引用格式:李翔硕,畅广辉,苏盛,等.变电监控系统网络安全威胁指标研究综述与展望[J].电力科学与技术学报,2024,39(4):1-10.
Citation:LI Xiangshuo,CHANG Guanghui,SU Sheng,et al.Review and prospect on cyber threat indicators of substation monitoring system[J].Journal of Electric Power Science and Technology,2024,39(4):1-10.

变电监控系统网络安全威胁指标研究综述与展望

李翔硕[1],畅广辉[1],苏 盛[2],阮 冲[3],吴 坡[3],李 斌[1]
(1.国网河南省电力公司调度控制中心,河南 郑州 450052;2.长沙理工大学电气与信息工程学院,湖南 长沙 410114;
3.国网河南省电力公司电力科学研究院,河南 郑州 450052)

摘 要:网络安全威胁指标(cyber threat indicators,CTIs)是描述或识别网络空间安全威胁所必需的信息,有效表征和刻画攻击行为的CTIs是保障网络安全的基础。与通用信息系统相比,变电监控系统所需应对攻击的强度和能力水平有显著差异,掌握有专业知识的有组织攻击可以通过供应链攻击等方式潜入生产控制区,因为能够突破身份权限管理限制,并不一定会引起安全告警。因此,沿用通用信息系统的CTIs难以准确检测针对变电监控系统定向设计的高隐蔽性网络攻击。为此,首先综述通用信息系统的传统CTIs;然后分析既有结合变电监控系统特点设计的CTIs。在此基础上,针对高隐蔽性安全威胁检测难题,利用变电监控系统的各业务系统按确定流程规则执行业务、一次系统状态以及二次系统通信与告警间具有强耦合性的特点,对基于合规性的变电站CTIs提取设计进行展望,有望准确刻画不触发告警但违反业务规则的高隐蔽性安全威胁,为进一步提高安全防护能力奠定基础。

关 键 词:变电监控系统;网络安全威胁指标;高隐蔽性安全威胁;合规性;异常检测
DOI:10.19781/j.issn.1673-9140.2024.04.001 **中图分类号**:TM863 **文章编号**:1673-9140(2024)04-0001-10

Review and prospect on cyber threat indicators of substation monitoring system

LI Xiangshuo[1], CHANG Guanghui[1], SU Sheng[2], RUAN Chong[3], WU Po[3], LI Bin[1]
(1.Dispatching Control Center,State Grid Henan Electric Power Company, Zhengzhou 450052, China; 2. School of Electrical & Information Engineering, Changsha University of Science & Technology, Changsha 410114, China; 3.Electric Power Research Institute, State Grid Henan Electric Power Company, Zhengzhou 450052, China)

Abstract: Cyber threat indicators (CTIs) refer to the information necessary to describe or identify cybersecurity threats in cyberspace. Effective CTIs that represent and depict attack behaviors are the foundation for ensuring cybersecurity. Compared with general information systems, the intensity and capability level of attacks that substation monitoring and control systems need to address exhibit significant differences. Organized attacks carried out by individuals with professional knowledge can infiltrate production control areas through supply chain attacks, bypass identity and access management restrictions, and may not necessarily trigger security alerts. Therefore, using CTIs designed for general information systems is inadequate for accurately detecting highly concealed cyber attacks specifically targeted at substation monitoring and control systems. To address this, the traditional CTIs of general information systems are first summarized, and then the existing CTIs designed in conjunction with the characteristics of substation monitoring and control systems are analyzed. Based on this, in response to the challenge of detecting highly concealed security threats, the design and extraction of substation-based CTIs focusing on compliance are anticipated, considering aspects such as the execution of tasks by various business systems in the substation monitoring and control system according to established process rules, and the strong coupling between the primary system status and the communication and alerting of the secondary system. This approach is expected to accurately characterize highly concealed security threats that do not trigger alerts but violate business rules, laying the groundwork for further enhancing security protection capabilities.

Key words: substation monitoring system; cyber threat indicators; highly concealed cyber threat; compliance; anomaly detection

收稿日期:2023-07-30;**修回日期**:2024-03-07
基金项目:国网河南省电力公司科研项目(SGHADK00DWJS2200211)
通信作者:畅广辉(1976—),男,教授级高级工程师,主要从事电力系统自动化研究;E-mail:sw612@126.com

网络安全威胁指标(cyber threat indicators,CTIs)是针对现存或潜在的网络攻击行为,基于情景和应对建议等一些经验循证知识为检测攻击提供决策依据的异常检测指标[1]。基于CTIs进行网络安全防御可及时分析所面临的威胁态势,从而辅助决策和增强安全防御能力。传统的威胁指标采集与识别主要从安全厂商过往的网络威胁攻击数据中提炼,例如:从企业内部网络、终端部署的检测设备或高交互蜜罐中产生的日志数据,也有一大部分威胁情报来源于订阅的安全厂商、行业组织收集的威胁数据等[2]。目前,主要根据CTIs进行入侵威胁检测和安全防护决策。

变电站作为电能传输的关键枢纽,是国家支持型网络攻击的重要对象和网络攻防对抗的重点场所[3-4]。中国电力行业高度重视网络安全防护,根据现行的《电力监控系统安全防护总体方案》(国能安全[2015]36号)的要求,不但以物理隔离的边界安全为基础构建了纵深防护体系,还推广应用了基于可信计算技术的监控终端[5-6],在技术和管理上具备了抵御一般性安全威胁和具有有限资源的有组织攻击的能力。国家支持型攻击的技术水平远超一般对手,采用美国国家安全局(national security agency,NSA)泄露的网络武器库中“永恒之蓝”漏洞传播的WannaCry勒索软件一度肆虐全球[7];基于控制和计算机系统专业知识研制的Stuxnet更突破边界安全防护,渗透侵入物理隔离的核电监控系统,进行隐蔽性攻击并造成严重后果[8-9]。近年来,西北工业大学和武汉地震监测中心都遭到了具有政府背景的网络攻击。因此,当前需要着力应对的正是掌握有丰富资源的国家支持型攻击[10]。

