安全科学与工程学报
Journal of Safety Science and Engineering
第 3 卷◆第 4 期◆版本 1.0◆2025 年
文章类型：论文丨刊号（ISSN）：2972-4716(P) / 2972-4724(O)

基于数字孪生技术的海关智慧实验室网络安全优化研究

韩晶[1] 梁召[1] 韩祎陟[2,*]
1 中国海关科学技术研究中心 2 呼和浩特海关
DOI:10.32629/jsse.v3i4.17872

[摘 要] 随着智慧实验室的快速发展,网络安全问题日益凸显。智慧实验室的智能化、数字化特性使其面临诸多网络安全风险,如数据泄露、系统漏洞、恶意攻击等。本文从智慧实验室的网络安全现状出发,分析其面临的主要网络安全挑战,并结合数字孪生技术的应用,探讨如何通过技术手段、管理措施和人才培养等多方面提升智慧实验室的网络安全水平。研究结果表明,数字孪生技术不仅能够优化智慧实验室的管理效率,还能为网络安全提供新的解决方案,为智慧实验室的建设和发展提供有力保障。
[关键词] 智慧实验室；网络安全；数字孪生技术；数据安全
中图分类号：TN915.08 文献标识码：A

Research on Cybersecurity Optimization of Customs Smart Laboratory Based on Digital Twin Technology

Jing Han[1] Zhao Liang[1] Yizhi Han[2,*]
1 Science and Technology Research Center of China Customs
2 Hohhot Customs, Hohhot

[Abstract] With the rapid development of smart laboratories, cybersecurity issues have become increasingly prominent. The intelligent and digital characteristics of smart laboratories expose them to numerous cybersecurity risks, such as data leakage, system vulnerabilities, and malicious attacks. This paper begins with the current state of cybersecurity in smart laboratories, analyzes the main cybersecurity challenges they face, and explores how to enhance the cybersecurity level of smart laboratories through technological means, management measures, and talent cultivation, in combination with the application of digital twin technology. The research results show that digital twin technology can not only optimize the management efficiency of smart laboratories, but also provides new solutions for cybersecurity, thereby providing strong support for the construction and development of smart laboratories.
[Key words] Smart Laboratory; Network Security; Digital Twin Technology; Data Security

引言

海关智慧实验室是海关系统数字化转型的重要组成部分,其通过物联网、大数据、人工智能等技术实现实验室的自动化、智能化和信息化。智慧实验室的网络系统不仅存储着大量的实验数据、科研成果和个人信息,还连接着各种高精度设备和复杂的实验环境,智慧实验室的网络化和数字化特性使其面临诸多网络安全风险,如数据泄露、系统漏洞、网络攻击等。因此,提升智慧实验室的网络安全水平是保障智慧实验室正常运行和科研成果安全的关键。

数字孪生技术作为一项前沿技术,为智慧实验室的建设和管理提供了新的思路和方法。通过构建物理实体的虚拟模型,并实现物理世界与数字世界的实时交互,数字孪生技术不仅可以优化智慧实验室的管理效率,还能为网络安全提供新的解决方案。本文将探讨如何结合数字孪生技术提升智慧实验室的网络安全水平。

1 智慧实验室网络安全现状

1.1智慧实验室的网络架构

智慧实验室的网络架构通常包括实验室内部网络、物联网设备、数据存储系统、实验室信息管理系统(LIMS)以及与外部网络的连接。这些系统和设备通过网络连接在一起,实现数据的共享和设备的远程控制。然而,这种复杂的网络架构也带来了诸多网络安全风险。

1.2面临的网络安全挑战

数据安全风险：智慧实验室存储着大量的实验数据、科研成果和个人信息,在数据的存储、传输和分析过程中,数据的完整性、保密性和可用性面临挑战,这些数据一旦泄露,将对科研

人员和实验室造成严重损失。

系统设备安全漏洞：智慧实验室的网络系统可能存在软件漏洞、配置错误等问题，实验室智能设备和传感器因接入复杂性增加，可能存在安全漏洞，容易被黑客利用进行攻击。

恶意攻击威胁：黑客可能通过网络攻击智慧实验室的系统，导致系统瘫痪、数据丢失或被篡改。

内部安全威胁：实验室内部人员可能缺乏网络安全意识，因操作不当或恶意行为导致网络安全事件，如未经授权访问敏感数据、篡改实验结果等，从而引发安全事件。

2 数字孪生技术在智慧实验室网络安全中的应用

2.1数字孪生技术概述

数字孪生技术通过构建物理实体的虚拟模型，并实现物理世界与数字世界的实时交互，为智慧实验室的建设和管理提供了强大的技术支持。数字孪生技术的核心在于实现物理实体和虚拟模型之间的数据同步和交互，通过对虚拟模型的分析和优化，为物理实体的运行提供决策支持。

