# 电力运维监控如何安全跨网闸数据同步

技术方案与实践深度解析

2026年电力行业运维专题分享

# 演讲目录

# PART 01

# 开篇与行业背景

洞察能源行业的时代变革，理解驱动运维模式升级的核心因素
在技术浪潮中把握机遇，构建面向未来的电力系统

# 演讲开场：从一个真实场景切入

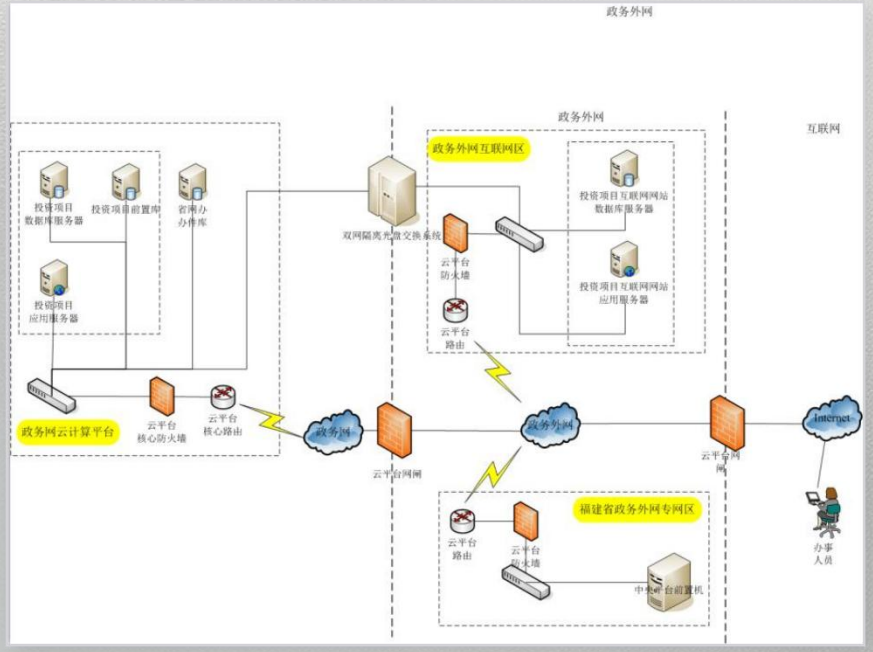
2026年迎峰度夏关键期，电力系统稳定关乎国计民生。调度数据网作为电网“神经网络”，其安全是基石。我们面临的核心挑战是：如何在严守“横向隔离”安全规定的前提下，实现跨安全区的统一、高效、安全的运维监控？

## 典型场景：省级调度中心的现实困境

某省级电力调度中心需统筹管理下属多地调的上万台IT设备。依据国家强制规定，承载实时控制的**生产控制大区（Ⅰ/Ⅱ区）**与承载管理信息的**管理信息大区（Ⅲ/Ⅳ区）**之间，必须部署单向物理隔离装置（网闸）。数据仅允许从生产区单向流向管理区，严禁反向连接，这直接造成了运维数据“看得见却摸不着、管不了”的现实难题。

# 核心矛盾：网闸带来的运维困境

传统监控工具无法跨网闸数据同步，导致生产区的设备状态与运行数据无法安全合规地同步至管理区，管理者难以实现全域统一监控，故障排查效率大幅降低，形成了运维管理的“数据孤岛”。




## 01 生产控制大区（安全Ⅰ、Ⅱ区）

承载电网核心调度指令与实时生产控制，是保障电力系统稳定运行的“大脑”，对数据传输的实时性、完整性和安全性有着极高要求，任何外部干扰都可能引发严重后果。

## 02 管理信息大区（安全Ⅲ、Ⅳ区）

涵盖生产管理、营销服务及日常办公等业务，是电力企业运营的“躯干”。该区域需支撑海量业务数据处理，同时面临来自互联网的潜在安全威胁，需兼顾业务协同与边界防护。

## 03 不可逾越的隔离红线

两区之间必须部署**电力专用横向单向安全隔离装置**，数据仅允许从生产区单向流向管理区，严禁任何反向连接或通用网络协议穿透，从物理层面阻断外网向内网的攻击路径。

# 深刻变革的两大背景：信创与安全

两大背景交织，形成当前电力运维的核心矛盾与挑战

“既要推进信创国产化替代，打破核心技术依赖，又要满足日益严格的等保合规与安全隔离要求，同时还要兼顾运维的高效性与监控的实时性。”


### 01 信创国产化：规模化落地加速

从核心芯片、操作系统到数据库的全面国产化替代，电力行业正构建自主可控的数字底座，推动业务系统向信创环境无缝迁移，实现技术自主与产业升级。

### 02 网络安全：攻防对抗形势严峻

全球能源基础设施成为网络攻击重灾区，勒索病毒与APT攻击威胁加剧。电力行业需严守“双网隔离”红线，构建主动防御体系，确保电网运行万无一失。

# 信创国产化进入规模化落地阶段

从“信创”到“可信信创”：电力运维的时代命题
这两个宏观背景交织在一起，指向同一个结论：电力行业的信创替代，不能只停留在“换设备、装软件”的层面，必须上升到“可信信创”的高度。

电力行业作为国家关键基础设施，信创已成为不可逆转的行业趋势。2026年，电力信创正式从试点探索迈入规模化落地的关键阶段，政策指引明确、市场应用深化、技术生态完善，行业转型步伐全面加速。

# 信创带来的核心运维挑战

国产化设备的快速普及打破了传统IT架构的平衡，市场上缺乏成熟的全栈式监控方案，大量国产软硬件因协议私有、架构差异无法被传统工具识别，形成了难以察觉的“监控盲区”，成为系统稳定性的潜在隐患。

