2024 年工业互联网安全年报

1. 执行摘要

2024 年，工业互联网安全领域面临着日益严峻的挑战和深刻的变革。随着全球工业数字化转型的加速，工业控制系统（ICS）和操作技术（OT）环境的互联互通性显著增强，与此同时，网络威胁的复杂性和针对性也达到了前所未有的程度。本年度报告旨在全面分析 2024 年工业互联网安全态势，总结关键威胁、漏洞利用趋势、重大安全事件，解读政策法规的演进，并提出战略性防御建议和未来展望。

回顾 2024 年，勒索软件和高级持续性威胁（APT）依然是工业领域最主要的网络威胁类型，其攻击手段愈发具有 OT 针对性，对关键基础设施的潜在破坏力不容小觑 [1]。供应链攻击的风险持续凸显，攻击者利用信任链条中的薄弱环节，对工业企业造成了广泛影响。同时，人工智能（AI）技术在网络攻击中的应用初露锋芒，为威胁行为者提供了新的工具和途径，进一步加剧了攻防不对称的局面 [3]。

在政策法规层面，中国工业和信息化部于 2024 年初发布的《工业控制系统网络安全防护指南》成为本年度的标志性事件 [5]。该指南的更新体现了国家层面对于工业控制系统安全防护的重视，并为企业构建结构化的网络安全防御体系提供了明确指引。这一举措也反映出全球范围内，各国政府和监管机构正积极应对工业互联网发展带来的安全挑战，但具体路径和侧重点有所差异，形成了复杂的国际合规环境。

然而，工业互联网安全领域依然面临诸多挑战。OT/ICS 安全专业人才的短缺问题尤为突出，成为制约企业安全能力提升的关键瓶颈 [7]。传统 OT 系统的老旧性与新兴工业物联网（IIoT）设备安全管理的复杂性并存，给企业带来了双重压力。

面对严峻的安全形势，业界对于构建更具韧性的安全体系已形成广泛共识。零信任架构、增强威胁情报能力、提升事件响应速度和效果，成为企业在 2024 年及未来一段时间内的战略核心。

展望未来，AI 技术在网络攻防两端的深度应用将是主要趋势之一。随着 IIoT 设备的激增和工业系统向云端迁移的加速，攻击面将持续扩大，对安全防护提出更高要求。工业企业必须认识到，网络安全已不再仅仅是 IT 部门的职责，而是关乎企业生存和发展的核心业务风险。在数字化浪潮下，将安全融入工业生产的全生命周期，构建主动、智能、协同的防御体系，是保障工业互联网健康、可持续发展的必然选择。

2. 2024 年工业网络安全威胁全景

2024 年，工业网络安全领域见证了威胁形势的持续演变和复杂化。随着工业企业数字化

转型的深入，原先相对封闭的操作技术（OT）环境日益暴露于更广泛的网络威胁之下。攻击者不仅在数量上有所增加，其技术手段和攻击目标也更具针对性，对全球工业生产和关键基础设施构成了前所未有的挑战。

2.1 主要全球威胁：APT、勒索软件与复杂恶意软件

高级持续性威胁 (APT)

APT 攻击在 2024 年依然保持高度活跃，对全球工业领域构成了严重威胁。这些攻击通常由具有国家背景或有组织犯罪集团支持的实体发起，目标明确，持续时间长，隐蔽性强。奇安信威胁情报中心的数据显示，Kimsuky、Lazarus、摩诃草（Transparent Tribe）、蔓灵花（Confucius）以及 APT28 等组织是 2024 年最为活跃的 APT 组织之一[1]。从地域分布来看，乌克兰、中国、美国、以色列和韩国等国家遭受 APT 攻击的频率较高，这在一定程度上反映了地缘政治冲突在网络空间的延伸[1]。

APT 组织针对工业领域的攻击往往具有明确的战略意图，如窃取关键技术信息、知识产权，或对关键基础设施进行预置和破坏，以获取地缘政治优势[3]。攻击手段日益复杂，包括利用零日漏洞进行初始渗透和横向移动，以及采用“伪旗”行动（false flag operations）来混淆攻击来源，增加溯源难度[9]。国家互联网应急中心（CNCERT）披露的案例显示，针对中国高科技企业的 APT 攻击中，攻击者利用了微软 Exchange 服务器漏洞，并部署了高度隐蔽的内存驻留木马，以窃取敏感数据和实现对内网关键设备的持久控制[10]。

勒索软件

勒索软件在 2024 年继续成为工业企业面临的首要威胁之一，其攻击频率、影响范围和索要赎金的数额均呈现上升趋势[1]。绿盟科技指出，工业互联网安全面临勒索软件的严峻挑战[12]。攻击者不再仅仅满足于加密数据，而是越来越多地采用“双重勒索”（数据窃取+数据加密）甚至“多重勒索”的策略，对受害者施加更大压力。

值得注意的是，勒索软件攻击正越来越多地直接影响 OT 环境，导致生产中断。根据 Dragos 的报告，2024 年针对工业组织的勒索软件团伙数量从 2023 年的 50 个激增至 80 个[2]。在其响应的勒索软件事件中，高达 75%导致了 OT 系统的部分停运，更有 25%导致了 OT 系统的全面停运[2]。制造业依然是勒索软件攻击的重灾区[2]。Clop 和 Black Basta 等勒索软件组织在 2024 年表现活跃，例如 Clop 利用 Cleo 文件传输产品中的漏洞发起了多起攻击[14]。这种通过直接中断物理生产过程来施压的策略，显示出攻击者对工业流程的理解正在加深，其目标也从单纯的数据勒索转向了对核心业务运营的直接威胁。

针对 OT 的恶意软件

2024 年出现了更多专门针对操作技术（OT）环境和工业控制系统（ICS）协议的恶意软件，这标志着攻击者正在投入更多资源研发针对性攻击工具。Dragos 在其年度报告中披露了两个新的 OT 恶意软件家族：FrostyGoop 和 Fuxnet [2]。

- **FrostyGoop**：于 2024 年初首次发现，该恶意软件专门设计用于操纵 Modbus TCP/502 通信。它能够篡改或伪造正常的工业过程指令，绕过传统杀毒软件的检测，并可能导致物理基础设施的损坏。一个典型的案例是其被用于攻击乌克兰的区域供暖系统，导致超过 600 栋公寓楼在严寒中供暖中断 [2]。
- **Fuxnet**：该恶意软件被用于攻击莫斯科市的市政传感器网络，通过覆写传感器网关的固件，使其无法正常工作 [13]。

这些 OT 专用恶意软件的出现，表明攻击者对 ICS 协议和工业流程的理解达到了新的水平，对工业安全构成了更为直接和严重的威胁。这不仅仅是 IT 层面数据泄露的风险，更是可能导致物理损坏、生产停滞甚至安全事故的风险。

2.2 工业环境中的关键漏洞与利用趋势

工业环境的独特性使其面临着特殊的漏洞挑战。2024 年，以下几个方面的漏洞和利用趋势尤为突出：

遗留系统与补丁困境：大量仍在运行的遗留 OT 系统在设计之初并未充分考虑网络安全因素，且由于其关键性，打补丁的窗口期非常有限，甚至难以实施，这使得它们成为攻击者长期利用的薄弱环节 [5]。

互联网暴露的 ICS/OT 设备：尽管业界一再强调隔离的重要性，但仍有大量 ICS/OT 设备直接或间接暴露在互联网上。SANS 的报告指出，近一半（47%）的 ICS 事件源于可从互联网访问的设备和远程服务 [8]。Dragos 在调查 FrostyGoop 事件时发现，全球有超过 46,000 个通过 Modbus 协议通信的 ICS 设备暴露于互联网 [2]。这些暴露的设备为攻击者提供了直接的攻击入口。

默认凭证与弱访问控制：使用默认出厂密码或弱密码，以及缺乏严格的访问控制策略，依然是工业环境中普遍存在的低级错误，极易被攻击者利用 [5]。

网络深层漏洞：攻击者一旦突破外围防御，往往能在目标网络的深层发现更多可利用的漏洞。Dragos 的研究发现，其分析的漏洞中有 70%位于 ICS 网络的深处，39%的漏洞可能导致操作员失去对工业过程的视野和控制，22%的漏洞通告涉及可从网络利用且面向边界的漏洞（较 2023 年的 16%有所上升）[2]。这表明，即使是看似安全的内部网络，也可能暗藏风险。

软件漏洞持续被利用：通用软件（如微软 Exchange [10]、VPN 解决方案如 Ivanti [16]、文件

传输工具如 Cleo [14]）和开源组件（如 XZ Utils [16]）中的已知漏洞持续被攻击者利用，对工业系统造成影响。

缺乏有效的网络监控：SANS 的报告显示，52%的组织在 ICS/OT 网络监控和异常检测方面能力有限或完全缺失 [8]。这使得许多攻击行为在发生后很长时间内都未被发现，错失了最佳的响应时机。

