鸿蒙赋能：无人机低空经济内生安全协同系统研究

曾许航
四川水利职业技术学院　四川　成都　611230

摘　要：低空经济的迅猛发展驱动无人机应用实现规模化扩张，但随之而来的地理信息安全风险与管控困境也逐渐凸显，成为制约行业规范化发展的关键瓶颈。传统无人机作业体系因数据分散存储、管控机制缺失等问题，难以满足规模化运营下的安全合规要求。本研究提出融合华为HarmonyOS分布式技术与小艺智能交互能力的无人机协同定位及任务赋能方案。该方案依托HarmonyOS分布式软总线、硬件互助及内生安全核心特性，构建覆盖地理信息数据采集、处理、流转全生命周期的安全防护体系，同时借助自然语言交互与跨设备协同技术提升作业效能。研究表明，该协同系统可为低空经济地理信息安全保障提供有效技术支撑，兼具重要的理论探索价值与实践应用前景。

关键词：HarmonyOS；低空经济；地理信息安全；无人机；协同定位

引言

低空经济作为国家战略性新兴产业，以无人机为核心载体，在物流、城市运维等领域广泛应用，持续产生高精度地理信息数据，兼具战略价值与敏感性。当前系统普遍存在“重功能、轻安全”问题，数据分散存储形成“孤岛”与“管控真空”，依赖终端简易防护和人员自律，缺乏全生命周期统一、强制、可追溯的安全体系，制约行业发展。现有研究聚焦通信链路、单机数据与飞行控制安全，属“被动防护”，存在三大短板：视角局限于单一环节，缺乏系统架构顶层设计；技术难以适配多设备、多部门协同的动态场景；安全与效能失衡，常以效率换安全。为此，本研究基于“架构创新—技术融合—场景落地”逻辑，聚焦三大问题：一是构建兼顾效能与数据“可用不可见、可控可审计”的协同作业系统；二是探讨HarmonyOS作为该系统技术载体的适配性；三是探索破解传统架构安全痛点的实施路径。

1 系统设计的理论基础与安全范式转型

1.1 为何选择HarmonyOS？

传统无人机系统存在安全管控分散、设备难以协同两大核心问题。经过技术验证与对比，本研究最终选择HarmonyOS作为技术底座，因其三大分布式核心能力恰好匹配低空经济需求：（1）分布式软总线：建立通用跨设备通信规则，自动屏蔽底层连接技术差异，为高清影像回传、多机态势共享等场景提供稳定低延时通信，并保障安全指令高效传递[1]。（2）硬件互助与资源池化：将异构设备硬件能力虚拟化，形成“超级终端”。例如，在GPS信号弱区，可调用地面终端的高精度定位模块，弥补单机性能不足，并让安全管控能力在设备间协同部署。（3）原子化服务与一次开发多端部署：将应用功能拆分为独立“元服务”，可灵活部署到不同设备上。安全功能（如加密、审计）可作为独立服务快速适配不同场景，并通过服务隔离确保其可靠性。

1.2 安全管理范式的根本性变革

HarmonyOS的深度整合，推动地理信息安全管理从“事后补救”向“事前预防”转型，其核心差异体现在以下维度：

表1：传统模式与鸿蒙赋能模式地理信息安全管控对比

管控维度	传统模式	鸿蒙赋能模式
数据产生与采集	依赖飞手自觉，事前预防薄弱	预设合规飞行包线，自动加载电子围栏；采集行为全流程审计，形成不可篡改证据链
数据存储与加密	明文存储，加密方案不统一	端侧全量加密，密钥与设备、身份绑定；分布式安全存储，单一设备丢失无法解读数据
数据流转与共享	非受控渠道分享，流向不可追溯	基于属性的动态访问控制（ABAC），策略与数据绑定；原子化服务安全隔离，防范越权访问
数据使用与销毁	人工清理，易遗漏	全生命周期自动化管理，到期自动触发安全擦除；操作全程留痕，满足合规审计

