# 安可替代产品在涉密网络环境下的管理优化研究

赵鞠萌 [1] 黄山 [2] 朱允超 [3] 于大川 [1] 黄缨涵 [1]
1 吉林省经济信息中心，吉林 长春 130000；
2 白城市产品质量检验所，吉林 白城 137000；3 长春嘉诚信息技术股份有限公司，吉林 长春 130000

**摘要**：随着信息化建设的深入推进，涉密网络环境对安全可靠的要求愈发严苛。安可替代战略在确保涉密网络安全方面发挥了关键作用，但在实际管理中，安可替代产品的应用仍面临技术适配性、管理效率和安全保障等多重挑战。本文结合涉密网络的特殊性，探讨安可替代产品在这一环境中的管理优化策略，以期为我国信息安全建设提供参考。

**关键词**：安可替代产品；涉密网络环境；管理；优化

## Research on Management Optimization of Encore Substitute Products in Secret Network Environment

**Zhao,Jumeng[1] Huang,Shan[2] Zhu,Yunchao[3] Yu,Dachuan[1] Huang,Yinghan[1]**
**1Jilin Provincial Economic Information Center, Changchun, Jilin, 130000, China**
**2Baicheng Product Quality Inspection Institute, Baicheng, Jilin, 137000, China**
**3Changchun Jiacheng Information Technology Co., Ltd, Changchun, Jilin, 130000, China**

**Abstract:** With the deepening of information construction, the requirements for security and reliability in classified network environment are becoming more and more stringent. The alternative strategy of encore has played a key role in ensuring the security of classified networks, but in actual management, the application of encore alternative products still faces multiple challenges such as technical adaptability, management efficiency and security guarantee. Based on the particularity of classified network, this paper discusses the management optimization strategy of encore alternative products in this environment, in order to provide reference for information security construction in China.

**Keywords:** Encore alternative products; Confidential network environment; Management; Optimize
DOI: 10.62639/sspis34.20250202

近年来，全球信息技术格局深刻变化，信息安全的重要性日益凸显。涉密网络作为国家安全的核心关键信息基础设施，其运行环境的安全性直接影响国家利益。安可替代产品以自主可控、安全可靠为核心理念，已成为涉密网络建设的中坚力量。然而，替代过程中，涉密网络管理的复杂性和高敏感性对安可产品的应用和优化提出了更高要求。如何在保证安全可靠的同时，实现管理的高效性与灵活性，是当下亟待解决的问题。

## 一、涉密网络环境对安可替代产品的特殊要求

涉密网络具有高度敏感性和严苛的技术要求，其对安可替代产品的需求不仅局限于功能层面，更体现在以下几个方面：

（一）绝对安全性：涉密网络的安全防护要求超出一般关键信息基础设施，需要安可产品在网络协议、数据存储和系统隔离等方面提供全面保障[1]。

（二）环境适配性：涉密网络使用场景多样且复杂，要求安可产品具有较高的技术适配性，能够无缝替代国外同类产品。

（三）自主可控性：要求产品的核心技术完全自主研发，确保在紧急情况下不受外部控制或威胁。

（四）管理可操作性：涉密网络管理通常涉及多层次、多部门的协调，需要安可产品具备易操作、易维护的特点。

## 二、安可替代产品在涉密网络管理中的现状与问题

在实际应用中，安可替代产品为涉密网络提供了坚实的安全保障，但也暴露出以下不足：

（一）技术适配与整合难题

安可替代产品虽然在涉密网络中担负起保障安全的重任，但其技术适配性和整合能力仍面临不少问题。部分产品在性能指标上，特别是数据处理效率和硬件兼容性方面，距离国外同类产品尚有差距，这一问题的根源在于基础技术积累的薄弱和生态体系的完善程度不足[2]。一些产品在面对复杂的硬件环境时，可能无法实现顺畅的兼

（稿件编号：IS-25-2-1039）

作者简介：赵鞠萌（1974-），男，汉，籍贯：吉林长春，硕士研究生，高级工程师，研究方向：网络管理，信息安全。
黄山（1992-），男，汉，吉林白城，本科，助理工程师，研究方向：软件工程。
朱允超（1989-），男，汉，吉林长春，本科，无，研究方向：计算机科学与技术、软件工程。
于大川（1986-），男，满，辽宁丹东，本科，管理八级，研究方向：信息安全。
黄缨涵（1998-），女，汉，吉林松原，本科，管理九级，研究方向：网络管理。