2.3 攻击向量分析：供应链、远程访问与新兴方法

2024 年，攻击者利用多种途径渗透工业网络，其中供应链攻击、远程访问漏洞利用以及一些新兴方法值得特别关注。

供应链攻击：供应链攻击已成为一种高效且影响广泛的攻击手段。攻击者通过攻击安全性相对较弱的第三方供应商、软件组件或托管服务提供商（MSP），将其作为跳板，进而入侵其最终目标——通常是安全防护更严密的大型工业企业 [5]。XZ Utils 后门事件便是一个典型的例子，恶意代码被植入广泛使用的开源库中，对全球众多 Linux 系统构成了潜在威胁 [16]。这种攻击方式利用了现代工业生态系统中普遍存在的信任关系，其隐蔽性和破坏性极高。

远程访问漏洞利用：随着远程办公和远程运维的普及，VPN 等远程访问工具成为工业网络的重要组成部分，同时也成为了攻击者重点关注的目标。Ivanti Connect Secure VPN 的多个零日漏洞在 2024 年初被大规模利用，影响深远 [16]。不安全的远程桌面协议（RDP）配置也持续为攻击者提供便利。中国工信部发布的 2024 年《工业控制系统网络安全防护指南》中，也特别强调了远程访问安全的重要性 [5]。

AI 赋能的攻击：人工智能技术开始被攻击者用于提升攻击效率和效果。例如，利用 AI 生成更具欺骗性的钓鱼邮件和深度伪造内容，或开发能够实时调整行为以规避检测的自适应恶意软件 [3]。AI 技术的应用降低了发起复杂攻击的技术门槛，使得更多技术水平不高的攻击者也能构成威胁 [3]。

内部威胁：尽管 2024 年的具体案例数据不多，但对内部风险管理的关注度正在提升 [12]。内部人员（无论是恶意还是无意的）造成的安全事件，其潜在破坏力不容忽视。

黑客行动主义 (Hacktivism)：出于地缘政治动机的黑客行动主义团体，在 2024 年也加强了对 OT 环境的攻击，试图扰乱能源、水务等关键公用事业的正常运行，部分攻击甚至达到了 ICS 网络杀伤链的第二阶段（武器投递和执行）[2]。

综合来看，2024 年的工业网络安全威胁呈现出高度的复杂性、针对性和破坏性。专门针对 OT 环境的攻击工具和团伙的出现，表明攻击者对工业领域的渗透正在深化。以往被认

为是安全孤岛的 OT 网络，在数字化浪潮的推动下，其边界日益模糊，传统防御理念面临严峻考验。特别是勒索软件，其攻击策略已从单纯的数据加密转向对物理生产的直接威胁，这种转变对工业企业构成了更为致命的打击。

下表总结了 2024 年工业网络安全领域的主要威胁及其趋势：

表 2.1：2024 年主要工业网络安全威胁与趋势

威胁类型	主要技战术特点 (TTPs) / 特征	代表性案例/组织	主要受影响工业领域
APT 攻击	零日漏洞利用、长期潜伏、针对性情报窃取、伪旗行动、地缘政治动机	Kimsuky, Lazarus, APT28, UNC5221, 针对中国的 APT 攻击 [1]	关键制造、国防、能源、高科技
勒索软件	双重/多重勒索、直接攻击 OT 导致停产、赎金高昂、团伙间协作复杂	Clop, Black Basta, 针对工业组织的 80 个团伙 [1]	制造业、医疗、能源、关键基础设施
OT 专用恶意软件	针对特定 ICS 协议（如 Modbus）进行操纵、可造成物理破坏、绕过传统 IT 安全检测	FrostyGoop, Fuxnet [2]	能源（供暖）、市政（传感器网络）
供应链攻击	攻击软件供应商、开源组件、MSP，利用信任关系进行渗透	XZ Utils 后门事件 [4]	广泛影响所有使用受感染组件/服务的行业
AI 赋能的攻击	AI 生成钓鱼邮件/深度伪造内容、自适应恶意软件、自动化漏洞扫描与利用	尚无大规模公开披露的特定组织，但趋势已现 [3]	所有行业，尤其针对高价值目标

远程访问漏洞利用	利用 VPN、RDP 等远程访问工具的已知或未知漏洞进行初始渗透	Ivanti VPN 漏洞利用 [16]	所有依赖远程访问的工业环境
黑客行动主义	出于政治或意识形态动机，针对 OT 环境进行破坏或干扰，以扩大影响	针对能源、水务等公用事业的攻击 [2]	能源、水务、政府控制的关键基础设施

3. 聚焦中国：政策与工业互联网安全发展

2024 年，中国在工业互联网安全领域展现出积极的政策导向和持续的基础设施建设投入。面对日益严峻的网络安全挑战和自身工业互联网产业的蓬勃发展，中国政府将工业互联网安全置于国家战略层面，通过出台指导性政策、完善监测体系和推动技术创新，力图构建坚实的工业网络安全屏障。

3.1 深度解读：2024 工信部《工业控制系统网络安全防护指南》——关键变化与影响

2024 年 1 月，中国国务院官网发布了由工业和信息化部（MIIT）制定的《工业控制系统网络安全防护指南》（工信部网安〔2024〕14 号）（以下简称“新版指南”）[5]。这是对 2016 年发布的《工业控制系统信息安全防护指南》的重大修订和升级，旨在适应新时期工业控制系统面临的网络安全形势，指导企业提升防护水平，夯实新型工业化发展的安全根基 [5]。

权威性与演进：新版指南由国务院官网发布，发文主体为工信部，体现了国家层面政策发布的统一性和权威性。与 2016 版相比，新版指南的名称从“信息安全”变更为“网络安全”，范畴有所扩大，更全面地覆盖了工业控制系统在网络空间面临的各类安全风险，包括传统的信息安全、功能安全乃至物理安全的相关网络层面 [5]。此次修订也是为了更好地衔接《网络安全法》、《数据安全法》、《密码法》等上位法律法规的要求，应对工业企业数字化转型加速带来的日益增长的网络安全风险 [5]。

核心理念：新版指南的一个显著变化是强调“以保障业务可用性为防护重心” [5]。这一理念的提出，深刻反映了工业场景下业务连续性的极端重要性，安全防护措施的部署必须优先考虑不影响或最大限度减少对正常生产运营的干扰。

四大聚焦：新版指南的理论框架更加清晰，提出了“四个聚焦”，为企业构建工控安全防护体系提供了宏观指导 [5]：

1. **聚焦安全风险管控：**突出管理要素，提升工业企业工控安全管理能力。

2. **聚焦安全薄弱关键环节**：突出技术防护的重点和难点。
3. **聚焦易发网络安全风险**：突出安全运营的实战性和有效性。
4. **聚焦工业企业资源保障**：突出责任落实和基础支撑。

具体要求解读：新版指南围绕安全管理、技术防护、安全运营和责任落实四个方面，提出了 15 项共计 33 条指导性要求，较旧版的 11 项 30 条更为全面和细致[5]。

- **资产管理**：要求全面梳理 PLC、DCS、SCADA 等典型工控系统及相关设备、软件、数据等资产，建立并动态更新资产清单，明确资产责任人，并定期核查资产的“运行状态”和“安全状态”（如系统配置、权限分配、日志审计、病毒查杀、数据备份等）。特别强调对“重要工业控制系统”（参照 GB/Z 41288-2022 定义，通常指等保三级及以上的工控系统）建立清单并实施重点保护，其关键工业主机、网络设备、控制设备等应实施冗余备份[5]。
- **配置管理**：强化账户及口令管理，要求“禁用不必要的系统默认账户和管理员账户，及时清理过期账户”，并“及时根据安全防护需求变化调整配置”。对于默认口令或弱口令，考虑到工业场景的特殊性，要求“避免”而非绝对“禁止”。同时，要求建立工控系统和安全防护设备的安全配置清单并定期审计，重大配置变更前需进行严格安全测试[5]。
- **供应链安全**：要求在与工控系统厂商、云服务商、安全服务商等供应商签订协议时，明确各方在管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等方面的安全责任和义务。使用纳入网络关键设备目录的 PLC 等设备时，需确保其通过安全认证或安全检测符合要求[5]。
- **主机与终端安全**：要求在工程师站、操作员站、工业数据库服务器等主机上部署防病毒软件（可采用白名单技术），定期升级病毒库和查杀恶意软件（如勒索软件）。对具备存储功能的介质接入工业主机前进行恶意代码查杀。有计划地实施操作系统、数据库等系统软件和重要应用软件的升级。拆除或封闭不必要的外部设备接口（如 USB、光驱），关闭不必要的网络服务端口。对工业主机、工业智能终端设备、网络设备的访问实施用户身份鉴别，关键主机或终端的访问采用双因子认证[5]。
- **架构与边界安全**：根据业务特点对工业以太网、工业无线网络等组成的工业控制网络实施分区分域管理。部署工业防火墙、网闸等设备实现域间横向隔离。当工业控制网络与企业管理网或互联网连通时，实施网间纵向防护，并对网间行为开展安全审计。设备接入工业控制网络时应进行身份认证。应用 5G、WiFi 等无线通信技术组网时，制定严格的网络访问控制策略，对无线接入设备采用身份认证机制，定期审计无线访问接入点，关闭 SSID 广播。严格远程访问控制，原则上禁止工业控制系统面向互联网开通 HTTP、FTP、Telnet 等高风险通用网络服务；对确需开通的网络服务，应采取安全接入代理等技术进行用户身份认证和应用鉴权；远程维护时，使用 IPsec、SSL 等协议构建安全网络通道（如 VPN），并严格限制访问范围和授权时间，开展

