桩与平台间通信协议

开放充电点协议成了充电桩同中央管理系统之间全球事实上的标准。该协议使用的是客户端 - 服务器架构，早期版本用的是 SOAP/XML 技术，目前广泛使用的是 OCPP 1.6J，而演进中的 OCPP 2.0.1 主要使用的是 JSON over WebSocket。WebSocket 技术支持全双工通信，云端平台可以主动向充电桩发送控制指令，不需要桩端进行轮询，从而减少通信时延、流量消耗。OCPP 定义了很多功能模块，例如：

引导通知：设备上电后向平台发送配置参数，并协商通信心跳间隔。

事务处理：记录充电会话的开始时间、计量数据和认证信息，作为计费依据。

心跳机制：定期发送存活报文，以维持 WebSocket 长连接的稳定性。

OCPP 2.0.1 版本对安全性、功能性做重大改进。设备管理功能加入以后，就可以对充电桩的内部参数和显示屏的信息进行深入的设置。更重要的是增加了 ISO 15118 标准支持，给即插即充提供协议支撑。在实际部署的时候，使用传输层安全协议对 WebSocket 的安全连接进行加密已经成为普遍的做法，目的在于防止中间人攻击所造成的窃听数据或者篡改指令。

（二）车载终端与后台通信

车载远程终端给电动汽车接入车联网提供了网关的功能，主要负责采集车辆的运行数据并与车企的 TSP 平台通信。车载远程终端用 CAN 总线直接从整车控制器、电池管理系统获取车辆位置、车速、电机转速、电池单体电压、温度等关键数据。通过内置的 4G/5G 通信模组，按照 GB/T32960 等国家现行标准协议对数据进行封装后，上传到国家监管平台以及企业监控平台。5G 由于具有高带宽、低时延的特点，在逐步取代 4G 之后，可以很好地处理海量车辆数据的实时并发。

除了数据采集之外，车载远程终端还有远程控制、无线升级的功能。用户通过手机 APP 发送开启空调、解锁车门或者预约充电的指令，云端将指令发送给车载远程终端，车载远程终端将指令解析成 CAN 报文，控制相应的执行器。在无线升级的场景中，车载远程终端需要下载数兆至数吉字节的固件包，并且要和车内的各个电控单元协调完成刷写升级。通信链路要稳定，也要支持断点续传和完整性校验。为了保证通信安全，车载远程终端里面一般都会集成一块安全芯片，用来存放设备密钥和数字证书，从而与后台进行双向的身份认证，并且对通信链路进行加密。

（三）充电设施局域组网技术

在住宅小区、办公楼宇或者大型公共场所，充电设施往往会成群结队地出现，局域组网技术对降低通信成本、提高控制响应速度起着至关重要的作用。电力线载波通信是利用已有电力线进行数据传输的一种技术，不需要另外架设通信线路。直流快充标准 CCS、ChaoJi 中使用电力线载波通信作为电动汽车与充电桩之间底层通信手段，传输电池参数、充电需求等信息。而在场站级组网当中，宽带载波技术可以实现桩对桩、桩对集中器的高速互联，尤其适合地下停车场等无线信

号覆盖差的地方。

ZigBee、Wi-Fi Mesh、LoRa 等无线局域网技术也被用在某些场合。ZigBee 由于低功耗、自组网等特性，可以用于家庭交流桩的智能控制和能耗监测，Mesh 拓扑结构可以扩大信号的覆盖范围。大型充电站可以使用工业级 Wi-Fi 或者私有无线协议将各个充电终端和站级边缘网关连接起来，使各个充电终端的本地控制器统一接收指令下发，并上传数据。局域组网作为广域网回传的有效补充，在本地控制器汇聚数据之后，用单根高可靠光纤或者 5G 链路接入云端。云边端这样的结构不仅可以大大减小核心网的流量压力，还能极大地提高系统的抗干扰能力。

电动汽车通信技术概述表

技术类型	主要协议 / 标准	特点	应用场景
桩与平台通信	OCPP 1.6J/2.0.1, JSON over WebSocket, TLS	全双工、实时控制、高安全性、互操作性强	充电桩状态监控、远程控制、计费、固件更新
车载终端与后台通信	GB/T32960, CAN 总线, 4G/5G, 安全芯片	数据采集、远程控制、无线升级、高带宽、低时延、高安全性	车辆运行数据上报、远程诊断、用户指令交互
充电设施局域组网	电力线载波通信 (直流快充标准 CCS/ChaoJi), ZigBee, Wi-Fi Mesh, LoRa	无需额外布线、低功耗、自组网、适用于信号弱区	桩与桩互联、桩与集中器互联、家庭交流桩控制、地下停车场组网

上表概述了电动汽车与电网互动中不同层级的通信技术及其应用。

第九章 电力通信新技术应用

第一节 5G 通信技术

一、5G 关键特性与电力应用场景

（一）eMBB：大带宽，支持视频巡检等

增强型移动宽带场景主要提供极高的数据传输速率和极大的系统容量，以满足极高的带宽需求业务。电力系统中的输电线路、变电站巡检工作传统上多采用人工方式，效率低、安全隐患大。随着无人机技术以及高清视频监控的发展，电网对于上行带宽的需求呈爆炸性增长。传统的 4G 网络下行速率还可以，但是上行链路受到频段和时隙分配的限制，不能支撑多路 4K 甚至 8K 高清视频的实时回传。eMBB 特性使用大规模天线阵列、更大的频谱带宽，峰值速率可以到达吉比特级。变电站巡检机器人可以实时传送红外测温高清图像与设备状态视频，后台的人工智能系统就能立即察觉并做出判断。

输电线路的无人机巡检属于 eMBB 技术的主要应用场景。无人机搭载高清摄像机、激光雷达等设备，在崇山峻岭等地形复杂的地区会产生大量数据。依靠 5G 网络的低时延特性，这些数据可以实时上传到指挥中心，运维人员好像身临其境一样，可以实时监视线路运行情况。利用增强现实眼镜辅助现场作业也成为可能，后台专家通过高清视频流实时指导现场人员进行复杂的设备检修工作，图纸、技术参数等信息可毫秒级叠加在维修人员的视野中，从而大幅度提高作业效率和安全性。大带宽能力将彻底改变电力运维以前“先采集数据、再分析”的离线方式，使电网运检走向实时化、智能化。

以 eMBB 为依托的沉浸式全景监控系统在配电房等室内场所正逐渐普及。利用多路高清摄像头和环境传感器，运维人员不用去现场就可以通过虚拟现实设备对配电房内部环境做 360 度无死角巡视。不仅可以减少人力成本，也可以提高对突发异常的反应速度。火灾、水浸告警发生的时候，高清视频流可以第一时间提供现场的情况，为应急指挥提供决策依据。5G 大带宽特性解决了目前视频业

务卡顿问题，也给未来全息投影交互、数字孪生电网的建设留了信息通道，是电网可视化管理的基础。

（二）uRLLC：低时延高可靠，支持精准负荷控制

超高可靠低时延是 5G 最突出的一个特点，它主要面向时延、可靠性要求很高的工业控制类业务，与以前的移动通信技术有明显的不同。新型电力系统当中，分布式新能源大量接入之后，电网稳定的局面就陷入了非常严峻的危机之中，对配电网准确执行负荷控制的需求变得近乎苛刻。传统的配电自动化大多依靠光纤通信，但是电网末梢处，光纤铺设费用高且施工困难，很多配电设备只能无奈地“盲调”。uRLLC 技术通过缩短空口传输时延、增加边缘计算节点，可以实现端到端毫秒级的通信时延，正好满足了配电网差动保护等关键业务的要求，使得无线通信首次具备了承载电网控制类业务的能力。

精准负荷控制系统可以在电网出现故障或者频率波动的时候，及时切除一些非关键负荷来保证主网的安全。这个过程一般要通信时延小于 100 毫秒，可靠性大于 99.999%。5G 网络利用帧结构优化、免调度传输等技术，将空口时延降低了很多。uRLLC 精准负荷控制终端可以迅速遵照调度指令，对空调，充电桩这些柔性负荷实施毫秒级的调节，弥补了传统无线公网在控制上的缺陷。这对于形成源网荷储协同互动的弹性电网十分重要，虚拟电厂场景中成千上万个分散的可调节资源需要实时聚合响应，uRLLC 提供不可或缺的通信保障。

（三）mMTC：海量连接，支持智能传感

海量机器类通信场景主要是解决海量物联网设备并发接入的问题，单平方公里可达百万连接。电力系统中为了全面感知设备状态，需要布设大量的传感器，温湿度传感器、局部放电监测装置、避雷器在线监测仪、数以亿计的智能电表。这些设备数量很多，且大多分布在环境恶劣、供电困难的地区，所以通信模块要具有极低的功耗以及很强的覆盖能力。采用改进的 mMTC 信号交互过程以及非正交多址接入方式，能够很大程度上提升系统容量，使得密集型电力物联网终端可以正常接入网络并上传数据到服务器。

智能电表信息采集是 mMTC 最基础也是最广泛的场景。随着双向互动服务需求量的不断增大，智能电表已经不再只是用来收费的工具，它还是电网了解用户负荷特性的一种触角。mMTC 技术把电表的数据采集频率提高到每天一次以上，支持电压、电流、功率因数等全部电气量的实时回传。这给电网企业做大数据分

析、画用户画像、监测窃电行为给予了丰富的数据源。凭借海量连接能力，电力公司可以对低压台区实施精细化管理，及时察觉三相不平衡，重过载等状况，主动改进供电服务品质。

除了计量之外，输变电设备的状态监测也成了 mMTC 大展身手的场所。特高压输电铁塔上装有倾斜、风偏、微气象等传感器，这些传感器大多用太阳能或电池供电，通信功耗非常敏感。mMTC 技术可以使终端进入深睡模式，只在需要传输数据的时候才会被唤醒，从而有效延长设备的使用寿命，节约运维成本。

1. 环境感知层的全覆盖又是 mMTC 技术的一大优点。对于地下电缆隧道、高压开关柜内部等传统信号难以到达的隐蔽工程，依靠 mMTC 技术覆盖增强特性，可以保证监测数据的正常传输，使电网公司能够随时了解隐蔽工程运行环境的温度情况，避免出现电缆火灾、开关柜过热等事故。

2. 分布式能源接入需要很多连接。屋顶光伏、分散式风电爆发式增长，电网侧需要监测的节点数量呈指数级增长。mMTC 技术可以把分散的、小容量的发电单元统一接入调度平台，实现分布式电源的可观、可测，为后续可调、可控打下基础，促进清洁能源的高效消纳。

5G 三大关键特性与电力应用对照表

5G 关键特性	主要能力	主要应用场景	电力行业应用示例
eMBB (增强型移动宽带)	极高数据速率、大容量	高清视频、虚拟 / 增强现实	无人机巡检、机器人巡检、AR 辅助检修、沉浸式全景监控
uRLLC (超高可靠低时延通信)	极低时延、超高可靠性	工业控制、自动驾驶	精准负荷控制、配电网差动保护、虚拟电厂聚合响应
mMTC (海量机器类通信)	海量连接、低功耗、广覆盖	物联网设备连接、智能传感	智能电表信息采集、输变电设备状态监测、分布式能源管理

从上表可以看出，5G 三大特性与电力行业的需求高度契合，共同推动电力系统的智能化升级。

二、5G 电力专网建设模式

(一) 5G 公网切片模式

5G 公网切片模式，就是利用网络切片技术，在运营商已大规模建设并覆盖的 5G 公共网络上，从逻辑上划分出一到多个虚拟的专用网络给电力行业。该模

式最大的优点就是建设速度快，覆盖面积大、初期投资小。运营商在无线侧、传输侧、核心网侧进行端到端的资源预留和隔离，保证电力业务在网络拥塞的时候依然能够获得带宽和时延的保障。对管理信息大区的移动办公、视频会议和一些安全等级不高、以采集为主的业务采用公网切片模式可以取得较好的效果，既快捷又经济。它使电力企业可以利用运营商遍布城乡的基站资源，快速实现业务的广域覆盖，不需要自建基站、传输线路，大大缩短了业务上线时间。

但是公网切片模式的安全性主要依靠逻辑隔离，物理上仍然和公众用户共享基础设施。尽管切片技术有严格的隔离性，但是当面对极端的网络攻击或者核心网故障的时候，电力切片还是会存在被波及的风险。为了提高安全性，一般采用切片 ID 隔离、IPSec 加密隧道等叠加安全方式。在实际部署时，电力企业需要同运营商进行深度的合作，对切片的管理平台的基础之上，实时检测切片的性能并做动态调整。该模式下数据的路由路径一般需要经过运营商的核心网节点，因此在数据不出厂、低时延路由优化上需要特殊配置，例如利用边缘计算节点 UPF 下沉，把电力用户面数据直接分流到电力内网，避免数据绕道公网核心。

公网切片模式适合于多点、面广、业务突发、单点数据价值小的场景，例如电动汽车充电桩计量计费数据传输、分布式光伏运行监测等。这些业务散布得很开，自建专网的性价比很低，但运营商的 5G 网络却可以覆盖到这些地方。配置高优先级的切片，在保证业务基本通信质量的同时可以大幅度降低通信成本。同时伴随着切片商城商业模式的成熟，电力企业可以像购买云计算一样，按需购买切片资源，实现通信资源的弹性伸缩，满足能源互联网业务快速迭代的特点。

（二）5G 行业专网模式

5G 行业专网模式指的是电力企业使用专用频率资源，自己建设或者与运营商合作建设物理隔离的 5G 网络基础设施。该模式可以提供最高的安全保障以及网络控制权，完全满足电网生产控制大区业务物理隔离的刚性需求。

1. 频率资源的独占性属于行业专网的一个特点。电力企业在此模式下一般会申请 230MHz 或者 1.8GHz 等工业专用频段，建设完全属于自己的基站和核心网。这就意味着电网业务不再与公众用户争夺空口资源，公网拥塞也不会影响电力业务，网络确定性达到极致。

2. 用物理隔离来保证网络边界的绝对安全。行业专网的硬件设备、传输链路以及网管系统都是独立的，不能从公网入侵。对于差动保护、安稳装置切机切负

荷等关系到电网“生命线”的核心业务，物理层安全隔离是必需的，完全符合电力监控系统安全防护的“安全分区、网络专用、横向隔离、纵向认证”的原则。

3. 自主可控的运维管理体系。自建专网可以使得电力通信部门对网络进行完全的配置和调度，根据电网检修计划随时改变通信参数，故障排查响应速度更快。但是这种模式会带来巨大的建设和运维成本，基站选址、设备采购、日常维护都需要投入大量的人力物力，专用频段的产业链较弱，终端芯片、模组成本较高。

（三）公网混合模式

公网混合模式集公网切片模式的经济性、行业专网模式的安全性于一体，是目前电力 5G 应用探索中最具潜力的主流方向。此种模式一般采用核心网专用、无线网共享或者控制面共享、用户面独享的方式。就无线接入侧来说，电力业务共享运营商宏基站资源，利用公网广覆盖的特点解决信号接入问题；核心网侧通过轻量级核心网元下沉至电力公司机房或者专用 UPF 设备部署在变电站侧，完成电力业务数据的本地卸载并独立处理。不但可以避免基站重复建设造成的高额费用，还可以保证电力数据不出园区，满足数据隐私要求，实现低时延。

