油气企业计算场景下信息化安全防护体系的构建路径

何星辰
中国石油化工股份有限公司华东油气分公司　江苏　南京　210019

摘　要：油气企业计算场景覆盖全业务链条，数字化转型下安全需求聚焦数据、业务与资产安全，面临外部攻击、内部泄露、系统脆弱性等多重风险。本文构建了“技术+管理+人员”三位一体的信息化安全防护体系总体框架，涵盖指导思想、总体架构与核心模块。提出从技术架构智能联动、管理机制全流程规范、人员能力分层培养三方面构建具体路径，以保障油气企业计算场景安全，推动业务稳定发展。

关键词：油气企业；计算场景；信息化安全防护

引言：在数字化转型浪潮下，油气企业计算场景已深度融入勘探、生产、运输、销售等全业务链条。随着业务与信息技术的深度融合，数据泄露、网络攻击、系统脆弱性等安全威胁日益凸显，不仅威胁企业核心资产安全，更关乎国家能源战略稳定。如何构建适应油气行业特性的信息化安全防护体系，成为保障业务连续性与可持续发展的关键命题。

1 油气企业计算场景安全需求与风险分析

1.1 典型计算场景分类

油气企业典型计算场景可按业务环节划分为四大类。勘探开发计算场景以高性能计算集群为核心，支撑地震资料处理、油藏数值模拟等密集型计算任务，数据处理量达PB级，对计算节点协同效率要求极高。生产运营计算场景采用工业控制与信息系统融合架构，涵盖井口监控、管道输送、炼化加工等实时控制模块，需保障毫秒级响应与设备联动稳定性。仓储运输计算场景依托物联网与地理信息系统，实现油库库存实时监控、运输车辆轨迹追踪，涉及跨区域数据传输与多终端接入[1]。销售服务计算场景基于云平台构建，支撑加油站收银、客户管理、线上订单处理等业务，面临高频次外部访问与交易数据安全保障压力。四类场景既相互独立又数据互通，形成全链条计算生态。

1.2 核心安全需求

油气企业计算场景核心安全需求围绕业务连续性与资产安全性形成多层体系。数据安全需求占据核心地位，地质勘探原始数据、油藏开发方案等核心数据需实现全生命周期保护，从采集阶段的完整性校验，到传输过程的加密传输，再到存储环节的分级备份，均需建立闭环管控。业务可用性需求针对生产关键环节，要求工业控制计算场景达到99.99%以上可用性，通过冗余架构设计与故障快速切换机制，避免因计算系统中断导致井口停采、管道停输等重大损失。边界防护需求聚焦内外网隔离，生产网与互联网需建立刚性隔离，同时对云平台、移动终端等接入节点实施严格身份认证与权限管控。另外，合规性需求不可忽视，需满足《网络安全法》《数据安全法》等法规要求，实现安全审计可追溯与风险事件可溯源。

2 油气企业计算场景下主要安全风险识别

油气企业计算场景因业务特殊性与架构复杂性，面临多层次、多维度安全风险，风险识别需结合技术特性与业务流程精准定位。外部环境中，网络攻击手段迭代升级，针对工业控制系统的专用恶意代码层出不穷；内部管理中，人员操作失误与权限滥用可能引发数据泄露；技术层面，新旧系统兼容产生的漏洞难以彻底消除。

2.1 外部攻击风险

外部攻击风险是油气企业计算场景最直接的威胁，呈现专业化、针对性强的特点。黑客组织与恶意分子常以破坏生产运营或窃取核心数据为目标，采用多种攻击手段实施渗透。针对工业控制场景，会利用专用协议漏洞注入恶意代码，如针对SCADA系统的勒索病毒，曾导致部分油气企业炼化装置被迫停工。针对云平台与销售系统，常发起分布式拒绝服务攻击，通过海量虚假请求占用计算资源，导致加油站收银系统瘫痪或线上服务中断[2]。钓鱼攻击手段隐蔽性极强，通过伪造企业内部邮件、伪装合作伙伴链接，诱骗员工泄露账号密码，为后续纵深攻击打开通道。外部攻击已形成产业链化运作，攻击工具智能化程度不断提升，给风险防御带来极大挑战。

2.2 内部泄露风险

内部泄露风险源于企业内部人员的有意或无意操作，具有隐蔽性强、识别难度大的特点。有意泄露行为多由利益驱动，部分掌握核心数据的技术人员或管理人员，为谋取私利将地质勘探数据、客户资源信息等出售

