

超融合架构下制药核心机房信息安全运维模型构建

王风格

山东永聚医药科技股份有限公司 山东 淄博 255400

摘 要：针对制药行业超融合核心机房运维架构冲突、合规管控薄弱、数据安全风险突出、应急运维滞后等行业痛点，结合GMP及国家数据安全法规要求，识别基础设施、虚拟化、业务数据、运维管理四层安全风险，搭建五层闭环安全运维模型，配套分级权限、标准化运维流程落地优化。实证表明，该模型可压缩故障修复时长、筑牢涉密数据防护屏障，全面提升机房运维效率与GMP合规通过率，为制药企业超融合机房合规安全运维提供标准化落地参考。

关键词：超融合架构下；制药核心机房；信息安全运维；模型构建

引言：制药行业数字化转型提速，超融合架构广泛应用于承载MES、LIMS等核心业务的制药核心机房，兼顾资源弹性调度与集约化运维需求。但行业兼具严苛法规约束与生产零中断刚需，传统分立运维模式难以适配虚拟化资源池化特性，滋生数据篡改、越权访问、审计缺失、业务宕机多重风险。立足制药行业合规与生产双重需求，本文剖析运维现存问题与风险，构建专项安全运维模型，破解架构适配、安全管控、合规审计多重行业难题。

1 相关概念界定与行业运维现状及风险分析

1.1 核心相关概念界定

（1）超融合架构核心内涵：将计算、存储、网络资源深度融合，通过虚拟化技术构建统一资源池，依托分布式集群实现横向扩展与高可用，具备弹性调度、线性扩展、故障自愈等核心特征^[1]。（2）制药核心机房界定：专指承载药品生产MES、质量控制LIMS、研发ERP、全流程追溯系统等关键业务的生产级数据中心，其运行状态直接决定药品合规性与生产连续性。（3）制药行业信息安全运维定义：在满足GMP等法规框架下，以“合规化操作、全过程可审计、业务零中断”为专属目标，保障超融合环境下数据保密性、完整性及可用性的运维体系。

1.2 制药核心机房架构与运维合规要求

（1）制药企业超融合机房部署架构：通常采用多节点集群部署，软硬件一体化交付，通过统一管理平台实现虚拟计算、分布式存储及SDN网络资源的集约化布局。（2）国家医药行业数据安全法律法规：需遵循《药品管理法》《数据安全法》《个人信息保护法》，以及药监局关于药品追溯、临床试验数据管理的专项规定。

（3）GMP等专项合规标准：GMP明确要求生产数据真实、完整、可溯源；运维日志需满足审计追踪功能，包

括操作记录、参数变更、异常告警等日志至少保存至药品有效期后一年。

1.3 当前制药超融合机房安全运维现存问题

（1）运维架构问题：传统按设备分立的运维模式与超融合资源池化、动态调度的特性冲突，导致故障定位难、责任边界模糊。（2）安全管控问题：虚拟化层与数据层边界动态变化，缺乏针对制药涉密数据（如配方、工艺参数）的有效隔离与防泄漏手段。（3）人员与流程问题：运维人员同时缺乏超融合架构和GMP合规知识，跨平台排障能力不足；合规操作流程未标准化，变更管理随意。（4）应急运维问题：生产业务停机时缺乏针对超融合环境的快速恢复预案，应急处置机制不完善，易造成批次数据丢失或生产中断。

1.4 超融合下制药机房信息安全运维风险识别

（1）基础设施层风险：服务器节点、分布式存储硬盘等硬件故障可能引发集群性能降级或数据重构失败风险。（2）虚拟化平台层风险：虚拟机逃逸、资源访问控制越权等漏洞可导致跨租户或跨业务的数据泄露。（3）业务数据层风险：MES/LIMS中的生产批记录、质控数据面临被篡改、勒索加密或误删除泄露风险。（4）运维管理层风险：运维人员违规操作（如越权查询数据库）、运维日志未开启或审计缺失，违反GMP追溯要求。

2 超融合架构下制药核心机房信息安全运维模型构建

2.1 运维模型构建原则与总体目标

（1）构建原则：坚持合规优先，以GMP、数据安全法等为底线；业务连续性，确保MES、LIMS等零中断；分层闭环，实现“监测-研判-处置-审计”完整闭环；轻量化运维，避免过度采集对超融合造成额外负载。（2）总体目标：系统性规避超融合虚拟化安全与资源池化冲突；全面满足药企生产、数据溯源、审计追踪等合规要求；显著降低硬件故障、人为误操作、配置偏差导致

