智能变电站二次系统安全防护技术与应用研究

姜 军 刘 飞
澄合矿业有限公司电力分公司 陕西 渭南 715200

摘 要：智能变电站二次系统作为电网运行控制的核心之一，二次系统的运行安全性与电网的可靠性和稳定性密切相关。随着电力系统复杂程度的提升以及网络攻击手段的增多，传统二次系统安全防护技术手段难以满足当下的防护要求。文章深入分析了智能变电站二次系统的安全防护目标以及运行中的安全风险因素，并进一步探讨了相关防护技术的应用和优化策略，以期为智能变电站安全运行提供参考。

关键词：智能变电站二次系统；安全防护；纵向加密；横向隔离；入侵检测

引言

智能变电站在新型电力系统建设中主要负责信息采集、命令执行、保护控制等功能，其二次系统由继电保护、测控、故障录波、同步相量测量等智能电子设备（IEDs）及支撑网络构成，二次系统的运行稳定性与变电站的自动化智能化密切相关。然而智能变电站二次系统的开放性和网络化特征，导致其在运行中面临着较多的网络安全风险因素影响，容易因为网络攻击等引发保护误动、拒动、停电等问题严重影响电力系统的运行稳定性。因此，深入研究智能变电站二次系统运行中的安全风险，并以此为基础探索并优化安全防护技术的应用，对于确保电力系统安全稳定运行具有重要作用。

1 智能变电站二次系统安全防护的基本目标

智能变电站二次系统安全防护的核心目标在于保障系统及其承载业务的机密性、完整性和可用性（CIA三要素）。具体体现为：

（1）保障控制指令安全，确保调度主站或站控层下发的遥控、遥调等重要控制命令在传输与执行过程中不被篡改、伪造或中断，防止恶意操作引发设备故障或系统崩溃。

（2）确保运行数据的完整可靠，保护SCADA数据、保护动作信息、故障录波、电能质量监测等关键运行数据在采集、传输、存储环节中的真实性和完整性，防止数据被窃取、篡改或破坏，为运行决策提供准确依据。

（3）确保系统的运行稳定性，通过安全防护保证继电保护、自动控制等关键功能能够在系统在遭受攻击和干扰时维持基本的服务能力，并在故障后快速恢复正常供电，最大限度减少停电范围与时间。

（4）构建纵深防御体系，依据“安全分区、网络专用、横向隔离、纵向认证”的防护原则，在网络边界、内部区域、终端设备等不同层次部署差异化防护措施，形成多层次、立体化的纵深防御能力。

2 智能变电站二次系统运行中的安全风险因素分析

智能变电站二次系统在运行中会受到多方面风险因素的影响，严重威胁新型电力系统的运行稳定性和安全性。具体风险因素体现在以下几方面：

（1）网络边界风险。智能变电站在运行过程中需要通过调度数据与上级调度中心进行频繁的数据交互和指令传输，构成了关键的纵向通信边界；同时站控层网络负责站内监控与数据采集，过程层网络主要负责保护和测控GOOSE跳闸命令、SV采样值等实时业务数据流。上述三个层次网络会与变电站与在线监测系统、视频安防监控系统等共同形成了复杂的网络边界，在变电站运行中，攻击者就会通过IEC 61850系列协议、MMS协议中尚未被完全修补的漏洞或者管理性缺陷利用网络扫描、渗透测试、暴力破解等方式跨越编制进入系统内部，进而破坏二次系统的防护系统[1]。在此过程中，边界防护措施的强度与策略有效性，直接决定了其抵挡外部威胁的能力。

（2）内部网络威胁。在攻击者成功攻破边界或者内部存在恶意因素，受内部网络的广播特性，如果某个智能电子设备被成功侵入并发出恶意GOOSE命令或篡改的SV数据包，恶意威胁信息就会迅速扩散至订阅该组播地址的所有相关设备，进而引起保护装置的误动和拒动，造成严重威胁。而内部影响因素，则主要是工作站服务器等受到木马或者病毒的感染，对二次系统安全造成威胁。

（3）设备本体脆弱性。二次系统的各类硬件设备主要包括保护测控装置（IED）、网络交换机、通信网关机、监控主机、服务器等设备，这类设备都在不同程度

作者简介：姜军1990-，男，汉族，辽宁辽阳，中级工程师，本科，主要研究方向：电力系统及其自动化。

刘飞1986-，男，汉族，陕西清涧，中级工程师，本科，主要研究方向：电力系统及其自动化。

上存在一些缺陷，比如IEDs、交换机、服务器等硬件设备可能存在后门、固件漏洞；嵌入式操作系统、应用软件的安全补丁普遍存在更新管理较慢的情况，并且许多变电站由于担心补丁引入会影响变电站的运行稳定性，在未出现问题的情况下漏洞长期未得到有效修补，这就会增加系统运行风险，攻击者可以利用漏洞篡改系统权限、植入恶意代码、窃取关键信息，影响智能变电站二次系统安全运行。