### 01 国产化操作系统

涵盖凝思、麒麟、统信UOS等。内核与指令集差异显著，传统监控探针难以适配，导致基础运行环境的资源、进程监控失效。

### 02 自主可控数据库

包括达梦、人大金仓等。私有协议与非标准接口使得传统工具无法解析其内部锁、会话及事务状态，数据层风险不可见。

### 03 国产算力服务器

以浪潮、联想为代表。ARM架构与x86差异巨大，硬件指标采集无统一标准，底层硬件故障难以通过传统方式及时预警。

### 04 全栈信创基础设施

如华为鲲鹏、昇腾生态。从芯片到整机的全栈自研体系，缺乏通用的监控插件支持，软硬件监控数据形成信息孤岛。

# 背景二：全球电力系统网络安全形势空前严峻

## 关键基础设施已成攻击重灾区

近年来，针对全球电网的网络攻击事件频发，不仅造成巨大经济损失，更引发了严重的社会秩序动荡，电力系统的网络安全已上升至国家安全战略高度。

**2018年**

俄指控美黑客组织对其能源基础设施发动长达两年的网络攻击，导致部分地区电力供应中断，暴露了工控系统的脆弱性。

**2020年底**

美政府机构遭大规模网络入侵，调查显示攻击者已渗透至关键基础设施领域，引发对能源供应链安全的广泛担忧。

**2020.12**

美国能源部发布禁令，限制特定电力系统产品进口，标志着全球能源领域的技术博弈与安全审查进入新阶段。

### 行业启示：隔离是生存的“必答题”

面对日益复杂的网络威胁，传统的防护手段已不足以应对。**“横向隔离”**不再是可选项，而是保障电力系统安全稳定运行、确保企业合规经营的刚性要求与底线思维。

# PART 02

# 政策演进与合规红线

回溯监管政策的演进脉络，明确行业不可逾越的合规底线，
为技术落地与业务发展构建坚实的安全屏障。

# 电力监控系统安全防护政策演进时间轴

## 2005 · 行业奠基

原电监会发布5号令，确立“**安全分区、网络专用、横向隔离、纵向认证**”十六字原则，成为电力二次系统安全防护的纲领性文件，奠定行业安全基准。

## 2014 · 深化细化

发改委14号令与能源局36号文联合发布，针对省调、地调、发电厂及变电站等核心场景，完成安全防护方案的细则落地与标准化规范。

## 2024 · 迭代升级

发改委27号令发布（2025年施行），新增“**安全免疫、态势感知、动态评估**”等主动防御要求，再次明确电力专用横向单向隔离装置的强制部署要求。


### 政策演进核心洞察

从“被动合规”向“主动免疫”转型，政策持续加码推动电力监控系统从单点防护迈向全生命周期的体系化防护，为新型电力系统的数字化、智能化转型筑牢安全底座。

# 2026年新规：从“合规要求”到“重大隐患判定”

## 合规不再是“可选项”

2026年4月9日，国家发改委发布第41号令（2024年第27号令修订，2025年施行），将电力监控系统网络安全要求从“合规项”直接升格为“重大事故隐患判定标准”，自7月1日起正式施行。这标志着网络安全防护已成为电力行业不可触碰的红线。

### 01 横向隔离：生产网与外网的物理屏障

生产控制区与管理信息区、安全接入区连接处，未部署**电力专用横向单向安全隔离装置**，即构成重大隐患，是网络边界防护的核心底线。

### 02 纵向加密：广域网通信的加密认证

生产控制区与专用网络广域网连接处，未部署**电力专用纵向加密认证装置或网关**，导致数据传输缺乏加密防护，属于关键通信链路的重大安全漏洞。

### 03 非法连通：绝对禁止的内外网直联

生产控制区内部网络与外部网络（含互联网、跨区直联）发生**非法连通**，直接破坏网络安全边界，是必须零容忍的重大违规行为。

# 新规重点解读与核心结论

合规红线不可触碰，技术方案必须满足单向、安全、可审计的要求

## 01 严守“单向传输”铁律

数据流向严格限定为“生产区→管理区”，严禁反向访问。任何试图从管理区直接穿透至生产区的行为，均被直接判定为重大安全隐患，是合规审查的绝对红线。

## 02 安全数据全流程留痕

严禁关闭、破坏安全防护设施，或篡改、销毁日志、告警及审计数据。安全设备产生的全量数据需完整留存、可追溯，其完整性是判定合规性的核心依据。

## 核心结论：合规从“可选项”升级为“必答题”

41号令的施行标志着电力运维合规进入“硬约束”时代。所有跨安全区的运维监控方案，必须以满足“横向隔离、纵向认证”为前提，任何绕过网闸或违规穿透的技术手段，均存在极高的合规风险与安全隐患，企业需将合规性作为方案设计的首要原则。

