新型电力系统主动防御技术体系白皮书（2023）

WHITE PAPER: SECURITY OF NEW POWER SYSTEM

2023.09

主编

程鹏、张镇勇、邓瑞龙

编写组成员

宋俊杰、王禀东、杨智博、邵宽、何涂哲秋、徐子东、陈光佳、朱俊彦、孟捷、赵成成、王鑫、方崇荣、汪京培

顾问专家

苏杨、张格、张涛、刘苇、岳东、周纯杰、贾庆山、谢永芳、陈阿莲、袁捷、王皓然、文杰

主编单位

浙江大学、贵州大学

指导单位

中国自动化学会、中国科学技术协会、中国南方电网、CICS-CERT 国家工信安全中心、国家电网全球能源互联网研究院、南瑞集团有限公司、南京邮电大学、华中科技大学、清华大学、山东大学、中南大学、贵州电网有限责任公司、贵州航天云网科技有限公司、中国自动化学会工控系统信息安全专业委员会

支持项目

科技部重点研发课题《工控系统安全主动防御机制及体系研究》，项目编号：2018YFB0803501；中国科协决策咨询项目《工业控制系统安全国家战略研究》，项目编号：20220615ZZ08010017；国家自然科学基金重大项目课题《面向新型电力系统开放互联业务的主动安全适配增强方法》，项目编号：62293503；国家自然科学基金重点项目《面向智能电网的信息物理安全理论及主动防御技术》，项目编号：61833015

前 言

工业 4.0 正在加速推进电力系统信息化进程，信息物理融合成为未来电力系统发展的典型特征。电力系统数字化转型和智能化发展，信息技术与电力系统物理设备紧密结合，构成了信息物理融合的新型电力系统。新型电力系统是以最大化消纳新能源为主要任务，以坚强智能电网为枢纽平台，以源网荷储互动与多能互补为支撑，具有清洁低碳、安全可控、灵活高效、智能友好、开放互动基本特征的电力系统[1]。然而，信息物理深度融合也为新型电力系统安全带来了风险。信息物理融合使得电力系统从传统孤立的闭环系统逐渐过渡到与外部网络相连接的开放系统。网络安全风险在信息空间中产生，并可以通过信息和物理之间的连接传播到物理空间。网络攻击、恶意软件、数据篡改等来自网络空间的各种安全威胁可能导致电力系统运行中断、设备损坏甚至引发重大事故。

近年来，针对电力系统的网络攻击屡见不鲜，说明电力行业面临的网络安全威胁迫在眉睫。2015 年，乌克兰电力公司遭到 Black Energy 病毒攻击，攻击者通过控制上位机实现远程控制变电站，导致乌克兰东部地区大面积停电[2]；2019 年，印度泰米尔纳德邦的核电站内网感染恶意软件，导致一座核反应堆关闭[3]；2020 年，委内瑞拉国家电网 765 干线遭攻击，造成全国大面积停电[4]；2020 年，巴西电力公司遭 Sodinokibi 勒索软件攻击，黑客勒索赎金高达 1400 万美元[5]。2019 年 5 月，国家互联网应急中心发现，全国共有 139 个水电监控管理系统暴露在互联网上，其分布于 25 省市，其中超过 47%的系统存在明显的安全隐患[6]。

2016 年 4 月，习近平总书记在网络安全和信息化工作座谈会上指出：“要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方

位感知网络安全态势，增强网络安全防御能力和威慑能力。”[7]为保障新型电力系统安全稳定运行，我国相继出台法律法规以保护电力网络基础设施和信息安全，制定行业标准和技术规范以指导电力企业落实网络安全措施。相关部门发布了《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国电力安全法》《信息安全等级保护管理方法》《关键信息基础设施保护条例》《电力行业信息系统安全基本要求》《电力行业信息系统等级保护定级工作指导意见》《电力行业监控系统安全防护规定》《电力设备安全技术规程》、GB 17859-1999《计算及信息系统安全保护等级划分准则》、DL/T 1234-2013《电力系统安全稳定计算技术规范》等相关文件。

在新型电力系统加速智能化的背景下，关注新型电力系统安全防护问题显得尤为重要。针对已知的电力系统风险，新型电力系统根据多年的运行经验积累建立了一套防护体系，主要包括面向物理系统和信息系统的防护。然而，由于攻防信息不对称性、认知逻辑缺陷、防护方案与电力系统可用性需求冲突等问题，现有防御技术体系难以为新型电力系统提供全面有效的深度保护。为解决现有防御技术体系的不足，迫切需要研究基于主动防御方法与技术的新型防御技术体系。主动防御方法与技术包括拟态防御、可信防护、内生安全等，具备动态可靠、适配性强、多维防御的特点，被认为是解决新型电力系统安全问题的潜在方案，协调识别、保护、检测、响应等多个环节，实现新型电力系统全生命周期一体化的主动协同安全防御。

本白皮书总结新型电力系统中存在的已知和未知威胁，结合新型电力系统的安全防护要求，设计了“识别(Identification)-保护(Protection)-检测(Detection)-响应(Response)(IPDR)”一体化的新型电力系统主动安全防御技术体系，提出一套

新型电力系统的主动防御参考模型，持续提升新型电力系统应对各类安全威胁的防御能力。

本白皮书旨在为新型电力系统安全领域的研究和探索做出贡献，推进新型电力系统安全技术的发展。为新型电力系统安全领域的研究者、从业人员和相关利益方提供指导和借鉴，促进知识的共享和交流。同时，呼吁政府、企业和研究机构加强合作，共同推进新型电力系统安全技术的发展和标准制定，为智慧能源时代的安全构建坚实基础。

目录

01

新型电力系统及其网络架构

1.1 新型电力系统背景

2021 年 3 月 15 日，习近平总书记在中央财经委员会第九次会议上对能源电力发展作出了系统阐述，首次提出构建新型电力系统。新型电力系统是以确保能源电力安全为基本前提，以满足经济社会高质量发展的电力需求为首要目标，以高比例新能源供给消纳体系建设为主线任务，以源网荷储多向协同、灵活互动为坚强支撑，以坚强、智能、柔性电网为枢纽平台，以技术创新和体制机制创新为基础保障的新时代电力系统，是新型能源体系的重要组成和实现 “双碳”目标的关键载体[8]。

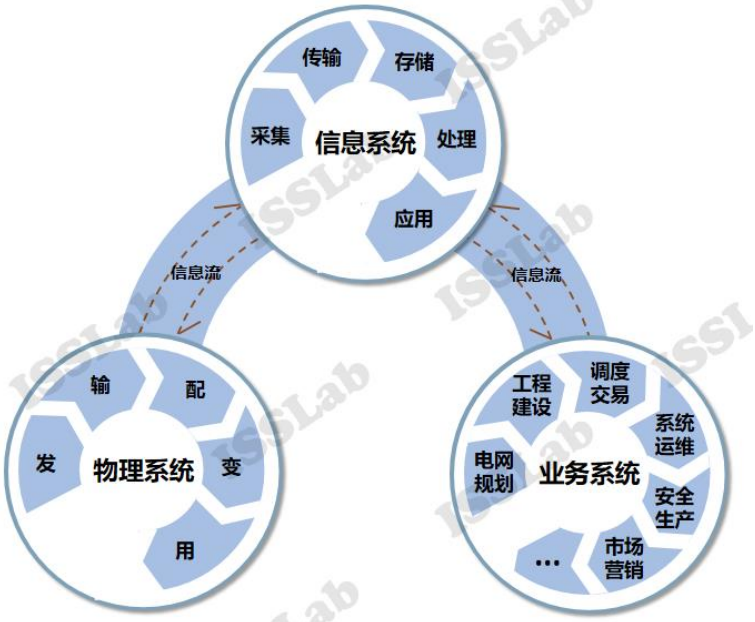

图 1-1 电力系统模型[9]

电力系统是当今世界规模最大的人造动态复杂网络系统，如图 1-1。其中，

物理系统主要涵盖发电、输电、变电、配电、用电等系统；信息系统主要包括信息采集、传输、存储、处理、应用等数据分析与处理系统；业务系统主要涵盖电网规划、调度交易、系统运维、安全生产、协调控制等业务过程[9]。

电力系统的发展经历三个阶段：

传统电力系统阶段。在电力系统发展早期，信息处理方式主要以手工处理为主，模拟信息仅有少量存在于继电器中，信息处理效率低、速度慢、能力弱。

信息电力系统阶段。电力系统大量使用计算机作为信息处理工具，信息开始以数字形式存在，但数字信息具有分散、局部、离线等特征。

数字电力系统阶段。电力系统信息处理方式进入信息化、智能化时代，信息系统以新一代数字技术实现大规模数据采集、传输、存储、处理、应用等，高效的信息系统促进了物理系统与业务系统建立更深入、更广泛的联系和融合，信息系统、物理系统、业务系统逐步形成一个有机的整体。当前，电力数据与社会数据高度融合互动，数字电力系统逐步演进为具备特大规模数字化服务能力的融合型关键信息基础设施，电力系统发展进入信息化、智能化的新型电力系统时代。

1.2 新型电力系统介绍

化石能源的储量限制和国家战略的迫切需要，新能源获得了快速的发展，传统电力架构越来难以支撑电网电建。用电侧：随着经济和人口的增长，电力负荷持续飙升，给电力系统的平衡和稳定性带来了巨大挑战。虽然采取有序的用电指令可以在一定程度上缓解电力紧张，但对正常的经济生活仍一定影响，比如限制工业和商业用电，导致生产活动无法正常进行。发电侧：恶劣天气的影响以及燃料价格的上涨，都给传统发电方式带来了很大的挑战。例如，燃煤或燃气发电站

因为天气原因无法正常运作，同时，燃料价格的上涨也会增加发电成本。这些原因将导致局部地区电力紧张，甚至出现电力短缺。电网侧：新能源的大量接入，对电力系统的安全构成了巨大威胁。例如，风能和太阳能等新能源的输出不稳定，可能会对电网的稳定运行产生影响。此外，如何有效地管理和调度这些新能源的输出，也是电网侧面临的一个挑战。为解决上述问题，传统电力系统亟需向新型电力系统转型。

新型电力系统是以承载实现碳达峰碳中和，贯彻新发展理念、构建新发展格局、推动高质量发展的内在要求为前提，确保能源电力安全为基本前提、以满足社会经济发展中电力需求为首要目标、以最大化消纳新能源为主要任务，以坚强智能电网作为枢纽平台，以源网荷储互动和多能互补为支撑，具有安全可控、灵活高效、清洁低碳、智能友好、开放互动等基本特征的电力系统。新型电力系统具有多能互补打破新能源发展瓶颈、多态融合打造更多新场景、多元互动新增产消群体三个特征[10]，具体如下：

（1）多能互补打破新能源发展瓶颈

新型电力系统中的多能互补，是指通过将不同种类的能源进行协同和优化配置，以满足电力系统的多元化需求。能源侧将在大时空尺度下进行优化配置，水利发电的定位由电量向容量转变，发挥其消纳不稳定能源的优势。光伏发电将逐渐称为发电主力军，风力发电也将进入加速发展阶段，形成风光水火储一体化供能，可解决光伏发电与风能发电的随机性和波动性问题，推动西南水资源丰富地区能源清洁化、绿色化转型。负荷侧实现电、气、氢、热、冷等应用场景的互补融合，局部区域多能协同。同时电网中信息流与能量流的深度融合，将促进传统工业耗能架构向源、网、荷、储多位一体转型。

（2）多态融合打造更多新场景

新型电力系统中的多态融合是指能源产业逐步呈现分布式、分散化、去中心的综合协调生产趋势，催生出“多杆合一”“多站融合”等新场景。新型电力系统电网向特高压主电网与微电网、局域网融合，交流大电网与交直流配电网共存的趋势发展。微电网的接入可以解决分布式能源的就近消纳问题，可节省大量输变电投资和运行费用；还可与主电网形成补充，减小整体电网容量，提高供电的可靠性。新型电力系统行业以传统变电站结构为基础，逐步实现储能电站、光伏电站、数据中心、北斗基站和虚拟电厂等单元的深度融合。虚拟电厂指利用通讯技术和信息采集技术，对广域空间内的新能源发电单元、分布式负荷单元以及储能单元进行信息物理深度融合，实现对分布式能源生产、储存及消纳的综合调度和有效利用。对于电力市场，虚拟电厂可实现对分布式资源的快速整合，无视地理区域制约，有利于资源合理运用及优化配置。

（3）多元互动新增产消群体

新型电力系统中电网负荷多元化，分布式光伏发电、电动汽车以及充电桩的接入提升了用户对电网容量的调节能力。多元负荷单元以及分布式储能设备的大量并网，使得消费者的身份从单纯的用电方向具有对电网双向调节能力的“产消者”转变。据统计预测，到 2025 年我国新能源汽车保有量将达到 2500 万辆，其电能转化量可达 1000 亿千瓦时，与相应的充电桩部署，将达到 1400 万根。与此同时，可实现电网调峰调频的电力辅助市场可调节电网出力、控制新能源所造成的电网波动。电力辅助市场不仅能够有利于新能源的消纳，也可为电力市场提供经济补偿，提高社会总福利。

（4）新能源互联网未来可期

新型电力系统的构建伴随着电源侧、负荷侧和用户侧的改革和重组。发电侧逐步形成以新能源为主体的多能互补电力供给系统；电网侧呈现“主电网+微电网”的电网形态，增强了区域消纳新能源能力的同时提升了电力系统的稳定性。同时，数字电网的兴起也为网荷储协调互动提供了保障；负荷侧以多元化的电网负荷构建了以电能为核心的综合能源消费体系。新型电力系统的构建要以确保能源电力安全为基本前提，以满足经济社会发展电力需求为首要目标，以坚强智能电网为枢纽平台，以源网荷储互动和多能互补为支撑，构建低碳清洁新能源互联网，为新型电力系统的安全稳定运行提供数据信息保障。

1.3 新型电力系统网络

新型电力系统旨在利用先进信息通信技术和智能化控制手段，提升能源利用经济性、系统运行可靠性和产业发展可持续性。新型电力系统网络由电力网络与信息网络构成，如图 1-2，电力网络包含各种能源基础设施，如发电系统、输电系统、配电系统、用电系统等，实现能量流动，以保障电力供应；信息网络包含控制中心、通信网络、监控与数据采集系统、远程终端单元、智能电力设备、可编程序逻辑控制器、相量测量单元等，实现信息流动，通过对电力网络物理系统运行数据采集与传输、状态估计与预测、实时反馈与控制等以保障电力的稳定供应。

图 1-2 新型电力系统网络模型

1.2.1 电力网络

- **发电系统**

将各种能源形式（如化石燃料、风能、太阳能、水能等）转换为电能的装置或系统。新型电力系统中的发电设备具有多样化、小型化和分散化的特点，以采用更加环保和可持续的方式生成电能，减少对传统化石燃料的依赖，并促进清洁能源的使用。分布式能源系统中的发电设备规模较小，分布在用户附近，接近能源需求点，与传统的集中式发电站相比，消除了远距离输电损耗和可靠性问题。

- **输电系统**

将发电设备输出的电能从发电站传输至用户所在地的系统，由高压输电线路及其附属设备组成，其主要包括：输电线路、支撑电塔、变电站、变压器、断路器等。

- **配电系统**

配电系统负责将电能从变电站传输到各个用户，包括配电变压器、配电线路和配电设备（如配电盘、开关等）。配电层将电能分配到生产厂区、医院、校园、居民区等，以满足各个用户的需求。

- **用电系统**

经配电系统将电压转换成适合用户使用的电压，以供不同用户的使用。用电是指最终用户在家庭、商业、工业等场所使用电能的过程。用户通过连接电器设备、开关和插座等设备来获取所需的电能，并用于照明、通信、加热、制冷、生产等。用户的用电量通过用电设备产生和计量，主要计量设备包括智能电表、负载传感器、功率计等。

1.2.2 信息网络

- **控制中心**

调度控制中心是电力系统信息处理、监视和控制的中心机构，是数据分析与处理平台、反馈与控制系统等电力业务的载体。根据电力系统当前运行状况和预测的变化进行判断、决策和指挥。由于系统庞大、任务繁重、能源分布式等问题，传统集中控制模式难以满足当前新技术新业务下的新需求。因此，分层控制已成为新型电力系统的主流控制模式[11]。例如，国家电网设有全系统的调度中心，称为国调。相应的各省设有省级调度中心，称为省调。省级调度中心下又有各地区调度所。各级调度所在“统一调度，分级管理”的原则下对所辖区域进行调度和管理。各调度中心之间通过通信网络进行数据交互、信息共享和指令下发。

1) 国家电力调度中心

国家电力调度中心，简称国调，是我国电网调度的最高级（如国家电网公司，南方电网不属于国家电网管辖），在该中心，通过计算机数据通信与各大区调度中心相连接，协调确定各大区之间的联络线潮流和运行方式，监视、统计和分析全国电网的运行情况。

2) 省局调度中心

省局调度中心，简称省调。省调也称中调，是各个省的电力调度中心，通常情况下发电计划逐级分配，总调安排中调的发电计划，中调安排各区域的发电计划。对于大型的发电站/变电站或有重要作用的发电站/变电站，会由中调甚至总调直接调度，于是有总调直调电厂的说法。

3) 地局调度中心

地区调度中心，简称地调（各省地级市电力局、电业局、供电局），采集当地电网的各种信息，进行安全检测，进行有关站点开关的远方操作，变压器分接头的调节，电力电容器的投切等。

调度控制中心之间通过调度数据网、综合数据网进行数据传输和信息交换。这些通信网络使用先进的通信技术，包括光纤通信、微波通信和卫星通信等，以确保快速、可靠的数据传输和迅速的决策响应。如图 1-3，通过这样的通信关系，不同级别的控制中心可以实现全面的电力系统监控、调度、运行和管理。

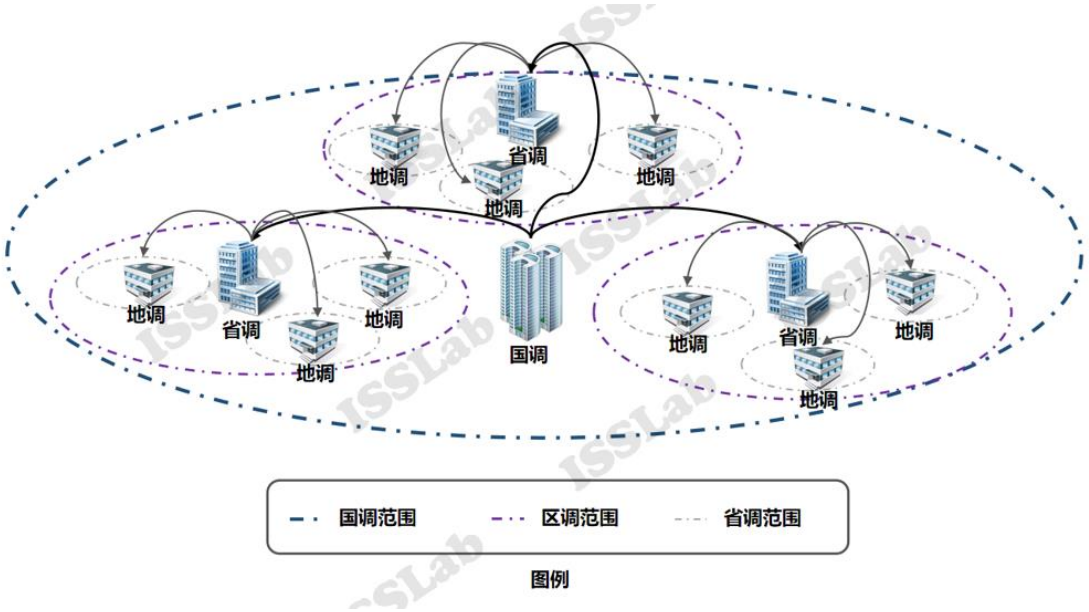

图 1-3 我国电力系统调度分层控制示意图

- **通信网络**

1) 通信设备与协议

作为信息流的载体，通信设备及其协议是新型电力系统信息网络的重要组成部分。常见的电力系统通信设备包括：

(1) 光纤通信设备：如光端机、光转换器等，用于传输高速率、大容量的模数信号信息，支持点对点、环形、星形等多种组网方式。

(2) 无线通信设备：如无线路由器、无线网桥等，用于在移动环境中实现设备之间的无线通信连接，适用于远程监控、数据采集等应用场景。

(3) 电力线载波通信设备：如调制解调器、电力线网卡等，利用电力线作为通信介质，实现设备之间的通信连接，具有无需布线、降低成本等特点。

(4) 串口通信设备：如串口服务器、串口转换器等，用于支持串口设备与其他通信设备之间的通信，包括 RS-232、RS-485 等多种接口类型。

(5) 数据网关设备：如路由器、交换机等，用于在不同网络之间进行数据转发和路由，支持多种网络协议和接口类型，实现网络之间的互联互通。

(6) 其他通信设备：如卫星通信设备、微波通信设备等，用于在特殊环境下实现通信连接，满足长距离、高速率等需求。

常见的电力系统通信协议包括：

(1) MODBUS：一种串行通信协议，用于连接电子设备，包括自动化控制系统和仪表系统，用于不同设备之间的通信和数据交换[12]。

(2) Ethernet/IP：一种广泛的、全面的、可认证的应用层协议，在电力系统中被广泛用于电力监控与控制，连接电力监控系统、SCADA 系统和 PLC 等[13]。

