谱写工业控制系统网络安全新篇章 走好新型工业化之路

国家工业信息安全发展研究中心主任 蒋艳

为适应新型工业化发展形势，提高我国工业控制系统网络安全保障水平，指导工业企业开展工控安全防护工作，以高水平安全护航新型工业化高质量发展，工业和信息化部正式印发了《工业控制系统网络安全防护指南》（以下简称《指南》），立足我国工业控制系统发展和安全建设实际，围绕安全管理、技术防护、安全运营、责任落实四方面，面向工业企业提出33项指导性安全防护基线要求，指导工业企业切实提升工控安全防护水平。

保障工控安全是加快推进新型工业化的重要举措

工业控制系统已成为网络攻击的重要打击目标。工业控制系统广泛应用于关系国民经济命脉的重要领域，是工业生产运行的基础核心，其网络安全事关工业生产稳定运行，事关经济社会发展和国家安全。随着攻击者针对关键工业领域的网络攻击能力不断提升，工业控制系统已成为国家、组织间网络攻击的重要打击目标。据国家工业信息安全发展研究中心（以下简称“国家工信安全中心”）监测，2023年瞄准境内工业控制系统实施的扫描嗅探行为超460万次。

做好工控安全是护航新型工业化的必要之举。当前，新一轮科技革命和产业变革加速演进，制造业数字化转型步伐加快，数字经济和实体经济深度融合，工业控制系统作为推进新型工业化的重要支撑，工控安全的基础性、保障性作用越发凸显。我国工业企业工控安全防护能力普遍薄弱，传统网络安全隐患和新型风险交织叠加问题突出，企业安全建设远远滞后于数字化转型，重发展、轻安全的思想仍普遍存在。要走好新型工业化之路，需坚持以发展促安全、以安全保发展，筑牢工业企业工业控制系统网络安全防线。

工业控制系统网络安全面临新形势与新挑战

新技术加快工业网络开放互联，新型网络安全威胁持续升级。工业以太网、TSN、WiFi6、5G等新型工业网络技术的应用进一步推动工业网络互联互通，在提供更多设备连接、更高网络带宽、更低传输延时、更远传输距离、更强穿透能力的同时，工控网络边界越发模糊，工业控制器、工业主机、仪器仪表、生产业务系统等工业控制系统暴露的攻击路径越来越多，传统网络安全风险向工业研发、设计、生产、运行、管理等各环节各领域全面渗透，勒索病毒等恶意软件在工业控制网络中加速蔓延，APT攻击等新型网络威胁频发。随着工业互联网的应用深入，工业控制系统上云上平台趋势明显，但企业普遍缺乏“安全上云”技术手段，平台与设备间的风险传导问题突出，平台自身漏洞和互联网攻击风险可渗透到工业控制系统及现场设备，接入设备的漏洞隐患也可被恶意利用并成为攻击云平台的入口。

工业控制系统海量异构，“带病”运行与低防护联网成常态。PLC、数控机床、RTU等传统类型设备及AGV小车、无线手持HMI、智能无线传感器、智能网关等智能工业设备广泛应用于工业内网，工业控制系统在设计之初缺乏安全考虑，设备固件、操作系统、应用软件、控制协议等漏洞频发。据国家工信安全中心统计，2023年国家工业信息安全漏洞库收录了工业领域漏洞1875条，累计收录9000余条，其中超60%为高危或极高危，漏洞在被利用时可能导致远程代码执行或拒绝服务等严重威胁。大量漏洞存在较长的修复周期，且难以验证漏洞修复是否会影响工业生产稳定运行，病毒威胁难以深层扫描、系统无法定期升级，导致工控系统“带病”运行成常态。