的故障率；实现生产、办公、研发区超融合资源统一管控。（3）边界界定：聚焦核心机房超融合集群，适配药品生产区（MES、SCADA）、质量控制区（LIMS）、研发区（ERP、PDM）、追溯系统（TTS）等全域业务场景，不涵盖公有云或跨广域网混合云。

2.2 运维模型整体架构设计

（1）五层架构：自下而上为物理基础设施层（服务器、存储、网络）、虚拟化平台层（计算虚拟化、分布式存储、SDN网络）、制药业务应用层（MES/LIMS/ERP等）、安全运维管控层（监测、防护、自动化运维）、合规审计管理层（日志审计、权限追溯、GMP报告）。各层通过标准化API与日志接口联动。（2）五大核心模块：风险监测模块（资源占用、异常流量、越权行为）、自动化运维模块（批量配置、健康巡检、故障自愈）、安全防护模块（虚拟防火墙、数据加密、防泄漏）、合规溯源模块（操作留痕、审计日志、合规报告）、应急处置模块（预案触发、业务迁移、快照恢复）^[2]。（3）运行逻辑：闭环流程包括多源数据采集（Agent及无代理方式）→风险研判（规则库与基线对比）→运维执行（隔离、修复、告警）→日志留存与审计标签→合规复盘与改进建议，实现持续优化。

2.3 模型核心子模块细化设计

（1）超融合资源全域监测运维子模块：实现对CPU、内存、存储IOPS、网络带宽等算力指标的秒级监控；统一纳管虚拟节点、容器节点及分布式存储池；设计资源水位预警与动态弹性伸缩策略，避免单点过载。

（2）制药涉密数据分级安全运维子模块：依据药品工艺配方、研发数据、质控批记录等敏感等级，划分L1-L3三级数据域；实施分级加密存储与访问控制；设计定期备份与异地容灾运维流程，备份周期与GMP数据保存要求对齐。（3）合规化运维审计子模块：完全贴合GMP附录《计算机化系统》要求，对所有运维操作（登录、配置变更、数据导出、权限授予）进行不可篡改的审计日志记录；引入双人复核机制与操作时间戳；对敏感操作实现即时告警与阻断。

（4）自动化故障自愈运维子模块：针对超融合节点宕机、虚拟化平台无响应、业务进程假死等典型故障，设计自动故障迁移、心跳检测重启、快照回滚等自愈动作；自愈过程全程记录并纳入合规审计范围，确保生产业务中断时间控制在分钟级。

2.4 模型运维权限与流程体系搭建

（1）运维人员分级权限划分：设置四类角色——管理员（负责集群全局配置与策略下发）、运维专员（执行日常巡检、备份、补丁升级）、审计员（独立审查审

计日志、生成合规报告）、药企业务岗（仅可查看自身业务状态，无权操作）。角色间权限严格隔离，遵循最小必要原则^[3]。（2）日常标准化运维作业流程制定：制定涵盖每日巡检、每周备份验证、每月合规自检、每季度应急演练的标准化流程。每项作业均要求填写电子工单，经审批后方可执行，完成后自动触发审计日志封存。（3）违规运维拦截与权限溯源流程设计：在运维操作入口嵌入实时行为分析引擎，对越权指令、高危命令（如rm、format、虚拟机删除）进行实时拦截并二次认证。所有操作均绑定唯一身份标识，支持全链路溯源至具体人员、时间、会话及受影响资源。

3 超融合架构下制药核心机房信息安全运维模型落地实施、效果优化与结论展望

3.1 运维模型落地实施策略

（1）药企机房软硬件适配改造方案：完成超融合平台北向API接口对接，支持vSAN、Nutanix、SmartX等主流平台的数据采集与策略下发；部署轻量级安全运维工具集，包括虚拟化防火墙、日志审计一体机、数据库安全防护（防水坝）及统一监控告警平台；原有分立式监控系统逐步下线，避免资源争用。（2）运维团队专业化能力重构：制定超融合架构与GMP合规双维度专项培训计划，涵盖虚拟机迁移、分布式存储排障、审计追踪配置、数据备份恢复等实操课程；设立合规运维专员岗，负责日志审查、整改跟踪及迎检支持；每季度组织跨架构应急演练，提升团队综合能力。（3）分阶段落地实施步骤：第一阶段，选取研发测试集群开展试点部署，验证模型接口兼容性与监测精度，运行2周；第二阶段，扩展至生产MES、LIMS及追溯系统全域上线，采用旁路监控模式运行两周，确认无业务影响；第三阶段，正式切换权限管控、审计闭环及自愈策略，启动流程试运行，持续优化基线策略，周期为1个月^[4]。

