南方能源建设
Southern Energy Construction
ENERGY CHINA PRESS

二次设备集中安防运维及主动感知和诊断预警关键技术的研究

巫聪云，刘斌，沈梓正，颜丽，廖晓春

引用本文:
巫聪云, 刘斌, 沈梓正, 等. 二次设备集中安防运维及主动感知和诊断预警关键技术的研究[J]. 南方能源建设, 2021, 8(4): 85–94.
WU Congyun, LIU Bin, SHEN Zizheng, et al. Research on Secondary Equipment Centralized Security Operation and Maintenance and Key Technologies of Active Perception, Diagnosis and Early Warning[J]. *Southern Energy Construction*, 2021, 8(4): 85–94.

DOI：10. 16516/j. gedi. issn2095-8676. 2021. 04. 012 OA：https://www.energychina.press/

二次设备集中安防运维及主动感知和诊断预警关键技术的研究

巫聪云[1]，刘斌[1]，沈梓正[1]，颜丽[2,✉]，廖晓春[2]
（1. 广西电网有限责任公司，南宁 530000；2. 武汉华电顺承科技有限公司，武汉 430071）

摘要：[**目的**]针对当前电力监控系统安防要求持续更新的难题和安防整改现场作业效率低下、效果不可控的问题，以及部分二次设备无有效整改方案而大面积脱网运行的现状，研究了二次设备集中安防运维及主动感知和诊断预警关键技术。[**方法**]变电站内统一部署合规并网装置，利用基于深度信念网络的多类支持向量机入侵检测和基于自适应概率标记的IP反向追踪技术筛选录波数据、主动感知和追溯诊断入侵威胁，采用基于威胁和对抗分析相结合的风险预警和综合评估技术进行影响评估和等级评定，利用现有的录波主站系统拓展安防运维管理业务，形成集中运维管理的模式。[**结果**]实践结果表明，该方法可实现变电站二次设备安防体系集中管理和运维效率大幅提升的目标。[**结论**]结合广西电网运行案例，证明了该方法在解决二次设备现场安防整改问题中的有效性和可行性。

关键词：二次设备；安防运维；主动感知；入侵检测；反向追踪
中图分类号：TM7；TP309. 7 **文献标志码：**A **文章编号：**2095-8676(2021)04-0085-10
开放科学(资源服务)二维码：

Research on Secondary Equipment Centralized Security Operation and Maintenance and Key Technologies of Active Perception, Diagnosis and Early Warning

WU Congyun[1], LIU Bin[1], SHEN Zizheng[1], YAN Li[2,✉], LIAO Xiaochun[2]
(1. Guangxi Power Grid Co., Ltd., Nanning 530000, China;
2. Wuhan Huadian Shuncheng Science Technology Co., Ltd., Wuhan 430071, China)

Abstract: [**Introduction**] Aiming at the current problems of the continuous update of the security requirements and low efficiency and uncontrollable effects of security rectification on-site operations for the power monitoring system, and the status quo of large area off-grid operation of some secondary equipment without effective rectification methods, secondary equipment centralized security operation and maintenance and key technologies of active perception, diagnosis and early warning are studied. [**Method**] Compliant grid-connected devices were unified deployed in substations, the technologies of deep belief nets multi-class support vector machine intrusion detection and adaptive probabilistic marking scheme IP traceback were used to filter recording data, active percept and retrospective diagnosis invaded threats, the risk early warning and comprehensive assessment technology based on combining with threat and adversarial analysis were adopted to carry out impact assessment and rating, and the existing recording master station system was used to expand the security operation and maintenance management business to form centralized operation and maintenance management model. [**Result**] Practical results show that this method can achieve the goals that the security system of substation secondary equipment is centralized managed and efficiency of operation and maintenance is higher. [**Conclusion**] The proposed method is effective and feasible to solve the problem of on-site security rectification of secondary equipment combined with the Guangxi power grid operation case.

Key words: secondary equipment; security operation and maintenance; active perception; intrusion detection; traceback

收稿日期：2021-08-16 **修回日期：**2021-09-01
基金项目：广西电网公司科技项目资助“安全受控的变电站录波器智能运维与合规并网关键技术的研究与应用”(046000KK52200016)

近年来，国际网络安全形势愈发严峻，乌克兰、委内瑞拉等国家级大规模停电事故时有发生，电网已成为网络攻击战的主战场。我国对电力系统网络信息安全监管引起了高度的重视，国家发展和改革委员会第 14 号令《电力监控系统安全防护规定》、国能安全 36 号文《变电站监控系统安全防护总体方案》和《中国南方电网电力监控系统安全管理办法》（Q/CSG 212001—2015）等陆续颁布，对保障电网稳定运行的监控系统网络信息安全加大了管控力度，对已经投运的变电站二次设备提出了严格的整改要求[1-3]。

变电站二次设备不仅分布广泛、数量庞大、类型繁杂，而且投放时间各异、安全水平参差不齐，安防整改同步实施难以实现。相较于采用入网软件直接并网的保护装置等嵌入式设备，利用后台管理机并网的录波器安全问题最为突出[4-5]。南方电网已有超过 50 %的录波器因无有效的安防整改手段，不得不大面积脱网运行，数据无法正常上送；部分安防整改后达标的录波器，虽暂时符合电网安全等级的要求，但其安防体系长期处于静态，仍存在安全隐患。目前采用分头安防整改的现场运维模式，已暴露出整改效率低下、效果不可控等问题，而且也无法从根本上解决安防要求持续更新的难题，变电站二次设备安防运维模式优化，成为电力系统网络信息安全保障工作中亟待解决的问题。

1 变电站二次设备安防运维现状分析

国内外对电力监控系统安防运维的探索多停留于智能终端安防体系的建立，对仍处于服役期但安防要求不达标的脱网二次设备安防运维方面的研究较少，安防运维模式优化及相关技术的研究更为鲜见，变电站二次设备安防运维现状如表 1 所列。本文考虑到现存部分二次设备安全整改不达标脱网运行后数据无法上送主站系统的现状，并结合文献[6]-[13] 所提方法，通过在变电站内部署安防体系完善的合规并网装置，实现变电站二次设备集中管理和数据安全输出，同时兼顾设备数据安全统一管理和装置安防体系集中运维，最终实现二次设备安防整改和维护管理效益的最大化。

