Research on Security Issues in Digital Twin Construction for Operational Network Data Centers

Xiaoming Tang Qidong Wang* ZhigangGuo

Unit 92192, Ningbo, Zhejiang, 315122, China

Abstract

While the introduction of digital twin technology in operational network data centers can significantly enhance maintenance efficiency, its highly interconnected nature also introduces complex security risks. This paper focuses on the construction of digital twins in operational data centers, conducting an in-depth analysis of potential security threats from three dimensions: data flow, system architecture, and human-machine applications. It identifies data tampering at the collection stage, transmission link hijacking, storage leakage, and application-layer logic flaws as core vulnerabilities. Based on this, a layered defense system architecture centered on "data-system-security" is proposed, offering corresponding technical countermeasures from three aspects: data lifecycle security protection, system platform resilience reinforcement, and application interaction with business logic security, aiming to provide insights for similar engineering practices.

Keywords

digital twin; network server room; network security; multi-layered defense

在运网络机房数字孪生建设中的网络安全问题研究

汤小明 王栖东* 郭志刚

92192部队，中国 · 浙江 宁波 315122

摘要

在运网络机房引入数字孪生技术虽能显著提升运维效能，但其高度互联的特性也带来复杂的安全风险。本文针对在运机房数字孪生建设，从数据流转、系统架构及人机应用三个维度深入剖析了潜在的安全威胁，指出采集端篡改、传输链路劫持、存储泄露及应用层逻辑缺陷是核心隐患。在此基础上，构建了一套以“数据—系统—安全”为主轴的纵深防御体系架构，从数据全生命周期安全防护、系统平台韧性加固、应用交互与业务逻辑安全三个方面提出了相应的技术对策，期望能为同类工程实践提供借鉴。

关键词

数字孪生；网络机房；网络安全；纵深防御

1 引言

传统机房运维长期受制于设备异构度高、信息多源难融合、决策高度依赖经验等瓶颈，导致故障响应往往处于被动救火状态，且任何一次微小的配置变更都可能引发不可预知的连锁反应[1]。为破解这一管理困局，数字孪生技术应运而生。该技术通过构建高保真的虚拟映射模型，实现了物理机房与数字空间的实时交互与闭环控制[2]。目前，在运营商骨干节点、金融机构数据中心以及高校智慧校园等场景中，数字孪生已展现出在资产可视化、能耗优化及故障预测等方面的巨大潜力[3]。

然而，在建设与运行过程中，由于数字孪生打破了传统机房的安全边界，将原本封闭的控制体系暴露给了更广阔的网络空间。新的安全隐患逐渐出现：在数据层，海量感知数据的采集与融合面临完整性与机密性挑战；在系统层，复杂的微服务架构与异构协议交互扩大了被攻击面；在应用层，人机交互若缺乏严格校验，极易成为逻辑攻击的跳板。一旦孪生系统被恶意控制，攻击者不仅可窃取敏感数据，甚至能通过控制通道对物理机房实施破坏性操作。因此，系统性地识别并防御这些新型安全风险，已成为在运机房数字孪生建设中亟待解决的关键课题[1]。

2 在运机房网络数字孪生建设面临的主要安全威胁

2.1 数据流转环节的安全隐患

数字孪生的价值基础在于获取完整、准确的数

【作者简介】汤小明（1987-），男，中国陕西汉中人，硕士，工程师，从事网络数字孪生、自动化运维、图神经网络研究。

【通讯作者】王栖东（1993-），男，中国广东广州人，本科，工程师，从事自动化运维、网络安防研究。

据，而在运机房环境复杂，数据从物理世界向数字空间流转的全生命周期均面临着严峻考验。

2.1.1 采集端的数据泄露与篡改

采集端是连接物理与数字世界的“神经末梢”。在机房中，为了获取温湿度、电力负载及设备状态等实时数据，需要部署大量传感器与探针。这类设备通常算力有限，难以运行复杂的加密与认证协议，且所处环境多无人值守，极易遭受物理接触攻击或无线信号劫持。攻击者可通过侧信道攻击窃取敏感信息，或直接篡改采集数据。例如，设备温度异常的情况下攻击者伪造了“设备温度正常”的错误信息，将导致冷却系统误判，进而引发物理设备过热宕机。这种“数据投毒”行为具有极高的隐蔽性，直接动摇了孪生系统决策的根基。