日志留存和审计。在工业控制系统中使用加密协议和算法时应符合法律法规要求，鼓励优先采用商用密码[5]。

- **上云安全**：针对工业云平台的安全防护提出了要求。企业自建工业云平台时，应利用用户身份鉴别、访问控制、安全通信、入侵防范等技术，有效阻止非法操作和网络攻击。工业设备上云时，需对上云设备实施严格标识管理，设备接入工业云平台时采用双向身份认证，禁止未标识设备接入。业务系统上云时，应确保不同业务系统运行环境的安全隔离[5]。
- **应用安全**：访问 MES、组态软件和工业数据库等应用服务时，应进行用户身份认证，关键应用服务采用双因子认证，并严格限制访问范围和授权时间。工业企业自主研发的工控系统相关软件，上线使用前应通过安全性测试[5]。
- **系统数据安全**：要求定期梳理工控系统运行产生的数据，开展数据分类分级，识别重要数据和核心数据并形成目录。围绕数据收集、存储、使用、加工、传输、提供、公开等全生命周期环节，使用密码技术、访问控制、容灾备份等技术对数据实施安全保护。法律法规有境内存储要求的重要数据和核心数据应在境内存储，确需向境外提供的，应依法依规进行数据出境安全评估[5]。
- **安全运营**：包括监测预警（在工控网络部署监测审计设备或平台，采用蜜罐等威胁诱捕技术）、运营中心（有条件的企业可建立工控安全运营中心，利用 SOAR 等技术提升集中排查和快速响应能力）、应急处置（制定应急预案并定期演练，重要日志留存不少于六个月并定期备份，重要系统应用和数据定期备份及恢复测试）、安全评估（新建或升级工控系统上线前、网络连接前开展安全风险评估，重要工控系统每年至少开展一次防护能力评估）和漏洞管理（密切关注官方漏洞信息，及时升级或加固，重要系统漏洞补丁需测试验证后实施）[5]。
- **责任落实**：工业企业承担本企业工控安全主体责任，建立工控安全管理制度，明确责任人和责任部门，按照“谁运营谁负责、谁主管谁负责”的原则落实保护责任。强化企业资源保障，确保安全防护措施与工业控制系统“三同步”（同步规划、同步建设、同步使用）[5]。

新版指南的发布，其详尽和具有针对性的规定，无疑是中国政府对当前工业互联网安全形势的直接回应。中国工业互联网的快速发展（如[19]所述的核心产业规模预计在 2024 年达到 1.53 万亿元人民币），使其成为网络攻击的重要目标（如 CICS-CERT 重庆报告中提及的境外恶意网络行为[18]，以及 CNCERT 披露的针对性 APT 攻击[10]）。因此，新版指南旨在通过强制性的指导，提升整个行业的安全基线。

其中，“三同步”原则的强调，标志着中国正推动工业企业从传统的“先建设后加固”模式向“安全内建”（Secure-by-Design）的理念转变。这与全球先进的安全实践相吻合，即在系统设计和采购初期就融入安全考虑，而非将其视为后期附加的成本。这种转变对于从根本上提升工业系统的安全性至关重要，因为在系统生命周期的早期阶段解决安全问题，远

比后期修补更为经济有效。

此外，新版指南对“系统数据安全”和“上云安全”的重点突出，也反映了中国工业安全策略正紧跟技术发展趋势。随着工业数据成为新的生产要素，以及越来越多的工业应用向云平台迁移，这两方面的安全风险日益凸显。指南中的具体要求，如数据分类分级、全生命周期保护、数据出境评估以及云接入控制等，为企业在这些新兴领域构建安全能力提供了明确的路线图。

3.2 中国国家级工业互联网安全基础设施建设进展

在政策的强力推动下，中国国家级工业互联网安全基础设施建设在 2024 年持续取得进展。

经济与产业背景：根据《中国工业互联网产业经济发展报告（2024 年）》，中国工业互联网产业规模持续快速增长，核心产业增加值预计在 2024 年达到 1.53 万亿元人民币，同比增长 10.65% [19]。全国已建成近 340 家具有一定影响力的综合型、特色型、专业型工业互联网平台，重点平台连接的工业设备数量接近 9700 万台（套）[19]。国家工业互联网大数据中心体系已基本建成，汇聚数据超过 14 亿条，数据要素登记（确权）平台体系建设也在持续推进 [19]。这一庞大的产业生态和数据体量，对安全保障提出了极高要求。

安全体系建设：报告明确指出，“工业互联网安全体系持续健全” [19]。国家级工业互联网安全技术监测服务体系不断完善，态势感知、风险预警和基础资源汇聚能力得到增强。国家、省、企业三级协同的工业互联网安全技术监测服务体系已基本建成，并在制度建设、技术手段、服务能力方面同步提升 [20]。中国还在积极推动网络安全分类分级管理制度的落实，鼓励企业“安全上云”，并加强数据保护 [20]。

3.3 国家工业信息安全发展研究中心 (CICS-CERT) 与中国信息通信研究院 (CAICT) 的贡献与发现

作为国家级的研究机构和智库，CICS-CERT 和 CAICT 在工业互联网安全领域扮演着重要角色。

CICS-CERT：

- 该中心定期发布各类洞察报告，例如《2024-2025 年度我国电子信息产业投融资情况分析》和《中国两化融合发展数据地图（2024）》等，为产业发展提供宏观分析和趋势研判 [22]。
- CICS-CERT 还提供区域性的工业互联网安全态势监测报告。例如，《重庆市 2024 年 1 月工业互联网安全态势监测简报》显示，当月监测到来自境外的恶意网络行为 7.5 万次，占恶意网络行为总数的 49.0%，主要来源于美国、德国和加拿大等国家。

攻击行为主要集中在软件和信息技术服务业、制造业，攻击类型以漏洞攻击、网络诈骗、应用探测为主[18]。

- CICS-CERT 负责运营国家工业信息安全漏洞库（CICSVD），是国内工业领域漏洞信息共享和管理的核心平台[24]。

CAICT：

- CAICT 发布的《中国工业互联网发展成效评估报告（2024 年）》指出，中国工业互联网已进入全面推进的快速增长期，基础能力、技术创新、产业发展、应用推广和发展环境均取得显著成效[21]。报告特别提到，安全保障体系在政府统筹下逐渐完善，管理体系和服务能力同步提升[21]。
- CAICT 在零信任安全架构方面也进行了深入研究，其《零信任发展洞察报告（2024 年）》强调了零信任技术在强化数据安全防护，特别是在金融、政务、工业互联网等关键领域数据安全以及物联网（如电力行业、汽车行业）安全中的应用价值[26]。

这些国家级机构的研究成果和监测数据，为中国工业互联网安全政策的制定和产业实践提供了重要的理论支撑和数据参考。

下表对 2024 年工信部《工业控制系统网络安全防护指南》的关键条款进行了梳理和分析：

表 3.1：工信部 2024 年 ICS 网络安全指南：关键条款与分析

指南领域	新版指南关键条款（摘要）	分析师解读/行业意义	与 2016 版或国际标准对比（如适用）
资产管理	全面梳理 ICS 资产，建动态清单，明确责任人，核查安全状态；重要 ICS 重点保护，关键设备冗余备份[5]。	强调资产可见性和风险识别是防护基础；对“重要 ICS”的定义和要求提升了关键系统保护级别。	较 2016 版更强调动态性和“安全状态”核查。与 IEC 62443 中对资产识别和管理的要求一致。
配置管理	禁用不必要默认/管理员账户，清理过期账户；及时调整配置；避免弱口令；建配置	提升账户安全和配置基线管理水平，减少因配置不当引入的风险。	新增清理过期账户、及时调整配置等要求。对弱口令从“禁止”调整为“避免”更贴

	清单并审计；重大变更严格测试[5]。		合工业实际。
供应链安全	与供应商签协议明确安全责任；使用认证/检测合格的关键网络设备（如 PLC）[5]。	将安全责任向上游延伸，应对日益突出的供应链风险。	较 2016 版更细化了供应商类型和协议责任内容。新增对关键网络设备的安全认证要求。
主机与终端安全	部署防病毒/白名单，定期升级查杀；移动介质接入前查杀；计划性升级 OS/软件；封闭不必要接口/端口；用户身份鉴别，关键主机双因子认证[5]。	强化端点防护，应对恶意软件和物理接入风险。	更具体地提到了勒索软件防护和白名单技术。
架构与边界安全	分区分域，工业防火墙/网闸隔离；与企业网/互联网连接时纵向防护并审计；无线网络（5G/WiFi）严格访问控制；严格远程访问，安全代理，VPN 加密[5]。	核心防御策略，通过隔离和访问控制限制攻击扩散和外部入侵。	对无线和远程访问安全提出了更细致和严格的要求，鼓励使用商用密码。与 NIST CSF 的“保护”功能域中网络安全部分类似。
上云安全	自建工业云平台安全防护；设备上云严格标识和双向认证；业务系统上云环境隔离[5]。	应对工业系统向云迁移的趋势，确保云环境和云连接的安全性。	此为新版指南重点增加的内容，体现了对新技术应用的关注。
系统数据安全	数据分类分级，识别重要/核心数据；数据全生命周期安全保护（加密、访问控制、容灾备份）；重要/核	强调数据作为核心资产的保护，与国家数据安全法规对齐。	此为新版指南重点强化和细化的内容，反映了数据安全在工业领域的重要性日益提升。