2022年爆发俄乌冲突以来,俄乌双方均出现了大量国家支持型攻击,网络空间对抗活动包括DDoS攻击、钓鱼欺诈、漏洞利用、供应链攻击、恶意数据窃取以及数据擦除攻击等。针对关键基础设施的长期性、高破坏性且有组织的高级可持续威胁(advanced persistent threat,APT)攻击表现尤为显著。从乌克兰方面看,乌克兰政府部门、银行系统和关键基础设施遭遇了持续、系统的网络攻击,多个电信基础设施因为网络攻击出现经常性服务中断;从俄罗斯方面看,俄罗斯在冲突爆发后也遭到全球黑客组织的大规模网络攻击,多个联邦政府网站遭遇供应链攻击,致使克里姆林宫、国家杜马、国防部网站、铁路系统和“今日俄罗斯电视台(Russia Today TV)”、红星电视台(Zvezda)等多家俄罗斯网站都曾暂时瘫痪,俄罗斯不得不作好启用本国互联网系统的准备[11]。关键信息基础设施的安全问题已经打破网络与物理世界的壁垒,构成了严重的现实威胁。与其他身份的攻击发起者相比,国家支持型攻击的特点不仅在于技术水平的提升,更在于攻击目的从一般性破坏或勒索转换为最大化的攻击破坏[10-14],为达成攻击目标往往还会利用目标系统的先验知识进行高隐蔽性攻击,传统的入侵检测等安全手段很难有效防护[15]。为强化生产控制大区内部的安全防护,电力行业在35 kV及以上变电站部署了网络安全监测装置,并将站内各类网络安全告警信息上送至调度主站网络安全管理平台,为开展融合多源数据检测高隐蔽性安全威胁、强化安全边界内部纵深防护奠定了基础[16-17]。近年来,围绕如何充分挖掘利用这一数据资源,实现对高隐蔽性安全威胁的检测开展了大量研究。

网络安全态势感知的特点是融合多源数据,来提高对隐蔽性安全威胁的检测能力,避免误报和漏报[18-19]。但安全态势感知并没有拓展CTIs,还是以网络安全威胁会触发安全告警为前提,采用不同来源融合后的安全告警日志作为指标来融合识别异常[20-21],一旦高隐蔽性安全威胁突破安全防护的基本假设、不触发异常告警,则基于安全日志数据融合的态势感知方法也将失效。

CTIs是准确检测网络攻击的重要基础。变电监控系统所需防护的是国家支持型的高隐蔽性攻击,通用信息系统常用的CTIs难以有效表征此类高隐蔽性攻击,亟待结合变电监控系统的特征提出针对性的CTIs设计方法。本文首先综述通用信息系统的CTIs;然后分析现有网络安全威胁检测与态势感知方法,再利用变电监控系统作为工业控制系统(industrial control system,ICS)在业务流程上具有确定性规则的特点,展望从业务操作合规性出发来提炼CTIs的可行性;最后结合变电操作的具体业务,归纳静态和动态CTIs的提取设计方法。

1 网络安全威胁指标

网络安全研究中CTIs可用来作为判断遭受攻击的指标。对于已知的网络安全威胁,可以用包含恶意文件Hash值、恶意软件特征、恶意IP地址以及网页链接一级域名等作为CTIs[1]。

在通用信息系统中,由于网络环境相对开放,用户行为不确定性较高,故很难用确定性的规则来

判断用户行为异常，只能基于一些原则性的常见CTIs进行大致判断。

1）异常的网络流量。异常的出站流量可能是数据泄露的迹象，而异常端口上的内部请求可能指向使用Netcat等常见黑客工具。

2）异常的DNS请求。例如拼写错误的域名，可能是网络上的恶意软件试图与外部命令和控制服务器（command and control server，C&C）通信的证据。

3）DDoS攻击。分布式拒绝服务攻击通常用于伪装网络上黑客的活动和意图。

4）特权帐户活动异常。特权帐户显示异常行为，如随机提升其他用户帐户或访问其正常工作功能之外的敏感数据，则表明该帐户已泄露。

5）数据库读取量激增。数据库读取量的异常峰值，特别是在异常时间段的流量异常，表明黑客正在访问或泄漏数据。

6）可疑变化。对注册表或系统文件的可疑更改表明系统被恶意软件感染，恶意软件可能被用来为数据泄露创建后门。

7）反复感染恶意软件。删除病毒或其他恶意软件后快速重新感染，可能是rootkit或高级持续威胁的证据。

8）异常通信。内部主机与业务范围之外的国家/地区进行通信，或公共服务器与内部主机通信。这可能表明远程通信标识的数据泄露。

除此以外，通信系统中一般会部署一些安全设备，主机和通信设备中对网络异常行为也会有一些告警，这些也是CTIs的重要构成部分[2]。进行网络安全分析时可以直接根据部分CTIs直接判断是否遭攻击；当无法直接判断时，需要进行多个CTIs的关联和融合来进行判断分析。

2　变电监控系统网络安全威胁检测

传统上变电监控系统依赖于专用通信协议和物理隔离的保护，主要考虑业务功能的实现而极少考虑网络安全问题。在采用IEC 61850协议网络化传输量测值和控制报文的智能化变电站中，伪造量测数据和控制报文均可造成保护与控制系统误动[15]，造成突出的网络安全问题。在变电监控系统网络安全威胁检测上，常用方法主要有基于误用检测、异常检测和安全态势感知3类方法，对应安全威胁的检测机制及存在的不足如表1所示。

表1　变电监控系统网络安全威胁检测方法对比

Table 1　Comparison of cyber threat detection methods for substation monitoring system