2.2数字孪生技术在智慧实验室网络安全中的应用场景

2.2.1实时监控与预警

数据采集与分析：通过在实验室设备和网络节点上安装传感器，实时采集设备运行数据和网络流量数据。这些数据被传输到数字孪生模型中进行分析，能够及时发现异常行为和潜在威胁。

智能预警系统：数字孪生模型可以根据预设的安全规则和异常模式，实时生成安全预警信息。一旦检测到异常行为，系统可以立即发出警报，通知管理员采取措施。

可视化监控：数字孪生技术可以将复杂的网络环境和设备状态以直观的三维模型形式展示出来，方便管理员快速了解网络安全状况，及时发现和处理问题。

2.2.2漏洞检测与修复

漏洞扫描与分析：利用数字孪生模型对实验室网络系统进行全面扫描，检测系统中的漏洞和配置错误。通过模拟攻击场景，评估漏洞的潜在风险。

自动修复与优化：数字孪生模型可以根据扫描结果，自动生成修复方案，并通过自动化工具对系统进行修复和优化。同时，模型可以对修复后的系统进行验证，确保漏洞被彻底修复。

持续监控与改进：数字孪生技术可以持续监控系统的运行状态，及时发现新的漏洞和风险，并根据实际情况动态调整安全策略。

2.2.3物联网设备安全管理

设备身份认证：通过数字孪生模型为每个物联网设备分配唯一的数字身份，实现设备的精准识别和管理。只有经过认证的设备才能接入实验室网络，防止非法设备的接入。

设备行为分析：通过数字孪生模型实时监测物联网设备的行为，分析设备的运行状态和数据传输情况。一旦发现设备行为异常，如数据传输量突增、设备位置改变等，系统可以立即采取措施，如断开设备连接、进行安全检查等。

设备固件更新：通过数字孪生模型远程监控物联网设备的固件版本，及时发现设备固件的漏洞和缺陷。通过自动化工具对设备固件进行更新和升级，确保设备的安全性和可靠性。

2.2.4数据加密与隐私保护

数据加密：利用数字孪生技术对采集到的数据进行加密处理，确保数据在传输和存储过程中的安全性。通过采用先进的加密算法，防止数据被窃取或篡改。

访问控制：根据用户的权限和角色，对数据进行细粒度的访问控制。只有经过授权的用户才能访问特定的数据和资源，防止数据泄露和滥用。

隐私保护：对敏感数据进行匿名化处理，确保用户隐私得到保护。同时，通过建立隐私保护机制，防止未经授权的第三方访问用户数据。

3 智慧实验室网络安全的优化策略

3.1技术手段

采用先进的网络安全技术，构建网络安全防护体系：如防火墙、入侵检测系统、防病毒软件等，构建多层次的网络安全防护体系。更重要的是，应以数字孪生平台为核心，整合这些孤立的安全能力，形成协同联动的防御体系。

加强数据加密与备份：对重要数据进行加密处理，并定期进行数据备份，防止数据丢失或被篡改，确保数据的安全性和可用性。数字孪生模型可以用于模拟数据恢复流程，验证备份数据的有效性和恢复时间目标(RTO)。

实施物联网设备安全管理：管理人员可以通过数字孪生技术对物联网设备进行身份认证、行为分析和固件更新，确保物联网设备的安全性以及数据的不可篡改和可追溯性。

利用人工智能与机器学习：管理人员可以通过人工智能和机器学习技术对网络流量和设备行为进行分析，及时发现异常行为和潜在威胁。数字孪生体为AI模型提供了丰富、高质量的训练数据，并能提供一个安全的模型验证环境，从而提升AI在安全应用中的准确性和可靠性。

3.2管理措施

建立健全网络安全管理制度和应急响应机制：制定网络安全政策、操作规程和应急预案，明确各部门和人员的网络安全责任。制定网络安全应急预案，确保在发生安全事件时能够快速响应和恢复。可以利用数字孪生技术进行无风险的网络安全应急演练，提升团队的实战响应能力。