(3) DNP3：一种通信协议，用于监控系统和自动化设备之间的数据交换，被广泛应用于电力系统中[14]。

(4) Profinet：新一代基于工业以太网技术的自动化总线标准，可以完全兼容工业以太网和现有的现场总线。

(5) GOOSE：又名通用面向对象变电站事件协议，是国际电工委员会 IEC 61850 标准套件的一部分，其中规定了变电站事件的通信方式。

(6) C37.118：电力系统中使用的通信协议，用于测量和控制设备之间的广域网通信，定义了数据格式和通信要求，支持高速数据传输和同步采样。

(7) ICCP：一种用于不同电力控制中心之间的通信协议，允许跨辖区进行数据交换和共享，实现电力系统的协调运行和控制。

2) 监控与数据采集(supervisory control and data acquisition, SCADA)

SCADA 系统是一种用于监控和控制远程设备和过程的系统[15]。SCADA 主要包含以下功能：(1) 数据采集：SCADA 系统通过传感器、遥测装置等采集现场设备和过程的数据，这些数据可以包括电压、电流、功率、频率等各种参数。(2)数据传输：采集到的数据需要通过通信网络传输到控制中心。传输方式可以采用有线通信(如以太网、串口等)或者无线通信(如无线局域网、GSM、GPRS 等)。(3) 数据处理：控制中心接收到数据后，进行数据处理和分析，包括报文解析、数据校验、数据转换等过程。处理后的数据可以存储在数据库中，以供后续查询和分析。(4) 控制命令下发：通过 SCADA 系统，操作员可以向远程设备发送控制命令，包括开关状态改变、参数设置、报警信号等，这些命令通过通信网络传输到远程设备进行执行。(5) 实时监控：SCADA 系统可以实时对远程设备和过程进行监控。控制中心可以接收远程设备的状态信息、报警信息等，并实时显示在操作界面上。同时，SCADA 系统还可以进行实时趋势分析、报表生成等。(6)报警处理：如果远程设备或过程出现异常，SCADA 系统通过通信网络发送声音、图形、短信等报警信息给操作员，操作员可以及时采取相应措施。

3) 远程终端单元（Remote Terminal Unit，RTU）

RTU 是安装在通信网络中的智能控制和通信设备，实现对设备的远程监测、操作。RTU 与 SCADA 系统相连，将电力系统现场侧运行数据进行采集和转发，并由 SCADA 传输到控制中心。

4) 智能电子设备（Intelligent Electronic Device，IED）

IED 是具有计算、通信和控制功能的电子设备，可以实现对电力系统的智能监测、管理和优化。常见 IED 设备包括智能电表、智能计量仪表、智能开关和保护装置、智能变压器、储能系统及智能电池充电设备等。这些设备互相之间或与

远程终端单元进行通信，对网络要求高可靠、低延迟。例如，当线路过载时，断路器需及时断开线路以避免火灾。

5) 可编程逻辑控制器（Programmable Logic Controller，PLC）

PLC 被广泛用于电力系统自动化控制和监测，基于数字计算技术，具有高度可编程性和灵活性，可用于执行复杂的控制逻辑和算法。IED 用于电路保护（如断路器），PLC 用于系统控制。控制中心通过 SCADA 向 PLC 发送控制命令，可以实现如下功能：自动控制、监测与数据采集、通信与协调、故障检测与报警等。

6) 相量测量单元（Phasor Measurement Unit，PMU）

一种高精度、实时测量电压、电流相位及其变化速度的设备，采用 GPS 同步技术，能够以非常高的时间分辨率（通常为 1 毫秒或更低）采集电力系统各节点的相量数据。PMU 在新型电力系统中的应用，能够有效提升电力系统的监测、控制和故障诊断能力，为电力系统智能化和自适应运行奠定基础。

基于电力网络和信息网络双层网络结构，能量流与信息流各自流动但相互关联，使得新型电力系统的信息空间与物理空间深度融合。通过 SCADA 系统，采集系统实时运行数据，并进行数据分析与处理，为后续应用提供可靠的数据基础；通过能源管理系统，实时监测和控制电力系统的运行状态，实现分布式能源资源的最大化利用，并及时发现和处理潜在问题，防止事故和故障发生，提高电力系统的可靠性和安全性；通过电力市场交易平台，实现能量、信息、数据的交易和结算，优化能源供应成本，降低输电线路拥塞，实现新型电力系统运行的智能化。

02

新型电力系统安全问题与挑战

2.1 安全风险分析

新型电力系统由电力网络和信息网络组成，实现能量流和信息流的流动和交互。分布式、多样化的能源结构使得新型电力系统呈现出信息物理深度融合的态势，如单台发电机有上千个传感器，采集的数据将会共享至多个控制中心，甚至跨越多个省市。能源供应小型化、分散化使得原本封闭的发电、输电、配电、用电逐渐开放化。信息物理融合带来的双向互动和协同，使得新型电力系统面临前所未有的安全风险。信息物理威胁相互耦合、交叉影响，单一的信息或物理防护难以应对跨越信息物理空间的协同威胁。

2.1.1 风险特征

针对新型电力系统的攻击呈现出信息物理协同、威胁来源复杂、攻击目的多样、攻击过程持续等特征。

信息物理协同：攻击者通过网络侧攻击修改电力系统数据，包括运行数据、测量数据等。导致系统管理员无法准确判断电力系统的状态和运行情况，产生错误决策，对电力系统的稳定性和安全性产生直接影响。此外，电力系统作为关键基础设施，攻击者可通过电力系统入侵其他行业的网络，或者通过其他行业的网络入侵电力系统，从而对整个社会基础设施产生连锁反应。

威胁来源复杂：新型电力系统庞大且复杂，融入了大量的新技术，攻击可能

来自不同类型的威胁源：(1) 外部攻击。来自黑客、网络犯罪分子、恶意竞争对手和国家级的网络攻击团队等具有高级的技术知识和资源的外部攻击者；(2) 内部威胁。内部员工滥用权限、窃取敏感信息、篡改数据或干扰系统操作，由于攻击者具有合法访问权限，内部威胁通常更难被检测和阻止；(3) 物理攻击。包括破坏设备、截断电力供应、引发火灾或爆炸等；(4) 网络攻击。通过恶意软件(如病毒、木马、勒索软件等)，攻击者可以远程控制电力系统组件、窃取数据、加密文件或瘫痪系统；(5) 社会工程攻击。攻击者通过社交工程技术欺骗用户、员工或管理员，获取敏感信息或非法访问权限，常用手段包括钓鱼邮件、电话诈骗、冒充身份和欺骗攻击。

攻击目的多样：(1) 经济利益。攻击者通过篡改电表读数、窃取用户个人信息、非法操纵市场交易等，以获取经济利益；(2) 窃取机密。攻击者窃取用户隐私数据、能源使用模式、商业机密等用于其他非法活动；(3) 破坏基础设施。攻击者直接破坏电力系统基础设施，如变电站、通信网络或控制中心，对整个电力系统造成严重破坏，并导致长时间的停电；(4) 政治和恐怖主义目的。攻击者为达到政治目的或恐怖主义动机，通过攻击电力系统来传递政治信息或制造恐慌，包括瘫痪城市供电系统、干扰国家能源供应等，造成社会和经济混乱。

攻击过程持续：针对新型电力系统的攻击不仅发生在某一次短暂的事件中，而是以持续、渐进的方式进行。攻击者通过设备、软件漏洞或者后门长期保持对系统的控制，并持续进行非法活动。为逃避检测或阻断，攻击者采用隐蔽和隐匿的方式进行，如使用高级持久性威胁技术，隐藏在合法流量中，规避安全监测系统的侦测，并持续地探索系统的弱点和漏洞。

为提高新型电力系统的网络安全水平，亟需采取一系列安全措施，建立建全

安全防护体系、实施加密技术、使用安全认证和身份验证技术等。需要加强对网络安全风险的识别和攻击检测，及时响应威胁事件和漏洞，并加强通信网络的安全管理和保护。

2.1.2 风险识别

电子通信技术和计算机技术在新型电力系统中的应用，会涉及大量的敏感信息和安全权益。安全风险是新型电力系统面临的主要挑战之一，物联网设备、通信协议、系统业务都存在安全风险。经过现场调研和对电力系统网络信息安全的深入分析，新型电力系统面临的安全风险如下：

- **设备安全风险**

电力系统中的漏洞难以避免，且多为能造成远程攻击、越权执行的严重威胁漏洞，并且漏洞数量呈快速增长趋势。电力系统通讯协议种类繁多，系统软件难以及时升级、设备生命周期长、系统补丁兼容性差等现实问题，造成电力系统补丁管理困难，难以及时处理严重的漏洞。许多电力软件健壮性较差，只能运行在操作系统的某个特定版本上，系统升级导致关键设备、软件、协议无法使用。

- **协议安全风险**

电力通信协议或规约在设计时通常只强调通信的实时性和可用性，对安全性考虑不足，比如缺少足够强度的认证、加密等。尤其无线通信协议，更容易遭受第三者的窃听和欺骗性攻击。为保证数据传输的实时性，部分通信协议多采用明文传输，易被攻击者劫持和修改。

- **业务安全风险**

新型电力系统的正常运行离不开各业务系统，如监控与数据采集系统、生产

与调度系统、安全监控与报警系统、电力市场管理系统等。各业务系统承担着不同的关键功能和任务，针对业务系统的攻击可能导致业务功能丧失，影响电力系统的稳定运行。如利用业务软件逻辑漏洞和算法缺陷执行错误数据注入、SQL 注入、拒绝服务、对抗样本等攻击，导致业务系统运行错误，甚至功能丧失。

- **防护边界风险**

网络边界安全防护对管理依赖度较高，实时监视和闭环管控力度不足。已有技术手段只能覆盖网络边界上的防护设备，不能全面监控系统内部的服务器、工作站和网络设备，不能全面监测外部网络访问、外部设备接入、用户登录、人员操作等事件，不能实现网络安全监视报警、分析定位、追踪处置、审计溯源、风险核查和协同管控。

- **供应链安全风险**

新型电力系统的供应链安全也是一个重要的关注点。电力系统供应链复杂，不可靠的供应商可能会给攻击者提供可乘之机。攻击者可能通过植入恶意代码、硬件后门等方式在供应链环节实施攻击，危及电力系统的安全性。

- **安全管理风险**

缺少分层分级的安全管理机制，导致管理难度增大。在电力行业，各类工作站、服务器和网络设备规模数量大，需要统一管理平台进行管理；在电力系统资产管理、安全策略管理、账户管理、配置管理、日志管理、日常操作等方面缺乏统一的技术手段和管理方法，也无法对日志、监测和报警数据等进行分析和统计。

- **人员管理风险**

电力系统员工缺乏网络安全知识，安全防护意识淡薄，相关安全技术匮乏，

安全技术操作不熟练。外部人员容易造成无意操作、错误操作、非法操作。

综上所述，由于新型电力系统的关键性和复杂性，必须整合各种安全技术和理念，需要构建完善的安全防御技术体系来保障新型电力系统的信息安全。同时，政府和相关机构应加强监管和管理，确保新型电力系统安全防护遵循法律规章，提高电力系统的安全性和稳定性。

2.2 安全防护现状

2.2.1 物理防护

物理系统的防护体系是针对电力系统发生自然或者人为故障时，电力系统如何提前预防或及时响应以保护物理系统运行，保证供电能力。由于电网物理系统是高度非线性的复杂时变系统，各项防护技术之间具有紧密的耦合关系，需要多种防护技术的有机协同配合，才能有效保障电力系统物理安全。

物理防护以国家电网合规管理制定的三道防线为主，意在通过不同的控制手段降低故障造成的损失[16]，如图 2-1 所示。一般故障发生时，由第一道防线保证供电不中断；严重故障发生时，由第二道防线保证不失去系统的完整性；特别严重的故障发生而被迫解列后，由第三道防线尽量减小停电规模和停电时间并恢复供电。第一道防线由继电保护装置快速切除故障元件，最直接最有效地保证电力系统暂态稳定。第二道防线采用稳定控制装置及切机、切负荷等措施，确保在发生大扰动情况下电力系统的稳定性。第三道防线是指当电力系统遇到多重严重故障而造成稳定性被破坏时，依靠失步解列装置将失步的电网解列，并由频率及电压紧急控制装置保持解列后两部分电网功率的平衡，防止事故扩大。

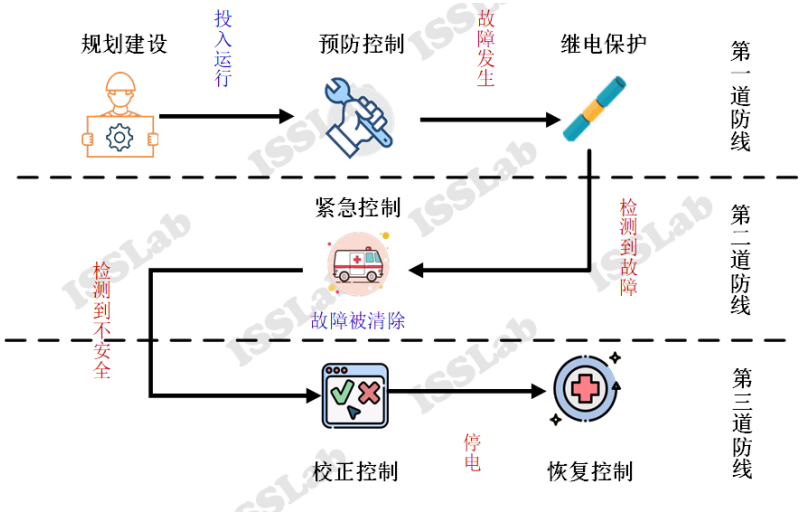

图 2-1 物理防护三道防线

第一道防线是在不损失电源和负荷的前提下，保证系统在不严重故障下的稳定性。例如，在规划建设期间加强电网结构，或在正常运行期间启停发电机组，调整发电功率，采用电力系统稳定器、并联和串联电容补偿控制、直流输电功率调制、动态无功补偿装置和静态无功补偿器等技术。一旦发生故障，继电保护装置以最小的停电范围将故障(或越限)设备从电网中快速隔离，以扩大稳定域。如果第一道防线已经将系统的运行点引导到预想故障所对应的稳定域内，则一旦该故障发生，不必采用其他措施就可以保持系统稳定。

第二道防线是减少系统在严重故障下失稳的风险。如果预防控制会使系统运行经济性太差，或者不同的故障对预防控制提出相互矛盾的要求时，依靠第一道防线来保证系统的稳定性并不可行。此时只能在检测到故障后实施以切除部分电源和负荷为代价的紧急控制，如连锁解列、切机、切负荷、强励、强补、快关汽门、动态制动。紧急控制只有在故障已经发生并可能导致失稳时才被执行，故虽然每次动作的代价较大，但平时并不需要付出控制代价。紧急控制措施在故障后实施得越早，效果越好。一旦判明故障的有关特征，就应该根据实际工况立即实施决策表中的相应措施。为了在保证系统稳定的前提下尽量减少控制代价，必须

提高对控制效果的预测精度。由于后者强烈依赖于故障前的工况，因此紧急控制的决策表的事先制作和实时匹配都必须基于广域信息。

第三道防线是弥补前两道防线的欠控制或拒动造成的风险，避免系统在极其严重的故障下发生大停电。由于紧急控制的决策表要根据事先指定的典型工况和故障来索引，而故障表又不可能涵盖所有潜在的故障，因此，如果实际工况（或故障场景）的匹配误差太大，甚至完全失配，则第二道防线可能严重欠控制。此时，只能依靠第三道防线来制止停电范围的扩大。显然，第三道防线不再能按工况和故障的组合来选择控制措施，而必须由系统变量的实际动态行为来触发。例如，在检测到失步后立即启动振荡解列，以及检测到过长时间的低频现象后分轮次切负荷等。由于是在不安全现象出现后才采用的措施，故称之为校正控制。

2.2.2 信息防护

随着电力系统由传统电力系统—信息电力系统—数字电力系统的发展进程，我国电力系统网络安全防护理念经历了三个阶段的演变[17]。

- **结构性安全防护机制**

我国早期电力系统信息安全防护总体策略：“安全分区、网络专用、横向隔离、纵向认证”。规定电力调度数据网只允许传输电力调度生产直接相关的数据，必须与公用信息网络在物理层面安全隔离，从而提出“结构性安全”的重要概念，成为电力系统信息安全体系建设的标准性起点。

- **基于等级保护的业务安全防护体系**

2007 年国家电监会启动电力行业信息安全等级保护定级，全面推进电力行业等级保护建设工作。在结构性防护基础上进一步完善电力系统的等级保护体系，

包括物理安全防护、网络安全防护、主机安全防护、应用安全防护、数据安全防护五个层面。

- **基于可信计算的电力系统主动防护体系**

随着新型攻击方式的出现，安全威胁特征库迅速增大，以“封堵查杀”为核心的被动安全措施对于实时控制系统安全防护不再高效。可信计算技术在新型电力系统中的应用，可以提升电力系统对未知恶意代码攻击的免疫能力，实现全程可测可控安全可信的计算机网络环境。其核心功能包括：可信引导、完整性度量、强制访问及执行控制、可信网络连接。

新型电力系统防护技术体系综合利用主被动防御技术，构建多道防线，形成综合、立体的网络安全技术防护体系，使得新型电力系统网络信息安全走向纵深防御阶段，主动防御技术体系需要构建以下三道防线：

第一道防线由网络安全防护措施组成，实行“安全分区、网络专用、横向隔离、纵向认证”十六字方针，使电力系统信息系统本身具有一定的抗攻击能力。安全分区是划分管理信息大区和生产控制大区，管理信息大区又细分为信息内网和信息外网；生产控制大区又细分为实时子网和非实时子网。网络专用是指生产控制大区和管理信息大区在各自信息传输方面单独组网，实现与外部网络的物理隔离。各网络间采用逻辑强隔离装置、单向隔离装置、防火墙进行隔离，是不同网络或网络安全域之间信息的唯一出入口，可根据网络的安全策略控制出入网络的信息流。纵向认证是采用认证、加密、访问控制等技术措施实现数据的远程安全传输以及纵向边界的安全防护。

第二道防线是检测，旨在实时发现系统遭受的攻击行为，由入侵检测系统、

漏洞检测系统组成。入侵检测系统通过在网络主机系统中主动寻找入侵信号来发现入侵行为并报警，提供对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前有效抵御入侵，能够将潜在的不安全因素消灭在萌芽状态。漏洞扫描系统构成利用漏洞扫描技术，对站点、网络、操作系统、应用服务以及防火墙进行漏洞扫描，及时修复在运系统中存在的安全漏洞，确保系统可靠运行。

第三道防线是保护，旨在使系统免受攻击行为危害或受攻击情况下很快恢复。由一系列终端安全防护措施组成，综合利用终端准入、病毒防范、加密认证，访问控制等技术，通过安全接入平台确保接入终端安全可信。当针对电力系统的网络攻击未能被信息侧预防手段有效阻断时，将开始对物理侧产生实际影响。

2.2.3 现有防护不足

面向中国制造 2025，随着物联网、5G、云平台等技术融入智能电网形成新型电力系统时，已有的防护体系已不能满足当前的安全防护需求。

- **物联网带来的安全边界改变**

在以物联网为核心的能源互联时代，能源系统正向分布式转型，并以万物互联、高度智能的形态存在，网络边界不再像传统经典结构那样清晰，智能终端设备急剧增加，数据信息多向流动，网络安全问题更加凸显，任何一个微小的电网设备漏洞都可能导致电网运行的重大安全风险。

- **通信新技术带来安全新风险**

5G 通信技术的终端多样化、网络功能虚拟化、网络切片化、业务边缘化、网络开放化以及应用多样化等特征，使得电力网络给攻击者的暴露面大幅度增加，通信协议的脆弱性给网络安全带来新的风险和挑战。

- **分布式能源带来的业务新问题**

目前，我国风电、光伏发电装机总量达到 3.5 亿千瓦。风电、光伏发电具有很强的随机性和波动性，大规模集中并网，对电网的适应性和调频调压能力提出了更高要求，而目前现有的防护措施并没有很好地应对分布式能源对系统带来的扰动与安全威胁，电力中心的小型化、分散化给业务系统之间的数据交互和功能衔接带来了业务安全新问题。

- **系统风险防护不完善**

分布式电源、微电网、智能用电、电动汽车、储能快速发展，配电网从无源网成为有源网，潮流由单向变为双向、多向，电力系统运行控制更加复杂，而现有的安全防护措施大多是针对单一的电力安全风险，没有形成电力行业的完善的安全防护体系，无法对复杂系统形成完善、有效的立体安全防护机制。

- **人工智能方法带来的安全新威胁**

人工智能已广泛应用于新型电力系统中，如使用机器学习算法预测区域负载、使用计算机视觉技术智能巡检电网设施、通过虚拟电厂进行分散电源的组合优化。然而，与人工智能相关的安全问题也被引入到新型电力系统中，形成了新的安全威胁。如 AI 模型安全性问题、AI 数据与隐私安全性问题、AI 系统安全性问题等。这些新威胁不仅严重损害人工智能技术的功能性，极大程度上破坏了人工智能技术在电力系统良性发展的生态，还会穿透到物理空间，造成关键基础设施受损，对新型电力系统的稳定高效运行造成极大的危害。

2.3 安全防护需求

新型电力系统防护的需求主要包括以下两个方面：

- **系统安全稳定运行需求**

国家市场监督管理总局及国家标准化管理委员会于 2019 年 12 月 31 日发布了《电力系统安全稳定导则》（简称《导则》），并于 2020 年 7 月 1 日起开始实施，在《导则》中提出了电力系统稳定运行的基本要求，其中包含以下六点：

