工业互联网的安全防护策略研究

罗 巍
中国黄金集团江西金山矿业有限公司，江西 上饶 334200

[摘要]在我国现代化科技行业发展过程中，工业互联网已经成为人们日常工作中必不可少的组成部分了，但是在具体运行的过程中所产生的安全问题较为突出，如果并没有采取科学性较强的应对方案，不仅会出现新的丢失，还会对用户造成较为严重的损失。因此要强化对工业互联网网络安全问题的有效关注，依据问题的发生原因选择针对性较强的应对方案，有效地减少对工业互联网使用所产生的影响，促进行业的稳定发展和进步。

[关键词]工业互联网；网络安全；措施
DOI：10.33142/sca.v6i6.9353 中图分类号：F42 文献标识码：A

Research on Security Protection Strategies for Industrial Internet

LUO Wei
China National Gold Group Jiangxi Mining Co., Ltd., Shangrao, Jiangxi, 334200, China

Abstract: In the development process of Chinese modern technology industry, the industrial internet has become an essential component of people's daily work. However, the security issues generated during the specific operation process are more prominent. If a scientifically strong response plan is not adopted, not only will new losses occur, but also serious losses will be caused to users. Therefore, it is necessary to strengthen effective attention to the security issues of industrial internet networks, select targeted response plans based on the causes of the problems, effectively reduce the impact on the use of industrial internet, and promote the stable development and progress of the industry.

Keywords: industrial internet; network security; measures

在进行工业互联网网络安全管理的过程中，要贯彻落实因地制宜的工作原则，按照不同安全问题的表现形式选择对应的应对策略，并且还需要强化风险防范的意识，将预防思维贯穿于不同的工业互联网使用环节。从根本上减少各种安全问题的发生，营造良好的网络生态，提高工业互联网的使用效果。

1 工业互联网常见安全隐患

1.1 欠缺安全接口统一标准

工业互联网的发展使得各种设备和系统能够相互连接，实现数据的共享和交流，为企业提供了更高效、智能的生产运作模式。然而，正是这种高度的互联性，也让我们的工业系统暴露在前所未有的安全风险中。其中，欠缺安全接口统一标准成为工业互联网常见的安全隐患之一[1]。安全接口统一标准的缺失，导致了工业互联网系统在接入、通讯、验证等环节的漏洞无法被根本解决。各个设备和系统的接口千差万别，缺乏统一的规范和标准，造成了信息传输的不稳定性和易受攻击的漏洞。这不仅给企业的生产运营带来了严重的风险，更给整个工业互联网的健康发展带来了巨大的隐患。以工业互联网中的物联网设备为例，其安全接口的缺乏使得设备的认证、权限管理、数据传输等环节容易受到攻击。黑客可以通过攻击设备的弱点，获取敏感信息或操控设备，对企业的生产线和数据造成极大的影响。在工业互联网的高度互联环境下，一旦一个安全漏洞被攻破，将会波及整个系统，造成无法挽回的损失。此外，缺乏安全接口统一标准也给企业的信息交流和合作带来了困难。各个企业的系统架构和接口设计差异很大，导致了信息传输的不统一和不兼容。这不仅增加了企业间协作的复杂性，也限制了工业互联网整体的发展速度。如果没有一个统一的标准，工业互联网的生态系统将无法形成，各个参与方之间的沟通和合作将受到严重阻碍。

1.2 应急管理机制不完善

工业互联网的迅猛发展，将信息技术与传统工业深度融合，为生产运营带来了巨大便利。然而，随之而来的是新的安全风险和挑战。在众多的安全隐患中，安全应急管理机制的不完善问题尤为突出。工业互联网的特性使得其更容易受到网络攻击。当互联网与传统工业设备相结合时，攻击者可以利用网络漏洞远程操控设备或者通过入侵企业内网获得重要信息。然而，对于这些安全威胁的应对，往往并未形成具体而成熟的安全应急管理机制，这使得潜在的危害进一步加剧。

首先，缺乏健全的风险评估体系是导致安全应急管理不完善的重要原因之一。在工业互联网环境中，诸如设备故障、网络攻击、人为操作失误等各种风险都可能导致重大安全事故。然而，很多企业在项目实施初期往往对这些

风险进行一次性评估，缺乏全面性和持续性。仅凭一次性评估难以覆盖风险的动态变化，从而难以针对性地制定安全应急预案。

其次，安全应急响应机制的缺失也是导致问题的重要因素。在现实生活中，事故的发生往往难以预料，因此需要制定相应的应急预案。然而，工业互联网领域往往缺乏健全的应急响应机制。一旦安全事故发生，企业可能面临无从应对的困境，导致安全风险的进一步扩大。此外，安全意识和文化的缺失也是安全应急管理不完善的重要原因。在工业互联网环境中，技术的不断进步并不能完全解决安全问题。当企业缺乏员工的安全意识和安全文化时，技术的防护措施往往难以达到预期效果。