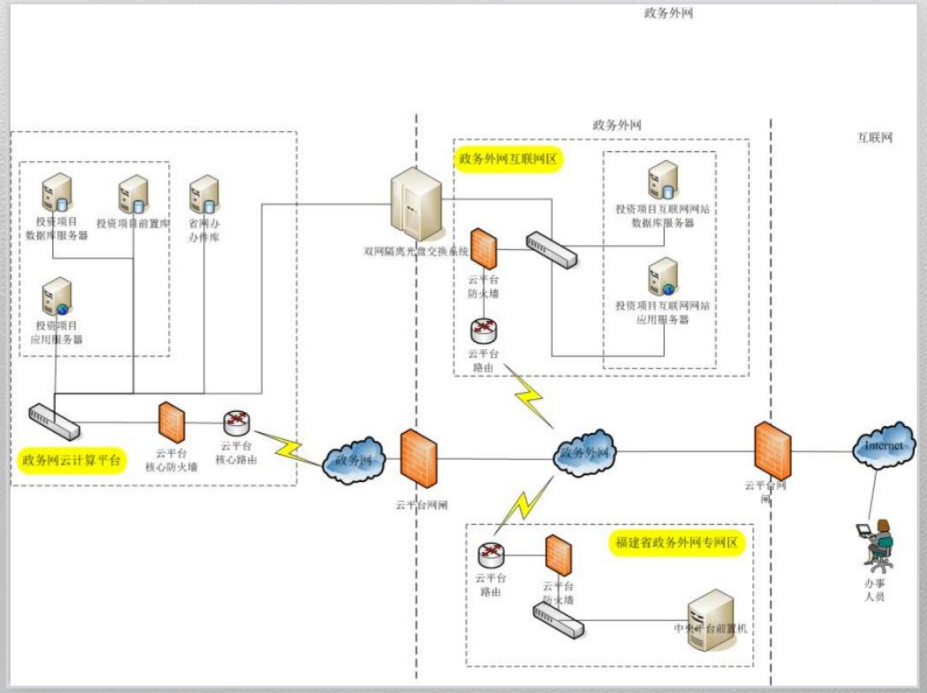
# PART 03

# 电力运维监控面临的四大挑战

随着新型电力系统建设加速，运维监控在海量数据处理、实时响应速度、安全防护等级及多源设备兼容上面临严峻考验，成为制约效率提升的关键瓶颈。

# 挑战一：网络物理隔离，监控数据难以汇聚

传统监控工具无法跨网闸数据同步，生产区设备状态无法实时获取




图示：电力系统多安全分区与网闸隔离网络拓扑

### 监控穿透难，数据链路断层

SNMP、SSH等传统协议无法跨越物理网闸，导致省调中心与地调生产区（I/II区）的数据链路断裂，关键设备状态无法实时回传。

### 运维视图割裂，故障排查低效

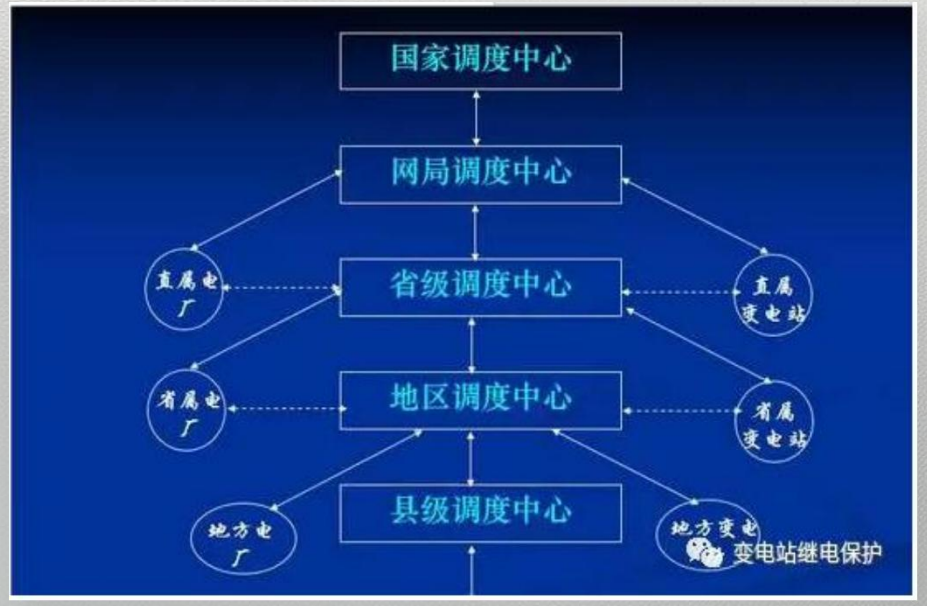
缺乏统一的全局监控平台，运维人员需频繁切换多套孤立系统进行故障定位，跨区协作耗时费力，平均响应时间大幅增加。

### 数据孤岛效应，决策缺乏支撑

生产区的告警、性能、日志等数据无法汇聚分析，形成信息孤岛。管理层难以基于全量数据进行趋势预判，隐患识别滞后。

# 挑战二：多层级架构，统一视图难以构建

电力调度系统呈现“多层级、跨区域、跨安全域”的复杂复合结构，层级间系统独立运行，数据无法互通，最终形成大量难以打破的“信息孤岛”，制约了调度效率与安全防御能力。




图示：电力调度四级分布式架构体系示意

### 信息壁垒：数据孤岛林立

各级调度系统独立建设、标准不一，跨层级、跨安全区的数据无法实时互通，形成物理与逻辑上的双重割裂，数据价值难以挖掘。

### 排查低效：故障定位繁琐

电网异常时，运维人员需频繁切换多套孤立系统，人工比对碎片化数据，无法快速串联故障线索，导致故障定位耗时费力，延误处置时机。

### 视野受限：缺乏主动防御

缺乏全网统一的全景态势视图，调度中心难以实时掌握跨区域运行状态，无法实现风险的提前预警与主动干预，运维决策被动且滞后。

# 挑战三：国产化设备缺乏统一监控方案

随着信创战略的深入推进，电力行业已规模化引入凝思OS、达梦数据库、华为云平台等国产化基础设施。然而，由于生态适配滞后，市场上缺乏成熟的统一监控方案，大量关键设备成为“监控盲区”，无法被传统运维工具有效感知，给系统的持续稳定运行埋下了隐患。

