 DOI: https://doi.org/10.12349/iser.v5i12.4048

Network Security Threats and Protection Strategies in Automation Control Systems

Jianquan Zhang

Jiangsu Fuergan Technology Co., Ltd., Nanjing, Jiangsu, 210026, China

Abstract

With the rapid development of automatic control system, the problem of network security has become increasingly prominent. This study takes the automation control system as the research object, analyzes the current network security threats faced by the automation control system, and puts forward the corresponding protection strategy. According to the analysis, there are widespread problems such as vulnerability exploitation, malware infection, illegal operation, and abuse of user rights in automated control systems. Therefore, it is suggested to take measures in the protection strategy: strengthen the system vulnerability management, strengthen the security audit and monitoring, implement the authority management system, strengthen the security protection measures and coping strategies. By finding out the weaknesses in the automation control system and effectively defending these weaknesses, the network security performance of the automation control system can be improved and the occurrence of security incidents can be reduced.

Keywords

automatic control system; cyber security threats; protection strategy; system vulnerability management; security audit; monitoring

自动化控制系统中的网络安全威胁与防护策略

张建全

江苏富而乾科技有限公司，中国 · 江苏 南京 210026

摘　要

随着自动化控制系统的飞速发展，网络安全问题日益凸显。本研究以自动化控制系统为研究对象，分析了当前自动化控制系统面临的网络安全威胁，并提出相应的防护策略。根据分析，自动化控制系统普遍存在漏洞被利用、恶意软件感染、非法操作、用户权限滥用等问题。因此，建议在防护策略上采取：强化系统漏洞管理、加强安全审计与监控、落实权限管理制度、加强安全防护措施及应对策略等措施。通过找出自动化控制系统中的弱点并对这些弱点进行有效的防御，可以提升自动化控制系统的网络安全性能，减少安全事件的发生。

关键词

自动化控制系统；网络安全威胁；防护策略；系统漏洞管理；安全审计；监控

1 引言

自动化控制系统由于其优越的性能和广泛的应用，已经成为现代工业生产中必不可少的一部分。这些系统可以帮助我们实现精确控制，提高生产效率，降低生产成本，并保证工作人员的安全。然而，随着自动化控制系统的飞速发展，系统本身也面临着越来越严重的网络安全威胁。在这些威胁中，普遍存在的问题包括系统漏洞被恶意利用，恶意软件感染，非法操作以及用户权限滥用等，这些网络安全问题已成为影响其正常运行的重要因素。针对这些问题，为了提升自动化控制系统的网络安全性能，减少安全事件的发生，论文将探讨一系列防护策略，内容包含强化系统漏洞管理，加强安全审计与监控，落实权限管理制度，以及加强安全防护措施及应对策略等。

2 自动化控制系统的网络安全现状

2.1 网络安全在自动化控制系统中的重要性

在当代工业与制造领域中，自动化控制系统被广泛应用于提高生产效率和优化过程控制[1]。这些系统的广泛采用也使其成为网络攻击的潜在目标，网络安全在自动化控制系统中显得尤为重要。自动化控制系统通常涉及多个组件和模块，通过互联网连接以实现数据交换和远程操作。这种联网特性使得控制系统更易受到网络攻击，如数据窃取、未经授权的访问及服务中断等。这类攻击可能导致生产流程的中断、安全隐患增加，甚至可能引发严重的经济损失和环境问题。

除了潜在的直接攻击风险，自动化控制系统的复杂性

【作者简介】张建全（1972–），男，中国安徽芜湖人，工程师，从事自动化研究。

使其更容易受到内部威胁的侵害。内部人员可能滥用其访问权限，从而对系统造成无意或恶意的破坏。这样的安全漏洞不仅源于技术层面的不足，也反映了管理层面的挑战。对于关键信息基础设施，网络安全事件可能造成难以估量的破坏，与公共安全乃至国家安全息息相关。

推进互联网环境下的自动化控制系统的网络安全性，对于维护生产持续性、保护知识产权及防止商业竞争对手利用安全漏洞而言，都是至关重要的。网络安全在这个背景下是确保自动化生产线及商业运营稳定性的基石。不仅需要关注技术解决方案，还需兼顾策略制定与管理实践的融合，以提供全面的安全保障。