分类	检测机制	缺陷
误用检测	在攻击行为模式已知条件下，提炼可标识攻击的特征项，然后基于身份认证、权限管理、数据包是否符合通信规约、通信行为是否违背接入控制和白名单等方式，以确定性的规则识别异常。具有误报率低和检测结果可解释的优势	针对已知类型的攻击提炼总结攻击检测的判断规则，可用规则的数量有限，对掌握行业专业知识、不触发检测规则的对手无效，且不适用于未知安全威胁
异常检测	以网络主体正常通信行为有一定的规律而网络安全威胁与正常行为存在明显差异为前提，通过对网络行为的统计分析或行为特征的匹配辨识来识别安全威胁。具有可检测未知安全威胁的优势	基于智能算法提炼标识异常的特征项、数据融合识别异常，原理上无法避免漏报和误报，缺乏可解释性，难以直接用于安全决策
安全态势感知	本身更接近异常检测，强调对多源信息的关联融合分析，除了可以提高对隐蔽性安全威胁的检测能力外，还可强化对系统自身缺陷等整体安全态势的感知能力	高隐蔽性安全威胁的检测能力在很大程度上取决于选配的安全态势指标

为提高变电监控系统的网络安全防护水平，早期的研究主要从协议层面进行强化设计。IEC 62351对变电监控系统通信的身份认证和数据加密进行了规范要求，可在通信时延允许范围内有效提高安全防护水平[22]。由于变电监控系统按照规约通信[23-26]，通过解析判断通信报文是否符合格式定义，因此其是一种实用的攻击检测方法。但以上方法仅对不掌握通信规约等专业知识的低技术水平攻击有效，而具有较高技术水平的攻击方当利用漏洞获得合法身份后，可提权进行攻击破坏。因为通信规约是开放的标准协议，具有专业知识的攻击方可以像2015年攻击乌克兰电网的Industroyer病毒一样，自动适配不同通信规约，发送伪造的指令进行攻击破坏[27]。

因为BlackEnergy侵入乌克兰变电站后外联进行了恶意软件下载，所以可以利用变电站通信具有

强周期性规律的特点，进行基于流量的异常检测。文献[28]基于监督学习和数理统计学习方法，提出了基于FARIMA回归理论的变电监控系统流量阈值模型与状态评估算法，可以识别网络安全威胁引发的异常高流量。在此基础上，还可利用变电监控系统通信的时、频域混合特征，结合FARIMA流量模型和小波包分析方法提取电力信息流量时、频域特征，识别异常流量。此类方法可有效检出流量异常模式的攻击，但定向设计的高隐蔽性攻击为隐匿行踪，可能像Stuxnet一样在先验知识的支持下，发起没有明显流量异常的攻击[29]，此时很难基于流量异常识别安全威胁。

近年来，新一代人工智能(artificial intelligence，AI)技术取得了突飞猛进的发展，基于AI的网络攻击和防御成为网络安全的新方向。美国国防高级研究计划局(defense advanced research projects agency，DARPA)引领基于AI的网络攻防对抗先河，发展了基于AI的漏洞挖掘和自主网络攻击等技术[30]。随着网络攻击行为的不断发展，人工方式获取异常行为特征的代价越来越高甚至不可行，采用机器学习可以从网络数据中自动提取异常行为特征和产生检测规则，识别未知异常行为。因此，利用具有长远发展潜力的AI技术来强化电力系统网络安全防护是重要的发展方向[30-33]。

传统上计算机领域主要采用入侵检测进行安全威胁检测[12]。由于所用数据来源单一，难以准确识别异常，往往频繁发出无效告警，存在大量误报、漏报，因此，一般仅用作事后分析而无法用作安全决策。目前，各大电网公司和发电集团普遍配置了网络安全监测装置，可以将厂站侧安全、主机及网络设备的各类安全告警信息上送至调度主站网络安全管理平台。当恶意软件渗透侵入变电站自动化系统时，可能在安全、网络及主机设备的日志告警数据中均有所反应。单独采用一种设备进行入侵检测和行为分析，难以提高判断准确率；融合安全、网络及主机设备的多元数据，则有可能形成对安全态势的整体判断，发现不伴随有显著异常流量的渗透攻击行为[19]。文献[34-35]抓住攻击方破坏大量变电站的同时造成大停电的特点，提出了融合多变电站告警事件识别安全威胁防护方法；文献[27,36]也利用敌对攻击同步攻击多个变电站的特点，提出了利用无站间通信同步机制的高隐蔽性安全威胁防护方法。值得注意的是，变电站安全态势感知系统采集的主要是告警信息，从机理上就难以有效检出供应链攻击等具有合法身份、不触发高危告警的高隐蔽性攻击。

网络安全态势感知的精髓是利用具有关联性的信息来提高对隐蔽性威胁的检测能力。在变电监控系统中，信息和物理系统对应的一次与二次系统的状态同样具有关联性，也可能为网络安全态势感知提供必要的信息。文献[37]围绕电力信息物理系统中信息和物理系统的耦合关系，探索了其间的交互特性。针对电网遭到网络攻击后不能及时确定安全威胁原因、难以及时恢复安全运行的问题，文献[38-39]提出可在检测到电网故障异常时匹配识别信息系统的异常，可在电网遭攻击之后确认和排查网络攻击引起的电网安全问题，有利于电网在攻击后恢复正常运行。

随着电力信息物理系统网络安全防护的深入，为了解决常规CTIs难以满足电力监控系统高可靠和低误报的安全威胁检测难题，研究人员结合电压稳定监测[39]、配电自动化[40-41]等应用场景提出了一些个性化的CTIs，为强化电力监控系统的信息安全防护拓展了新的思路。

3 变电监控系统的操作合规性分析

通用信息系统中网络环境开放，用户行为模型多样、不确定性强而难以预测，很难将异常的用户行为和正常行为区分开，是网络安全威胁检测困难的重要原因[42]。变电监控系统处于封闭网络环境中，是一种典型的ICS，其体系架构和工作机制具有特殊性，接入设备按确定的业务逻辑和业务流程运行，与一般信息系统的工作机制存在显著差异[43]。变电监控系统差异对比如表2所示。

表2 变电监控系统与一般信息系统通信特性差异对比

Table 2 Comparison of communication characteristics between substation monitoring system and general information system

