内容简介

《电力信息系统建设技术与实践》是一部系统阐述现代电力企业信息化建设理论、技术架构与工程实施路径的专业著作。本书立足于国家“双碳”战略与新型电力系统建设背景，紧扣电力行业数字化转型的核心需求，全面梳理了从底层通信规约、数据平台构建、数据库选型优化，到自动化运维、安全防护体系等关键环节的技术脉络与实践方法。

全书以“技术—管理—安全”三位一体为逻辑主线，首先深入剖析电力信息系统特有的通信标准体系，包括IEC 60870-5系列远动规约、IEC 61850变电站自动化标准以及我国自主的DL/T 645电能表协议，阐明其在保障实时性、可靠性与互操作性方面的不可替代作用；继而系统论述数据库技术选型策略，针对营销计费、实时监控、历史数据分析等不同业务场景，科学匹配关系型数据库（如Oracle、MySQL）、时序数据库（如InfluxDB）与大数据平台（如Hadoop、Spark），并提供物理模型设计与性能调优的具体方法。在运维层面，本书前瞻性地引入自动化巡检、故障自愈与运维知识图谱等智能运维理念，构建基于“监控—决策—执行”闭环的主动式运维体系，并依托运维大数据平台实现故障预测与根因分析。尤为突出的是，全书将ITIL服务管理框架深度融入电力信息系统全生命周期，从服务战略、设计、转换到运营与持续改进，建立标准化、流程化的IT治理机制。最后，专章论述电力信息系统安全防护体系，强调在融合通用IT技术与电力专用规约的复杂环境中，必须构建覆盖物理、网络、应用与数据的纵深防御体系。本书兼具理论高度与工程实操性，既可作为电力企业信息化规划、建设与运维人员的技术指南，也可供高校能源互联网、智能电网等相关专业师生教学参考，是推动电力行业高质量数字化发展的权威实践读本。

ISBN 978-1-80641-124-5

9 781806 411245

PRICE: £49.00

电力信息系统建设技术与实践
Technology and Practice of Power Information System Construction

彭乃勇 著

SCIENTIFIC Publishing Limited

Technology and Practice of Power Information System Construction

电力信息系统建设技术与实践

彭乃勇 著

SCIENTIFIC Publishing Limited

作者简介

彭乃勇（1979-），男，汉族，安徽明光人，研究生学历，副高级工程师，国网安徽电力有限公司淮北供电公司党委书记、副总经理，从事电力设备、电气工程等相关工作。参与“高压绝缘用 NCS 微晶玻璃材料开发”“高渗透光伏台区储能布置优化与经济投资激励运行研究”等多项安徽省电力有限公司科技项目研究，参与淮北凌云220千伏输变电工程、淮北庙台220千伏输变电工程等多项大型电网基建工程建设，具有丰富的电力系统研究和电网工程建设经验。

Technology and Practice of Power Information System Construction

电力信息系统建设技术与实践

彭乃勇　著

SCIENTIFIC
Publishing Limited

British National Bibliography

Cataloguing-in-Publication(CIP) programme

Title: Technology and Practice of Power Information System Construction

Author: Naiyong Peng, author.

Publisher Details: Cambridge: UK Scientific Publishing, 202602.

Identifier: p25091781100575337

ISBN: 9781806411245

BNB: GBC6076585

Technology and Practice of Power Information System Construction
电力信息系统建设技术与实践

SCIENTIFIC Publishing Limited

Address: Dollman Street, Birmingham, United Kingdom, B7 4RP

Tel: +441223603549

Email: contact@ukscip.com

Format: 170mm×240mm 1/16

Sheets: 16.25

Word Counts: 200,000

UK Scientific Publishing Limited

前言

PREFACE

当前，全球能源格局正经历深刻变革，以新能源为主体的新型电力系统加速构建，电力系统的运行形态、控制逻辑与业务模式发生根本性转变。在此背景下，电力信息系统已从传统的支撑性辅助工具，跃升为保障电网安全稳定、提升资源配置效率、驱动能源服务创新的核心引擎。然而，电力信息系统的建设并非简单地将通用信息技术套用于电力场景，而是需要在深刻理解电力生产运行特殊规律的基础上，实现信息技术与电力专业技术的深度融合与协同创新。

本书正是在这一时代命题下应运而生。我们深知，一个坚强可靠的电力信息系统，必须同时满足三重严苛要求：一是高可靠与高实时性，调度指令、保护动作等关键业务毫秒级响应不容有失；二是异构系统深度集成，从调度主站到变电站、从营销系统到用电采集终端，需打破信息孤岛，实现数据贯通；三是安全韧性，在日益严峻的网络攻击威胁下，确保电力“神经中枢”绝对安全。要同时达成这些目标，既需要扎实掌握 IEC 61850、IEC 60870-5-104 等电力行业专用通信规约的技术精髓，也需要灵活运用关系型数据库、时序数据库与大数据平台等现代数据基础设施，并在此之上构建科学的 IT 服务管理体系与主动防御的安全架构。

本书的编写，力图超越零散技术点的堆砌，而是从系统工程视角出发，构建一个完整的“设计—建设—运维—安全”闭环知识体系。我们特别强调“实践导向”：在数据库章节，不仅说明“用什么”，更详解“为何用”及“如何调优”；在自动化运维部分，通过故障自愈剧本、知识图谱构建等实例，展示如何将专家经验转化为可执行的智能流程；在安全管理上，则结合电力监控系统安全防护的最新政策要求，提出分区分域、纵深防御的落地策略。同时，我们引入 ITIL 框架，旨在帮助电力企业将 IT 服务从“救火式响应”转变为“价值共创”，真正实现 IT 与业务战略的对齐。

本书的读者对象包括电力企业信息化部门的工程师、项目经理、系统架构师，也适用于从事智能电网、能源互联网研究的高校师生及科研人员。我

们期望，通过本书的系统梳理与实践总结，能够为我国电力信息系统建设提供一套兼具先进性、适用性与安全性的方法论参考，助力构建更加智能、高效、绿色、安全的现代能源体系。

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。

—— 彭乃勇

目录

CONTENTS

第一章 电力信息系统概述 …… 1

第一节 电力信息系统基本概念 …… 1

第二节 电力信息系统发展历程 …… 7

第三节 电力信息系统架构组成 …… 13

第四节 电力信息系统建设意义 …… 19

第二章 电力信息系统需求分析 …… 27

第一节 电力业务需求分析 …… 27

第二节 系统功能需求分析 …… 32

第三节 性能指标需求分析 …… 39

第四节 安全可靠性需求分析 …… 46

第三章 电力信息系统设计方法 …… 53

第一节 系统总体设计原则 …… 53

第二节 系统架构设计方法 …… 57

第三节 数据库设计技术 …… 62

第四节 接口设计规范 …… 67

第四章 电力信息系统开发技术 …… 75

第一节 软件开发方法 …… 75

第二节 系统集成技术 …… 81

第三节 数据采集与处理 …… 85

第四节 实时监控技术 …… 90

第五章 电力信息系统测试技术 …… 99

第一节 测试方案设计 …… 99

第二节 功能测试方法 …… 105

第三节 性能测试技术 …… 111

第四节 安全测试要点 …… 117
第六章 电力信息系统部署实施 …… 125
第一节 系统部署规划 …… 125
第二节 硬件环境配置 …… 131
第三节 软件安装调试 …… 138
第四节 系统切换方案 …… 144
第七章 电力信息系统运维管理 …… 151
第一节 运维管理体系 …… 151
第二节 故障诊断处理 …… 157
第三节 系统优化升级 …… 163
第四节 运维监控技术 …… 169
第八章 电力信息系统安全防护 …… 175
第一节 安全防护体系 …… 175
第二节 网络安全技术 …… 181
第三节 数据安全保护 …… 187
第四节 应急响应机制 …… 193
第九章 电力信息系统标准规范 …… 201
第一节 国家标准要求 …… 201
第二节 行业标准规范 …… 207
第三节 技术标准体系 …… 214
第四节 管理标准要求 …… 221
第十章 电力信息系统实践案例 …… 229
第一节 智能电网信息系统 …… 229
第二节 配电自动化系统 …… 233
第三节 电力营销系统 …… 239
第四节 调度自动化系统 …… 245
参考文献 …… 253

第一章 电力信息系统概述

电力信息系统建设的过程就是现代电力工业向数字化、智能化转型的内在驱动力。本章从电力信息系统的基本组成、核心理念和分类方法入手，为读者建立电力信息系统的基础框架，为后面分析电力信息系统的地位和实现技术提供理论基础。

第一节 电力信息系统基本概念

为了正确把握电力信息系统的内涵，首先要从源头入手，即通用信息系统的定义、功能以及发展历史。了解信息系统的一般规律，才能更好的认识电力信息系统的特殊本质及其发展演变方向。

一、信息系统的定义与特征

信息系统不是简单的技术堆砌，而是一个包含技术、管理、人员等要素的综合体系，信息系统的定义和特点体现出信息在现代组织中的价值。它依靠系统的科学方法论把原始数据转化为有利于决策的有效信息，是组织运作的神经网络。

（一）信息系统的基本组成要素

一个完整的系统一般是由几个互相联系的部分组成的有机整体，其目的是实现对信息的系统管理，为组织决策和控制提供服务。基本组成要素协同起来形成信息系统运作的基础框架。要素包括计算机硬件、软件、数据库、网络通信、参与系统活动的人员、保证系统正常运行所制定的规章制度。

硬件给信息系统提供物理基础，包括从大型服务器到各种终端、输入输出设备等所有的实体设备。软件是核心，分为系统软件和应用软件，系统软件驱动硬件运行，应用软件支持业务功能。信息资源指的是系统处理的数据，它是系统最宝贵的资源，信息资源的好坏直接影响系统的价值。网络通信是系统血脉，把各个部分联系起来，使信息可以快速流动共享。人员就是系统的使用者、设计者和

管理者，也是决定系统成败的关键力量。规章制度给系统的计划、开发、应用和维护赋予了行为准则和流程标准，保证系统可以稳定、安全、高效地运行，而且同组织的战略意图相契合。

（二）信息系统的基本功能与作用

信息系统有着很强的功能与影响，它是现代组织的神经中枢，通过一系列有条不紊的信息处理活动，极大地改善了组织的运作效率、管理效能和战略决策能力，是获得竞争优势的重要手段。

信息系统的基本功能可以归纳为以下几个关键环节：

1. 信息输入与采集：系统从组织内外部环境中以各种方式获取原始数据，为后面处理打基础。

2. 信息存储：把收集到的数据以结构化的方式存储到数据库中，保证数据的持久性、一致性、可追溯性，形成组织宝贵的信息资源。

3. 信息加工处理，即信息系统的主要功能，对信息进行计算、分析、汇总等处理，使之成为有用的信息。

4. 信息输出和展示：用报表、图表、查询等方式把处理过的信息提供给用户，给管理、决策提供直观依据。

5. 系统具有自监督、自调节的功能，用权限管理、数据加密等手段保护信息资源不被未经授权者访问、修改或者破坏。

互相配合、发挥作用的各项功能，使得信息系统能优化业务流程，辅助各个层次管理者作出决策，加强组织内部交流与合作，从而促进组织的改革与发展。

（三）信息系统的发展阶段与趋势

信息系统的发展与信息技术的发展关系密切，从最初的数据处理工具发展到今天企业战略的重要组成部分，发展的各个阶段都体现出技术推动的管理变革。进入 21 世纪之后，云计算、大数据、人工智能等新技术持续出现，信息系统正向智能化、集成化发展。

追溯其发展大致可分为以下几阶段，初期是单机应用的数据处理系统，主要是对一些重复的事务处理任务进行处理。后来由于网络技术的发展而产生了管理信息系统和决策支持系统，开始为中高层管理者提供战术级、战略级的信息支持。企业资源计划、客户关系管理等集成化系统发展至今已经成为主流，有效地消除了企业内部的信息孤岛。未来信息系统的特点是更加突出智能化、移动化、平台

化、数据化的特点。人工智能会赋予系统自我学习、预测的能力，云计算带来的是灵活的资源部署，移动应用使信息服务无所不在，对海量数据进行深度挖掘和分析，才是创造商业价值的关键。

二、电力信息系统的独特内涵

电力信息系统具有一般信息系统的基本属性，但是由于服务对象的特殊性而具有独特的内涵。它把信息技术和电力系统的运行规律结合起来，是为了满足电力工业生产、输送到用户全链条特定需求而形成的一个专门的信息系统。

（一）电力生产流程的特殊性要求

电力系统生产、传输、分配、使用过程是瞬时完成的、高度耦合的，不能中断的，这就对信息系统的可靠性、实时性、安全性提出了远高于一般商业系统的要求。电力属于特殊商品，生产、供应、销售三者同步进行，不能储存大量，因此电力信息系统需要有很高的实时响应能力来应对电网潮流的变化。

电网是覆盖范围广、各个环节相互联系的复杂物理系统，任何一个节点出现故障都会引起连锁反应，造成大面积停电。这就需要信息系统，尤其是调度自动化、继电保护等生产控制类信息系统，必须具备金融级的安全性和接近 100% 的可用性。电力系统运行状态数据，比如电压、频率、相角等，都需要以毫秒级的精度进行采集和监控，这就对数据采集系统提出了很高的实时性、精度要求。由于新能源的大规模接入，源荷互动越来越频繁，电力系统运行的不确定性越来越大，对信息系统的数据处理和智能分析的要求也越来越高，以达到预测、调度和控制的智能化。

（二）电力信息系统的核心目标与任务

电力信息系统的主要目的就是保证电力系统的安全、稳定、经济运行，不断提高电网企业管理和服务水平。总目标被分解为电力生产、传输、消费、交易等各方面的具体任务，用数字化和智能化的手段给现代电力工业提供全方位支持。

它最重要的任务就是保证电网安全稳定。依靠实时监控系统、广域测量系统等准确地获取电网运行状态，及时发现故障并加以解决，防止事故进一步扩大，这是电力信息系统最主要的任务。它要达成电力资源的优化调度、经济运行，依靠能量管理系统这些高级应用，加上负荷预测、发电计划、市场信息，合理安排机组出力，优化潮流分布，尽可能地削减网损和发电成本。再次提高经营管理效

率，利用营销管理系统、资产管理系统等管理业务、服务客户，实现企业精益化管理。随着能源转型的深入，支持新能源消纳、用户侧友好互动，构建以数据流驱动能量流的新型电力系统也越来越成为它的主要任务。

（三）电力信息系统与传统信息系统的区别

电力信息系统同制造业、金融业这类传统信息系统存在很大差别，这种差别出自于电力行业特有的物理属性和业务要求。最根本的区别就是对于实时性、可靠性有很高的要求。电力生产控制系统响应时间以毫秒计，稍有延迟或者中断就会造成电网崩溃，造成严重后果；而传统商业系统哪怕中断几分钟，也只是造成业务层面的损失，很少会牵涉到社会公共安全。

电力信息系统的系统架构以及安全防护以物理隔离和纵向认证为主。按照“安全分区、网络专用、横向隔离、纵向认证”的原则，生产控制大区和管理信息大区之间必须部署严格的安全防护装置，有效抵御外部网络恶意攻击。严格的分区隔离在大部分传统信息系统里并不常见。

电力信息系统要处理很多传感器、智能设备产生的实时时序数据，数据采集频率高、数据量大，而且这些数据和电网的物理拓扑结构有关联。这就对数据处理、存储、分析技术提出了特殊的要求，促使实时数据库、时序数据库等专用技术的产生和发展。

从服务对象和服务范围来说，电力信息系统关乎国计民生和公共安全，其稳定与否牵涉到整个社会是否能够正常运转。传统信息系统的影响范围一般只局限在企业或者特定的用户。由于其造成的影响是广泛的、深刻的，所以对电力信息系统的规划、建设、运作都会遇到更为严格的行业监督与国家的审查。

三、电力信息系统的分类体系

由于电力业务繁杂多变，于是形成了庞大的电力信息系统。为了对其有效地规划、建设和管理，需要从不同的角度对其进行科学的分类。这样的分类可以很清楚地把各类系统功能、技术要求、安全等级区分开。电力信息系统主要分类如下表所示：

电力信息系统主要分类表

分类维度	具体类别	主要特点与应用举例
按业务领域	生产控制系统	确保电网安全稳定运行，实时性、可靠性要求极高。如调度自动化、继电保护系统。
	电力营销系统	支撑电费结算、客户服务、市场交易等业务。如用电信息采集、客户关系管理系统。
	经营管理系统	提升企业运营效率，管理内部资源。如财务管理、人力资源管理系统。
按部署架构	集中式	数据和功能集中于少数服务器，易管理、数据一致性高，但扩展性受限，风险集中。
	分布式	功能和数据分布于多个节点，扩展性好、可靠性高，但管理复杂。
按实时性要求	实时系统	毫秒到秒级响应，直接影响电网安全。如安全稳定控制、高频次调度功能模块。
	准实时系统	秒到分钟级响应，用于监控和快速管理。如配电自动化故障定位、智能量测系统相关数据采集与分析。
	非实时系统	小时到周或更长，处理无时间敏感性要求的业务。如财务管理、资产管理、报表分析等。

1. 生产控制系统直接为电力生产和调度运行服务，是保证电网安全稳定的中枢。其最突出的特点就是实时性要求很高，数据采集和控制指令的传递要在秒级或者毫秒级完成，可靠性、安全性要求也最严格。

2. 电力营销系统：这一类系统面对的是电力市场和最终用户，主要是电费结算、客户服务、市场交易等相关业务。用电信息采集系统、客户关系管理系统、电费核算与收取系统等等。虽然它们对实时性要求没有生产系统那么高，但是对数据处理的准确性、业务流程的规范性、客户信息的安全性有很高的要求。

3. 经营管理系统：经营管理系统主要对企业内部的人、财、物等资源进行管理，目的是提高企业的运作效率。常见的人力资源管理系统、财务管理系统、物资管理系统、办公自动化系统等等。这类系统大多是是非实时系统，重流程标准、管理精细。

（二）按部署架构划分

信息系统的部署架构决定着计算资源和数据资源是怎么组织的，也影响着系统的可扩展性、可靠性和维护成本等。电力信息系统也可以根据所采用的技术架构分为集中式和分布式两种，实际应用中也会出现结合两种特点的混合式架构。

集中式架构即所有的数据处理、存储功能都集中在中心机房内少数几台大型主机或者高性能服务器上，各个终端通过网络连接到中心进行操作。该种模式的优点有便于管理维护、数据一致性好、安全性容易管理。在电力系统发展的初期，调度自动化系统等主要应用多采用该种结构。缺点是中心节点的负荷大，一旦出现故障就会导致整个系统瘫痪，垂直扩展的成本高，灵活性差。

分布式架构就是将系统的功能、数据分散到网络中的各个计算节点上，各个计算节点相互配合，共同完成任务。伴随着互联网技术以及云计算的发展，分布式架构在电力行业应用越来越广，尤其在用电信息采集、新能源监控等需要处理大量终端和数据的场景中应用较多。它的优点是具有良好的扩展性，利用水平扩展来降低系统的成本增加系统的容量，单个节点的故障一般不会影响到整个系统，可靠性高。但是，分布式系统在数据一致性保证、系统管理、运维方面比较复杂。

（三）按实时性要求划分

根据系统对数据处理和响应时间的要求不同，可将电力信息系统分为实时系统、准实时系统、非实时系统。该维度直接体现出信息系统同电力物理过程结合的紧密程度，是开展系统设计和资源配置的主要依据。

实时系统对时间的要求最为严格，它必须在规定的时间内（一般为毫秒到秒），对外部事件作出确定的反应。电力系统中的安全稳定控制系统、继电保护信息管理系统、高频次的调度自动化功能模块都属于此类型。一旦系统超时或者出现错误都会直接危及电网的安全。

准实时系统的响应时间比较宽松，一般为几秒到几分钟。该类系统主要用在监控和需要快速响应的管理活动中，但是其延迟一般不会造成灾难性的后果。如配电自动化系统中故障定位，智能量测系统的数据采集及分析，电网运行人员的态势感知等。

非实时系统处理无时间敏感性要求的业务，可以按小时、按天、按周或者更长的时间来处理。这一类系统在电力信息系统中所占比例很大，大部分的经营管理类系统，如财务管理、客户关系管理、资产管理、报表分析等都属于此类。它们主要用在企业后台支持和长周期决策分析上，侧重于业务逻辑是否正确，数据是否完整。

第二节 电力信息系统发展历程

电力信息系统的发展不是一蹴而就的，它与信息技术发展大潮同步，并且同电力行业自身管理变革和技术创新需要相融合，共同进步，具有较强的阶段性特征。从最初的自动化控制到现在全面智能化，其发展的轨迹也体现出了电力系统由保障安全生产向精益管理、智慧运营的转变过程。

电力信息系统发展的主要阶段及其特点，可见下表。

电力信息系统发展阶段概览

阶段名称	时间范围	核心特征 / 技术	主要成就 / 突破	面临挑战
萌芽阶段	20 世纪 70-80 年代	自动化、单机应用	提升生产安全性、局部办公效率	数据孤岛、缺乏共享
网络化阶段	20 世纪 90 年代	局域网、客户端 / 服务器架构、部门级系统	部门内数据共享、业务管理规范化	跨部门集成难、网状接口
信息化阶段	21 世纪初	企业资源计划、数据仓库、企业服务总线	企业级管理整合、数据驱动决策	生产与管理数据融合不足
智能化阶段	智能电网建设至今	物联网、大数据、人工智能、云计算	全面感知、智能决策、驱动业务变革	数据治理、安全隐私、技术迭代

一、萌芽阶段：自动化与单机应用

二十世纪七八十年代是电力信息系统萌芽的时期。该时期的主要特征为自动化技术开始用于生产领域，管理工作中出现了单机版软件。由于系统建设分散且相互独立，为以后信息化建设埋下了“数据孤岛”的隐患。

（一）早期自动化装置的应用

电力系统信息化刚开始的时候，主要的工作重心就是生产过程的自动化控制，目的是提高电网运行的安全性、可靠性。继电保护装置、远动装置、早期调度自动化系统等开始在电网和发电厂里应用。这些设备可以对电力设施的状态实施远程监测和简单的控制，极大地提高了调度员对电网的感知能力以及处理故障的效率。

这些系统具有很强的专用性，技术架构也很封闭，主要是为调度、变电站监

控等生产环节服务。它们虽然解决了生产环节的自动化难题，但是产生的数据主要用作实时监控和事后故障分析，并没有进入企业的整体管理信息流。此时信息技术的应用呈点状分布，工具性较强，其价值体现更多的是保障生产安全，对管理效率的提升还没有产生明显的作用。

（二）单机版管理软件的出现

随着个人计算机在办公中的普及，电力企业的各个管理部门也试着用计算机来处理自己的日常工作。像财务电算化、人事档案管理、物资库存管理这些需求，产生了很多依靠单机运行的管理软件。这些软件大都用 dBase、FoxPro 等桌面型数据库开发工具开发，功能较简单，主要目的就是代替手工操作，提高某一岗位的办公效率。

这些单机版软件实现了从无到有的突破，把一部分管理工作从纸质台账、人工计算中解放出来，属于管理信息化的初级形态。各个部门根据自身需要独立开发或者购买软件，形成的是以岗位或者部门为单位的应用模式。

尽管这种模式大大提高了局部效率，但是由于没有统一规划、标准，使得各软件间数据格式、编码体系不相容。信息被困在各自计算机里，不能流通、共享，严重制约了企业信息化的发展。

（三）数据孤岛问题的形成

萌芽时期的建设模式造成了“数据孤岛”的出现。生产领域自动化系统同管理领域单机版软件相互隔离，造成各自为政的局面，形成封闭的数据集。调度系统数据、财务软件数据和人事系统数据互相隔绝，不能进行有效的关联与综合利用。

各自为政的隔离状态存在许多弊端。数据冗余指的是如设备台账这样的信息被多次录入不同的系统当中，这样不但增加了维护的成本，而且提高了出错的概率。其次就是数据不一致，由于更新不及时或者标准不统一，不同的系统中同一个数据项可能会有不一样的值，这就造成了决策依据的混乱。信息获取变得异常困难，管理者需要从不同的独立系统中拼凑报表，很难对企业整体的运营状况形成全面准确的认知。数据孤岛成了电力企业管理水平提高的瓶颈，促使信息系统向着网络化、集成化方向发展。

二、网络化阶段：局域网与系统集成

进入 20 世纪 90 年代以后，计算机网络技术特别是局域网技术的迅速发展，给打破数据孤岛带来了可能。电力信息系统建设进入网络化阶段，重点由单机应用转向部门级系统建设以及初步的系统集成。

（一）企业局域网的普及

以太网技术以及 TCP/IP 协议族已趋向于成熟，也正因其普及程度较高，所以可以使得企业内部创建快速且可靠的局域网成为可能。电力企业投入大量的资源建设起覆盖总部、下属单位乃至偏远场站的内部网络。网络全面铺开，为信息系统赋予了必要的“神经脉络”，让数据在各个计算机之间、各个部门之间往来变得可行。

物理层面的互联互通，给后面的信息共享和系统集成打下了基础。企业局域网建立起来不只是满足了简单的文件共享、打印等基本办公需求，更重要的是为以后建立以客户端 / 服务器为基础的部门级信息系统提供了网络平台。信息化重心也由原来的单一节点应用转为网络化整体布局。

（二）部门级信息系统的建设

在局域网的基础上，电力企业各个专业部门开始建设面向自身业务管理的网络版信息系统。这些系统大多数都采取了客户端 / 服务器结构，数据被集中存储于各个部门的服务器之中，客户端经由网络去访问并处理这些数据。典型的系统有生产管理系统、营销管理系统（用电或收费系统）、设备管理系统等。

相较于单机版软件，部门级系统可以实现部门内数据集中管理、共享，多个用户可以同时进行协作处理，业务处理能力和数据管理规范性都有了很大的提高。供电局营销系统所有营业厅收费员可以实时查看客户、电费数据，有效避免了信息不对称问题。

此类系统大大提高了某一业务领域的信息化程度，以及部门内部管理规范化、高效率的程度。但是由于各个系统是由各个业务部门各自建设的，技术和数据标准不统一，跨部门的数据共享问题仍然没有得到根本的解决。

（三）初步的系统集成与数据共享

随着部门级系统越来越多，新的问题又来了，生产系统要调用物资系统的备品备件信息，营销系统要调用调度系统的停电通知等。跨部门业务协同需求愈加

急迫，开始尝试初步的系统集成。

此阶段的集成大都采用点对点的方式。通过专门开发的接口程序定时从一个系统数据库中抽取数据，经过格式转换之后再导入另一个系统数据库。文件传输、数据库视图、中间表等都是当时常用的方法。此种“头痛医头，脚痛医脚”的集成办法，在一定程度上解决了燃眉之急，达到了局部数据共享的效果。但是随着集成点位的增加，系统之间就会形成一个复杂的“蛛网”式的连接，接口数量呈几何级数增长，造成系统之间耦合度非常高，使得系统之间的维护和升级变得异常困难，为以后推行更加规范的企业级集成架构埋下了隐患。

三、信息化阶段：企业级系统与数据整合

21 世纪以后，电力企业管理理念趋向精细化、集团化，对信息系统的要求也由支撑部门业务提升到支撑企业整体战略。信息化阶段的主要任务就是构建企业级一体化系统，以数据整合为手段打破业务壁垒，给经营决策提供全方位的支持。

（一）企业资源计划系统的引入

为了实现对企业核心经营资源的集中管理以及合理配置，电力行业大范围地使用了企业资源计划系统。这些管理软件本是制造业中成熟的产品，后来经过改造并行业化，用以整合电力企业人、财、物、项目等各项管理流程。企业资源计划系统的中心思想，就是用一个数据库、一套标准的业务流程，把以前分散的财务会计、人力资源、物资采购、项目管理等业务领域，整合到一个平台上。

企业资源计划系统实施属于深层次的管理变革。它不但是技术系统更替，更是对企业原有业务流程的梳理、优化甚至再造。借助企业资源计划，电力企业第一次实现了管理信息的横向整合，也就是财务、物资、人事等各部门之间的信息壁垒被打破，为企业实现集团化治理、提高整体经营管理水平奠定了基础。

（二）数据仓库与决策支持系统建设

企业资源计划系统虽有效整合了企业交易型数据，但其是面向日常业务的处理，所以在对数据进行深入分析以及面向主题的分析上较弱。为了给管理层提供经营分析以及制定战略决策所需的数据支撑，数据仓库及决策支持系统建设迫在眉睫。数据仓库技术用抽取、转换、加载的过程，把来自企业资源计划、生产系统、营销系统等各类业务系统的数据清洗、整合、汇总，形成面向分析的主题数据。

企业以数据仓库为依托，通过使用商业智能工具创建报表平台、多维分析以及数据挖掘的应用等一系列的决策支持系统。管理者可以借助这些系统迅速获得各个业务、各个周期的经营指标，进行下钻、切片等交互式分析，从而掌握企业经营情况，发现问题以及机会。

数据仓库和决策支持系统的创建，是电力企业信息化从支持业务操作到支持管理决策的一种跨越，数据真正被当作一种战略资产来管理和使用。

（三）信息一体化平台的探索

在企业资源计划、数据仓库建设取得一定成果之后，电力企业认识到，实现全面信息化，必须打通生产域和管理域。只有把生产调度数据、设备状态数据和经营管理数据三者融合起来，才能形成公司信息完整视图。因此，创建企业级信息一体化平台的探索也随之出现。探索主要表现在以下几方面：

1. 推广企业服务总线。通过创建统一的企业服务总线平台，把各种异构系统以即插即用的方式接入，代替以前的网状点对点的集成，实现了系统的松耦合、标准化交互。

2. 创建统一的身份认证系统以及信息门户。为用户创建一个唯一的登录入口，将各个系统功能、信息综合起来，用个性化的门户界面来展示，极大地改善了用户最终体验。

3.3、建立企业级的统一数据模型。建立覆盖生产、营销、管理等全部业务领域的一致数据模型和主数据管理体系，从源头上保证数据的一致性、准确性，为数据的彻底融合打下基础。

四、智能化阶段：物联网、大数据与人工智能

随着智能电网建设的全面推进和云计算、大数据、物联网、移动互联网、人工智能等新一代信息技术的迅猛发展，电力信息系统已经进入了以感知、互联、智能为特征的新时代。信息系统不再只起到支撑作用，而是深深地融入到电力系统各个环节当中，成为推进业务变革的主要动力。

（一）智能电网概念的提出与实践

智能电网建设目的是使电网具有可靠、经济、高效、友好等特性，其根本就是信息技术与电力技术的深度融合。传统电网以“源随荷动”的单向运行模式为基础，而现在正在转变为“源网荷储”的互动模式以及信息双向流动模式，对信

息系统提出了前所未有的要求。高级量测系统、广域测量系统、智能变电站、配电自动化等智能电网关键技术的应用，产生大量的、多样的实时数据。

信息系统是智能电网的大脑和中枢。它要有着强大的接入能力，承载起数以亿计的智能电表、传感器并发的数据流；要有强大的处理能力，对海量数据实施即时分析并迅速做出反应；还要具备高级的应用能力，支撑需求侧响应、分布式能源并网、电动汽车充放电管理这些新业务。电力信息系统的结构、性能、功能因此而发生根本性的改变。

（二）大数据技术在电力系统的应用

智能电网造成数据量呈爆炸性增长，数据类型也由原来的结构化数据扩展到时序数据、文本数据、图像视频数据等多样化形式，形成了电力大数据。传统的基于关系型数据库以及数据仓库的技术对于这样规模、这样复杂的数据已经力不从心了。以 Hadoop、Spark 等为代表的大数据技术栈进入电力行业，给海量数据的存储、计算和分析带来了新的解决思路。

依靠大数据平台，电力企业新的应用不断涌现。以用电数据做大量用电数据的精准负荷预测、用户画像分析，为精准营销、需求侧管理提供支持；整合设备状态数据、环境数据、运行数据等开展设备健康状态评估及故障预兆预警，丰富了状态检修的做法；根据电能质量监测数据快速发现并诊断电能质量问题。

大数据技术的使用使得电力企业的数据挖掘能力有了质的飞跃，使企业的运行方式从以前的经验驱动转变为现在的数据驱动。

（三）人工智能赋能电力信息系统

在拥有大量数据和强大计算能力之后，人工智能技术才成为电力信息系统智能化的“点睛之笔”。机器学习、深度学习、自然语言处理等人工智能算法被广泛应用到电力系统的各个领域里，从而使信息系统由以前的支持性决策上升为智能决策。

以电网调度为例，用强化学习算法来优化调度策略，有效应对新能源出力带来的不确定性；以设备运维为例，用无人机巡检和图像识别技术，自动发现设备的缺陷；以客户服务为例，智能客服机器人可以处理大量的用户咨询、业务办理请求；以网络安全为例，使用人工智能算法分析网络流量、用户行为，智能识别并阻止潜在的网络攻击。随着人工智能技术的发展，人工智能给电力信息系统带来了深远的影响，使电力信息系统的价值得到了极大的提升，电力行业进入到了

更加高级的智慧化运营阶段。

第三节 电力信息系统架构组成

电力信息系统是现代电力工业的核心，它的整体架构设计、实现直接关系到电力系统的安全、稳定、高效运行。该架构一般采用分层解耦的设计思想，自下而上地构建，保证系统具有较好的灵活性、扩展性、可维护性，给复杂的电力业务提供强有力的支撑。

一、物理层（感知层）架构

物理层是电力信息系统的基础，对电力系统运行各方面数据进行全方位的感知和采集。它相当于物理世界和数字世界的重要的连接点，给上层的数据处理和分析提供真实可靠的输入数据。

（一）传感器、智能终端设备

电力信息系统的感知能力来自于发电、输电、变电、配电、用电各个环节上各种传感器、智能终端。传感器把温度、湿度、压力、电流、电压这些物理量转变成可以被处理的电信号，它是数据采集的最小单位。它们犹如系统的末梢神经，可以即时反映电网的状态，是进行状态监测、故障诊断的原始数据。

智能终端设备属于感知层的主要组成。它们把数据采集，处理，控制以及通信功能融合在一起，而且拥有本地自主决策的能力，这对实现电网智能化起着非常重要的作用。如变电站的保护测控装置、智能电表、故障录波器、在线监测单元等都属于智能终端设备。设备之间用标准通信协议相连接，可以自主地向上级系统汇报数据，并且可以接受并执行上级系统下发的控制指令，实现对电网设备的精确控制和快速反应，为坚强智能电网的建设打下基础。

（二）通信网络与数据采集设备

通信网络是物理层的动脉系统，把传感器、智能终端等采集的大量数据安全、可靠、高速地传送到数据中心。电力系统对通信的可靠性和实时性要求很高，所以一般会建立一个覆盖范围大、使用多种技术组合而成的专用通信网。光纤通信由于具有带宽大，抗干扰能力强等特点，现在已经成为电力通信骨干网的主要通信方式。电力线载波、无线专网、微波、卫星通信等其他通信方式作为辅助通信

方式，在复杂的环境中保证数据的顺畅传输，对偏远地区以及移动终端实行全方位的覆盖。

数据采集设备，远动终端、数据采集与监视控制系统的采集单元、配电自动化终端、集中器等，都是现场设备和主站系统之间的桥梁。它们会按照预设的规则与频率从指定的设备上读取数据，先做初步处理并缓存起来，然后再经由通信网络上传。这些设备在设计时必须考虑到现场电磁环境的恶劣，要求具有较高的可靠性、稳定性，以保证数据采集的可靠性、完整性，是保证整个信息系统感知敏锐、运行可靠的“眼睛”。

（三）数据中心与服务器硬件

数据中心对于电力信息系统来说是重中之重，它是数据集中存放、处理、运算的地方。其物理架构设计要符合高可靠性、高可用性、高安全性这三个原则。包含给海量服务器、存储设备和网络设备提供稳定运行环境的基础设施，即不间断电源、精密空调、消防系统、安防系统等。为了防止单点故障的发生，数据中心一般会采取冗余设计，即使某一个设备或者线路出现故障，核心业务依然可以不间断的进行。

服务器硬件是数据中心的核心计算设备，选择和配置好服务器硬件，才能保证整个信息系统的处理能力。根据不同的应用需求，数据中心会配置不同类型的服务器，有支持大型数据库、处理核心业务的高性能小型机，构建计算集群和虚拟化资源池的机架式服务器，还有处理大量并行计算任务的刀片服务器等。伴随着大数据和人工智能技术的大范围应用，越来越多的数据中心开始配置 GPU 服务器，用来满足深度学习及复杂模型训练对算力的需求。高效的、绿色的、可扩展的服务器硬件架构，给电力信息系统应对将来业务挑战提供强大助力。

二、平台层（数据层）架构

平台层在电力信息系统架构里属于承上启下的层次。对物理层得到的大量原始数据进行有效的组织、存储、管理、加工，将数据转化为有业务价值的信息资产，并统一标准向上层应用提供数据服务接口。

（一）数据库管理系统（关系型、时序型）

数据库管理系统属于平台层的基础，保证数据有序存放并能快速查找。电力信息系统中根据各个业务场景的需求混合使用各种数据库。

1. 关系型数据库 Oracle、MySQL 等，因为严格的数据一致性、成熟的事务处理能力、强大的关联查询功能，长期以来是电力核心业务系统首选的数据库。它们主要用来存放结构化的业务数据，像用户信息、设备台账、资产管理和电费结算之类，这些数据大多逻辑繁杂且对数据的完整性能提出非常高的要求。

2. 时序数据库 TDengine、InfluxDB 等专门用来处理带有时间戳的序列数据。智能电网发展以后，传感器、智能电表等设备产生的数据量剧增，这些数据有典型的时间序列特征。时序数据库在数据写入、压缩存储、聚合查询等各方面有明显的性能优势，可以有效支持电网运行状态实时监测、历史趋势分析、故障追溯等业务。

不同数据库类型特点对比可见下表：

数据库类型特点对比表

特性	关系型数据库	时序数据库
典型产品	Oracle, MySQL, SQL Server	TDengine, InfluxDB, OpenTSDB
主要数据类型	结构化数据 (如用户信息、资产台账)	带有时间戳的序列数据 (如传感器读数)
数据特性	强一致性，复杂关系，事务完整性	高并发写入，高压缩比，时间有序性
核心优势	复杂关联查询，事务处理能力强	海量时序数据的高效存储与查询，聚合分析快
典型应用	业务管理系统、财务结算、资产管理	电网实时监测、历史趋势分析、故障追溯

（二）数据存储与管理技术

因为数据量的猛增，传统的单一存储已经不能满足要求。现代电力信息系统的存储架构采用多层分布式方式，很好地解决了上面的问题。分布式文件系统、对象存储技术在存储海量非结构化或者半结构化数据 (例如图像、视频、文档等) 上具有明显的优势，具备良好的扩展性以及经济性。数据仓库、数据集市技术则是把来自各个业务系统的数据进行集成，清洗，转换，生成面向主题的分析型数据集来为管理决策提供支持。

数据管理对保证数据质量，发挥数据价值起着至关重要的作用。创建全域统一的数据模型和标准，实行企业级主数据管理，保证核心数据在各个系统间的准确性、一致性。同时使用元数据管理系统来对数据的来源、格式、处理流程、业

务含义等做了详细的说明，形成数据地图和数据血缘关系方便理解追溯数据。实行数据生命周期管理策略，对数据从产生，应用，归档到销毁的全部流程加以控制，较好地达成了数据可用性与存储成本之间的均衡。

（三）数据交换与共享平台

为了打破各个业务系统间的“信息孤岛”，实现数据互通共享，建立统一的数据交换共享平台迫在眉睫。该平台一般以企业服务总线或者微服务的形式存在，通过统一的数据接口以及协议转换服务，隐藏了底层异构系统之间的技术差别。各个业务系统既可以将自身需要共享的数据发布到平台上，也可以从平台上订阅所需的数据，从而实现系统的松耦合集成。

该平台除了能提供数据传输之外，还能给用户带来数据服务目录、接口管理、访问控制、流量监控、安全审计等一系列的服务。通过服务化的方式对外开放数据能力，既可以满足企业内部各个部门、各个业务之间的数据协同需要，又可以为企业与上下游合作伙伴、政府监管机构等外部实体进行安全可控的数据共享奠定基础，从而为能源互联网生态系统的构建提供有力支撑。

三、应用层架构

应用层是电力信息系统价值的体现者，它直接面对具体的电力业务需求，把平台层处理过的数据变成可用的功能。构建各种业务应用来支持电力企业在生产、经营、决策等各个方面的各项工作，是系统功能最丰富、用户交互最频繁的一层。

（一）生产运行类应用

生产运行类应用是保证电网安全稳定运行的工具集，具有实时性要求高、可靠性要求高的特点。这些应用主要是给电网调度、监视、运维、检修等重要的生产环节提供服务。电网能量管理系统、配电管理系统属于典型的集成数据采集与监视控制功能的系统，可以对主网、配网进行实时监控、潮流计算、事故告警、调度操作。

资产全生命周期管理系统对设备的规划、采购、安装、运行、维护、报废全过程进行管理，使设备状态可控。伴随着数字化转型的推进，无人机巡检、机器人作业、设备状态智能诊断等新的应用不断涌现出来，人工智能、物联网技术的运用使电网运维越来越高效、智能化，大大降低了人工巡视的风险和成本，是智慧运维的重要组成。

（二）经营管理类应用

经营管理类应用主要给电力企业市场化运营、内部资源管理提供服务，目的是提高电力企业的经营效益和管理效率。营销业务系统为核心，包含客户服务、抄表核算、电费收缴、业扩报装等所有的客户侧业务，是电力企业与终端用户之间的重要联系纽带。

从企业的内部管理角度来讲，企业资源计划系统把财务、人力资源、物资采购、项目管理等重要管理流程包含在内，从而达成企业内部资源的合理调配以及业务流程的标准化。协同办公系统是员工日常工作的平台，也是流程审批、发布信息、内部交流的平台，提高组织的协作效率。这是企业运营的数字化基础，也是电力企业进行市场精细化管理、高效运作的基石。

（三）综合分析与决策支持类应用

综合分析与决策支持类应用处于应用层的顶端，它依靠大数据、人工智能技术，对生产、经营等各个方面的海量数据进行深度挖掘和智能分析，给企业战略规划和管理决策提供科学依据。

1. 对电网的历史负荷数据、气象资料及社会经济资料进行综合分析，建立准确的负荷预测模型，为发电计划和调度提供依据。

2. 对设备运行数据、缺陷记录、环境因素进行相关性分析，可以对设备故障进行预警，给出设备健康状况评价结果，支持预防性维护活动。

3.3、利用用户画像分析可以识别出各个客户群体的用电行为特点，为差异化电价策略和增值服务的制定提供支撑。

这些高级的应用把数据变成洞见，让管理者既能站在高处看全局，又能蹲下身子看细节，从而对电网运行的规律和市场变化了如指掌，推动企业由依靠经验决策转向依靠数据决策。

四、展现层（用户层）架构

表现层是电力信息系统面向最终用户的窗口。其设计的主要目的就是给出直观、友好、高效的交互界面。它把应用层复杂的业务功能和大量的数据，用用户容易理解、操作的方式来展示，直接体现系统可用性以及用户体验。

（一）人机交互界面

人机交互界面属于展现层的主要组成要素，它是用户同系统进行信息交流的

窗口。现代电力信息系统界面设计以人为本，操作简单。采用统一的视觉风格、使用统一的控件库、采用统一的交互方式，降低用户的学习成本，提高用户的操作效率。根据调度员、运维人员、管理人员等不同用户的具体工作场景，界面会做定制化的设计，突出用户最关心的信息和最常操作的功能。比如调度员的界面是电网接线图，经营分析人员的界面却是各种各样的统计图表和报表。一个好的好的人机交互界面设计，可以将复杂的隐藏起来，使得用户能够高效并且简单的完成工作。

（二）大屏幕与可视化系统

大屏幕和可视化系统是电力调度中心、集控中心、应急指挥中心必不可少的重要组成部分，承担电网宏观态势的全景展示任务。采用地理信息系统以及电网实时运作数据相融合的方式，可在大屏幕上实现电网的地理分布情况、设备的状态、功率潮流、负荷曲线等重要信息的动态逼真显示。数字孪生技术的应用，可以将物理电网在数字空间中进行精确的复制，实现电网运行情况的三维可视化监测。

该可视化系统可以产生震撼性的视觉效果，还可以将大量、多维的数据变成可以直接观察的态势图，使决策者对整个电网运行情况有很直观、完整的认识，并及时发现电网运行当中存在的薄弱环节和可能的风险。电网出现故障或者需要紧急处理的时候，大屏幕系统可以准确显示受影响区域、资源分布和修复进度等信息，为指挥决策提供有力的信息支持。

（三）移动应用与门户系统

随着移动互联网技术的发展，移动应用和门户系统作为展现层的重要延伸，把电力信息系统服务的能力从固定的办公场所扩展到任何时间、任何地点。企业门户系统是业务系统入口及信息汇集站，为员工提供一个统一工作平台，支持单点登录、个性化信息订阅。

移动应用针对现场作业人员和管理者不同的需求，开发出轻量化、场景化的功能。运维人员可以随时利用手机查看到设备图纸，接收工单，填写巡视记录以及上报缺陷等等，大大方便了现场作业。管理者可以利用手机或者平板电脑，随时随地查看重要的生产经营指标报表，及时审批重要的流程，实现移动办公，移动决策。移动化、门户化的系统设计冲破了时空的束缚，让信息服务更加便捷、高效地到达每一个用户。

第四节 电力信息系统建设意义

一、保障电力系统安全稳定运行

电力系统安全稳定的运行，是社会经济发展不可缺少的基础。电力信息系统构筑起全方位、全过程、全天候的数字化、智能化支撑体系，给这张繁杂的能源网络赋予了前所未有的安全保障机能，堪称现代电网的“中枢神经”。

（一）提升电网监控与故障处理能力

电力信息系统建设的根本意义之一，在于它革命性地提升了对广域、复杂电网的感知能力和控制水平。传统的电网运维模式，主要依赖人工巡检与周期性试验，信息传递滞后，难以实现对设备状态的实时、全面掌握。而现代电力信息系统，尤其是 SCADA、EMS 和 WAMS 等核心应用（其功能详情可见下表核心电力信息系统应用），依靠分布在整个电网上的海量传感器以及高速通信网络，能够以毫秒级的精度采集并汇集大量的电网运行数据，这些数据涵盖电压、电流、频率、相角、开关状态等诸多关键参数。这使得调度控制中心能够对超高压骨干网架、中低压配电网络的每一个角落都了如指掌，从而构建起一幅动态、透明、高清的电网运行全景图。这种全局态势感知能力，无疑是从小范围局部感知到大范围全局掌控的质变。

核心电力信息系统应用

系统名称	英文缩写	主要功能
数据采集与监视控制系统	SCADA	实时采集、监视和远程控制电力设备运行数据
能量管理系统	EMS	优化电网运行、管理发电与负荷平衡、安全分析
广域相量测量系统	WAMS	实时监测电网动态相量数据，提升广域稳定性

当电网发生故障的时候，信息系统就体现出不能替代的价值。以往故障处理过程比较慢而低效，故障发生之后要经过定位、隔离、抢修等环节，耗时可达数小时甚至更长。而如今，集故障录波、行波测距、智能告警等先进技术于一身的信息系统，可以在故障发生的一瞬间精确找到故障点，误差小到米级。系统根据故障信息，快速得出最优的隔离方案然后传送给调度员，调度员马上切断故障元件，使停电的范围减小到最小。电网自愈功能启动，系统自动切换运行方式，利用其它的完好线路恢复供电，大部分用户根本就没有感觉到电网出了问题。针对

必须到现场处理的故障，信息化平台会立刻创建抢修工单，利用 GIS、GPS 技术，将任务详情，最佳路线，所需物资等信息准确发送到最邻近的抢修人员终端，从而达成资源的合理调配和抢修过程的闭环管理，明显缩减了用户停电时长，很大程度改善了供电可靠性。

（二）增强电力系统预警与防御能力

电力信息系统的出现把电网安全管理由“事后的处理”转变为“事前的预防、事中的干预”，使系统具有了预警和防御的能力。对大量的历史运行数据、设备状态数据以及外部环境数据（天气、地质灾害等）进行深度挖掘和关联分析，进而建立复杂的电网风险评价模型。利用人工智能和机器学习算法，可以预测出以后可能会出现的风险事件。按照天气预报和线路覆冰模型提前发布预警提示输电线路存在舞动、覆冰的危险；分析变压器油色谱在线监测数据，可提前发现设备存在的隐患。这种预测性维护和主动预警模式，使电力企业可以提前安排防范措施，把大多数的故障隐患消灭在萌芽之中，从而大大降低非计划停运的可能性。

电力信息系统要构筑起一道抵御外界干扰、防止连锁反应的坚固屏障。现代电网是一个高度耦合的复杂系统，局部的扰动如果处理不当，很容易造成大范围的连锁反应，甚至导致系统崩溃。为此建立了电力信息系统三道防线即安全稳定控制系统、失步解列装置、低频低压减载装置是防止事故扩大。这些系统依靠实时准确的数据来做出决定，在紧急情况下可以在数毫秒内完成切机、切负荷等稳定控制措施，就像是给电网装上了“安全气囊”和“自动刹车”，把风险消除于无形之中。与此同时，信息系统的自身网络安全防护体系就形成了一个纵深防御、主动监测、快速反应的数字长城，有效抵御了网络攻击，保障了物理电网和数字空间的双重安全，给大电网运行提供了一道坚实的数字盾牌。

（三）支撑大面积停电事故的应急处置

大面积停电事故是电力系统所面临的一大挑战，它所造成的影响广泛而深远，造成的经济损失也非常巨大。电力信息系统在大面积停电事件中起到的中枢指挥、决策支持作用是不可替代的。它穿插在应急管理的全过程之中，即预防、准备、响应、恢复，是科学、有序、高效应对的根本保证。信息系统在事故发生之前就可以对各类应急预案实施数字化的管理、推演和动态调整，对应急抢修队伍、应急物资、备用电源等资源进行信息化管理，保证随时可以投入使用。

一旦大面积停电事故不幸发生，信息系统便成为应急指挥中心的“眼睛”和

“大脑”。

1. 该系统可以迅速融合电网信息、地理信息、社会信息，把停电范围、重要用户（医院、交通枢纽等）的状态、电网关键断面、可用电源点等信息显示在同一张地图上，为指挥决策提供全面、实时的态势感知能力。

2. 应急资源的统一调度，在应急指挥平台支持之下，能够对抢修队伍、车辆、物资、专家实施可视化指挥、扁平化调度，打破部门壁垒，使跨区域、跨专业的救援力量能在最短时间内抵达最重要的地方。

3. 恢复方案的科学制定。信息系统在黑启动和电网恢复中承担着重要的计算仿真任务，可以模拟所有的恢复路径，评价方案的可行性和安全性，避免恢复过程中由于操作失误造成的二次冲击或者设备损坏，指导调度员按照“先主干后分支，先重点后一般”的原则，安全、有序、快速地恢复供电。

事故处置结束之后，由信息系统所保存下来的完整过程数据，为后来对事故展开深入剖析、探究原因乃至追责，赋予了客观的根据。对整个事件进行复盘，可以发现应急预案和管理流程中存在的不足，进而不断改进，形成一个“分析 - 学习 - 提升”的闭环管理体系，不断强化电网抵御极端灾害的能力。信息系统把分散、隔离的信息孤岛有效地联系在一起，大面积停电事故不再是一场混乱的“遭遇战”，而是一场有准备、有组织的“合成战”。

二、提升电力企业运营管理效率

电力信息系统的创建，既牵涉到电网的安全，也是促使电力企业内部管理革新，缩减运营成本，提升经济效益，达成高质量发展的重要推动力。依靠数字化手段再造企业业务流程，最大限度地挖掘数据价值，全面提高企业管理的精细化程度，提高企业的市场竞争力。

（一）优化业务流程，降低运营成本

电力企业属于资产密集型、流程密集型，传统的运营模式存在着部门壁垒森严、信息流通不畅、人工操作繁琐、运营效率低下的状况。电力信息系统建设的重要目的之一就是消除信息孤岛，实现业务流程在线、自动、智能。ERP、EAM、SCM、HRM 等一系列一体化信息系统把原本分散的规划、基建、生产、营销、财务、物资等各个方面的数据和流程整合在一起，形成一个高效的协同运作的企业运营整体。设备的采购需求是生产系统检修产生之后，物资系统进行库

存查询、招标采购以及控制预算支付结算等，在资产体系中完成建档入账的工作。全程透明，无缝对接，降低部门间沟通成本，缩减业务操作时间。

流程优化带来的经济成本节约十分明显。电子化审批取代纸质单据流转带来的纸张、打印、存储开支大幅缩减，最重要的是决策速度加快了。物资管理智能化利用精准的需求预测以及库存分析，从而做到对备品备件的经济库存管理，防止出现物资积压和浪费的情况。工程项目管理信息化系统可以对工程项目的进度、成本、质量、安全实行全过程精细化管理，能及时发现问题并智能预警，有效规避了工程项目的超概算、超工期风险。对企业自身电、热、水、气等能源消耗实施在线监测与分析，有利于制定并采取更有利的节能举措，进而缩减运营能耗。电力信息系统是一台强大的流程再造机和成本压缩器，把精益管理的理念渗透到企业运营的每一个环节中，从而系统性地降低企业总体运营成本。

（二）实现精细化管理与科学决策

电力信息系统的创建给企业积累了前所未有的数据资产。精细化经营、科学决策的关键就是把大量数据转变成深刻洞察、明智行动。现代电力信息系统的架构，尤其是数据中台的创建给这个目标赋予强大的科技支持。数据中台可以对来自各个业务系统的大量异构数据进行统一采集、清洗、整合、治理，从而产生出标准、规范、可复用的数据资产和服务，给上层各种应用提供高质量的数据弹药。因此企业管理也由原来的依靠经验、直觉、局部信息的粗放式管理，变为以数据为驱动的精细化、精准化管理。

资产管理领域中，精细化就是由原来的“计划性维修”向“状态检修”和“预测性维护”转变。信息系统把设备的在线监测数据，离线试验数据，运行工况，环境数据等各种信息归集起来，用大数据分析和故障诊断模型，精确地对每台设备的“健康状况”作出评判，预估它将来发生故障的概率以及还能使用多少时间。企业可以对症下药，只对确实存在问题的设备进行维护，避免了过度维修造成的资源浪费，又能有效预防由于维修不足而引起的突发故障，实现了资产效能和投入成本的最佳平衡。

信息系统是管理层进行科学决策的有效工具。企业高管能够随时对企业的售电量、线损率、利润以及投资回报率等重要关键绩效指标进行深入分析，然后由表及里地去寻找影响数据的因素。当某区域线损率出现较大异常时，系统就会关联该区域的负荷特性、配电变压器运行情况、用户有无窃电嫌疑等信息，从而帮

助管理者准确找到问题所在。对于新建电厂、输电线路项目这类重大投资决策，信息系统可以开展复杂的潮流计算、经济性分析、风险分析等，给企业决策给予全面、客观的科学支撑，进而规避投资风险，保障企业战略目标的达成。

（三）提升客户服务质量和满意度

伴随着电力市场化改革的不断深化，客户满意度成了评判电力企业核心竞争力的主要指标。电力信息系统形成起现代化的客户服务体系，全面改变电力企业同用户之间的互动方式，明显改善了服务品质，优化了客户体验。以前用户办理业务必须到营业厅排队，查询信息只能拨打客服热线，体验单一，不便。以网上国网等移动应用为代表的线上服务渠道，在强大的信息系统支撑下，把电力服务浓缩到用户指尖。用户可以随时随地通过手机 APP、微信公众号、网上营业厅等途径办理电费查询、账单查询、用能分析、业务报装、故障报修等几乎所有的业务，真正实现了“一次都不跑”的便捷服务。24 小时不间断服务模式能够很好地适应现代社会快节奏、个性化的服务需求。

信息系统给消费者带来的服务质量改善，并不是简单的销售渠道更加便利，而是表现在服务变得智能化、主动化、个性化等各个方面。对用户用电行为数据进行深入分析之后，系统能够为用户提供详细的用电账单，并展示其用电量、峰谷用电比例等信息，并且同同类用户进行比较，从而为用户提供节能建议以及电价套餐推荐。在计划停电或者突发故障的时候，系统可以利用短信、APP 推送等形式，提前或者实时地将停电信息准确地告知受影响的用户，并且动态地更新抢修的进度，彻底改变了过去用户被动等待的局面，大大减轻了用户在停电期间的焦虑情绪。对企业的电能质量监测、负荷预测、需求侧响应指导等增值业务，电力信息系统也能为企业提供，有利于企业改善其用电结构、降低用电成本。从单一电力供应商变成综合能源服务商，只有强有力的信息系统才能更好地了解用户的需求、为用户提供更加贴心有价值的服务、与用户建立互信的关系。

三、推动能源革命与可持续发展

电力信息系统不只是电力行业的一项业务支撑工具，而且是关系到我国能源革命的一项国家战略，是实现我国“双碳”目标和社会可持续发展的重要基础设施。它给能源的生产、传输、消费、存储增添智慧基因，进而成为创建清洁低碳、安全高效现代能源体系的数字根基。

（一）支撑新能源大规模并网消纳

以风电、光伏等新能源是未来能源供应的主体，但是其固有的随机性、波动性、间歇性给电力系统的安全稳定运行带来巨大挑战。怎样才能做到大规模新能源的可靠并网和高效消纳，这是能源革命面前首先要面对的难题。电力信息系统为此提供系统的解决办法。

1. 精确功率预测，先进的电力信息系统整合了数值天气预报、卫星云图、场站实测数据和人工智能算法，可以对未来数小时到数周的风电、光伏出力做出高精度预测。这样预测的能力给电力调度机构提前安排常规电源启停、调节火电出力曲线、规划抽水蓄能等调节资源的运用提供科学依据，从而给新能源接入电网预留最大的空间。

2. 智慧化调度控制。新能源出力变化无常，传统的人工调度已经无法适应。新一代智能调度系统计算能力很强，可以对电网潮流实施滚动优化计算和安全校核，在分钟级或者秒级的时间尺度范围内，自动调整电网运行方式，协调控制水电，火电，储能等多种类型的灵活性资源，迅速平抑新能源波动，保证电网频率和电压稳定。

3. 友好型并网管理，依靠新能源场站内监控系统和协调控制系统，对单个风机、光伏逆变器实施精细化控制，使其可以主动支持电网运行，参与调频、调压、提供惯量支撑等，由单纯的电能发出者转变为电网的友好型参与者，极大提高了电网接纳新能源的能力。

依靠这些信息技术的综合运用，电力信息系统很好地化解了新能源并网带来的不确定性，突破了消纳难题，为我国风电、光伏装机容量的飞跃式增长形成了强大的技术支撑，成为推动能源结构朝清洁低碳方向转变的重要“稳定器”。

（二）促进源网荷储互动与能源优化配置

传统的电力系统是“源随荷动”的单向模式，即发电侧被动地跟随用户侧的负荷变化。但是随着新能源占比越来越高，这种方式就越发僵化低效。电力信息系统通过建设先进的通信、计算、控制平台，正在孕育一个源、网、荷、储多元协同、双向互动的新能源生态。电力用户不再只是能源的消费者，而是具有主动参与电网调节能力的“产消者”。利用智能电表和需求响应信息平台，工业用户、商业楼宇、居民家庭等可以响应电网的实时电价或者激励信号，在用电高峰期主动降低或者推迟非必要的用电负荷，也可以用自身储能设备和电动汽车充电桩向

电网反向供电。

这大大提高了电力系统灵活、经济。它把用户侧分散的海量可调资源聚集起来，形成一个巨大的“虚拟电厂”，它的调节能力可以跟大型发电厂相媲美，可以很好地平抑新能源的波动，可以延缓甚至避免对电网基础设施进行昂贵的投资扩建。信息系统作为实现这一切的“神经中枢”，发布价格信号、计量响应电量、协调控制策略、结算补偿费用。它把发电侧常规电源、新能源，电网侧输配电设施，用户侧负荷、分布式电源、储能设备等所有要素放在同一个优化框架里，在安全的前提下以全局最优为目标，协调调度各方要素，使能源在更广阔的时间和空间范围内得到最优配置，最大程度地提高整个能源系统的综合效率。

（三）服务“双碳”目标实现

碳达峰、碳中和的实现是一次社会经济大转型、大变革，而电力行业绿色低碳转型也是其中的一个方面。电力信息系统在这个历史进程里是不可缺少的“计算器”、“监测器”、“优化器”，给实现“双碳”目标赋予了明晰可行的数字化道路。信息系统是碳排放精准计算的前提。通过建立能源生产，传输，消费全环节的碳排放监测核算体系，系统可以对每一个发电企业，每一条输电线路，每一个用电客户产生的碳排放数据进行实时追踪和分析，实现碳足迹的全景穿透式管理，并以可视化的方式呈现出来。给政府制定碳排放政策、企业开展碳资产管理、市场进行碳交易提供真实可靠的数据支持。

信息系统是实现全社会节能增效的最主要手段。供给侧，信息系统对调度进行优化，先用清洁能源，减少化石能源的消耗。消费侧依靠需求侧管理、综合能源服务推广等手段，促使用户养成绿色低碳的用电习惯。借助能源互联网平台可以实现工业园区、大型公共建筑中电、热、冷、气等多种能源形式的用能的综合监控和智能调节，从而更好地挖掘出节能潜力，达成能源梯级利用以及能效最大化的目的。

从深层次来说，电力信息系统搭建起了以新能源为主体的新型电力系统的“数字孪生”。在虚拟数字空间里，可以模拟、推演各种能源政策、市场机制、技术路线对于碳减排的影响，评价其成本效益，进而找到实现“双碳”目标的最佳途径。它把宏伟的战略目标拆解成一个个可以量化、可以执行、可以考核的数字化任务。因此电力信息系统的创建与发展，不但是技术问题，更是关系到能否如期实现“双碳”目标、中华民族能否走上可持续发展道路的重大战略性问题。它正给这场深刻的绿色革命提供最坚实的、最有力的数字引擎。

第二章 电力信息系统需求分析

电力信息系统搭建不能只是功能的简单叠加，它是一项以业务需求为导向的复杂工程。因此各项业务信息化程度进行全面、深入和准确的分析，对于系统建设能否成功具有决定性意义。本章主要从电力行业的发电、输变电、配用电、管理决策这 4 个核心业务领域入手，对电力行业信息化需求进行详细的分析，为后面技术架构的设计和功能的实现提供清晰的方向。

第一节 电力业务需求分析

电力业务贯穿能源生产、传输、分配、消费全过程，每个环节的业务特性都不相同，相应地信息系统在功能、性能、可靠性方面的要求也不同。本节将对这些业务逐个进行分析，从中找出信息化过程中最核心的需求点，从而构建出一个可以全面支持并不断改进整个业务流程的信息系统，实现技术和业务的完美融合。

一、发电业务需求

发电是电力系统生产电能的起始环节，它的安全、稳定、经济运行对整个电力系统来说十分重要。发电业务信息化需求主要是为了提高生产效率、保证设备可靠性、适应能源结构变化这三点展开的。依靠信息技术手段，做到对生产过程的精细把控，对设备整个生命周期的智能管理，对新型能源形式的高效融合，这就是发电环节信息化建设的主要目的。

（一）机组运行监控与优化需求

发电机组的运行监控和优化是保证电力稳定供应的重要环节，信息化需求就是对生产过程全方位、及时、智能化的掌控。信息系统要有强大的数据采集和处理能力，可以将来自集散控制系统的大量数据，比如机组的温度、压力、振动、转速等重要运行参数整合起来，做到实时显示并支持历史记录查询，给运行人员赋予全局态势感知的能力。

更进一步，系统还要建立机理模型和数据驱动分析模型，对机组的运行效率、煤耗、厂用电率等主要的经济技术指标进行在线计算和分析，找出偏离最优工况的原因。利用大数据分析以及人工智能算法，系统可以对设备运行参数间的隐藏联系加以发掘，从而达成对机组性能劣化早期的诊治与预知，给燃烧调节，负荷分配合等改良操作赋予准确的支持，进而优化机组的经济效益并改善其运作灵活性。

（二）设备状态检修与寿命管理需求

传统的周期性预防维修模式已经不能满足现代发电企业降本增效、提高可靠性的需要，因此向状态检修和设备全生命周期管理转变势在必行。信息系统要支持这样的转型，主要需求就是建设一个集成设备数据、维修策略和备件管理的智能化资产管理平台。这个平台第一要连上在线监测系统（油色谱，振动监测）的数据，还要连上离线巡检记录，试验记录，历史维修记录等等，形成一个完整的设备健康档案。

在此基础上，系统还要依靠先进的诊断算法和故障预测模型，不断对锅炉、汽轮机、发电机等重要设备的健康程度加以评判并打分，进而提前发出故障警报。利用振动频谱趋势分析来预测转子不平衡或者轴承磨损。同时还要有剩余使用寿命的预测功能，从而可以制订出长期的维修、技术改造和报废计划。以状态为基准的维修决策可以大大降低由于非计划停机而造成的损失，并且能优化备品备件储备，最大限度的发挥设备的价值。

（三）新能源功率预测与并网管理需求

随着风能、太阳能等新能源在电源结构中所占的比重迅速增大，其固有的间歇性、波动性、随机性给电力系统安全稳定运行带来了巨大挑战。因此对新能源场站的信息化管理有了特殊的、迫切的需求。首要的需求就是高精度的功率预测系统，该系统要结合数值天气预报、卫星云图、场内实测气象数据（风速、风向、光照强度）和发电机组历史运行数据，利用机器学习、深度学习等人工智能算法，建立短期、超短期功率预测模型，为电网调度计划的制定提供准确的输入。

此外，信息系统还要有强大的新能源并网运行监控和协调控制能力。系统要实时监测新能源机组电压、频率、有功、无功出力，保证其满足并网技术要求。当电网调度指令下达的时候，系统需要能快速准确地把功率目标分解给每一台风机或者逆变器，实现场站级功率和电压联合控制。另外，随着储能系统配置的越

来越普遍，信息系统还要加入对储能系统充放电控制的功能，采用风、光、储联合优化调度的方式，抑制出力波动，提高新能源的电网友好性和可调度性。

二、输变电业务需求

输变电环节是把发电与用电联结起来的桥梁，同时也是电力系统主网架的重要组成部分。它的信息化需求本质就是保证大电网的安全、可靠和高效运行。不仅包含对于广域分布的电网和设备状态实行无死角、高精度的实时监视，而且包含对于资产运维、工程建设的全过程实施精细化、数字化的管理，保证电网资产的健康水平和投资收益。

（一）电网运行实时监控与调度需求

电网安全稳定的运行属于输变电业务中最重要的一部分，对于信息系统的实时性、可靠性、安全性有着非常高的要求。主要表现在以能量管理系统、广域相量测量系统等为代表的高级应用上。信息系统必须可以高速地从 SCADA 系统获取全网断路器状态、线路潮流、母线电压等各种实时数据，并且可以图形化地直观显示系统当前的实时运行状况，给调度员提供全局透明化的态势感知。

基础监控之上，系统更深层次的需求就是提供强大的分析决策能力。这涉及到利用状态估计功能给出更为准确的全网运行断面，执行在线潮流计算以及静态安全分析，模拟预想事故并评判其后果，从而为调度决策给予科学支撑。系统还要具有自动发电控制、经济调度等闭环控制功能，才能实现区域发电与负荷秒级平衡、最优经济调度。电网规模变大，动态特性变得越发复杂，对动态稳定分析，暂态电压稳定评价这些高级应用的需求也变得越发强烈。