	心数据境内存储，出境安全评估[5]。		
安全运营	监测审计，蜜罐；建安全运营中心（SOAR）；应急预案与演练，日志留存（不少于 6 个月）；上线前/年度安全评估；漏洞管理与补丁验证[5]。	提升主动防御、事件响应和持续改进能力。	对安全运营的各个环节（监测、响应、评估、漏洞管理）都提出了更具体的要求，如 SOAR 应用、蜜罐、日志留存时长。
责任落实	企业主体责任，建管理制度，明确责任人；“谁运营谁负责、谁主管谁负责”；“三同步”（安全与 ICS 同步规划、建设、使用）[5]。	明确企业在工控安全中的法律和管理责任，推动安全内建。	“三同步”原则是新版指南的核心管理要求之一，旨在从源头提升安全水平。

4. 2024 年重大工业网络安全事件及经验教训

2024 年，全球范围内发生了一系列针对工业领域和关键基础设施的网络安全事件，这些事件不仅造成了巨大的经济损失和运营中断，也为工业组织提供了深刻的经验教训。

4.1 重大全球及 OT 特定事件案例分析

具有物理影响的 OT 特定事件：

- **FrostyGoop 恶意软件攻击（乌克兰，2024 年 1 月）：**该事件是针对性 OT 攻击的典型案例。攻击者使用名为 FrostyGoop 的恶意软件，专门操纵 Modbus TCP/502 通信协议，成功攻击了乌克兰的区域供暖系统。这起事件直接导致了超过 600 栋公寓楼的供暖中断，对民生造成了实际物理影响[2]。
- **Fuxnet 恶意软件（俄罗斯，2024 年）：**Fuxnet 恶意软件被用于攻击莫斯科市的市政传感器网络。攻击者通过覆写传感器网关的固件，使得这些关键的城市基础设施组件失效[13]。

这两起事件清晰地表明，针对 OT 系统的网络攻击已具备直接造成物理世界破坏或功能失效的能力。

针对关键基础设施和广泛使用系统的攻击：

- **Ivanti Connect Secure VPN 漏洞利用（全球，2024 年 1 月）：**Ivanti Connect Secure VPN 产品中爆出多个高危零日漏洞（如 CVE-2023-46805, CVE-2024-21887, CVE-2024-21893），并迅速遭到大规模利用。全球数千台 VPN 设备受到影响，受害者包括美国网络安全和基础设施安全局（CISA）等政府相关实体。Mandiant 将此次攻击活动与名为 UNC5221 的威胁团伙关联起来[16]。此事件凸显了远程访问基础设施的脆弱性及其在关键网络攻击中的枢纽作用。
- **Change Healthcare 勒索软件攻击（美国，2024 年 2 月）：**美国最大的医疗处方服务商 Change Healthcare 遭到 Blackcat/Alphv 勒索软件团伙的攻击，导致美国医疗保健系统持续数周的大规模中断，处方处理和支付系统瘫痪。事件还造成了大规模数据泄露，据称影响了三分之一的美国人[3]。该事件是勒索软件对关键基础设施造成灾难性影响的又一例证。
- **XZ Utils 供应链攻击（全球，2024 年 3 月）：**这是一起精心策划的供应链攻击。攻击者在广泛使用的 Linux 数据压缩工具 XZ Utils 中植入了恶意后门代码，险些在全球众多 Linux 发行版的 SSHD 服务中留下可被利用的后门，其潜在影响难以估量[16]。
- **全球 Windows 操作系统“蓝屏”事件（全球，2024 年 7 月）：**一次影响全球数百万台 Windows 操作系统的“蓝屏”死机现象，导致了航班停飞、医疗设备瘫痪、金融系统中断等一系列连锁反应，显示了通用操作系统漏洞对全球关键服务运行的巨大潜在影响[3]。
- **CDK Global 勒索软件攻击（北美，2024 年 6 月）：**为约 15000 家汽车经销商提供 SaaS 平台的 CDK Global 遭到勒索软件攻击，导致其服务瘫痪，汽车经销商的日常运营受到严重影响。据报道，该公司最终可能支付了数千万美元的赎金[16]。这起事件暴露了 SaaS 服务提供商作为供应链关键环节所面临的风险。

APT 攻击事件（CNCERT 披露案例）：

- **针对中国某先进材料设计研究院的 APT 攻击：**据 CNCERT 报告，美方 APT 组织利用该单位邮件服务器（Microsoft Exchange）的漏洞进行入侵，植入高度隐蔽的内存木马，并以此为跳板对内网 30 余台重要设备（包括邮件服务器、办公系统服务器、代码管理服务器等）发起攻击，窃取敏感数据[10]。
- **针对中国某大型商用密码产品提供商的 APT 攻击：**CNCERT 披露的另一起事件显示，美情报机构利用某客户关系管理系统漏洞入侵中国一家大型商用密码产品提供商，植入特种木马程序，窃取了大量商业秘密信息，包括 950MB 的客户及合同数据和 6.2GB 的研发项目代码[11]。

这些 APT 案例揭示了国家级行为者针对高科技和关键信息基础设施进行网络间谍活动和

数据窃取的持续威胁。

其他值得关注的事件（来自卡巴斯基 2024 年第四季度报告 [27]）：

- 2024 年第四季度，有超过 100 家公司公开报告了遭受网络攻击。
- 两家制造企业（德国的 Kreisel GmbH & Co.和美国的 Stoli Group USA/Kentucky Owl）在遭受网络攻击后宣布破产，网络攻击成为其财务困境的促成因素之一。
- 能源管理和自动化解决方案巨头施耐德电气（Schneider Electric）确认遭到网络攻击，Grep (Hellcat) 黑客组织声称窃取了数据。
- 日本电子产品集团卡西欧（Casio Computer Co., Ltd.）遭到勒索软件攻击，导致系统中断和潜在数据泄露。
- 关键基础设施持续成为攻击目标，例如巴西水务公司 Sabesp、哥斯达黎加能源供应商 RECOPE 以及罗马尼亚电力分销商 Electrica Group 均在第四季度报告了攻击事件。

4.2 影响分析与工业组织经验教训

2024 年的重大安全事件对工业组织造成了多方面的影响，并带来了深刻的教训：

运营中断：许多事件，如 Change Healthcare、CDK Global、FrostyGoop 攻击以及 Windows 蓝屏事件，都直接导致了长时间的运营中断 [2]。在工业环境中，运营中断直接等同于生产停滞、订单延误和合同违约，是企业最不愿看到的后果。

财务损失：网络攻击带来的财务损失是巨大的，包括支付赎金（尽管不被推荐）、系统恢复成本、法律诉讼费用、监管罚款、品牌声誉受损以及因运营中断造成的收入损失。部分企业甚至因此面临破产，这警示所有工业组织，网络安全事件可能构成生存威胁 [27]。

数据泄露：工业数据，如设计图纸、工艺参数、客户资料、源代码等，是攻击者的重要目标。CNCERT 披露的 APT 案例清楚地表明，国家级攻击者对窃取此类敏感数据抱有浓厚兴趣 [10]。数据泄露不仅可能导致知识产权损失，还可能违反数据保护法规。

供应链连锁反应：XZ Utils 和 Ivanti VPN 等事件表明，供应链中的任何一个薄弱环节都可能被利用，从而对整个生态系统造成连锁反应 [16]。对 SaaS 服务提供商（如 CDK Global）的攻击也证明了这一点，其服务中断会直接影响下游成千上万的客户。

信任危机：成功的网络攻击会严重侵蚀客户、合作伙伴乃至公众对受害组织的信任。

经验教训：

- **主动的漏洞管理至关重要**：零日漏洞和已知漏洞（N-day）的持续利用，要求企业建立快速、高效的漏洞识别、评估、修补和缓解机制。

- **秉持“假设已被入侵”的心态**：鉴于攻击手段的复杂性和隐蔽性，组织必须假设自身网络可能已被渗透，并在此基础上构建强大的检测、响应和恢复能力。
- **加强第三方风险管理**：对供应链合作伙伴、软件供应商和服务提供商进行严格的安全审查和持续监控，是防范供应链攻击的关键。
- **OT 特定防御的必要性**：通用的 IT 安全解决方案不足以应对针对 OT 环境的特定威胁（如 FrostyGoop、Fuxnet）。企业需要部署专门针对 OT 协议和行为的监控与防护工具，并培养具备 OT 安全知识的专业人才。
- **韧性设计与冗余备份**：在系统设计阶段就应考虑安全韧性，确保关键系统具备冗余备份，并定期测试备份和恢复计划的有效性，以最大限度地减少攻击事件造成的停机时间。

这些事件深刻揭示了现代关键基础设施的内在关联性。例如，Change Healthcare 攻击或全球 Windows“蓝屏”事件，清晰地展示了一个高度互联生态系统（如医疗 IT、通用操作系统）中的单点故障如何引发跨关键服务乃至整个社会的广泛连锁反应。工业系统日益融入这个更广泛的数字结构，意味着对共享组件（如操作系统或主要服务提供商）的攻击或重大漏洞，都可能触发级联故障，其影响远超最初受攻击的实体，凸显了超越单个组织防御的系统性韧性思维的必要性。