容或会出现性能瓶颈，使得实际部署过程中，技术整合难度明显增加。同时，不同产品之间标准不统一，进一步加剧了系统整合的复杂性。

（二）管理工具的缺乏

涉密网络的运行管理本身具有高精细化的特点，需要依赖全面、强大的工具体系。然而，目前部分安可替代产品在管理功能开发上相对滞后，导致实际操作中的效率较低。具体表现为，管理平台往往无法很好地整合监控、运维和安全策略配置功能，管理人员在使用时需要切换多个系统，既增加了操作复杂性，也容易形成安全隐患。此外，缺乏智能化的管理工具，也导致日常运维更多依赖于人力，大大降低了工作效率。更令人担忧的是，这种工具上的欠缺可能在关键时刻拖慢应急响应速度，从而放大潜在的安全风险 [3]。

（三）人才与运维不足

安可替代产品的技术路线相对独特，使用这些产品需要运维人员具备较高的专业水平。然而，当前专门针对安可产品的培训资源仍然不足，导致实际工作中合格人才的储备与需求之间存在较大差距，进而限制了安可产品的推广速度，也在一定程度上削弱了产品本身的应用价值。特别是在涉密网络环境中，操作的复杂性和任务的紧迫性都要求运维人员能够迅速上手并熟练使用产品。如果缺乏系统化的培训和长期的人才储备计划，现有的运维团队很可能难以胜任日益复杂的管理需求。

（四）安全策略的一体化欠缺

涉密网络的安全需求往往涉及多层次、多维度的保护，而部分安可替代产品在安全策略设计上缺乏系统性思考。当前的许多产品更多关注某一单一领域的安全保障，却未能很好地适配复杂的涉密网络需求，导致防护水平参差不齐。在访问控制、数据传输加密以及网络攻击防护之间，可能缺少有效的联动机制，最终形成安全上的“断点”，从而使得整体网络防护体系显得不够连贯，无法充分抵御多维度的安全威胁。

## 三、安可替代产品在涉密网络管理中的优化策略

针对上述问题，本文提出以下优化策略：

（一）加强产品性能优化与技术适配

在安可替代产品的优化与适配中，产品性能的提升和技术契合度始终是关键议题，而核心技术研发无疑是推动整体进步的动力引擎。优质算法的开发与硬件兼容性的提升，直接决定其在涉密网络环境中的实际表现 [4]。现阶段，企业需要更高强度地聚焦于基础算法的优化，以解决数据处理效率低、资源消耗过高等痛点。可以引入更加智能的压缩算法与轻量级加密技术，减少存储与计算的开销，从而大幅提升系统运行效率。同时，硬件兼容性的问题也不容忽视，涉密网络环境的多样性要求产品在广泛硬件平台上实现稳定运行，避免出现因硬件型号差异导致的功能不匹配。为此，研发过程中需建立多样化测试场景库，将产品置于不同硬件条件中进行严苛测试，以反复校验其性能表现是否达到预期。

安可产品的设计应更贴近涉密网络的复杂应用场景，单纯的技术优越性往往难以满足多样化需求。深入调研用户使用习惯，理解具体场景下的功能侧重，是研发定制化解决方案的基础。在信息高密度交互的环境中，可以为产品添加动态负载均衡功能，以避免资源分配不均导致的系统卡顿；在高风险任务场景中，可以引入细粒度权限管理模块，最大程度防范人为操作失误带来的安全隐患。此外，性能提升的同时，产品的稳定性与可靠性不能被忽略。用户使用时希望系统能够长时间稳定运行而不间断，这就要求研发团队从底层架构设计开始注重冗余机制的构建，例如通过双机热备、分布式存储等技术手段，提升抗故障能力和数据恢复效率。更重要的是，定期进行模拟故障测试，排查潜在风险隐患，才能在实战中从容应对突发事件 [5]。因此，安可产品的性能优化不仅是一项技术性任务，更是需要关注用户体验的系统性工程。