（4）安全协议缺失。IEC 61850（涵盖MMS、GOOSE、SV）、Modbus TCP/IP等通信协议作为变电站二次系统运行的关键，在上述协议的设计阶段多数缺乏对身份认证机制的考虑，这就导致攻击者可以轻易伪造原地址，假冒合法设备发送控制命令，并且协议中传输的数据也缺乏有效的加密保护，导致数据在传输过程中面临被窃听、篡改的风险[2]。

针对上述风险需要从多方面入手，采取有效的安全防护技术措施，切实保证智能变电站二次系统的安全稳定运行。

3 智能变电站二次系统安全防护技术应用

3.1 纵向加密认证装置的部署与优化策略

在智能变电站运行中，纵向加密认证装置能够有效防护来自调度数据网方向网络攻击，确保纵向边界安全。纵向加密认证装置通常串联部署于站控层核心交换机与远动通信网关机（或数据通信网关机）之间，从而在调度数据网接入区与站内生产控制大区（安全I区或Ⅱ区）之间形成逻辑强隔离边界，确保纵向通信的机密性、完整性与身份真实性。纵向加密认证装置的主要防护功能体现在以下几点：

（1）双向强身份认证。在通信会话建立之初，装置强制要求调度主站与变电站网关机之间进行基于数字证书的双向身份鉴别，验证对方证书的有效性，确保通信双方身份真实可信，杜绝假冒主站或变电站的非法接入。

（2）确保数据机密。装置会自动加密穿越边界的所有业务数据报文，确保即使在传输链路被窃听的情况下，攻击者也无法获取明文信息内容。

（3）数据完整性保护。装置会对传输的每一条有效数据报文附加基于密码算法（如SM3）生成的消息验证码（MAC），接收方只有利用共享密钥对报文内容重新计算MAC并与接收到的MAC进行比对，如果报文被篡改，就会因为对比失败被装置丢弃，以此来确保数据的完整性和不可篡改性。

（4）访问强制控制。纵向加密认证装置，内部设置有访问控制列表（ACL），策略规则明确规定仅允许来自预先授权的主站特定IP地址、通过指定的通信端口、使用规定的应用层协议访问站内特定的业务系统资源[3]，例如实时数据库服务、历史数据库服务、图形网关服务等数据源，任何不符合规则的访问请求都会被阻断。

但是面对智能变电站高实时性、高可靠性的严苛要求，纵向加密认证装置在部署过程中也必须进行进一步的优化和提升。第一，优先选用配备高性能专用密码芯片，如支持SM2/SM4/SM3/SM9的国密硬件加速卡的装置型号，通过硬件加速能够提升密码运算速度，避免因加密引入的延迟影响系统正常功能。第二，基于业务、源/目的IP、端口、协议等开展多维度、细粒度的访问控制，例如可配置仅允许主站A通过104协议访问远动机的遥控点表，而主站B只能访问遥测、遥信数据，有效控制相关权限。第三，建立严格的密钥生成、分发、存储、使用、更新和销毁的全生命周期管理机制，并定期更换通信会话密钥，尽可能采用更安全的密钥分发协议和平台，确保信息数据安全。

3.2 横向隔离技术在二次系统中的应用与验证

横向隔离技术则是根据智能变电站的内部安全分区，以“网络专用，横向隔离”为原则所采取的技术手段，其能够有效控制不同安全等级和业务属性网络间的数据流动，避免危险因素在站内网络的横向扩散。该技术的应用主要体现在硬件防火墙和单相隔离装置两个方面。

（1）硬件防火墙也就是状态检测防火墙，广泛应用于站控层内部不同安全区之间，例如监控区（安全I区）与管理信息区（安全Ⅱ区）的边界，也可以设置在站控层核心交换机与过程层核心交换机之间。发货箱不仅能够检查数据包的源/目的IP地址、端口号、协议类型（TCP/UDP/ICMP等），还能够实时跟踪通信会话的状态，如TCP连接的三次握手、会话状态等[4]。