同时，XZ Utils 事件是软件供应链中信任被武器化的一个典型例子。攻击者能够渗透到软件供应链中深受信赖的组件，将合法软件转变为威胁载体，这从根本上破坏了软件开发和分发的信任模型。现代软件，包括工业环境中使用的软件，严重依赖开源组件和第三方库。攻击者日益将这些上游组件作为目标，以便同时危害众多下游用户。此类攻击难以检测，一旦成功，可能造成毁灭性后果。这迫切要求向更严格的软件供应链安全实践转变，包括软件物料清单（SBOM）、代码签名和依赖项漏洞扫描。

此外，CDK Global 等公司在关键业务受威胁时据报愿意支付巨额赎金的现象，尤其值得警惕。这种行为，特别是在关键运营面临风险时，虽然可能被视为恢复服务的捷径，但实际上助长了勒索软件经济，并激励了针对类似目标的进一步攻击，形成了一个恶性循环，使关键行业成为勒索软件组织更具吸引力的目标。

下表对 2024 年部分重大工业网络安全事件进行了分析：

表 4.1：2024 年部分重大工业网络安全事件分析

事件名称/类型	发生时间（约）	目标领域/实体	攻击向量/利用的漏洞	主要影响	对工业安全的主要教训/

					启示
FrostyGoop OT 恶意软件	2024 年 1 月	乌克兰能源（区域供暖系统）	针对 Modbus TCP/502 的操纵 [2]	供暖中断，影响民生	OT 系统面临直接物理影响威胁；需专门的 OT 恶意软件检测与防护能力。
Ivanti VPN 零日漏洞利用	2024 年 1 月	全球 VPN 用户，包括政府相关实体	CVE-2023-46805, CVE-2024-21887 等 [16]	大量设备遭入侵，关键信息泄露风险	远程访问基础设施是高价值目标；零日漏洞响应速度至关重要。
Change Healthcare 勒索软件攻击	2024 年 2 月	美国医疗保健系统	Blackcat/Alphv 勒索软件，初始入侵途径未详 [16]	医疗服务大规模中断，数据泄露	关键基础设施易受勒索软件重创；业务连续性和灾难恢复计划不可或缺。
XZ Utils 供应链攻击	2024 年 3 月	全球 Linux 用户	在开源压缩库中植入后门 [16]	潜在的大范围 SSHD 后门风险，险些成功	软件供应链安全是系统性风险；需加强对第三方和开源组件的审查与监控。
CDK Global 勒索软件攻击	2024 年 6 月	北美汽车经销商 SaaS 服务	勒索软件攻击，具体入侵细节未公开 [16]	汽车经销商运营瘫痪，据报支付巨额赎金	SaaS 服务提供商是供应链关键节点；需评估供应商安全并制定自身应急预案。
针对中国高科技企业的	2024 年	中国先进材料、商用密码	邮件服务器漏洞、CRM 系	敏感设计数据、客户合	国家级 APT 攻击持续针对

APT 攻击		等高科技企业	统漏洞、特种木马 [10]	同、项目代码被窃	高价值目标；需加强纵深防御和威胁情报能力。
德国/美国制造企业因攻击破产	2024 年第四季度	德国 Kreisel，美国 Stoli Group/Kentucky Owl	勒索软件等网络攻击 [27]	企业运营受限，财务困难加剧，最终破产	网络攻击可直接导致企业生存危机；需将网络安全视为核心业务风险。

5. 不断演进的威胁行为者战术与方法论

2024 年，网络威胁行为者在战术、技术和程序（TTPs）方面持续演进，展现出更高的适应性、复杂性和隐蔽性。他们积极利用新兴技术，并针对工业控制系统（ICS）和操作技术（OT）环境的特点，不断优化攻击手段。

5.1 人工智能在进攻性网络行动中的作用

人工智能（AI）技术在 2024 年开始被攻击者更广泛地应用于网络攻击的各个阶段，显著提升了攻击的效率和成功率 [3]。

- **增强型钓鱼与社会工程学攻击：**AI 工具能够生成高度逼真和个性化的钓鱼邮件、短信甚至语音信息。深度伪造（Deepfake）技术也被用于制作虚假的音视频内容，用于针对特定目标（如高级管理人员）的社会工程学攻击，使得传统的人工识别更加困难 [4]。
- **自适应恶意软件：**AI 驱动的恶意软件具备在受感染系统中实时调整其行为模式的能力，例如改变通信方式、加密方法或潜伏策略，以规避安全软件的检测和分析 [4]。
- **自动化漏洞发现与利用：**尽管尚处于早期阶段，但 AI 在辅助攻击者自动扫描目标系统、识别潜在漏洞，甚至协助生成初步的漏洞利用代码方面展现出潜力。
- **降低攻击门槛：**AI 工具的出现，使得一些原本不具备高深技术背景的攻击者也能够发起更为复杂和有效的网络攻击。攻击工具的智能化和自动化，提高了攻击效率，同时降低了攻击成本 [3]。

5.2 主要及新识别的威胁组织活动

2024 年，老牌 APT 组织持续活跃，同时新的、更专注于 OT 领域的威胁组织也浮出水面。

- **老牌 APT 组织：**如 Kimsuky、Lazarus、摩诃草（Transparent Tribe）、APT28

等，继续针对全球范围内的政府、国防、能源和关键基础设施等目标进行网络间谍活动和破坏性攻击[1]。这些组织通常拥有丰富的资源和高超的技术能力，能够发起持续数月甚至数年的复杂攻击行动。

- **新兴 OT 特定威胁组织**：Dragos 在其 2024 年度报告中识别并命名了两个新的、专门针对 OT 环境的威胁活动组：**GRAPHITE** 和 **BAUXITE**[2]。尽管关于这两个组织具体 TTPs 和目标的详细信息在公开材料中尚不多见，但它们的出现本身就标志着一个重要趋势：攻击者正在投入更多精力研究 OT 系统和工业协议，开发专门针对工业环境的攻击能力。这与此前观察到的 OT 攻击更多是 IT 攻击的溢出效应或使用通用恶意软件的情况有所不同，预示着未来 OT 系统将面临更加精准和专业的威胁。
- **勒索软件卡特尔**：奇安信的报告指出，在追踪分析 2024 年度 74 个活跃的勒索软件及组织后发现，许多勒索软件组织之间存在着非常复杂的关联关系[1]。这可能包括共享攻击基础设施、恶意软件代码、攻击策略，甚至进行联合攻击行动，形成了类似卡特尔的合作网络，进一步增强了其攻击能力和影响力。
- **黑客行动主义团体**：受地缘政治冲突等因素影响，一些黑客行动主义团体在 2024 年也表现活跃，他们利用新的攻击途径，针对能源和水务等公用事业的 OT 环境发起攻击，试图扰乱其正常运营，以表达其政治诉求[2]。

5.3 高级持久化与规避技术

为了实现长期潜伏和躲避检测，威胁行为者在 2024 年采用了更为高级的持久化和规避技术。

- **“伪旗”行动（False Flag Operations）**：APT 组织越来越多地采用“伪旗”策略，即在攻击过程中故意留下误导性的痕迹，将攻击嫁祸于其他国家或组织，以干扰防御方的归因和溯源工作，达到隐藏自身真实身份的目的[9]。
- **“就地取材”（Living Off the Land, LotL）与无文件攻击**：攻击者倾向于利用目标系统中已有的合法工具（如 PowerShell、WMI 等）和进程执行恶意操作，并将恶意代码直接加载到内存中运行（无文件攻击），从而避免在磁盘上留下痕迹，有效规避基于签名的传统端点检测方案[9]。
- **劫持僵尸网络 C&C 服务器**：一些 APT 组织通过接管现有的僵尸网络命令与控制（C&C）服务器，将其改造为自身的间谍活动平台或攻击跳板，利用已有的受感染主机网络来发起攻击或中转数据[9]。
- **利用信任关系进行横向移动**：攻击者在获得初始立足点后，会积极利用不同网络区域之间或与合作伙伴组织之间存在的信任关系（如共享凭证、网络连接等）进行横向移动，逐步扩大控制范围。
- **内存驻留恶意软件**：如 CNCERT 报告中披露的案例所示，攻击者部署仅在内存中运行的木马程序，不写入硬盘存储，这使得基于磁盘扫描的检测方法失效，增加了检测和清除的难度[10]。

- **滥用多因素认证（MFA）**：卡巴斯基在其 2024 年第四季度 APT 攻击报告中观察到，有亲伊朗的攻击者通过“推送轰炸”（向用户发送大量 MFA 验证请求）和“MFA 疲劳”（利用用户对频繁验证请求的麻痹心理）等手段，成功绕过多因素认证机制[27]。
- **针对虚拟化基础设施的攻击**：像 Akira/Howling Scorpius 这样的组织，正在开发针对虚拟化基础设施的新型攻击方法，试图绕过在虚拟环境中部署的 EDR（端点检测与响应）等安全解决方案[27]。