在网络资源按业务等级分配的时候采用混合模式。对于一般的管理信息类业务可以使用公网资源；对于生产控制类业务则可以利用无线侧资源块预留技术、核心网独立网元来保证。这样的一个灵活的体系结构，使电网企业可以在成本与安全之间找到最佳的平衡。以变电站区域为例，采用公网基站覆盖，但部署站内移动边缘计算 MEC，对视频监控数据在现场进行分析处理，只有告警信息回传到主站，节省了回传带宽，提高了响应速度。对部分重要变电站或者调度中心，可以局部采用自建微基站的方式来补盲或者增强覆盖，形成宏基站和微基站相互结合的立体网络。

混合模式要做复杂的网络切片协同运营。电力企业要和运营商建立联合运维机制，利用运营商网络切片能力开放的 API 接口，把运营商网络切片能力集成到电力统一通信管理平台中。电力调度员在发布电力调控指令的时候，也能体会到通信通道的健康情况。主用切片性能下降的时候，可以自动切换到备用切片或者备用路由。5G 局域网、时间敏感网络等新特性被引入之后，混合模式下的 5G 网络将会有更好的二层组网能力和确定性传输能力，性能指标越来越接近光纤通信，为未来的无线化智能变电站、配电网打下基础。顺应通信技术 IT 化、云化的趋势是电力通信网走向开放、智能、融合的必然之路。

第二节 物联网技术

一、物联网体系架构

（一）感知层、网络层、平台层、应用层

感知层是电力物联网的“五官”和“皮肤”，主要对电力系统全环节对象进行全方位的感知与识别。这一层有种类繁多的传感器、RFID 标签、摄像头、智能终端、各种边缘采集设备等。输电侧微气象传感器、导线测温装置、杆塔倾斜监测仪实时采集线路运行状态；变电侧局部放电监测、油色谱分析仪、红外热成像仪构成设备健康监测网络；配用电侧智能电表、故障指示器、海量智能家居融合终端不断采集电压、电流、功率、环境参数。感知层的功能不再只是被动采集，越来越多带有边缘计算能力的智能感知终端被部署，它们可以在数据源头进行清洗、压缩，甚至初步分析，从而大大减少无效数据的传输，提高数据处理效率。

网络层是电力物联网的神经系统，是数据传输和通信的部分。由于电力业务场景千差万别，网络层采用有线无线结合、专网公网并用的异构融合的通信方式。光纤通信具有高带宽、低时延、抗干扰等优点，依然是骨干网及重要站点的主要手段；而无线通信技术在覆盖广泛的配用电末端起到了重要的作用。5G 技术凭借大带宽、低时延以及广连接等特点，正在对精准负荷控制、配网差动保护等业务进行赋能；而低功耗广域网例如 NB-IoT、LoRa 等，经常用来做状态监测等低频次、小数据量的业务。电力无线专网，比如部署在某些区域的 LTE 230MHz 和 1.8GHz 频段，也能给感知数据提供安全可靠的通信保障，使得大量的感知数据可以及时、准确地传送到数据中央处理中心。

为了更加直观的了解不同的通信技术在电力物联网中的使用特点，下表给出了几种主要的通信技术的关键参数对比。

电力物联网主要通信技术对比表

特性 / 技术	5G	NB-IoT	LoRa	光纤通信	电力无线专网
带宽	极高	低	极低	极高	中高
覆盖范围	中	广	广	点对点 / 区域	区域性
功耗	高	极低	极低	低	中
时延	极低	高	高	极低	低

续表

特性 / 技术	5G	NB-IoT	LoRa	光纤通信	电力无线专网
部署场景	实时控制、高带宽业务 (精准负荷控制)	远距离、低频次数据 (状态监测)	远距离、低频次数据 (状态监测)	骨干网、重要站点	关键业务、专用通信
主要优势	高速、低时延、大连接	广覆盖、低成本、长续航	广覆盖、低成本、长续航	大容量、高可靠、抗干扰	安全、可靠、专有

平台层处在架构的中心位置，类似于电力物联网的“大脑”，主要是指物联管理中心以及全业务数据中心。物联管理中心对海量终端进行接入管理、设备认证、状态监测和全生命周期管理，它隐藏了底层异构终端的差别，给应用层供应统一的数据服务接口。全业务数据中心汇纳各环节、各专业的数据资源，依靠云计算技术、大数据分析技术、人工智能技术对数据实行深层次挖掘和治理。本层建设统一的数据模型，保证数据以统一的标准进行存储和共享，很好地避免了过去存在信息孤岛的现象。平台层通过使用云原生技术可以对计算资源做灵活调度的操作，以微服务的形式为上层应用提供强大的算力以及数据支持，从而使得上层应用能够实现快速的开发和迭代。

应用层是电力物联网价值落地的最终出口，面向电网运行、企业管理、客户服务等各方面的应用需求，提供多样化的应用服务。电网侧有设备资产管理、电网故障抢修、新能源消纳分析等应用，用户侧有智慧用能服务、虚拟电厂、电动汽车有序充电等新型业务。应用层调用平台层微服务组件及数据接口，从而达到业务逻辑灵活组合的目的。通过各种移动作业 APP、可视化大屏、智能决策系统等直接将经过处理的、高价值的信息展示给运维人员以及决策者，从而极大地提高了电网的运作效率和服务水平，真正实现了用数据来推动业务变革。

（二）电力物联网特征

电力物联网和通用物联网相比，具有很强的行业特征。必须符合电力系统对于安全可靠、实时等严格要求。电力基础设施遍布各地，无论是繁华的城市还是深山荒野，设备运行环境都是复杂的、多样的，这就需要物联网设备有很强的环境适应性，可以耐高温、耐极寒、耐高湿、抗强电磁干扰。数据传输的高可靠性也是电力物联网的一个特点，电力控制类业务一般要求毫秒级的通信时延、极低的数据丢包率，通信中断会造成电网事故，因此电力物联网在通信协议、网络架构的设计上一直把可靠性放在首位。

电力物联网的另一个特点就是海量连接，大规模接入。配电网变得越来越细，

用户侧的互动需求越来越多，接入电网的终端数量已经达到了亿级。既包括传统的电力设备，也包括充电桩、分布式光伏逆变器、智慧楼宇控制器等各种新型负荷。面对如此巨大的接入规模，电力物联网必须具有很强的并发处理能力以及地址管理能力。

全方位安全防护体系一直都是电力物联网的核心组成部分。电力系统属于国家重要的基础设施，它的网络安全关系到国家安全。电力物联网采取“安全分区、网络专用、横向隔离、纵向认证”的防护策略，对感知层设备本体进行安全加固，用高强度加密传输来保护网络层，对平台层用户身份进行认证及访问控制。尤其对控制类业务，实行物理隔离或者逻辑强隔离，保证核心控制指令不被篡改、不被伪造。

（三）边-云协同的物联网架构

在海量异构终端接入和实时业务需求双重驱动下，仅靠云端集中式处理已经不能满足目前的要求了，边云协同架构随之出现。该架构把计算、存储、智能分析等职能下放到网络的边缘，也就是靠近数据源头的变电站、配电房或者智能终端那边。边缘计算节点具备本地数据处理、协议解析、实时控制、本地决策的能力，可以对高频、高带宽的原始数据进行就地处理，只把提取出的关键特征数据或者异常报警信息上传到云端。

云端主要是做全局性的、非实时的数据处理、长时间跨度的数据分析、模型的训练和跨域的业务协同。云平台汇聚了全网的数据，有无限的算力和海量的存储，可以训练出高精度的 AI 算法模型，把优化好的模型通过空中下载的方式下发给边缘节点，让边缘设备变得越来越聪明。

边云协同使得资源可以得到最优分配。边缘侧快速反应可以达到继电保护、精确负荷控制等对时延的要求，云端以“上帝视角”保证电网规划、长期能效预测等宏观决策的正确性。两者通过标准的南向、北向接口进行互动，形成了云端训练、边缘推理，云端控制、边缘自治的良好循环，极大降低了骨干网带宽的占用，提高了系统的鲁棒性、反应速度。

二、电力物联网典型应用

（一）智慧变电站/换流站

智慧变电站就是电力物联网在枢纽侧的集大成者。部署全维度感知设备之后，

变电站就由以前的定期体检变成实时监护了。站内主变压器、GIS 组合电器、开关柜等主要设备都安装了声、光、电、热、化学等多参数传感器。以变压器油中溶解气体、套管介质损耗的在线监测为例，可以提前发现绝缘劣化趋势；依靠特高频传感器捕捉 GIS 内部微弱的局部放电信号，可精确定位到设备内部的故障。

智能巡检机器人和高清视频监控系统一起组成了变电站的“流动哨兵”。轮式机器人装有可见光摄像机、红外热像仪、高灵敏度拾音器，按事先设定好的路线进行全天候巡检，可以自动读取表计示数、辨别开关分合状态、检测设备热点。高空设备可以用挂轨机器人或者无人机轻松覆盖巡检死角。前端采集到的数据在站端边缘计算网关处汇总，然后经过 AI 算法的实时分析，一旦出现异常就会发出警报，并将视频画面传送到远端运维中心。

数字孪生技术的使用，使得智慧变电站进入了三维可视化时代。利用 BIM 建模与实时运行数据，运维人员可以在虚拟空间用三维全景图查看全站设备的运行工况。数字孪生体要表现物理实体的外观，更要体现它的内在逻辑与物理场的分布，在虚拟仿真的环境里可以开展操作演练，推演故障处置方案，提升现场作业的安全性以及事故应急处置的能力。

（二）输电线路智能巡检

输电线路一般会跨越山川，传统的人工巡检效率低、危险高，但是电力物联网技术完全改变了一种作业方式。以无人机为依托的空地一体化的智能巡检系统已经成为主流。装载激光雷达、高清变焦镜头、红外相机的工业级无人机，可以对输电通道做高精度的三维建模，并且可以做详细的巡检。无人机搭载 RTK 高精度定位技术，可实现厘米级自主飞行，自动对准绝缘子、金具、导线等重要部位多角度拍摄；采集的影像数据可以 5G 或者专网实时回传，也可以先存储起来交给 AI 平台批量识别缺陷。

在线监测装置是分布于高塔之上的“神经末梢”，是线路安全可靠的“守护神”。微气象区安装覆冰监测装置，通过拉力传感器实时测量导线覆冰厚度；地质灾害多发区布设杆塔倾斜、地基沉降传感器；大跨越区使用导线舞动监测系统。分布式故障诊断装置使用行波测距技术，当线路发生雷击或者短路故障的时候，系统可以在几秒钟内捕捉到暂态行波信号，把故障点定位在几百米之内，指引抢修人员快速到达现场。

可视化监拍装置的大范围部署，成功地解决了外力破坏的问题。前端内嵌的

边缘 AI 芯片可以对吊车、挖掘机、高杆植物等外部隐患实行实时识别。当大型机械进入线路保护区内的时候，装置会立即发出声光报警并驱赶，同时向输电运检人员发送告警图片。人防加技防的模式，把外破隐患治理由事后抢修变为了事前预防。

（三）智能楼宇与综合能源服务

用电侧智能楼宇、综合能源服务是电力物联网挖掘负荷侧调节潜力、提高能效的重要场景。智能楼宇已不再只是钢筋混凝土的堆砌，它有了智慧的大脑。借助物联网技术，楼宇内部照明，空调，电梯，给排水这些高能耗设备全部互相连接。用 LoRa 或者 ZigBee 无线传感器网络把整个建筑的所有角落都给覆盖住，实时采集温湿度、照度、二氧化碳浓度和人流密度这些数据。

楼宇能源管理系统用这些数据来做细致的调节。系统根据室外天气、室内人员分布情况动态调节空调机组的送风温度、风机转速，保证舒适度的前提下达到最大的节能；智能照明系统会按照自然光的强弱及人员活动情况自动开灯或者调光。对于“光储直柔”建筑来说，物联网平台俨然就是个微网控制器，可以协调屋顶光伏、储能的充放电以及建筑负荷，实现能源自给自足，就地消纳。

综合能源服务把应用边界进一步扩展。依靠电力物联网平台，供电企业从单一的电力服务提供商转变为综合能源服务提供商，给工业园区、商业综合体等提供电力、水、气、热、冷一体化解决方案。用多能耦合的感知设备对用户的用能习惯、负荷特性展开深入剖析，进而给用户量身定制专属的能效改良方案。更重要的是，分散的智能楼宇、园区负荷被物联网聚合成虚拟电厂后可以参加电网的需求响应市场。当电网高峰负荷的时候，虚拟电厂平台向成千上万个柔性负荷发出削峰指令，楼宇就自动把空调温度调高、照明调暗、储能放电，在用户几乎察觉不到的情况下完成电网的削峰填谷，实现了源网荷储的良性互动。

第三节 边缘计算技术

一、边缘计算概念与价值

（一）边缘计算的定义与架构

边缘计算指的是把网络、计算、存储、应用等核心能力集成到一起，在物理世界或者数据源头端侧形成的开放平台，目的是为数据源提供最接近的数据服务。其应用程序直接在边缘侧启动，可以实现网络服务的快速响应，很好地满足了行业对于实时业务、应用智能、安全、隐私保护等基本需求。电力系统边缘计算架构一般被分为终端层、边缘层和云端层三大部分。终端层主要是智能电表、传感器、微型同步相量测量单元等感知设备组成，主要任务是完成原始数据采集并初步上传。边缘层是整个架构的核心，边缘网关、智能配变终端、变电站边缘服务器等设备组成，部署在变电站、配电房或者输电线路杆塔上，主要对本地数据进行清洗、协议解析、边缘推理等工作。

利用 SDN（软件定义网络）与 NFV（网络功能虚拟化）技术来实施对计算资源动态分配、灵活配置的功能。边缘节点使用容器技术，各个微服务可以快速部署又互相隔离，不同的业务功能可以同在一个物理平台上同时运行，互不影响。边缘计算平台使用统一南向接口连接不同的现场总线和通信协议，实现各类设备的接入；利用北向接口同云平台保持链路畅通，上交重要的业务数据，并接收云端下发的控制指令及模型更新包。分层结构很好地分担了核心网数据传输的负担，大量的高频高带宽数据处理都在本地完成，只把提炼出来的高价值信息传给中心云，重塑了电力通信网的数据流转逻辑。

（二）边缘计算与云计算的协同

边缘计算不是云计算的完全替代，而是云计算的重要补充和延伸。两者互相配合，共同给电力系统智能运行给予支撑。云计算中心是云边协同体系的大脑，有大量的存储资源和超强的超大规模计算能力，主要是对非实时、长周期、全局性的数据分析，如电网运行趋势预测、全网资源优化调度、复杂的 AI 模型训练与更新等。云端汇聚各个边缘节点上传的特征数据以及摘要信息，依靠大数据平台进行深度挖掘，使用机器学习算法训练出高精度的业务模型，之后把优化过的模型参数下传到边缘侧。

边缘侧是“触手”，根据云端下发的模型，对实时性、周期短的本地业务进行现场推理执行。拿变电设备故障诊断来说，云端凭借历史大量样本培养出通用的故障识别模型，边缘节点加载这个模型以后，对现场实时监测数据实施快速推断，一旦察觉异常就马上发出告警或者执行断路器动作，还将异常样本数据上传到云端，供模型不断改进。云端训练、边缘推理，云端统筹、边缘执行这样的机制，充分发挥了云计算在资源整合、复杂计算方面的优势，又体现出了边缘计算在低时延响应、本地化处理方面的特点。两者通过制定标准的协同协议来进行交流，实现了资源、数据、智能、应用等各方面的协同，保证了电力业务全局优化与局部敏捷的协调统一。

