基于工业以太网的华电综合管理系统通信架构优化

黄 睿[1] 邱 丽[1] 翁超逸[1] 张昌森[2]
HUANG Rui QIU Li WENG Chaoyi ZHANG Changsen

摘 要 华电综合管理系统作为电力生产与运营的核心支撑平台，其通信架构的稳定性与高效性直接影响电力系统的安全运行。文章针对当前华电综合管理系统通信架构存在的实时性不足、安全性薄弱、兼容性差等问题，提出了一个基于工业以太网的优化方案。通过分析现有架构的瓶颈，从网络拓扑重构、协议标准化、安全机制强化、带宽管理优化等维度设计优化策略，并结合华电实际应用场景验证方案的可行性，以期为华电系统的数字化转型提供可靠通信支撑。

关键词 工业以太网；华电综合管理系统；通信架构；网络优化

doi：10.3969/j.issn.1672-9528.2026.03.022

0 引言

随着电力行业数字化转型的深入，华电综合管理系统已从单一的生产监控向“生产 - 调度 - 运维 - 管理”全链条协同演进，对通信架构的实时性、可靠性、扩展性提出了更高要求。传统基于专用总线和普通以太网的通信架构，存在数据传输时延大、协议碎片化、安全防护层级低等问题，难以满足新能源并网、智能巡检等新业务的需求。工业以太网凭借高带宽、低时延、强抗干扰性等优势，成为电力系统通信升级的核心技术。本文基于工业以太网技术，针对华电综合管理系统通信架构进行优化设计，旨在解决现有架构的瓶颈问题，为电力生产的高效协同与安全运行提供保障。

1 华电综合管理系统通信架构问题

1.1 实时性瓶颈与数据传输延迟

现有架构的实时性问题主要体现在三个方面：一是总线传输速率受限，现场设备层的 RS485 总线最大传输速率仅为 12 Mbit/s，在新能源电站（如风电、光伏）中，数千个分布式逆变器的数据并发上传时，常出现数据丢包（丢包率达 3%~5%）；二是协议转换耗时，现场层专用协议与监控层 TCP/IP 协议的转换需通过网关完成，单次转换时延为 50~100 ms，某光伏电站的汇流箱数据经过 3 次协议转换后，时延累计达 250 ms；三是网络拥塞，管理层与监控层共用带宽，在每日 9:00—11:00 的报表生成高峰期，网络带宽占用率达 90% 以上，导致现场设备的告警信息传输延迟，某水电厂曾因机组振动超限信号延迟 15 s 送达调度中心，险些引发设备故障。此外，传统以太网的“尽力而为”传输机制缺乏优先级调度，关键数据（如发电机定子温度）与非关键数据（如环境温湿度）混流传输，在网络拥堵时，关键数据无法优先送达 [1]。

1.2 安全防护体系薄弱

当前通信架构的安全防护存在“重边界、轻内部”的问题：一是边界防护单一，仅在管理层与监控层之间部署防火墙，缺乏深度入侵检测能力，2024 年某电厂曾遭受勒索病毒攻击，导致 SCADA 系统数据加密，因未部署工业防火墙，病毒通过 U 盘从管理层渗透至监控层；二是数据传输未加密，现场设备层与监控层的数据以明文传输，攻击者可通过嗅探工具获取 PLC 控制指令，某变电站的断路器分闸指令曾被截获篡改，造成线路误跳闸；三是设备身份认证缺失，现场传感器、智能仪表等设备未采用接入认证机制，易被伪造设备替换，某风电场的风速传感器被植入虚假数据后，风机因“风速超标”误停机，损失电量 1.2×10^4 kW·h。此外，系统日志审计机制不完善，对异常登录、指令篡改等行为缺乏实时记录与告警，导致安全事件发生后难以溯源。

1.3 兼容性问题与系统孤岛

华电集团旗下电厂因建设年代不同，通信设备与协议标准差异显著，形成“系统孤岛”：一是硬件接口不兼容，老电厂的汽轮机监控系统采用 RS232 接口，而新上线的智能诊断系统仅支持以太网接口，需部署大量协议转换器，某老电厂的 20 台汽轮机需配备 15 种不同型号的转换器，维护成本增加 40%；二是协议碎片化，火电厂多采用 Modbus 协议，水电厂以 DNP3.0 协议为主，新能源电站常用 IEC61850 协议，导致集团级数据汇总时需进行多协议转换，某区域调度中心的协议转换服务器日均处理数据错误达 2 000 余次；三是数