(1) 保证电力系统运行的稳定性，维持电网频率、电压的正常水平，系统应有足够的静态稳定储备和有功功率、无功功率备用容量。备用容量应分配合理，并有必要的调节手段。在正常负荷及电源波动和调整有功、无功潮流时，均不应发生自发震荡。

(2) 合理的电力系统结构和电源结构。在电力系统的规划设计阶段，应当统筹考虑，合理布局。规划周期内的电力系统建设应该按照确定的电力系统规划方案执行。电力系统运行方式安排也应注重电网结构和电源结构的合理性。

(3) 在正常运行方式下，所有设备均应不过载、电压不越限，系统中任一元件（发电机、线路、变压器、母线）发生单一故障时，应能保持系统安全稳定运行。

(4) 在事故后经调整的运行方式下，电力系统仍应有规定的静态稳定储备，并满足再次发生单一元件故障后的暂态稳定和其他元件不超过规定事故负荷能力的要求。

(5) 电力系统发生稳定破坏时，必须有预定的措施，以防止事故范围的扩大，减少事故损失，满足国务院令第 115 号、第 599 号的相关要求。

(6) 低一级电网中的任何元件（包括线路、母线、变压器等）发生各种类型的单一故障，均不得影响高一级电压电网的稳定运行。

此外《导则》中还对电网结构、电源结构、无功平衡及补偿、对机网协调及厂网协调、防止电力系统崩溃以及电力系统全停后的恢复做了详细的说明。并且分别从电力系统的静态稳定储备标准、电力系统承受大扰动能力的安全稳定标准以及一些特殊情况的角度，明确了电力系统的安全稳定标准，为电力系统安全运行制定了边界。

- **系统信息安全需求**

新型电力系统网络信息安全工作面对的挑战具体如下：(1) 信息安全的暴露面较大。用户侧和各级系统节点部署了海量终端及网络接口，因此，恶意攻击者能够获取的基于物理层面的可接触点数量相对较多，且对这些点的全面、实时监控的实现难度较大；(2) 可攻击的路径较多。在新型电力系统中，无线专网、卫星网络、5G、NB-IoT、近场通信等网络通信技术得到了重点应用，实现了接入成本降低以及便利性提高，与此同时，也增加了恶意攻击者可以展开攻击的网络路径；(3) 智能终端网络安全漏洞较多。对于智能终端来说，其实际使用操作系统、嵌入式设备、芯片等型号较多，通信协议、规约和接口实现方式也存在差异，导致安全漏洞出现的概率增加，提升了全面修复漏洞的难度，导致遭受恶意攻击者攻击渗透更加容易；(4) 新型电力系统中电力业务与互联网的融合程度逐步加深，对现有信息内外网及互联网的防护格局产生了较大的冲击，现有网络结构已无法满足业务部署及防护的现实要求；(5) 全面感知推动了终端的泛在化，对现有终端接入防护策略产生了较大的冲击，现有的边界防护结构与防护设备的性能无法完全满足要求；(6) 新型电力系统中电力物联网的数据共享、业务协同实现了运营成效的明显提升，然而也对现有的网络信息安全管理体系产生了较大冲击；(7) 新型电力系统中机器学习应用提升了系统的实时决策能力、预测能力，利用人工

智能强大的数据分析能力，实现电力系统大规模控制的自动化和智能化，以及高效的故障检测和早期预防，然而机器学习的脆弱性也对系统的安全保护能力提出了更高的要求。

针对数据隐私安全防护需求，在新型电力系统业务系统中，积累了大量的电力敏感数据，例如财务数据、营销数据、人资数据、市场信息、生产管理信息等，这些来自于不同的应用系统的数据集中存储在数据库中。内部人员、第三方运维人员、Oracle 数据库系统的 DBA、新模块的程序开发人员对数据库中的数据都需要频繁地访问，诸多的人群和过高的权限造成电力敏感数据集中泄露的风险，经营方面的数据也有被异常篡改的风险。对于数据库的安全防护措施属于当前安全体系的薄弱环节，相应的防御手段及所需要达到的效果如表 2-1 所示。

表 2-1 等保数据应对点

功能	备选产品	保护效果
身份鉴别	数据库漏扫	检测数据库的弱口令、连续登录失败锁定的次数等
访问控制	数据库漏扫 数据库防火墙 数据库加密	检查数据库系统的缺省账户，多余、过期的共享账户 提供细粒度的访问控制、提供行数限制的阈值控制等 防止特权用户敏感数据访问；对重要信息形成敏感标记
安全审计	数据库审计	每个用户的行为、各种可疑操作进行告警通知，能对操作记录进行全面的分析，提供自身审计进程的监控，审计记录防止恶意删除，同时具备自动归档的能力
入侵防范	数据库漏扫 数据库防火墙	可以检测出数据库漏洞、补丁未升级 虚拟补丁技术能阻止针对补丁未升级的恶意攻击行为
恶意代码防范	数据库漏扫 数据库防火墙	能检测存储过程、函数中存在的恶意代码 SQL 注入等漏洞特征库、通过虚拟补丁防范恶意攻击
资源控制	数据库防火墙	提供每个用户对敏感数据的最大连接数限制等
数据保密性	数据库加密	对数据库中敏感信息按列进行加密保存

2.4 安全防护规范

2.4.1 安全防护要求

《电力行业信息安全等级保护基本要求》是中国电力行业制定的针对信息系统和网络安全的保护标准，旨在加强电力行业信息安全管理，保障电力系统和网络的安全可靠运行。根据《电力行业信息安全等级保护基本要求》，新型电力系统主动防御技术体系应满足以下要求：

- **等级划分要求**

要求根据信息系统和网络的重要性、功能和风险等级，划分为不同的安全等级，以确定相应的保护要求和控制措施。包括一般级、重要级、关键级等不同安全等级。

- **控制措施要求**

对于不同安全等级的信息系统和网络，要求实施相应的安全控制措施，包括物理安全、人员安全、访问控制、通信安全、应用软件安全、数据备份与恢复等方面，确保信息系统和网络的安全可靠性。

- **安全技术要求**

要求采用安全技术手段和方法，包括身份认证、访问控制、加密算法、防火墙、入侵检测与防御系统(IDS/IPS)、安全审计等，来提供必要的安全保护。

- **安全管理要求**

要求建立健全的安全管理制度，包括安全策略和规程、安全培训教育、安全风险评估与管理、安全事件响应等方面，确保信息系统和网络的持续安全运行。

- **监测和报告要求**

要求建立安全事件监测和报告机制，及时发现和报告安全事件，并采取相应的处置措施，以减轻安全风险对电力系统和网络的影响。

- **审计和验证要求**

要求定期进行安全审计和验证，包括漏洞扫描、安全防护能力测试等，以评估系统的安全性和有效性。

- **合规性要求**

要求遵守相关法律法规和标准要求，如《中华人民共和国网络安全法》等，并进行必要的合规性审查和整改。

2.4.2 安全防护依据

- **法律法规**

《中华人民共和国网络安全法》

《中华人民共和国数据安全法》

《信息安全等级保护管理方法》

《关键信息基础设施保护条例》

《电力行业信息系统等级保护定级工作指导意见》

《电力监控系统安全防护规定》

《电力行业网络与信息安全管理办法》

《电力行业信息安全等级保护管理办法》

- **标准及规范**

GB 17859-1999《计算及信息系统安全保护等级划分准则》

GB/Z 20986-2007《信息安全事件分类分级指南》

GB/T 30976.1-2014《工业控制系统信息安全 第一部分：评估规范》

GB/T 30976.2-2014《工业控制系统信息安全 第二部分: 验收规范》

GB 38755-2019《电力系统安全稳定导则》

DL/T 1234-2013《电力系统安全稳定计算技术规范》

网络安全等级保护定级指南（GB/T 22240-2020)

网络安全等级保护实施指南（GB/T 25058-2019）

网络安全等级保护测评指南（GB/T 28449-2018）

网络安全等级保护基本要求（GB/T 22239-2019）

网络安全等级保护设计技术要求（GB/T 25070-2019）

2.4.3 安全防护原则

- **管理与技术并重**

需要同时注重管理和技术手段的应用。管理层面包括建立健全的安全管理制度、制定安全规范和流程、培训员工的安全意识和技能等，以确保人员的安全行为和责任意识。技术层面则涉及安全设备的选择和配置、安全控制系统的建设、安全监测和预警技术的应用等，以提供可靠的技术支持和保障。

- **外防与内治结合**

外防是指通过外部措施来防止新型电力系统安全事件的发生。这包括建立强大的边界防护体系，采用入侵检测系统、防火墙、访问控制等技术手段，限制非授权人员的进入和恶意攻击的发生。同时，内治是指在新型电力系统内部加强安全管理和监控。这包括实施访问权限管理、加密通信、安全审计等内部安全措施，及时发现并处理内部的安全风险和威胁。

- **全方位整体联动**

需要全方位地覆盖各个环节和组成部分。从电力生产、传输到供应，涉及到发电厂、变电站、输电线路、配电网络以及终端用户等各个环节。全方位整体联动意味着在这些环节中采取相应的安全措施，确保整个系统的安全性。不仅要重视关键节点的安全，还要考虑整个系统的连续性和一体化，确保各个环节之间的协同与衔接。

- **全过程协同管控**

电力系统防护需要贯穿整个生命周期，从规划和设计、建设和运维到退役和更新等各个过程。全过程协同管控要求在每个环节都加强安全意识和风险评估，采取相应的安全策略和措施。这包括安全规划和设计、安全培训和管理、安全监测和预警等。通过全过程的协同管控，可以提前发现和解决潜在的安全隐患，确保电力系统在各个阶段的安全性和可靠性。

- **全面覆盖与重点防护结合**

全面覆盖确保在电力系统各个层面和环节都进行安全防护，从供电到终端用户，包括发电、传输和配电等。同时，重点防护针对关键节点、重要设备和敏感

信息进行特别保护，通过风险评估确定薄弱环节并采取针对性措施。全面覆盖与重点防护相结合可以实现系统整体安全和关键资源保护，确保核心功能不受威胁。

- **合规性与法规遵循原则**

遵守相关的法律法规和标准要求，如《中华人民共和国网络安全法》等，并进行必要的合规性审查和整改，确保符合法律法规的要求。

2.5 安全防护挑战

2.5.1 已知威胁挑战

在新型电力系统中，为了对发电、输电、配电、用电进行统一的控制，在各个环节中均存在着大量量测、控制和通信设备。不仅这些设备本身存在一定的风险漏洞，设备间的通信协议也存在一定的风险漏洞，且在数据处理的终端业务系统中也存在一定的风险问题。这些已知的风险漏洞数量大、范围广、交叉作用、相互影响，为安全防护体系的构建造成了巨大挑战。

- **设备漏洞**

设备漏洞长期以来一直是网络安全中不可回避的重点、难点问题。我国信息安全漏洞共享平台(CNVD)发布的数据显示，近十年设备漏洞数量飙升，如图 2-2 所示，新型电力系统中设备漏洞的数量也呈增长趋势。

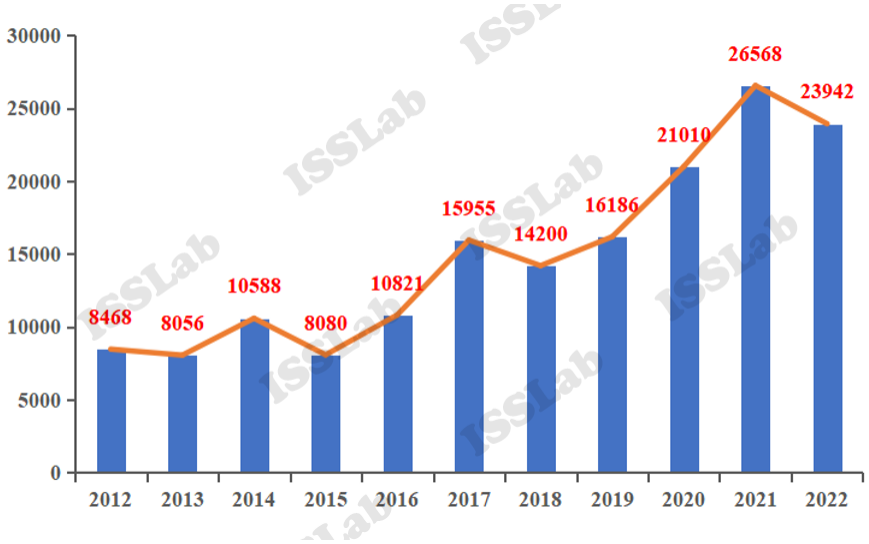

图 2-2 CNVD 公布设备漏洞总数（2012-2022）

经过广泛调研与深度研究，列举部分常见设备漏洞及其影响如表 2-2。

表 2-2 常见电力系统设备漏洞

设备类型	CVE-ID	漏洞描述	受影响产品型号	漏洞评分
发电设备	CVE-2023-29411	该漏洞可能允许更改管理凭据，从而导致潜在的远程代码执行，而无需在 Java RMI 接口上进行事先身份验证。	Schneider Electric APC Easy UPS On-Line 2.3	9.8
电气控制设备	CVE-2022-22725	施耐德数字化保护继电器存在不检查输入大小的缓冲区复制漏洞，当特制数据包通过网络发送到设备时，可能会导致缓冲区溢出，从而导致程序崩溃和任意代码执行。通过 GOOSE 的保护功能和跳闸功能可能会受到影响。	Easergy P3（V30.205 之前的所有版本）	8.8
电气控制设备	CVE-2023-28766	受影响的数字式保护继电器缺乏对托管 Web 服务的 http 请求参数的正确验证。未经身份验证的远程攻击者可能会发送特制的数据包，从而导致目标设备出现拒绝服务情况。	SIPROTEC 5 通信模块 ETH-BD-2FO（所有版本 ＜V9.40）；SIPROTEC 5 Compact 7SX800 (CP050)（所有版本 ＜V9.40）	7.5
通信设备	CVE-2018-0485	思科第二代集成多业务路由器 (ISR G2) 和思科 4451-X 集成多业务路由器 (ISR4451-X) 上的 SM-1T3/E3 固件中的漏洞可能允许未经身份验证的远程攻击者导致 ISR G2 路由器	ISR G2；ISR4451-X	8.6

		或 ISR4451-X 上的 SM-1T3/E3 模块重新加载，导致受影响的设备出现拒绝服务 (DoS) 情况。		
通信设备	**CVE-2021-0285**	QFX5000 系列和 EX4600 系列交换机上的 Juniper Networks Junos OS 中存在不受控制的资源消耗漏洞，允许攻击者发送大量发往设备的合法流量，导致 ICCP 协议通讯中断，从而导致多交换机之间的控制连接不稳定。机箱链路聚合组 (MC-LAG) 节点可能会导致流量丢失。持续接收此数量的流量将造成持续的拒绝服务 (DoS) 情况。	QFX5000 系列和 EX4600 系列交换机	7.5
数据采集设备	**CVE-2021-35533**	Hitachi Energy RTU500 系列的双向通信接口 (BCI) IEC 60870-5-104 功能中的 APDU 解析器中的不正确输入验证漏洞允许攻击者在收到特制的数据时导致启用 BCI 的接收 RTU500 CMU 重新启动信息。默认情况下，BCI IEC 60870-5-104 功能处于禁用状态（未配置）。	Hitachi Energy RTU500 系列 CMU 固件版本 12.0.*（所有版本）；CMU 固件版本 12.2.*（所有版本）；CMU 固件版本 12.4.*（所有版本）	7.5
数据采集设备	**CVE-2022-27480**	受影响的 RTU 设备不需要用户经过身份验证即可访问某些文件。这可能允许未经身份验证的攻击者下载这些文件。	SICAM A8000 CP-8031（所有版本 < V4.80）;SICAM A8000 CP-8050（所有版本 < V4.80）	7.5
数据采集设备	**CVE-2022-43545**	SICAM 系列的多功能测量设备存在未正确验证对端口 855/tcp 上的 Web 界面的请求中的记录类型参数。这可允许经过身份验证的远程攻击者使设备崩溃（然后自动重新启动）或在设备上执行任意代码。	SICAM Q200 (<V2.70) 系列；SICAM P850 (<V3.10)系列	8.8
数据采集设备	**CVE-2023-30901**	SICAM 系列的测量设备的 Web 界面容易受到跨站点请求伪造攻击。通过诱骗经过身份验证的受害者用户单击恶意链接，攻击者可以代表受害者用	SICAM Q200 (<V2.70) 系列	8.8

		户在设备上执行任意操作。		
控制与操作设备	**CVE-2011-5007**	3S CoDeSys 3.4 SP4 Patch 2 和更早版本的 CmpWebServer 组件中基于堆栈的缓冲区溢出，如 ABB AC500 PLC 和可能的其他产品所使用的那样，使远程攻击者可以通过长 URI 到 TCP 端口 8080 执行任意代码。	ABB AC500 PLC	10
控制与操作设备	**CVE-2015-3938**	MELSEC FX3G PLC 设备上的 HTTP 应用程序允许远程攻击者通过长参数导致拒绝服务（设备中断）。	Melsec Fx3g	7.8
控制与操作设备	**CVE-2016-9158**	发送到端口 80 / tcp 的特制数据包可能导致受影响的设备进入缺陷模式。需要冷重启才能恢复系统。	SIMATIC S7-300 CPU 系列包括相关 ET200 CPU 和 SIPLUS 变体）（所有版本）；SIMATIC S7-400 PN/DP V6 及以下 CPU 系列；SIMATIC S7-400 V7 CPU 系列（所有版本）	7.5
控制与操作设备	**CVE-2017-6030**	受影响的产品生成的随机 TCP 初始序列号不够充分，这可能使攻击者可以根据先前的值预测该数字。这可能会使攻击者欺骗或破坏 TCP 连接。	Modicon M221 v.1.1.1.5; Modicon M241 v.0.3.20; Modicon M251 v.0.3.20	6.5
控制与操作设备	**CVE-2018-17924**	未经身份验证的远程威胁参与者可能会向受影响的设备发送 CIP 连接请求，并在成功连接后向受影响的设备发送新的 IP 配置，即使系统中的控制器已设置到硬运行模式。当受影响的设备接受此新的 IP 配置时，设备与系统其余部分之间会发生通信丢失，因为系统流量仍在尝试通过覆盖的 IP 地址与设备进行通信。	MicroLogix 1400; Rockwell 1756 ControlLogix	8.6
控制与操作设备	**CVE-2019-18269**	Omron 的 CS 和 CJ 系列 PLC 存在不受限制的外部访问锁定漏洞。	Omron PLC CJ series, all versions; Omron PLC CS series, all versions	9.8
控制与操作设备	**CVE-2019-10955**	一个开放的重定向漏洞可能允许未经身份验证的远程攻击者输入恶意链接，以将用户重定	MicroLogix 1400 控制器 A 系列、所有版本 B 系列、v15.002 及	6.1

		向到可以在用户计算机上运行或下载任意恶意软件的恶意站点。	更早版本;MicroLogix 1100 控制器 v14.00 及更早版本;CompactLogix 5370 L1 控制器 v30.014 及更早版本;CompactLogix 5370 L2 控制器 v30.014 及更早版本;CompactLogix 在 5370 L3 控制器（包括 CompactLogix GuardLogix 控制器）v30.014 及更早版本中	
控制与操作设备	**CVE-2019-6820**	ATV IMC 中收到特定的以太网帧时，存在缺少关键功能的身份验证漏洞，该漏洞可能导致设备 IP 配置（IP 地址，网络掩码和网关 IP 地址）的修改。	Modicon M100 Modicon M200 Modicon M221 Modicon M241 Modicon M251 Modicon M258	8.2
控制与操作设备	**CVE-2021-22713**	设备存在内存缓冲区范围内的操作限制不当,这可能导致测量仪重新启动。	PowerLogic ION8650、ION8800、ION7650、ION7700/73xx、ION83xx/84xx/85xx/8600	7.5
控制与操作设备	**CVE-2018-1992**	引导加载程序固件存在缓冲区溢出漏洞，如果攻击者能够用一个经过精心构造且足够大的恶意替代品替换初始引导固件映像，就有可能导致引导加载程序在加载该映像时覆盖自己的指令内存并绕过安全启动保护，安装木马等恶意软件	IBM Power 9 OP910、OP920 和 FW910	6.4
控制与操作设备	**CVE-2022-43768**	受影响产品的网络服务器包含漏洞，可能导致资源分配不受限制的情况。攻击者可能会导致受影响产品的网络服务器出现拒绝服务情况。	SIPLUS NET CP 443-1 Advanced（所有版本 < V3.3）；SIPLUS S7-1200 CP 1243-1（所有版本）；SIPLUS S7-1200 CP 1243-1 RAIL（所有版本）；SIPLUS TIM 1531 IRC（所有版本） < V2.3.6)；TIM 1531	7.5