这种协同模式的特点，可见下表所示：

云边计算协同特点对比

特征	云计算	边缘计算
计算能力	强大的超大规模计算	有限但专精的计算
存储能力	海量存储	本地缓存、短期存储
响应时延	相对较高（毫秒级到秒级）	极低（微秒级到毫秒级）
数据处理	全局、长周期、非实时	本地、短周期、实时
典型任务	模型训练、资源调度、大数据分析	实时推理、即时控制、数据预处理
部署位置	集中式数据中心	靠近数据源头（变电站、杆塔等）
带宽需求	高（原始数据上传）	低（仅传输关键信息）
安全隐私	依赖网络传输及中心存储安全	本地处理，提升数据安全隐私保护
鲁棒性	易受单点故障及网络中断影响	离线自治，提高系统鲁棒性

（三）边缘计算在电力系统中的价值

边缘计算技术出现以后，对传统电力通信网的数据处理和业务响应模式造成了很大的改变，给创建清洁低碳、安全高效的现代能源体系赋予了强大的内生动力。边缘计算在电力系统中主要的价值体现在以下几个方面：

1. 时延、带宽大幅下降，由于电力物联网数据量呈指数级增长，若把所有原始数据都直接传送到云端，就会造成通信骨干网带宽的压力很大。长距离传输造成的时间延搁不能满足继电保护、配网自动化这些毫秒级业务的要求。边缘计算把数据在本地进行过滤、压缩和分析，只把关键变化信息和分析结果传出去，从而大大降低了回传流量。它把控制闭环限制在本地局域网内，可以实现毫秒级或者微秒级的业务响应，从而保证电网控制的实时性、确定性。

2. 提高数据的安全以及隐私的保护。电力数据关系到国家能源安全和用户隐私,敏感数据不能传送到公共网络或者集中存放。边缘计算可以对数据进行本地处理,并且可以本地存储,不需要将数据从物理安全域之外的节点传过来,所以能有效减少数据被窃听、篡改的风险。通过在边缘侧对数据做脱敏、加密、权限控制,可以满足业务需求的情况下,最大限度地保护用户用能行为等隐私信息,符合越来越严格的数据安全法律法规的要求,有利于构筑起坚固的电力数据安全防线。

3. 业务可靠性,系统鲁棒性。传统的集中式架构有单点故障的风险,一旦与云端的通信链路断开,现场的业务就会陷入瘫痪。边缘计算赋予现场设备独立计算、决策的功能,在云端连接断开或者离线状态时,边缘节点依靠本地存储规则、模型完成基本业务运行,比如就地故障隔离、微网孤岛等等。该种分布式智能架构可以有效地增强电力系统对于网络波动、突发事件的抵御能力,保证重要电力业务的连续性,大幅度提高供电可靠性。

二、边缘计算应用场景

(一) 本地业务智能分析与决策

在配电台区侧,智能配变终端就是典型的边缘计算节点,担负着台区管理智能化的任务。它不再只是数据转发通道,它具有很强的本地分析能力。边缘节点对台区内电压、电流、有功功率、无功功率等电气量进行实时采集,并可以就地对电能质量进行深入分析,实时监测三相不平衡度、电压偏差和谐波含量等主要指标。当监测指标超过限定值时,边缘节点不需要等待云端指令,根据预先设定的策略自行调节无功补偿装置或者有载调压变压器,从而迅速改善电能质量,保证用户侧供电的稳定性。

边缘计算对于低压台区线损精益化管理也起到很重要的作用。智能配变终端实时汇聚了台区总表及各分户表的高频采集数据,在本地完成了同步计算和比对,实现了台线损分钟级精细化计算和分析。相比传统的每天一次分析方法来说,该实时分析模式可以更快地发现线损的异常波动,并配合拓扑识别算法来准确定位窃电行为或者计量故障点。依靠边缘侧拓扑自动识别功能,在执行电流特征注入以及电力线载波通信特征分析之后,系统可以创建起完整的低压配电网物理拓扑结构,完全化解了长久以来一直困扰低压配电网的“盲管”难题,为运维人员给

予准确的故障导航和抢修帮助，大幅度改善了配电网的精细化运作水准。

（二）数据预处理与实时响应

在输电线路监测场景中，对杆塔上各种传感器的布置，实现了对微气象、导线舞动、杆塔倾斜、绝缘子污秽度等状态信息的全天候监测。传感器产生的数据量很大，其中存在很多重复、无效的冗余信息。杆塔侧部署的边缘网关承担着数据预处理的任务，对采集到的原始波形数据进行清洗、去噪和特征提取。如导线舞动监测，边缘网关依靠内置算法对加速度传感器数据做频域分析，去掉风吹等造成的常规振动干扰，只有当发现类似舞动特征的异常频谱时才会触发高频录波，把告警数据包传到监控中心。有效防止无效数据占用通信链路，并延长了监测终端的电池使用寿命。

边缘计算在变电站辅助设备监控中也起着不可缺少的作用。变电站内水泵、风机、空调、照明等辅助设备数量很多，传统的控制方式多是人工巡检或者定时控制。引入边缘计算后，边缘联动控制器可以接入温湿度传感器、水浸传感器和安防设备等，在本地做逻辑编程来实现设备之间智能的联动控制。当烟感探测器报警时，边缘控制器会立刻断开通风系统电源、启动灭火装置、打开门禁系统供人撤离。所有的动作都是在本地瞬间完成的，不会受到外部网络拥塞的影响。由此而形成的一种以边缘端为依托的实时联动响应机制，大大提升了变电站的安全防护水平以及应急处置能力，也是建设无人值守智慧变电站的一项重要的技术基础。

（三）图像识别与 AI 推理

随着无人机巡检、视频监控在电力系统中广泛应用，海量图像、视频数据处理成了一个巨大的难题。传统的视频回传云端分析模式存在带宽瓶颈、高昂的流量成本问题，特别是在网络信号不好的偏远山区，不能保证实时性。边缘计算把人工智能推理引擎往前端摄像头、无人机机载计算机或者变电站内的边缘分析服务器推移，从而达成视频图像的就地智能化处理。载有边缘计算模块的无人机在飞行中可以实时对所拍摄影像进行分析，并用轻量级的深度学习算法自动判断出绝缘子破损、导线断股、鸟巢异物等各种缺陷。

无人机不需要把所有的高清视频传回地面站或者后台，只需要把识别出的缺陷图片和 GPS 坐标传回去就行，这样大大减少了对通信链路的要求，也让巡检人员可以现场马上确认隐患，大大提高了巡检效率。边缘侧视频分析盒子部署在

变电站和施工现场的边沿，可以对摄像头传输过来的实时图像进行分析。一旦发现违章行为，系统就会立即启动现场广播发出驱离和告警信号，实现了由以往的事后追溯向事前预防、事中阻止的管控模式转变。红外热成像数据的边缘分析也被用来监测设备的温度。边缘设备能自脱环境温度的影响，对接头过热等缺陷进行准确识别，产生温度趋势图上传到服务器，为设备的状态检修提供精准的数据依据。

第四节 人工智能应用

一、AI 在通信网络管理中的应用

（一）智能故障诊断与预测

电力通信网覆盖范围广、设备种类多、运行环境复杂，故障发生具有随机性和隐蔽性，给运维工作造成很大困难。采用人工智能中的深度神经网络对大量的历史告警数据、性能指标、日志文件做相关性分析，可以准确的识别故障特征模式。系统不再只是简单的阈值报警，可以学习设备参数的时间序列变化规律，构建设备健康度评估模型。只要监测数据有一点点异常波动，模型就会立刻察觉并发出警报，实现故障的“未病先治”。

智能诊断系统在实际运用中，会用到知识图谱技术，把零散的故障案例、专家经验等转化为数字形式，形成庞大的故障知识库。网络出现异常时系统可以很快地找到故障原因，并给出最好的解决方案。对于光缆中断、设备掉电等常见的故障，AI 算法利用多方面的数据互校验，有效排除了误报信息，大大减少了运维人员无谓的排查工作量。对不易复现的软故障，长短期记忆网络可以追溯历史状态，找出造成故障的深层逻辑链条，给彻底解决顽疾提供科学依据。由原来的“事后抢修”变为“事前预防”的运维模式，极大地提高了电力通信网的可用率。

（二）网络流量智能调度与优化

电力业务种类的多样化给通信网络的带宽、时延、抖动提出不同的服务质量要求。传统的静态路由配置不能很好地应对突然出现的业务流量冲击，容易引发局部网络拥塞。人工智能技术和软件定义网络相结合，给网络流量的智能调度开辟了新的途径。强化学习算法作为核心引擎，可以感知全网链路状态、业务流分布情况，与网络环境不断交互试错，得到最好的路由策略。按照业务的重要程度

给继电保护、精准负荷控制等重要业务开辟绿色通道，保证其畅通无阻。

1. 即动态带宽分配是按预计业务流量的趋势进行带宽的动态调用的方式。用电高峰期系统自动增加营销采集业务的带宽配额，保证计量数据的及时上传；电网故障处理的时候优先保障调度数据网的传输资源，抑制非关键业务流量，最大限度提高网络资源利用率。

2. 拥塞避免与均衡：依靠图神经网络对于网络拓扑结构分析的能力，系统可以对整个网络负载情况做出全面的掌握。当某条链路负载率接近告警值的时候，AI 算法就会提前计算出备用路径，通过微调流量流向将数据平稳地转移到负载低的链路上，避免拥塞现象的发生，达到全网络负载均衡的目的。

（三）通信网络安全智能防护

电力系统属于国家重要的基础设施，它的通信网络正遭受着越来越严重的网络攻击。传统的特征库匹配防护方法对于 APT、未知漏洞攻击没有办法。利用人工智能技术构建的网络安全防护体系，在建立起流量行为基线之后，就可以对异常流量进行及时的监测并加以智能判断。无监督学习算法可以对通信报文的载荷特征、时空分布规律等展开深入分析，自行找出正常模式下异常的行为。又如僵尸网络控制指令、少量慢速扫描探测之类隐蔽的威胁，也都难逃 AI 的眼睛。

利用对抗生成网络技术可以提高防御系统鲁棒性。经由模仿黑客攻击来创造许多对抗样本，既充实了训练数据集，又让防范模型在持续发展当中加强了对各类变种攻击的识别力度。智能清洗系统对分布式的拒绝服务攻击即 DDoS，能够做到毫秒级的响应速度，经过层层过滤之后把恶意流量剥离出去，保证正常的业务可以正常进行。联邦学习技术冲破各个区域网络之间的数据壁垒，于保持数据隐私的前提下达成威胁情报的交流并实行协同防御，塑造起全天候、全方位的网络安全免疫体系。

二、AI 在电力业务分析中的应用

（一）基于通信数据的负荷预测

负荷预测是电力系统调度运行和规划的基础，它的好坏直接影响到电网的安全经济运行。传统的负荷预测方法主要利用历史负荷数据和气象信息，没有充分挖掘通信网侧丰富的数据。引入人工智能以后，预测模型就可以把通信网流量数据、智能电表采集频次、社交媒体舆情等多源信息融合起来。通信数据的波动一

般会先于电力负荷的变化出现，如某地通信基站流量突然增大，一般会预示着该地大型活动的到来，从而推断出该地的电力负荷也会随之增加。

深度学习中长短期记忆网络、门控循环单元特别适合于时间序列数据的处理。模型可以自动提取负荷数据中的长期周期性特征和短期突发性扰动，并考虑气象因素的非线性影响，可以准确预测未来负荷，实现超短期、短期和中长期的精细化预测。对分布式新能源接入较多的微电网来说，AI 算法在接收到逆变器通信报文之后，可以立即修正光伏、风电的出力预测误差，降低新能源波动给主网带来的冲击。利用跨域数据融合的预测模型，可以很大程度上提高负荷预测的准确率与鲁棒性，给电力供需平衡调节提供更好的数据支撑。

（二）电网运行状态智能评估

电网运行状态实时评价是防止大范围停电的又一道重要防线。电网规模变大、电力电子设备大量投入使用的时候，系统动态特性就变得十分复杂。人工智能技术应用广域测量系统得到的大量同步相量数据，迅速接近电网稳定性的边界。卷积神经网络把电网拓扑结构转成图像特征，清楚显示电压稳定情况以及频率变动情形。系统受到扰动的时候，AI 模型可以毫秒级地完成暂态稳定判断，判断系统是否处于失稳风险之中。

依靠数字孪生技术搭建智能评估平台，用实时通信数据驱动虚拟电网模型同步运行。系统通过比较物理电网与虚拟模型的运行参数差异，可以很容易发现互感器漂移、开关接触不良等隐性问题。根据变压器油色谱在线监测数据、局部放电信号以及设备全生命周期积累的全部数据信息，利用设备侧 AI 算法来判定主设备的绝缘老化状况和剩余寿命。从小到大的、由设备到系统全貌的状态评估，给电网检修策略的制定提供科学依据，促使检修方法由“定时检修”向“按状态检修”彻底转变，大大提高了资产的全生命周期效益。

（三）用户用电行为分析

智能电表的全面普及加上通信网络的全覆盖，从而产生大量的用户用电细颗粒度数据。人工智能技术经过深度挖掘之后，就可以得到用户的用电画像。聚类分析算法根据用户的负荷曲线形态、用电时段偏好和峰谷特性，把大量的用户分为工业生产、商业运营、居民生活等不同类别，再细分出高能耗用户、对电价敏感型用户、新能源消纳型用户。从而给电力公司制定出有差电价套餐、需求侧响应策略提供数据支持。

非侵入式负荷监测技术利用高频采样的总进线电流电压数据,采用模式识别算法,把用户内部主要电器的启停状态和耗电情况准确地分离出来。电力公司据此可以为用户出具个性化的能效诊断报告,指导用户淘汰高耗能的老旧家电,养成良好的用电习惯,从而降低用户的电费支出。在反窃电上用同类用户用电模式对比、线损异常波动、电表事件记录等信息来判断是否存在疑似窃电行为,进而打击违约用电。利用大数据开展精细化服务和管理,既改善了用户的满意程度,又给予创建公正有序的供用电秩序赋予技术支撑。

三、AI 技术融合挑战

(一) 数据质量与标注问题

高质量的数据是训练出高性能 AI 模型的前提,而电力通信网实际运行中获取“干净”的、标注完整的数据并不是一件容易的事。电网设备长时间工作于复杂的电磁环境之中,传感器所采集到的数据当中常常掺杂着各种噪声干扰,数据缺失和异常值漂移的情况也时常出现。直接使用这些低质量的数据来训练模型,容易造成算法难以收敛或者得出错误的结论。数据清洗和预处理经常占到 AI 项目开发时间的大多数,并且很大程度上依靠领域专家的经验,不能完全自动化。

1. 样本不平衡问题,在故障诊断中,电网设备的高可靠性造成故障样本非常少,正常运行数据却非常多。严重的类别不平衡会造成分类器把所有的样本都预测为正常类,从而漏掉重要的故障。生成式对抗网络可以生成一部分虚拟样本,但是其物理一致性要经过严格的检验。

2. 标注成本高,监督学习算法需要大量的有标签数据,而电力数据的标记需要大量的专业知识。依靠人工对海量的波形图、红外影像一个一个进行标注,效率低,而且容易受到主观因素的影响产生不一致。缺少统一的、标准的行业数据集,是 AI 算法在电力领域应用推广的又一重大阻碍。

