引用格式： 李永刚，潘善民.从合规到实战：MITRE ATT&CK 赋能新型电力系统关键基础设施安全保护标准的实施路径 [J]. 标准科学，2026 (4)：69-77.
LI Yonggang, PAN Shanmin. From Compliance to Real War: Implementation Roadmap of MITRE ATT&CK Supporting New Power System CIS Security Defense Criteria[J]. Standard Science, 2026(4)：69-77.

从合规到实战：MITRE ATT&CK 赋能新型电力系统关键基础设施安全保护标准的实施路径

李永刚[1,2] 潘善民[1,2]

〔1.国网思极检测技术（北京）有限公司；2.国网思极网安科技（北京）有限公司〕

摘 要：【目的】新型电力系统逐步开放、互联、智能化，在新能源、智能终端接入的同时无限放大了新型电力系统对外暴露面，带来严峻的网络安全挑战，为解决现有防护体系难以防御高持续性威胁的问题，亟须提升新型电力系统安全防御能力。【方法】通过将MITRE ATT&CK威胁建模框架映射到GB/T 39204—2022《信息安全技术 关键信息基础设施安全保护要求》中，建立了“合规基线+实战能力”协同防御体系，通过“分析识别、安全防护、检测评估、响应恢复”四步实施路径，形成一套可操作、可度量的技术实施清单和技术能力评价指标体系。【结果】通过在某集中式光伏电站的验证，本方案能系统性地提高对恶意控制指令攻击的检测与防范水平，将平均威胁检测时间从小时级缩短至分钟级。【结论】验证了该方法在提高新型电力系统安全保障能力的有效性，为关键信息基础设施的安全防护提供了可行的技术手段。

关键词： 新型电力系统；关键基础设施；GB/T 39204；MITRE ATT&CK；协同防御

DOI编码： 10.3969/j.issn.1674-5698.2026.04.006

From Compliance to Real War: Implementation Roadmap of MITRE ATT&CK Supporting New Power System CIS Security Defense Criteria

LI Yonggang[1,2] PAN Shanmin[1,2]

(1. State Grid SLJI Testing Technology (Beijing) Co., Ltd.; 2. State Grid Cyber Security Technology (Beijing) Co., Ltd.)

Abstract: [Objective] The gradual opening-up, interconnection, and intelligentization of the new power system, along with the integration of new energy sources and smart terminals, infinitely expands the attack surface of the system externally, posing severe cybersecurity challenges. To tackle the challenges posed by existing protection systems in the context of defending against high-persistence threats, and to strengthen the security defense capabilities of the new power system. [Methods] The paper develops a collaborative defense system that integrates the “compliance baseline” with “practical capability” by aligning the MITRE ATT&CK threat modeling framework with the GB/T 39204-2022, *Information security technology—Cybersecurity requirements for critical information infrastructure protectio*n. Through a structured four-step implementation process of “analysis and identification, security protection, detection and evaluation, response and recovery”, the paper develops a set of actionable and measurable technical implementation checklists and technical capability evaluation index systems. [Results] At a centralized photovoltaic power station, this solution is validated to systematically improve detection and prevention of malicious control command attacks, reducing the average threat

作者简介： 李永刚，本科，高级工程师，研究方向为电网网络安全。
潘善民，硕士，工程师，研究方向为电网网络安全。

detection time from hours to minutes. [Conclusion] This study confirms the effectiveness of the method in enhancing the security assurance capability of new power systems, offering a feasible technical approach for security protection of critical information infrastructure.

Keywords: new power system; critical infrastructure; GB/T 39204; MITRE ATT&CK; collaborative defense

0　引 言

随着能源转型的加速，以开放互动、灵活智能为特征的新型电力系统[1]，已成为现代能源体系的重要组成部分，同时也导致其网络的暴露面显著增加。传统的安全防护体系难以有效防御诸如Industroyer、TRITON等新型网络攻击武器的定向攻击，使得网络安全面临前所未有的挑战。新型电力系统内发电、输电、配电、用电等多环节的紧密耦合，以及海量分布式能源资源的接入，构成了一个复杂的信息物理系统[2]。而网络攻击可能穿透虚拟空间，直接对物理设备造成破坏，威胁电力供应的安全稳定。