表 1 变电站二次设备安防运维现状分析

Tab. 1 Analysis on the current situation of security operation and maintenance for secondary equipment in substation

文献	安防运维方法/技术	安防特点	运维特点	安防效果			备注
				感知	诊断	预警	
传统	定期下站安检和运维/人工干预	静态	现场分散	×	√	×	现场分头整改、依赖人工经验效果不可控，运维效率低下
[6]	搭建新安防运维系统/立体化、全局式的智能防护和控制技术	动态	—	√	×	√	新系统投入成本高，无实际应用案例参考
[7],[8]	建立智能终端安防体系/芯片层、终端层和交互层防护技术	动态	—	√	√	×	适用于电力系统智能终端设备信息网络安防，无实际应用案例参考
[9]	建立终端设备的零信任安全架构/可信感知、安全认证技术	动态	—	√	√	×	
[10],[11]	建设智能变电站安防体系/风险识别技术和战略响应机制	动态	现场分散	√	√	√	国外注重基础设备智能化安防监控和管理，在调度集成系统方面投入落后于国内
[12],[13]	二次设备的远程运维/服务端数据集中管理和按需输出、数据服务化技术、设备状态监视技术	—	远程集中	—	—	—	减少现场巡视频率，满足对变电站运行状态的远程巡视和操作需求，提高设备的精细化管理水平，无实际应用案例参考
本文	基于合规并网装置统一部署的变电站二次设备集中安防运维方法/威胁主动感知和追溯诊断、风险实时感知和综合评估技术，就地安防管控和集中安防运维模式	动态	远程集中	√	√	√	同时适用于变电站内智能设备以及现存安防整改不达标脱网老旧二次设备的安防问题管理，落实装置投入和运维一体化、常态化的建设目标

基于上述分析，本文提出二次设备集中安防运维及主动感知和诊断预警关键技术的研究，在变电站内统一部署合规并网装置，就地解决录波器并网和数据安全传输的问题，提供高可靠的录波数据传

输和访问服务；利用录波主站拓展运维业务应用，开发集中运维管理平台，将对数量多、分布广和改造难度大的异构录波器进行安防整改，转换成对规格一致的合规并网装置进行安防策略升级和统一维护，形成变电站二次设备集中安防运维的新模式。

2　变电站二次设备集中安防运维架构

在合规并网装置接入变电站后，通过集中运维的方法不断升级和优化装置内部的安防体系，保持装置高安全防护标准。变电站二次设备集中安防运维架构主要包含合规并网装置、录波主站系统和运维管理平台三个部分，其中合规并网装置的作用在于安全防护录波数据和威胁追踪处理，录波主站系统和运维管理平台是利用调度侧主站多源数据分析能力和运维业务拓展功能，对分散的合规并网装置安防体系进行全盘统筹和维护管理，如图 1 所示。

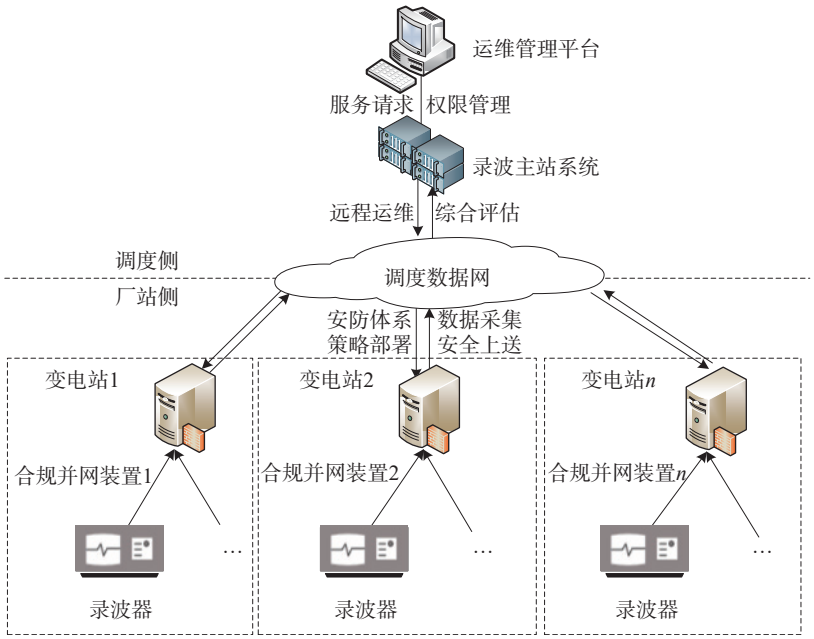

图 1　变电站二次设备集中安防运维架构

Fig. 1　Substation secondary equipment centralized security operation and maintenance architecture

1）合规并网装置：装置有多个物理通信接口与变电站录波器进行互连，具备健全的安防体系，包含设备安全管理、网络状态监视、漏洞扫描、病毒查杀、权限管理、日志审计和服务优化等，在录波器和调度数据网之间起到安全隔离的作用。将接入的数据根据通信协议和特征属性进行数据分类、主动感知和威胁分离，确保上送的数据安全可靠。

2）录波主站系统：利用现有的主站系统，进行合规并网装置安防体系集中运维业务的延伸，通过录波主站和装置之间建立的通信连接，接收分布式合规并网装置上送的录波数据和预警的威胁信息整理结果，站在全局角度对风险进行综合评估。

3）运维管理平台：录波主站对所有连接的合规并网装置触发安防体系巡检任务，生成记录合规并网装置安防体系版本信息的检查报告，调度统一制定相应的应对策略，通过专用运维接口，对合规并网装置进行规范化的策略部署，包括但不限于病毒库升级、漏洞修复和系统升级，实现集中安防运维管理。