(二) 算法模型的可解释性

电力系统属于物理系统,它的运作受到严格物理规律的约束,调度员执行控制操作之前,必须要明白其背后蕴含的逻辑根据。目前主流的深度神经网络模型被视作“黑盒”,虽然在预测精度上表现良好,但是它的内部决策过程具有非线性性的特点,不能用自然语言清楚地表达出来。当人工智能模型给出切负荷命令或者路由切换指令的时候,倘若不能给出令人信服的因果解释,调度人员便很难接受这

些指令，这在很大程度上制约了人工智能技术在电网核心控制方面的深入使用。

提高模型可解释性的方法有深入研究、应用可解释人工智能技术。一种途径就是给出决策结果的时候强调模型所关注的输入特征，比如因为某个时段电压波动而发出故障预警。第二种途径就是结合物理机理模型和数据驱动模型，构造物理信息神经网络。在损失函数里加入基尔霍夫定律等物理约束，让神经网络学习的映射关系符合物理规律。融合模型可以提高预测的可信度，也可以保证训练数据覆盖范围之外的泛化能力，为 AI 和电力物理系统和谐共生打开了新的大门。

（三）AI 应用的安全与伦理

随着电力通信网中 AI 技术的渗透率提高，算法的安全性问题也开始凸显出来。对抗样本攻击成为新的威胁，攻击者只需要对输入的数据加上人眼几乎察觉不到的小扰动，就能使 AI 模型做出完全相反的判断，例如把正常设备的红外图像识别成过热故障，从而导致系统误操作。由于电力系统的连锁反应性质，一个节点的算法判断失误就会放大为整个电网的震荡。算法后门也存在风险，供应链上的第三方预训练模型中如果植入恶意代码，在特定的触发条件下就会造成系统瘫痪。

数据隐私和伦理问题也不可轻视。智能电表采集的高频数据非常敏感，可以推断出用户的作息规律、家庭成员情况、经济水平等隐私信息。如果这些数据在传输、存储或者被 AI 分析的过程中泄露，会对用户的隐私造成严重的侵犯。在算法决策上要防止“算法歧视”，也就是由于训练数据有偏见，对某些地区或者某类用户不公平地实施限电。健全人工智能在电力通信网中算法安全审查机制、伦理规范，确定算法决策的责任主体，积极采取差分隐私、多方安全计算等隐私保护计算技术，是人工智能在电力通信网中健康、可持续发展的必然要求。

第五节 区块链技术

一、区块链基本原理

（一）分布式账本、共识机制、智能合约

分布式账本是区块链主要的物理形式，摒弃了传统的中心化服务器数据存储方式，将数据的维护工作分给网络中每一个节点。每一个节点都保存完整的账本

副本，所以数据一旦发生变化，就会在整个网络里广播并被确认。冗余存储使得数据可靠性变高，即使节点出现损坏或遭攻击整个系统依然能保证数据的完整及可用性。电力通信网络中的大量电表数据、设备状态信息不再依赖单一的控制中心，而是分布在各个边缘计算节点或变电站服务器中，从物理结构上避免了单点故障。

共识机制是区块链的“决策大脑”，它解决了在没有中央权力机构的情况下，分布式网络怎样达成数据一致性协议的问题。常用的共识算法有工作量证明、权益证明、实用拜占庭容错算法等，各有利弊。工作量证明用算力竞争保证安全，但是能耗巨大；权益证明用币龄或权益的方式来减少资源消耗；实用拜占庭容错算法更适用于对吞吐量要求高、节点数量相对稳定的联盟链环境。电力场景下，由于电网业务对于低时延的要求以及一定的去中心化程度，所以会更多地使用投票或授权类的共识机制。

智能合约是区块链的自动化执行层，是部署在区块链上的、可以自动执行的计算机程序。当预设的条件满足时，智能合约就会自动执行合同中的相应条款，不需要人工干涉，也不能更改。这一特点把传统的被动式数据记录转变为主动式价值交换，给电力系统中的自动化交易赋予了技术实现途径。代码即法律，智能合约执行的结果是确定的，可以保证多方合作流程的规范性以及资金安全，彻底杜绝人为违约的现象，从而降低制度性交易成本。

（二）区块链的类型与特点

1. 公有链是完全开放的区块链网络，任何人都可以加入或者退出，并且可以参加记账和共识的过程。具有最高的去中心化程度、最大的数据透明度，但由于吞吐量低、延迟高，不能直接用在要求实时性高的电网控制业务上，更多地被用在公众参与度高的碳普惠或积分激励场景上。

2. 联盟链是由多个机构共同来管理的一种区块链，介于公有链和私有链之间。其达成共识的过程是由预先选择好的节点控制的，接入网络也需要授权。在保持一定去中心化的前提下，大大提高了处理效率和隐私保护能力，是目前电网企业与发电企业、售电公司创建多方合作平台的主要架构。

3. 私有链完全是某个组织控制，读写权限严格控制。虽然去中心化程度不高，但是交易速度很快，而且具有很好的匿名性，适合电网企业内部跨部门的数据共享、审计和流程优化，在不改变现有管理体制的基础上提高数据流转效率。

区块链技术的特点有去中心化、不可篡改性、可追溯性、开放性，其中去中心化打破信息孤岛，促进数据跨域流动；不可篡改性用哈希指针和链式结构来保证历史数据真实性；可追溯性保证了每一个交易或者数据记录都可以追溯到源头；开放性让不同主体接入网络中，使能源生态更加繁荣。这些特性一起形成了区块链支持电力通信网络的技术基础，可以满足不断增长的能源互联需求。

（三）区块链与电力系统的结合点

电力系统正在由单向供电向源网荷储互动发生改变，大量的分布式资源接入使系统具有很强的离散性及复杂性。区块链的去中心化特性同分布式能源的物理分布特性天然相适。从物理的角度讲，分布式光伏、储能装置和电动汽车这些设备分布到了用户端；而从逻辑角度来讲，区块链节点可以布置在智能电表、能源路由器等终端设备上，达到物理网络与信息网络拓扑同构的目的，为分布式资源的本地化管理与自组织协作提供了条件。

多主体信任的建立是两者又一个重要的契合之处。随着电力体制改革的不断深入，市场主体也越来越多，电网公司、发电集团、售电侧、终端用户之间相互之间的博弈也越来越复杂。传统依靠中心化机构建立的信任方式，成本高、效率低。但是区块链使用数学算法创建了机器信任，互不相识的主体可以依靠一个可信网络完成安全的交易。重建信任机制对降低市场准入门槛、促进市场活力有决定性的作用。微电网内部采用区块链技术可以实现产消者之间的能源点对点交换，减少对上级电网调度的依赖。

数据资产的价值挖掘也是结合的一部分。电力数据是工业互联网的血液，有巨大的经济价值。但是数据确权难、隐私保护难一直阻碍着数据的流通。区块链使用密码学技术，可以做到数据所有权和使用权分离，保证数据共享过程中数据可用不可见。这样电力数据可以在银行征信、保险理赔、政府决策等领域得到应用，而不会侵犯用户隐私权，真正发挥出电力大数据的要素价值。

二、区块链在电力通信中的应用探索

（一）分布式能源交易与结算

分布式能源交易中使用区块链来创建去中心化的点对点交易平台，彻底改变了传统的统购统销模式。分布式光伏业主、小型风电场、带有储能的用户通过区块链网络发布售电信息，与周边的用电需求方进行匹配。智能合约在这里起自动

撮合、结算的作用。当买卖双方就价格、电量达成一致，或者满足预设的交易算法条件的时候，智能合约就会自动触发交易执行，记录电量转移，同步完成资金划转。此种模式一方面削减了中间商赚取差价的机会，提高了发用电双方的收益；另一方面也实现了电能的就近消纳，减轻了主网的输送压力。

传统的电力结算周期一般一个多月或者更长，资金占用高且容易产生计量争议。使用区块链之后，每一度电的产生、传输、消耗都会即时记录在区块链上，数据不能被篡改，并且所有节点都会同步。依靠实时数据流，交易结算是可以实现日结甚至实时结算的。即时性大大加快了资金周转速度，降低交易对手的风险。对于电动汽车充电桩共享这种小额高频的交易场景，区块链的微支付通道技术提供了一种低成本的解决办法，用户在充电结束后拔枪的瞬间就可以立即完成自动扣费，不需要繁琐的确认过程，用户体验得到了很大的提升。

（二）绿色证书追溯与管理

绿色电力证书是推进可再生能源消纳的重要政策工具，但是传统的管理方式存在着重复计算、双重使用、溯源困难等问题。区块链技术给绿证的整个生命周期经营给予了完美的解决办法。绿色电力从产生的一刻起，智能电表就会把发电数据上传到区块链上，生成唯一的数字资产凭证。凭证上详细列出了电力的来源、种类、产生时间、碳减排量等各方面信息。因为区块链有不可篡改的属性，信息产生以后就被永久锁定，不可能出现数据造假的情况。

在绿证流转的每一个环节都会完整的记录进分布式账本里。监管机构、购电者、社会公众利用区块链浏览器来查看绿证的状态与历史，达到电证合一的效果。企业用绿证抵消碳排放指标的时候，智能合约会自动注销对应的绿证，从而避免出现绿证被多次出售或者反复申报的现象。透明化的管理方式使绿色电力市场更加可信，调动了社会各界消费绿电的积极性，为我国双碳目标的实现提供了有力的技术支持。

（三）网络安全与数据存证

电力通信网络是重要的基础设施，所受到的网络攻击威胁也愈加严重。传统的边界防御系统对于高级持续性威胁以及内部攻击起不到作用。区块链技术给出了一种新的安全防护思路。在设备认证方面，基于区块链的身份认证机制抛弃了传统的中心化 CA 认证，将设备的身份信息分散到整个网络里。每一个接入电网的物联网终端，比如智能电表、传感器等等，都有一个唯一的区块链数字身份。

设备间的通信要使用私钥签名,伪造的接入请求由于不能通过共识验证而被拒绝,从而有效地防止非法终端进入系统。

区块链的又一重要应用就是关键业务数据的存证。电力调度指令、故障录波数据、市场交易记录等敏感数据,用区块链技术可以实现防篡改存证。数据一旦上链之后,就无法单方面被修改或者删除。即使黑客破坏了一个数据库节点,也不能篡改其他节点上保存的副本。这对电力事故的责任认定也有着十分重要的意义。电网发生故障时,链上的操作日志和状态数据就成为无法否认的电子证据,调度人员的操作、保护装置动作的先后顺序一目了然,为事故调查分析提供客观公正的凭据。

区块链也可以用来管理软件供应链的安全。电力系统中各种控制软件、固件升级包的哈希值可以存入区块链。终端设备在执行版本更新或者补丁分发的时候,会先对下载的文件进行哈希计算,然后和链上记录进行比对,只有比对成功之后才会允许安装。这就有效地防止了恶意代码混入正常的软件更新中,保障了电力二次系统的软件环境安全。依靠创建以区块链为基础的可信数据环境,电力通信网络的防御纵深得到了很大程度的延伸。

三、面临的挑战与发展趋势

(一) 性能与可扩展性问题

性能瓶颈成了区块链在电力系统大规模使用时面对的第一道障碍。电力系统是毫秒级实时控制的庞大物理网络,高频次的量测数据采集和实时的控制指令下发,对通信系统的吞吐量和时延有很高的要求。目前公有链技术每秒可以处理的交易量为几十到几百,不能满足电网级高并发的要求。即便是性能较好的联盟链,在数以亿计的物联网终端接入的时候,也会出现网络拥塞、数据膨胀的现象。随着时间的推移全量账本的数据量呈指数增长,会加重节点存储空间和带宽的压力。

解决这个矛盾的方法是分片技术、侧链技术、闪电网络这几种二层扩展技术。分片技术把网络分成若干子网,平行处理交易,理论上吞吐量可以成比例增加;侧链技术把很多小额、高频的交易转到链下处理,只把最终的结算结果上链,减轻主链的负担。根据电力业务的特点来对区块链的共识算法和区块结构进行优化,在嵌入式设备这样的限制性条件下也能高效运行,因此区块链技术适合于电力物联网的边缘计算环境。

（二）技术标准与监管政策

没有标准体系是阻碍区块链技术大范围应用的一个重要因素。目前电力行业区块链应用还没有形成统一的技术标准、数据规范，各厂商开发的区块链平台更像一个全新的信息孤岛，底层协议不兼容，跨链交互困难。不但会增加系统集成难度，而且会影响业务之间协同。制定包含底层架构、智能合约、数据格式、安全防护等各方面电力区块链标准体系，是实现行业级应用协作的前提。

监管政策不确定带来的也是发展的风险。区块链的去中心化、匿名性特征和电力行业强监管属性存在着天然的矛盾。智能合约的法律效力、分布式交易的纳税主体如何认定、跨境电力交易中的数据主权等都不在现行法律法规的调整范围之内。技术创新的同时还要探索建立穿透性监管的技术手段，运用监管沙盒机制来确保区块链的应用按照合规的轨道进行。既要保证市场主体创新积极性，又要防止系统金融风险 and 网上安全风险的发生，让技术发展和政策监管处于一个动态平衡之中。

（三）“区块链+”融合创新

区块链不应该被看作是一项单独的技术，而应该看作是各种数字技术之间的“胶水”。未来发展的趋势必然就是区块链与多技术的融合创新。

区块链与其他技术的融合优势

与人工智能结合	AI 算法可提升区块链共识效率与网络路由；区块链为 AI 提供可信数据和模型训练记录，解决 AI 的黑盒信任问题。在电力交易中，AI 预测电价波动，智能合约自动执行最优交易策略，两者互相促进。
与 5G 通信技术融合	5G 的高速率、低时延、广连接特性为区块链节点间海量数据同步提供了高速通道，尤其在移动储能、车联网等场景下保障了网络连接稳定。同时，区块链可管理 5G 基站间频谱资源共享、网络切片计费等，构建更公平开放的通信基础设施。

多技术跨界融合将产生虚拟电厂、综合能源服务等新的商业模式，电力通信网络也将成为价值互联网，最终实现能源流、信息流、价值流的“三流合一”。

第十章 电力通信网发展展望

第一节 技术发展趋势

一、通信技术的融合与演进

新一代通信技术飞速发展，给电力通信网注入了源源不断的动力。移动通信技术代际更迭、空天地一体化覆盖的形成、算力和感知能力的深度融合，这三点就是未来电力通信技术发展的一条主线。多种技术的深度融合会大大扩大电网的感知范围，并且会明显提高信息交流的及时性、广泛性。未来电力通信主要技术趋势，见下方通信技术特性对比表。

通信技术特性对比表

技术类型	主要优势	电力应用场景	未来展望
5G-Advanced	大带宽、低时延、广连接、高精度定位、确定性传输	差动保护、配电自动化、变电站巡检机器人、高清视频监控、电力资产全生命周期管理	持续标准化完善，无源物联特性增强，成本降低。
6G	全息通信、感官互联、内生智能、内生安全	电网数字孪生、沉浸式运维、远程全息专家支持、资源动态调整、系统鲁棒性与适应性增强	连接物理与数字世界，实现网络自优化、自免疫。
空天地一体化网络	全球覆盖、全地形接入、低时延、高通量	偏远地区电力设施接入、海上风电场数据回传、跨国输电线路监控、应急通信保障、临时组网、特定区域长时间驻留覆盖	打破异构网络壁垒，终端无缝切换，统一接入标准，高效资源调度。
算力网络	计算与网络深度融合、分布式算力池、智能感知路由	边缘智能分析、快速决策、数据不出站、业务低时延、智能调度最优计算节点	算力像水电般按需调度，支撑海量边缘数据处理。
感知网络	通信感知一体化、环境感知、目标定位、动作识别	输电线路异物入侵监测、覆冰感知、导线舞动实时感知、电力神经网络构建、资源共享互促	缩减硬件成本，通信与感知资源共享，实现全域感知。

