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），保障工业企业工业控制系统信息安全，制定《工业控制系统信息安全防护指南》，现印发你们。

工业和信息化部指导和管理全国工业企业工控安全防护和保障工作，并根据实际情况对指南进行修订。地方工业和信息化主管部门根据工业和信息化部统筹安排，指导本行政区域内的工业企业制定工控安全防护实施方案，推动企业分期分批达到本指南相关要求。

工业和信息化部

2016年10月17日

（联系电话：010-68208171）

工业控制系统信息安全防护指南

工业控制系统信息安全事关经济发展、社会稳定和国家安全。为提升工业企业工业控制系统信息安全（以下简称工控安全）防护水平，保障工业控制系统安全，制定本指南。

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、评估的企事业单位适用本指南。

工业控制系统应用企业应从以下十一个方面做好工控安全防护

工作。

一、安全软件选择与管理

（一）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。

（二）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。

二、配置和补丁管理

（一）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。

（二）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。

（三）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。

三、 边界安全防护

（一）分离工业控制系统的开发、测试和生产环境。

（二）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。

（三）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。

四、物理和环境安全防护

（一）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。

（二）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。

五、身份认证

（一）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。

（二）合理分类设置账户权限，以最小特权原则分配账户权限。

（三）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。

（四）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。

六、远程访问安全

（一）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。

（二）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。

（三）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。

（四）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。

七、安全监测和应急预案演练

（一）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。

（二）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。

（三）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。

（四）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。

八、资产安全

（一）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。

（二）对关键主机设备、网络设备、控制组件等进行冗余配置。

九、数据安全

（一）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。

（二）定期备份关键业务数据。

（三）对测试数据进行保护。

十、供应链管理

（一）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。

（二）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。

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。