给竞争对手，此类行为对企业核心竞争力造成致命打击。无意泄露则多因操作失误导致，如员工在非加密终端存储敏感数据、误点钓鱼链接导致终端中毒、违规将生产数据拷贝带出办公区域等。内部权限管理漏洞加剧了泄露风险，部分岗位存在权限过度授权情况，员工可越权访问非本职工作相关的核心数据，且缺乏有效的操作行为监控。内部人员对企业计算架构熟悉，其引发的泄露风险往往能绕开常规防护措施，造成的损失难以估量。

2.3 系统脆弱性风险

系统脆弱性风险贯穿油气企业计算场景的硬件、软件、网络等各个层面，是安全防护的薄弱环节。硬件层面，部分老旧生产设备服役年限过长，未配备完善的安全防护模块，且难以兼容新型安全设备，如早期井口监控终端缺乏身份认证功能，易被非法接入操控。软件层面，新旧系统兼容性问题突出，生产系统为保障稳定性多采用成熟但版本较旧的操作系统，存在未修复的已知漏洞；自主开发的业务系统在编码阶段若缺乏安全测试，易遗留逻辑漏洞。网络层面，跨场景数据传输架构存在隐患，勘探开发网、生产控制网、销售服务网之间的数据交互若缺乏严格的访问控制策略，易形成风险传播通道。云平台虚拟化技术的应用也带来新脆弱性，虚拟机之间的资源隔离不足可能导致漏洞跨实例传播。

3 油气企业信息化安全防护体系的总体框架构建

油气企业信息化安全防护体系构建要立足行业特性，以“技术+管理+人员”为核心，形成全业务、全流程纵深防御。需结合数字化转型战略，解决当下风险并预留升级空间。打破场景壁垒，协同联动安全策略，遵循系统化思维，从三维度推进，保障全业务计算安全。

3.1 体系构建的指导思想与核心原则

体系构建以“安全赋能业务，防护保障发展”为指导思想，坚持安全与业务同规划、同建设、同运营，将安全理念贯穿计算场景建设全生命周期。核心原则包括四大方面：一是纵深防御原则，构建“边界防护-网络防护-主机防护-数据防护”多层防线，避免单一防护点失效导致整体风险；二是场景适配原则，针对勘探开发高性能计算、生产运营实时控制等不同场景，制定差异化防护策略，如生产网采用“白名单”访问控制，销售网强化交易加密；三是动态适配原则，建立风险动态监测机制，根据攻击手段、系统架构变化及时调整防护策略，定期开展安全评估与体系优化；四是合规性原则，严格遵循能源行业网络安全标准与国家法律法规，确保防护措施满足等级保护、数据安全等合规要求，实现安全与合规的有机统一[3]。

3.2 体系总体架构设计

体系总体架构采用“五横三纵”立体架构，五横分别为物理环境层、网络通信层、计算平台层、数据安全层、业务应用层，形成从底层基础到上层应用的全栈防护。物理环境层聚焦数据中心、井口机房等关键场所的门禁、监控、防雷击防护；网络通信层部署防火墙、入侵检测系统，实现跨网数据传输加密与访问控制；计算平台层针对云服务器、工业控制主机等实施漏洞扫描与病毒防护；数据安全层建立分级分类管控体系，实现数据加密、备份恢复与脱敏处理；业务应用层嵌入安全审计模块，对应用操作进行全流程记录。三纵分别为安全管理体系、技术支撑体系、应急响应体系，贯穿五横各层，其中安全管理体系明确岗位职责与流程规范，技术支撑体系提供工具平台与技术保障，应急响应体系实现风险事件快速处置，形成横向覆盖、纵向贯通的防护架构。

3.3 体系的核心功能模块

体系核心功能模块包括五大关键模块，协同实现安全防护的全流程管控。风险智能监测模块是核心枢纽，整合网络流量分析、主机行为监控、数据操作审计等多源数据，通过人工智能算法实现异常行为实时识别与风险预警，为精准防护提供依据。边界安全防护模块部署下一代防火墙、网闸等设备，实现生产网与互联网、各业务子网之间的刚性隔离，对出入网数据进行深度检测，拦截恶意代码与攻击行为。数据全生命周期防护模块覆盖数据采集、传输、存储、使用、销毁各环节，采用国密算法进行数据加密，建立异地容灾备份中心，对敏感数据实施动态脱敏，确保数据安全可控。安全运维管理模块建立自动化运维平台，实现漏洞扫描、补丁分发、配置管理的自动化处理，同时规范运维人员操作流程，避免人为失误引发风险。应急响应处置模块制定场景化应急预案，建立应急演练机制，配备专业处置团队，实现风险事件的快速响应、溯源分析与恢复重建。

4 信息化安全防护体系的具体构建路径

信息化安全防护体系构建遵循“技术筑基、管理提效、人员赋能”路径，分阶段推进。要结合业务实际，先解决关键场景风险，再扩展至全链条。技术实现设备联动，管理规范全流程，人员打造复合队伍。三条路径相互支撑，形成闭环，保障防护体系落地见效。