分类	一般信息系统	变电监控系统等ICS
通信行为	按协议通信，对通信行为无明显约束	通信行为清晰明确。业务流量分为周期性流量和事件触发的突发流量。通信的源和目的明确固定
业务流程	一般没有确定性的业务流程	业务操作一般都有明确固定的流程规范
接入管控	一般无接入管控，接入网络即可通信	接入管控严格，进行接入设置后才能访问网络

1)通信行为清晰明确。变电监控系统为封闭系统，其中业务流量主要分为定期发送的周期性和

事件触发的突发流量。周期性报送的量测数据通信的源和目的都很明确固定，而事件触发的通信也会按照确定的响应规则发生在设定的对象之间。

2）业务流程固定。变电站执行特定的业务有明确固定的业务流程，如调度主站为保障电网的无功平衡和电能质量，每天都会定时按固定的流程遥控无功补偿电容器投退，投切过程前、后主站与监控系统以及监控系统与电容器控制屏之间的通信会有强时序关联性。

3）接入管控严格，接入终端固定。变电监控系统为满足实时性要求，大量采用白名单机制进行安全管控。接入的所有终端均需进行接入设置后才能访问网络，其所能访问的也只是白名单中的IP地址和端口。

除以上差异外，ICS中信息系统服务和作用于物理系统，物理设备的运行状态与信息系统的工况之间存在较强的耦合特性。文献[44]提出可以融合信息系统的信息流和物理系统的状态流，通过检测操作时序和次序的合理性，利用设备状态的改变识别异常操作来检测网络安全威胁。变电监控系统同样具有信息系统与物理系统状态强耦合的特性。文献[45]利用这一特性，对标识信息系统行为的监控告警等信息进行向量化建模，再融合知识库和深度学习来诊断识别对应物理电网的异常事件。实际上，早期的电网故障诊断也是应用信息系统侧的数据融合来诊断实际电网中的异常位置[46]。

除了信息和物理系统的耦合特性以外，电力监控系统还有明确的业务流程规范性；同时，除了对突发事件的响应会有明确的规范要求外，对电力系统的业务操作也有相应的规范步骤。通过检测这种业务流程规范的合规性，同样可以进行异常检测、实现电力监控系统高隐蔽安全威胁检测。类似方法在学术研究和工程应用中已有先例。跳闸攻击的目的仅在于跳开尽可能多的断路器，以破坏电网结构造成大停电，而正常的电网倒闸操作需要考虑对相关线路的影响，避免引起其他线路过负荷。文献[47]提出了对电力调度操作指令的安全校核方法，可以对接收到的控制指令进行安全性校核，以避免执行不合规的异常指令；文献[48]也利用业务逻辑提出了电力业务报文攻击识别方法，该方法将误用检测与异常检测相结合，通过业务逻辑黑白名单的模式匹配，实现对黑白名单中的当前业务状态的误用检测；然后，对不在黑白名单之列的状态序列进行相似度匹配，并将电网时间风险与业务重要性融入基于黑白名单的相似度匹配异常检测方法之中，对相似度进行修正。

基于合规性的异常检测与基于协议的异常检测均属于误用检测，具有确定性程度高、误报率低的优势，但两者又存在一些差异。基于协议的异常检测，所依据的协议是开放性有确定文本的，敌对攻击方按照协议设计定向攻击即可令异常检测失效。合规性检测涉及具体的业务流程，并没有明确发布的统一文本定义，甚至可能在不同省份或版本上因为习惯不同还有细微差异，攻击方难以针对性地进行隐匿设计。因此，可以提炼变电监控系统的业务规范，归纳形成可标识异常的CTIs，为准确识别高隐蔽性安全威胁奠定基础。

变电监控系统中异常检测误报率、漏报率和检测率等是评价异常检测效果的核心指标。由于变电监控系统具有高实时性和无法暂停更新等特点，故其对网络安全威胁检测的误报率指标更敏感。变电站要求按流程操作，采用合规性作为异常检测指标能有效避免误报，更适合变电监控系统的特点。

4　基于合规性的安全威胁检测指标设计

具有专业知识的敌对组织编制的恶意软件，会利用合法身份不违反通信规约地进行高隐蔽性的攻击。既有变电站入侵检测和网络安全态势感知系统采集的是主机、网络及安全设备的安全告警信息。当高隐蔽性攻击不引起告警时，以此为基础的网络安全威胁检测无法检出高隐蔽性安全威胁。

变电站二次系统实现一次系统的监视与控制，网络通信行为具有明确的规律性，并与一次系统运行状态具有强关联性。从合规性角度出发，可以利用一、二次系统在各种运行场景下的耦合特性、变电站业务场景转换时的操作流程以及安全敏感行为的合规性等方面来提炼和设计CTIs。

4.1　考虑业务流程的一、二次系统状态耦合 CTIs

变电站一次系统随电网运行方式和检修需要调整运行状态。在各种运行状态下，一、二次系统之间会有不同的耦合特性，基于合规性的变电监控系统网络安全威胁指标如图1所示，利用耦合特性可以从以下5个方面提炼CTIs。