			IRC（所有版本 < V2.3.6）	
服务器设备	**CVE-2022-38138**	对少量未初始化指针的访问，这可能允许攻击者使用受影响的库来瞄准任何客户端或服务器，从而导致拒绝服务情况。	Triangle Microworks IEC 61850 库（任何使用版本号为 11.2.0 或更早版本的 C 语言库的客户端或服务器，以及使用版本号为 5.0.1 或更低版本的 C++、C# 或 Java 语言库的任何客户端或服务器）更早版本）；60870-6 (ICCP/TASE.2) 库（任何使用版本号为 4.4.3 或更早版本的 C++ 语言库的客户端或服务器）	7.5
服务器设备	**CVE-2022-43724**	受影响的软件以明文形式传输内置 SQL 服务器的数据库凭据。结合默认启用的 xp_cmdshell 功能，未经身份验证的远程攻击者可以执行自定义操作系统命令。	SICAM PAS/PQS（所有版本 <V7.0）	8.3
服务器设备	**CVE-2022-29922**	在中处理特制的 IEC 61850 数据包时存在不正确的输入验证漏洞，该数据包具有有效的数据项，但数据类型不正确。该漏洞可能会导致 SYS600 产品的 IEC 61850 OPC 服务器部分出现拒绝服务。	Hitachi Energy MicroSCADA X SYS600、MicroSCADA Pro SYS600 的 IEC 61850 OPC 服务器	7.5
服务器设备	**CVE-2023-28343**	Altenergy 电力系统控制软件，存在安全漏洞，该漏洞是由 /set_timezone 中的操作系统命令注入漏洞引起的。攻击者可以执行任意命令来获取服务器权限。	Altenergy Power Control Software C1.2.5	9.8

为保障电力系统的相对独立性，同时考虑到系统的稳定运行，通常在系统投入运行后很少对系统平台安装任何安全补丁，或不能及时安装安全补丁，导致系统存在被攻击的可能，从而埋下安全隐患。随着时间的推移，以前以安全著称的

Linux 系统目前也暴露出越来越多的漏洞，并且通常由于厂商实力等原因，安全补丁晚于 Windows 平台发布，操作系统层面漏洞越来越明显。

- **协议安全**

新型电力系统结构复杂，不同设备间的通信往往需要专属的通信协议。如 Modbus、Ethernet/IP、OPC、DNP3、Profinet、GOOSE、IEEE C37.118 等。

(1) Modbus 协议

一种简单、可靠且易于实施的协议，用于不同设备之间的通信和数据交换。Modbus 协议可以通过串口（如 RS-232、RS-485）或以太网（如 TCP/IP）进行通信，使用二进制编码传输不同类型的数据、地址寻址不同设备和寄存器、功能码标识请求的操作类型。Modbus 协议的格式如图 2-3 所示。其安全风险如下：

功能	描述	功能	描述
01	读取卷状态	07	读取异常状态
02	读取输入状态	08	诊断
03	读取多个保持寄存器	11	读取通信事件计数器(仅串口)
04	读取输入寄存器	12	读取通信事件日志(仅串口)
05	写入单个卷	14	读取设备标识
06	写入单个保持寄存器	··	···

图 2-3 Modbus 协议格式

缺乏身份验证和加密：传统的控制系统被认为是独立于网络空间的孤岛系统，使得串行 Modbus 协议在设计上没有设计身份验证、访问控制以及加密机制，导致攻击者可以轻易地窃取或篡改通信数据。

易受网络攻击：基于 Modbus 协议发展出来的 Modbus TCP 协议建立在

TCP/IP 协议栈上，其远程访问安全机制完全依赖于 TCP/IP 协议，使得网络空间的安全问题也会波及工业控制系统，如端口扫描、拒绝服务攻击、中间人攻击等。缺乏数据完整性和消息验证机制，使得攻击者可以伪造或篡改传输消息，导致非法操作、错误数据注入或拒绝服务的情况发生[18]。

(2) Ethernet/IP 协议

一种广泛的、全面的、可认证的应用层协议，可用于各种自动化设备。在电力系统中被广泛用于电力监控与控制，连接电力监控系统、SCADA 系统和 PLC 设备，实现对电力系统的实时监控和控制，还可用于智能电表、智能变压器和分布式能源设备与监控系统的通信，其协议格式如图 2-4 所示。其安全风险如下：

Ethernet/IP 采用 CIP 应用层协议规范，同时使用 TCP/IP 技术来传送 CIP 通信包，使其面临两者带来的风险[19]。CIP 规范没有定义任何显式或隐式的安全机制，存在极大的安全风险。在工业生产环境下，使用通用工业协议必须对通信对象进行设备标识，使得攻击者可轻易进行设备识别和枚举。当 Ethernet/IP 与 UDP 相结合时，由于两者都缺乏控制机制，因此，攻击者易于注入伪造数据或注入 IGMP 控制报文操纵传输。

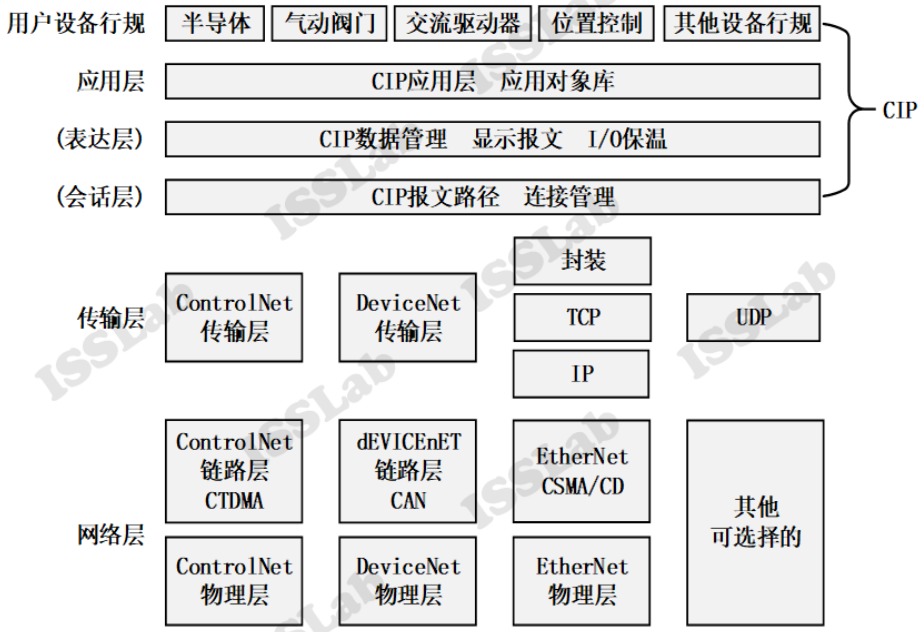

图 2-4 Ethernet/IP 协议格式

未经授权的访问：攻击者可通过枚举设备标识的方式未经授权地访问网络中的 Ethernet/IP 设备，从而可以获取敏感信息、修改关键配置或执行非法操作，干扰系统正常运行。

数据篡改和劫持：攻击者可以篡改 Ethernet/IP 通信中的数据包，注入伪造的错误数据，修改控制指令或传感器数据，导致误操作、系统故障或安全事故。

(3) OPC 协议

用于连接各种设备，如传感器、监测仪表、PLC、SCADA 系统等。通过 OPC 协议，电力系统可以实现实时数据采集、监测和控制，支持故障诊断、状态监视、能源管理等应用。同时，OPC 协议提供了标准化的接口和数据模型，使得不同设备和系统能够互操作，加快了系统的集成和部署过程[20]。其安全风险如下：

服务拒绝攻击：通过发送大量无效请求或恶意数据包，攻击者可以导致 OPC 服务器过载，从而使系统的可用性受到影响。

数据篡改和劫持：攻击者可能篡改 OPC 通信中的数据，修改控制指令或传感器数据，导致误操作、系统故障或安全事故。

(4) DNP3 协议

一种用于远程监控和控制的通信协议，主要用于电力系统的监控、自动化和数据采集。DNP3 协议支持对分布式设备（如遥测终端单元、遥控终端单元等）进行实时数据采集、状态监测和远程控制。通过 DNP3 协议，电力系统可以实现对电压、电流、频率等参数的监测，实时数据传输和历史数据记录，以及远程控制和事件报告等功能。其安全风险如下：

数据篡改和劫持：攻击者可以篡改 DNP3 通信中的数据包，修改测量值、控制命令或状态信息，导致误操作、系统故障或安全事故。

服务拒绝攻击：攻击者可能通过发送大量无效的请求或恶意数据包，导致 DNP3 设备或网络过载，造成系统的不可用和性能下降。

(5) Profinet 协议

截至 2017 年，Profinet 协议占所有工业网络市场份额的 11%，被称为业界使用最多的协议，大约 2000 万台设备基于该协议进行通信。该协议基于中心站和分散式设备的供应者/消费者通信模型，设备交互模型如图 2-5 所示，其中供应者向消费者提供过程数据。由于 Profinet 协议是基于以太网标准，因此在与集成其他协议的设备共享同一物理介质方面有许多优势，但是这种特性也给它带来了许多风险因素。其安全风险如下：

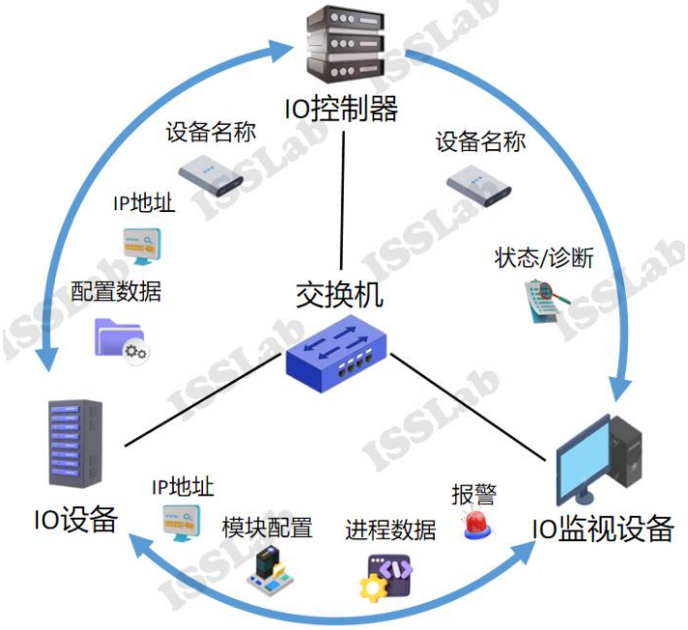

图 2-5 Profinet 设备交互模型

中间人攻击：攻击者通过发送一个带有伪造以太网报头的帧，并在该帧中构造受害设备的 MAC 地址作为源地址，交换机重新配置其内部路由表，从而发送到受害设备的帧将由攻击者接受，这种攻击方式又被称为中间人攻击。

拒绝服务攻击：攻击者通过伪造的 DCP 标识响应来干扰 IP 地址分配的阶段，如果欺骗帧在 DCP 超时之前到达 IOController 就会导致错误，因为这样作为响应标准的符号设备名称不再唯一。

(6) GOOSE 协议

GOOSE 协议又名通用面向对象变电站事件协议，是国际电工委员会 IEC 61850 标准套件的一部分，其中规定了变电站事件的通信方式。GOOSE 是存在于数据链路中的多播协议，通常部署于光纤或屏蔽双绞线电缆。该协议的通信机制采用订阅者/发布者模式。

由于 GOOSE 协议使用数据链路层进行多播，因此没有逻辑地址和流控制能力，也没有消息和身份验证机制，且由于 GOOSE 消息对时间性能要求严格，因

此影响传输速率的安全原则在 GOOSE 中并不被接受。其安全风险如下：

挟持和拒绝服务风险：GOOSE 协议中的状态号机制会使得设备不处于状态号低于先前接受消息的 GOOSE 帧，因此，可以构造恶意的 GOOSE 消息，挟持订阅者和发布者之间的通信，并且阻止订阅者处理后续的 GOOSE 消息或者强制其处理伪造的 GOOSE 消息。这种情况常出现于合法的 GOOSE 消息的状态号小于或等于伪造消息中的状态号，这种攻击方式被称为 GOOSE 中毒。

常见协议脆弱性及风险分析如表 2-3 所示。

表 2-3 常见协议漏洞

协议名称	脆弱性	攻击风险
Modbus	缺乏认证机制、缺乏权限区分、数据明文传输、缺乏广播抑制（串行 Modbus）	敏感信息识别、信息欺骗、洪泛攻击、重放攻击
Ethernet/IP	加密、认证机制缺陷、完整性验证缺陷	伪造数据攻击、中间人攻击
OPC	过时授权服务、RPC 漏洞、多余端口服务	拒绝服务攻击、远程代码执行
DNP3	数据帧完整性、授权机制不足	中间人、重放、窃听、数据篡改、拒绝服务、缓冲区溢出
Profinet	授权、加密、认证缺陷	控制进程数据、读取设备状态
GOOSE	状态号机制存在被利用的可能	挟持、拒绝服务攻击

- **业务问题**

新型电力系统业务系统庞大，如信息采集与监控系统、能源管理系统、发电调度与运行系统、数据管理与分析系统、人力资源系统、财务报表系统等。各业务系统功能的正常使用依赖于原始数据的正确采集、数据分析模型的稳定性与鲁

棒性、业务系统之间数据交互的规范与统一。然而，由于新型电力系统网络深度融合，多源异构数据采集的不确定性、数据网络传输的不安全性、业务计算模型的不可信性、人工智能应用的不确定性使得业务系统存在脆弱性，甚至导致业务功能丧失，如表 2-4 中所示。

表 2-4 业务系统脆弱性分析

影响	说明
基础设施损坏	攻击者通过网络攻击操纵电力系统物理设备，如传感器、发电机、变压器等，导致设备损坏或运行异常。导致设备无法正常工作，甚至可能导致整个电力系统运行中断。
经济损失	攻击可能破坏发电调度与运行系统，导致无法进行有效的负载平衡和优化，增加供需不匹配的风险，造成的业务中断、市场交易无法实现、电费计量错误等问题。
拒绝控制	网络攻击可能导致业务系统的控制权被恶意攻击者获取，从而使其能够远程操纵电力设备和系统，锁定物理设备或加密系统软件，致使控制失效。
功能丧失	攻击导致业务系统的关键功能无法正常运行，例如能源管理系统、发电调度与运行系统等，从而影响负载平衡、能源需求预测、市场交易和电网稳定性管理等业务活动，进而影响整个电力系统的运行。
信息窃取	攻击者获取敏感的电力系统数据，如能源需求预测、电力市场交易信息等，用于非法目的，如竞争对手的利益损害、市场操纵或勒索等。
数据篡改	网络攻击可能导致电力系统中的数据被恶意篡改，如能源需求数据、发电量数据等。导致不准确的数据分析和决策，进而影响能源生产和供应链的计划和运营。
服务中断	网络攻击导致业务系统的服务中断，使得用户无法进行关键操作和访问系统功能。例如，信息采集与监控系统无法实时监测设备状态、能源管理系统无法对消费者进行实时需求响应等。
可靠性下降	网络攻击可能导致电力系统的可靠性下降，引发设备故障、停电或

	事故等安全风险。攻击可能使设备运行在异常状态下，增加设备的负荷、磨损和损坏的风险。
市场不稳定性	网络攻击可能对电力市场产生影响，例如通过操纵能源需求或市场交易数据来扰乱市场供需平衡。导致价格波动、市场失真和市场参与者的经济损失。
AI 模型鲁棒性缺乏	攻击者可能通过对输入样本添加微小的异常扰动，使模型输出错误的预测结果。这可能导致业务系统基于错误的数据做出错误的决策，从而影响电力系统的运行和安全。

2.5.2 未知威胁防护挑战

- **外部设备接入**

针对新型电力系统的外部设备接入是指攻击者利用外部设备接入电网并对其发起攻击。如外接智能电表，进行偷电窃电；外接网络设备，进行数据窃取篡改；外接控制设备，进行恶意操作等。

攻击流程：(1) 攻击者获取合法的外部设备，如控制器；(2) 攻击者修改外部设备上的软件，注入恶意程序；(3) 攻击者通过合法渠道将恶意外部设备接入新型电力系统；(4) 恶意外部设备接入成功，攻击者利用恶意软件执行攻击指令。攻击方式如干扰供电稳定、破坏设备及网络、窃取敏感信息、对电力分配恶意操纵；(5) 撤除恶意设备，掩盖攻击痕迹。

防护挑战：(1) 新型电力系统设备多，网络复杂，对于新接入的设备难以及时发现、定位及跟踪；(2) 外接未知设备，意味着安全漏洞知识库中难以查到对应设备的型号及安全漏洞，难以提前部署安全防护策略；(3) 外接设备由攻击者掌控，可绕过部分身份认证及权限控制系统。

- **信息物理协同攻击**

单一的物理攻击，如物理破坏电力系统设备、切断输电线路等攻击方式成本高并且容易被系统检出；单一的信息攻击，如拒绝服务攻击、恶意软件勒索等攻击方式实现难度高，攻击收益低。通过融合物理空间与信息空间双重知识，构建“系统接入-数据伪造-控制篡改”的攻击链，制定符合物理规律的隐蔽性信息物理协同攻击，以逃避异常数据检测机制；利用低威胁的网络攻击隐藏真实的物理攻击，传播攻击效果。

攻击流程：可根据部分输电线路断开后线路两端注入功率的变化，基于线路功率对节点注入功率的灵敏度矩阵，计算发生故障后其余线路的潮流变化，以此设计造成大面积线路过载的攻击方案，造成大范围线路中断。另外，可根据部分负载节点用电突变，基于安全经济调度，计算发电节点功率变化和线路潮流变化，以此设计针对发电成本或社会效益的电力市场攻击方案。

防护挑战: (1)广域测量系统和 SCADA 系统采集的多源异构数据导致传统的状态估计系统难以识别精心设计的隐蔽性信息物理协同攻击；(2) 提高针对隐蔽性信息物理协同攻击检测准确性和鲁棒性，目前尚无好的方法和技术；(3) 确保测量数据的完整性和真实性是防护的关键。现有的数据验证机制尚存在漏洞，需要进一步加强和改进；(4) 在隐蔽性信息物理协同攻击检测过程中，需要平衡鲁棒性和计算效率。检测算法需要具备足够的鲁棒性来应对各种攻击，同时保持较高的计算效率以适应实时性要求。

- **安全策略和管理流程问题**

在新型电力系统中，安全策略和管理流程的重要性不可低估。随着能源网络

的数字化和智能化程度不断提升，有效的安全策略和管理流程可以确保电力系统的稳定运行，保护关键设施和数据免受恶意攻击和故障的影响。目前尚存在一些问题，如(1) 网络安全组织体系、责任体系需进一步健全；(2) 网络安全运行体系和应急机制仍需完善；(3) 网络安全全生命周期管控需进一步强化；(4) 电厂和新能源厂站等涉网单位存在诸多薄弱环节；(5) 常态化渗透测试与实战攻防对抗力度不足；(6) 内外部网络安全支撑需进一步强化。

03

新型电力系统主动防御技术体系

3.1 信息系统安全防御技术体系

PDR 防御技术体系是最早体现主动防御思想的一种网络安全模型。PDR 模型是建立在基于时间的安全理论基础之上的，包括 protection（保护）、detection（检测）、response（响应）三个过程，是一个可量化、可数学证明的安全模型[21]。由于信息安全相关的所有活动，无论是攻击行为、防护行为、检测行为还是响应行为，都要消耗时间，因而可以用时间尺度来衡量一个体系的能力和安全性。在 PDR 模型的基础上，美国国际互联网安全系统公司 ISS 将其优化为循环式 PDR 模型，即 P2DR 模型，也称可适应网络安全模型。该模型包含 4 个主要部分：policy（安全策略）、protection（防护）、detection（检测）和 response（响应）[22]。在整体安全策略的指导下，通过部署安全防护措施对风险进行及时处置，并对处置过程中的经验进行总结，从而保证防护、检测和响应组成了动态安全循环。

在 P2DR 模型的基础上，进一步将恢复环节提升到与防护、检测和响应等环节同等重要的程度，提出了 PPDRR 模型，也称为 P2DR2 模型。该模型是在整体安全策略的控制和指导下，综合运用防护工具和检测工具的同时，通过适当的响应策略将系统调整到“最安全”和“风险最低”的状态。该模型能够被用来解决业务连续性要求很高的系统安全防护问题[23]。

APPDRR 模型作为进一步发挥主动防御思想的网络安全模型，它认为网络

安全模型的第一个重要环节是风险评估，通过风险评估，掌握网络安全面临的风险信息，进而采取必要的处置措施，使得网络安全水平呈现动态螺旋上升的趋势。第二个重要环节是安全策略，一方面，安全策略应当随着风险评估的结果和安全需求的变化做相应的更新；另一方面，安全策略在整个网络安全工作中处于原则性的指导地位，其后的检测、响应诸环节都应在安全策略的基础上展开。系统防护是安全模型中的第三个环节，体现了网络安全的静态防护措施。接下来是动态检测、实时响应、灾难恢复三环节，体现了安全动态防护和安全入侵、安全威胁“短兵相接”的对抗性特征[24]。