面对高级持续性威胁（Advanced Persistent Threat，APT）的严峻挑战，当前网络安全防御体系与真实攻击行为之间存在显著脱节。为破解此难题，本文探索以 ATT&CK（Adversarial Tactics，Techniques & Common Knowledge）为“攻击者视角导航”[3]，以GB/T 39204 为“合规骨架”[4]，将ATT&CK框架系统性地嵌入“分析识别、安全防护、检测评估、响应恢复”的网络安全生命周期，引导防护体系从被动合规向主动、动态、可度量的实战化防御转变[5]，最终让新型电力系统的安全韧性得以提升，保障国家能源安全。

1　标准与框架

构建新型电力系统的安全防护体系[6]，GB/T 39204—2022对关键信息基础设施保护提出了明确要求，其核心活动涵盖“分析识别、安全防护、检测评估、监测预警、主动防御、事件处置”6个方面。该标准确立了防护的“基线”，明确了“做什么”，是安全建设的法定依据和基本框架。

MITRE ATT&CK框架则是一个基于全球真实攻击案例构建的知识库[7]，它详细描述了攻击者在攻击生命周期中可能采用的技战术。本文将ATT&CK的12项核心战术概括为“初始访问、执行与持久化、横向移动、业务影响”4个关键阶段，用于匹配电力CPS（Cyber-Physical Systems）攻击链，为防御者提供了“攻击者视角”和一套通用的行为描述语言，精准回答了“如何攻击”的问题，是提升实战能力的“工具箱”。

二者的融合，本质上是“合规基线”与“实战能力”的深度融合。GB/T 39204构筑了防御体系的“骨架”，确保了防护的全面性与合法性；而MITRE ATT&CK则为骨架填充了“血肉”，使得安全防护变得可衡量、可验证[8]，从而解决防护与威胁脱节的问题。具体实现的技术能力包括场景化建模能力、精准检测技术（含技术ID即规则需求对应）、实战评估能力（采用红蓝共用矩阵）、统一度量技术（以覆盖热力图指引投入）。

2　技术路径

将MITRE ATT&CK的技战法应用在GB/T 39204—2022的各个阶段，构建新型电力系统的安全治理技术指南，驱动闭环管理，实现安全防护能力的整体提升。表1对安全生命周期的4个阶段目标、关键动作和成果进行了整理。

2.1 分析识别

新型电力系统是非常复杂的信息物理系统（CPS），传统的基于资产清单梳理和漏洞扫描的方法难以对付高级威胁。“分析识别”阶段的成果不是简单的资产清单和漏洞清单，因为它不能回答

表1 ATT&CK与GB/T 39204融合实施路径

阶段	核心目标	关键动作（融入MITREATT&CK）	成果
1. 分析识别	识别关键业务、资产及威胁	1. 业务场景攻击链建模；2. 资产和威胁的映射关系；3. 风险量化排序	可能的攻击路径、资产—ATT&CK映射链条、高风险清单
2. 安全防护	部署纵深防御措施	1. 绘制防护覆盖的热力图；2. 进行差距分析并强化改进措施；3. 进行策略优化与防护热力图优化方案的制定	策略优化后的防护热力图、差距分析报告、安全防护的优化建议方案
3. 检测评估	检测并及时发现攻击并分析有效性	1. 建立检测规则库，并及时识别攻击行为，评估有效性；2. 使用统一的数据采集平台；3. 开发基于ATT&CK的红蓝对抗检测规则库	开发的检测规则库、安全态势视图、渗透测试报告
4. 响应恢复	快速响应事件并恢复业务	1. 编制针对性的剧本；2. 实施主动防御集成；3. 对响应剧本库、事件溯源报告以及闭环更新记录进行溯源分析	响应剧本库、事件溯源报告、闭环更新记录

攻击者将如何利用系统弱点，对电力生产、传输、配送造成实质性物理影响这类核心问题。

引入MITRE ATT&CK框架后，把安全治理的焦点从“存在什么漏洞”转为“可能会遇到什么样的攻击”，这就有了一个具体、明确的标准化方法。把ATT&CK和“分析识别”阶段的资产、威胁关联起来，这对实现安全治理精准、实效而言是很关键的。