（二）设备状态评估与运维管理需求

输变电设备分布广、种类多、价值高，它的运维管理正在由传统的“巡视、检测、消缺”模式向更智能的状态驱动模式转变。信息系统要支持这样的转型，关键就是搭建起一个集成的设备资产智能运维平台。该平台要整合变压器油中溶解气体在线监测、GIS 局部放电监测等在线数据，无人机、机器人巡检采集到的图像、点云数据，人工巡视、红外测温、带电检测等离线数据。

系统要从大量的数据中挖掘出并进行智能分析。使用图像识别算法来判定绝缘子污闪、导线异物，再用数据趋势分析加上专家系统模型来对变压器、断路器等重要设备的健康状态进行量化评价并做风险预测。系统应该可以生成设备健康

指数和状态评价报告，给运维资源的分配、检修计划的制定、大修技改的决策提供数据支撑，在保证设备可靠性的基础上，最大限度地提高运维效率和效益。

（三）输变电工程全生命周期管理需求

输变电工程投资量大、周期长、技术要求高、专业多，传统运作模式不能保证信息的及时沟通、合作的高效。因此，创建一个包含工程“规划、设计、采购、施工、验收、移交、运维、退役”全生命周期的信息化管理平台，就成为迫切需要。

信息系统的建设需求具体体现在以下几个方面：

1. 设计阶段：采用三维设计、BIM 技术，实现工程设计的可视化、参数化，做碰撞检测、施工模拟，从源头上提高设计质量与可施工性。

2. 建设阶段系统要对工程进度、成本、质量、安全实施精细化控制，依靠移动应用、物联网等技术实时获取现场数据，实现项目管理动态跟踪、协同作业。

3. 运维阶段：系统要无缝承接竣工模型和数据，将其当作数字孪生体，同实时运行数据融合起来，给设备维护，状态评定，技术改造赋予基本支撑，从而达成设计，建设，运维数据的连续性，一致性，冲破信息孤岛。

三、配用电业务需求

配用电环节是电力服务的最后一公里，直接面对广大电力用户，业务特点是多点、面广、对象复杂。随着分布式能源、电动汽车等新型用能方式的加入，配用电业务的信息化需求也出现新的发展方向，自动、互动和智能化，从而达到提高供电可靠度、改善客户体验、促进能源高效利用的目的。

（一）配电网自动化与自愈控制需求

现代配电网向着高可靠、高互动发展，对配电网自动化和智能化水平的要求也变得越来越高。配电网自动化的核心信息需求，就是建立一个可以快速处理故障、可以自我修复网络的智能系统。该系统需要实时采集配电网中的开关、环网柜、配电变压器等设备的状态信息和电气量信息，并具有很强的拓扑分析能力，实时掌握配电网的运行方式。

当线路发生故障的时候，系统就要和馈线自动化终端、站所终端这些智能设备配合起来，在毫秒到秒的时间里，把故障的位置找出来，快速地把故障的部分隔开，把其他还能用的设备上的负荷转移到别处去，就叫做自愈。这可以大大缩短停电时间，提高用户的供电可靠性。系统还需要保证配电网良好运行，即网络

重构、负荷平衡、网损最小化等等，使得系统更加经济、安全。

（二）用电信息采集与负荷管理需求

用电信息采集是实现电网与用户互动的前提，也是电网各项营销、计量、调度业务的数据来源。其主要需求就是建立一个对所有用户、稳定可靠的用电信息采集系统，也就是高级计量架构。该系统要能对智能电表数据进行定时、实时、随机采集，除了用户电量数据外，还要包含电压、电流、功率因数等电能质量数据，从而达到对用户用电情况全方位感知的目的。

完成数据采集之后系统应具有很强的数据管理和分析功能，可以对大量的数据进行存储、校验、估算和补采。根据采集到的数据进行分析可以支撑线损精细化管理、窃电嫌疑分析、三相不平衡治理等业务。更重要的是这些负荷数据是需求侧管理、需求响应的基础。系统应该可以支持分时电价、阶梯电价等各种灵活的电价策略的发布和执行，给用户削峰填谷、参与电网互动提供技术支持，从而提高整个电力系统的运行水平。

（三）客户服务与营销管理需求

在电力市场化改革和服务业导向理念转变的影响下，电力营销、客户服务的信息化需求，从最初仅仅满足于业务处理，向以客户为中心提供智能化、多样化服务转变。核心需求就是构建一个集客户关系管理、计量计费、账务处理、线上服务渠道为一体的营销信息平台。该平台要实现客户档案、业扩报装、合同、抄表、核算、收费、账务等主要营销业务全流程线上管理，保证业务流程规范高效、数据准确一致。

同时为了提高客户体验，全渠道客户服务中心需要具备很强的功能，将营业厅、95598 热线、网上营业厅、手机 APP、微信公众号等所有服务渠道整合在一起，提供业务办理、电费查询缴纳、信息订阅、故障报修等一站式便捷服务。深层次需求即大数据分析之后，对用户的用电行为和服务需求进行画像，精准营销、推送个性化的服务，预测客户的需要，从而提高客户满意度和忠诚度。

第二节 系统功能需求分析

系统功能需求分析是电力信息系统建设的基础，它准确地刻画了系统应该具有的功能，直接决定系统是否能够满足电网调度、运行、管理等核心业务的实际需求。本节主要从核心业务、辅助管理、未来扩展这三个方面，对电力信息系统的功能需求进行系统的阐述。

一、核心业务功能需求

核心业务功能是电力信息系统价值的集中反映，是直接为电网安全、稳定、经济运行提供服务的功能。这些功能是系统的“骨架”，可以随时掌握电网运行状态并及时作出反应，是保证电力供应可靠性的“技术大脑”。

（一）数据采集与监视控制 SCADA 功能

数据采集和监视控制，也就是 SCADA 功能，是电力信息系统的“感官”和“神经末梢”。它就如同电网的眼睛和耳朵，不间断地从电网各处，变电站、发电厂、开关站等，采集大量的遥测、遥信、遥脉数据。遥测数据包括电压、电流、有功功率、无功功率等模拟量，可以反映电网的实时运行情况；遥信数据是断路器、隔离开关等设备的开关位置状态，是判断电网拓扑结构的基础；遥脉数据一般指电能量的累计值。系统必须具备高可靠、高实时的数据采集能力，支持多种通信协议和传输通道，保证数据的完整性、准确性，给上层应用提供可靠的数据支撑。

监视功能就是将采集到的数据用直观、易懂的方式显示给调度运行人员。一般采用图形化的人机界面 HMI 来实现，在地理接线图、主接线图、厂站图上实时刷新数据和设备状态。系统应该能够实现画面的缩放、漫游、导航等功能，并且可以对设备进行定位以及关联数据查询。关键数据的越限或者变位应该用醒目的颜色、闪烁、声音等方式来提示，以便运行人员第一时间发现电网异常。趋势曲线、棒图、数据表格等监视方式也不可或缺，它们给运行人员赋予了从多个角度认识电网运行趋势的手段。

控制功能是 SCADA 系统的“手臂”，是调度中心对远方设备进行远距离操作的能力。这主要是断路器、隔离开关的遥控分合，变压器分接头的遥调，发电机组出力的遥调等。由于遥控操作关系到电网安全和人身安全，其功能需求应该把安全性放在首位。系统必须要具有严格的操作权限校验，采用“选择 - 返校 -

执行”的操作闭环流程，防止误操作。对关键操作要设置双重确认。所有遥控操作，不论成功或失败，都必须做好记录，记录操作人、操作时间、操作对象和操作结果，以备日后查考分析。

（二）数据处理与分析计算功能

数据处理以及分析计算功能相当于电力信息系统的“大脑”，会把最初态的，分散开来的数据变成更有用的，系统化的资讯，而且它还是做决策支撑的关键基础。就是对大量的实时数据以及历史数据加以深度加工并实施智能分析。实时数据处理主要是对采集数据进行有效性检验、量纲变换、坏数据识别剔除等预处理工作。在此基础上系统可以实时计算线路功率因数、负载率、电压合格率等派生量以及关键断面潮流计算等，计算结果可以更好的反映电网运行状况。

高级应用分析属于数据处理功能的重要组成，对电网的经济、优化运行起到关键的支持作用。这部分功能一般包含状态估计 SE。它依靠冗余量测数据，凭借最优化算法算出整个电网最可能的运行状况，给所有别的分析应用供应一个统一的，精确的，完整的实时网络模型。根据状态估计的结果，可以进行潮流计算、静态安全分析 N-1 校验、最优潮流等计算。高级应用可以预知电网在各种运行方式下的情况，评判可能存在的运行风险，找到最优的控制策略，在保证安全的基础上，尽可能地降低网损，提升输电效率。

历史数据的处理和分析也不能忽略。系统必须要有很大的历史数据库，可以快速存取数年甚至更长时间的历史运行数据。系统应该依据历史数据来提供各种分析工具。比如负荷预测功能，它依靠历史负荷数据、气象信息、社会经济指标等，经由统计算法或者人工智能模型，来预测未来一段时间的电力需求，进而给发电计划和调度方案的制订赋予有力支撑。设备运行状态评价、故障信息统计分析、运行指标考核等功能实现都需要依靠挖掘历史数据来获得支持，从而为电网规划、设备维护、管理决策提供数据依据。

（三）事件告警与操作控制功能

事件告警、操作控制功能属于电网安全运行的重要部分以及规范操作的手段。可以及时响应电网的各种动态变化，给运行人员提供标准化的安全交互方式。事件处理的功能是系统对于电网中所发生的各种状态变位，数据越限和保护动作等事件作出正确的记录。对高精度的顺序事件记录 SOE 来说，系统必须保证毫秒级的时间分辨率，这样才能在故障发生之后，准确地还原出事故的过程，给故障

分析赋予可靠的根据。

告警功能是事件处理的延伸，可以对大量的信息进行筛选，从而找出运行人员必须马上处理的告警事件。系统应该支持灵活的告警定义，对告警进行分级，并用不同的声光提示方式来区分告警级别。为了防止电网发生大规模扰动的时候，系统出现“告警风暴”把关键信息淹没的情况，系统还需具有告警抑制、告警过滤的功能。按照电网拓扑关系，对因同一个根本原因造成的多个关联告警进行抑制，只保留根本原因告警。告警的确认、屏蔽、恢复等全生命周期管理也是不可缺少的，保证每一个告警都能得到妥善处理。

操作控制的规范化管理是防止人为失误、保障电网安全的重要防线。

1.1、操作票、工作票管理功能，实现操作任务的全流程电子化。从操作票生成、审核、模拟预演、现场执行到归档，系统都应该有标准的模板和流程引擎，保证每一个步骤的操作都符合规程。

2. 防误闭锁功能对于保证操作安全十分重要。系统应该内嵌强大的逻辑引擎，根据实时电网拓扑以及预设的“五防”规则，对每一个即将执行的遥控或者就地操作进行实时的检查。系统会及时闭锁，发出明显的警告信息，从源头上杜绝因为错误的操作而发生的事故。

3. 操作和事件追溯记录，为运行责任制打下基础。系统必须以不可篡改的形式记录下每一个用户的登录、退出、画面调用、参数修改、控制命令下达等所有的行为，构成完整的行为日志，作为事故调查和责任认定的依据。

二、辅助管理功能需求

辅助管理功能是指对电力信息系统自身稳定运行、高效管理、便捷使用起到支撑作用的功能。虽然它们不直接参与电网控制，但是是系统可用性、安全性、可维护性的保证，为系统核心业务功能的正常运行打下基础。

（一）系统运行管理与权限控制

系统运行管理即对整个电力信息系统本身进行监督管理。系统应给提供一个集中监控仪表盘来实时显示服务器的 CPU 使用率，内存占用情况，磁盘空间，网络带宽等重要的指标。系统中各类服务和应用程序都必须具有心跳检测和状态监视功能，服务中断或者出现异常时，应当立刻报警并且尝试自愈。系统还要具有监控网络设备、数据库、中间件等基础环境的能力，从而建立起立体的、全方

位的运维监控体系，保证问题能够被及时发现和定位。

权限控制是电力信息系统安全的基础，其主要目的就是保证“正确的人在正确的授权下做正确的事”。系统必须用基于角色的访问控制 RBAC 模型。管理员可以预先设置调度员、工程师、系统管理员、浏览用户等不同的角色，再对每一个角色的权限进行细致的分配。这就简化了用户管理、提高管理效率和安全性。人员岗位发生改变时，只需要对人员所对应的角色进行修改，不需要一个一个地去调整具体的权限。

权限的颗粒度需要足够小，才能跟上复杂的管理需求。它不仅要控制用户可以访问哪些模块、哪些画面，还要控制数据和操作。可以控制某个用户对某一个厂站的遥测数据只读，而不能看到其他厂站的数据；或者允许某位调度员只对本地区的线路进行遥控，不能操作其它地区的设备。所有权限修改和用户增删等敏感操作都需要产生审计日志，可以追溯。

（二）报表统计与信息发布

报表统计功能的作用就是将系统中大量的数据转化为结构化的、有价值的信息，为管理决策、运行分析、对外汇报提供支持。系统应具有强大的报表引擎，用户可以用拖拽的方式来自定义报表模板，用户可以自由地选择数据源、统计周期和表现形式（表格、曲线图、饼图等）。报表内容应包括电网运行的各个方面，负荷曲线报表、电量平衡报表、电压合格率统计、设备利用率分析、告警事件分类统计等。

为了提高工作效率，报表功能应该自动化。用户可以设定报表的生成规则，比如日报每天零点自动创建，月报每月初自动汇总。系统应该可以自动抓取所需数据，进行处理，排版，最后生成指定格式的文件（PDF、Excel、Word 等）。报表生成之后可以采用自动打印、邮件发送、网络共享目录推送等分发方式。这样自动化的能力就可以把运行人员从繁重、重复的报表制作劳动中解放出来，让他们更多的参与到电网运行当中。

信息发布功能是系统与外界用户联系的纽带。系统应该具有一个内部的信息发布门户或者接口，使经过授权的用户能够方便、快捷地将系统内部的重要信息、统计报表、运行简报等发布到公司内部的办公自动化系统、门户网站或者其他信息平台。有益于打破信息孤岛，达到跨部门的信息共享、业务协同。发布功能要有一些格式转换和内容适配的能力，保证信息在不同的平台上展示效果不错。

（三）系统配置与维护工具

系统配置与维护工具，是保证电力信息系统能够长久、稳定和高效运行，并且可以随着电网的发展作出改变的必要手段。提供一套图形化的、一体化的配置工具集是十分必要的，可以大大降低系统的维护成本以及对原厂商的依赖。其中数据库建模以及组态工具最为重要。电网的设备和拓扑结构不断变化，新建或改造变电站的时候，维护人员借助图形化界面就能轻松地添加或者删除设备模型，配置数据点（遥测、遥信等），设定通信参数，不需要编写繁琐的代码或者直接对数据库表进行操作。

除数据库配置外，其它各种维护工具也不能缺少。人机界面画面组态工具可以像使用绘图软件一样绘制、修改主接线图、地理图等图形元件，并将图形元件与数据库中实时数据点联系起来。通信前置机和通道配置管理工具，用以管理远动终端的通信链路和规约。系统应提供备份和恢复工具，可以实现系统配置、实时数据库、历史数据库等的定期自动备份和手动一键恢复，在系统出现灾难性故障的时候能够迅速重建系统。诊断工具集，报文监视、日志分析、网络诊断等都是维护人员快速定位问题、解决问题的利器。

三、扩展功能需求

随着技术的发展和业务需求的深入，现代电力信息系统已经不能是单独的监控平台，要具有良好的扩展性，能够满足“大云物移智”（大数据、云计算、物联网、移动互联网、人工智能）等新技术发展的需求，也能与其他业务系统深度整合，创造出更大的价值。

（一）与其他系统的接口与集成

电力信息系统属于生产控制领域的大脑，要拥有很强的开放性以及互联互通能力，从而冲破信息壁垒，达成数据横向与纵向的流动。系统要给出标准的数据接口，方便和其他重要的业务系统相连接。GIS 地理信息系统的集成之后，可以将电网设备当前的实时运行状态叠加在地理图层上面，达到设备和地理位置以及运行状态之间联动分析的目的。与生产管理系统 PMS、资产管理系统 AMS 集成以后可以实现设备台账、检修记录和实时工况之间的互动，给设备状态检修和全生命周期管理提供数据支持。

为了达到广泛集成，系统设计要遵循行业内通用的标准规范。可以采用以服

务为基础的架构 SOA 或者微服务架构，将系统的各项功能封装成独立的服务，通过企业服务总线 ESB 或者 API 网关对外提供。数据交换上优先采用国际电工委员会 IEC 制定的公共信息模型 CIM/IEC61970、IEC61850 标准和 OPC UA 等通用工业数据交换协议。标准化接口与数据模型可以大幅度降低异构系统集成难度与成本，使电力信息系统真正成为企业级数据枢纽，为企业级分析应用和统一决策平台提供数据来源。

系统之间进行集成，不只是数据之间的交流，更深的程度是业务流程之间的协作。当 SCADA 系统检测到某个设备出现故障告警时，就可以通过接口自动生成一条缺陷记录或者维修工单，并将该条记录或工单通知给相应的维护人员。调度计划系统制定出新的日发电计划，可以自动下达给电力信息系统作为机组出力调整的依据。跨系统业务流程自动化可以大大提升电网运行效率和响应速度。

（二）移动应用与远程访问

随着移动互联网技术的发展，将电力信息系统延伸到移动终端已经迫在眉睫。移动应用主要是面向现场运维人员、管理人员、值班工程师，可以随时随地获得重要的电网运行信息。移动端要提供关键断面潮流、重要厂站电压、主变负载率等重要数据的实时监视。并且要支持告警信息的实时推送，移动端可以对告警信息进行确认。查询功能也必不可少，比如设备参数查询、历史曲线查询、操作票和工作票信息查询等，给现场工作提供方便。

移动应用设计时就必须考虑到移动设备的特点。用户界面 UI 简单，交互设计 UX 方便单手操作，自适应不同大小的屏幕。由于现场网络环境具有不确定性，所以移动应用需要具有离线数据缓存和断线重连的功能，保证移动应用的基本功能可以正常使用。数据展示要突出重点，不要在小屏幕上显示太多信息，多用图形化、仪表盘式的展示方式。

移动应用和远程访问的生命线就是安全。由于数据需要通过公共网络进行传输，所以必须建立端到端的立体安全防护体系。需要建立安全远程接入通道，一般用虚拟专用网络 VPN 技术加密传输数据。用户认证可以采用多因素认证 MFA 的方式，即密码加手机验证码或者指纹识别来提高身份验证强度。移动设备自身也应该对应用程序以及本地缓存的数据进行加密，并且具备远程擦除数据的功能，防止移动设备丢失或者被盗后导致信息泄露。后台对所有的移动访问行为都要做严格的权限控制以及日志审计。

（三）三维可视化与仿真模拟

三维可视化技术给电力信息系统带入了全新维度，以物理电网为依托创建起数字孪生体，将二维平面图纸升级成了逼真的三维模型。主要的应用场景之一就是变电站的三维可视化。系统对变电站进行精细化建模，可以 1:1 还原站内所有的设备、构架、电缆沟等，并且可以将 SCADA 系统采集到的实时数据（刀闸状态、设备温度、实时电流等）叠加渲染到三维模型上，实现“所见即所得”的沉浸式监控。这大大加强了运行人员对于设备空间排列及运行情况的直观认识。

三维可视化不仅用于监视，对培训和运维也有重大意义。对于新员工培训，可以在虚拟的三维变电站中进行设备认识、巡视路线、模拟操作等训练，安全又高效。运维人员进场前可以根据三维模型规划好工作路线，了解设备内部结构、模拟拆卸过程等，利用增强现实 AR 技术把维修指导信息叠加在真实的设备上，提高工作精确性、安全性。

仿真模拟功能是电力信息系统由“监视控制”向“预测决策”的飞跃。它依靠精确的电网模型，给运行人员提供一个可以交互的“沙盘推演”环境。调度员要执行一项复杂或者风险较大的操作时，可以先在仿真环境里模拟这个操作，系统就会迅速算出并显示这个操作可能会引发的潮流转移，电压波动，稳定性破坏等影响。这种预执行的能力给决策人给予以前所未有的洞察力，可以规避危险。仿真功能也成了调度员培训、反事故演习的有效手段，在不影响实际电网运行的前提下，可以模拟各种极端故障，提高运行人员的应急处理能力。

三维可视化 + 仿真模拟技术结合之后，电网的运行管理就不再只是平面的、被动的，而是立体的空间上的、主动的预测，不再是单向度的信息展示，而是交互式的体验。先进的工具可以提升运维效率，从根本上提高电网的安全性、韧性及智能化水平。

为了更直观地理解这些高级功能在电力系统中的应用层次与价值，可以参考以下表格：

电力信息系统高级功能应用价值表

功能类别	核心价值	主要应用场景	技术特点	提升效果
三维可视化	直观展示、辅助决策	变电站空间管理、设备运维、培训	数字孪生、实时数据叠加、沉浸式体验	提高空间认知、缩短培训周期、优化维护流程
仿真模拟	风险预演、策略优化	复杂操作评估、事故演习、调度培训	精确电网模型、实时计算、交互式沙盘	降低运行风险、提升决策质量、强化应急能力
移动应用	灵活访问、现场支持	现场巡检、告警确认、移动办公	离线缓存、跨平台、多因素认证	提高响应速度、增强工作便捷性、打破时空限制
系统集成	互联互通、业务协同	与 GIS/PMS/AMS 对接、信息共享	标准化接口、服务化架构、数据模型统一	消除信息孤岛、优化业务流程、提升系统整体效能

第三节 性能指标需求分析

性能指标是对电力信息系统好坏的度量标准，需求分析是否深入、准确决定着系统建设的成败和最终运行的效果。好的系统不仅可以极大地改善用户体验，还可以给电网核心业务稳定高效地运行提供可靠的保障。本节主要从实时性、可靠性、并发处理能力这三个核心性能指标出发，对电力信息系统在这些方面具体的要求进行详细的分析。

一、实时性指标需求

电力系统安全稳定运行要依靠信息的实时传递和处理。电网运行状况瞬息万变，信息滞后就会造成误判，甚至错过最佳处理时间。因此实时性成了电力信息系统性能需求分析中首要考虑的因素，直接影响系统对于电网动态的感知、响应和控制能力。

（一）数据采集与刷新周期

数据采集刷新周期是电力信息系统实时性的一个基本度量标准，代表系统对于电网物理状态变化的感知时间粒度。拿电力调度自动化系统来说，远动信息，比如开关位置，电压，电流，有功功率等等，其采集周期也是十分重要的。常规的 SCADA 系统数据刷新周期为 2 到 10 秒，即从远动终端采集数据、前置机处理、数据库更新、界面呈现整个过程必须要在规定的时间内完成。

广域相量测量系统数据来源是 PMU，数据刷新率要求更高，一般为每秒 25

次到 100 次，即刷新周期为 40 毫秒到 10 毫秒。高频数据采集给电网动态稳定分析以及低频振荡监测打下了基础，但是也对系统的网络传输带宽、数据处理吞吐能力、存储能力提出了严峻的挑战。需求分析阶段要按照监测对象的特性以及分析应用的实际需要，确定各种数据类型的采集及刷新周期。像变电站的保护信息、故障录波数据，时间分辨率要是毫秒级的，才能把故障的过程真实的展现出来。但对于营销或者资产管理系统中的电能量数据，刷新周期可以做到分钟级、小时级甚至天级。因此差异化、精细化的周期需求定义是系统设计的前提。

需求分析阶段就要设置固定周期性指标，电网遇到扰动或者故障等非正常工况时，还得保证关键数据能够实现动态加密传输。系统应当依照实际情况作出数据采集策略的动态改变，从而使得当信息需求最为急迫的时候，以最高效的方式去获取关键数据。这就意味着系统在架构设计的时候要具有一定的灵活性和弹性，从而可以适应不同场景下的实时性需求差别，保证决策的及时性。

（二）命令下发与响应时间

命令下发与响应时间属于电力信息系统控制能力的准则指标，它是从操作员发出控制指令开始，一直到远方设备执行动作并予以确认为止的全部时间。直接影响电网事故处理、运转方式改变的效率和安全度。对电网调度控制来说，遥控操作（分合断路器）和遥调操作（调节发电机出力、调整变压器分接头等）成功率和响应时间都不能出现任何差错。

关键设备遥控命令下达到响应设备的时间一般是秒内。具体而言，从调度员在主站系统的操作按钮上点击一下，直到远方的开关设备动作完毕并把状态变位信息反馈到主站，这个闭环过程应当在 2 ~ 5 秒之内完成。其中包含了主站系统自身处理的时间、网络信道的传输延迟、远动终端或者智能设备执行的时间、状态返回的传输和处理时间。需求分析环节，要对各个环节的最大允许耗时实施细致的分解并予以明确的界定，从而给系统的设计、设备的选择以及网络的规划赋予可靠的依循。响应时间过长，会使得调度员不能及时对电网故障做出干预，倒闸过程中还会出现不协调动作，造成电网安全隐患。

定义此项指标时还要考虑命令的优先级。以紧急事故处理遥控命令（切除故障线路）为例，其优先级最高，系统必须保证这种情况下，其它常规业务数据不能对它产生任何影响。这就需要系统有服务质量保证机制，在网络和处理资源紧张的时候优先服务高优先级的控制指令。对批量下发或者顺序执行的控制序列来

说，系统还要保证其时序的正确性以及执行的确定性，防止由于指令乱序或者执行延迟造成逻辑混乱。

（三）事故告警与处理时间

事故告警和处理时间就是电力信息系统在遇到异常或者故障的时候，应急能力的一种体现。它是指从电网事件发生、被监测设备检测出来、告警信息在主站系统界面上声光显示、相关人员确认处理的全过程所经历的时间。此指标的好坏直接关系到运维人员是否能在故障发生初期介入，从而抑制故障的发展，减少停电损失。

具体而言，该指标可分解为以下几个关键时间节点：

1. 告警产生到传输的时间，即现场设备发现异常（如电压越限、保护动作）到告警信息到达主站服务器所用的时间。对于重要的告警，应该小于 1 秒。这就要求底层采集网络具有低延迟、高可靠的特点。

2. 告警处理和入库时间：主站系统接收到原始告警信息之后，需要对其进行解析、定性、关联分析（告警根源分析），然后存入实时或者历史数据库等一系列处理过程。该过程应当在几百毫秒内完成，以保证信息可以及时推送给上层应用。

3. 告警显示和通知时间，告警信息在数据库中就绪后，应立即在调度员或集控中心的操作界面上用最醒目（闪烁、变色、弹窗）的方式显示，并有声光提示。系统还应该使用短信、App 推送等多种方式通知有关责任人。从信息入库到用户感知，整个过程理想上不能超过 1 秒。

需求分析要确定各级告警的处理时间需求。对于直接威胁电网主设备或者人身安全的严重告警，端到端处理时间必须达到最严格的标准。而对于一般的提示性告警，时间要求可以放宽一些。系统设计要形成完备的告警分级、过滤及抑制体系，防止电网碰到大扰动时产生“告警风暴”，淹没重要的根源告警信息，妨碍调度员的判断和决策。

系统要给出详细的告警处理日志，把告警出现的时间，推送的时间，人员确认的时间，措施执行的时间等都记清楚，形成一条完整的事件追查链条。这些日志不但是事后事故分析的重要依据，也是改进系统性能、优化运维工作方式的量化指标。经过对上述时间的统计分析，可以找到系统或者管理流程中的瓶颈，从而进行有针对性的改进，不断提高系统的整体应急响应水平。

二、可靠性指标需求

电力信息系统属于保证电网安全运行的关键性基础设施，它的可靠性是不能动摇的基石。系统中哪怕出现很小的故障或者数据错误，都会被放大，给电网运行造成严重影响，甚至引发大面积停电事故。所以系统可靠性的要求要全面、严密、细致，保证在任何情况下都能提供连续、稳定、正确的服务。

（一）系统可用性与平均无故障时间

系统可用性是对电力信息系统的服务能力做最直接的评估，一般用年停机时间在总运行时间中的占比来表示。99.999%（五个九）的可用性意味着一年中停机时间不超过 5 分钟 26 秒。平均无故障时间是从另一个角度来反映系统可靠性的一个指标，即系统两次相邻故障之间正常工作的平均时间。两个指标一起构成系统稳定性的重要量化要求。

承载电网实时监控和控制的主系统，如调度自动化系统、能量管理系统等，其可用性一般大于 99.99%。对地市级或者以上的省级以上调度中心，可用性目标要达到 99.999%。要达到这么高的可用性，那就表示从系统的设计、部署到运维的整个生命周期里，都要坚持高可靠性这个原则。在需求分析阶段就要确定各个子系统的可用性等级，把它拆解为平均无故障时间、平均恢复时间等可以量化的具体指标。核心服务器的平均无故障时间要达到数万小时以上，网络交换设备等也应达到电信级的可靠性标准。

为满足这些严苛指标，系统架构设计必须充分考虑冗余配置，具体包括：

1. 硬件冗余关键的服务器、存储、网络、电源等均采用 N+1 或者 N+N 冗余，不能出现单点故障。

2. 软件与应用冗余：核心应用进程以主备或集群方式部署，当主用进程出现问题时，备用进程可以在毫秒级或者秒级的时间内无缝接替服务，对于用户来说是透明的。

3. 数据链路冗余，厂站、变电站与控制系统之间应该有主备通道，能够自动切换，保证数据流不会中断。

采用以上冗余方式，即使局部出现硬件或者软件故障，系统对外提供的服务也不会中断，或者只出现短暂的中断，从而达到很高的可用性，满足电网安全运行对信息系统连续性的严格要求。

（二）数据完整性与准确性

数据完整性与准确性属于电力信息系统可靠性的重要组成部分，它保证了系统里存储的、传输的以及处理的数据真实可信，没有被改动，并且也没有缺失。电力系统当中，倘若出现数据出错或者不一致的情况，就有可能导致调度人员作出错误的判断，从而引发不必要的保护装置动作，在电费结算时也可能会出现纠纷。所以从数据产生的一刻起就没有任何松懈的空间。

数据完整性是指数据在传输过程中不会出现丢包或者比特错误。这就需要在通信协议中加入 CRC 校验、消息确认、重传等等机制。从数据存储的角度来说，数据库应该具有事务处理能力，保证操作的原子性、一致性、隔离性、持久性，防止由于系统异常中断造成数据处于不一致的中间状态。对时序数据进行断点、坏点检测，对检测出的断点、坏点进行标记或者采用合理的插值法进行估算，保证数据序列的连续性以及可用性。

数据准确性指的是数据内容是否真实的反映了物理世界的实际状况。这就要求前端的测量设备要准确、已校准。系统上要创建数据质量在线校核体系。可以利用状态估计等高级应用，对全网量测数据做一致性校验，找出并剔除误差较大的坏数据。对人工输入数据应该建立严格的合法性校验规则和逻辑约束，比如数值范围检查、格式校验、关联数据逻辑一致性检查等等，从源头上减少错误数据的产生。对重要的参数进行修改时，要严格控制修改的权限，实行操作审计制度，保证每一次修改都有据可查。

（三）系统容灾与备份恢复能力

系统容灾和备份恢复能力属于电力信息系统应对极端情况，保证业务连续性的一道最后防线。要求系统在火灾、地震、网络攻击等灾难性事件造成主用站点完全失效的时候，依靠事先设定的备份和恢复机制，在最短的时间内恢复主要业务的功能。本项需求主要是用恢复时间目标、恢复点目标两个主要指标来衡量的。

恢复时间目标即系统出现灾难之后，从中断到恢复到正常运作状态所经历的时间。电力调度系统等重要系统恢复时间目标也非常高，分钟级。备用站必须在极短的时间内接替所有的业务。恢复点目标 RPO 就是指系统在灾难发生之后能够接受的最大数据丢失量。恢复点的目标为零，即系统必须能够恢复到灾难发生前的瞬间状态，不能有数据丢失。交易结算类数据的恢复点目标为零是硬性规定。

要达成不同的恢复时间目的和恢复点目的，就要制订不同级别的容灾方案。

下表给出的是不同等级容灾方案的恢复时间目标和恢复点目标：

典型容灾方案 RTO 与 RPO 指标概览

容灾等级	主要特点	恢复时间目标	恢复点目标	实施方式举例
数据级容灾	成本较低，数据远程备份	较长 (数小时至数天)	较长 (数小时至数天)	磁带异地备份、数据准实时复制
应用级容灾	异地备用系统，恢复应用	中等 (数十分钟至数小时)	中等 (数分钟至数小时)	异地建立备用系统环境，加载数据恢复
业务级容灾	“两地三中心”模式，业务不中断	极短 (分钟级甚至秒级)	极短 (秒级甚至为零)	同城双活、异地灾备中心实时同步

数据级容灾主要是远程备份。定期把数据备份磁带送到异地，或者通过网络将数据实时或准实时地复制到远程备份中心。该种恢复时间目标较长，但是成本较低。

应用级容灾就是异地建立一套完整的备用系统环境。当主站点发生灾难的时候，用数据备份来恢复应用。这会大大地缩短恢复时间的目标。

业务级容灾：指建立同城热备中心和异地灾备中心的“两地三中心”模式。同城中心之间用高速光纤做数据实时同步和应用自动切换，可以实现恢复点目标为零、恢复时间目标小于一分钟。异地中心是用来防备区域性的大范围灾难的。

需求分析阶段就要把业务关键程度，中断会带来的损失，投资成本综合考虑进去，给各个子系统设定合适的恢复时间目标和恢复点目标，然后按照这些目标选择合适的容灾技术架构和建设方案。还要制定详细的灾难恢复预案并定期演练，以保证在灾难真正发生的时候，容灾系统能够切实发挥作用，保证电力核心业务的连续性。

三、并发处理能力需求

智能电网建设不断深入、电力市场化的推进、用电信息采集范围的扩大，使得电力信息系统所承载的用户数量、数据流量急剧增加。系统并发处理能力的好坏，直接决定了系统在业务高峰期是否能够稳定运行，是否可以提供高质量的服务。因此并发处理能力需求分析，也是保证系统具有较好的扩展性、适应未来变化的重要环节。

（一）最大在线用户数与并发连接数

最大在线用户数、并发连接数等都是反映系统并发承受能力的指标。最大在

线用户数，某一时间段内，系统支持已经登录并且保持会话的用户数量。并发连接数，就是某一瞬间向服务器发起请求的活跃连接数量。两者相关，但侧重点不同。前者考的是系统的会话管理、内存分配；后者直接给服务器的 CPU 处理速度、I/O 性能、网络吞吐量加压。

需求分析阶段需要对系统用户的角色和使用场景做详细的分析。一个省级电力信息系统的用户群体中，包含几百名进行实时操作的调度员，几千名查询分析的管理人员，数万名使用 Web 或者移动 App 进行访问的现场运维人员，甚至可以包括上百万乃至上千万通过互联网查询电费的普通电力客户。不同的用户所对应的访问频次、操作复杂程度和在线时长也大相径庭。因此不能以所有的注册用户数作为并发设计的依据，而应该根据典型业务场景，估算高峰时段各种用户平均在线率和瞬时请求并发率。同时还要留有设计余量，以备节假日、迎峰度夏 / 冬等特殊时期访问量激增时使用，也要考虑未来 3 到 5 年业务发展的需要。

（二）大数据量处理与响应时间

现代电力信息系统已经进入了大数据时代，需要处理的数据种类和数量非常大。每秒成千上万的 PMU 量测数据、数百万的智能电表分钟数据、大量的设备状态数据和操作日志等。大数据量处理与响应时间这项指标，系统要能够在 TB 级或者 PB 级的数据下依然能够完成存储、查询、统计、分析等任务，在用户可以接受的时间里返回结果。

在线事务处理场景中调度员对于数据的响应时间要求为秒级。这就对实时数据库查询优化、索引设计提出了极高的要求。而在线分析处理场景中，管理层想要对去年一年的线损率进行多维度钻取分析，用户对于响应时间的忍耐度会稍微高一些，也许是在几十秒到几分钟之内，但是其背后所涉及的计算量却是非常巨大的。这就需要系统使用分布式计算框架（Hadoop、Spark 等）、列式存储数据库、内存计算等大数据技术，采用并行处理的方式来提高复杂查询的速度。

需求分析的时候，要找出系统里的主要大数据处理任务，然后对这些任务牵涉到的数据量，计算复杂度，期望的反应速度等展开量化分析。用户规模达到 1 亿的时候，对任意用户的过去一年的日用电量进行查询，响应时间应该小于 3 秒；对全省所有配电变压器过去一个月的负载率曲线做聚合统计分析，任务应该在 5 分钟内完成。具体的量化指标将影响后面技术的选取以及架构的设计。

系统应该可以同时处理高并发短时查询、长时间运行复杂分析任务混合负荷，

并且不会造成严重的资源争夺和性能影响。要依靠合理的资源隔离、任务调度、架构分离（读写分离、分析型数据库与交易型数据库分离等等）等技术来实现。

（三）峰值负载下的系统稳定性

峰值负载下系统稳定性的好坏是检验系统是否健壮的最终标准。它意味着系统面对远超平均水平的并发请求和数据流量冲击时，不会崩溃也不会拒绝服务，它能保持核心功能的可用性，以可预见的方式平稳运行，做到优雅降级。此指标对电力系统来说十分重要，因为业务高峰期一般也是电网运行的关键时期，系统一旦出现故障，后果将十分严重。

需求分析要确定峰值负载的量级，一般峰值负载是平均负载的几倍，还要确定峰值的维持时长。系统要可以承受 3 倍于日均并发量的用户访问，1 小时内不能断线。为了保证系统能达到这样的需求，压力测试、容量规划是必不可少的。经过模拟预期的峰值负载状况，可以找到系统性能短处，像数据库连接池用尽，中间件线程堵塞，网络带宽达到上限之类，然后有针性地加以改善。

在设计层面，系统应具备完善的自我保护机制，例如：

1. 限流、熔断，请求量大于系统处理阈值的时候，主动丢弃非核心的业务请求，保证核心交易能够正常进行。当下游服务响应速度慢或者失败率很高的时候，系统可以自动熔断，暂停调用，避免造成连锁故障。

2. 弹性伸缩，云环境下系统根据实时负载情况，自动增加或者减少计算资源（虚拟机、容器实例等）来应对负载的变化。

经过严格的峰值负载稳定性要求以及充分的验证之后，就可以保证电力信息系统在各种复杂、极端的运行环境中，仍然能够像磐石一样稳固，给电网的安全、稳定、经济运行提供可靠的信息支持。

第四节 安全可靠性需求分析

电力信息系统属于国家能源命脉的关键基础设施，它的安全可靠与否关乎电网能否稳定运行以及社会秩序是否得以维持。因此对电力信息系统的安全可靠性需求进行全面、系统的分析是构筑坚固防线、提高系统韧性的前提。

一、网络安全需求

网络是信息系统的血脉，承载着电力生产、调度、营销等各方面的业务数据流。网络安全是整体安全的第一道防线，要构筑起纵深防御体系，切实防范好来自内忧外患的各类网络攻击，保证信息通道不被侵扰，信息流干净畅通。

（一）网络边界防护与访问控制

电力信息系统的网络边界是抵御外部攻击的第一线，网络边界防范是否严密非常重要。在不同的安全域之间部署高性能的下一代防火墙，对网络流量做深度包检测和应用层识别。对电力生产控制大区和管理信息大区之间进行隔离，采用物理隔离或者逻辑强隔离的方式，防止跨区非法访问、阻止恶意代码的传播，保证核心生产系统安全可靠。

访问控制属于边界防护的重要手段，执行时要细致入微并且具有灵活性。遵循最小权限原则，制定严格的访问控制策略，规定出谁、何时、何地、以何种方式可以访问什么资源。对远程运维、第三方接入等高风险的场景必须单独配置 VPN 通道并配置多因素认证手段，每次接入之前都要对终端进行安全检测，保证访问的合法性、安全性。

伴随着业务发展、云技术使用，电力信息系统网络边界越来越模糊，也越来越复杂。传统的静态边界防护已经不能应对出现的新威胁，要向零信任安全架构转变。零信任架构的核心思想就是“永不信任、始终验证”，它认为内外网存在威胁。因此每一个访问请求，不管来自哪里，都必须经过严格的身份验证和权限校验，从而把以网络为中心的防护转变为以身份为基础的动态访问控制。

（二）入侵检测与防御系统

入侵检测和防御系统属于网络边界防护的一种补充手段，它如同在网路的各个角落布设监控探头与哨兵一般，能够对正在发生的攻击行为做出及时的发现并予以阻止。电力信息系统要配置集特征库检测、异常行为分析、威胁情报等多重技术于一身的入侵检测与防御系统。对工业控制网络需专门部署能够解析 SCADA、IEC61850 等工业协议的工业入侵检测系统来防范工控设备及相应的协议被攻击，避免通用 IT 系统不能辨识工业协议产生漏报。

防御系统是否有效，不在检测能力，而在响应与处置是否完备。该系统应当能自主阻断攻击流量、隔离被感染的主机、协同防火墙自动更新访问策略等等，

从而缩短对攻击响应的时间，把损失降到最低。还要建立完善的误报处理程序。在电力生产环境中，任何一个错误的拦截都会导致业务中断，所以系统告警的研判与处理要格外慎重，保证安全策略执行时不会影响到电网的正常运转。

（三）安全审计与日志管理

安全审计、日志管理都是保证安全事件可以追溯、建立事后追责机制的前提。缺少全面、准确、完整的日志记录，安全事件调查分析就成为无源之水。电力信息系统应当创建起集中式的日志管理平台，涵盖网络设备、服务器、数据库、中间件以及各种应用系统等。

该平台应该具备强大的日志采集能力，能够兼容各种品牌、不同种类的设备日志，并将之统一格式化。日志数据在传输和存储过程中要保证其完整性、保密性，不能被未授权的第三方篡改、泄露。使用数字签名或者散列校验等手段来保证日志的不可抵赖性，为之后审计、取证提供可靠依据。

只收集日志是不够的，更重要的是关联分析、深度挖掘。应当采用安全信息与事件管理系统，用大数据分析和机器学习的方法对大量日志进行自动检测，找出异常行为模式和可疑的入侵行为线索，从而达到全面提高安全态势感知能力的目的。

安全审计工作要制度化、常态化。对重要用户的操作行为，系统配置的修改，关键权限的分配等开展定期的审计工作，提前发现违规的行为以及潜在的风险。审计结果应该形成报告，作为改善安全策略、完善管理制度的依据，实现安全管理的闭环。

二、数据安全需求

数据是电力信息系统的核心资产，电网运行状况、设备健康状况、用户信息、经营决策等重要信息在其中有很多。保证数据机密性、完整性和可用性，属于信息系统建设、网络安全目标。

（一）数据传输与存储加密

电力信息系统中的数据在网络上传输时很容易受到窃听、截获、篡改等风险的影响。所有经过公共网络或者内部非信任网络传输的敏感数据，例如远程调度指令，用户信息，支付信息等等，均须采用高强度加密协议加以保护。应全面推广使用 TLS 协议对 Web 应用和 API 接口进行加密；跨区域、跨广域网的数据交

换则要建立IPSec VPN或者SSL VPN加密隧道，保证数据在传输链路中是机密的、完整的。

数据静态存储也存在风险，物理介质丢失或者服务器被攻击，就会引发数据泄露。因此对存储在数据库、文件服务器等处的敏感数据进行有效的加密就显得尤为重要。可以采用数据库自带的透明数据加密功能或者文件系统级加密技术，数据加密之后再写入磁盘。密钥管理是加密体系的重中之重，必须建立安全的密钥管理系统，对密钥的整个生命周期进行管理，即密钥的生成、保存、传递、更换、销毁等各个环节都要加以管理，并且严格控制密钥的访问权限。

（二）数据备份与灾难恢复

对于硬件故障、人为误操作、勒索软件攻击、自然灾害等不可预测的风险来说，完善的备份数据及灾难恢复机制就成了最后一道防线。根据不同的业务系统重要程度以及数据特性来制定适合的备份策略，保证任何情况下都可以恢复任何重要的数据。

数据备份策略的各项关键考量因素及灾难恢复目标，可参见下表：

数据备份策略关键要素

要素	说明	示例 / 考虑点
备份周期	根据业务重要性与数据变化频率确定备份频率	核心系统实时复制，非核心系统每日 / 每周备份
备份方式	选择全量、增量、差异备份的组合	兼顾恢复效率与存储成本，例如每周全量 + 每日增量
备份介质管理 (3-2-1 规则)	至少保存三份备份，采用两种不同介质，一份异地存放	硬盘、磁带、云存储；本地、异地数据中心
恢复时间目标	业务中断后，系统恢复至可用状态所需的最长时间	数分钟到数小时，取决于业务容忍度
恢复点目标	业务中断后，数据可能丢失的最大时间量	零数据丢失到数小时的数据丢失容忍度

灾难恢复计划是保证灾难发生时能够有条不紊、高效地恢复业务。计划中需要明确恢复时间目标RTO，恢复点目标RPO，应急响应组织架构，各个岗位职责，恢复流程以及技术方案。另外，不能只将灾难恢复计划停留在书面上的形式，要通过模拟真正发生灾难时的场景来进行检验和演练，以此来测试应急预案，完善预案的不足之处并提高系统的抗灾能力。

（三）用户权限与数据隐私保护

用户权限失控属于数据泄露以及恶意破坏的最主要内部原因。因此必须按照职责分离和最小权限的原则来设计权限体系。基于角色的访问控制模型，即把权限授予角色而不是直接授予用户，通过用户所拥有的不同角色来控制数据的访问和操作权限。所有权限的授予、更改、收回必须严格审批，并有记录。

随着电力市场化改革推进以及智能用电服务推广，电力信息系统承载大量用户个人信息及用电行为数据，这些数据高度敏感。必须建立数据隐私保护体系，遵守国家相关法律法规。数据采集、使用、共享等过程中都必须告知用户并获得其授权。对于敏感的个人身份信息，在非必要的情况下，应当采用数据脱敏技术对其加以处理，例如屏蔽、变形、散列等手段，在开发、测试、数据分析等场景中使用经过脱敏处理的数据，从技术上杜绝隐私泄露的可能性。

三、应用安全需求

应用系统是用户同数据直接打交道的地方，同时也是安全防护体系中最容易遭到攻击者的攻击的部位。它自身的漏洞可以绕过底层网络和系统防护直接威胁数据的安全，因此必须引起重视。

（一）身份认证与授权管理

身份认证是指确定用户的身份过程，同时也是各种安全措施的基础。电力信息系统不能只依靠静态口令进行弱认证。对所有的关键业务系统以及远程访问入口执行强制多因素认证，比如口令加短信验证码，动态令牌或者生物特征识别等等，使身份冒用的难度大大增加。密码策略必须强制复杂度、定期更换、有防暴力破解。

授权管理主要是确定用户能做什么，对认证通过后的用户行为进行细粒度的限制。应该创建统一身份认证以及授权管理平台，达成用户集中管理身份、统一配置认证策略以及应用系统权限集中分派的目标。不仅可以提高管理效率，而且可以保证用户入职、转岗、离职时能迅速准确地赋予、变更或者收回权限，有效防止幽灵账户等安全问题的发生。

单点登录技术可以改善用户体验，用户只需要认证一次就可以访问多个应用系统。在实现单点登录的时候，需要选择安全、成熟的协议，并保证身份提供方自身的安全。同时还应该建立会话管理机制，对用户登录状态进行严密监控，提

供超时自动退出、异地登录告警、强制下线等功能来防止会话被劫持。

（二）应用软件漏洞防护

无论是通用商业软件，还是自编业务软件，都不可避免地存在着安全漏洞。要创建常态化的漏洞管理流程，包含漏洞的发觉，评判，修补以及核实这些步骤。采用自动化漏洞扫描工具加人工渗透测试相结合的方式，定期对在线运行的应用系统进行安全检测，主动发现其中存在的 SQL 注入、跨站脚本、文件上传漏洞、不安全的反序列化等各种高危风险。

发现漏洞就要马上修好，建立补丁更新制度。对通用软件应该尽快根据厂商安全公告评估、测试并打补丁。对自主研发的平台来说，开发团队要迅速调试代码，发布新的版本。当漏洞不能及时修复的时候，可以用 Web 应用防火墙等虚拟补丁技术，从网络层面识别拦截利用该漏洞的攻击流量，为漏洞修复争取时间，提供临时补偿防护。

（三）安全编码与代码审计

将安全融入软件开发的整个生命周期，是从源头上杜绝漏洞、创建内生安全应用的最佳办法。必须采用安全软件开发生命周期模型，在软件的生命周期中即需求分析、设计、编码、测试、部署等各个阶段都要加入安全活动。开发团队应该参加系统安全编码培训，知道常见的漏洞产生原因和修补方法，按照统一的安全编码规范开展开发工作。

代码审计是对安全编码实践成果的一种检验，可以分为静态审计和动态审计两种方式。静态应用安全测试是在代码不运行的情况下，分析源代码或者字节码来发现可能存在的安全隐患，例如不安全的函数调用、硬编码密码等。动态应用安全测试是在应用运行时模拟攻击行为来检测漏洞，可以发现静态分析不能发现的业务逻辑漏洞。

利用自动化代码审计工具可以大大提高审计效率，将其整合到持续集成 / 持续部署（CI/CD）流程中，在代码提交时立即启动自动化安全扫描，在开发早期就能快速发现并纠正安全隐患，从而降低修复成本。对核心业务系统的重要模块除了工具扫描之外，还应该组织专家进行人工代码审核，对业务逻辑进行深入的分析，发现更深层次、隐蔽性更高的安全风险。

第三章 电力信息系统设计方法

电力信息系统设计是把业务需求和实现技术联系起来的重要桥梁，对系统建设的好坏起着决定性的作用。本章将对电力信息系统设计所遵循的主要方法、原则做系统的论述。这些指导思想以及实践框架，目的在于给复杂的系统建设提供科学、严谨而可行的指导，保证最终建成的系统可以有效地、稳定地、安全地支撑电力业务的运行和发展。

第一节 系统总体设计原则

系统总体设计原则是整个设计过程中纲领性要求，也是保证信息系统满足电力行业特殊性需求、具有长久生命力和核心价值的基础。它从宏观上给技术选型、架构设计、实施策略等具体的工作给出了明确的方向以及评判准则，是评判各项设计决策是否合理的标杆。

一、统一规划与分步实施原则

该原则要求在系统建设的过程中兼顾长远目标和近期效益，用全局性的顶层设计来指导具体的阶段性建设。这一原则很好地体现了战略性同战术性相结合的思想，可以避免由于缺少全局眼光而造成的重复建设、信息孤岛以及后期整合困难等弊端，是大型复杂系统工程管理中的一项重要指导思想。

（一）顶层设计与蓝图规划

电力信息系统的建设要从企业战略的角度，对全局进行统筹规划。顶层设计就是确定系统建设目标、价值、总体架构，形成一份清晰可行、具有指导意义的技术业务蓝图。本阶段需要对电力企业的业务模式、管理流程、发展战略、未来信息技术发展趋向展开深入分析，把信息科技规划同企业发展规划有效融合。

蓝图规划不单单是技术层面的架构图，更是一个包含应用架构、数据架构、技术架构、安全架构等各方面的综合性方案。它明确地指明了系统将来的形式，

各个子系统间的关系，数据流动规则和技术选型标准。科学的顶层设计和蓝图规划，可以保证后续所有的建设工作步调一致，从根本上保证系统各个要素的一致性、协同性、整体性。

（二）明确阶段目标与实施路径

在宏伟蓝图的指引下，庞大的建设任务必须被分解成若干可以加以管理、可以分阶段完成并加以评价的组成部分。分步实施是达成复杂系统“软着陆”的一种策略。每个阶段要有具体的目标，比如完成某项关键业务流程的数字化、某个重要数据域的治理、搭建某个基础技术平台等等。阶段性目标应该具体、可衡量，给用户带来实实在在的价值。

与阶段目标相对应的，就是具体的实施路径规划。制定各阶段的建设顺序、时间表、资源投入、预期成果。路径设计要考虑到业务的紧急性、技术可实现的难易程度、各模块之间相互依赖的关系以及投资回收期。通过灵活采用滚动计划、迭代开发的方式，控制项目风险，根据项目内外部环境的变化及时调整项目的实施方式，保证项目按正确的方向一步步推进，积小胜为大胜。

（三）确保系统的可持续发展

统一规划、分步实施的最终目的，就是为了保证系统可持续发展能力。系统的生命力在于它是否能够不断适应变化的业务需求，并且不断地跟上技术的更新换代。设计之初就应该把系统生命周期的管理考虑进去，不能因为短期的目标而牺牲长期发展的可能性。这就意味着架构的设计要具有前瞻性，能够考虑到未来技术的升级和业务的发展。

分步实施的过程就是不断学习、不断完善的动态过程。每一个阶段建设成果都需要经过实践检验，它所反馈的信息将会成为下个阶段进行规划和设计的有效资源。螺旋式上升的模式使系统在动态的环境里不断的发展、完善。在规划时还要留有充分的技术和资源储备，以应对未来可能出现的新技术浪潮或者重大业务变革，保证信息系统一直是企业发展的强大推动力，而不是阻力。

二、安全可靠与稳定运行原则

电力系统属于国家重要的基础设施，它的信息系统安全、稳定运行关系到社会经济正常运转以及人民群众的日常生活。因此，安全可靠、稳定运行是电力信息系统设计的第一原则，也是不能逾越的红线。任何设计决策都必须把本原则放

在第一位。

（一）安全设计贯穿始终

电力信息系统的安全防护不是后期增加的功能点，应该在设计之初就融入系统设计过程，贯穿需求分析、架构设计、编码实现、测试部署、运维管理等整个生命周期中。安全内建的思想是从根源上消除安全隐患，构建起纵深防御体系。

1. 体系化安全策略，设计要符合国家以及行业有关网络安全等级保护、关键信息基础设施安全保护等法规和标准的要求，创建起物理环境、网络通信、计算环境、应用系统、数据等多层次、立体化的安全防护体系。

2. 主动防御、威胁预警系统应该具有主动防御、威胁预警的能力，通过入侵检测、态势感知、威胁情报等技术，把被动响应转变为积极主动的防御。安全设计要考虑对各种已知的、未知的攻击进行识别和防御。

3. 数据安全与隐私保护，对电力系统大量生产、经营和用户数据建立严格的数据分类分级制度，采取访问控制、数据加密、数据脱敏等一系列技术手段，保证数据在采集、传输、存储、使用、销毁全生命周期的安全性、完整性、可用性，防止数据泄露或者被滥用。

（二）关键设备与链路冗余配置

为了保证系统在出现单点故障的时候仍然可以提供服务，冗余设计是保证系统高可用性的主要方法。电力信息系统中关键节点出现故障，很容易引发连锁反应，造成大面积的业务中断。因此，在设计时就要对所有可能出现单点故障的环节做冗余配置。这里指的是服务器、存储、网络交换机、路由器、防火墙等核心硬件的冗余，一般采用主备、双活、集群等高可用部署方式。

除设备冗余之外，通信链路的冗余也十分重要。连接总部、分支机构、厂站和数据中心的骨干网络链路，应至少配置一条与之完全隔离的物理备份链路，并采用支持动态路由协议的方式，在故障发生时实现自动切换。数据中心内部服务器与核心交换机之间应该使用双网卡、双上联方式保证网络连接的可靠性。经过全面的冗余设计之后，硬件故障或者链路中断给系统稳定性造成的冲击就被减小到最低限度，业务连续性有了坚实的硬件基础。

（三）建立完善的应急恢复机制

即使进行了全面完善的安全防护措施和冗余设计，也无法完全避免由于无法预知的自然灾害、重大软硬件缺陷以及高强度网络攻击所造成系统的故障。因此，

建立一套完备高效的应急恢复机制，就成了保障系统稳定运行的最后一道防线。应急恢复机制设计的主要目的就是减少业务中断的时间，减小数据的丢失量。

应该有科学的备份制度，根据不同数据的重要程度和变化速度，采用全备、增备、差备等各种各样的数据备份方式，同时把备份的数据存放在不同的地方，定期对这些数据的可用性进行检查。制订出详细的灾难恢复预案，对各种故障情形下所需要采取的应急响应流程、组织架构、职责分配、恢复步骤做出明确的规定。预案的关键指标有恢复时间目标、恢复点目标等，见下面的表格。

应急恢复目标指标

指标名称	说明
恢复时间目标	业务中断后，从灾难发生到业务系统恢复至可接受服务水平所需的最长时间。
恢复点目标	业务中断后，系统能够恢复到的数据状态，衡量数据丢失的最大可承受时间。
最大可接受中断时间	在不严重影响业务连续性的前提下，业务系统可以承受的最大停机时间。

要定时举行应急演练。经由模拟真实的故障情况，考察预案的可行度，团队配合的默契程度，恢复操作的熟练程度，从中找出并加以改进，保证真实灾难来临时能够临危不乱，迅速而有条不紊地应对并恢复正常。

三、先进性与实用性相结合原则

电力信息系统的技术选择、架构设计，不能只追求技术的先进性或者单纯追求现实可行。过度追求先进性会引进不成熟的技术，造成高成本、不可预知的风险，固守陈旧技术会限制系统性能的发展，不能满足未来业务创新的需求。

（一）采用成熟可靠的主流技术

系统核心和重要的业务领域应该使用业界普遍认可、生态环境好、市场占有率高的主流技术。这些技术一般具有较好的稳定性、高可靠性以及可预测的性能。以选择数据库为例，成熟的关系型数据库管理系统在处理事务性核心业务的时候，仍然是首选方案；在选择操作系统、虚拟化平台的时候，主流产品可以得到强大的社区支持和商业服务保障，从而减轻运维难度，降低技术风险。使用主流技术就意味着可以更易地招聘到合格的技术人才、获得充足的技术资料及解决方案，从而降低项目总拥有成本，保证系统长期稳定的运行。

（二）适度引入前沿技术进行探索

在保证核心系统稳定可靠的基础上，为了保持技术先进性、驱动业务创新，电力信息系统也应该注意前沿技术，适度地引入和应用。可以在非核心业务、创新应用、试点项目中尝试使用人工智能、大数据分析、物联网、边缘计算、区块链等新技术。这种探索性引入可以以技术实验室开展概念验证的方式进行，也可以选取某个业务场景，比如设备故障预测、负荷准确预测、客户画像分析等，实施小规模的试点应用。这样做可帮助企业在风险可控范围里获得新的技术应用的经验，并可以评估出新技术应用给电力业务带来实际的价值，为以后大规模技术的应用以及升级做好充分的准备，从而避免在技术革命中处于被动状态。

（三）确保技术方案经济可行

任何的技术方案的选择都是不能脱离经济成本的制约的。先进性与实用性的结合点，最终还是需要经济可行性来衡量。技术选型不能只看初始采购费用，应该从系统全生命周期的角度来评估整个成本，即软件许可费、硬件投入、开发集成费、后期运维人力费、升级迁移费等。设计方案要以满足业务需求、达到性能指标为前提，在保证性能指标达标的同时，力求取得最好的投入产出比。技术上稍弱一些但是成本效益更高的方案，有可能比技术尖端但是价格昂贵的方案更符合企业实际的需求。因此，技术决策要与财务预算紧密结合，保证最后方案技术上先进、业务上适用、经济上合理。

第二节 系统架构设计方法

系统架构设计属于电力信息系统创建的重要部分，它既关乎系统的技术基本框架，又关系到系统的性能最高限度，发展潜质以及运维费用。好的架构设计可以使得系统既可以满足当前的需求，又可以应对未来可能出现的技术变革与发展的需要。本节主要从集中式架构、云原生架构等主流设计方式出发，对电力进行分析。

一、集中式架构设计

集中式架构是信息系统发展早期的形态，核心思想是把所有的计算资源、数据存储和处理逻辑都集中到一台或者几台高性能的中心计算机上。在电力系统信

息化之初，对重要的业务来说起到了稳定运行的作用。

（一）大型主机 / 服务器架构

大型主机或者服务器架构为典型的集中式设计。本模式中一台或多台高性能主机或者小型机构成为系统的核心，完成大部分的数据处理和计算任务。所有的终端设备，即功能简单的“哑终端”或“瘦客户端”，只负责数据的输入和显示，通过专用网络与中心主机相连，把用户的操作请求发送给中心主机，接收处理后的结果。

电力系统早期多用此种架构来搭建核心的生产管理、调度自动化系统。早期的电网调度 SCADA 系统里数据采集、实时监控、状态估计、安全分析等所有计算任务都由调度中心的中央服务器群完成。可以保证数据处理的一致性、计算任务的协调性，对电网安全稳定运行起着重要的作用。它的高可靠性以及强大的事务处理能力，在很长一段时间内都是电力核心业务系统首选的技术。

（二）集中式数据存储与处理

在集中式架构里所有的业务数据都存在一个中心数据库里。这样设计大大简化了数据管理工作，所有的数据备份、恢复、安全控制、权限管理都可在一个中心进行。电力系统对于数据的准确性、一致性要求很高。采用集中式存储，可以防止分布式环境下数据的冗余、不一致，保证电量数据、客户档案、设备台账等重要信息的唯一和权威，让企业内任何地方的数据都是相同的。业务逻辑更新或者进行数据分析的时候可以直接操作中央数据库，保证业务规则即刻生效、数据分析具有全局性。

（三）适用场景与优缺点分析

集中式架构由于结构简单、容易管理、容易控制等特性，在一些场合下仍然有不可替代的作用。它特别适合于数据一致性、安全性、事务完整性要求比较高的核心业务系统。以电力营销系统中的计费收费模块为例，每笔交易的原子性不能出错，不能出现漏计费、坏账等现象，集中式架构强大的事务处理能力恰好可以满足这样的要求。同样电网调度控制系统需要有全网络全局实时的视图，集中式处理模型可以保证调度指令的统一和准确。

但是它的缺点也很明显，可扩展性差，系统的整体性能受中心服务器的处理能力限制。业务量增加时只能依靠升级硬件来进行垂直扩展，成本高而且存在性能瓶颈。系统可靠性风险高度集中，任何一个中心服务器或者数据库出现问题都

会造成整个系统崩溃，引发大面积业务中断，对于需要 7x24 小时连续工作的电力系统来说，这是一个巨大的威胁。开发维护成本高、技术封闭、业务扩展性差、技术迭代慢、缺乏灵活性。

二、分布式架构设计

由于网络技术不断发展以及业务规模不断扩大，集中式架构已经越来越显现出它的瓶颈。在这种情况下，分布式架构出现了，它把原本集中在一个地方的功能和数据分散到很多节点上，各个节点通过网络相互连接，一起协作来完成任务。

（一）客户机 / 服务器架构

客户机 / 服务器架构，简称 C/S 架构，是分布式计算的早期经典模型。它把应用程序分成客户端和服务器端两个部分。客户端一般是指安装在用户桌面上，功能比较完备的应用程序，主要完成用户界面、业务逻辑处理、数据展示等工作；服务器端主要是完成数据管理、存储、共享服务。两者通过网络进行通信。电力系统中继电保护配置工具、调度员培训仿真系统等许多生产管理软件长期以来一直使用 C/S 架构。这样的架构可以充分发挥客户端计算机的处理能力，给用户带来反应迅速、交互性好的操作界面，也可以处理复杂的图形和本地计算，适合那些专业度比较高的桌面应用。

这种结构的缺点是布置与维系成本高。每次更新应用都要对成百上千的客户端进行更新，对于地域分布广大的电力企业来说，这是一项巨大的工作量。客户端软件开发测试要考虑各种不同的操作系统、硬件配置是否兼容，这会增大开发的复杂程度。

（二）浏览器 / 服务器架构

浏览器 / 服务器架构，即 B/S 架构，是 C/S 架构的一种改进和升级。在多层的结构中，用户界面及部分业务逻辑被移到了标准的网页浏览器中，客户端变得很“瘦”，用户不需要安装任何专门的软件，只需使用浏览器就可以访问系统。核心业务逻辑及数据处理主要在应用服务器和数据库服务器上完成。B/S 架构使得系统部署与维护简单，系统的更新只需要在服务器上进行即可，用户刷新浏览器就可得见新版本。这对于拥有众多分支机构、有移动办公需求的电力企业来说有巨大的吸引力。目前大部分的电力管理信息系统，如协同办公、人力资源管理、物资管理、营销客服等均已采用 B/S 架构。

实现跨平台访问，使用什么操作系统都行，有浏览器条件就可以访问系统。将业务逻辑集中到服务器端之后，系统也变得更加安全和可控。

（三）微服务架构

微服务架构是一种比较彻底的分布式架构方式，近些年才出现。它提倡把大型的单体应用程序（单体应用）拆分成许多小的、松散耦合的服务。每个服务都是以某个具体的业务功能为基础来构建的，可以独立地进行开发、部署和扩展。服务之间用轻量级的通信方式交互，比如 HTTP/REST API。电力信息系统当中，一个庞大的营销系统可以被拆分成客户管理微服务、电表计量微服务、账务计算微服务、在线缴费微服务等等。

该架构具有很多优点，极大地提高了系统的敏捷性。各个业务团队可以同时开发和发布自己的服务，加快新功能上线的速度。各个微服务可以自由选择最适合自身业务的技术栈，不再受单体应用技术选型的限制。系统容错性也得到增强，单个服务的故障不会造成整个系统崩溃，只会影响到它所对应的那部分功能，实现了故障隔离。微服务可以依据各自所承受的负载来实现弹性伸缩，从而更加有效地利用计算资源，更好地应对电力系统中突然发生的高负荷状况，例如用电高峰期、批量计费。

三、面向服务的架构设计

面向服务的架构是企业在组织和利用分布式的计算能力时所持的一种设计观念。它并不是一种新技术，而是一种设计思想和原则，其目的在于利用标准化的“服务”来对企业的不同时期、不同技术搭建的异构系统进行封装与整合，从而实现业务的灵活与重用。

（一）服务封装与接口标准化

SOA 的核心就是“服务”的思想。服务是一个独立的、自包含的功能单元，它是具有明确业务能力的业务能力单元。服务封装即对已有的、甚至可能是老旧的应用系统功能进行封装，使之成为具有标准接口的、可供外部调用的服务。它把底层复杂的技术实现细节隐藏起来。接口标准化是互操作性的保证，一般用基于 XML 的 Web 服务技术（SOAP、WSDL）或者更轻量级的 RESTful API。由此可知，无论是老旧大型机应用还是新开发出的 Java 应用，都可以被统一抽象成服务，为企业数据共享、流程整合打下了基础。

（二）企业服务总线的应用

企业服务总线属于 SOA 架构中的一种常用中间件，它被视作企业信息系统“中央动脉”，对各信息传递和集成提供统一标准。所有的交互系统和服务都连到 ESB 上，而不是点对点的直接连接。ESB 在这里起到多种重要的作用：

ESB 主要功能概览

功能名称	作用描述	典型应用场景
协议转换	实现不同通信协议的服务间互通，屏蔽异构系统间的技术差异。	将 HTTP 请求转换为 JMS 消息，或将 SOAP 请求转换为 REST。
消息路由	根据预设规则，智能地将请求消息路由到正确的服务提供方。	根据业务类型或数据内容，将请求分发给不同的处理服务。
数据格式转换	将不同服务间传递的数据格式进行转换，并可对数据内容进行增强。	将 XML 格式的数据转换为 JSON 格式，或对数据进行清洗、校验。
服务编排与监控	提供对服务调用链的监控、日志记录和安全控制能力。	实时追踪服务调用路径，记录操作日志，实施访问权限控制。

电力企业业务流程当中，ESB 主要用来打通生产域和管理域之间存在的信息孤岛现象，把调度系统实时的负荷数据发送至营销系统，进而支撑负荷预测，需求侧管理等业务方面的合作。

