《工业控制系统信息安全防护指南》解读

ICS产品管理团队 王晓鹏 张学聪

关键词：工控安全 工控信息安全 工控安全生命周期 等级保护 防护指南

摘要：11 月 7 日，《中华人民共和国网络安全法》通过，在第三十一条明确规定，”国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。”

工信部近期也发布了《工业控制系统信息安全防护指南》，而在此之前，工信部曾经发布过工信部协 [2011]451 号《关于加强工业控制系统信息安全管理的通知》（下文简称 451 号文），从通知文件到防护指南，适用范围更加聚焦，目标更加明确，本文从不同角度做出解读，并给出相关解决方案。

差异性分析

适用范围的差异

451 号文适用于核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关的领域；《工业控制系统信息安全防护指南》则直接指出该指南适用于工业控制系统应用企业以及从事工业控制系统规划、设计、建设、运维、评估的企事业单位，范围更广，目标更加明确。

落实的手段差异

防护指南深化了对原有 451 号文要求的内容，在工业控制系统

信息安全防护的落实手段上进行了强化。原有 451 号文旨在加强各相关机构针对工业控制系统信息安全的重要性和紧迫性的认识，如各级政府工业和信息化主管部门要加强对工业控制系统信息安全工作的指导和督促检查；有关行业主管或监管部门、国有资产监督管理部门要加强对重点领域工业控制系统信息安全管理工作的指导监督；有关部门要加快推动工业控制系统信息安全防护技术研究和产品研制；国有大型企业要切实加强工业控制系统信息安全管理的领导。侧重点在于加强各部门对工业控制系统信息安全防护的认识上，并没有提出具体的责任要求。

防护指南对工控系统信息安全防护落实手段进行了进一步的明确。规定了地方工业和信息化主管部门要根据工业和信息化部的统筹安排，对本行政区域内的工业企业进行指导并制定工控安全防护实施方案。要求各相关单位建立工控安全管理机制、成立信息安全协调小组等方式，明确工控安全管理责任人，落实工控安全责任制，部署工控安全防护措施。

可以看出，从原 451 号文到防护指南的推进，工控系统安全防护落实的手段进一步得到了加强。从要加强、要加快、切实加强到建立、成立、明确、部署，整体防护落实手段有了一个质的飞跃。

技术方向的差异

目前防护指南深化了对原有 451 号文要求的内容，强调了可落地的防护技术手段，已经可以具体到工业防火墙和网闸等具体的措施上。

防护指南在原有 451 号文有关连接管理要求基础上进行了细化，涉及企业信息网络 (生产管理层、信息管理层) 和企业生产网络 (过程监督层、过程控制层) 的数据交互明确了防护措施。除了指出禁止没有防护的工业控制网络与互联网连接，还提供了具体的边界安全防护手段，如规定将工业控制系统的开发、测试和生产环境进行分离，通过工业控制网络边界防护设备对工业控制网络与企业网或互联网之间的边界进行安全防护，通过工业防火墙、网闸等防护设备对工业控制网络安全区域之间进行逻辑隔离安全防护。

涉及企业信息网络向企业生产网络的远程访问安全，防护指南参考了电力等先进发展行业中已经采用并得到检验的技术手段，如严格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；确需远程访问的，采用数据单向访问控制等策略进行安全加固，对访问时限进行控制，并采用加标锁定策略。

涉及企业过程监督层、过程控制层的安全配置管理方面，防护指南在原有 451 号文有关配置管理要求基础上进行了细化，加入了补丁管理和身份认证相关要求。如密切关注重大工控安全漏洞及其补丁发布，及时采取补丁升级措施。在补丁安装前，需对补丁进行严格的安全评估和测试验证；在工业主机登录、应用服务资源访问、工业云平台访问等过程中使用身份认证管理。对于关键设备、系统和平台的访问采用多因素认证；合理分类设置账户权限，以最小特权原则分配账户权限。

防护指南对原有 451 号文有关应急管理要求进行了加深，引入了安全监测机制和应急预案演练手段。规定了需要在工业控制网络部署网络安全监测设备，报告并处理网络攻击或异常行为；在重要工