3　变电站二次设备集中安防运维方法

利用合规并网装置解决变电站录波器安全并网问题，对接收到的录波数据进行安全管控，通过入侵检测和反向追踪进行威胁感知和追溯诊断，录波主站根据威胁预警信息进行风险综合评估，调度制定应对策略，通过集中部署的方式进行变电站侧安防体系统一升级和维护。变电站二次设备集中安防运维管理方法主要包含威胁入侵拦截、风险综合评估和安全策略部署三个部分，如图 2 所示。

1）威胁入侵拦截：合规并网装置实时接收站内录波器上送的数据，为防止录波器数据被非法篡改或与录波器连接的链路遭受网络攻击等问题的发

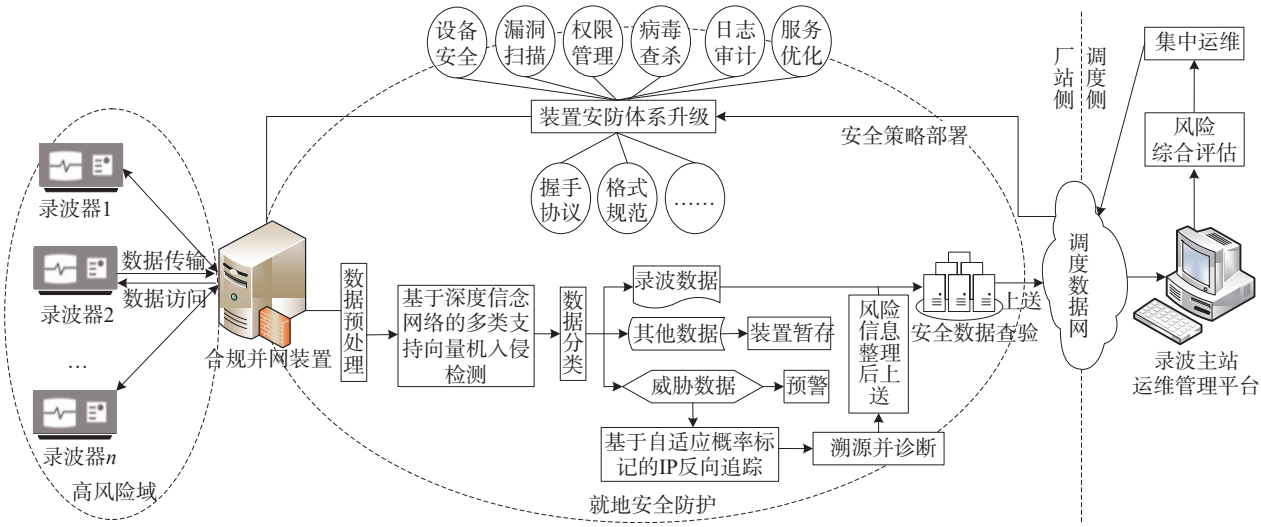

图2 变电站二次设备集中安防运维方法

Fig. 2 Substation secondary equipment centralized security operation and maintenance method

生，对数据源IP、MAC地址、设备端口、数据格式、携带病毒等情况进行检查，利用入侵检测技术筛选出符合预先通信设置和格式、内容审计要求的录波数据，过滤出符合入侵特征的威胁数据，利用反向追踪技术，追溯到恶意代码、非法行为的来源，进行威胁拦截和阻断。

2）风险综合评估：合规并网装置利用威胁和对抗分析相结合的方式对感知到的威胁进行评估和预警，录波主站对装置上报的风险进行综合评估和等级评定，制定相应的短期对策，如高危端口暂时屏蔽、数据传输链路转移等应对办法，使得风险可以暂时规避，争取更多时间制定长期有效的安防策略。

3）安全策略部署：对风险进行策略的制定和验证，进行攻防演练，确认策略的有效性、可行性和归属类别，在全网范围内实施有效防御措施。运维管理平台利用策略部署的方式进行分布式合规并网装置安防体系策略库的版本升级，实现变电站内合规并网装置安全策略的统一部署和集中运维的目标，提高装置自身的安全防护能力。

4 变电站二次设备集中安防运维关键技术

4.1 基于入侵检测和反向追踪的威胁主动感知和追溯诊断

合规并网装置处于录波器和主站系统之间，其作用是安全传递录波数据，该装置接收与自身达成通信协议要求的录波器数据，对监测到的数据的来源、格式和内容等信息做数据检测和安全检查，筛选出主站所需的录波数据，以及感知和诊断二次设备入侵的威胁，提高录波数据上送的安全可靠性[14-15]。基于入侵检测和反向追踪的威胁主动感知和追溯诊断如图3所示。

1）基于入侵检测的威胁主动感知：建立录波数据特征库和入侵特征信息库，对录波数据的需求内容进行定义，对已出现过的非法入侵等风险行为进行特征提取，利用适合于海量数据环境的基于深度信念网络的多类支持向量机（deep belief nets multi-class support vector machine，DBN-MSVM）入侵检测技术进行数据筛选[16]。

a）特征降维：对高维、非线性接收到的数据进行DBN特征降维处理，去除冗余特征。

b）深度检测：利用深度数据包检测（deep packet inspection，DPI）对低维特征数据检测其传输协议、头部信息和有效载荷等，使用录波数据特征库和网络攻击入侵特征信息库进行快速匹配。

c）数据筛选：采用MSVN分类器分离出不同类别的数据，包含录波数据、威胁数据和其他数据三类：

①录波数据：将遵循协议要求且符合暂态数据交换通用格式（common format for transient data exchange，COMTRADE）标准的录波数据，与其他数据初步分离开来，录波数据需经过合规并网装置安全检查，确认安全后上送录波主站。

