**《工业控制系统信息安全防护指南》解读**

发布时间：2016-11-08  来源：信息化和软件服务业司

工业控制系统信息安全（以下简称“工控安全”）是国家网络和信息安全的重要组成部分，是推动中国制造2025、制造业与互联网融合发展的基础保障。2016年10月，工业和信息化部印发《工业控制系统信息安全防护指南》（以下简称《指南》），指导工业企业开展工控安全防护工作。

**一、背景情况**

工控安全事关经济发展、社会稳定和国家安全。近年来，随着信息化和工业化融合的不断深入，工业控制系统从单机走向互联，从封闭走向开放，从自动化走向智能化。在生产力显著提高的同时，工业控制系统面临着日益严峻的信息安全威胁。为贯彻落实《国务院关于深化制造业与互联网融合发展的指导意见》（国发〔2016〕28号）文件精神，应对新时期工控安全形势，提升工业企业工控安全防护水平，编制本《指南》。

**二、总体考虑**

《指南》坚持“安全是发展的前提，发展是安全的保障”，以当前我国工业控制系统面临的安全问题为出发点，注重防护要求的可执行性，从管理、技术两方面明确工业企业工控安全防护要求。编制思路如下：

（一）落实《国家网络安全法》要求

《指南》所列11项要求充分体现了《国家网络安全法》中网络安全支持与促进、网络运行安全、网络信息安全、监测预警与应急处置等法规在工控安全领域的要求，是《国家网络安全法》在工业领域的具体应用。

（二）突出工业企业主体责任

《指南》根据我国工控安全管理工作实践经验，面向工业企业提出工控安全防护要求，确立企业作为工控安全责任主体，要求企业明确工控安全管理责任人，落实工控安全责任制。

（三）考虑我国工控安全现状

《指南》编制以近五年我部工控安全检查工作掌握的有关情况为基础，充分考虑当前工控安全防护意识不到位、管理责任不明晰、访问控制策略不完善等问题，明确了《指南》的各项要求。

（四）借鉴发达国家工控安全防护经验

《指南》参考了美国、欧盟、日本等发达国家工控安全相关政策、标准和最佳实践做法，对安全软件选择与管理、配置与补丁管理、边界安全防护等措施进行了论证，提高了《指南》的科学性、合理性和可操作性。

（五）强调工业控制系统全生命周期安全防护

《指南》涵盖工业控制系统设计、选型、建设、测试、运行、检修、废弃各阶段防护工作要求，从安全软件选型、访问控制策略构建、数据安全保护、资产配置管理等方面提出了具体实施细则。

**三、内容详解**

《指南》坚持企业的主体责任及政府的监管、服务职责，聚焦系统防护、安全管理等安全保障重点，提出了11项防护要求，具体解读如下：

（一）安全软件选择与管理

1. 在工业主机上采用经过离线环境中充分验证测试的防病毒软件或应用程序白名单软件，只允许经过工业企业自身授权和安全评估的软件运行。

**解读：**工业控制系统对系统可用性、实时性要求较高，工业主机如MES服务器、OPC服务器、数据库服务器、工程师站、操作员站等应用的安全软件应事先在离线环境中进行测试与验证，其中，离线环境指的是与生产环境物理隔离的环境。验证和测试内容包括安全软件的功能性、兼容性及安全性等。

2. 建立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。

**解读：**工业企业需要建立工业控制系统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用必要的安全预防措施。安全预防措施包括定期扫描病毒和恶意软件、定期更新病毒库、查杀临时接入设备（如临时接入U盘、移动终端等外设）等。

（二）配置和补丁管理

1.做好工业控制网络、工业主机和工业控制设备的安全配置，建立工业控制系统配置清单，定期进行配置审计。

**解读：**工业企业应做好虚拟局域网隔离、端口禁用等工业控制网络安全配置，远程控制管理、默认账户管理等工业主机安全配置，口令策略合规性等工业控制设备安全配置，建立相应的配置清单，制定责任人定期进行管理和维护，并定期进行配置核查审计。

2.对重大配置变更制定变更计划并进行影响分析，配置变更实施前进行严格安全测试。

解读：当发生重大配置变更时，工业企业应及时制定变更计划，明确变更时间、变更内容、变更责任人、变更审批、变更验证等事项。其中，重大配置变更是指重大漏洞补丁更新、安全设备的新增或减少、安全域的重新划分等。同时，应对变更过程中可能出现的风险进行分析，形成分析报告，并在离线环境中对配置变更进行安全性验证。