2.1.1 建立“业务—资产—威胁”映射链条

GB/T 39204这一标准的重点就是去识别关键业务、关键资产，还有面临的威胁。利用ATT&CK框架建立了动态且可追溯的映射关系[9]。

（1）关键资产识别与属性扩展

首先，要识别电力行业的关键业务，如“互联网数据接入”“配电自动化”，把其流程分解为“数据采集→状态估计→指令下发”的形式。并进一步识别支撑流程的IT/OT资产，同时列出IP地址和主机名等主要资产属性，建立资产档案，包括以下内容：

1）识别与关键性赋值。识别每个业务流程的IT与OT资产，建立资产档案，包括物理属性（设备型号、固件版本等）、功能属性（业务角色、支持协议等）、网络属性（安全区域、访问路径）、资产等级（按照风险评估对资产的重要性进行赋值）等。

2）对关键业程的数据流图进行绘制。把信息的路径从传感端[智能电表、PMU（Power Management Unit）]到控制端[主站、SCADA（Supervisory Control and Data Acquisition）]，再到执行端[PLC（Programmable Logic Controller）、断路器]的路径完整地展示出来，这是后续分析攻击路径的依据。

（2）精细化威胁识别

传统的威胁识别只是泛化概念，像“病毒、黑客、木马”等。ATT&CK框架一旦引入，就以MITRE ATT&CK（Enterprise + ICS）矩阵为核心威胁库，构建资产—技术映射，生成一张“资产—威胁映射表”，清晰呈现每个关键资产面临的主要威胁技术。例如：

1）边界部署的VPN（Virtual Private Network）服务器存在遭受T1133–External Remote Services（利用外部远程服务）攻击的风险。

2）SCADA服务器易受 T1059.003 – Windows Command Shell（Windows命令行执行）攻击。

3）PLC是T0859–Theft of Operational Information（窃取操作信息）和T0856–Modification of Control Logic（修改控制逻辑）的直接目标，从而形成“资产—威胁映射表”，以展示资产面临的各类威胁。

2.1.2 威胁建模与风险量化

在资产和威胁的映射之上，结合信息安全风险评估的方法，对业务、资产、威胁进行赋值，实现动态威胁建模。

（1）攻击链构建

采用攻击链方法，针对特定场景进行建模。以“篡改储能电站逻辑”场景为例，可构建如下攻击链：利用鱼叉式钓鱼附件（T1566.001）发起攻击，接着调用命令行解释器（T1059），再获取有效账户（T1078），随后进行远程系统发现（T1018），最终实现修改控制逻辑（T0856）。将攻击链用工具可视化，让每个节点与具体资产和ATT&CK技术相关联。

（2）集成漏洞数据（CVE）与资产配置

MITRE的CAPEC（常见攻击模式枚举和分类）数据库描述了攻击的技术本质，借助关联CVE（Common Vulnerabilities and Exposures），把攻击链中的每个技术节点与已知的CVE漏洞和不当配置联系起来[10]，比如把T1190–Exploit Public–Facing Application 与相关CVE漏洞关联；把T1078 –Valid Accounts 与“默认密码未改”等配置问题关联起来。

最终形成综合风险视图，其中攻击路径的风险值取决于技术的可行性（参考ATT&CK技能要求）、关联漏洞严重性（Common Vulnerability Scoring System，CVSS分值）、目标资产关键性等因素，以此达到从“威胁”到“风险”的转化。

2.1.3 构建动态知识库

本阶段输出并非简单的清单，而是价值极高的动态知识库，主要有：

（1）新型电力系统专属威胁库：基于ATT&CK定制的威胁知识库。

（2）高风险攻击路径集。以优先级排序的可视化攻击链，将最脆弱环节处标注出来（如“通过智能电表集中器渗透配电主站”）。

（3）安全控制差距分析报告。把攻击链节点对应到现有措施，加入风险防控清单。

（4）量化风险评估。可以通过集成多源数据的风险数据，实现量化评估，作为管理者决策依据。

2.2 安全防护

GB/T 39204—2022第7章“安全防护”中提出了要有纵深防御与主动防御的要求。将MITRE ATT&CK深度嵌入这一环节中，则可以推动防护模式由静态、基于合规清单的被动响应，逐步过渡为动态、基于威胁的可验证能力建设。具体来说就是能够建立一条清晰逻辑链：针对某项资产面临的具体ATT&CK技术，实施定向防控并进行效果检验，且进行效果检验，增强防护体系的精准性、可衡量性和自适应能力。

