DOI 10.15302/J-SSCAE-2025.08.018

关键信息基础设施物联网安全发展态势及展望

徐文渊，程雨诗*，陈艳姣，冀晓宇

（浙江大学电气工程学院，杭州 310027）

摘要：随着关键信息基础设施物联网加速向规模化应用迈进，其在能源、交通、工业等关键领域的广泛部署，正带来前所未有的安全挑战。物联网技术在推动行业智能转型的同时，也带来了系统性安全隐患，直接关系国家安全、经济运行和社会稳定大局。本文从通用风险与专属场景威胁两个维度切入，系统剖析传统物联网“云–管–边–端”架构中的安全问题，并针对新兴趋势带来的风险展开探讨，覆盖具身智能等五大典型应用场景的安全议题。基于物联网安全现状与发展趋势，本文进一步阐释了关键信息基础设施物联网的安全内涵与核心风险，结合其架构特点与实际应用需求，提出“通域统一保障 + 专域定制增强”的防护理念，倡导构建覆盖全域、动态协同、智能自适应的新一代安全防护体系与治理路径，并从战略、制度、技术、人才与国际合作五个方面系统推进，以实现可持续演进的安全治理能力。

关键词：关键信息基础设施；物联网；安全风险；安全防护

中图分类号：TP393　　**文献标识码：**A

Internet of Things Security in Critical Information Infrastructure: Trends and Prospects

Xu Wenyuan, Cheng Yushi*, Chen Yanjiao, Ji Xiaoyu

(College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China)

Abstract: As the Internet of Things (IoT) in critical information infrastructure rapidly scales up, its widespread deployment in sectors such as energy, transportation, and industry is introducing unprecedented security challenges. While driving intelligent transformation across industries, the IoT technology also brings systemic security risks that impact national security, economic operations, and social stability. This study examines security issues in traditional IoT architectures—cloud, pipe, edge, and device—from both general and scenario-specific risk perspectives, and explores emerging threats in trends such as embodied intelligence and four other key application areas. Based on current conditions and development trends, the study clarifies the security implications and core risks of IoT in critical infrastructure. Aligned with its architectural features and practical needs, a “universal guarantee + customized enhancement” protection approach is proposed, advocating a new-generation security system that offers full coverage, dynamic collaboration, and adaptive intelligence. Systematic efforts in strategy, regulation, technology, talent, and international cooperation are recommended to achieve sustainable and evolving security governance.

Keywords: critical information infrastructure; Internet of Things; security risks; security protection

收稿日期：2025-08-13；**修回日期：**2025-10-21

通讯作者：*程雨诗，浙江大学电气工程学院研究员，研究方向为物联网安全；E-mail: yushicheng@zju.edu.cn

资助项目：中国工程院咨询项目“网络空间安全新技术新应用风险研究”(2023-JB-01)；国家自然科学基金项目(61925109, 62222114)

本刊网址：sscae.engineering.org.cn

一、前言

随着“十四五”规划的实施，我国已将关键信息基础设施安全上升至国家战略高度，明确提出建设智能化、综合性数字信息基础设施的目标。近年来，物联网技术在感知、传输、边缘计算和终端智能等方面取得显著进展，在此背景下，关键信息基础设施与物联网的深度融合已成为必然趋势。

当前，关键信息基础设施物联网（以下简称“关基物联网”）安全已成为全球数字安全体系的战略高地，其重要性引发主要国家的高度关注。近年来，多起典型事件凸显了关基物联网安全风险的现实性与破坏性。2019年，委内瑞拉电力系统受到多源协同攻击引发全国停电；2024年，美国Change Healthcare公司遭遇勒索软件攻击导致大规模数据泄露及大范围服务中断；2024年，黎巴嫩贝鲁特发生针对寻呼设备的融合电磁频谱干扰、供应链预置与认知操控等手段的复合型攻击，造成重大伤亡。这些事件表明关基物联网安全风险已由传统网络攻击向跨域联动、多层渗透的系统性威胁演变。传统问题不断演化、新型威胁不断涌现，给当前防护体系带来挑战。面对关基物联网引发的系统性风险，美国、欧盟等发达国家和地区率先布局，美国网络安全与基础设施安全局（CISA）、俄罗斯联邦安全局（FSB）、欧盟网络与信息安全局（ENISA）、日本内阁网络安全中心（NISC）等机构持续投入研发，旨在主导物联网安全标准并掌握技术主动权。在漏洞挖掘、入侵检测、安全认证以及基于人工智能（AI）的主动防御等核心技术领域，上述国家已形成明显优势。在法律法规层面，各国普遍将关基物联网安全治理上升为国家战略[1]，从立法层面强化制度保障与风险预控能力。相比之下，我国虽拥有全球最大的物联网应用市场，并在部分应用层安全技术上取得进展，但在一体化安全防护等关键环节仍存在不足，安全风险形势严峻。相关法律法规及标准（如《信息安全技术 关键信息基础设施安全保护要求》（GB/T 39204—2022））已陆续出台[2]，推动关基物联网安全标准体系系统化发展，但仍存在法律层级不健全、关键环节法律支撑薄弱等问题。

随着关基物联网安全风险日益凸显，国际竞争态势愈发激烈，加强关基物联网安全研究，不仅是保障能源、交通、金融等关键领域安全运行、维护社会稳定的基础，更是突破国际技术壁垒、掌握发展主动权、支撑数字中国建设的迫切需求。

面向“十五五”发展阶段，本文基于对关基物联网发展趋势的研判，提出安全防护需由局部静态防御向全域动态协同演进。结合关基物联网覆盖广、异构性强、接入复杂等特征，本文提出“通域统一保障+专域定制增强”的综合防护体系，以支撑大规模应用的安全落地。同时，围绕具身智能、低空经济、工业互联网、卫星互联网、新型电力系统等关键场景，系统分析潜在风险并提出针对性防护路径，推动关键信息基础设施智能化与信息化发展，实现高水平安全与高质量发展的协同并进。

二、关基物联网架构体系与发展趋势

（一）关基物联网架构体系

关基物联网是指基于物联网技术构建、支撑国家关键信息基础设施安全稳定运行的重要系统，广泛应用于能源、电力、交通、金融、通信等关键领域，直接影响国家安全、经济命脉、社会稳定与公共利益[3]。该系统通过智能感知、泛在连接、数据融合与自动化控制等关键技术，实现对基础设施运行状态的实时监测、智能管理与协同优化，是新型基础设施体系的重要组成部分。