加强网络安全培训与教育：定期对实验室人员进行网络安全培训，提高实验室工作人员的网络安全意识和操作技能。利用数字孪生平台创建沉浸式的培训场景，让员工在模拟的网络安全事件中进行操作，加深理解。

落实制度要求，积极开展网络安全审计与评估：严格按照国家网络安全法和相关法规要求，落实网络安全等级保护制度。定期对实验室的网络安全状况进行审计和评估，及时发现和解决网络安全问题。

数字孪生体可以记录所有的网络操作和状态变化，为安全审计提供完整、不可篡改的数据证据链。

加强与外部机构的合作，与网络安全企业、科研机构等合作，共同开展网络安全研究和技术应用，借鉴先进经验和技术，提升海关智慧实验室网络安全水平。

3.3人才培养

建立激励机制加强网络安全专业人才培养：通过提供良好的职业发展空间，吸引网络安全人才；通过海关教育培训平台、职业技能培训等方式，培养一批具备网络安全专业知识和技能的人才。

鼓励跨学科人才培养：鼓励计算机科学、信息安全、海关实验室管理、海关业务监管等多学科交叉培养，培养具备综合能力的网络安全人才。

4 数字孪生技术在智慧实验室网络安全中的优势

4.1实时性与动态性

数字孪生技术能够实时反映物理实体的运行状态，并根据实时数据动态调整安全策略。这种实时性和动态性使得智慧实验室能够快速响应网络安全事件，减少损失。它改变了传统安全防护静态、被动的局面，实现了安全与业务的同步演进。

4.2可视化与直观性

数字孪生技术通过三维模型直观展示实验室的网络环境和设备状态，方便管理员快速了解网络安全状况，及时发现和处理问题。这种“一张图”式的管理极大地降低了安全运维的门槛和复杂度。

4.3预测性与预防性

数字孪生技术可以通过模拟攻击场景和分析潜在风险，提前预测网络安全事件的发生，并采取预防措施。这种预测性和预防性能够有效降低网络安全事件的发生概率。

4.4集成性与协同性

数字孪生技术可以将多种网络安全技术集成在一起，实现不同技术之间的协同工作。这种集成性和协同性能够提高智慧实验室的网络安全防护能力。

5 结论

智慧实验室的网络安全是保障其正常运行和科研成果安全的关键。数字孪生技术作为一项前沿技术，为智慧实验室的网络安全提供了新的解决方案。通过实时监控与预警、漏洞检测与修复、物联网设备安全管理以及数据加密与隐私保护等应用场景，数字孪生技术能够显著提升智慧实验室的网络安全水平。同时，结合技术手段、管理措施和人才培养等多方面的策略，可以进一步完善海关智慧实验室的网络安全体系。未来，随着技术的不断发展，海关智慧实验室网络安全建设需要持续优化和创新，例如探索数字孪生与区块链技术结合以确保安全日志的不可篡改性，或研究零信任架构在数字孪生环境下的具体实施路径，以应对日益严峻和复杂的网络安全挑战。

[参考文献]

[1]张宇晴.数字化转型背景下档案安全风险评估与防控体系构建研究[J].办公室业务,2025(16):108-110.

[2]杨九祥,李明,王荣,等.高等级生物安全实验室智慧化管理平台开发及关键技术研究[J],2025,55(08):66-71+59.

[3]曹雪英.变电系统常见故障及基于数字孪生的变电运维技术研究[J].电力设备管理,2025(09):41-43.

[4]张翔.基于数字孪生技术的医疗网络数据安全保护系统设计智能物联技术[J].2025,57(01):71-74.

[5]梁晓莹,事业单位档案管理信息化的安全性问题及保障措施[J],办公室业务,2024(22):16-18.

[6]励渊伟,浅析常用网络安全威胁因素及网络安全审计的应用与研究[J].网络安全技术与应用,2025(10):23-25.

[7]杜文,邓靖,马鹏飞,等.数字孪生技术在海关应用中的安全性探索[J].中国口岸科学技术,2024,6(10):20-24.

作者简介：

韩晶(1980--),女,学士,高级工程师,主要从事海关实验室信息化管理研究方向。

*通讯作者：

韩祎陟(1970--),男,学士,高级工程师,主要从事海关实验室管理研究方向。