

智能电力调度自动化主站网络安全 防护机制探讨

李宣儒

(国网山西省电力有限公司芮城县供电分公司)

【摘要】智能电力调度系统在高度自动化与智能化演进过程中,自动化主站作为核心控制节点,其网络安全风险持续加剧。文章聚焦智能电力调度自动化主站,研究其系统架构与调度业务的安全敏感特征,识别网络边界接入、系统漏洞利用、智能接口滥用等关键安全威胁,构建包含边界访问控制、系统环境加固、智能行为识别三大模块的防护机制。研究成果可为调度系统网络安全体系构建提供技术支撑,增强主站对复杂威胁的感知能力与主动防御能力。

【关键词】智能电力调度;自动化主站;网络安全;边界控制

中图分类号:TM734;TP393.08

DOI: 10.13655/j.cnki.ibci.2025.S2.161

Discussion on the Network Security Protection Mechanism of Intelligent Power Scheduling Automation Master Station

LI Xuan-ru

(State Grid Shanxi Provincial Power Co., Ltd. Ruicheng County Power Supply Branch)

【Abstract】In the process of highly automated and intelligent evolution of intelligent power dispatching system, the automated master station as the core control node continues to increase its network security risk. This article focuses on the intelligent power scheduling automation master station, studies the security sensitivity characteristics of its system architecture and scheduling services, identifies key security threats such as network boundary access, system vulnerability exploitation, and intelligent interface abuse, and builds a protection mechanism including three modules: boundary access control, system environment reinforcement and intelligent behavior recognition. The research results can provide technical support for the construction of the network security system of scheduling system, and enhance the master station's perception ability and active defense ability against complex threats.

【Keywords】intelligent power scheduling; automated master station; network security; boundary control

1 引言

智能电力调度系统依托大数据分析、人工智能决策与多源信息融合技术,实现对电网运行状态的全局感知与动态调控。自动化主站作为调度系统的信息中枢,承载着核心数据交互、指令下发与远程控制等关键功能。在高度集成化与智能化架构下,其通信链路、控制接口与计算平台不断拓展,系统边界趋于复杂,调度业务对网络实时性、连续性和数据完整性的要求显著提升,主站运行环境对安全防护体系的适配能力提出更高技术标准,有效防护机制的构建结合主站系统结构与智能调度特性展开。

2 主站结构特性与调度安全需求

2.1 主站架构特征

智能电力调度系统依托自动化主站实现对电网

运行状态的集中监控与控制指令下发,其核心构成包括SCADA系统、EMS系统、通信前置机、调度数据服务器、控制策略引擎与操作终端。SCADA模块负责采集厂站实时量测数据与状态量,经由通信前置机进行协议解析与数据规整,传输至数据库与调度平台。EMS模块提供潮流计算、负荷预测、最优调度等功能,为智能决策模块提供计算支撑^[1]。控制引擎根据实时运行图谱生成调度指令,联动远程终端设备执行调度动作。

在系统结构上,主站采用分层解耦架构,数据层、服务层与应用层逻辑独立,支撑模块具备集中部署与远程协同双重运行模式。为满足调度全过程智能控制需求,主站系统引入AI辅助诊断模块与多源数据融合接口,功能由传统被动监控演化为主动分析与预测控制体系,通信链路结构呈现多入口、跨区段、高并发特征。整体系统结构如图1所示。