（三）服务组合与业务流程编排

在 SOA 架构中，一个单独的服务只完成一个简单的业务功能。若需要对复杂的跨越多个系统的业务流程进行处理，则要将多个原子服务进行组合编排。新装用户接电业务流程需要依次调用客户信息创建服务、工程物资申请服务、现场施工派单服务、计量点归档服务。服务编排一般由业务流程引擎（例如用 BPEL 语言定义的流程服务器）来实现，以图形化方式来定义这些服务的调用顺序、条件分支以及异常处理逻辑。该种方式把业务流程逻辑从底层应用代码中剥离出来，使业务流程的调整和改进更加灵活迅速，企业可以更快地适应市场的变化，重组自身业务能力，而不需要对底层系统进行大范围改动。

第三节 数据库设计技术

数据库对于电力信息系统来说就像大脑一样，它储存着来自发电、输电、变电、配电、用电等各个方面的大量数据。本节主要对电力信息系统创建过程中数据库设计技术进行详细的阐述，包含数据模型从抽象到具体的流程，根据不同的业务情况选择合适的数据库，给出系统高效稳定运行的性能调优方案，为数据的可靠架构打下技术基础。

一、数据库模型设计

数据库模型设计属于业务需求和技术实现的中介，它把繁杂的电力业务逻辑转化成结构化的数据存储形式。好的模型设计不仅可以准确地反映业务规则，而且可以为系统以后的扩展和性能打下一个良好的基础。一般分为概念、逻辑、物理三个阶段，逐步递进，保证设计的完整性、科学性。

（一）概念模型设计

概念模型设计属于数据库设计的起始阶段，主要任务就是对现实世界中的业务需求实施抽象化处理，从而得到一个与任何具体的数据库系统无关的概念化表达。电力信息系统中该阶段一般用实体 - 关系图做为主要的工具。E-R 图用实体、属性、关系这三个基本元素，清楚地画出了电力业务里的主要对象和它们之间的联系。变电站、线路、电表等可以看作是实体，每个实体包含电压等级、投运日期、资产编号这些属性。变电站和线路之间存在着“连接”的关系，这种关系可以是“一对多”，也可以是“多对多”。

设计时要和电力业务专家充分交流，把系统边界内的所有重要实体找出来，比如发电机组、变压器、用户档案、电价策略等等，还要确定它们之间的业务规则。一个用户可以拥有多块电表，但是一块电表只能属于一个用户，这就是一对多的关系。设计者借助 E-R 图，能把复杂的业务逻辑以直观且标准化的图形方式表现出来，形成一份项目各方都能理解的设计蓝图，这份蓝图给后续的逻辑设计和物理设计给予清晰、无歧义的输入。此阶段是否成功直接关系到数据库能否真实、完整的反映电力系统运行的真实情况。

（二）逻辑模型设计

逻辑模型设计阶段承接概念模型，主要任务就是把 E-R 图转换成数据库模型

所支持的逻辑结构。电力信息系统构建的时候，关系模型因为结构清楚，理论成熟而被普遍采用。本阶段的主要工作就是把概念模型中的实体和它们之间的关系，转换成关系数据库中的二维表。一般一个实体对应一个独立的表，实体的属性对应表的字段。实体之间关系是用主键和外键来表达的。

在 E-R 图中识别出的用户、电表这两个实体，在逻辑模型中分别设计成用户信息表和电表信息表。用户信息表中用户编号为主键，用以唯一地标识每一个用户。电表信息表除了自身的属性之外还有一个字段叫做所属用户编号，该字段引用了用户信息表的主键。这样一来，两张表之间的一对多关系也就确定下来了，保证数据参照完整性。

该阶段还要按照数据库设计的范式理论，即第一范式、第二范式、第三范式对表结构进行规范化处理。规范化的目的是为了消除数据冗余，防止数据更新、插入、删除的时候产生异常，保证数据的一致性。比如把一个有很多重复信息的复杂的大的表拆成一些比较简单、相关性更强的小表。一个好的逻辑模型能保证数据的完整性的同时，可以实现高效的查询，它是建立高效可靠的电力应用系统的重要保证。

（三）物理模型设计

物理模型设计是数据库设计的最后一环，它把逻辑模型转换成可以在具体的数据库管理系统上运行的物理实现。本阶段要考虑目标数据库的特点、硬件性能、存储空间、预期的应用负载等各个方面，详细规定表结构、列的数据类型、存储参数、索引策略等等。这就意味着数据库设计从理论变成现实，它的好坏直接影响系统运行效率与稳定性。

在物理设计阶段首先要对每一个字段选择最合适的数据类型。电能量数据用高精度数值类型，故障发生时间等时间戳用日期时间类型。正确的数据类型定义可以节省存储空间，也可以提高数据处理速度。第二，按照业务规则定义约束，如非空、唯一、检查等，从数据库层面保证数据的合法性与准确性。更不可忽视的就是索引的设计，索引是提升数据库查询速度的重要技术。电力系统中经常需要按照时间范围、设备编号或者用户区域来查询数据，所以应该在这些经常被用作查询条件的列上建立索引。给用电信息采集表的采集时间和电表编号创建复合索引，可以大大提高历史用电数据的查询速度。

二、数据库选型与优化

电力信息系统创建时，数据库的选择与改良是系统性能，可靠性和扩展性好坏的关键部分。电力行业的数据种类很多，有需要高事务一致性的结构化数据、大量的实时监测数据以及有待挖掘分析的非结构化数据。因此要根据不同的应用场景的特殊要求来选择并组合各种数据库技术，构建最合适数据架构。

对于电力信息系统复杂多变的数据需求，不同类型的数据库及其在电力行业中的典型应用以及优势如下表所示：

电力信息系统数据库选型参考表

数据库类型	典型产品	核心优势	适用场景（电力行业）	示例数据类型
关系型数据库	Oracle, MySQL	强事务一致性，数据结构化，完整性保障	核心业务系统：营销计费，调度指令，资产管理，用户信息	客户档案，合同数据，设备台账，财务交易
时序数据库	InfluxDB, Prometheus	高吞吐写入，高效时间序列查询，强压缩	实时监控，传感器数据采集，SCADA, 智能电表数据	电压 / 电流曲线，温度 / 压力数据，同步相量测量单元数据，负荷数据
大数据平台	Hadoop, Spark	海量数据存储与处理，分布式计算，灵活扩展	历史数据分析，负荷预测，设备状态预测，窃电分析	多年用电量，设备运行日志，气象数据，历史故障记录

（一）关系型数据库（如 Oracle, MySQL）

关系型数据库管理系统是电力信息系统中应用最广泛、也是最基本的一种数据存储技术。由于有强事务处理能力、严格的 ACID 事务特性、成熟的技术生态系统，它们成了存放重要业务数据的首选。电力系统营销计费、调度指令、资产管理、用户信息等重要业务数据对数据的准确性、完整性要求高，给这些数据提供准确完整的支撑的是关系型数据库。

1. Oracle 数据库凭借其卓越的性能、高可靠性和完善的安全机制，长期以来在大型电力企业的核心系统中占据主导地位，尤其适用于需要处理大规模并发事务和复杂查询的场景，如省级电网的营销系统和调度自动化系统。它的高可用解决方案，如两地三中心部署，能够满足电力业务 7x24 小时不间断运行的严苛要求。

2. MySQL 作为一个性能优异、稳定可靠的开源关系型数据库，因其灵活性

和较低的拥有成本，在电力行业的各类辅助管理系统、监控系统和互联网应用中得到了广泛部署。随着其功能的不断增强和社区的持续活跃，越来越多的非核心但同样重要的应用，如设备运维管理、数据分析报表等，也开始采用 MySQL 作为后台数据库。

（二）时序数据库（如 InfluxDB, Prometheus）

随着智能电网、物联网技术的广泛应用，电力系统中产生了大量的带有时戳的序列数据，SCADA 系统、智能电表、微型同步相量测量单元等实时监测数据也越来越多。这类数据的典型特征就是产生频率高、数据量大、写操作远远多于读操作。传统的基于关系的数据库在频繁写入和大量时间序列数据查询的时候，很容易出现性能瓶颈。时序数据库就是为高效处理时间序列数据而设计的专用数据库。

InfluxDB 是目前使用较多的开源时序数据库，数据写入速度快、数据压缩算法好、提供丰富的时序数据查询函数。电力监控系统当中，各个监测点（线路电流，变压器温度，电能质量指标）的实时数据能够快速地被写入到 InfluxDB 当中。分析人员可以利用它的类 SQL 查询语言，快速完成时间范围筛选、聚合计算（求平均值、最大值）、降采样等操作，从而对电网运行状态进行实时监控、发出故障告警、开展趋势分析，性能要比同等条件下关系型数据库好得多。

（三）大数据平台（如 Hadoop, Spark）

电力系统不但是数据的主要生产者，而且还是海量历史数据的存储者，比如多年的用户用电记录、设备运行日志、气象数据等。数据价值巨大，但是数量庞大和复杂的程度超出了传统数据库所能处理的能力。大数据平台出现以后，使得深度挖掘这些“数据金矿”成为可能。电力行业的相关大数据技术主要是离线对数据进行分析、利用机器学习做复杂的关联计算来给负荷预测、设备状态分析、窃电分析等更为复杂的业务应用提供服务。

Hadoop 生态系统以分布式文件系统、分布式计算框架为核心，可以处理 PB 级的数据存储、批处理。电力企业可以将多年的用电数据、设备工况数据存到 Hadoop 分布式文件系统里，再用 MapReduce 或者 Hive 做大规模的数据清洗、转换、统计分析。Spark 是一种新的内存计算框架，它使大数据处理的速度变得很快，善于迭代计算和交互式分析。使用 Spark 训练电力负荷预测模型，用海量的历史数据快速迭代学习，可以大大提高预测的准确度，给电网经济调度、安全运行提

供科学依据。

三、数据库性能调优

数据库性能调优是系统工程，其目的就是通过各种技术手段找到并消除系统的瓶颈，最大限度地发挥数据库的处理能力，保证电力信息系统在各种负载下都能提供快速、稳定的服。调优工作是系统设计全生命周期中 SQL 编码、索引设计、系统参数配置等工作的重要组成，也是保证用户体验和系统可靠性的持续性工作。

（一）SQL 语句优化

SQL 语句是应用程序和数据库之间的桥梁，执行效率直接关系到系统性能。复杂的业务逻辑一般会被转化成多表连接、嵌套子查询等复杂的 SQL 语句，不恰当的写法很容易造成性能瓶颈。SQL 优化是应用层面最直接、成本最低的优化方式。核心原则就是减少不必要的查询，使查询优化器能够生成最好的执行计划。

优化方法包括用 `SELECT *` 只获取业务上实际需要的字段以减少网络传输和内存占用；使用索引列来提高 `WHERE` 子句查询的效率，注意不要在索引列上使用函数造成索引失效；多表连接时要保证连接字段有索引，按表大小、数据分布情况合理安排表的连接顺序。利用数据库提供的执行计划分析工具，可以很直观地看到 SQL 的执行路径、索引是否被使用、预估的成本，从而对 SQL 有针对地重构，提高查询效率。

（二）索引设计与优化

索引是提高数据库查询效率最有效的方法之一，建立指向数据表中特定数据的数据结构，使得数据库不必对整个数据表进行扫描就可以快速找到所需要的数据。不合理的设计不能提高性能，反而由于增加了数据插入、更新、删除时的维护开销而使系统变慢。因此索引设计与优化要采取科学的策略，做出权衡。

1. 索引创建要有针对性，应该先对在 `WHERE` 子句、`JOIN` 操作和 `ORDER BY` 子句中经常使用的列创建索引。对于多条件查询来说，建立复合索引比建立多个单列索引更高效，但是一定要遵守最左前缀原则，把过滤性最好的列放在索引的前面，使索引使用率最大。

2.2、索引不是越多越好，每个新增加的索引都会在数据发生变动的时候带来新的维护开销。所以需要定时查看索引的使用情况，删除那些很少用或者根本不用的冗余索引。同时还要注意索引碎片的问题，当表中的数据经常发生变动的

时候，索引的物理存储就会出现碎片情况，进而使得查询速度降低。定期重建或者重组织索引，可以恢复索引性能。

（三）数据库参数配置与分区

数据库参数配置是对数据库管理系统自身行为进行细致的调整，通过对内存分配、I/O行为、并发连接数等参数的合理设置来使它更符合电力系统的工作负荷。对于报表分析系统里读写都很频繁的数据库，适当加大数据块在内存中的缓存量以减少硬盘 I/O 操作。实时监控系统对于并发量大的情况，要按照并发数的多少适当增大最大连接数等参数，防止出现连接资源耗尽而拒绝服务的情况。

单表数据量达到千万或者亿级的时候，就算是最优秀的 SQL 语句和索引也会遇到性能瓶颈。分区技术就成为解决该问题的有效手段。它把一个大表在物理上分成多个更小、更易管理的部分（分区），但是逻辑上仍然作为一个整体对外提供服务。查询时，优化器按照分区键（如时间、地域等）做分区裁剪，只扫描有关的分区，减少 I/O 量，提高查询速度。对历史数据表按月或者按年进行范围分区，电力用电信息采集中经常使用并且非常有效的优化手段。

第四节 接口设计规范

电力信息系统的各个子系统、模块之间数据交换、业务协同十分重要。接口是系统之间交流的桥梁，接口设计的好坏直接影响到整个系统的性能、稳定性以及可扩展性。本节要详细分析电力信息系统建设中接口设计的原则、主要的技术以及应用规范，给电力信息化体系的构建提供可靠的技术依据。

一、接口设计原则

接口设计是系统集成和数据交互的基础，遵守相应的原则可以保证接口的健壮性、灵活性以及生命力。这些原则考虑到技术与非技术因素，是保证电力信息系统长期稳定、未来可以发展的关键，在接口定义的各个生命期均适用。

（一）标准化与规范化

标准化和规范化是实现电力信息系统互连互通的前提。接口设计要先遵循国际、国家和行业发布的各项相关标准。电力行业出台的《电力可靠性管理信息系统数据接口规范》等技术标准，给数据交换提供了一个统一的架构和语言。采用

统一的数据模型与通信协议，可大大减小异构系统整合的难度及费用，防止出现由于厂商或者技术不一样而形成的数据孤岛现象。典型的实践案例就是在设计电网模型相关接口的时候，参照《电力系统模型数据动态消息编码规范》等标准，保证模型数据在各个应用之间的一致性以及正确性。

规范化更多是组织内部的技术约定和管理流程统一接口命名规范，参数定义规范，返回码规范，文档模板规范。接口命名要明确体现业务功能，不能用“getData”这种模糊的名称，而应该用“queryMeterReadingData”这样的具体表述。参数名称应该统一使用小写，每个参数的数据类型、长度以及是否必填要清楚。返回的数据结构要一致，状态码、消息提示、业务数据这三项都不能少，这样调用方便能统一处理错误并解析结果。内部细致的分类规范可以大大提高开发效率、降低沟通成本，给以后的自动化测试以及运维监控打下良好的基础。

（二）松耦合与高内聚

松耦合、高内聚是衡量软件架构设计好坏的重要指标，也适用于接口设计。松耦合意味着系统或者模块之间应该尽可能减少互相依赖，接口是实现松耦合的主要方式。设计好的接口要像一份稳定的契约一样，调用方只需要关心接口提供的功能和数据约定，不需要了解服务提供方的内部实现逻辑。因此，服务提供方内部的架构、数据库或者业务逻辑发生变化时，只要接口定义和行为没有改变，调用方就不受任何影响。电力系统中的发电管理应用和调度应用之间通过松耦合接口进行交互，发电侧的技术升级不需要强制要求调度侧同步改造，从而使各个业务领域可以独立发展。

高内聚即接口的功能职责是单一的、明确的。一个接口只应该做一件事，并且做好这件事。获取用户用电信息的接口不应该同时包含修改用户信息等业务逻辑。把不同的功能强行绑在一起，就会使接口变得臃肿、难以理解、难以维护。当需求发生改变的时候，对其中一个功能点的修改可能会给其他功能带来意想不到的影响，从而导致系统稳定性下降。电力营销系统的客户信息查询、电费计算、账单生成等各个功能都设计成了独立的内聚接口，每个接口对应一个具体的业务场景，使系统结构更清晰，利于系统复用、测试、管理。

接口是系统间唯一的交互方式，接口的设计要隐藏内部实现的复杂性。调用者不需要、也不应该关心接口背后复杂的数据库查询、多系统数据整合或者大数据平台的实时计算。通过接口实现服务提供方和服务消费方之间的解耦，服务提

供方可以自由地进行内部改进或者重构，比如将原来的单体服务拆分成微服务或者更换底层数据存储方式等等。只要对外承诺的接口契约得到遵守，整个系统就能平平稳稳地运行，不会受到任何影响。依靠接口实现隔离，这就是实现系统架构灵活演进和技术迭代的关键所在，也是构建弹性、可扩展电力信息系统所必需的基础。

（三）易用性与可维护性

接口的易用性会直接影响到开发人员的接入效率以及开发体验。易于使用的接口应该有清晰、完整的文档说明，包括接口用途、请求参数解释、返回数据结构示例、详细的错误码列表。接口命名要直观易懂，参数设计要符合开发人员的直觉，不要使用生僻的缩写或者复杂的嵌套。设计 RESTful 风格接口的时候，恰当运用 HTTP 方法（GET、POST、PUT、DELETE）来对应资源的增删改查操作，可以使接口行为更加规范，容易理解。提供相关的开发包可以降低接入的难度，使开发者更多的精力放到业务逻辑实现上，而不用从零写请求和解析响应。

接口的维护性关系到系统的长期运维和系统的发展，也会影响系统的运维成本。可维护性包含很多内容，其中日志记录就十分重要。接口要保存详尽的调用日志，请求来源，请求参数，响应结果，响应时长都要记录下来，这对排查问题，分析性能，安全审计都很有利。统一的异常处理机制同样不能缺少，不管接口内部发生何种异常，都应该统一返回给调用方一致的错误信息，不能将底层系统异常的具体信息原样返回给外部。接口版本管理也是可维护性的一部分，在接口路径或者 HTTP 头部加上版本号，就可以实现接口的平滑升级，使旧版客户端在一段时间内仍然可以正常使用。

二、接口类型与协议

电力信息系统当中，依据应用情况以及技术堆栈的不同，接口千差万别，协议各不相同。从底层的数据访问到上层的业务协同，选择合适的接口技术对构建高效稳定的系统来说十分重要。本部分主要分析几种主流接口类型及其在电力领域的应用特点。

（一）数据库接口

数据库接口是应用系统同数据库管理系统之间的底层通道，主要是用来执行结构化查询语言命令，完成数据的增、删、改、查等操作。电力信息系统创建

时，不论采用传统的客户关系管理，还是新兴的电网资产经营体系，都会同数据库展开多次交互。最常用两种标准数据库接口是 JDBC 和 ODBC。JDBC 主要面向 Java 平台，它提供了一个标准的 API，可以使得 Java 程序同各种关系型数据库之间可以互相通信。ODBC 是通用数据库接入标准，用 ODBC 驱动程序结构的应用程序可以访问任何支持 ODBC 接口的数据库，从而实现了跨语言、跨平台的数据库访问能力。

电力行业处理大量时序数据很常见，电网传感器每秒产生的监测数据就达到百万级。这就对数据库接口的性能和稳定提出了很高的要求。现代数据库接口在设计的时候就考虑到性能的优化，使用连接池技术复用数据库连接，减少建立和关闭连接所造成的开销，采用批处理的方式，把多个数据库操作合并成一次网络往返，大大提高了数据写入的速度。根据具体场景数据库接口有异步查询、流式数据处理等，可以满足电力系统实时监测和大数据分析的需求。

选择合适的数据库接口技术，要按照开发语言，目标数据库种类，性能要求以及团队对技术的熟悉程度来决定。

数据库接口选择要点

特性 / 考量因素	JDBC	ODBC	原生驱动程序	标准化程度
开发语言支持	Java 原生支持，生态成熟	支持多种语言开发，适合混合技术栈	针对特定数据库产品，提供最佳性能	降低应用程序与特定数据库的耦合度
性能与功能	生态成熟，工具丰富	跨语言、跨平台存取能力	通常提供最佳性能和最全面功能	有助于未来数据库迁移，提升灵活性
应用场景	Java 应用程序	多种语言开发的混合系统	性能要求极致、需特定功能时	提高系统的灵活性和可维护性

通过上表可以知道 JDBC 是 Java 原生支持，生态完善，工具齐全，ODBC 支持多语言开发，适合混合技术栈。就特定的数据库产品而言，原生驱动程序一般能够提供最佳的性能以及最全面的功能支持，在性能要求极高的情况下，可能会跳过通用接口标准，直接使用数据库厂商提供的专用接口库。遵循 JDBC 或者 ODBC 的标准可以减小应用程序和特定的数据库之间的耦合度，这样在以后迁移数据库产品的时候，可以显著减少应用程序的代码改动量，提高系统的灵活性和可维护性。

（二）Web 服务接口

Web 服务接口是目前分布式系统中集成度最高的一种方式，它通过标准的 Web 协议（主要是 HTTP）来进行通信，因此非常适用于跨网络、跨平台的系统之间的交互。电力信息系统内部 ERP 和 SCADA 等各个业务系统之间，以及电力信息系统与银行、政府等外部机构之间数据交换，Web 服务都处于非常重要的位置。两种主要的 Web 服务实现风格就是 SOAP 和 RESTful API。SOAP 是一种严格的基于 XML 的协议，有完整的标准体系，包含 WSDL 来描述服务，WS-Security 来控制安全。SOAP 因为具有很强的严格性，所以依然被应用在要求极高的交易原子性保证等事务性的、安全性的、可靠性的企业级应用上（如电费支付接口）。

相比于 SOAP 的重量级，RESTful API 更轻量、灵活，它是一种架构风格而不是具体的协议，主要体现在资源、统一接口、无状态通信、可缓存性等设计原则上。RESTful API 一般用 JSON 作为数据交换格式，其简洁易读的特点使得开发和调试更加方便，也更适应移动应用和前端应用的调用。电力物联网中有大量的智能电表、传感器需要将采集到的数据上传到云平台，使用轻量级的 RESTful API 通信可以降低终端设备的能耗和网络流量。设计良好的 RESTful API 用 URL 来定位资源，用 HTTP 动词表示操作，用 HTTP 状态码返回结果，达到直观高效的交互。

在构建现代电力信息系统的时候，RESTful API 一般会被作为首选。其灵活性和低耦合性正好与目前的微服务架构相匹配。每一个微服务都可以利用 RESTful API 对外公布自身的业务能力，各个服务之间通过调用 API 来完成复杂的业务流程。这样就使得系统更加容易进行扩展与维护，单个服务的更新部署不会影响整个系统。虽然 SOAP 仍然存在在某些领域，但是由于 RESTful API 的简单高效和良好与 Web 之间的兼容性，它已经成为电力信息服务体系中技术的主流。

（三）消息队列接口

消息队列接口属于异步、解耦的通信方式，在电力系统实时数据采集、事件驱动架构、系统削峰填谷等方面有着无法取代的作用。与同步调用的 Web 服务不同，消息队列可以让生产者在把消息放到队列之后马上返回，不需要等消费者的处理结果，这样就大大提高了系统的响应速度和吞吐量。电力系统当中，异步特性显得格外重要。以电网调度指令下发为例，采用消息队列可以保证各个执行

单元接收到指令，即使有的单元暂时离线，在恢复连接之后仍然可以接收到指令并执行指令。

MQTT 是为物联网设计的轻量级发布 / 订阅模式消息协议。协议开销小、网络带宽要求低，可以提供不同的服务质量等级以保证消息可靠传送。这就使其非常适合于电力系统中分布广、网络环境不稳定的各种终端设备，如智能电表、配电终端、环境传感器等等。设备采集到的状态数据、告警信息等以 MQTT 消息的形式发布到中心服务器，达到大量设备实时监控和数据汇总的目的。

Apache Kafka 是高吞吐量、分布式的流处理平台，可以对海量数据的实时管道进行处理。电力大数据应用中 Kafka 起着数据总线的作用。来自全省数千万智能电表的用电数据可以实时流入 Kafka 集群，后端的大数据分析平台、计费系统、负荷预测系统等作为消费者，按照需要订阅并处理这些数据流。Kafka 的持久化存储以及高可靠性可以保证数据不会丢失，水平扩展性可以应对业务增长所引发的数据洪峰。MQTT 采集数据接入 Kafka 后，就形成了完整的物联网数据链路，从终端感知一直到云端智能分析都可以实现。

三、接口规范定义

清晰明确的接口规范是实现高效协作、保证产品质量的前提。它就像技术世界里的“法律文本”，是接口实现者和调用者共同遵守的标准。一套完整的规范定义要包含技术细节，数据格式，版本管理策略等等，使得接口在其生命周期内始终保持清晰，稳定，兼容。

（一）接口定义语言

接口定义语言是用来描述软件组件接口的一种规范化语言，主要价值在于用一种独立于具体编程语言的中立的方式来表述接口。开发者使用接口定义语言来定义接口名称、方法、参数的数据类型、返回值以及可能抛出的异常等，之后再由编译器将接口定义语言文件编译成对应编程语言（Java、C++、Python）的接口代码。这使不同的客户端和服务端用不同的语言开发，但仍然能理解同一个接口契约并正确通信。

电力行业的复杂异构系统中，接口定义语言的应用价值就显得更加突出。一个用 C++ 编写的底层电网仿真系统需要给上层用 Java 编写的调度应用提供计算服务。使用接口定义语言来定义服务接口，可以自动生成 C++ 服务端骨架代

码以及 Java 客户端存根代码，开发者只需要填写业务逻辑即可，不需要面对跨语言数据类型转换和底层通信细节等复杂问题。这不但可以大大提高开发效率，而且从根本上保证了接口的正确性和一致性，避免了由于人的理解偏差或者编程错误造成的接口集成问题。常用的接口定义语言技术体系有 CORBA、Thrift、WSDL，WSDL 在 Web 服务中使用最广。

（二）数据格式与编码规范

数据格式以及编码规范属于接口定义的重要部分，它关乎到数据传输的速度快慢，是否容易被人读懂，能否与其他系统顺利衔接。现代电力信息系统中用得最多的两种数据格式是 JSON 和 XML。因为 JSON 具有简洁、轻量、机器易于解析、人类易于阅读等特点，所以成为 RESTful API 最常用的数据格式。由于 XML 具有很强的结构化表达能力以及丰富的标准支持，因此 SOAP Web 服务等场合下仍然使用 XML。制定数据格式规范时应该确定数据对象的结构、字段命名规则（驼峰命名法）、空值处理方式、必填字段等。

编码规范同样至关重要，它确保数据在不同系统间传输时不会失真。

1. 字符集规范，所有接口通信统一使用 UTF-8 编码，这是处理多语言、特殊字符的行业标准，可以防止乱码。

2. 数据类型映射：应该给出逻辑数据类型（例如日期、时间、高精度小数）到物理数据格式转换的规则。所有日期时间字符串必须使用 ISO 8601 格式（如 2025-12-08T10:30:00Z），所有涉及金额或者电量的数值都必须用字符串传输，防止浮点数精度问题。

3. 枚举值定义：状态、类型等枚举字段需要给出完整的枚举值列表及其含义，不能使用魔法数字。

（三）接口版本管理与兼容性

在电力信息系统的长期发展过程中，由于业务需求和技术架构的变化，接口变更几乎是必然。有效的接口版本管理以及兼容性策略是保证系统可以顺利升级、防止服务中断的重要手段。缺少版本管理会带来牵一发而动全身的问题，对接口做一点小的调整都会让现有的客户端瘫痪，造成巨大的更新成本和风险。因此，接口设计之初就应加入版本管理机制。常见的做法就是把版本号作为一个 URL 的参数，或者在 HTTP 请求头的 Accept 字段中进行指定。

兼容性策略的核心原则就是向后兼容。对非破坏性变更 (如增加可选参数或

者修改返回数据中的字段等)，可以在旧版本接口基础上进行修改，不会影响到现有的客户端使用。对删除字段、修改字段的数据类型或者改变核心业务逻辑等破坏性的修改，需要创建新版本接口。新版本接口发布后，旧版本接口不应该立即被废弃，而应该设置过渡期，并通知所有调用方进行升级。

在转型期，新的旧的接口应该同时运行，利用监控工具分析旧的接口调用情况。等所有或者大部分客户端都升级到新版本之后，才可正式下线旧版本接口。下线前将旧版本标记为废弃，响应中添加提示信息，引导未升级客户端更新。有条理、受控制的版本演进过程，可以最大程度上减少由于系统升级而带来的风险，保证电力业务的连续性、稳定性。

第四章 电力信息系统开发技术

第一节 软件开发方法

软件开发方法选择直接关系到项目是否能够成功。不同的软件开发方法论适合于不同特点的电力项目。本节主要对电力信息系统建设中常用的几种开发方法进行介绍，并对其适用场景以及优缺点进行分析。

一、瀑布模型及其在电力系统中的应用

瀑布模型是一种传统的、经典的软件开发模型，以严格的流程、文档驱动为主要特点，现在仍然被电力行业的部分大型信息化项目和需求稳定的项目所采用，对电力行业的软件工程实践产生了深远影响。

（一）阶段划分与文档驱动

瀑布模型把软件生命周期划分成需求分析、系统设计、编码实现、测试、部署、维护等固定的阶段，且阶段是线性的。每一个阶段都必须在前一个阶段结束后才能开始，整个开发过程就像瀑布一样一层一层地往下推进，不能回头。此模式重视计划的预见性以及流程的严密性，在项目开始时就要确定所有细节。

该模型最大的特点就是文档驱动。每一个阶段都会产生大量的、规范的文档，比如需求规格说明书、概要设计说明书、详细设计说明书等。这些文档既是阶段成果，又是推动下阶段工作的唯一依据。该做法在电力系统中的优势就是能有效地传递和存档知识，为系统长期运维、升级以及合规审核打下基础，保证关键系统的可追溯性以及可维护性。

在电力调度自动化系统、变电站监控系统等关键基础设施的建设中，瀑布模型的阶段划分和文档驱动的特点就显得更加重要。由于该类系统对安全、可靠性要求很高，任何一个环节出现疏漏都会造成严重后果。经过严格的评审程序之后，每一个设计决定、每一个功能达到都要有充分的论证和验证过程，从而把项目风险降到最低。

（二）适用于需求明确的项目

瀑布模型成功的前提条件就是项目初期必须有全面、清晰、稳定的需求。因为一旦在设计阶段需求被冻结，之后任何的修改都会造成巨大的成本和时间的浪费，甚至造成项目的返工。因此它最适合于业务逻辑成熟、功能边界明确、在可预见的将来不会发生重大变化的项目。

电力行业许多重要的业务系统都具有这样的特点。像电费计费和收取系统，核心的算法以及业务流程被国家政策和行业标准严格规范着，需求是比较固定的。电网继电保护定值管理系统、电力设备资产管理系统等，功能需求大多都是根据多年的运行经验以及既定的管理规范来确定的，变化不大。在这些项目中使用瀑布模型，可以依靠周密的计划和结构化的流程，保证系统建设的质量和进度，实现可预测的交付。

（三）优缺点分析

瀑布模型属于一种历史悠久的开发范式，它的优点和缺点都很显著，电力系统项目在应用的时候，其效果同样具有两面性。其结构化是优点同时也是主要的局限性，项目团队在选择的时候应当依照实际情况加以考虑。

瀑布模型的优势与劣势，具体可参见下表：

瀑布模型优缺点对比表

优点	缺点
阶段划分清晰，职责明确	模型僵化，缺乏对需求变化的适应能力
为项目管理提供便捷框架和检查点	难以应对电力市场化改革或新技术引入带来的业务动态调整
高度重视文档完整性、规范性，形成宝贵知识资产	开发周期冗长，用户反馈滞后
极大地便利了后期系统维护、交接与升级	用户往往在项目最终阶段才能看到可运行系统
适用于需求稳定、技术方案成熟的电力项目	风险暴露集中于后期
能通过严格流程控制确保软件质量	测试阶段发现的设计缺陷可能导致高昂的修复成本

电力行业里对可靠性、安全性、规范性要求极高，需求稳定，属于传统核心系统的项目仍然可以使用瀑布模型。但是对于需要快速应对市场、用户的新业务系统，采用更加灵活的开发方式。

二、敏捷开发方法

面对快速变化的市场环境和技术革新，在以用户体验、数据应用等新兴电力业务为主的领域中，敏捷开发方法由于具有灵活、快速的反应特点，渐渐成为一种重要的补充或者替代方式，使开发模式发生转型。

（一）Scrum 与看板方法框架

敏捷开发实践当中，Scrum 是具有代表性的框架之一。它不是一套详细的流程或者技术，而是一个用于管理和控制复杂产品开发的框架。Scrum 的核心是以许多短周期的迭代为基础，称之为冲刺，一个冲刺一般为两周到四周。每次冲刺都会产生出一部分产品功能。该框架定义了产品负责人、敏捷教练以及开发团队这三个关键的角色，另外还有五个事件以及三个工件一起促使团队合作并保持进度透明。

看板方法是另一种流行的敏捷实践，它更注重工作流程的可视化以及持续交付能力的提升。与 Scrum 以时间盒为单位的迭代不同，看板方法是一种基于流程的实践，它有以下四个核心原则，可视化工作流、限制在制品数量、管理流动、明确过程策略。团队成员把待办事项列表中的任务“拉”到看板上，任务卡片随着工作的推进，在看板上不同列之间来回移动，直到完成。特别适合运维支持、缺陷修复这些流入没有规律、优先级经常变化的工作。

Scrum 与看板方法在电力信息系统开发中的特性和适用场景对比可见下表：

Scrum 与看板方法对比表

特性	Scrum	看板方法
核心理念	基于时间盒的迭代开发，增量交付	基于持续流的工作可视化与管理，优化交付流程
关注点	复杂产品的开发与管理，团队协作与透明化	工作流的可视化，限制在制品，管理流动，持续改进
迭代周期	固定时间盒（“冲刺”），通常 2-4 周	持续流动，无固定迭代周期
角色	产品负责人、敏捷教练、开发团队	角色更灵活，通常有服务请求者、服务提供者等
主要实践	每日站会、冲刺计划、冲刺评审、冲刺回顾	可视化工作流（看板）、限制在制品、管理流动、明确过程策略
适用场景	新产品 / 新应用开发，需求探索性强，项目范围较大	现有系统维护与持续改进，需求流入不规律，优先级频繁变动

在电力信息系统的开发中，Scrum 框架适合于开发新产品或者新的应用，如开发一套全新的分布式能源管理平台。而看板法则更适合于对已有系统不断改进与维护的情形，如电网调度中心处理用户的反馈及功能改善请求，能够助力团队用稳定有效的方式去应对一连串不断出现的新需求，从而加强响应能力。

（二）迭代开发与快速响应变化

敏捷开发的主要思想就是迭代增量地交付。它把庞大复杂的项目分解成一个个可以掌控的小块，再通过一系列短周期的开发阶段（也就是迭代）去一个个实现。每次迭代结束时，都会交付一个可以工作、有商业价值的软件增量。增量功能虽然不完全，但是已经可以演示、测试、评估。

该模式最大的优点就是可以快速响应变化。传统瀑布模型中用户的反馈通常在项目后期才能获得，这时做修改的成本非常高。敏捷开发中，在每个迭代周期结束后会召开评审会议把业务方、最终用户这些重要利益相关者邀请过来。他们可以试用最新的软件版本，随时给出反馈。根据这些建议，在下一轮的开发中做出优先级的调整、设计的修正或者新增功能，从而使得产品能够更好的满足用户的需要、适应市场的发展。

（三）在电力系统项目中的实践

敏捷开发方法被广泛地应用在电力信息系统建设当中，对于那些与用户交互较多、需求具有探索性质的领域来说，更加适合采用敏捷开发方式。面向一线运维人员的移动巡检应用、面向电力客户的能效管理服务平台、面向管理层的决策支持数据可视化驾驶舱等，都特别适合用敏捷的方式来做。

用开发一套新能源功率预测系统来举例的话，业务需求由于算法研究的深入以及市场规则的变化而不断演进。如果使用敏捷 Scrum 框架，在第一个冲刺中就可以交付基于基础算法的预测原型，然后和电网调度员、交易员一起评审。根据反馈在后续冲刺阶段可以逐步加入更复杂的气象数据源、优化机器学习模型或者改善预测结果的表现形式。这种渐进式开发方式保证了系统功能一直和实际的业务需求保持一致，有效的避免了项目后期高昂的重构成本。

结构复杂的大型电力系统，如新一代配电自动化系统，一般会采用瀑布与敏捷相结合的混合模型。其中，系统的核心平台、底层通信协议等基础架构部分由于对稳定性、标准化要求很高，采用类瀑布模式进行规划、设计。上层应用功能模块（如故障定位分析、线损管理、电能质量监测）可以分成多个并行开发小的

敏捷团队，保证核心系统的稳定又保持上层应用的灵活性。

三、DevOps 开发运维一体化

DevOps 是一种先进的软件开发和交付理念，它把文化、实践、工具融合起来，打破开发与运维之间的壁垒，依靠自动化、协作，加快电力信息系统的价值交付速度、可靠性、频率，满足数字化转型的需求。

（一）持续集成与持续交付

DevOps 理念下的主要实践就是打造自动化的软件交付流水线，而持续集成和持续交付则是这条流水线的两个主要技术支柱。它是一套为了缩短软件从开发到上线部署的周期所使用的方法和原则。

持续集成需要开发人员不断的把修改合并到共同的主干分支上。每次合并都会触发构建过程并运行一系列的自动化测试。能够尽早发现代码模块间的集成错误，防止小问题积少成多从而有效提高代码质量以及开发效率。对于协同开发复杂的电力市场交易系统来说，持续集成可以保证各个功能模块一直能很好协作。

持续交付在持续集成的基础上，把经过全部自动化测试的代码自动部署到类生产环境。这就意味着软件已经处于随时可以发布的状态。一般而言，是否将应用部署到生产环境是由人工来决定的，并且还需要得到业务部门的批准。这样既可以完成交付过程的自动化，又可以保留对上线时机的最终控制权。

持续部署是持续交付的延伸，整个流程完全自动化，所有通过测试的代码更改直接、自动地部署到生产环境。电力方面，高度自动化的持续部署一般只适合于风险较低的非核心系统，比如企业门户网站内容更新、内部管理工具功能迭代等，以此来达到最快的价值交付速度。

（二）自动化测试与部署

自动化成为 DevOps 价值产生的发动机，自动化测试、自动化部署又是软件快速交付高质量的重要保证。快速迭代的开发节奏下，传统的依靠人工测试、部署的方式已经不能适应，必须使用自动化的方式来保证流程的高效、可靠。

自动化测试存在于完整的持续交付流水线当中，成为了一道可靠的品质防线。在电力信息系统中一般会建立分层的自动化测试体系：

1. 单元测试是对代码中最小的可测试单元，即函数或者类进行测试，保证基本逻辑的正确性，是保证代码质量的基础。

2.2、集成测试：验证各个模块或者服务之间接口对接、交互是否正常，例如营销系统和财务系统数据交换接口的测试。

3. 性能测试，模拟高并发用户访问或者海量数据处理的情况，对用电信息采集系统、负荷预测系统等进行压力测试，保证系统在高负载的情况下可以稳定、及时地响应。

4. 安全测试，采用静态代码扫描，动态渗透测试等自动化手段对系统进行测试，主动找出系统中存在的安全漏洞，这对保护重要的电力基础设施不受网络攻击有着非常重要的意义。

自动化部署主要是对软件经过测试之后如何安全、平稳地部署到生产环境这一问题的解决。蓝绿部署、金丝雀发布等高级部署策略在电力系统中有重要应用。例如，在电网调度主站升级应用模块时，可以采用金丝雀发布方式：将新版本先推送给少部分调度员使用，验证无误后再逐步扩大发布范围，最后覆盖全部用户。此种方式可以最大程度降低上线变更带来的风险，保证核心业务的连续性。

（三）文化与工具链的构建

成功的 DevOps 实践，技术工具固然重要，但是更深层次来说它更需要组织文化上根本性的转变。DevOps 反对长期以来存在于开发和运维团队之间形成的“部门墙”，提倡一种沟通、协作、共同负责的新工作文化。在这样的文化之下，团队成员共同对应用的整个生命周期（设计、开发、运维）负责。失败不再被认为是个人的或者团队的过错，而是当作为整个团队学习与改进的机会，用事后无指责复盘来持续改善流程。

为了支持协作文化，需要有一条集成化的工具链，把软件交付过程中每一个环节都自动化、标准化。它不是单一的产品，而是不同阶段各种工具相互配合的结果。它就如同数字化的流水线，保证代码从开发者的电脑流向生产环境时的高效、可靠。

电力信息系统 DevOps 实践的典型工具链组成是使用 Git 等版本控制工具对代码进行管理、协同开发，使用 Jenkins 等持续集成服务器对构建、测试、部署的过程进行自动化，使用 Docker 等容器化技术、Kubernetes 等编排平台为电力应用提供一致、可移植、弹性伸缩的运行环境，不管是私有云还是公有云。

工具链里还得有基础设施即代码工具，像 Ansible，用来自动配置服务器和环境，保证开发、测试、生产环境一致。强大的监控和日志分析工具，比如

Prometheus，Grafana，ELK Stack，是电力系统健康运转的“眼睛”和“耳朵”，可以对系统运行情况实施监视并加以剖析，让运维人员可以及时察觉并处理问题，进而达成从开发到运维的闭环反馈。这种文化合力、工具的合力就是电力企业能于数字时代保持竞争力的秘密。

第二节 系统集成技术

电力信息系统建设的复杂性表现在它由很多异构的子系统组成，有电网调度系统、营销收费系统、资产管理系统、新能源监控系统等等。系统集成技术就是破解“信息孤岛”的重要方法，它所要达成的主要目的就是让数据、应用、流程无痕对接，进而形成起统一、协同、高效的整体信息化架构，这样就能有力地支持电力企业各项业务做到精细化运作和智能化决策。

一、点对点集成技术

点对点集成是直接且传统的系统连接方式，在两个指定的应用系统之间建立专用通信线路。该模式因为实现简单、开发周期短，在电力系统信息化建设初期被广泛使用。可以快速满足特定业务环境的消息交互需求，但是随着系统数量的增多，网状连接模式的维护和管理会变得越来越困难。

（一）应用程序接口

现代点对点集成主要的方式为应用程序接口调用。它采用事先规定的函数、协议和工具，使不同的系统可以进行标准化的服务请求和数据交换。应用程序接口给出明确的调用契约，把复杂的内部逻辑包装起来，使调用方不必关心被调用系统具体的实现。在电力方面，应用程序接口常用于实时性要求较高的场合，新能源发电预测系统会调用电网调度系统的接口，将预测的功率曲线实时上报；调度系统也可以通过接口对可调节负荷资源发出控制指令。不但可以完成系统之间松耦合的设计，更为构建开放电力数据服务生态打下技术基础。

（二）数据库直连

数据库直连是一种比较原始的集成方式，即一个应用系统在获得授权后，直接连接到另一个应用系统的后端数据库，对数据库中的数据进行读取或者写入。技术上实现起来非常简单，省去了开发接口的过程，适合内部系统之间简单的、

非核心的数据查询和同步需求。然而，电力信息系统中这种方式存在较大的风险：破坏了应用系统封装性和独立性；造成系统之间高度技术耦合；直接访问数据库可能会对源系统性能产生影响，甚至会引发数据锁死等严重的问题；把数据库访问权限暴露给外部系统，也会带来严重的数据安全隐患。鉴于上述风险，现代电力信息系统架构设计中数据库直连方式一般不被采用。

（三）文件交换

文件交换是一种历史悠久且至今仍被广泛使用的集成方式，尤其适用于批量化、非实时数据的传输。

1. 其基本流程为源系统按一定格式（CSV、XML 或报文格式）批量产生待交换的数据文件。

2. 随后，通过文件传输协议、共享网络目录或专用文件传输系统，将文件发送至目标系统。

3. 目标系统收到文件之后，再做解析和加载处理。在电力企业里，文件交换常指跨越网络安全区域的交换，把生产控制大区的运行数据定时汇总到管理信息大区加以统计分析，或者和外界单位交换数据，批量处理银行代扣电费的回盘文件，定时向监管机关报送统计报表等等。这种方法的优点是简单可靠，可以支持大数据量的传输。它的缺点是实时性差，文件完整性校验、错误处理和安全审计等还需要另外的机制来保证。

点对点集成模式的几种主要技术及其特点可见下表：

点对点集成技术比较表

特性	应用程序接口	数据库直连	文件交换
实现复杂度	中等	低	低
实时性	高	高（存在潜在风险）	低
耦合度	较低	极高	适中
数据安全性	较高	低	中等（需额外机制保障）
适用场景	实时服务调用、开放生态、业务系统互操作	简单查询、非核心数据同步、内部系统辅助集成	批量数据传输、跨安全域数据交换、非实时数据同步

二、基于中间件的集成技术

随着电力系统信息化的规模越来越大，复杂性越来越高，点对点集成模式的“蜘蛛网”式缺点也越来越明显。随着中间件出现，一种新的系统间集成技术也

被开发出来，它用一个独立的中间层来管理各个应用系统之间的通讯、转换、协同工作。大大降低系统的耦合度，提高整个系统架构的灵活性、扩展性、可维护性。

（一）消息中间件

消息中间件属于异步通信集成方案的一种，它借助生产者 - 消费者模式或者发布 - 订阅机制的消息队列，从而让应用程序可以彼此独立。发送方（生产者）把消息放到中间件里，不用立刻关注接收方（消费者）是否在线或者准备就绪；接收方会在适当的时机从中间件中取出消息并处理。这种异步通信方式可以提高系统的整体可用性，还可以削峰填谷。电力系统中消息中间件的应用场景十分丰富，遍布电网的智能传感设备可以将自己所采集的海量实时状态数据（电压、电流、温度等等）作为消息发布到消息中间件上，供状态监测、故障预警、负荷分析等等各个后端系统根据需要进行订阅和消费，这样既保证了数据能够被可靠的分发出去，又避免了采集前端直接与多个应用系统相连带来的复杂性和性能问题。在营销业务当中，用户在线缴费请求可以被消息队列所缓冲，后台处理系统能够按照自身的处理能力平稳地进行处理，从而有效地抵御业务高峰期的冲击。

（二）应用服务器

应用服务器给应用程序提供标准、稳定、高效的运行环境，事务管理、安全控制、连接池、集群支持等一系列通用服务功能也在其中。它既起着承载核心业务逻辑的作用，又是重要的整合中心。电力企业的重要业务系统例如营销系统、客户关系管理系统或者资产全生命周期管理系统等等，一般都会运行于高性能应用服务器上。该系统利用应用服务器给出的标淨接口以及框架与其他系统进行交互，从而达成复杂的业务流程。应用服务器把底层技术复杂性有效管理起来，开发人员就可以集中精力于业务逻辑实现，加快了应用开发、集成，并保证企业级应用具有较好的可扩展性和稳健性。

（三）企业服务总线

企业服务总线是比传统中间件集成架构模式更全面、更高级的一种中间件集成架构模式，被比喻为企业应用的“中央神经系统”。

1. 企业服务总线为所有需要交互的应用系统提供了一个标准的“总线”，所有的应用系统都连接在这条总线上，通过服务的方式进行通信。它不仅仅是简单的消息传送者，而且是具有协议转换、数据格式转换、服务路由、服务编排和安全监控等功能的强大服务中介。

2. 大型电力集团存在大量异构的老旧系统以及新建系统，这些系统所使用的技术、协议、数据标准可能不一样。企业服务总线可以扮演适配器和转换器的角色，把异构服务统一包装成标准的服务接口，然后发布到总线上。

3.3、例如，基于现代微服务架构新建的客户服务门户，可以通过企业服务总线调用仍在运行的、使用专有协议的陈旧计费系统的功能，不需要对这两个系统做任何代码修改。企业服务总线对企业复杂集成拓扑结构进行集中管理控制，极大地简化了集成工作，是面向服务的架构的重要基础设施。

三、数据集成技术

系统集成指的是不同应用间的交互、流程联动，数据集成技术的主要目的就是将各个系统的数据汇聚、整合、管理起来，消除各个系统之间数据的壁垒，形成统一、准确的数据资产全貌，为企业数据分析、业务洞察、智能化决策奠定坚实的基础。电力行业属于数据密集型行业，因此数据集成就显得尤为重要。

（一）抽取、转换、加载

抽取、转换、加载是数据整合领域最经典、最重要的技术过程。

抽取阶段就是从用电信息采集、财务管理、设备管理系统等各个业务系统源数据库中提取所需要的信息。

转换阶段是 ETL 的核心，把抽取出来的异构数据进行清洗（剔除错误、重复项）、转换（统一数据格式、单位、编码标准）、规整（匹配、合并来自不同源的数据），使其符合目标数据仓库或者数据集市的预定义模型和标准。

加载阶段是指把经过变换的高质量数据保存在目的存储介质(例如数据仓库) 里，供以后分析使用。电力企业 ETL 流程对各种业务分析主题的创建有着广泛的应用，也就是通过 ETL 将客户档案、电量电费、缴费行为等数据进行融合生成客户统一视图以支持精准营销、信用评价等。

（二）数据仓库与数据湖

数据仓库、数据湖是现代数据集成架构中两种主要的存储形式，两者相辅相成。数据仓库是面向主题、集成、相对稳定、反映历史变化的数据集合，存储的是经过 ETL 处理后结构化、高质量的数据，主要用来支持企业级商业智能报表、在线分析处理和常规决策分析。电力企业经营分析数据仓库可以给管理者提供售电量、线损率、电费回收率等主要指标趋势分析和多维钻取功能。数据湖是以原

始格式存储海量结构化、半结构化、非结构化数据的设施，例如 SCADA 系统每秒产生的时序数据、无人机巡检图像视频、气象数据、社交媒体文本等。数据湖的主要目的就是给高级数据探索、数据科学实验、人工智能模型训练等提供支持。电力企业对数据湖中的大量数据进行训练，就可以建立负荷预测模型、设备故障诊断模型等，从而达到更好的数据价值挖掘效果。

（三）主数据管理

主数据管理就是一套保证企业核心业务实体（主数据）在各个信息系统中的一致性、准确性、完整性的规则、技术、解决方案。电力企业中主数据主要是客户、电表、变压器、员工、供应商等实体。由于营销、生产、财务、人资等不同业务系统会创建和维护这些实体的信息，所以就会出现数据不一致、不完整、重复等问题。主数据管理依靠创建权威且集中的“黄金记录”来源，凭借数据集成和同步机制，保证各个系统在引用这些核心实体的时候，都能指向同样的准确数据。对于跨业务条线流程贯通、数据分析等来说都起着至关重要的作用，比如，如果要给大客户提供“一户一策”精准服务，那么首先得有一个统一的客户主数据视图来支持。

第三节 数据采集与处理

数据是电力信息系统的生命线，也是实现电网智能化、运营精益化、服务优质化的基石。数据采集和处理属于数据价值链的起始环节，数据采集技术和数据处理技术是否先进、是否规范，直接关系到上层应用分析的深浅。本节主要对电力系统中多源数据采集、预处理和实时处理的技术做系统的阐述。

一、数据采集技术

电力信息系统的数据来源广泛、形式多样，包括生产运行、经营管理等各方面的数据。有效的数据采集是进行数据分析的前提，根据数据源的特点，采取不同的技术手段，以保证数据的全面性、准确性和及时性。

（一）SCADA 系统数据采集

SCADA 系统是电力系统运行监控的核心，也是生产控制域最主要的来源。它就是利用厂站、变电站、线路等的远程终端单元来对电网的重要运行参数实施

实时的采集。数据是保证电网安全稳定运行的基础，具有高实时性、高可靠性。

采集的数据分为三种，模拟量，数字量，电能量。模拟量数据如电压、电流、有功功率、无功功率等是反映电网实时运行状况的连续变化的物理量。数字量数据，又叫状态量，是指开关、刀闸的分合位置等离散的状态信息，用来判断电网的拓扑结构和设备的状态。电能量数据就是功率在一段时间内的积分，用来计量统计。

SCADA 数据采集一般会用到 IEC 60870 系列、DNP3 或者 CDT 等工业通信协议。数据通过专门的网络从各个远动终端集中到调度中心的主站系统。在建设过程中要解决不同厂商设备、不同版本协议之间兼容性的问题，一般采用协议转换网关或者标准接口的方式，接入和解析不同异构数据，给全网统一视图和高级应用提供可靠的数据支持。

（二）物联网数据采集

伴随着物联网技术的发展，其在电力系统中应用也越来越广泛，数据采集的范围和精度也随之扩大。物联网相较于主网、重要枢纽变电站所采用的 SCADA 系统来说，可以深入到配电网、用户端乃至新能源发电装置的“毛细血管”中去，从而实现对大量终端设备的全面连接和感知。

物联网数据采集对象很多，有智能电表采集的用电信息，配电网自动化终端采集的线路故障信息，输电线路上的微气象和覆冰监测装置数据，变压器等重要设备的在线状态监测数据，还有无人机，机器人巡检采集的高清图像和视频数据。这几种数据呈现出的特点是数据量大、数据类型丰富、时间空间不统一。物联网采集技术一般采用无线通信方式，如 NB-IoT、LoRa、4G/5G 等，以满足不同应用场景下成本、功耗、带宽等各方面的不同需求。在采集架构上，由于边缘计算节点的加入可以对数据进行初步清洗、聚合、特征提取，从而减少中心云平台的计算和存储压力，并且可以满足一些业务场景对于低时延响应的需求，所以边缘计算节点的加入变得十分必要。

（三）日志文件与业务数据采集

除了物理世界中运行感知数据之外，电力信息系统自身运行产生的日志文件、支撑企业经营管理工作开展的业务数据也属于重要的数据资源。这些数据对于 IT 系统运维、网络安全态势感知、客户行为分析、经营决策优化来说都是不可缺少的。

日志文件数据来自于服务器、网络设备、安全设备、数据库、应用程序等各种来源。它们用半结构化文本格式记录系统运行状态、用户操作、异常告警等信息。使用日志采集工具 (Filebeat、Logstash) 集中收集解析分散的日志，可以建立统一的运维监控平台，快速发现故障，有效跟踪安全事件。业务数据被存放在电力营销系统、客户关系管理系统、资产管理系统等各种业务数据库中。这些数据一般是结构化的，可以采用数据库同步、接口调用或者 ETL（抽取转换加载）工具来实现数据的采集。把这几种业务数据同电网运行数据混合起来加以分析，就能产生新的价值，像把用电数据同客户档案融合起来做精确的负荷预测，或者把资产数据同设备的状态数据混在一起，从而改进检修计划。

二、数据预处理技术

各种来源的原始数据一般都会有“脏数据”问题，即格式不统一、内容不全、数值异常、信息重复等，不能直接用于高级分析或建模。数据预处理指对原始数据进行清洗、变换、规约等操作，目的是改善数据质量，使数据可以被后续的数据分析和挖掘所使用。

（一）数据清洗与缺失值处理

数据清洗属于数据预处理的第一步，主要目的是找出并修正数据中的错误、不一致性以及异常之处。电力系统数据中的噪声和异常值大多是由传感器故障、通信干扰或者人为录入错误造成的。处理好这些问题才是保证分析结果准确的前提。

1. 异常值处理：异常值指的是数据集中与其他大多数观测值相比明显不同的那些数据。检测方法有基于统计的方法（3 σ 原则、箱线图）、基于距离的方法（K 近邻）和基于密度的方法。识别出的异常值根据业务逻辑决定剔除或者修正（用相邻值的平均数或中位数替换），也可以作为重点关注的事件进行处理。

2. 缺失值处理，数据缺失在电力系统中十分常见，传感器临时离线就会造成某时间段数据的缺失。处理缺失值的方法有很多，简单的删除有缺失值的记录会丢失信息。常用的方法是进行插补，例如用均值、中位数或众数来填充；对于时序数据，可以采用前后时刻数值的线性或样条插值；也可以建立预测模型（回归模型、K 近邻算法）来预测缺失值。根据数据特点以及缺失率来决定采用哪种方法。

3. 不一致性的处理，单位不一致、编码冲突、命名不规范等属于数据不一致

的情况。各个变电站上报的电压数据有的用伏特，有的用千伏。建立元数据标准、数据字典，把不一致的数据规范转换起来，这样就能在全区域范围内做到有效的比较与分析。

（二）数据变换与规范化

数据变换就是把数据从一种形式变成另一种更有利于分析的形式。数据规范化属于数据变换的一种类型，它的目的在于抹除数据在量纲以及取值范围方面的差别，使得各个指标之间可以相互比较。这对于许多依靠距离计算的机器学习算法（支持向量机、K 近邻等）来说尤其重要。

数据变换的方法有对数变换、平方根变换等，可以改变数据的分布，把偏态分布的数据转换成接近正态分布的数据，使它符合一些统计模型的假设条件。在实际运用当中，对于原始的负荷数据进行对数变换之后，有时会发现模型的预测精度有所提升。

最小 - 最大归一化把原始数据线性地映射到所指定的区间中，即 [0，1] 或者 [-1，1]。Z-score 标准化，又叫标准化，把数据转换成均值为 0、标准差为 1 的分布。选择什么样的规范化方法，要根据后续分析模型的要求以及数据本身的特性来决定。

（三）数据规约与降维

对于电力系统海量、高维的数据特征，用数据规约技术来减少数据量，提高数据处理和分析的效率，并尽可能保留原始数据集中重要的信息。数据规约可以在行和列两个方面进行。

属性规约，也就是降维，是处理高维数据的关键技术。电力系统监测数据中很多变量之间存在很强的相关性，同一个母线下的各个馈线的电压波动有很强的同步性。主成分分析是经典的线性降维方法，它用线性变换把原始高维特征投影到一组新的低维正交坐标轴上，这些新的坐标称为主成分，可以最大程度保留原始数据的方差信息。用少量的主成分就可以在损失很少信息的情况下降低数据维度。其他降维方法还有线性判别分析，以及基于流形学习的非线性降维方法。

记录数规约是从总体中选取最能代表总体的一组数据子集。常用的方式有随机抽样、分层抽样、数据聚合。数据聚合就是将多个数据点合并成一个单独的数据点，比如将分钟级的功率数据聚合为小时级或者天级的电量数据，这对于长期趋势分析或者负荷统计非常有效。经过数据规约后一方面可以大大降低存储和计

算成本，另一方面也能在一定程度上消除噪声，使得后续的数据挖掘模型更健壮高效。

三、实时数据处理技术

智能电网对态势感知、故障预警、动态优化的需求越来越强，传统的基于批处理的数据处理方式已经不能满足业务对实时性的要求。实时数据处理技术可以对产生的数据进行即时分析，在数据产生后以毫秒或者秒为单位做出响应，给电网的即时决策提供技术支持。

（一）流处理框架

流处理框架是实时数据处理的引擎，可以对连续不断、永无止境的数据流进行计算。与批处理一次性处理整个静态数据集不同，流处理是以事件为单位，对到达的数据进行逐条或者微批次实时处理的。

Flink、Spark Streaming 是目前业界最主流的两种分布式流处理框架。Flink 被视作新一代的纯流式计算引擎，它主要支撑事件时间与处理时间，而且可以做到精确一次的状态处理。它可以实现低延迟、高吞吐的计算，提供了丰富的窗口操作（滚动窗口、滑动窗口、会话窗口），适合用于电力系统实时告警、实时监控、实时计量等场景。

Spark Streaming 是用 Spark 批处理引擎建立起来的微批次处理框架。将数据流切分成一个个的小时间片之后再使用 Spark 引擎做批量处理。虽然它的延迟比纯流处理引擎要大一些，但是可以和 Spark 生态系统中的批处理、机器学习、图计算等组件无缝对接，利于构建统一的大数据处理平台。电力信息系统创建时，要依照业务所处的延迟敏感程度和系统架构的一致性需求，来挑选恰当的流处理框架。

（二）复杂事件处理

复杂事件处理是从连续无序的事件流中发现有意义模式或者组合的一种专门技术。它不是对单一事件作出反应，而是利用事先定义好的一系列规则来实时匹配事件流，从而找到由多个简单的、具有特定业务意义的事件所构成的复杂事件。

电力系统当中 CEP 技术有着非常大的应用价值。定义一个线路跳闸故障的复杂事件模式：在一秒内检测到某条线路的电流瞬时增量超过设定的阈值之后，紧接着检测到该线路的断路器从合位变为分位并且电压为零。CEP 引擎可以实时

对相关的事件流进行监控，一旦发现匹配的模式就立即发出告警，并且联动故障定位系统。CEP 可以更好的辨别出故障情况，减少错误报警。CEP 引擎一般会提供类似于 SQL 的声明式查询语言（Esper 的 EPL），业务专家可以很方便地定义、修改事件模式，不需要编写底层代码。

（三）实时数据仓库

传统数据仓库采用离线分析的方式，一般按照天或者小时为单位进行批处理，不能实时查询决策。实时数据仓库试图弥补这个缺陷，它把流处理与传统数据仓库技术结合在一起，创建出一种能够实现实时数据接入、支持实时分析查询、并且可以对大量历史数据执行分析的统一平台。

目前实时数据仓库的流行架构为 Lambda 架构和 Kappa 架构。Lambda 架构采用并行的批处理层和速度层（实时处理层），低延迟、数据最终一致。速度层用流处理技术来提供实时视图，批处理层定时将全部历史数据重新计算，修正速度层可能会产生的误差，最后结果合并到服务层供查询。Kappa 架构是对 Lambda 架构的简化，认为所有的数据处理都应该在流处理框架下完成，用统一的流处理管道来同时满足实时和历史数据的计算需求，批处理被当作流处理的一种特殊情况，从而降低系统的维护难度。实时数据仓库可以给电网实时运行状态的全景监控、新能源出力的分钟级预测、用户用电行为的即时分析等应用场景提供强大的数据支撑。

第四节 实时监控技术

电力信息系统的稳定运行，是保证电网安全、高效、清洁发展的基础。实时监控技术属于电力信息系统运维体系的重要组成部分，类似人体的神经网络，不断感知、采集并分析系统的各种状态信息，给系统健康运行赋予即时的洞察和警报，是达成系统高可用、高性能、高安全的关键技术支撑。

一、实时数据监控

实时数据监控主要针对电力信息系统中的业务数据，如同监控生命系统血液循环一样，不仅要保证数据正常流动，还要保证数据的质量、时效性以及业务价值。对核心业务数据不断的度量与审视，可以使得决策依据准确可靠，从而实现

电力业务的精运作。

（一）关键性能指标监控

关键性能指标，也称 KPI，是反映对一个部门或整个公司业务成果和业务状况的重要数据。电力行业中的这些指标同具体的业务场景联系紧密，营销系统电费回收率、交易平台交易成功率、调度自动化系统主站可用率等都是如此。对这些指标进行监控，就相当于直接守护业务目标。一个好的、对于关键绩效指标进行监测的体系可以把复杂的系统运行情况，简化为与企业的业务目标有直接相关性、可以量化的几个数值，使管理者能在短时间内掌握整体情况，看清企业的经营活动状况。下表给出了电力系统一些重要的性能指标。

电力信息系统关键性能指标示例表

系统类别	指标名称	指标说明
营销管理系统	电费回收率	衡量电力销售回款情况的核心业务指标
交易平台	交易成功率	反映电力市场交易撮合效率与系统稳定性
调度自动化系统	主站可用率	衡量调度中心核心系统连续稳定运行的能力
生产管理系统	设备平均无故障时间	评估发电设备或输变电设备的可靠性
新能源监控系统	发电功率预测准确率	评估对风电、光伏等间歇性能源出力预测的精准度

建立关键性能指标监控体系要从业务流程入手，和业务部门一起梳理并确定最具代表性的指标。这些指标必须具有可度量、高相关、强时效的特征。从技术角度来说，采用接口调用、数据库查询或者消息队列订阅等形式，从生产管理、营销管理、地理信息等各个底层异构业务系统中准实时地抽取原始数据。数据经过清洗、转换、聚合等一系列处理之后形成最终的指标值，存入专门的时序数据库或者性能数据库里，供以后展示、分析、告警使用。保证指标的准确性、一致性，避免数据孤岛造成统计口径不一致的问题。

有效的指标监控不单只是数据被动的展示，还应该具有趋势预测以及智能的相关性分析的能力。剖析关键性能指标的历史数据，可以找出周期性波动的规律，预估未来走向，给资源规划和业务决策提供前瞻性参照。当某项指标出现异常的时候，系统应该可以自动关联其它相关指标、底层系统运行指标的同步变化，从而追溯问题产生的根本原因。由此得出的关联性强的分析能力，把监控层次由发现问题提升到辅助诊断上来，实现了质的飞跃。

（二）实时数据可视化

实时数据可视化是把海量监控数据和人的认识联系起来的桥梁，把抽象的数据转换成生动直观的图像，可以大大减少信息理解的成本，提高决策效率。在电力信息系统监控中心，一张设计精美的监控大屏就可以在数秒之内把整个系统的健康状况、业务运行情况以及潜在风险点清楚地展示给运维人员。其主要价值是“一图胜千言”，用图形的力量去发现数据背后的故事。

好的数据可视化设计要以用户为中心，根据不同系统运维人员、业务分析师、高级管理者等用户的需要提供不同的视图。运维人员看服务器负载、网络流量、错误日志数量这些底层技术指标；业务分析师在意交易量、用户活跃度、负荷曲线这类业务数据；管理者则更喜欢宏观、概括性的关键性能指标视图。常见可视化形式有：展示时间序列数据的折线图、比较分类数据的柱状图、表现占比的饼图和环形图、实时状态的仪表盘和进度条、地理空间信息的地理信息系统地图。合理地组合和布置这些图表元素，就可以组成功能强、表现力好的监控驾驶舱。

地理信息系统在电力信息系统的可视化实践当中起着重要的作用。电网的厂站、线路、设备的信息与实时运行数据在地理图层上叠加之后，电网的运行全貌就一目了然。以不同颜色（绿色为正常，黄色为预警，红色为过载）在地图上对各个区域变电站的负载率进行渲染，调度人员就可以清晰地掌握整个电网的负荷分布情况。某条线路发生故障时，地图上立刻显示出故障点，受影响的用户区域被高亮显示出来，给快速抢修和负荷转移给予决策支撑。结合空间维度数据展示的方法具有直观性，是传统图表所无法达到的，极大地提高了电网运行监测和指挥的效率。

（三）阈值告警与异常检测

阈值告警是实时监控系统最基本、最核心的功能，是系统由被动观察向主动响应转变的标志。它按照既定的规则，不断地对监控的指标进行判断，如果指标的值超过了正常范围的边界，就会产生告警，通过短信、邮件、电话或者集成告警平台等方式，快速地将异常的信息告知相关的负责人。这样的机制可以保证问题能够被第一时间发现，给故障处理争取时间，是防止小隐患变成大事故的重要防线。

阈值确定属于技术性与经验性相结合。静态阈值，即固定不变的门限值（如CPU 使用率大于 90%），规则简单明了，容易实现，适合于正常范围清楚的指标。

动态阈值更智能，能根据指标历史数据动态计算出告警基线，可以和上周同一时间的数值做同比，也可以和过去一小时的平均数做环比。动态阈值可以较好的应对业务周期性波动，减少业务高峰等造成的误报，提高告警的准确性。不管是静态阈值还是动态阈值，在实际使用中都需要不断的评价和修正，使告警的灵敏度与准确性达到最佳状态，不能出现告警风暴或者告警麻木现象。

随着系统复杂度的增加，单个指标阈值告警已经不能满足所有的场景了。很多复杂的故障都是由多个指标的微小变化共同造成的，但是单个指标未必会触动告警阈值。这时就需要用到更高级的异常检测算法。使用统计学的方法，例如3-sigma 原则、移动平均法等可以识别出偏离正常统计分布的数据点。而基于机器学习的算法，孤立森林、聚类分析等可以学习系统正常运行时多维数据的模式，从而在不预先定义规则的情况下，发现以前没有发现的复杂多变量关联异常。智能化技术正在成为电力信息系统开展预测性维护、主动运维的重要技术支持。