关基物联网普遍采用“云–管–边–端”的现代化架构，构建覆盖国家重点行业的智能基础设施网络，形成由感知采集、通信传输、边缘处理到云侧决策的闭环体系（见图1）。① 云侧平台层作为智能中枢，依托AI与云计算实现数据汇聚、分析决策与策略下发，支撑行业统一调度与业务管控；② 网络通信层构建高可靠、低时延的融合网络，保障关键数据在跨域、跨层间的安全传输；③ 边缘计算层部署于现场近端，具备本地处理与自治控制能力，在断网场景下可独立运行，增强系统实时性与韧性；④ 终端设备层感知物理环境，负责数据采集与指令执行，直接控制关键基础设施对象。各层协同配合，实现系统全流程闭环运行，构建支撑国家关键信息基础设施数字化转型的智能底座与技术保障体系。在实际应用中，不同行业往往会根据业务特性、安全等级及合规要求，对该通用架构进行差异化部署。例如，电力系统通常采用生产控

制内网与管理信息外网的物理隔离模式，以保障核心控制域不被外部网络直接访问；部分工业控制系统则构建双网双机与工业隔离区，进一步强化边缘与云侧的数据交互管控。

（二）关基物联网发展趋势

随着关基物联网在重点行业中的加速落地，其体系架构与功能边界持续拓展，逐步由传统的信息采集与远程控制系统，演进为融合智能感知、边缘处理与自主决策的新型基础设施形态。在这一演进过程中，关基物联网呈现出终端设备海量化、跨域风险实体化、通信技术多元化、决策生成智能化与值守运行无人化等五大显著趋势（见图2）。这些变化不仅体现出技术系统自下而上的发展逻辑，也折射出国家安全战略对关键信息基础设施系统自主可控、智能可管的现实要求。

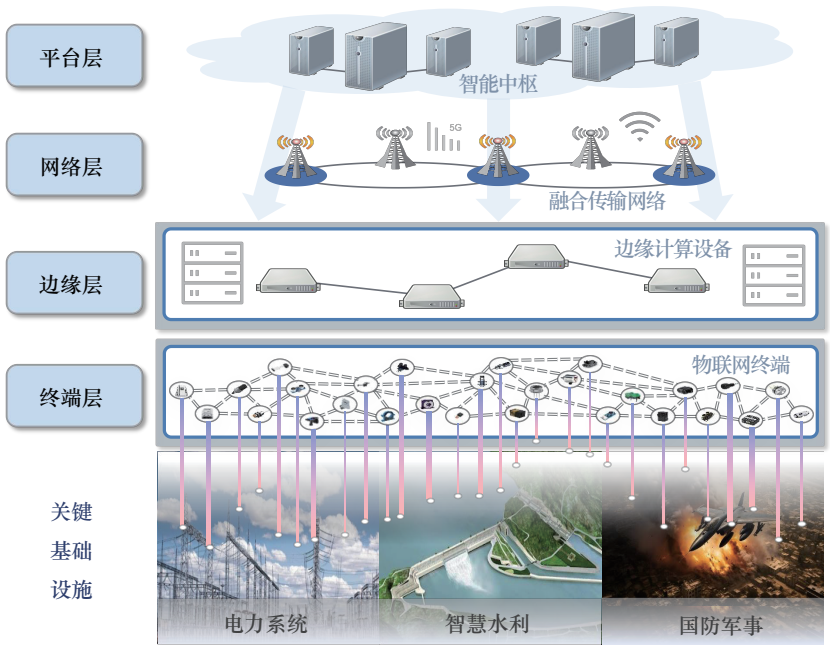

图1　关基物联网“云－管－边－端”架构体系

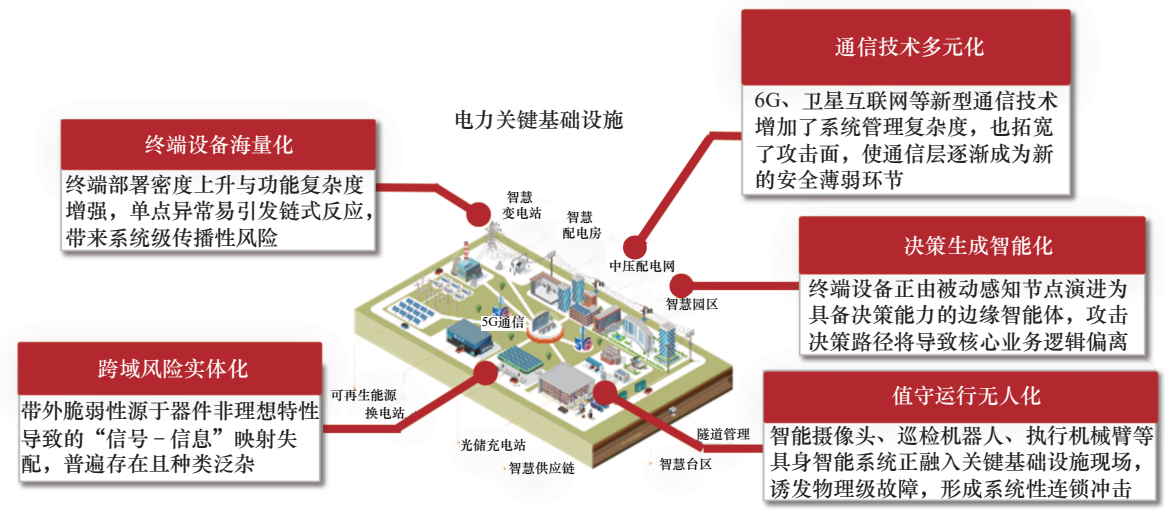

图2　关基物联网发展趋势与特点

注：5G为第五代移动通信；6G为第六代移动通信。

（1）终端设备海量化，边缘节点指数增长。端侧正由“单纯传感”加速迈向“感知–决策–执行”一体化的自治节点，推动系统响应速度与资源分布效率显著提升。但随着终端部署密度上升与功能复杂度增强，系统安全边界随之扩展，单点异常易引发链式反应，带来系统级传播性风险[4]。

（2）带外脆弱性激增，跨域风险实体化。随着系统设计日益复杂、组件高度封装以及多模态交互的广泛应用，“信号–信息”之间的理想映射难以长期稳定维持，催生大量传统防护难以覆盖的新型带外脆弱性。在这种跨域交互场景中，攻击者可操控物理域输入，诱导信息域产生误判，绕过既有逻辑约束并触发异常响应，形成结构性、强隐蔽性的攻击路径，显著提升系统整体失稳风险[5]。

（3）通信技术多元化，攻击面显著扩大。6G、卫星互联网、近地无线以及面向中低速场景的5G 轻量化（RedCap）等新型通信技术快速涌现，推动“最后一千米”连接向空中、地下及边远区域延伸。通信链路的异构化与协议碎片化显著增加了系统管理复杂度，加上无线通信的开放性使通信层成为安全薄弱环节[6]。特别是RedCap等轻量化技术，为兼顾成本与功耗对安全协议进行了裁剪，其简化的认证与加密机制更易遭受中间人攻击与伪基站接入。