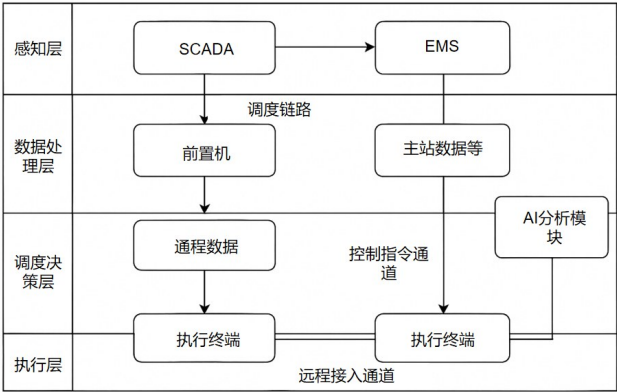


图1 智能电力调度自动化主站系统功能结构图

2.2 调度业务对网络安全的关键需求

自动化主站在调度业务中承担着状态采集、调度计算、指令分发与反馈接收的全流程中枢职能,调度数据流在不同模块间高速交换,任何中断或伪造均可能引发调度失稳或指令失效。控制指令在链路中传输时对数据一致性与低延迟要求极高,调度响应窗口小于 500ms^[2]。主站网络结构需确保各环节具备访问控制边界与链路完整性校验机制,防止未经授权的访问或中间人篡改。远程操作行为依托人机终端与可视化接口执行,其访问行为需具备强认证与审计能力。面向智能化趋势,调度系统还支持 AI 模块自动接管调度逻辑,智能接口必须具备调用验证与行为边界判定机制,以防接口滥用形成逻辑型攻击路径。

3 主站网络安全面临的威胁分析

3.1 外部链路接入风险

调度主站通过远程通信链路变电站、监控终端及云平台交互数据,公网穿透、VPN 链路异构网络接入方式广泛存在。部分调度系统采用固定静态 IP 进行终端接入,缺乏动态验证机制,使得攻击者可利用网络扫描与端口探测手段精准识别入口节点。VPN 通道中如未强制密钥更新策略,静态密钥一旦泄露即导致接入信道失控,非法终端可直接映射进入调度主站边界^[3]。某些工程实施阶段遗留的临时远程调试口未封闭,亦可能成为攻击路径。

3.2 系统漏洞利用风险

调度主站核心服务运行在 Linux 或 Windows 平台上,调度平台软件及其支撑环境(数据库、中间件、脚本引擎)长期运行暴露版本更新滞后问题。默

认服务端口开放、弱口令账户未清理、路径注入未过滤是主站中常见的脆弱点^[4]。例如,在已公开的 CVE-2021-3129 中,远程攻击者可构造恶意请求绕过验证并执行任意代码,该类漏洞在未封闭的 Web 运维平台中风险显著。部分调度指令交互模块存在参数未校验现象,易被注入恶意脚本,实现主站进程控制流劫持。底层控制引擎若与上层调度平台无权限隔离机制,攻击者一旦获取控制台权限,直接操作设备模拟命令下发,破坏调度指令的合法性。

3.3 智能接口异常操控风险

主站系统引入的 AI 分析模块、辅助调度接口与开放数据交互通道,导致接口调用频率、类型及行为边界显著扩展。AI 决策引擎通常部署于与主站逻辑隔离的协同处理平台,通过数据总线传输指令建议,若其接口调用缺乏行为认证与调用来源校验机制,外部系统可能伪造合法数据格式直接介入调度过程。

部分平台采用脚本化方式实现调度任务编排,若预设脚本缺乏校验机制,调用者可嵌入逻辑重代码绕开平台策略控制,导致调度决策链被篡改。远程服务访问中嵌套的 API 接口若同时开放 GET 与 POST 通道,可能被利用以业务合法形式触发异常调用,形成非权限账户操控调度策略的入口。

4 主站网络安全防护机制

4.1 边界访问控制机制

主站边界访问控制应明确通信路径分类并实施分级隔离,SCADA 通道、控制指令链路与管理维护接口在逻辑结构上必须划分为独立通信域。SCADA 侧连接前置机模块时应设定静态 IP 白名单访问约束,调度链路则使用点对点封闭通道,不开放动态路由引导。

对边界访问控制的精细化设计应结合主站网络拓扑结构与调度行为特性,表 1 给出主站边界访问类型、接口协议与访问控制建议参数区间,以便进行约束配置的参考。物理隔离与逻辑域划分构成边界安全的第一层屏障,访问流量的认证与协议控制构成第二层拦截机制。在主站边界,命令入口、数据出口和运维通道均应实施分离策略,确保访问路径的最小化与识别性。边界安全机制在部署时应明确配置参数区间,不使用默认规则,并结合运行态下的访