二、系统运行监控

如果说数据监控是关注“上层建筑”的话，那么系统运行监控就是为夯实“底层基础”。它深入到电力信息系统每一个软硬件单元中去，保证服务器、网络、应用服务等基础设施的稳定、健康，为上层业务应用的正常运行提供一个可靠、稳定的支撑平台。

（一）服务器资源监控

服务器属于电力信息系统的计算中心，服务器的资源利用情况关乎应用程序的表现及稳定程度。对中央处理器、内存、磁盘这三大块进行监控，这是系统运维的基础。CPU 监控主要看它的使用率，平均负载以及上下文切换次数。持续高位的 CPU 使用率说明存在计算瓶瓶颈，低效算法、死循环或者并发请求过多都会造成这种情况。内存监控就是查看用内存、可用内存、交换空间使用率等指标。内存耗尽会引发应用崩溃或服务器宕机，对内存使用趋势进行监控有利于提前发现内存泄漏或者进行容量规划。

磁盘资源的监控分两个部分，空间使用率和 I/O 性能。磁盘空间耗尽会使得数据无法写入，造成严重的应用程序错误或者系统崩溃，所以对各分区的使用率进行监控、告警是十分必要的。磁盘的读写速率、IOPs、队列长度都会影响到数据密集型应用响应速度。高 I/O 等待时间说明磁盘成了性能瓶颈，应该考虑升级

成更高性能的存储设备或者对数据库进行优化。实现这些监控一般需要在服务器上安装 Node Exporter、Zabbix Agent 等轻量级采集代理，采集代理定时从本地收集资源指标，通过标准协议上报给中心监控服务器统一处理和展示。

（二）网络流量与连接状态监控

随着分布式架构在电力信息系统中越来越多地被应用，服务组件之间及系统同外部终端之间的数据交换必须经由网络实现。网络是连接一切的生命线，它的稳定性、通畅性以及安全性直接关系到整个系统是否可用。网络监控就是为了保证这条生命线的健康，及时发现网络拥塞、中断、异常行为，监控对象主要是网络设备端口流量、带宽利用率、网络延迟、丢包率、数据包错误率等。

网络流量监控能了解网络负载状况，找出流量异常的设备或者应用，给网络容量规划提供数据支持。从流量来源、去向入手分析，可以发现外部非法扫描或者内部应用的异常通信模式。连接状态监测是对网络连接建立、维持、断开过程的检测。对服务器上 TCP 连接数以及连接状态（ESTABLISHED、TIME_WAIT）进行监控，可以发现由于配置错误或者程序缺陷引起的连接资源耗尽问题。

网络监控的技术手段有很多，简单网络管理协议是监控交换机、路由器等网络设备状态的标准。如果需要进行更加深入的流量分析，那么使用 NetFlow、sFlow 等流分析技术就可以得到细粒度的关于源 IP、目的 IP、端口、协议的会话信息。采用 ICMP Ping、TCP 探测等主动探测方式，不断地对网络节点之间是否能够连通，服务端口是否可达进行检测，模仿用户访问路径，以端到端的方式来进行网络质量的评价。这些方法一起形成一个立体的网络监控系统，保证电力信息系统的数据血脉畅通无阻。

（三）应用服务可用性监控

服务器运行正常、网络畅通，并不完全代表应用服务就能用。应用服务可用性监控主要关注从用户角度出发，保证应用的核心功能可以正常使用，这才是真正的可用性，是服务等级协议中最重要的考核指标。相比起底层资源监控来说，可用性监控更贴近业务，它的结果也更加直接。

实现应用服务可用性监控一般采取合成监控、真实用户监控两种办法。合成监控即在全球各地部署探测节点，按照事先设定的脚本模拟真实用户行为来访问应用。这些操作既可以是对端点的简单健康检查，也可以是复杂多步骤的业务流程巡检。

1. 端点健康检查，这是最简单的可用性探测。向应用服务的某个特定接口（比如一个 HTTP 健康检查 URL）发送请求，然后检查返回的状态码是不是 200 OK，或者响应体里是否包含某个特定的关键词，以此来快速判断服务进程是否还活着，能不能响应请求。

2. 业务流程巡检，属于更高层次的探测方法。探测脚本模仿用户完成一次业务操作，比如，在电力营销系统中模仿用户登录、查询电费、支付电费、退出。任何一个环节的失败都会引发即时告警。这种方法能从整体上检查应用及它所依赖的数据库、缓存、第三方服务等整条调用链路的健康状况。

以上各种监测方法结合起来运用，就能组成一个从基础设施到应用层，涉及全方面多种层面的一套监视系统。一旦应用出现问题，合成监控就能立刻察觉并发出告警，让运维团队可以在大多数真实用户受到影响之前开始应急响应，尽可能地保证电力信息系统服务连续性以及用户体验。

三、日志监控与分析

日志是电力信息系统运行的记录者，它用文本的形式把系统运行过程中发生的各种事件、操作和异常都记录了下来。日志记录了大量的数据，是故障排查、性能分析、安全审计和用户行为分析的重要数据来源。有效的监控、分析日志数据是提高系统可观测性的一个重要部分。

（一）集中式日志收集与管理

现代电力信息系统采用分布式微服务架构，应用程序和服务分布在成千上万个服务器节点或者容器中，产生的日志也分散在各处，给日志的查看和分析带来巨大困难。建立集中式日志管理的目的就是解决日志分散、格式不一、不能统一搜索、无法统一管理的问题。其核心思想就是将应用日志、系统日志、网络设备日志、安全设备日志等各种来源的日志，用统一的方式收集并传输到一个中心化的存储和处理平台。

典型的集中式日志系统一般由日志采集、传输、存储、索引、分析和可视化这六个部分组成。每台服务器上分别部署文件贝特、弗兰德斯德姆等采集代理来监控日志文件的变化情况，获取产生的新日志。采集到的日志用 Kafka 等消息队列做缓冲，安全传输，削峰填谷，提高系统的稳定性。日志在存储之前，会经过解析、结构化、丰富化的处理，把非结构化的文本日志解析成包含时间戳、日志

级别、主机名等字段的结构化数据，并为它补充地理位置、应用归属等上下文信息。

最后经过处理的日志会被写入强大的搜索引擎里并且创建快速检索的索引。于是就实现了对原来分散的日志进行规范化、集中化管理，为之后快速查询、关联分析、故障诊断打下了坚实的基础。集中式日志管理大大提高了运维效率，而且可以对日志进行统一的存储备份，满足安全合规性对于日志保留时长和不可篡改性的要求，其战略价值显而易见。

（二）日志检索与实时分析

当海量的日志数据集存在储并建立索引之后，如何从中快速、精确地挖掘出有价值的信息，就成为了日志分析的主要任务。强大的日志查询能力是它最基本的功夫。现代日志分析平台给运维人员带来了类似搜索引擎的体验，可以用丰富的查询语法来根据时间范围、主机名、应用名、日志级别、特定关键词或者多条件组合的方式在 TB 或者 PB 级的日志中实现秒级的定位。即时检索能力把过去需要登录多台服务器、翻阅大量文件等繁琐的工作简化为几个轻松的鼠标点击和键盘输入。

日志的价值不仅仅只是被动查询，对实时流入的日志流进行持续的聚合分析，就可以创建实时的业务和运维洞察仪表盘。实时统计每分钟的错误日志数量，用折线图展示它的变化趋势；统计 HTTP 访问日志中各种响应状态码（200、404、500 等）所占的比例，用饼图表示；统计用户登录失败的次数以及来源 IP，用列表或者地图来展示。基于日志数据的实时分析视图给运维人员打开了一个观察系统内部“新陈代谢”的窗口，任何异常波动，比如错误日志激增、接口响应时间突然变长等，都可以被及时捕捉，从而实现问题的早期预警。

（三）基于日志的故障诊断

日志在故障排查的时候就是“第一现场”，它是还原问题真相最有力的证据。当监控系统告警时，运维工程师最常规的动作就是查看告警时间点附近的相关组件的日志。日志里记录的错误堆栈信息、异常详情和上下文参数，经常直接或者间接地反映出问题的原因。一个典型的故障诊断流程，就是根据告警信息大致判断出哪个应用或者服务可能出问题，然后进一步去检索日志，一层套着一层，最后找到引起问题的具体代码行或者配置项。

微服务中一个用户请求要经过很多个后台服务。要定位这种跨服务的复杂问题，就需要将全链路追踪技术与日志结合起来。在用户请求的入口生成一个全局

唯一的追踪 ID，让这个 ID 随着请求在服务调用链中传递，每个服务在打印日志的时候带上它。当问题出现的时候，只要根据这个追踪 ID，就可以从大量的日志中找到这个请求在各个服务上留下的全部痕迹，从而可以快速地对跨服务调用的时序关系进行分析，定位性能问题和错误原因。

通过对大量的历史故障日志进行学习，也可以建立基于日志的智能故障诊断模型。模型可以自动识别出日志中出现的异常模式，并且还可以将当前出现的异常同知识库里面已有的故障模式做匹配，从而给出一些可能的问题原因以及解决建议。像当系统发现很多“数据库连接超时”的日志的时候，就可以自动关联知识库，提示运维人员去查看数据库连接池的配置，网络防火墙的规则，或者数据库本身所承受的负载情况。智能化日志分析能力加入以后，传统的被动、人工故障排查模式，正在向主动、智能化的新型运维模式转变。

第五章 电力信息系统测试技术

电力信息系统是保证电网安全、稳定、经济运行的基础，质量好、可靠性高。系统测试是最后一道发现并解决软件缺陷，检验系统功能性能，保证系统符合设计要求和用户需求的防线。本章会详细探究电力信息系统测试的重要技术及操作办法，从而为塑造优良的电力信息系统赋予结实的依靠。

第一节 测试方案设计

测试方案设计就是整个测试工作的顶层设计，是整个测试工作活动目标、活动范围、活动策略、活动所需资源以及活动时间的总体规划。一份完整的、严密的测试方案是保证测试工作有条不紊、按部就班地推进的基础，也是项目需求和测试执行的桥梁，更是决定电力信息系统最终交付质量的关键。

一、测试策略制定

测试策略可谓测试方案之魂，它依照项目特性以及风险分析，确定项目总体的测试方针和方法论，具体规定了在项目各个阶段应当开展的测试级别、使用的测试类型、配置的测试环境和资源，为之后具体的测试计划给予宏观引领。

（一）测试级别与类型划分

电力信息系统生命周期里不同的测试环节相互配合，组成了从点到面的质量控制网。最低一级的单元测试一般由开发人员来进行，目的是检验软件中最小可测单元（即函数或者方法）的正确性。集成测试把已经完成单元测试的模块整合起来，着重对模块之间的接口以及交互情况加以考察，这对于电力系统当中数据采集，实时监控，告警处理等这些功能模块的协作尤为关键。系统测试把整个软硬件系统作为一个整体来看待，在高度仿真的实际运行环境中，对它的所有功能和非功能需求进行全面的检验。最后是验收测试，一般由最终用户或者客户来主导，主要目的是确定系统是否完全符合合同所约定的需求，是否能够实现企业的

业务目标。

除了上述的测试级别外，还有许多种类的测试类型，它们对于保证电力信息系统的质量起着不可替代的作用。功能测试主要检验系统是否按照需求说明书的要求，正确地实现所有预定的功能，例如电费计算的准确性、票据打印的正确性等都属于它的范畴。性能测试主要考察系统在不同负载下响应时间、吞吐量、资源利用率等指标，对调度自动化系统或者用电信息采集系统来说，性能测试是衡量其稳定性的主要标准。安全性测试主要寻找系统存在的安全漏洞，防止未授权的访问、数据泄露或者恶意攻击，对以国家能源安全为己任的电网而言，其意义不言而喻。兼容性测试保证系统可在不同的操作系统，数据库平台或者浏览器上正常运行。各种测试方式互相补充，形成一个完善的电力信息系统质量保证体系。

（二）测试环境与数据准备

测试环境质量的好坏直接影响测试结果的真实性和有效性。理想的测试环境，硬件配置、软件版本、网络拓扑等各方面尽可能地模拟真实的生产环境。对电力信息系统来说，这就意味着要部署与生产环境相同的服务器、操作系统、数据库，模拟特定的网络设备、通信协议 IEC 61850 以及与外部系统交互的接口。同时环境的隔离性也很重要，它可以避免测试活动对生产系统造成干扰，也可以防止各个测试团队之间的相互影响。虽然搭建高保真测试环境花费较高，但是这是发现环境相关缺陷，准确评估系统性能、稳定性的必要前提。

测试数据的准备是测试工作中的一项非常艰巨的工作，它的质量好坏、覆盖度多少都会影响测试的深度和广度。准备测试数据要遵照如下主要原则：

1. 真实性、代表性，数据要尽可能地反映真实的业务场景。对电力系统而言，这就意味着要模拟电网日常运行数据、典型故障事件序列和用电高峰与低谷时段用户负荷曲线。

2. 全面性、多样性：数据要包含所有的输入组合，有效的、无效的、边界内的、异常的都要包括。拿电价计算模块测试来说，除了正常的用电量数据以外，还要准备零用电量、极大用电量和格式错乱的输入数据。

3. 合规性与安全性，使用生产环境数据时必须进行严格的脱敏处理，剔除所有的个人身份信息、敏感业务数据，以符合数据保护法规要求，防止信息泄露。

准备测试数据的方法很多，可以利用脚本高效生成大量数据，特别适合进行性能测试和负载测试；也可以从生产数据库中抽取数据，经过脱敏后使用，获得

的数据最接近实际情况。复杂业务逻辑要人工构造一些特殊的数据。精心准备的测试数据是设计出高质量测试用例的基础，也是发现深层次软件缺陷的钥匙。

（三）测试工具与资源规划

选择合适的测试工具可以大大提高测试的效率和质量。市面上测试工具繁多，大致可以分为几类。下表给出了常用的测试工具以及这些测试工具的作用。

常用电力信息系统测试工具表

工具类别	工具示例	主要用途
测试管理工具	Jira 配合 Zephyr 或 Xray	用于管理测试计划、测试用例、执行过程及缺陷跟踪。
自动化测试工具	Selenium, JMeter	分别用于 Web 前端自动化和接口性能测试，能将重复性手动测试自动化，缩短回归测试周期。
安全扫描工具	Nessus, AppScan	用于扫描系统存在的安全漏洞，评估系统安全性。
代码静态分析工具	SonarQube	在编码阶段分析源代码，及时发现代码缺陷、坏味道和不规范之处。

选择工具的时候，要全面考虑项目的技术架构，团队成员的技术栈，预算约束，工具的生态系统和社区支撑情况。

资源规划是对测试活动进行顺利开展的保障，它包含测试工具的采购与部署，但更重要的是对人力、硬件资源进行详细的规划。人力资源规划要确定测试团队的人员组成和职责，比如测试经理、测试架构师、功能测试工程师、性能测试工程师、自动化测试工程师等，还要按照各个阶段的工作量和工作难度，预估需要多少人以及需要什么样的技能。硬件资源规划需根据测试环境需求申请并配置相应的服务器、存储设备及网络带宽。一份周全的资源规划应列出各种资源规格、数量、到位时间和成本预算，并将其整合到项目总体计划中，防止因资源不足而造成测试进程延误。

二、测试计划编写

测试计划是把抽象的测试策略转化为具体的可执行的任务的详细文档。它对测什么、谁来测、何时测、如何测等核心问题做了明确的规定，既是测试团队开展工作时的行动纲领，又是与其他项目干系人进行沟通协调的重要依据。

（一）测试范围与目标

确定明确的测试范围是编写测试计划的第一件事。测试范围要确定本次测试活动所涉及的功能模块、业务流程、非功能性需求和待测系统平台。明确不测量什么同样很重要，可以防止范围蔓延和浪费资源。在一个新的配电自动化系统项目中，测试范围可以包含遥信、遥测、遥控功能和故障处理逻辑，但是不包括底层通信网络设备的固件测试。范围的界定要和产品经理、开发团队、最终用户进行充分的沟通并且达成一致意见，最后以书面形式确定下来。

建立具体的、可以衡量的测试目标，是评判测试工作是否成功失败的标准。好的测试目标应具有具体、可度量、可达成、相关、时限等五个特点。功能测试目标可以是：本轮系统测试结束时，高优先级业务流程测试用例的执行率 >=100%，通过率 >=98%。性能测试的目标可以设定为：在并发用户数量为 500 的时候，核心交易响应时间的平均值不大于 3s，服务器 CPU 利用率不大于 75%。质量目标可以是系统上线前致命和严重缺陷数量为零。这些具体的目标为测试执行指明了方向，也给评价测试活动的效果提供客观的依据。

（二）测试进度与人员安排

测试进度计划是保证测试工作按时间表进行的计划。要同项目的整体开发进程紧密衔接，把整个测试过程分成测试设计、环境搭建、首轮执行、多轮回归测试、性能测试等诸多重要环节，给每个环节确定清晰的开始和结束时间以及里程碑事件。像“全部核心功能测试用例评审完毕”这种重要的节点。使用甘特图等项目管理工具可以体现出任务间的相互依赖关系、关键路径以及在任何时候测试经理都可以随时跟踪到进度、找到影响进度的各个风险。

人员安排是测试计划中的核心环节，即把合适的工作分给合适的人。计划中要列出测试团队的组织架构以及成员名单，而且要清楚每个人所承担的角色和肩负的责任。张三做整体测试管理及对外沟通，李四做性能测试方案设计与执行，王五带领功能测试小组对营销模块进行测试。职责明确可以提高团队协作效率，防止出现工作交叉或者遗漏。在计划中要考虑到现在的人员的技能存量、必要的培训需求、关键岗位的人员替换，以防止突然发生的人员变动带来的影响。

（三）风险分析与应对措施

测试过程中，各种预料之外的事情都可能会发生，从而给测试进度和质量带来冲击。风险分析的目的就是提前发现这些潜在的风险，并预先做好应对预案。

电力信息系统测试中存在需求经常变更导致测试用例大量失效，开发版本交付延期，挤占宝贵的测试时间，测试环境不稳定或者和生产环境差异过大，核心技术人员突然离职，测试过程中发现的缺陷数量太多，修复时间过长等各种风险。识别风险之后，就要对风险发生的可能性以及可能造成的后果加以评判，以此来决定先处理哪个。

对每一个已识别并评价的风险，应制定具体的应对措施，一般分为风险规避、风险转移、风险缓解和风险接受。对于需求经常变更风险，可以在项目开始时就制定严格的需求变更控制流程，并且采用敏捷测试的小步快跑方式来快速应对需求的变更，这就是一种风险缓解的方法。对于测试时间被压缩的风险可以采取增加测试人力、安排周末加班、优先保障核心功能测试、将次要功能推迟到下一版本等办法进行应对。将所有的风险以及应对措施加入到测试计划中，可以引起管理层和项目团队对于潜在问题的足够重视，在风险实际发生时，能够快速、有序地采取应对措施，将负面影响降到最低。

三、测试用例设计方法

测试用例是指导测试过程的脚本，它对测试的输入、测试的条件、测试的结果等做了详细的定义。设计好的测试用例是好的发现软件缺陷。采用系统化设计的方法，用最少、最好的用例集，对程序逻辑进行最大程度的覆盖，以提高测试的效率和效果。

（一）等价类划分法

等价类划分法是黑盒测试用例设计中使用最广、最基本的方法。其核心思想就是将程序的输入域划分成若干个互不相交的子集，这些子集就称为等价类。理论上讲，同一等价类中任意一个输入数据对程序错误的暴露效果是一样的。所以，我们只需要从每一个等价类中任选一个代表性的数据当作测试用例，就能覆盖该类的所有其它数据。等价类分为有效等价类和无效等价类：有效等价类是符合程序规格，合理的输入数据集合；无效等价类是不符合规格，不合理或者非法的输入数据集合。

用电力负荷预测系统中参数“历史数据回溯天数”来举例，假设它的有效输入为 1 到 30 之间的整数。据此可知，有效等价类就是区间内的整数。无效等价类有小于 1 的整数（0，-5），大于 30 的整数（31，100），非整数，非数字字符等。

只需要从每个等价类中选取一个代表值，比如从有效等价类中取 15，从各个无效等价类中分别取 0、35、10.5 和‘A’来设计测试用例，就可以有效地检验系统对不同类型输入的处理逻辑是否正确。

（二）边界值分析法

边界值分析法可以看作是等价类划分法的一种重要的补充和优化。大量的程序错误都发生在输入输出范围边界外而不是范围内部。因此，设计边界条件的测试用例，可以更有效地找到缺陷。边界值分析法认为应该选取等价类边界上的值，以及刚好在边界内侧和外侧的值作为测试数据。一般对于闭区间 [min，max] 取四个值 min、min+1、max-1、max；对开区间 (min，max) 取两个值 min+1、max-1。还要测试刚好在边界外的值，即 min-1 和 max+1。

继续使用“历史数据回溯天数”的例子。采用边界值分析法，所需要测试的数值不仅仅是等价类中某个代表值，而是以边界点为中心的一组关键值。具体为：边界上的值 1、30；边界内的值 2、29；边界外的值 0、31。对边界点进行重点测试可以有效地找出程序存在诸如把“<=”写成“<”等边界条件的处理错误。将边界值分析和等价类划分结合起来可以产生覆盖范围更广、针对性更强的测试用例集。

（三）因果图法

当一个功能的实现需要多个输入条件的复杂组合，并且会产生不同的输出结果时，因果图法就是一种非常有效的分析方法。单一的输入条件测试，很难发现由于多条件组合而产生的问题。因果图法采用图形化的方式，把“原因”（输入条件）和“结果”（输出或者系统状态变化）之间的逻辑关系表现出来，之后依据这些关系得出判定表，再由此生成测试用例。

使用因果图法一般经过以下过程，先对需求规格进行详细分析，找出所有原因和结果；确定原因和结果之间是逻辑关系，有与、或、非等关系，还要考虑各个原因之间的约束关系，比如异或，两个原因只有一个为真；蕴含，一个原因为真时，另一个也必须为真的情况；最后根据因果图画出判定表，判定表的每一列表示一种原因组合及对应一个明确的结果，每一个结果可以对应一个具体的测试用例。

想象一下一个电力系统保护装置的跳闸逻辑：当线路电流超限（原因 A）并且非紧急手动闭锁（原因 B）的时候，或者线路电压异常（原因 C）的时候，装

置就会执行跳闸（结果 X）。这逻辑就是 OR C -> X。利用因果图以及转换后的判定表，可以有条理地产生包含所有逻辑组合的测试用例，比如测试 A、B 为真、C 为假；测试 A 为假、C 为真；测试 A、B、C 全为真；测试 A、B、C 全为假等等。这种方法可以对复杂的控制逻辑进行全部验证，这对保证电力系统的安全运行是很重要的。

第二节 功能测试方法

功能测试是电力信息系统建设中不可缺少的重要环节，主要是检验系统各项功能是否完全满足需求规格说明书的要求。通过模拟用户在真实业务场景中操作的方式，对系统功能逐项检查和验证，目的在于发现并修正功能缺陷，保证系统上线之后可以平稳、可靠地支撑起各项电力业务，最终满足用户的实际需求。本节主要对单元测试、集成测试、系统测试这三个主要的功能测试方法进行详细的阐述。

一、单元测试

单元测试是软件测试的基础，测试的对象是软件设计中最小的可测试单元，即模块或者组件。在电力信息系统的开发过程中，对独立的函数、方法或者类进行严谨的测试，可以使得在开发初期就能及时发现并隔离缺陷，从而大大降低后期集成与系统测试的复杂度和成本。这就需要开发人员为每一个被测试单元编写独立的测试代码，保证它的逻辑正确和健壮，从而为建设高质量系统奠定基础。

（一）测试对象与目的

单元测试的对象是电力信息系统中粒度最小、可以独立进行测试的模块，比如一个计算电价的函数、一个处理用户请求的类方法、一个与硬件设备通信的独立组件等。单元一般表现为代码层面的函数、过程或者类。测试的核心目的，就是在一个尽可能小的代码范围里，保证代码逻辑的正确性，也就是保证代码单元能够严格按照设计的要求，正确处理各种各样的输入，包括正常的值，边界值，以及非法的值。

对这些最小单元进行严格的测试，可以在软件开发初期就有效地发现和定位问题。不仅能大幅减少缺陷修复成本，有效避免问题在后期集成阶段被放大，更能从根本上提高代码的内在质量与可维护性。对复杂的电力算法、重要的控制逻

辑、核心的数据处理模块进行细粒度的单元测试，是保证其准确无误、稳定可靠的一种必要手段，是建造坚固软件大厦的第一块基石。

（二）测试框架与工具

单元测试的好坏不能脱离成熟的测试框架以及辅助工具。对于用 Java 语言开发的电力信息系统来说，JUnit 是使用最广泛的单元测试框架。使用注解的方式可以方便的设置测试的方法、测试前后环境的准备工作、清理工作，也提供了非常丰富和准确的断言函数库来验证所测试结果的正确性。JUnit 广泛使用后大大简化了测试用例的编写和管理。

为了实现测试单元的有效隔离，模拟技术应运而生，Mockito 是 Java 生态中功能强大的模拟框架。它可以创建、配置模拟对象，替换被测单元所依赖的外部模块或者资源，比如数据库连接、硬件接口、服务等。这样做的好处就是测试可以完全围绕被测单元自身的逻辑展开，不会受到外部依赖项稳定与否、是否可用的影响。比如对一个从数据库读取配置信息的模块进行测试，可以使用 Mockito 来模拟数据库访问对象，并且预先设置好当这个对象接收到某个查询时，返回什么样的配置数据，从而营造出一个干净且可控的测试环境。

JUnit 与 Mockito 的组合拳，给 Java 应用程序带来了一套强大的、灵活的单元测试方案。开发者可以以此来创建独立的、可重复的自动测试用例，用以快速的验证程序的逻辑。此举不但可以提高测试效率，而且可以促进代码设计的不断改进，因为容易测试的代码一般也具有较低的耦合度和较高的模块化程度，这一点对结构复杂、规模庞大的电力信息系统来说尤其如此。

（三）代码覆盖率分析

代码覆盖率是用来衡量单元测试完整性的一个重要的量化指标，它度量的是测试过程中源代码被执行到的情况和比例。分析覆盖率报告可以明确地找出没有被测试的代码，有针对性地增加测试用例，缩减测试盲区，提高软件质量。代码覆盖率一般有行覆盖率、分支覆盖率、方法覆盖率等。

在 Java 的技术栈中，JaCoCo 是使用最广的开源的代码覆盖率工具。它利用在 Java 字节码中植入“探针”的方式，在测试运行的时候动态收集代码的执行信息，无需改动源代码。测试完成之后，JaCoCo 可以生成一个包含图片、文字的 HTML 报告，以绿色完全覆盖、黄色部分覆盖、红色没有覆盖这样的颜色高亮的方式把类、方法以及代码覆盖率显示出来，甚至还可以逐行展示出每个逻辑

分支的状态。

合理地使用代码覆盖率分析可以给测试工作提供数据驱动的指引。它可以对测试工作进行量化评价，甚至可以把覆盖率作为持续集成流程中的一个质量门槛。但必须要指出的是，高覆盖率并不等于高质量的测试，因为高覆盖率不能保证测试用例本身的逻辑正确。因此，代码覆盖率分析应当与其他测试方法以及代码评审活动相结合，成为发现测试用例缺失、评判测试充分性的一种有效辅助手段，而不是测试的最终目的。

二、集成测试

在各个模块通过单元测试之后就进入集成测试阶段。在这个阶段，按设计要求，把独立的模块综合起来，组成可以联合工作完成的软件，然后做全面的测试。集成测试主要是检测模块间接口的正确性，交互的协调性，组装后的整体功能表现。电力信息系统中，模块之间的相互作用一般都存在复杂的数据交换以及业务流程调用，集成测试可以有效地发现由于接口定义不同、数据格式错误、调用时序等问题所引起的深层次缺陷。

（一）自顶向下与自底向上集成

集成测试的实施策略有自顶向下、自底向上和结合两者优点的混合式集成三种。不同的策略在实施途径、资源投入、问题发现时间点上都有所区别。下表清楚地对比了这几种集成测试方法的特点。

集成测试策略对比表

策略	核心思想	优点	缺点	辅助工具
自顶向下	从系统主控模块开始，按层次结构逐级向下集成和测试。	可较早验证系统主流程和高层逻辑，功能尽早可见。	底层关键模块的测试被推迟，桩模块开发维护成本高。	桩模块
自底向上	从系统最底层的基础模块开始，逐步向上集成和测试。	可尽早、充分地验证底层组件的功能，支持并行集成。	系统整体功能直到最后才能体现，高层设计缺陷发现晚。	驱动模块
三明治 / 混合式	以系统中间某一层为起点，同时向上和向下进行集成。	结合两者优点，能较早验证关键业务逻辑和底层服务。	策略相对复杂，可能存在中间层测试不够充分的风险。	桩模块与驱动模块

在电力信息系统的创建过程里，由于系统的复杂性，一般会采取更加灵活实用的三明治集成（也称混合式集成）方式。以系统的核心业务逻辑层作为分界线，

上层用自顶向下的方式，下层用自底向上的方式，可以提前验证关键的业务流程，又能保证底层基础服务的稳定可靠，实现效率和质量之间的平衡。

（二）基于接口的集成测试

随着分布式、微服务架构在电力信息系统中应用越来越广泛，系统间的交互更多地依靠接口来实现，因此基于接口的集成测试就变得十分重要。它的关注点是各个模块或者服务之间数据交换的正确性和稳定性，不关心模块内部具体的实现。测试的主要目的是保证接口的请求和响应完全符合事先定义好的“契约”，也就是协议、数据格式、参数、返回值等等都必须符合规范。

进行基于接口的集成测试时，通常遵循以下步骤：

1. 接口契约分析，首先要对接口设计文档有深入的理解，明确接口的URL、请求方式（GET、POST）、请求头、请求体数据格式、参数约束、响应报文格式、状态码等契约内容。

2. 测试用例设计：根据接口契约设计全面测试用例，涵盖正常和异常场景。测试所有参数合法时接口是否可以返回正确的结果，测试必填参数缺失或者格式错误时系统是否返回预期的错误码和提示，对需要权限控制的接口进行越权访问尝试。

3. 工具执行利用 Postman、SoapUI 等接口测试工具执行测试用例。这些工具可以方便的创建 HTTP 请求，发送到被测接口，并清楚的显示响应结果。编写自动化脚本也可以把接口测试无缝集成到 CI/CD 流程里，实现自动测试和回归。

4.4、结果验证和断言：接口响应出来以后必须进行严格的验证。这包含查看 HTTP 状态码是否符合预期，响应体里关键字段的值是否正确，数据结构是否和接口定义一致。自动化脚本里一般都会有较多的断言语句，用以判定测试是否成功。

接口式集成测试可以有效的将缺陷定位于服务与服务之间，从而实现快速排查问题。在复杂的电力系统当中，不论是调度系统同营销系统之间的数据交流，还是监控系统同资产管理系统之间信息的同步，都必须经过严格的接口测试，从而保证数据流可以在各个子系统之间准确而顺利地流动。

（三）集成测试环境搭建

一个稳定可靠、高度仿真的生产环境集成测试环境，是保证集成测试有效性的基础。创建这样的环境需要对于系统的整体架构、依赖关系以及部署方式有清

楚的认识。其主要目的就是创造一个隔离的、可重复使用的测试空间，保证测试活动既不会影响到开发环境，也不会受到其他无关活动的影响。

集成测试环境的搭建一般会牵涉到很多内容。首先是硬件和网络规划，给所有待测应用模块、数据库、第三方服务分配合理的服务器资源。网络需要配置好各个模块之间的互相通讯，而且网络策略（防火墙规则等）要尽可能的接近生产环境，这样可以尽早的发现潜在的连接问题。

其次就是软件环境的部署，包括操作系统、中间件（消息队列、应用服务器）、数据库等安装配置。为了提高效率，保证一致性，业界越来越倾向于采用基础设施即代码的办法来自动化创建、配置环境。同时 Docker 为代表的容器化技术大大简化了部署过程，用标准化的镜像包装整个应用程序以及所有的依赖项，并实现快速一致的部署，有效地避免了由于开发环境不同导致的无法运行的常见问题。最后是测试数据的准备，数据要具有代表性，可以覆盖各种业务场景。数据的生成可以采用数据库脚本、数据模拟工具或者对生产数据脱敏来完成。优秀的集成测试环境是开发和生产之间的桥梁，它的稳定性和真实程度直接影响到集成测试的好坏。

三、系统测试

系统测试是在集成测试完成之后，将软件作为一个完整的整体，与硬件、网络环境、外围设备等所有系统元素结合在一起，在高度仿真的运行环境中进行的一系列严格且全面的测试。其实质就是对电力信息系统进行测试，以保证其满足需求规格说明书所规定的所有功能和非功能需求，保证整个系统作为一个整体能够正确、有效地工作。

（一）功能符合性测试

功能符合性测试属于系统测试的重要部分，它的主要工作是对电力信息系统的所有功能一项项进行核对，查看它们是否全部按照需求规格说明书的要求来执行。这个测试一般采取黑盒测试的办法，测试人员不用关心系统内部的实现逻辑，只是站在最终用户的立场上，查看系统的实际表现同需求文档，用户手册等所描述的是否完全符合。

测试开始是从需求规格说明书的详细分析入手，把每一个功能需求转化为具体的、可以执行的测试用例。每一个测试用例都应该清楚的知道自己的前提条件、

输入的数据、需要执行的操作步骤以及预期的结果。如对电力营销系统中电费计算这一功能来说，设计出来的测试用例就要包含不同用电种类、不同阶梯电价搭配、不同用电时段等状况，保证计算出的结果绝对正确。

测试人员在执行测试的时候，会依照测试用例的步骤来进行，然后把实际得到的结果和预期的结果做比较。任何不一致的现象都会被当作缺陷来记录。功能符合性测试的覆盖面要全面，既不能只测试明确的各项功能点，又不能忽视隐含的需求及各种边界条件。对数据查询功能，除了要验证查询结果是否正确，还要测试当查询结果为空或者数据量非常大时，系统是否能给出合理的、稳定的响应。

系统性地进行功能符合性测试，可以有效地保证最终交付的电力信息系统功能完整、正确，保证每一个功能点都能够准确地实现其设计目标，满足用户的业务需求。这个过程是保证软件产品功能完整性的又一道防线。

（二）业务流程测试

电力信息系统的真正价值并不只是提供孤立的功能点，而是要能顺畅地支持端到端的整个业务流程。业务流程测试就是以整体角度来审视许多独立的功能点，按照完整业务场景模拟出真实业务运行时是否正确、顺畅、协调。此种测试方法冲破了单一功能的束缚，更加贴近用户的实际使用情形。

电力客户服务系统内的一个典型的“新用户报装”业务流程一般包括客户信息录入、现场勘查任务下达、供电方案拟定、合同签订、装表接电、业务归档等。业务流程测试就要完整地模拟从客户申请到最终送电的整个过程，观察数据在各个模块、各个角色之间传递是否正确，流程状态转换是否符合业务规则，各环节处理是否及时高效。

设计业务流程测试用例时，需要测试人员对电力企业核心业务有深刻的认识。测试用例要包含主要的业务流程，重要的分支流程，异常处理的途径。以上面的“新用户报装”为例，就要对供电方案被驳回、用户资料不全需补充等异常分支的处理流程做足文章。通过端到端的测试来发现由于模块之间配合不当、数据传递丢失、业务规则实现错误等原因导致的深层次问题，保证系统可以真正支持复杂的、变化的电力业务。

（三）用户界面测试

用户界面是人与计算机交互的入口，设计的好坏直接关系到用户的工作效率和满意度。用户界面测试的主要目的就是保证界面上所有可见元素的功能正常，

视觉呈现、易用性以及交互逻辑均符合设计规范和用户习惯。优秀的用户界面应该是直观的、一致的、容错的。

用户界面测试通常涵盖以下几个维度：

1. 控件功能测试：逐个对界面中所有的控件进行检查，如按钮、文本框、下拉列表、单选和复选框等等，看是否能正常响应、工作。例如点击“查询”按钮之后系统是否可以正确执行查询操作，日期选择控件是否可以准确选择日期。

2. 界面布局与美学，观察界面的整体布局是否合理美观，各个元素是否对齐，颜色搭配是否和谐，字体字号是否清晰可辨。还要保证在不同的分辨率、窗口大小下，界面布局自适应，不会出现元素错位或者重叠的现象，即响应式检验。

3. 导航与流程逻辑，测试用户在各个界面之间进行跳转的逻辑是否正确、顺畅。从列表页面点击详情链接，是否可以正确跳转到详情页面；点击返回按钮，是否可以回到之前的页面。整个操作流程要符合用户的心理预期以及操作习惯。

4.4、易用性以及提示信息：审查系统提供的提示信息是否清楚、友好、及时。当用户出现输入错误或者执行非法操作的时候，系统就应该给出清楚的错误提示，并且指引用户如何进行改正。对复杂操作给出必要的帮助文档或者即时提示。

对那些要显示很多实时数据以及图形的复杂应用，例如电力监控系统，用户界面测试就显得非常关键。测试人员要保证数据图表（曲线、柱状图）可以正确及时地刷新，各种告警信号能够醒目地显示出来，界面的交互响应速度要快，不能因为数据量太大而产生卡顿现象。细致的用户界面测试可以很大程度上改善电力信息系统的用户体验，提高系统的价值。

第三节 性能测试技术

电力信息系统的稳定高效是保证整个电力网络正常运转的基础。性能测试是保证系统品质的重要环节，它用多种运行负载和环境对信息系统的处理能力、稳定性及资源利用率进行系统的检测和评价，目的是找到系统存在的性能瓶颈，给系统优化和容量规划提供科学依据。

一、性能测试类型

性能测试不是一种单一的概念，而是由各种不同的具体性能测试类型组成的

集合，每一个具体的性能测试类型都有不同的目的、不同的应用范围。为了对电力信息系统的性能表现作出全面评价，一般要综合采用不同类型的测试，从多个方面考察系统在不同压力下的行为特点，从而保证系统能够在各种预期乃至极端情况下正常工作。

（一）负载测试

负载测试属于关键的性能测试手段之一，主要目的是考察电力信息系统在预期正常与峰值负载时的工作状况。通过模拟一定的并发用户，在一定的时间内执行电费查询、报修申请、用电数据上报等典型的业务流程，来检验系统是否满足设计之初所设定的性能指标。关键在于验证而不是破坏，目的是检验系统在预期的负载范围内能否稳定、高效地工作。

负载测试是在逐步增大系统上负荷的过程中，考察关键性能指标。随着并发用户数的增加，交易的平均响应时间是否还在合理的范围内，系统的吞吐量能否达到预期的目标。通过此过程可以找到系统性能的拐点，在保证性能指标的前提下，系统所能承受的最大负载水平。这对于容量规划来说非常重要，能帮助电力企业了解当前的硬件资源是否足够，在用户增长的时候什么时候需要进行扩容。

（二）压力测试

压力测试，顾名思义，是一种试图找出电力信息系统性能极限的测试方法。与负载测试不同的是，压力测试的目的就是不断加大负载，直到系统出现性能瓶颈、处理速度明显下降或者崩溃。极限施压可以确定系统绝对最大负载，也可以观察到系统资源耗尽或者接近饱和时的行为模式。例如模拟远超预期用户量短时间内并发进行电费缴纳操作，看系统的反应。

此过程对于找到系统的“断裂点”十分重要。在压力测试中，除了要考察系统在什么情况下会失效，更要注意它是如何失效的。系统可以优雅地降级服务，即拒绝新的连接，但是保证已经建立的连接，还是会在突然崩溃的时候导致数据丢失？系统在压力解除之后能否自动恢复正常运行状态？这就是压力测试要回答的问题。对电力调度、交易等核心系统来说，知道它们在极端情况下会怎样，这是制定应急预案和灾难恢复计划的基础。

（三）稳定性测试

稳定性测试又叫浸泡测试或者耐久性测试，主要用来检验电力信息系统长时间、中负荷连续运行的可靠性。测试周期一般要持续数小时、数天甚至更长的时

间来模拟系统在现实世界中长期不间断运转的场景。其关注的重点是发现内存泄漏、数据库连接未及时释放、线程阻塞等在短时间测试中难以发现的问题。

电力行业中的很多系统比如电网监控系统、用电信息采集系统等都需要7×24小时不间断的运行，而稳定性测试模拟的就是这样的工作状态。测试阶段要重点观测系统资源利用率的变化趋势。一个健康的系统，其内存、CPU等资源占用应该是在一个稳定的范围内来回变化。如果发现内存占用量慢慢、持续地增加，即使增加的幅度很小，也可能是内存泄漏的迹象，长时间积累就会造成系统崩溃。经过稳定性测试之后，那些隐蔽而致命的缺陷就能被提前找到并予以修正，进而保证系统可以长久地稳定运行。

二、性能测试指标

为了对电力信息系统的性能进行科学、定量的评价，必须有一系列标准化的性能指标。这些指标好比一份系统的体检报告，从不同的角度来体现系统“健康状况”。对这些指标准确的测量与分析，既可以判断系统的性能是否达标，也可以准确的找到造成系统性能低下瓶颈。

（一）响应时间与吞吐量

响应时间是对系统处理效率最直观的度量，响应时间即用户发出请求到收到系统最后答复所经过的全部时间。对于电力信息系统来说，响应时间越快就意味着用户体验越好、业务效率越高。如果电力营销系统客服代表在通话过程中查询用户信息的时间过长，会对服务质量造成严重影响。核心交易的响应时间要求是秒级或者毫秒级。

吞吐量用来衡量系统在单位时间内成功处理的请求数或者事务数，一般用TPS（每秒事务数）或者QPS（每秒查询数）来表示，是衡量系统处理能力的主要指标。高吞吐量即系统可以同时为更多的用户服务或者处理更多的业务。用电信息采集系统必须有很高的吞吐能力，才能在规定的时间内处理数百万甚至上千万智能电表的海量数据。

响应时间和吞吞吐量存在着互相制约的关系。当系统的负载较低的时候，随着并发用户数的增加，吞吐量大体是成线性增长的，而响应时间不变。系统一旦达到或者接近处理能力的极限，继续增加负载就会导致响应时间急剧延长，吞吐量就会趋于饱和甚至开始下降。找到这两个指标的最好平衡点，就是性能优化的

主要目的之一。

（二）并发用户数与资源利用率

并发用户数指的是同时给系统发起请求或者进行操作的用户数量。它直接体现系统负载情况，通过模拟不同的并发用户数量，可以检验系统在各种负载下的表现。并发用户数不等于在线用户数。在线用户不一定做了任何操作，而并发用户指的是那些在同一个时间给服务器造成压力的用户。典型的并发场景是月底很多用户一起查电费，或者恶劣天气预警时用户一起去看停电工。

资源利用率指的是服务器 CPU、内存、磁盘 I/O、网络带宽等硬件资源在测试期间的利用状况，是找出性能瓶颈的主要依凭。一个好的系统应该可以充分利用硬件，并且是均衡的利用。如果测试发现 CPU 使用率长期大于 90%，内存和磁盘 I/O 都很空闲，那么瓶颈很可能就出在 CPU 或者应用代码的计算消耗上。反之若所有的资源利用率都很低，但是系统的响应时间很长，则说明应用自身可能存在逻辑上的问题，例如线程阻塞、不合理的等待等等。

对于资源利用率的不断监测与剖析，乃是展开性能调优的基本事务。内存利用率在负载结束后不回落，一般为内存泄漏的信号；磁盘 I/O 一直繁忙，可能是由于大量的日志读写或者数据库低效访问所导致的。电力系统中数据量大的场景，比如调度日志分析或者用户用电数据的挖掘，对于数据库、磁盘读写操作等的优化就显得更加重要了。

（三）错误率

错误率就是系统处理失败的事务数与总事务数之比，是反映系统稳定可靠程度的指标。理想状况下，不管负载多大，错误率都应该是 0。但实际上在负载高或者压力大时由于资源不足、程序缺陷或者配置错误等原因会导致处理失败。

对于电力信息系统来说，错误率不能容忍。一次错误的计费、一条失败的调度指令，都会造成严重的后果。因此在性能测试中对错误进行详细的记录与分析就显得非常重要。每一个错误出现的时候，都要找到根源，弄清楚是服务器超时，网络断开，数据库连接失败，还是程序内部的逻辑错误引起的。

分析错误时，既要看数量，也要看类型和发生时间。如果负载一开始就出现大量连接错误，说明应用连接池配置过小；当负载达到某个阈值之后突然出现大量的连接错误，就说明了系统的性能拐点。对错误模式进行深入分析之后，测试人员可以给开发人员提供准确的缺陷定位信息，进而有效地提高系统在各种负载

下的鲁棒性。

三、性能测试工具与实践

理论和指标最终要依靠有效的工具、科学的实践来落实。性能测试的实践是项系统性工程，牵涉到挑选恰当的测试工具，规划逼真的业务场景，剖析测试成果，找到并修正性能问题等诸多环节，形成一个闭环流程。这一过程对保证电力信息系统的稳定运行有很重要的作用。

（一）LoadRunner, JMeter 等工具介绍

性能测试领域有各种成熟的商业、开源工具，其中 LoadRunner 和 JMeter 是应用最广的两种，它们各有特点，可以满足不同的测试需求。下表对比了这两种主流工具的主要特点。

LoadRunner 与 JMeter 工具对比表

特性	LoadRunner	JMeter
授权类型	商业软件，需付费授权	开源软件，完全免费
技术支持	官方提供专业技术支持	依赖活跃的开源社区和插件
协议支持	极为广泛，覆盖多种企业级协议	主要支持 Web 相关协议，可通过插件扩展
脚本复杂度	功能强大，但脚本开发与调试较复杂	脚本相对简单，上手速度较快
报告分析	提供强大、多维度的分析引擎和图表	报告功能基础，可借助插件增强
适用场景	大型、复杂的企业级系统，协议多样化	Web 应用、API 接口、微服务等

1. LoadRunner 是一款功能强大的商业性能测试工具，以其广泛的协议支持和专业的分析能力著称。它能够支持包括 Web、数据库、中间件以及 SAP、Citrix 等多种复杂的企业级应用协议，这使其在覆盖电力行业多样化的信息系统时具备天然优势。LoadRunner 提供了强大的脚本录制与增强功能，以及详尽、多维度的实时监控和结果分析图表，能帮助测试人员快速、精准地定位性能瓶颈。尽管其学习曲线较陡峭且成本高昂，但在大型、复杂的企业级项目中，其专业性与全面性仍是许多机构的首选。

2. JMeter 则是一款广受欢迎的开源性能测试工具，它基于 Java 开发，具有出色的跨平台性。其主要支持 HTTP、JDBC、SOAP 等协议，非常适合对基于 Web 的应用和各类 API 接口进行性能测试。JMeter 的优势在于其免费、开源的特性，以及活跃的社区支持和丰富的插件生态，这赋予了它强大的扩展能力。它

的图形化界面相对直观，上手较快，对于预算有限或以 Web 应用为主的电力信息系统（如网上营业厅、移动 APP 后端服务）性能测试项目而言，JMeter 是一个性价比极高的选择。

（二）测试场景设计与执行

测试场景设计是性能测试实践的灵魂，测试场景设计的好坏直接影响到测试结果的有效性以及参考价值。一个好的测试场景必须尽可能地贴近真实世界用户的行为模式与系统负载特征。对于电力信息系统，需要了解具体的业务才能进行场景设计，电力营销系统和调度自动化系统的业务模型是不一样的。设计过程一般包含业务建模、确定测试目标、准备测试数据、制定执行策略等步骤。

需要给核心业务建立模型，分析各个业务的操作频率以及用户占比。以电力营销系统为例，大多数访问是电量查询请求，而缴费、业务办理等操作所占的比例比较小。测试场景就要按这个比例去组合不同的业务请求，而不是单独测试一个功能。必须考虑电力系统周期性的影响，月初月末效应，月初、月末的缴费和账单查询业务量会激增，测试场景要模拟这样的峰值负载。测试数据的准备也十分重要，需要大量的数据支持，数据的分布也要接近实际情况，避免因为缓存命中率过高或者数据过于单一导致测试结果失真。

测试执行阶段要采取逐步增加虚拟用户数的方法，平稳地加大虚拟用户数，并仔细观察各项性能指标。监控范围应该从前端应用服务器到后端数据库服务器整个技术栈。执行的时候需要详细记录各时刻的并发数、响应时间、吞吐量、服务器资源利用率等数据，并且要捕获全部的错误信息。经过多次重复测试、对比分析来保证结果的稳定性、可靠性，为之后的瓶颈分析打下坚实的数据基础。

（三）性能瓶颈分析与调优

性能瓶颈分析、调优为性能测试的最终目的，也是最难的一环。要求测试人员、开发人员有全局观念、技术高，可以从大量繁琐的测试数据中找出问题所在。性能瓶颈可以出现在系统的任何层次上，硬件资源、操作系统、中间件、应用程序代码、数据库等等都会出现。

分析过程一般用自顶向下的方法。首先从宏观指标入手，用关联分析的方法对响应时间、吞吐量和资源利用率等曲线图进行分析，大致判断出瓶颈属于的资源类型。当 TPS 增长停止，CPU 利用率又达到饱和的时候，瓶颈很可能就是服务器的计算能力和应用代码的 CPU 消耗。如果 CPU 和内存资源充足，但是响应

时间很长，那么就可能是网络延迟或者 I/O 等待导致的。

定位到大致的瓶颈方向之后，就要用专业的诊断工具进行深入分析。对于应用层面的问题可以使用代码剖析工具来定位出消耗 CPU 或者内存最多的热点代码，从而进行针对性的优化。数据库瓶颈问题采用慢查询日志、执行计划分析为主要手段来诊断，通过分析是否存在全表扫描、索引失效等状况给 SQL 优化和索引重建提供方向。在处理大量的用电历史数据查询的时候，没有索引会使数据库的性能急剧下降。

性能调优是反复试验，逐步修正的过程。在找到并修复一个瓶颈之后，需要重新进行性能测试，来验证优化的效果，并警惕“瓶颈转移”，旧的瓶颈解决了之后，新的瓶颈就会在系统的其他部分浮现出来。采用测试、分析、调优、再测试的循环过程，使系统性能逐步提高，达到或者超过预期业务目标。

第四节 安全测试要点

电力信息系统的安全稳定运行，直接关乎电力生产、电力输送、电力调度、电力营销等各项核心业务能否顺利开展，而且对整个社会的能源供应安全有着十分深刻的影响。因此在系统建设的各个阶段，尤其是上线前，进行全方位的安全测试就显得十分必要。安全测试通过主动模仿各种网络攻击和恶意行为，目的是找出并修正系统中存在的安全漏洞，保证系统可以抵御不断变化的网络威胁。

一、漏洞扫描与渗透测试

漏洞扫描和渗透测试是对电力信息系统安全状况最直接、最有效的一种检测手段。它把自动化工具的高效性同安全专家的人工智慧融合起来，从攻击者的角度对系统的安全防护能力展开全面的考察，主动发现技术上和业务逻辑上的潜在风险，给后续的安全加固赋予准确的决策依据。

（一）自动化漏洞扫描

自动化漏洞扫描主要使用专业的安全扫描工具，按照工具内置且不断更新的漏洞知识库，对目标电力信息系统的网络设备、服务器、操作系统、数据库和应用软件实行系统的安全检测。可以快速、大范围地对目标资产进行探测，可以发现软件版本过旧、危险的系统配置、重要的安全补丁缺失、常见的服务层已知漏

洞。其最大的优点就是扫描速度快、覆盖面广，适合对大量资产做初步的安全检查，是周期性安全风险评价以及合规性检验的基本方式。

自动化漏洞扫描在电力信息系统安全运维实践当中，起到的是“安全体检”的关键作用。测试人员要根据系统的实际情况来量身定做扫描策略，确定扫描目标范围和深度，最后开始扫描任务。扫描结束后会自动生成详细的报告，其中不仅会列出已找到的漏洞还会标注每一个漏洞的风险等级 (高、中、低) 同时会对每一个漏洞做出详细的说明，解释危害以及给出解决方案。形成起对扫描、分析、修护及复测的闭环工作程序，这是不断削减系统安全风险，防止已有漏洞被利用的关键保证。

（二）手动渗透测试

与自动化扫描广度优先的策略不一样，手动渗透测试是一种深度优先、目标明确的攻击模拟活动。由有着丰富安全经验的专家扮演攻击者，采用各种各样的攻防手段，包括信息搜集、漏洞分析和社会工程学等等来攻破系统的安全防线。专家的创造性、逻辑推理能力，可以发现自动化工具无法发现的复杂的业务逻辑漏洞、访问控制漏洞、多个低危漏洞组合起来的高危安全威胁。

手动渗透测试严格按照方法论进行，完整的覆盖前期信息收集、中间渗透、最后达到目标的全过程。信息收集阶段测试人员尽可能多地获取目标系统架构、技术栈、业务功能等信息。然后进行威胁建模和漏洞分析来发现潜在的攻击路径。获得正式授权之后，测试人员会试着用已经发现到漏洞进行渗透，比如偷盗数据库中敏感数据、篡改电力营销系统计费信息、甚至向信息系统内横向移动来渗透生产控制网络。其目的在于真实模拟攻击者可能用到的各种高级攻击手段，来检验系统的实际防御能力。

手动渗透测试的最终产物就是一份高质量的渗透测试报告。这份报告不是漏洞的罗列，是整个攻击过程的记录，对于攻击路径中每一步所用到的漏洞，都有清楚的描绘，并且用实际攻击成果证明漏洞真实危害。这样系统负责人就可以直接看到安全风险对业务造成的影响，更有针对性地进行修复与加固，从而大大提高系统纵深防御的能力。

（三）常见 Web 漏洞测试

电力信息系统中的各种管理平台、数据门户、客户服务网站等 Web 应用由于直接暴露在互联网上，成为网络攻击的主要目标，因此安全测试的重点是这些

Web 应用。对上述的应用进行常见的 Web 漏洞测试，可以保证系统入口的安全。SQL 注入、跨站脚本属于破坏性较大，且代表性比较明显的两种漏洞。SQL 注入漏洞会使攻击者经由输入框或者 URL 参数来构造恶意的 SQL 查询，进而对后端数据库实施未经授权的增删改查操作，造成核心生产数据以及客户信息泄露。跨站脚本漏洞是指攻击者可以往网页中嵌入恶意脚本，当其他人浏览到该网页的时候，就会在他们的浏览器中执行这个脚本，从而实现窃取用户的会话、篡改网页内容或者将用户重定向到恶意网站等攻击。

对这些常见 Web 漏洞的测试需要细致和全面，其核心要点可见下表。

常见 Web 漏洞测试要点表

漏洞类型	漏洞描述	测试核心
SQL 注入	攻击者利用应用对用户输入验证不严的缺陷，注入恶意的 SQL 代码，从而操纵或窃取数据库中的数据。	对所有用户输入点（表单、URL 参数、HTTP 头等）提交特殊字符和逻辑语句，观察系统响应，并使用专业工具验证。
跨站脚本	攻击者将恶意脚本注入到网页中，当其他用户访问时，脚本在用户浏览器中执行，可能导致会话劫持或信息泄露。	在各输入点提交不同类型的脚本代码，验证系统是否对输入和输出进行了充分的过滤或编码，覆盖存储型、反射型和 DOM 型 XSS。
跨站请求伪造	攻击者诱导已登录的用户在不知情的情况下，向服务器发送非预期的请求（如修改密码、转账等）。	检查系统是否采用 Token、验证 Referer 或二次验证等机制，来确认关键操作是否源自用户的真实意图。
不安全的直接对象引用	应用程序通过 URL 参数等方式直接暴露内部对象（如用户 ID、文件名），导致攻击者可通过修改参数来访问未授权的数据。	尝试修改 URL 中的 ID 等参数值，检查是否存在水平越权（访问他人数据）或垂直越权（访问更高权限资源）的缺陷。

除了上表列出的漏洞之外，SQL 注入测试还要覆盖所有接受用户输入的接口，即表单、URL 参数、HTTP 头部。提交含有数据库查询特殊字符（单引号、分号等）或者逻辑判断的输入，观察应用是否会出现异常信息返回或者页面结果出现非预期的变化，以此来大致判断是否存在漏洞。之后就可以用专业的工具或者手工构造延时查询、布尔盲注等高级技巧来对它进行验证和评估。

跨站脚本测试的核心就是检验系统对用户输入、输出是否进行了严格的过滤、编码。测试人员会往不同的输入点注入诸如 `<script>alert</script>` 这样的探测脚本，看它们是否能在页面上成功执行，需要覆盖存储型、反射型以及基于 DOM

的全部 XSS 情形。

二、数据安全测试

数据是电力信息系统最核心的资产，包括电网运行状态数据、设备状态数据、用户信息数据以及经营管理工作数据等各种数据。数据安全测试的根本目的是保证数据在数据的整个生命周期内（传输、存储、使用等过程）的机密性、完整性、可用性，测试系统对数据的保护能力。

（一）数据传输加密测试

在复杂的网络环境下，特别是数据要通过公共网络进行传输的时候，被窃听、篡改和伪造的风险就会成倍增加。数据传输加密测试，对电力信息系统内部所有敏感数据的通信链路进行检查，应使用足够强度的加密措施。测试重点对象有用户登录时提交的账号密码、用户的个人身份信息、支付数据、远程下发的控制指令、内部系统之间交互的重要业务数据等。任何以明文形式传输的敏感信息都容易被攻击者截获。

数据传输加密测试一般用网络流量分析技术来完成。测试人员用 Wireshark 等网络协议分析工具截取客户端和服务器间通讯的数据包。分析数据包可判定系统强制要求用 TLS 等安全协议通信，可以检查加密协议版本是否有已知的安全漏洞，比如 PoODLE 攻击，核对服务器证书是否有效、签发机构是否可信、客户端有没有正确验证证书，防范中间人攻击。还需检查页面是否有混合内容加载，也就是在 HTTPS 页面上通过 HTTP 方式传输资源，因为这也会造成安全风险。

（二）数据存储加密测试

即使系统的网络边界以及应用层的防御坚不可摧，也不能保证不会被攻破。当攻击者已经绕过外围的防护直接接触到后端的数据存储系统的时候，这时数据存储加密就成为最后的防线来保护核心资产。此项测试主要检验系统针对存储在数据库、文件系统或者备份介质里的敏感信息采取的加密保护措施是否有效。对于电力信息系统来说，就是用户的用电数据、计费信息、员工个人信息、电网地理信息等关键数据。

数据存储加密的测试过程较为复杂，通常要求测试人员模拟已获取数据库访问权限或服务器文件系统读取权限的场景，以验证数据的安全状态。测试人员会直接查询数据库中的敏感字段，或者分析数据文件的二进制内容，来判断数据是

否以密文的形式进行存储。确认数据被加密只是第一步，还要看其采用的加密算法强度是否达到行业标准，密钥管理机制是否安全。加密密钥若被硬编码在代码中，或者存储加密的配置文件里是明文形式，或者密钥轮换、分发机制有缺陷，那么存储加密措施就形同虚设。

（三）权限控制测试

权限控制是保证数据安全、系统功能安全的重要手段，权限控制的设计与实现的好坏，直接关系到系统抵抗内部威胁、权限滥用的能力。权限控制测试是为了验证系统是否严格遵守最小权限原则，即保证每个用户只能访问被明确授权的资源、功能，不能越权访问权限之外的数据。健全的权限控制体系可以有效地阻止攻击者在获得低权限账户之后，通过各种手段提升权限（垂直越权）或者访问同级别其他用户的数据（水平越权）。

权限控制测试主要是围绕垂直越权、水平越权这两种情况进行。垂直越权测试就是模拟低权限用户去尝试做高权限的操作，比如，营业厅普通操作员访问只对管理员开放的系统配置页面，或者尝试执行数据批量导出等敏感功能。水平越权测试模拟普通用户访问别的用户的私有数据，即电力客户修改 URL 的客户编号来查看其它客户的用电账单或用电详情等。

为了能够有效地进行权限控制测试，测试人员必须创建或者获取具有不同角色、不同权限的账号来进行登录。他们会分析应用的请求逻辑，主要是 URL 路径以及请求参数，试图构造出可以访问无权限 API 接口或者页面的请求。验证的关键点是所有的权限判断逻辑都必须在服务器端强制执行，而不能只依靠前端界面的元素隐藏或者禁用来完成，因为客户端的任何限制很容易被绕过。只有严密的后端权限校验，才是一切越权漏洞的杜绝之本。

三、应用安全测试

安全测试主要是针对应用程序自身逻辑、功能、配置进行测试，它的范围不单是数据保护，更多的是发现并修补攻击者可以利用的业务流程漏洞、认证授权缺陷、不安全的系统部署配置。这是保证电力信息系统核心功能稳定可靠、不受恶意控制的重要测试领域。

（一）身份认证与授权测试

身份认证是应用安全的第一道大门，用来判断用户身份是否合法；授权是在

身份确认之后，决定用户可以做些什么。身份认证与授权测试目的，就是全方位地检验这道大门的牢固程度，保证只有合法用户才能进入系统，而且在系统内部也要严格遵守为每个用户划定的权限边界。对于直接和电网调度控制相关的电力信息系统来说，任何一个微小的认证漏洞都会造成不可挽回的损失。

对身份认证机制的测试需覆盖其完整的生命周期,包含但不限于以下关键点:

1.1、检测密码策略强度是否符合要求，即强制用户使用大小写字母、数字和特殊符号结合构成的密码，长度满足要求，历史记录也符合要求。并且应该测试系统有没有防暴力破解的机制，比如登录失败次数限制、账户锁定、验证码等。

2. 认证绕过尝试：直接请求需要登录才能访问的内部 URL，看系统是否存在没有权限访问漏洞。

3.3、凭证传输安全：确保用户登录凭证一直走加密通道，避免在传输过程中被窃听。

4. 多因素认证有效性，如果系统开启了多因素认证，需要对它的逻辑进行严密的测试，看是否存在验证码可以被暴力破解、第二因素验证可以被绕过的漏洞。

5.5、辅助认证功能的安全：对忘记密码、通过邮箱或者手机重置密码等功能进行详细的测试，防止攻击者利用其中的逻辑漏洞来重置任意用户的密码。

（二）会话管理测试

用户成功登录之后，应用就会为其创建一个会话，在之后的交互中，会根据会话标识来保持用户的登录状态。会话管理机制是否安全，决定别人能否盗用你的登录状态。会话管理测试的主要任务，就是对会话标识从生成、传输、验证到销毁的整个生命周期展开安全检测，从而防止会话劫持、会话固定等攻击。

对会话管理进行测试的时候，测试人员会重视会话标识自身是否安全。会话标识的长度和随机性要足够大，不能被攻击者用猜测或者暴力破解获取到。同时需要给承载会话标识的 Cookie 设置合适的安全属性，用 Secure 属性保证它只通过 HTTPS 传输，用 HttpOnly 属性保证客户端脚本不能访问，从而有效防止网络嗅探、XSS 攻击。还要检验系统会话超时机制 (空闲超时、绝对超时等) 是否有效，即确保用户点退出登录后，服务器端会话被彻底销毁，不只是清除用户的客户端 Cookie，从而完全杜绝会话重用的风险。

（三）安全配置审计

大量的安全事件并不是由于代码漏洞造成的，而是因为系统配置不安全。服

务器软件、中间件、数据库甚至操作系统，若采用默认配置或者配置不当，都会给攻击者留下可乘之机。安全配置审计属于一种系统的检查工作，它一般会依照行业里公认的 CIS Benchmarks 这类安全基线标准，对依靠的全部技术栈实施全面的安全配置审核并加以加固。

电力信息系统实践中的安全配置审计范围很广。它包含查看生产服务器上是否存在不必要的服务或者多余的开源程序，是否打开了不必要的网络端口，这些都是可能的入侵点。审计工作会验证所有的管理员账户是否被重命名或者禁用，其默认密码是否已经修改成强密码。并且要仔细查看文件系统以及重要的配置文件的访问权限是否恰当，符合最小权限原则。除以上所列之外还要审计应用程序是否关闭了调试模式、错误信息是否过于详细以至于会泄露系统的内部架构和技术细节。保证系统以及应用程序的安全日志功能已经开启，并且配置了合适的审计策略，这是实现威胁检测和事后追溯的基础，也是配置审计的一部分。

第六章 电力信息系统部署实施

电力信息系统部署实施就是将它由设计蓝图变为现实使用的桥梁。本章主要对部署规划、环境准备、方案制定的全过程进行详细的阐述，给复杂电力信息系统平稳高效的上线提供一套完整、严谨、可操作的技术与管理框架，保证系统建设可以真正为业务服务，创造实际的价值。

第一节 系统部署规划

系统部署规划作为部署实施的第一步，给部署实施指明了方向，确定了目标。周密的部署规划要预见可能存在的风险，合理安排资源，保证系统按计划规定的时间、质量要求顺利完成上线。本节主要是对部署架构设计、环境准备、方案制定这三个方面做出具体的分析。

一、部署架构设计

部署架构设计属于系统部署规划的关键部分，部署架构设计的好坏直接关系到系统是否健壮、是否易于扩展以及是否便于维护。优秀的部署架构要满足现在的业务需要，也应留有扩展余地以便能够支撑未来业务的发展和技术的变化。

（一）物理部署与逻辑部署

物理部署和逻辑部署是部署架构设计里互相联系、互相依赖的两个方面。物理部署指的是系统各组成部分的实际放置以及连接方式，是构成系统物质基础。服务器在哪个机柜、存储设备怎样连接、网络交换机怎样级联等问题都会涉及，直接关系到系统的物理安全、网络可达性以及硬件资源利用率。

逻辑部署是在物理部署的基础上，从系统的功能和服务的角度来进行系统组织和划分的。定义了应用软件、中间件、数据库等逻辑组件之间的分布关系以及交互方式，不考虑到底层物理承载的细节。以一个电力调度系统为例，它在逻辑上可以被划分成前端展示层、业务处理层、数据服务层等等，这些层是可以灵活

部署到不同的虚拟机或者物理服务器之上的。逻辑部署更接近于应用架构，重视服务的高内聚低耦合，利于系统的开发、测试、维护。

物理部署和逻辑部署分离又协作就体现出现代信息系统的灵活性。利用虚拟化、容器化的技术，使得应用服务迁移、扩容、升级更简单地把物理资源同逻辑部署分开。对电力信息系统来说，解耦设计十分关键，它可以在保障基础设施稳定高效的基础上，让业务快速迭代，从而达到资源最优配置和系统性能全面提升的目的。

（二）集中式、分布式部署模式

电力信息系统架构选型中集中式、分布式是两种各有特点的基础部署方式。集中式部署，系统核心计算资源、数据存储、应用服务集中到一个或者几个地理位置相近的数据中心上。它的优点是结构简单，管理维护方便，集中管理的所有资源利于保证数据一致性、安全性。大部分管理性强、实时性要求不高、业务量大的电力信息系统（总部的财务管理系统、人力资源系统等）采用集中部署方式可以大大降低运维成本，提高工作效率。

分布式部署就是将系统不同的模块或者数据分散到地理上不同的节点，各个节点通过网络协同工作来完成共同的任务。电网规模大、地域分布广的情况下，分布式架构就体现出它的优势。分布式部署省级调度自动化系统、地市级配电管理系统等可以提高数据及计算靠近业务现场的便利程度，减少依靠骨干网络的必要性，进而增加局部业务响应的速度和可靠度。同时分布式架构具有良好的横向扩展性，可以应对业务量的增加，单个节点的故障一般不会造成整个系统瘫痪。

集中式或者分布式部署要按照电力信息系统具体业务特性、性能需求、可靠性需求、建设成本。现代电力信息系统设计大多使用混合模式，即核心数据、核心业务集中式部署以保证统一管理、数据权威性，边缘计算、高实时性要求的业务分布式部署以达到快速响应、就近服务的目的。混合架构把两种模式的优势结合在一起，是建设新一代电力信息系统的一种常见选择。

