制造业自动控制网络安全问题初探

杨东霖
葫芦岛锌业股份有限公司　辽宁　葫芦岛　125000

摘　要：随着制造业数字化转型加速推进，自动控制系统在生产中广泛应用。本文聚焦制造业自动控制网络安全问题展开初步探讨。首先阐述了制造业自动控制网络安全的重要性，其关乎生产连续性与稳定性、企业核心数据资产保护以及供应链安全维护。接着分析了该领域面临的常见网络安全问题，如系统漏洞与配置错误、恶意软件与病毒攻击、供应链攻击以及物联网设备安全风险等。最后提出了一系列防护策略，包括建立分层分区防护体系、加强系统漏洞管理与补丁更新、实施数据加密与访问控制、部署入侵检测与防御系统以及加强供应链安全管理，为制造业自动控制网络安全提供参考。

关键词：制造业；自动控制；网络安全；防护策略

引言：在数字化浪潮席卷全球的当下，制造业正经历着前所未有的变革，自动控制技术成为推动其发展的关键力量。自动控制系统借助先进的信息技术，实现了生产过程的高度自动化与智能化，极大提升了生产效率与产品质量。然而，随着网络技术的深度融入，制造业自动控制系统也面临着日益严峻的网络安全挑战。一旦自动控制系统遭受网络攻击，不仅可能导致生产中断、设备损坏，还会使企业核心数据泄露，甚至影响整个供应链的稳定运行。因此，深入探究制造业自动控制网络安全问题，探寻有效的防护策略，已成为保障制造业可持续发展的当务之急。

1 制造业自动控制网络安全的重要性

1.1 保障生产连续性与稳定性

制造业自动控制系统犹如生产运营的“神经中枢”，精准调控着生产流程的各个环节。一旦遭受网络安全威胁，如恶意软件入侵、网络攻击干扰等，系统可能出现故障、指令错乱等情况，导致生产设备停机、生产线中断。这不仅会造成生产进度延误，影响产品按时交付，还会增加生产成本，如设备维修费用、人工闲置成本等。保障自动控制网络安全，能确保系统稳定运行，使生产流程顺畅无阻，维持生产的连续性，提升企业生产的可靠性和稳定性，增强企业在市场中的竞争力[1]。

1.2 保护企业核心数据资产

制造业自动控制系统存储着大量企业核心数据，涵盖产品设计图纸、生产工艺参数、客户订单信息等。这些数据是企业的核心竞争力所在，具有极高的商业价值。若因网络安全问题导致数据泄露，竞争对手可能获取关键信息，模仿产品、优化工艺，使企业失去竞争优势。同时，数据泄露还可能引发客户信任危机，影响企业声誉。加强自动控制网络安全防护，能有效防止数据被窃取、篡改或破坏，保护企业核心数据资产的安全，为企业的持续发展提供坚实的数据支撑。

1.3 维护供应链安全

在全球化背景下，制造业供应链紧密相连、环环相扣。自动控制系统作为供应链中的关键节点，其网络安全状况直接影响整个供应链的稳定。若某一环节的自动控制系统遭受攻击，可能导致生产中断，进而影响上下游企业的原材料供应、产品交付等环节，引发供应链的连锁反应。维护制造业自动控制网络安全，可确保供应链各环节的信息准确传递和协同运作，避免因网络问题导致的供应链中断、延迟等问题，保障供应链的安全与稳定，促进整个制造业生态系统的健康发展。

2 制造业自动控制系统面临的常见网络安全问题

2.1 系统漏洞与配置错误

制造业自动控制系统多依赖各类软件和硬件协同工作，软件在开发过程中难免存在编程缺陷，硬件也可能因设计或制造问题存在漏洞。这些漏洞如同隐藏的“后门”，可能被攻击者利用，进而获取系统控制权，干扰生产流程。同时，系统配置错误也较为常见，如不恰当的权限设置、错误的网络参数配置等。错误的配置可能使系统暴露在不安全的环境中，让攻击者有机可乘，导致数据泄露、设备异常运行等问题，严重影响自动控制系统的安全性和稳定性。

2.2 恶意软件与病毒攻击

随着制造业数字化程度的提升，自动控制系统与外部网络的连接日益紧密，这为恶意软件和病毒的传播提供了途径。恶意软件和病毒可通过网络下载、移动存储设备等渠道侵入系统。一旦进入，它们可能篡改系统

程序、窃取敏感数据，甚至控制生产设备，造成生产混乱。而且，新型恶意软件和病毒不断涌现，其隐蔽性和破坏性更强，传统的安全防护手段难以完全抵御，给制造业自动控制系统带来了巨大的安全威胁[2]。