本白皮书提出的新型电力系统主动防御技术体系如图3-1所示，从防御模型、方法技术、防御体系、影响分析四个角度进行体系构建。

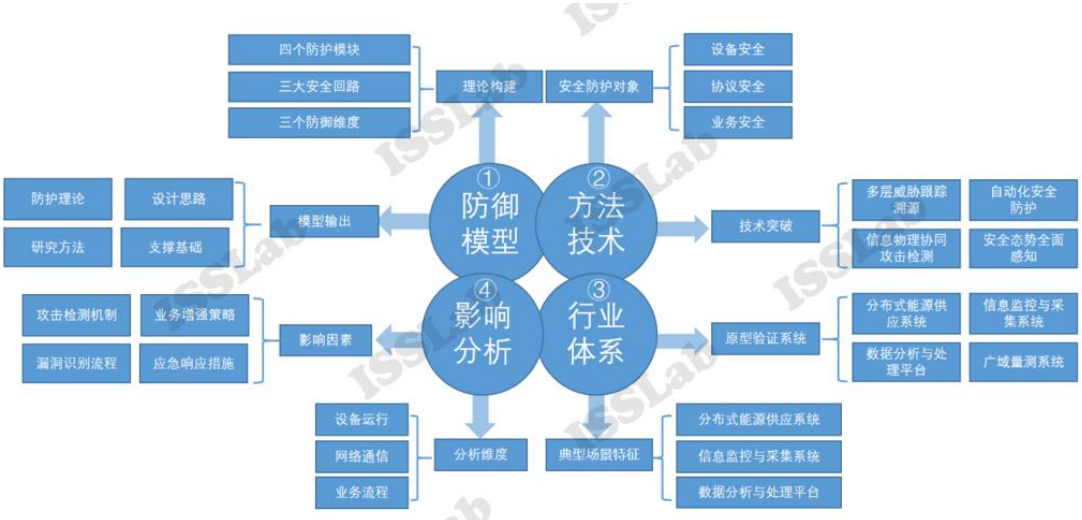

图 3-1 新型电力系统 IPDR 主动防御技术体系

防御模型：IPDR 一体化新型电力系统安全主动防御模型，主要包括四个防护模块、三大安全回路、三项防御维度。

方法技术：针对电力系统设备、协议、业务三类安全防护对象，防御技术体系分别从控制器分析与测试、操作系统本体安全防护、安全态势全面感知、多层威胁跟踪溯源等方面进行方法技术总结。

防御体系：融合新型电力系统典型场景特征，考虑设备、协议、业务三个维度，构建了电力行业典型场景下的主动防御技术体系，并设计了新型电力系统安全态势感知原型系统。

影响分析：考虑攻击检测机制、本体增强策略、漏洞识别流程、应急响应措施等多种影响因素，从设备运行、网络通信、业务流程等多维度出发，设计了安全保护技术对新型电力系统功能流程与性能指标的影响分析方法。

3.2 IPDR 一体化主动防御模型

针对新型电力系统网络安全风险和安全防护需求，本白皮书提出“识别(**I**dentification)-保护(**P**rotection)-检测(**D**etection)-响应(**R**esponse)”一体化的新型电力系统主动防御模型 **IPDR**。IPDR 体系包括四大安全模块：风险**识别**、系统**保护**、入侵**检测**、实时**响应**。信息物理融合新型电力系统 IPDR 主动防御模型针对分布式发电、长距离输电、智能配电、广域量测等电力行业关键技术，通过对电力系统中潜在安全风险进行识别，建立安全基线与漏洞知识库，进行风险等级划分并制定相应预案，通过自动化、智能化的系统防护机制，探寻新型入侵检测技术，以保证系统出现入侵攻击或漏洞时，可以对安全威胁进行实时响应处置，并启动相应的保护方案与防护设备，从而实现对电力系统中设备层、网络层、控制层以及业务层关键场景全覆盖，具备应对全场景的未知安全威胁的防护能力，新型电力系统 IPDR 主动防御模型如图 3-2 所示。

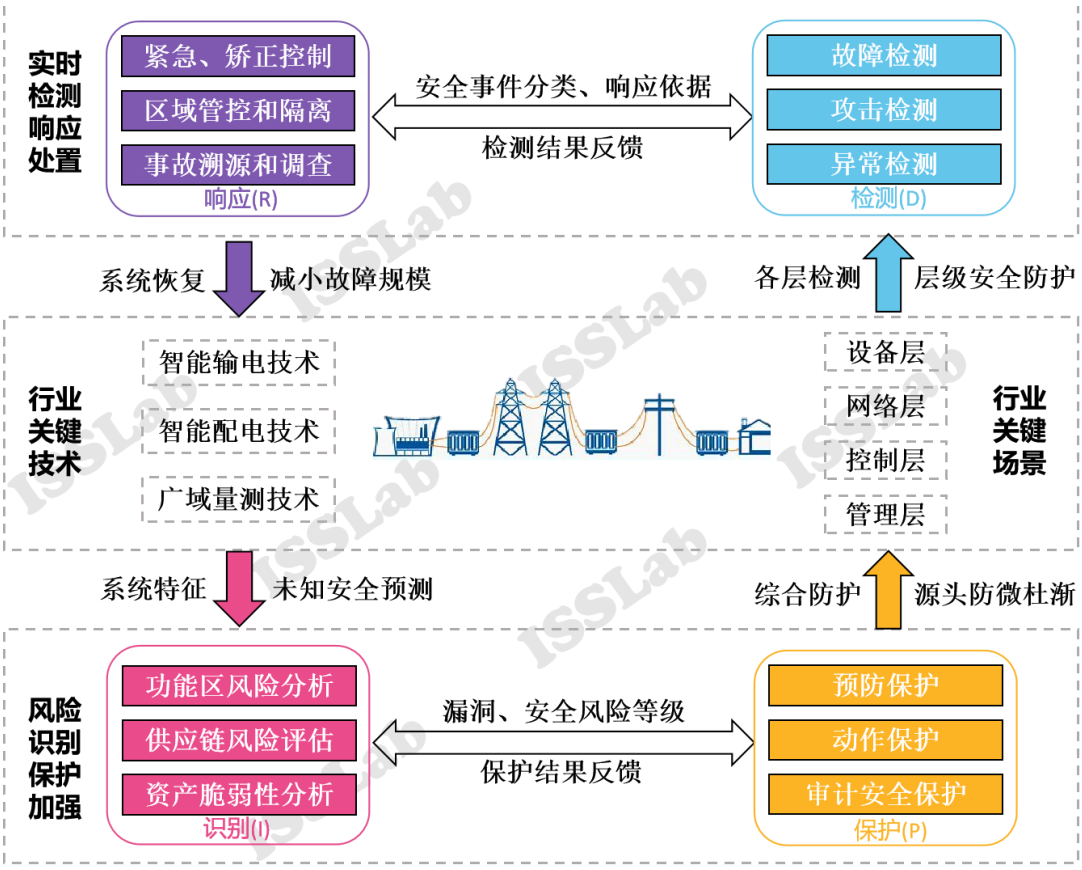

图 3-2 新型电力系统 IPDR 主动防御模型

3.2.1 风险识别

基于新型电力系统网络及其安全风险分析，结合新型电力系统已知威胁，规划风险识别方案。在设计时考虑到潜在的安全风险及系统脆弱性，从源头增强系统的鲁棒性，加强系统的抗安全风险能力；针对电力网络中的物理设备，信息网络中的通信设备、通信协议、业务系统，对安全风险进行细化，针对细分的安全风险设计出识别方法，为系统的响应与保护提供可靠的识别结果。

针对已识别出的风险，以等级保护标准规范为基础，结合新型电力系统的特点，建立适合于新型电力系统的安全基线库及漏洞库，为风险威胁识别提供知识库支撑。

3.2.2 系统保护

通过研究针对局部攻击与分布式攻击的弹性安全控制理论以及基于加密机制的主动防御安全技术，构建新型电力系统安全加固回路，实现信息物理融合攻击下的有效应对与防护。

实现新型电力系统安全保护能力在线评估。改变现有基于人工方式的等级保护安全测评方式，利用技术手段，实现设备加固自动化、协议增强智能化、业务修正常态化。针对识别出的设备风险，自动更新和修复设备漏洞，采取密码学技术加强设备认证和访问控制，实施定期的设备安全检查与维护；针对识别出的协议风险，智能增强通信协议安全，采用安全加密技术确保通信过程中数据的完整性、机密性；针对识别出的业务风险，增强业务系统算法鲁棒性，定期更新安全补丁，修复已知漏洞；通过人工智能建立安全模型以及权限分离的模式，实现海量数据的安全审计以及配置管理的多权分离日志审计和报警功能，从多个维度实现对电力物理、信息系统的保护。

3.2.3 入侵检测

构建新型电力系统多维度融合的入侵检测体系。针对“设备—协议—业务”多维度的入侵攻击，单一的物理空间安全保护技术或信息空间异常检测技术已不足以应对跨越信息物理空间的新型电力系统攻击行为。新型电力系统入侵检测体系需融合信息流、物质流、能量流等多维工程特征，针对“系统接入—数据伪造—控制篡改”的攻击链，增强电力系统安全检测能力，实现系统异常的快速准确发现。

通过设计网络边界入侵检测、信息管理网络攻击检测以及电力生产网络攻击

检测方法，并结合智能学习建立电力网络环境的通信和行为模式，及时发现针对电力系统的入侵行为，实现不同网络的全面入侵攻击检测，从而针对不同的攻击事件和安全风险，实现对整个网络系统的安全保护。

3.2.4 实时响应

提升新型电力系统信息安全预警及响应能力。通过关联分析、异常分析、行为分析等技术，结合安全基线、电力系统软硬件漏洞库、威胁情报，实现对新型电力系统全局的脆弱性评估、风险分析与威胁预警，实现新型电力系统信息安全可视化。对于新型电力系统异常访问，实现根据预定义规则在网络层面动态阻断。

基于新型电力系统网络安全态势感知平台，充分利用大数据分析及预测技术，大幅提高安全事件监测预警能力，提升动态防御及快速响应能力，保障电力监控系统安全稳定运行。

3.3 新型电力系统 IPDR 关键技术

3.3.1 风险威胁识别关键技术

- **风险规划技术**

电网的规划在整个电力系统的电网建设中占有重要的地位，电网合理的布局、优化的结构及设备的合理选用，是保证一个供电区域乃至整个国家电网的安全稳定、供电可靠和降低损耗的基础。

电网规划是根据规划期间的负荷预测结果来进行电源等供电设备的新增，以及将这些设备形成更好的供电结构，以满足电力需求。规划建设研究内容为资料收集、负荷预测、确定规划方案以及成果分析四个阶段。负荷预测和电网 N-1 静

态安全约束式电网规划的重要基础，负荷预测技术和 N-1 安全校验技术如表 3-1 和表 3-2 所示。

表 3-1 负荷预测技术

负荷预测技术	简介
趋势外推法	通过研究负荷的历史趋势，利用适当的数学模型对未来负荷变化进行预测的方法。
时间序列法	将预测值及其相关因素视为随机变量，利用历史负荷值作为自变量，构建随机过程模型来预测未来的负荷值。
灰色模型	适用于小样本、高预测精度的电力负荷预测，通过将负荷数据视为变化的灰色量，采用各种数据产生方法整理数据，构建灰色模型进行预测。

表 3-2 N-1 安全校验技术

N-1 安全校验技术	简介
支路开断模拟	对基本运行状态的电力系统，通过支路开断后的潮流计算来分析系统的安全性，成熟的方法有直流法、补偿法和灵敏度法。
发电机开断模拟	通常采用的方法有：直流法、发电量转移分布系数法、广义发电量分布系数法、计及系统频率特性的一类方法。

- **风险细化技术**

根据电力网络与信息网络的特点，将风险细化为物理安全风险和信息安全风险。针对信息网络的特有结构，从设备风险、协议风险、业务风险的角度分别制定风险管理方案。另外，通过将整个电力系统进行细化，根据分层控制模式，针对不同等级的调度控制中心，实行不同的风险细化规则。

- **控制器脆弱性分析识别框架**

基于完整的电力系统控制器安全分析架构，在访问控制机制、安全通信缺陷及逻辑程序风险三个方面，从以攻带防的视角，突破控制器脆弱性分析与测试难题。该脆弱性分析识别框架可分析西门子、罗克韦尔、施耐德等全球排名前十的工控厂牌，二十多款工业控制器。

访问控制机制脆弱性：访问认证过程在上位机软件上进行，攻击者可篡改软件程序流程，无需凭证即可控制 PLC，如表 3-3 所示。

表 3-3 访问控制机制脆弱性示例

厂商	型号	认证相关漏洞			
		弱口令传输	CVE	认证绕过	CVE
Rockwell	Micrologix ***	√	CVE-2020-****	connection password	CVE-2020-****
Schneider	M***	Hash	N/A	connection password	CVE-2019-****
	M***	Hash	N/A	connection password	CVE-2019-****
GE	RX**	√	N/A	X	–
WAGO	PFC***	√	N/A	X	–
Nandaauto	NA***	Hash	N/A	connection password	CNVD-2019-*****
	NA***	Hash	N/A	connection password	CNVD-2019-*****
Hollysys	LK***	√	N/A	7	–
	LK***	√	N/A	7	–
	FM***	√	N/A	No password	N/A
Triconex	MP***	√	N/A	connection password	CNVD-2019-*****
Supcon	J**0	X	N/A	protect pass	–
Mitsubishi	R***CPU	√	N/A	remote operation password	CVE-2020-****

安全通信缺陷：缺少加密、校验码、时间戳等安全通信机制，攻击者可通过重放攻击掌握 PLC 控制权，如表 3-4 所示。

表 3-4 安全通信缺陷示例

协议	攻击向量		
	嗅探	欺骗	错误数据注入
GE-SRTP	√	√	√
M241-Codesys v3	√	√	√
M258-Codesys v3	√	√	√
M340-Modbus	√	√	√
M580-Modbus	√	√	√
MelSoft	√	√	√
Hollysis-Codesys v2	√	√	√
S7comm	√	√	√
S7comm-plus P3	√	x	x
PCCC	√	√	√
PCCC-plus	√	x	x
WAGO-Codesys v2	√	√	√
ABB-Codesys v2	√	√	√
Haiwell self-owned	√	√	√
NA300 self-owned	√	√	√
NA400 self-owned	√	√	√
TRISTATION	√	√	√
FINS	√	√	√

逻辑程序风险：工程文件权限高，攻击者可通过逻辑炸弹耗尽系统计算资源进行 Dos 攻击，如表 3-5 所示。

表 3-5 逻辑程序风险示例

厂商	型号	检验	Dead-loop
Naauto	N****00	monitoring	DoS (High CPU)
	N****400	monitoring	halt
Sins	CPU****	monitoring	halt
	CP****17c	monitoring	halt
	CP********11-1	compile-time	halt
Roell	ControlLogi****61	monitoring	halt
	Micrologi****00	monitoring	halt
Sider	M****8	monitoring	halt
	M****1	monitoring	halt
	M****8	monitoring	halt
	m****0	monitoring	halt
	M****0	monitoring	halt
GE	R****3i	x	DoS
WO	PF****00	monitoring	halt
****y****ys	L****07	monitoring	reboot
	L****10	monitoring	reboot
	F****802	monitoring	reboot
****nex	M****008	compile-time	N/A

- 基于程序分析的工控协议逆向方法

基于程序分析的工控协议逆向方法由程序分析模块和日志分析模块组成，其中，程序分析模块使用动态污点分析记录报文数据在函数上下文中的调用情况；设计了污点初始化、污点传播方法；设计了日志记录系统，用于后续日志分析。日志分析模根据函数上下文恢复协议字段树；根据指令特征判断特殊字段语义。如图 3-3 所示。

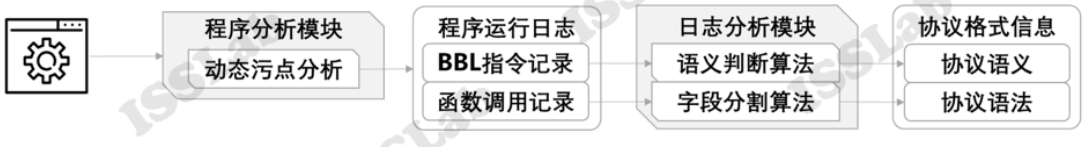

图 3-3 基于程序分析的工控协议逆向方法

- **序列模式挖掘与聚类分析**

序列模式挖掘与聚类分析相结合的技术是漏洞库构建过程中常用的关键技术[25]。将收集的漏洞信息采用频繁序列模式挖掘算法，得到频繁漏洞序列库，表示发生频率在一定比率上的漏洞信息序列。再采用聚类分析技术，将得到的大量的频繁序列进行聚类分组，得到簇状频繁序列漏洞库，相近的聚类被分到同一个簇中，有助于定位漏洞信息的发生的可能范围。一个属性完备，划分明确的漏洞库是高效精准定位漏洞信息的基石。

- **无损漏洞扫描技术**

采用 Nessus、Appscan、Whatweb 等工具进行无损漏洞扫描，其支持主机扫描、Web 扫描和自定义漏洞扫描等功能。主机扫描主要包含主机的基本信息、端口与服务、漏洞信息和口令猜测。Web 扫描主要包括基本信息、端口与服务、子域名、敏感信息泄露、SQL 注入和 XSS 跨站漏洞。新增漏洞需及时提交至漏洞库，保持漏洞库定期更新[26]。

针对设备漏洞挖掘技术，过往研究中 CCS 2017 提出了一种基于马尔可夫链模型的灰盒测试技术，该技术利用代码插装技术，通过建立马尔可夫链模型来指导种子测试用例选择和变异策略，并在此基础上开发了一款 AFLFast 测试工具，大大提高了 AFL 测试工具的测试效率，并据此发现了超过 40 个漏洞[27]。过往研究完善了一个结合了多种二进制分析技术的二进制分析框架，并开源了这个二进制分析框架 angr。该框架支持二进制分析中常用的技术包括污点分析、符号执行、基于符号执行的模糊测试、约束求解器等[28]。 2013 年 Drew Davidson 提出工具 FIE[29]，这是一种基于符号执行的方法，先通过对固件源码进行编译，然后提供模块化的方法，指定外围设备到内存的映射区域和中断响应时间，完成对 MSP430 系列的 16bit 微处理器的固件代码进行审计。过往研究提出一种跨平台的固件漏洞关联算法，对函数间调用图、函数内控制流图、函数基本信息进行特征选择和数值化处理，并采用神经网络计算待匹配函数对的相似程度，在此基础上采用结构化匹配方法进一步提高匹配精度。过往研究结合了符号执行技术和模糊测试技术，实现了一款漏洞挖掘工具 Driller，这个工具通过动态符号执行对程序的深入分析，以此来对输入变量进行合适的突变，生成相应的输入测试，进而触发 Fuzzing 之前无法探测到的代码部分，然后再通过 Fuzzing 组件进入该代码部分继续执行，缓解了模糊测试技术中的效率低、覆盖率低等弱点，使用符号执行技术主要用来搜索深层次的路径信息，能够挖掘更深层次的漏洞。过往研究提出了一种基于污点分析的自动化检测技术，先给不信任的输入（如网络数据流）做标记，然后随着程序的执行，通过跟踪污点数据的扩散范围，该方法可以检测到写覆盖如覆盖了函数的返回地址攻击，并能自动化生成漏洞的详细信息。

- **基于日志数据的风险评估方法**

从用户行为及企业规范中中提取用户危险行为清单，根据危险行为清单从网络安全设备用户日志等数据中提取用户危险行为特征，根据用户危险行为特征训练用户各危险行为上的高斯混合模型，并得到用户风险分级概率集，基于证据融合理论设计用户风险分级概率融合方法，并根据用户的风险概率融合结果决定用户是否存在行为异常风险[30]。

- **基于攻击图的网络脆弱性分析技术**

针对新型电力系统通信网络的风险威胁识别可采用基于攻击图的网络脆弱性分析模型[31],如图 3-4 所示，其由攻击图构建和网络脆弱性分析两部分组成。

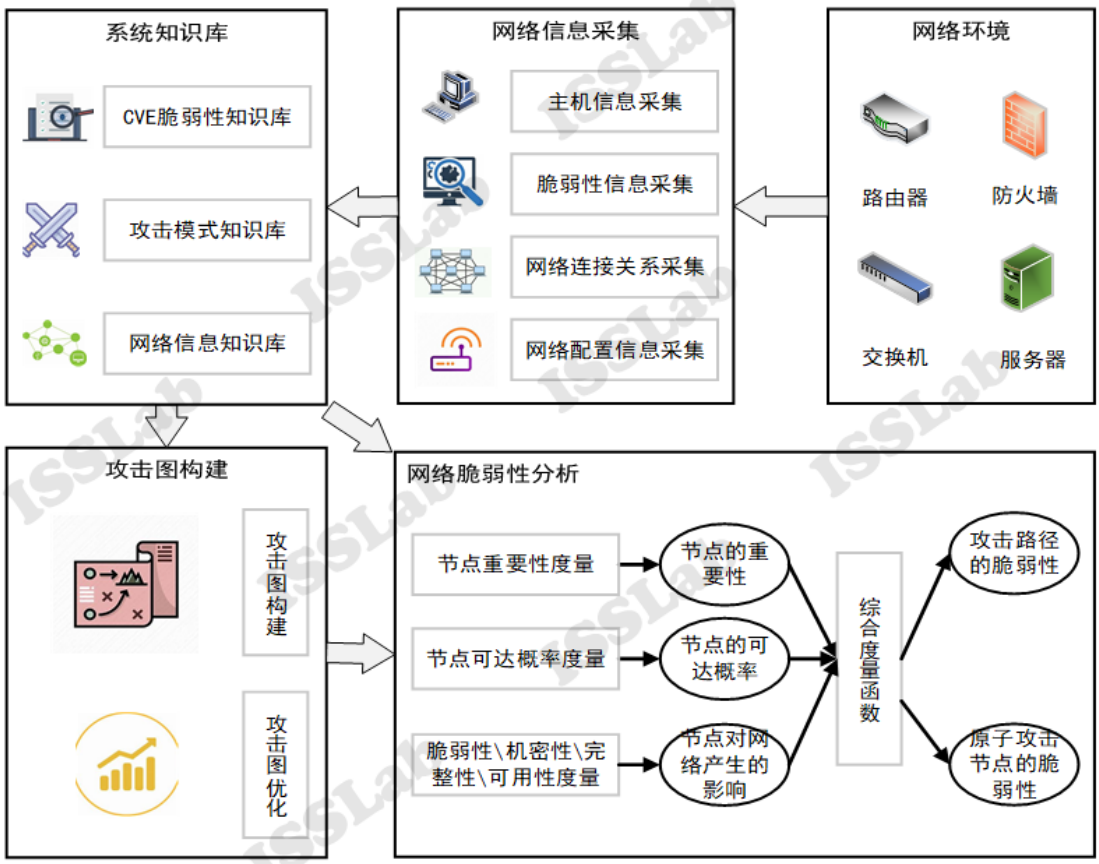

图 3-4 基于攻击图的网络脆弱性分析模型

根据新型电力系统网络信息和攻击者信息进行建模，利用攻击图构建算法生成攻击路径，采用最大跳数和最低可达概率作为限制策略，减小攻击图的生成规模。网络脆弱性分析部分以生成的攻击图为分析平台，分别计算节点的重要性、