### 标准缺失，方案碎片化

国产软硬件架构差异大，缺乏统一的监控数据采集标准。现有监控方案多为厂商定制开发，难以跨品牌、跨平台规模化复用，维护成本高昂。

### 感知断层，形成监控盲区

部分国产操作系统与数据库未开放标准监控接口，传统工具无法识别和采集关键运行指标，设备状态如同“黑盒”，故障无法被及时发现。

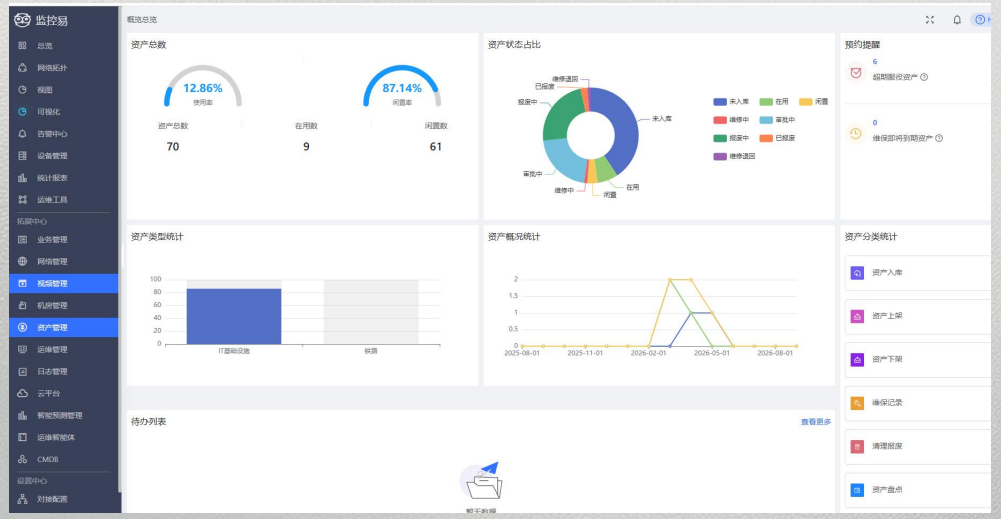
### 预警滞后，风险难以管控

无法实时掌握设备健康度，运维人员难以预判潜在故障。一旦发生异常，往往已造成系统中断，严重影响电力生产调度的连续性与安全性。

典型国产化信创环境

# 挑战四：设备资产状态无法实时感知

资产从“静态管理”到“动态感知”的断层，制约IT运维效能提升与资源优化配置




通过智能巡检机器人等前沿技术，打破传统静态台账的信息滞后性，实现对电力基础设施运行状态的全天候、无死角主动感知。

核心困境：目前电力设备资产信息多局限于调控云的静态台账（如型号、配置），缺乏对CPU负载、网络吞吐、数据库连接等动态运行数据的实时采集。这导致运维团队难以预判设备健康度，既无法避免资源闲置浪费，也难以在故障发生前及时预警，制约了资产的精细化调度。

### 算力层监控

实时采集CPU利用率、内存水位、磁盘I/O吞吐量及网卡流量，精准定位服务器资源瓶颈，避免性能过载。

### 网络层感知

监测网络设备端口流量、带宽利用率与丢包率，快速识别链路拥塞节点，保障电力业务数据传输畅通。

### 数据层透视

追踪数据库连接池状态、SQL请求并发量及锁等待情况，防止事务阻塞，保障核心业务数据服务高可用。

# PART 04

## 解决方案：四级分布式架构 + 跨网闸合规数据同步

构建高可用、高安全、高合规的全域数据协同体系，打破物理隔离限制，实现多级节点间的数据实时联动与安全共享，重塑政企数据流转新范式。

# 核心思路：穿透而非绕过，合规实现数据汇聚

方案摒弃“绕过”网闸的风险模式，核心是在合规框架内实现数据的安全“穿透”。严格遵循国家“横向隔离、纵向认证”的安全规范，通过技术手段打破数据孤岛，在保障生产网绝对安全的前提下，实现数据的高效汇聚与价值挖掘。

## 01 分布式采集

在生产区与管理区内部署轻量化采集代理，贴近数据源进行实时采集与边缘清洗。此举避免了跨区直接拉取数据的风险，从源头减少安全暴露面，同时保证了数据的实时性与原始完整性。

## 02 合规推送

依托单向网闸构建物理隔离通道，实现生产区向管理区的单向数据流动。传输全程采用加密协议，并经过严格的合规性校验，符合等保与电力监控安全规范，彻底杜绝外部网络的反向渗透风险。

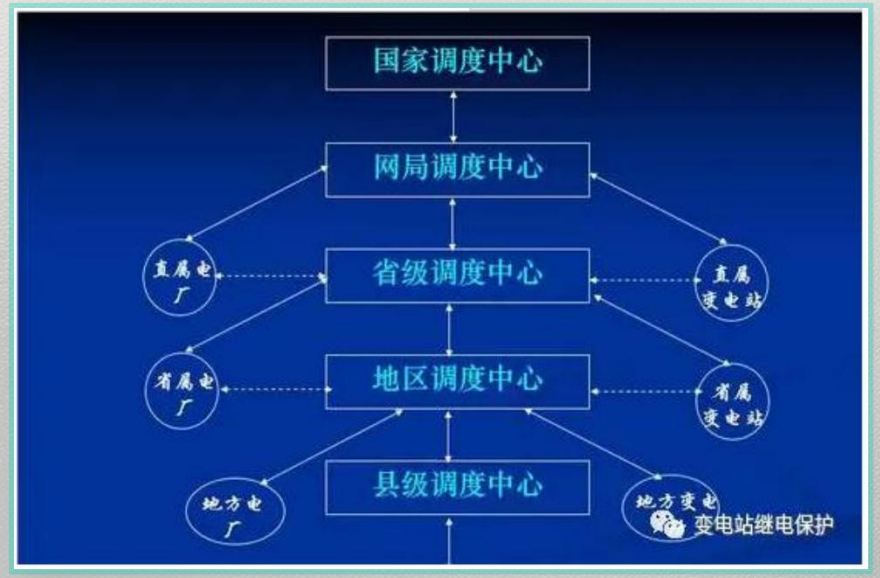
## 03 分级管理

构建“现场-场站-分中心-总部”四级管理架构，实现数据分级汇聚与权限管控。支持告警信息的本地研判与分级上报，既保障了集团层的全局统一监控，又赋予了各场站自主运维与快速应急处置的能力。