这些不断演进的 TTPs 对工业企业的安全防护能力提出了更高的要求。一方面，新兴技术的普及，如 AI 工具和潜在的 OT 专用恶意软件或漏洞利用工具包的商品化，可能会降低高级攻击的技术门槛，使得更多行为者有能力对工业系统构成威胁。如果 OT 攻击工具变得更容易获取，那么更广泛、技术水平不那么高的攻击者也可能对工业目标构成威胁，从而增加整体攻击量。

另一方面，攻击者对规避检测和溯源的重视程度与日俱增。大量采用“伪旗”行动、无文件攻击、内存驻留恶意软件以及 MFA 绕过技术等，都表明攻击者不仅致力于寻找入侵系统的途径，更投入大量精力来躲避检测和混淆归因。这使得防御工作变得异常困难，因为基于签名的传统检测方法效果大打折扣。因此，防御策略必须向基于行为的异常检测和主动威胁狩猎等更高级的模式转变。

6. 战略防御：对策、最佳实践与建议

面对 2024 年日益严峻且不断演变的工业网络安全威胁，组织必须采取多层次、纵深化的战略防御措施。这不仅涉及技术层面的加固，更需要政策、治理和人员能力的全面提升。

6.1 技术要素：零信任、网络分段、威胁狩猎、安全设计

- **零信任架构 (Zero Trust Architecture)**：零信任已成为工业环境推荐采纳的核心安全理念。其核心思想是不默认信任网络内部或外部的任何用户或设备，对每一次访问请求都进行严格的身份验证和授权。中国信息通信研究院（CAICT）在其《零信任发展洞察报告（2024 年）》中强调，零信任对于加强工业互联网、物联网等关键领域的数据安全至关重要[26]。
- **网络分段与隔离 (Network Segmentation and Isolation)**：这是控制攻击影响范围、阻止恶意软件横向移动的关键措施。通过将 IT 网络与 OT 网络有效隔离，并在 OT 网络内部根据生产流程和关键性划分不同的安全区域（分区分域管理），可以显著降低单点故障演变为大规模生产中断的风险。中国工信部的新版指南对此有明确要求[5]。部署工业防火墙、单向网关等技术可实现有效的微隔离。
- **威胁狩猎 (Threat Hunting)**：鉴于高级威胁行为者（如 APT 组织）具备高超的隐蔽

能力和逃避检测技术，被动防御已不足以应对。组织需要建立主动的威胁狩猎机制，由专业的安全分析师利用威胁情报、行为分析和异常检测等手段，在自身网络环境中主动搜寻潜在的入侵迹象和恶意活动[2]。

- **安全设计原则 (Secure-by-Design)**：将网络安全融入工业系统和产品的整个生命周期，从设计、研发、采购、部署到运维和退役的各个环节都充分考虑安全需求。中国工信部指南中提出的“三同步”（安全与 ICS 同步规划、同步建设、同步使用）原则，以及 CISA 倡导的“安全设计”（Secure by Design）计划，都体现了这一理念的重要性[5]。制造商应承担起确保客户安全的责任，提高产品透明度，并引领问责制。
- **漏洞管理与补丁策略 (Vulnerability Management and Patching)**：建立常态化的漏洞扫描、风险评估和补丁管理流程。针对 OT 系统补丁更新困难的特性，应制定详细的测试验证计划，并在非生产时段进行，或采用虚拟补丁、网络隔离等补偿性控制措施[2]。
- **OT 环境的端点检测与响应 (EDR/XDR for OT)**：部署专门为 OT 环境设计的 EDR 或 XDR 解决方案，这些方案能够理解 OT 特有的协议和行为模式，从而更有效地检测和响应针对工业控制系统的攻击。
- **强身份认证与访问控制 (Strong Authentication and Access Control)**：全面推行多因素认证（MFA），尤其针对特权账户和远程访问。严格遵循最小权限原则，确保用户和系统仅拥有完成其任务所必需的权限[5]。
- **数据加密 (Encryption)**：对传输中和静态存储的敏感工业数据（如工艺参数、配方、知识产权等）进行加密保护，是防止数据泄露和篡改的重要手段[5]。

6.2 政策与治理：事件响应规划、供应链风险管理、人才队伍建设

- **事件响应规划 (Incident Response Planning)**：制定全面、可操作的网络安全事件应急响应预案，明确事件上报流程、处置步骤、各方职责和沟通机制。定期组织应急演练，检验预案的有效性并持续改进[3]。
- **供应链风险管理 (Supply Chain Risk Management)**：对第三方供应商（包括硬件、软件、服务提供商）进行严格的安全评估和背景审查。在合同中明确安全责任和要求，推广软件物料清单（SBOM）的使用，并对供应链进行持续的安全监控[3]。
- **人才队伍建设与培训 (Workforce Development and Training)**：工业网络安全领域专业人才的短缺是全球性难题[7]。企业需加大投入，培养和引进具备 OT 和 ICS 安全知识与技能的专业人才。毕马威（KPMG）的报告指出，尽管网络安全预算有所增加，但技术工人短缺仍是主要担忧[7]。OPSWAT 与 SANS 联合发布的报告更揭示了严峻的现实：超过 50%的 ICS 从业人员经验不足五年，51%缺乏行业特定的安全认证；然而，仅有 25%的组织将网络安全预算主要用于员工培训和招聘，而 52%的预算则投向了技术采购[8]。这表明，尽管技术投入重要，但对“人”这一关键因素的投入明显不足。

- **安全意识教育 (Security Awareness)**：面向全体员工，特别是能够接触到 OT 系统的操作员、工程师和管理人员，定期开展网络安全意识培训，使其了解常见的攻击手段（如钓鱼邮件、社会工程学），掌握安全操作规程，提升整体安全素养 [5]。
- **数据治理与保护 (Data Governance and Protection)**：建立完善的数据治理框架，对工业数据进行分类分级，明确数据所有权、使用权和管理权。依据相关法律法规（如 GDPR、中国《数据安全法》等）制定和执行数据保护政策 [5]。

6.3 对标监管框架与标准

积极对标并遵循国内外主流的工业网络安全标准和监管要求，是提升自身安全水位、满足合规性要求的必要途径。例如，国际上广泛认可的 IEC 62443 系列标准、NIST 网络安全框架（CSF）等。在中国，企业应重点关注并落实工信部发布的《工业控制系统网络安全防护指南》中的各项要求 [5]。欧洲的 NIS2 指令也对关键基础设施运营者提出了更高的网络安全要求 [15]。SANS 的报告指出，由首席信息安全官（CISO）领导并集中管理 ICS 安全事务的组织，其对行业标准的符合率（82%）远高于领导权分散的组织（42%），这凸显了强有力的领导和统一治理在标准落地中的重要性 [8]。

尽管技术不断进步，但人的因素仍然是工业网络安全防御链条中至关重要的一环，同时也是当前投入相对不足的薄弱环节。多份报告均指出 OT 安全专业人才的短缺是制约企业安全能力提升的主要瓶颈 [7]。OPSWAT/SANS 的报告更是用数据揭示了这一问题：高达 66%的组织认为“人”是 ICS 环境中的最大风险，但仅有 25%的网络安全预算用于人员培训和招聘，而技术投资则占去 52% [8]。这意味着，如果不能有效解决人才短板问题，即使投入再先进的安全技术，其效能也可能大打折扣，因为零信任架构的实施、高效的威胁狩猎、及时的事件响应乃至基础的配置管理，都离不开高素质专业人才的支撑。

同时，虽然监管合规（如遵循工信部指南 [5] 或 NIS2 指令 [15]）能够推动企业提升安全基线，但仅仅满足于“勾选合规项”的企业仍将难以应对复杂多变的威胁。真正的安全需要超越合规，建立基于风险评估和主动防御的安全文化。因为威胁行为者总是在不断调整其战术、技术和程序（TTPs）以绕过已知的控制措施 [9]。合规往往关注特定时间点的特定控制措施，而安全则是一个持续适应和改进的动态过程。最具韧性的组织将是那些将安全融入企业文化和运营流程，并基于对自身特定风险的深刻理解来驱动安全建设的组织。

此外，业界对“弹性优先于预防”的理念认知正在加深。鉴于高级威胁（如 APT、复杂勒索软件）的持续性和隐蔽性，实现 100%的入侵预防已不现实 [1]。而 OT 系统一旦遭受攻击，其影响往往非常严重 [2]。因此，最大限度地缩短停机时间和恢复时间成为首要目标。这促使企业更加重视快速检测、有效响应以及强大的备份恢复能力，正如 Critical Start 在其 2024 年回顾中强调的那样，预算和资源正向事件响应、灾难恢复和网络保险等增强韧性的方面倾斜 [4]。