②威胁数据：利用入侵特征信息库，主动感知

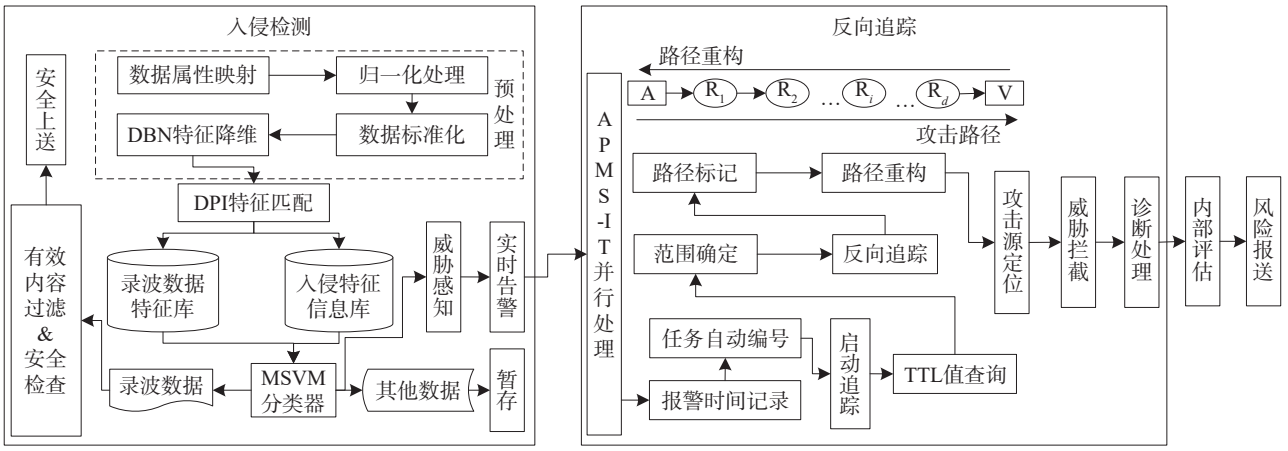

图3　基于入侵检测和反向追踪的威胁主动感知和追溯诊断

Fig. 3　Threat active perception and traceback diagnosis based on intrusion detection and traceback

带有攻击性质的入侵行为或企图，发出威胁入侵告警信号，并对识别到的恶意代码、病毒、漏洞等威胁进行有效隔离。

③其他数据：非录波数据和威胁数据，可以设定保留期限，将其进行暂存处理，保留期间无主站主动召唤，不得上传，减少网路开销。

2）基于反向追踪的威胁追溯诊断：网络攻击者在实施攻击之时或之后，会留下登录的记录、文件权限更改等证据，利用基于自适应概率标记的IP反向追踪 （adaptive probabilistic marking scheme IP traceback，APMS-IT）技术对威胁数据进行破译，消除威胁者伪造IP标记的影响，重构攻击的完整路径阻断威胁[17-18]，并根据收集的信息利用安防体系进行威胁诊断和跟踪处理。

a）启动追踪：根据威胁入侵告警信号，发起反向追踪，并做相应的追踪任务编号，实现威胁追踪任务的并行处理。

b）范围确定：IP首部包含8位生存时间TTL（time-to-live）字段，设置了数据包可以经过的最多路由器数。对接入网端口进行统一TTL值配置，依据数据包每经过一个路由器TTL值减1的特性，从TTL值的变化推断数据包经过的路由器跳数，自适应调整标记数据包的概率，从而确定IP标记追踪的路由器范围。

c）反向标记：利用开始时刻和路由器范围，触发该范围内路由器级数的标记工作。

d）路径重构：进行威胁攻击路径的反向重构，追溯威胁发起者的实际物理地址。

e）威胁诊断：合规并网装置根据攻击路径，可迅速采取限流、过滤等拦截手段，阻断威胁并控制影响范围，利用装置部署的漏洞扫描、病毒查杀、设备安全检查、权限检查、日志审计、服务检查等安防手段对控制的威胁进行诊断定位，并持续跟踪处理。

4.2　基于威胁和对抗分析相结合的风险预警和综合评估

根据过往经验、知识总结，不断更新合规并网装置的入侵特征信息库，使其具备快速发现代码或者环境安全问题的能力，并利用自身所建立的安防体系对抗威胁产生的攻击，进行威胁博弈状态的动态分析和风险评估，实现风险快速预警的目标。主站系统根据单台装置上报的风险概率和严重程度，进行风险影响范围的全面评估和等级评定，实现风险信息全盘掌控和快速应对的目标，基于威胁和对抗分析相结合的风险预警和综合评估技术如图4所示。

1）装置风险预警：合规并网装置利用威胁和对抗分析相结合的方式，对感知到的威胁进行内部评估和风险预警，并整理追踪过程中收集到的证据，按照主站协议要求和安全汇报形式进行风险信息报送。

a）对于合规并网装置a安防体系的对抗能力，生成对抗性集合$A=\{A_i|i=1,2,\cdots,n\}$，其中，n表示装置对抗性种类的数量，A_i表示第i种对抗性。

b）合规并网装置主动感知到的威胁集合为$T=\{T_j|j=1,2,\cdots,m\}$，其中，m表示装置识别出的威胁

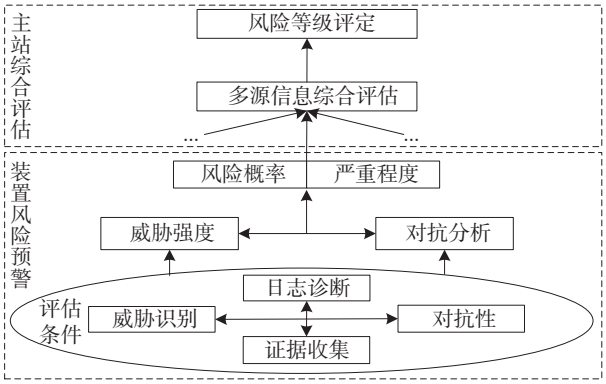

图 4 基于威胁和对抗分析相结合的风险预警和综合评估

Fig. 4 Risk early warning and comprehensive assessment based on the combination of threat and adversarial analysis