问行为建立基础流量模型,作为后续行为识别模块的数据参考基础。

表1 智能电力调度主站典型边界访问类型与控制参数示意表

通信路径类型	接入协议类型	接入方向	控制参数	建议访问策略
SCADA通道	IEC 60870-5-104	单向下行	报文频率≤500ms/帧	单向白名单传输
VPN远程通道	IPsec/L2TP	双向访问	会话持续时间≤30分钟	动态密钥自动重协商
控制指令链路	TCP/IP	单向上行	报文字节校验码强制开启	协议字段固定格式校验
远程运维接口	HTTPS/SSH	双向登录	密钥长度≥2048位	接入双因子验证机制
数据同步服务	MQTT/AMQP	上行推送	每条数据包体积≤512KB	异常流量速率自动限流

4.2 系统运行环境加固机制

主站平台中广泛部署 Linux 或类 Unix 操作系统,存在服务端口常年开启、内核补丁延迟部署、账号权限等级设置单一等安全薄弱点。调度平台多基于服务型架构运行,脚本引擎、数据库连接池、中间件组件构成多种入口,攻击者可借由任一薄弱服务节点实现逻辑注入或进程劫持。

数据库系统作为主站的数据中枢,需实施角色最小权限策略,不授予调度应用进程系统级操作权限。调度日志记录模块中的中间缓存数据若未加保护,存在通过后台数据注入方式篡改历史调度记录的可能性。

主站运行环境安全加固过程涉及配置参数修改、服务约束与访问权限调整三个层面。Linux 主机中应启用 SELinux 安全模块,配置策略文件用于限制应用行为范围,调度服务脚本部署路径应启用访问控制列表(ACL),仅授权应用进程账户访问并锁定执行权限。数据库服务端口不应向外暴露,调度服务与数据库交互限定在主站内部网段中完成。控制台操作权限应依附多级账户模型,预置操作审核列表与命令执行锁定机制,限制命令越权执行场景的发生。

4.3 智能行为识别机制

智能电力调度系统在运行过程中涉及大量人机交互指令、自动生成策略逻辑与远程控制命令流,调度主站作为核心执行节点,需要对行为数据进行特征分析与策略联动的能力,传统调度系统对指令来

源与内容仅作基本合法性检查,难以识别行为意图与执行背景。在智能化条件下,主站行为识别引入基于行为模型的动态感知机制,通过建立行为图谱、访问模式与设备控制响应间的特征联系,实现对异常行为路径的感知与响应。

行为识别模型以调度行为数据为样本集,包括调度终端登录记录、控制模块调用日志、AI 模块参与频次与内容摘要等维度。行为向量的构建需提取操作路径长度、执行时间间隔、接口调用深度等参数,并与历史正常行为进行聚类比对。以调度指令发起路径为例,标准路径应表现为:控制终端登录→指令平台发起→反馈接收→执行确认,若路径中存在跳步、重发、延迟异常等行为,应触发行为风险评分模块。

AI辅助识别模型可采用自监督学习方式建立无标签识别体系,适用于调度行为特征变异性大、干预样本稀疏的运行场景。模型训练过程可使用单节点异常分数阈值设定方式,结合滑动窗口算法实现对低频高危行为的实时捕获。行为识别系统可联动日志审计模块,将风险行为路径写入审计系统,并将其指令执行状态与真实响应情况进行比对验证,增强异常行为识别的判定准确率。

5 结语

智能电力调度自动化主站在智能化电网体系中承担关键调度指令处理与状态数据交互任务,其系统架构呈现分层解耦、模块密集、接口开放的运行特性,调度业务对网络通信、指令控制和数据完整性提出高可靠性要求,实际运行中面临边界链路暴露、系统服务漏洞、智能接口滥用等多源威胁。构建由访问控制、环境加固与行为识别组成的多层防护机制可提升主站对复杂攻击路径的识别与应对能力。

参考文献

[1] 张浩, 黄玮. 智能技术在电力调度系统中的应用[J]. 电子技术, 2024, 53 (11): 192-193.
[2] 赵旭. 智能技术在电力调度自动化系统中的应用[J]. 集成电路应用, 2024, 41 (11): 326-327.
[3] 主丹丹. 电力调度中的智能技术应用[J]. 集成电路应用, 2023, 40 (12): 322-323.
[4] 曹建华, 邓秋根, 陈铭. 智能电网调度自动化系统设计[J]. 电工技术, 2023 (11): 94-96.