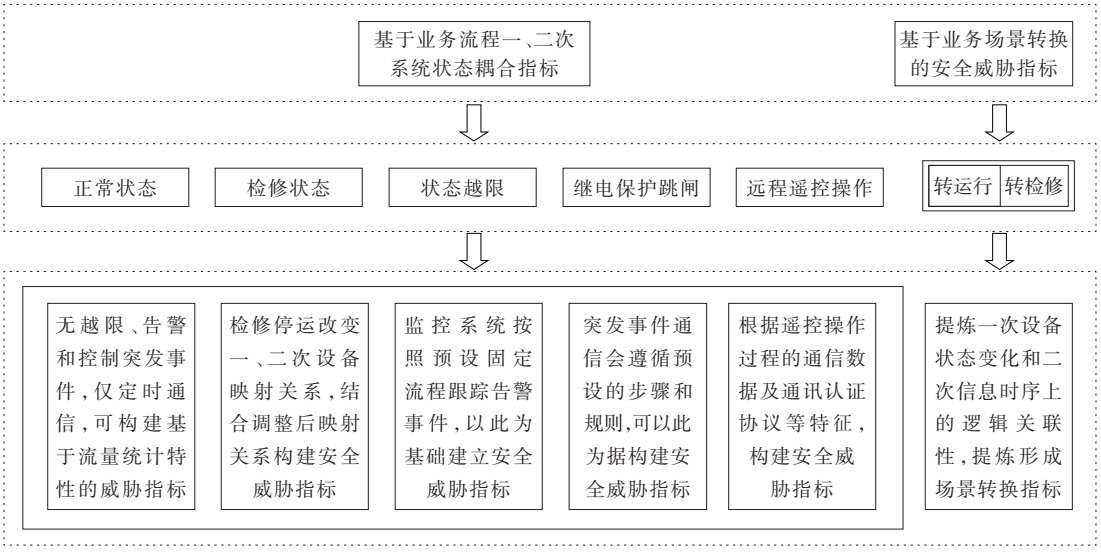

图1 基于合规性的变电监控系统网络安全威胁指标

Figure 1 Comparison of communication characteristics between substation monitoring system and general information system

1）正常运行。

变电站内主要分为周期性的高频报文和突发事件触发的GOOSE报文。正常运行时变电站内主要是小数据量、高频率的SV报文和IED终端心跳报文。没有突发事件也就没有对应的突发报文，可以将一次系统没有状态量越限等触发突发事件的状态与二次系统没有突发事件的流量匹配，构成CTIs。

2）不同检修模式运行。

除正常运行外变电站也会阶段性运行于各种检修模式下。此时，系统只是与正常运行时的运行方式有所变化，在变电站配置描述文件所描述的一次设备和二次通信数据的耦合状态匹配上有所调整，并没有发生变压器超温、电压越限等突发事件及对应的事件响应通信。可在正常运行的CTIs基础上，增加对检修停运设备与二次系统的匹配筛查，设计检修状态下的CTIs。

3）状态量越限。

变压器油温越限、瓦斯告警及母线电压越限是变电监控系统中常见的异常告警，将会在二次系统触发突发事件及对应响应通信。当油温越限时，主变监视系统会同时向事件顺序记录系统（sequence of event，SoE）、站控系统及调度中心报送状态告警，站控系统和调度中心在接到告警信号后将按预设流程发出状态查询并确认信息。站控系统和调度中心按预先确定的固定流程进行告警事件的跟踪监视，通过检测一次系统状态、二次系统告警以及随后突发事件响应通信行为的匹配程度，针对性设计状态量越限的CTIs。

4）继电保护跳闸。

当电力设备故障导致继电保护装置动作跳闸时，对应的电气量会有显著波动，跳闸的继电保护装置会输出动作指令给对应的断路器，同步向变电站SoE报送状态变化。此外，关联的继电保护即便没有输出动作跳闸信号，也会向SoE发送保护启动信号。此时一次系统电气量的波动、二次系统中特定GOOSE报文的流向和往复以及站控层、过程层和间隔层的突发事件通信行为都遵循设定的规则。应用这些强关联的信息可以设计表征继电保护跳闸事件的CTIs。

5）远程遥控操作。

现有变电站多为无人值守，大量依赖远程遥控完成日常的投退电容器和程序化控制等操作。此类操作经过RTU遥控端口通信，根据已知遥控操作过程中对应的通信数据包的源IP地址、目的IP地址、源端口号、目的端口号、协议类型、时间戳、包长等数据包特征，以及数据通信进行遥控过程的握手和认证协议等，形成确定的流程规则。根据是否违反操作规范，可定义远程遥控操作通信响应的CTIs。

4.2 基于业务场景转换的CTIs

变电站运行场景整体可分为正常运行和检修模式2类。从运行转检修和从检修转运行的2种模式切换过程中，变电站需要按照技术规程设定的标准流程进行操作。在一次设备转检修和转运行时，变电监控系统依据操作对象和目的的不同按照正确的时序进行特定作业，会在一、二次系统状态变

化上表现出确定的规律。根据一次设备运行状态和二次采集信息时序上的逻辑关联性,分析操作过程中可以总结提炼形成业务场景转换的规则。以变电站主变运行转检修和检修转运行为例,所需的操作步骤如表3所示。

表3　变电站主变操作时序

Table 3　Operation sequence of main transformer in substation

序号	主变运行转检修操作内容
1	10 kV#1电容器522断路器由运行转热备用
2	10 kV523线523断路器由运行转热备用
3	10 kV524线524断路器由运行转热备用
4	10 kV#1所用变521断路器由运行转热备用
5	#1主变低压侧511断路器由运行转热备用
6	合上#1主变高压侧111-9中性点接地刀闸
7	#1主变高压侧111断路器由运行转热备用
8	#1主变低压侧511断路器由热备用转冷备用
9	#1主变高压侧111断路器由热备用转冷备用
10	合上#1主变高压侧1114BD接地刀闸
11	合上#1主变低压侧511BD接地刀闸
序号	**主变检修转运行操作内容**
1	拉开#2主变高压侧1124BD接地刀闸
2	拉开#2主变低压侧5124BD接地刀闸
3	投入#2主变后备保护跳低压侧分段开关压板
4	#2主变高压侧112断路器由冷备用转热备用
5	#2主变低压侧512断路器由冷备用转热备用
6	#2主变高压侧112断路器由热备用转运行
7	拉开#2主变高压侧112-9中性点接地刀闸
8	110 kV分段101断路器由热备用转运行
9	#2主变低压侧512断路器由热备用转运行
10	10 kV分段501断路器由运行转热备用
11	投入10 kV分段501断路器分段备自投
12	110 kV分段101断路器由运行转热备用