下表按工业网络安全领域分类，列出了推荐的对策和最佳实践：

表 6.1：按工业网络安全领域划分的推荐对策与最佳实践

网络安全领域	具体对策/最佳实践	原则/益处（对工业环境的重要性）
网络安全	实施零信任网络访问（ZTNA）；OT 网络分段与微隔离（工业防火墙/网关）；部署入侵检测/防御系统（IDS/IPS），特别是针对 OT 协议的；定期进行网络安全审计。	最小化攻击面；限制横向移动，控制爆炸半径；及时发现和阻止恶意网络活动。[5]
端点安全（主机/终端）	部署 OT 专用的端点检测与响应（EDR）方案；使用应用白名单技术；强化配置管理，禁用不必要服务/端口；对移动存储介质进行严格管控和扫描。	保护工控系统中的关键计算节点（如工程师站、操作员站、服务器）；防止恶意软件执行和未授权访问。[5]
数据安全	工业数据分类分级；对敏感数据进行加密（传输中和静态存储）；实施严格的数据访问控制和权限管理；建立数据备份和恢复机制。	保护知识产权、工艺参数等核心工业数据；满足合规要求；确保数据在遭受攻击后的可恢复性。[5]
应用安全	对工业应用（MES, SCADA 软件, HMI 等）进行安全开发生命周期（Secure SDLC）管理；定期进行安全测试（如 SAST, DAST）；强化用户身份认证（MFA）。	确保工业应用自身的安全性，防止其成为攻击入口。[5]
云安全	对接入工业云平台的设备进行严格身份认证和授权；采用云安全态势管理（CSPM）工具监	保障工业数据和应用在云环境中的安全，应对“上云”趋势带来的新风险。[5]

	控 OT 云环境；确保云服务提供商满足工业安全要求。	
供应链安全	对软硬件供应商进行严格的安全审查和风险评估；要求提供软件物料清单（SBOM）；在合同中明确安全责任。	防范来自第三方产品或服务的安全风险，减少供应链攻击的可能。[3]
事件响应与运营	制定并定期演练 OT 特定的应急响应预案；建立安全运营中心（SOC），或采用托管检测与响应（MDR）服务；进行主动威胁狩猎；确保日志完整记录和安全存储（至少 6 个月）。	提升对安全事件的快速检测、分析、遏制和恢复能力；从被动防御转向主动防御。[2]
人员与治理	开展针对性的 OT 安全专业技能培训和认证；进行常态化的全员网络安全意识教育；明确工控安全责任体系和管理制度；确保 CISO 对 OT 安全有充分的领导和监督。	提升人员安全技能和意识，弥补人才短板；建立有效的安全治理结构，确保安全策略落地。[5]

7. 未来展望：工业网络安全的新兴趋势与前景（2025 年及以后）

展望未来，工业网络安全领域将持续受到技术革新、威胁演变和市场动态的多重影响。新兴技术的双刃剑效应、不断扩大的攻击面以及日趋严格的监管环境，将共同塑造 2025 年及以后的工业安全格局。

7.1 人工智能、量子计算与云原生架构对安全的变革性影响

- **人工智能（AI）在防御端的应用：**AI 和机器学习（ML）技术将在工业网络安全防御中扮演越来越重要的角色。它们能够处理海量的遥测数据，用于高级威胁检测、复杂攻击模式识别、异常行为分析，并辅助实现自动化的安全响应，这对于日益复杂的工业环境至关重要[15]。
- **AI 作为威胁倍增器：**与此同时，攻击者也将继续深化对 AI 技术的利用，开发更智能、更具规避性的攻击工具和策略。AI 驱动的自动化攻击、高度仿真的社交工程以及能够自主适应环境的恶意软件，将对现有防御体系构成持续挑战[3]。这预示着一场围绕 AI 的网络安全“军备竞赛”可能愈演愈烈，攻防双方都将越来越依赖 AI 能力。最

终，网络安全的有效性可能在很大程度上取决于谁能更好地掌握和应用 AI 技术，同时，AI 在网络战中的伦理和管控问题也将日益突出。

- **量子计算的远期影响：**尽管量子计算的广泛应用尚需时日，但其对现有公钥加密体系构成的潜在颠覆性威胁，已开始引起关注，特别是在保护需要长期保密的关键基础设施数据方面。奇安信在其 2024 年度漏洞报告中提及，量子计算是 2025 年值得关注的新兴技术发展趋势之一，其可能对漏洞利用和密码体系带来深远影响[30]。工业界需要开始思考后量子密码（PQC）的迁移策略，以应对未来的安全挑战。
- **OT 环境中的云原生架构：**随着越来越多的 OT 系统和工业应用向云原生平台（如容器化、微服务架构）迁移，传统的安全模式面临挑战。云原生架构带来了更高的灵活性和可扩展性，但也引入了新的安全考量，例如容器安全、API 安全、服务网格安全等，这些都需要在工业场景下得到专门的解决和保障[28]。

7.2 管理工业物联网（IIoT）与互联系统不断扩大的攻击面

- **IIoT 设备激增带来的风险：**工业物联网（IIoT）设备的指数级增长是未来几年工业领域最显著的趋势之一，这也意味着攻击面将以前所未有的速度急剧扩大[15]。许多 IIoT 设备在设计时可能未充分考虑安全性，或者由于成本和上市时间的压力而牺牲了安全特性。这些设备往往数量庞大、种类繁杂、部署分散，且生命周期较长，使得统一的安全管理和及时的补丁更新变得异常困难。
- **IIoT 的“安全债”：**如果当前这种为了追求运营效益而快速、有时甚至是不安全地部署 IIoT 设备的趋势得不到有效遏制，未来可能会积累巨大的“安全债”。这批缺乏内建安全机制的设备一旦被大规模利用（例如形成类似 Mirai 的物联网僵尸网络），可能引发针对工业基础设施的灾难性攻击。因此，从设备设计、网络接入、数据传输到平台管理，都需要构建端到端的 IIoT 安全解决方案。
- **攻击面管理（ASM）的重要性：**为了有效应对不断扩大的攻击面，组织需要借助攻击面管理（ASM）工具和技术，来持续地发现、评估和监控其面向内外部的数字资产和潜在暴露点，以便更清晰地了解自身面临的风险，并优先处理最关键的脆弱环节[12]。

7.3 预期的监管转变与市场动态

- **监管日趋严格与具体化：**预计全球各国政府将继续加强对工业网络安全的监管力度，出台更多具有针对性和强制性的法规。中国工信部 2024 年指南、欧洲 NIS2 指令等只是这一趋势的开端[15]。未来可能会看到更多针对特定行业（如能源、水务、交通等）的细化安全要求。
- **工业网络安全市场持续增长：**在日益增多的网络威胁和不断收紧的监管政策双重驱动下，全球工业网络安全市场预计将保持强劲增长。据 ReportsnReports 分析，全球工业网络安全市场规模预计将从 2022 年的 163 亿美元增长到 2028 年的 244 亿美

元，年复合增长率（CAGR）达到 7.7% [28]。其中，亚太地区由于其快速的工业化进程和对网络安全基础设施的大力投资，预计将成为增长最快的市场 [28]。

- **市场整合与平台化趋势**：随着市场成熟度的提高，工业网络安全解决方案提供商之间可能会出现更多的并购和整合。同时，客户对集成化、平台化安全解决方案的需求将增加，以简化管理复杂性并提高安全运营效率。
- **网络保险的角色演变**：针对 OT 环境的网络保险市场可能会进一步发展，但保险公司在承保前对企业的安全状况和风险管理能力的审查也将更加严格和细致 [4]。

IT、OT 与云的深度融合，正从根本上改变工业企业的运营模式和风险版图。传统的 IT 安全团队与 OT 工程团队各自为政的安全管理模式已难以为继。攻击者不会区分 IT 或 OT 边界，他们会利用任何可乘之机。因此，建立一个统一的安全治理模型，通常由具备广泛职责的首席信息安全官（CISO）领导，对跨 IT、OT 和云域的风险进行整体把控，制定统一的安全策略、风险管理流程和事件响应机制，已成为必然要求 [8]。这种融合不仅是技术层面的，更是组织架构、流程和文化的深度融合。

8. 结论

2024 年是工业互联网安全领域充满挑战与变革的一年。全球工业数字化转型的浪潮不可逆转，随之而来的是网络攻击面的持续扩大和威胁复杂性的显著升级。本报告通过对全年主要威胁态势、重大安全事件、政策法规进展以及防御策略的梳理分析，可以得出以下核心结论：

1. 威胁持续演进，OT 针对性增强： 以 APT 攻击和勒索软件为代表的高级威胁依然是工业领域的主要挑战，其攻击手段更加隐蔽，且越来越多地表现出对 OT 系统和工业流程的深刻理解。OT 专用恶意软件的出现（如 FrostyGoop, Fuxnet）以及勒索软件直接导致生产中断的案例频发，标志着攻击已从传统的 IT 层面渗透到核心的物理生产环节，对工业企业的运营安全和业务连续性构成直接威胁。

2. 供应链与新兴技术带来新风险维度： 软件供应链攻击（如 XZ Utils 事件）和对第三方服务提供商的攻击，凸显了工业生态系统中信任链的脆弱性。人工智能等新兴技术在被用于提升防御能力的同时，也正被攻击者利用以增强攻击效果和降低攻击门槛，攻防两端的技术对抗日趋激烈。

3. 政策法规成为推动安全水位提升的重要力量： 以中国工信部 2024 年《工业控制系统网络安全防护指南》为代表的政策法规，正在为工业企业构建网络安全防线提供更明确的指引和更严格的要求。这些政策强调“安全内建”、“数据安全”和“云安全”，反映了监管层对当前主要风险点的准确把握，并在推动行业整体安全水平的提升。