（三）高可用与容灾部署方案

高可用和容灾部署是电力信息系统业务连续性的生命线，对于承载核心业务、关系电网安全稳定运行的系统来说更是如此。高可用性就是利用冗余设计，尽可能地减少单点故障造成的系统停机时间，保证系统持续提供服务。

高可用部署通常在单一数据中心内部实现，其实现方式多种多样：

1. 关键组件冗余，对服务器、存储器、网络、电源等任何一种存在单点故障的可能硬件都做了双机热备、服务器集群、磁盘阵列、双路电源等冗余方案。

2. 负载均衡：利用负载均衡器把业务请求分配给后端多个处理单元，可以防止某个单元超负荷，也可以在某个单元失效的时候自动从服务池中剔除，从而不影响整体服务。

3. 故障自动切换，用心跳检测等手段对系统的各个组件的健康状况实施实时的监视。当主节点或者主服务发生故障的时候，高可用集群软件可以快速地把业务切换到备用节点上，整个切换过程对于用户来说是透明的，可以在秒级或者分钟级内完成业务的恢复。

容灾部署是在高可用的基础上，对可能导致整个数据中心毁灭性破坏的灾难，如火灾、地震、大面积断电等做出的考虑。它依靠在异地建立一个或者几个备份数据中心，保证主数据中心完全瘫痪之后业务仍然能够恢复并继续运转。容灾方案的核心指标是恢复时间目标和恢复点目标，根据这两个指标的不同，可以选用不同等级的方案，具体见下表。跨地域的容灾部署模式，就是电力关键信息基础设施安全最后一道防线。

电力信息系统容灾等级参考表

容灾等级	恢复时间目标	恢复点目标	技术 / 方案特点
数据级容灾	小时级至天级	小时级	采用远程磁带备份、数据异步复制等技术
应用级容灾	分钟级至小时级	秒级至分钟级	部署备用站点、应用热备、数据同步或异步复制
业务级容灾	秒级至分钟级	零或秒级	实施两地三中心、异地多活、全局负载均衡等方案

二、部署环境准备

部署环境指的是电力信息系统运行所处的物理平台和基本条件，它的好坏直接影响到系统能否顺利部署并实现长时间稳定运行。环境准备工作复杂而且要求严格，一定要按设计规范执行，为系统顺利入驻和高效运行打下良好的基础。

（一）机房环境要求（电力、空调、消防）

电力信息系统的正常运转，完全依靠一个专业可靠的机房环境。机房环境建设要严格按照国家标准《数据中心设计规范》等执行，给信息设备营造出安全、

洁净、恒温恒湿的“家”。

电力供应是机房的生命线，对承担重要业务任务的电力信息系统来说，机房必须提供持续、纯净、不间断的电源。一般需要配置双路市电引入、大功率不间断电源系统和备用柴油发电机组。不间断电源可以在市电中断或者电压波动时平滑过渡，在切换至发电机供电前不会对设备造成影响，从而保证业务连续性。所有的供配电线路设计应标识清楚、布线规范，并具备过载、短路保护功能。

温湿度控制也不能忽视，服务器、存储这些电子设备工作的时候会发出很多热量，如果不能及时散发出去，就会对它们的性能和寿命造成很大的影响。因此机房需要安装专门用空调设备来保持机房环境温度、湿度在一个标准区间内（环境温度一般要求 22 ± 2℃，相对湿度 40%~60%），使空气洁净。空调系统也要有冗余设计，保证单台设备出现故障或者维护时，机房环境参数不会产生大的波动。

消防安全是机房环境建设中的重中之重，一定要防患于未然。机房要使用防火材料进行装修，设置独立的消防分区。消防系统应配置高灵敏度的温感、烟感火灾探测装置，采用对电子设备无损害的气体灭火系统，例如七氟丙烷、IG541 等。完备的消防报警与联动控制、应急照明、疏散通道是人员、设备安全的保障。

（二）网络环境规划与配置

网络是电力信息系统各组成部分的“神经系统”，网络规划与配置的好坏直接影响到数据传输的快慢、是否可靠、是否安全。电力系统网络环境规划较为复杂，既要保证生产控制大区和管理信息大区之间严格隔离，又要保证调度生产业务绝对安全。

网络规划首先要做需求分析，确定系统内部各个组件之间、系统与外部用户以及其他关联系统之间的通信需求、带宽需求和服务质量等级。在此基础上设计网络拓扑结构，一般采用成熟的核心层、汇聚层、接入层三层架构，该架构层次分明、易于扩展、带宽高。电力调度数据网中，网络被划分为不同的安全域，实时控制区（安全一区）、非控制生产区（安全二区）等，各安全域之间用防火墙、安全隔离网闸等设备进行逻辑或者物理隔离，严格遵循网络专用、横向隔离、纵向认证的原则。

网络配置具体的工作有 IP 地址和虚拟局域网的规划、路由协议的选择和配置、交换机和路由器端口的设置等。IP 地址规划要具备前瞻性，为将来业务发展

留有余地。虚拟局域网划分可以有效地隔离广播域，提高网络安全。选择路由协议要考虑网络规模和收敛速度这两个因素。还必须要有严格的网络安全策略，对访问控制列表进行配置，部署入侵检测和防御系统等，以抵御内外部网络攻击，保护电力信息系统的网络边界安全。

（三）硬件设备选型与采购

硬件设备是承载电力信息系统的物质基础，它的性能、可靠性、兼容性一起决定了整个系统能达到的上限。硬件选型是综合技术先进性、业务适用性、成本效益、长期服务保障等各方面因素来做出的一种决策过程，主要是指服务器、存储、网络、安全等设备。

服务器选择要按照应用负载特性来决定，计算密集型应用选主频高、核心多的处理器，内存密集型应用配大容量内存。选择存储设备要考虑容量、读写性能（IOPS、吞吐量）以及数据保护，根据数据的重要性、访问频率选择合适的存储技术，存储区域网络、网络附加存储、分布式存储。选择交换机、路由器等网络设备主要看所选择的设备端口密度、背板带宽、交换容量、支持哪些协议等是否满足规划的流量模型和性能要求。

采购是选型工作的继续，应该按照公开、公平、公正的原则，采用招标、竞争性谈判等方式进行。采购时不仅要考虑设备的初次购置成本，而且应该考虑设备全生命周期总拥有成本，即包括设备功耗、维保等后续支出。供应商选择也不能忽视，要考察供应商的技术实力、市场信誉、售后服务能力、备品备件保障体系。在签订合同时应当明设备的具体规格、交货时间、安装调试服务、质保年限、技术支持响应等级等内容，保证采购工作顺利进行，保障项目单位的合法权益。

整个选型采购的过程里一份详尽的技术规格书非常重要。它要清楚、无歧义地说明设备所有的技术参数和功能要求，成为评判供应商响应方案、后续设备验收的依据。只有经过规范的程序、严格的控制，才能保证所采购的硬件设备能够满足电力信息系统建设的需求，为电力信息系统的稳定高效运行提供可靠的硬件支持。

三、部署方案制定

部署方案就是把部署规划中的宏观设计转化为可以实施的步骤。一份周密详细的部署方案，对于庞大复杂的部署工程可以做到有条不紊、高效率、低风险地

进行。方案的制订要多方合作，从技术细节、人力资源和潜在风险三方面加以考虑。

（一）部署步骤与时间计划

详细拟定部署步骤及时间表对于保证项目按时交付有非常重要的作用。这就需要把整个部署过程拆解成一系列具体的、可以量化的任务，为每一个任务安排一个合理的完成时间以及所需资源。

1. 任务分解和依赖性分析，将部署工作由大到小地进行分解，得到完整的工作分解结构。任务的颗粒度要适中，便于跟踪、管理。部署一般分为：机房环境验收、硬件设备上架通电、操作系统与虚拟化平台安装、存储网络配置、数据库安装配置、中间件部署、应用软件安装、数据初始化、系统联调测试、安全加固、性能优化、用户验收测试和最终系统上线切换。并且要确定任务之间的逻辑依赖关系，例如应用软件的安装只能在数据库和中间件安装完成之后才能进行。

2.2、时间计划的制定，以任务的分解为基础，使用甘特图、网络图等项目管理工具制定出具体的时间计划。给每个任务确定一个工期，指出开始和结束的日期。利用关键路径法找出影响项目总工期的关键任务序列，也就是关键路径。项目管理团队要重视关键路径上的工作，把最好的资源投放在关键路径上的工作上，保证关键路径上的工作不延误，进而保证整个部署项目按计划进行。计划中应该有明确的里程碑节点，例如硬件环境就绪、应用部署完成、验收测试通过等，用作检验阶段性成果的检查点。

（二）人员分工与职责

明确的分工、清楚的责任是实现高效团队合作的基础，可以防止工作之中出现推诿扯皮或者责任真空的情况，保证布置下去的每一个环节都有专人去承担。电力信息系统部署项目一般要组建由业主单位项目经理、技术人员，软件开发商实施顾问，硬件供应商工程师，系统集成商技术专家等人员组成的联合项目团队。

为了做到权责对等，可以引入责任分配矩阵这样的管理工具。责任分配矩阵清楚地定义了在每一项任务上谁去执行、谁做主管、谁需要被咨询、谁应该被告知。以“数据库安装”任务为例，数据库管理员是执行者，技术总监是负责人，应用开发团队是被咨询方，项目经理是被告知方。这样每个人就会明确自己的职责，保证工作沟通更加有效、执行更到位，为复杂部署工作奠定良好的组织保障。

（三）风险评估与应急预案

在电力信息系统部署过程中，会遇到很多事先没有预料到的技术问题或者管

理风险。对项目风险做全面评估并制定应急预案，是化被动为主动、提高项目抗风险能力的必要步骤。此项工作目的在于找出潜藏的威胁，剖析其出现的可能性以及影响的大小，预先制订应对方案，保证问题发生的时候能快速且有效地加以解决，将对项目进度和质量的不良影响控制在最小范围。

风险识别阶段要集思广益，从技术、管理、资源、外部环境等各方面分析可能遇到的问题。技术风险有软件版本不兼容、硬件设备到货晚或有毛病、新旧系统数据迁徙失败、网络性能不佳等等。管理风险有人员配合不到位，需求理解有误，沟通渠道不畅通等情况。对识别出的每一个风险，都要对其进行发生的概率和发生之后所造成的后果的严重性进行评估，来确定风险的优先级，从而对高优先级的风险进行重点监控。

对每一个已经识别出来的关键风险，都要制定出具体的、可操作的应急预案。预案中要明确风险发生的预警信号，应急响应的组织架构及负责人，详细的处置步骤，需要调用的资源以及事后恢复流程。以核心交换机突发故障为例，应急预案包括立即启用备用交换机、通知网络设备供应商紧急技术支持、上报项目管理层等。定期进行应急演练，检验预案的可行性，使团队成员熟悉操作流程，是保证预案在危机时刻能发挥真正作用的重要环节。通过严格的风险控制可以大大提高部署项目成功的概率。

第二节 硬件环境配置

电力信息系统的稳定运行以及高效处理，不能缺少一套经过精心设计并且合理配置的硬件环境。硬件基础设施指的是承载各种业务应用以及海量数据的物理平台，硬件基础设施的可靠性、性能优劣、是否具备可扩展性及安全性等状况，直接影响到整个信息系统服务质量的好坏。本节主要研究服务器、网络、存储等核心硬件设备配置技术以及实施要点，给电力信息系统的物理基础建设提供指导。

一、服务器配置

服务器是电力信息系统的计算中心，运行着操作系统、数据库以及各种应用软件，它的性能好坏直接影响到整个系统反应的快慢和处理问题的能力强弱。合理的服务器配置应当依照业务需求，数据量，可靠性，发展预期等各方面的考虑，

在保证电力业务连续运行的前提下，以最小的代价创建起一个稳定的，高效的，可以拓展的运算平台，支撑电力业务创新发展。

（一）服务器选型（机架式、刀片式）

电力信息系统建设中，服务器的形态选择是建立基础架构的第一步，主要是在机架式服务器和刀片式服务器之间进行权衡。机架式服务器为高度标准化的工业产品，宽度统一为 19 英寸，高度用 U 来表示。该类服务器优点是配置灵活，单个设备就可以具备独立的电源、风扇和管理模块，可以独立部署。对于分布式部署的电力站点或者中小型数据中心来说，机架式服务器提供了一种简便的横向扩展方法，业务增长的时候可以逐步增加服务器数量，不需要对现有架构做大的改动。成熟的生态系统以及广泛的兼容性，也使备件获取、维护方便，可以承载各种通用型应用和特定的业务。

刀片式服务器就是一种高密度、集成化的计算平台。它把若干个独立的服务器主板也就是“刀片”，放进同一个共享机箱里面，这些刀片共用电源，散热，网络交换以及管理模块。此种设计最大的优势在于空间利用和能源利用率都很高，适合大规模集中部署如大型电力数据中心、云计算平台等。利用统一的管理界面对机箱内所有的刀片进行集中控制、部署、维护，大大简化了运维工作，降低了管理成本。刀片架构非常适合需要大量计算资源的虚拟化环境、高性能计算集群以及需要业务快速横向扩展的应用。

根据具体应用场景以及长远规划来决定采用机架式或者刀片式服务器。对要灵活使用、支持异构平台共存或初期投入较少的项目来说，机架式服务器更具有经济性。反之对于追求高密度部署、简化管理、看重能效、计划大规模标准化建设的大型电力企业数据中心来说，刀片式服务器在整合度、管理效率和总体拥有成本上的优势更加明显。决策时也要考虑到数据中心的物理空间、电力容量、散热情况、运维团队的管理能力。

（二）CPU、内存、磁盘配置

服务器的性能铁三角是中央处理器、内存和磁盘组成的，这三项的恰当配置会决定电力信息系统处理效率与稳定性的高低。中央处理器是服务器的大脑，选择时主要考虑核心数、主频、缓存。对实时监控、交易处理这种要求迅速响应的单线程密集型任务来说，采用主频较高的处理器比较合适；对于大数据分析、虚拟化平台这种多任务并行处理的应用，选择物理核心多的处理器会获得更好的并

发处理能力。

内存是中央处理器和磁盘之间数据高速公路，内存容量和速度影响系统处理数据的速度。电力系统中的各种应用软件尤其是内存数据库、实时分析平台等对于内存的大小非常敏感。内存的数量如果足够多，那么热点数据和应用进程就可以被缓存起来，进而大幅度减少对低速磁盘的读写请求，延迟也会因此得到改善，系统吞吐量也会提升。选择有错误校正码功能的内存可以检测并纠正内存中发生单比特错误，给电力系统数据的完整性以及服务器长时间的稳定运行提供保障。磁盘是数据的最终存储载体，它的好坏直接影响到数据的存取速度。目前主流的配置大部分都是使用固态硬盘 + 机械硬盘的混合存储。固态硬盘由于读写速度非常快，所以适合存放操作系统、数据库索引和高频交易数据；机械硬盘由于单位容量成本低，所以适合存放日志、归档数据和非关键业务文件，从而达到性能和成本的平衡。

（三）RAID 配置与磁盘管理

独立磁盘冗余阵列就是把多个独立的物理磁盘组合成一个逻辑单元，目的是提高存储性能、保证数据冗余。数据安全和可用性是电力信息系统极为重要的因素，因此选择正确的 RAID 配置成为了服务器部署的关键部分。不同的 RAID 级别为性能、容量利用率和冗余度之间提供了不同的权衡方案。表中清楚地比较了这些常用的 RAID 级别特性与适用场合。

常见 RAID 级别特性对比表

RAID 级别	最少磁盘数	容错能力	性能特点	电力系统适用场景
RAID 5	3	容忍 1 块磁盘故障	读性能好，写性能一般，磁盘利用率高	文件服务、Web 应用等读多写少场景
RAID 6	4	容忍 2 块磁盘同时故障	读性能好，写性能较差，数据安全性更高	承载关键业务数据、要求长期稳定运行的核心系统
RAID 10	4	容忍每组镜像中 1 块磁盘故障	读写性能俱佳，随机 I/O 性能优异	数据库、在线交易处理等需要高 I/O 和低延迟的应用

从上表可以看出 RAID 5 因为读性能好，磁盘利用率高，所以是读密集型应用的经济之选。RAID 6 使用双奇偶校验，能提供更好的数据保护，适合用来存放重要业务数据。RAID10 由于综合性能最好，所以成为高负载数据库等重要应

用的选择。

磁盘管理不只是RAID初次配置，而是在以后动态调整和维护中也会使用到。逻辑卷管理技术给操作系统提供很大的灵活性，可以在线调整逻辑卷大小，使存储空间分配和调整更加方便，甚至可以不中断服务。有效的磁盘管理包含定时对磁盘的健康状况实施检查，从读取磁盘的健康状态监测信息来发出警报。RAID阵列发生磁盘故障的时候，要及时替换并重建才能保证系统的冗余性。电力系统要形成标准的磁盘故障处理程序，保证备件储备充足，还要定时做恢复演练。对重要业务系统来说，配置热备盘可以在主盘出问题时立即启动重建过程，使数据暴露在风险中的时间缩短到最少，从而最大程度上保证电力信息系统的连续性以及数据完整性。

二、网络设备配置

网络是电力信息系统各硬件单元之间联系的“脉络”，其配置好坏直接决定数据传输的速度、稳定性以及安全性。一个精心设计的网络架构，可以保证信息流从数据采集终端到后台处理中心，再到各级管理应用之间畅通无阻。网络设备的配置包括基本的交换路由功能以及安全、负载均衡、地址规划、逻辑域划分等高级策略。

（一）交换机、路由器配置

交换机和路由器是形成电力信息系统网络骨架的基本设备。交换机核心的配置任务就是创建分层、无环、高效的二层网络环境。在典型的三层架构中，接入层交换机直接和服务器、终端等设备相连，需要配置好虚拟局域网成员关系、端口速率、双工模式；汇聚层交换机用来汇集接入层的流量并执行访问策略，一般会使用链路聚合技术来提高带宽和可靠性; 核心层交换机以高速转发为主要目的，连接各个汇聚层和核心路由设备，保证网络主干道的畅通。为防止网络环路造成广播风暴，必须开启并优化生成树协议或者快速生成树协议。

路由器负责在不同的网段、不同地理位置网络之间进行数据包的寻址和转发。电力广域网中路由器配置的核心就是选择路由协议和实施路由策略。开放式最短路径优先等内网关协议，可以依据链路状态动态计算最佳路径、快速收敛路由、均衡负载，被广泛应用于大型企业的内部网络。边界路由器如果连接外部网络或者不同的自治系统，则要配置边界网关协议来精细控制路由的发布和接收。细致

的路由策略配置，路由过滤、路径属性改变等都是保证网络安全、实施流量工程、满足特殊业务通信需求的重要方法。

（二）防火墙与负载均衡器配置

防火墙是电力信息系统的一道安全门，它的主要任务就是按照事先设定的策略，严格地控制进出网络的数据流，使内部资源不被未经许可的人访问或者遭受恶意攻击。防火墙基础配置就是定义访问控制列表，对源地址、目的地址、端口号、协议进行精确匹配后来决定数据包的放行还是阻止。对电力系统而言，也要遵循最小权限原则，也就是默认拒绝所有的流量，只有业务必需的端口和服务才予以开放。新一代防火墙具有入侵防护、应用识别、用户认证等功能，它具备更深层次的威胁检测和防护的能力，所以策略配置要与电力业务的实际情况相结合。

负载均衡器是提高应用可用性以及扩展性的主要设备。它可以把客户请求流量智能地分配到不同的服务器上，避免单点过载的发生，保证服务不中断。负载均衡器的配置核心就是定义虚拟服务器（对外提供服务的 IP 地址和端口）、创建后端服务器池，并选择合适的调度算法，如轮询、最少连接数或加权算法，具体选择要根据服务器性能和业务特点来定。健康检查是负载均衡器的又一主要功能，可以定时去探测后端服务器的应用情况。当发现某台服务器出现异常情况的时候，负载均衡器就会自动把该服务器从服务池中剔除出去，等它恢复到正常状态之后再重新加入进来，从而达成故障的透明切换，保证业务的高可用性。

对要求较高的可用性及安全性核心业务的防火墙、负载均衡器一般都会采用高可用部署方案。通过主备或者双活集群的方式，当一台设备出现故障的时候，另一台设备可以立刻接替它的工作，从而避免因为单一故障点造成的网络隔离或者服务中断情况的发生，给电力信息系统的稳定运行保驾护航。

（三）网络 IP 地址与 VLAN 规划

网络 IP 地址以及虚拟局域网的规划属于网络设计过程中的基础性工作，它同网络的管理效能、安全保障和未来发展息息相关。科学的 IP 地址规划要按照结构化、前瞻性的原则来实施，不能随便用掉 IP 地址或者后期乱调 IP 地址。

1. 分层规划：IP 地址分配要和网络物理或者逻辑结构一致。可以给不同的地理区域、不同的业务系统（生产控制网、办公信息网、调度数据网）或者不同的设备类型（服务器、网络设备、终端用户）划分连续而独立的地址段。于是就有了这样的分层结构，这就形成了路由汇总的基础，能大大减少路由表的条目数，

提高路由的速度。

2. 预留与扩展，在规划的时候，就要给每一个网段留出足够的地址空间，以备日后业务增长和设备增加时使用。合理的预留可以避免因为地址耗尽而做复杂的网络重组工作，保证网络可持续发展。

虚拟局域网技术可以使物理网络里存在多个逻辑上互不干扰的广播域。对不同的部门、业务或者安全等级的设备进行分类，然后将它们划分到不同的虚拟局域网中，既可以限制广播风暴的范围，又可以提高网络性能，也是很重要的网络安全隔离手段。以需要高度保护的电力监控和数据采集系统终端为例，将其和普通的办公电脑划分到不同的虚拟局域网中，再通过路由器或者三层交换机配置详细的访问控制列表，严格限制两个虚拟局 GAN 之间的互相访问，就可以很大程度上降低安全风险，保护核心生产系统。

三、存储设备配置

存储设备是电力信息系统的数据仓库，对生产运行、经营管理等各方面产生的海量数据进行长期保存。存储配置的目标就是创建一个高性能、高可用、高扩展并且容易管理的存储平台。数据量出现爆炸性增长时，挑选适合的存储架构和设备，做好细致的配置工作，对保证数据的安全以及业务的连续性来说非常关键。

（一）存储区域网络配置

存储区域网络是用专用的高速网络（一般用光纤通道）连接存储设备和服务器的一种架构，按块级的方式提供数据访问。远端存储像服务器本地磁盘一样可以访问，它性能高、延迟小，很适合做电力系统中大型数据库、虚拟化平台等交易密集型应用的承载体。

存储区域网络的配置属于一项细致的工作，它主要在于逻辑单元号的划分以及访问控制。存储管理员先在磁盘阵列上创建 RAID 组，在 RAID 组中再分出 1 个或者几个逻辑单元号。每个逻辑单元号对于服务器来说，就相当于一个独立的物理硬盘。为了保证数据的安全和隔离，必须对访问加以严格的控制。主要通过两种技术实现：第一种是“分区”技术，在光纤交换机上配置，它定义了哪些服务器的主机总线适配器可以和存储阵列的目标控制器端口通信，从网络层面将不同主机隔离开来。

第二种是“LUN 屏蔽”，它在存储阵列控制器上进行配置，它进一步规定

了特定的服务器（由主机总线适配器的全球通用名称标识来确定）可以访问哪些具体的逻辑单元号。分区、LUN 屏蔽这两种方法结合一起就能产生一个安全的存储环境，使服务器不能直接接触被指定的存储区，防止数据发生误操作或者越权访问现象。配置多路径 I/O 软件也十分重要，它可以使服务器对同一个逻辑单元号使用多条物理路径进行连接，达到路径冗余、负载均衡的目的，从而大大提升数据的访问可靠性以及性能。

（二）网络附加存储配置

网络附加存储是一种专用的文件级存储服务器，它通过标准以太网接入网络，使用 NFS 或者 CIFS/SMB 等网络文件系统协议，给网络中的各种客户端提供文件共享服务。相比提供块级裸设备的存储区域网络，网络附加存储提供的是即装即用的文件系统，部署和管理更加方便，适合电力企业内部办公文档共享、设计图纸存储、邮件附件存储、各种非结构化数据存储等场景。

配置网络附加存储设备，首先要将其接入企业局域网，并给它分配一个静态 IP 地址。管理员通过 Web 管理界面创建共享文件夹（共享卷），在创建时指定共享名称、容量配额、访问协议。根据不同的用户和应用的需求可以设置精细的访问权限，即给用户、用户组或者主机 IP 地址授予读取、写入或完全控制等不同的级别权限。与活动目录或者轻型目录访问协议服务整合，可以实现用户身份统一认证，极大简化权限管理工作。大多数网络附加存储设备都具有快照功能，可以定时为共享文件夹创建“时间点副本”，数据误删或者受损的时候可以快速恢复。

（三）备份存储设备配置

电力行业数据是核心资产，任何数据丢失都会造成严重的生产事故或者经济损失。因此，建立一个可靠的备份系统，是保证业务连续性的最后一道屏障。备份存储设备的配置属于整个备份体系的物理根基，其选择与配置决定着备份窗口的长短、恢复时间目标以及恢复点目标。

备份存储设备的种类很多，传统的磁带库单位成本低、具有离线存储特点，至今仍是长期数据归档和异地容灾的优选方案。而以磁盘为载体的备份设备，尤其是带有重复数据删除功能的虚拟磁带库或者备份一体机，可以实现更快的备份和恢复速度，大大缩减了备份窗口，能够符合更加苛刻的恢复时间目标要求。配置备份存储的时候，一定要按照备份策略去安排它的容量和性能。像业界熟知的

“3-2-1”备份黄金法则，也就是保存三份数据副本，采用两种不同的存储介质，且把一份放在异地，这就对存储介质的种类和容量提出了具体的要求。

备份软件同备份存储的联动配置非常关键。这就需要在备份服务器上识别出并配置好备份设备（创建存储池等），然后创建备份作业。备份作业要详细定义备份对象（整台服务器、特定的数据库文件、虚拟机），备份类型（全量、增量、差分），执行计划（备份频率、时间窗口），数据保留策略（数据在备份介质上保存多久）。定期恢复演练是检验备份系统是否有效唯一的依据，模拟灾难场景并实际恢复数据或者系统，可以保证在需要的时候，备份的数据是完整的、可用的，并且可以满足业务恢复的时效性要求。

第三节 软件安装调试

软件安装调试是把设计蓝图转变为实际运行的实体系统的关键步骤，也是把理论上的规划变为业务上实践的重要环节。本节主要对底层操作系统到上层应用全过程技术要点进行详细的描述，保证系统部署的规范性、稳定性、高效性。

一、操作系统安装与配置

操作系统是所有上层软件运行的基础，安装是否规范，配置是否合理直接影响到整个系统性能和安全。经过精心配置、安全加固的操作系统可以给电力核心业务提供可靠、稳固的运行环境，必须予以高度重视。

（一）服务器操作系统安装

选择并安装服务器操作系统，是电力信息基础设施建设的开端。Linux 系统由于开源、稳定、高效和强大的可定制性，在后台服务和数据库支撑方面得到广泛的应用；Windows Server 因为友好的图形界面、完善的商业支持、丰富的生态系统，常被用作桌面虚拟化以及特定应用服务的平台。具体选用哪种系统，要按照应用的实际需求，运维团队的技术栈以及安全等级综合考虑。

安装过程一定要严格按照标准化规范来操作。建议制作一个标准的分区方案、基础软件包和预设配置的自动化安装镜像，可以采用 Kickstart 来定制 Linux 的安装流程，也可以利用 Windows 部署服务实现 Windows Server 的无人值守安装。不但可以大大提高部署效率，而且可以保证多台服务器环境的一致性，减少人为

操作失误造成的差异。磁盘分区规划要按照系统用途做细致的设计，把根目录、用户目录、日志目录、临时文件目录等分别挂载到不同的逻辑分区，便于管理控制磁盘空间占用，同时可以设置不同的挂载参数来提高系统安全性。安装完成后要详细记载主机名，IP 地址，分区情况，初始账户密码等关键的配置信息，这些信息也是后期运维的主要参照档案。

（二）系统参数优化与安全加固

操作系统默认的安装配置不能满足电力生产环境的严格要求，必须做深层次的参数调节和安全加固，才能充分发挥系统的性能，尽可能地减小攻击面。参数优化主要是从 CPU、内存、网络和磁盘 I/O 四个方面入手，其目的是使系统资源的分配更符合上层应用的使用模式。对数据库服务器来说，可以调节内核参数，增大共享内存段大小，优化文件句柄数限制；对网络密集型应用来说，可以调节 TCP/IP 协议栈参数，增大传输缓冲区，改变连接队列长度，从而提高网络吞吐量和并发处理能力。

安全加固是电力信息系统安全的第一道防线，它的基本思想就是最小权限和纵深防御。这是一道系统工程，包含很多方面：

1. 服务与端口最小化，关闭不需要的系统服务和网络端口，比如 Telnet、FTP 等不安全的服务，只开放业务需要的端口，从源头上减少攻击的入口。

2. 账户和权限精细化：禁用或者重命名高权限的默认账号，禁止 root 或者 administrator 等账户的远程直接登录。强制推行强密码策略，对密码复杂度、长度、更换周期等做出具体规定。使用 sudo 等工具对不同的管理员的权限进行细致化分配并做审计。

3. 配置访问控制及防火墙，以 IP、端口、协议等对服务器的访问做严格限制。并且使用主机层面的访问控制（例如 TCP Wrappers）对具体服务增加额外的访问授权检查。

4. 开启并且配置全面的系统日志记录功能，保证所有的关键操作，例如用户登录、权限修改、软件安装等都被详细记录。开启日志转储功能，把全部日志汇聚到中央日志服务器上，集中起来加以分析并长久保存。

5. 文件系统安全：给重要的系统文件和目录设置严格的读、写、执行权限，防止被非法篡改。挂载文件系统时使用 nosuid、nodev、noexec 等安全选项来限制可执行文件和设备文件可能造成的影响。

（三）高可用集群软件配置

对于承载着电力调度、交易、营销等重要业务的系统来说，业务不能中断，单点故障是不能接受的。所以部署高可用集群成了保证系统可靠性的一种标准做法。高可用集群把多台服务器虚拟为一个逻辑整体，可以做到故障自动检测和业务快速切换，对外提供连续的服务。常用的有 Linux 平台的 Pacemaker、Corosync，Windows 平台的故障转移群集。下表给出两种主流方案的主要组件和特点。

主流操作系统高可用集群方案对比表

组件 / 功能	Linux 方案 (Pacemaker + Corosync)	Windows 方案 (故障转移群集)
核心组件	Pacemaker (资源管理器), Corosync (集群通信)	Cluster Service (集群服务)
集群通信	心跳网络，支持多播 / 单播	心跳网络，集成于集群服务
资源管理	灵活的资源代理 ，支持约束与规则	资源 DLL，通过角色进行组织管理
隔离机制	STONITH	节点隔离、磁盘隔离、云见证等
适用场景	开源环境，高度定制化，异构应用整合	Windows 生态系统，与 AD、Hyper-V 等深度集成

配置高可用集群是一项复杂精细的工作，主要就是定义集群资源、资源约束、节点间健康检测机制。需要配置集群节点之间的心跳网络，这是集群判断成员是否存活的基础，一般建议使用独立的物理网络。必须要有隔离机制，这是保证集群决策一致性的关键。集群在不能判断节点状态的时候（比如心跳中断），就会采取隔离措施，强制重启或者关闭节点，防止出现脑裂现象，从而避免数据不一致所造成的灾难性后果。

资源配置就是集群功能的体现。需要把构成业务系统的各个组件，比如应用服务、虚拟 IP 地址、共享存储等等，视为集群资源，然后组织成资源组，从而保证它们的启动、停止、迁移是原子操作。配置资源的启动顺序、位置约束、协同约束等可以准确的控制业务在集群上的运行行为。比如指定数据库服务只能在共享存储挂载之后才能启动，或者指定 Web 服务应该优先在性能更好的节点上运行。配置完毕之后，还要开展严密而完整的故障切换测试，经由模仿单节点宕机，心跳网络中断，共享存储故障这些故障情况，来考察集群的切换行为是不是符合预期，切换时间是否达到业务恢复时间目标的要求。

二、数据库软件安装与配置

数据库是电力信息系统的数据中枢，所有的电网运行、企业管理等业务数据都在这里。其安装配置的质量好坏直接影响数据存储的可靠性、访问效率和未来扩展能力，任何疏忽都会造成性能瓶颈或者数据安全隐患。

（一）数据库软件安装

数据库软件安装要经过周密细致的安排。安装之前，需要做充分的准备工作，根据数据库厂商官方文档仔细核对操作系统版本、补丁级别、所有必需的依赖软件包是否完全符合要求。任何一个缺少依赖包都会导致安装失败或者后续运行异常。同时要预先创建一个用于运行数据库软件的操作系统用户和用户组，并给予恰当的目录权限，这是十分重要的一个安全措施，可以防止由于使用高权限账户来运行数据库服务所引发的各种问题。

数据库软件安装一般有图形化界面和静默安装两种模式。单次安装或者非标准环境，图形界面提供直观的向导进行操作。但是大型、标准化的电力系统强烈建议使用静默安装。事先制作好应答文件，把所有安装选项，包括安装路径、软件组件、字符集等等参数固定下来，就能达到无人值守的自动安装效果。这种方式虽然极大的提高了部署效率，但更重要的是所有的数据库服务器环境完全一样，为之后的统一运维打下了基础。安装完成后要仔细检查数据库二进制文件的完整性，确认环境变量设置正确，妥善保存详细的安装日志以便追溯。

（二）数据库实例创建与配置

数据库软件安装完成，仅仅说明系统具有运行数据库的能力，只有创建成功数据库实例后，才可以真正开始存储和管理数据。数据库实例是数据库在内存中的映像，由一组内存结构和后台进程组成，它和物理存储的数据库文件一起构成完整的数据库系统。创建实例是十分重要的一步，配置的好坏直接影响到数据库的性能与稳定性。

创建实例的时候，必须慎重确定一些重要的参数。数据库字符集选择尤其重要，设定后后续修改非常困难，风险很高。对支持多种语言和特殊符号的电力信息系统，一般推荐使用 UTF8 或者 AL32UTF8 等通用字符集来彻底解决乱码问题。第二是数据库文件的存储布局（数据文件、控制文件、重做日志文件）。最佳实践就是将不同类型的文件存放到不同的物理磁盘或者存储卷中，将重做日志文件

和数据文件分开放置，将经常被访问的表、索引分开放置以分散 I/O 负载，避免磁盘竞争。还需要合理规划表空间，给不同的业务模块数据创建独立的表空间，方便空间管理、权限控制、备份恢复。实例创建完成后还需要配置网络监听服务来接收应用服务器连接请求，并且创建相应的数据库用户、角色、权限体系以完成数据库的初始化工作。

（三）数据库参数调优

数据库参数调优是依据工作负载分析而进行的不断优化过程，其目的就是充分利用服务器硬件资源，达到最好的应用性能。数据库软件自带的默认参数配置是按照通用场景来设计的，不能满足电力系统高并发、大数据量等特定的性能需求。调优工作要以对系统业务特性充分认识为前提，清楚区分系统负载属于联机事务处理类型，还是联机分析处理类型，或者是两者兼有类型的混合负载。

内存参数是调优的关键，应该合理地把总的内存分给系统全局区、程序全局区等主要的部分。数据缓冲区的大小直接决定数据块内存命中率，在物理内存允许的范围内尽可能设得大一些，减少物理 I/O。共享池缓存 SQL 执行计划和数据字典，大小影响 SQL 解析速度，对 SQL 解析频繁的 OLTP 系统很关键。OLAP 系统为排序、哈希等操作留有更多的内存。

内存之外其它方面的优化也非常重要。I/O 调优，合理布局数据文件，开启异步 I/O，调整数据库写进程数等都可以减少 I/O 等待。CPU 调优方面，设置合理并行度来充分利用多核 CPU 的处理能力加快复杂查询的执行。更深一层便是 SQL 调优，这就得数据库管理员同开发人员密切配合，经由剖析 SQL 语句的执行计划来找出性能短板，之后再借助创建或者修改索引，改变 SQL 逻辑，采用优化提示等手段加以改进。必须常规使用数据库性能监控工具，Oracle 的 AWR 报告、MySQL 的 Performance Schema 都是发现性能问题、评价调优效果的有效工具。

三、应用软件部署与配置

应用软件是直接为用户提供业务功能的载体，也是电力信息系统价值的最终体现。标准化部署、精细化配置是保证电网规划、生产运行、营销服务等核心业务流程顺畅、高效、安全的基础，直接关系到最后的用户体验和业务目标。

（一）应用服务器安装与配置

应用服务器是应用程序代码的运行容器，给应用提供运行环境、事务管理、安全控制、连接池等一系基础服务。常用应用服务器有 Tomcat、WebLogic、JBoss 等。安装过程一般比较简单，大多为解压二进制包或者执行安装程序，但真正的考验是在生产环境高性能、高可用性要求下进行后续的精细化配置。

安装前一定要检查前置条件是否已经满足，尤其是 Java 运行环境的版本要和应用服务器及应用程序的要求完全一致。为了安全起见，为每个应用服务器实例创建独立的、权限较低的操作系统用户来运行，不能使用 root 等高权限账户。配置阶段的主要工作是调整 Java 虚拟机参数。其中，堆内存大小的设定要与应用程序的内存消耗模式、服务器物理内存相结合，不能让内存溢出或者使用过多交换空间。数据库连接池以及线程池的参数设置，包括最大连接数、最小连接数等，对于保证应用在高负载情况下仍能做出稳定的反应来说是十分关键的。在多机部署的情况下还要配置应用服务器集群、负载均衡、会话复制等实现水平扩展和高可用性。

（二）应用程序部署与参数配置

应用程序部署，就是把开发完成的应用代码包（一般以 WAR 或者 EAR 格式存在）放到应用服务器上，从而可以被执行并被访问的过程。现代电力信息系统建设中，基本上使用持续集成和持续部署流水线取代了传统的手工部署。自动化部署使部署过程变得标准化、可重复、可追溯，极大程度上减小了由于人为失误所造成的生产事故。

应用程序配置是部署过程不能缺少的一环。为了适配开发、测试、生产等不同的环境，应用软件需要做到代码和配置的分离。所有与环境有关的参数，数据库连接地址、用户名密码、外部服务 URL、消息队列地址、文件存储路径等，都应通过外部配置文件、环境变量或者配置中心来进行统一管理。配置外部化的方式使得应用程序包本身不变，不同环境中只需替换对应的配置即可。对数据库连接池这类重要的资源要仔细设置最大连接数、最小空闲数、连接超时时间、空闲连接回收策略等参数，在资源使用率和系统响应速度之间找到一个平衡点。日志配置同样十分重要，根据生产环境的要求设置恰当的日志级别（INFO 或 WARN），配置好日志文件的滚动策略以及存放位置，利于日常的监控和问题的排查。

（三）应用间接口联调

现代电力信息系统属于一个复杂的分布式系统，在调度自动化系统、地理信息系统、营销计费系统等等各子系统之间要紧密地进行数据交换以及业务协作。应用间接口联调的目的，就是保证这些系统之间的后台交互能够正确、快速、可靠地完成。该阶段是集成测试的重点，是检验系统全部业务流程是否能够顺畅运转的重要环节。

接口联调一般在各个子系统完成单元测试并且独立部署以后进行。联调团队应按照详细的接口设计文档编写全面的联调测试用例。用例不仅要包含正常的业务场景，还要重点测试各种异常情况以及边界条件，比如接口超时、网络中断、数据格式错误、对方服务不可用等。测试人员模拟调用方发出接口请求，检测接收方是否能正确处理请求，返回期望的响应，验证数据在系统间是否可以正确同步。该过程一般需要多个技术人员的配合，通过查看应用日志、分析数据库记录、网络抓包等手段来定位并解决问题。联调成功意味着原先分散的子系统已经变成了一个有机整体，可以顺利支撑复杂的跨系统业务流程，为系统的最终上线交付打下基础。

第四节 系统切换方案

系统切换是电力信息系统建设最后的阶段，它把项目建设和后期的运维阶段联系起来。核心任务就是将新开发出的系统正式投入到生产环境，替换原有的系统来处理实际业务。切换方案周密性以及执行力的好坏，直接决定项目能否顺利实施，并且尽可能降低对电力企业核心业务的影响，具有重要意义。

一、切换策略选择

选择合适的切换策略是整个方案的基础。不同方法在风险、成本以及实施难易程度等各方面也不尽相同。电力企业要按照新系统的重要程度、业务影响的范畴、技术架构的繁杂程度、可以接受的停机时长、项目资源等要素展开全面评定，从中选出最契合自身情况的策略。

（一）直接切换

直接切换又叫一步到位式切换，即在预定时间点，彻底关闭旧系统，立刻开

启新系统。此种方式干净利落，所有的用户和外部接口在同时从旧环境转移到新环境。优点在于逻辑清晰，不需要处理新旧系统并行期间复杂的同步和协调问题，在切换之后系统环境单一，只保留新系统，大大降低了以后的管理成本。

但是这种策略的风险很高，无异于“破釜沉舟”，一旦失败就无法收场。新系统在切换后如果暴露出未曾预见的严重缺陷，就会造成业务中断，对电力系统的稳定运行以及服务质量造成巨大的冲击。因此采用直接切换的方案需要建立在全面的、严格的测试基础之上，从单元测试、集成测试、性能测试、用户验收测试等各个方面进行考虑，保证新系统在各种环境下都能够稳定可靠地工作。在电力行业里，这办法常被用在非核心的内部管理信息系统，或者挑在业务影响最小的时段（节假日深夜）执行。

（二）并行切换

并行切换就是新系统和旧系统在同一时间段里同时运行。所有的业务数据、操作指令会同时输入到两个系统里，业务人员可以同步使用新旧系统来处理业务，也可以用旧系统为主、新系统为辅的方式来试运行。其最大的优点就是安全，旧系统可以作为一个非常可靠的备份，给新系统的顺利运行提供了一个缓冲期和参照物。

在此期间可以持续比较、验证两个系统的处理结果，及时发现新系统存在的潜在问题。用户在真实的业务操作中逐步适应新系统。并行切换可以降低切换风险，在新系统出现故障的时候，可以迅速把业务切回到旧系统上，保证业务的连续性。但是并行运行的代价也很高。不仅要花费双倍的硬件资源来运行两个系统，还需要投入大量人力来进行数据核对、差异分析和系统维护。尤其对电力调度或者交易这类对实时性有着极高要求的系统来说，实现完全同步的并行输入以及结果比对，在技术上存在极大的困难。

（三）分段切换

分段切换是一种渐进的上线方式，也叫逐步切换或者模块化切换。它不是一次性将新系统的所有功能模块、业务条线或者用户范围全部上线，而是按照功能模块、业务条线或者用户范围，分批次、分阶段部署新系统。这一策略把庞大的、复杂的切换过程拆分为许多小的、可控的切换行动，把总风险分散到各个小的行动中去。下表对这三种主要的策略特点进行归纳对比。

系统切换策略对比表

切换策略	主要优点	主要缺点	风险等级	适用场景
直接切换	逻辑简单，管理成本低，环境纯粹	风险高，无退路，对前期测试要求极高	高	非核心、业务影响小的系统；有充分测试和回退计划的项目
并行切换	安全性高，有可靠备份，用户适应期长	资源和人力成本高昂，数据同步复杂	低	核心业务系统，对连续性要求极高的场景
分段切换	风险可控，分步实施，用户冲击小，可积累经验	切换周期长，需要管理新旧系统共存的复杂性	中	大型、复杂的系统，如大型电力集团的 ERP、营销系统等

各个阶段转换算是一种小规模的直接或并行切换，执行团队能从小得失利弊当中汲取教训，并对下一阶段方案加以改良。这种方式对用户的冲击小，相关的培训和支撑工作也可以分步骤进行，更有针对性。分段切换适用范围广泛，对大型电力集团来说更是如此。

1. 可按照业务模块分批上线，例如新的营销信息系统可以先上线客户服务模块，待其稳定运行之后再依次上线计量采集、电费核算等模块。

2. 可以按照地理区域或者组织单位逐步推广，新的生产管理系统可以先在某个试点供电局或者发电厂成功应用，获取经验后再推广到全网。

二、数据迁移方案

数据是电力信息系统的生命线，也是企业的金矿。系统切换的本质就是业务处理能力的转移，系统切换成功的关键保证是业务数据的平稳过渡。一个完整的数据迁移方案必须保证历史数据和增量数据准确、完整、一致地从旧系统迁移到新系统，为新系统的顺利启用打下良好的基础。

（一）数据迁移策略（全量、增量）

数据迁移一般用全量迁移和增量迁移相结合的方式。全量迁移就是将源系统所有的需要迁移的数据一次性、完整地迁移到目标系统。一般作为数据迁移工作的开端，在项目开始之初或者某个业务暂停的长窗口期内进行。对拥有数千万用户的省级电力公司来说，客户档案、历史电量电费、设备台账等数据量可达 TB 级，全量迁移耗时漫长，必须做充分的性能测试和时间预估。

增量迁移就是只迁移上次迁移以来新增或者改变的数据。系统切换之前过渡

阶段时旧系统仍在处理日常业务，数据不断地产生、变化。为了使新系统上线的时候有最新的数据，必须采用增量迁移。常规做法就是先在正式切换前一段时间内完成全量数据的迁移，形成一个数据基线。在切换前数周或者数天里定时运行增量迁移脚本，把变更数据同步到新系统。在正式切换前最后一个停机窗口期内执行最后一次增量迁移，保证切换时刻的数据一致性。该策略既考虑了效率又考虑了业务的连续性，是大型电力信息系统切换的较好选择。

（二）数据迁移工具与脚本

数据迁移要用高效的、可靠的工具以及脚本去完成。项目团队要按照数据源的异构性，数据清洗转换逻辑的繁杂程度，数据量的多少，项目预算的高低这些因素，挑选出恰当的实现方式。商业化的抽取、转换、加载工具功能强大，图形化开发界面、完善的调度、监控功能可以解决复杂的整合问题，但是价格昂贵。

对一些技术架构陈旧、数据结构特殊的电力业务系统而言，用专门的迁移脚本转移更为灵活和廉价。这些脚本一般使用 SQL、Python、Java 等语言编写，可以精确地从源数据库或者文件中提取数据，根据新旧系统数据模型的不同做字段映射、格式转换、数据清洗和业务逻辑重构，最后把处理后的数据加载到新系统数据库中。开发迁移脚本时，一定要保证代码健壮、可重复执行，附带详细的日志和异常处理，这样出错时就能快速找到问题所在，有些情况下还能实现断点续传。

（三）数据一致性与完整性校验

数据迁移的最终目的，就是保证新系统中的数据在业务上和旧系统保持一致、完整。校验工作必须贯穿迁移的全过程，是保证数据质量的生命线。迁移之前，要对源系统数据展开全面的探查和分析，弄清楚数据质量的现状，找出可能存在的“脏数据”，诸如空值，非法字符，逻辑矛盾之类的问题，然后预先设定清洗规则。

迁移完成后，必须立即开展严格的校验工作。校验方法由浅入深、循序渐进。基础方面有记录数核对，关键字段如金额、电量的总量核对，保证不漏项。其次为按照业务规则进行校验，客户与关联计量点的关系是否正确，电价方案是否符合客户的类别等。对于最核心的关键数据甚至要逐字段、逐记录的进行比对。校验过程同样需要工具和脚本的支持，自动化比对程序可以大大提高校验效率和覆盖面，生成详细的差异报告，给数据修复工作提供指引。校验是迁移工作最后一

步，只有通过严格校验的数据才值得信赖。

三、切换演练与回退

周密的计划、充分的准备是成功切换的必要条件，但不是充分条件。系统切换属于高风险、高压力的复杂过程，任何一点小的失误都会造成严重的结果。因此，在正式切换之前进行反复的演练，做好详细的回退方案，是建立切换安全屏障、保证万无一失的重要措施。

（一）制定详细的切换演练计划

切换演练计划是一份详细的剧本，用以使所有的参与者熟悉整个过程，并各负其责。这份计划要细化到分钟，把从切换窗口开启到新系统宣布稳定的一整个过程中的每一步骤，每一项任务的负责人，预计耗时，前置条件以及完成标准全部列清楚。详细的操作手册就成为整个切换行动的总指挥图。

计划内容不仅要涵盖技术操作，还应覆盖组织协调与沟通机制：

1. 创建切换指挥中心，决定决策链及信息发布途径。指挥中心是切换过程中唯一一个作出决策和发出指令的中心。

2. 明确技术团队、业务用户、管理层、供应商等各方的职责。每个人都应该清楚在切换过程中自己要做什么、什么时候做、向谁汇报。

这种清晰的组织架构和沟通路径，是确保在高压环境下依然能够协同作战、有序推进的基础。

（二）模拟切换过程，验证方案可行性

切换演练的核心就是模拟，在接近生产环境的预发布环境中，严格按照切换计划执行所有的流程。演练就是用“实战”的方式检验切换方案是否可行，时间估算是否准确，各项技术操作是否正确，以及团队协作能力。演练时会出现计划中考虑不周、脚本里出现的错误以及操作人员所犯的错。

电力信息系统的演练一般包含最终增量数据的迁移、数据库切换、应用部署、接口联调、系统配置检查等步骤。演练之后，业务验证组立即介入，针对新系统核心功能的快速检测来决定该系统是否已经可用。演练的目的就是在低风险的环境中提前暴露并解决技术、流程、协作等各方面的问题，为正式切换扫清障碍。项目一般会开展两轮及以上演练，每轮演练结束后都要进行复盘总结，将发现的问题一个一个解决，对切换计划进行迭代优化，直到整个过程顺畅无误。

（三）制定回退方案与触发条件

回退方案是项目最后的安全网，它定义了在切换过程中遇到重大问题的时候，怎样有条不紊地恢复到旧系统的状态。这不能简单地用撤销来解释，它也有一套需要精心设计的标准流程。在回退方案里一定要涵盖旧系统数据库的恢复、应用版本的回退、网络和接口指向重新配置这些具体操作，还要为每一个任务指定完成人以及操作说明。

比方案本身更重要的就是明确定义回退的条件。这些条件必须是客观的、可量化的、没有争议的，并且在切换前得到所有关键干系人的认可。定义为：关键数据迁移校验失败率超过 1% 时触发回退；或者核心业务（电费发行、调度指令下达）的新系统上线在 2 小时之内不能正常执行则触发回退。指挥中心对实时监控结果同预设触发标准执行对比之后，便能当即作出决策。明确的触发条件可以防止在混乱和压力之下做出错误的决定，给企业的核心业务安全留下最后的保障。

第七章 电力信息系统运维管理

电力信息系统是电力企业核心业务运转的神经中枢，它的运行稳定、安全、高效对电力企业的整体运营十分重要。运维管理是保证系统长时间安全稳定运行的重要环节，依靠一系列的技术、流程、组织手段来保证服务品质，以适应不断发展的业务。本章会对电力信息系统运维管理的全部体系进行系统的介绍。

第一节 运维管理体系

科学完善的运维管理体系是实现高效运维的前提。它对运维工作开展的组织架构、人员分工、规章制度、主要流程做出明确阐述，给日常运维工作赋予了清楚的指向和统一的标准。这是保证各项运维工作有序、可控、高效进行的基础，能够大幅度提高电力信息系统的服务质量和可靠性。

一、运维组织架构与职责

设计合理的运维组织结构、明晰各个岗位职责，是构建运维管理体系的首要任务。运维团队的合作效率直接决定着系统故障的响应速度和处理能力。优良的组织架构可以保证指令畅通、责任到人，凝聚成强大的运维合力，给电力信息系统平稳运行提供强有力的组织保障。

（一）运维团队组织模式

电力企业创建运维团队的时候，一般会依照企业的规模，业务的繁杂程度以及信息化水平来挑选最合适的组织形式，常见的有集中式，分散式和混合式这三种。

集中式模式即把所有的运维人员集中在同一个部门进行统一管理。该模式可以集中调配资源、共享知识经验，可以迅速形成专业优势，保证技术标准和运维规范得到统一实施。它特别适合信息化建设初期或者信息系统比较集中企业的应用，可以快速建立起标准化的运维能力。

分散式模式就是将运维人员派驻到各个业务部门或者地区分公司。此种模式更贴近业务一线，可以给予更为迅速灵活的现场支撑。但是其弊端也很明显，容易造成技术力量分散、标准不一、各自为战，不利于整体运维水平的提高和复杂问题的跨部门协调。

混合式模式，对于大型的电力集团来说，采用混合模式会更加合适。该模式一般会设立一个总部的核心运维中心，负责核心基础设施、关键共性系统运维以及技术标准制定，各个业务单元或者区域保留一部分现场运维人员，主要负责特定应用系统或者日常支持。该种模式既专业化又标准化，同时具有现场响应速度快的特点，达到资源的最佳配置。

（二）运维岗位职责与分工

有明确岗位职责、细碎的分工才能让运维团队高效的运转。电力信息系统运维工作要涵盖系统生命周期的各个方面，日常监控，应急处置，技术支持，管理决策。因此运维团队一般会按照不同的技术层次、专业领域组成一个金字塔形的支撑结构。

运维岗位根据技术纵深和职责范围，大体上可以划分为一线、二线、三线支持。下表清楚地列出各个线运维岗位主要工作及分工。

电力信息系统运维岗位分工表

运维层级	主要角色	核心职责
一线运维	监控中心、服务台人员	7x24 小时不间断监控，接收用户报障与告警；执行标准化初步排查，记录并分派工单。
二线运维	专业领域工程师（网络、系统、数据库等）	处理一线升级的复杂技术事件，进行故障诊断与修复；负责系统日常维护、性能优化与变更实施。
三线运维	核心技术专家、架构师、研发或厂商专家	解决深层次、根源性技术难题；负责核心代码修正、系统架构优化及重大疑难问题攻关。

除技术岗位外，还需要设置运维管理岗位，制定和监督运维流程、度量服务质量、考核团队绩效、推动持续改进计划的实施，保证整个运维体系向着设定的目标健康向前发展。

（三）运维流程与规范

运维流程和规范是组织、人员和技术三者之间的一种纽带，也是实现运维工作标准化、程序化的基础。个人零散的经验、能力汇聚成组织集体能力，减少对

某个人的依赖性，使运维服务质量稳定、可预见。电力行业运维流程及规范的建立十分重要，因为任何小的操作失误都可能造成连锁反应，给电力调度、市场交易或者营销等核心业务带来严重影响。

关键的流程及规范有监控告警处理规范，对各类告警响应时间、处理流程、分级程序做出规定；巡检规范，对每日、每周、每月检查项目和标准进行规定以达到提前识别风险的目的；应急预案，对各种类型的故障事件制定详尽的处理方案、指挥机制与恢复方法保证出现时可冷静应对。所有的流程和规范都必须文档化管理，定期组织培训和演练，使所有成员都能熟练掌握。并且文档要随着技术、业务的变化不断修改更新，保证其时效性、有效性。

二、运维管理制度

制度是运维体系正常运转的刚性约束，把管理要求以规章制度的形式固定下来，给运维人员的行为提供明确的准则和依据。完备的运维管理制度有利于加强责任意识、规范操作行为、防范操作风险，是提高运维纪律性、保证电力信息系统安全可靠运行的重要保障。

（一）值班与交接班制度

电力核心信息系统的服务具有连续性、不间断的特点，所以必须实行 7x24 小时值班制度，保证任何时段都有专业人员在岗，可以及时发现并处理系统异常。值班制度对值班人员的责任、权限、工作纪律做出规定。在岗人员必须一直关注各类平台，注意告警信息，根据预案对告警进行初步分析和处理，并做好值班记录。对于不能独立解决的问题，必须依照上报程序，及时上报给二线技术人员或者相关负责人。

交接班属于值班制度中的重要部分，是信息传递与责任转移的节点。为防止由于信息遗漏或者误解而产生的问题，必须建立交接班规范流程。交接班过程必须采用面对面的方式，并填写标准化的交接班日志。交班方要详细说明当班期间系统运行情况、已处理和待处理事件、正在进行的变更操作、需要重点关注的系统隐患及其他需要下一班注意的事项。接班方在确认所有的信息都清楚、系统状态正常之后，才可以在日志上签字确认。这样一种仪式化的交接程序，保证了运维工作连续、责任明确，是保证系统平稳过渡的一种有效手段。

（二）变更管理制度

据统计数据表明，几乎所有的由于信息系统本身所引发的生产事故，都是因为没有经过足够评估与测试的变更操作引起的。建立一套严格的、规范的变更管理制度，是控制运维风险、保证系统稳定性的主要方法。变更管理就是对生产环境中所有可能影响它的活动加以控制，例如硬件更换、软件升级、配置修改、数据迁移等。其主要目的在满足业务发展需要的同时，把变更所带来风险降到最低。

完整的变更管理流程一般包括变更申请、技术评审、风险审批、实施计划和变后评审等步骤。所有的变更需求都必须通过正式的变更请求来启动，详细的说明变更的原因、潜在的风险、影响范围、实施方案和回退计划。变更请求会被提交至变更顾问委员会来执行评定与批准任务，此委员会一般由技术专家，业务代表以及管理者构成。高风险重大变更要进行更高级别的审批。只有得到批准的变更，才能在规定好的“变更窗口期”进行变更。变更完成之后，还要对变更产生的效果加以验证，做回顾评审，总结经验教训。紧急变更可以简化流程，以便快速响应，但是事后必须补全所有的记录和审批手续，保证每一次变更都有据可查。

（三）事件与问题管理制度

事件管理和问题管理是运维工作中的两个重要且密切相关的活动，但是两者在目标和方法上存在着本质的区别，必须通过制度来进行明确的区分。事件管理的目标就是尽快恢复服务，即服务中断之后，怎样最快地使业务系统回到正常工作状态，将业务的影响降到最小。事件管理流程重视的是响应速度、效率，它的过程有事件发现记录、分类定级、初步诊断、上报升级、最终解决、关闭。

问题管理则要找出事件产生的根本原因，其最终目的就是防止事件的再次发生。当某个事件反复发生或者单个事件造成重大业务影响的时候，就要启动问题管理流程。问题管理常用“五个为什么分析法”、鱼骨图等方法对问题进行根本原因分析，目的是找出隐藏在现象之下深层次的技术或管理漏洞。找到根源之后，问题管理流程就会给出彻底的解决办法，可能是程序补丁，也可能是一次配置更改，或者是一项架构改良。该方案将会被当作一个变更请求，经过变更管理程序的实施从而形成被动响应到主动预防的改进闭环。健全事件和问题管理制度，可以促使运维队伍从“救火队”变为“预防队”，进而提高系统本身的健壮性。

三、运维流程管理

借鉴成熟的运维管理理论来指导实践，是提高电力信息系统运维水平的有效途径。信息技术基础设施库是 IT 服务管理领域全球公认的最好实践框架，其核心思想与流程给电力行业运维工作给予了非常宝贵的参照和引导，促使企业搭建起一个以服务为中心、以流程为核心的高效运维体系。

（一）服务台与事件管理

服务台是 ITIL 实践中唯一直接面对用户的职能部门，在运维团队和用户之间起一个单一的联系点的作用。在电力信息系统运维当中，一个专业的、高效的的服务台是必不可少的，它是接受用户报障、咨询、服务的唯一入口，也是展示运维专业形象的一面镜子。服务台会对所有的用户请求进行记录，并利用知识库进行初步的回答与支持，尽可能的在第一时间帮助用户解决问题。对于不能马上处理的请求，服务台会生成一张标准的事件记录单，按照事先确定好的优先级以及影响范围，把这张单子送达到对应的二线技术支持小组。

事件管理流程和服务台紧密相连，它的主要目的就是当服务出现中断或者质量下滑的时候，能够迅速将服务恢复如初，它所看重的是速度和效率，而不是去追究深层次的原因。一个典型的事件管理生命周期由以下几个步骤组成：

1. 事件识别和记录：利用用户报告、服务台接收到的告警等方式来发现事件之后，服务台会在系统中创建唯一的事件记录。

2. 事件分类与初步支持：对事件进行分类和定级，并尝试运用已知的解决方案进行处理。

3. 调查与诊断：若一线支持无法解决，事件将被升级至二线或三线技术团队进行深入分析。

4. 解决与恢复：实施有效的解决方案，恢复系统服务。

5. 事件关闭：在确认服务已恢复且用户满意后，正式关闭事件记录。

通过实行标准化的事件处理流程，电力企业能够保证故障应对与处理的过程一直处在可控、可衡量并且不断改善的状况之中。

（二）问题管理与变更管理

问题管理是事件管理的延伸和深化，其目的就是从根源上消除造成事件的原因，减少以后事件的发生数量和影响。当同一类事件不断发生，或者某一个事件

对业务造成重大影响的时候，就需要开启问题管理流程。该流程中最重要的活动就是根因分析，通过系统的分析方法，找到隐藏在表面现象背后的系统漏洞或者管理漏洞。问题管理的输出是产生一个或者多个已知错误记录，并将它们存入到已知错误数据库里，给事件管理团队提供临时解决方案或者规避措施。

当问题的根本原因被找出并且永久性的解决措施被确定之后，就要通过变更管理流程来执行该方案。变更管理是一个正式的控制过程，它保证所有的 IT 基础设施改变都是经过了评估、批准、执行和检讨的，在业务灵活性与服务稳定间获得一个均衡。问题管理所做的修复方案将变成变更请求，然后进入变更管理流程。变更顾问委员会在经过对风险及影响进行全面分析之后决定是否批准。获得批准的变更会在计划的时间窗口内被部署到生产环境中，从而彻底解决问题。这就形成了事件、问题、变更的闭环管理，促进运维质量螺旋式上升。

（三）配置管理与发布管理

配置管理的目的在于提供全部电力信息系统基础设施的逻辑模型，并对全部配置项的生命周期，版本以及状态予以识别，控制，保持并核实。配置项可以是任何需要被单独管理的资源，可以是一台核心交换机、一套调度自动化系统，也可以是一个应用模块、一份技术文档。所有配置项及其相互间的关系都被保存在配置管理数据库中。准确、完整的配置管理数据库是实现高效运维的前提，也是事件管理、问题管理、变更管理的重要数据来源。当某台服务器出现故障的时候，查询配置管理数据库可以立即知道该服务器上运行的应用，进而快速判断业务受影响的范围。

发布管理负责规划、设计、构建、测试并发布那些已经得到变更管理批准的硬件和软件变更，将它们打包成一个“发布”单元，然后一起发布到生产环境中。它与变更管理密切相关但是各有侧重，变更管理关注的是“是否变更”和“批准变更”，发布管理关注的是“怎样组织并实施变更”。完善的发布管理可以保证所有的新的版本或者新的服务，在发布之前都做了充分的测试和协调，从而将风险控制在可管理的范围内。电力行业的发布一般会牵扯到很多相互关联的系统，采用周密的发布计划、回退方案、验证步骤等使整个过程平稳、有条理地开展，降低对电力业务的影响。配置管理与发布管理的有机结合，可以保证 IT 环境的所有变更都在严格受控的状态下。

第二节 故障诊断处理

电力信息系统的稳定运行是保证电网安全、企业高效运转的基础，任何小的故障都可能引起连锁反应，造成无法估量的损失。因此，建立一套科学、规范的故障诊断处理体系就显得十分重要。本章将会从故障分类定级、诊断的方法和工具、标准化的处理流程这三方面来展开，从而提高运维人员应对故障的速度以及解决故障的效率，保证电力信息系统的高可用性。

一、故障分类与定级

对故障进行系统的分类、定级，是进行差异化、精细化管理的先决条件。确定故障性质、重要程度，可以保证核心业务正常运转，按照既定的响应时间有条不紊地进行应急处理，不会出现处置时的混乱、拖延等情况，将故障造成的影响降到最小。

（一）按影响范围与紧急程度分类

电力信息系统故障的分类，主要是按影响范围、紧急程度这两个标准来进行的。影响范围是指故障波及的业务功能、用户数量或者系统模块的宽窄。以电网调度实时控制系统为例，它所遭遇的故障，造成的波及范围绝不是仅仅针对内部办公协同系统就能比拟的。紧急程度用核心业务被冲击的严重度，数据重要程度和修复的紧迫性来评定。一个威胁到主网稳定的系统异常，它的紧急程度毫无疑问是最高的。

两个维度结合就形成了故障矩阵。影响范围广、紧急程度高的故障称为关键故障；影响范围小、紧急程度低的称为一般故障。这样的分类方式可以使得运维人员能很快的判断出故障的严重性。对于生产控制大区的系统故障，特别是直接关系到电网运行的数据采集与监视控制系统、能量管理系统等，一般都会被归类为影响范围广、紧急程度高的类型，以保证第一时间调集最强的资源来处理。

分类体系还要考虑到潜在的影响。一些当前影响较小，但如果不在意，后患无穷的故障也需要注意。当存储阵列单块硬盘出现报警的时候，冗余机制可以在极短的时间之内保证业务的正常运行，但是如果不能及时更换的话，一旦冗余盘也出现故障了，就会造成严重的后果。因此，在分类时要结合预判，适当提高存在潜在升级风险的故障等级，达到预防性管理的目的。

（二）故障定级标准与处理时限

根据故障类型来建立具体的定级标准以及相应处理时限，是达到管理要求具体化、量化的关键。该套标准属于运维服务水平协议中重要的一部分，给故障处理的及时性给出了一个客观的衡量标准。电力信息系统故障被分为 4 个等级，并且每个等级都有自己的响应时限和处理时限要求。下表为电力信息系统故障定级标准及处理时限要求表。

电力信息系统故障定级与处理时限标准表

故障等级	级别定义	影响描述	处理时限要求
一级故障	紧急 / 灾难级	导致电力生产、调度、交易等核心业务中断，或引发大范围电网安全风险。	5 分钟内启动应急预案，1-2 小时内恢复核心功能。
二级故障	严重 / 重大级	造成核心业务性能显著下降或重要功能不可用，但未导致业务完全中断，如交易申报系统响应迟缓。	30 分钟内响应，2-4 小时内解决。
三级故障	普通 / 一般级	影响非核心业务功能或核心业务的非关键功能，导致用户体验下降，如信息发布网站部分栏目无法打开。	工作日内响应，8-24 小时内排除。
四级故障	轻微 / 提示级	对业务无实质性影响，如界面显示错误、日志中的非关键警告等，优先级最低。	归入后续版本迭代或维护计划，处理时限灵活。

实行这套标准之后，运维资源就可以集中到最高级的故障上，从而达到有效的应急指挥和调度。定期对各级故障处理达标率进行分析，也成了持续改进运维管理体系、提高服务质量的一种手段。

（三）故障上报与通报机制

规范化故障上报、通报机制，可保证故障处理信息在流程中及时、准确地传递。该机制目的在于明确向谁汇报、汇报什么、何时汇报、如何汇报，从而建立起闭环的信息流动体系。电力行业对时效性的要求非常高，信息传递的任何延误或者失真都会造成最佳处理时机的丧失，甚至会扩大故障的影响。

故障上报流程要遵照“逐级上报、并行通知”的准则。一线运维人员或者系统监控平台在发现故障的时候，首先要根据定级标准来确定故障的严重程度，然后立即把情况上报给运维主管或者二线技术专家。对达到一、二级严重故障的必须打开快速通道，立即上报应急指挥小组负责人、相关业务部门主管、企业高层

领导。上报内容要简明扼要，包括故障现象，初步的影响范围，发生的时间以及已经采取的应急措施，以便于决策者作出判断。

通报机制主要在于横向的信息同步，即让受影响的用户、协同处理技术的公司客服等有关方面，马上知道故障情况、大概什么时候能好、临时怎么绕开等等信息。通报可以利用系统公告、电子邮件、即时消息群组等不同的方式，以保证信息能够被所有的相关人员所接收。