节点的可达概率和节点对网络产生的影响，基于这三个评估指标，利用综合度量函数，可以分别计算出单个节点以及所有攻击路径的脆弱性，便于后续安全管理者进行系统安全管理。

- **基于人工智能的系统脆弱性分析技术**

无监督学习算法可对电力系统中的相关数据进行训练和分析，以识别系统中的异常行为、攻击模式或安全漏洞[32]。强化学习算法可以模拟攻击者的行为并进行系统的渗透测试，以评估系统对不同攻击的防御能力，并提供相应的加固建议。

3.3.2 系统安全保护技术

- **操作系统国产化**

电力系统是国家的关键基础设施，是保障国家能源安全的重要部分。电力设备操作系统国产化可以避免国外操作系统存在的安全风险，保障国家能源安全。通过国产化操作系统，可以根据国内电力系统的特点和需求，定制化开发安全策略和机制，更好地适应本地电力系统架构、通信协议和数据传输方式，提供更高的安全性能和可靠性，基于国产处理器的硬件安全扩展如图 3-5 所示。

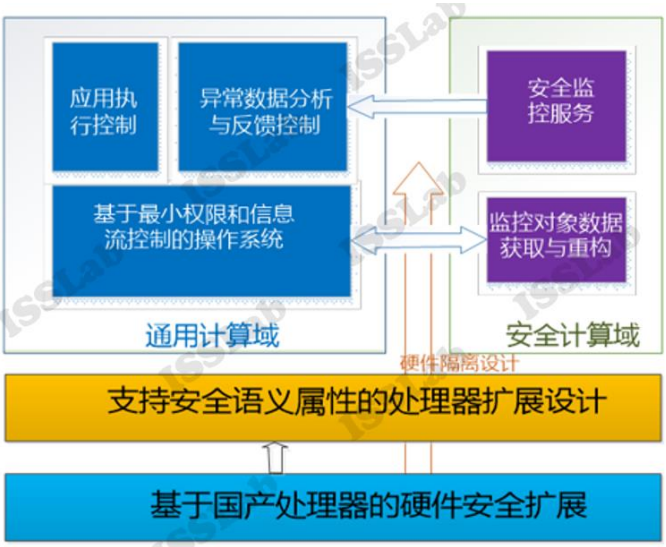

图 3-5 基于国产处理器的硬件安全扩展

在加密和认证算法方面，我国提出了中国密码算法标准，用于保护国家重要信息系统和数据安全，如：SM1 是基于对称密钥的分组密码算法，可用于数据加密、数据解密和数字签名等安全应用；SM2 是基于椭圆曲线密码学的数字签名算法，可用于生成和验证数字签名，实现数据完整性和身份认证。SM3 是基于哈希函数的密码算法，可用于数据完整性校验、数字签名和随机数生成等安全应用；SM9 算法是基于椭圆曲线密码体制的算法，可以用于数字签名、加密和解密等安全应用。国密算法是国家战略资源的一部分，其在新型电力系统中的应用可以为国家电力供应提供自主可控、安全可靠的密码安全保障。

- **工控上位机本体安全防护技术架构**

围绕上位机的安全控制需求，实现动态安全防护技术，国产软硬件平台上工控软件的安全高效运行。如图 3-6，基于国产新一代飞腾处理器所具备的隔离计算架构、虚拟化扩展机制、TrustZone 安全域，融合多域安全操作系统设计和可信计算技术体制，设计软硬协同的本体安全防护与动态安全框架。根据不同安全运行需求对系统实施分层设计（内核态、系统态和用户态）避免通用计算中利用后门漏洞对安全控制机制和核心安全应用劫持干扰，结合可信运行控制机制及强制访问控制策略，为关键核心应用提供安全可信的计算环境，为工控系统中控制平台提供软硬一体的综合安全防御体系。该体系主要由六个支撑技术部分组成，包括：基于国产处理器的安全可信增强框架、面向工控系统的安全操作系统执行环境、多层次密码服务机制、内生可信计算体系、动态安全防护框架和面向工控应用的软件动态安全管理。

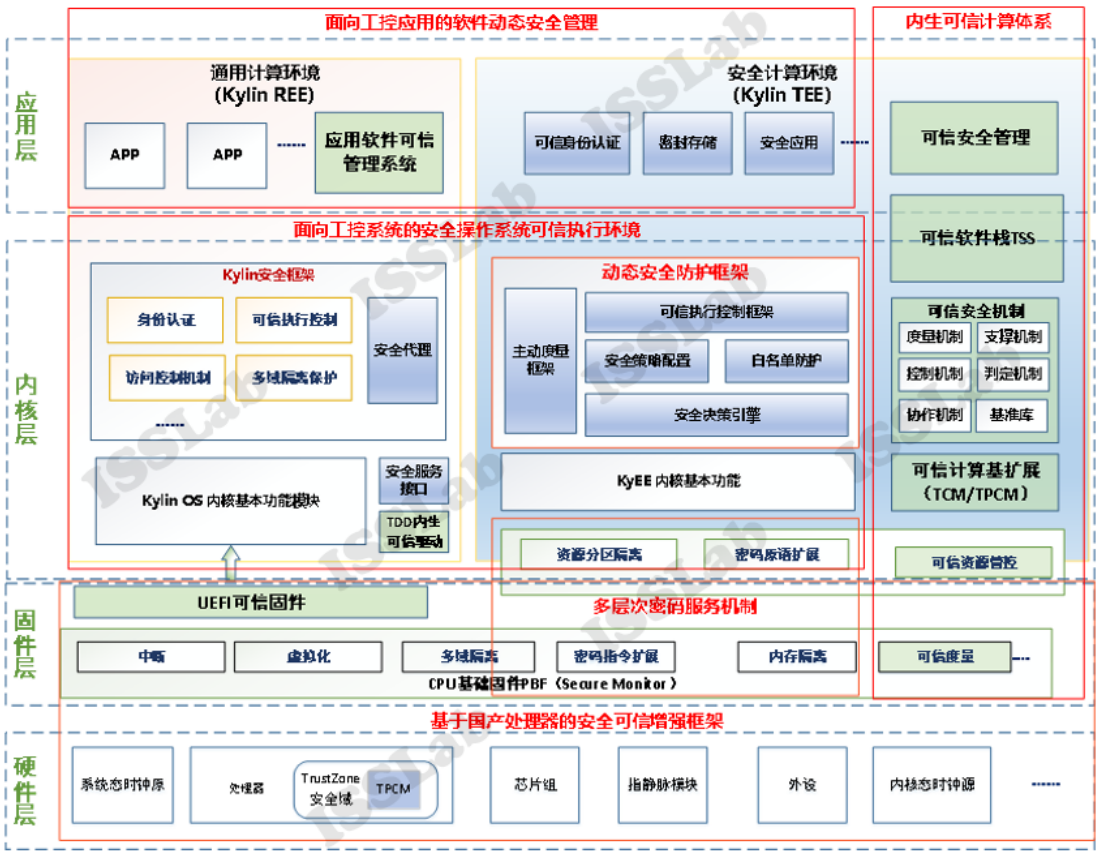

图 3-6 工控上位机本体安全防护技术架构

- **基于加密机制的主动安全控制技术**

综合考虑新型电力系统运行稳定性、关键参数安全性，设计数据分级动态加密机制，依据实时数据流、控制计算等的实时性、可用性、完整性和保密性等级要求，采用不同强度不同类别的加密算法，实现信息物理融合的未知攻击下的主动防御。

- **自身感知等级保护合规检测技术**

基于自动化等级保护合规检测，综合在线等级保护工作管理，搭建等级保护合规分析系统，如图 3-7 所示，实现等级保护安全合规结果可视化、自动化、智能化，让安全管理者能够从业务全局的角度了解安全的整体运行状态，并且进行集中化的安全监控与安全事件处理。

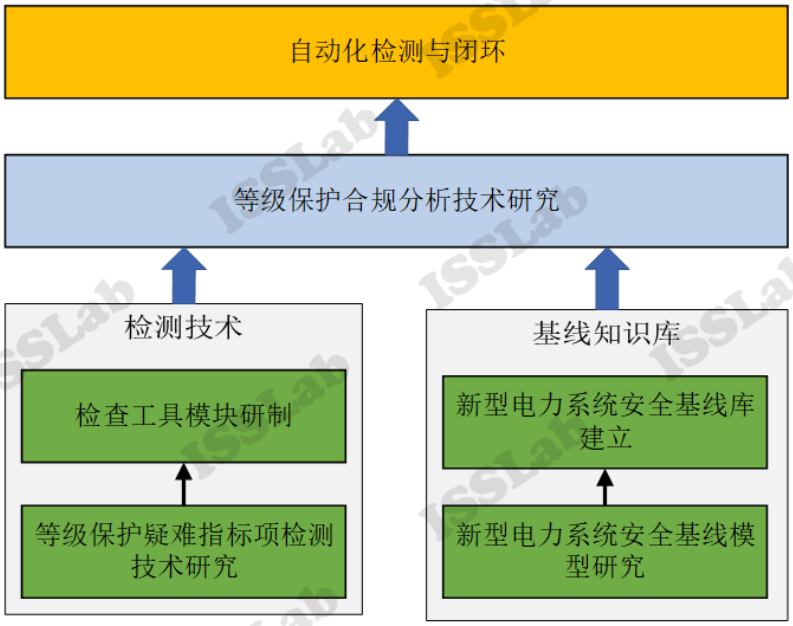

图 3-7 等级保护合规分析系统

- **基于人工智能的攻击向量移除技术**

攻击向量移除是为了恢复被攻击量测数据到未受攻击状态，以减轻数据完整性攻击对新型电力系统的影响。传统的机理建模方法难以挖掘数据之间的深层联系和时间关联性，因此无法实现电力数据的恢复。相比之下，机器学习方法具有强大的数据挖掘能力，可以实现被攻击数据的恢复。目前，无监督学习和监督学习方法已被应用于该问题。

在无监督学习方法中，矩阵分解是常用的技术之一。通过鲁棒主成分分析等无监督矩阵分解技术，可以移除攻击向量并恢复实际量测矩阵，其中包含了受攻击影响的低秩量测值矩阵和稀疏攻击矩阵的叠加。然而，基于矩阵分解的方法计算复杂度较高，并且矩阵的稀疏度会影响恢复的精度。

一些无监督神经网络算法，如降噪自动编码器和生成对抗网络，可以重建受 FDIA 影响的量测值，以消除攻击引起的偏差。然而，这些方法都会替换未受攻

击的量测部分。

另一方面，一些研究将监督学习方法应用于攻击向量移除。例如，通过贝叶斯状态估计和多层前馈神经网络的结合，可以实时去除不可靠的量测值并降低计算复杂度。然而，贝叶斯技术对于高度动态的电力 CPS 适应能力较差。

卷积神经网络（CNN）在图像去噪任务中具有较高的有效性。一些研究将 CNN 应用于移除被攻击的量测值，但同样会导致未受攻击的量测部分被替换。

目前，针对移除攻击向量的研究主要面临两个难题。首先，如何准确确定量测数据中受攻击部分的位置，以保证未受攻击部分的完整性。其次，在攻击向量移除的过程中，需要最大限度地保护未受攻击部分，以使恢复的量测数据更接近原始数据。

- **新型电力系统攻击行为审计技术**

电力系统的日常运行包括设备间的物联通信与调度人员的指令决策，其会产生大量的系统数据与运行日志。通过对海量的系统运行日志进行分析，使用 OCSVM 算法建立针对每位用户的行为单类分类器，并根据类标签对存在滥用风险的用户作出预警，从而达到预警个人攻击行为，检测违规操作指令，识别数据恶意篡改，审计操作人员行为，并生成安全预案[33]。

- **预防保护技术**

在预防保护中，主要包含预防控制、隔离与认证。预防主要针对电力系统的物理系统的日常运行，而隔离与认证则主要针对信息侧的预防保护，下面将分别对着三项预防保护手段进行阐述。(1)预防控制技术。预防控制在故障发生前将运行工作点移入到可控安全域内，是电网并未真正发生故障情况下采取的防患于未

然的安全稳定控制。对于大电网的预防控制而言，不但要考虑正常运行状态下的运行约束，还有考虑预想故障状态下的电网稳定裕度约束。对于原先不稳定的预想故障，如果要保证系统不失去任何电源和负荷，就必须通过调整运行工况使该故障变为稳定。调整后的工况也往往有利于减小故障概率。由于预防措施在无故障时已经实施，故在故障发生瞬间就影响到系统的受扰动态。其控制效果可以得到充分发挥，有效减小故障对系统的冲击。(2)隔离保护技术。隔离保护主要是将不同功能与级别的信息与控制系统进行物理与网络隔离，避免威胁的传播，主要技术手段包括安全隔离与横向隔离，如表 3-6 所示。(3)认证保护技术。认证保护主要是通过确认身份信息，从而对其操作权限进行相应的限制，从而避免人为的操作带来的威胁，其中包含的主要技术有纵向认证与加密认证。

表 3-6 主动防御体系优势

隔离保护技术	简介
安全隔离	针对电力系统的内部网络，在被动防护方面使用防火墙、入侵检测技术等技术，而在主动防护方面则采用物理、协议和网闸隔离等技术来实现。
横向隔离	是电力信息系统安全防护体系的横向防线。采用不同强度的安全设备隔离各安全区，在生产控制大区与管理信息大区之间必须设置经国家指定部门检测认证的电力专用横向单向安全隔离装置。

- **动作保护技术**

动作保护是指当电力系统中已经出了相应的威胁后，系统按照预先的保护预案进行的进行相应的动作保护，防止威胁进一步扩散，主要包继电保护与访问控制。(1)继电保护技术。继电保护对电力系统中发生的故障或异常情况进行检测，从而发出报警信号，或直接将故障部分隔离、切除的一种重要措施。对运行中电

力系统的设备和线路，在一定范围内经常监测有无发生异常或事故情况，并能发出跳闸命令或信号的自动装置。继电保护装置必须具有正确区分被保护元件是处于正常运行状态还是发生了故障，是保护区内故障还是区外故障的功能。保护装置要实现这一功能，需要根据电力系统发生故障前后电气物理量变化的特征为基础来构成。针对不同故障所具有的电气特征，对继电保护进行设置，以便能够反应于不同故障而触发不同的保护行为，使故障快速切除以保护系统稳定。目前，针对不同电气设备，配置不同的保护，保护之间通过整定计算配合，以满足继电保护选择性、速动性、灵敏性和可靠性四个基本要求。(2)访问控制技术。电力系统自动化要求实现变电站远程控制，目前影响远程控制的关键技术是保证对变电站设备的安全访问和控制，为了防止对变电站设备的非法访问、越权访问和不当操作给变电站按要求方式安全运行造成破坏，保证变电站的正常运行，要求变电站远程控制必须具有很好的访问控制机制。

- **人工智能应用数据保护技术**

电力系统人工智能应用在 AI 模型的训练和测试过程中可能会造成模型与数据隐私泄漏，包括训练阶段模型参数更新导致的训练数据信息泄漏、测试阶段模型返回查询结果造成的模型数据泄漏和数据隐私泄漏。即便在没有被直接攻击破解的情况下， AI 模型正常训练和使用的过程中产生的信息也会导致数据隐私的间接泄漏。为了解决这类数据隐私泄漏，研究人员们采用的主要思想就是在不影响 AI 模型有效性的情况下，尽可能减少或者混淆这类交互数据中包含的有效信息。AI 模型部署时可以采用以下几类数据隐私保护措施：模型结构防御，该类方法是指在模型的训练过程中对模型进行有目的性地调整，降低模型输出结果对于不同样本的敏感性；信息混淆防御，该类方法通过对模型输出和模型参数更新

等交互数据进行一定的修改，在保证模型有效性的情况下，尽可能破坏混淆交互数据中包含的有效信息；查询控制防御，该类防御通过对查询操作进行检测，及时拒绝恶意的查询，从而防止数据泄漏。(1)模型结构防御。面向模型的防御是通过对模型结构做适当的修改，减少模型泄露的信息，或者 降低模型的过拟合程度，从而完成对模型泄露和数据泄露的保护。(2)信息混淆防御。面向数据的防御是指对模型的预测结果做模糊操作。通过这些模糊操作，在保证 AI 模型输出结果正确性的前提下，尽可能地干扰输出结果中包含的有效信息，从而减少隐私信息的泄露。这些数据模糊操作主要包含两类：一类是截断混淆，即对模型返回的结果向量做取整操作，抹除小数点某位之后的信息[33 [35]；另一类是噪声混淆，即对输出的概率向量中添加微小的噪声，从而干扰准确的信息[36]。(3)查询控制防御。查询控制防御是指防御方可以根据用户的查询行为进行特征提取，完成对隐私 泄露攻击的防御。攻击者如果想要执行隐私泄露攻击，需要对目标模型发起大量的查询行为，甚至需要对自己的输入向量进行特定的修饰，从而加快隐私泄露攻击的实施。根据用户查询行为的特征，我们可以分辨出哪些用户是攻击者，进而对攻击者的查询行为进行限制或拒绝服务，以达到防御攻击的目的。查询控制防御主要包含两类：异常样本检测和查询行为检测。

- **人工智能应用安全评估技术**

（1）模型鲁棒性增强

模型蒸馏：通过使用预测结果作为标签来训练一个蒸馏出来的模型，以增强基于神经网络的能量盗窃检测模型的鲁棒性。这种技术利用了一个已经训练好的模型的知识，将其转移到一个新的模型中，从而提高模型的性能和稳健性[36,37]。

模型集成：模型集成用于提高能量盗窃探测器的性能并过滤出异常功耗数据[39]。该研究提出了一种组合模型，包括带有 LSTM 单元的自编码器、带有 GRU 的循环层、全连接层和输出层，旨在增强检测器对扰动功耗数据的敏感性。然而，尽管组合模型相对较复杂，但对能量盗窃检测的性能稍有下降，下降幅度为 1%-3%。

对抗训练：通过引入对抗样本，即经过故意设计的带有微小扰动的样本，模型在训练过程中逐渐适应这些样本，并学会识别和抵御攻击。对抗训练常使用生成对抗网络和对抗性样本生成等方法。

（2）模型鲁棒性评估

鲁棒性分析：尽管大部分鲁棒性增强方法都是专门为应对特定的对抗攻击算法而设计的，但也有一些独立于具体攻击算法的通用鲁棒性下界被推导出来[40]。为了衡量电力系统中 AI 应用的鲁棒性，可以通过基于局部 Lipschitz 连续性的假设推导出对抗扰动的下界，从而验证了对抗鲁棒性[42]。当神经网络模型中包含 ReL（修正线性单元）激活函数时，采用后向传播和可微逼近技术来处理非可微约束问题。然而，计算和实现这种下界通常是困难的。鲁棒性的边界与数据集、ML 模型参数和功率系统模型参数等因素相关，因此从这种指标中获得关于鲁棒性的洞察是困难的。因此，鲁棒性分析需要综合考虑多个因素，并结合具体的应用背景来评估模型的鲁棒性。

带物理约束的鲁棒性分析：现有的鲁棒性分析没有考虑到物理约束和糟糕的数据检测器对结果的影响。为了解决这个问题，[43]提出了一个系统框架，深入分析物理约束和 BDD（错误检测机制）对基于 AI 的安全评估模型的鲁棒性的影

响。该框架考虑到 AI 模型受到物理约束的限制，因此可以提高输入数据的鲁棒性。此外，攻击者对电力系统和传感器测量的知识有限，这进一步削弱了其对基于 AI 的安全评估模型成功发起敌对攻击的能力[44]。研究结果表明，一旦系统操作员能够保护一些脆弱的传感器测量值，基于 AI 的安全评估模型的鲁棒性就会得到显著提高。然而，这些结论仅适用于特定的场景和数据集，缺乏一般性的分析结论。这导致很难精确定位电力系统中人工智能应用输入的鲁棒区域。因此，进一步的研究还需要探索通用的分析方法，以便更准确地确定电力系统中 AI 应用的鲁棒性范围。

3.3.3 攻击入侵检测技术

- **统计方法**

统计方法是一种成熟的异常检测方法，通过使入侵检测系统学习主体的日常行为，将那些与正常活动之间存在较大统计偏差的活动标识成为异常活动。

- **预测模式生成**

预测模式生成基于如下假设：审计事件的序列不是随机的，而是符合可识别的模式的。与纯粹的统计方法相比，它增加了对事件顺序与相互关系的分析，从而能检测出统计方法所不能检测的异常事件。根据已有的事件集合按时间顺序归纳出一系列规则，在归纳过程中，随着新事件的加入，不断改变规则集合，最终得到的规则能够准确地预测下一步要发生的事件。