2.2.1 现状评估

通过绘制“防护覆盖热力图”，可明确当前能力与威胁要求的差距，主要步骤如下。

（1）构建映射矩阵。构建一个矩阵，把ATT&CK for ICS技术当作行、已有的具体控制措施当作列。控制措施需以如下的形式呈现。

1）网络层。采用东西向微隔离策略，比如只允许SCADA服务器与指定PLC的502端口通信。

2）主机层。在主机层实施SCADA服务器应用程序白名单策略。

3）身份层。采用双因子认证的运维堡垒机。

4）数据层。对PLC逻辑代码变更予以数字签名验证。

（2）赋值和可视化。对每个“技术—控制”的单元予以赋值，具体为完全防护的为绿色、部分防护的为黄色、未防护的为红色，以及不适用这4种情况。由此产生的热力图直观展示了未覆盖的技术范围及其深度，也展示了部分覆盖的技术范围及其深度，所以“横向移动”“权限提升”等战术就出现了许多黄色或红色区域。

2.2.2 差距分析与优先级

热力图识别出的缺口可能很多，不过资源有限，得按照风险进行优先级排序。

（1）风险量化模型。对每个攻击性ATT&CK技术，依据前序“分析识别”所得结果，计算其对应的风险值。

风险值=技术可行性×业务影响

（2）技术可行性。参考ATT&CK技术本身所

需的技能等级（Low/High）、是否需要特殊设备等。也可引入威胁情报，以识别出APT组织是否常用此技术。

（3）业务影响。该技术成功执行后，对电力系统安全稳定运行所造成的潜在影响等级，比如导致机组脱网、频率波动、大面积停电等潜在的影响等级。

（4）确定强化优先级。把高风险值且当前防护等级为“未防护”或“部分防护”的技术，列为最高优先级的强化对象。比如修改控制逻辑（T0866 – Modification of Control Logic）和未授权指令消息（T0885–Unauthorized Command Message）。这类情况一般对业务影响很大，要优先部署防护。

2.2.3 针对性的防护措施

按照优先级为关键攻击技术进行设计和部署精准的防护，比如工业防火墙的“逻辑变更白名单”功能、工控主机应用程序白名单。

（1）对控制逻辑的修改（T0856–Modification of Control Logic）予以防护

1）预防性措施（逻辑变更白名单与签名）。使用管理平台部署专用软件，对预防措施而言是可行的。任何下载至PLC的逻辑都需要验证签名，要确保仅授权工程师可执行此操作。此措施应满足IEC（International Electrotechnical Commission）62443–3–3关于“系统完整性”的要求。

2）检测性措施（协议深度解析）。在OT网络部署支持深度包检测（Deep Packet Inspection，DPI）的IDS（Intrusion Detection System），检测性措施是这样配置的：要对异常工程协议指令进行检测，如非工作时间的逻辑块写入请求或来自非授权IP下载的会话。该措施映射《工业控制系统安全指南》（NIST SP 800–82）Rev.2监控建议的遵循。

（2）对窃取操作信息（T0889–Theft of Operational Information）的防护技术措施

监控与审计措施。在SCADA历史数据库服务器启用详细审计策略，借助SIEM（Security Information and Event Management）建立访问行为基线，对异常数据查询（如非工作时间大批量访问）进行检测。该措施对应GB/T 39204标准中“安全审计”要求。

（3）横向工具传输（T0846–Lateral Tool Transfer）的防护技术

微隔离与通信加密。以SDN（Software–Defined Networking）或者下一代防火墙来实施“工作负载”级策略，比如规定“HMI–A只能主动访问PLC组–B的502端口”这类情况。可对敏感的OT协议进行安全扩展，或者采用IPsec VPN加密，以防止窃听与横向移动的攻击。该措施足以达到GB/T 39204中“安全通信网络”和“安全区域边界”两项具体规定的要求。

