工业控制系统安全网络防护分析

李新玲[1] 夏 栋[2]
1. 浙江大学 浙江 杭州 311107
2. 浙江大华技术股份有限公司 浙江 杭州 310053

摘 要：随着工业自动化与信息化的深度融合，工业控制系统的网络安全问题日益受到关注。本文深入探讨了工业控制系统的网络安全威胁及其来源，并针对这些威胁提出了一系列具体的网络安全防护策略。文章旨在通过多层次、多维度的防护措施，提升工业控制系统的网络安全水平，确保工业生产的连续性和稳定性。

关键词：工业控制系统；网络安全；防护策略；多层次防护

引言

工业控制系统（ICS）是现代工业自动化的核心组成部分，其安全性对于企业的稳定运营至关重要。然而，随着网络技术的飞速发展和工业互联网的兴起，ICS面临的网络安全威胁也日益增多。为了确保工业控制系统的网络安全，必须从多个角度出发，构建全面的安全防护体系。

1 工业控制系统面临的安全威胁

1.1 外部攻击

工业控制系统面临的外部攻击，主要是指黑客通过网络途径非法渗透进入控制系统。这种攻击行为不仅可能导致生产流程受到严重干扰，甚至可能引发连锁反应，造成安全事故。黑客一旦成功入侵，他们可能会篡改生产指令，导致设备故障、生产效率下降，甚至造成整个生产线的瘫痪。更为严重的是，黑客还可能窃取敏感数据，如核心生产配方、客户信息等商业机密。这些数据一旦泄露，不仅会对企业的声誉和竞争力造成严重影响，更可能带来巨大的经济损失。因此，企业必须高度重视工业控制系统的外部攻击威胁，采取有效的安全防护措施，确保控制系统的网络安全，从而保障企业的正常运营和信息安全。

1.2 内部漏洞

工业控制系统的内部漏洞，是威胁其安全的重要因素。由于工业控制系统的软件、硬件以及网络通信可能存在设计上的缺陷或者配置错误，这些漏洞无形中为黑客提供了潜在的攻击点。一旦这些漏洞被黑客发现并利用，他们便能够轻松地绕过系统的安全防护，获得对系统的控制权[1]。此时，黑客不仅可以随意篡改系统设置，干扰正常生产流程，甚至还可以窃取关键数据，如生产数据、配方信息等。这些漏洞的存在，无疑为企业带来了巨大的安全风险。因此，及时发现并修复这些内部漏洞，加强系统的安全防护，是确保工业控制系统安全稳定运行的关键。企业需要定期进行系统漏洞扫描和风险评估，以便及时发现问题并采取相应的补救措施。

1.3 人为因素

在工业控制系统中，人为因素同样是一个不可忽视的安全威胁。由于操作不当、安全意识薄弱或恶意行为，员工可能会对系统的安全造成潜在或直接的损害。例如，员工在操作过程中可能因为疏忽或技能不足导致误操作，这种误操作可能触发设备故障，甚至造成重要数据的泄露。更为严重的是，如果企业内部存在不满或具有恶意的员工，他们可能会出于报复、利益驱使或其他不良目的，故意破坏系统稳定性或泄露敏感信息。这些行为都会对企业的运营和信息安全带来极大的风险。因此，企业必须加强对员工的安全培训和操作指导，提升全员的安全意识，同时建立完善的内部监管机制，以防止和减少人为因素对工业控制系统安全的威胁。

2 工业控制系统网络安全防护策略

2.1 建立完善的网络安全管理制度

为了确保工业控制系统的网络安全，建立完善的网络安全管理制度至关重要。这一制度不仅是企业信息安全的基础，也是防范各种网络威胁的第一道防线。首先，企业需要制定详细的网络安全政策和操作规范。这些政策和规范应该明确各级人员的安全职责，确保每个人都清楚自己在网络安全中的角色和责任。通过明确职责划分，可以形成有效的监督机制，防止因职责不清而导致的安全问题。其次，定期开展网络安全培训和演练是增强员工安全意识和应急响应能力的关键。企业应该定期组织员工参加网络安全培训课程，让他们了解最新的网络安全威胁和防护措施。同时，通过模拟网络攻击等演练活动，可以让员工在实际操作中提升应急响应能力，确保在真实面对网络威胁时能够迅速做出正确的反