（二）构建高效的管理工具体系

在涉密网络环境中构建高效的管理工具体系是一项系统性工程，既要满足复杂环境的多样化需求，又需保障操作简便与管理效率。开发专属管理平台成为突破管理瓶颈的关键路径。针对涉密网络中安可替代产品的多元化特点，这一平台应具备高度的集成能力，将监控、运维以及安全策略配置等功能无缝融合在一个统一的界面之下，监控模块可以实时呈现网络运行状态，运维模块提供设备健康状况分析，而安全策略模块则支持快速配置访问权限与防护规则。这样一来，管理人员在面临复杂场景时，可以依赖统一平台快速响应，避免因多系统切换带来的管理盲区或效率损失。

同时，涉密网络管理需要迈向智能化，以减轻传统运维中依赖人工操作的负担。引入人工智能技术可以成为提升工具体系效能的重要助力。在故障诊断中，AI 算法能够通过分析历史数据和实时运行数据，精准定位潜在问题，并给出具体的优化建议。对于日志审查、资源分配或系统补丁更新等常见的运维任务，智能化管理工具可以根据既定规则自动执行操作，既降低人为操作错误的风险，也大幅减少重复劳动所耗费的时间。此外，AI 驱动的预测功能还能够根据系统运行状态的变化，提前预警可能发生的故障，从而为管理人员争取宝贵的应对时间。在平台的实际设计上，应充分考虑用户的操作习惯与涉密网络的特殊性，例如设置个性化的可视化界面，方便管理人员直观掌握全局动态；优化人机交互设计，使得任务调度与信息查询过程更加便捷流畅。只有将精细化管理和智能化技术完美结合，才能真正赋能涉密网络的安全与效率升级。

（三）加大人才培养力度

人才培养是推动安可替代产品在涉密网络中广泛应用的基石。面对日益复杂的网络环境与快速迭代的技术更新，单靠现有的运维人员储备显然难以支撑系统的长效稳定运行。因此，建立覆盖全国的培训网络显得尤为紧迫。该网络应以标准化和系统化为核心，涵盖基础理论、操作实践以及风险应对等多层次内容。可以设置分级课程

体系，针对新手的基础运维技能培训，以及为高级技术人员提供的深度问题解决和优化能力提升课程。培训的形式需要灵活多样，既包括集中授课，又囊括线上教学平台的构建，以适应不同地区和岗位的人员需求。同时，还可以引入虚拟仿真技术，搭建模拟涉密网络环境，让学员在真实情境中学习应对潜在挑战，强化实践能力。

高校与科研机构在人才培养中扮演着不可替代的角色。将安可产品技术与应用纳入高等教育课程体系，是从根本上扩充专业人才储备的有效举措。一方面，可以在计算机科学与信息安全等相关专业中开设专门课程，使学生在理论学习阶段就能接触国产替代产品的核心技术与实际案例，缩短毕业后适应工作的时间；另一方面，可以通过产学研合作，联合企业开发课程或开展项目研究，使课程内容更贴合实际需求。还可以探索设立专项实验室或实训基地，鼓励学生动手实践甚至参与技术创新。与此同时，激励措施也需同步跟上，例如设立奖学金、提供就业推荐等方式，吸引更多学生投身这一领域。人才培养不仅是一项长远战略，更需要脚踏实地地结合当前实际需求，构建从理论到实践、从初级到高阶的全面体系，为涉密网络安全管理的未来积蓄强大的后备力量。

（四）完善安全策略的一体化设计

完善安全策略的一体化设计是构建涉密网络安全防护体系的关键环节，要求在政策引导与技术落地之间找到平衡点，使安可产品能够从硬件到底层软件，从网络架构到用户终端实现无缝覆盖。一体化设计需要跳出传统的孤立防护思维，转而强调系统的整体协同效应。在硬件层面，部署具有自主知识产权的国产化服务器和存储设备，以减少硬件层面的潜在风险；在软件层面，加强对操作系统、数据库和中间件的适配与优化，形成从底层到应用的全链条国产化保障。在具体实践中，推动行业标准的统一显得尤为重要，这样既能为开发和采购提供明确的技术规范，又能促进不同安可产品间的无缝对接，从而避免因兼容性问题导致的管理漏洞。