2.2.4 防护能力优化

“安全防护”这一阶段，其成果不是简单的设备清单，而是一个需要持续运营的知识库，并且要形成基于ATT&CK的《安全防护能力差距分析》和《防护策略优化方案》，为防护能力提升提供参考。

（1）动态的安全控制矩阵。将ATT&CK技术、安全控制措施、配置参数、关联资产关联起来，从而达到安全矩阵的动态管理，进而开展挂图作战。

（2）防护策略优化清单。编制一份包含风险评估、防火墙规则变更建议、IDS签名更新计划、系统加固等内容的安全措施的优化清单，以便支持日常的安全运维工作。

（3）安全架构演进路线图。依据防护缺口的相关的技术防护路径，找出何时部署终端检测与响应（Endpoint Detection and Response，EDR）、何时实施全流量威胁检测平台等，根据防护的重要程度，编制安全架构的优化建议，从而为安全架构规划提供决策依据。

（4）合规性举证材料：通过对照风险清单编制的安全防护措施，开展ATT&CK热力图和对应的控制措施矩阵动态优化，并建立常态化的更新机制，从而满足合规管理的证据要求。

2.3 监测与审计

GB/T 39204—2022第8章“检测评估”规定，要及时发现攻击的痕迹、要周期性验证现有防护

是否仍然有效。传统监测平台虽日志比较全面，但信息量庞大，比如告警条数十万条且误报过多，查找有效线索困难。通过引入MITRE ATT&CK后，视角由“签名与异常”转向“行为链条”，运营人员只需解决“能不能找到某条ATT&CK技术被触发的实例？”

2.3.1 构建工程化的检测能力

将ATT&CK技术转化为可运行、可维护的检测逻辑，这是提升检测能力的基础。方法是以规则库为载体，为每一个高优先级的技术编写具体的检测规则。比如针对T0889，对SCADA历史数据库的非工作时间、大批量查询行为进行检测。

（1）检测规则库开发

先要进行数据源的识别，然后编写ATT&CK技术的检测规则，再进行检测规则库的开发。

1）数据源识别和标识。依据ATT&CK框架对每个技术的描述，明确所需数据源。比如检测T0847 – Rogue Master（恶意主站）时，需要采集网络流量数据（识别Modbus/TCP报文中的异常）以及进程监控数据（检测未授权软件实例）。

2）检测逻辑设计。以检测T0856 – Modification of Control Logic为例，需要有多源联动的情况。

3）进程数据。对工程软件（如TIA Portal）的启动命令参数进行监控，以发现异常路径或非授权用户启动行为。

4）网络流量。要借助DPI解析S7comm（Siemens S7 Communication Protocol）这类工控协议，来检测非工作时间的逻辑块下载（DB Download）请求，或者来自非授权IP的指令。

5）文件监控。对PLC逻辑存储区的哈希值变化进行比较。

6）规则实现与优化。主要目的是持续减少误报，提升检测效率，借助Splunk SPL、Elasticsearch KQL或通用的Sigma规则，来实现上述逻辑，而且还得持续调优以减少误报。

（2）建设统一数据平台

构建一个统一的数据平台，用于汇聚并关联IT与OT数据，并确保数据质量[11]。

1）数据采集。把IT数据（防火墙日志、EDR（Endpoint Detection and Response）、Windows事件）、OT（工业防火墙日志、工控IDS告警、HMI/SCADA系统日志）数据汇聚起来，再进行格式统一等标准化工作，这样才能满足数据的采集要求。

2）数据规范化与富化。以SIEM（Security Information and Event Management）、SOAR（Security Orchestration, Automation, and Response）平台为基础，为每个安全事件打上ATT&CK技术ID标签。比如将OT–IDS的“异常Modbus写操作”告警映射至关联 T0801，实现事件与技术点的关联。

3）态势的可视化。通过SOC（Security Operations Center）来展示ATT&CK战术层级的攻击链视图，横向展示各个技术分部，纵向标注受影响资产与严重程度，如此一来，就能快速研判攻击严重程度，从而开展应急处置的工作。