（4）决策生成智能化，边缘智能全面下沉。终端设备正由被动感知节点演进为具备本地决策能力的边缘智能体，支持分布式计算、快速响应与任务自治。尽管系统效能显著提升，但也引入了模型篡改、推理操控等新型风险，一旦攻击者干预决策路径，可能导致核心业务逻辑偏离。智能决策所依赖的智能传感器数据若在源头被物理欺骗或篡改，将导致核心业务逻辑发生根本性偏离。

（5）值守运行无人化，具身智能加速融合。智能摄像头、巡检机器人、执行机械臂等具身智能系统正加速融入关键信息基础设施现场，构建“感知–决策–执行”的闭环控制体系。在高度自动化环境中，一旦智能控制系统遭遇欺骗或劫持，其响应偏差将快速扩散至执行层，诱发物理级故障，形成系统性连锁冲击。

综上所述，关基物联网正迈入“能力跃升–风险外溢”并行发展的新阶段。一方面，终端智能化、通信泛在化与决策边缘化不断提升系统的运行效率与自适应能力；另一方面，带外脆弱性、链路异构与安全空窗等问题日益加剧系统的暴露面与不可控性。在此背景下，重塑多层次、跨域协同的新型安全防护体系，已成为保障国家关键信息基础设施安全稳定运行的关键路径。

三、关基物联网面临的新型威胁与挑战

为提升整体防护能力，亟需从体系层面对关基物联网的安全内涵进行重新审视，并构建一套适应技术演进、覆盖多场景的新型安全框架。关基物联网安全的核心任务是保护系统中的物联网终端、通信链路、边缘节点和云平台等关键组件，防止非法访问、操控与破坏。传统架构基于“云–管–边–端”模型构建，已具备一定的纵深防护能力，但在实践中仍面临新型威胁与挑战：一方面，通用系统暴露出带外攻击、新通信协议漏洞等全局性问题；另一方面，新兴场景下的关键信息基础设施（如具身智能系统、卫星互联网、低空经济平台、新型电力系统、工业互联网等）具有特殊的结构与运行模式，需开展定制化的安全分析与加固。

基于此，本文提出“通域+专域”双层安全体系（见图3），以支撑多类型关基物联网的系统性防护。① 通域安全：面向所有关基物联网系统，在“云–管–边–端”架构基础上，纳入带外脆弱性、新型通信链路安全等新型风险，实现可复用、可扩展的基础能力建设。② 专域安全：聚焦特定场景，针对其独特架构与攻防特性，设计差异化的专有安全策略与技术手段。该双层体系强化了通用防护的广度与专用防护的深度，推动关基物联网安全能力从“统一治理”向“场景驱动”升级，为构建持续演进、自适应的安全保障体系奠定基础。

（一）通域安全威胁

（1）云侧风险：集中虚拟，平台薄弱。云平台为了适配物联网高并发、高弹性需求，普遍采用轻量协议、虚拟化架构和开放接口，但也为云侧引入三方面风险：① 数据层面，海量敏感数据集中存储易引发保密性、完整性与可用性风险；② 虚拟化层面，在多租户共享结构下，虚拟机逃逸、镜像泄露和弱隔离设计等问题频发[7]，可导致跨租户信息泄露与攻击跳跃；③ 接口层面，云侧接口开放

图3 关基物联网“通域–专域”双层安全体系

性强，易遭遇结构化查询语言（SQL）注入、身份伪造和分布式拒绝服务（DDoS）等攻击，破坏数据交互与服务稳定性，严重时甚至可下行影响物理系统控制链路。

（2）管侧风险：链路开放，协议脆弱。物联网通信管道作为物联网设备通信的基础，其信道、协议、流量均面临风险：① 信道层面，无线信道缺乏物理隔离，面临干扰、中间人、重放等攻击。② 协议层面，物联网通信多依赖低功耗协议，协议栈庞杂，典型如LPWAN类协议因功耗限制削弱了安全加密机制[8]，易被伪造响应、能耗攻击或协议回退等手段突破防线。③ 数据层面，在开放网络环境下，传输数据常面临明文泄露、流量嗅探与泛洪攻击等问题，攻击者可借助流量分析或DDoS攻击使通信路径瘫痪，进而阻断系统运行链路。

（3）边侧风险：节点暴露，权限紊乱。边缘节点作为协同处理中心，虽具备一定算力与决策能力，但其运行在复杂异构环境中，面临多方面风险：① 边缘节点面临安全计算脆弱性，物理暴露、权限混乱、软件脆弱性使其成为攻击者优先突破目标。攻击方式包括DDoS、身份冒充、侧信道窃取与远程控制等。② 节点管理层面，在多任务系统下权限边界模糊，越权调用或横向移动极易发生。③ 数据层面，边缘设备频繁与终端和云侧交换数据，若数据链加 / 解密流程不完善，易在本地缓存或传输中被截获或篡改。

（4）端侧风险：设备异构，防控薄弱。物联网终端设备分布广、数量大、异构性强、物理暴露，成为安全防护的薄弱环节。① 海量分散设备难以准确识别和有效管理，特别是无源物联等“沉默”节点，其资产清点和状态监控尤为困难，资产信息泄露易提供精准攻击目标，且设备老化导致性能下降、漏洞长期存在。② 设备硬件资源受限，更新滞后，漏洞无法修复，在5G RedCap终端、无源节点等极端受限设备上，此问题近乎无解，弱口令和薄弱认证易被破解，物理暴露更易遭受篡改、窃听、传感器欺骗等物理攻击。③ 设备采集的敏感数据易被篡改或仿冒，智能传感器作为数据源头，其物理暴露性使其易受带外信号注入攻击，导致系统基于错误信息决策。④ 终端设备频遭恶意软件感染，如Mirai、Bashlite等可构建大规模僵尸网络，用于发起DDoS攻击或远程控制系统，直接威胁关键信息基础设施的物理运行安全[9]。在资源极端受限的终端上，此问题尤为突出。例如，无源物联节点依赖环境能量采集与反向散射通信，无法执行任何加密运算，极易遭受信号干扰、数据重放与标签克隆攻击；而智能传感器作为感知末梢，其固件更新机制往往缺失，且直接暴露于物理环境中，易被激光、超声波等带外信号欺骗，导致感知数据被恶意操控。

（5）带外脆弱性：映射失配，跨层破坏。带外脆弱性源于物理域与数字域之间的映射失配，表现

为非功能设计层的“信号–信息”转换缺陷[10]。该脆弱性在各类传感器上的表现尤为典型。带外脆弱性具体表现为四类安全风险：① 跨场输入，即传感器因设计外的换能效应接收设计模态外的物理信号，导致系统被异常控制或输入污染，如调制电磁信号注入导线，干扰光伏逆变器测量，导致设备异常[11]。② 跨场输出，即器件工作产生设计模态外的物理信号，形成信息泄露侧信道，造成敏感状态或数据被非授权用户获取[12]。③ 超限输入，即传感器因固有物理特性响应设计数值范围外的信号，导致测量失真或功能异常。④ 超限输出，即设计内输出信号隐含超出设计意图的信息，造成用户隐私或设备敏感信息泄露[13]。此类攻击具有高隐蔽性、高精度和跨层破坏性，正在从研究走向实用，严重威胁物理世界的控制安全。例如，监控摄像头的光学传感器会对激光脉冲产生异常响应，加速度计会受特定频率声波的干扰，此类攻击可绕过系统逻辑直接污染信息源。