二、故障诊断方法与工具

故障诊断是整个处理流程中技术含量最大、难度最高的环节。准确有效地定位出问题根源，是进行有效修复的前提。面对电力信息系统日益复杂的特性，运维人员要熟练地掌握各种诊断方法，并善于利用各种先进的诊断工具来建立从现象到根源的逻辑推理路径，在大量的信息中准确找到“病灶”。

（一）日志分析与排查

日志是系统行为最忠实的记录者，也是故障诊断最基础、最重要的数据来源。操作系统、中间件、数据库、应用程序运行过程中会产生很多日志，包含各种事件、状态变化以及错误。日志分析的主要任务就是对大量的日志记录进行审查、过滤、关联、模式匹配，从中找出与故障现象有关的线索。

有效的日志排查要遵照科学的方法论。首先确定排查范围，根据故障现象大致判断可能涉及的系统模块，确定需要查看的日志文件。其次是以故障发生的时间为基准，向后查看系统的异常表现，向前追溯系统运行状态。系统崩溃之前，应用日志里是否出现大量错误堆栈信息，数据库日志中是否存在慢查询以及锁等待超时的记录。

现代电力信息系统的架构很复杂，各个服务之间联系紧密，单一系统日志不能反映全局问题。因此建立集中式日志管理平台就显得十分必要。经过把各个服务器和应用的日志集中起来存储到同一个平台，并加以索引和分析之后，运维人员就能做到跨系统地检索与关联分析日志。当用户反馈交易请求失败的时候，可以利用唯一的请求 ID 来串联起从 Web 前端、应用服务器到数据库的完整调用链日志，迅速定位到出问题的地方。

日志分析不但可以对故障作出被动反应，也可以对潜在风险做出主动的发现。通过对关键字告警规则 (Error、Exception、Timeout) 或者使用机器学习算法对日

志模式的异常偏离来实现问题的早发现，从而实现从“救火”到“防火”。

（二）网络诊断工具

网络是电力信息系统中各个部分之间互相连接的“血脉”，网络层面的故障一般具有隐蔽性高、影响范围广的特点。因此，故障诊断一开始就要尽快确定网络是否连通、路径状况如何。ping 和 traceroute 是最基本、最常用的网络诊断工具，也是每个运维工程师必须掌握的基础技能。

ping 命令会发出 ICMP 回显请求报文，并且等待回显应答，以此来判定源主机和目的主机之间是否能够互通。其作用有三点，一是判断可达性，如果能收到应答说明物理链路和 IP 路由都通；二是测延迟，通过往返时间可以大致衡量网络传输时延，延迟的剧烈波动一般意味着网络拥塞或者设备性能瓶颈；三是看丢包率，连续执行 ping 命令，如果有部分请求超时就说明网络中有数据包丢失，这会对应用服务的可靠性造成严重影响。诊断时先在客户端 ping 服务端，再在服务端 ping 数据库，通过分段测试可以迅速判断出问题链路。

traceroute 命令可以对网络路径做更深层次的探测。它可以逐跳列出从源主机到目标主机所经过的所有路由器节点，并且可以显示每一个跳的延迟情况。网络访问缓慢或者不通的时候，使用 traceroute 可以清楚的看到数据包在哪个中间节点被丢弃或者产生巨大延迟。如果某一跳之后所有的节点都显示星号，则说明该节点或者其下一跳链路可能出现了故障。复杂电力广域网当中，traceroute 可以快速确定问题出现在本地网络，运营商线路还是目标机房网络，进而缩小排查范围。

（三）性能监控与分析工具

就故障的预防和诊断来说，不断进行的性能监控就像是系统的“哨兵”和“听诊器”。单纯依靠事后的日志分析与网络测试属于被动式的方法，但实时的性能监测可以给予系统健康状况的连续画面，让运维人员可以在性能下滑或者故障出现之前察觉到异常的信号。通过对系统关键性能指标采集、聚合、展示、告警，给系统稳定运行提供保障。

性能监控的对象包括信息系统的各个层面。在基础设施上主要对服务器的 CPU 使用率、内存占用、磁盘 I/O、网络吞吐量进行监测。CPU 使用率长期处于高位，可能是计算资源不够用，也可能是有死循环的进程；内存泄漏会使得可用内存不断减少，最终导致系统崩溃。在应用层面监控的更多，服务响应时间、吞

吐量、错误率、数据库连接池、JVM 堆内存、垃圾回收等。这些都是可以直接反应应用的健康度和体验的。

不管是 Zabbix 之类的开源工具同 Grafana，Prometheus 搭配使用，还是商业化应用性能管理工具，都有非常强大的数据可视化以及智能分析功能。可以将海量的性能数据用仪表盘、趋势图等直观地呈现出来，使运维人员可以一眼就看出系统的总体运行态势。最重要的是它们有强大的告警引擎，可以按历史基线或者固定阈值来设置告警规则。一旦某一个指标超过正常范围，系统就会立即用短信、邮件或者即时通讯工具向运维人员发出警报，实现秒级发现问题。通过对比告警前后性能曲线，一般可以直接找到造成性能瓶颈或者功能异常的根本原因。

三、故障处理流程

制定一份标准化的故障处理流程，是保证在混乱高压的环境下所有操作有条不紊、高效完成的基础。这套流程给运维团队赋予了一套从故障被察觉，到系统功能彻底恢复正常并加以确认的全部操作指南，保证了处理过程具有可以追查、符合标准并且能相互配合的特点。

（一）故障发现与报告

故障处理的起点就是故障的发现，发现途径有 2 种：自动化监控系统告警和用户人工报告。自动化监控更加理想，它依靠事先设置好的性能监控与日志分析工具，可以随时扫描系统异常。当指标脱离基线或者出现某些错误日志的时候，就会触发告警并通知运维人员。反应及时，能在用户感觉到问题之前就介入处理。

用户报告是自动化监控的有益补充，对一些复杂业务逻辑错误或不易被监控发现的“隐性”故障，能起到一定的补充作用。用户通过服务台、电话、即 - 时通讯工具等报告问题时，服务台人员起着至关重要的作用。他们要成为第一响应人，安抚用户情绪，按照事先准备的故障报告模板引导用户提供关键信息。

一份合格的故障报告应该包括：报告人信息、故障发生时间、受影响的系统或者业务、故障现象详细描述、错误提示或者截图、用户相关操作步骤、故障影响范围和紧急程度的初步判断。结构化的信息给故障定位提供了初步的输入，在缺少信息的时候，可以减少技术人员主观臆断，大幅度提高诊断效率。

（二）故障定位与隔离

故障定位是处理流程中技术难度最大的一个环节，它的目的就是尽快、准确

地找到问题的根本原因。这是一个系统的排除与求证过程，很大程度上依靠运维人员扎实的专业知识、清晰的逻辑思维和丰富的实战经验。定位一般遵照分层排查的准则，也就是从网络层、系统层、中间件层再到应用层，逐层向上或者向下检查并验证。

定位的第一步就是找到并复现问题。技术人员接到故障报告后，首先要尝试自己复现故障现象，确定故障是稳定发生的还是有条件触发的。如果问题不能稳定复现，排查难度会大大增加，这时需要和用户进行更深入的沟通，并扩大日志分析的范围。接下来用排除法逐个排除嫌疑。比如 Web 服务不能访问，先查看网络是否连通，排除网络问题；再查看服务器硬件状态、操作系统负载，排除系统资源问题；最后查看 Web 服务器、应用服务器的进程状态及日志，定位软件层面的错误。

复杂的分布式系统当一个故障点发生的时候，很容易会引发连锁反应，使得多个服务都出了问题，这无疑加大了问题定位的难度。这时必须用架构图、调用链监控工具理清服务间依赖关系，从最底层的服务开始排查。应用异常时首先要检查数据库服务是否正常。

当初步判断出疑似故障部件的时候，应立即进行故障隔离。隔离的目的在于阻止故障影响范围的扩大，保护系统中的其它健康模块，并给修复操作创造一个受控的环境。隔离手段有负载均衡器切断流量、防火墙或者路由政策切断与故障节点的联系、应用层面上采取服务熔断或者降级暂时禁用有问题的服务接口等方式。有效的隔离是控制危机、减少损失的第一步。

（三）故障恢复与验证

故障恢复的核心目的就是以最快、最安全的方式将受影响的业务功能恢复正常。恢复策略的选择是被故障的种类、故障的严重程度、系统本身体系结构所决定的。在进行任何恢复操作前，必须要制定出详细的方案，在预发布环境里进行演练，从而评价、规避风险。

常见的故障恢复手段包括：

1. 重启服务或者系统，对由于软件缺陷或者资源暂时性耗尽所引起的故障，重启应用程序进程、中间件服务或者整个操作系统，是一种简单有效的恢复手段。

2. 切换和容灾对于部署了高可用架构的系统来说，当主节点出现故障时，恢复最快的方式就是进行主备切换，把业务流量切换到备用节点或者备用数据中心。

这就需要系统具有自动或者手动切换故障的能力。

3.3、配置变更与回滚：故障如果是由近期的配置更改、代码发布或者补丁升级所造成，最直接的恢复方式就是将变更的操作回滚到上一个已知稳定的版本。

4. 数据恢复，数据损坏或者丢失的时候，马上开始数据备份恢复，从最近可以使用的备份集合里把数据取回来。这是个高风险操作，一定要按预案来。

故障恢复操作完毕之后，工作才刚刚开始。必须进入严格的故障验证阶段，保证问题从根子上得到了解决，恢复操作没有带来新的问题。验证过程要全面细致，核心功能测试得做，保证受影响的业务流程恢复正常，性能监控指标也要检查，CPU，内存，响应时间这些关键指标得保证回到正常范围，还要继续观察一段时间，保证系统稳定，没有类似告警再出现。只有所有的验证步骤都通过之后，本次故障处理流程才可以正式关闭。

第三节 系统优化升级

电力信息系统的建立不是静态的、一次性完成的工程，而是动态的、不断发展的过程。由于业务需求增加，技术架构不断演变，用户数量增大等影响下系统必定会出现性能瓶颈、功能落后、容量不足等问题。因此，系统优化升级是保证电力信息系统长期稳定、高效、安全运行的重要环节，它的目的就是提高系统服务质量、延长系统生命周期，满足电力业务持续创新发展的要求。本节主要研究系统性能优化、版本升级和容量管理这三种技术手段以及具体的操作方法。

一、系统性能优化

系统性能属于电力信息系统服务能力的主要度量标准，它关乎到用户体验以及业务处理速度。性能优化属于一项繁杂的系统工程，它牵涉到硬件，软件，网络等诸多方面，其目的是借助技术手段来最大限度地发挥系统的潜能，消除性能瓶颈，并且用更低的资源消耗支撑起更高的业务量。好的性能优化对于提高系统的响应速度、吞吐量以及稳定性都有着非常大的影响。

（一）硬件资源优化

硬件是信息系统运行的物质基础，硬件配置的好坏以及使用效率的高低直接影响系统的性能。硬件资源优化就是保证计算、存储、网络等硬件资源能够被合

理的分配和利用，为上层应用提供有力的性能支持。这一般要对服务器的中央处理器、内存、磁盘输入输出、网络接口等重要硬件部件做全面的评价并加以调整。

优化起点是对现有硬件资源做全面盘点与持续监控。通过对各种硬件指标的使用率、饱和度和瓶颈点进行分析，可以确定出资源优化的方向。以中央处理器的负载长期处于高负载为例，可以考虑升级核心数更多、主频更高的 CPU，也可以采用负载均衡的方式将计算任务均摊到多个节点上。内存资源可以通过增大物理内存容量的基础上，还可以用大页内存的技术方法降低内存管理耗费。

磁盘的输入输出性能往往会成为数据密集型应用（电能量采集系统、营销收费系统等）的瓶颈。采用固态硬盘替代传统的机械硬盘，随机读写性能可以提高几个数量级。在存储系统上可以利用 RAID 阵列来提高数据的可靠性以及读写性能，例如采用兼具性能和冗余的 RAID10。网络上采用优化网络拓扑、更换交换机、网卡启用巨帧等方式均可改善网络的延迟、提高带宽，保证各个模块之间数据交流。

（二）操作系统与数据库参数优化

操作系统和数据库是承载应用程序的基础软件，其内部运行参数配置的好坏，对整个系统性能有着至关重要的影响。软件默认配置一般以通用性、稳定性为设计目标，未必完全符合电力系统高并发、大数据量的特有业务场景。因此，对参数有针对地调整，是激发系统潜能，提高处理效率的一种方法。

从操作系统层面来说，需要根据应用的特点对内核参数进行细致的调节。对需要处理海量并发连接的调度或者交易系统来说，应该适当地提高系统最大文件描述符的数量以及网络连接队列的长度，避免因为资源不够而使连接请求被抛弃。改变操作系统内存管理策略，譬如改良虚拟内存交换行为参数，可以削减无谓的磁盘交换，保证核心应用长久留在物理内存里，进而得到更快的回应。

数据库参数优化更复杂，直接关系到数据存取效率。数据库连接池大小、查询缓存、数据缓冲区等核心参数，要根据系统的并发用户数和数据访问模式来确定。合理地设计连接池可以复用数据库连接，从而大大减少创建和销毁连接所引起的开销。数据缓冲区也就是 InnoDB 的 Buffer Pool 大小决定着数据、索引在内存中缓存的比例，对于查询性能影响较大。优化 SQL 查询日志记录方式，调整事务日志刷写策略，可以不同程度上提高数据库写入性能以及数据一致性保障能力。索引的合理创建和维护是数据库优化的永恒话题，可以将耗时的全表扫描转

变为高效的索引查找，是提高查询速度最直接的办法。

（三）应用程序代码优化

应用程序是业务逻辑的最终载体，代码质量好坏直接决定系统性能的好坏。即使有再强的硬件和调优过的软件基础，低效的应用程序代码也依然是整个系统的性能短板。从代码层面进行优化最贴近业务，也最考验开发人员的业务理解能力以及编程功底。

算法效率就是代码优化的重中之重。面对海量电力数据，选择恰当的数据结构和算法就变得很重要。一个时间复杂度为 $O(n^2)$ 的算法，在小数据量下还可以应付，但是随着数据量增加会急剧恶化。此时就必须重新构建算法，寻找时间复杂度为 O 甚至 O(n) 的算法，这对于电网潮流计算、负荷预测等计算密集型场景来说尤为重要。

内存管理也不可小视，不恰当的内存使用，例如频繁创建、销毁大对象等行为，会给垃圾回收器造成很大负担，导致系统出现周期性的卡顿现象。内存泄漏就更糟糕了，它会不断蚕食可用内存，最终使服务崩溃。开发人员要借助工具来剖析内存的占用状况，适时地释放掉那些不需要的对象，绝不能出现内存泄漏的现象。

与数据库交互的方式也会影响性能。减少数据库访问次数为基本原则，可以用批量操作将多次单条插入或者更新合并成一次执行。应极力避免在循环中执行数据库查询，循环中执行数据库查询是典型的性能杀手，N+1 查询就是其中的一种。引入缓存机制可以应对高频读取的情况，将电价配置、组织机构等热点数据存入分布式缓存中，可以大大降低数据库的读取压力，实现系统秒级响应。

二、系统版本升级

随着技术的不断发展和技术的更替，电力信息系统也必须不断的进行版本的更新来添加新的功能，修复现有的 bug 以及提升系统的安全性和兼容性。系统版本升级是一项高风险、高技术要求的工作，它不但是软件版本的更替，也是对系统稳定性以及业务连续性的一次严峻考验。严谨严密的升级过程，成为业务平稳过渡，充分释放新技术红利的先决条件。

（一）升级需求分析与方案制定

系统升级不能盲目进行，首先要做的是对升级的必要性和可行性做详细的需

求分析。这包含明晰新版本须要支撑的业务需求，比如适配新的电价政策，接入新的用电采集设备等；评定当下版本已然存在的技术债务，包含待修复的安全漏洞，待改良的性能问题等；解析新版本所具备的技术优势，包含更高效的架构，更多的接口等等。

明确了升级的原因之后，必须制定一份详细的周密的升级方案，作为整个升级工作的行动指南。方案里要规定出升级目标、范围，具体的技术路径可选择原地升级或同时部署新系统进行数据迁移。一个完整的计划还要具体到小时、分清任务、列好软硬件资源清单。其中制定清楚的回滚计划尤其重要，在升级过程中遇到不能预料的重大问题时，回滚预案是保证业务连续性、把损失降到最小的关键生命线。

（二）升级测试与风险评估

升级方案确定之后不能直接使用到生产环境里，要经过严格的、充分的测试。测试的目的是在升级前最大程度上找出新版本中隐藏的各种问题，以及它给现有业务带来的潜在影响。为此需要建立一个和生产环境相似的预发布或者测试环境，使它的硬件配置、操作系统、网络结构甚至测试数据量尽可能接近真实情况。

在此环境中，需开展多维度的测试工作：

1. 功能 + 回归测试，验证新版本的功能是否满足需求，同时保证升级前已经存在的功能在升级之后仍然可以正常工作。

2. 性能、压力测试：模拟生产环境真实负载甚至更高压力，对新版本并发访问、大数据量处理等性能进行测试，保证性能不劣于旧版本。

3. 安全测试：对新版本进行漏洞扫描和渗透测试，排查是否存在新的安全风险。

测试的时候必须对可能存在的风险进行全面的评价。它们可能是升级期间的数据丢失或者损坏，核心业务功能的短时间或者长时间中断，新旧模块之间以及同外部系统之间的接口不兼容等等。每一个风险点都应该对其发生的概率以及影响程度进行评价，并且制定出相应的应对预案。

（三）升级实施与验证

升级实施是整个流程中最重要的，也是风险最大的一个阶段。该阶段所有操作都应严格按照事先拟定的方案进行，力求准确、迅速。选择合适的实施窗口期也很重要，一般选择在业务量最少的凌晨时段，最大程度地减少对用户、业务的

影响。实施前必须完成所有的前置检查，并对生产环境的数据库和应用程序做完整的备份，这是执行回滚操作的最后保障。

升级过程根据业务连续性的要求不同可以采用不同的发布策略，常见的蓝绿部署和金丝雀发布的对比如下表所示。

常见升级发布策略对比表

发布策略	核心思想	停机时间	风险控制	适用场景
蓝绿部署	准备两套完全相同的生产环境（蓝 / 绿），流量在新旧环境间快速切换。	极短，接近于零停机。	风险较低，可快速回滚至旧环境。	对业务连续性要求极高，资源成本相对较高的场景。
金丝雀发布	将一小部分真实流量引入新版本，逐步扩大流量范围直至完全替代旧版。	无停机。	风险可控，问题影响范围小，但回滚相对复杂。	功能迭代频繁，需要在线验证新版本稳定性的场景。

实施期间要由专人实时监控系统日志、性能指标和业务指标，保证一切正常运行。出现异常应立即启动应急预案，判断是继续修复还是回滚。升级结束后立刻验证。技术人员检测系统各个服务是否正常启动，关键性能指标是否在预期范围内，业务人员登录系统，对核心业务流程进行端到端的穿行测试，保证功能可用。只有技术层面上和业务层面上的验证都通过了之后，整个升级工作才算真正完成。

三、系统容量管理

系统容量管理是事先的一系列管理工作，目的是保证电力信息系统能应付当前的及未来的业务负荷。其目的在于通过不断的监视、分析和规划，使系统所提供的 IT 资源与业务需求之间保持动态平衡，既不会因为资源不够而造成服务质量下降或者中断，也不会因为资源过度配置而造成浪费。容量管理对于保证系统的可持续发展起着非常重要的作用。

（一）容量规划与预测

容量规划是一种主动的而不是被动的管理工作，其核心就是对未来业务增长和资源需求进行科学的预测。静态地分配资源是短视的，因为电力业务，比如用电客户数量、数据采集频率、线上办电业务量等，都是不断增长的。良好的容量规划要有对业务发展动向的充分认识。

预测的方法有很多。一种是根据历史数据的趋势分析法，即通过对近几年

CPU、内存、存储等资源使用率增长曲线进行分析，采用线性回归等统计学方法来预测未来的需要量。另一种是业务驱动的预测，即根据建立起来的 IT 资源消耗与关键业务指标（如新增装表用户数、日均交易笔数）之间的关联模型，用业务指标增长的预估来推算资源需求。迎峰度夏时，负荷控制指令的下发量会大幅增加，这就得预先安排好相应的控制通道带宽和处理服务器的计算能力。

精准的容量规划可以为预算的制定、设备的采购、系统架构的调整提供关键的决策依据，使资源的扩容不再是临时的应急响应，而是有计划、有步骤的战略部署，保证系统始终能够从容应对业务洪峰的挑战。

（二）资源使用率监控

没有监控就没有管理。容量管理的基础是对资源使用率进行实时、准确的监控。只有掌握系统的各种资源当前状态之后才能进行分析、预警和规划。完整的资源视图，必须包含所有的关键的 IT 资源。

监控的指标体系应该全面而深入。对 CPU 使用率，不仅要考虑总体占用，还要关注用户态与内核态所占的比例、负载平均值、上下文切换次数等深层指标。对内存来说，除了总使用率，还要看交换空间的使用情况，因为频繁的内存交换是性能下降的一个明确的信号。磁盘资源的监控要包含空间利用率、IOPS（每秒读写次数）和 I/O 延迟这三个指标，它们直接影响到数据存取性能。网络资源主要是监控带宽利用率、数据包丢失率、网络延迟。想要做到有效的监控，就要部署专业的自动化监控工具，可以随时随地对大量的指标数据进行采集，并将这些数据存入时序数据库当中加以分析和可视化展示，在仪表盘以及趋势图上清晰地呈现出系统容量的状况。

（三）容量预警与扩容

容量预警机制是把监控和扩容联系起来的纽带，它是从事后处理转向事前干预。给关键资源使用率指标设定合理阈值，当该指标长时间超过安全阈值的时候系统就自动发出警告，提醒管理者存在的容量风险。阈值设定要科学又得艺术：阈值太低，会生成大量的无效告警，干扰正常工作；阈值太高，就会造成预警滞后，错失最佳干预时机。一般会设置警告和严重这两个等级的阈值来区分问题的紧急程度。

收到容量预警且确认为持续增长趋势的时候，应该启动扩容程序。扩容有垂直扩容和水平扩容两种方式。垂直扩容就是提升单个服务器节点的能力，比如增

加 CPU 核心数、扩充内存、换更快的硬盘。这种方式实现起来比较简单，但是由于受到单台服务器物理的限制，成本高且存在单点故障的风险。

水平扩容就是增加更多的服务器节点分担负载，在分布式、微服务架构中更加推崇。当发现 Web 应用服务器 CPU 使用率一直偏高的时候，可以增加新的 Web 服务器实例并将其加入到负载均衡集群中分担压力。水平扩容有较好的弹性和可扩展性，可以支持系统规模的线性增长。云原生环境下，采用容器作为部署单元，依靠自动化编排平台，甚至可以根据实时的负载情况实现水平的自动扩容和缩容，在资源利用效率和系统可用性之间找到一个最佳的契合点。

第四节 运维监控技术

电力信息系统的稳定运行是保证整个电力系统安全、可靠运转的基础。随着系统规模越来越大，业务越来越复杂，传统的运维模式已经不能满足现实的需要。运维监控技术属于提高运维效率、保证系统可靠性的主要手段，以对系统资源实施实时监测、自动管理、智能数据分析为基本方式，实现了由被动应对向主动防御的根本性转变，已经成为电力信息系统建设的重要组成部分。

一、集中监控平台

集中监控平台是电力信息系统“监、管、控”一体化的“大脑”。它汇集网络设备、服务器、数据库、中间件、应用软件等各种资源的监控数据，经过集中处理和呈现，给运维人员呈现出现有系统全方位、清晰的运营视图，大大提高故障发现和处置效率。

（一）监控平台架构与功能

电力信息系统集中监控平台一般用分层、模块化的设计来保证高可用性、可扩展性和安全性。该架构大体上是由数据采集层、数据处理层、应用服务层和展示层构成的。数据采集层利用各种协议和代理工具从分散的电力生产、调度、营销等各个环节的 IT 基础设施上获取运行数据。数据处理层对大量的原始数据进行清洗、聚合以及关联分析，给上层的应用提供高质量的数据支撑。应用服务层是平台的核心部分，主要包括状态监测、告警管理、性能分析、拓扑可视化等模块。展示层通过统一门户，以图形化、可视化的方式将系统健康状况、资源使用

情况、业务运行态势等直观展示出来。

平台的主要功能就是对电力信息系统的全部栈资源进行统一监视。既可以对数据中心机房的动力环境进行监控，保证物理上的安全；又能网络设备、防火墙、服务器等硬件设备进行纳管，及时了解它的运行状态。同时监控还会对操作系统、数据库、中间件等基础软件进行监控，采集其性能指标和日志信息。平台用模拟用户访问，跟踪业务调用链的方式实现了端到端的检测业务健康度，保证重要电力业务的稳定可靠。依靠这样全方位、立体化的监控系统，平台给电力信息系统打造起一道牢固的防线。

（二）监控指标采集与展示

全面、精确地对监控指标进行采集，才是集中监控能够有效发挥效用的前提。依照电力信息系统的特性，在包含通用的 IT 资源监控项的同时还需要有行业的特有关键指标。通用指标主要是服务器 CPU 使用率、内存占用率、磁盘 I/O、网络带宽、数据库连接数、事务处理速度、锁等待情况、应用系统响应时间、吞吐量、错误率等。

就电力行业而言，监控指标体系所关注的性能参数更偏向于同业务相关联的那些。电力调度自动化系统中关键的遥测、遥信数据传输延迟和成功率是主要的监控对象，电力营销系统中电费计算、账单生成等核心交易处理耗时和成功率也十分重要。下表给出了电力信息系统当中一些主要的通用和行业专用监控指标。

电力信息系统核心监控指标示例表

监控类别	具体指标项	核心价值
基础设施	机房温度、湿度、漏水、供配电状态	保障 IT 设备物理环境安全
硬件设备	服务器 CPU/ 内存 / 磁盘 I/O，网络设备带宽利用率	评估硬件资源健康度与容量
基础软件	数据库连接数、事务速率，中间件线程池状态	洞察系统底层软件性能瓶颈
业务应用	系统响应时间、吞吐量、错误率、业务调用链追踪	端到端衡量业务健康度与用户体验
电力专属	遥测 / 遥信成功率、数据传输延迟、终端在线率	保障核心电力业务的连续性与准确性

这些指标的采集一般依靠专用探针或者代理，用 SNMP、JMX、WMI 等标准协议来完成。对采集到的大数据进行可视化展示便于观察。好的集中监控平台具有很强的定制性，运维人员可以按照不同的场景和管理需求，任意组合图表、

指标、拓扑图等，创造出自己喜欢的监控视图。例如，给数据中心创建带机柜空间、电力容量、温湿度云图的 3D 可视化场景；给核心业务系统创建显示交易流程、重要节点性能的业务拓扑图。平台支持大屏展示，把核心系统运行状态、关键性能指标、告警信息投影到监控中心，方便集中值守、应急指挥。

（三）告警管理与通知

告警管理是集中监控平台的核心能力之一，它的目的就是在系统发生异常或者潜在风险的时候，第一时间通知相关人员，并且触发后续的处理流程。一套完善的告警管理体系应该包含告警产生、告警收敛、告警分析、告警派发、告警处理等环节。平台按照预先设定好的阈值规则或者事件关联规则来发出告警，比如服务器的 CPU 使用率连续 5 分钟一直大于 90%，或者某个重要的业务接口响应时间超过 2 秒的时候，系统就会自动产生告警。

为了避免产生告警风暴给运维人员造成干扰，平台就必须具有很强的告警收敛能力。采用告警抑制、告警聚合、关联分析等方式，将因同一根源问题产生的多条告警合并成一条根源告警，便于运维人员快速定位问题根本原因。当一台核心交换机发生故障的时候，与它关联的服务器和应用都会产生告警，告警收敛机制可以将这些告警合并，直接指向根本原因是交换机故障。

告警的及时有效的通知非常重要，平台支持灵活的告警通知策略，按告警等级、影响范围、发生时间段等分场景选择短信、语音电话、邮件、即时通讯工具等方式将告警信息通知到相对应的运维人员或者团队。告警管理模块一般和工单系统深度集成，实现告警自动派单。重要告警产生后系统会自动创建故障工单并分派给负责人，形成从监控发现到工单流转再到故障解决的管理闭环，保证每一个告警都能得到有效的处理。

二、自动化运维

自动化运维是电力信息系统运维发展的高级阶段，是利用脚本、工具、平台将大量重复的、标准化的运维操作转变成自动化流程，以解放人力、提高效率、降低操作风险，将运维工作从“手工作坊”模式转变成标准化、智能化的“工业化”生产模式。

（一）自动化部署与配置

伴随着电力信息系统业务快速迭代，新的系统上线、扩容、升级的情况也越

来越频繁。传统的依靠人工安装部署、手动配置的方式既低效又容易因为人为失误造成配置不一致，给生产环境埋下隐患。自动化部署配置技术采用的是基础设施即代码的思想，用代码化、模板化的方法实现了 IT 资源的快速批量交付和标准化管理。

自动化部署就是指从申请硬件资源、安装操作系统、部署应用软件包这些步骤的总称。运维人员可以预先定义出包含操作系统、中间件和应用程序的标准化模板，在需要新环境的时候只需调用模板，指定少量的参数，自动化平台就可以在数分钟内搭建出一套或多套运行环境。配置管理是自动化部署的一个重要环节，用 Ansible、Puppet、SaltStack 等主流工具，可以将所有服务器的配置项用代码形式集中管理并做版本控制。任何配置变更都需要通过修改代码、执行自动化任务的方式来实现，保证各个环境配置的一致性，也给配置审计、快速回滚提供可靠的依据。

（二）自动化巡检与诊断

传统手工巡检是运维人员依次登录设备执行命令检查设备运行状况，该方法费时费力且覆盖范围、深度难于保证，很难发现深层隐患。自动化巡检依靠事先设定好的策略和脚本，定时、自动地对电力信息系统里的各种软硬件进行全方位的检查。

巡检内容可以包含硬件状态、系统资源利用率、关键进程存活、日志错误信息、数据库表空间、应用服务端口连通性等数百个检查项。巡检脚本可以模拟人工巡检的逻辑，用脚本里的规则去智能分析采集到的数据。巡检脚本可以自动检测主备数据库数据同步延迟，也可以判断负载均衡设备下所有应用节点是否正常。

当自动化巡检发现异常的时候，系统会自动生成巡检报告并触发告警，甚至可以联动自动诊断流程，对异常现象做进一步分析。诊断脚本依据事先设置的故障模型收集相关信息、做关联分析，试图找到问题的根源。当发现应用响应速度慢的时候，可以对相关的数据库、中间件、网络链路等做性能检测，得出初步诊断结果，极大缩短了故障排查的时间。

（三）自动化故障处理

自动化故障处理也就是“故障自愈”，是自动化运维能力走向成熟的标志。它的目的就是当系统出现某些故障的时候，不需要人工介入，由自动化平台按照事先设定好的规则和剧本，自动执行恢复操作，让业务中断时间尽可能短。对于

保证 7×24 小时不间断运行的电力核心业务系统来说，具有重大的意义。

故障自愈要依靠一个完整的“监控、决策、执行”闭环。集中监控系统会持续监视系统运行状态，当发现任何达到设定的自愈条件的故障时，会立刻执行自动处理程序。监控系统检测到某应用服务器进程异常崩溃的时候，会尝试自动重启该进程；如果重启失败就继续将这个服务器节点从负载均衡集群中摘除，防止影响用户访问，并同步创建需要人工跟进的告警工单。

其他典型的故障自愈场景有：检测到服务器磁盘空间不足时，自动清理临时文件或者日志文件；当主数据库出现故障的时候，自动执行主备切换流程；当应用版本更新之后，发现有很多报错的时候，自动执行回滚操作至上一个稳定的版本。自动化故障处理的达成，须要深厚运维经验的积累，把成熟的故障处理预案转变成标准化的自动化剧本，在充分测试验证之后再慢慢投入使用，从而保证操作的安全性与可靠性。

三、运维数据分析

伴随着电力信息系统的不断扩容，监控工具广泛应用，运维工作中所产生大量的、多维度的性能指标、日志、告警、配置变更的数据当中存在巨大的价值。运维数据分析指的是利用大数据、人工智能技术，对数据进行挖掘并开展智能分析，从而让运维工作由原来的被动救火，转变成主动预警、依靠数据来决策的新趋势。

（一）运维大数据平台

为了对庞大的运维数据进行有效的管理和利用，创建统一的运维大数据平台已经势在必行。该平台的主要任务就是将各个监控系统、日志系统、配置管理数据库、工单系统等各种数据源所产生的数据汇聚、存储并进行处理。技术架构大多采用 Hadoop、Spark 这样的主流大数据技术框架，数据处理分析的能力强。

运维大数据平台的重要任务之一就是创建统一的运维数据模型。平台对异构、非结构化数据进行整合、清洗、关联之后，把分散的各个数据点连在一起，形成一张可以反映 IT 资产状况以及它们之间时空关系的立体视图。比如一台服务器的性能指标、其上运行的应用日志、相关的告警事件、最近的配置变更记录等，都成为之后智能分析的良好底座。平台处理之后得到的高质量数据，既可以服务于运维场景，也可以为规划设计、安全审计等其它领域提供有力的支持。

（二）故障预测与根因分析

故障预测属于运维数据分析当中最具价值的应用之一。它利用机器学习算法，尤其是时间序列预测模型，对设备以及系统过去性能指标（CPU 占用率，磁盘空间，网络流量等）进行学习，进而预估其未来的发展趋向。当预测到某个指标将来会超过安全阈值时，系统就可提前发出预警，给运维人员留出足够的时间采取干预措施，将故障消灭在萌芽之中。通过分析磁盘写入速率、历史增长趋势来预估磁盘被占满的时间，提前告警。

而根因分析是解决复杂故障场景的利器。在庞大的电力信息系统中，一个故障现象是由很多互相影响、关联的因素造成的，传统的根因定位高度依赖资深专家的经验。用大数据、人工智能的根因分析技术，通过对告警事件、性能指标异常、日志异常的时序和拓扑关系进行分析，可以构建出故障传播链，快速准找到故障根本原因。当大量用户反馈某个业务无法访问的时候，智能根因分析系统就会通过关联分析，快速地发现所有的告警都指向同一个数据库实例，再结合该实例的性能指标异常，就判定故障原因为数据库死锁。

（三）运维知识库建设

运维知识库是存放企业运维经验、智慧的地方。传统的知识管理大多依靠分散的文档或者个人笔记，不能共享也不能检索。现代运维知识库建设就是对运维过程中产生的故障处理预案、操作手册、历史故障案例等各类信息实施结构化、智能化管理与应用。

构建运维知识库的重要技术就是知识图谱。知识图谱把运维领域的概念（设备、故障、操作）抽象成“实体”，把它们之间的关系（设备 A 出现故障 B，通过操作 C 可以解决）定义成“边”，从而构建起一张庞大的运维知识网络。这张网很好地展示了知识之间的联系，也给智能问答、智能推荐这些应用带来了可能。

运维人员在处理疑难杂症的时候，可以凭借自然语言同知识库对话，智能问答系统依据知识图谱开展推理，从而直接给出答复或者提供有关历史案例和解决办法的推荐。系统可以依据故障出现时的情况，在知识库中自动检索出最匹配的处理流程。运维知识库的形成有利于知识的累积与流传，降低对资深专家的依赖性，提升整个运维团队的技术水平以及解决问题的效率。

第八章 电力信息系统安全防护

电力系统与信息技术融合之后，电力信息系统安全防护就成为了保障电力稳定运行、保证国家能源安全的关键部分。本章主要从电力信息系统安全防护体系整体构建、关键技术应用、全生命周期管理实践三方面展开论述，为打造坚强的电力信息系统提供理论指导与实践参考。

第一节 安全防护体系

创建起全面的、立体的、动态的安全防护体系，这是防范各种网络攻击、保证系统核心功能和数据安全的基础。该体系是一个有机整体，它把技术、管理、运维等多方面融合在一起，采用分层、分域的方式，从而达成对安全风险的纵深防御和精确控制。

一、安全防护总体框架

安全防护总体框架是指指导电力信息系统安全建设的总体架构，在安全防护工作中起到顶层设计的作用，确定了安全防护工作的覆盖范围、重点要素和基本策略，是各项安全措施具有系统性、完整性和协调性的基础，是整个安全工作的大纲。

（一）物理、网络、数据与应用安全

物理安全是电力信息系统安全的第一道防线，主要指对承载信息系统的硬件设备、设施以及所在环境等采取各种措施，防止其受到以物质形态存在的威胁。采取的具体措施有对数据中心、机房、变电站等重要场所实施严格的物理安全保护措施，即安装门禁系统、安装视频监控系统、安排安保人员进行巡检；并且还配置环境监测系统实时检测温度、湿度、供电和消防数据，发现异常立即报告。物理安全一旦遭到破坏，那么其他任何安全措施都将变得毫无意义，它的关键性是显而易见的。

网络安全、数据安全属于防护体系的主要部分。网络安全主要是针对电力信息系统网络基础设施进行保护，使之具有可用性、完整性以及保密性，常用手段有防火墙、入侵检测系统与防御系统、网络流量分析等，防止网络攻击、病毒感染、未经授权的访问。数据安全是数据在其整个生命周期中被保护的过程，数据在采集、传输、存储、处理到销毁的各个阶段都会被考虑进去。这就要求使用加密技术保护数据传输和存储的机密性，用数据防泄露技术阻止敏感信息的泄露，同时用数据备份和恢复的方式保证数据的完整性和可用性。尤其是遇到勒索软件的时候，强大的数据恢复能力是十分重要的。

应用安全同业务功能是否稳定可靠密切相关，它是安全防护的最终落脚点。电力调度、营销，生产管理等主要的应用系统是攻击者攻击的目标。因此，应用安全要从软件开发生命周期的源头抓起，按照安全编码规范来减少代码漏洞。系统上线之后要部署 Web 应用防火墙来防止 SQL 注入，跨站脚本等常见的 Web 应用攻击。还应该做细访问控制，保证用户只能访问自己被授权的功能和数据，通过定期漏洞扫描和渗透测试，主动发现并修复应用层的安全隐患，形成漏洞发现和修复的闭环。物理层、网络层、数据层、应用层四层互为联系、深入到里，组成一个坚固的技术防护墙。

（二）安全管理、安全技术与安全运维

安全管理、安全技术、安全运维是构成电力信息系统安全防护能力的三大支柱，三者相互依存、相互缺一不可。安全管理相当于防护体系的大脑和神经中枢，它依靠制定、执行一系列的安全方针、策略、制度和规范来明确各个组织机构、人员的安全责任，给安全工作提供制度保障。这主要是建立完善的组织架构、组织全员安全意识教育培训、定期开展安全合规性检查与审计等，从根上提高整个组织的安全文化及水平。

安全技术是实现安全目标的手段、武器，是落实安全策略的具体措施。它包含从物理环境到应用系统各方面的安全产品和解决方案，防火墙、安全隔离网闸、加密机、态势感知平台、终端安全管理系统等。技术的选择和部署要同业务需求、风险状况相结合，不能出现过度防护造成资源浪费或者防护不足留下安全隐患的情况。先进适用的技术可以大大加强自动化防御的水平，缩减因为人为操作失误引发的风险，成为形成坚固技术防线的关键支柱。

安全运维是联系管理和技术的一座桥、一个执行者，把安全策略和技术手段

落实到日常工作中。这是贯穿于系统整个运行阶段的一项持续性工作，内容包括7x24 小时不间断的安全监控、日志分析、漏洞管理、补丁更新、安全事件应急响应和处置等。一支高效的运营安运团队，在第一时间就可以发现威胁，并迅速地作出应对攻击的决策，并且能持续对安全体系进行优化，从而使安全体系处于一个持久、高效的工作状态。只有将周密的管理、先进的技术、专业的运维三者有机结合，才能形成强大的安全合力，才能真正保证电力信息系统长久平安。

（三）纵深防御与分域防护

纵深防御是电力信息系统安全防护的核心思想，它的理念来自于军事防御思想，主张在攻击者可能通过的路径上设置多道、多样化的并且互相联系的防御关卡。它并不指望某一种安全措施就能抵御所有的攻击，而是构筑起多层次的防线，让攻击者即使绕过外围防线，也会在内部碰到层层阻拦和检测。每一层都有不同的防御重点，在网络边界用防火墙、入侵防御系统等，服务器上用主机保护、微隔离等，数据库上用访问控制、加密等。多层次结构使攻击变得困难、昂贵且耗时，给检测和响应攻击争取到了宝贵的时间。

分域防护就是纵深防御思想在网络空间结构上的具体体现，按照电力信息系统内部各个业务单元的属性、重要程度和安全需求，把整个网络划分成若干个彼此隔离的安全域。电力调度生产控制大区和管理信息大区之间必须严格隔离，在生产控制大区内部还可以细分为不同的控制区。每一个安全域有独立的边界以及统一的访问控制策略，安全域之间的所有数据交互都要经过边界的安全设备审查控制。分域防护意在“分而治之”，把安全风险局限在某个区域之内，阻止威胁在全部网络里横向扩散。一旦某个区域被攻占，其影响范围也会被限制，不会直接波及其它核心区域，这对于保证电力核心业务的连续性和安全性十分关键。

二、安全域划分与边界防护

安全域划分、边界防护，属于纵深防御、分域防护策略的技术实践。根据科学合理的安全域来界定，并针对各安全域的边界实施精细化的访问控制可以形成内部分区、层层设防的安全格局。

（一）安全域划分原则

电力信息系统的安全域划分属于一项复杂的顶层设计工作，必须依据一些科学的原则来保证其合理性以及有效性。核心依据就是业务功能以及重要性等级。

需要对业务属性相似、安全需求相同的系统或设备划分为同一个安全域，如所有与实时调度控制相关的系统划入生产控制域，办公自动化、人力资源等系统划入管理信息域。按照业务中断可能造成的影响，对各个域的重要性进行评级，重要程度越高的区域，所配置的安全防护措施就应越强。

安全域划分还要遵循最小化原则、边界明确原则。最小化原则要求尽可能缩小每一个安全域的范围，使得域内的资产都具有高度一致的安全需求，从而可以实施统一并且严格的安全策略。边界明确原则指明安全域之间的边界要清晰，网络上不能有模糊地带或者非法的连接路径。所有的跨域通信都要通过预设的、唯一的边界安全通道，给边界防护策略的实施打下了良好的基础。采用以上多种原则相结合的方式才能建立一个结构清晰，容易管理、具有一定的防御性的域安全体系。

（二）边界访问控制策略

边界访问控制是安全域隔离和保护的主要手段，它的根本目的就是保证所有跨越安全域边界的流量都必须经过授权、检查。制定访问控制策略的时候要遵循“默认拒绝，例外允许”的黄金法则，即默认禁止所有域间的通信，只对有实际业务需求、经过充分风险评估的通信请求逐个开放。这种“白名单”机制相对于“黑名单”机制来说有着天然的安全性，可以更好的防止未知威胁。

访问控制策略定义要尽可能地细化，至少要到源地址、目的地址、协议类型和端口号这“四个要素”。对于关键业务还要更细一些，比如限制到具体的应用层协议或者指令。策略的制定必须要有详细的业务流程梳理作为基础，保证每一条放行策略都有具体的业务需求来支撑。

1. 要建立严格的策略生命周期管理流程，包含申请、审批、发布、审查和清理等环节。临时策略要设有效期，到期就自动失效；长期策略得定时回顾是否还必需，及时清理不需要的冗余策略，防止策略太多反而降低安全防护效果。

2. 双向访问控制，既要控制从低安全域到高安全域的访问（由外向内），也要对高安全域发起的访问进行限制（由内向外），防止高安全域被攻陷后成为攻击内部其他区域的跳板。

3. 对于允许通过边界的应用协议要启用应用层深度包检测功能，对传输的内容进行检查，从而发现并阻止隐藏在正常业务流量中的攻击代码或者违规操作。

（三）安全隔离装置部署

为了在物理或者逻辑上实行边界访问控制策略，必须在安全域边界安置合适

的隔离设备。设备选择与部署方式要根据所连安全域安全等级有无差异、业务通信需求是否需要等来确定。对安全等级相差很大的区域，例如电力调度生产控制大区与管理信息大区之间，必须使用安全隔离网闸等物理隔离技术。安全隔离网闸依靠“内外网主机、隔离交换”的体系结构，在断开网络层连接的基础上，以受控的方式进行安全的数据交换，从根本上杜绝一切基于网络协议的攻击渗透，是保障核心控制系统安全的最高级别防护手段。

对于安全级别相当或者需要进行协议级交互的域间连接，一般会使用高性能的下一代防火墙。下一代防火墙除了有传统的状态检测包过滤功能外，还集成了应用识别、入侵防御、病毒过滤等众多安全能力，能够对边界流量进行多维度的深度检测与精细化控制。防火墙需要使用高可用模式 (主备或集群) 部署，以保证边界防护的业务连续性。其策略配置必须与前面提到的访问控制策略精确匹配，保证策略有效落地。同时在网络复杂的环境下还可以通过虚拟局域网、虚拟路由转发等网络技术进行逻辑上的隔离，从网络层面上对不同的安全域之间进行分隔，作为物理隔离和防火墙隔离的补充，从多个角度构建起牢不可破的一道边界。

三、安全生命周期管理

电力信息系统的安全不是一次建成就完成的，它是伴随着电力信息系统从规划、建设到报废整个生命周期的动态、持续的过程。实施安全生命周期管理，就是将安全要素嵌入到系统各阶段中去，实现安全能力的左移以及持续改进。

（一）需求、设计、开发、测试、部署、运维各阶段安全

在信息系统生命週期的起始阶段，也就是需求分析阶段，就应当把安全当作一项核心需求明确地表达出来。确定系统安全目标、梳理相关的法律法规和标准规范要求、定义数据分类分级标准，并将它转化为具体的、非功能性的安全需求，为后续所有的安全工作打下基础。

进入设计阶段之后，安全设计的重点就是创建一个内生安全、有弹性恢复能力的系统架构。此时就需要开展威胁建模活动，主动发现系统所面临的潜在威胁和攻击路径，并针对这些威胁和路径设计相应的缓解措施，比如安全域的划分、认证授权机制的设计、数据加密和脱敏方案的规划等等。安全架构设计要与业务架构设计同步开展，把安全措施嵌入到系统中。

开发阶段就是把安全设计从蓝图变为代码实现的关键环节。需要给开发团队

给出明确、可行的安全编码规范并开展相关的培训，提升开发人员的安全意识和能力。应该采用成熟的开发框架、组件库，避免因为自己“造轮子”而带来风险。同时可以采用静态应用安全测试工具，在编码阶段就对源代码进行扫描，及时发现并修补存在的安全漏洞。

测试阶段是检测系统安全性的环节。除传统的功能和性能测试外，还需要进行专门的安全测试。动态应用安全测试是用模拟攻击的方式来检测系统运行时存在的漏洞；渗透测试则是安全专家以攻击者的视角对系统进行全方位的攻击尝试，找出更深层次、更复杂的安全问题。所有的漏洞都要评级并且跟踪修复，直到系统达到安全基线才能上线。部署运维阶段安全工作由一次性的建设转变为长期的保障和监控，开展安全基线配置、定期漏洞扫描及补丁管理、实时安全监控与日志审计、制订并演练应急响应预案，保证系统长时间稳定运行。

（二）安全风险评估与处置

安全风险评估属于安全生命周期管理的关键循环环节，动态地对电力信息系统遭遇的各种安全风险实施识别、分析并加以评价。它为决策者回答遇到怎样的威胁、薄弱环节在哪里、会造成多大的损失等关键问题提供了科学依据，是制定并调整安全策略的依据。评估过程一般包含资产识别、威胁识别、脆弱性识别、现有安全措施分析、风险计算等环节，最后用定性或者定量的方式，得出各个风险点的风险等级。

风险评估的结果一定要转变成具体的风险处理行动。风险处置一般有四种基本策略，即风险规避、风险降低、风险转移和风险接受。如下表所示为四种策略的总结。

安全风险处置策略表

策略类型	核心思想	处置方式举例
风险规避	调整业务或系统设计，从根本上避开风险	停止某项高风险的互联网业务，从而消除相关的网络攻击威胁。
风险降低	采取额外的安全控制措施，降低风险发生的可能性或造成的影响	针对已发现的系统高危漏洞，立即开发并部署安全补丁。
风险转移	通过合同或协议，将风险带来的财务损失转嫁给第三方	购买网络安全保险，将潜在的重大经济损失转移给保险公司。
风险接受	在充分评估后，对发生概率极低或影响微小的风险，有意识地接受其存在	对于某些修复成本远超潜在损失的低危漏洞，经审批后接受其风险。

处理高等级风险一般使用风险减低的方法，即增加新的安全控制措施。对一些不能降低或者降低成本过高的风险，可以采取风险规避或者风险转移。对概率极小且影响不大、级别较低的风险，在评估和批准之后可以采取接受风险的策略。所有的风险处置决定都要有详细的记录，并持续跟踪处置措施的效果和有效性。

（三）安全持续改进

安全威胁和技术环境在不断变化，电力信息系统安全防护体系不能一成不变。安全持续改进是生命周期管理的最终目的，即形成闭环、螺旋式上升的安全管理循环。此过程一般会采用戴明环模型，也就是“计划、执行、检查、处置”这四个环节组成的循环。按照风险评价的结果以及业务的变化来制订新的安全目的和手段（计划）。执行具体步骤方案叫行动。经过连续的监控、定期的审计和检测对安全措施的有效性和合法性进行检验。

处置阶段为循环的决定性一环，根据检查阶段发现的问题，改善已有的安全策略与控制手段。当安全监控发现新的攻击方式的时候，就要立刻更新入侵检测规则，修改应急预案；当审计发现某项安全制度没有得到落实的时候，就要分析原因，加强培训或者调整流程。经过这样周而复始的过程，电力信息系统的安全防护水平就能在不断变化的内、外部环境中不断改进和加强，进而达成由被动防护向主动防御、由静态构建向动态适应的转变，从而保证电力信息系统的长久安全稳定。

第二节 网络安全技术

电力信息系统属于国家关键信息基础设施的重要部分，它的网络安全状况牵涉到电力系统能否稳定运行以及国家能源安全。信息化、数字化转型深入进行以后，原本物理隔离的电力监控系统逐步与管理信息网、互联网连接起来，网络安全技术就成为保障电力信息系统安全、稳定、可靠运行的关键环节和重要支撑。

一、网络边界防护

网络边界是电力信息系统安全防护的第一道防线，主要作用就是隔离不同安全等级的网络区域，精准控制内外部网络之间的信息交换与访问行为，有效阻止未授权访问和网络攻击，给内部网络构筑起基础的安全屏障。

（一）防火墙技术

防火墙是在不同的网络或者安全域之间执行访问控制的安全组件。用预设的策略规则来审查流经的网络数据包，决定放行或者阻断。在电力信息系统中，防火墙是实现网络分区隔离的基本技术手段，在生产控制大区和管理信息大区之间部署工业防火墙，就可以对两大区进行有效的逻辑隔离。传统的防火墙是按照 IP 地址、端口号等网络层的信息来进行访问控制的，一般称之为包过滤防火墙或者状态检测防火墙。

伴随着网络攻击技术的不断发展，新一代防火墙随之出现。它除了具有传统防火墙功能外，还集成了应用层检测、用户认证、入侵防护等高级功能。对电力系统常用的一些 IEC104、Modbus 等工业控制协议来说，要使用可以支持这些协议深度包检测的工业防火墙。通过对协议指令级进行细粒度分析，可以识别、阻止非法的、异常的控制指令，防止对工业控制系统进行恶意操作，实现对核心生产业务的纵深防护。

（二）入侵检测与防御系统

入侵检测系统和入侵防御系统都是防火墙功能的一种扩展和补充，它们可以更加深入的分析网络流量来发现并阻止潜在的网络攻击。形象地说，入侵检测系统就像网络里的监控摄像头，主要是监测和报警；而入侵防御系统更进一步，可以主动拦截和阻断已经被识别出来的攻击流量，就像一位尽职尽责的网络安全卫士。

入侵检测与防御系统的核心就是它的检测方法，主要分为基于特征的检测和基于异常的检测。基于特征的检测采用匹配已知攻击模式库的方法来识别攻击，效率高、误报率低，但不能发现未知的零日攻击。基于异常的检测则是通过建立网络正常行为基线模型，把偏离基线的行为识别为异常或者攻击。对于运行模式比较固定的电力监控系统网络来说，基于异常的检测有着独特的优点，可以及时发现具有针对性的未知攻击企图。入侵检测与防御系统一般以串联或者旁路的方式设置在区域边界、服务器前端等关键网络节点，对进出核心区域的流量进行实时监测和防护，从而形成动静结合的立体防御体系。

（三）VPN 与远程访问安全

随着电力系统智能化程度的不断加深，对变电站、新能源场站等远程运维以及数据采集的需求也越来越大。虚拟专用网络技术可以利用公共网络创建一条加

密的逻辑专用通道，给远程访问提供安全可靠的解决办法，保证数据在传输过程中不被窃听、不被篡改，具有很高的保密性、完整性以及认证性，防止数据被窃听或者篡改。

电力信息系统远程访问时必须采取严格的控制安全措施。使用高强度的加密算法来保证虚拟专用网络通道本身的安全，还要建立认证机制。强烈建议采用数字证书、动态口令、生物特征识别等多因素认证方式代替传统的静态密码认证，保证接入用户可信度。同时要按照最小权限原则，针对不同的运维人员角色，细化其能够访问的范围、可以执行的操作，并且对所有的远程访问会话进行详细的记录和审查，在事后追查的时候可以明确责任，杜绝越权行事以及内部风险。

二、网络内部安全

网络边界防护并不能完全阻止所有的攻击。当攻击者突破边界防线入侵内部，或者攻击来源于内部时，内部安全防护措施就成了防止威胁扩散、减少损失的第二道重要屏障。内部安全重点是对已经接入的设备、用户、流量做更细粒度的安全控制。

（一）网络准入控制

网络准入控制是一种先进的终端安全防护技术，它对于企图接入内部网络的每一个设备都必须执行身份认证、安全检查、持续监控等一系列的严格控制措施，保证只有符合安全策略的、可信任的设备才能接入网络，从源头上阻止安全风险的引入。网络准入控制的实行，完全冲破了传统网络“一接入就全信任”的旧有理念，创建起“先认证后接入，不合规即隔离”的安全接入新模式。

网络准入控制的一般流程有身份认证、安全评估和访问控制这三个步骤。设备想要接入网络的时候，系统就会强制该设备进行身份认证。认证通过之后，系统会对设备的安全状况进行评价，即查看其操作系统补丁、防病毒软件版本以及病毒库是否更新到最新。系统最后根据评估结果给设备分配完全访问权限、限制访问权限或者将其重定向到隔离区等不同的网络权限。在电力调度中心、变电站等重要场所部署网络准 au 入控制，能够防止私接乱连、非工作人员非法接入、携带病毒的终端接入核心网等行为，极大提高内网整体安全基线。

（二）VLAN 划分与端口安全

在结构复杂的电力信息系统网络中，利用交换技术对安全域做细粒度的划分，

可以提高内部安全。虚拟局域网技术可以把物理上属于同一个局域网的设备，在逻辑上分成若干个相互隔离的广播域。不同虚拟局域网之间通信要经过路由器或者三层交换机，这就为在它们之间实施访问控制策略提供了可能。在电力系统中，一般按照业务类型和安全等级将 SCADA 系统虚拟局域网、保护管理虚拟局域网、办公自动化虚拟局域网等划分成不同的网络，可以隔离不同业务流量，即使某个虚拟局域网发生安全事件，也能将其影响限制在局部，不扩散到其他网络。

基于对虚拟局域网的划分，在交换机上对端口实施安全保护可以做更为基础的接入控制。配置交换机端口上的安全策略，对接入设备做物理层精准控制。下表给出了常用的端口安全技术以及其作用。

交换机端口安全技术对比表

技术手段	功能描述	应用效果
MAC 地址绑定	将交换机端口与特定设备的物理 MAC 地址进行静态绑定。	确保只有指定的授权设备才能通过该端口接入网络，有效防止非法设备仿冒或替换。
MAC 地址学习限制	限制单个交换机端口能够学习到的 MAC 地址最大数量。	防止用户在端口下私接交换机或集线器等设备，避免网络结构的无序扩张。
违规处理机制	当端口检测到违反安全策略的 MAC 地址时，可配置告警、丢弃数据包或直接关闭端口等自动化响应动作。	实现对违规接入行为的实时响应和快速处置，极大增强了网络接入点的防御能力。

如上表所示，这些措施共同构筑起一道坚固的网络接入“铁壁防线”。

（三）无线网络安全

无线网络因为具有部署灵活、使用方便等特点，在电力系统移动巡检、数据采集、应急通信等场合中应用越来越广泛。但是由于无线信号的开放性传播特性，无线网络的安全问题比有线网络更加严峻，例如非法接入、数据窃听、中间人攻击等。保证无线网络安全必须采取一整套综合性的技术手段。

要创建安全的电力无线网络，首先要使用高强度的 WPA3 加密协议来保证无线信道上传输的数据是保密的。虽然隐藏服务集标识符、启用 MAC 地址过滤可以在一定程度上增加攻击者发现并接入网络的难度，但这不能成为主要的安全措施。核心的安全保障在于创建强有力的身份认证系统，使用 802.1X 协议和 RADIUS 服务器结合的方式来对接入用户实行数字证书或者用户名 / 密码的严格

认证。同时将无线接入和网络准入控制系统联动起来，对无线设备在接入网络之前做全面的安全检测。为不同的业务建立无线流量隔离，利用无线入侵防御系统实时监测并阻止无线环境中恶意行为的发生，也是构成电力无线网络纵深防御体系的重要部分。

三、网络攻击防护

随着攻防对抗的不断升级，网络攻击也越来越复杂、有组织、持久化。电力信息系统的威胁已经不再只是传统的病毒或者孤立的黑客，而已经演变成以窃取情报、实施破坏为目的的高级威胁。因此必须创建出能够抵御某种特定攻击类型的专项防护能力。

（一）DDoS 攻击防护

分布式拒绝服务攻击是通过控制大量的“僵尸主机”，向特定的服务器或者网络发起大量的无效请求，就像洪水一样消耗目标带宽或者系统资源，使得目标不能对合法用户的正常请求作出响应。电力企业对外服务的网上营业厅、客户服务门户等互联网应用，都是分布式拒绝服务攻击的主要攻击目标。一旦这些系统瘫痪，就会对客户服务和企业形象造成严重影响，甚至会波及正常的业务流程。

分布式拒绝服务攻击的防护关键就是准确的检测和快速的清洗。现代防护体系一般是立体的，既有本地防护又有云端防护。在本地部署抗分布式拒绝服务设备，可以在攻击流量进入内网之前快速识别和过滤，对小规模的攻击有很好的防护效果。但是当面对超大规模的流量攻击时，本地设备是无力抵抗的，这时就需要将流量引导到云端的“清洗中心”。云清洗服务商具备大量的带宽资源以及专业的防护设备集群，可以将攻击流量清洗掉，再把干净的业务流量回注到源站，以此保证业务连续性。根据电力系统自身的特点，为关键通信线路提供对抗此类攻击的保障措施，也可以使用物理隔离或者专用链路。

（二）APT 攻击检测与防御

高级持续性威胁指的是有组织、有预谋、长时间地对某个目标进行网络渗透的一种行为。攻击者一般都具有专业的背景和充足的资源，其攻击手段十分隐蔽，攻击过程长且持久，目的是窃取重要的敏感数据或者对重要的系统进行潜伏性的破坏。电力、能源等关键基础设施是高级持续性威胁攻击的主要目标，其造成的危害非常严重，不能有丝毫的松懈。

防御高级持续性威胁是项繁杂的系统工程，不能指望靠某种安全产品就能完成，必须打造“一直监视、迅速应对”的动态防御能力。必须有全方位的态势感知能力，网络关键节点安装流量探针，终端上装 EDR，利用安全信息和事件管理平台集中分析网络中所有的日志、流量数据以及终端的行为情况，用大数据与人工智能技术挖掘出异常的行为。积极地把威胁情报纳入进来，掌握最新出现的攻击手法以及 IOCs 指标，从而提高检测的准确性以及实时性。沙箱技术可以把可疑文件、链接放到隔离环境里模拟运行，进而看清其真实的行为意图，有效地找出未知的恶意软件。必须要有专业的应急响应团队和应急预案，一有高级持续性威胁攻击的蛛丝马迹，就立即开展溯源分析、隔离处理、系统加固和恢复工作，尽可能将损失降到最低。

（三）恶意代码防护

恶意代码即病毒、蠕虫、木马、勒索软件、间谍软件等各种恶意程序的统称。它可以利用系统漏洞、电子邮件、移动存储介质等途径进行传播，对电力信息系统的机密性、完整性、可用性造成直接威胁。尤其是近几年来肆虐的勒索软件，一旦在电力监控系统或者办公网络中爆发，就会造成大范围的系统瘫痪和业务中断，后果不堪设想。

构建有效的恶意代码防护体系，需从“预防、检测、响应”三方面出发，采取综合手段。在预防阶段除了对传统的防病毒软件进行部署，并保证病毒库及时更新以外，更重要的是实行应用程序白名单策略，也就是坚持“非许可，即禁止”的原则，仅允许被许可的应用程序运行，这样可以阻止绝大多数的未知恶意代码的执行。同时对操作系统以及应用软件进行安全补丁管理，修复已知漏洞。检测阶段应该结合邮件安全网关、Web 安全网关等边界设备，在恶意代码进入内网之前进行过滤和拦截。响应环节要定期开展数据备份恢复演练。这样即使遭到勒索软件等破坏性的攻击，也可以快速、完整的恢复业务系统和核心数据，这是保证业务连续性最后一道坚固的屏障。

第三节 数据安全保护

电力信息系统担负着国家能源运行重要数据，它的安全与否牵涉到电网是否能够稳定运行、社会经济能否正常运转乃至国家安全。因此，给电力信息系统打造起一道稳固的数据安全防线，是它建设过程中的一个关键步骤。本节将就数据分类分级、数据加密技术、数据备份与恢复这三个主要方面，对电力信息系统数据安全保护的技术和方法进行系统的阐述，以期给相关从业人员提供一套全面、可行的技术参考。

一、数据分类分级

数据分类分级是实行差别化安全策略、做到细化数据保护的基础。梳理电力数据资产，对电力数据资产进行分类分级、确定重点，有针对性地将有限的资源优先投入核心重要的数据保护中，从而达到数据安全管理成本效益最大化的目的，满足合规性要求。

（一）数据分类分级标准

电力信息系统数据分类分级标准要结合业务性质，数据敏感度，可能造成的影响范围和法律法规要求来确定。实践中一般会遵循系统性、稳定性、可扩展性这三个原则。数据分类可以按照业务领域来进行划分，可以分为电网运行数据、营销与客户服务数据、企业经营管理数据等。在每一大类之下还可以再分出具体的子类，电网运行数据可以细分为调度自动化、继电保护、能量管理等子类。

数据分级是按照数据一旦被泄露、篡改或者破坏之后，对国家安全、社会秩序、公共利益以及企业及个人权益所造成的危害程度来确定的。按照国家以及行业指导规范可以将数据分成三个或者更多个安全级别。敏感级（第三级）是指该数据被破坏之后，会对关键行业造成严重的影响；低敏感级（第二级），其被破坏会带来中等程度的影响；非敏感级（第一级），被破坏影响范围一般局限在机构内部。电力行业的关键电网设备实时运行参数、重要的调度指令等属于最高安全级别的数据，普通的公开性政策文件属于较低级别。建立一套明确具体的分类分级标准，是后面所有的安全工作的基础。

（二）不同级别数据的保护要求

不同的安全级别对应不同的数据，应当对数据采取相应的保护措施，做到防

护力度与数据价值匹配。这些保护的要求需要渗透到数据的采集、传输、存储、处理、使用、销毁的整个过程之中。不同安全等级的数据具体保护要求见下表。

电力数据安全保护级别与要求对照表

级别	描述	核心保护要求
非敏感级（第一级）	破坏的影响范围通常局限于机构内部。	保障数据的完整性与可用性。采用基础访问控制和常规备份，防止数据被轻易篡改，确保数据在内部网络中按需可用。
低敏感级（第二级）	破坏会带来中等程度的影响。	在第一级基础上，增加更严格的访问控制和安全审计。数据传输时应采用通道加密，存储于受保护区域，访问行为需明确授权并留存记录。
敏感级（第三级）	破坏将对关键行业造成严重影响。	采取最严格的保护措施。数据全生命周期强制执行高强度加密（传输加密与存储加密）。访问控制遵循“最小权限”和“按需知密”原则，并启用多因素认证。所有操作均需被严密监控和深度审计，并制定专门的数据销毁规程。

具体来说：

1. 非敏感级数据，第一级的重点就是保证数据在流转过程中的完整性和可用性。可以使用基本的访问控制以及常规的备份方式，保证数据不会被随意更改，在需要的时候可以随时调用。这类数据一般容许在内部网络里常规共享，防护重点是阻止未授权的修改。

2. 低敏感级别（第二级）数据，在满足第一级的基础上还需要采取更严格的安全访问控制和审计。数据在传输时要走通道加密的路，存起来就得放在有保护的地带。对于此类数据的访问要经过明确授权，行为也需要被记录下来，以便事后追溯、审计。

3.3、对于敏感级 (三级) 数据要采取最严密的保密措施。数据在全生命周期的各个阶段都需要实施高强度的加密保护，包括传输加密和存储加密。访问控制要严格按照最小权限和按需知密原则，并启用多因素认证。对于敏感的数据所有的操作都需要有严密的监控以及深入的审计。还要制定专门的数据销毁程序，使敏感数据在生命周期结束之后被完全清除并且无法恢复。涉及个人敏感信息的，应当遵守有关个人信息保护的法律法规。

（三）数据资产梳理

数据资产梳理属于数据分类分级工作落地执行环节，主要目的在于把电力信

息系统内部的“数据家底”彻底摸清，从而形成一份完整的、准确的数据资产目录。这就如同给企业所有的数据资源做一张精确的“地图”，是做好企业数据治理和安全管控的前提。这项工作牵扯到跨部门的配合，特别是信息技术部门和业务部门的配合。

梳理流程一般从确定范围和目标开始，即确定要盘点的业务系统、数据库、文件等。综合使用自动扫描工具和人工访谈的方法来全面地找到数据、确定存储位置，了解数据源及大致流向。在此基础上对各数据资产进行元数据采集记录，即数据定义、格式、结构、所有者、创建时间等，来建立数据目录。同时还要分析数据之间的血缘关系，也就是追踪数据从产生到加工、流转、融合的全过程，理清数据的上下游依赖关系，这对于认识数据的价值、评价安全风险十分关键。最终把成果同分类分级标准融合起来，给每项数据资产加上分类和级别的标签，形成一份会自己更新的数据资产清单，从而为后面安全策略的精确制订给予支撑。

二、数据加密技术

数据加密是保证数据机密性的主要技术手段，用密码学算法把明文数据变成不能直接读取的密文，这样，没有得到授权的人即便得到了数据也不能知道它的内容。电力信息系统当中，加密技术的使用涉及数据传输和数据存储这两个过程，而它的安全状况很大程度上取决于密钥管理是否到位。

（一）传输加密

电力信息系统内数据在各个节点、系统、网络之间不断流动，终端采集设备与主站系统之间，或者不同的业务应用之间数据的交互。在这其中传输的数据处于开放或者半开放的网络当中，很容易被他人窃听、修改、仿造等。传输加密技术的主要目的就是保证数据在网络传输过程中机密性、完整性以及真实性。