4. “人”的因素依然是安全防护的核心与短板： 尽管技术不断进步，但专业的 OT/ICS 安全人才短缺、员工安全意识不足以及预算分配不均（重技术、轻人员投入）等问题，依然是制约工业企业安全能力提升的关键瓶颈。有效的安全防护离不开高素质的专业人才和全员参与的安全文化。

5. 防御策略向主动、智能和韧性转变： 面对无法完全杜绝的入侵风险，“假设已被入侵”的理念得到更广泛认同。零信任架构、网络分段、主动威胁狩猎、快速事件响应以及构建业务韧性，成为企业战略防御的重点方向。

展望未来，工业互联网安全仍将面临严峻挑战。IIoT 设备的激增将进一步扩大攻击面，AI 技术的深度应用将加剧攻防对抗的复杂性，而 IT、OT 与云的深度融合则要求企业建立更为统一和协同的安全治理体系。

因此，对于所有工业组织而言，将网络安全提升至战略高度，将其视为保障业务连续性、维护核心竞争力和履行社会责任的关键要素，已刻不容缓。唯有持续投入资源，构建技术、管理与人员能力并重的纵深防御体系，不断提升对新兴威胁的认知和应对能力，才能在日趋复杂的网络环境中，确保工业互联网的健康、安全与可持续发展。

引用的著作

1. 网络安全威胁 2024 年度报告-奇安信, 访问时间为 五月 26, 2025，https://www.qianxin.com/threat/reportdetail?report_id=335
2. Dragos Reports OT/ICS Cyber Threats Escalate Amid Geopolitical Conflicts and Increasing Ransomware Attacks, 访问时间为 五月 26, 2025，https://www.dragos.com/resources/press-release/dragos-reports-ot-ics-cyber-threats-escalate-amid-geopolitical-conflicts-and-increasing-ransomware-attacks/
3. 警惕网络安全五大新风险-瞭望周刊社, 访问时间为 五月 26, 2025，https://lw.news.cn/20250330/a946f924ac8f41549cefdd532ff3eefd/c.html
4. 2024 Cybersecurity Year in Review - Critical Start, 访问时间为 五月 26, 2025，https://www.criticalstart.com/2024-cybersecurity-year-in-review/
5. 《工业控制系统网络安全防护指南》2024 版解读, 访问时间为 五月 26, 2025，https://www.secrss.com/articles/69417
6. 工业和信息化部关于印发工业控制系统网络安全防护指南的通知- 武汉 ..., 访问时间为 五月 26, 2025，https://home.wuhan.gov.cn/zcfg/202407/t20240719_2431172.shtml
7. 2024 年控制系统网络安全年度报告- 毕马威中国, 访问时间为 五月 26, 2025，https://kpmg.com/cn/zh/home/insights/2024/09/control-system-cybersecurity-annual-report-2024.html
8. OPSWAT《SANS 2024 ICS/OT 网络安全报告》揭示了在网络威胁 ..., 访问时间为 五月 26, 2025， https://chinese.opswat.com/blog/opswat-sponsored-sans-2024-

ics-ot-cybersecurity-report-uncovers-critical-workforce-gaps-in-securing-industrial-control-systems-amid-growing-cyber-threats
9. 2024 APT Annual Landscape Report - NSFOCUS, Inc., a global ..., 访问时间为 五月 26, 2025， https://nsfocusglobal.com/company-overview/resources/2024-apt-annual-landscape-report/
10. 国家互联网应急中心：发现处置两起美对我大型科技企业机构网络攻击事件, 访问时间为 五月 26, 2025， https://www.stdaily.com/web/gdxw/2025-01/17/content_287481.html
11. 美情报机构对中国发动网络攻击，详情披露 - 科技日报, 访问时间为 五月 26, 2025， https://www.stdaily.com/web/gdxw/2025-04/28/content_332665.html
12. 守初心创新质-绿盟科技 2024 网络安全报告, 访问时间为 五月 26, 2025， https://wlaq.njau.edu.cn/info/1254/2226.htm
13. Dragos's 8th Annual OT Cybersecurity Year in Review Is Now ..., 访问时间为 五月 26, 2025， https://www.dragos.com/blog/dragos-8th-annual-ot-cybersecurity-year-in-review-is-now-available/
14. Q4 and Full-Year 2024 Cyber Threat Report | PDI Security and Network Solutions, 访问时间为 五月 26, 2025， https://security.pditechnologies.com/resources/q4-and-full-year-2024-cyber-threat-report/
15. Cyber Insights 2024: OT, ICS and IIoT - SecurityWeek, 访问时间为 五月 26, 2025， https://www.securityweek.com/cyber-insights-2024-ot-ics-and-iiot/
16. 盘点：2024 年上半年典型网络攻击事件- 安全内参| 决策者的网络安全 ..., 访问时间为 五月 26, 2025， https://www.secrss.com/articles/67655
17. Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways | CISA, 访问时间为 五月 26, 2025， https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b
18. 信通安全丨重庆市 2024 年 1 月工业互联网安全态势监测简报, 访问时间为 五月 26, 2025， https://www.cqcaict.ac.cn/achievement/xintonganquan/2024/0621/2138.html
19. 中国工业互联网产业经济发展报告（2024 年）, 访问时间为 五月 26, 2025， https://www.china-aii.com/u/cms/www/202412/%E4%B8%AD%E5%9B%BD%E5%B7%A5%E4%B8%9A%E4%BA%92%E8%81%94%E7%BD%91%E4%BA%A7%E4%B8%9A%E7%BB%8F%E6%B5%8E%E5%8F%91%E5%B1%95%E6%8A%A5%E5%91%8A%EF%BC%882024%E5%B9%B4%EF%BC%89.pdf
20. 中国工业互联网产业经济发展报告（2024 年）, 访问时间为 五月 26, 2025， https://china-aii.com/u/cms/www/202412/%E4%B8%AD%E5%9B%BD%E5%B7%A5%E4%B8%9A%E4%BA%92%E8%81%94%E7%BD%91%E4%BA%A7%E4%B8%9A%E7%BB%8F%E6%B5%8E%E5%8F%91%E5%B1%95%E6%8A%A5%E5%91%8A%EF%BC%882024%E5%B9%B4%EF%BC%89.pdf
21. 中国工业互联网发展成效评估报告 - 重庆信息通信研究院, 访问时间为 五月 26, 2025， https://www.cqcaict.ac.cn/uploads/soft/241015/1-241015111200.pdf

22. 国家工业信息安全发展研究中心-首页, 访问时间为 五月 26, 2025， https://www.cics-cert.org.cn/
23. 国家工业信息安全发展研究中心, 访问时间为 五月 26, 2025， https://www.cics-cert.org.cn/web_root/webpage/main_index.html
24. 智库成果 - 国家工业信息安全发展研究中心, 访问时间为 五月 26, 2025， https://www.cics-cert.org.cn/web_root/webpage/page_content_101006.html
25. 中国信通院发布《中国工业互联网发展成效评估报告（2024 年）》, 访问时间为 五月 26, 2025， https://www.aii-alliance.org/index/c185/n5121.html
26. 《零信任发展洞察报告(2024)》正式发布(附下载) - 安全内参, 访问时间为 五月 26, 2025， https://www.secrss.com/articles/74273
27. Industrial cybersecurity in 2024: trends and forecasts | Kaspersky ..., 访问时间为 五月 26, 2025， https://ics-cert.kaspersky.com/cards/industrial-cybersecurity-in-2024-trends-and-forecasts/
28. Future Outlook of the Industrial Cybersecurity Industry, 访问时间为 五月 26, 2025， https://www.reportsnreports.com/semiconductor-and-electronics/future-outlook-of-the-industrial-cybersecurity-industry/
29. CISA's 2024 Year in Review document details cyber defense, infrastructure protection milestones, 访问时间为 五月 26, 2025， https://industrialcyber.co/cisa/cisas-2024-year-in-review-document-details-cyber-defense-infrastructure-protection-milestones/
30. 奇安信研究报告-汇聚安全大数据、分享实战新经验, 访问时间为 五月 26, 2025， https://www.qianxin.com/threat/reportaptlist
31. (CS)2AI-KPMG 控制系统网络安全年度报告 2024, 访问时间为 五月 26, 2025， https://assets.kpmg.com/content/dam/kpmg/cn/pdf/zh/2024/09/control-system-cybersecurity-annual-report-2024.pdf
32. 奇安信科技集团股份有限公司 2024 年半年度报告, 访问时间为 五月 26, 2025， https://pdf.dfcfw.com/pdf/H2_AN202408291639578083_1.pdf
33. 2024 年度网络安全漏洞威胁态势研究报告-奇安信, 访问时间为 五月 26, 2025， https://www.qianxin.com/threat/reportdetail?report_id=333
34. WSN and IoT - An Integrated Approach for Smart Applications 9781032566894, 9781032567716, 9781003437079 - DOKUMEN.PUB, 访问时间为 五月 26, 2025， https://dokumen.pub/wsn-and-iot-an-integrated-approach-for-smart-applications-9781032566894-9781032567716-9781003437079.html
35. Industrial cybersecurity leadership is evolving from stopping threats to bridging risk, resilience, 访问时间为 五月 26, 2025， https://industrialcyber.co/features/industrial-cybersecurity-leadership-is-evolving-from-stopping-threats-to-bridging-risk-resilience/