3.2 模型运行效果评价与实证分析

（1）评价指标体系构建：构建四类核心指标——安全风险指标（越权操作次数、数据泄露事件数、高危命令拦截率）、运维效率指标（平均故障修复时间MTTR、日常巡检耗时、自动化自愈成功率）、合规达标指标（审计日志完整率、GMP检查项通过率、日志保存合规率）、业务稳定指标（生产业务连续运行时长、计划外宕机次数、RTO达成率）。（2）案例实证：选取某中型化学制药企业，其核心机房部署4节点超融合集群，承载MES、LIMS、ERP及追溯系统。在确保生产业务不中断的前提下，按4.1策略完成模型全模块部署，持续运行三个完整生产周期（约90天），采集全量运维数据。（3）

运行结果对比：与传统分立运维模式相比，越权操作事件由月均5.3次降至0.7次，高危命令拦截率达100%；审计日志完整率从72%提升至100%，满足GMP审计追踪及数据完整性要求；平均故障修复时间（MTTR）由4.2小时缩短至0.8小时，虚拟机卡死、存储慢盘等自动化自愈成功率达82%；计划外业务中断次数由每季度2次降为0次；GMP合规检查一次性通过率提升40%。

3.3 模型现存短板与优化改进策略

（1）模型运行现存短板：海量研发数据（如试验批次记录、色谱图文件）持续高并发写入，导致分布式存储IOPS消耗过大，监测模块响应延迟增加；极端故障场景（如双节点同时宕机、元数据损坏）自愈能力不足，仍需人工介入恢复；部分老旧超融合版本API接口不全，影响自动化执行效率。（2）技术优化：引入AI智能预警引擎，基于历史运维日志与实时指标（存储延迟、IOPS、CPUstealtime）训练异常检测模型，对性能衰减、非法访问趋势实现提前15分钟预判，优化风险研判准确性；开发自动化补丁与配置漂移修复脚本，减少人工介入。（3）管理优化：紧跟新版《药品记录与数据管理要求（试行）》及GMP附录《计算机化系统》修订要求，每季度迭代审计日志字段、报告模板与保留策略；建立跨部门合规联席会议机制，将运维审计结果纳入药企年度质量回顾分析；完善极端故障场景手动恢复SOP^[5]。

3.4 研究结论与未来展望

（1）研究结论：本模型系统解决了超融合架构下制药核心机房“运维架构冲突、合规审计缺失、应急响应薄弱”三大行业痛点，实现了资源池化弹性与GMP全流程可追溯的有机统一，为制药企业提供了可落地、可复制的安全运维范式。（2）研究不足：实证案例仅

覆盖中型化学制药企业，样本单一；对无菌生物制剂、细胞治疗等特殊生产场景的适配性尚未验证；小型药企因IT投入有限，模型轻量化程度有待提升；极端故障自愈能力仍需增强。（3）未来展望：结合云原生技术（Kubernetes、服务网格）重构监测与自愈模块，支持容器化运维及弹性伸缩；引入零信任架构，实现细粒度动态访问控制与持续信任评估；进一步适配制药工业互联网场景下的跨机房协同、边缘节点运维及工业安全态势感知平台。

结束语

本文完成制药超融合机房安全运维模型搭建与落地验证，有效化解架构适配、合规运维、应急处置核心痛点，兼顾业务连续性与药监合规双重需求。研究存在样本范围有限、特殊药企场景适配不足、极端故障自愈能力薄弱等缺陷。后续将依托云原生、零信任、AI预警技术优化模型，补齐运维短板，拓宽行业适配场景，贴合最新药监法规迭代体系，打造适配多类型药企、高容错的智能化合规运维体系。

参考文献

- [1]董泽宇,刘鑫.超融合数据中心内生安全运维模型构建与风险防控[J].计算机工程与应用,2025,61(8):231-238.
- [2]陈俊.制药企业核心机房超融合架构部署及信息安全合规运维研究[J].医药工程设计,2024,45(5):56-61.
- [3]赵睿.面向GMP合规的医药行业机房信息安全运维体系优化设计[J].网络安全技术与应用,2024(7):142-144.
- [4]周思远.超融合架构下机房虚拟化安全隐患与闭环运维模型搭建[J].信息技术,2023,47(11):78-83.
- [5]吴海波.医药企业核心业务数据中心超融合安全架构改造实践[J].自动化技术与应用,2023,42(3):167-170.