应。此外，实施定期的安全审查和风险评估也是网络安全管理制度的重要组成部分。企业应该定期对工业控制系统进行全面的安全审查，检查系统中是否存在潜在的安全隐患。同时，通过风险评估，企业可以了解系统面临的各种威胁和脆弱性，从而制定相应的防护措施。这一过程需要专业的网络安全团队参与，他们可以利用专业的工具和技术对系统进行深入的分析和检测。除了上述措施外，企业还可以考虑建立网络安全事件应急响应机制。一旦发生网络安全事件，该机制可以确保企业迅速启动应急响应流程，及时处置安全事件，降低损失。同时，企业还应该建立完善的网络安全日志管理和审计制度，以便在发生安全问题时能够迅速追踪和定位问题源头。

2.2 构筑坚固的网络防线

为了构筑坚固的网络防线，确保工业控制系统的网络安全，必须采取一系列高效且精准的安全措施。（1）部署高性能的防火墙是防御外部攻击的首要步骤。防火墙作为网络安全的门户，能够实时监测并过滤进出网络的数据包，从而有效阻断非法访问和潜在的恶意流量。与此同时，入侵检测/防御系统（IDS/IPS）的引入，为网络提供了另一层保护。IDS/IPS能够深度分析网络流量，及时发现并阻止潜在的入侵行为，为工业控制系统提供实时的安全监控和预警。（2）数据加密传输是确保数据在传输过程中不被窃取或篡改的关键。VPN（虚拟专用网络）技术的使用，为数据的传输提供了一个加密的通道。通过VPN，数据在传输前会进行加密处理，确保即使数据在公共网络上传输，也不会被未经授权的第三方轻易获取或篡改。这不仅保障了数据的机密性，也维护了数据的完整性和真实性。（3）实施网络隔离策略是降低攻击风险的有效手段[2]。工业控制系统通常包含许多关键的基础设施和信息，一旦遭受攻击，后果将不堪设想。因此，将工业控制系统与其他网络隔离开来，形成一个相对独立、封闭的网络环境，能够显著降低外部攻击的风险。这种隔离不仅可以通过物理隔离实现，如使用独立的网络设备和线路，还可以通过逻辑隔离实现，如利用VLAN（虚拟局域网）等技术手段。

2.3 强化系统安全配置

为了强化工业控制系统的安全配置，确保系统免受潜在威胁的侵害，需要采取一系列细致而周密的措施。首要任务是定期更新系统和应用软件。软件和系统漏洞是黑客常利用的攻击点，因此，及时修补这些漏洞至关重要。企业应建立一套完善的漏洞管理机制，定期检查并更新系统和应用软件，确保所有已知漏洞得到及时修复。这不仅能显著降低系统被攻击的风险，还能提升系统的稳定性和性能。其次，限制不必要的网络服务和端口开放也是关键。过多的开放端口和服务会为黑客提供更多的攻击机会。因此，企业应详细审查并关闭那些不必要的网络服务和端口，尤其是那些与工业控制系统无关的服务。通过这种方式，可以大大缩小系统的攻击面，提高整体的安全性。此外，实施最小权限原则和用户身份验证机制是防止未经授权的访问和操作的重要手段。根据最小权限原则，每个用户或系统进程只应被授予完成任务所需的最小权限。这意味着，即使某个用户或进程被黑客利用，黑客也只能获得有限的权限，从而降低潜在损害。同时，实施严格的用户身份验证机制，如多因素认证，可以确保只有经过授权的用户才能访问系统。这种双重验证方法显著提高了系统的安全性。除了上述措施外，企业还应考虑实施定期的安全审计和日志监控。这些措施可以帮助企业及时发现并应对潜在的安全威胁。安全审计可以评估系统的安全性，并发现可能存在的安全隐患；而日志监控则可以实时追踪系统的活动，及时发现异常行为。

2.4 数据备份与恢复策略

数据备份与恢复策略在工业控制系统的网络安全中占据着举足轻重的地位。为了确保数据的完整性和业务的连续性，建立全面的数据备份机制显得尤为重要。这一机制应包括定期自动备份和手动备份两种方式，以应对不同情况下的数据恢复需求。定期自动备份能够确保数据的实时性和完整性。通过设定固定的时间间隔，系统可以自动将数据备份到指定的存储位置。这种方式不仅减轻了人工操作的负担，还降低了因人为失误而导致数据丢失的风险。同时，手动备份方式则提供了更大的灵活性，允许在特定情况下进行即时备份，如系统升级、重要数据变更等。为了确保备份数据的完整性和可用性，需要对备份数据进行定期验证。这一过程包括检查备份数据的可读性、完整性和一致性，以确保在需要恢复时能够准确无误地还原数据。此外，备份数据的存储和管理也是关键。应选择安全可靠的存储设备，并制定严格的访问控制策略，以防止未经授权的访问和数据泄露。除了数据备份外，制定详细的灾难恢复计划（DRP）也是必不可少的。DRP应明确在发生严重安全事件时的应对措施和恢复流程，以确保业务的快速恢复。这包括确定恢复目标、制定恢复策略、分配恢复任务、准备恢复环境等。通过定期的演练和评估，可以不断完善DRP，提高应对突发事件的能力[3]。在实施数据备份与恢复策略时，还需要考虑相关法规和标准的要求。例