业界广泛使用传输层安全协议和它的前身安全套接字层来实现传输加密。TLS 协议是传输层和应用层之间的一个协议，可以为上层应用的数据，比如 HTTP 或者 FTP 建立一个安全的通道。其核心就是握手协议，在正式的数据传输开始之前，客户端和服务器端通过一系列的交互来完成相互的身份验证，协商加密套件，并且交换会话密钥。该过程一般采用非对称加密算法和数字证书来验证服务器的身份，然后安全地协商出后面通信所用的对称密钥。

握手成功后所有的应用数据都用这个临时对称会话密钥加密、解密。由于对

称加密算法的运算效率比非对称加密要高得多，所以混合加密模式既安全又高效。电力系统建设中对所有涉及敏感数据或者控制指令的网络通信，都必须强制启用基于 TLS 加密传输，即把 HTTP 升级为 HTTPS，保证从发送端到接收端的整个通信过程中都是加密的，从而防止中间人攻击和数据窃取。

（二）存储加密

静态存储的数据也存在安全隐患，物理介质（硬盘、磁带）丢失或者被盗，内部人员非法访问等都会造成数据泄露。存储加密就是对持久化保存的数据进行加密，保证存储介质被非法获取时，其中的数据不能被读取。

数据库加密是存储加密的重要领域，因为大部分重要的业务数据被存放在关系型或者非关系型的数据库中。透明数据加密为当前主流的技术手段，它是数据库引擎直接对数据文件完成加解密的流程。数据写入磁盘的时候自动加密，从磁盘读入内存的时候自动解密，整个过程对上层应用软件完全透明，不需要修改任何应用代码。除了 TDE 之外，还可以在操作系统层面采用文件系统加密，对整个数据库文件或者某个目录进行加密。另一种方式是应用层加密，即由应用程序在数据存入数据库之前自行加密，但是这种方式实现起来较为复杂，并且可能会对数据库的查询和索引性能造成影响。文件加密主要是对非结构化或者半结构化的数据进行加密，比如配置文件、日志文件、设计图纸等。对单个文件或者整个文件夹进行加密，也能有效地防止由于文件被非法复制而造成的信息泄露。

（三）密钥管理

加密技术安全程度很大程度上取决于密钥本身是否安全。一旦密钥泄露，那么所有的加密措施就都等于白费。密钥管理就是密钥从生成、分发、存储、使用、轮换、归档到最后销毁全生命周期的过程。健全并安全的密钥管理系统，成为数据加密实践能否成功的根本保证。

密钥生成必须具备足够的随机性、强度，来抵御暴力破解攻击。密钥的存储是管理过程中的重中之重，绝不能和它们所要保护的数据存放在一起，更不能以明文形式进行存储。业界一般使用专用的硬件安全模块或者密钥管理系统来安全地生成、保存和管理密钥。专用的设备和系统对密钥给予强有力的物理及逻辑保护，可以防止密钥被窃取。

密钥的使用要严格遵守最小权限原则，只有被授权的用户或者应用才能在指定的时间里使用指定的密钥。而且密钥轮换也是不能忽略的安全措施。定期更换

密钥可以缩短单个密钥的生命周期，即使旧密钥被泄露，造成的损害也被限制在很短的时间里。密钥轮换策略要依照数据的重要性以及密钥的使用频次来制订。

密钥的生命周期结束或者保护的数据不再需要的时候，必须执行安全销毁程序，确保密钥及其所有副本被完全清除，不能恢复。一个完善的密钥管理体系中还应该包含密钥的备份与恢复机制，防止出现密钥丢失或者损坏等情况，并且所有的操作都应该有详细的审计日志进行记录，方便之后的安全追溯。

三、数据备份与恢复

在复杂的、不断变化的运行环境中，不可能有任何一个信息系统是绝对安全的，硬件出问题，软件有漏洞，人操作失误，网络遭攻击，甚至是自然灾害，这些风险一直存在。数据备份与恢复属于数据安全的最后一道防线，不能轻视。其主要目的就是当出现灾难性事件造成数据丢失或者损坏的时候，可以迅速且完整地将数据以及系统恢复到正常状态，以此来保证业务的连续性。

（一）备份策略

选择合适的备份策略，就是要在备份效率、存储开销和恢复时间目标这三个方面找到一个最佳点。电力信息系统依据数据的重要程度，变化快慢等要素，可自由选择采用下列几种基础备份策略之一或者组合使用。

1. 全量备份是最基本的备份方式，也就是完整地复制所选的所有数据。优点是恢复过程最简单、速度最快，只需要最近一次的全量备份集就可以完成。但是每次备份所花费的时间比较长，并且占用的存储空间最大。

2. 增量备份：备份自上次备份（全量备份或者增量备份）以来改变过的数据。此方法速度快、占用空间小。但是它的数据恢复过程比较复杂而且耗时，需要依次恢复上次全量备份及之后所有的增量备份集，链中的任何一个环节出错都会导致恢复失败。

3.3、差异备份：只备份自上次全量备份后所有改变过的数据。其备份时间和空间占用在全量备份和增量备份之间。恢复时只需要用上一次的全量备份集和最近一次的差异备份集，因此恢复过程比增量备份更简单。实际运用时一般会采用组合的方式，比如每周做一次全量备份，每天做一次差异或者增量备份，从而达到资源和效率之间的最好平衡。

（二）备份介质管理与异地存放

数据备份的最终目的就是在灾难发生之后能够成功地恢复数据，因此备份副本自身安全十分重要。规范备份介质的管理，可靠的异地保存，都是保证备份数据可用性和安全性的关键环节。备份介质可以是物理磁带、磁盘阵列，也可以是云存储。对这些介质要进行规范化管理，即标签清楚、存放安全、定期做介质健康检查，以防介质损坏造成备份数据无法读取。

将备份的数据保存在与生产数据中心物理上不同的地方，也就是异地存放，这是防范区域性灾难（火灾、地震、洪水等）的根治办法。若备份的数据和原始数据同处一地，遭遇一次灾难两者都会遭受毁灭，造成无法恢复的局面。异地存放的方式有很多，可以定期将物理介质（磁带等）运送至安全的异地保管库，也可以通过网络将数据远程复制到异地数据中心，还可以使用公有云或者私有云提供的云备份服务，将数据副本存放到云端。

选择异地存放地点要考虑到地理距离、网络带宽、环境安全和成本等各方面的因素。存放地点应该足够远，以避免受到和主数据中心一样的灾难的影响。但是必须保证数据在传输到异地时是加密的，防止数据在途中被盗取。完善的介质管理加上异地存放策略，两者共同构成了数据容灾的根基，也是保证电力业务连续性的生命线。

（三）恢复演练与验证

仅有备份数据、恢复计划是不够的，还要进行恢复演练以检验恢复计划是否可行、有效。灾难恢复演练是对备份数据完整性的检验、对恢复流程是否正确的检验、对技术方案是否可行的检验、对运维团队应急响应能力的检验。未经演练的恢复预案就如同一个没有实战经验的指挥员，在真正的紧急情况下很容易出现疏漏。

恢复演练分不同的层次，由最简单的桌面推演或者叫沙盘推演到最高级别的模拟演练。桌面推演以会议形式组织有关人员，按照预设的灾难情景进行理论上的应急响应演练，目的在于找出预案中明显的逻辑缺陷或者职责不清等缺陷。模拟演练又进一步，在一个与生产环境隔离的测试环境中，使用备份数据真实地启动系统和应用，完整地执行一次恢复过程，检验恢复时间目标和恢复点目标是否可以达到。通过演练可以找出技术实现上存在的潜在问题，操作手册存在的不合理之处，人员技能上的不足。

演练结束之后，必须对全过程展开复盘总结，从中提炼出成功的经验和失败的教训，进而据此修订并完善灾难恢复预案，由此形成一个持续改进的闭环。只有经常开展模拟实战的恢复演练，才能在真正灾难来临时临危不惧、迅速恢复业务、保证工作正常开展。

第四节 应急响应机制

电力信息系统属于国家重要的信息基础设施，它的安全稳定运行关系到国计民生。因此，建立和完善起来的应急响应机制，是电力系统在应对网络攻击、系统故障等各种安全事件时，及时应对、妥善处理、快速恢复的最后一道坚固防线，对于保障电力供应的连续性、可靠性具有不可替代的战略意义。

一、应急响应组织与职责

成熟的应急响应体系，核心就是应急响应组织机构的建立和应急响应职责的明确。可以保证在混乱的危机情况下各项工作的有条不紊地开展，有效防止由于权责不明而造成的响应延误或者决策失误，为高效处理安全事件提供强有力的组织保障。

（一）应急响应小组组建

电力企业应急响应小组的创建，属于应急响应能力建设中的关键部分。该小组可以是常设或虚拟的，专门负责处理安全事件，是企业应对网络安全威胁的指挥中心和执行单位。由于电力信息系统既有信息技术又有操作技术的双重复杂性，所以小组成员的组成要体现出专业性与综合性，从而达到跨领域知识相互补充、能力相互促进的目的。

典型的电力应急响应小组应当包括一些重要的职位。组长一般为信息化或安全生产主管领导，重大事件时起决策、调配资源的作用。技术分析骨干是团队的主力，必须精通网络攻防、恶意代码分析、数字取证、系统加固等技术，可以对攻击行为做深入的分析。协调联络岗负责公司内部各个部门之间的信息传递和与外部监管机构、合作伙伴、执法机关等机构之间沟通交流，保证信息传递的准确性和效率。小组应包含生产运行、调度控制、法律合规和公共关系等相关部门的代表，保证应急处置方案从业务影响、法律风险、舆论导向等多个角度进行考虑。

队员要随时做好全天候的备战状态来应对一切突发事件。

（二）应急响应流程与预案

标准化的应急响应流程以及高可操作的应急预案，都是应急响应小组按部就班工作的指导性文件。流程就是指对事件从开始到结束整个过程的组织管理，预案是对某种情况的处理提供具体指导的方案。两者互相配合，一起形成起一套从战略到战术的完整应对体系，保证在紧急情况下可以快速反应，妥善处理。

应急响应流程大致遵循国际通行的六阶段模型，即准备、检测、分析、遏制、根除、恢复，结合电力行业实际情况进行改进。准备阶段属于日常工作，主要工作为风险评估、制定策略、布置工具、培训人员。检测与分析阶段对应事件发现、研判。遏制、根除、恢复是事件处置的主要过程，目的是控制影响范围，清除威胁源，使系统恢复正常运行。最后一个阶段为事后总结，通过复盘实现持续改进。这样的流程就保证了每个事件都能够闭环。

应急预案则是流程的具体化和情景化体现。电力企业需要制定一套分层分类的预案体系：

1. 综合性预案： 宏观指导全公司的应急响应工作，明确总体原则、组织架构和通用流程。

2. 专项预案，对某一种类别的安全事件如勒索软件攻击、DDoS 攻击、数据泄露、调度主站系统异常等给出具体的处置步骤和技术手段。

3. 现场处置方案，即针对某一个系统或者物理场所的应急操作卡，具有很强的细节性、可操作性，供一线人员直接使用。

预案内容应明确规定事件启动条件、响应等级、处置方法、报告途径、恢复目标、终止标准，并且随技术环境及威胁态势的变化定期评审、更新。

（三）应急演练与培训

纸面上的预案、流程，只有经过反复演练，长时间的训练之后，才会变成团队的能力。应急演练是检验预案是否有效的最好途径，也是磨合团队合作、发现问题的最好方式；培训是保证团队成员能够胜任其职责的基础。两者互相促进、共同提高应急响应的实战能力。

应急演练的形式很多，根据目标、资源的不同来选用最适合的方式。桌面推演是最基本的一种形式，参演人员在会议室里针对预案，就虚拟的事件场景展开口头上的讨论和决策推演，主要是检验流程是否合理，决策是否正确。功能性演

练会更进一步，对应急响应的某一个具体环节或者功能进行实际测试，比如测试备用系统切换流程、数据恢复的实际耗时等。最高等级的就是全实景模拟演练，尽可能模拟一个完整的网络攻击事件，在压力之下测试团队综合应对的能力，比如模拟针对变电站监控系统的攻击来检查 IT 到 OT 跨域协同响应的能力。演练结束后必须进行详细的评估，并形成报告，把发现的问题及时反馈给预案和流程的修订。

人员培训是保证应急响应能力一直保持先进的办法。培训内容应该包括技术和管理两大部分。技术培训主要是针对最新的攻击手段、防御技术、取证工具的使用、恶意代码分析等，保证技术人员可以跟上威胁发展的步伐。管理培训主要是对管理者应急指挥、决策方法、沟通协调、媒体应对、法律法规等进行学习，提升管理者的领导能力。培训不能是一次性的，而应该形成常态化的培训机制，用内部知识分享、外部专业培训、认证考试等方式打造出一支学习型、专业化应急响应队伍。

二、安全事件处置流程

规范、明确的安全事件处理流程是保证应急响应机制有效运作的重要条件。它把应急响应由被动的、混乱的“救火”行动，变成标准化的、可重复的、高效的作业程序，最大限度地缩短响应时间、减少损失，从中吸取教训，不断改进安全防护体系。

（一）事件发现与报告

事件的及时发现和准确报告是应急响应的起点，它的好坏直接影响到后面处理的效果。电力信息系统广袤且繁杂，想要在其中构建起一个多维全面的事件监测网络，并形成一条畅通无阻的报告通道，这是赢得应急处置“黄金时间”的保障。

事件发现依靠的是技术以及人员这两方面。技术方面要部署和整合入侵检测系统、安全信息与事件管理系统、终端检测和响应系统、网络流量分析系统等安全监控工具。依靠对网络流量进行实时监测，对系统日志做深入的分析，对异常行为做精确的检测，从而自动发现潜在的安全威胁并向管理员发出警告。在电力监控系统等特殊环境下还要部署工业控制协议的异常检测技术。在人员上要加强全体人员的安全意识，使其能识别钓鱼邮件、异常弹窗等常见的威胁，并知道发现可疑情况应该怎样报告。外部情报，即安全厂商威胁通告、行业信息共享平台

预警等，也可以是发现事件的来源。

报告流程设计要突出简单迅速。企业应该有唯一并且易于知晓的安全事件报告接口，例如专门的邮箱、电话或者内部工单系统。报告模板要清楚写明报告中必须包含的主要内容，例如发现的时间、现象、涉及的系统或者资产、估计影响范围以及报告人的联系方式等等。不同等级的事件要有不同的上报时限和上报路径。尤其对于牵涉到电力生产安全的事件，必须要开辟一条直达应急响应小组和高级管理层的应急信息传递“绿色通道”，保证信息畅通无阻，为快速做出决策、调配资源创造条件。

（二）事件分析与研判

应急响应小组接到事件报告后应当立即行动，对事件进行分析、判断。这一阶段的任务就是去伪存真，核实事件是否真实发生，判断事件的性质和严重程度，努力还原攻击的攻击链路，找到攻击的源头，为制定有效的遏制和恢复对策提供决策支持。

事件分析是技术性很强的一种侦探工作。分析人员首先要对告警或者报告进行初步验证，排除误报。如果认定是真实的事件，就要立刻开始收集证据。从受到影响的服务器、网络设备、终端收集系统日志、应用日志、内存镜像、磁盘镜像、网络抓包数据。在电力生产控制大区取证时要格外小心，操作必须符合规定，首先要保证业务的连续性，防止因取证造成二次故障。

获取到证据后就是分析，分析人员利用取证工具、分析平台对收集到的数据进行关联分析。核心任务就是回答三个问题：攻击者是如何进入系统的（攻击入口）？使用了何种工具和技术（攻击手段）？哪些资产被攻陷（影响范围），攻击者的目的是什么（窃取数据、破坏系统、长期潜伏）？从这些问题的答案出发，把事件分成一般、较大、重大、特别重大这四个等级。研判的结果会直接决定启动什么样的应急预案、调用什么样的应急资源以及向管理层和监管部门报告的内容。

（三）应急处置与恢复

应急处置和恢复是整个流程中最关键、最困难的一个步骤，直接关系到能不能控制住事态，清除威胁以及业务的恢复程度。这一阶段环环相扣，包含遏制、根除、恢复这三个重要步骤，保证电力系统安全稳定之后再果断、审慎地做每一件事。

遏制是应急处置的第一要务，它的目的就是“止损”，即阻止事件影响蔓延。根据事件分析的结果，响应小组要立即采取隔离措施。防火墙屏蔽恶意 IP 地址、切断被感染主机的网络连接、隔离存在漏洞的网段、必要时关闭非核心业务系统。所有的隔离操作都必须严格通过风险评价和审批程序，优先选择主备通道不发生影响、不影响系统安全稳定运行的处理方法，即逻辑隔离而不是物理隔离。

根除阶段的主要目的就是彻底清除系统中的安全隐患，防止其死灰复燃。根据分析阶段的发现，正确清除恶意软件，删除攻击者留下的后门，修复被利用的系统漏洞，重置所有泄露或者被猜中的账户密码。对于不能确定是否被彻底清除的系统来说，最稳妥的办法就是重新安装系统。在根除之后，需要验证清除的效果，保证威胁已经被完全清除。恢复阶段是环境安全确定以后，把业务系统和服务的状态恢复成正常的状态。一般是从可信的备份中恢复数据以及系统配置。恢复之后要有一段强化的观察期，仔细留意系统的举动。经过业务部门确认服务已经完全正常之后，应急响应才算完成一个重要里程碑。

（四）事件总结与改进

应急响应的闭环不是业务恢复之后就结束的，在事件总结和改进中才得以持续。这是一个宝贵的学习过程，目的就是把每次代价昂贵的实战经验转化为组织安全能力的不断改进。这要求对于防护体系、响应流程、团队能力等各方面的内容进行全面系统的复盘、反思，找出短板并且提出切实可行的改进措施。

事件处理完毕后，应急响应小组要在规定时间内组织召开总结复盘会议，所有参与者都应该一同回顾事件处理的全过程。会议的主要任务就是对事件的根本原因进行一次“无指责”的根本原因分析，也就是从技术、管理流程、人员意识等各方面寻找事件发生的根源。并且，对应急响应过程中的得与失做出全面的评判，好的经验固化成标准，不足的地方，比如预案不适用、工具不趁手、协调不畅等等问题，都要暴露出来并加以解决。

复盘的结果就是一份完整的《安全事件总结报告》。该报告不但是事件的详细记录，也是改良的行动指南。报告中要包括时间线、影响分析、根本原因分析、处置过程评价、最重要的改进建议清单。这些建议要具体，可衡量，可执行，还要有负责的部门和完成的时间。建议可以是给某类服务器装上终端检测与响应系统，修订勒索软件应急预案，搞一次钓鱼邮件演练等等。经由创建针对改进建议的追踪和核实体系，保证每一次事件所带来的教训能够真实地转变成更为坚固的

防范举措，塑造起一个不断自我进化并完善的防护安全闭环。

三、应急响应工具与资源

正所谓“工欲善其事，必先利其器”。除了专门队伍、规范流程之外，事前准备好的、种类齐全的工具箱和畅通的信息沟通、对外联络渠道一起构成应急响应能力的“军火库”，是保证应急响应小组能够及时准确地完成各项工作的物质基础。

（一）应急响应工具包

应急响应工具包，也就是在处置突发事件时可以随时使用的“武器库”。它是一套事先筛选、配置、打包好的软硬件组合，可以应对不同的安全事件和分析任务。建立标准化工具包，可以很大程度上提高现场处置效率，避免紧急情况下到处找、下载工具，浪费宝贵时间。

工具包应该包含所有应急响应过程，有 Windows 系统的不同版本、Linux 系统的不同版本以及工控系统。各种应急响应工具及功能见下表。

应急响应工具类型及其功能

工具类别	主要功能	示例工具类型
分析取证类	收集并分析数字证据，还原事件真相	磁盘 / 内存镜像工具、专业数字取证平台、主机信息收集工具集
网络监控类	捕获并分析网络流量，发现异常通信	网络抓包分析工具、命令行流量分析工具
恶意代码分析类	对可疑文件进行静态 / 动态分析，识别恶意行为	静态分析工具、动态沙箱系统
安全加固与恢复类	修复系统漏洞，强化安全配置，恢复业务运行	漏洞扫描工具、补丁管理工具、数据备份 / 恢复软件

这些工具要存在专用的安全加固便携式硬盘或者笔记本电脑之中，定时更新病毒库以及软件版本，保证随时可用且自身安全。

（二）安全信息共享平台

信息在现代的网络攻防斗争当中是生命线。创建和使用安全信息共享平台，对克服信息孤岛、实现协同防御有十分重要的作用。既包含企业内部进行事件管理、知识积累的平台，也包含与行业内外交换威胁情报的外部平台。

内部应急响应平台就是事件处置的协同作战中心。可以把来自各个监控系统产生的告警、人工报告的事件、分析过程中产出的证据和发现、处置过程中的每

一步操作记录、团队成员之间讨论交流等所有信息都集中到一起。既可以给当前事件处置提供统一的作战视图，避免信息混杂、遗漏，又能方便以后审计复盘。从长远看，这个平台会逐渐形成一份宝贵的企业内部安全知识库，里面包含过去的事件案例、分析报告、解决办法等，给以后类似事件的处理提供宝贵的参考。

外部信息共享，就是把企业的防御视野从内部扩张到整个行业，再扩大到全网。电力行业属于关键的基础设施，参加国家级、行业级的网络安全信息共享分析中心很重要。企业可以经由上述平台及时获取有关电力行业新型攻击手段、恶意样本、失陷指标等高价值威胁信息，进而做到有的放矢地开展预警和防护工作。当自身受到攻击时，在保证敏感信息脱敏的前提下，将相关情报分享出去，帮助其它同业单位避免受到同样的攻击，形成一种“我为人人、人人为我”的集体防御局面。

（三）外部支持与协作

即使大型电力企业一般都会设有专门的内部安全队伍，但是当面对技术上比较复杂、规模较大的安全事件时，内部资源仍然会感到心有余而力不足。因此建立一个稳定可靠、互相支持、互相协作的外部支持网络，就成为应急响应能力体系的一个重要补充和保障。

和专业的第三方安全服务商建立合作关系，是获得外部帮助最直接、最有效的方法。这包括与外部专家团队签订应急响应服务合同，保证重大事件发生时可以及时得到外援支持。这些专家一般拥有更多的实战经历以及更新颖的分析工具，能够帮助解决一些较为棘手的攻击问题，如对高级持续性威胁攻击进行追查，对复杂的恶意软件执行逆向分析等。与外部服务商合作应在平时就建立起来，用共同演练等方式进行磨合，以保证战时能够无缝对接。

除了商业合作之外，同政府监管部门、执法部门的合作也是必不可少的。电力行业网络安全被提升到国家层面的重视。发生重大及以上级别网络安全事件时，企业应当按照有关法律法规的规定，及时向国家或者地方的网信部门、能源主管部门和公安机关报告。保持同这些机构日常沟通渠道的畅通，知晓报告要求和流程，利于事件发生时依照规定，有条不紊地对外发布。网络犯罪的配合公安机关工作、提供线索、提供证据既是一种法律责任，又可以有效地打击网络犯罪，净化网络环境。这样一种合作使得企业一旦发生安全事件就不再是孤军奋战，而是有国家的帮助和庇护。

第九章 电力信息系统标准规范

电力信息系统是保障电力工业安全、稳定、高效运行的中枢神经，它的建设与实践必须以完备的标准规范体系为基础。这些标准规范是系统设计、开发、运维、废止全生命周期的重要遵循，也是保障电力网络安全、数据安全、软件质量的基础。本章主要对与电力信息系统建设相关联的国家法律、法规和技术标准进行整理，为行业合规性建设以及技术实践提供方向。

第一节 国家标准要求

国家制定的各种法律、技术标准都是电力信息系统建设必须遵循的最高级规范和行为规范。涉及网络安全、数据安全、软件工程等诸多方面，既有宏观的法律体系，又有具体的、技术性的规范，为电力关键信息基础设施的稳定运行、电力数据资源的合理利用、信息系统软件质量的提高打下了良好的制度和技术基础。

一、网络安全法相关要求

中华人民共和国网络安全法属于我国网络安全领域的一部基本性法律，它是我国电力信息系统安全建设、运营的根本性法律依据。它就网络运营者应当享有的安全保护权利做出全面规定，就涉及电力等重要的行业提出更为严格、具体的安全要求，目的在于打造一个稳定而可控的网络环境，从而有效应对不断升级的网络安全风险。

（一）网络安全等级保护制度

网络安全等级保护制度是我国网络安全的一项基本国策，也是《网络安全法》的重要内容。该制度规定，网络运营者应当根据信息系统的地位、作用及其被破坏、失去功能或者数据泄露之后所造成的危害程度，把信息系统分为五级安全保护等级，采取相应的安全保护措施。

对于电力行业来说，有着非常重要的现实意义。电力调度系统、变电站监控

系统、发电厂控制系统等对电网安全稳定运行、电力可靠供应起关键作用的系统，一般属于第三级或者更高级别。电力企业是责任主体，在系统规划设计阶段要确定自身的安全保护等级，并且通过专家评审，采取一个中心、三重防护的纵深防御理念，同步规划、建设、使用安全技术和管理措施。

等级保护的实施过程是循环的过程，定级、备案、建设整改、等级测评、监督检查等过程。电力企业要定时委托有资质的测评机构实施安全等级测评，发现安全隐患和不足之处马上加以改正。国家能源局及其派出机构会不定期对电力企业，尤其是经营第三级以上网络的电力企业实施抽查，保证等级保护工作得到真正有效的执行。

（二）关键信息基础设施安全保护

电力行业属于关系到国计民生、国家能源安全的重点行业，被明确规定为网络安全法所规定的重点保护对象关键信息基础设施。关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融等行业和领域中，一旦遭到破坏、丧失功能或者数据泄露，会严重危害国家安全、国计民生、公共利益的系统和设施。电力监控系统及其运行所依赖的通信网络设施，无外乎是 CII 的典型存在。

国家把 CII 当作重点保护对象，在网络安全等级保护制度上提出更高的安全要求。电力企业作为 CII 的运营者，除了要履行一般网络安全保护义务外，还需要承担特殊的网络安全保护责任，如设置专门的安全管理机构，确定负责人，对负责人以及关键岗位人员进行安全背景审查。运营者应当自行或者委托有资质的单位，每年至少进行一次网络安全检测和风险评估，发现安全隐患的应当及时排除，并向主管单位报告。

法律对网络产品和服务的采购也有规定。如果采购的产品或者服务会对国家安全造成影响，就需要经过国家网络安全审查办公室组织的安全审查。原则上法律规定 CII 运营者在中国境内运营中收集、产生个人信息和重要数据应当在境内存储，确需向境外提供的，应当进行安全评估。这些规定目的在于从源头控制风险，打造出一道坚不可摧的安全屏障，保证作为国家命脉的电力信息系统绝对安全。

（三）个人信息与重要数据保护

随着电力营销业务、客户服务和智能电网应用的不断发展，电力信息系统所处理的信息量及重要数据量越来越大，其安全保护工作也愈加重要。该法就这一问题作出了清楚严格的限定，给电力行业数据处理活动划出了明确的法律红线，

目的在于守护公民权益，保障国家安全和社会公共利益。

对个人信息的处理来说，法律规定的是“合法、正当、必要”的原则。电力企业在收集、使用用户信息（如姓名、身份证号、用电量、联系方式等）的时候，应该告诉用户自己收集、使用信息的目的、方式、范围，取得用户的同意。企业应当采取技术和其它必要的措施，保证所收集的个人信息安全，防止信息泄露、损毁、丢失。出现或者可能出现信息泄露等异常的情况时，应当立即采取补救措施，按相关规定及时向用户和有关部门报告。

对于重要数据的保护是站在国家和公共利益的角度上进行保护。重要数据一般是指一旦被篡改、破坏、泄露或者非法使用，就会对国家安全、公共利益造成危害的数据。在电力行业里，这可能是电网运行方式、发输变电设备的重要运行参数、跨区域电力交易数据之类的东西。法律给关键信息基础设施运营者实行了严格的保护，还规定了数据出境安全评估办法，给跨国能源合作、数据交流定下了合规性标准。电力企业要建立内部数据保护制度，规定数据的操作权限与流程，保证重要的数据不会被滥用或者非法外流。

二、数据安全法相关要求

中华人民共和国数据安全法的颁布和实行，是我国数据治理进入新的发展阶段。该法以更高的角度去统筹数据发展和安全的关系，并制定了若干个基本制度。对于数据密集型行业来说，该法既是行为底线，又是重要的指引，是行业用好数据资源、推进数字化转型、实现高质量发展的行动指南。

（一）数据安全与发展并重

数据安全法规定，维护数据安全要坚持数据安全与开发利用并重，鼓励数据的合法合理有效利用。这对电力行业开展深度数字化转型有重要意义。智能电网、能源互联网、虚拟电厂等新业态的迅速崛起，都是以海量数据为基础，以数据为驱动。经过对发、输、变、配、用各个环节的数据进行深入挖掘、分析之后，可以实现源网荷储的精准协同、优化电网运行方式、提高供电可靠性和服务水平。

该原则提出，目的是打破以前因为担心安全问题而不敢用数据的局面，促使电力企业安全使用数据，探索数据的价值。企业应该制定完善的个人信息保护制度，运用先进技术手段对个人信息进行控制，保证电网安全、用户信息安全的同时最大程度地发挥数据作为生产要素的作用。这就要求电力信息系统建设不能只

重视防护，还要构建一个安全可靠、支持数据高效流通和深入应用的平台，为电力市场经营决策、新能源消纳预测、用户端精细化服务提供支持，从而提高整个能源体系的综合效能。

（二）数据分类分级保护制度

数据分类分级是进行数据安全精细化管理的基石性、决定性步骤，同时也是《数据安全法》中确立的一项基本法律制度。根据数据对经济社会发展的作用大小和数据被篡改、泄露或者非法使用所造成的危害程度的不同，将数据分为不同的等级，并采取相应的保护措施。实行该制度改变了过去“一刀切”的粗放型数据保护方式，使安全资源的投入更加有方向、经济。

电力行业数据种类繁多，价值及敏感程度也不相同。电网拓扑结构、实时运行状态的调度数据、宏观用电数据对国家经济运行分析意义重大，其重要性远大于一般的营销信息、设备台账数据。电力企业应当依据国家以及行业的指引标准，制订符合自身业务特征的数据分类分级体系。数据一般可以分为核心、重要、一般三个等级，也可以从业务领域、信息内容等角度进行分类。

对已完成分类分级并且形成了目录清单的数据，企业要实行不同的安全策略。核心数据、重要数据在数据采集、传输、存储、处理、共享、销毁整个生命周期内，应该用加密、脱敏、访问控制、安全审计等更为严格的技术手段和管理措施来保护。精细化管理途径可以有效保护重要数据资产，在保证安全的前提下使一般数据有序流动和分享，达到发展与安全之间的协调。

（三）数据安全风险评估

为了及时发现、处理数据安全风险，保证数据安全，《数据安全法》设置了数据安全风险评估制度。该制度要求重要的数据处理者要定期对其数据处理活动开展风险评估，并上报给有关主管部门。这样一种机制化的评价，是数据安全由被动防御到主动治理转变的一个重要环节，也是电力系统这一重要信息基础设施安全运行所必须的。

电力信息系统面临的风险有外部网络攻击、内部的人为误操作或者恶意行为、系统本身的技术漏洞等。数据安全风险评估要全面识别并剖析各类风险源，评判其出现的可能性，还要衡量其对数据机密性，完整性和可用性所造成的危害。评估内容一般包含数据安全管理制度的完备情况，技术防护手段的有效状况，数据处理流程的合法情况以及应急预案的可行情况等。

风险评价不仅要检验目前情况，而且应该可以促进持续改进。风险及薄弱环节进行评价之后，电力企业就要制订出整改方案并且落实好整改措施，以此构成评估、整改、再评估的循环。电网中一些重要的运行数据发生安全事件，会引发连锁反应，造成大面积停电事故。因此要建立完善的常态化的数据安全风险评估预警机制，预见并防范重大安全风险，保障电力系统安全稳定运行、公共利益安全有重大意义。

三、其他相关国家标准

除了基本法律框架外，电力信息系统建设、运行过程中相关技术标准也给具体操作指引、评价参照提供详细的方案。国家标准把法律的原则性要求转化成可以度量、可以执行的技术指标和管理流程，成为保证系统安全性和软件质量的基础。其中最具有代表性的就是信息安全技术网络安全等级保护基本要求、信息技术软件工程质量要求。

电力信息系统重要国家标准概览

标准类别	标准名称	核心内容	在电力行业中的应用
网络安全	GB/T 22239 信息安全技术 网络安全等级保护基本要求	规定了网络安全等级保护的技术要求和管理要求，涵盖物理环境、通信网络、区域边界、计算环境、安全管理中心等五个技术方面，以及管理制度、机构、人员、建设管理、运维管理等五个管理方面。	为电力信息系统（如调度、生产控制、管理信息系统等）定级、建设、测评提供技术和管理规范，确保系统具备与其重要性相符的安全防护能力。
软件工程	GB/T 8566 信息技术 软件工程质量要求	详细规定了软件生命周期各阶段（需求分析、设计、编码、测试、安装、验收和维护）的活动内容、实施方法及应产出的文档制品，强调过程控制以保障软件质量。	指导电力调度自动化、能量管理系统等关键应用软件的开发与管理，确保软件高可靠性、高实时性，降低缺陷率，提升系统整体质量和可维护性。
数据安全	GB/T 35273 信息安全技术 个人信息安全规范	规定了个人信息收集、存储、使用、共享、转让、公开披露、删除等环节的安全要求，以及个人信息主体权利保障等内容。	指导电力企业在客户服务、营销业务等环节中，合法合规地处理用户个人信息，保护用户隐私，防范数据泄露风险。

续表

标准类别	标准名称	核心内容	在电力行业中的应用
数据安全	GB/T 37988 信息安全技术 数据安全能力成熟度模型	提供了数据安全能力建设和评估的框架，帮助组织识别当前数据安全水平，规划提升路径。	帮助电力企业系统评估自身数据安全管理现状，制定数据安全建设路线图，持续提升数据安全防护和治理能力。
信息分类	GB/T 38667 信息安全技术 网络安全数据分类分级指南	提供了数据分类分级的原则、方法和流程，帮助组织建立数据分类分级体系。	指导电力企业对电网运行、客户信息、内部管理等各类数据进行科学分类分级，并实施差异化的安全保护策略，实现精细化管理。

（一）信息安全技术 网络安全等级保护基本要求

《信息安全技术网络安全等级保护基本要求》是国家网络安全等级保护制度推行的主要技术标准，也是各行业信息系统安全创建和监管的指导文件。此标准对从一级到四级的安全保护等级对象的安全通用要求、安全扩展要求做了详细的说明，给电力信息系统的安全建设提供技术参考。

该标准将安全要求分为技术和管理两大类，体现了技术与管理并重、纵深防御的综合防护思想。

1. 技术要求包含五个方面，分别是安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心。对于电力监控系统而言，就是按照生产控制区、管理信息区等各个安全分区所具有的安全需求，严格实行网络隔离措施，布置防火墙和入侵检测系统，加强主机和应用的安全配置，建立统一的安全管理平台来实现集中监控和审计。

2. 管理要求包括安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理这五部分。这就需要电力企业建立健全、科学严谨、严格控制的完整安全体系，明确各个层级单位、人员的安全职责，对系统建设、运行过程严格控制，实行严格控制、变更控制、漏洞管理、应急演练等一系列活动，保证安全措施的持续有效性。

GB/T 22239 标准根据不同的安全保护等级，对于每一个控制点都提出了不同的要求强度。等级越高要求就越严格、越细致。电力企业信息系统建设过程中要对照相应等级要求逐项落实安全措施，系统建成之后通过等级测评来验证其符合性，从而保证系统具有与其重要性相适应的安全防护能力。

（二）信息技术 软件工程 质量要求

《信息技术软件工程质量要求》（GB/T8566）是指导软件开发及项目管理的国家标准，采用了国际上先进的软件工程理论和方法，对软件产品实行全过程控制，从而保证软件质量。特别是调度自动化、能量管理系统等重要的应用软件系统规模庞大，逻辑十分复杂，可靠性与实时性的要求很高。任何一点软件上的疏漏都会造成严重的结果。因此按照此标准提高电力软件的质量就显得十分重要。

该标准对软件生命周期的全过程都作了规定，即需求分析、设计、编码、测试、安装、验收、维护等各个阶段的活动内容、实施方法、产出文档制品均有明确要求。需求分析阶段需要清晰、完整的给出系统功能和非功能需求，得到用户确认；设计阶段要对系统架构、模块接口做详细的设计；测试阶段要制定出周密的测试计划，包括单元测试、集成测试、系统测试等各个方面，充分发现并解决软件存在的各种问题。

按照 GB/T 8566 标准操作，可以改善电力信息系统建设过程中软件开发流程的正规化、透明度，减少由于需求不明、设计不合理、测试不充分等原因造成的返工、质量问题。规范的文档管理能够使软件具有良好的可维护性、可追溯性，方便以后对系统进行升级、增加新的功能。把软件工程的质量需求融入到项目管理的各个流程当中，这是形成安全、可靠、高效的电力信息系统的软件的基本保障。

第二节 行业标准规范

电力信息系统的建立和发展不能缺少统一完备的标准规范体系。这是保证系统安全稳定运行、实现信息互联互通、引领技术创新发展的基本要求，也给整个行业的数字化转型提供重要的技术指导和制度保障，对系统从设计到运维全生命周期给出明确指导。

一、电力行业网络安全标准

信息技术与电力系统深度融合之后，网络安全成为电力行业必须面对的严峻问题，其重要性也越来越明显。为了建立一个坚固的安全防线，国家以及行业主管部门制订了一系列有针对性的网络安全标准，并构建了一个包含管理、技术、运行等各个方面的多层次的防护体系。

（一）电力监控系统安全防护规定

《电力监控系统安全防护规定》属于保障电力系统安全运转的指导性文件，对于直接控制或者影响电力生产环节的全部监控系统，提出了完整的防护标准。该规定是由国家发展和改革委员会发布，由国家能源局负责监督执行，目的是有效地防范内部和外部的网络攻击、非法入侵、数据泄露等安全事件的发生，保证电力监控系统可以抵御已知和未知的安全威胁，保证电力系统的安全稳定运行。

其核心就是确定了“安全分区、网络专用、横向隔离、纵向认证”的十六字方针。安全分区要求对电力监控系统按照业务功能划分成不同的安全区域，如生产控制大区、管理信息大区等，确定各个安全区域之间安全边界。网络专用指生产控制大区的网络物理上或者逻辑上要与外部公共网络、企业内部管理网络完全隔离。横向隔离指的是在生产控制大区内部，不同的业务子系统之间也要进行隔离，防止安全事件横向传播。纵向认证是在生产控制大区和管理信息大区之间建立经过认证、访问控制的通道，一般采用“正向隔离”和“反向隔离”装置实现数据的单向或可控传输。

除了宏观的安全架构原则之外，该规定还对安全防护所用的技术和管理的细节做出了具体的规定。技术上包含物理安全、网络安全、主机安全、应用安全、数据安全等各个方面，例如关键设备放置于具有访问控制的机房中；在网络边界部署防火墙和入侵检测系统；对主机系统进行安全加固并安装防病毒软件；对重要数据执行加密和备份操作。从管理上讲，应该建立完善的安全生产制度，明确安全生产责任，定期开展风险评估，制定应急预案并进行演练，加强安全生产人员的培训和背景调查等，形成技术与管理相辅相成的纵深防御体系。

（二）电力行业网络与信息安全管理办法

《电力行业网络与信息安全管理办法》属于电力行业网络安全领域的关键综合性管理规范，重点在于从组织、制度、流程等角度创建系统的安全管理体系。明确电力企业各层次组织、人员网络与信息安全工作的职责和义务，以规范化的工作活动，保证安全责任落实到实处，实现对网络安全风险常态化、制度化管理。

本办法突出网络安全工作全周期的管理思想。它要电力企业创建并推行完备的网络安全体系，囊括从规划，创建，运作到废止的全部过程。具体有：

1. 安全责任体系：企业主要负责人是网络安全的第一责任人，设置专门的网络安全管理机构或者岗位，逐级分解落实安全责任。

2. 风险控制机制，定期进行网络与信息安全风险评价，找到系统所面临的一切内外部威胁和自身的弱点，并根据评价结果来制订和执行风险处理方案。

3. 监测预警与应急处置，建立网络安全监测预警体系，做到及时发现网络安全威胁和事件。并且要制定详细的应急预案，确定应急组织、处置流程和资源保障，经常开展应急演练，提高应急响应与恢复能力。

4. 监督检查和持续改进，建立常态化监督检查机制，采取自查和上级检查相结合的方式，对各项安全管理制度落实情况进行监督检查。依据检查的结果以及安全事件分析来持续改进安全策略及管理流程，形成闭环管理。

该办法一出，使电力企业的网络安全工作由原来的“救火式”的被动应对，变为以风险为出发点的、以预防为主导的、主动的管理模式，安全防护渗透到业务流程的方方面面，极大地提高了整个行业网络安全的成熟度以及综合防御能力。

（三）电力行业信息系统安全等级保护基本要求

国家信息安全等级保护制度在电力行业的具体化、深化化实践就是《电力行业信息系统安全等级保护基本要求》。根据信息系统在国家安全、经济建设、社会生活中的重要程度，以及系统一旦遭到破坏，对国家安全、社会秩序、公共利益、公民、法人及其他组织的合法权益造成的危害程度，将电力信息系统划分为不同的安全保护等级，对不同等级提出不同的安全要求。

该标准的主要思想是建立定级、备案、建设整改、等级测评、监督检查的闭环管理流程。电力企业应当组织专家对本单位的信息系统进行科学的定级，电网调度自动化系统（SCADA/EMS）一般定为第三级或者以上，一般的办公自动化系统定为第二级。定级之后需要向公安机关和行业主管部门备案。企业应按照相应的等级安全要求进行系统建设或者安全整改，安全要求分为技术类和管理类。技术要求包括物理环境、网络通信、设备计算、应用数据等各个方面，管理要求包括安全策略、机构人员、建设运行、应急响应等各个方面。建设整改完毕后，由企业自行或者委托有资质的测评机构进行等级测评，验证系统是否达到相应等级的保护要求。最后，监管部门将就等级保护工作开展情况实行长期的监督和检查。

各个安全等级之间要求大相径庭。第二级系统可以抵御外部小规模、弱强度的恶意攻击；第三级系统在统一的安全策略下可以抵御有组织、较强度的恶意攻击，在系统受到破坏之后可以很快恢复功能；而第四级系统需要抵御国家级别的、

有组织的、高强度的恶意攻击。各个不同等级的保护要求见下表。

电力信息系统安全保护等级主要特征

等级	典型威胁应对能力	恢复能力
二级	抵御外部小规模、弱强度恶意攻击	具备基本恢复能力
三级	抵御有组织、较强度恶意攻击	系统受损后可较快恢复
四级	抵御国家级别、高强度恶意攻击	具备快速、全面恢复能力

电力行业依靠等级保护，可以将有限的安全资源集中到最需要的地方，重点保护最重要的信息系统，从而对核心业务系统进行重点防护，形成主次分明、重点突出的差别化安全保障体系，有力应对日益复杂的网络安全威胁。

二、电力行业信息化标准

在保证安全的基础上，电力行业信息化的主要目的就是实现数据的高速流动和充分挖掘，从而消除长久以来的“信息孤岛”现象。为此，行业制定了信息化标准来统一数据模型、接口协议、业务流程，为企业级信息平台的搭建打下基础。

（一）电力企业信息集成规范

电力企业信息集成规范，是为了打破电力企业内部各个信息系统之间数据壁垒、应用孤岛而制定的重要标准。本规范参考 SOA 思想，通过建立统一的技术框架、数据标准和集成模式来达到企业内部发电、输电、变电、配电、用电、调度等各个业务环节的信息系统互联互通、高效协同。

其主要目的就是创建以企业服务总线为核心的集成平台。企业服务总线就像信息交换的“中央高速公路”，给所有接入系统的应用提供统一的服务注册、发现、路由、转换和调用能力。各个业务系统（生产管理系统、营销管理系统、财务管理系统等）不需要进行复杂的点对点连接，而是通过统一适配器将自身数据和服务发布到企业服务总线上，并可以从总线中订阅其他系统所提供的服务。松耦合架构大大简化了系统集成，降低了成本，使系统具有很高的灵活性、扩展性。

规范的另一部分就是主数据管理。主数据是企业在内部分享的各个部门、各个系统的核心业务实体数据，例如电网设备台账、客户信息、组织机构、员工信息等等。规范要求建立统一的主数据标准和管理平台，保证企业内部各部数据的一致性、准确性、唯一性，从源头上解决由于数据标准不统一造成的企业内部各部数据冗余、不一致、集成困难等问题。推行信息集成规范，目的在于消除电力

企业数据流动的障碍，达成各业务部门流程上的协同以及数据的高效利用。

（二）电力系统数据交换协议

电力系统数据交换协议用来规范电力信息系统之间怎样准确、高效、可靠地传递信息，是各个系统互操作的基础。协议对数据格式、传输方式、通信流程、检验方法等作出规定。电力行业的数据交换协议根据应用场合可以分为两类：一类是面向实时监控的协议，另一类是非实时信息交换协议。

就实时监控而言，在 IEC 制定的 IEC 60870 系列协议里，特别是 IEC 60870-5-101、IEC 60870-5-104 协议得到了广泛的应用。IEC 101 是以串行通信为基础的远动协议，早期调度中心和远动终端之间使用较多。它规定了平衡与非平衡两种传输方式，采用严格帧结构、链路控制和应用功能，在信道条件不好时仍能可靠地传输数据。IEC 104 是按照 TCP/IP 网络设计的版本，符合网络化的趋势，传输效率和灵活性都更好，现已成为新建、改造调度自动化系统的主要选择。协议对遥信、遥测、遥控、遥调等“四遥”信息报文结构、传输方式（如循环扫描、变化上送）、可靠传输等作出详细规定，保证调度中心能及时、正确地掌握厂站实时运行情况并发出控制命令。

就企业管理和系统集成而言，以公共信息模型以及可扩展标记语言为基石的交换协议正起到越来越大的作用。IEC 61970 标准定义了 EMS（能量管理系统）的应用程序接口，其中心就是 CIM，提供了一个描述电力系统网络模型和资产的标准化对象模型。IEC 61968 标准把 CIM 扩展到 DMS（配电管理系统）及其他企业信息系统接口上。利用 CIM 的 XML 文件交换，可以使不同厂商、不同类型的系统（电网模型分析软件、资产管理系统、客户关系管理系统等）之间，交换复杂的、结构化的电网模型数据以及业务数据，给高级应用、跨系统业务流程的实现提供强有力的数据交换能力。

（三）智能电网相关技术标准

智能电网是电力工业未来发展的主要方向，其建设依靠的是庞大的协同技术标准体系。智能电网有关的技术标准，涵盖发电、调度全流程，是促进信息技术和电力技术融合的工具，引导电网走向自动、信息和交互化的发展道路，提高电网的安全性、经济性、灵活性。

其中 IEC 61850 标准是智能变电站建设的重中之重，也是立身之本。它不只是一个通信协议，它还是一个完整的解决方案，给变电站内所有的智能电子设备

提供统一的数据模型、配置语言、通信服务。采用面向对象的数据建模，使 IEC 61850 的设备信息具有自描述性。其定义的 GOOSE（通用面向对象变电站事件）和 SV（采样值）报文可以利用变电站内局域网高速传输，与传统的硬接线相比，具有更好的保护和闭锁逻辑，更少的二次回路，更高的系统可靠性和灵活性。

用电侧的 AMI 标准把用户和电网连接在一起，成为一种高效、先进的交流方式。DL/T645 及以后的标准对智能电能表和数据采集终端之间通信协议作了规定，可以实现远程抄表、费率下发、负荷控制等。该标准可以支持大规模智能电表的部署，也给需求侧响应、分时电价、接入分布式能源等智能用电业务提供大量的细粒度数据。针对新能源并网、电动汽车充换电设施、微电网运行与控制等领域也出现了众多的技术标准，共同构成了智能电网发展的庞大标准体系，持续推动电网技术的创新和发展。

三、电力行业调度自动化标准

电网调度自动化是电网安全、稳定、经济运行的大脑和中枢神经，技术复杂性高，对可靠性要求极高。有关的标准规范从系统功能、运行管理、数据通信、设备术语等角度给出统一的技术依据和行为规范，给电网集中监控、优化调度、故障快速处理提供支持。

（一）电网调度自动化系统运行管理规程

电网调度自动化系统运行管理规程是指导各级电力调度中心日常运行、维护工作的一本操作手册、管理宪章。该规程意在凭借标准的流程和制度，保证调度自动化主站系统及其附属设备（服务器，网络设备，人机交互界面等）一直处在稳定，可靠，高效的运转状态当中，从而给调度员赋予准确的决策支撑。

规程对于调度自动化系统运行管理职责、工作制度、操作程序做了具体的规定。确定了系统运行、设备维护、软件管理、数据管理等岗位的职责，要求严格执行值班制度、操作票制度、工作许可制度，防止误操作。规程对系统日常监视和巡检作出具体规定，运行人员应定时查看主备机状况、数据库是否同步、网络流量、CPU 占用率等主要指标，仔细填写运行日志。系统维护方面对软硬件变更、设备检修、系统升级等高风险操作流程做出规定：必须制定详细的方案，并经过严格的审批之后，在非关键时段执行，从而将电网监控受到的影响降到最低。规程中还包含系统备份与恢复、应急处理等有关内容的规定，是保证调度中枢功能

连续性的制度保障。

（二）远动设备及系统术语

《远动设备及系统术语》标准的主要功能就是统一电力调度自动化领域的基本概念和专业术语，给行业内部的技术交流、标准制定、产品设计以及工程实践提供一个无歧义的通用语言环境。在复杂的系统当中，术语的清晰以及统一是避免产生混淆、保证准确交流的前提，对于系统的兼容性以及人员之间的合作效率有着非常重要的作用。

该标准对远动技术以及调度自动化系统中的主要术语做了权威的定义。明确的远动是指利用通信信道对远方的设备进行监视、控制的技术。在此基础上对最基本的四遥功能做了详细的说明，如下表所示：

远动系统“四遥”功能详解

功能	定义	示例
遥信	远程传输远端设备的状态量。	开关位置、保护信号、断路器跳闸指示
遥测	远程测量和传输远方设备的模拟量。	电压、电流、功率、频率
遥控	控制中心向远方设备发出离散控制指令。	断路器分闸 / 合闸、开关跳合
遥调	控制中心向远方设备发出模拟或脉冲式调节指令。	调节发电机有功出力、变压器分接头调节

除以上的基本功能外，标准中对使用在系统架构里的远动终端单元、调度中心主站系统、能量管理系统、配电管理系统等作出了明确的规定，同时也明确了各个系统的功能和相互关系，给行业内的人员建立一个清楚的知识体系。

（三）电力系统通信协议

电力系统通信协议就相当于调度自动化系统的神经网络，用来确定调度主站与遍布电网的远动终端和厂站自动化系统之间信息交互的规则。协议的可靠性、效率直接影响到调度中心对于全网的态势感知、精准控制的能力，是调度自动化系统安全稳定的生命线。

电力系统上 IEC 60870-5 系列成为主要的标准，是调度通信协议的基础。IEC 60870-5-101 协议（简称 IEC 101）是面向串行通信链路（租用专线、电力线载波）的，规定了平衡和非平衡两种传输方式，采用严格的帧结构、链路控制和应用功能，即使在信道条件不好时也能保证数据的可靠传输。随着网络技术的发展，以以太网和 TCP/IP 为基础的 IEC 60870-5-104 协议（以下简称 IEC 104）出

现了并迅速发展成为主流。直接把 IEC101 应用层的数据单元装到 TCP 报文里，借助现成的 TCP/IP 协议栈所提供的连接管理、纠错等特性，达成更有效也更灵活的网络化通信，支持更为繁杂的网络拓扑与冗余安排。

除 IEC101、IEC104 协议外，在调度自动化领域有新的协议技术不断加入其中来应对新出现的挑战。随着变电站内全面采用 IEC 61850 标准，调度主站与智能变电站之间也慢慢向着 IEC 61850 协议体系转变，从而实现从站内到主站的“无缝”数据建模和信息交互。由于网络安全威胁日趋严重，怎样提高传统远动协议的安全性也成了研究和应用的热点。对 IEC 104 协议外部加装 TLS 或 SSL 加密通道或者对协议本身的安全性进行研究，保证调度指令和电网数据的机密性、完整性、真实性。

第三节 技术标准体系

技术标准体系给电力信息系统的建设打下基础，在系统开发、集成、运维全过程之中对系统进行规范，保证系统之间的互操作性、安全性和可扩展性。健全统一的技术标准体系能有效地指导技术选型，规范开发行为，降低系统间的耦合度，大幅度提高整体投资效益。本节将对支撑电力信息系统建设的三大标准体系进行详细的阐述：基础技术标准、软件工程标准、通信接口标准。

一、信息技术基础标准

信息技术基础标准是任何信息系统的建立所遵循的最基本的技术规范，它给电力信息系统的硬件选择、软件创建和平台搭建提供了一个统一参照的标准。保证各个产品、技术在一个框架里相互配合，是实现系统开放性、可移植性的必要条件。其包含的内容有编程语言、数据库和操作系统等主要的技术领域。

（一）编程语言标准

电力信息系统软件资产的长期价值，不能缺少编程语言的标准化。按照国际或者国家标准的编程语言，比如已经被 ISO/IEC 标准化的 C++、Java 等，可以保证代码在不同平台之间的可移植性，减少对特定编译器或者开发环境的依赖，有利于开发团队的组建以及成员的培训。标准化的语言、规范化语法规则使得代码更容易被人理解，利于代码的阅读、修改。这在生命周期很长、业务逻辑复杂且

对可靠性要求很高的电网调度自动化系统、电力市场交易系统中就显得格外重要。

在电力企业级业务系统建设，尤其是在开发服务和互联网服务项目的时候，Java 语言由于具有强大的跨平台能力、成熟稳定的 JVM 技术以及庞大的活跃开源社区等优势，占据着主导地位。标准化推动了其生态的发展，可用来构建基于 Java 技术栈的大规模、高并发电力营销系统以及客户服务等系统。

对于实时性要求非常高的电力监控、保护控制等系统，由于 C/C++ 语言运行效率高、可以直接操作硬件，所以被广泛使用。安全关键系统对编码规范的要求更为严格，采用 MISRA C 标准可以减少程序中存在的问题，使代码更加安全可靠。随着人工智能、大数据技术在电力行业的发展，在数据科学领域有强大库支持的简洁易懂的 Python 语言，也开始成为电力负荷预测、设备状态评价等新领域中一种重要的语言。

（二）数据库语言标准

数据库是电力信息系统的核心，里面存有电网运行、企业经营、客户服务等大量的数据。数据库语言标准，对于数据的有效管理和共享起着保障作用。SQL（结构化查询语言）已经成为关系型数据库的标准，其标准由 ISO/IEC 9075 系列规范来定义。该标准详细规定了数据定义语言、数据操纵语言、数据控制语言、事务控制语言的语法和语义，为遵循此标准的关系型数据库管理系统（Oracle、MySQL、SQL Server 等）提供了一种通用的数据访问接口。

电力信息系统在设计之初如果能遵循 SQL 标准，那么应用系统与底层数据库之间就会保持松耦合。开发人员可以集中精力于业务逻辑上，而无需操心各个数据库之间语法上的差异，从而提升开发效率，并且保证数据互操作性。不同业务系统之间（生产管理系统和财务系统等）的数据交换和集成变得简单可靠，为未来数据库平台的迁移提供极大便利。近些年来，智能电网发展起来之后，大量的非结构化和半结构化数据，像智能电表采集的数据，设备故障录波数据之类，给数据处理带来了新的难题。因此非关系型数据库（NoSQL 数据库）应运而生，虽然它们所用的查询语言（例如 MongoDB 查询语言、CQL）并没有形成统一的国际标准，但是在各自领域中已经成为了事实上的标准，为电力大数据应用场景提供了灵活而高可扩展的解决方案。

（三）操作系统标准

操作系统是硬件和应用软件之间的纽带，它标准化的程度直接影响到电力信

息系统的稳定、安全以及应用生态的发展。POSIX 是操作系统领域最重要的标准之一，它规定了一套 C 语言应用程序接口，目的是提高应用程序在不同的操作系统之间可以互相移植。遵循 POSIX 标准的操作系统主要是各种 UNIX、Linux 发行版，给上层应用提供统一的运行环境，方便电力应用软件的开发和部署。

电力系统后台服务器和数据中心领域，以开源、稳定、安全、成本低为特点的 Linux 操作系统已经成为主流。Red Hat Enterprise Linux 或 CentOS 等发行版被用作调度中心、营销系统、企业资源规划等核心业务平台的操作系统。这些系统基本上都是兼容 POSIX 标准的，保证商业软件和开源软件可以正常运行。同时 Windows Server 操作系统具有用户友好的界面以及与微软生态系统的紧密集成等特点，在办公自动化、门户网站等场合下也有一定的应用。

对发电厂、变电站内嵌式控制设备以及实时监控系统来说，操作系统最根本的需求就是实时性、确定性。实时操作系统要保证任务在规定的时间内完成，对电网的安全稳定运行有着十分重要的意义。虽然实时操作系统领域并没有像通用操作系统那样有一个统一的标准，但是 VxWorks、QNX 等商用实时操作系统和 RT-Linux 等开源实时操作系统都是主要的选择方案，它们具有精确的任务调度、中断处理和低延迟通信的特点，为电力实时控制的应用提供了基础的支撑。

二、软件开发与文档标准

软件开发以及文档标准是保证电力信息系统项目质量，提高开发效率，减少维护成本的重要条件。它给软件生命周期的各个阶段提供明确的规范、统一的术语、客观的评价依据，是实现软件工程化管理、避免项目混乱、杜绝个人英雄主义式开发的重要制度保障，对保证电力系统这样大型复杂工程的成功具有重要意义。

（一）软件文档编制规范

软件文档是软件产品的重要组成部分，软件开发过程中涉及的思想、决策、设计、测试等信息都被记录在软件文档中，对团队协作、项目管理、质量保证、后期维护和升级都起着非常重要的作用。我国的 GB/T 8567-2006《计算机软件文档编制规范》是软件文档编写的主要国家标准，对软件生命周期各个阶段文档的类型、内容、格式做出详细的指导。

按照该规范编写的文档可以保证项目文档的完整性、一致性以及规范性。电

力信息系统项目实践过程中一般会编写如下重要文档：

1. 规划阶段、需求阶段产出《可行性研究报告》、《软件需求规格说明书》。《可行性研究报告》说明项目的目、范和益，《软件需求规格说明书》详述系统的全功能和非功能需求，是之后一切工作的根基。

2. 设计阶段：产生概要设计说明书和详细设计说明书。《概要设计说明书》描述系统的体系结构、模块划分、接口定义；《详细设计说明书》描述每一个模块内部的算法、数据结构、处理流程。对于数据密集型的系统还要编写《数据库设计说明书》。

3.3、实现与测试阶段：产出软件测试计划和软件测试报告，指导和记录测试活动，保证软件质量。面向最终用户的《用户手册》和《操作手册》也在此时交付。

标准化文档既是项目阶段评审的依据又是知识传递的媒介。开发人员更换或者系统升级的时候，完备的文档能很大限度地减轻交接和维护的困难与费用。

（二）软件工程术语

在复杂的电力信息系统建设工程里，牵涉到项目经理，系统分析师，开发人员，测试人员，运维人员以及最终用户等诸多角色。为了保证各方之间可以准确、明确、无歧义地交流，建立一个统一的软件工程术语体系是必要的。GB/T 11457-2006《软件工程术语》国家标准制定了软件工程领域内基本概念、活动和产物的定义，为行业交流提供共同的语言基础，从而实现上述目的。

对于术语的标准化理解可以很大程度上避免项目的风险。标准中明确区分了“验证”与“确认”，验证就是证明我们开发的产品是正确的，即产品满足设计和规范；确认就是保证我们开发了正确的产品，即产品真正满足用户需求。混淆这两个概念会导致测试目标偏离，最后交付出来的产品技术上完美但是不能满足用户的需求。同样，对“模块”、“组件”、“接口”、“耦合度”、“内聚度”等设计概念要有相同的认识，是架构师与开发人员之间进行有效交流，共同打造高质量易维护的软件架构的基础。需求评审、设计审查、代码走查、验收测试等重要活动上使用标准术语，可以大大提升沟通效率，提高评审质量，也可以减少由于理解不同而造成的返工。

（三）软件质量评价标准

软件质量对电力信息系统的生命力起到决定性的作用，它影响电网的安全稳

定运行，也影响公司的经济效益。怎样科学、客观地度量与评价软件质量，是软件工程管理中的一项重要研究课题。ISO/IEC 25010 标准是目前国际上应用最广的软件产品质量评价模型，它取代了以前的 ISO/IEC 9126 标准，给出了更完善的质量评价体系。我国国家标准 GB/T 25000.10-2016 亦是如此。

该标准把软件产品质量定义为功能适用性、性能效率、兼容性、易用性、可靠性、信息安全性、可维护性、可移植性等八个一级特性。每个一级特性又包括若干个子特性。如电网调度自动化系统，成熟性、容错性、可恢复性属于可靠性范畴的质量指标；电力营销计费系统，保密性、完整性、抗抵赖性属于信息安全性范畴的质量指标，功能完备性、正确性属于功能适用性范畴的质量指标；面向公众的手机 APP，易用性直接影响用户体验和满意度。

标准化质量模型与度量指标，给电力信息系统的质量管理作业赋予了具体且可行的指引。项目初期，根据该模型确定项目的质量目标和验收标准；项目开发中，根据该模型进行测试用例的设计，对软件质量进行监控；项目交付时，作为第三方机构进行符合性测试和质量评估的依据。用这些标准可以将抽象的“高质量”要求转化为具体的、可量化的技术指标，从而达到软件质量有效控制和持续改进的目的。

软件质量一级特性与关键指标

一级特性	关键指标示例	典型应用场景
功能适用性	完备性、正确性、互操作性、安全性	电力营销计费、调度自动化
性能效率	时间特性、资源利用率	电力实时监控、大数据分析
兼容性	共存性、互操作性	跨系统集成、多平台部署
易用性	易理解性、易学性、操作性、用户错误保护	面向公众 APP、企业办公系统
可靠性	成熟性、容错性、可恢复性	电网调度自动化、保护控制
信息安全性	保密性、完整性、抗抵赖性、可审计性	电力交易系统、客户信息管理
可维护性	模块化、易分析性、易修改性、易测试性	所有大型软件系统
可移植性	适应性、易安装性、易替换性	操作系统升级、硬件平台迁移

这些具体且可量化的软件质量特性，如上表所示，为电力信息系统的评估提供了清晰框架。

三、接口与协议标准

接口和协议标准是实现电力信息系统内异构子系统之间，系统与设备之间信

息互联互通的前提。在庞大的电力系统中，发电、输电、变电、用电各个环节所用的设备和系统一般是由不同的供应商提供的，采用的技术也不同。这些标准规定了数据交换格式、通信过程、控制信令等内容，一起构成了电力物联网通用语言。

（一）TCP/IP 协议族

TCP/IP 协议族是现代信息网络的基石，也是电力信息系统内部网络通信的事实标准。它不是单一的协议，而是由很多个协议所组成的分层的体系结构，一般分为应用层、传输层、网络层和网络接口层。其中 IP 协议给网络中每一台设备分配唯一的地址，从而可以实现数据包的路由和转发；TCP 协议为用户提供面向连接的可靠数据传输服务，可以保证数据不丢失、不重复、有序地到达；UDP 协议提供无连接的尽力而为的数据报服务，适用于对实时性要求高但是对可靠性要求不高的情况。

电力信息系统中 TCP/IP 协议的应用是无处不在的。所有的上层企业管理应用，比如办公自动化、企业资源计划、营销管理等，都建立在 TCP/IP 网络之上，通过 HTTP、FTP、SMTP 等应用层协议互相传递信息。更重要的是随着技术的发展，TCP/IP 协议也越来越深入到传统的过程控制当中。以现代 SCADA 系统主站和远端终端单元之间、变电站自动化系统内部各个设备之间大量使用基于 TCP/IP 的通信方式取代传统的串行通信为例，可以达到更高的带宽、更加灵活的组网方式以及更加方便的远程维护。生产控制大区如果使用 TCP/IP 协议，则一定要配合严格的网络安全策略，工业防火墙、网络隔离、访问控制等措施都要用上，才能抵御网络攻击。

（二）Web 服务标准

随着面向服务架构思想的流行，Web 服务成了电力企业内部异构系统之间进行跨平台、跨语言集成的主要技术手段。不管是将原有的孤立系统连接起来，还是创建统一的数据共享平台，Web 服务标准都能给出灵活且有效的解决办法。它使不同的应用系统可以像调用本地函数那样，通过网络来调用其他系统提供的功能，从而实现业务流程的灵活编排以及数据资源的共享。

SOAP 是一个用 XML 定义的 Web 结构化信息交换协议。它对消息格式、处理模型、Web 服务描述语言、统一描述、发现和集成之间配合方式做了严格的规定，形成了一个完整的 Web 服务开发技术体系。SOAP 有很高的标准化程度，可以做复杂的事务处理和安全特性。因此，SOAP 在以前被用于可靠性高、安全性

要求严格的企业级核心业务对接上，比如跨省电力交易、银行系统支付接口等。

近几年，由于 RESTful 架构风格简单、轻量、高效等优势，渐渐地成为 Web 服务的主要选择。RESTful 不是协议，它是一系列设计原则的集合，它使用 HTTP 协议本身的方法（GET、POST、PUT、DELETE）来表示对资源的操作。RESTful 服务一般使用 JSON 作为数据交换格式，相比 XML 更加轻便，易于解析。无状态、以资源为设计思想、统一的接口，所创建的服务具有较好的可伸缩性以及松耦合性。目前移动应用、物联网平台以及微服务架构中电力行业的接口设计都以使用 RESTful 为主。

（三）电力行业常用通信规约

除通用信息技术协议外，电力系统的安全稳定运行还依靠一些专用于实时监控、保护和控制的行业通信规约。这些规约充分考虑了电力系统特有的运行环境，例如电磁干扰、严格的时间同步要求以及高确定性传输要求等，是建立电力监控系统“神经网络”的基础。

在电力自动化领域，存在多种广泛应用的标准化规约，它们在不同层级和场景下发挥着关键作用。

1. IEC 60870-5 系列： 这是国际电工委员会制定的远动通信标准。其中，IEC 60870-5-101 是基于串行通信的配套标准，而 IEC 60870-5-104 则将串行通信承载在 TCP/IP 网络之上。它们广泛应用于调度中心与厂站（变电站、发电厂）的远动终端之间，完成遥测、遥信、遥控、遥调等功能。

2. IEC 61850： 这是面向变电站自动化系统的一种革命性国际标准。它不仅仅是一个通信协议，而是一整套包含数据建模、配置描述语言和工程流程规范的体系。通过采用抽象通信服务接口和面向对象的数据模型，IEC 61850 实现了不同厂家智能电子设备之间的真正互操作性。其定义的 GOOSE 和 SV 报文能够利用交换式以太网在毫秒级时间内完成信息交换，满足继电保护、安全自动装置等对时间性能的严苛要求。

3. DL/T 645： 这是我国电力行业制定的一种多功能电能表通信协议标准。该标准及其后续版本（如 2007 版）详细规定了电能表与主站或集中器之间数据交换的帧格式、命令集和数据标识体系，是居民和工商业用户用电信息自动采集系统的基础，为电费结算、负荷管理、需求侧响应提供了重要数据支撑。

这些专业规约同通用信息技术协议相融合，这就是智能电网信息技术发展的

一种趋向。IEC 60870-5-104、IEC 61850 等都是以 TCP/IP 为基础的。融合提高了系统的集成度与灵活性，但也会给网络安全和一体化运维提出更高的要求，系统设计与建设时需要予以考虑。