以合规为基石，以技术为桥梁，实现工业数据的安全互联与价值最大化

# 四级分布式架构，支撑多层级统一管理

从顶层设计上解决“多层级、跨区域、跨安全域”的管理难题，构建高效协同的管控体系




图示：四级分布式架构层级逻辑与数据流向示意

## 01 省调总控层 (GCCU)

**部署：**省调中心核心节点。作为全局指挥中枢，负责全网数据的最终汇总、统一监控展示、全局资源视图呈现及跨区域告警的集中指挥调度。

## 02 地调集中管控层 (CCU)

**部署：**各区域地调中心。作为区域管理节点，统筹本区域采集任务分发、数据清洗汇聚、告警分级研判与故障快速定位，承接并执行省调指令。

## 03 采集处理层 (TS)

**部署：**变电站及本地机房。作为数据感知触角，实时采集服务器、网络、数据库等设备的性能指标，进行本地预处理与异常初判，减轻带宽压力。

## 04 全域监控对象层

**覆盖：**生产控制大区（Ⅰ/Ⅱ区）及管理信息大区（Ⅲ区）。全面纳入服务器、网络设备、存储资源、数据库及业务应用，实现基础设施无死角监控。

# 四级分布式架构的核心优势

兼顾全局管控与区域自主，实现高效、灵活的运维管理

## 数据分散采集

摒弃单点采集的性能瓶颈，显著提升大规模监控效率，可稳定支撑省级电网数万台设备的并发接入与实时数据处理需求。

## 告警本地处理

关键告警无需上传中心层即可本地发现与处置，实现毫秒级响应，大幅缩短故障处理周期，避免因网络延迟导致的处置滞后。

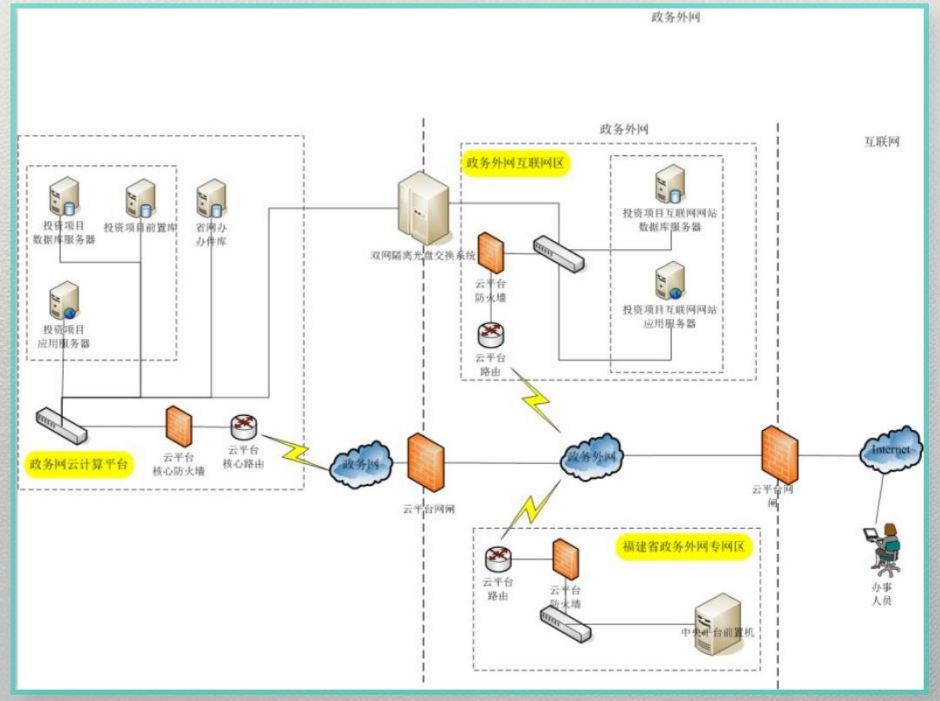
## 信息分级上传

数据按需、分级向中心传输，有效减轻云端服务器负载，契合电力行业分级管理规范，实现全网“一盘棋”的统筹调度与管理。

## 跨安全域适配

采集节点可灵活部署于生产区与管理区，通过合规单向传输技术打通数据链路，完全满足电力系统横向隔离的安全防护标准。

# 跨网闸数据同步：合规穿透物理隔离




## 实时数据：协议级单向直传

针对告警、遥信变位等高频数据，利用网闸支持的专用安全交换协议实现毫秒级单向传输，在满足物理隔离合规要求的同时，确保调度数据的实时性与准确性。

## 批量数据：加密文件摆渡机制

对于历史日志、性能报表等大容量数据，采用定时加密摆渡模式。数据经压缩加密后写入网闸前置区，管理端单向拉取解析，兼顾传输效率与数据资产安全。

**合规与实效双赢：**该方案完美适配电力行业“横向隔离、纵向认证”的安全防护规范，成功打破生产控制区与管理信息区的信息孤岛。省调中心可实时汇聚全域设备状态，为智能调度、故障研判及电力大数据分析提供完整、可信的数据底座。

# 跨网闸数据同步的安全保障

## 01 数据加密

采用国密标准算法对全量数据进行端到端高强度加密，实现传输链路的隐私保护。即使数据包被意外截获，也无法解析破解，从底层筑牢数据机密性防线。

## 02 身份认证

基于数字证书的双向强身份鉴权机制，严格校验采集节点与接收端的合法性。确保只有经过授权的可信设备才能接入传输，有效防范非法节点冒充与数据注入。

## 03 完整性校验

结合哈希摘要校验与非对称数字签名技术，实时检测数据是否被篡改或丢失。保障数据在跨网传输过程中的完整一致，实现数据来源可追溯、不可否认。

## 合规性验证与行业适配

完全符合《电力监控系统安全防护规定》要求，严格遵循“单向隔离、无反向连接”原则，不破坏现有网闸的物理隔离架构。方案已通过国家权威信息安全检测机构的合规性认证，确保在电力生产控制等关键场景下的安全稳定运行。

# 国产化设备统一纳管，消除监控盲区

随着信创战略的深入推进，平台内置丰富的国产化设备适配器，深度适配电力行业主流国产软硬件生态。从底层芯片到上层应用，实现全栈式监控覆盖，彻底消除国产化环境下的“监控盲区”，为信创替代的平稳过渡提供坚实可靠的运维保障。

### 操作系统全兼容

完美适配凝思、麒麟、统信UOS等主流国产操作系统，实现进程、资源、日志的全面监控。

### 国产数据库深度监控

全面支持达梦、人大金仓等数据库，实时监测连接数、锁等待、慢查询等核心指标。

### 信创云平台纳管

无缝对接华为云等国产化云环境，统一监控云主机、存储、网络等资源的运行状态。

### 国产服务器运维

适配浪潮、华为、联想等国产服务器，实时监控CPU、内存、硬盘及硬件健康状态。

### 网络设施全覆盖

支持华为、H3C等国产交换机、路由器，监控端口流量、丢包率及设备运行温度。

### 安全设备联动

集成深信服、启明星辰等安全设备，实现告警联动与安全态势的统一可视化管理。

# 设备资产状态实时感知

## 从“静态管理”到“动态感知”，为IT优化管理提供数据支持

通过集成SNMP、SSH、API、JMX等多元采集协议，实现对全栈IT设备运行状态的毫秒级实时感知。突破传统资产台账的静态局限，为IT资源的动态调度、容量规划、故障预判及成本优化提供精准、实时的数据支撑，让资产管理从“被动响应”转向“主动治理”。