（6）新型通信：架构变革，攻击面广。新一代通信技术（如6G）通过泛在连接、智能内生和多域协同，支撑关键场景的感知与控制，但其异构、分布式、跨域特性也带来新的系统性风险。① 网络层面，分布式组网的自动注册机制存在认证缺陷，易被伪造身份接入；卫星与地面网络切换中的身份重认证不足，可能造成服务中断或信令劫持；通信节点拓扑动态变化、天基节点处理能力低下，进一步扩大了信任漏洞。② 数据层面，资源受限边缘节点采用轻量加密算法，暴露在窃听、篡改等风险之下。③ 技术集成层面，6G原生集成AI、区块链与量子通信等技术，AI模型训练阶段可能遭受数据投毒，导致频谱分配、网络切换等关键系统误判；舒尔（Shor）算法等量子攻击手段可破解现有RSA/ECC体系，威胁根密钥安全[14,15]。④ 业务场景层面（如工业控制、通感一体、沉浸式应用），由于需要开放第三方应用程序编程接口（API），加之超大流量的冲击和极高可靠低延时通信导致的安全协议简化，权限校验机制薄弱，可能导致核心算力与敏感数据暴露，甚至被用于发起攻击或侵害公共 / 个人隐私。

（二）专域安全威胁

（1）具身智能：软硬件深度耦合，交互复杂。具身智能系统融合计算、感知与控制，其安全风险呈现出多维叠加、软硬一体的特性。① 智能体本体层面，算法可能受到对抗样本和越狱攻击威胁，造成模型误判并执行危险指令[16,17]；传感器与执行器易受激光、电磁等物理信号干扰，进而导致感知失真或动作失控；训练数据若遭投毒易植入后门，运行中收集的隐私数据也面临泄露风险。② 环境交互层面，具身智能在与人、物和其他设备协作中可能发生传感错误或识别失败，导致人员伤害、货物破损或协作混乱等问题。③ 应用层面，具身智能面临信息域的恶意代码注入、物理域的设备干扰或劫持、社会域的伦理争议和责任归属不明等深层挑战，已逐渐演化为关系到公共安全与社会稳定的系统性安全问题。

（2）卫星互联网：链路脆弱，供应链易受攻击。卫星互联网作为覆盖全球的新型空间网络信息基础设施，其安全威胁贯穿物理设施、通信链路、系统软件与供应链多个层面。① 物理层面，轨道与频谱资源存在先占优势带来的竞争风险，自然环境如太阳活动亦可能干扰卫星运行；此外，反卫星武器、设计缺陷与人为操作失误等因素都可能对卫星构成实质性破坏。② 网络层面，开放的链路结构[18]与高时延特性使卫星通信极易遭受窃听、劫持与干扰，域名服务器劫持等网络攻击风险显著加剧。③ 系统层面，软件设计缺陷、后门漏洞与更新限制共同导致入侵防护能力不足，恶意程序或配置错误更可能造成服务中断。④ 业务层面，社会工程攻击、身份欺诈等风险不容忽视；此外，由于供应链组件多来源、验证链条复杂，恶意代码植入、硬件篡改或开源模块污染等问题难以溯源修复，其隐蔽性与持久性风险贯穿系统全生命周期。

（3）低空经济：系统脆弱，管理缺位。低空经济依托无人系统快速发展，其安全问题集中体现在系统、网络、任务与管理多个环节。① 系统层面，开源飞控系统普遍存在全球导航卫星系统欺骗[19]和指令注入风险，边缘嵌入式平台易受提权攻击或物理总线劫持，攻击隐蔽性强且恢复难度大。② 网络层面，通信链路加密认证机制薄弱，面临信号压制、链路劫持与动态拓扑下的认证失效等挑战。③ 任务与数据层面，飞行轨迹、日志与联邦学习过程可能泄露任务信息或被逆向还原任务逻辑，模型亦可能被窃取。④ 管理层面，权限划分不清、

监管技术滞后[20]、响应机制碎片化、运维平台长期失效，难以有效阻断攻击扩散或适应复杂态势变化，构成整体安全防线的关键短板。

（4）新型电力系统：多元融合，防护断层。新型电力系统在融合物理与信息网络的同时，也引入了差异化主体参与、多样化终端接入与复杂化数据交互等新型安全挑战。① 终端接入层面，海量设备能力不一、安全机制不全，协议标准化不足且更新缓慢，成为潜在的攻击跳板。② 网络通信层面，涉控业务无线化导致攻击面扩大，通信保障存在带宽、时延等物理瓶颈，防护措施缺乏统一部署。③ 数据流转层面，内部权限控制与共享机制薄弱，外部共享范围不明，分类分级保护规范缺失，云化与微服务等技术的快速引入进一步加剧数据泄露与篡改风险，形成系统性的防护断层。④ 协同机制层面，多方协同主体之间缺乏统一标准与应急协同机制，多交互方式共存致使防护边界模糊，传统安全方案难以兼容多样化的业务需求。

（5）工业互联网：开放融合，漏洞多发。工业互联网支撑智能制造和远程运维，其开放融合特性也带来了多维交叉的安全风险。① 算法层面，AI 模型易受后门植入、数据投毒与对抗样本攻击影响，造成自动决策误判甚至生产事故，AIGC 生成内容也可能扰乱监测与控制环节。② 设备层面，工业控制器与传感器因设计封闭未充分考虑网络安全、补丁机制不健全而长期暴露于漏洞攻击中[21]，侧信道攻击更可能绕过认证机制获取敏感数据。③ 网络通信层面，传统的工业控制通信协议如 Modbus、S7Comm 等缺乏基本加密与认证机制[22,23]，明文传输易遭监听与篡改，跨层网络结构防护薄弱使攻击传播路径迅速扩大。④ 管理层面，安全治理体系缺失、资产管理混乱、应急响应不足等问题普遍存在，员工安全意识淡薄与第三方组件滥用也进一步放大了安全威胁，全方位考验系统的韧性与恢复能力。

四、关基物联网安全防护

当前，关基物联网面临传统风险与新型威胁的双重挑战。传统以“云－管－边－端”为核心的防护体系虽然在设备漏洞、数据泄露等常规风险上取得了一定成效，但在低空经济、工业互联网、具身智能等新兴场景下，已暴露出明显的适应性不足与技术空白。随着针对物联网的攻击手段趋于复杂化，攻击面持续扩展，亟需构建覆盖通用领域与专有领域的统一防护体系，推动防御机制从单点应对向纵深防御、多层协同演进，以实现对复合型安全威胁的有效应对（见图4）。