第四节 管理标准要求

电力信息系统建设不能脱离成熟标准的指导。本节主要阐述 IT 服务管理、信息安全管理和项目管理这三个标准体系，给电力信息系统全生命周期管理提供坚实的理论基础以及实践参照。

一、IT 服务管理标准

ITIL 是全球公认的 IT 服务管理最佳实践框架，给电力企业提供了系统化的方法，目的是把 IT 服务同业务需求结合起来，改善服务品质和运营效率，从而最大化 IT 的价值，保证电力核心业务的稳定运行。

（一）服务战略、设计、转换、运营、持续改进

ITIL 的核心思想用完整的服务生命周期来体现，它由服务战略、服务设计、服务转换、服务运营和持续服务改进五个互相联系的阶段组成。服务战略是生命周期的起点，主要工作就是确定 IT 服务提供方的市场定位、服务组合和财务管理，保证 IT 战略与电力企业的整体业务战略一致。以新一代调度自动化系统规划为例，在服务战略阶段要确定该系统为业务部门提供什么样的服务、创造什么样的价值、怎样衡量投资回报。

服务设计阶段承接战略目标，将战略目标转化为具体的可行的服务方案。此阶段的工作有服务目录的设计、服务级别协议的设计、基础架构的设计、流程的设计、度量指标的设计。电力信息系统的服务设计要考虑到系统高可用性、高可靠性和高安全性，来满足电网 7x24 小时不停歇的严格要求。服务转换阶段，就是服务设计完成后安全、可控的转入生产环境的过程，包括变更管理、发布和部署管理、服务验证与测试等活动，尽量减少服务上线给现有机房业务造成的影响。

服务运营是 IT 服务价值的最终体现，主要目的是保证已经上线服务的稳定高效运行，满足用户需求以及服务级别目标。本阶段主要对日常运维活动进行管理，即事件管理、问题管理和请求处理。当电力交易系统性能下降的时候，服务

运营团队就要立即响应，尽快恢复服务，找到根本原因。持续服务改进阶段存在于整个生命周期当中，对服务绩效展开持续的监控、评判并加以改善，使得 IT 服务不断进行迭代，形成闭环的管理体系，保证 IT 服务能力可以适应电力业务发展的动态改变。

（二）服务管理流程

ITIL 框架的重点在于标准化的 IT 服务管理工作，它被 IT 服务生命周期各个阶段所包围，给 IT 服务的交付和管理提供支持。给电力企业的 IT 部门提供具体的操作指导，把复杂的 IT 管理工作分解成可以衡量、可以重复、可以优化的步骤，进而提高管理成熟度。通过执行以上流程可以明显提高服务响应速度，降低运维成本，有效控制由于变更而造成的风险。

在电力信息系统的实践中，以下核心流程发挥着关键作用：

1. 事件管理的主要目的就是尽快使受影响的服务恢复正常。当监控发现营销系统数据库响应变慢的时候，事件管理流程就会被触发，相关技术人员也会立即前往处理。

2.2、问题管理：要从根本上解决引起问题的原因，防止类似的问题再次发生。从事件数据中找出并解决背后的技术或者管理缺陷。

3. 变更管理：保证所有的 IT 基础设施和服务变更都被评估、批准、执行、审查，用标准化的方式控制变更过程，把变更引入的风险降到最低。电网调度系统十分重要，任何未经许可的变更都会造成严重的后果，所以必须严格按照变更管理流程来操作。

4. 服务级别管理，同业务部门协商、确定并签订服务级别协议，对服务绩效进行持续监控，保证 IT 服务的提供达到业务部门预期。

（三）服务角色与职责

好的 IT 服务管理要有好的流程，还需要有明确的角色和职责。ITIL 提倡为每一个流程、活动指定明确的负责人、参与者，使得各项工作都有明确的负责人、执行人、监督人，形成权责对等的管理体系。电力企业当中成立这样的组织架构，有益于击破部门壁垒，推动跨团队合作，改善全部服务效能。

ITIL 规定了一系列的重要角色，其中服务负责人要对其所负责的某种服务的整个交付过程及质量负责，并且充当着 IT 与业务间的桥梁，保证所提供的服务可以持续满足业务的需求。流程负责人主要负责某项管理流程的设计、执行和

持续改进，比如变更管理流程负责人要保证所有的变更活动都按照规定规范进行。服务台充当用户同 IT 部门间的唯一接洽点，一般起着“IT 门面”的作用，负责记录并初步处理所有用户的请求和服务事件的报告，服务水平直接影响到用户的满意程度。构成一个有机服务管理团队，互相配合协作来保证电力信息系统服务的顺利交付。

二、信息安全管理标准

在日趋复杂的网络环境下，电力信息系统安全稳定的运行关系到国家能源安全和人民生活的安定。ISO/IEC 27001 标准给出一个全面的信息安全管理体系框架，使电力企业有条理地发现、应对并减少信息安全风险，保证信息的保密性、完整性、可用性。

（一）信息安全管理体系

信息安全管理体系属于 ISO/IEC 27001 标准的主要内容，它不是一种单独的技术解决办法，而是包含组织管理、人员、流程和技术等各个方面的综合管理方法。信息安全管理体系的目标就是将信息安全看成一种风险管理，使信息安全成为企业运作和文化的一部分，从而保证信息资产的持续保护。对于电力企业来说，建立信息安全管理体系就是将安全要求渗透到电网调度、市场交易、客户服务等所有的信息处理业务流程中。

信息安全管理体系的建立和运行依照经典的 PDCA（Plan、Do、Check、Act，即计划、执行、检查、处置）循环，保证体系的持续改进。计划阶段组织要确定信息安全方针、明确信息安全管理体系的范围、开展风险评估、制定风险处理计划。这是整个体系的基础，决定了信息安全工作的方向和重点。如电力企业在这一时期要确定调度控制系统的调度控制大件、继电保护信息等重要资产并分析这些资产所面对的内、外部威胁。

进入执行阶段的时候，组织要依照已经制定的风险应对计划，推行安全控制措施，开展安全意识培训，提高所有员工的安全能力。具体措施有配置防火墙，对通信数据进行加密，实行访问控制策略等。随后就是检查阶段，用内部审核、管理评审、绩效监控等方式对信息安全管理体系的效果进行评价，看安全措施是否达到预期效果，找出运行中存在的问题。

在处置阶段，根据检查阶段发现的问题采取相应措施对信息安全管理体系进

行改进和提升。本阶段为持续改进的关键点，使信息安全管理体系持续改善去适应新出现的安全威胁以及业务变动。依靠 PDCA 循环推进，电力企业的信息安全防护能力不断与风险相匹配，从而形成动态防护、自我完善的安全管理闭环。

（二）风险评估与处理

风险评估属于信息安全管理体系的根基和驱动力，它通过系统的手段识别组织所面临的信息安全风险，给之后的风险处理决策赋予依据。该过程大体上分为风险识别、风险分析、风险评价三个步骤。在电力信息系统建设过程中，风险识别环节需要对信息资产进行全面梳理，即硬件设备、系统软件、业务数据、关键人员等，还要识别这些资产可能遭遇的威胁，即黑客攻击、病毒感染、内部人员误操作等，也不能忽略资产自身的脆弱性，即系统漏洞、管理缺陷等。

风险分析是在识别的基础上，对风险发生的可能性以及风险发生后可能给业务带来的影响进行分析，以确定风险等级。如电网实时监控系统如果被攻击成功造成服务中断，调度中心就无法得到实时数据，业务影响十分严重，所以风险等级很高。风险评价则是将分析得出的风险等级与组织预先设定的风险接受准则进行比较，以判断哪些风险是不可接受的，必须优先处理。完成风险评价之后，组织就要制订相应的风险处理计划，选择合适的策略来应对已经识别出来的风险。常见的风险处理方法有：采取控制措施降低风险（风险消减）、在可接受的风险范围内主动承担风险（风险接受）、通过改变业务流程避开风险（风险规避）、将部分风险转移给第三方（例如购买网络安全保险，风险转移）。电力企业应根据风险特点和成本效益分析，选择最合适的组合方法。

（三）控制目标与控制措施

控制目标是为了实现信息安全所期望达到的状态声明，而控制措施则是为达到这些目标所采取的具体行动、策略、程序或者机制。ISO/IEC27001 标准利用其附录 A 给出了一份 114 个控制措施的标准集合，把这 114 个控制措施归入到 14 个安全范畴当中，给企业挑选并执行安全措施赋予了全面的参照。

电力信息系统的安全建设当中，控制目标与控制措施的选择要同风险评价的结果紧密联系。每一个需要处理的风险都应有相应的控制目标，对应一条或多条控制措施。对于风险“防止非授权人员访问生产调度网络”可以设置控制目标为“对网络、网络服务进行控制”。为达到这个目的，可以采取的具体控制措施有部署网络隔离设备、实行严格的访问控制列表策略、对网络管理员进行身份认证、

定期分析网络访问日志。

控制措施涵盖多个方面，例如：

物理和环境安全：如数据中心等的门禁控制。

人力资源安全：如背景调查及离职程序等员工安全措施。

通信安全：如网络流量加密和安全传输协议等技术手段。

系统开发维护安全：如安全编码规范、变更控制等软件技术措施。

经过计划性的挑选并实施这些控制手段，并将它们融入信息安全管理体系之中之后，电力企业的安全防护体系就形成了纵深化的防护机制，从而可以抵御各种攻击的危害。常见的控制措施分类如下表所示：

ISO/IEC 27001 附录 A 控制措施领域

领域编号	领域名称	示例控制措施
A.5	信息安全策略	制定信息安全方针和审查
A.6	信息安全组织的组织	信息安全角色和职责
A.7	人力资源安全	雇前检查、安全意识培训、纪律处分流程
A.8	资产管理	资产清单、信息分类、介质处理
A.9	访问控制	访问控制策略、用户访问管理、系统和应用访问控制
A.10	加密	加密控制策略、密钥管理
A.11	物理和环境安全	物理安全区域、设备安全、线缆安全
A.12	操作安全	备份、日志记录和监控、漏洞管理、恶意软件防护
A.13	通信安全	网络安全管理、信息传输安全
A.14	系统获取、开发和维护安全	安全开发策略、安全测试、测试数据保护
A.15	供应商关系	供应商信息安全策略、供应链风险管理
A.16	信息安全事件管理	事件管理流程、事件响应计划
A.17	信息安全方面业务连续性管理	信息安全业务连续性计划、冗余
A.18	符合性	法律法规要求、合同要求、独立审查

三、项目管理标准

电力信息系统的建设本身就是一项复杂的工程，牵涉多方协调、技术复杂、投资巨大。项目管理知识体系指南是项目管理领域的权威标准，给出了一套通用的知识、技能、工具、方法集来保证项目按期、按预算、按质量完成。

（一）项目管理五大过程组

项目管理知识体系指南对繁杂的项目管理活动进行了简化，归纳为五个逻辑上相互联系的过程组，这五个过程组构成了项目从开始到结束的全过程管理框架。这五个过程组不是项目的阶段，而是项目生命周期内根据需要反复进行的管理活动的集合。

1. 启动过程组：主要是正式授权项目开始，任命项目经理。该过程组制定项目章程，确定项目商业价值、主要目标、关键干系人、总预算、总工期，为项目后续各项工作打下基础。

2. 规划过程组：这是项目管理中最为详细、重要的一个部分，其主要目的就是制定一份全面可行的项目管理计划。项目范围确定、工作结构分解、活动资源与时间估计、预算编制、质量规划、沟通计划、风险应对计划等都包括其中，给项目执行和控制提供蓝图。

3. 执行过程组：这个过程组的工作是根据项目管理计划，调配人力、物力等各种资源，完成项目中所规定的各项工作，最后交付产品、服务或成果。电力信息系统创建时存在编码，硬件采购，系统整合以及测试等工作。

4. 监控过程组：就是对项目进行持续的监视、检验和反馈，把项目的实际进度同项目管理计划进行比较，发现偏差并及时加以纠正。它保证项目一直走在正确的轨道上，对各种变化、问题能够作出及时的反应。

5. 收尾过程组：负责正式结束项目或者项目阶段的所有活动。包括客户的正式验收，项目收尾工作，解散项目团队，总结项目经验教训等，为以后类似的合作积累宝贵的经验。

（二）项目管理十大知识领域

项目管理知识体系指南把项目管理知识体系分成十大知识领域，这些领域同五大过程组相互交叉，就形成了项目管理的完整矩阵。十大知识领域分别是：项目整合管理、范围管理、进度管理、成本管理、质量管理、资源管理、沟通管理、风险管理、采购管理、干系人管理。它们代表了项目经理所应当具有的一些核心能力以及管理的幅度。

电力信息系统建设项目中，各个知识领域都有着各自不同的价值。项目整合管理居于核心位置，协调着所有其它知识领域的工作，保证项目各个部分无缝连接。范围管理十分重要，它对项目范围和产品范围做出准确的界定，防止出现“范

围蔓延”使项目失去控制。进度管理保证项目在规定的时间内完成，成本管理保证项目在批准的预算范围内完成。质量管理主要是保证系统满足功能和性能的要求，例如严格的测试来保证电费计算的准确性。

由于电力信息系统涉及的部门和人员较多，所以干系人管理、沟通管理是重中之重。项目经理必须识别出全部干系人（电网调度员、运维人员、管理层等）并对其诉求和影响力进行详细的分析之后再选择最有效的沟通方法，使信息在项目团队和干系人间畅通无阻。风险控制能让项目组找出技术、市场、政策等各方面的风险，事先制定应对措施，保证项目可以顺利开展。

（三）项目成功标准

传统的项目成功衡量标准一般只考虑项目是否在规定的范围内、规定的时间、规定成本内完成。过去人们认为按期、按预算完成所有预定功能的系统是成功的。该标准明确、容易衡量，给项目控制设定了清晰的目标，现在仍被作为评价项目绩效的一个重要维度。

随着项目管理理论和实践的发展，项目的成功定义也越来越广、越来越深。现代观点认为，仅仅满足铁三角约束是不够的，项目成功还需要考虑它是否实现了预期的商业价值和战略目标。对于新建的电力信息系统而言，其真正的成功并不在于项目本身是否顺利完成，而在于该系统投入使用以后，能否真正提高电网运行安全水平、提高生产效率、改善客户服务水准或者降低运营开支。因此一个项目的成败应该从整个产品的生命周期的角度来考虑，考虑的是它给组织带来的长期利益。项目经理不能只关注项目执行过程，应该了解项目背后的商业驱动因素，保证项目成果和组织的战略方向保持高度一致，最终得到关键干系人的认可。

第十章 电力信息系统实践案例

本章通过具体的案例对电力信息系统在智能电网中应用进行分析。主要对智能电网信息系统创建概念、创建关键技术和创建意义进行阐述。

第一节 智能电网信息系统

智能电网是电力技术与信息技术的结合，要使智能电网正常工作，必须要有强大的信息系统支持。本节以某地区的智能电网信息系统建设过程，即概念规划到实施的过程进行详细的论述。

一、系统概述与建设目标

复杂的系统建设要从清晰的蓝图、明确的目标开始。要对智能电网信息系统的技术架构与实际成效有全面的认识，就必须先对它的核心概念、重要性以及具体的建设目的有清晰的把握。

（一）智能电网的内涵与特征

智能电网不是传统电网的简单升级，而是场深刻的革命。核心就是将先进的传感、通信、分析和控制技术同物理电网深度融合，构建信息流、能量流、业务流高度融合的能源网络。在这个网络里，电力从产生到消费的每一个环节都会变得透明可控，电网自身就有自我调节、优化的能力，可以高效地吸纳分布式能源，并且能与用户实现双向的实时交互，从而达到最优的电力资源配置。

智能电网具有信息化、自动化、互动化这三个特点。信息化就是充分运用遍布电网的智能终端，对电网状态、设备运行和用户行为进行全方位的实时感知。自动化指的是电网可以迅速诊断、隔离故障并自愈，从而快速恢复供电，大大提高供电可靠性。互动化是它的根本标志，它冲破了传统电网的单向壁垒，创建起双向的信息与能量交流平台，让用户从单纯的电力消费者变成可以积极参与电网调节并从中获益的“产消者”。

（二）信息系统在智能电网中的作用

把物理电网比作智能电网的躯体，那么信息系统就是智能电网的大脑和中枢神经系统，它在发电、输电、变电、配电、用电、调度等所有环节中起着重要的作用，使电网具有感知、思考、决策、执行等智能。其主要作用是采集、传输、处理物理电网产生的大量数据，形成全局态势感知，根据预设的策略或者算法生成控制指令，从而精准调控电网运行，保证电网安全、稳定、经济、环保运行。

信息系统的作用有多个方面的体现，在运行监视方面，它依靠新一代的能量管理系统和配电自动化系统，对电网运行情况做到实时的观测并能迅速确定故障发生的位置。资源管理上能很好地支持大规模新能源、分布式电源、储能系统、电动汽车等的有效管理和协同优化。在用户服务上可以自动采集用电信息的基础上，还可以支持需求侧响应、分时电价等新型业务，从而引导用户养成更加合理的用电习惯。

（三）案例系统建设目标与范围

该省电网新一代智能电网信息支撑平台本节的案例。平台总体目标就是打破专业壁垒，建设技术先进、数据共享、应用灵活、安全可靠的集一体化信息系统，为电网全业务领域决策提供数据驱动，全面提高电网智能化经营水平。

为达成此目标，把系统建设分成了许多具体的目标，即：对关键输变电设备进行全覆盖状态监测；提高配电网的自动化程度；大幅度降低用户的年平均停电时间；依靠准确的预测能力，将电网接纳新能源的能力提升至 20%；创建统一的客户服务平台来提供便捷的用户服务，如网上办电、能效分析等。

该系统建设范围是电力业务的全过程。在物理上它升级整合了调度自动化和能量管理系统的主站，并新建了配电自动化和用电信息采集主站。在数据层面，建立企业级数据中心、数据中台，将海量异构数据汇聚、治理、服务化封装。从应用层面来看，开发出了设备预测性维护、电网风险评估等众多智能应用。

二、系统架构与关键技术

宏伟的建设目标必定要坚实的技术架构来支撑。本部分主要分析案例系统的核心设计思想，以及实现时所用到的先进科技。

（一）分层分布式系统架构

本案例系统使用的是业界主流的“云、管、边、端”四层分层结构，保证系

统具有很好的灵活性和可扩展性。其中，“端”指终端感知层，主要是智能电表、在线监测装置等设备的数据采集；“边”是边缘计算层，接近数据源头进行初步处理和即时响应，从而降低中心平台的压力；“管”是网络通信层，利用光纤、无线等方式形成高速泛在的数据传输通道；“云”是云平台层，是系统的中心，提供海量的数据存储、强大的计算能力和各种应用服务。分层解耦的结构使得每一层都可以独立的发展与进化。

云平台使用的是先进的分布式微服务架构。传统单体应用被精细拆分为负荷预测、设备诊断等许多功能内聚、松散耦合的微服务单元，每个服务可以独立开发、部署和扩展。此架构可以大大提升系统的容错能力，有效避免单点故障，提高研发效率和系统的弹性伸缩性，能依据业务负载状况对计算资源实行动态分配，最大范围地利用起资源。

（二）物联网、大数据、人工智能技术应用

物联网技术是智能电网的神经网络的基石。它依靠大量的智能传感终端来实现对电网各种“物”的全面连接。输电线路上的微气象监测装置、变电站里的数字化采集设备、配电网中的智能开关、用户的智能电表等等，一起形成起了一个庞大的感知网络。终端通过物联网通信技术，将多维电网状态数据实时上传至信息平台，为精细化管理打下了坚实的数据基础。

物联网广泛应用，产生了大量的数据，大数据技术起到了举足轻重的作用。数据湖可以存储 PB 级的异构多源数据，并且对数据的处理也十分高效。并且使用分布式计算框架可以同时对大量数据进行计算以及深入挖掘，例如通过对电流波形数据的分析来发现设备劣化征兆，或者对用户用电曲线进行聚类分析以识别不同的用电模式，从而为精准营销提供有力支持。

人工智能技术是数据潜在价值被释放出来、系统智能决策实现的发动机。本平台把人工智能模型深度应用到多个重要业务场景中，具体如下

1. 智能巡检。 利用计算机视觉技术，自动分析无人机图像，高效识别线路及杆塔缺陷。

2. 负荷预测。 融合深度学习模型，综合多维因素，高精度预测未来中短期电力负荷。

3. 资产健康管理。 通过机器学习建模，精准评估设备健康度，实现状态驱动的智能检修。

（三）信息物理系统融合

智能电网属于典型的信息物理系统。其主要部分是信息技术同物理电网融合并进行实时交换，对物理世界实施精确控制的闭环反馈回路。其工作流程是，在信息空间中由各种传感器对物理电网的实时状态进行感知，然后经过快速分析与智能决策后再作用于物理电网，形成一个闭环的“感知、分析、决策、控制”过程，从而使电网控制更加精细，响应更加迅速。

在本案例中，信息物理系统的思想渗透到整个系统的设计当中。区域源网荷储协同控制就是这样一个例子：该系统可以实时采集区域内的光伏发电、储能状态、可中断负荷等各种数据。信息平台上优化模型（信息世界）对这些数据进行快速计算，得到最优控制策略，然后立即发送给储能装置或者用户负荷，发出调节指令（物理世界），从而实现区域内新能源就地消纳和电网动态平衡。

三、建设成效与经验启示

任何一项技术实践的价值，最终都要从取得的成就、积累的经验中体现出来。本部分对本案例的建设成果进行总结，并给出未来发展的启示。

（一）提升电网智能化水平

信息系统投入使用以后，电网智能化水平显著提高，许多重要的运行指标都有了明显的提升。配电自动化和故障自愈使平均停电时间降低超过 40%，供电可靠性达到前所未有的水平。基于人工智能的负荷预测模型，在某一时段的预测准确率大于 98%。新能源功率预测同智能调度紧密联系起来，很好地解决了弃风弃光的问题，使区域新能源消纳率一直维持在较高水平上，产生了明显的经济和环保效益。

除了这些可以量化的指标之外，就是运营管理模式的改变。电网运行状态由过去的局部感知、事后分析转变为现在全局透明、实时洞察。运维人员借助三维可视化界面可以对电网的运行状况有全面的掌握。决策过程也由原来的以经验为主转变为以数据模型、算法为主，风险控制更加主动、精准。从“人治”到“数治”的变化，就是电网迈向高阶智能化的一个标志。

（二）面临的主要挑战与解决方案

智能电网信息系统建设与运营过程中遇到的诸多问题中，主要问题及应对策略如下表所示：

智能电网信息系统建设挑战与解决方案

网络安全	采取纵深防御策略：构建生产控制大区与信息管理大区物理隔离；对敏感数据进行加密脱敏处理；加强访问控制和审计；建立专业网络安全应急响应小组，并定期开展攻防演练，确保系统安全可控。
海量异构数据整合	针对电网中普遍存在的“烟囱式”系统及数据标准不一导致的数据孤岛问题，核心举措是建设企业级统一数据中台。通过统一数据模型和规范，对各类业务数据进行清洗、汇聚、服务化封装，从根本上打破数据壁垒，实现高效共享。
技术复杂性与人才缺乏	面对大数据、人工智能等新兴技术带来的高门槛和人才短缺问题，采取内外结合的解决办法：内部广泛开展技术培训，促进员工知识结构转型；外部与高校、科研机构深度合作，借助外部智力资源解决技术难题，并建立持续性人才培养与引进机制，为系统长期发展储备智力资源。

（三）对未来智能电网信息系统建设的启示

本案例的实践给以后智能电网信息系统创建给予了很好的借鉴。其中非常重要的一点就是必须坚持顶层设计、标准先行。智能电网是一个复杂的巨系统工程，如果没有统一的、前瞻的架构蓝图，很容易造成重复建设以及新的信息孤岛。因此项目启动之初就要确定整个技术路线、数据模型和接口标准，使各个子系统在统一的框架下协调发展。同时推动行业标准的制定，对保证系统间的互相连接有长远的战略意义。

电力信息系统今后再不能仅仅充当封闭的业务支持系统，而应该转型为开放的价值创造平台。在双碳目标之下，电力系统要肩负起更多的社会职能，电动汽车同电网的深度互动、聚合虚拟电厂等新的业务。所以信息系统要创建开放平台生态，依靠开放应用程序接口来召唤第三方开发者加入，从而一同培养新的应用和服务。开放协同的模式是数据价值的发挥，新的商业模式的发展必由之路。

第二节 配电自动化系统

配电自动化是运用现代电子、通信和计算机网络技术，对配电网实行智能控制和管理的一种先进技术体系。其主要目的就是提高供电可靠性、改善电能质量、提高运行效率。整合各类信息资源，它就形成了一套完整的自动化管理系统，是建设坚强智能电网不可缺少的重要环节。

一、系统功能与业务流程

配电自动化系统的核心就是对配电网络的全面感知与精确控制，包含数据采集、故障自愈全过程，用标准化的业务流程来保证系统规范高效运行。

（一）配电 SCADA 功能

配电 SCADA 是配电自动化的基础平台，也是配电自动化的主要部分。它的主要任务就是对配电网设备的运行情况进行实时监测，并把各种数据详细记录下来。系统可以采集线路的电压、电流、功率、频率、开关位置等遥信遥测信息，并将大量的数据实时上传到主站系统。调度人员依靠友好的人机交互界面，对电网整体运行情况有全面的掌控，可以实现对电网潮流、设备状态的动态监视。

SCADA 系统具有监视功能，同时也具有调度人员远程控制和调节配电设备的功能。调度员可以进行断路器的分合操作，调节变压器分接头，甚至对无功补偿设备进行投切，来迅速响应负荷的变化或者处理异常工况。系统还有很强的告警、事件记录功能。当参数越限或者开关变位时，系统可以自动发出报警信号，按照事件发生顺序记录有关的数据信息，给故障分析、事故追查提供准确的数据支持。集中式管理模式大大提高了配电网调度效率以及决策的科学性。

SCADA 系统依靠建立主站、通信网络、远方终端单元构成的分布式测控体系，来达到对广域配电网集中管理的目的。主站是整个系统的中枢，对现场采集到的数据进行处理和分析，发布控制命令。现场终端设备是数据采集和命令执行的末梢神经，也是整个系统物理实现的基础。这套体系正常运转，才是实现配电网透明化管理、精细化运维的前提。

（二）馈线自动化功能

馈线自动化是配电自动化系统中最重要的一种高级应用功能，它所要达到的主要目的就是当配电线路出现故障时，能自动、快速地找到故障发生的位置，将故障区段隔开，并且让没有故障的区域继续正常供电，从而实现电网的“秒级自愈”。该功能依靠部署在馈线关键节点的智能终端设备相互配合，几乎不需要或者只需要很少的人工参与，从而大大缩短故障停电时间，缩小停电范围，明显提高供电可靠性。

馈线自动化实现逻辑主要是由故障检测、故障定位、故障隔离、负荷转供这四个部分组成。当线路某处发生短路或接地故障的时候，沿线的智能终端可以立

刻感知电流、电压的异常变化，把故障信息传送给它或者通过终端间通信传递。系统接到各个终端传来的情况之后，通过内置的算法快速判断出故障发生于哪两个开关设备之间，实现精准定位。随后系统就会自动给故障区段两侧的开关发出跳闸命令，把故障点从电网中隔离出来。故障被隔开之后，系统就会对非故障区段的负荷情况以及备用电源的容量展开分析，并自动操作联络开关，用别的线路或者电源给非故障区段重新供电。这一系列的过程一般都在几秒或者几分钟内完成，用户不会有停电的感觉。

（三）配网运行管理业务流程

在配电自动化系统的支撑下，配网运行管理业务流程从以前的被动响应转变为现在的主动运维，整个流程更趋闭环高效。一般包含日常监视、故障处理、计划检修等几个方面，保证配电网的安全、稳定、经济运行。

故障处理是其中最具代表性的业务流程。具体流程如下：

1. 配网某处发生故障的时候，馈线自动化功能被立即触发，SCADA 系统几乎同时收到现场终端发出的故障信号和开关变位信息，然后以声光等多种方式向值班长发出告警。

2. 故障自动处理对于已经实现馈线自动化的线路，系统会自动完成故障定位、隔离以及非故障区段的负荷转供，在调度界面上也会显示新的网络拓扑结构。调度员只需要对处理结果进行确认就可以发布抢修指令了。

3. 人工干预和抢修，对不能实现自动化或者自动化处理失败的区域，调度员根据 SCADA 系统的实时数据和故障信息进行人工判断、遥控操作，隔离故障。系统产生的故障定位信息会指引抢修人员去现场排查修复。

4. 恢复送电与归档：故障排除后，抢修人员向调度汇报，调度员用遥控方式对这个区域实行正常的送电。系统会对故障处理过程中出现的事件和操作进行记录，形成一个完整的报告，供以后做故障分析和评价时参照使用。

二、系统实现与技术难点

配电自动化系统构建属于复杂的系统工程，牵涉到通信、终端设备以及软件算法等诸多方面。系统成功实现并不依靠先进技术，而是在现场部署和运行维护过程中解决出现的一系列技术问题，保证系统功能稳定可靠。

（一）通信网络建设

通信网络属于配电自动化系统的神经中枢，其可靠程度、实时性以及覆盖面都会直接影响到配电自动化系统是否能正常工作。它是主站和终端之间大量遥测、遥信、遥控以及故障信息等数据的传输平台。由于配电设备分布区域广，环境复杂多变，通信网络一般采用有线与无线相结合的方式来组网。

城市核心区、电缆线路密集区域一般采用工业以太网光纤环网。该种方式带宽大、抗干扰能力强、可靠性高，可以满足高密度数据采集和控制的要求。

对架空线路地理位置分散、敷设光纤成本高的地方，无线通信是主要方式。早期用的 GPRS 公网通信方式建造成本低，使用方便，但在用电高峰期或者基站信号不好时会出现网络拥堵，断线等情况。为克服这些缺点，电力无线专网技术，例如基于 LTE 技术的专网，正被越来越多地使用。无线专网可以提供更加安全、可靠的服务质量保障，但是其建设与维护成本较高。因此，怎样依据各地区业务需求、地理环境、投资效益等条件，因势利导地选择最适合的通信方式，如何实现多种通信方式之间的无缝对接和相互备份，就成了通信网络建设的关键问题。

通信网络安全问题也不容忽视。系统的智能化程度越高，网络受到的攻击就越危险。因此在网络架构设计之初就要充分考虑安全隔离、数据加密等措施，划分不同的安全区域、设置防火墙、采取端到端加密等方式来防止非法入侵、数据被篡改，保证配电网控制指令的安全可靠。

（二）终端设备部署

配电自动化终端属于主站系统与一次设备之间的纽带，也是完成数据采集并使控制指令得以落实的最基本物理单元。主要有馈线终端单元、站所终端单元、配电变压器监测终端。

配电自动化终端设备概述

终端类型	英文缩写	典型部署位置	主要功能
馈线终端单元	FTU	柱上开关、环网柜	馈线故障快速检测与隔离控制
站所终端单元	DTU	开闭所、配电室	对多个线路进行监控
配电变压器监测终端	TTU	配电变压器	监测配电变压器负载率、温度等状态

上表给出了常见的配电自动化终端设备类型及功能。其中 FTU 一般安装在柱上开关或者环网柜中，主要用来检测馈线故障并迅速隔离。DTU 多使用于开

闭所或者配电室，可以实现对多条线路的监控。TTU 主要对配电变压器的工作负载率、温度情况实施监视。这些终端就像电网的感觉神经，布置是否合理，自身是否可靠都十分重要。

终端设备部署存在诸多技术问题。其次就是环境适应性问题，室外布置大量的终端设备需要承受高温、低温、潮湿、雷击等恶劣环境。因此对设备的防护等级、工作温度范围、电磁兼容性等都有很高的要求。其次是设备选型和标准化。由于不同的设备厂家生产出来的终端设备功能、性能、通信协议各不相同，如何选择符合电网实际情况的、有良好互操作性的设备，以及建立统一的设备标准和测试规范，对于保证系统的兼容性、可扩展性来说都是很重要的一个方面。终端的安装、调试以及后期的运维工作量大，需要制定合理的部署策略和高效的运维管理机制，降低全生命周期的成本。

（三）故障定位、隔离与恢复算法

故障定位、隔离、恢复算法可以被看作馈线自动化功能的大脑和灵魂，先进的、可靠的算法是保证故障处理高效、准确的关键。传统的故障定位方法主要是采用电流定则或者阻抗法，对简单的辐射状网络是有效的，但是对于复杂的环形或者多分枝网络，在分布式电源接入的情况下，容易产生误判或者定位精度不高。

为了应对配网结构日趋复杂化的发展趋势，又提出了许多先进的算法。以人工智能技术为基础的故障诊断方式有专家系统、模糊逻辑、神经网络、深度学习等，能将故障录波数据、历史故障记录等信息综合起来，用模式识别、自动学习的方法，大幅度提高故障诊断的准确率、智能化水平。利用深度学习算法对大量的故障波形数据进行分析，可以更加准确的判断故障的类型及特性，即使在信噪比较低的情况下也可以有效识别。同时分布式故障处理逻辑也成为了发展方向，它会把一部分决策功能下放至智能终端，利用终端间的对等通信，快速协同，实现不需要主站的就地型故障隔离和恢复，大大缩短了反应时间，供电可靠性得到进一步提高。

但是这些高级算法的实现是有技术难题的。算法效果很大程度上由输入数据好坏决定，对传感器精度和通信及时性要求较高。要创建并训练一个算法模型，必须要依托大量实际的数据做基础，在实际运用的时候，也要持续对这个算法模型加以改善和提升，使之可以适应电网运行方式的改变。怎样保障算法在诸多复杂的工况下仍能保持鲁棒性、安全性，避免由于算法误判引发故障范围加剧或者

设备受损，这是在研发和应用时务必加以严格控制的难题。

三、应用效果与改进方向

配电自动化系统得到广泛的应用，大大提高了配电网运行效率以及供电服务质量。在肯定其巨大成效的同时，也要看到目前建设和运维中存在的一些问题，积极探索未来的发展方向，以适应新型电力系统的发展要求。

（一）提高供电可靠性与管理水平

配电自动化系统最直接的效果就是大大提高了供电的可靠性。使用馈线自动化功能在电网发生故障的时候，可以迅速将故障区段隔离并且对非故障区段恢复供电，把原来需要数小时的人工操作缩短为分钟甚至秒，大大减少用户的停电时间和范围。这直接促使和供电可靠性有关的重要指标（SAIDI、SAIFI）持续提高。SCADA 系统提供的全景监视、远程控制功能，使调度人员可以对电网的负荷分布进行实时监视，进行科学的负荷预测、潮流调节，避免设备超载，保证电网安全经济运行。

管理水平提高也是其价值之一。系统实现了配网信息的透明化、精细化管理，给设备状态评价、资产管理等各方面工作提供数据支持。过去主要依靠人工巡查、凭经验判断的劳动方式已经被以数据为依托、用数据来进行在线监测和预警的方式取代了，运维效率与决策水平出现了质的飞跃。自动化流程减少了现场的操作次数，也降低了运维人员的劳动强度和安全风险。

（二）存在的问题与不足

虽然配电自动化建设取得了很大的发展，但是配电自动化建设中也存在一些问题和不足。系统实用化水平参差不齐。部分地区装有自动化设备，但是由于通信通道不稳定、终端设备故障率高或者基础数据不完整等原因，造成遥信不准、遥控不动等问题仍然存在，自动化功能无法发挥。陈旧设备改造难度大、投资大，自动化覆盖率很难在短时间内全面提高，新旧设备共存给统一管理带来困难。

二是运维工作面临新挑战。配电自动化系统中有很多的二次设备、通信设备，日常巡检、处理故障、软件更新等都需要具备通信、自动化、计算机等多方面知识的复合型人才，但是目前的运维队伍技能结构不能完全满足要求。系统规模扩大后，海量告警信息的处理、终端设备定期维护、电池更换等工作给运维带来了巨大的压力，急需更智能的运维手段。

（三）未来发展趋势与改进方向

随着分布式新能源的大规模接入和电动汽车等新型负荷的快速增长，配电自动化也向智能化、灵活化、高效化方向发展。

1. 向主动配电网发展：传统配电网是无源的，而新型配电系统里存在大量的分布式电源，具有源荷双向互动的特点。配电自动化系统应该从单纯的“监”和“控”向具备潮流主动调控、电压主动管理、新能源消纳优化等功能的“主动管理”转变，实现对分布式资源的有效聚合与协同控制。

2. 更深入地融合人工智能、大数据技术：通过挖掘电网运行数据、设备状态数据、气象数据甚至社会经济数据来实现负荷预测的更精准，故障诊断与自愈的更智能，设备状态预测性维护的前瞻性，最后形成具有自我感知、自我诊断、自我决策能力的自愈型电网。

3. 配电物联网化：随着物联网的发展，配电自动化会向感知范围更广、更灵敏的配电物联网方向发展。利用大量的低成本、低功耗的智能传感器，对中低压配电网和用户端设备状态进行全方位的感知，为精细化的负荷管理、电能质量治理、用户侧灵活互动提供强有力的支撑，推动电网向能源互联网转变。

第三节 电力营销系统

电力营销系统是电力企业与终端用户的连接纽带，也是电能商品价值的实现平台、客户服务承载的平台。本节主要研究电力营销系统所包含的业务范围，核心技术，在能源革命和数字化浪潮的双重推动下，其在现代电力企业中的战略地位越来越突出，发展态势愈加明显。

一、系统业务范围与核心模块

电力营销系统包含从客户接入电网到最终电费结算及服务全过程，其业务完整性、流程自动化水平直接影响电力企业的运营效率和客户满意度。核心模块设计从人、户、表、费、价等要素入手，具体的内容请参考下表。

电力营销系统核心要素表

要素	中文含义	系统作用
客户	指与电力公司发生经济关系的自然人或法人实体	客户管理，服务对象识别
用户	指用电户号或合同账户	业务办理单元，电费结算主体
表	指计量表计，如电能表	电量计量，数据采集源
费	指各类电费、附加费	计费规则执行，费用生成
价	指电价标准、资费政策	电价管理，结算依据

（一）业扩报装与抄表收费

业扩报装是电力营销业务的起点，是新用户申请用电、增容、变更等全过程。系统借助工作流引擎，把受理申请、现场勘查、供电方案答复、设计审查、中间检查、竣工检验、装表接电等工作环节做到流程化、规范化。大大提高了办电效率，全过程透明化管理、时限控制，大量纸质文件电子化，建立完整的客户工程档案，为之后的资产管理、运维工作打下坚实的数据基础。因此，这一过程数字化转型是优化营商环境、提高客户获得电力体验的直接体现。

抄表收费属于电力营销系统中最基础、最频繁的业务，它同电力企业的现金流乃至生存紧密相关。抄表环节系统要有强大的兼容性，支持多种抄表方式并存的复杂环境，人工抄表核对、电力线载波或无线公网远程自动抄表、智能电能表实时交互的高级计量基础设施。系统会对采集得到的大量原始数据进行清洗、校核、估算，保证电量数据的准确无误。

收费环节用预设电价政策、复杂的计费规则来对审核无误的电量数据进行费用的计算，并产生电费账单。随着支付技术的迅猛发展，系统集成了多种收费渠道，从传统的营业厅柜台、银行代收、现代化的网上银行、手机应用程序、第三方支付平台等，大大方便了用户。系统欠费管理功能齐全，能够自动执行催缴、停复电操作指令，形成业务闭环。

（二）用电检查与客户服务

用电检查指的是对电力使用进行监督管理，保证电网的安全稳定运行以及正常的供用电秩序。电力营销系统给用电检查业务给予了全方位的信息化支撑，包含检查计划的制订，任务的下达，现场信息的移动化采集并立即回传。检查人员可以利用手持终端，随时对客户的用电情况、设备状态、私拉乱接等违约用电行为进行记录，并且可以现场拍照取证。系统按照检查结果自动生成整改通知单或

者违约用电处理单，对处理过程进行全过程的跟踪，保证问题能够得到解决。系统内建的反窃电分析模型，可对用户用电行为的异常波动展开深入分析，给精准稽查赋予有力线索。

客户服务对树立企业的良好形象、提高客户的忠诚度有着重要的作用。现代电力营销系统整合了多种服务渠道，创建起 95598 热线、网上营业厅、移动应用程序、微信公众号等全方位的客户服务平台。该平台的核心是一个统一的客户关系管理系统，可以给客服人员提供客户 360 度全景视图，即客户基本信息、缴费历史、报装记录、历史诉求、用电曲线等所有相关数据。在客户用不同的途径提出业务咨询、故障报修、投诉建议等请求的时候，系统能立即给出回应，实行“一口对外”保证服务质量的一致高效。知识库、智能问答机器人等技术的使用，使得服务自动化程度大大提高，大量的简单重复的咨询被分流，人工坐席可以将更多的精力放在解决复杂问题上。

（三）计量与线损管理

计量管理是对电力营销中计量源头的精确控制，计量源头的准确性是实现公平公正交易的前提。营销系统中的计量资产管理模块对电能表、互感器、采集终端等所有的计量设备实行全生命周期管理。设备采购入库、检定、安装、周期性轮换、故障更换、报废处置等各个环节都详细记录在系统里。这形成起一个庞大的计量资产电子档案库，里面一一分列着每块表计的规格型号、装设地点、运行情况以及过往历史，给故障诊断、资产清点和精确轮换工作赋予了可信的根据。

线损管理是反映电网企业经营效益的重要指标。电力营销系统同生产管理系统、地理信息系统达成数据互通互用，创建起依靠电网拓扑关系的线损理论计算模型。系统可以自动汇总关口电量与所有终端用户的销售电量，得出指定区域或者线路的实际损失电量，即统计线损。通过对比分析实际线损和理论线损，可以快速找到高损耗的变压器台、线路，对线损的组成进行深入分析。

1. 技术线损分析：可以识别出由于设备老化、三相不平衡、无功补偿不足等原因造成的损耗，给电网优化改造提供决策依据。

2. 管理线损分析：主要是查找计量装置故障、抄表错误、窃电等非技术损失，为以后的用电稽查、计量运维等工作指明方向。

二、系统架构与数据模型

先进的电力营销系统，其后台技术架构和数据模型是系统高性能、高可用、易扩展的根基。科学的数据模型和合理的架构设计，可以使其很快地适应业务的变化。

（一）面向服务的架构与微服务实践

早期电力营销系统大多数使用单体式架构，即将所有的功能模块打包到一个大的应用中。此种架构在系统规模较小的时候尚能应对，但随着业务变得愈发繁杂，它的弊端便开始凸显出来，模块之间的耦合度过高，稍微改动就有可能导致全局出现问题，技术栈单一，无法引入新技术，系统升级和部署耗时且风险较高。为解决这些问题而出现的面向服务的架构。它把庞大的系统拆分成一系列松散耦合、可以独立部署的服务，服务之间通过良好定义的接口进行通信，这使得系统变得非常灵活，可重用性大大提升。

近些年来，微服务作为面向服务架构理念的深化发展，在电力营销系统创建时被广泛使用。微服务把服务的粒度分得更细，每个微服务都只负责一个具体的业务功能，并且有独立的数据库和技术栈。客户管理、账务处理、抄表管理、支付服务等都可以成为独立的微服务。这种架构的优势很明显：开发团队可以并行工作，独立开发、测试、部署各自的服务，大大加快了迭代速度；根据各个服务实际负载情况独立进行弹性伸缩，提高资源利用率；单个服务故障不会导致整个系统崩溃，使系统更加容错、健壮。容器化技术与微服务编排工具的不断发展，给微服务架构的实现给予了强大的技术支撑。

（二）客户主数据模型

电力企业信息系统中客户资料分散在营销、生产、调度等各个系统里，造成数据不一致、不完整。因此客户主数据模型的创建，其目的就是建立全企业统一、权威的客户数据视图，即单一事实来源。经过主数据管理实践，把分散的客户数据清洗、合并、规范，最后得到好的“黄金记录”。

电力营销系统客户主数据模型一般以客户、用电地址、用户、合同账户、计量点这几个核心实体来搭建。这些核心实体的具体定义及作用见下表。

客户主数据模型核心实体表

核心实体	定义	特点与作用
客户	与电力公司发生经济关系的自然人或法人实体	法律主体，服务对象
用电地址	用电行为发生的物理空间位置	具有唯一地理坐标，服务地点
用户	用户在某个用电地址接受电力服务的业务关系	一个客户可在不同地址有多个用户关系
合同账户	电费结算的财务主体	确定电价、结算周期等商务条件
计量点	电能计量的物理点	安装电能表等设备，电量采集源头

明确各个实体之间联系，构建出稳定合理易于扩展的数据模型。这一规范化的数据模型给上层业务应用赋予了良好的数据根基。

（三）与其他系统的集成

电力营销系统不是孤立存在的，它处在企业信息流转的核心枢纽位置，需要同诸多外部和内部的系统实现高效、可靠的数據交换。实现业务流程的协同，打破信息孤岛的关键就是集成。主要的集成对象有生产管理系统，获取设备台账、电网拓扑数据，支持线损计算、资产关联；地理信息系统，可以将客户、设备在地图上可视化，支持勘查、抢修等外勤业务；财务管理系统，实现电费收入的自动记账、核销，保证业财一体化。

营销系统还要同调度自动化系统整合起来，一旦出现停电情况，就能马上得到停电区域，随即把消息通知给受影响的客户，在故障抢修恢复供电之后立刻告知。银行、第三方支付机构等外部金融机构集成，保证资金流动顺畅，结算准确。集成技术也经历了发展，由最初的点对点接口、文件交换，发展为基于企业服务总线的集中式集成，再到现在的微服务架构下基于 API 网关的轻量级、去中心化的集成。从而形成电力企业数字化经营庞大的网络。

三、系统演进与创新发展

能源结构转型、信息技术变革、客户需求提升这三个因素的叠加效应，正在将电力营销系统由原来的管理手段变为价值创造平台。它不再只是后台的业务处理器，是企业面对市场、服务客户、创新商业模式的前哨站。

（一）从传统营销到“互联网 + 电力服务”

传统的电力营销是以企业为中心、以线下业务办理为主、被动式服务。客户

常常需要亲自去营业厅办理业务，获取信息的途径少，服务方式单一。在这个时期电力营销系统被用于内部管理，重视的是工作流程的规范化及效率的提升。随着“互联网 +”战略深入发展，电力营销也由原来的以客户为中心、线上线下融合的主动式、智能化服务模式。

互联网电力服务的关键之处在于依靠移动互联网、云计算等技术，把电力核心业务和服务拓展到用户的指尖。电力营销系统开发出了功能丰富的手机应用程序和网上营业厅，实现了业务的线上办、掌上办。用户可以随时、随地查询电费、缴纳电费，办理移表、新装申请，还可以查看家庭用电情况。系统仿佛成了一个“用电管家”，主动给用户发送停电通知、电费账单、节能小妙招等各类信息，由原先的被动的获取信息转变为积极主动地关心用户的用电需求。既提高了用户的感受度，又降低了企业的运营成本，更重要的一点就是获得了大流量、用户交互等数据资源，为以后拓展新的业务开辟道路。

（二）大数据分析与精准营销

电力营销系统属于企业内部最大的数据生产者之一，不断地产生大量的用户用电数据、交易数据和服务交互数据。在传统的模式下，这些数据主要被用于账单的产生以及事后统计，深层次的价值并没有被充分挖掘出来。大数据技术的应用，能对大量的、多维的数据做进一步的分析，进而使业务决策由原来的经验主导向现在的数据主导转变。

大数据分析在电力营销领域应用范围广。对用户用电曲线进行聚类分析，可以得到更加详细的客户画像，发现不同群体用户的用电习惯和消费偏好。根据画像数据实施精准营销，在夜间用电高峰时给用电高峰时段的用户推销峰谷电价套餐，对近几年用电量逐年提升的工业用户推销能效诊断服务等等。大数据分析可以大大改善运营效率，

1. 精准负荷预测：利用历史用电数据、天气情况、社会经济活动等各方面数据来创建更加精确的负荷预测模型，给电网调度和电力市场交易提供决策支持。

2. 客户信用评定：从用户的缴电情况、用电的稳定性等方面入手建立客户的信用评分模型，根据不同的信用等级对用户采取不同的授信和催收措施。

3.3、用机器学习算法在大量的数据里找出异常用电行为，从而大幅度地提高稽查的精确率和效率。

（三）未来营销系统发展趋势

电力营销系统今后的发展趋向智能化、平台化、生态化，成为新型电力系统创建和能源互联网发展主要的支撑平台。未来营销系统发展趋向可参考下表。

电力营销系统未来发展趋势表

发展趋势	核心特征	主要体现
智能化	融合人工智能技术	智能客服、精准预测、预测性维护
平台化	开放能源服务平台	接入分布式能源、支持市场交易、聚合商 / 虚拟电厂入口
生态化	能源生态创造者	开放 API、P2P 交易、绿证溯源、综合能源服务

系统将会充分发挥人工智能的作用，人工智能驱动的智能客服可以给用户带来更加人性化的、全天候的人机交互体验，基于深度学习的负荷预测、市场分析会更准确，根据计量设备运行的数据提前预知可能发生的故障，从被动应对转为自动维护。

系统将从封闭式业务处理系统转变为开放式的能源服务平台。随着分布式光伏、储能、电动汽车等分布式能源的不断增多，营销系统不仅要能够接入这些数量众多、分布广泛的源、荷、储资源，还要对其实施计量、监控以及协调控制。它将成聚合商、虚拟电厂等新兴市场主体参加需求响应、辅助服务等市场化交易的入口以及结算平台，从而支持“源网荷储”之间友好互动。

营销系统会变成能源生态的创造者。利用开放 API 接口，吸引第三方开发者参与进来，共同开发各种各样的能源服务应用，综合能源服务、电动汽车充电服务、智能家居、碳足迹管理等。区块链等去中心化技术在 P2P 电力交易、绿证溯源等方面会有一定的作用，可以创建更加透明可信的交易环境。未来的电力营销系统，不会只是销售电能的工具，而会是推动社会能源消费方式变革、创造多种价值的智慧能源服务中心。

第四节 调度自动化系统

调度自动化系统是现代电力系统的神经中枢，也是保证电网安全、稳定、经济运行不可缺少的技术支撑。它把先进的计算机技术、通信技术以及控制理论结合在一起，对大规模的电力网络实行全方位的实时监控、分析、决策以及控制。本节详细阐述调度自动化系统结构，核心技术和发展方向来体现它在电力信息系

统中的重要性和实践价值。

一、系统组成与核心功能

调度自动化系统是一个复杂的综合性的技术平台，可以对电网运行的全方位情况做出感知与控制。该系统一般由若干相互协作的子系统组成，各司其职，共同保证发电、输电、配电各环节协调运转，形成一个有机的整体，保证整个电力系统脉动。

调度自动化系统的主要核心组件及其功能见下表。

调度自动化系统核心组件

组件	核心功能	关键特点 / 技术	主要价值
能量管理系统	电网实时监控、分析、决策与控制	数据采集与监控、网络拓扑、状态估计、安全分析、自动发电控制、经济调度	确保电网安全、经济运行；辅助调度决策
广域测量系统	电网动态实时监测与分析	同步相量测量单元、毫秒级同步采样、GPS 时间同步	提供广域、同步、实时动态信息；提升电网动态稳定性感知与分析能力
调度员培训模拟系统	调度员技能培训与应急演练	强大的仿真引擎、电力设备及保护装置模拟、多样化场景模拟	提高调度员业务水平与应急响应能力；验证新策略与技术

（一）能量管理系统

能量管理系统简称 EMS，是调度自动化系统的大脑和中枢神经，担负着保证电网安全、经济调度的责任。它依靠数据采集和监控系统，网络拓扑分析，状态估计，安全分析，自动发电控制等众多高级应用，给调度员提供全方位，多层次的电网运行景象，而且还有许多辅助决策工具。SCADA 功能让 EMS 可以随时得到全网电压、电流、功率等重要运行数据，还能监视断路器、隔离开关这些设备的工作情况。

在数据采集的基础上，EMS 用网络拓扑分析功能实时地构造出和实际电网接线方式一致的模型，为后面的潮流计算、安全分析提供准确的基础。按照系统频率偏差、联络线功率交换计划准确地调节发电机组的出力，保证电网实时功率平衡、频率稳定。这些功能互相配合，就使得 EMS 既能够掌握电网的现状，又可以预知电网的发展趋向，从而达到对电网进行精细化经营和操控的目的。

EMS 通过经济调度功能，以满足所有的安全条件为前提，安排各发电机组的最低成本出力计划，达到电力资源的优化分配的目的。系统在存在潜在故障风险的时候，安全分析模块可以模拟各种预想的事故，对系统的安全性进行评价，并提前向调度员发出预警，给采取预防性控制措施留出时间，有效地防止连锁故障的发生，提高电网的韧性。

（二）广域测量系统

广域测量系统简称 WAMS，是以同步相量测量单元为基本单元而建立的一种新型电网动态监测与分析系统，给调度自动化提供前所未有的时空同步数据维度。WAMS 和传统的 SCADA 系统不一样，它每秒钟采样的次数不是重点，而是以比秒更小的时间单位，也就是毫秒级别，去采集分布在全国各地电网各个节点上的电压、电流的相量，并且依靠高精度的时间同步，一般会采用 GPS 作为时间源，使得所有被采集的数据具备相同的时间基准。因此 WAMS 可以准确地捕捉到电网受到扰动之后的发展变化过程，对系统的功率角、频率、电压的变化规律进行更加细致的研究。

WAMS 的主要价值在于给调度中心提供广域、同步、实时的动态信息，大幅度地提高了调度中心对电网大范围动态行为的感知能力。利用 WAMS 数据可以开发出低频振荡在线监测与抑制、暂态稳定性快速评估、电压稳定性实时监测等一系列高级应用。通过分析节点间的相角差来判定系统的稳定裕度，可以及时发现使系统产生失步的隐患。故障发生后，WAMS 记录的同步数据对事故精确分析和快速复盘来说，是任何其他数据都无法替代的，它可以用来评价保护装置的动作行为，改进系统运行策略。

（三）调度员培训模拟系统

调度员培训模拟系统简称 DTS，是电力调度领域不可缺少的重要工具。用仿真环境模拟真实的电网，给调度员提供了一个零风险的培训和演练平台。DTS 可以模拟多种电力操作、复杂的故障情景以及电网的正常运行情况，调度员可以在近似的环境中进行业务技能的练习、应急操作的演练，进而提高调度员的业务水平及心理素质。

系统的核心是强大的仿真引擎，可以对发电机、变压器、输电线路等各种电力设备在各种工况下的物理特性进行精确的仿真，并且还可以对继电保护和自动装置的行为进行仿真。在 DTS 环境下调度员可以发出潮流调整、倒闸操作、事

故处理等各种调度指令，并即时观察系统对这些操作的反应。身临其境的培训效果比理论学习要好得多。

DTS 既用作新调度员入职培训，也用在资深调度员提高解决罕见、复杂的故障上。定期举行大范围停电事故、连锁故障等极端情景下的模拟演练，可有效检验并完善应急预案的科学性以及操作性，从而保证当真实危机发生时调度团队可以沉着冷静，应对有方。

DTS 也可以用作新技术、新方法的实验平台。新的控制策略或者自动化功能在真正启用之前，可以利用 DTS 做充分的安全性以及经济性检测与验证。这可以缩减技术应用的风险，加快电网调度技术的更新速度，为塑造更为智能，更加可靠电力系统打下根基。

二、关键技术应用与挑战

调度自动化系统的发展要依靠一些关键技术的支持和推动。这些技术对于提高系统的性能、拓展系统的使用功能起着举足轻重的作用。海量数据实时处理、底层模型精准建模、复杂决策智能分析等等每一个技术的突破都会给电网的精细化、智能化调度带来新的可能。但是，技术应用的同时也会出现新的问题。

（一）实时数据库技术

实时数据库是调度自动化系统的核心，主要用来存储和管理电网各个采集点大量、高并发的实时数据。不同于一般的数据库，电力实时数据库要具有很高的数据吞吐率以及很低的读写延迟，这样才能符合调度系统对数据实时性的要求。它使用专门为时序数据设计的存储引擎和索引，保证每一个调度周期（一般为秒级）内数百万甚至上千万个数据点可以被快速更新、查询和计算，从而保证调度员和上层应用获取到的电网状态快照是最新的、最准确的。

目前实时数据库面临的主要难题就是数据量激增和数据种类繁杂。新能源大规模并网、AMI 部署以后，数据点数激增，数据更新速度也变得越来越快。除传统的 SCADA 数据之外，WAMS 产生的各种高速相量数据、气象数据、设备状态监测数据等也要集成到一个统一的管理平台中。这就对新一代的实时数据库提出了更高的要求：能够横向扩展来应对数据量增大的情况，可以处理各种类型的结构化和非结构化的异构数据，还要能够提供灵活的数据服务接口以满足上层应用复杂的分析需求。

（二）电力系统状态估计与安全分析

电力系统状态估计和安全分析都是能量管理系统里的高级应用，二者一同给电网的可靠运行赋予科学的决策支撑。

1. 电力系统状态估计就是利用带有测量误差、冗余的、从 SCADA 系统获取的量测数据，采用最优估计算法，求解整个电力系统最可能的运行状态。本质上就是对数据进行清洗、校正，去除量测中的坏数据，求出网络中所有母线的电压幅值和相角。准确的状态估计是潮流计算、安全分析、最优潮流等高级应用的前提。随着广域测量系统的广泛应用，怎样有效地将高精度的 PMU 同步相量数据与传统的 SCADA 异步数据融合起来，是提升状态估计精度和动态性能的关键技术途径。

2. 电力系统安全分析以状态估计得到的当前网络运行状态为基准，对预设的各种故障（线路跳闸、发电机或者变压器停运等）进行仿真计算，以判断系统在发生这些故障之后是否会出现过载、电压越限等问题。预演式的分析可以提前发现电网的薄弱环节、风险点，并制定相应的预防措施，把事故扼杀在萌芽之中。目前安全分析所面临的难题就是计算速度和模型精度的权衡。大容量交直流混合电网的动态安全问题，必须要设计出更加高效的算法来满足实时在线决策的要求。

（三）多时间尺度数据融合与处理

现代电力系统数据明显地具有多时间尺度的特征，WAMS 的毫秒级同步相量数据、SCADA 的秒级遥测数据、负荷预测的分钟级或者小时级数据、计划编制的长周期数据，一起构成了电网运行状态的全貌。多时间尺度数据融合处理技术，就是把各种来源、不同时间分辨率、不同精度的数据加以整合并协同分析，从而找出单个数据源无法显示的深层信息，给调度决策给予全面准确的支持。

该技术主要的难题就是解决各个数据源之间异构性、时空不匹配等状况。怎样将 WAMS 提供精确动态信息和 SCADA 提供完整稳态信息结合起来，提高状态估计的准确性以及动态反应能力？在负荷预测时又如何把高频的实时用电数据、低频的气象预报信息和社会经济活动等很多因素融合到预测模型中，从而提高预测准确性？要解决上面的问题，就需要用到信号处理、数据挖掘、机器学习等很多技术，构建起一个能够自适应处理各种尺度上多模态数据的智能分析体系，把数据变成信息，再把信息变成知识，从而支持智能调度控制。

三、未来发展与展望

随着“双碳”目标的提出、能源革命的不断深入，电力系统正处在前所未有的大变革之中。调度自动化系统是电网运行的大脑，它的必然趋势就是越来越智能、高效、协同。新技术不断出现，会给解决未来电网的复杂性、不确定性带来巨大的推动力，使调度模式发生根本变化。

（一）与新能源预测系统深度融合

随着风能、太阳能等可再生能源在电力结构中所占比例的迅速增加，它们自身所具有的波动性、间歇性给电网的安全稳定运行带来了巨大的难题。因此调度自动化系统要与新能源预测系统前所未有的紧密结合。这不只是简单地接上一些数据，它涉及到对调度决策过程进行彻底的改变。高精度的新能源功率预测，尤其是短期和超短期预测，将会成为日前发电计划制定、日内滚动调度的重要输入。

未来调度系统可以按照预测结果，提前做多时间尺度的随机性场景分析，预估各种新能源出力情况下的电网运行风险，从而改进备用容量的安排和调整方法。当系统预测到未来数小时内因为云层遮挡导致光伏出力急剧下降时，就会提前启动应对措施，即快速响应的燃气机组或者调度储能装置放电，从而维持电网频率的稳定。

深度融合就是调度策略由原来的“源随荷动”模式变为“源网荷储”协同互动模式。新能源预测系统给出“源”侧不确定性的观测结果，调度自动化系统按照这些观测结果来安排电网的传输能力、柔性负荷的响应能力和储能系统的充放电能力，从而使新能源得以高效地被利用，并使系统整体处于最优状态，于是就产生了一个更为灵活且具有韧性特征的电力系统。

（二）人工智能在调度决策中的应用

以深度学习和强化学习为代表的人工智能技术正在为解决电力调度复杂决策问题开辟新途径。传统上依靠精确的模型以及优化算法来进行调度的方法，面对新型电力系统的高不确定性、高复杂性时，计算维度大、求解速度慢的问题越来越突出。但是 AI 技术可以依靠大量的历史数据来学习隐藏的规律和模式，给调度决策提供强有力的“数据驱动”的支持。

在负荷预测以及新能源出力预测上，深度学习模型就有着优于以往所有统计方法的性能。故障诊断和处理中人工智能可以对大量的报警信息、故障录波数据

进行剖析，并快速地发现故障原因并给出最佳的恢复方案来缩短停电时间。强化学习技术也被寄予厚望，来解决电网的动态最优控制问题。仿真环境中大量试错学习，强化学习智能体可以自主学习各种复杂的电压调节、频率控制、潮流优化策略，决策能力可以超过传统的依靠预设规则的自动控制系统，媲美经验丰富的调度专家。

未来有众多的人机合作型的调度自动化系统会含有 AI 内核的智能决策。AI 系统可以对大量的信息进行快速分析并给出建议，但是由人类调度员来负责审查确认，并处理那些比较复杂、不常见且不能由 AI 系统独自解决的案件。调度工作更加准确高效，电网调度向着智能化的方向前进。

（三）构建新一代智能调度控制系统

为了应对能源转型所带来的一切变化，创建可以适应未来电网形态和运行特点的新型智能调度控制系统，已经成为行业共识。新的系统将会形成一个物理上分布、逻辑上统一的云边协同体系，具有全景感知、智能决策、高效协同控制的能力。

1. 全景感知、云边协同，未来的调度系统会把 WAMS、PMU、智能电表、在线监测装置、卫星气象等各种感知数据汇集起来，形成一个囊括“源网荷储”全部环节的数字孪生电网。数据处理使用云边协同架构：边缘侧（变电站或者区域控制中心）完成就地数据处理和快速控制，实现毫秒级响应；云端（主调度中心）汇聚全网络的数据，依靠强大的计算力做全局分析、趋势预测、顶层策略优化等，实现物理系统和数字空间之间的实时同步、虚实互动。

2. 主配一体化和协同调控，由于大量分布式光伏、电动汽车充电桩、储能等接入配电网，传统的主站管输电、子站管配电的调度模式已经不能适应。新一代系统会冲破输配电网的调度壁垒，达成主配一体化的规划与运作。利用先进的配电自动化和通信技术，调度中心可以对大量的分布式能源进行聚合、监视和控制，将它们当作虚拟电厂来参与系统级的平衡和调节，这样就使电网变得更加灵活，资源的利用效率也更高。集中控制和分布自治相结合，自上而下和自下而上相融合的模式，将成为智能调度的主要特点。

参考文献

[1] 李显.电力信息系统安全防护智能预警模型设计[J].自动化仪表, 2025, 46(2):85-91.

[2] 高明慧,崔旭东,李勃,等.电力信息系统网络安全配置核查方法研究[J].微型电脑应用, 2025(6).

[3] 高国庆,徐天竹,屈巍,等.电力信息系统网络安全态势智能评估方法[J].微型电脑应用, 2024, 40(11):145-148.

[4] 谢炯,李祺,陈晓宇.大数据驱动的电力信息系统非法入侵行为识别方法[J].电子设计工程, 2025(16).

[5] 刘立亮,文涛,叶磊.基于卷积神经网络模型的电力信息系统安全状态监测[J].电气自动化, 2024, 46(5):11-14.

[6] 王国峰,唐云善,徐立飞.电力信息系统软件代码漏洞检测系统的设计与实现[J].微型电脑应用, 2023, 39(11):118-121.

[7] 尹卓超.GIS技术与开源云计算在电力信息系统数据集成中的应用[J].自动化与仪器仪表, 2025(3).

[8] 凌玲,沈志宏,张良,等.基于动态口令的电力信息系统用户身份自动认证方法[J].信息技术, 2025, 49(5):84-88.

[9] 路朋,陈思捷,张宁,等.计及区间预测信息的含风电电力系统有功多时间尺度协调调度优化方法[J].中国电机工程学报, 2024, 44(16):6263-6277.

[10] 杨挺,李浩,赵宇明,等.电力信息物理系统故障通信恢复策略[J].电网技术, 2025(1).

[11] 刘雨晴,刘墅,王小君,等.融合同步知识和时空信息的电力系统暂态稳定评估框架[J].电网技术, 2025, 49(6):2334-2346.

[12] 樊强,刘东,王宇飞,等.电力信息物理系统形态演进关键技术及其进展[J].中国电机工程学报, 2024(21).DOI:10.13334/j.0258-8013.pcsee.230658.

[13] 严康,陆艺丹,白晓清,等.电力信息物理系统需求操控攻击策略及防护分析[J].

电力系统自动化, 2025(8).
[14] 董昱,周劼英,张晓,等.新型电力系统信息物理安全防护体系研究[J].中国电机工程学报, 2025(15).
[15] 彭飞,田增垚,张晓华,等.基于量子安全的电力信息系统安全增强方法研究[J].重庆大学学报, 2024, 47(2):62-74.
[16] 何瑞文,陆嘉亮,杨长鑫,等.新型电力系统下电力二次系统仿真的设计方法[J].上海交通大学学报, 2025, 59(11):1581-1591.DOI:10.16183/j.cnki.jsjtu.2023.556.
[17] 胡炎,谢小荣,韩英铎,等.电力信息系统安全体系设计方法综述[J].电网技术, 2005, 29(1):5.DOI:10.3321/j.issn:1000-3673.2005.01.008.
[18] 胡炎,谢小荣,辛耀中.电力信息系统现有安全设计方法分析比较[J].电网技术, 2006.DOI:JournalArticle/5ae19b54c095d71120ae7643.
[19] 陈郑平,王先培,王泉德,等.弹性文件系统在电力信息系统中的应用[J].电网技术, 2005(23):5.DOI:10.3321/j.issn:1000-3673.2005.23.015.
[20] 王保义,王蓝婧.电力信息系统中基于属性的访问控制模型的设计[J].电力系统自动化, 2007, 31(7).DOI:10.3321/j.issn:1000-1026.2007.07.017.
[21] 李红升.基于粒子群算法改进电力信息系统的安全研究[J].科技通报, 2013.DOI:CNKI:SUN:KJTB.0.2013-04-056.
[22] 曲朝阳,刁赢龙,薄小永,等.基于多预测树组合算法的电力信息系统数据库缓存模型[J].电测与仪表, 2014, 000(006):70-75.
[23] 高翔,陈贵凤,赵宏雷.基于数据挖掘的电力信息系统网络安全态势评估[J].电测与仪表, 2019.
[24] 蒋宏图,袁越.电力系统自动化综合应用信息平台设计与实现[J].电力自动化设备, 2009, 29(5):113-113.DOI:CNKI:SUN:DLZS.0.2009-05-027.
[25] 胡炎,谢小荣,辛耀中.电力信息系统建模和定量安全评估[J].电力系统自动化, 2005, 29(10):6.DOI:10.3321/j.issn:1000-1026.2005.10.007.