1. 华电（福建）风电有限公司 福建福清 350300
2. 华电（南平）能源集团有限公司 福建南平 353000

据格式不统一，同一参数（如“机组负荷”）在不同系统中的定义、单位、采样频率存在差异，某省公司的负荷统计报表需人工校准 30% 的数据，严重影响决策效率 [2]。

2 华电综合管理系统通信架构优化方案

2.1 网络拓扑结构重构

现场设备层 TSN 环形拓扑的核心技术实现依托 IEEE 802.1AS-2020 时间同步协议，通过主时钟（Grandmaster Clock）与从时钟（Slave Clock）的分层同步机制，实现全环设备微秒级时间对齐。主时钟部署在环网核心交换机，每 128 ms 发送一次 Sync 同步报文，从时钟通过测量报文传输时延（采用 PTP 协议的 E2E 时延测量机制）动态校准本地时钟，确保各节点时间偏差控制在 ±50 ns 以内。802.1CB 帧复制机制的具体实现中，源节点在帧头添加 16 位 Sequence ID 字段，该字段由节点 MAC 地址（6 Byte）与递增计数器（2 Byte）组合生成，确保全局唯一性。复制帧通过主备链路传输时，交换机基于 BFD（双向转发检测）协议实时监测链路状态，当主链路丢包率超过 1% 时，自动将 60% 的复制帧切换至备用链路，接收节点通过维护长度为 16 的 Sequence ID 缓存队列，对到达的帧进行比对，仅保留最早到达且校验无误的帧，其余帧通过硬件加速模块直接丢弃，整个去重过程耗时不超过 5 ms[3]。

厂级监控层双星型拓扑中，核心交换机的 VRRP 协议采用 IPv4 组播报文（目的 IP 224.0.0.18）实现主备交互，主交换机每 1 s 发送一次 Hello 报文（包含虚拟路由器 ID、优先级、路由表摘要），备用交换机通过计算 Hello 报文的接收间隔（超时阈值设为 3 s）判断主设备状态。当主交换机故障时，备用交换机立即发送 Advertisement 报文宣告接管，同时通过 IS-IS 路由协议（配置 Level-1 区域）在 50 ms 内完成路由表收敛。汇聚交换机与 TSN 交换机的千兆互联链路启用 IEEE 802.3az 节能机制，空闲时自动切换至低功耗模式，且通过 LLDP（链路层发现协议）每 30 s 交换一次设备能力信息，确保链路协商参数（如流量控制、双工模式）实时匹配。

集团管理层的 MSTP 专线采用 GFP（通用成帧规程）封装，将 2.5 Gbit/s 带宽划分为 8 个时隙（每个时隙 312.5 Mbit/s ），其中时隙 1~3 分配给实时监控数据（采用固定带宽调度），时隙 4~6 分配给业务管理数据（采用统计复用），时隙 7~8 预留为应急通道。时隙调度通过 SDH 帧结构的 AU-4 指针调整实现，每个时隙的净荷区（149 760 Byte）采用 CRC-32 校验，确保数据完整性。IPsec VPN 的实现中，区域分公司与电厂的网关采用 ESP（封装安全载荷）协议，在传输模式下对 IP 报文的净荷进行加密，加密前通过 HMAC-SHA256 算法生成 128 位认证码，密钥交换采用 IKEv2 协议，第一阶段通过预共享密钥（PSK）认证，第二阶段协商出的 ESP 密钥每 8 h 通过 Diffie-Hellman（DH）组 24 重新生成，确保会话安全性 [4]。具体如表 1 所示。

表 1 优化后的网络拓扑

层级划分	拓扑结构	核心设备 / 组件	连接方式与带宽
现场设备层	TSN 环形拓扑	— 传感器、执行器、PLC 等终端设备 — 工业以太网交换机（TSN 交换机）	1 Gbit/s 光纤介质，支持双向数据传输 TSN 交换机与终端设备互联，形成环形链路
厂级监控层	双星型拓扑	— 车间汇聚交换机 —2 台互为冗余的核心交换机（主 / 备）	— 汇聚交换机与现场层 TSN 交换机：千兆以太网互联 — 核心交换机与汇聚交换机：10 Gbit/s 光纤链路连接
集团管理层	三层架构	— 总部骨干网设备 — 区域分公司网络设备 — 下属电厂网络设备	— 总部与区域分公司：2.5 Gbit/s MSTP 专线构建骨干传输网 — 区域分公司与下属电厂：1 Gbit/s IPsecVPN 加密互联

