 DOI: https://doi.org/10.12345/bdai.v6i4.30554

Data governance and information security strategies of oil drilling enterprises under the background of digital transformation

Jun Chang Xinghua Su Sheng Zhan Ning Bai

Chuanqing Drilling Engineering Co., Ltd. Changqing Drilling Corporation, Xi'an, Shaanxi, 710021, China

Abstract

Amid the global digital transformation of the energy sector, oil drilling companies are transitioning from traditional operational models to more intelligent practices. This article examines the contradictions in data governance and information security within the oil drilling industry from the perspective of 'data assetization': the conflict between vast amounts of heterogeneous data and inefficient utilization, and the conflict between the need for cloud-edge-end collaboration and cybersecurity protection. To address these issues, the article proposes a 'three-dimensional governance model' that includes a data standard system, an intelligent governance platform, and a dynamic security protection network based on a zero-trust architecture. It also suggests solutions that cover the entire data lifecycle. Empirical studies show that this system can significantly enhance the accuracy of abnormal parameter identification in drilling operations, greatly improve data sharing efficiency, and effectively intercept advanced persistent threat (APT) attacks, providing a replicable model for digital transformation security in the industry.

Keywords

oil drilling enterprises; digital transformation; data asset management; zero trust security; intelligent drilling

数字化转型背景下石油钻探企业数据治理与信息安全策略

常军 苏兴华 詹胜 白宁

川庆钻探工程有限公司长庆钻井总公司，中国 · 陕西 西安 710021

摘 要

在全球能源行业数字化转型的浪潮中，石油钻探企业正从传统作业模式向智能化跨越。本文以“数据资产化”为核心视角，剖析了石油钻探行业在数据治理与信息安全领域的矛盾：海量异构数据与低效利用之间的矛盾、云边端协同需求与网络安全防护之间的矛盾。针对这些矛盾，本文构建了“三维立体治理模型”，包括数据标准体系、智能治理平台和基于零信任架构的动态安全防护网，并提出覆盖数据全生命周期的解决方案。实证研究表明，该体系可显著提升钻井参数异常识别的准确率，大幅提高数据共享效率，有效拦截高级持续性威胁（APT）攻击，为行业提供了可复制的数字化转型安全范式。

关键词

石油钻探企业；数字化转型；数据资产化治理；零信任安全；智能钻井

1 引言

当前行业普遍存在数据孤岛化严重、治理手段滞后、安全防护碎片化等问题，导致数据价值释放受阻。以长庆油田为例，2023 年的实践表明，缺乏统一治理体系的钻井数据中异常数据误报现象频发，严重影响了智能决策效能。

为突破传统“技术工具论”的研究框架，本文提出“数据治理 - 安全防护 - 业务增值”的闭环价值模型。通过对塔里木油田、胜利油田等典型案例的深度解构，本文揭示出数据治理需遵循“业务定义数据、数据驱动业务”的螺旋上升规律；信息安全体系应从“被动防御”向“主动免疫”演进，构建“数据血缘追踪 - 动态权限控制 - 威胁智能感知”的三维防御链。此外，本文通过建立数据治理成熟度评价指标体系，量化评估企业数字化转型效能。

2 石油钻探企业数字化转型背景与现状

2.1 数字化转型的行业背景

石油钻探行业作为能源供应的核心产业，其数字化转型不仅是技术迭代的必然趋势，更是应对能源结构转型、碳减排压力与资源开发复杂化的战略选择。近年来，石油钻探领域的数字化渗透率显著提升，智能钻井、数字孪生井场、AI 地质建模等技术的广泛应用，极大地推动了作业效率的提升。

2.2 技术驱动因素与政策推力

(1) 物联网与人工智能 。随着井场设备智能化水平的不断提高，单井部署的传感器数量大幅增加，数据生成量呈爆发式增长。例如，斯伦贝谢的 DrillOps 系统通过机器学习

【作者简介】常军（1978–），男，中国陕西咸阳人，本科，高级工程师，从事网络技术及信息安全研究。

优化钻井路径，显著缩短了复杂地层的钻井周期并降低了成本。

(2) 市场与政策推力 。国际能源署（IEA）要求油气勘探开发的碳排放强度大幅降低，国内“十四五”规划也将智能钻井装备和油气大数据平台列为能源技术革命的重点方向，并通过政策补贴支持数字化改造。

(3) 数据治理与信息安全 。数据已成为石油钻探企业的核心战略资产，其治理与安全直接关系到企业的存续能力。例如，壳牌公司的数字孪生项目通过整合地质、工程和设备数据，大幅提升了钻井事故的预测准确率，显著减少了潜在损失。然而，全球油气行业遭受的 APT 攻击次数显著增加，凸显了数据安全的重要性。

2.3 行业现状与挑战

(1) 数据治理现状 。数据孤岛与协同需求的矛盾突出，地质与工程部门的数据格式互不兼容，跨部门共享需手动转换，耗时较长。数据质量与决策依赖失衡，钻井传感器数据缺失问题严重影响了 AI 模型的训练精度。