2.3.2 开展评估并实施处置

定期主动开展风险评估及威胁监测分析，以此评估安全防护是否有效，进而构建可持续化的运营能力建设。

（1）攻防对抗采用ATT&CK框架

按照GB/T 39204要求，定期开展渗透测试。ATT&CK框架给出了标准化的评估方法和基线。主要包括3个步骤：

1）基线设定。攻击方演习完全基于ATT&CK攻击链开展，防守方能不能在各个战术阶段及时察觉并告警，这是衡量标准。

2）度量方法。核心指标为攻击链检测覆盖率和各战术阶段平均检测时间（Time to Detect，TTD），而不是简单的“是否发现”。

3）输出报告。报告清晰地指出检测体系对哪些ATT&CK技术存在盲区，给出精确改进优化方向和具体的工作清单，方便后续的实施。

（2）主动威胁猎杀

基于威胁的攻击，即攻击者主动实施的活动，是超越自动化检测能力的主动安全举措。主要包括：

1）假设驱动的方法。从攻击者角度筛选出高危技术，构建可证伪命题，比如“攻击者通过利用供应链污染（关联 T0815）在监控软件中植入后门”。

2）狩猎执行。猎手把命题拆成行为特征，通过数据平台进行高级查询，像翻账本一样，对风机监控软件的异常外联记录进行比对。

3）闭环反馈。无论是否察觉威胁，结果都会被输入规则库，新增或优化检测逻辑，提升整体能力。

2.3.3 打造长效的运营机制

评估阶段目标是不断地优化安全运营能力，组建专业的运营团队，构建长远的运营体系，并且定期开展相关工作，比如编制ATT&CK的《检测规则清单》《攻击仿真测试案例》和《安全有效性评估报告》等，以优化工作。核心技术包含：

（1）成熟度模型的度量评估方法[12]。该模型通过量化指标，综合考虑ATT&CK技术覆盖率和检测效率（如通过检测时间（TTD）来衡量），对检测能力进行评级。

（2）动态检测规则库。根据ATT&CK矩阵的更新、动态验证以及优化检测规则集合（像Sigma规则库之类的）构建。

（3）高质量的威胁评估报告。按照ATT&CK的渗透测试和红蓝对抗报告，给出具体且可操作的改进建议，达成风险和威胁的闭环管理。

（4）制度化的猎杀手册[13]。通过对猎杀手册进行制度化的完善，以形成可重复的猎杀方法，提升整体团队的威胁发现能力。

2.4 响应恢复

GB/T 39204—2022第11章对事件响应与恢复有所要求。在传统的“分级—上报—处置”响应模式之下，在面对定向的APT攻击时，常出现处置滞后这类问题。MITRE ATT&CK框架的引入促使事件响应从“被动应急”转变为“主动战役”，形成“定位—遏制—根除—恢复”的闭环管理，这样能减少业务中断时间，确保威胁彻底处理掉。

2.4.1 搭建基于剧本的响应体系

在现代安全运营中，剧本化响应（Playbook）是很核心的内容。ATT&CK框架给剧本的编写提供了最理想的结构化输入与输出标准。

（1）事件信息增强及剧本触发机制

1）统一语义。在SOC平台接收到告警后，首先将告警信息映射为ATT&CK技术ID。例如“可疑PowerShell执行”告警映射为T1059.001，“异常Modbus写操作”映射为T0801。

2）攻击链重建与自动触发。将各类单一的攻击与防御（ATT&CK）技术告警进行关联分析。当识别出具有某种攻击链状况时，就激活相应剧本。当资产在战术时序上出现 T1566.001→T1059.005→T1018等行为组合，系统判定该资产“内网渗透初步成功”，并启动对应剧本。