3.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。

**解读：**工业企业应密切关注CNVD、CNNVD等漏洞库及设备厂商发布的补丁。当重大漏洞及其补丁发布时，根据企业自身情况及变更计划，在离线环境中对补丁进行严格的安全评估和测试验证，对通过安全评估和测试验证的补丁及时升级。

（三）边界安全防护

1.分离工业控制系统的开发、测试和生产环境。

**解读：**工业控制系统的开发、测试和生产环境需执行不同的安全控制措施，工业企业可采用物理隔离、网络逻辑隔离等方式进行隔离。

2.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，禁止没有防护的工业控制网络与互联网连接。

**解读：**工业控制网络边界安全防护设备包括工业防火墙、工业网闸、单向隔离设备及企业定制的边界安全防护网关等。工业企业应根据实际情况，在不同网络边界之间部署边界安全防护设备，实现安全访问控制，阻断非法网络访问，严格禁止没有防护的工业控制网络与互联网连接。

3.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。

**解读：**工业控制系统网络安全区域根据区域重要性和业务需求进行划分。区域之间的安全防护，可采用工业防火墙、网闸等设备进行逻辑隔离安全防护。

（四）物理和环境安全防护

1.对重要工程师站、数据库、服务器等核心工业控制软硬件所在区域采取访问控制、视频监控、专人值守等物理安全防护措施。

**解读：**工业企业应对重要工业控制系统资产所在区域，采用适当的物理安全防护措施。

2.拆除或封闭工业主机上不必要的USB、光驱、无线等接口。若确需使用，通过主机外设安全管理技术手段实施严格访问控制。

**解读：**USB、光驱、无线等工业主机外设的使用，为病毒、木马、蠕虫等恶意代码入侵提供了途径，拆除或封闭工业主机上不必要的外设接口可减少被感染的风险。确需使用时，可采用主机外设统一管理设备、隔离存放有外设接口的工业主机等安全管理技术手段。

（五）身份认证

1.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。

**解读：**用户在登录工业主机、访问应用服务资源及工业云平台等过程中，应使用口令密码、USB-key、智能卡、生物指纹、虹膜等身份认证管理手段，必要时可同时采用多种认证手段。

2.合理分类设置账户权限，以最小特权原则分配账户权限。

**解读：**工业企业应以满足工作要求的最小特权原则来进行系统账户权限分配，确保因事故、错误、篡改等原因造成的损失最小化。工业企业需定期审计分配的账户权限是否超出工作需要。

3.强化工业控制设备、SCADA软件、工业通信设备等的登录账户及密码，避免使用默认口令或弱口令,定期更新口令。

**解读：**工业企业可参考供应商推荐的设置规则，并根据资产重要性，为工业控制设备、SCADA软件、工业通信设备等设定不同强度的登录账户及密码，并进行定期更新，避免使用默认口令或弱口令。

4.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。

**解读：**工业企业可采用USB-key等安全介质存储身份认证证书信息，建立相关制度对证书的申请、发放、使用、吊销等过程进行严格控制，保证不同系统和网络环境下禁止使用相同的身份认证证书信息，减小证书暴露后对系统和网络的影响。

（六）远程访问安全

1.原则上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。

**解读：**工业控制系统面向互联网开通HTTP、FTP、Telnet等网络服务，易导致工业控制系统被入侵、攻击、利用，工业企业应原则上禁止工业控制系统开通高风险通用网络服务。

2.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。

**解读：**工业企业确需进行远程访问的，可在网络边界使用单向隔离装置、VPN等方式实现数据单向访问，并控制访问时限。采用加标锁定策略，禁止访问方在远程访问期间实施非法操作。

3.确需远程维护的，采用虚拟专用网络（VPN）等远程接入方式进行。

**解读：**工业企业确需远程维护的，应通过对远程接入通道进行认证、加密等方式保证其安全性，如采用虚拟专用网络（VPN）等方式，对接入账户实行专人专号，并定期审计接入账户操作记录。

4.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。

**解读：**工业企业应保留工业控制系统设备、应用等访问日志，并定期进行备份，通过审计人员账户、访问时间、操作内容等日志信息，追踪定位非授权访问行为。

（七）安全监测和应急预案演练

1.在工业控制网络部署网络安全监测设备，及时发现、报告并处理网络攻击或异常行为。

**解读:**工业企业应在工业控制网络部署可对网络攻击和异常行为进行识别、报警、记录的网络安全监测设备，及时发现、报告并处理包括病毒木马、端口扫描、暴力破解、异常流量、异常指令、工业控制系统协议包伪造等网络攻击或异常行为。

2.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。

**解读：**在工业企业生产核心控制单元前端部署可对Modbus、S7、Ethernet/IP、OPC等主流工业控制系统协议进行深度分析和过滤的防护设备，阻断不符合协议标准结构的数据包、不符合业务要求的数据内容。

3.制定工控安全事件应急响应预案，当遭受安全威胁导致工业控制系统出现异常或故障时，应立即采取紧急防护措施，防止事态扩大，并逐级报送直至属地省级工业和信息化主管部门，同时注意保护现场，以便进行调查取证。