在运行过程中，防火墙仅允许来自特定监控主机（IP地址）的MMS协议（端口102）流量访问指定的保护装置（IP地址），用于定值读写、装置状态监测；同时也只有来自特定保护装置的GOOSE/SV报文流向指定的交换机端口，并且在此过程中，其还能够利用深度包检测（DPI）功能识别并过滤伪装成合法端口的异常流量和潜在攻击载荷。

（2）单向隔离装置（物理/逻辑网闸），单向隔离装置一般部署在生产控制大区（安全I区、Ⅱ区）与状态监测系统、视频监控系统、办公网接口等管理信息大区间的物理和逻辑边界，其能够有效阻断任何从安全级别较低的管理信息区发起的、对生产控制系统的访问或攻击路径。由于物理网闸通常采用“2+1”架构，内外网主机

（分别连接生产区和信息区）完全物理断开，中间通过专用隔离硬件（如高速摆渡存储、反射内存板或光闸）实现数据的单向摆渡。数据流向严格限定为从生产区（内网主机）到信息区（外网主机）。逻辑网闸则在网络层和应用层实现强制的单向传输控制，通常结合协议剥离与内容审查技术，仅允许特定类型（如非实时的历史数据文件、事件报告）的数据从生产区流向信息区，反向通信被物理或逻辑上禁止。

但是横向隔离技术在应用过程中，为确保应用效果，必须做好对技术应用的适应性验证。比如在完成防火墙部署后，必须进行详尽的策略验证测试，通过网络测试仪或渗透测试工具模拟各类合法业务流量和非法/可疑流量，以此来检验防火墙规则是否能够匹配相关业务需求，是否存在误阻断或规则冗余、安全隐患等的情况。而对于网闸类设备，则必须严格测试其单向传输特性，确保从管理信息区主机向生产控制区主机发起任何形式的连接都应被确认阻断且无任何响应，并且还需要进一步验证从生产区到信息区的数据传输功能是否正常，检查传输内容是否完整、准确，同时也无任何反向通信通道存在的情况。

3.3 安全监测与入侵检测系统的设计与实施

安全监测与入侵检测系统（IDS/IPS）是智能变电站二次系统安全防护体系的“神经系统”和“主动哨兵”，致力于实现全网安全态势的可视化、威胁行为的及时发现与响应，从被动防御转向主动防御。系统设计需紧密结合智能变电站二次系统的网络架构、通信协议和业务特点，构建层次化的监测分析能力：数据采集层（全面感知）。在关键网络路径的核心交换机上配置端口镜像（SPAN/RSPAN），将流经该交换机的所有数据包（包括站控层MMS流量、过程层GOOSE/SV组播流量、对时协议流量等）复制一份发送至专用的网络流量探针（Sensor）。探针部署位置需精心规划，覆盖站控层核心交换机、过程层核心交换机，以及重要间隔层交换机等关键节点。同时在关键服务器、工作站、保护装置部署轻量级主机代理，收集系统日志、进程信息、文件完整性等主机安全数据，然后再基于特征匹配（识别已知攻击模式、恶意代码特征）与异常检测相结合的混合检测机制，就能够识别偏离度高的异常流量、行为，如异常的GOOSE命令风暴、非授权SV订阅等[5]。但是上述系统在应用过程中，首先必须确保关键网络路径和核心主机设备均在监测范围内，避免出现监测盲区；其次，分析引擎的处理能力和存储容量需与变电站的网络规模和流量水平相匹配，确保能实时处理海量数据，避免丢包或分析延迟；再者，做好规则库和检测模型的定期更新调整，根据新的威胁情报、漏洞信息以及变电站业务变化，及时调整规则和模型参数，以此来提高检测准确度。

结语

为确保智能变电站二次系统的安全稳定运行，相关运维部门和人员需要系统分析二次系统安全运行中的相关风险因素，做好对纵向加密认证、横向隔离、安全监测与入侵检测等关键技术的研究和优化应用，切实保证二次系统的安全运行。但是随着新型电力系统的不断推进，在现阶段需要进一步推动二次系统安全防护与人工智能、大数据等先进技术的融合应用，进一步提升二次系统的抗风险能力和安全防护能力。

参考文献

[1]钟昱.智能变电站二次系统安全防护技术研究[J].灯与照明,2025,49(03):168-170.

[2]崔丽丽.浅析智能变电站二次安全防护系统设计[J].机电信息,2020,(20):129-130.

[3]董峰.变电站二次系统安全防护策略的研究[J].科学技术创新,2020,(12):187-188.

[4]梁伟清.智能变电站二次安全防护系统设计与应用[J].通信电源技术,2019,36(08):30-31+34.

[5]杜明亮.智能变电站二次系统安全防护研究[J].通信电源技术,2019,36(07):40-41.