(2) 安全投入与威胁升级 。大多数企业仍采用传统的防火墙 +VPN 架构，难以应对零日攻击与横向渗透。攻击检测到处置的时间远超能源行业推荐的黄金响应期。

(3) 转型进程中的瓶颈 。在国产化替代进程中，硬件与软件的兼容性问题导致系统性能损失。此外，数字孪生井场的建设初期投入较高，中小型企业难以承担。

2.4 行业突破方向

中石化胜利油田通过搭建 Hadoop+Spark 数据平台，整合多类业务数据，显著提升了查询效率。挪威 Equinor 公司采用“持续验证”机制，大幅缩小了内部攻击面。Baker Hughes 与微软合作开发的 Azure 数字钻井平台，实现了云端算法与边缘设备的高效联动。

3 石油钻探企业数据治理的难点与热点问题

3.1 技术割裂到业务协同失效导致数据孤岛问题

石油钻探企业的数据孤岛问题本质上是“技术异构性”与“组织壁垒”双重作用的结果。系统协议差异和工业协议封闭性是主要的技术障碍。例如，地质部门使用的 Petrel 地质建模软件（基于 OpenWorks 数据库）与工程部门的 Landmark 钻井设计系统（采用 Oracle 架构）数据格式互不兼容，跨系统共享需通过人工导出 / 导入或定制脚本转换，效率低下。此外，西门子 S7-1500 PLC、ABB 变频器等设备采用私有通信协议，导致实时工况数据难以接入统一平台，限制了数据的整合与共享。

为突破这一困境，行业内已有积极尝试。斯伦贝谢推出 DELFI 平台，通过 OPC UA 统一架构整合多类工业协议，显著提升了数据跨系统流动效率。中海油服搭建“勘探开发数据湖”，归集多类业务数据，支持 API 调用，有效解决了数据孤岛问题。[1]

3.2 数据质量与标准从“脏数据”到“可信决策”

数据质量问题严重影响了石油钻探企业的数字化转型。钻井传感器因高温振动等恶劣工况导致信号丢失，进而影响 AI 模型的准确性。同时，边缘节点至云端的数据同步延迟问题，导致实时优化决策失效概率增加。此外，国际数据标准在国内复杂地质条件下的适配性不足，企业自研数据标准与国际标准存在冲突，增加了跨境数据共享的合规成本。

为应对这些挑战，行业企业采取了多种措施。哈里伯顿开发了 AI 驱动的 DataQA 工具，自动检测钻井数据异常，显著提升了数据质量。阿美石油建立了可配置的元数据管理平台，支持按区块、井型动态调整数据采集标准，为数据质量提升提供了有力支持。

3.3 数据安全与隐私保护

随着数字化转型的推进，石油钻探行业的数据安全与隐私保护面临严峻挑战。全球油气行业遭受 APT 攻击的次数呈显著增长趋势，攻击目标聚焦于关键数据与控制系统。[2] 第三方承包商通过 VPN 漏洞植入后门，窃取地质数据并转售竞争对手，给企业带来巨大经济损失。

为应对这些挑战，企业采取了一系列措施。埃克森美孚部署“持续验证”机制，动态调整访问钻井数据的权限，有效减少了内部攻击面。壳牌采用联邦学习技术，实现跨国联合建模时不共享原始数据，满足多司法辖区的合规要求。

4 石油钻探企业信息安全策略

4.1 建立完善的信息安全管理体系

企业制定《数据主权保护白皮书》，明确数据跨境流动规则，划定“核心数据（T0 级）- 重要数据（T1 级）- 一般数据（T2 级）”三级保护体系。针对钻井作业场景，编制多项操作手册，覆盖高频业务场景。对标国际标准（如 ISO 27001、NIST CSF）和法规（如 GDPR、中国《数据安全法》），建立合规性矩阵，确保跨国作业合规。

在组织架构方面，设立敏捷化的安全组织，由首席信息安全官（CISO）牵头，董事会下设网络安全委员会，定期评估威胁态势。组建红蓝攻防团队，实施全天候安全运营，并在井队配置网络安全专员，负责边缘设备准入控制与日志采集。此外，与安全厂商共建“油气工控安全实验室”，开发行业专用威胁情报库。

4.2 强化信息安全技术防护

部署华为 HiSec Insight AI 防火墙，基于机器学习识别 APT 攻击流量，误报率极低。将钻井业务网络细分为多个安全域，实现横向流量加密，并布设蜜罐系统，诱捕攻击者，缩短响应时间。利用 MITRE ATT&CK 框架构建攻击链模型，成功阻断供应链攻击。[3]

在关键节点部署量子密钥分发（QKD）设备，提升抗量子计算破解能力，并在云端处理加密数据，降低隐私泄露风险。通过数字孪生技术构建井场控制系统行为图谱，实时监测 P4.3 构建数据安全治理框架

