

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，工业控制系统在国民经济中的地位日益重要。然而，工业控制系统面临着日益严峻的信息安全风险。本文旨在分析工业控制系统信息安全的主要风险，并提出相应的防范建议。

一、工业控制系统信息安全的主要风险

1. 系统漏洞与恶意攻击

工业控制系统往往存在大量的安全漏洞，这些漏洞可能被攻击者利用，对系统进行非法访问、篡改或破坏。此外，攻击者还可以通过网络对工业控制系统进行远程控制，导致生产中断或设备损坏。

2. 供应链安全风险

工业控制系统的供应链日益全球化，供应链中的任何一个环节出现问题，都可能影响到整个系统的正常运行。例如，供应商提供的硬件或软件存在质量问题，或者供应商被攻击者渗透，都可能给工业控制系统带来安全风险。

3. 人员安全意识薄弱

工业控制系统操作人员的安全意识往往比较薄弱，容易受到钓鱼邮件、木马病毒等攻击。此外，操作人员的不当操作也可能导致系统出现安全问题。

4. 数据泄露与篡改

工业控制系统中存储了大量的生产数据，这些数据一旦被泄露或篡改，将对企业的生产经营造成严重影响。例如，竞争对手可以通过窃取数据来了解企业的生产情况，或者攻击者可以通过篡改数据来破坏企业的生产秩序。

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）