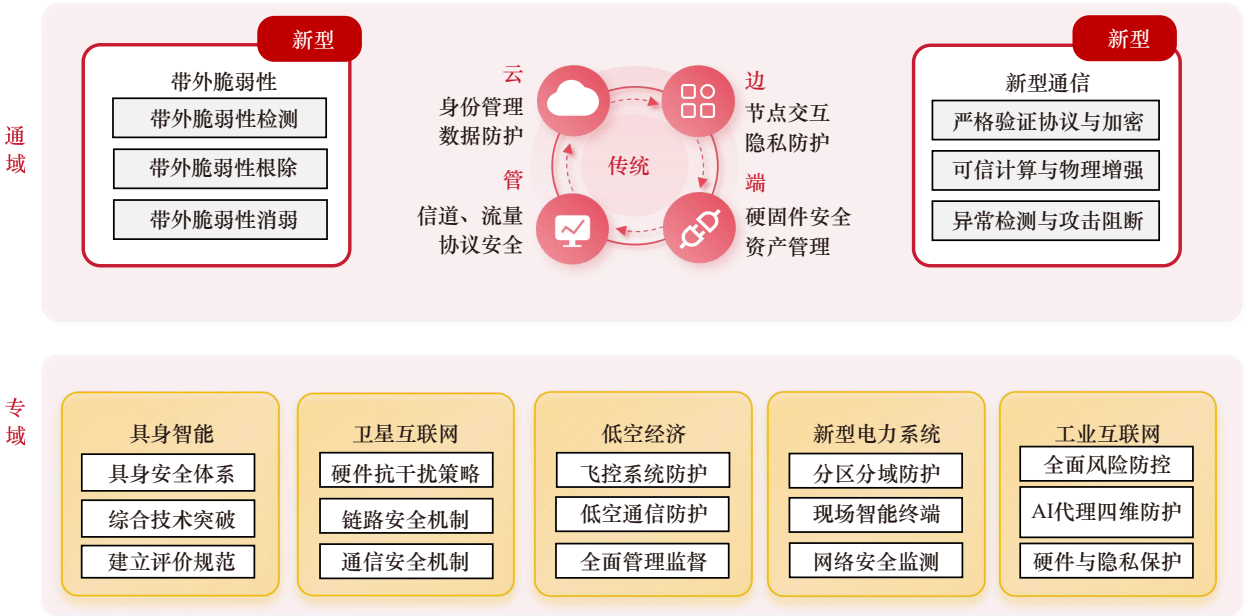

图4 关基物联网“通域－专域”双层安全防护体系

（一）通域安全防护

（1）云侧防护。云计算作为物联网的核心支撑平台，在数据存储与处理过程中面临数据集中化、虚拟化复杂等安全挑战[24]。当前云安全防护已形成四大技术体系：① 身份管理层面，采用联合认证和无密码认证技术，并通过分层证书架构实现设备认证；② 数据保护层面，构建端到端加密体系，结合差分隐私和区块链技术保障数据全生命周期安全；③ 虚拟化安全层面，通过可信执行环境、微隔离等技术防范容器逃逸等风险；④ 威胁防护层面，融合动态沙箱和机器学习检测，建立行为基线识别异常活动。

（2）管侧防护。物联网通信管道作为连接“云–边–端”的关键纽带，面临协议碎片化、开放信道威胁及复杂流量攻击等安全挑战。当前防护体系主要从三个层面构建：① 信道安全层面，采用跳频扩频、物理层动态密钥和信道指纹认证等技术，其中量子密钥分发[25]已在关键场景试点；② 协议安全层面，通过封装网关加固传统工业协议，为轻量级协议设计优化方案，针对RedCap等新型轻量化通信技术，制定与之能力匹配的轻量级安全协议框架，并运用模糊测试评估私有协议风险；③ 流量安全层面，结合加密流量元数据分析和深度学习异常检测，并借助边缘计算实现分布式实时分析。

（3）边侧防护。边缘计算作为物联网的关键组件，在降低延迟的同时面临物理安全、数据隐私等多重威胁。当前防护体系主要从三方面构建：① 流量安全层面，采用轻量级深度包检测和分布式机器学习分析，结合数字孪生技术实现仿真测试；② 节点交互安全层面，通过硬件指纹、国密（SM2）算法和区块链认证确保身份可信，并利用可信执行环境隔离敏感计算；③ 隐私保护层面，运用同态加密、k–匿名化和差分隐私等技术进一步保障边缘侧数据安全。

（4）端侧防护。物联网终端设备作为直接连接物理世界的“神经末梢”，面临物理篡改、固件漏洞、弱认证等安全威胁。当前防护体系主要从三个维度构建：① 硬件安全层面，采用可信平台模块建立信任根，结合物理不可克隆函数[26]防仿冒，探索适用于无源节点的超轻量级物理不可克隆认证机制，并部署抗侧信道攻击技术；② 固件安全层面，通过安全启动建立信任链，实施运行时防护，采用差分更新等轻量级固件升级方案，对于智能传感器等固件更新困难的设备，应强化启动镜像的完整性校验与运行时行为监控；③ 身份认证层面，从数字证书向动态认证演进，结合行为特征分析实现连续认证，并利用区块链技术强化资产管理。

（5）带外脆弱性防护。带外脆弱性作为硬件与系统间非理想映射所暴露的隐蔽风险，当前检测与防护技术仍处于发展阶段，主要分为检测、根除与消弱三类路径：① 脆弱性检测层面，人工渗透测试结合电磁、激光等物理注入手段仍是主流方式，但依赖专家经验，效率较低。新兴仿真工具（如EMSIM、HyPFuzz）[27,28]通过模拟硬件响应及多场景行为进行漏洞预测，在提升覆盖率与精度之间仍需权衡。物理测试手段则借助功耗、电磁辐射等侧信道信息识别风险点，具备较强实用性。② 脆弱性根除层面，聚焦于阻断非理想映射链路、修正错误感知路径，但常受制于系统设计的功能与成本约束。③ 脆弱性消弱层面，对于难以根除的漏洞，引入异常信号监测、输入输出混淆、攻击面缩减等手段，有效抑制潜在危害。未来，带外防护方向应聚焦高精度多模态检测模型、多源感知信息融合机制及低开销部署技术，构建以“理论–标准–演练–工具–架构”为核心的多层防护体系，为AI物联网、数字孪生等新兴场景提供可信保障。