2.2 自动化控制系统面临的网络安全威胁

自动化控制系统在不断发展中，其面临的网络安全威胁日益多元且复杂。系统漏洞成为被攻击者广泛利用的突破口，这些漏洞不仅来源于操作系统和应用程序，也可能存在于网络协议和设备固件中。一旦这些漏洞被利用，攻击者可能将未经授权的指令注入系统，导致系统行为异常或功能失效。恶意软件的入侵对自动化控制系统构成严重威胁 [2]。攻击者利用漏洞传播病毒、蠕虫或勒索软件等恶意程序，这些程序可以中断系统正常运行、窃取敏感信息，甚至对系统进行远程控制。非法操作和用户权限的滥用也是自动化控制系统面临的重要威胁。一些内部人员可能因操作失误或故意进行未经授权的操作，导致数据泄露或系统瘫痪。而不当的权限设置可能使得普通用户获取不该拥有的权力，增加了潜在的安全风险。上述威胁的存在，严重影响了自动化控制系统的安全性和稳定性，需要引起足够重视以确保系统的可靠运行。

2.3 自动化控制系统网络安全问题的影响

自动化控制系统的网络安全问题对其运行和管理产生了深远的影响。网络安全事件不仅可能导致系统停机和生产中断，还可能造成重大经济损失 [3]。网络安全漏洞的利用可能导致敏感数据泄露，严重影响企业的业务发展和市场竞争力。关键基础设施若遭受网络攻击，可能对社会公共安全产生连锁反应，导致广泛的社会影响。系统稳定性和可靠性由于安全问题而下降，进而影响企业的信誉和用户信任。自动化控制系统在工业、交通、电力等领域的大量应用，使得网络安全问题的严重性更加突出。这种现象强调了加强网络安全防护措施的重要性，以确保系统持久、稳定、安全地运行。

3 自动化控制系统的网络安全威胁分析

3.1 系统漏洞被利用的状况

在自动化控制系统中，系统漏洞的存在为网络攻击者提供了可乘之机，使其能够利用这些漏洞发起攻击，破坏系统的正常运行。自动化控制系统由于涉及的设备和协议众多，各系统之间的互操作性要求很高，这导致其往往复杂性上升，不易管理，进而增大了漏洞被发现和利用的风险。一些自动化控制设备仍在使用过时的软件和操作系统，这些过时的软件可能未能获得厂商的持续支持与安全更新，使之成为攻击者眼中理想的攻击目标。

攻击者可通过扫描系统识别未修补的漏洞，以注入恶意代码获取未经授权的访问权限，或中断和篡改数据，进而操控整个自动化流程。尤其值得关注的是，许多自动化控制系统与互联网连接，连接安全性不足进一步加剧了被攻击的风险。黑客通过网络窃取控制信息或植入恶意程序，可能造成生产过程的停滞、设备的损坏，甚至带来严重的安全事故。

针对这些漏洞问题，加强漏洞管理和及时更新系统是一项重要的防护措施。通过定期进行系统检测和监测，可以及早识别潜在的安全隐患，并采取修补措施，以防止可能的安全威胁。期望通过对系统漏洞的细致分析与管理策略的实施，能够有效降低自动化控制系统在网络环境中的安全风险。

3.2 恶意软件感染的现象

在自动化控制系统中，恶意软件感染已成为一个显著的安全威胁。恶意软件适应性和隐蔽性的不断提高，使其更容易突破传统的防护机制，进而感染系统。自动化控制系统通常由多种软硬件组合而成，且涉及多个接口，这些特性增加了其受恶意软件攻击的风险。攻击者可能通过钓鱼邮件、恶意链接甚至是联网设备间的自动传播等多种方式，将恶意软件引入系统。一旦感染，恶意软件可能会导致系统性能下降，甚至可能远程操控系统功能，导致生产中断，经济损失严重。许多自动化控制系统往往与组织的核心业务密切相关，恶意软件如果窃取机密信息或进行数据篡改，则会对公司声誉和市场竞争力产生不可估量的影响。由于恶意软件种类繁多，攻击模式不断更新，企业必须不断调整防护策略，通过部署智能防护系统和实时更新安全策略，以减轻恶意软件带来的潜在损害，确保自动化控制系统的稳定运行和数据安全。

3.3 非法操作与用户权限滥用对系统安全的威胁

自动化控制系统中的非法操作与用户权限滥用是重要的网络安全威胁。系统的开放性和互联性，使其容易受到未经授权的访问和操作，这些非法操作可能导致数据篡改、信息泄露及系统瘫痪等严重后果。用户权限滥用则通常由内部人员引起，因权限配置不当或监督不足，导致用户未授权地访问敏感资源或执行高风险操作。这种滥用行为不仅破坏了系统的完整性，还可能引发安全事故。尤其在自动化控制环境中，权限的误用可能对生产过程产生直接干扰，影响生产安全和产品质量。合理的权限划分和严格的权限管理制度显得极为重要，需通过定期审计和持续监控，确保用户的操作合法合规，维护系统的安全性与稳定性。