2.1.2 传输链路的安全风险

机房设备虽然处于一个相对封闭的物理环境中，但在数字孪生架构下，数据可能需跨域传输至云端或中心分析平台。若传输协议缺乏强加密保护，或密钥管理机制存在缺陷，数据在传输途中就可能被中间人攻击截获、解密甚至重放。特别是在利用公网或跨网闸传输时，传统的边界防护手段往往难以应对高级持续性威胁（APT）的渗透。此外，传输链路的可靠性将直接影响孪生模型的准确度，网络拥塞或抖动导致的丢包，虽然不是恶意攻击，却会造成孪生平台与物理实体间的状态失步，引发运维误判。

2.1.3 数据存储风险

数字孪生系统需要长期保存海量的历史运行数据以不断完善预测模型，这使得存储系统成为重点攻击目标。一方面，硬件故障、勒索软件加密或管理员误操作均可能导致核心数据永久丢失，造成孪生系统“失忆”；另一方面，随着数据量的指数级增长，若未能及时动态调整存储系统的访问控制策略，极易出现权限过度开放或未授权访问等问题。特别是在多租户或跨部门共享数据的场景下，若缺乏细粒度的隔离和保护机制，敏感数据的泄露风险将会显著增加。

2.2 系统层面的安全隐患

支撑数字孪生平台运行的底层架构与操作系统，其自身的脆弱性是系统安全的重大考验。

2.2.1 系统自身漏洞

数字孪生平台通常采用微服务、容器化技术及云原生架构，组件多且更新频繁。若架构设计存在缺陷，如服务间通信缺乏双向认证、API接口权限控制粒度不够精细，将比代码级漏洞更具危害。在实现层面，内存越界、逻辑错误等传统漏洞依然存在，且由于开源组件的广泛应用，整个数据处理链条的安全风险被进一步放大。此外，多源异构数据的融合处理逻辑非常复杂，任何一个模块的异常都可能导致整个系统崩溃。

2.2.2 外部攻击威胁

数字孪生平台一旦上线，便直面外部攻击的威胁。除了常规的恶意软件与病毒外，针对系统的DoS/DDoS攻击可导致孪生平台瘫痪，从而无法对机房进行有效监控。通过APT攻击，攻击者可能在系统中长期潜伏，通过钓鱼邮件、0day漏洞等方式逐步获取系统权限，最终目标是窃取核心网络拓扑、密钥资产或下达破坏性指令。

2.3 应用层面的安全隐患

应用层是运维人员与数字孪生系统交互的主要接口，也是安全体系构建的“最后一公里”。

2.3.1 人机交互安全

数字孪生系统提供了丰富的可视化与反向控制功能，这极大提升了运维效率，但也引入了新的攻击面。人机交互界面若缺乏严格的输入校验与输出编码，就可能遭受跨站脚本（XSS）、命令注入等Web攻击。攻击者可利用这些漏洞绕过前端权限检查，直接在后台执行高危指令。在机房管理场景中，交互界面往往集成了批量重启、配置下发等关键职能，一旦会话被劫持或连接凭证被盗，攻击者便可借“合法运维人员”之手，对物理设施实施准确打击。

2.3.2 业务逻辑层面的安全

与传统Web应用不同，数字孪生的业务逻辑与物理设备的操作规程高度关联。若系统设计时未充分考虑可能出现的异常情况，如权限校验顺序错误、状态机跳转异常等，将导致严重的逻辑漏洞。此外，配置管理也是重灾区，默认口令未修改、敏感配置明文存储、安全策略未及时下发等问题，在快速迭代、多人合作的开发模式下不断出现。随着孪生平台功能的持续扩展，业务逻辑的复杂度将不断增加，安全风险也会随之不断累加。

3 安全防护策略与技术手段

3.1 纵深防御体系架构设计

为有效应对上述安全风险，指望依靠单一安全产品或技术已不现实。本文提出了一个分层级、多维度的纵深防御体系，沿着“数据-系统-应用”这条主线，搭建一个贯穿安全治理全周期的框架。该框架力图把安全能力长到业务链条里去：在数据层，实施全生命周期的机密性与完整性保护，确保“数据可用却看不透”；在系统层，通过提高架构韧性，并配合主动防御技术，让系统具备了自愈能力；在应用层，建立基于身份与上下文的动态访问控制体系，把“最小权限”与“零信任”原则落到实处。

3.2 数据全链路安全防护

3.2.1 采集端的安全加固

针对边缘设备防护薄弱的问题，防护思路应往前挪。在硬件选型时就应要求其具备可信计算模块（TPM），让每台设备入网之前先过身份关。在数据传输前，利用轻量级数字签名技术给数据盖章，平台拿到数据后，就知道是否被篡改。同时，部署边缘清洗网关，在数据入湖前把异常值过滤掉，并进行实时脱敏，后端处理压力小了，就能降低泄露风险。