如，某些行业可能对数据的保留期限、备份方式、恢复时间等有明确的规定。因此，在制定策略时需要充分了解并遵循这些法规和标准，以确保合规性。

2.5 物理安全防护

物理安全防护是工业控制系统安全的重要环节，它涉及对重要设备的实体保护，以防止未经授权的访问、破坏或数据泄露。为了确保工业控制系统的稳定运行和数据安全，必须对关键设备进行物理加固和保护。首先，对重要的工业控制系统设备进行物理加固是至关重要的。这包括但不限于加固设备的外壳，使用防破坏、防篡改的材料和设计，以增强设备本身的抗破坏能力。同时，应采用专门的安全锁具、封闭式的设备机架和防护罩等物理隔离手段，进一步防止未经授权的访问和恶意破坏。除了设备加固，还需要确保设备运行环境的安全性。这包括安装监控摄像头、入侵检测系统和报警装置，以便实时监控设备的运行状态和周围环境，及时发现并处置任何异常事件。同时，应定期对设备进行维护保养，确保其正常运行，延长使用寿命。此外，建立严格的设备进出管理制度和审计机制也是物理安全防护的重要组成部分。所有设备的进出都应有详细的记录和审批流程，确保只有经过授权的人员才能接触和操作关键设备。同时，应建立完善的设备台账，记录设备的名称、型号、序列号、使用部门、安装位置等信息，以便进行设备追踪和管理。为了进一步确保设备的安全性和可追溯性，还应实施定期的设备盘点和审计。通过对比台账记录和实际设备情况，及时发现和解决设备丢失、损坏或挪用等问题。同时，审计机制还应包括对设备操作记录、维护保养记录等的审查，以确保设备的合规使用和及时维护。

2.6 安全监测与日志分析

安全监测与日志分析在工业控制系统的安全防护中扮演着至关重要的角色。为了实时掌握系统的安全状况，必须对工业控制系统的网络流量、系统日志和操作行为等关键信息进行持续、实时的监测。通过网络流量监测，我们可以追踪和分析进出系统的数据包，从而识别出异常流量模式，如突发的数据请求或大量的外部连接尝试。这些可能是潜在的网络攻击或数据泄露的迹象。系统日志则记录了系统的运行状态、用户活动和潜在的安全事件，对于事后追溯和调查至关重要。为了更有效地分析这些数据，我们可以利用大数据分析和机器学习技术。大数据分析能够处理海量的监测数据，提取出有价值的信息；而机器学习技术则能从这些数据中学习到正常的行为模式，并自动检测出与正常模式不符的异常行为。这种深度挖掘和分析不仅能及时发现潜在的安全威胁，还能预测未来的安全趋势，为安全防护提供有力的数据支持[4]。当然，仅仅依靠监测和分析是不够的。当发现安全事件时，必须能够迅速、有效地做出反应。因此，建立完善的安全事件应急响应机制至关重要。这个机制应该包括明确的响应流程、负责人员和沟通渠道，确保在发现安全事件时能够第一时间进行处置，降低损失。此外，定期的安全培训和演练也是必不可少的。通过培训，我们可以提升员工的安全意识和技能；而通过演练，可以检验应急响应机制的有效性，发现并修正其中可能存在的问题。

结语

工业控制系统的网络安全防护是一项长期而艰巨的任务。本文提出的防护策略旨在为工业控制系统提供全方位的安全保障，从制度、技术、管理和物理等多个层面进行综合防护。然而，随着技术的不断进步和威胁的不断演化，我们还需要不断更新和完善防护策略以应对新的挑战。未来研究方向可包括探索更加智能化的安全防护技术和方法、加强国际合作共同应对网络安全威胁等。

参考文献

[1]杨轶茜,张龙山.大数据背景下工业控制网络信息安全防护存在的问题及措施[J].网络安全和信息化,2023(3):119-121.

[2]郝文涛,鲁晔,水永莉.工业控制网络入侵检测技术研究[J].工业控制计算机,2022,35(4):4.

[3]蒲永杰.工业控制系统网络安全防护措施的研究[J].设备管理与维修,2022(21):114-115.

[4]房亮,蔡东东.工业控制网络安全的研究与应用[J].网络安全技术与应用,2022,(04):100-101.