2.3 供应链攻击

制造业自动控制系统的供应链涉及众多环节，包括零部件供应商、软件开发商、系统集成商等。攻击者可将目标瞄准供应链中的薄弱环节，通过在零部件中植入恶意芯片、在软件中预留后门等方式，在系统建设初期就埋下安全隐患。由于供应链的复杂性和跨地域性，一旦某个环节出现问题，可能迅速蔓延至整个系统，影响生产的正常进行。并且，供应链攻击往往难以提前察觉，增加了自动控制系统面临的安全风险。

2.4 物联网设备安全风险

在制造业自动控制系统中，物联网设备的应用越来越广泛，如传感器、智能仪表等。这些设备通常具有计算和通信能力，但安全防护能力相对较弱。它们可能存在默认密码、弱加密算法等安全问题，容易被攻击者破解和利用。攻击者可通过控制物联网设备，获取系统中的敏感信息，或者干扰设备的正常运行，进而影响整个自动控制系统的性能。此外，物联网设备数量众多、分布广泛，管理难度较大，也进一步增加了其面临的安全风险。

3 制造业自动控制网络安全防护策略

3.1 建立分层分区防护体系

建立分层分区防护体系，是保障制造业自动控制网络安全的关键策略，可全方位抵御网络威胁。(1)分层防护是核心要点。自动控制系统可划分为控制层、监控层、管理层等不同层次。控制层部署工业防火墙等设备，严格限制网络访问，仅放行必要通信流量，防止外部非法入侵干扰生产指令。监控层借助安全审计、入侵检测等技术，实时监测系统运行状态，及时发现异常与潜在隐患。管理层采用加密技术处理重要数据，保障数据在传输和存储时的保密性与完整性。(2)分区防护同样不可或缺。依据系统功能和安全需求，将其划分为生产区、办公区、管理区等安全区域。不同区域间设置严格安全边界，通过访问控制策略限制数据流动与用户访问。如生产区作为核心，严格控制外部设备接入，仅允许授权设备通信，避免恶意软件或病毒入侵。(3)要注重各层各区间的协同防护。各层次和区域的安全防护设备与技术需相互配合、信息共享，形成有机整体。一旦某一层次或区域检测到安全威胁，能迅速将信息传递给其他部分，触发相应防护机制，实现快速响应与协同防御，提升整个自动控制系统的安全防护水平，为制造业稳定生产筑牢安全防线。

3.2 加强系统漏洞管理与补丁更新

加强系统漏洞管理与补丁更新是维护制造业自动控制网络安全的核心环节，能有效降低系统被攻击的风险，保障生产的稳定运行。(1)要建立全面的漏洞扫描机制。定期使用专业的漏洞扫描工具对自动控制系统进行全面检测，涵盖操作系统、应用程序、网络设备等各个方面。这些工具能够自动识别系统中存在的已知漏洞，如未修复的安全补丁、配置错误等。通过定期扫描，可以及时发现潜在的安全隐患，为后续的修复工作提供依据。(2)及时获取并评估漏洞信息。密切关注安全厂商、开源社区等发布的安全公告和漏洞信息，及时了解新发现的漏洞及其影响范围和严重程度。对获取到的漏洞信息进行详细评估，分析其是否会对自动控制系统造成威胁。对于高风险的漏洞，要优先安排修复工作，避免攻击者利用这些漏洞对系统发起攻击。(3)制定合理的补丁更新策略。根据漏洞评估结果，制定详细的补丁更新计划，明确补丁更新的时间、范围和方式。在更新补丁前，要对补丁进行充分的测试，确保其不会对系统的正常运行产生负面影响。对于关键的生产系统，可以采用分阶段更新的方式，先在测试环境中进行验证，确认无误后再在生产环境中部署。同时，要建立补丁更新的记录和跟踪机制，及时掌握补丁的更新情况，确保所有系统都能及时得到修复[3]。