### 服务器核心监测

实时追踪CPU负载、内存使用率、磁盘I/O吞吐及网卡流量，精准捕捉性能瓶颈。支持对物理机、虚拟机及容器化环境的统一纳管与状态监控。

### 网络链路全景监控

覆盖交换机、路由器、防火墙等核心设备，实时监测端口速率、带宽利用率、丢包延迟及网络拓扑连通性，保障数据传输链路的高可用性。

### 数据库性能透视

深度解析连接池状态、SQL请求并发量、缓存命中率及锁竞争情况。提前预警慢查询、表空间不足等风险，保障数据层稳定高效。

### 中间件服务治理

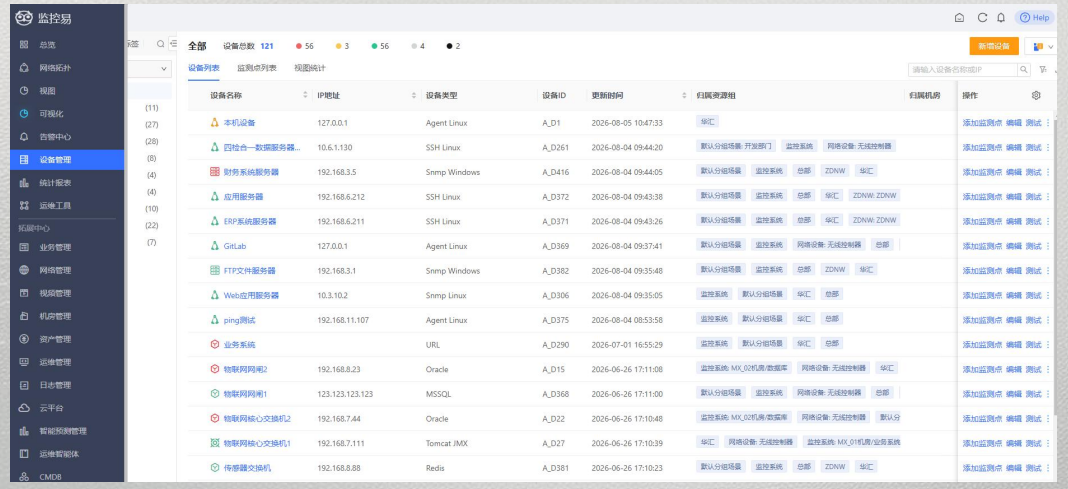
监控应用容器、消息队列、Web服务器的线程堆栈、堆内存GC频率及服务响应时间。快速定位中间件层的性能瓶颈与可用性风险。

# PART 05

# 关键技术能力详解

深度剖析支撑业务创新的六大核心技术支柱，从底层架构到应用层赋能，构建高可用、高扩展、高安全的数字化技术底座，驱动业务持续增长。

# 能力一：带外监控——服务器“失联”时的最后一道防线




通过专用的硬件管理芯片（BMC）建立独立通道，实时采集并可视化展示服务器的CPU温度、风扇转速、电源状态等核心指标，实现对硬件底层的无死角监控。

## 01 技术原理：绕过OS的底层直连

基于IPMI / Redfish工业级带外协议，直接与服务器内置的硬件管理芯片（BMC）通信，完全绕过操作系统内核与网络协议栈，构建一条独立于业务系统的“硬件直连通道”。

### 独立于系统的“硬件透视眼”

即便操作系统死机、业务网络中断，仍能远程查看硬件健康状态，彻底避免服务器“失联”变成“黑盒”，实现底层硬件状态的完全可控。

### 跨安全区场景的运维生命线

在电力调度、金融核心等强隔离场景下，作为独立于业务网的监控通道，保障生产控制区服务器在任何故障下的可见性，是运维保障的最后一道防线。

# 带外监控的支持范围与应用场景

全面支持浪潮、华为、曙光、联想等国内主流厂商，以及IBM、HP、DELL等国际品牌，深度适配电力行业复杂的服务器运维环境与合规要求。

**品牌全覆盖 · 打破硬件壁垒**

兼容x86/ARM等主流架构，实现跨品牌统一监控，降低运维复杂度。

## 硬件故障预警

实时监测CPU温度、电源状态、硬盘健康度等核心指标，提前识别潜在硬件隐患并主动告警，避免业务意外中断。

## 系统死机排查

OS完全死机时，通过带外通道直连硬件层读取日志与状态，快速判定故障根源，避免盲目重启导致的数据丢失风险。

## 跨安全区运维保障

在生产区网络完全隔离或OS失联的极端情况下，仍可通过带外通道穿透隔离，确保运维对硬件状态的可见性。

## 远程硬件管理

支持远程开关机、固件升级及虚拟光驱挂载，无需人员亲临现场即可完成系统修复，大幅降低运维成本与响应时间。

# 能力二：大规模高性能监控

自研高性能时序数据库，专为海量时间序列数据的存储与高并发查询场景深度定制

### 单台监测容量

**10,00+**监测点/节点

单机即可承载高密度采集，显著降低硬件部署成本与运维压力。

### 最小轮询频率

**5秒**/ 次高频采集

满足对时效性要求极高的关键设备监控，数据实时回传，异常毫秒级感知。

### 超大规模验证

**50,000+**设备接入规模

已成功支撑省级交控与部委级监控项目，具备成熟的规模化部署能力。

### 核心价值：构筑监控系统的性能底座

自研时序数据库彻底打破了传统数据库在海量时间序列数据下的性能瓶颈，确保在数据量爆发式增长时，系统依然保持毫秒级查询响应与高并发写入能力。这不仅保障了监控数据的实时性与准确性，更为上层的智能分析、故障预警提供了坚实的数据基础，实现了从“看得见”到“看得清、反应快”的跨越。

# 能力三：内置丰富监测适配器

### 01 覆盖广度

20,000+

内置海量设备监测器，全面覆盖服务器、网络、数据库、安全设备等电力行业核心IT基础设施，无需额外适配即可快速接入。

### 02 指标深度

200,000+

多维度深度指标监控，涵盖硬件状态、系统性能、业务运行等全链路数据，满足电力场景下精细化、高颗粒度的运维需求。

### 03 核心价值

极速上线

大幅缩短部署周期，降低实施与开发成本。快速适配电力行业复杂多样的设备环境，开箱即用，有效提升运维响应效率。

无需大量二次开发，即可快速适应电力行业复杂设备环境，实现监控体系的高效落地与价值兑现。

# 能力四：资产状态感知与调控云对接

## 01 技术实现

依托标准化接口，无缝对接调控云等电力行业主流资产管控系统。打破传统系统间的数据壁垒与信息孤岛，实现跨平台、跨层级的数据高效互通与业务协同，为资产智能化管理筑牢技术底座。