（2）剧本结构与自动化动作

以“响应T0856（修改控制逻辑）事件剧本”为例，围绕“遏制—根除—恢复”这一设计进行针对性的动作。

第一阶段：遏制（Containment）。

技术动作1（网络微隔离）：此技术依靠防火墙API，把受害PLC的IP访问策略限制为“仅允许备份工程师站访问”，且把被攻陷的工程师站隔离开来，防止其横向移动。

技术动作2（逻辑冻结）：借助管理平台将PLC设为“只读/停机”模式，让恶意逻辑不再有执行环境。

第二阶段：根除（Eradication）。

技术动作1（取证溯源）：针对工程师站磁盘镜像开展集中检索，充电查找T1059（命令行相关痕迹）、T1071（C2通信相关痕迹）等，以此获取完整攻击路径。

技术动作2（资产清理）：重装工程师站系统，把相关凭证重置，修补导入口的漏洞，清除持久化的载体。

第三阶段：恢复（Recovery）。

技术动作1（逻辑回滚）：调用带有数字签名的备份数据，再重新下载给PLC，然后通过校验工具来确保一致性。去除T0856的影响。

技术动作2（业务验证）：在隔离测试环境中，

先对PLC功能予以验证，再把其重新接入网络，并提升监控级别。

系统借助SOAR平台预设接口完成整套动作的调用，执行结果即时反馈至SOC，生成可追溯、可审计的响应记录。

2.4.2 集成主动防御与深度溯源

GB/T 39204所倡导的“主动防御”理念，在ATT&CK框架下得以落地，满足及时、响应精准需求。

（1）整合主动防御（Active Defense）

1）欺骗技术。在OT网络部署高仿的蜜罐（像伪装成关键PLC），这样就能以之为手段，当剧本触发怀疑存在T0840（横向移动）这一情况时，把攻击流量引导至蜜罐，记录攻击者技战术，获取反制情报。

2）动态防御技术。通过发现入侵的行为时，可以通过网络结构的动态调整（如修改VLAN），以延迟攻击进度，为人工干预争取时间。

（2）ATT&CK化的溯源（Forensics）

将所有离散证据（例如主机痕迹、流量元数据、蜜罐日志）统一标上 ATT&CK 技术编号，按时间轴自动拼接成攻击链图[14]，这样就能展示从入口到目标的完整路径、各阶段使用的技战术及证据，用于责任认定、体系加固和向上汇报。

2.4.3 实现响应效能提升与闭环管理

凭借剧本化来实现响应的标准化及效能提升，同时建立了可度量、可进化的闭环机制。

（1）标准化与知识沉淀：打造可重复的ATT&CK响应剧本库，保证不同团队进行处置的一致性。通过定义基于ATT&CK的评价指标，像有攻击链遏制时间（从某个技术被检测到后续技术被阻止的时间）等，按期量化响应效率。

（2）威胁情报闭环：从每次事件的溯源分析中提炼出新的攻击者技战术，将这些技术反馈至检测规则库，调整响应剧本，从而形成“检测→响应→情报→增强检测”的管理机制。

（3）具备强合规的证据：留存的ATT&CK响应剧本及演练记录，可以作为强合规的证据，以满足GB/T 20985.1—2025（征求意见稿）关于“风险相适应”事件处置能力的举证要求。

3　实践验证

为验证“合规基线+ATT&CK实战能力”模型是否有效，以青海某集中式光伏电站为验证对象，使用“无线接入侧异常”与“逆变器控制指令篡改”这个高风险场景进行验证。

3.1 验证方法

（1）基线评估任务：绘制场站的ATT&CK防护热力图，明确标出T1133（外部远程服务）、T0856（控制逻辑修改）这2项“红色”缺口。

（2）针对性加固：1）在网络边界上，增加零信任网关、开启动态权限控制，并关闭那些非必要且不必要的远程通道；2）集控区与发电区之间部署白名单级协议过滤，以屏蔽非业务指令。

（3）攻击演练：红队以厂区无线CPE进行渗透，进而获取运维终端权限，并下发异常控制指令的路径进行演练，整个过程仅使用公开协议字段，没有涉及任何设备私有指令或参数细节，以此确保演练环境与现实环境的一致性。

3.2 验证结果

攻击者利用无线CPE渗透至集控区，还试图篡改逆变器指令，异常流量在横向移动阶段就会被标记，恶意指令会被白名单实时拦截，平均检测时间由1.2小时缩至4分钟，核心攻击路径防护覆盖率提升了32%，验证模型有效。

在新的检测机制下，攻击行为在“横向移动”阶段即被察觉，并在恶意指令下发（T0801）时被成功阻断。威胁平均检测时间从小时级缩短至3分钟以内，实现了对关键攻击的有效拦截。验证完毕后，系统ATT&CK热力图中相关技术的防护状态，从原本未防护（红色）状态，提升为现在的已防护（绿色），其核心攻击路径防护覆盖率提升超过30%。通过实验验证，此方法能够精准定位防护不足之处，并开展安全措施实施，增强了威胁的快速发现和处置能力。