由表3可见,主变投退过程中主变断路器、电容器断路器和刀闸的动作时序按技术规范的要求具有确定的时序依赖特性。同样,线路、母线和断路器等设备转检修和转运行时都会有对应的时序特征。可以分析各种业务场景转换的时序逻辑关系,以该先验知识为基础,提出基于领域知识的CTIs,为准确感知异常安全态势提供可靠判据。

一次设备运行状态变化时二次系统也会对应调整。一次设备检修时二次设备侧相关保护退出,自动化系统正常运行;涉及扩建和出线改变时会开展二次系统调试,包括变电站之间联调、遥控开关变位、保护跳闸测试以及状态量信息核对等。二次设备检修时周期性的报文流量会出现部分中断,检修完成后会流量恢复;在开展设备调试工作时,如遥控开关变位、保护跳闸测试以及状态量信息核对等,报文流量会明显增加。结合具体流程,均可设计标识合规性的安全威胁检测指标。

5　结语

为提高变电监控系统高隐蔽性安全威胁检测能力,本文围绕一、二次信息融合的变电站合规性CTIs展开研究。

1)分析了变电监控系统中既有各类网络安全防护技术的特点与存在的不足,指出变电站安全态势感知系统的数据源为安全、网络及主机设备的安全告警信息,如高隐蔽性攻击不触发告警,安全态势感知系统也将无从检出安全威胁。

2)分析指出变电监控系统具有环境封闭、一次与二次系统运行状态之间具有强耦合性且业务操作有确定流程规范的特点,提出可以利用这些耦合特性和流程合规性设计CTIs。

3)从考虑业务流程的一、二次系统状态耦合、业务场景转换规则的角度分析了可以提炼设计的CTIs。所提指标可从另一层面刻画不触发安全告警的高隐蔽性安全威胁,有助于提高对高隐蔽性安全威胁的感知能力。

电力监控系统和一般信息系统在系统特性和所需防护的网络攻防对抗对手上均存在显著差异,从系统和攻击的特征出发,提炼可准确刻画异常的CTIs是做好变电监控系统网络安全威胁检测的重要基础。本文抛砖引玉,从合规性角度出发展望了设计CTIs的可能方式。未来一方面需要根据本文所提方法结合实际监测数据建立和完善CTIs指标,研究适用的异常评估方法;另一方面还要根据其他CTIs设计方法,为电力系统网络安全防护做好技术支撑。

参考文献:

[1] UMARA N, ZAHID A, TEHMINA A, et al. A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise[J]. Future Generation Computer Systems, 2019, 96:227-242.

[2] 崔琳,杨黎斌,何清林,等.基于开源信息平台的威胁情报挖掘综述[J].信息安全学报,2022,7(1):1-26.
CUI Lin, YANG Libin, HE Qinglin, et al. Survey of cyber

threat intelligence mining based on open source information platform[J].Journal of Cyber Security,2022,7(1):1-26.

[3] 杨安,孙利民,王小山,等.工业控制系统入侵检测技术综述[J].计算机研究与发展,2016,53(9):2039-2054.
YANG An,SUN Limin,WANG Xiaoshan,et al.Intrusion detection techniques for industrial control systems[J].Journal of Computer Research and Development,2016,53(9):2039-2054.

[4] 李田,苏盛,杨洪明,等.电力信息物理系统的攻击行为与安全防护[J].电力系统自动化,2017,41(22):162-167.
LI Tian,SU Sheng,YANG Hongming,et al.Attacks and cyber security defense in cyber-physical power system[J].Automation of Electric Power Systems,2017,41(22):162-167.

[5] 童晓阳.基于可信计算的广域保护与变电站通信安全防御策略[J].电力系统自动化,2011,35(20):53-58.
TONG Xiaoyang.Proactive defense strategies for wide-area protection and substation communication based on trusted computing[J]. Automation of Electric Power Systems,2011,35(20):53-58.

[6] 于杨,姚浩,习伟,等.具有主动免疫能力的电力终端内嵌入式组件解决方案[J].南方电网技术,2020,14(1):65-73.
YU Yang,YAO Hao,XI Wei,et al.Solution scheme of embedded component with active immunity for electric power terminals[J].Southern Power System Technology,2020,14(1):65-73.

[7] 叶夏明,文福拴,尚金成,等.电力系统中信息物理安全风险传播机制[J].电网技术,2015,39(11):3072-3079.
YE Xiaming,WEN Fushuan,SHANG Jincheng,et al.Propagation mechanism of cyber physical security risks in power systems[J].Power System Technology,2015,39(11):3072-3079.

[8] 彭勇,江常青,向憧,等.关键基础设施信息物理攻击建模和影响评价[J].清华大学学报(自然科学版),2013,53(12):1653-1663.
PENG Yong,JIANG Changqing,XIANG Chong,et al.Cyber-physical attack modeling and impact on critical infrastructure.Journal of Tsinghua University(Science and Technology),2013,53(12):1653-1663.

[9] 彭勇,江常青,谢丰,等.工业控制系统信息安全研究进展[J].清华大学学报(自然科学版),2012,52(10):1396-1408.
PENG Yong,JIANG Changqing,XIE Feng,et al.Industrial control system cybersecurity research[J].Journal of Tsinghua University(Science and Technology),2012,52(10):1396-1408.

[10] 单瑞卿,盛阳,苏盛,等.考虑攻击方身份的电力监控系统网络安全风险分析[J].电力科学与技术学报,2022,37(5):3-16.
SHAN Ruiqing,SHENG Yang,SU Sheng,et al.Risk analysis of power system cyber security considering identity of malicious adversaries.Journal of Electric Power Science and Technology,2022,37(5):3-16.

[11] 郎平.从俄乌冲突看网络空间武器化及其影响[EB/OL].http://iwep.cssn.cn/xscg/xscg_sp/202208/t20220802_5445851.shtml,2022-08-02.

[12] 苏盛,吴长江,马钧,等.基于攻击方视角的电力CPS网络攻击模式分析[J].电网技术,2014,38(11):3115-3120.
SU Sheng,WU Changjiang,MA Jun,et al.Analysis of power CPS network attack mode based on the attacker's perspective[J].Power System Technology,2014,38(11):3115-3120.