接下来,我们将对这些关键技术进行详细阐述。

(一) 5G-Advanced 与 6G 技术前瞻

5G Advanced 是第五代移动通信技术的改进版,继承了高带宽、低时延、大连接的特性,在保持大容量、低时延、大数据的特点上还提高了上行性能,定位精度和确定性传输的性能。对电力场景来说,可以更好的满足差动保护、配电自动化等业务对于时延抖动的苛刻需求,也能给变电站巡检机器人、高清视频监控等大上行带宽业务提供更好的承载方式。随着标准化的不断完善,其在无源物联方面所表现出的独特特点,会使得电力资产全生命周期管理成为现实,从而大幅度降低终端部署成本和维护难度。

展望第六代移动通信技术,其意义早已超出通信速率的简单提升,而在于搭建起物理世界与数字世界的桥梁。对于电力系统来说,6G 的全息通信、感官互联等特性,可以让电网数字孪生技术达到一个新的水平。沉浸式交互体验会彻底改变电力设备运维的模式,专家可以依靠远程全息投影进行非现场技术支持。同时内生智能、内生安全特性使网络具有自我优化、免疫能力,可以根据电网业务实时变化动态调整资源分配,从根源上提高通信系统鲁棒性、适应性。

(二) 空天地一体化网络

创建全球、全地形的空天地一体化通信网络,这是解决偏远地区电力设施接入难题的一种有效途径。传统的地面光纤网络和无线基站不能对深山、沙漠、海洋等恶劣环境进行覆盖,卫星通信和高空平台可以很好的弥补。低轨道卫星星座的大规模组网可以明显减小卫星通信的时延,可以承载中低速的电力控制业务。海上风电场,跨国输电线路等结合高通量卫星技术可以为其提供稳定的、可靠的、全方位的监控数据回传通道。

无人机属于中低空通信平台,在应急通信保障以及临时组网方面起着不可替代的作用。地面基础设施遭到自然灾害破坏的时候,携带通信载荷的无人机可以快速起飞,搭建起临时的应急通信链路,从而恢复受灾地区的电力指挥调度。平流层飞艇等高空平台具有卫星的广覆盖和地面的低时延双重优势,可以对某一区域长时间驻留覆盖。

1. 层次网络融合会打穿异构网络壁垒,终端设备能够在地面基站,无人机,卫星之间自由切换,保证电力业务随时随地都能得到连续的通信服务。

2. 一体化协议体系建立之后可以统一空天地接入标准,简化网络管理的复杂

性，实现跨域资源的高效灵活调度，从而大幅度提高全网的资源利用率。

（三）算力网络与感知网络

伴随着电力物联网终端数量的爆炸式增长，边缘侧产生了大量的数据，传统的集中式云计算模式已经无法满足其实时处理的要求。因此算力网络应运而生，算力网络主张计算资源与网络资源的深度融合，希望将算力像水电一样统一调度、按需分配。电力场景中变电站、配电房等边缘节点会拥有很强的计算能力，于是就形成了一个分布式的算力池。通过互联网对算力进行智能感知和路由，业务请求可以实时调度到最优的计算节点去处理，数据不出站、业务低时延，有力支持电网边缘智能分析和快速决策。

通信感知一体化技术给通信网络赋予了超越传统数据传输的新能力。按照无线信号反射、散射等性质，通信基站以及终端就可以对周围环境实现感知，完成目标定位、动作辨识、环境观测等功能。通信感知技术可以实现输电线路周边异物入侵、覆冰和导线舞动的实时感知，不需要再单独布置专用的传感器。

通感融合模式一方面可以大大降低硬件的部署成本，另一方面也可以实现通信和感知资源的共享。感知的辅助可以提高通信波束对准的准确性，而通信的交互则可以把感知数据实时回传，共同形成全域感知的电力神经网络。

二、网络架构的变革

（一）SDN/NFV 技术的深度应用

软件定义网络，控制面与转发面分离后，使网络流量可以集中控制和调度。在电力骨干通信网中采用 SDN 技术可以全局视角对流量路径进行优化，避免局部拥塞，提高带宽利用率。发生光缆中断等故障时，控制器能在毫秒级之内下发流表，自动重路由业务链路，保证继电保护等重要业务不间断运行。SDN 可以针对不同的电力业务等级创建隔离的虚拟切片，保证高优先级业务独占资源，不受低优先级业务流量的干扰，在一个物理网络上对不同业务实现差异化承载。

网络功能虚拟化，把防火墙、路由器、加密机等专用硬件设备的功能软件化，在通用服务器硬件上运行。使设备部署更灵活，新业务上线也无需冗长的硬件采购和安装过程。智能变电站场景下，采用 NFV 技术把站内通信、计算设备进行整合，建立统一的虚拟化基础设施平台。

1. 弹性伸缩能力使得网络资源可以随着业务量的变化而动态调整，当业务量

较小的时候释放资源，当业务量大的时候自动扩容，从而大大降低建设投资和运行能耗。

2. 统一的编排管理平台可以实现跨厂商、跨域的端到端服务自动化开通，运维人员只需要简单的配置就能完成复杂的网络服务链部署，大大提高了运维效率。

（二）确定性网络发展

随着新型电力系统对于控制精度的要求越来越高，传统的以太网“尽力而为”的传输方式已经不能满足配电网差动保护、精准负荷控制等业务对于时延和抖动的极致要求。确定性网络技术是在以太网的基础上，采用时隙调度、帧抢占、循环排队转发等方法来为重要的业务提供有界时延、低抖动、零丢包的传输服务。使以太网电力通信网可以承担起原来需要 SDH 等专用技术承载的实时控制类业务，真正实现信息技术和操作技术网络的深度融合。

在变电站过程层网络中使用确定性网络技术，可以保证采样值、GOOSE 报文的实时传输，消除由于交换机排队延迟带来的不确定性。这对于数字化变电站的稳定运行来说十分重要，可以避免由于通信延时所造成的保护误动或者拒动。时间敏感网络标准和产业链日趋成熟完善，确定性网络将由局域网扩展到广域网，构建跨广域的确定性传输通道。届时，未来发出的电力调度指令将会和本地总线指令一样，以微秒级的时延跨越千里到达分布式能源终端，达到全网络范围内协调精确控制的效果。

（三）意图驱动与自治网络

意图驱动网络属于网络自动化高级阶段，用户可以通过自然语言或者高层次的业务逻辑表达运营意图，不需要关注具体的底层配置。网络系统把它们转译成对设备的配置指令，一直观察网络情况，保证实际运行结果符合用户的想法。当调度员输入“保障某条特高压线路保护业务最高优先级、双路由备份”时，网络会自动计算路径、预留资源、下发策略，对不能满足条件的状态进行闭环处理，全程不需要人工干预。

自治网络在意图驱动的基础上加入了人工智能、机器学习的技术，想要达到网络“零接触”运维的效果。通过对大量的历史运维数据进行学习，自治网络就有了对故障的预测、对根因的分析以及自我修复的能力。当光缆出现劣化征兆的时候，系统就会发出预警，并且自动切换业务，把故障消灭在萌芽之中。

自治网络既可以依据事先设计好的方案自行运转，也可以对流量的涨落作出

相应的反应。用电高峰期自动加大通信带宽以应对大量的数据交互，夜间低峰期利用休眠节点的方式来达到节能的目的。这种由“人治”走向“智治”的转变，将会解放运维人力，给电力通信网赋予真正的智慧大脑。

三、安全技术的创新

（一）零信任安全架构

传统网络安全架构大多按照“边界防护、内部信任”这个假设来搭建，边界一旦被攻破，攻击者就能在内网里逍遥法外。零信任架构就抛弃了这个假设，一直保持验证的状态。电力通信网在采用零信任原则之后，不论是面对外部互联网的访问，还是内部局域网中的终端互相连接，均需通过认证以及权限判定。每一次数据访问请求都要按照用户的身份、设备的状态、应用的环境等各方面情况实施动态的信任评价，只给予完成本次任务所必需的最小权限。

零信任理念把安全边界收缩到每一个终端、每一个应用、每一个数据包。分布式光伏、充电桩等分散式接入终端可以利用零信任架构下软件定义边界技术，将应用服务隐藏起来，只允许经过认证的合法终端访问服务器，有效地抵御扫描探测和拒绝服务攻击。即使某个终端被攻破，攻击者也不能利用跳板将窃取到的核心数据转移出去，因为该终端的权限范围已经被严格限制。动态信任评分机制可以对终端行为异常做出实时的感知，当发现违规操作或者环境风险时就立刻对终端进行降权或阻断，从而达到安全防御的动态化、精细化的目的。

（二）量子通信与量子计算

量子技术的迅猛发展，在给传统密码体系造成严重威胁的同时，也给信息安全开辟了新的解决途径。量子计算的并行计算能力给现有的公钥加密算法带来了潜在破解威胁，因此电力系统要加快向后量子密码转移的步伐，研发抗量子攻击的新型加密算法来保证电力数据长期的机密性。量子密钥分发技术使用的是量子力学的测不准原理和不可克隆定理，可以得到无条件安全的密钥分发。

在电力骨干通信网上建设量子保密通信网络，可以给调度数据网、营销业务网提供非常高安全级别的加密服务。在光纤网络中叠加量子信道来生成和即时更新密钥，可以保证每一个通信会话都使用不同的随机密钥。量子通信技术已经尝试在部分电力现货交易、配自动化方面进行运行。

1. 使用量子随机数发生器来产生高质量的随机数，可以大大提升加密系统中

的熵源质量，从而有效地避免由于伪随机数的规律被预测所造成的安全漏洞。

2. 量子直接通信等前沿技术的研究，可能会实现信息直接以量子态进行传输，彻底颠覆目前的通信加密方式，给电网重要指令的传输打造一个坚不可摧的量子防护体系。

（三）AI 赋能的安全防御体系

引入了人工智能技术之后，网络安全防御就从被动的应对变成了主动防御的新阶段。传统的基于特征库的入侵检测系统很难应对未知威胁、高级持续性威胁，基于人工智能的安全分析平台可以对海量流量数据、日志进行分析来构建基线模型，从而进一步认识正常业务行为的特点。任何偏离基线的异常流量、隐蔽的信道通信、异常数据外传等行为都会被人工智能算法及时发现并标记出来，从而暴露出隐藏在网络深处的未知攻击。

利用人工智能加以改进的自动化响应编排系统，可以很好地将零散的安全工具整合成规范化的应急响应脚本。当人工智能发觉勒索病毒流传或者僵尸网络活动的时候，系统就会立刻启动阻断策略，把被感染的主机隔离起来，修正漏洞，把由于攻击引发的损失控制在尽可能小的范围内。利用生成对抗网络，防御系统能自动生成对抗样本做模拟攻击演练，不断找出并加固自身的安全漏洞。这种以攻代防、攻防一体的发展方式，会使电力通信网的安全防御体系具有自我学习、自我进化的功能，可以适应不断变化的网络攻击方式，保证智能电网的正常安全稳定运行。

第二节 标准化进程

一、国际标准化动态

（一）IEC/IEEE 在智能电网通信标准的进展

国际电工委员会、电气电子工程师学会是电力和通信领域的两个权威机构，对于智能电网通信标准的制定采取了相互融合、相互补充的方式。国际电工委员会标准 IEC 61850，变电站自动化系统的核心协议，正逐步从传统的变电站物理边界中脱离出来，向配电网、分布式能源、电动汽车充电设施等方向延伸。这并不是简单的复制已有协议，而是重构底层的数据模型，再做轻量级适配。由于配电网设备的资源有限，所以国际电工委员会相关工作组正在努力推动受限应用协

议映射方法，来减轻协议栈给计算资源带来的负担。为了满足广域测量和控制系统对时间同步严格的要求，国际电工委员会、电气电子工程师学会正在联合攻关将 IEEE 1588 精确时间协议同 IEC 61850 采样值传输紧密结合起来，在复杂的网络环境中也可以实现微秒级的时间同步精度。

电气电子工程师学会 802 工作组正在制定电力系统中时间敏感网络技术的标准。时间敏感网络是在标准以太网的基础上增加了时间感知整形、帧抢占等机制，为电力业务提供确定性低时延保障。目前已经制定出关于电力系统专用配置模型和流量调度策略的草案，可以有效解决传统以太网面对突发性保护业务时出现的时延抖动问题。由此可见，电力通信网正从尽力而为的数据传输模式，向确定性服务质量保证模式演进，为跨广域网的差动保护等关键业务提供了坚实的标准化基础。各个设备厂商按照最新的标准草案来制造原型机，在很多跨国的互操作性测试活动中，对不同厂商的设备在同一时间敏感网络环境下能否共同存在、协同工作进行了测试。

（二）3GPP 等组织在垂直行业标准的推进

第三代合作伙伴计划是全球移动通信标准制定机构，对 5G 和垂直行业融合方面做了很多工作，电力行业是最重要的垂直行业之一，其标准化进程受到很大影响。随着 Release 16、Release 17、Release 18 版本的不断冻结和持续发展，第三代合作伙伴计划标准体系在高可靠低时延通信、非公共网络、授时服务等各方面规定越来越完善。这些标准特性使蜂窝移动通信网络第一次从逻辑上、物理上具备了替代或者补充光纤接入的可能。尤其在配用电接入网环境下，根据最新的 5G 切片技术来对电力业务进行端到端的资源隔离和业务质量保证，很好地解决了传统无线公网存在安全性和可靠性方面的先天缺陷。

1. 非公共网络架构：就网络架构而言，第三代合作伙伴计划标准给非公共网络布置方式做了规定，允许电力公司使用运营商提供的频谱资源搭建独立的网络核心部分，从而掌控网络的数据。这一标准特性很大程度上打消了电力企业对于数据外泄的顾虑，使得 5G 专网在电力生产控制大区开始试点应用。

2. RedCap 技术：RedCap 的提出，为电力物联网的大规模部署提供了一种高性价比的终端方案。该技术裁剪了冗余的带宽和天线数量，大幅降低了 5G 模組的成本和功耗，同时保留了切片、低时延等关键能力，精准匹配了智能电表、配电自动化终端等大量连接场景的需求。

（三）开源组织与标准化

在数字化转型的浪潮之下，开源组织成了电力通信标准落地、技术创新的主要力量，冲破了过去标准制订与产品研制之间漫长的周期壁垒。Linux 基金会能源项目等开源社区集全世界开发者智慧于一身，正在推进通用硬件 + 开源软件的电力通信基础设施建造。这样的“代码就是标准”，使得技术规范一出生就有参考的实现，大大降低厂商研发门槛和互操作性测试成本。开源社区公开的虚拟化变电站架构，把保护控制功能软件化地部署到通用服务器上，实现了硬件和软件的彻底解耦，这样的架构正逐渐成为事实上的行业标准。