数量，T_j表示第j种威胁。

c）$P_j=P(T_j, A)$表示威胁T_j与合规并网装置的安防体系A对抗后，威胁事件发生的可能性。

d）I_a表示合规并网装置a的重要程度，V_j表示威胁事件T_j发生后装置安防体系脆弱性，$S_j=S(I_a, V_j)$表示威胁事件T_j发生后装置受损的严重程度。

e）$R_j=P_j\times S_j$超过合规并网装置设定的安全阈值R_S，装置即刻发出风险预警[19]。

由于合规装置安防体系对抗威胁产生的攻击，属于一个博弈的过程，可以参考文献［19］进行博弈模型的搭建、威胁攻击成功的概率$P_j=P(T_j, A)$和装置受损严重程度$S_j=S(I_a, V_j)$的计算，最后得到威胁风险R_j，并和历史安防经验选取的对抗性阈值R_S比较，定性判断出合规并网装置对抗威胁能力的强或弱。

2）主站综合评估：对合规并网装置预警的威胁事件展开全网范围内的排查，经过多源信息融合分析[20-21]，进行影响范围的综合评估。对攻击类型相同、源地址一致，以及攻击时间相近的威胁统计合规并网装置上报的总次数，计算该次数与全网该装置总数的比值k，根据合规并网装置a在威胁事件T_j发生后的风险R_j，最终计算全网风险$R_j^*=k\times R_j$，并归一化到区间［0，1］，利用表 2 映射关系，将风险划分为高、中、低三个级别[22]。

5 变电站二次设备集中安防运维运作模式

变电站二次设备集中安防运维遵循“最小授权和最少服务”的原则：

1）最小授权：以最小权限开放 IP 地址及端口，阻止装置被安装未授权、未许可的恶意软件，防止不法分子对装置的非法访问和信息篡改等问题。

2）最少服务：禁用高危服务，合规并网装置仅支持录波数据的安全传输和主站系统的定制运维业务需求。

变电站二次设备安防运维采用就地安防管控和集中运维管理相结合的运作模式，如图 5 所示。

1）就地安防管控：合规并网装置实现变电站内所有录波器受控并网和录波数据安全上送，对录波数据外的威胁进行主动感知和反向追踪，拦截威胁将风险控制在最小范围，根据装置安防体系对抗性分析确认风险严重程度，上报主站系统进行风险综合评估[23-24]。装置配备运维专用接口，既支持运维管理平台远程统一升级，也支持运维策略的现场落地。

2）集中运维管理：运维平台基于合规并网装置的设备序列号和安全版本信息，选择需要升级的装置，通过专用运维接口和堡垒机进行权限审核后，利用补丁或系统更新等方式，制定相应的升级策略、升级包和升级情况管控表单进行进度跟踪处理，确保合规并网装置安全策略升级成功，并配套更新主站数据库中的装置安全版本信息。

集中安防运维的新模式，全面替代以往录波器长期脱网、分头整改、重复下站的现场安防运维模式，该模式集中修复合规并网装置安防体系存在的风险，提高装置安防体系的安全级别和运维效率[25-26]。

表 2 基于威胁和对抗分析相结合的风险综合评估映射关系

Tab. 2 Comprehensive risk assessment mapping relationship based on the combination of threat and confrontation analysis

装置风险值比较	装置对抗性	覆盖范围	综合风险值	综合风险等级
$R_j>R_S$	弱	k=上报风险次数/装置总台数	$R_j^*=k\times R_j$	低风险：$R_j^*\leqslant 0.3$ 中风险：$0.3<R_j^*<0.7$
$R_j<R_S$	强			高风险：$R_j^*\geqslant 0.7$

6 实例应用

6.1 变电站二次设备数据威胁主动感知和追溯诊断

对电力监控系统二次设备历史数据网络传输过程中发现的威胁按攻击类型进行分类，大致分为拒绝服务类、获取权限类、信息收集类、网络监控类等，根据不同类型威胁的入侵特征及攻击链建立入

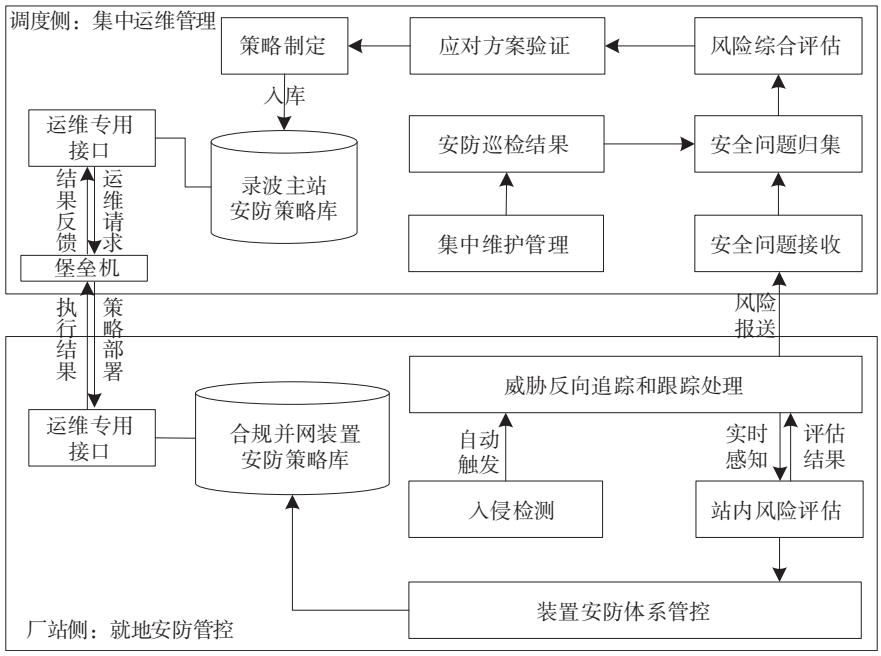

图5　变电站二次设备集中安防运维运作模式

Fig. 5　Substation secondary equipment centralized security operation and maintenance mode