[13] 肖鹏,王柯强,黄振林.基于IABC和聚类优化RBF神经网络的电力信息网络安全态势评估[J].智慧电力,2022,50(6):100-106.
XIAO Peng,WANG Keqiang,HUANG Zhenlin.Security situation assessment of power information network based on IABC & clustering optimized RBF neural network[J].Smart Power,2022,50(6):100-106.

[14] 杨杰,郭逸豪,郭创新,等.考虑模型与数据双重驱动的电力信息物理系统动态安全防护研究综述[J].电力系统保护与控制,2022,50(7):176-187.
YANG Jie,GUO Yihao,GUO Xinhua,et al.A review of dynamic security protection on a cyber physical power system considering model and data driving[J].Power System Protection and Control,2022,50(7):176-187.

[15] 王宇飞,赵婷,李韶瑜,等.采用改进最小闭包球向量机的电力信息网络入侵检测方法[J].电网技术,2013,37(9):2675-2680.
WANG Yufei,ZHAO Ting,Ll Shaoyu,et al.An intrusion detection method for electric power information network based on improved minimum enclosing ball vector machine[J].Power System Technology,2013,37(9):2675-2680.

[16] 刘权莹,李俊娥,倪明,等.电网信息物理系统态势感知:现状与研究构想[J].电力系统自动化,2019,43(19):9-21.
LIU Quanying,LI Jun'e,NI Ming,et al.Situation awareness of grid cyber-physical system:current situation and research ideas[J].Automation of Electric Power Systems,2019,43(19):9-21.

[17] 于群,李浩,屈玉清.基于深度神经网络和内外部因素的大电网安全态势感知研究[J].电测与仪表,2022,59(2):16-23.
YU Qun,LI Hao,QU Yuqing.Research on security situation awareness of large power grid based on deep neural network and internal and external factors[J].Electrical Measurement & Instrumentation,2022,59(2):16-23.

[18] 龚俭,臧小东,苏琪,等.网络安全态势感知综述[J].软件学报,2017,28(4):1010-1026.

GONG Jian, ZANG Xiaodong, SU Qi, et al. Survey of network security situation awareness[J]. Journal of Software,2017,28(4):1010-1026.

[19] 刘效武,王慧强,吕宏武,等.网络安全态势认知融合感控模型[J].软件学报,2016,27(8):2099-2114.
LIU Xiaowu,WANG Huiqiang,LÜ Hongwu,et al.Fusion-based cognitive awareness-control model for network security situation[J]. Journal of Software, 2016, 27(8): 2099-2114.

[20] 钱斌,蔡梓文,肖勇,等.基于模糊推理的计量自动化系统网络安全态势感知[J].南方电网技术,2019,13(2):51-58.
QIAN Bin,CAI Ziwen,XIAO Yong,et al.Fuzzy Inference based cyber security situation awareness of advanced metering system[J].Southern Power System Technology, 2019,13(2):51-58.

[21] BASU C, PADMANABAN M, GUILLON S, et al. Situational awareness for the electrical power grid[J]. IBM Journal of Research & Development, 2016, 60(1): 1-10.

[22] 陶士全,王自成,李广华,等.基于 IEC 62351 的安全通信对站控层通信性能的影响[J].电力系统自动化,2018,42(23):155-158.
TAO Shiquan,WANG Zicheng,LI Guanghua,et al.Effect of IEC 62351 based security communication on communication performance of station level[J]. Automation of Electric Power Systems, 2018, 42(23): 155-158.

[23] 胡国,梅德冬.智能变电站采样值报文安全分析与实现[J].中国电机工程学报,2017,37(8):2215-2222.
HU Guo, MEI Dedong. Research and application on network security of SMV in smart substation[J]. Proceeding of CSEE, 2017, 37(8):2215-2222.

[24] 席禹,邹俊雄,蔡泽祥,等.基于报文识别与流量管控的智能变电站保护控制信息安全防护方法[J].电网技术,2017,41(2):624-629.
XI Yu, ZOU Junxiong, CAI Zexiang, et al. Information security protection method for smart substation communication network based on message identification and flow control.Power System Technology,2017,41(2):624-629.

[25] 王文博,刘绚,张博,等.基于协议特征的电力工控网络流量异常行为检测方法[J].电力系统自动化,2023,47(2):137-145.
WANG Wenbo, LIU Xuan, ZHANG Bo, et al. Protocol characteristics based detection method for abnormal flow behavior in electric power industrial control network[J]. Automation of Electric Power Systems,2023, 47(2):137-145.

[26] 王文博,刘绚,张博,等.基于协议特征的电力工控网络流量异常行为检测方法[J].电力系统自动化,2023,47(2):137-145.
WANG Wenbo, LIU Xuan, ZHANG Bo, et al. Protocol characteristics based detection method for abnormal flow behavior in electric power industrial control network[J].Automation of Electric Power Systems,2023, 47(2):137-145.

[27] 王坤,苏盛,左剑,等.变电站自动化系统扰动同步协同攻击及防护分析[J].电网技术,2021,45(11):4452-4461.
WANG Kun, SU Sheng, ZUO Jian, et al. Synchronous disturbance coordinated attack and analysis of defense for substation automation system. Power System technology,2021,45(11):4452-4461.

[28] 郝唯杰,杨强,李炜.基于 FARIMA 模型的智能变电站通信流量异常分析[J].电力系统自动化,2019,43(1):158-167.
HAO Weijie, YANG Qiang, LI Wei. FARIMA model based analysis of communication traffic anomaly in smart substation[J]. Automation of Electric Power Systems,2019,43(1):158-167.

[29] 杨挺,侯昱丞,赵黎媛,等.基于时—频域混合特征的变电站通信网异常流量检测方法[J].电力系统自动化,2020,44(16):79-86.
YANG Ting, HOU Yucheng, ZHAO Liyuan, et al. Abnormal traffic detection method of substation communication network based on time-frequency domain mixed features[J].Automation of Electric Power Systems,2020,44(16):79-86.