2.2 通信协议标准化与转换

IEC61850 协议的逻辑节点（LN）建模采用 ASN.1（抽象语法标记）编码，例如变压器逻辑节点（TCTR）的“电流测量值”属性定义为：TCTR1.Amp.mag.f[0]，其中“Amp”表示电流对象；“mag”表示量值；“f[0]”表示浮点格式（IEEE 754 单精度），采样值的时标信息通过 SVCB（采样值控制块）携带，采用 UTC 时间戳（精确到 1 μs）。新设备的 ACSI 接口实现中，数据读取服务（Get Data Values）采用客户端 - 服务器模型，客户端发送的请求报文中包含 LN 引用（如“LD0/TCTR1”）和属性列表，服务器在 20 ms 内返回携带 BER（基本编码规则）编码数据的响应报文，超时未响应时自动触发重传（最多 3 次）。

协议转换网关的硬件架构基于 NXP Layerscape LS1046A 处理器（四核 ARM Cortex-A72），内置专用协议转换加速引擎（PTAE）。对于 Modbus RTU 到 IEC61850 的转换，网关首先通过 RS485 接口读取设备的保持寄存器（地址 0x0000-0x0FFF），解析出的寄存器值（16 位）通过映射表转换为 IEC61850 的 MX（测量值）逻辑节点属性，例如将 Modbus 寄存器 0x0001 的电压值（单位 V，分辨率 0.01）映射为 MXU1.U.phsA.cVal（浮点型，单位 kV，转换公式：kV=V/1 000）。转换过程中，网关通过硬件定时器（精度 1 ms）对数据添加时标，且每 5 min 与 TSN 主时钟同步一次，确保时标偏差不超过 10 ms。

数据模型的标准化中，12 类逻辑节点的属性采用统一的命名规则，如“状态”属性以“st”结尾（布尔型）；“测量值”以“cVal”结尾（浮点型）；“控制指令”以“ctlVal”结尾（枚

举型）。软件接口的 RESTful API 采用 HTTPS 传输，接口路径遵循“/api/v1/[设备类型]/[设备 ID]/[属性]”格式，例如获取 #1 发电机转速的请求为 GET /api/v1/generator/1/speed，返回的 JSON 数据包含“timestamp”（时标）、“value”（值）、“quality”（质量码，如 0x00 表示有效）三个字段，其中质量码采用 IEC61850 的 QoS 定义，包含有效性、精确性等 6 个维度的状态标识。

2.3 安全机制多层级强化

安全机制的构建遵循“纵深防御”原则，通过边界防护、终端安全、数据加密与安全审计的多层协同形成完整防护体系（见表 2）。边界防护在各层级间部署专用安全设备，现场层与监控层之间的工业防火墙的深度包检测（DPI）基于专用 ASIC 芯片实现，对 IEC61850-9-2 采样值报文的解析深度达 L7 层，提取 SVID（采样值标识）、APPID（应用标识）等字段，与规则库中的白名单（包含合法 SVID 范围 0x0001-0x0100、APPID 固定为 0x8001）比对。规则库通过与国家能源局威胁情报平台联动，每小时更新一次，新增规则通过增量推送方式加载（不中断业务）。对于异常报文（如 SVID 为 0x0101），防火墙不仅拦截报文，还通过 SNMPv3 发送 trap 告警至安全管理平台，告警信息包含报文的源 MAC、目的 MAC、异常字段值。

表 2 多层级强化的安全机制

安全机制层级	核心措施	关键指标	作用与目标
边界防护	部署专用安全设备	下一代防火墙攻击阻断率达 99.9%	精准拦截异常控制指令，抵御 SQL 注入、缓冲区溢出等攻击，保障各层级边界安全。
终端安全	实现设备接入控制	— 防止证书伪造与中间人攻击	严格控制终端接入，确保接入设备的合法性与安全性。
数据加密	采用端到端保护策略	— 保障数据传输和存储环节的保密性	避免传输中密钥泄漏风险，确保数据在存储和传输时的保密性。
安全审计	实时采集与分析相关日志	日志数据留存时间不少于 6 个月	及时发现并处置异常行为，满足合规性要求，提升系统安全性。

终端安全方面，终端接入的 802.1x 认证采用 EAP-TLS 流程，终端设备的数字证书由集团 CA 中心颁发（基于 SM2 椭圆曲线算法，密钥长度 256 位），证书包含设备唯一 ID（如“PLC-#1 炉 -001”）、有效期、issuer 信息。认证过程中，交换机作为认证者（Authenticator），首先向终端发送 EAP-Request/Identity 报文，终端返回包含证书的 EAP-Response 报文，认证服务器（RADIUS）通过验证证书的数字签名（采用 SM3 哈希算法）和 CRL（证书吊销列表）判断合法性，整个认证流程耗时控制在 800 ms 内，认证失败的终端被分配至隔离 VLAN（VLAN ID 999），仅允许访问 CA 服务器进行证书更新。