侵特征信息库，一级特征提取信息展示如表3所列。

表3　威胁类型及特征信息

Tab. 3　Treat classification and character information

威胁攻击类别	特征集
拒绝服务类	protocol_type, dst_bytes, service, logged_in, is_hot_login, is_guest_login, srv_dif_host_rate, srv_serror_rate, srv_rerror_rate, diff_srv_rate
获取权限类	protocol_tupe, service, num_file_creations, dst_host_count, dst_host_srv_rate
信息收集类	duration, service, dst_bytes, count, dst_host_count, dst_host_srv_count
网络监控类	protocol_type, src_bytes, hot, logged_in, is_hot_login, srv_serror_rate, dst_host_count

合规并网装置利用DBN-MSVM入侵检测技术，利用文献［14］中目前较为权威的Lincoln实验室KDD'99测试数据集入侵检测模型搭建方法，从训练样本集中选取2 000个数据作为候选，其中正常录波数据1 796个，携带威胁数据204个，该装置对实时接收到的录波器数据进行威胁特征识别，利用RBF核函数，调整核参数gamma=0.125，惩罚系数C=8，通过10折交叉验证获得平均超过95%的验证准确率，并从威胁标注完成后的准确率和误报率两个角度表征入侵检测模型的精度，如表4所列，实现不同类别的威胁数据主动感知、快速检测和分离。

表4　基于DBN-MSVM入侵检测技术的主动感知结果

Tab. 4　Active perception result based on DBN-MSVM intrusion detection technology

威胁攻击类别	主动感知	
	准确率/%	误报率/%
拒绝服务类	98. 11	0. 10
获取权限类	96. 02	0. 33
信息收集类	98. 26	0. 12
网络监控类	91. 77	0. 25

合规并网装置利用威胁类别特征更为细分的二级、三级特征子集进行威胁数据入侵特征匹配，记录每个数据入侵特征匹配的可信程度，按威胁入侵特征可信度进行优先级排序并诊断，利用APMS-IT技术查询TTL值，自动探测威胁数据覆盖范围和传播路径，反向追踪找到威胁入网端口并取证，拦截威胁，将风险控制在当前变电站最小范围内，从而为威胁数据诊断和风险评估预警争取有利时机。

6.2　变电站二次设备集中安防运维管理模型

利用入侵检测主动感知威胁数据，利用反向追踪和安防手段进行威胁溯源和诊断分析，采用威胁和对抗分析相结合的方法进行风险预警和综合评

估，使用补丁、脚本、操作规范和软件升级等方式进行集中的安全策略统一部署。

变电站二次设备集中运维管理模型如表 5 所列，从表中可清晰呈现面对不同风险，合规并网装置的对抗性，以及主站评估的风险影响范围、等级和策略配置需求，安防运维人员可根据运维管理平台汇总的安防管理信息有计划、有策略地进行合规并网装置的安防升级和维护管理，实现变电站安全问题参差不齐的录波器安防管理和集中运维的目标。

表 5 变电站二次设备集中安防运维管理模型

Tab. 5 Substation secondary equipment centralized security operation and maintenance management model

威胁诊断	风险预警	综合评估	策略配置
漏洞扫描	(1)震网三代;(2)远程桌面 CVE-2019-0708 漏洞。	对抗性:弱;影响范围:全网风险等级:高	补丁安装: (1)震网三代(KB4072212);(2)CVE-2019-0708 漏洞(KB4499175)。
病毒查杀	勒索病毒	对抗性:弱;影响范围:全网风险等级:高	病毒库更新或补丁安装: 勒索病毒补丁安装(KB4022722)
设备安全检查	(1)telnet、FTP 远程工具使用;(2)非法访问;(3)敏感文件信息泄露;(4)root 操作。	对抗性:强;影响范围:单台风险等级:低	(1)安装 SSH,通过使用 SSH 代替 telnet、FTP;(2)配置本机访问控制列表,限制远程 SSH 管理 IP;(3)传输敏感文件加密;(4)root 用户远程登录限制。
权限检查	(1)默认账号登录;(2)FTP 用户账号;(3)用户登录会话超时。	对抗性:弱;影响范围:全网风险等级:高	(1)账号限制使用;(2)拒绝系统默认的系统帐号使用 ftp 服务;(3)设置登录超时控制用户登录会话时间为 300 s。
日志审计	(1)syslog 登录事件;(2)日志系统未配置文件保护。	对抗性:强;影响范围:1/3 风险等级:低	(1)syslog 登录事件记录捕获 authpriv 消息;(2)修改日志配置文件(syslog. conf)权限为 400(管理员账号只读)。
服务检查	e-mail、telnet、rlogin、ftp 系统服务	对抗性:弱;影响范围:单台风险等级:低	服务不支持

6.3 变电站二次设备集中运维效率提升

对于最常发生的漏洞和病毒安全问题，运维人员通过安防体系集中运维管理平台，即可全盘掌握变电站合规并网装置规格信息和软件版本，为安防体系的策略部署提供必要的信息支撑。原来需要协调不同厂商重复下站安防整改，现在只需要对变电站内合规并网装置版本信息调取和后台部署升级即可，可大大减少沟通、管理成本和人力投入。

以合规并网装置诊断预警的远程桌面漏洞为例，采用变电站二次设备现场和集中安防运维模式，其效率比对结果如表 6 所列。从表中可以看出，CVE-2019-0708 漏洞集中运维的效率提升 90% 以上，利用运维管理平台跟踪装置后台补丁安装进程，同步更新安全版本信息库，即可实现装置安防体系的集中升级和运维管理，缓解运维人员的工作压力和劳动强度。

表 6 远程桌面漏洞/两种模式的变电站二次设备安防运维效率比对

Tab. 6 Remote desktop vulnerability/comparison of security operation and maintenance efficiency of two modes for substation secondary equipment