4.1 技术架构构建：实现多场景安全防护的智能联动

技术架构构建以“智能联动、精准防护”为核心目标，致力于打造一个一体化安全技术平台，为油气企业的多场景安全防护提供坚实支撑。首先搭建统一安全管

理中心，它如同整个安全体系的“大脑”，将各场景分散的防护设备数据进行全面整合。通过集中展示风险态势，让管理人员对整体安全状况一目了然；同时实现策略统一下发，避免不同设备因策略不一致而出现防护漏洞，有效解决传统防护设备“各自为战”的弊端。针对勘探开发高性能计算场景，部署高性能入侵防御系统，并优化计算节点间数据传输加密方案，确保大规模并行计算在安全高效的环境下进行。在生产运营控制场景，采用工业防火墙与安全PLC设备，实现控制指令的完整性校验与异常拦截，利用边缘计算节点减少对云端的依赖，提升实时防护能力。建立跨场景数据安全网关，对勘探数据向生产系统、生产数据向销售系统传输进行严格的安全校验与权限管控。引入人工智能与机器学习技术，训练针对油气行业的攻击行为模型，实现攻击行为的精准识别与自动化拦截，通过技术架构的智能联动，全面提升多场景协同防护能力。

4.2 管理机制构建：实现安全防护的全流程规范

管理机制构建旨在形成一套覆盖“事前预防、事中管控、事后追溯”的全流程规范体系，为油气企业的安全防护提供全方位保障。在事前预防阶段，建立安全规划与准入机制至关重要。在新计算系统建设前，开展全面的安全评估，明确安全建设要求，对接入系统的终端、设备实施严格准入认证，未达到安全标准的坚决禁止接入，从源头上杜绝安全隐患。事中管控阶段，制定场景化安全管理制度。勘探开发场景重点规范数据采集与存储管理，确保数据的完整性和保密性；生产运营场景强化操作权限审批与流程管控，防止违规操作；销售服务场景完善交易安全与客户信息保护规范，保障客户权益。建立定期安全检查机制，每月开展漏洞扫描，每季度进行渗透测试，及时发现并修复管理与技术漏洞。事后追溯阶段，建立安全审计与责任追究机制，对所有安全事件进行溯源分析，明确责任主体，形成事件处理报告并整改优化。同时建立安全绩效考评体系，将安全职责履行情况纳入员工绩效考核，提升全员管理执行力度。

4.3 人员能力建设：打造复合型安全人才队伍

人员能力建设需要构建一个“分层培养、精准赋能”的人才培养体系，打造一支兼具油气业务知识与安全技术能力的复合型队伍。针对管理层，开展安全战略与合规培训，使其深入了解行业安全趋势与法规要求，提升安全决策的科学性和前瞻性。通过培训，管理层能够站在战略高度，制定符合企业发展的安全规划和策略。针对技术人员，实施场景化专项培训。勘探开发技术人员重点培训数据加密与高性能计算安全技术，使其能够保障勘探开发过程中数据的安全传输和存储；生产运营技术人员强化工业控制安全与应急处置能力，通过实操演练提升漏洞修复与攻击防御技能，确保生产运营的稳定性和安全性[4]。建立内部安全人才认证体系，设立安全工程师、应急处置专员等岗位认证，激励员工提升专业能力。同时加强外部合作，与高校、安全企业共建人才培养基地，引入外部专家开展专题讲座，让员工了解行业前沿技术与攻击手段。建立安全人才激励机制，对在安全防护工作中表现突出的个人与团队给予表彰奖励，形成“培养-认证-激励”的人才建设闭环，为企业安全防护提供坚实的人才保障。

结束语

油气企业计算场景的信息化安全防护是一项长期且复杂的系统工程。本文构建的防护体系框架与具体路径，从技术、管理、人员三方面着手，为油气企业应对计算场景下的安全挑战提供了全面且可行的方案。未来，随着技术的持续发展与业务模式的不断创新，油气企业需不断优化和完善安全防护体系，以适应新形势下的安全需求，确保企业安全稳定运营与可持续发展。

参考文献

[1]魏娜.数字信息化背景下的油气预防泄露体系建设探析[J].科学与信息化,2019(16):84,87.

[2]李文.油气生产物联网信息化建设研究[J].石化技术,2025,32(9):277-279.

[3]黄寰宇.智能油田建设:信息化技术在油气生产管理中的应用与优化[J].信息系统工程,2025(2):97-100.

[4]杨爱敏,宋合志,张宪金.液化石油气用户侧信息化管理探索[J].现代职业安全,2025(1):29-31.