随着边缘计算在电力系统中的逐步推广，开源组织在边缘侧的标准话语权越来越大。EdgeX Foundry 等开源项目正在定义边缘网关的通用架构以及南向设备接入标准。电力场景中这就意味着不同的厂商传感器、智能终端可以使用统一的驱动接口接入边缘节点，不需要为每一个设备单独开发私有协议转换器。标准化边缘计算框架一方面简化现场运维，另一方面促进边缘智能算法跨平台迁移。电力企业可以依靠统一的微服务接口，将故障识别、负荷预测等算法容器化后部署到各种边缘设备上，从而实现软件定义电力终端的目标。

与此同时开源组织也在积极推进通信协议栈的开源。以前的闭环昂贵的 IEC 61850、DNP3 等协议栈现在已经有高质量的开源版本可以供选择。开源协议栈被社区大量使用并不断修补，性能和可靠性已经可以和商业版本媲美。电力通信设备开发正从以前的重复造轮子向组装式创新转变。标准化组织同开源社区的交流愈发频繁，不少标准提案直接取自开源项目中最好的实践经验，新出台的标准很快就在开源代码里得到应用。这样快速的双向反馈，明显加快了电力通信技术更新的速度，也提高了标准化进程实际效能。

二、国内标准化重点方向

国内电力通信标准化工作依靠新型电力系统创建和“双碳”目的战略需求，努力创建自主可控、安全高效的标准化体系。在新能源高比例接入、源网荷储协同互动的新形势下，国内的标准化单位正在加紧填补关键技术领域标准空白，推动电力通信网向着全感知、全连接、全智能前进。国内标准化工作重点方向如下表所示：

国内电力通信标准化重点方向

重点方向	核心目标	关键技术 / 标准	覆盖领域
新型电力系统通信标准体系建设	适应源荷边界模糊、系统惯量下降、控制对象海量化等特征，支持高频交互、广域协同控制。	超长距离光传输、全光交换（灵活栅格）、天地一体化（卫星通信融合接口）、宽带电力线载波、微功率无线、工业以太网、双模通信模块、网络切片、服务质量映射。	骨干网、接入网、业务层（虚拟电厂、源网荷储）
电力物联网与数字孪生标准	统一物联模型，规范感知接入，促进边缘智能，提升数据采集质量和价值挖掘能力。	统一描述语言设备信息模型、微功率无线传感协议、边缘网关通用架构、南向设备接入、电力通信网数字孪生体建模、实时状态数据映射。	感知层、边缘层、平台层（数字孪生）
电力通信网络安全标准	应对日益严峻的网络安全形势，构建自主可控、内生安全的安全防护体系。	量子密钥分发设备接口、密钥管理系统架构、量子加密业务承载流程、基于零信任理念的接入认证（国密算法、终端安全基线、动态授权策略）、数据分类分级、加密脱敏、审计、数据水印、安全多方计算。	物理层、网络层、应用层、数据层（全生命周期安全）

（一）新型电力系统通信标准体系建设

新型电力系统存在源荷边界模糊、系统惯量降低、控制对象海量化等特性，给通信系统提出前所未有的覆盖范围、实时性能和调度灵活性的要求。为此，国内标准化工作会集中力量创建起契合高频次交互、广域协同控制的通信标准体系。骨干网层面，对于超长距离光传输、大容量数据调度需求，相关标准会针对光传送网技术发展走向做出规范，就全光交换的灵活栅格技术指标予以确定，从而支撑起未来数据中心同电力调度中心之间海量数据的实时互备。同时正在制定天地一体化电力通信网络架构标准，对卫星链路和地面网络的融合接口及业务切换过程进行规定。

接入网侧针对大量的分布式光伏、电动汽车等分散资源接入，标准化重点就是制定异构融合网络协同控制规范。正在推进的标准有宽带电力线载波、微功率无线、工业以太网等通信技术的互联互通机制。这些标准意在拆除各种通信制式之间的壁垒，从而可以对不同网络的资源实行统一的抽象和调度。针对低压台区的复杂通信环境，有关标准中对于双模通信模块的自适应切换逻辑、路由算法作

出规定,保证某个信道不通时可以自动切换到备用信道,保证业务数据连续传输。采用统一的接入网管理信息模型,上层管理系统就可以无差别地对下层的各种通信设备实施监控和配置,给配用电业务的精细化管理赋予标准化的网络底座。

新型电力系统通信标准体系尤其要重视业务需求和网络能力精确匹配。对于虚拟电厂、源网荷储一体化这些新的业务形态,标准化组织正在开展通信需求的分级分类研究,力求制定出不同的服务质量映射标准。从而给不同的业务流设置不同的带宽、时延、抖动、丢包率阈值,并将它们映射到网络切片或逻辑通道上,以保证在网络拥塞的情况下核心控制业务不受影响。该标准化服务质量控制体系,是电网由刚性调度到柔性协调的支撑保障,使得通信网络可以同电力网一样实现资源精确定位、管理分配。

（二）电力物联网与数字孪生标准

电力物联网是物理电网与数字世界之间的神经末梢,它的标准化程度决定着数据采集质量的好坏和价值挖掘的深浅。目前我国电力物联网的标准化工作主要是围绕统一物联模型、规范感知接入、推进边缘智能展开的。在物联模型上大力推行统一描述语言的设备信息模型标准。本标准规定各个感知终端在出厂时应具有自我描述能力,能向主站系统报告自己的属性、功能和状态信息,从而达到设备即插即用的目的。彻底改变以前靠人工配置点表低效的方式,有效解决了大量感知设备接入和自动运维的难题。

1. 感知接入技术:对于感知接入技术而言,各微功率无线传感技术的物理层、链路层标准正在不断完善,逐渐克服频段干扰、互操作性差等长久以来的难题。通过定义统一的空中接口协议、组网策略来创建密集型可靠的感知网络,并使得不同的传感器设备协同运行。

2. 数字孪生应用:正在建立电力通信网数字孪生体的创建和交互标准。该标准对通信设备、链路、拓扑等物理实体的数字化建模方法进行了规定,并对实时状态数据的映射规则做了说明。按此标准可创建和物理通信网实时同步的数字镜像,用以开展网络仿真、故障推演、优化决策。

（三）电力通信网络安全标准

网络安全情况越来越严重,电力通信网络安全标准就成了国家安全标准体系里的关键部分。国内标准化工作以“安全分区、网络专用、横向隔离、纵向认证”为原则,并在此基础上针对新技术的应用进行深化和拓展。我国正在制订量子保

密通信在电力行业应用的一系列标准，其中包含量子密钥分发设备接口标准、密钥管理系统架构标准、量子加密业务承载流程标准。在关键骨干链路上部署符合标准的量子加密设备，会给电力调度数据传输赋予无条件安全保障，从而固若金汤地守卫好电网安全的最后一道防线。

对于大量异构终端接入造成攻击面扩大问题，标准化组织正在按照零信任思想推进接入认证标准。本标准不再默认信任内网中的任何设备，要求每次访问请求都要进行严格的身份验证和环境感知。具体的规范有基于国密算法的轻量级认证协议、终端安全基线检查标准、动态授权策略。不管终端处在怎样的网络环境之中，都要通过诸多方面的安全检测之后才会得到访问的许可，而且这种许可还会依据环境的改变而做出相应的调整。该标准的推行可以阻止仿冒终端的接入以及横向渗透攻击，保证电力物联网接入的安全。

数据安全标准也属于目前的重点建设内容。正在制定电力大数据从采集、传输、存储、处理、共享交换整个生命周期安全防护的细化的分类分级标准和防护规范。各类敏感数据的加密强度、脱敏规则、审计要求都会被明文规定，用户隐私数据、电网运行关键数据等都会被纳入其中。尤其在数据跨域交互的情况下，相关标准对于数据水印、安全多方计算等隐私计算技术的应用接口和性能指标做出规定，以达到“数据可用不可见”的目的，在保证数据安全的前提下充分释放电力大数据要素的价值。通过建立这样的一个完整的网络安全标准体系，国内电力通信网就具备了对抗高级持续性威胁的内生安全能力。

第三节 产业化前景

一、电力通信设备市场

（一）芯片、模块等核心器件国产化

高端光通信芯片、高性能路由交换芯片、工业级无线通信模块一直依赖进口，一定程度上限制了电力通信产业安全可控水平的发展。在复杂的国际局势和供应链安全问题之下，核心器件的国产化替代已经不是单纯从成本的角度去考虑了，而是关系到国家能源安全的战略必选项。国内芯片企业加大研发力度，在高速率模数转换器、跨阻放大器、大容量交换芯片设计制造上解决难题，希望能在重要

指标上达到并跑，最终达到领跑。

随着制造工艺的日趋完善，设计水平的不断提高，国产电力专用通信芯片的性能稳定性也被证明是可靠的。由于电力工业现场电磁环境复杂多变，温差大，本土企业针对芯片的抗干扰性和宽温特性做了专门的优化，推出许多符合工业级标准的芯片。这些国产化器件正由原来的边缘接入设备向核心汇聚设备发展，在配电自动化终端、智能电表通信模块等设备上占据了很大的市场份额。

产业链上下游配合的更加紧密，加快了国产器件更新换代的速度。电网企业制定的更加严格的入网检测标准、提高国产化率，使得设备商在选择核心元器件的时候更倾向于国产，留出给国产芯片试错和改善的空间。这种市场牵引机制一方面可以降低整机厂商的采购成本，另一方面也会带动国内半导体封测、晶圆制造等各个相关环节的发展，从而形成一条逐渐完善的自主可控供应链条，为电力通信设备市场稳健发展奠定坚实基础。

（二）电力专网通信设备市场格局

电力专网通信设备市场向来就具备高门槛、强监管的特点，大部分的市场份额被一些有着深厚行业积淀、产品线完备的头部厂商所占据。这些传统的强势企业由于多年的积累，在光同步数字体系、光传送网、分组传送网等方面有着深厚的技术积淀，所以占据了骨干网和核心网设备的大部分市场。它们凭借持续的技术更新，把超高速率、超大容量的光传输设备安置于特高压线路和省际互联通道之上，形成起电力通信的大动脉，牢牢占据着难以撼动的市场地位。

但是随着配用电侧通信需求的爆发，市场格局也开始发生变化。传统的骨干网设备市场已经饱和，增长动力正在从网络中心转向网络边缘。给那些专注于工业以太网交换机、工业无线路由器、电力载波通信设备的中小型企业提供突围的机会。新兴力量一般能够在细分领域具有独特的敏捷优势，能迅速响应地市级、县级乃至末端台区的定制化通信需求，依靠提供高性价比的接入层设备来占领有利市场份额，造成整个市场出现“骨干稳固、边缘活跃”的多元化竞争局面。

（三）新兴技术驱动的市场增长点

新一代信息通信技术融合给电力通信设备市场带去了强劲的增长动力。下表给出了这些新出现的技术以及它们在电力通信里所起的作用。

新兴技术在电力通信中的应用

技术	主要特点	电力应用场景
5G (第五代移动通信技术)	低时延、大连接、网络切片	差动保护、配网自动化、覆盖盲区补充
量子通信技术	绝对安全性、密钥分发	关键控制指令、调度数据加密、高安全等级通信
工业物联网	低功耗、自组网、海量连接	输电线路状态感知、变电站环境监测、配电设备参数采集

第五代移动通信技术具备低时延、大连接特性，电力垂直行业里大显身手。支持网络切片技术的 5G 工业网关、CPE 终端、嵌入式模组需求量大增，成了设备市场的新宠。可以满足差动保护、配网自动化等业务对于通信性能的高要求，很好地解决了光纤覆盖不到的区域通信空白问题，促进无线公网与电力专网相互融合的应用发展。

量子通信技术的逐步商用化，给高安全等级的通信设备开拓了一条新赛道。因为电网控制指令和调度数据属于敏感信息，所以选择在重要的节点上使用量子密钥分发加密通信设备做试点部署。不但推动量子网关、量子交换机等硬件的研发制造，还促进了传统光通信设备同量子加密模块的结合发展。虽然目前规模还很小，但是量子通信凭借其理论上的绝对安全性，被认为是对未来电力核心保密通信重要的增长极。

工业物联网技术的发展，给大量的物联传感终端提出了通信要求。为了实现输电线路状态、变电站环境、配电设备运行参数的全方位感知，各种集成了微功率无线通信功能的智能传感器、汇聚节点设备大量涌现。这些设备一般具有低功耗、自组网、免维护等特点，数量众多且更新换代快，成为电力通信设备市场中长尾效应最明显的一个增长板块，极大地增加了设备种类和市场容量。

二、电力通信服务市场

（一）网络规划、设计与集成服务

现代电力通信网是由光纤、微波、载波、无线专网、公网等多种手段组成的异构融合网络，其规划设计的复杂性是前所未有的。专业的规划设计服务已经从简单的路线勘察、容量计算发展到业务流量模型分析、网络生存性评价、全生命周期投资收益分析等更高层次。设计单位要采用先进的仿真软件、数字孪生技术，

建立虚拟网络模型，对不同的技术制式、不同厂家的设备的兼容性进行预演，保证网络架构的科学性、前瞻性。

系统集成服务对于电网的数字化转型来说是起“粘合剂”作用的。存量网络和新建网络共存、多代技术标准混用的时候，集成商会给出由方案咨询、设备挑选、安装调试、业务割接的一条龙服务。尤其是在调度数据网搬迁、核心路由器升级等高风险操作的时候，高水平集成服务最大程度上减少了电网生产业务受影响程度。跨专业集成能力，也就是通信系统同自动化系统、继电保护系统的深入联调，成了评价服务商核心竞争力的标尺。

能源互联网向用户端延伸，配用电通信网规划集成需求也变得碎片化、定制化。各个地区的地理环境、负荷特性、配电网架构存在很大的差别，因此服务商要具有因地制宜的定制化设计能力。如城市核心区主要规划光纤复合低压电缆入户方案，偏远山区主要规划中压载波或无线专网覆盖方案。这些琐碎的服务需求使规划集成环节的附加值大幅增加，推动行业朝知识密集型方向发展。

（二）运维外包与增值服务

电力通信网运维工作出现设备数量激增与专业人员短缺的结构性矛盾。为了降低运维成本、提高运维效益，电网企业将非核心、重复性的运维工作剥离出来，外包给专业的运维公司。这就产生了大量的第三方运维公司，它们从事着从线路巡检、机房环境维护到末端设备抢修等各种基础的工作。专业的运维人员有专业的检测仪器、抢修车辆，并有 7×24 小时保障。

在基础运维之上，依托大数据的智能运维增值服务出现。服务商采用探针设备对网络流量、光功率、误码率等实时数据加以采集，再经由人工智能算法进行关联分析，给出故障预估、健康度评定以及网络改善提议。把被动应对转变为主动防范的高级服务，可发现隐患并防止重大通信事故的发生。

高端技术咨询、培训服务等属于服务市场。伴随着 SDN、NFV、IPv6+ 等新技术不断出现，电网内部技术人员面临很大的知识更新压力。专业的培训机构、设备厂商高级服务部门提供定制化技术认证培训、专家驻场指导、疑难故障会诊服务，提升客户的技术掌控能力。该类知识转移性质的服务具有较高的客户黏性，可以成为建立长期合作关系的纽带。