**解读：**工业企业需要自主或委托第三方工控安全服务单位制定工控安全事件应急响应预案。预案应包括应急计划的策略和规程、应急计划培训、应急计划测试与演练、应急处理流程、事件监控措施、应急事件报告流程、应急支持资源、应急响应计划等内容。

4.定期对工业控制系统的应急响应预案进行演练，必要时对应急响应预案进行修订。

**解读：**工业企业应定期组织工业控制系统操作、维护、管理等相关人员开展应急响应预案演练，演练形式包括桌面演练、单项演练、综合演练等。必要时，企业应根据实际情况对预案进行修订。

（八）资产安全

1.建设工业控制系统资产清单，明确资产责任人，以及资产使用及处置规则。

**解读：**工业企业应建设工业控制系统资产清单，包括信息资产、软件资产、硬件资产等。明确资产责任人，建立资产使用及处置规则，定期对资产进行安全巡检，审计资产使用记录，并检查资产运行状态，及时发现风险。

2.对关键主机设备、网络设备、控制组件等进行冗余配置。

**解读：**工业企业应根据业务需要，针对关键主机设备、网络设备、控制组件等配置冗余电源、冗余设备、冗余网络等。

（九）数据安全

1.对静态存储和动态传输过程中的重要工业数据进行保护，根据风险评估结果对数据信息进行分级分类管理。

**解读：**工业企业应对静态存储的重要工业数据进行加密存储，设置访问控制功能，对动态传输的重要工业数据进行加密传输，使用VPN等方式进行隔离保护，并根据风险评估结果，建立和完善数据信息的分级分类管理制度。

2.定期备份关键业务数据。

**解读：**工业企业应对关键业务数据，如工艺参数、配置文件、设备运行数据、生产数据、控制指令等进行定期备份。

3.对测试数据进行保护。

**解读：**工业企业应对测试数据，包括安全评估数据、现场组态开发数据、系统联调数据、现场变更测试数据、应急演练数据等进行保护，如签订保密协议、回收测试数据等。

（十）供应链管理

1.在选择工业控制系统规划、设计、建设、运维或评估等服务商时，优先考虑具备工控安全防护经验的企事业单位，以合同等方式明确服务商应承担的信息安全责任和义务。

**解读：**工业企业在选择工业控制系统规划、设计、建设、运维或评估服务商时，应优先考虑有工控安全防护经验的服务商，并核查其提供的工控安全合同、案例、验收报告等证明材料。在合同中应以明文条款的方式约定服务商在服务过程中应当承担的信息安全责任和义务。

2.以保密协议的方式要求服务商做好保密工作，防范敏感信息外泄。

**解读：**工业企业应与服务商签订保密协议，协议中应约定保密内容、保密时限、违约责任等内容。防范工艺参数、配置文件、设备运行数据、生产数据、控制指令等敏感信息外泄。

（十一）落实责任

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。

**解读：**工业企业应建立健全工控安全管理机制，明确工控安全主体责任，成立由企业负责人牵头的，由信息化、生产管理、设备管理等相关部门组成的工业控制系统信息安全协调小组，负责工业控制系统全生命周期的安全防护体系建设和管理，制定工业控制系统安全管理制度，部署工控安全防护措施。

**四、贯彻落实**

一是面向地方工业和信息化主管部门、中央企业等开展《指南》宣贯，依据《指南》要求组织培训，指导工业企业进一步优化工控安全管理与技术防护手段。

二是选择工业聚集发展城市及地区，设立工控安全防护试点区，组织区内工业企业开展工控安全防护应用试点，遴选优秀试点企业分享工控安全防护经验，总结提炼工业控制系统防护示范案例。

三是将《指南》要求纳入年度工业行业网络安全检查项目，强化责任落实到位，管理、技术落实到位。通过自查、抽查、深度检查等方式促进工业企业深入贯彻并落实《指南》。

地方工信主管部门负责对本地区内的工控安全防护工作进行监督管理，并配合工业和信息化部做好工控安全相关工作。工业企业应按照《指南》各项要求，开展和完善工控安全防护工作，改善自身安全防护能力的同时，为全面提升我国工业信息安全防护水平提供支撑。