威胁类型	策略配置	运维模式	运维工作量*	厂站侧就地安防管控			主站侧集中运维管理	运维效率	备注
				主动感知	诊断	预警			
CVE-2019-0708 漏洞	补丁	现场运维	6 000 台录波器	—	非实时	—	—	>300 人天	协调 9 大主流厂商下站安防整改
		集中运维	1 000 台合规并网装置	实时	实时	实时	实时	<5 人天	补丁 KB4499175 集中升级

注：*以 220 kV 变电站为例，变电站录波器与合规并网装置数量比例近似为 6∶1。

7 结 论

本文所研究的二次设备集中安防运维及主动感知和诊断预警关键技术，通过厂站侧合规并网装置对接入的数据进行深度检测，对威胁主动感知、追溯诊断和风险预警，利用调度侧录波主站系统接收

的多源信息和对装置的安全版本管理，全盘考虑威胁的影响程度和范围进行综合评估，制定相应的安全策略，集中进行策略部署和升级维护，通过动态的安防运维，保障合规并网装置安防体系持续地升级和完善。此方法基本解决了安防要求不断更新的难题和现场安防效率低下、效果不可控的问题，大幅度提高了变电站二次设备的安防运维效率。

参考文献：

[1] 国家发展和改革委员会. 电力监控系统安全防护规定 [EB/OL]. (2014-09-30)[2021-08-16]. http://www. gov. cn/gongbao/content/2014/content_ 2758709. htm.
National Development and Reform Commission. Security protection regulations on power monitoring system [EB/OL]. (2014-09-30) [2021-08-16]. http://www. gov. cn/gongbao/content/2014/content_2758709. htm.

[2] 黄鑫, 陈德成, 孙军, 等. 网络攻击下电力系统信息安全研究综述 [J]. 电测与仪表, 2017, 54(23): 68-74.
HUANG X, CHEN D C, SUN J, et al. A review of information security research in power system under cyber attack [J]. Electrical Measurement & Instrumentation, 2017, 54(23): 68-74.

[3] 赵俊华, 梁高琪, 文福拴, 等. 乌克兰事件的启示: 防范针对电网的虚假数据注入攻击 [J]. 电力系统自动化, 2016, 40(7): 149-151.
ZHAO J H, LIANG G Q, WEN F S, et al. Lessons learnt from the Ukrainian blackout: protecting power grids against false data injection attacks [J]. Automation of Electric Power Systems, 2016, 40(7): 149-151.

[4] 陈文睿, 陈创, 廖晓春. 变压器和断路器远程在线监视系统的设计与应用 [J]. 南方能源建设, 2018, 5(1): 132-138.
CHEN W R, CHEN C, LIAO X C. Design and application of remote online monitoring system for transformer and circuit breaker [J]. Southern Energy Construction, 2018, 5(1): 132-138.

[5] 李海勇, 田君杨, 蒋连钿, 等. 基于云边协同的集控式继电保护设备智能运维方法 [J]. 电力信息与通信技术, 2021, 19(10): 38-45.
LI H Y, TIAN J Y, JIANG L D, et al. Centralized intelligent operation and maintenance method of relay protection equipment based on cloud-edge collaboration [J]. Electric Power ICT, 2021, 19(10): 38-45.

[6] 王栋, 陈传鹏, 颜佳, 等. 新一代电力信息网络安全架构的思考 [J]. 电力系统自动化, 2016, 40(2): 6-11.
WANG D, CHEN C P, YAN J, et al. Pondering a new-generation security architecture model for power information network [J]. Automation of Electric Power Systems, 2016, 40(2): 6-11.

[7] 张涛, 赵东艳, 薛峰, 等. 电力系统智能终端信息安全防护技术研究框架 [J]. 电力系统自动化, 2019, 43(19): 1-8+67.
ZHANG T, ZHAO D Y, XUE F, et al. Research framework of cyber-security protection technologies for smart terminals in power system [J]. Automation of Electric Power Systems, 2019, 43(19): 1-8+67.

[8] 吴小娟, 张丛丛, 潘洪湘, 等. 变电站自动化广域运维系统安全防护技术的设计与实现 [J]. 浙江电力, 2020, 39(1): 41-46.
WU X J, ZHANG C C, PAN H X, et al. Design and implementation of safety control technology for substation automation wide-area operation and maintenance system [J]. Zhejiang Electric Power, 2020, 39(1): 41-46.

[9] 高鹏, 陈智雨, 闫龙川, 等. 面向零信任环境的新一代电力数据安全防护技术 [J]. 电力信息与通信技术, 2021, 19(2): 7-14.
GAO P, CHEN Z Y, YAN L C, et al. A new generation of power data security protection technology for zero-trust environment [J]. Electric Power Information and Communication Technology, 2021, 19(2): 7-14.

[10] LI Z, SHAHIDEHPOUR M, AMINIFAR F. Cybersecurity in distributed power systems [J]. Proceeding of the IEEE, 2017, 3(23): 1-22.

[11] BAGGOTT S S, SANTOS J R. A risk analysis framework for cyber security and critical infrastructure protection of the U. S. electric power grid [J]. Risk Analysis, 2020, 40(9): 1744-1761.

[12] 刘晓华, 邓科, 陈理, 等. 基于远程监控的变电站二次设备运维主站系统的开发与设计 [J]. 电子设计工程, 2018, 26(17): 57-61.
LIU X H, DENG K, CHEN L, et al. Development and design of main equipment system for secondary operation of substation based on remote monitoring [J]. Electronic Design Engineering, 2018, 26(17): 57-61.

[13] 姚志强, 黄海峰, 吴艳平, 等. 基于透明访问的集中式变电站远程运维系统建设方案探讨 [J]. 电力系统自动化, 2019, 43(14): 166-172+181.
YAO Z Q, HUANG H F, WU Y P, et al. Discussion on construction scheme for remote operation and maintenance system of centralized substation based on transparent access [J]. Automation of Electric Power Systems, 2019, 43(14): 166-172+181.

[14] 徐吉用, 廖晓春, 李福, 等. 智能变电站站控层在线监测技术的应用研究 [J]. 电力信息与通信技术, 2019, 17(8): 50-56.
XU J Y, LIAO X C, LI F, et al. Research on the application of on-line monitoring technique in the station control layer of smart substation [J]. Electric Power ICT, 2019, 17(8): 50-56.