业控制设备前端部署具备工业协议深度包检测功能的防护设备，限制违法操作；定期对工业控制系统的应急响应预案进行演练。

另外，防护指南还特别指出需要保留工业控制系统的相关访问日志，并对操作过程进行安全审计。

管理方面的差异

安全软件选择与管理

引入工控安全软件验证测试的环节，防病毒软件和白名单软件需要在离线环节中进行测试和验证。防病毒和白名单软件是近几年工控系统比较流行的安全软件，《指南》中强调了在这些软件上线前需要做好充分的测试，防止因为这些软件导致工控系统的故障。

引入防病毒和恶意软件入侵管理机制，对工业控制系统及临时接入的设备采取病毒查杀等安全预防措施。对于任何接入已有工控系统或新上线的工控系统都需要进行上线前的安全检查。

配置和补丁管理

引入重大配置变更的管理，在进行重大配置变更前进行影响分析和严格的安全测试。

在配置管理的基础上引入补丁管理，相关企事业单位需要及时进行补丁升级，并且在安装前需要进行安全评估和验证。现阶段很多安全厂商已经具有了扫描工控系统漏洞的能力，但是在扫描出相关的漏洞后如何进行漏洞的修复一直是一个问题，《指南》中着重强调了在进行配置变更（包含业务配置变更和安全基线配置变更）和漏洞修复前都需要在试验环境中进行验证和测试。

身份认证

引入身份认证的要求，并且提出对于关键资产的访问需要采用多因素认证。多因素认证也是《指南》中新增的针对工控系统的要求，相关的关键资产应该采用口令加 RFID 等多种认证方式进行认证。

引入最小特权原则；

引入强口令的要求，并要求对一些工控软件定期更换口令。工控系统大部分还是使用厂家配置的默认口令，或使用弱口令，通过设置强口令，并定期更换，可以增加攻击者暴力破解口令的难度。

新提出了加强对身份认证证书信息保护力度，禁止在不同系统和网络环境下共享的要求，防止身份认证信息泄露，从而导致身份认证失效。

安全监测和应急预案演练

提出在工控网络部署网络安全监测设备，及时发现威胁。相关的建议在一些行业规范中也可以找到对应的条例，现阶段工控系统的安全状况还是处于一个朦胧的阶段，管理员并不清楚自己负责的工控系统中是否已经具有相关的威胁，所以在工控系统中部署网络入侵检测装置可以很好的帮助管理员了解该系统现有的安全状况和水平。

提出在重要资产前部署具备工业协议深度包检测功能的防护设备即工控防火墙类设备，限制违法操作；

在 451 号文的基础上提出工控安全事件需逐级报送直至属地省级工业和信息化主管部门，并提出注意保护现场便于取证。该建

议在 451 号文的基础上提出了保护现场和取证的要求，工控安全不仅要做到“防得住”，还要尽量做到“查得到”。

资产安全

引入资产安全明确资产的责任人，建立台账和资产的处置机制等，这些是目前工控系统普遍比较欠缺的，在防护指南中提出并做了相关要求。

提出对关键主机，网络，控制组件进行冗余备份

数据安全

提出对动态和静态数据的保护；

提出对测试数据进行保护，一是方便后期的维护，二是测试环境大都按照真实环境进行模拟，攻击者获取测试环境的数据后可以参考这些数据对真实系统发动有针对性的攻击；

供应链管理

在 451 号文供应商选择和在合同中明确安全责任和义务的基础上增加了保密条例，防范敏感信息外泄，做好数据防泄漏工作，很多工控系统涉及国计民生，相关的生产流程，生产工艺都属于秘密信息，因此在 451 号文的基础上《指南》提出了防泄密的要求。

落实责任

提出通过建立工控安全管理机制、成立信息安全协调小组等方式，明确工控安全管理责任人，落实工控安全责任制，部署工控安全防护措施。很多企事业单位工控系统的使用者和管理者是两批人，可能负责信息安全的又是另一拨人，因此存在责任主体不明确的问题，落实此条建议可以避免生产部门和信息部门之间工控系统安全责任落实不明确，没有责任人的问题。