3.3 实施数据加密与访问控制

在制造业自动控制网络里，实施数据加密与访问控制对保障数据安全、防止信息泄露意义重大，可大幅提升系统安全性与可靠性。(1)数据加密是保护数据机密性的关键手段。自动控制系统中存储和传输着大量敏感数据，像生产工艺参数、设备控制指令、客户订单信息等。存储时，将数据加密后存入数据库或存储设备，即便数据被非法获取，攻击者也难以直接读取内容。传输过程中，利用加密技术确保数据不被窃取或篡改。常见的对称与非对称加密算法，可根据数据安全需求和使用场景灵活选用。(2)访问控制能有效限制用户对系统资源的访问权限。依据用户角色和职责分配不同权限，保证用户仅能访问工作所需的数据与功能。例如，生产操作人员只能接触生产控制相关内容，管理人员则可访问全面系统信息并开展管理操作。同时，建立严格的身份认证机制，如用户名、密码、数字证书等，防止非法用户进入。(3)要定期审查和更新访问控制策略。企业业务发展和人员岗位变动时，及时调整用户访问权限，撤销

离职或不再需要权限人员的访问资格，保证策略有效及时。还可借助日志审计功能记录用户访问行为，以便在安全事件发生时追溯分析，为系统安全稳定运行提供坚实保障。

3.4 部署入侵检测与防御系统

在制造业自动控制网络里，部署入侵检测与防御系统（IDS/IPS）是增强安全防护能力、及时应对网络威胁的重要手段。(1)入侵检测系统能实时监测网络流量与系统活动。它如同敏锐的“哨兵”，持续扫描网络中的数据包，分析其特征和行为模式。通过对正常行为基线的建立，一旦检测到异常流量，如异常的访问频率、非授权的端口访问等，便会立即发出警报。这种实时监测能力，可让安全人员第一时间察觉潜在的网络攻击，为后续的应对争取宝贵时间，避免攻击进一步扩散造成更大损失。(2)入侵防御系统具备主动阻断攻击的能力。当入侵检测系统发现可疑活动并判定为攻击行为后，入侵防御系统会迅速采取行动，自动阻断攻击源与目标系统之间的连接。它可以丢弃恶意数据包、重置网络连接，防止攻击者继续深入系统内部，有效保护自动控制系统的核心设备和关键数据不受侵害。(3)要定期更新入侵检测与防御系统的规则库。网络攻击手段不断演变，新的攻击方式和漏洞层出不穷。定期更新规则库，能使系统及时识别最新的攻击特征，提高检测的准确性和防御的有效性。同时，结合系统的日志分析功能，不断优化检测策略，提升系统对各类复杂网络攻击的应对能力。

3.5 加强供应链安全管理

制造业自动控制系统的供应链涉及众多环节，加强其安全管理对保障整个系统稳定运行至关重要。(1)严格供应商筛选与管理。在选择供应商时，要对其技术实力、安全资质、信誉等方面进行全面评估。优先选择具有良好安全记录和成熟安全管理体系的供应商，确保其提供的产品和服务在安全方面有可靠保障。与供应商建立长期合作关系时，要签订明确的安全协议，规定双方在安全方面的责任和义务，从源头上降低供应链安全风险。(2)强化供应链产品安全检测。在产品进入自动控制系统前，要对其进行严格的安全检测。包括对硬件设备的物理安全检查，查看是否存在被篡改或植入恶意硬件的痕迹；对软件进行漏洞扫描和安全评估，确保其不存在已知的安全漏洞和恶意代码。只有通过安全检测的产品，才能进入系统使用，防止不安全的产品成为系统安全的薄弱环节。(3)建立供应链安全信息共享机制。与供应商保持密切沟通，及时共享安全信息。当发现供应链中存在安全威胁或漏洞时，能够迅速通知相关供应商，共同采取措施进行应对和修复。同时，供应商也能及时向企业反馈产品安全状况和更新信息，形成安全防护的合力，提升整个供应链的安全水平[4]。

结束语

制造业自动控制网络安全问题，是数字化浪潮下企业必须直面的关键挑战。从系统自身漏洞、恶意攻击，到供应链环节潜藏的风险，每一处隐患都可能引发生产停滞、数据泄露等严重后果。本文所探讨的分层分区防护、漏洞管理、数据加密、入侵防御以及供应链安全管理等策略，为构建安全防线提供了思路。然而，网络安全形势瞬息万变，未来仍需持续投入研究，紧跟技术发展，不断优化防护体系。唯有如此，才能确保制造业自动控制系统在安全的环境中稳定运行，推动制造业向智能化、高效化稳步迈进。

参考文献

[1]顾鑫.铝电解自动控制网络安全问题及对策研究[J].建筑设计及理论,2022.109.

[2]吴龙飞杨勇.机械制造业的网络安全措施分析[J].文化科学,2021.212.

[3]宋雨婷.基于轨迹交叉理论的制造业生产安全问题研究[J].建筑理论,2023.167

[4]颜仕柱.制造业企业信息安全问题探讨[J].文化科学,2022.256