[15] 杨至元, 张仕鹏, 孙浩. 电力系统信息物理网络安全综合分析与风险研究 [J]. 南方能源建设, 2020, 7(3): 6-22.
YANG Z Y, ZHANG S P, SUN H. Integrated cyber-physical contingency analysis and risk estimates [J]. Southern Energy Construction, 2020, 7(3): 6-22.

[16] 高妮, 贺毅岳, 高岭. 海量数据环境下用于入侵检测的深度学习方法 [J]. 计算机应用研究, 2018, 35(4): 1197-1200.

GAO N, HE Y Y, GAO L. Deep learning method for intrusion detection in massive data [J]. Application Research of Computers, 2018, 35(4): 1197-1200.

[17] 张钰莎, 蒋盛益. 基于风险数据挖掘追踪技术的网络入侵检测研究 [J]. 重庆理工大学学报(自然科学版), 2019, 33(10): 127-135.
ZHANG Y S, JIANG S Y. Research on network intrusion detection based on risk data mining tracking technology [J]. Journal of Chongqing University of Technology(Natural Science Edition), 2019, 33(10): 127-135.

[18] 王卓然. 面向网络安全事件应急响应的入侵跟踪与取证 [D]. 南京: 东南大学, 2017.

[19] 黄鹏, 张娜. 基于网络安全风险评估的攻防博弈模型 [J]. 西昌学院学报(自然科学版), 2014, 28(4): 71-74+86.
HUANG P, ZHANG N. Attack and defensive game model based on network security risk assessment [J]. Journal of Xichang College (Natural Science Edition), 2014, 28(4): 71-74+86.

[20] 游昊, 石恒初, 杨远航, 等. 基于改进 D-S 证据理论的电网故障多源信息智能融合诊断方法 [J]. 广东电力, 2020, 33(11): 16-25.
YOU H, SHI H C, YANG Y H, et al. Intelligent fusion diagnosis method for multi-source information of power grid fault based on improved D-S evidence theory [J]. Guangdong Electric Power, 2020, 33(11): 16-25.

[21] 石恒初, 游昊, 李本瑜, 等. 继电保护主站信息融合决策系统的设计与应用 [J]. 电力信息与通信技术, 2021, 19(1): 81-90.
SHI H C, YOU H, LI B Y, et al. Design and application of information fusion decision system for relay protection main station [J]. Electric Power ICT, 2021, 19(1): 81-90.

[22] 梁智强, 林丹生. 基于电力系统的信息安全风险评估机制研究 [J]. 信息网络安全, 2017(4): 86-90.
LIANG Z Q, LIN D S. Information security risk assessment mechanism research based on power system [J]. Netinfo Security, 2017(4): 86-90.

[23] 周佳, 邓永晖, 贾悠, 等. 安全配置策略自动生成与验证技术研究 [J]. 通信技术, 2020, 53(9): 2257-2263.
ZHOU J, DENG Y H, JIA Y, et al. Automatic generation and verification of security configuration policy [J]. Communications Technology, 2020, 53(9): 2257-2263.

[24] 汪溢, 胡春潮, 高雅, 等. 变电站自动化设备远方配置维护及在线监护系统 [J]. 自动化技术与应用, 2018, 37(12): 171-175.
WANG Y, HU C C, GAO Y, et al. Remote configuration maintenance and online monitoring system for substation automation equipment [J]. Techniques of Automatic and Applications, 2018, 37(12): 171-175.

[25] 韦恒, 李海勇, 黄超, 等. 基于边缘计算的继电保护海量录波数据轻量级传输优化方法 [J]. 电力信息与通信技术, 2021, 19(8): 24-31.
WEI H, LI H Y, HUANG C, et al. Optimization method for relay protection mass recording data lightweight transmission based on edge computing [J]. Electric Power ICT, 2021, 19(8): 24-31.

[26] 巫聪云, 刘斌, 沈梓正, 等. 基于边缘计算的故障录波主站信息快速智能处理方法 [J]. 南方能源建设, 2021, 8(2): 91-98.
WU C Y, LIU B, SHEN Z Z, et al. Fast and intelligent information processing method for fault recorder master station based on edge computing [J]. Southern Energy Construction, 2021, 8(2): 91-98.

作者简介：

巫聪云

1979-，男，广西宾阳人，高级工程师，电气工程专业硕士，主要从事电力系统继电保护管理工作（e-mail）252644051@qq. com。

巫聪云

刘斌

1986-，男，湖北仙桃人，高级工程师，学士，主要从事电力系统继电保护运行维护及专业管理工作（e-mail）279777084@qq. com。

沈梓正

1988-，女，黑龙江佳木斯人，高级工程师，硕士，主要从事电力系统继电保护管理工作（e-mail）1563587491@qq. com。

颜丽（通信作者）

1984-，女，湖北武汉人，工程师，物理电子学硕士，主要从事智能电网、继电保护信息集成技术研究工作（e-mail）274237534@qq. com。

廖晓春

1976-，男，湖北武汉人，高级工程师，计算机应用技术博士，主要从事智能电网、继电保护信息集成技术研究工作（e-mail）whsckj@139. com。

项目简介：

项目名称 “安全受控的变电站录波器智能运维与合规并网关键技术的研究与应用”（046000KK52200016）

承担单位 广西电力调度控制中心，武汉华电顺承科技有限公司

项目概述 项目主要研究包括：（1）研制合规并网装置，实现嵌入式、低功耗、自维护运行，与录波器同寿命、等规格的长效安全并网保障；（2）建立最小化、无污染、高安全、性能优的系统信息安防环境，支持主站统一安全策略部署与远程运维；（3）建立录波数据的无损标准化、故障信息分拣上送的边缘预处理机制，解决传统数据海量异构问题，成倍提升现有录波主站性能。

（责任编辑 李辉）