2 工业互联网的安全防护策略

2.1 制定统一安全接口标准

工业互联网的蓬勃发展，为生产制造业注入了新的活力，然而，随之而来的网络安全风险也日益凸显。为了保障工业互联网的安全，制定统一安全接口标准成为当务之急。在工业互联网中，物联网设备和工业控制系统的连接和交互过程中，涉及各种复杂的通信协议和数据格式。这给网络安全防护带来了诸多挑战，因为各个厂商的设备和系统往往采用不同的安全接口，导致安全策略的统一难以实现。为解决这一问题，制定统一安全接口标准显得尤为重要。首先，统一安全接口标准可以实现不同设备和系统之间的无障碍互通。通过确立统一的接口标准，可以建立广泛的合作共识，使得各个厂商能够基于共同的安全标准进行开发，从而建立起安全防护的联动机制[2]。

其次，统一安全接口标准可以提升网络安全防护的效率和准确性。通过统一标准，可以有效降低安全策略的制定和执行的复杂性。同时，统一标准能够提供更加精确的安全指引，使得网络安全防护能够更早地发现和应对潜在的威胁，有效遏制网络攻击的蔓延。然而，制定统一安全接口标准并非易事。首先，各个厂商的利益关系错综复杂，需要在平衡各方利益的基础上达成共识。其次，技术层面上的挑战也不容忽视，需要进行大量的技术研究和实践验证，以确保标准的可行性和稳定性。为了成功制定统一安全接口标准，企业需要跨越厂商之间的壁垒，建立起紧密的合作机制。政府、企业和专家学者应当共同参与，形成多方共治的格局，共同制定标准。此外，还需要加强技术研发力量，在全国范围内组织专业的研究机构和团队，推动安全接口标准的研究和实践，积极引进国际先进的经验和技术。制定统一安全接口标准，是保障工业互联网安全的关键一步。通过统一的标准，我们能够构建起更加稳固的工业互联网安全体系，为生产制造业的可持续发展提供坚实保障。

2.2 健全应急管理机制

首先，建立一个完善的安全应急预警系统是至关重要的。通过采用先进的监测技术和数据分析手段，能够及时发现和预测潜在的安全威胁。在监测过程中，可以引入人工智能技术，对大数据进行分析，识别异常行为和风险点，从而有效地预警和预防安全事件的发生。这种科技手段的应用将大大提高安全预警的准确性和效率，为应对突发事件提供有力保障[3]。

其次，构建一个高效的应急响应机制是至关重要的。一旦发生安全事件，及时、有效的应对和处理是保障企业安全的关键。在应急响应机制中，需要明确应急责任人，建立科学合理的指挥体系，制定详尽的应急预案，并定期进行演练和训练。同时，与相关机构建立紧密的合作机制，形成跨部门、跨领域的协同作战能力，提高应对突发事件的能力和水平。此外，加强信息共享和协同合作是提升安全应急管理机制的关键一环。工业互联网的安全问题涉及多个主体和领域，需要各方共同参与和合作。建立信息共享平台，使各方能够及时了解安全威胁和风险，共同制定应对策略和措施。同时，加强国际的合作与交流，借鉴他国的先进经验和技术，形成全球范围内的安全应急网络。只有形成了一个协同合作的生态系统，才能更好地应对工业互联网安全挑战。

总之，健全安全应急管理机制是工业互联网安全防护的核心要素。通过建立完善的安全应急预警系统、高效的应急响应机制和信息共享与协同合作机制，我们能够更好地应对安全威胁和风险，保障企业的安全和稳定发展。

2.3 强化病毒防护

工业互联网的蓬勃发展，为生产制造行业带来了前所未有的便利和机遇，然而，随之而来的是日益严峻的网络安全威胁。在这个数字化时代，病毒的威胁已经不再局限于个人电脑，而是扩展到工业控制系统中。为了确保工业互联网的安全可靠运行，强化病毒防护显得尤为重要[4]。强化病毒防护的方法多种多样，下面将介绍几种行之有效的措施：

首先，建立健全的安全基础设施是强化病毒防护的前提。对工业互联网系统进行全面彻底的网络安全评估，发现潜在的安全风险，修补系统漏洞，加强网络监控和流量分析，确保系统的稳定和可靠性。同时，建立安全事件响应机制，及时发现并应对安全事件，减少病毒入侵的危害。

其次，加强对网络设备和系统的安全防护是非常重要的。通过采用高级的防火墙、入侵检测系统和入侵防御系统等安全设备，可以有效阻挡病毒的入侵。并且，及时更新和升级防病毒软件以及其他安全工具，以应对新出现的病毒和安全威胁，确保系统的持续运行和数据的安全。此外，建立良好的权限管理制度也是强化病毒防护的重要环节。通过制定合理的权限策略，限制用户的操作和访问权限，防止恶意软件利用系统漏洞进行病毒传播。同时，加强对用户行为的监控和审计，及时发现和处理异常行为，