（三）数据服务与平台运营

电力通信网不但是信息传输的通道，同时也是大量的电力大数据的承载平台。

随着数据被认定为核心生产要素，以通信数据挖掘、清洗、分析、运营服务为内容的新兴产业正在迅猛发展。数据服务商构建起统一的通信管理平台，把散布在网络各个角落的网管系统里的告警数据，资源数据以及性能数据收集起来并加以治理，进而冲破信息孤岛，给电网企业高层管理者给予可视化的决策支撑，像给出准确的投资指引，资产全生命周期视图之类。

通信网络能力开放运营属于一种新的商业模式探索。依靠覆盖面广的电力杆塔资源、光纤网络资源，电网企业可以开展通信基础设施共享运营服务。向电信运营商出租输电铁塔挂载基站，或者提供光纤芯资源租赁服务。专业平台经营方要承担动态资源管理、计费结算、客户服务等任务，把电力通信资产从沉睡中唤醒，使它变成持续增长的现金流，最大化地发挥电力通信资产的价值。

综合能源服务的通信平台运营前景十分广阔。微电网、虚拟电厂等新兴业态中，通信平台要完成源、网、荷、储各个环节信息的实时交互。运营服务商给能源主体提供云架构下通信中间件服务，使各类能源主体快速接入电网调度系统、交易平台，从而实现能量流、信息流的协调优化。平台化运营服务模式具有明显的边际成本递减效果，形成规模以后就会出现强大的网络效应和经济收益。

三、产业生态构建

（一）产学研用协同创新

高校是基础理论创新的发源地，新型光通信编码机制、太赫兹通信、水下通信等前沿研究领域都由高校来担当探索者的角色。高校若想借助建立联合实验室或者课题组等方式，将最新颖的科研成果同行业需求有效衔接起来，进而给电力通信技术的持续健康发展赋予永不枯竭的智力支撑，那么就完全可以在实际操作过程中做到。科研院所起桥梁作用，把学术界的理论模型转化为工程可用的技术原型，攻克技术落地时遇到的工程化难题，设备电磁兼容设计、协议标准化制定之类的问题。

设备制造企业是创新成果产业化的主要力量。根据科研院提供的技术标准和原型，投入大量研发资金开展产品化开发、生产工艺改进，把技术转化为成熟可靠的商用产品。电网企业作为最终用户，向新技术产品开放试点工程和应用场景，给新产品提供实战演练的场所。运行数据和改进意见的产生直接反馈给研发部门、制造部门，从而形成一个以需求牵引、技术研发、产品制造、应用验证、反馈迭

代为闭环的创新生态系统。

该种协作创新方式有效地解决了技术研究同市场需求的相脱离的问题。产学研用深度融合的强大爆发力，在攻克特高压配套通信工程、大规模配电物联网这些世界级难题的时候得到了充分的体现。多方联合攻关可以缩短研发周期，也可以培养出很多通信技术和电力业务相结合的复合型人才，为产业的持续发展储备了核心竞争力。

（二）产业链上下游协同发展

1. 上游原材料与元器件供应的稳定性保障

产业链上游有光纤预制棒、有色金属、特种工程塑料、各种电子元器件供应商。基础材料的质量及供应是否稳定，直接决定中游设备的水平以及能否按时交货。中游制造企业同上游供应商形成长期的战略合作关系，实行供应链信息共享制度，可以及时掌握到原材料价格和生产能力的最新情况，进而改善库存控制，制订出更加有效的生产计划。同时上游企业根据中游提出的高性能要求不断改进材料配方、加工工艺，一起提高整个产业链制造水平。

2. 中游设备制造与软件开发的标准统一

中游环节主要是通信设备制造商、光缆生产商、网管软件开发商。这个环节上标准化的协同就显得十分重要。行业协会以及标准化组织协调各个厂商，共同制定互联互通的标准以及接口规范，有效防止私有协议造成的市场割裂。硬件厂商与软件开发商互相配合，使得底层硬件性能和上层软件功能可以衔接起来，从而实现软硬件解耦、网络功能虚拟化技术的应用，使整个产业链更具有弹性，反应速度更快。

3. 下游应用场景拓展与需求反馈机制

下游主要是电网公司、发电企业、新兴的综合能源服务公司。下游需求不断变化，成了产业链升级的根本动力。当上下游建立起需求对接的常态机制之后，下游用户对新型业务场景下存在的通信痛点能更有效地传递给上中游。例如，远距离大带宽的海上风电运维难题提出后，很快传导到中游设备商和上游光缆商，推动海底复合光缆和长距离微波设备的协同研发与应用，最终实现产业链对市场需求精准响应。

（三）开放合作与生态共赢

开放是产业繁荣的前提。电力通信行业正在由原来的封闭系统向更加开放的

生态系统转变。技术上开源社区、参与国际标准的制定，使用通用的 IT 技术和互联网架构。采用 SDN、NFV 等开放架构以后，电力通信网可以兼容各个厂商的设备，也可以灵活地加载第三方开发的网络应用程序，比如流量清洗 APP、智能路由优化插件等。该种应用商店式的生态模式使得创新门槛大幅降低，从而引起众多中小开发者对电力通信功能的开发和完善。

跨界合作已经成为生态共赢的一种新的常态。电力行业和电信运营商、互联网企业之间越来越模糊。电信运营商共享基站站址、光缆管道可以节约大量的基础设施投资，也可以达到社会资源集约利用的目的。同互联网企业达成合作，把云计算、大数据分析等领域的前沿理念和算法模型引入进来，这样就使得电力通信网的智能化运作水平得以提升。跨行业资源互补、能力叠加产生的生态价值远远大于简单的相加。

国际化合作属于生态构建的重要部分。依靠“一带一路”，中国的电力通信标准和技术装备正在走向世界。通过参加国际电工委员会、国际电信联盟等国际组织的活动，中国积极提出自己的方案，推动电力通信标准在国际上互相承认。与海外电力企业开展项目合作，输出了产品和服务的同时，也输出了成熟的建设运营经验，在全世界范围内形成了互利共赢的电力通信产业朋友圈，极大拓宽了产业发展的地理边界和市场纵深。

第四节 挑战与对策

一、技术挑战

（一）极端环境下的通信可靠性

在电力系统所涉及的广阔地域内，通信基础设施一直面临着严峻的自然环境考验，无论是高海拔的严寒地带还是沿海地区的台风多发区，极端天气都会给通信链路的稳定运行造成严重威胁。尤其在特高压输电线路跨越无人区或者地形复杂的山区的时候，常规的光纤敷设和维护十分困难，而无线通信方式又很容易受到地形遮挡和电磁干扰的影响。在深山峡谷或者地下电缆隧道这类的信号盲区当中，传统无线信号因为衰减严重而造成数据传输断续或者误码率飙升，无法达到继电保护等业务所要求的高可靠性。

遭遇地震、洪涝、冰灾等大规模自然灾害的时候，电力通信杆塔和机房会首当其冲，极易造成杆塔倒塌、线路中断、设备损坏或者水浸等问题，造成通信孤岛，严重影响应急指挥和抢修调度工作的进行。尽管已经使用了卫星通信等应急手段，但是在恶劣的气象条件下，卫星信号连通率、带宽仍然受到很大影响，不能完全取代地面骨干网。随着电力电子设备的大规模应用，电网电磁环境日趋复杂，高压强磁场对通信设备电磁兼容性的要求也越来越高，在强电磁干扰下如何保证微弱通信信号的完整性、准确性已经成为保证通信可靠性的关键技术难题。

（二）海量异构终端的接入与管理

新型电力系统终端设备爆发式增长，除了智能电表、变电站监控终端等传统设备外，光伏逆变器、充电桩、智能断路器和各种微型环境传感器也大量出现。这些终端设备的数量非常庞大，预计将来会达到几十亿之多，而且种类繁多，各个厂商生产的设备型号也千差万别，使用的通信接口和协议标准也各不相同。现有的通信网络结构很难承担这么多并发连接请求，容易引起信令风暴，造成网络拥塞甚至瘫痪。

1. 终端接入标准化程度低，这是目前面临的主要问题。由于缺少统一的物联网接入标准，各个厂商的设备大多使用各自的私有协议或者非标数据格式，造成系统之间存在着大量的信息孤岛，数据互联互通非常困难。既大幅增加了网络适配、集成费用，又严重阻碍了数据价值开发、利用。

2. 异构终端管理复杂度呈指数级增长：大量分散的终端设备用传统的集中式管理已经力不从心，不能实现对海量终端全生命周期状态的监测和远程配置。对于配用电侧来说，大量的低功耗、低成本的哑终端几乎没有完善的网管功能，当出现故障或者掉线时，运维人员很难快速找到问题所在，这会对业务感知的及时性以及准确性产生影响。

（三）网络复杂性与运维难度剧增

伴随着软件定义网络、网络功能虚拟化、边缘计算等新技术的广泛使用，电力通信网架构也从原来的刚性管道向灵活智能的云网融合架构转变。这种结构的转变，在提高资源调度灵活度的同时，也使网络的逻辑变得较为繁杂。网络控制平面与数据平面的分立使故障定位不能只是物理链路的排查，还需要分析复杂的逻辑映射关系和流表策略，这就对运维人员的技术水平和所需工具提出了更高的要求。

电力通信网所承载的业务种类越来越多，生产控制、企业管理、视频监控等各种性质不同的业务流互相交织在一起，各类业务对于带宽、时延、抖动、丢包率的要求也不尽相同。在一个物理网络上承载多业务切片并保证服务质量，对流量工程和拥塞控制提出了很高的精细化要求。目前运维体系仍然主要依靠人工经验以及静态配置，没有网络流量的实时动态感知和智能化调优的能力。当网络出现突发拥塞或者故障的时候，不能在秒级的时间内完成业务的迂回和恢复，造成重要生产业务中断或受损。同时存在多层级、多制式的网络（光传输网、数据网、无线专网等），全网统一监控、协同运维难度大，跨专业故障定界、协同处置效率低。

二、安全挑战

（一）攻击手段的智能化与规模化

目前能源行业的网络攻击已经不是个人零星的攻击行为，而是有组织、有预谋的国家级对抗或者黑产集团的攻击行为。攻击者利用人工智能及自动化工具进行网络扫描漏洞、生成变种恶意代码的工作，在网络上实现快速入侵，使得攻击频率以及强度大为提高。分布式拒绝服务攻击的规模创历史之最，攻击者利用大量的僵尸物联网设备，对电力网站或者关键业务系统发起流量洪峰攻击，目的是耗尽网络带宽和计算资源，造成服务停摆。

最险恶的就是 APT 攻击，高级持续性威胁。APT 攻击者常潜伏很长一段时间，以钓鱼邮件、水坑攻击等方式入侵内部网后，利用零日漏洞横向移动并提升权限。针对工业控制协议的固有缺陷，精心构造畸形报文或者恶意指令，直接攻击变电站监控系统或者发电厂控制系统。该类攻击行为具有很强的隐蔽性，传统的基于特征匹配的防火墙和入侵检测系统很难进行有效的识别。攻击成功会引发大面积停电、设备损坏等严重后果。篡改远程终端单元的测控数据，导致调度系统作出错误的控制决定，会造成电网频率震荡或者电压崩溃，对国家安全和社会稳定造成极大的威胁。

（二）数据安全和隐私保护压力

电力大数据属于国家重要的战略资源，具有巨大的经济和社会价值，也成了黑客窃取和倒卖的重点对象。伴随着电力市场化交易、虚拟电厂等新业务的推行，电网企业和发电企业、售电公司、用户、第三方服务商之间的数据交互也越来越

频繁。数据流转环节变多，攻击面也跟着变大，数据在采集、传输、存储、处理、共享的任何一个环节都存在泄露、篡改、滥用的风险。

用户侧的隐私数据保护处于非常大的压力之下。智能电表高速采集来的用电数据可以反映用户家庭生活情况，工厂生产情况等敏感信息。数据传输过程中没有采用高强度的加密方式，云端存储时权限管理不到位，隐私数据很容易被不法分子截取并恶意使用。同时缺少完善的数据分类分级和脱敏机制，容易造成重要敏感数据违规扩散。随着越来越严格的数据安全法律法规的监管要求，怎样在保证数据安全和隐私的基础上，充分发挥数据要素的价值，实现数据可信共享和流通，已经成为电力通信网亟待解决的关键问题。

（三）供应链安全风险

电力通信网的建立要依靠一个极其复杂的全球供应链系统，它包括芯片、操作系统、数据库、应用软件、硬件设备等各方面的内容。供应链上任何一个环节的安全漏洞，都可以被攻击者所利用，成为植入后门、逻辑炸弹的破口。近几年来，供应链上游的开发商、集成商或者服务商不断遭受攻击，攻击者通过污染软件更新包、预装硬件后门、利用开源组件漏洞等手段，把恶意代码植入到电力通信设备当中，从而达到“一点突破，全网沦陷”的效果。

国外的核心技术产品依赖，仍然是造成供应链安全问题最主要的因素。国产化替代速度变快，在一些高端光通信芯片、高性能路由交换芯片以及底层操作系统方面，还存在着被别人控制的情况。国外产品可能存在未公开的漏洞或者后门，一旦地缘政治冲突出现，就会陷入技术封锁或者远程断供的困境。开源软件在电力系统中的应用越来越广泛，也带来了新的安全问题。如果没有对开源代码进行严格的审查与维护，大量的已知漏洞不能得到及时的修复，就会给攻击者提供可乘之机。对供应链全生命周期的安全管控还没有形成严密闭环的风险防控体系，即供应商准入、产品测试验证、在网设备代码审计等全过程缺少有效的风险防控措施。

三、管理与人才挑战

（一）跨学科复合型人才短缺

新型电力系统形成以后，通信人员要掌握光传输、数据网络、无线通信这些传统通信技术的知识与技能，还要学会电力系统一次设备原理、继电保护逻辑、

调度自动化流程,以及人工智能、大数据分析、云计算这些数字技术的应用。目前的教育培训体系重学科知识的传授而轻视交叉学科知识的培养,造成通信专业人员对电网业务的了解不深,无法主动发现业务需求,也很难给出相适应的解决方案;电网运行人员对于通信网络的特性及瓶颈认识不够,业务规划时忽略了通信层的支撑能力。

高端领军人才、实战型攻防人才更是凤毛麟角。网络安全对抗愈发激烈的时候,高水平的渗透测试、威胁情报分析以及应急响应的红队专家短缺,企业面对高级别的网络攻击就会陷入被动挨打的状态。同时伴随着网络架构软件化、智能化的发展趋势,对掌握编程、建模、运维自动化技术人才的需求越来越多。现有的运维队伍技能结构以硬件安装调试、简单故障处理为主,不能满足未来代码定义网络运维的需求。人才培养周期的滞后性同技术更新的加速性之间的矛盾,造成的人才短缺问题短期内无法得到根本解决。

（二）传统管理模式与新技术发展的冲突

电力企业长期以来细致的专业分工、严格的管理模式在保障电网安全稳定运行方面发挥了重要作用,但是面对数字化转型所需要的敏捷性、融合性,却存在不适应的问题。通信专业与电网调度、运检、营销等业务部门之间存在部门墙,跨部门协调工作大多依靠行政命令或者线下沟通,流程繁杂、效率低下。配电自动化建设中通信终端的选型、安装、调试等工作由不同的部门分段完成,缺少统筹规划,造成建设周期长、接口不匹配、运维责任不清等问题。