## 02 核心功能

深度融合调度云的资产静态台账与平台的实时动态感知数据，打通设备“身份信息”与“运行状态”的关联通道。实现资产配置、流转流程、实时工况的一体化监控，让资产状态可视、可控、可追溯。

## 03 核心价值

实现资产从采购、部署、运维到退役的全生命周期闭环管理。基于多源数据的深度挖掘与分析，为资产优化配置、电网容量规划及设备风险评估提供科学的大数据决策支撑，提升资产管理的精细化与智能化水平。

**总结：**通过数据融合与智能感知，构建起“静态台账+动态状态”的资产全景视图，为电网资产的安全运行、精益管理与科学决策提供坚实的数字化保障。

# 能力五：全面适配电力行业国产化设备

有效支持电力行业国产化升级，保障运维连续性与业务稳定性

### 国产操作系统深度兼容

完美适配凝思、麒麟等主流国产操作系统，实现业务系统无缝迁移与稳定运行，消除兼容性壁垒。

### 信创数据库全面支持

深度集成达梦、人大金仓等国产数据库，保障数据存储的安全性与高可用性，满足海量数据处理需求。

### 国产化云平台无缝对接

全面适配华为云、浪潮云等信创云环境，支持多云架构部署，确保云端资源的统一监控与运维。

### 国产服务器硬件适配

兼容浪潮、华为、联想等主流国产服务器，针对鲲鹏、飞腾等架构深度优化，释放硬件性能潜力。

### 国产网络设备纳管

统一监控华为、H3C等品牌的交换机、路由器及防火墙，保障电力通信网络的稳定与高效互联。

### 信创安全设备集成

集成深信服、启明星辰等国产安全设备，构建一体化主动防御体系，全方位保障电力系统安全。

**核心价值：**深度契合电力行业信创战略，实现从底层硬件到上层应用的全栈国产化兼容。在保障现有业务零中断的前提下完成平滑升级，为电力系统的自主可控、安全稳定运行提供坚实的技术底座，加速构建安全可靠的现代化电力运维体系。

# 能力六：可视化大屏与分级管理视图


依托高清可视化大屏，将全省电网运行数据、告警信息及设备状态实时汇聚，打造“一屏观全域”的智能监控模式，实现电网运行态势的直观感知与快速响应。

## 01 省调级：全域统筹监控

覆盖下属所有地调、变电站及安全区设备，实现跨区域、跨层级的统一监控与态势感知，全局电网运行状态一目了然，助力宏观调度决策。

## 02 地调级：区域精细运维

聚焦本地网区域内的设备监控与调度管理，提供专属化、场景化的视图界面，支持对辖区内电网故障、负荷变化进行快速响应与精准处置。

## 核心价值：决策效率跃升

打破信息孤岛，实现“全局一盘棋”的管理模式，让管理者从海量数据中快速捕捉关键信息，大幅缩短决策周期，提升电网调度的精准性与安全性。

# PART 06

# 实战案例分析

以省级电力公司数字化转型为样本，全景式复盘解决方案的落地路径与价值产出
深度解析技术架构与业务场景的融合之道，探寻可复制的行业标杆实践

# 案例一：某省级电力公司一体化运行指挥平台项目


项目实景为省级电力调度中心监控大屏，通过一体化平台实现对全省电网二次系统、设备资产及安全状态的全景式可视化监控与指挥调度，是保障电网安全稳定运行的“智慧大脑”。

## 项目背景与建设动因

针对电力二次系统传统运维中存在的跨安全区协同难、国产化设备监控盲区、故障响应滞后等痛点，建设省级一体化运行指挥平台，实现对下属三地调及全网设备的实时感知与统一调度，筑牢电网安全防线。

## 五大核心建设目标

### 全域统一监控

跨区跨层级打破壁垒，实现全景式运维，消除信息孤岛。

### 消除设备盲区

全覆盖国产化设备监控，保障关键设施运行可视可控。

### 资产实时感知

动态采集状态数据，智能分析健康度，赋能精益管理。

### 安全合规保障

符合等保合规要求，筑牢网络安全防线，提升故障效率。

# 改造前的五大痛点

## 01 资产状态感知盲区

调控云仅维护静态台账，缺乏设备实时运行数据，无法即时判断设备健康度与工况，形成关键的监控感知空白。

## 02 故障排查耗时漫长

业务异常需跨多套孤立系统人工逐一排查，平均定位耗时超2小时，严重拖慢电网故障处置的响应速度。

## 03 跨域监管存在壁垒

省调与地调跨安全分区物理隔离，数据互通困难，形成多个“信息孤岛”，难以实现全网的统一监管与调度。

## 04 国产化监控覆盖缺失

凝思OS、达梦数据库、华为云等国产化软硬件广泛应用，但传统监控工具兼容性不足，无法实现全面覆盖，形成大量监控盲区，难以保障国产化环境的稳定运行。

## 05 可视系统重展示轻管理

现有三维可视化仅停留在界面展示层面，缺乏与底层设备状态的实时联动，不具备告警触发与运维闭环能力，无法真正支撑调度人员的运维决策与管理需求。

# 实施后收益一：资产状态感知，助力设备资产优化配置

通过与调控云无缝对接，打破传统数据孤岛，实现资产基础信息、运维流程与实时运行状态的一体化管理。运维人员可全天候掌握全网设备的运行态势，为资源动态扩容、设备智能汰换与架构持续优化提供精准的数据支撑，推动资产管理从“被动响应故障”向“主动预判风险”的根本性转变。

### 动静数据融合联动

打通资产静态台账与动态监控数据，实现设备运行状态实时可视、数据同源，彻底消除信息滞后与数据不一致的管理盲区。

### 全生命周期闭环管理

覆盖设备采购、部署上线、日常运维、故障处置直至报废回收的全流程，建立标准化管理体系，实现资产全流程可追溯。

### 科学决策智能支撑

基于实时运行数据与历史趋势分析，为IT资产扩容、资源调配及容量规划提供量化依据，避免资源闲置浪费与过度投入。

### 运维模式主动升级

从传统“故障后抢修”的被动运维模式，升级为“风险预判+主动预警”的智能化运维，大幅降低设备故障率与业务中断风险。

# 实施后收益二：故障快速定位，处理速度大幅提升

基于告警信息与网络拓扑图的深度联动，实现故障“一键定位”至具体设备与关键指标，彻底改变传统依赖人工排查的被动局面，极大缩短故障处置周期，显著提升电网运行的安全性与稳定性。