4 网络安全防护策略

4.1 强化系统漏洞管理的策略

在自动化控制系统中，系统漏洞管理的有效性直接影响其整体安全性能。鉴于自动化控制系统中可能存在的漏洞

利用现象，必须在防护策略中优先考虑加强漏洞管理。需要建立全面的漏洞检测机制，通过引入先进的扫描工具和技术手段，能够定期和实时地监控系统的漏洞情况。其目标是尽早发现潜在的漏洞，避免它们被威胁者利用。在检测到漏洞后，及时的修补和更新是关键。采用补丁管理系统可以确保所有应用程序和操作系统都保持最新版本，降低已知漏洞的被利用风险。而针对零日漏洞，通常由于其未被公开或未有补丁，须采取临时隔离、关闭相关服务等措施，直至正式补丁发布。

紧跟在漏洞检测及修复之后，制定持续改进的安全管理制度也是实现长期安全目标的重要路径。通过定期的安全培训和教育，提升系统操作人员的风险意识和安全技能，能够在日常操作过程中主动识别和避免安全隐患。管理层则需承诺对安全资源的持续投入，并对漏洞管理策略的实施效果进行定期评估和调整，以适应不断变化的网络安全环境。强化的系统漏洞管理不仅能减缓潜在攻击带来的风险，也为自动化控制系统的稳健运行奠定坚实基础。

4.2 安全审计与监控的重要性

安全审计与监控在自动化控制系统中的重要性不可低估。自动化控制系统在其运行过程中，常常面对复杂的网络环境，这使得其暴露在多种潜在的网络安全威胁之下。为了有效应对这些威胁，实时开展安全审计与监控成为一种必要手段。安全审计能够记录和分析系统中的各类活动及操作历史，从而为识别异常行为提供重要的数据支持。这种审计过程能够帮助识别潜在的威胁路径，以及可能被攻击者利用的脆弱点，为后续的安全防护策略制定提供依据。

监控则为系统提供了一种动态防御的机制，通过对网络流量、用户活动和系统操作进行实时监控，可以快速发现并响应异常行为，防止小范围的安全事件演变为大规模的系统崩溃。监控系统的配置应具备智能化的分析能力，能够根据历史活动模式识别新型威胁，以保证其在面对不断变化的网络攻击手段时保持有效性。

结合安全审计与监控的双重措施，可以显著提高自动化控制系统的安全性能。这不仅增强了系统对潜在安全威胁的预测能力，也提升了系统在面对安全事件时的响应速度和处理效率，对确保系统的持续可靠运行至关重要。

4.3 权限管理制度和安全防护措施的实施

权限管理制度和安全防护措施的有效实施是提升自动化控制系统网络安全的重要环节。权限管理制度应划分不同用户角色，明确各角色的访问权限和操作范围，定期更新权限配置，防止权限滥用或因人员变动导致的权限泄露。为确保安全防护措施的落实，必须依托技术手段对系统进行实时监控和审计。应引入多因素认证技术，加强账户安全，以减少未授权访问的风险。在实现制度执行前，强调安全意识培训，确保操作员和用户充分理解并遵循安全规程，以保障自动化控制系统的总体安全性和稳定性。

5 结语

在此研究中，我们探讨了自动化控制系统面临的网络安全威胁，并针对这些威胁提出了具体有效的防护策略，诸如强化系统漏洞管理、加强安全审计与监控、落实权限管理制度、加强安全防护措施及应对策略等。我们相信，对这些安全威胁的认识和处理，以及这些防护策略的实施，将极大地提升自动化控制系统的网络安全性能，并有助于减少安全事件的发生。然而，我们也认识到，目前的研究还存在一定的局限性。网络安全是一种动态的、复杂的状态，它需要持续的关注和实践来适应和对抗新的威胁。因此，未来的研究需要进一步探索如何持续和有效地提升自动化控制系统的网络安全性能。例如，如何建立和优化动态的、自适应的安全防护机制等。

参考文献

[1] 陆卫军,黄文君,章维,等.网络化控制系统的安全威胁分析与防护设计[J].自动化博览,2019(2):60-65.

[2] 过建春.浅析自动化控制系统网络安全隐患与对策[J].浙江冶金,2020(4):43-45.

[3] 钱程.办公自动化网络安全及防护策略[J].科学与财富,2020(5):48.