（6）新型通信技术防护。目前针对新型通信技术的防护聚焦于三个层面：应用层、网络层与物理层。① 应用层安全层面，作为新型通信技术防护的核心内容，分为六大场景：在沉浸式通信方面，为应对超大流量与超高速率威胁，形成了密码学、行为认证与弹性架构的三重协同防御；超大规模连接场景依赖多维度分层策略，强化对海量低功耗终端的攻击识别[29]；高可靠低时延服务采用轻量化安全机制，简化协议以兼顾性能与防护；在AI融合通信方面则聚焦算法安全、数据可靠性及大模型风险管控；在通感一体方面使用以物理层安全技术为核心的安全防御策略，侧重隐私保护与数据完整性机制；泛在连接采用跨域边界防护及协议一体化设计，应对开放时变网络风险。② 网络与物理层面，主要防护策略为使用多种加密技术保障通信与终端安全，同时通过联邦学习与对抗训练增强相关基础设施的抗侵入能力。未来，亟需构建“通信–感知–

计算–智能”四位一体的内生安全体系，推进多模信任架构、区块链、量子安全通信与自适应动态防护机制，强化从协议到模型的纵深控制，夯实新型通信网络的可信基础。

总体而言，尽管通域防护体系已初具雏形，但在应对未来攻击挑战方面仍存在诸多不足：云侧防护难以抵御量子计算破解与后门攻击，管侧对加密流量识别与隐蔽通道的防护能力有限，边侧节点策略存在性能损耗大与协同困难等问题，端侧设备则面临防护部署率低与更新滞后的风险；各层级间联动机制薄弱，威胁情报共享不足，整体呈现“短板制约”效应。与此同时，带外脆弱性与新型通信技术的防护研究尚处于起步阶段，现有成果多为局部试验，尚未形成可支撑实战部署的系统能力。因而，通域安全防护体系亟需持续演进，向协同感知、动态响应与纵深联动方向拓展：主体层面应建立统一安全控制平面与策略编排框架，实现安全策略的全局一致性与多域协同部署；感知层面应构建跨域威胁情报共享与联合检测体系，利用知识图谱与安全大模型提升异常行为的识别准确率；响应层面应引入智能自适应算法，实现策略的实时调整与风险闭环响应。上述机制协同运作，形成“通域统一保障”以筑牢关键信息基础设施物联网的统一安全底座。

（二）专域安全防护

（1）具身智能防护。为构建安全可靠的具身智能体系，当前已建立了涵盖标准制定、技术防护、评测验证与科学治理的综合防护框架。① 标准层面，对于本体安全、交互安全和应用安全等，多维标准体系已经形成，包括基础术语定义、场景分级规范、技术指标要求以及标准化评测流程。② 技术层面，全链路安全防护技术、可信具身智能的价值对齐与策略自解释技术的突破提高了具身智能系统对多种威胁的快速响应能力；在数据防护方面，已构建从传感器端到数据应用的隐私保护体系，并采用联邦学习等隐私计算技术；利用核心元器件自主可控保障软硬件供应链安全。③ 评测层面包含多模态攻击样本测试数据集的制作与虚实结合的仿真评测平台的搭建，重点检测算法鲁棒性、硬件带外脆弱性等指标，为科学评测体系的形成奠定了良好基础。④ 治理层面，已落实全生命周期监管，模型、硬件备案制度和“黑匣子”溯源机制的确立明确了事故责任划分；多主体协同治理促进了 AI 安全、硬件安全与社会伦理等领域的交叉融合。未来，在具身智能方向需加强基础理论研究与产业转化，培养兼具 AI 算法、硬件安全和法律伦理素养的复合型人才，形成“研发–防护–治理”的良性生态，确保具身智能发展既保持创新活力又具备可靠的安全基线。

（2）卫星互联网防护。卫星互联网系统安全防护构建了覆盖硬件、链路、认证和网络的综合防御体系。① 硬件安全层面，采用了硬件信任根[30]和安全启动链确保系统的完整性，如 Starlink 部署 STSAFE-A110 安全芯片实现固件签名验证，并通过空中下载技术更新快速修复漏洞。② 链路安全层面，采用动态频谱捷变、跳频扩频和自适应调制编码技术，结合激光通信和波束成形提升抗干扰能力。③ 认证安全层面，通过局域网地址随机化防止终端追踪，增强用户隐私保护。④ 网络安全层面，基于零信任架构实施最小权限原则，采用 AES-256 端到端加密，并部署 AI 驱动的威胁检测系统。军事级扩展功能如量子密钥分发预备架构和多层级跳频进一步提升防护等级。未来，应做到全面部署硬件信任根和防篡改设计并采用动态波形和软件定义无线电架构来进一步提高针对卫星互联网的安全保障。

（3）低空经济防护。当前低空经济无人系统安全防护构建了“跨域可信、数据驱动、动态验证、策略自适应”的综合防护体系。① 系统安全层面，采用了轻量级可信执行环境（TEE）和安全引导链确保系统完整性，部署多源传感器异常检测机制识别欺骗攻击，并运用模糊测试技术发现软件漏洞。② 网络防护层面，实施轻量级国密算法加密和物理层设备指纹认证，建立协作干扰抑制机制应对信道攻击，采用图神经网络进行异常行为检测。③ 任务安全层面，强调数据全生命周期保护，应用同态加密和安全多方计算技术，部署 AI 模型防窃取机制和基于自编码器的任务轨迹异常检测系统。④ 管理安全层面，采用智能策略编排技术，实现了安全策略的实时动态调整；建立了全链路审计机制，确保操作可追溯；通过多域联防平台实现安全态势协同监测，同时结合区块链、AI 等技术，形成闭环管理防护体系。未来，需重点突破形式化

验证的飞控系统、基于物理层特征的内生安全技术、隐私保护计算平台和标准化治理框架。通过构建覆盖系统、网络、任务、管理的纵深防御体系，实现从硬件隔离到行为监测的全方位防护，为低空经济发展提供可靠的安全保障。

（4）新型电力系统防护。新型电力系统安全防护体系建设聚焦“分区分域、边端防护、边界安全、数据防护、态势监测”五个关键领域。① 分区分域层面，构建了生产控制区、管理信息区和安全接入区的三级防护体系，采用电力专用隔离装置实现物理隔离，对分布式光伏等外部接入实施加密认证和双向身份验证。② 现场边端层面，采取分级策略：关键涉控终端部署高级威胁检测，普通物联终端配置安全网关和行为分析系统，资源受限设备采用轻量级认证方案，并通过模块化架构实现安全功能灵活部署。③ 网络边界层面，采用国产密码算法，加强无线通信安全检测，在光伏电站、虚拟电厂等场景部署专用加密认证设备，利用边缘计算节点管控第三方设备接入。④ 数据安全层面，针对云化业务开发微服务安全组件，重点保护调控指令等核心数据，建立多维度风险分析模型。⑤ 感知监测层面，实现全业务覆盖，通过嵌入式探针构建“端–边–云”协同监控体系，实时感知新型电力设备的安全状态。未来，为应对新型电力系统网络安全挑战，需加快布局零信任、内生安全、AI、量子密码及隐私计算等技术，强化防护边界、终端接入与数据流转安全。