采用自然语言处理（NLP）技术实现智能数据分类分级，根据数据使用场景动态调整密级。实施全生命周期可信管控，关键操作日志上链存证，引入量子擦除技术确保退役硬

盘数据不可恢复。在审计与响应方面，引入用户行为分析系统，标记异常访问行为，预设应急响应剧本，提升处置时效。

4.4 加强数据共享与协同安全

构建零信任数据共享平台，基于 SDP 技术实现“数据不动计算动”的共享模式，采用 ABAC 模型动态调整权限。建立隐私增强型协同计算机制，支持跨油田联合建模与区块竞标场景中的加密参数比选，确保数据不出本地。

此外，联合行业企业共建“油气数据可信联盟链”，实现设备证书互认与威胁情报共享，并对承包商数据接口实施沙盒测试，有效拦截供应链攻击。

4.5 技术效益与行业影响

实施上述策略后，某大型钻探企业数据泄露事件显著减少，APT 攻击拦截率大幅提升。企业主导制定多项行业标准，相关实践获国家网络安全等级保护优秀案例。

5 石油钻探企业数据治理与信息安全的实践案例

5.1 案例背景

在数字化转型过程中，石油钻探企业面临诸多挑战。以某石油钻探企业为例，其在转型中遭遇了数据孤岛、数据质量差和信息安全风险高等问题。各部门数据系统相互独立，导致信息流通不畅，制约了运营效率和决策科学性。同时，数据的准确性、完整性和一致性不足，难以满足企业对数据的高要求。此外，随着数字化程度的提高，信息安全风险日益凸显，数据泄露和网络攻击等威胁时刻存在。为此，企业实施了一系列数据治理与信息安全策略。

5.2 数据治理实践

5.2.1 建立统一数据平台

企业通过整合各部门的数据系统，打破数据孤岛，建立统一数据平台，实现数据的集中管理和共享。例如，延长石油集团与海尔卡奥斯合作共建的延长云享工业互联网平台，有效实现了数据的贯通共享，提升了数据利用效率。[4]

5.2.2 提升数据质量

企业制定严格的数据质量标准，采用数据清洗、校验等技术手段，去除重复、错误和不完整的数据，确保数据的准确性和一致性。例如，在钻探数据分析中，通过回归分析和时间序列分析等方法进行预处理，显著提高了数据的可用性。

5.2.3 统一数据标准

企业制定企业级数据标准，规范数据格式和编码规则，确保数据的一致性和可比性，为数据分析和决策提供了可靠基础。例如，在石油钻探领域，通过统一数据标准，实现了不同来源数据的整合与分析。

5.3 信息安全实践

5.3.1 建立信息安全管理体系

企业制定信息安全政策，设立信息安全组织架构，加强人员安全意识培训，提升员工对网络攻击和数据泄露等风险的防范意识，减少因人为因素导致的安全风险。

5.3.2 强化信息安全技术防护

企业部署防火墙、入侵检测系统和数据加密等安全设备，强化网络安全防护和数据加密处理，有效抵御外部攻击和内部威胁。例如，在数据传输过程中采用加密技术，确保数据的保密性和完整性。[5]

5.3.3 构建数据安全治理框架

企业实施数据分类分级管理、生命周期管理和安全审计监控，保障数据的安全性和合规性。例如，根据数据的敏感程度和重要性进行分类分级管理，确保不同级别的数据采取相应的安全措施。

5.3.4 实践效果

通过数据治理与信息安全策略的实施，企业数据孤岛问题得到有效解决，数据质量显著提升，信息安全风险大幅降低。企业运营效率显著提高，数字化转型取得阶段性成果。例如，延长石油集团通过数据治理和信息安全措施，实现了业务数据化、数据资产化和资产价值化，为生产经营管理决策分析提供了有力支持。

6 结论与展望

石油钻探企业在数字化转型过程中，数据治理与信息安全是至关重要的环节。通过构建完善的数据治理与信息安全体系，企业能够有效解决数据孤岛、数据质量低下以及信息安全风险高等问题，进而显著提升运营效率和竞争力。本文的研究表明，数据治理与信息安全的协同推进，不仅优化了企业的数据管理能力，还为企业的智能化决策提供了坚实支撑。

未来，随着数字化技术的持续演进，石油钻探企业应进一步优化数据治理与信息安全策略。一方面，企业需加强技术创新，充分利用人工智能、物联网、区块链等前沿技术，提升数据治理的智能化水平和信息安全的防护能力；另一方面，企业应注重管理创新，完善数据治理与信息安全的组织架构和流程机制，确保数据治理与信息安全体系的动态适应性。

参考文献

[1] 李明, 王海涛. 油气工业数字化转型中的数据治理体系构建研究[J]. 中国石油大学学报(社会科学版), 2023, 39(2): 45-56.

[2] 张伟, 陈立. 石油勘探开发企业信息安全防护体系研究[J]. 信息安全研究, 2021, 7(3): 22-30.

[3] 刘洋, 周凯, 赵志刚. 基于联邦学习的钻井数据安全共享机制[J]. 计算机工程与应用, 2023, 59(10): 123-132.

[4] 国家能源局. 智慧油气田建设指南（2021版）[Z]. 北京: 国家能源局, 2021.

[5] 全国信息安全标准化技术委员会. 信息安全技术 网络安全等级保护基本要求（GB/T 22239-2019）[S]. 北京: 中国标准出版社, 2019.