- **专家系统**

专家系统是针对有特征的入侵行为的检测方法。所谓的规则，即是知识，专家系统的建立依赖于知识库的完备性，知识库的完备性又取决于审计记录的完备

性与实时性。

- **Keystroke Monitor**

Keystroke Monitor 是一种简单的入侵检测方法，通过对用户击键序列的模式分析检测入侵行为，可用于监控和审计用户的键盘输入，或分析用户的输入习惯，以判定是否存在入侵行为。

- **基于入侵行为模型的检测方法**

基于入侵行为模型的概念是指通过分析入侵者在攻击系统时采取的特定行为序列，并将其构建成具有行为特征的模型，以便实时检测恶意攻击企图。入侵者在攻击系统时会展现一系列可观察到的行为序列，例如猜测口令、扫描端口等。这些行为序列被整理并建立成具有一定行为特征的模型。通过分析模型所代表的攻击意图可及时发现入侵行为并采取适当的应对措施。该方法可以选择性地检测一些主要的审计事件，降低审计事件处理的负荷，提高系统性能和效率。

- **基于通信网络指纹的外部设备接入检测技术**

设备间的差分信号可以反映整个系统终端设备的拓扑结构，可作为识别系统状态特征的指纹信息。当系统中被攻击者插入外接设备时，系统中设备间的相对位置发生改变，进而引起信号的衰减系数改变，从而来检测外部设备的非法入侵。

- **基于小波变换的特征提取检测技术**

通过一系列小波基函数对混合量测信息进行多尺度时频分解，获得量测信息的时频域局部信息，挖掘被攻击量测信息与不同时间尺度、不同空间尺度量测信息的依赖特征，为检测模型的设计提供依据。

- **基于深度学习的攻击检测模型技术**

构建基于循环神经网络(RNN)和受限玻尔兹曼机(RBM)的信息完整性攻击检测模型，以区分量测信息中的正常值和恶意值。以离散小波变换的混合量测时间序列信息特征提取结果作为输入，以 RNN 和 RBM 分析多尺度量测信息的时间相关性和单个时间的空间相关性，构建信息完整性攻击的检测方案。

- **基于主动诱导的智能电网控制指令篡改攻击检测技术**

柔性交流输电系统是综合电力电子技术、微处理和微电子技术、通信技术和控制技术而形成的用于灵活快速控制交流输电的新技术。柔性交流输电系统可以通过调节电力传输线路的电压和功率因数，提高电网的稳定性和鲁棒性。并且通过改变电力线路的参数和运行模式，主动干扰攻击者对系统信息的获取。例如，引入虚假的指令或欺骗信息，以误导攻击者，并使他们在错误的方向上浪费时间和资源。

- **基于机器学习的异常检测技术**

异常检测在新型电力系统网络安全领域被广泛应用，无监督学习和监督学习是常用的方法[45]。强化学习也用于该领域。一些方法用于检测数据中的离群点，如局部异常因子法和独立森林算法。其他方法基于主成分分析和核心子空间来检测攻击。数据分布的改变导致检测模型需要重新训练。

动态环境下的电力系统需要考虑数据相关性和变化。迁移学习[46]可用于将已有模型的参数迁移到新模型中。监督学习方法准确性高，而基于规则的方法具有可解释性。决策树方法兼顾解释性和实时性。神经网络具有非线性特征提取能力，但解释性差。集成学习方法提高了检测性能。

将攻击检测问题设计为马尔可夫决策问题，并使用强化学习方法求解，可在平衡误报率和检测速度方面进行优化。

- **基于机器学习的错误数据检测技术**

FDIA 遵循物理定律，传统的坏数据检测方法无法检测这种隐蔽性攻击。监督学习、半监督学习、无监督学习和强化学习方法已经应用于 FDIA 检测研究。早期的监督学习方法包括 K 最近邻分类、支持向量机、稀疏逻辑回归、感知机、自适应增强算法、多核学习和贝叶斯推理等。随着计算能力和数据量的增加，基于深度神经网络的方法开始得到关注。深度学习方法具有强大的非线性特征提取能力，但牺牲了可解释性。集成学习方法也用于 FDIA 检测。监督学习需要大量标记数据，而新型电力系统安全相关的标记数据难以获得。半监督学习利用少量标记数据和大量无标记数据进行学习。无监督学习方法如主成分分析、聚类和自编码器被应用于 FDIA 检测。深度强化学习技术可解决局部可观马尔可夫决策过程的 FDIA 检测问题，适用于新型电力系统环境中的大状态-动作空间[47]。

- **基于机器学习的短路攻击检测技术**

传统的机理建模方法可以相对准确地检测断路攻击，但随着电力系统规模的增大，计算量大的机理建模方法无法满足实时检测的需求。一些研究开始尝试基于机器学习的检测方法，但目前相关研究较少，且仅有监督学习方法应用于该领域。其中，使用支持向量机和线性回归的方法分别应用于断路攻击检测。另外，还有研究比较了支持向量机、朴素贝叶斯和 K 最近邻分类算法在检测断路攻击方面的性能，结果显示基于朴素贝叶斯的方法表现最佳。然而，以上研究仅能检测单条线路中断，另一项研究结合贝叶斯推理和前馈神经网络的思想，实现了实

时检测多条线路中断的能力[48]。

- **基于机器学习的偷电检测技术**

对于偷电检测，主要的数据来源是用户侧安装的智能电表。与检测电网异常、攻击等情况不同，偷电检测主要针对用户用电行为。虽然偷电通常不会对电网稳定性产生影响，但会导致电力公司经济损失。在构建偷电检测模型时，由于正常用户远多于偷电用户，导致样本类别不平衡。为处理这一问题，可以采用支持向量机通过调整样本权重、随机欠采样等技术。另外，由于电表数据含有丰富特征，神经网络类模型可以学习特征之间的非线性关系，在偷电检测任务中应用广泛。例如 CNN 可以学习不同时刻电表数据特征，LSTM 可以学习长期时间依赖性。因此一些研究探索将 CNN 和 LSTM 结合,以同时利用数据的短期和长期时间特征。总体来说，偷电检测可以看作一个样本不平衡的预测问题，需要选择合适的机器学习或深度学习模型，并充分提取电表数据的时序特征[49]。

- **数据完整性攻击的可检测性分析理论**

考虑信息物理系统中一般化的攻击隐蔽性建模与性能影响评估问题，本理论研究了攻击可检测性与系统性能下降之间的权衡关系。具体而言，攻击者通过恶意篡改信息物理系统的执行器控制指令数据以进行攻击，而攻击检测器则通过对卡尔曼滤波器的估计残差执行假设检验以检测攻击[50]。

- **基于周期性水印优化调度的信息物理系统的重放攻击检测**

针对信息物理系统中的不连续重放攻击，考虑基于水印认证机制的检测性能优化与提升问题，提出了周期性的水印调度与优化策略。首先，通过分析真实的伊朗震网病毒攻击事件可知，重放攻击在许多情况下是不连续的。由于这种攻击

的不连续性，当系统检测器对添加的水印信号不敏感时，在控制输入信号上施加连续水印信号的现有方法可能会导致控制成本的浪费。对此，针对攻击的非连续性，本研究建立了重放攻击的单次攻击持续时间模型[51]。

3.3.4 实时预警响应技术

- **新型电力系统网络安全态势感知体系**

在新型电力系统中，按照设备自身感知、监测装置分布采集、管理平台统一管控的原则，构建电力态势感知体系的三层逻辑结构，如图 3-8 所示。

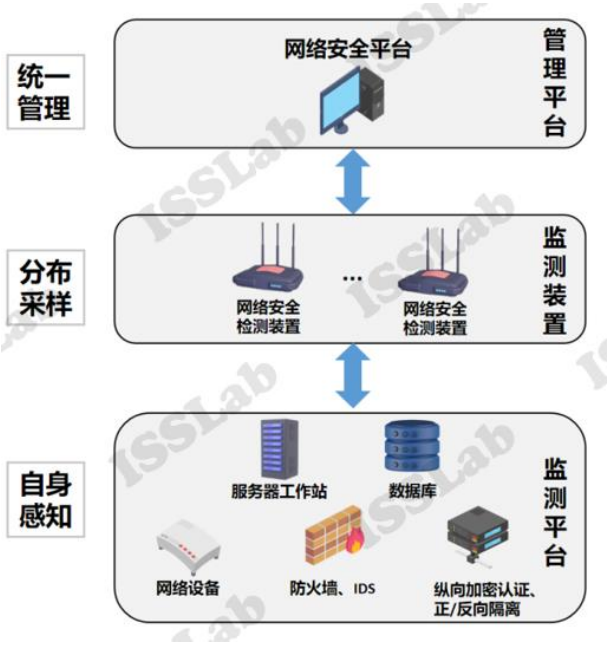

图 3-8 态势感知体系三层逻辑结构

底层自身感知实现服务器、工作站、交换机、纵向加密、正/反向隔离等设备自身可信计算和网络安全数据的感知及上报，识别各个多个潜在威胁特征，采集多个安全事件；平台管理层实现态势感知在线实时监视、告警、分析、审计、核查等功能的集成，满足对电力系统的检测和响应。

- **基于大数据的安全事件分析技术**

通过采用特征工程、关联性分析、信息聚类、数据建模等大数据相关技术，解决电力系统安全事件过度分散、数据量大、结构复杂、难于分析和有针对性地及时处理、无法溯源和预测等问题，对新型电力系统检测的实时数据进行处理和分析，建立安全事件行为模式聚类模型和电力系统威胁模型，最终实现对电力系统整体安全态势的理解、预测和溯源[52]。

- **基于支持向量回归的新型电力系统安全态势评估技术**

支持向量回归模型广泛应用于对钻井泄漏风险、空气质量、风力涡轮机风速、输出功率等领域的评估。模型结合了理论驱动、易于分析的统计方法，是一种灵活的机器学习方法，能够解决样本数量少、维度高及非线性等实际问题。通过支持向量回归模型建立评估指标和评估结果的之间的映射关系，最终根据输入评估的指标数据来获得最终的评估结果[53]。

- **紧急控制技术**

紧急控制是针对刚刚发生的，且会使系统失稳的那个特定故障，通过投切非故障设备（切机、切负荷等）来保证电力系统的稳定性[54]。其决策过程往往限于离散空间，对应于离散规划问题。为了使措施在短暂的暂态过程中充分发挥效果，应该在故障被识别出来后的第一时刻实施足量的紧急措施。因此，只能采用针对具体工况和故障的前馈控制律，按预先算出的决策表实施。其控制效果取决于预测的精度。由于不了解预先计算时所用模型和参数的误差以及工况匹配的误差对系统实际动态行为有多大的影响，目前普遍的做法是选用相当保守的措施。

- **校正控制技术**

校正控制分为主动解列、频率异常控制、电压异常控制。主动解列是一种通

过实时、全面监测系统状态，能够准确识别发电机分群，快速搜索合理的解列断面，并在适当的时间采取解列操作，以平息系统振荡，防止事故范围扩大的电力系统控制手段。目前主动解列研究的问题主要集中在两方面:解列判据（是否进行解列）和解列断面（在哪里进行解列）。频率异常控制对于电网运行安全越来越重要，在电力系统紧急状态下，频率异常降低时，除了需要尽快动用各种备用容量外，最有效最广泛采用的措施是切除部分负荷。现阶段，低频减载整定计算可以分为基于平均频率动态的等值单机模型和基于多机系统仿真的算法两大类，其中，基于等值单机模型的低频减载整定方法可以分为逐轮切负荷的传统法、通过频率变化率估算功率缺额的自适应法、在传统法基础上增添频率变化率判断根据的半自适应法；基于多机系统仿真的低频减载整定方法包括试凑法、规划优化法和基于受扰动轨迹量化分析法等；人工智能算法也常常应用于低频减载方案优化问题中，例如神经网络和遗传算法等。电压异常控制，低压减载是指在电力系统发生严重故障，可能导致电压跌落至失稳时，通过切除部分负荷使系统电压恢复的一种紧急控制措施。按照国内《电力系统安全稳定导则》，低压减载是电力系统安全稳定运行第三道防线的重要组成部分，对于防止系统崩溃和大面积停电，保证重要负荷供电，意义重大。

- **电力系统动态连锁故障建模**

在电力系统中存在的复杂多样的继电保护设备为连锁故障的动态建模带来了极大的挑战，为了克服这些挑战与难题本研究为了解决上述挑战，研究人员提出了一种基于交流潮流模型的集成级联故障继电保护的动态模型。研究人员的工作侧重于继电器建模，并使用交流潮流计算来获得更准确的潮流值，从而通过继电保护的动作来确定支路状态。该模型由三种类型的继电保护组成：距离保护、

纵联距离保护和累积过负荷保护。纵联距离保护和距离保护代表输电线路的主备保护。 累积过载保护代表传输线过热并下垂到植被中，从而导致分支关闭。给定电网的动态数据和一组初始扰动，所提出的模型能够计算触发事件在级联故障过程中的影响[55]。

- **隐蔽性移动目标防御策略设计**

针对电力系统状态估计错误数据注入（False Data Injection，FDI）攻击，安全专家设计了移动目标防御（Moving Target Defense，MTD）策略，该策略通过改变输电线路参数（阻抗）来实现对 FDI 攻击的检测[56]。

3.4 IPDR 主动防御技术体系的优势

与其它防御体系相比，IPDR 主动防御技术体系优势如表 3-7 所示。新型电力系统 IPDR 主动防御技术体系具有实时性、快速响应、主动防御、智能决策和自我优化等优势，能够为电力系统提供全面的安全保护，确保新型电力系统的安全稳定运行。

实时性和快速响应：IPDR 主动防御技术能够实时监测新型电力系统中的各个节点和通信链路，及时感知潜在威胁并作出快速响应。这使得系统能够迅速采取措施来应对安全事件，减轻攻击造成的影响。

表 3-7 主动防御体系优势

提出机构	防御技术体系	是否面向电力系统	所包含的防御模块				是否包含对物理系统的性能影响分析	防御模型创新
			识别(I)	检测(D)	保护(P)	响应(R)		
本白皮书	IPDR	√	√	√	√	√	√	与现有防御模型相比IPDR模型面向新型电力系统需求，形成了覆盖全生命周期的一体化防御体系，并分析了防御技术对新型电力系统运行性能的影响
ISS	PDR	×	×	√	√	√	×	
ISS	P2DR	×	×	√	√	√	×	
启明星辰	APPDRR	×	×	√	√	√	×	
NIST	IPDRR	×	√	√	√	√	×	
和利时	TDDRP	√	×	√	√	√	×	

威胁检测和分析： IPDR 主动防御技术利用机器学习和数据挖掘等先进算法，进行威胁检测和分析，能够识别出电力系统中的异常行为和潜在的威胁。通过不断学习和适应，系统能够提高对新型攻击和威胁的识别能力，提供更高的安全性。

主动防御能力：IPDR 主动防御技术体系采用主动防御策略，能够主动干扰攻击者的活动，引导攻击流量走向误导的路径，并减少攻击对电力系统的影响。它可以根据监测到的威胁行为自动做出反制措施，确保电力系统的持续稳定。

智能决策和优化：IPDR 技术通过智能化的决策支持系统，为电力系统管理人员提供有针对性的建议和方案。基于实时监测数据和威胁情报，系统能够辅助进行智能决策，以优化电力系统的运行和安全性。

04

新型电力系统 IPDR 应用方案

搭建新型电力系统四维安全态势感知平台，具备信息网络漏洞扫描与分析模块、设备加固自动化模块、协议增强智能化模块、业务修正常态化模块、立体式入侵检测模块、动态防御模块、人工智能增强模块、实时响应模块。

4.1 识别：信息网络漏洞扫描与分析模块

- **电力系统安全基线及漏洞知识库**

安全基线是信息系统安全防护的最低安全要求。安全基线涵盖安全漏洞、安全配置、安全状态三个安全防护范畴，将抽象的安全防护规范，落实为可执行的基础指标项，安全基线如图 4-1 所示。

图 4-1 安全基线示意图

安全漏洞：由于系统自身的问题引发的安全缺陷，主要包括登录漏洞、拒绝

服务漏洞、缓冲区溢出、蠕虫后门、意外情况处置错误等，反映系统自身的安全脆弱性。

安全配置：由于人为的疏忽造成的安全缺陷，主要包括帐号、口令、授权、日志、IP 通信等，反映系统配置的脆弱性。

安全状态：由于系统运维管理不当引发的安全缺陷，主要包括系统运行状态、网络端口状态、进程、审计等，反映系统当前所处环境安全状况。

根据安全基线防护对象类型，划分电力监控系统安全基线技术规范为网络设备安全基线、安全设备安全基线、主机系统安全基线、数据库系统安全基线等分册。每个分册又各包括具体设备的安全基线技术规范，如图 4-2，网络设备安全基线包括中兴路由器安全基线、中兴交换机安全基线、华为路由器安全基线、华为交换机安全基线等。将等级保护、风险评估等标准要求细化，并进一步分解根据具体设备特性形成设备级的基线指标，符合可执行、可实现的目标和要求。

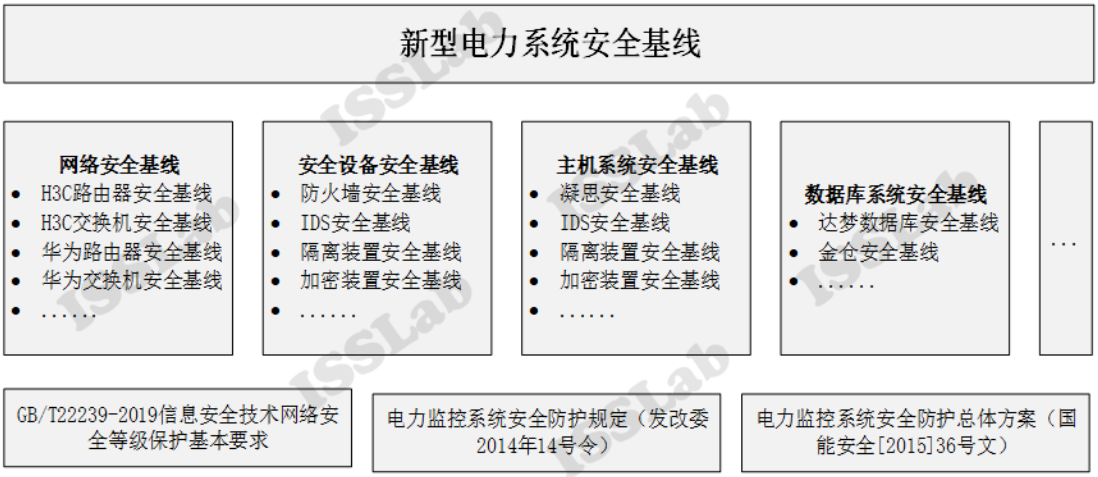

图 4-2 安全基线技术规范分类

- **基于云的漏洞扫描与分析**

基于云的漏洞扫描系统是指利用云计算技术，通过云端集中管理和调度漏洞扫描资源，实现对各类服务器、网络设备、安全设备等操作系统环境、数据库环

境、WEB 应用等进行综合漏洞扫描检测的系统。其架构主要包括以下几个部分：客户端、服务端、数据库、云管理平台、漏洞库。其中，云管理平台统一调度漏洞扫描插件，以实现对不同电力设备、电力通信协议的特殊扫描。基于云平台的漏洞扫描系统能够有效解决电力系统网络 IP 节点数量庞大、安全保障要求高等问题。充分利用云平台虚拟化技术，能够根据安全漏洞扫描需求变化，动态调整漏洞扫描插件和虚拟资源分配，达到扫描资源利用最优化，如图 4-3 所示。

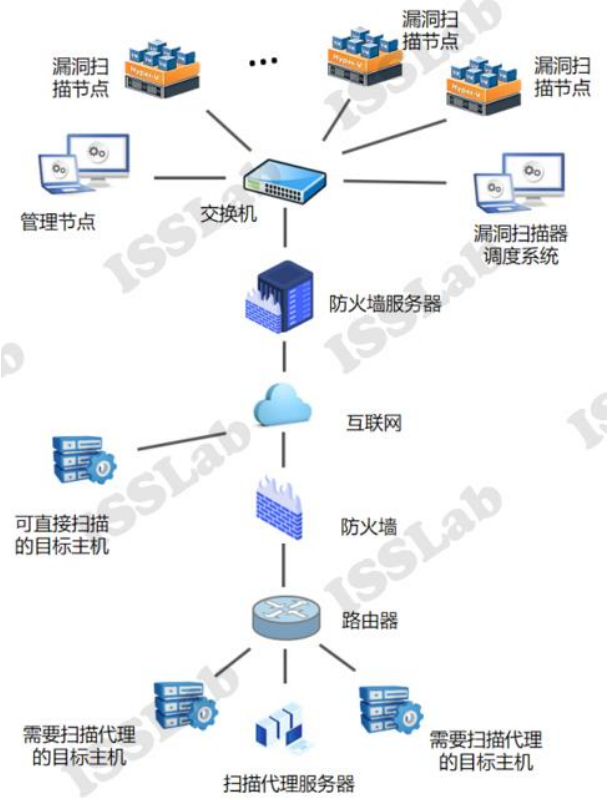

图 4-3 基于云的漏洞扫描与分析模块

4.2 保护：电力系统安全保护模块

基于电力网络数字孪生监控模块的信息采集，信息网络漏洞扫描与分析模块的风险识别，电力系统安全保护模块将实现漏洞修复与系统增强的自动化与智能化，其包括设备加固自动化模块、协议增强智能化模块、业务修正常态化模块。