（5）工业互联网防护。工业互联网安全防护已构建了融合技术创新与场景适配的多层次体系，围绕AI智能体、内容真实性、硬件环境与数据隐私等关键风险开展全链路防御。① AI智能体安全层面，构建“身份–权限–行为–环境”四维体系，基于RBAC[31]实现细粒度权限控制，结合属性加密技术保障通信链路安全。② 深伪内容风险层面，采用多模态融合检测策略，利用视觉、红外、声纹等传感器交叉验证内容真实性。③ 硬件环境层面，形成以TEE为核心的“芯片–固件–系统–应用”全栈防护框架，借助ARM TrustZone[32]将关键控制逻辑封装于安全域中。④ 数据隐私保护层面，结合同态加密、零知识证明与区块链智能合约，设计安全可信的数据交换协议。未来，应加快构建可信AI基础设施，利用数字孪生与安全沙箱打造仿真测试环境，推进联邦学习与区块链深度融合，强化TEE与AI加速硬件协同设计，并前瞻布局量子加密机制。通过技术创新与生态协同，逐步形成具备强韧性与适应性的工业互联网安全体系。

当前，专域场景下的关基物联网安全防护体系呈现出高度定制化与精细化的特征，需针对不同领域的技术架构与风险特性构建差异化防御机制。未来，专域防护需持续突破形式化验证、隐私计算、量子加密等前沿技术，关注技术防护、管理治理与产业生态的协同发展，并将更多的新兴关基物联网应用纳入专域场景防护，构建兼顾领域特性和发展弹性的专业化关基物联网安全体系。

五、关基物联网安全发展建议和未来展望

面对“云–管–边–端”体系持续扩展与专有场景安全风险加剧的双重挑战，关基物联网安全保障体系亟需从局部、静态和孤立的防护模式，转向全域覆盖、动态协同与智能自适应的体系建设。为实现这一目标，应在战略、制度、技术、人才与国际五个层面系统推进，构建具备持续演进能力的安全治理新范式。

（1）战略统筹方面。将关基物联网安全纳入国家网络安全整体战略，建立跨部门、跨行业的国家级统筹协调机制，形成覆盖全域的统一安全底线，破解当前多头管理、标准不一的治理困境；强化顶层设计与行业落地的协同，在能源、交通、工业等重点领域制定差异化安全战略，推动安全政策与产业发展同频共振；建立覆盖“物理域–信息域–认知域”的全域风险映射机制，绘制全国关基物联网安全风险图谱，实现跨行业威胁情报实时共享与联动处置；设立国家级专项基金，引导社会资本投入关基物联网安全领域，形成长效投入机制。

（2）制度建设方面。构建“基础通用–行业专用–动态更新”的分层标准体系，细化各行业安全基线，针对具身智能、低空经济等新兴场景制定专项规范；建立跨域冲突协调与统一标准映射机制，实现全域策略与行业专属标准之间的高效兼容；建立全生命周期合规治理机制，推行设备安全准入制度与供应链安全审查机制，强化厂商安全责任，做到快速修补和更新[33]，同时明确关基运营者、技术服务商的安全权责，创新算法安全与自主决策的责

任认定规则，建立容错与追溯并行的管理制度；此外还需推动国际标准与自主标准的衔接，在工业互联网、卫星通信等领域主导制定符合我国技术路线的国际规则，提升制度话语权。

（3）技术体系方面。针对当前防护体系中存在的云侧后门风险、通信加密盲区、边端资源约束与终端防护滞后等问题，建议发展以AI驱动的跨层安全检测体系，构建跨行业安全态势感知中枢，实现对未知威胁的早期预警与自动响应；通过策略映射引擎与智能冲突解析算法，建立跨域安全协同中枢，在多域间自动识别并协调安全策略冲突；构建基于零信任架构的动态防御范式，开发适配“云–边–端”异构环境的分布式认证与权限管理技术；强化核心技术自主可控，突破可信芯片、工业操作系统等“卡脖子”技术，构建“芯片–固件–协议–平台”的自主安全产业链，推广国密算法与内生安全技术在关键场景的深度应用。针对新型风险，还应加快带外脆弱性分析，AI通信系统安全性验证，面向RedCap、无源物联等使能技术的专用安全框架研究，以及新型模态感知系统的防护机制落地。对于专域场景方面开展针对性技术攻关，基于通用防护体系开展定制增强。

（4）人才培养方面。鼓励高校与重点实验室联合开设新兴课程，如卫星通信安全、感知融合安全、联邦智能隐私保护等，推动安全与AI、通信工程、控制科学等多学科的深度交叉。同时完善职业认证与继续教育体系，建立从顶尖科学家到一线运维工程师的多层次人才梯队，强化应对新型威胁的实战能力。此外，需加大科研资助力度，设立重点专项推动基础性与颠覆性技术研究，培养具备国际竞争力的安全创新团队。

（5）国际协同方面。在单边主义抬头和科技竞争加剧的背景下，我国应更加主动融入国际网络安全治理体系，积极参与国际标准组织的工作，推动在6G安全、AI治理、量子加密、低空经济管理等新兴领域形成以我为主或共同主导的国际标准。同时，探索建立跨境关基物联网安全事件通报与协作机制，倡导开放、透明、互信的合作氛围，共同应对供应链安全、跨境数据流动和网络犯罪等全球性挑战，提升我国在国际物联网安全规则制定中的话语权。

综上，关基物联网将向更高程度的智能化、泛在化和自治化方向发展，其安全边界将持续扩展，威胁形态更趋复杂。通过战略引领、法规保障、技术驱动、人才支撑和国际协作的多路径协同，构建起“通域统一保障+专域定制增强”的一体化安全体系，最终实现关基物联网的可控、可信与可靠运行，为国家数字竞争力的提升奠定坚实的安全基石。

利益冲突声明

本文作者在此声明不存在任何利益冲突或财务冲突。

Received date: August 13, 2025; **Revised date:** October 21, 2025

Corresponding author: Cheng Yushi is a research fellow from College of Electrical Engineering, Zhejiang University. Her major research field is Internet of Things (IoT) security. E-mail: yushicheng@zju.edu.cn

Funding project: Chinese Academy of Engineering project “Study on Risks Associated with Emerging Technologies and Applications in Cyberspace Security” (2023-JB-01); National Natural Science Fund Project (61925109, 62222114)

参考文献

[1] 张弛, 崔占华. 美国关键基础设施安全管理综述 [J]. 信息安全研究, 2017, 3(8): 736–746.
Zhang C, Cui Z H. Analysis on American critical infrastructure security management [J]. Journal of Information Security Research, 2017, 3(8): 736–746.