4 结论与展望

本文针对新型电力系统面临的严峻网络安全挑战，探索了将MITRE ATT&CK实战化框架与GB/T 39204—2022合规标准相结合的防护路径。构建了“合规基线为骨架、实战能力为血肉”的协同防御模型，有效改善了传统静态防护体系在主动防御方面存在的不足。采用系统设计的“分析识别、安全防护、检测评估、响应恢复”四阶段实施路径，再加上配套的技术清单，把抽象的国家标准要求转化为可操作、可度量的具体方法。在某集中式光伏电站中的实践应用表明，该方法能够精准定位防护短板，提高安全防护措施的针对性，还将对恶意控制指令等关键攻击平均检测时间从小时级显著缩短至分钟级，从而使新型电力系统的安全韧性得到提升。同时使关键信息基础设施的安全防护从“被动合规”转变为“主动、动态、可度量”的实战化防御范式。

以后的工作将围绕智能化集成、供应链安全深化、标准体系完善3个方面不断地深化应用。探索将人工智能技术应用到ATT&CK攻击链的自动化建模以及实时推演之中，实现更精准的威胁预测和自适应防御；把ATT&CK框架的应用拓展到上游，推动构建一个覆盖电力行业软硬件供应链的协同威胁评估模型，从源头降低安全风险；推动形成基于ATT&CK的电力行业安全能力成熟度评估标准，让本文提出的方法成为行业最佳实践，以推动整个电力行业安全防护水平的整体提升。

参考文献

[1] 《电力系统自动化》编辑部.“新型电力系统数字化关键技术综述”专辑评述[J].新型电力系统,2024,2(1):52–64.

[2] 郭剑波,王铁柱,罗魁.新型电力系统面临的挑战及应对思考[J].新型电力系统.2023,1(1):32–43

[3] MITRE Corporation.MITRE ATT&CK? Framework [EB/OL]. [2025–09–20].Available: https://attack.mitre.org/.

[4] 信息安全技术 关键信息基础设施安全保护要求：GB/T 39204—2022[S].2022.

[5] 徐胜超,蒋大锐,吕峻闽.考虑AI大模型的多维网络安全度量及主动防御策略[J].计算机技术与发展,2026,36(3):215–221.

[6] 电力监控系统安全防护规定:国家发展改革委令第27号[Z].

[7] MITRE Corporation. MITRE ATT&CK Version 16 Release Notes. October 2024[EB/OL]. [2025–09–20]. Available: https://attack.mitre.org/resources/updates/updates–october–2024/.

[8] 张静,张光洲,金学奇,等.电力监控系统基于ATT&CK框架的威胁路径构建方法研究[J].电力信息与通信技术,2024,22(12):55–61.

[9] MITRE Corporation. MITRE ATT&CK? for Industrial Control Systems[EB/OL]. [2025–09–20].Available: https://attack.mitre.org/matrices/ics/.

[10] MITRE Corporation. MITRE CAPEC? (Common Attack Pattern Enumeration and Classification)[EB/OL]. [2025–09–20].Available: https://capec.mitre.org/.

[11] HINDY H, BROSSET D, BAYNE E, et al.A Taxonomy of network threats and the effect of current datasets on intrusion detection systems[J].IEEE Access,2020:8104650–104675.

[12] MUNDT M, MüCKE S, WRESSNEGGER C. On the evaluation of security detection capabilities with MITRE ATT&CK[C]//Proceedings of the 15th ACM Workshop on Artificial Intelligence and Security. New York: ACM, 2022: 1–10.

[13] LOZANO M A,LLOPIS I P ,DOMINGO M E. Threat Hunting Architecture Using a Machine Learning Approach for Critical Infrastructures Protection[J]. Big Data Cogn. Comput,2023,7:65.

[14] 杨秀璋,彭国军,刘思德,等. 面向APT攻击的溯源和推理研究综述[J]. 软件学报, 2025,36(1):203–252.