与此同时，引入零信任架构是实现动态化安全防护的重要手段。零信任理念的核心在于摒弃“边界即安全”的传统观念，强调对每一次访问进行严格验证，无论用户或设备位于网络内部还是外部。在设计零信任架构时，可以从身份验证和访问控制两方面入手。建议采用多因素验证机制，不仅限制单一凭据的失效风险，还能在用户行为异常时触发进一步的安全措施；对资源访问权限进行细粒度划分，确保每个用户只能触及与其职责相关的最小数据集，减少因权限滥用引发的隐患。此外，还可以引入动态信任评估机制，基于实时分析调整访问权限，例如当用户行为偏离常规模式时自动触发风险预警或隔离操作。零信任架构的应用需要与涉密网络的具体需求深度结合，同时保持政策支持和技术创新的双轮驱动，为构建安全、可靠、动态的一体化防护体系注入持续动力。

（五）推动生态协同与产业升级

推动生态协同与产业升级是安可替代战略发展的重要方向，其核心在于促进多方合作与资源整合，使技术创新与产业链发展能够齐头并进。当前，安可产品制造商、涉密网络管理单位以及科研机构各自掌握不同的核心资源，但孤立的研发与应用方式容易导致技术割裂和资源浪费。建立协作机制，让这三方形成密切互动的技术闭环，是实现整体升级的关键步骤。制造商可以将市场反馈与应用难点带回研发环节，科研机构则能够利用实验室优势为新技术提供理论支撑，而涉密网络管理单位则可以在实际应用场景中测试产品性能，实现技术从研发到落地的完整循环。在具体操作中，可以组织跨领域的联合攻关项目，搭建技术分享平台，让不同主体之间的知识流动更加顺畅，同时设立专项基金支持具有协作性质的研究与开发工作。

国产化信创生态圈的建设为产业升级提供了强有力的基础，推动产品与服务的深度融合是当前的重要任务。信创生态圈的优势在于其具备系统性和包容性，能够将安可产品与上下游服务商、解决方案提供者联合起来，形成涵盖硬件、软件、运维和支持服务的综合技术支撑体系。为了强化这种融合，可以制定统一的生态标准，让各类产品在技术规范上实现互联互通，提升整体协同效应。与此同时，鼓励在信创生态圈内开展试点示范工程，通过真实场景的实践检验产品与服务的融合度，并不断优化生态圈内部的资源配置。在涉密网络中部署一整套以安可产品为核心的解决方案，涵盖服务器、存储、操作系统、数据库以及安全管理平台，充分发挥国产化产业链的整体优势。

## 四、结语

安可替代产品在涉密网络中的应用，是我国信息安全建设不可或缺的重要组成部分。性能的持续提升、管理工具的优化升级、专业人才的培养以及安全策略的深入完善，共同推动着安可产品在这一领域发挥更大的潜力。这些努力为涉密网络的高效运行和安全防护奠定了坚实的基础。展望未来，随着技术的发展日新月异，以及产业生态的日益健全，安可替代产品将在涉密网络的实践中展现更深远的价值，为推动我国信息技术的自主创新和安全保障提供更加有力的支撑。

**参考文献：**

[1] 冉文学，郑翰雯．考虑消费者偏好和可替代产品的供应链绿色开发投资与协调策略 [J]．供应链管理，2024，5 (01)：31-43.
[2] 王永健，陈伟达，王站杰，卞家涛．基于现金流管理的单向可替代产品制造 / 再制造生产决策研究 [J]．工业工程与管理，2020，25 (01)：87-94.
[3] 陈克兵，孔颖琪，雷东．考虑消费者偏好及渠道权力的可替代产品供应链的定价和绿色投入决策 [J]．中国管理科学，2023，31 (05)：1-10.
[4] 高峻峻，袁君霞．基于需求学习的可替代服装产品动态库存与定价联合决策模型 [J]．上海大学学报 ( 自然科学版 )，2019，25 (06)：1023-1033.
[5] 菲亚特动力科技进一步扩展欧 V 产品组合 展示可替代燃料动力产品 [J]．工程机械文摘，2019，(03)：22-23.