新技术出现以后就打破了传统的物理界限以及责任划分。云网融合导致计算资源和通信资源的深度耦合,传统的将通信网当做单纯的管道来管理的思维方式已经不再适用。算力网络调度需要通信部门与数据中心部门相互配合,但是目前的组织架构把两者割裂开来,造成算力资源无法统一编排、优化配置。数字化项目快速迭代开发模式(开发运维一体化)同电力行业稳健保守的决策流程发生冲突,制约了许多创新技术的快速推广。怎样创建适应数字化生产力的柔性组织架构和协同机制,打破数据壁垒和业务隔阂,成为管理变革的重点。

（三）应对策略与发展建议

对于以上这么多的挑战,要树立系统的观念,把发展的需求和安全的要求统一起来,从技术研发,架构改进,管理革新以及人才培育等诸多方面同时发力。建设技术先进、安全可靠、管理高效的现代电力通信网体系,给新型电力系统提

供全方位支撑和赋能。

1. 加大关键核心技术攻关力度，推进国产化替代。加大对超长距离光传输、确定性网络、低功耗广域物联网、卫星融合通信等方向科研的投入，攻克极端环境下通信保障技术瓶颈。全面推进通信芯片、操作系统、数据库等基础软硬件的国产化替代工程，创建起自主可控的技术生态体系，从根本上消除供应链的安全隐患。

2. 建立全场景网络安全纵深防御体系。采用零信任安全架构，打破内外网之间的信任边界，对所有的访问主体实行持续的身份认证和动态授权。打造全网统一态势感知平台，依靠人工智能技术对未知威胁做到实时监控并智能阻断。强化数据全生命周期的安全防护，采用隐私计算、量子加密等前沿技术来实现敏感数据安全共享和价值释放。

3. 推动网络架构向云网边端协同发展的方向发展。加快软件定义网络、网络功能虚拟化的规模化应用，打造弹性、灵活、智能调度的通信网络底座。统筹规划边缘计算节点，业务数据就近处理，快速响应，减小主干网回传压力。搭建云网编排管理平台，对算力资源和网络资源进行统一规划、统一调度、统一运维。

4. 创新人才的培养机制以及管理办法。深化产教融合，以校企合作形式设立电力通信交叉学科专业，定向培养复合型技术人才。建立红蓝军常态化攻防演练制度，实战化锻炼网络安全队伍。打破部门壁垒，建立跨部门的柔性攻坚小组，以项目为依托，实行一体化运作。建立健全容错纠错体系，宽容失误，包容失败，鼓励技术创新、试验应用，营造勇于创新、宽容失败的开放包容氛围。

5. 完善标准体系及顶层设计。按照国内国外技术发展动态，修订完善电力通信网的技术标准、管理规定等。重点加强物联网终端接入、数据交换格式、网络安全防护等各方面标准化的建设。强化顶层设计引领，制定科学合理的通信网发展规划，使通信网络建设同电网主网架建设同步规划、同步实施、同步投运，实现源网荷储各环节的全面感知和泛在互联。

第五节 未来发展方向

一、构筑全域泛在的电力物联网

（一）实现“万物互联”的电力感知

在新型电力系统架构下，感知的广度和深度直接影响到系统调控的精细化程度。传统电网监测主要集中于变电站和主干线路，而大量的配电变压器、分布式电源、电动汽车充电桩以及用户侧的智能家居设备长期处于监测盲区或弱连接状态。未来的发展方向就是克服这些不足之处，利用低功耗广域网、微功率无线通信和 5G 海量机器类通信技术，把感知的触角伸向电网的“神经末梢”。扩展并不只是简单地增加连接数量，更重要的是设备状态、环境参数、电气量特征等实时精准的采集。在配电网线路安装高密度微型传感器，实时监测导线温度、覆冰厚度及局部放电；在用户侧智能量测系统上除了电能以外还可以测量电压暂降、谐波污染等电能质量指标。

构建起多层次、立体化的感知系统，电力通信网就会给物理设备赋予开口说话的能力。海量的异构终端接入会造成巨大的数据流量，对接入网的并发处理能力提出了前所未有的高要求。因此在未来通信架构中采用更加灵活的频谱共享方式、自适应接入协议，在密集部署的情况下仍然能够保证连接的稳定与低时延。各类传统哑设备加装无源感知标签或者嵌入式通信模块，转变成可以被识别、定位、互动的智能实体，在数字空间中对物理电网的实时运行情况实现完整的呈现。实现全域感知能力，会彻底改变以往电网依靠经验模型进行运维的方式，转而采用依靠实时数据的精确状态检修、全生命周期管理的模式。

（二）支撑能源互联网的“神经网络”

电力物联网并不是简单的终端连接，它还是数据价值挖掘和传递的“神经网络”。就像生物神经系统一样，它也必须具有从末端接收信息、传递到中枢并做初步分析的能力。未来的体系架构当中会布置很多边缘计算节点。因为海量的数据全部回传到云端数据中心，一方面会造成很大的带宽压力，另一方面也会造成无法接受的延迟。因此，把算力下放到通信网络的边缘，也就是变电站、配电房甚至智能电表的地方，成了必然的趋势。在边缘侧部署通信、计算、存储一体化的智能网关，从源头对原始数据进行清洗、聚合、提取特征，只把重要的状态变

化、异常告警上传到主站，从而大大提升系统的响应速度、通信效率。

具体而言，这将通过以下途径实现：

1. 建设“云-边-端”通信算力体系，实现算法模型远程下发、边缘侧即时推理，让故障研判、负荷预测等业务可以毫秒级完成闭环。

2. 采用软件定义广域网技术，对数据传输路径进行优化，按照业务优先级动态分配网络资源，保证控制指令等重要数据流在复杂的网络拓扑结构中能够找到最快、最短的传输路径。

由此带来的架构演变，会使电力通信网不再只是单一的信息传输通道，而发展成为可以加工数据的增值服务平台。随着分布式能源的爆发式增长，电网潮流流向变得越发复杂多变，作为“神经网络”的通信网就必须适应这种双向互动的特性。它要支持成千上万个分布式节点彼此通讯、互相协调控制，让局部微网在并网与孤岛这两种状态间平滑转换，保证能源互联网在各种情况下都有鲁棒性、自愈能力。

二、打造智能敏捷的电力通信网

（一）具备自感知、自决策、自优化能力

把人工智能技术深度嵌入网络管理平面，就是创建智能电力通信网的主要办法。未来的网络管控系统不会只是简单的告警信息展示屏，而会是一个拥有深度学习能力的智能分析中心。通过对历史流量数据、设备日志、网络拓扑状态不断的学习，得到通信网络常态运行基线。当网络出现异常流量波动或者潜在的硬件劣化征兆的时候，人工智能算法就会发出警报，并且在故障出现之前，采用路由迂回、重新分配资源等手段来进行预防性干预。拿光传输网络来说，机器学习能预估信道性能，业务出问题之前察觉光纤损耗异常，然后自动切换到备用路径，让用户感觉不到故障恢复的过程。

智能通信网在突然出现的大规模网络拥塞，或者由于自然灾害造成部分节点瘫痪的情况下，会表现出很强的自决策、自愈能力。系统可以全局视角瞬间算出几千种业务重路由方案，并且自动下发配置指令，不需要人工干预就可以完成网络拓扑的重构。自优化就是体现在动态精细化的网络资源管理上。依据不同时段、不同区域的业务潮汐效应，智能网络可以自动改变带宽分配策略，在闲时减少非关键节点的能耗，在忙时集中资源保证核心业务，从而求得网络能效比的最佳解。

全自闭环运维体系可以大大释放人力资源，使通信网络真正成为一个有自我演进能力的智能生命体。

（二）实现网络即服务

“网络即服务”思想出现以后，电力通信网的服务方式就发生过一次革命。传统的物理一张网承载所有业务的尽力而为的模式，将会转变为按业务需要进行定制化的网络切片服务模式。采用网络功能虚拟化与软件定义网络等手段，把物理通信设施拆分成彼此互不影响、逻辑上独立的虚拟网络切片，每一个切片具备独立的拓扑结构、带宽资源、安全策略和服务质量等级。

主要电力业务对通信切片的需求分析表

业务类型	主要特点	核心通信需求	典型切片策略
继电保护	高实时性、确定性	微秒级时延、抖动极低、绝对安全	硬切片（时隙独占、物理隔离）
精准负荷控制	高实时性、确定性	微秒级时延、抖动极低、绝对安全	硬切片（时隙独占、物理隔离）
视频监控	大带宽、高速数据传输	高吞吐量、低丢包率	软切片（高吞吐量资源）
巡检机器人	大带宽、高速数据传输	高吞吐量、低丢包率	软切片（高吞吐量资源）
计量采集	海量、低频、小数据包	低功耗、大连接、长周期稳定	物联网切片（低功耗、大连接）

从上表可以看出，对于继电保护、精准负荷控制等对时延、抖动十分敏感的生产控制类业务，网络可以为其提供确定性硬切片通道，采用时隙独占、物理隔离的方式实现微秒级的传输时延、绝对安全的传输，不会受到其他业务流量的影响。对于视频监控、巡检机器人这样的大带宽的高速数据传输业务，网络给视频监控、巡检机器人软切片分配高吞吐量的资源，可以满足大量的数据传输需求。对海量低频的计量采集业务来说，网络提供的是低功耗、大连接的物联网切片。灵活的切片服务能力建设使得通信部门可以像点菜一样，给电网各个部门、各种应用场景快速提供相匹配的通信服务，实现网络资源的最大化利用，并使业务响应速度发生质的飞跃。

三、赋能新型电力系统建设

（一）支撑高比例新能源接入

随着风力发电、太阳能等可再生能源在电网中所占的比例越来越高，电网

的转动惯量逐渐变小，抗扰动能力也越来越低。为了能够消纳这些“靠天吃饭”的能源，必须建立起覆盖全部新能源场站和分布式电源的超高速通信监测系统。未来的通信网可以实现高频次的数据采集，实时掌握每一个风机、每一个光伏板的出力情况以及气象环境数据，并将庞大的数据在毫秒级的时间内传送到调度中心或者区域控制节点。根据以上数据，功率预测系统可以结合气象模型，精确预测未来几分钟到几小时的发电功率变化曲线，给电网调度留出足够的时间进行调节。

具体保障措施包括：

1. 构建广覆盖的无线专网和光纤复合网，解决偏远地区新能源场站通信最后一公里接入难题，保证每一个并网节点都在可观测、可控制范围内。

2. 利用 5G 低时延特性支撑分布式新能源集群控制，当局部电网电压或频率出现波动时，通信网可以快速发出调频调压指令，协调成百上千个逆变器同时响应，提供毫秒级的虚拟惯量支撑。

在海上风电等恶劣的环境下，通信网必须有很高的可靠性和抗恶劣环境的能力。利用卫星通信、海底光缆、微波接力等多种方式进行融合组网，就可以形成海上风电场的海陆空一体化综合通信保障系统。即使在台风这样的恶劣天气下，也能完成海上风电场设施的实时监测以及紧急控制工作，可以避免由于通信中断而造成设备和电网被破坏的情况，保证大容量新能源的开发和安全供电。

（二）保障源网荷储协同互动

构建起起源网荷储之间深层次的互动机制，才是破解新能源消纳难题，提高系统灵活性的根本办法。这就要求电力通信网打破发、输、变、配、用的垂直壁垒，构建横向贯通、纵向到底的泛在互联平台。在这种体系下，通信网要承担起支持虚拟电厂等新型调节形式大规模应用的任务。它要实时处理数以百万计的并发控制指令，把用户侧分散的空调负荷、电动汽车电池、分布式储能等海量微小的资源聚合成一个可控的整体，使其像实体电厂一样准确地执行电网的调度命令。

这不仅是技术和市场的互相配合，更是市场信息的互相传递。通信网会变成电力市场交易信息的传递途径，把分时电价，需求响应邀请这些市场信号及时传达到用户端，促使用户依照市场信号来调节用电行为，从而实现削峰填谷的效果。在车网互动场景中，通信网把数以亿计的电动汽车和充电桩联系在一起，靠双向

通信技术，在电网负荷低谷时驱动车辆充电，在高峰期时让车辆反向放电，这样一来，电动汽车就成了一个庞大的移动储能资源库。为了保证通信网络的安全性、高效性，通信网络需要提供端到端的加密通道以及很低的延迟，以保证所有的功率指令都能够被正确执行，所有的交易数据都能够被完整的、可信的记录下来。用一张紧密相连的互动网将电力系统由刚性平衡变成柔性匹配，从而达到能源利用效率最优化。

参考文献

- [1] 张斯扬.电力通信网分组传送技术的可靠性与安全性分析[J].通信电源技术, 2025, 42(2):70-72.
- [2] 赵东升,赵旭升,彭玉清.现代电力通信网的安全防护措施研究[J].中国新通信, 2025, 27(3):4-6,41.
- [3] 黄新武.简析光传输技术在电力通信网中的运用[C]//第13届钢铁行业职业教育培训优秀多媒体课件活动系列研讨会——电力工程与技术创新论文集.2024.
- [4] 马秀珍.光纤传输技术在电力通信网中的应用分析[J].华东科技:学术版, 2017(8):1.
- [5] 杨娟娟.物联网技术在电力通信网中的应用探究[J].中文科技期刊数据库(文摘版)工程技术, 2023(4):105-106.
- [6] 赵续.针对电力通信网的信息安全技术研究[J].艺术与设计(电子版), 2024(2): 0180-0182.
- [7] 陆鹏.自动化技术在现代配电网无线通信架构中的应用[J].通信电源技术, 2025, 42(7):150-152.
- [8] 张强,张进.泛在电力物联网的关键技术与应用前景[J].电力系统装备, 2019(14):2.
- [9] 张利军,徐晨博,范娟娟,等.区域能源互联网多能系统规划决策关键技术及应用[J].现代电力, 2018, 35(4):8.
- [10] 胡珂珏.电力无线通信专网关键技术及主要问题[J].通讯世界, 2018(10):2.
- [11] 项鹏程,刁波澜.电力物联网的关键技术与应用前景分析[J].现代工业经济和信
息化, 2019:36-37.
- [12] 孙维,王兴龙.电力通信网中无线专网技术的实际应用研究[J].数字技术与应用, 2019, 37(8):2.
- [13] 韦晓鹏.光通信传输网排除故障的关键技术分析[J].电子测试, 2018(22):3.
- [14] 范丽娜.电力通信网的风险分析及其控制措施探究[J].建筑工程技术与设计, 2017(2):39-41.

- [15] 梁顺宁.关于电力通信网风险分析与控制[J].建筑工程技术与设计, 2017, 000(025):1787-1787.
- [16] 石伟.配电网规划中智能化技术与通信网络的融合应用分析[J].通信电源技术, 2025, 42(3):173-175.
- [17] 杭泱 顾佳.智能电网环境下变压器在线监测技术研究[J].无线互联科技, 2025, 22(4):69-71.
- [18] 胡春霞.基于大数据的电力通信网的安全防护系统及实现研究[J].中国新通信, 2018, 020(023):141.
- [19] 马亮.配电物联网在电力系统中的应用研究[J].科技资讯, 2025(3):45-46.
- [20] 曹春勇.智能电网时代电力信息通信技术应用研究[J].名城绘, 2017(12):1.
- [21] 邓旭聪,刘星.电力通信网风险管理关键技术分析[J].中国战略新兴产业, 2017(3X):2.
- [22] 师浩瀚.现代通信网络技术的创新和应用[J].网络安全技术与应用, 2017(4): 19-21.