电力系统安全保护模块主要实现对系统应用程序的执行控制、关键文件的完

整性保护、内核模块保护和动态连接库加卸载保护等功能。针对电力系统运行时环境的完整性、稳定性需求，基于国产安全操作系统，研究内核模块加卸载控制技术、动态链接库加载技术、关键文件防删除防篡改技术，保护电力操作系统的完整性，确保操作系统运行时的安全、稳定和可控。结合国内外操作系统的安全机制，基于应用程序执行控制机制，实现对系统应用程序主动标记识别和执行权限约束，确保应用来源的可靠性和应用本身的完整性。通过对可执行文件、关键文件、内核模块和动态连接库的标记，实现对应用程序执行时的完整性检查；确保合法且完整的应用程序才能执行。结合电力操作系统运行环境的非法外来软件主动识别及主动防御技术可实现对内核模块、动态链接库及关键文件的加卸载、防删除防卸载等保护；该技术包含非法外来软件主动识别技术和基于访问控制的行为约束技术。

结合定时任务、触发机制、强化学习等技术，实现设备加固自动化、协议增强智能化、业务修正常态化。

- **设备加固自动化模块**

使用定时任务框架（如 Cron）来执行设备加固操作。可以设置每天或每周的特定时间进行设备扫描和加固；基于事件驱动的触发机制，当设备出现漏洞报告或异常行为时自动触发加固操作。例如，使用 IDS/IPS 系统实时监测设备流量和日志，如果检测到异常行为，触发加固操作；通过监控设备的行为，并建立奖励机制来指导设备加固过程。例如，使用强化学习算法（如 Q-learning 或 Deep Q-networks）对设备行为进行分析，给予奖励或惩罚以调整加固策略。自动加固模块可以自动更新安全补丁，消除了由于未及时更新补丁而导致的安全漏洞。

- **协议增强智能化模块**

定期执行协议评估与优化。使用定时任务来触发协议性能和安全性的评估工作。可以设置每月或每季度进行协议检查与优化；当新的协议版本发布时，自动触发评估其安全性和性能。例如，使用版本控制系统（如 Git）监测协议更新，并根据设定的规则自动触发评估流程；通过强化学习算法对协议的实时使用情况、用户反馈和监控数据进行分析，以优化协议的设计和功能。例如，使用深度强化学习算法（如 Proximal Policy Optimization）来提取协议使用模式并自动调整协议参数或结构。

- **业务修正常态化模块**

定期检查业务流程的运行状态。使用定时任务来监测关键业务指标，并在预定时间间隔内执行状态检查；基于阈值或异常条件触发修正操作。例如，当系统错误率超过一定阈值时，自动触发修正措施，如自动重启服务或切换到备用服务器；利用强化学习算法根据业务数据、用户行为等信息，优化业务流程。例如，使用深度强化学习算法进行业务策略优化，根据奖励机制改进流程，以提高用户满意度和效率。

4.3 检测：电力安全入侵检测模块

围绕新型电力系统电力网络与信息网络两层网络结构，设备、协议、业务三类安全问题，构建立体式入侵检测模块，从设备、协议和业务角度设置入侵检测关键技术库，结合动态防御、人工智能增强等关键技术，实现综合全面的立体式入侵检测框架。

设备检测技术：包括对电力设备的物理访问控制、外接设备发现与识别技术

等，实现对电力设备的实时监控和识别。

协议检测技术：包括对网络协议和通信协议的漏洞扫描、入侵检测、防火墙等技术，实现对网络通信的实时监测和防御。

业务检测技术：包括对业务系统的应用安全扫描、数据库审计等技术，实现对业务系统的安全监测和防御。

动态防御技术：通过动态调整电力系统网络的安全策略和防御机制，实现对电力系统网络的实时防护。例如，通过动态防火墙、入侵检测系统等技术，实现网络访问的实时控制和监测。

人工智能增强技术：通过对电力系统网络流量进行分析和处理，利用人工智能算法识别和预测潜在的安全威胁，实现智能化的入侵检测和防御。例如，通过机器学习和深度学习技术，实现对网络流量的异常检测和识别。

通过建立立体式入侵检测模块和入侵检测关键技术库，结合动态防御和人工智能增强技术，可以实现综合全面的立体式入侵检测框架。该框架可以全面覆盖电力系统的物理层、逻辑层和业务层，实现多层次、多维度的安全监测和防御。在综合全面的立体式入侵检测框架下，可以实现对电力系统网络的实时监控、预警和防御，提高电力系统的安全性和可靠性，保障电力系统的稳定运行。同时，该框架还可以根据实际情况进行灵活扩展和调整，适应不同用户的实际需求。

4.4 响应：电力安全恢复响应模块

综合识别、防护、检测，搭建电力态势感知平台，以实现对电力安全恢复的实时响应。电力态势感知平台通过各种传感器、数据采集设备、网络传输技术，

实时采集电力系统中各种运行数据和信息，包括电力系统的电压、电流、功率、频率、气象、地理等信息。通过各种算法和模型，对采集到的数据进行分析和处理，识别和预测电力系统中的各种安全问题和风险，包括电网的稳定性、设备的故障、网络攻击等。结合地理信息系统、气象数据分析等，实现全面和准确的态势感知和分析。在发生突发事件或电力系统故障时，电力态势感知平台可以提供应急响应和决策支持功能，包括自动化控制、快速定位问题点、提供解决方案等。同时，结合应急预案和专家知识库，实现快速、准确和有效的响应和决策支持。

基于电力态势感知平台威胁识别、入侵检测的结果，将控制器实时检测与恢复系统通过旁路方式部署在电力网络中，对控制器的控制程序是否遭受恶意篡改进行实时监测，并对遭受篡改的控制程序进行快速恢复。响应模块具备控制组态、代码在线监测的功能，支持同时对 PLC 控制组态、代码的周期性在线监测；支持 PLC 控制组态、代码的篡改、插入、删除等破坏在线精确识别。通过控制组态和代码备份，支持 PLC 控制组态和代码的加密备份以及 PLC 控制组态和代码的快速精确恢复。

响应模块通过实时监测控制器健康状态，采用特有安全监测算法，对设备的运行状态、数据状态等控制器健康状态进行实时监测，并通过备份控制器关键数据及控制代码、硬件配置、原始参数等关键数据，在控制器遭受攻击导致数据和配置缺失后进行相应的恢复。

综上，电力态势感知平台满足新型电力系统 IPDR 模型，包括识别、保护、检测、响应四项防护模块，彼此之间协同配合，实现新型电力系统脆弱性识别、安全保护、异常检测和实时响应的一体化联动和持续提升。底层自身感知确保发电机、输电线路、配电网络、用电设备等电力基础设施的安全与可靠，实现传感

设备、通信网络、服务器、工作站、交换机等设备纵向加密、正/反向隔离、自身可信计算和数据安全的感知及上报，识别各类潜在威胁特征，采集多种不同安全事件；平台管理层集成实时监视、告警、分析、审计、核查等功能；平台控制层实现高效精准控制，保证电力系统的快速精确恢复。

4.5 态势感知平台人机交互系统

依据总体设计原则的要求，设计实现时选择先进、成熟的技术路线、架构、开源产品，同时兼顾目前国家电网公司信息化系统现状，即要体现先进性，又能保证与已有技术路线的兼容。经过调研分析，态势感知平台人机交互系统选择分布式 Web 技术架构，使用 Java、JavaScript、Node.js 等语言开发，支持 JAVA EE 部分规范，采用分层技术和面向接口和服务的技术架构，支持主流中间件，融合主流、成熟的开源软件。具体技术路线选择见下表 4-1 所示。

表 4-1 态势感知平台人机交互系统技术路线

分类	技术路线
构架选型	针对不同业务模块及部署场景采用不同架构： ✓ 微服务架构（Microservices Architecture）：将系统拆分为一组小型、独立部署的服务，每个服务负责特定业务功能。使用轻量级通信机制（如 RESTful API 或消息队列）实现服务之间的通信。 ✓ 容器化架构（Containerization Architecture）：使用容器技术（如 Docker）对系统进行打包和部署，提供隔离、可移植和可伸缩的环境。 ✓ 混合云架构（Hybrid Cloud Architecture）：结合公共云和私有云资源，根据需求选择合适的云服务提供商和部署模式。可以采用 IaaS（基础设施即服务）、PaaS（平台即服务）或 SaaS（软件即服务）等服务模型。
技术选型	✓ 后端开发框架：选择目前主流的后端开发框架，例如 Java、Node.js、JavaScript、Python 等，根据不同系统的技术栈和业务需求进行选择。 ✓ 前端开发框架：React、Angular、Vue.js，构建用户界面和交互体验。

	✓ API 网关：选择合适的 API 网关（如 NGINX、Kong 或 Apigee）用于路由、认证、限流和请求转发等功能。 ✓ 日志管理：使用 ELK（Elasticsearch、Logstash 和 Kibana）或 Splunk 等工具进行日志收集、分析和可视化。
部署模式	✓ 云原生部署：将系统部署在云平台上，利用云服务提供商的弹性资源和自动化管理功能。可以使用容器编排工具（如 Kubernetes）来实现自动扩展和负载均衡。 ✓ 边缘计算部署：将一部分计算任务和数据处理推向网络边缘，减少网络延迟和带宽占用。适用于需要实时响应和低延迟的场景，如物联网设备管理。
中间件	✓ 消息队列：选择高可用和可伸缩的消息队列中间件，如 Apache Kafka 或 RabbitMQ，用于实现异步通信和解耦系统组件。 ✓ 分布式缓存：使用分布式缓存中间件（如 Redis 或 Memcached）来提高系统性能和扩展性。 ✓ RPC 框架：选择适合项目需求的 RPC 框架，如 gRPC 或 Dubbo，用于实现跨服务的远程调用。
数据库	✓ 关系型数据库：选择主流的关系型数据库，如 MySQL、PostgreSQL 或 Oracle。 ✓ NoSQL 数据库：根据项目需求选择适合的 NoSQL 数据库，如 MongoDB（文档型数据库）、Redis（键值存储）或 Elasticsearch（全文搜索）。
开源软件	✓ Git：用于版本控制和协作开发。 ✓ Jenkins：用于持续集成和自动化部署。 ✓ Docker：用于容器化应用程序。 ✓ Kubernetes：用于容器编排和管理。 ✓ Prometheus：用于监控和告警。

参考文献

[1] 陈欣, 张姗姗, 方小枝. 新能源电力系统中新型储能高质量规模化配置-以安徽新型电力系统为例[J]. 攀枝花学院学报, 2022, 39(05): 64-72.

[2] 洪乾晖. 基于自组织映射神经网络的工业控制系统欺骗攻击异常检测方法研究[D]. 浙江大学, 2021.

[3] 李林波, 钱凯, 莫浩等. 风电场网络安全管理思路[J]. 云南水力发电, 2022, 38(S1): 97-100.

[4] 王智勇,刘杨钺.网络空间安全博弈的策略分析[J].国防科技,2021,42(05):75-82.

[5] 门天宇. 国外电力系统网络安全事件对我国的启示[J]. 电器工业, 2022(10): 80-82.

[6] 国家互联网应急中心．水电行业工控网络安全研究报告[R]．2019 年 5 月.

[7] 朱继东. 网信事业必须始终贯彻以人民为中心的发展思想-学习贯彻习近平总书记在网络安全和信息化工作座谈会上的重要讲话[J].先锋, 2017, 570(05): 43-44.

[8] 《新型电力系统发展蓝皮书》编写组. 新型电力系统发展蓝皮书[M]. 中国电力出版社, 2023.

[9] 中国南方电网. 数字电网标准框架白皮书[M]. 中国南方电网, 2022.

[10] 林志波. 新型电力系统将呈现“三多”特征[J]. 中国电力企业管理, 2022(16): 45-48.

[11] 陈皓勇, 谭碧飞, 伍亮等. 分层集群的新型电力系统运行与控制[J]. 中国电机工程学报, 2023, 43(02): 581-595.

[12] N. Ortiz, A. A. Cardenas and A. Wool, "A Taxonomy of Industrial Control Protocols and Networks in the Power Grid," IEEE Communications Magazine, vol. 61, no. 6, pp. 21-27, June 2023.

[13] V. Schiffer, "The CIP family of fieldbus protocols and its newest member - Ethernet/IP," ETFA 8th International Conference on Emerging Technologies and Factory Automation. Proceedings, Antibes-Juan les Pins, France, pp. 377-384, 2001.

[14] V. Kelli, P. R. Grammatikis, T. Lagkas, E. K. Markakis and P. Sarigiannidis, "Risk Analysis of DNP3 Attacks," IEEE International Conference on Cyber Security and Resilience, Rhodes, Greece, 2022, pp. 351-356, 2022.

[15] 李红波. 工业领域大规模分布式 SCADA 系统设计与研究[J]. 现代信息科技, 2023, 7(06): 165-167+171.

[16] 刘茜, 李鑫, 周宇烨. "三道防线"提升拆回计量资产管理水平[J]. 大众用电,

2021, 36(12): 64-65.

[17] 申宇. 电力系统网络安全立体防护体系构建研究[J]. 软件, 2021, 42(03): 130-132.

[18] A. S. Mohammed, N. Saxena and O. Rana. "Wheels on the Modbus - Attacking ModbusTCP Communications," Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks, New York, USA, pp. 288-289, 2022.

[19] P. Brooks, "Ethernet/IP-industrial protocol," ETFA 8th International Conference on Emerging Technologies and Factory Automation, Antibes-Juan les Pins, France, pp. 505-514, 2001.

[20] M. Hildebrandt, K. Lamshöft, J. Dittmann, T. Neubert and C. Vielhauer. "Information Hiding in Industrial Control Systems: An OPC UA based Supply Chain Attack and its Detection," Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, New York, USA, pp. 115-120, 2020.

[21] W. Shen, Y. Liu, Q. Wu, Y. Tian, Y. Liu and H. Peng, "Application of Dynamic Security Technology Architecture for Advanced Directional Attacks in Power System Information Security," International Conference on Power System Technology, Guangzhou, China, pp. 3042-3047, 2018.

[22] D. Li, Z. Aung, J. Williams and A. Sanchez, "P2DR: Privacy-Preserving Demand Response system in smart grids," International Conference on Computing, Networking and Communications, Honolulu, HI, pp. 41-47, 2014.

[23] H. Zhou, Z. Qiu, J. Xiao, "Network Active Defense Security Model and Architecture," Journal of PLA University of Science and Technology: Natural Science Edition, 2005.

[24] J. Pan, A. Liu. "Research on Network Security System Based on APPDRR Model," Telecommunication Engineering Technology and Standardization, 2009.

[25] D. Perera, J. Kay, I. Koprinska, K. Yacef and O. R. Zaïane, "Clustering and Sequential Pattern Mining of Online Collaborative Learning Data," IEEE Transactions on Knowledge and Data Engineering, vol. 21, no. 6, pp. 759-772, Jun. 2009.

[26] Z. Zou, J. Yin, L. Yang, C. Luo and J. Fei, "Research on Nondestructive Vulnerability Detection Technology of Power Industrial Control System," IEEE 6th Information Technology and Mechatronics Engineering Conference, Chongqing, China, pp. 1591-1594, 2022 .

[27] Lemieux, Caroline, and S. Koushik, "Fairfuzz: Targeting rare branches to rapidly increase greybox fuzz testing coverage." arXiv:1709.07101, 2017.

[28] Cheng, "Binary Analysis and Symbolic Execution with angr," (Doctoral dissertation, PhD thesis, The MITRE Corporation), 2016

[29] Davidson, D. Moench, B. Ristenpart, "on firmware: Finding vulnerabilities in

embedded systems using symbolic execution," 22nd USENIX Security Symposium, pp. 463-478, 2013.

[30] 周亚东, 胡博文, 朱星宇, 管晓宏. 一种基于网络安全设备日志数据的用户风险度评估方法和系统, 国家发明专利, 201910971150.X, 授权

[31] S. Wang, J. Wang, G. Tang and G. Kou, "A Network Vulnerability Assessment Method Based on Attack Graph," IEEE 4th International Conference on Computer and Communications , Chengdu, China, pp. 1149-1154, 2018.

[32] Z. Thierry, U. Andreas, K. Stephan, H. Gabriela, "Unsupervised Learning Methods for Power System Data Analysis," Big Data Application in Power Systems, pp. 107-124, 2018.

[33] W. Shang, L. Li, M. Wan and P. Zeng, "Industrial communication intrusion detection algorithm based on improved one-class SVM," World Congress on Industrial Control Systems Security (WCICSS), London, pp. 21-25, 2015.

[34] F. Tramèr, F. Zhang, A. Juels, "Stealing machine learning models via prediction," 25th USENIX security symposium, pp. 601-618, 2016.

[35] B. Wang, N. Z. Gong, "Stealing hyperparameters in machine learning," IEEE symposium on security and privacy, pp. 36-52, 2018.

[36] M. Juuti, S. Szyller, S. Marchal, "PRADA: protecting against DNN model stealing attacks," IEEE European Symposium on Security and Privacy, pp. 512-527, 2019.

[37] J. Li, Y. Yang and J. S. Sun, "Exploiting Vulnerabilities of Deep Learning-based Energy Theft Detection in AMI through Adversarial Attacks," 2020.

[38] J. Li, Y. Yang and J. S. Sun, "SearchFromFree: Adversarial Measurements forMachine Learning-based Energy Theft Detection," IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, pp. 1-6, Nov. 2020.

[39] A. Takiddin, M. Ismail, U. Zafar and E. Serpedin, "Robust Electricity Theft Detection Against Data Poisoning Attacks in Smart Grids," IEEE Transactions on Smart Grid, vol. 12, no. 3, pp. 2675-2684, May 2021.

[40] G. Katz, C. Barrett, D. Dill, K. Julian and M. Kochenderfer, "Reluplex: An efficient smt solver for verifying deep neural networks," 29th International Conference on Computer-Aided Verification, Springer, 2017.

[41] C. Szegedy, W. Zaremba, I. Sutskever, "Intriguing Properties of Neural Networks," International Conference on Learning Representations, 2013.

[42] C. Ren and Y. Xu, "Robustness Verification for Machine Learning-based Power System Dynamic Security Assessment Models under Adversarial Examples," IEEE Transactions on Control of Network Systems, Early Access, 2022.

[43] Z. Zhang, M. Sun, R. Deng, C. Kang and M.-Y. Chow, "PhysicsConstrained Robustness Verification of Intelligent Security Assessment for Power Systems," IEEE Transactions on Control of Network Systems, pp. 1-15, 2022.

[44] Z. Zhang and D. Yau, "CoRE: Constrained Robustness Evaluation of Machine Learning-based Stability Assessment for Power Systems," IEEE-CAA Journal of Automatica Sinica, vol. 9, no. 0, pp. 1-3, Sept. 2022.

[45] 彭莎, 孙铭阳, 张镇勇等. 机器学习在电力信息物理系统网络安全中的应用[J]. 电力系统自动化, 2022, 46(09): 200-215.

[46] Y. Zhang, J. Yan, "Domain-adversarial transfer learning for robust intrusion detection in the smart grid," IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), October 21-23, 2019, Beijing, China.

[47] D. An, Q. Yang, W. Liu, et al. "Defending against data integrity attacks in smart grid：a deep reinforcement learning-based approach," IEEE Access, vol. 019, no. 7, pp.110835-110845.

[48] Y. Zhao, J. Chen, H. Poor, "A learning-to-infer method for real-time power grid multi-line outage identification," IEEE Transactions on Smart Grid, vol. 11, no. 1, pp. 555-564, 2020.

[49] M. Ismail, M. Shaaban, M. Naidu, et al. "Deep learning detection of electricity theft cyber-attacks in renewable distributed generation," IEEE Transactions on Smart Grid, vol. 11, no. 4, pp. 3428-3437, 2020.

[50] C. Fang, J. Chen, Y. Qi, R. Tan, "WeiXing Zheng. Stealthy actuator signal attacks in stochastic control systems: Performance and limitations," IEEE Transactions on Automatic Control, pp. 3927-3934, 2019.

[51] C. Fang, Y. Qi, P. Cheng, W. Zheng, "Optimal Periodic Watermarking Schedule for Replay Attack Detection in Cyber-Physical Systems," Automatica, 2020.

[52] B. P. Bhattarai, S. Paudyal, Y. Luo, M. Mohanpurkar, K. Cheung, Reinaldo. Tonkoski, Rob. Hovsapian, K. S. Myers, R. Zhang, P. Zhao, M. Manic, S. Zhang, X. Zhang, Big data analytics in smart grids: state-of-the-art, challenges, opportunities, and future directions," IET Smart Grid, vol. 2, no. 2, pp. 141-154, 2019.

[53] A. Widodo, B. S. Yang, "Support vector machine in machine condition monitoring and fault diagnosis," vol. 21, no. 6, pp. 2560-2574, 2007.

[54] K. Zhang, J. Zhang, P. D. Xu, T. Gao and D. W. Gao, "Explainable AI in Deep Reinforcement Learning Models for Power System Emergency Control," IEEE Transactions on Computational Social Systems, vol. 9, no. 2, pp. 419-427, 2022.

[55] Y. Yang, Y. Zhou, J. Wu, Z. Xu, X. Guan,W. Chen, T. Liu, "A Dynamic Cascading Failure Model Integrating Relay Protection in Power Grid," IEEE 16th International Conference on Automation Science and Engineering, pp. 1331-1336, 2020.

[56] Z. Zhang, R. Deng, David K. Y. Yau, P. Cheng, J. Chen, "On Hiddenness of Moving Target Defense against False Data Injection Attacks on Power Grid," ACM Transactions on Cyber-Physical Systems, pp. 1-29, 2020.