解决方案

根据防护指南对工控安全的防护要求，可以从两个方面来看

工业控制系统全生命周期

工业控制系统全生命周期的角度去考虑贯穿于系统生命周期各个阶段的防护措施。

• 在**设计阶段**，将信息安全因素考虑其中，给出成型的系统建设信息安全解决方案；

• 在**设备选型阶**段，选择成熟的融合信息安全的工业控制系统（DCS、PLC、RTU、IED 等）和经过严格测试和认证的全线工控安全产品；

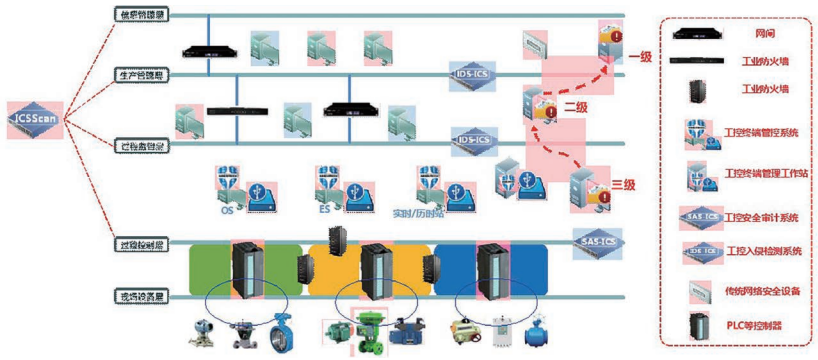
• 在**测试阶段**，通过漏洞检测与挖掘技术对已成型的系统进行严格的安全测试，通过渗透测试、漏洞扫描、漏洞挖掘等方式发现系统存在的安全隐患并进行加固和修复，同时，需要分离工业控制系统的开发、测试和生产环境，确保风险的隔离。

• **在运行阶段**，通过非法入侵检测与异常行为安全审计等手段实现安全管理；

• **在系统检修阶段**，继续通过漏洞扫描、漏洞挖掘等手段对系统进行二次安全测试；

• **在废弃阶段**，对系统残余风险进行确认，确保系统正常报废无风险遗留。

工控网络架构部署



工业控制网络综合防护拓扑图

一、在企业工业控制网络区域中部署工业防火墙，通过工业防火墙对安全区域之间进行逻辑隔离安全防护，包括对重要工业控制设备的安全防护。工业防火墙应能提供针对工业协议的数据级深度过滤，实现对 Modbus、OPC 等主流工业协议和规约的细粒度检查和过滤，帮助用户阻断来自网络的病毒传播、黑客攻击等行为，限制违法操作，避免其对控制网络的影响和对生产流程的破坏。

二、在企业工业控制网络区域与企业网或互联网区域之间部署工业防火墙或网闸设备，解决控制网络如何安全接入信息网络的问题，解决控制网络内部不同安全区域之间安全防护的问题。

三、对于确需远程维护的工作站，可通过工业防火墙自带的 VPN 等安全接入方式进行连接。

四、在确需使用 USB、光驱、无线等接口的情况下，通过工控终端管控系统对外设进行严格的访问控制。工控终端管控系统还可兼具防病毒及应用程序白名单功能，只允许经过工业企业自身授权和安全评估的软件运行。

五、在工业控制网络区域部署网络安全监测设备，如工控入侵检测系统、工控安全审计系统，及时发现、报告并处理网络攻击或异常行为。安全监测设备应能识别多种工控协议，适应攻防的最新发展，准确监测网络异常流量，自动应对各层面安全隐患，通过对相关工控协议进行解析，发现潜在的异常行为，并在第一时间进行告警。

六、工业控制系统应用企业上级监管机构可通过扫描器等合规性检查工具对相关单位的工业网络资产进行安全评估，包括对资产的漏洞修复情况和配置合规情况的审计。同时，工业控制系统应用企业也可通过合规性检查工具完成对本单位工业网络资产合规性的自查工作。合规性检查工具应实现针对 DCS、PLC、RTU 等工业控制设备的漏洞扫描，以及针对传统上位机系统软件、组态软件的漏洞扫描，其应该具备发现漏洞、评估漏洞、展示漏洞、跟踪漏洞等完备的漏洞管理能力。