[30] Defense Advanced Research Projects Agency.Reimaging the future of artificial intelligence for national security [EB/OL].https://www.darpa.mil/work-with-us/ai-forward, 2024-07-07.

[31] 李伟,霍雪松,张明,等.基于残差全连接神经网络的电力监控系统异常行为检测方法[J].东南大学学报(自然科学版),2020,50(6):1062-1068.
LI Wei, HUO Xuesong, ZHANG Ming, et al. Abnormal behavior detection method for power monitoring system based on fully connected residual neural network[J]. Journal of Southease University (Natural Science Edition),2020,50(6):1062-1068.

[32] 王蓓,韩俊飞,李勇,等.基于智能监控平台的电网安全预警技术研究[J].电网与清洁能源,2023,39(6):33-38.
WANG Bei, HAN Junfei, LI Yong, et al. Research on power grid security early warning technology based on intelligent monitoring platform[J]. Power System and Clean Energy,2023,39(6):33-38.

[33] TEN C, HONG J, LIU C. Anomaly detection for cybersecurity of the substations[J]. IEEE Transations Smart Grid,2011,2(4):865-873.

[34] 王坤,苏盛,赵奕,等.变电站自动化系统时间同步协同攻击的检测与防护方法[J].电力系统自动化,2021,45(6):231-239.

WANG Kun, SU Sheng, ZHAO Yi et al. Detection and protection method for time-synchronized coordinated cyber-attack on substation automation system[J]. Automation of Electric Power Systems, 2021, 45(6): 231-239.

[35] 夏云舒,王勇,周林,等.基于改进生成对抗网络的虚假数据注入攻击检测方法[J].电力建设,2022,43(3):58-65.
XIA Yunshu, WANG Yong, ZHOU Lin, et al. False data injection attack detection method based on improved generative adversarial network[J]. Electric Power Construction,2022,43(3):58-65.

[36] 高昆仑,王宇飞,赵婷.电网信息物理系统运行中信息—物理交互机理探索[J].电网技术,2018,42(10):3101-3109.
GAO Kunlun, WANG Yufei, ZHAO Ting. Exploration of cyber-physical interaction mechanism in power grid cyber-physical systems operation[J]. Power System Technology,2018,42(10):3101-3109.

[37] 刘权莹.考虑网络攻击的有源配电网运行态势感知研究[D].武汉:武汉大学,2019.
LIU Quanying. Situation awareness of active distribution network considering cyber-attack[D]. Wuhan: Wuhan University,2019.

[38] 周睿.网络攻击下电力CPS态势分析和网络异常辨识[D].南京:南京邮电大学,2021.
ZHOU Rui. Power CPS situation analysis and network anomaly identification under cyber attack[D]. Nanjing: Nanjing University of Posts and Telecommunications, 2021.

[39] GHAFOURI M,AU M,KASSOUF M,et al.Detection and mitigation of cyber attacks on voltage stability monitoring of smart grids[J]. IEEE Transactions on Smart Grid,2020,11(6):5227-5238.

[40] GANJKHANI M, GILANIFAR M, GIRALDO J, et al. Integrated cyber and physical anomaly location and classification in power distribution systems[J]. IEEE Transactions on Industrial Informatics,2021,17(10):7040-7049.

[41] ROY P, BHATTACHARJEE S, ABEDZADEH S, et al. Noise resilient learning for attack detection in smart grid PMU infrastructure[J].IEEE Transactions on Dependable and Secure Computing,2024,21(2):618-635.

[42] 陈清清,苏盛,畅广辉,等.电力信息物理系统内部威胁研究综述[J].南方电网技术,2022,16(6):1-13.
CHEN Qingqing, SU Sheng, CHANG Guanghui, et al. Review on the research of insider threat of cyber physical power system[J]. Southern Power System Technology,2022,16(6):1-13.

[43] 赖英旭,刘增辉,蔡晓田,等.工业控制系统入侵检测研究综述[J].通信学报,2017,38(2):143-156.
LAI Yingxu, LIU Zenghui, CAI Xiaotian, et al. Research on intrusion detection of industrial control system[J]. Journal on Communications,2017,38(2):143-156.

[44] 杨安,胡堰,周亮,等.基于信息流和状态流融合的工控系统异常检测算法[J].计算机研究与发展,2018,55(11):2532-2542.
YANG An, HU Yan, ZHOU Liang, et al. An industrial control system anomaly detection algorithm fusion by information flow and state flow[J]. Journal of Computer Research and Development,2018,55(11):2532-2542.

[45] 孙国强,沈培锋,赵扬,等.融合知识库和深度学习的电网监控告警事件智能识别[J].电力自动化设备,2020,40(4):40-47.
SUN Guoqiang, SHEN Peifeng, ZHAO Yang, et al. Intelligent recognition of power grid monitoring alarm event combining knowledge base and deep learning[J]. Electric Power Automation Equipment,2020,40(4):40-47.

[46] 文福拴,韩祯祥.基于模拟进化理论的电力系统的故障诊断[J].电工技术学报,1994,9(2):57-63.
WEN Fushuan, HAN Zhenxiang. Fault section estimation in power systems using simulated evolution[J]. Transactions of China Electrotechnical Society, 1994, 9(2):57-63.

[47] 刘绚,严康,于宗超.电力调度操作指令安全校验方法及系统[P].中国专利:CN202011590065.8,2020-12-29.
LIU Xun, YAN Kang, YU Zongchao. Safety check method and system of power dispatching operation instruction[P]. Chinese Patent: CN202011590065.8, 2020-12-29.

[48] 王海翔,朱朝阳,王宇,等.基于业务逻辑的电力业务报文攻击识别方法[J].电力自动化设备,2020,40(8):217-226.
WANG Haixiang, ZHU Chaoyang, WANG Yu, et al. Identification method of power service packet attacks based on service logic[J]. Electric Power Automation Equipment,2020,40(8):217-226.