[2] 杨婷, 左晓栋. 美国提升关键基础设施网联设备安全措施分析 [J]. 工业信息安全, 2023 (1): 11–17.
Yang T, Zuo X D. Study on US actions to better secure Internet-connected devices of critical infrastructure [J]. Industry Information Security, 2023 (1): 11–17.

[3] Djenna A, Harous S, Saidouni D E. Internet of Things meet Internet of threats: New concern cyber security issues of critical cyber infrastructure [J]. Applied Sciences, 2021, 11(10): 4580.

[4] Shi W S, Cao J, Zhang Q, et al. Edge computing: Vision and challenges [J]. IEEE Internet of Things Journal, 2016, 3(5): 637–646.

[5] Cárdenas A A, Amin S, Sastry S. Research challenges for the security of control systems [R]. San Jose. The 3rd Conference on Hot Topics in Security, 2008.

[6] Nguyen V L, Lin P C, Cheng B C, et al. Security and privacy for 6G: A survey on prospective technologies and challenges [J]. IEEE Communications Surveys & Tutorials, 2021, 23(4): 2384–2428.

[7] Abusaimeh H. Virtual machine escape in cloud computing services [J]. International Journal of Advanced Computer Science and Applications, 2020, 11(7): 327–331.

[8] Chen Y, Sambo Y A, Onireti O, et al. A survey on LPWAN-5G integration: Main challenges and potential solutions [J]. IEEE Access, 2022, 10: 32132–32149.

[9] Marzano A, Alexander D, Fonseca O, et al. The evolution of bashlite and mirai IoT botnets [R]. Natal: 2018 IEEE Symposium on Computers and Communications (ISCC), 2018.

[10] Giechaskiel I, Rasmussen K. Taxonomy and challenges of out-of-band signal injection attacks and defenses [J]. IEEE Communica-

tions Surveys & Tutorials, 2020, 22(1): 645–670.

[11] Yang F C, Dan Z H, Pan K K, et al. ReThink: Reveal the threat of electromagnetic interference on power inverters [EB/OL]. (2024-09-26)[2025-07-08]. https://arxiv.org/abs/2409.17873.

[12] Luo S Q, Nguyen A, Farooq H, et al. Eavesdropping on controller acoustic emanation for keystroke inference attack in virtual reality [R]. San Diego: 2024 Network and Distributed System Security Symposium, 2024.

[13] Ba Z J, Zheng T H, Qin Z, et al. Accelerometer-based smartphone eavesdropping [R]. London: The 26th Annual International Conference on Mobile Computing and Networking, 2020.

[14] Shakib K H, Rahman M, Islam M, et al. Impersonation attack using quantum shor's algorithm against blockchain-based vehicular ad-hoc network [J]. IEEE Transactions on Intelligent Transportation Systems, 2025, 26(5): 6530–6544.

[15] Thombre R, Jajodia B. Experimental analysis of attacks on RSA & Rabin cryptosystems using quantum shor's algorithm [R]. Online: International Conference on Women Researchers in Electronics and Computing, 2021.

[16] Wen C C, Liang J Z, Yuan S H, et al. How secure are large language models (LLMs) for navigation in urban environments? [EB/OL]. (2024-02-14)[2025-07-08]. https://arxiv.org/abs/2402.09546.

[17] Zhang H T, Zhu C Y, Wang X L, et al. BadRobot: Jailbreaking embodied LLMs in the physical world [EB/OL]. (2024-07-16)[2025-07-08]. https://arxiv.org/abs/2407.20242.

[18] 代玥玥, 辛鑫, 赵薏皓, 等. 空天地一体化通信网络安全 [J]. 移动通信, 2025, 49(10): 136–147.
Dai Y Y, Xin X, Zhao Y H, et al. Security of space-air-ground integrated communication networks [J]. Mobile Communications, 2025, 49(10): 136–147.

[19] Papadimitratos P, Jovanovic A. GNSS-based positioning: Attacks and countermeasures [R]. San Diego: 2008 IEEE Military Communications Conference, 2009.

[20] 张依, 谢思. 我国低空经济监管的演进逻辑、困境挑战与创新路径 [J]. 中国流通经济, 2025, 39(10): 83–97.
Zhang Y, Xie S. The evolutionary logic, challenges and innovative paths of low-altitude economy regulation in China [J]. China Business and Market, 2025, 39(10): 83–97.

[21] European Union Agency for Network and Information Security (ENISA). Good practices for security of Internet of Things in the context of smart manufacturing [R]. Heraklion: ENISA, 2018.

[22] Huitsing P, Chandia R, Papa M, et al. Attack taxonomies for the modbus protocols [J]. International Journal of Critical Infrastructure Protection, 2008, 1: 37–44.

[23] Alsabbagh W, Langendörfer P. You are what you attack: Breaking the cryptographically protected S7 protocol [R]. Pavia: 2023 IEEE 19th International Conference on Factory Communication Systems (WFCS), 2023.

[24] Zhou J, Cao Z F, Dong X L, et al. Security and privacy for cloud-based IoT: Challenges [J]. IEEE Communications Magazine, 2017, 55(1): 26–33.

[25] Scarani V, Bechmann-Pasquinucci H, Cerf N J, et al. The security of practical quantum key distribution [J]. Reviews of Modern Physics, 2009, 81(3): 1301–1350.

[26] Herder C, Yu M D, Koushanfar F, et al. Physical unclonable functions and applications: A tutorial [J]. Proceedings of the IEEE, 2014, 102(8): 1126–1141.

[27] Tan T K, Raghunathan A, Jha N K. EMSIM: An energy simulation framework for an embedded operating system [R]. Phoenix-Scottsdale: 2002 IEEE International Symposium on Circuits and Systems, 2002.

[28] Chen C, Kande R, Nguyen N, et al. HyPFuzz: Formal-assisted processor fuzzing [EB/OL]. (2023-06-24)[2025-07-08]. https://arxiv.org/abs/2304.02485.

[29] Sattar D, Matrawy A. Towards secure slicing: Using slice isolation to mitigate DDoS attacks on 5G core network slices [R]. Washington DC: 2019 IEEE Conference on Communications and Network Security (CNS), 2019.

[30] Dwoskin J S, Lee R B. Hardware-rooted trust for secure key management and transient trust [R]. Alexandria: The 14th ACM Conference on Computer and Communications Security, 2007.

[31] Sandhu R S. Role-based access control [M]// Zelkowitz M V, ed. Advances in Computers. Amsterdam: Elsevier, 1998: 237–286.

[32] Pinto S, Santos N. Demystifying arm TrustZone: A comprehensive survey [J]. ACM Computing Surveys, 2019, 51(6): 1–36.

[33] European Union Agency for Network and Information Security (ENISA). Baseline security recommendations for IoT in the context of critical information infrastructures [R]. Heraklion: ENISA, 2017.