数据加密方面，TLS1.3 的握手过程采用 ECH（加密客户端问候）扩展，客户端在 ClientHello 报文中加密真实 SNI（服务器名称指示），避免被中间人截获。ECDH 密钥交换选用 secp256r1 曲线，双方生成的临时公钥（64 字节）通过 TLS 记录层加密传输，会话密钥（128 位）由 HKDF（基于 HMAC 的密钥派生函数）生成，派生过程中加入握手随机数、服务器证书哈希等参数增强随机性。SM4 加密存储时，数据按 128 位分组处理，初始向量（IV）采用设备 MAC 地址（6 字节）与时间戳（6 字节）组合生成，敏感数据的 AES-256 加密采用 GCM 模式，除密文外还生成 128 位认证标签，用于检测存储数据是否被篡改。

安全审计系统的机器学习模型采用基于 LSTM 的异常检测算法，通过采集 3 个月的正常操作日志（包含操作人 ID、设备 IP、操作类型、时间戳）构建训练集，提取操作序列的 *N*-gram 特征（*N*=3），模型对 PLC 程序下载操作的识别准确率达 99.7%。当检测到异常时（如非授权 IP 的“写操作”），系统通过 NETCONF 协议向交换机发送流表项，50 ms 内阻断该连接，同时触发 SOAP 告警至运维平台，告警等级按严重程度分为 Critical（红）、Major（黄）、Minor（蓝）三级 [5]。

2.4 带宽管理与流量调度

VLAN 隔离的实现中，控制网、监控网、管理网分别对应 VLAN ID 10~19、20~29、30~39，802.1Q 标签的 TCI 字段中，PRI（优先级）分别设为 7（最高）、5、3，确保交换机在转发时优先处理控制网数据。控制网的 802.1Qbv 时间片调度采用 100 ms 周期，其中 0~10 ms 分配给机组控制指令（P0 级），10~30 ms 分配给阀门调节信号（P1 级），30~100 ms 为空闲窗口（禁止其他业务占用）。时间片的 gate 控制列表（GCL）存储在交换机的 TCAM（三态内容可寻址存储器）中，支持硬件级快速匹配，每个时间片的开始 / 结束时间通过 TSN 主时钟同步，偏差不超过 100 ns。

WFQ 算法的权重配置中，P0~P4 级队列的权重比为 10∶6∶3∶2∶1，交换机每处理 100 个数据帧重新计算队列权重，当 P0 级队列有数据时，通过 WRR（加权轮询）机制优先调度，确保其带宽利用率不低于 90%。流量整形器的令牌桶参数配置为：承诺信息速率（CIR）=10 Mbit/s ，承诺突发尺寸（CBS）=1 MB，超额突发尺寸（EBS）=512 kB，令牌生成速率为 (10 Mbit·s^{-1})/8=1.25 MB/s，当突发流量超过 CBS 时，超额部分被标记为“丢弃 eligible”，在网络拥塞时优先丢弃。

SDN 控制器基于 ONOS 架构，通过 OpenFlow 1.3 协议与交换机通信，每 5 s 采集一次端口流量统计（包含入 / 出字

节数、帧速率），采用 Dijkstra 算法计算最优路径。当某区域带宽利用率超过 80% 时，控制器向相关交换机下发流表项（匹配字段为业务类型、源 IP），将非关键业务（如报表上传）的转发路径切换至负载较低的链路，同时通过 NETCONF 协议调整该业务的发送窗口（从 100 ms 延长至 500 ms），降低发送速率。动态调整的决策周期为 10 s，确保网络负载在 2 min 内回落至 70% 以下。

2.5 冗余设计与容错机制

冗余设计从设备、链路、数据三个维度构建高可用体系，确保单点故障不影响系统运行（如表 3 所示）。

表 3 冗余设计与容错机制

类别	设计维度	具体设计模式 / 机制	关键参数 / 指标
冗余设计	设备冗余	1+1 热备模式（关键设备）	设备切换时间 ≤50 ms；电源支持热插拔更换
	链路冗余	双路径设计	现场层切换时间 <100 ms；支持负载均衡与故障切换
	数据冗余	“三副本”存储策略	灾备中心接管业务时间 ≤3 s
容错机制	算法优化	前向纠错（FEC）编码	可纠正 99.9% 的随机错误
	数据处理优化	卡尔曼滤波算法	测量误差从 ±5% 降至 ±0.8%