确保系统的安全和稳定。

最后，加强员工安全意识教育和培训也是强化病毒防护的关键。定期组织网络安全知识培训，提高员工对病毒防护的认识和意识，让他们了解病毒的危害和防范措施，并且知道如何正确使用网络和互联网资源，避免在工作中存在安全漏洞。

2.4 系统的科学维护

近年来，随着工业互联网的快速发展，企业的生产与管理方式发生了翻天覆地的变化，信息技术也成为了推动生产力提升的重要力量。然而，随之而来的信息安全问题也愈发突出，网络攻击频频发生，给企业的生产经营带来了严重威胁。为了应对这一挑战，系统科学维护成为了工业互联网安全防护的重要方法之一。系统科学维护是一套系统性的、综合的安全防护方法，通过对工业互联网系统进行全方位的保护和维护，确保其正常运行和安全可靠。它借鉴了系统科学的思维和方法，结合信息安全技术，为工业互联网的安全运行构建了坚实的防线。

首先，系统科学维护强调的是整体性。工业互联网系统是一个复杂的网络结构，涵盖了多个终端设备、网络设备、传感器等组成部分。系统科学维护将重点放在整个系统的运行和安全性上，而非局限于某个部分。它通过全面识别和分析系统的安全隐患和风险，对系统的各个部分进行监测和维护，保证整个系统的运行稳定和安全可靠。

其次，系统科学维护注重的是动态性。工业互联网系统的运行是一个动态变化的过程，随着企业的发展和需求的变化，系统也需要不断进行更新和升级。系统科学维护通过对系统的实时监测和分析，及时发现潜在的安全隐患，并采取相应的措施进行修复和改进。它能够对系统进行动态调整，不断适应复杂多变的安全环境，保持系统的安全性和稳定性。此外，系统科学维护还注重的是预防性。传统的安全防护方法往往是被动式的，只有在攻击发生后才能进行应对。而系统科学维护通过综合运用现代信息安全技术，对系统进行全面的预防性保护。它通过建立安全策略和规范、加强访问控制和身份验证、进行数据加密和备份等手段，有效地阻止潜在的攻击和入侵，确保系统的安全性和可靠性。在实际应用中，系统科学维护方法得到了广泛的认可和应用。它帮助企业建立了一个全方位的安全体系，从物理安全到网络安全，从设备安全到人员安全，实现了对工业互联网系统的全面防护。凭借其优越的性能和高度的可靠性，它为企业的生产运营提供了可持续的保障。

2.5 安全隐患动态监测

安全隐患动态监测是一种全面且精准的安全监测手段。它通过收集和分析大量的数据信息，以实时、准确的方式掌握安全隐患的动态变化，从而及时采取相应的预防措施，保障人们的生命和财产安全。

首先，安全隐患动态监测依托于先进的传感技术和物联网技术。通过在工业互联网中大规模布置传感器和设备，可以实时感知工作环境中的各种安全风险因素，如温度、湿度、气体浓度等，以及设备的运行状态、风险事件的发生等。这些数据会被传输到云平台上，经过分析和处理后，转化成可视化的信息，为人们提供直观、全面的安全监测结果。

其次，安全隐患动态监测通过机器学习和人工智能算法的引入，进一步提高了监测的准确性和效率。通过分析历史数据和实时数据，可以建立一套有效的安全预测模型，预测未来可能发生的安全隐患，并通过智能决策系统提供相应的预防方案。例如，在工业生产中，当设备温度升高到一定程度时，系统会自动发出警报并采取措施降温，从而避免设备损坏和安全事故的发生。

3 结束语

在工业互联网使用过程中，安全防护是必不可少的工作环节，不仅要配合现代化的技术方案来选择合适的防护策略，还需要使用户具备一定的安全防范意识，融合不同的技术模式，搭建一体化的安全防护网络，灵活地应对在工业互联网运行中存在的各项隐患，在前期将隐患扼杀在摇篮之中。有效地减少诸多因素对工业互联网运行所产生的影响，进一步地提高网络的安全系数。

[参考文献]

[1]张富强.大数据时代的计算机网络安全及防范措施[J].通信电源技术,2020,37(9):177-178.
[2]邢方方.计算机通信与网络远程控制技术的应用研究[J].信息通信,2020(6):148-149.
[3]吕金龙.基于预防策略的工业互联网防御技术分析[J].科学技术创新,2019(35):70-71.
[4]家玮.试论新时期计算机网络信息安全及防火墙技术应用研究[J].通信与信息技术,2019(6):41-43.

作者简介：罗巍（1986.12—），男，南昌大学，计算机科学与技术，中国黄金集团江西金山矿业有限公司，电气副主任，工程师。