发文机关：工业和信息化部

标　　题：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

发文字号：工信部网安〔2024〕14号

成文日期：2024-01-19

发布日期：2024-01-30

发布机构：网络安全管理局

分　　类：网络安全管理

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

工信部网安〔2024〕14号

各省、自治区、直辖市、计划单列市及新疆生产建设兵团工业和信息化主管部门，有关企事业单位：

现将《工业控制系统网络安全防护指南》印发给你们，请认真抓好落实。

工业和信息化部

2024年1月19日

工业控制系统网络安全防护指南

工业控制系统是工业生产运行的基础核心。为适应新时期工业控制系统网络安全（以下简称工控安全）形势，进一步指导企业提升工控安全防护水平，夯实新型工业化发展安全根基，制定本指南。

使用、运营工业控制系统的企业适用本指南，防护对象包括工业控制系统以及被网络攻击后可直接或间接影响生产运行的其他设备和系统。

一、安全管理

（一）资产管理

1.全面梳理可编程逻辑控制器（PLC）、分布式控制系统（DCS）、数据采集与监视控制系统（SCADA）等典型工业控制系统以及相关设备、软件、数据等资产，明确资产管理责任部门和责任人，建立工业控制系统资产清单，并根据资

产状态变化及时更新。定期开展工业控制系统资产核查，内容包括但不限于系统配置、权限分配、日志审计、病毒查杀、数据备份、设备运行状态等情况。

2.根据承载业务的重要性、规模，以及发生网络安全事件的危害程度等因素，建立重要工业控制系统清单并定期更新，实施重点保护。重要工业控制系统相关的关键工业主机、网络设备、控制设备等，应实施冗余备份。

（二）配置管理

3.强化账户及口令管理，避免使用默认口令或弱口令，定期更新口令。遵循最小授权原则，合理设置账户权限，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。

4.建立工业控制系统安全配置清单、安全防护设备策略配置清单。定期开展配置清单审计，及时根据安全防护需求变化调整配置，重大配置变更实施前进行严格安全测试，测试通过后方可实施变更。

（三）供应链安全

5.与工业控制系统厂商、云服务商、安全服务商等供应商签订的协议中，应明确各方需履行的安全相关责任和义务，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。

6.工业控制系统使用纳入网络关键设备目录的 PLC 等设备时，应使用具备资格的机构安全认证合格或者安全检测符合要求的设备。

（四）宣传教育

7.定期开展工业控制系统网络安全相关法律法规、政策标准宣传教育，增强企业人员网络安全意识。针对工业控制系统和网络相关运维人员，定期开展工控安全专业技能培训及考核。

二、技术防护

（一）主机与终端安全

8.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，定期进行病毒库升级和查杀，防止勒索软件等恶意软件传播。对具备存储功能的介质，在其接入工业主机前，应进行病毒、木马等恶意代码查杀。

9.主机可采用应用软件白名单技术，只允许部署运行经企业授权和安全评估的应用软件，并有计划的实施操作系统、数据库等系统软件和重要应用软件升级。

10.拆除或封闭工业主机上不必要的通用串行总线（USB）、光驱、无线等外部设备接口，关闭不必要的网络服务端口。若确需使用外部设备，应进行严格访问控制。

11.对工业主机、工业智能终端设备（控制设备、智能仪表等）、网络设备（工业交换机、工业路由器等）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。

（二）架构与边界安全

12.根据承载业务特点、业务规模、影响工业生产的重要程度等因素，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。

13.应用第五代移动通信技术（5G）、无线局域网技术（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，对无线访问接入点定期审计，关闭无线接入公开信息（SSID）广播，避免设备违规接入。

14.严格远程访问控制，禁止工业控制系统面向互联网开通不必要的超文本传输协议（HTTP）、文件传输协议（FTP）、Internet 远程登录协议（Telnet）、远程桌面协议（RDP）等高风险通用网络服务，对必要开通的网络服务采取安全接入代理等技术进行用户身份认证和应用鉴权。在远程维护时，使用互联网安全协议（IPsec）、安全套接字协议（SSL）等协议构建安全网络通道（如虚拟专用网络（VPN）），并严格限制访问范围和授权时间，开展日志留存和审计。

15.在工业控制系统中使用加密协议和算法时应符合相关法律法规要求，鼓励优先采用商用密码，实现加密网络通信、设备身份认证和数据安全传输。

（三）上云安全

16.工业云平台为企业自建时，利用用户身份鉴别、访问控制、安全通信、入侵防范等技术做好安全防护，有效阻止非法操作、网络攻击等行为。

17.工业设备上云时，对上云设备实施严格标识管理，设备在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工业云平台。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。

（四）应用安全

18.访问制造执行系统（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。访问关键应用服务时，采用双因子认证，并严格限制访问范围和授权时间。

19.工业企业自主研发的工业控制系统相关软件，应通过企业自行或委托第三方机构开展的安全性测试，测试合格后方可上线使用。

（五）系统数据安全

20.定期梳理工业控制系统运行产生的数据，结合业务实际，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。

21.法律、行政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，应当依法依规进行数据出境安全评估。

三、安全运营

（一）监测预警

22.在工业控制网络部署监测审计相关设备或平台，在不影响系统稳定运行的前提下，及时发现和预警系统漏洞、恶意软件、网络攻击、网络侵入等安全风险。

23.在工业控制网络与企业管理网或互联网的边界，可采用工业控制系统蜜罐等威胁诱捕技术，捕获网络攻击行为，提升主动防御能力。

（二）运营中心

24.有条件的企业可建立工业控制系统网络安全运营中心，利用安全编排自动化与响应（SOAR）等技术，实现安全设备的统一管理和策略配置，全面监测网络安全威胁，提升风险隐患集中排查和事件快速响应能力。

（三）应急处置

25.制定工控安全事件应急预案，明确报告和处置流程，根据实际情况适时进行评估和修订，定期开展应急演练。当发生工控安全事件时，应立即启动应急预案，采取紧急处置措施，及时稳妥处理安全事件。

26.重要设备、平台、系统访问和操作日志留存时间不少于六个月，并定期对日志备份，便于开展事后溯源取证。

27.对重要系统应用和数据定期开展备份及恢复测试，确保紧急时工业控制系统在可接受的时间范围内恢复正常运行。

（四）安全评估

28.新建或升级工业控制系统上线前、工业控制网络与企业管理网或互联网连接前，应开展安全风险评估。

29.对于重要工业控制系统，企业应自行或委托第三方专业机构每年至少开展一次工控安全防护能力相关评估。

（五）漏洞管理

30.密切关注工业和信息化部网络安全威胁和漏洞信息共享平台等重大工控安全漏洞及其补丁程序发布，及时采取升级措施，短期内无法升级的，应开展针对性安全加固。

31.对重要工业控制系统定期开展漏洞排查，发现重大安全漏洞时，对补丁程序或加固措施测试验证后，方可实施补丁升级或加固。

四、责任落实

32.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”的原则落实工控安全保护责任。

33.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。