设备冗余的 1+1 热备中，主备交换机通过 10 Gbit/s 专用同步链路（采用 OSPFv3 协议）实时同步配置信息，同步内容包括 VLAN 表、ACL 规则、路由表，同步频率为每 100 ms 一次，采用增量同步机制（仅传输变化的配置项）。主备切换通过 BFD 协议触发，当连续 3 次未收到 BFD 报文（检测间隔 20 ms）时，备用交换机立即将自身 VRRP 优先级从 100 提升至 200，接管虚拟 IP 地址，同时通过 LLDP 报文通知下游设备更新 MAC 地址表，整个切换过程的业务中断时间不超过 30 ms。电源模块的 N+1 设计中，每个模块输出电压为 48 V，采用均流电路（误差 ≤5%），当某模块故障时，监控芯片（如 MAX749）在 10 ms 内发出告警，同时自动调整其余模块的输出电流，确保总功率稳定。

链路冗余的双环网采用 ERPS（以太网环保护协议），配置环网节点数为 8 个，控制 VLAN ID 为 4 094，主节点每 200 ms 发送一次健康检查帧（R-APS 报文），从节点收到后立即转发。当链路故障时，故障节点发送 R-APS（SF）报文，主节点收到后在 50 ms 内阻塞备用端口，完成环网重构。LACP 聚合组的配置中，活动端口数设为 2，超时时间为 90 s，采用源 MAC+ 目的 MAC 的哈希算法分配流量，当某端口丢包率超过 5% 时，自动将其切换为备用状态，流量无缝转移至另一端口。

数据冗余采用“三副本”存储策略，基于 Ceph 分布式存储系统，采用 CRUSH 算法将数据分片（每个分片 4 MB），副本分布在不同机架的服务器（容错域设为机架），副本同步通过链式复制机制实现（主副本 → 次副本 → 三副本），同步时延控制在 200 ms 内。当本地服务器故障时，灾备中心通过 Heartbeat 协议（每 1 s 发送一次检测报文）在 1 s 内检测到异常，立即激活副本数据，同时通过 iSCSI 协议接管业务，整个切换过程的 I/O 中断时间不超过 2 s。

容错机制中，FEC 采用 RS(255, 239) 编码，对每个 239 字节的数据块添加 16 Byte 冗余校验码，接收端通过 Berlekamp-Massey 算法纠正不超过 8 字节的连续错误或 16 字节的随机错误，纠错成功率达 99.9%。数据处理优化采用卡尔曼滤波算法，卡尔曼滤波的状态方程设为 $x(k) = 0.98x(k\text{-}1)+w(k)$（$w$ 为过程噪声，方差 Q=0.01），观测方程为 $z(k) = x(k)+v(k)$（v 为测量噪声，方差 R=0.1），滤波增益 $K(k)$ 通过递归计算动态调整，对传感器数据的平滑处理使连续 5 次测量值的波动幅度从 ±5% 降至 ±0.8%，有效滤除电磁干扰导致的尖峰脉冲。

3 结语

基于工业以太网的华电综合管理系统通信架构优化，通过网络拓扑重构、协议标准化、安全机制强化、带宽管理与冗余设计，有效解决了传统架构的实时性差、安全性弱、兼容性低等问题。实际应用表明，优化后的架构可满足电力生产的高可靠性需求，为华电集团的数字化转型提供了坚实的通信支撑。未来，随着 5G 与工业以太网的融合，需进一步探索边缘计算与云边协同技术，实现通信架构的智能化升级。

参考文献：

[1] 于会群，黄贻海，彭道刚，等 . 工业以太网网络互联技术与发展 [J]. 电子技术应用 ,2022,48(4):1-5.

[2] 王靖然，刘明哲，徐皑冬，等 . 工业以太网信息安全通信方法的研究与实现 [J]. 控制工程 ,2022,29(10):1774-1779.

[3] 郑伟锋 . 工业自动化系统中各种通信方式及其应用分析 [J]. 电工技术 ,2023(22):8-11.

[4] 孙骜，张振华，秦旭军，等 . 基于工业以太网的分布式智能传输控制系统 [J]. 工业仪表与自动化装置 ,2022(4):105-107.

[5] 王瑞丰，黄春晓，刘禹辉，等 . 一种基于以太网技术的工业网络应用分析 [J]. 冶金自动化 ,2021,45(S1):307-310.

【作者简介】

黄睿（1999—），女，福建永定人，硕士，中级工程师，研究方向：信息化。

（收稿日期：2025-08-15 修回日期：2026-03-03）