

工业控制系统信息安全 风险提示

2016年第2期(总第7期)

2016年3月14日

工业控制

工业控制系统信息安全风险提示

随着工业4.0、智能制造等概念的提出，工业控制系统（ICS）在工业生产中的地位日益重要。然而，ICS的安全风险也随之增加。本文旨在分析ICS面临的主要安全风险，并提出相应的防范建议。

一、ICS面临的主要安全风险

1. 网络攻击：黑客通过互联网或其他网络渠道，对ICS进行非法访问、篡改数据或破坏系统。近年来，针对ICS的网络攻击事件频发，给工业生产带来了严重损失。

2. 恶意软件：病毒、木马、蠕虫等恶意软件通过U盘、光盘等物理媒介或网络传播，感染ICS设备，导致系统瘫痪或数据丢失。

3. 内部威胁：企业内部员工因操作失误、疏忽大意或故意破坏，导致ICS系统出现安全漏洞或数据泄露。

4. 供应链风险：ICS设备制造商或供应商提供的设备存在安全缺陷，或被植入后门，给ICS的安全运行带来隐患。

5. 物理安全：ICS设备存放场所的物理环境不安全，如火灾、水灾、盗窃等，可能导致设备损坏或数据丢失。

单与“SCADAPass”清单的对比核查，梳理出受默认密码风险影响的工控设备；2. 修改工控设备默认密码并强化用户密码；3. 断开工控设备不必要的公网连接，关闭工控设备的HTTP/Telnet/FTP/SSH等不必要的传统网络服务；4. 部署其它辅助的访问控制和安全认证措施。

编制单位：工业和信息化部电子科学技术情报研究所

发送：各地工业和信息化部主管部门、有关国有大型企业
有关工业控制系统厂商

地址：工业和信息化部信息化和软件服务司

（联系人：李耀兵 010-88683438）