3.2.2 传输链路的加密保护

传统的网络边界防护已不再够用，应全面启用内核为国密算法的TLS 1.3协议，确保传输通道的机密性与抗量子计算能力。针对跨域传输场景，引入软件定义边界（SDP）技术，身份验证通过，再给通道，将业务端口对公网完全隐藏，扫描和暴力破解就无从谈起。此外，利用硬件安全模块（HSM）实现密钥生成、存储与轮换的自动化，构建符合机房业务逻辑实际的动态密钥管理机制，杜绝密钥泄露隐患。

3.2.3 存储安全的组合策略

数据存储方面，应采用“透明加密+独立密钥管理”的组合策略，数据本身用强加密锁起来，密钥单独保管，就算硬盘被搬走了，没有密钥也是一堆乱码。对于那些需要多方协作或审计溯源的关键数据，可以考虑区块链作为存证工具，利用其不可篡改特性构建可信的数据血缘图谱。同时，部署数据库审计与异常行为分析系统，确保面对批量导出、非工作时间访问等高危操作，系统能够及时反应并阻断。

3.3 系统平台的韧性加固

系统安全的核心在于“假设被突破”的前提下，仍能维持核心功能的可用与可控。

3.3.1 漏洞的全流程管理

漏洞不能等上线了再查，要从编写就开始盯，把DevSecOps的理念嵌进开发流程里，代码一提交就自动跑SAST静态分析和DFT模糊测试。针对已上线系统，不能动则停机打补丁，通过虚拟补丁机制，在网络层做拦截，临时修复高危漏洞，为正式补丁的测试与部署留出缓冲时间。同时，开源组件的供应链安全也不能忽视，要建立组件准入清单和持续检测机制，第一时间响应0day漏洞情报。

3.3.2 主动防御外部威胁

全面落地零信任架构，不能再抱有“内网即安全”的旧想法，对所有访问请求都要基于身份、设备、环境等多维度进行持续验证。部署基于机器学习的入侵检测系统（IDS），深度挖掘海量日志和流量数据里的信息和模式，学习什么是正常的业务基线，对于偏离基线的异常行为（如低频慢速攻击、内部横向移动等），就可以精准判别，从而具备对APT攻击的早期预警与自动化响应能力。

3.4 应用层的安全管控

应用层是运维人员使用频率最高的模块，安全方面收的过紧则会影响效率，太松则会出现风险，需要实现灵活与安全的平衡。

3.4.1 细粒度访问控制

基于角色的静态授权（RBAC）过于粗放，已不再适用了，一个人一个角色，应转向ABAC——基于属性的动态授权。系统每次有人要操作，就根据这个人当前的身份属性、在干什么、用的设备安不安全、要操作的数据有多敏感，当场算一下该给多大权限。例如，当运维人员从非授信终端访问时，自动触发多因子认证（MFA）或限制其仅能查看而不能修改。凡是涉及到关键配置的操作，全部走二次确认加审批的流程，确保关键指令的可追溯与可审计。

3.4.2 业务逻辑的完整性校验

建立统一的输入校验与输出编码框架，从架构层面杜绝注入类漏洞。得对数字孪生平台的核心控制逻辑做好形式化验证或自动化配置核查，确保每一条指令都不会让设备跑到不安全的状态。在系统迭代时，引入混沌工程理念，主动往系统里扔故障、或者进行非常规操作，注入异常数据，看看业务逻辑是否足够健壮，容错机制是否真的管用，别等出事了才亡羊补牢。

4 结束语

在运网络机房数字孪生建设是一项复杂的系统工程，网络安全不仅是其底线，更是促使其不断迭代的内生动力。本文从数据、系统、应用三个维度剖析了当前面临的安全威胁，并提出了纵深防御框架与关键技术对策。然而，安全与对抗是一场没有终点的比赛，随着人工智能技术的不断渗透，基于AI的自适应安全引擎将成为标配，推动防御范式向意图驱动演进。同时，零信任架构将与数字孪生底座深度耦合，构建起无处不在、无时不有的安全免疫系统。此外，同态加密、多方安全计算等隐私计算技术的成熟，将为跨域、跨层级的数据协作提供更好的解决方案。这些也是本文后续工作研究的主要方向。

参考文献

[1] 郭夙昌;黄金涛;邓雷升;吴茜;刘在爽;林夕. 网络安全数字孪生研究[J]. 信息安全与通信保密, 2023, (6): 29-39.

[2] 刘喜洋;周阳;朱原;刘柏强;陈磊. 基于数字孪生的移动网络机房数智化管控应用研究[J]. 电子产品世界, 2024, 31(6): 13-15.

[3] 梁建都. 浅谈计算机机房的安全管理与维护[J]. 新潮电子, 2024, (3): 154-156.