工控系统重点保护的“关键少数”不突出，企业安全建设与运维管理问题严峻。工控系统生命周期长达15~20年，工业领域门类复杂，不同行业的工控系统形态和功能的差别明显，存在安全防护重点、保护规则不同等特点。我国规模以上工业企业超48万家，运行的工控系统众多，各工控系统对于国民经济和行业发展的重要程度、遭破坏后对国家安全和社会稳定的影响程度也存在差异，工控系统重点保护的对象不突出。目前，工业企业对工业控制系统网络安全防护意识薄弱，人员专业技能匮乏，供应链管理不规范、安全责任落实不到位、采购云服务后责任划分不明晰、安全运维难以落到实处等问题较为严峻。

《指南》有力指导企业提升工控安全防护水平

指导企业建立工控安全综合防护体系。为应对复杂严峻的安全威胁形势、多变的网络攻击路径、持续升级的网络攻击手段，《指南》强调技管结合，从技术防护、安全管理、安全运营、责任落实四方面指导企业建立综合防护能力，突出管理重点对象，强化技术应对策略，增强威胁发现及处置能力，切实提升企业工控安全防护水平。

提升新形势新挑战下的风险防范应对能力。顺应异构工业终端海量接入、新型工业网络技术应用、工业控制系统设备上云上平台、新型网络威胁频发等新发展趋势，《指南》与时俱进，充分衔接已有法律法规相关要求，提出贴合实际、适应变化、落实有效的安全防护策略。《指南》明确智能终端安全、无线网络安全、上云安全、监测预警运营中心、应急处置、漏洞管理、供应链安全、资产管理等要求，指导企业理清系统资产底数，防范内外部网络攻击，强化网络安全事前、事中、事后全流程安全风险应对能力。

聚焦重要工业控制系统网络安全防护。重要工业控制系统承载业务的重要性高、规模大，发生网络安全事件的危害程度高，《指南》强调要建立重要工业控制系统清单并实施重点保护，要求对重要工业控制系统相关设备实施冗余备份，加强对重要工业控制系统安全防护能力评估，定期开展重要工业控制系统漏洞排查，及时对系统升级加固。

压实企业工控安全主体责任。企业是网络安全的责任主体，承载着维护网络安全的重要职责，《指南》强调工业企业承担本企业工控安全主体责任，应明确责任部门和责任人，建立健全工控安全管理制度，落实工控安全防护要求，强化企业资源保障力度，确保安全防护措施与工业控制系统同步规划、同步建设、同步使用。

以高水平工控安全护航新型工业化

在新时期、新形势下，要积极落实《指南》要求，以护航新型工业化网络安全为目标，以重点行业企业、重要工业控制系统安全管理为主线，加强政策标准体系建设、优化安全管理模式、提升技术手段能力、增强协同化产业供给。

完善工业领域网络安全政策标准体系。加强《指南》与工业领域网络安全工作的统筹协同，完善标准体系建设，有序推动重点国家和行业标准研制与发布。研究制定重要工业控制系统识别认定规则，建立健全工业领域网络安全信息共享与通报、应急处置等工作机制。体系化开展工业领域网络安全政策标准宣贯与培训，引导企业提升安全意识与防护水平。

强化重点行业企业、重要系统安全管理。有序推进工业领域网络安全工作向重点行业深化落地，深入实施工业互联网企业网络安全分类分级管理，建立重点工业互联网企业清单。推动开展全国重要工业控制系统识别认定，强化重要工业控制系统防护能力评估、漏洞排查与修复，掌握“关键少数”底数，“以点带面”探索构建工业控制系统差异化安全管理和防护。

提升工业领域网络安全技术能力。打造集工业领域网络安全监测预警、信息通报、应急处置、分析溯源于一体的技术手段，强化主动监测、精准预警、实时处置等关键能力，形成“横向联通、纵向联动”的协同监测与响应体系。深入开展工控安全漏洞专项治理行动，提升工业控制系统安全漏洞发现、验证、修复能力，强化工控安全漏洞全生命周期管理。

把握《指南》重点要求，推动工控安全防护管理走深向实。督促企业落实网络安全主体责任，强化安全防护体系建设与资源保障力度。有序开展全国工控安全防护能力评估试点，深入开展安全深度行活动，遴选打造工控安全防护优秀解决方案。加强产学研用协同，优化工业控制系统网络安全产业供给。