### 传统人工排查模式

平均耗时 2 小时| 依赖人工研判，定位链路长，效率低

### 智能一体化诊断体系

压缩至 5 分钟内| 自动关联拓扑指标，秒级锁定故障根因

### 体系闭环化

建立“告警-拓扑-指标”联动机制，打破数据孤岛，实现故障诊断全流程自动化。

### 定位精准化

不再盲目排查，系统直接定位到具体故障设备与关键异常指标，直击问题核心。

### 风险最小化

极速响应大幅降低故障持续时间，有效减少对电网安全运行及用户供电的影响。

### 运维高效化

释放运维人员精力，将工作重心从被动抢修转向主动预防与优化，提升管理效能。

# 实施后收益三：提供分级管理视角，助力科学决策


依托可视化监控大屏，省调可实时掌控全网运行态势，地调则能聚焦区域运维细节，真正实现了管理层面的上下联动与信息互通。

## 构建“全局+区域”的双重管理维度

打破传统层级壁垒，为省调、地调定制差异化视图，实现宏观管控与微观运维的有机结合，大幅提升调度决策的科学性与及时性。

### 省调全局掌控

通过全景可视化大屏，实时掌握全网负荷、电网拓扑及告警信息，实现宏观调度。

### 地调精细管控

聚焦本区域变电站、线路运行状态，快速响应故障，落实精细化运维与现场管理。

### 三级数据互通

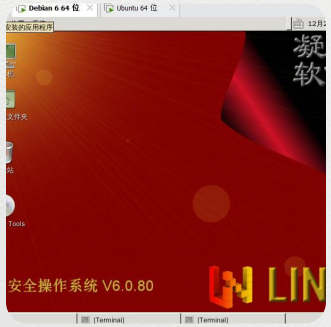
打通省、地、站三级数据壁垒，实现SCADA、用电信息等多源数据的实时同步共享。

### 决策效率跃升

基于数据的智能辅助决策，缩短故障研判与调度指令下发时间，提升电网响应速度。

# 实施后收益四：国产化设备统一监控，有效支持国产化升级

实现对全栈国产化设备的统一纳管与实时监控，彻底消除信创环境下的监控盲区，确保国产化升级过程中的运维连续性，为企业信创战略的顺利实施提供坚实的技术保障。




## 操作系统深度适配

全面覆盖凝思、麒麟等国产OS，实时监控资源负载，保障基础算力环境稳定可控。

达梦数据

## 核心数据库统一监管

纳管达梦、人大金仓等信创数据库，监控会话、锁状态及存储健康，规避数据层风险。

## 信创云平台一体化运维

适配华为云等国产云环境，打通云主机、容器与网络监控，实现云端资源全景可视。

## 国产化服务器集群

深度纳管浪潮、华为、联想等信创服务器，实时监测硬件健康、CPU/内存负载，保障算力基座稳定可靠。

## 信创安全设备联防

覆盖深信服、启明星辰等安全设备，监控防火墙策略、入侵检测与日志审计，筑牢信创安全防线。

## 国产网络设施监控

统一监控华为、H3C等网络设备，实时掌握带宽流量、端口状态与路由健康，保障网络通道畅通。

PART 07

# 未来趋势与总结

从技术创新到模式升级，全面洞察电力行业智能运维的演进方向；
回顾核心实践成果，总结数字化转型的关键路径与价值增长点，为未来发展指明方向。

# 智能运维演进趋势：从“被动响应”到“主动预警”

随着AI技术的深入应用，电力运维正从“事后救火”的被动响应，向“事前预警、主动防御”的新模式演进。这一变革不仅响应了《电力监控系统安全防护规定》中“安全免疫、态势感知”的要求，更通过技术创新为电力系统的稳定运行构建起坚实的智能防线。

国家人工智能应用中试基地实景
能源行业智能化转型的标杆示范窗口

## 前沿探索：具身智能重塑电力巡检

2026年5月挂牌的国家级中试基地，将电力巡检作为能源行业唯一入驻场景。依托多模态感知、协同控制等前沿技术，推动巡检机器人实现自主决策与智能调度，打造行业智能化转型的“试验田”与技术孵化平台。

## 实战成效：国网浙江电力的智能运维答卷

| 13次 | 3起 | <5分钟 |
| --- | --- | --- |
| 系统性能劣化预警 | 重大异常故障规避 | 故障根因定位耗时 |

# 核心观点总结

## 01合规送达，而非穿透

摒弃“穿透”网闸的高危方式，通过在安全区内部署轻量采集器，将数据封装为合规格式单向推送，既实现生产区设备状态可视，又严守电力安全边界，兼顾监控需求与合规底线。

## 02带外监控是最后防线

带外监控是服务器“失联”时的救命稻草，即便系统死机或网络中断，仍能通过独立通道查看硬件健康状态，是跨安全区电力调度系统中保障运维可见性的关键兜底手段。

## 03需要“懂国产”的监控体系

信创环境下的运维，核心在于深度适配。监控体系需全面兼容国产CPU、操作系统、数据库及中间件，打破生态壁垒，让信创设备的运行状态可管、可控、可预判，实现从容运维。

## 04四级分布式架构是关键

“边缘采集+中心管控”的四级分布式架构，是解决电力行业多层级、跨区域、跨安全域监控难题的核心，既满足数据分级传输的合规要求，又能实现全网设备的统一监控与全局视图。

## 05资产实时感知是前提

从“看不见”到“看得见”是智能化运维的起点。通过资产实时感知，动态掌握设备的位置、状态、负载与关联关系，为故障快速定位、资源动态调度与IT资产优化提供坚实的数据基础。

## 06信创与合规双重驱动

2026年电力信创进入规模化落地阶段，41号令将“横向隔离”纳入重大隐患判定标准，合规与国产化替代形成双重推力，倒逼运维监控体系同步升级，以适配行业发展的新要求。

# 感谢聆听

## Q & A

欢迎各位领导、专家提问交流，共同探讨与进步