这一转型使安全能力从应用层下沉至系统底层，安全防护逻辑从“依靠人员自觉”转变为“架构内生免疫”，为数据全生命周期安全提供保障。

2 系统架构与核心技术实现

2.1 系统整体架构：内生安全驱动的协同管控体系

系统基于HarmonyOS分布式架构与内生安全特性，构建“交互层–智能中枢层–执行层”三级协同架构。初期采用“安全模块外挂”方式，导致安全与业务脱节、协同效率下降超30%、策略响应滞后等问题。经三次迭代，确立“安全深度嵌入业务流程”原则，最终形成当前架构。其可行性依托HarmonyOS三大能力：统一设备管理、可信运行环境（TEE）构建、分布式服务调度。

2.1.1 交互层：基于原子化服务的智能安全交互

聚焦“安全引导+便捷交互”，利用HarmonyOS原子化服务与小艺语音交互，在用户发出高风险指令（如敏感区飞行）时，自动触发二次确认并推送区域安全等级与合规要求，从源头防范误操作。任务配置可在终端与遥控器间无缝同步，提升效率同时保障安全。

2.1.2 智能中枢层：分布式安全策略与审计核心

作为系统“智慧与安全中枢”，包含两大模块：一是安全策略引擎：动态同步空域法规、地理围栏与行业标准，按场景（如生态监测、城市巡检）自动匹配规则，实现任务前合规检查、作业中实时监控、异常时即时干预；二是审计溯源中枢：基于区块链记录设备接入、数据采集、权限变更等全流程操作，生成不可篡改日志，加密存储于可信节点，支持合规审计与事件追溯。该层还通过鸿蒙分布式软总线调度多设备算力，支撑高负载安全计算。

2.1.3 执行层：可信设备联盟与终端安全基座

由无人机、遥控器、智能终端等组成，所有设备须通过HarmonyOS分布式数字身份完成双向认证，加入“可信设备联盟”，未认证设备无法接入。各终端内置TEE，确保密钥管理、身份认证、数据加密等核心安全功能免受系统漏洞影响[2]。系统实时监测设备安全状态（如是否被Root、注入恶意程序），一旦发现风险，立即注销密钥并隔离设备，筑牢终端防线。

2.2 核心赋能场景：安全与效能协同验证

2.2.1 合规勘察与“出生即安全”的数据脱敏

针对军事区、基础设施周边等敏感区域勘察中的三大痛点——禁飞区误入、数据传输泄露、事后脱敏滞后，系统构建“合规飞行–安全采集–可控流转”闭环。初期在复杂电磁环境下电子围栏同步延迟，后采用“多源冗余校验”（卫星+基站+惯导）解决；数据脱敏由全局模糊优化为“动态分级脱敏”，依区域敏感度与地物类型精准处理，兼顾安全与可用性。作业流程为：用户语音指令触发安全校验→中枢完成合规预检→无人机接收合规飞行包线（底层限飞）→TEE实时加密原始数据+像素级脱敏→脱敏数据用于现场分析，原始数据仅回传可信终端。

2.2.2 跨部门应急救援中的“收放自如”数据共享

传统模式存在设备异构、非受控传输、静态权限三大瓶颈，导致协同低效与数据泄露风险。本系统构建“精准共享–权限可控–全程追溯”机制：指挥员指令（如“向‘闪电救援’单位共享01号无人机画面至20时，禁止下载”）触发中枢通过分布式软总线互联多部门设备，统一数据格式；基于ABAC策略动态分配权限（如医疗看人员位置、消防看地形）；数据经端到端加密传输，所有访问行为上链审计；任务结束自动清除临时副本并生成审计报告。

3 关键技术实现路径与安全保障机制

3.1 基于分布式数字身份的可信设备联盟：筑牢设备接入安全根基

依托HarmonyOS分布式数字身份体系和设备内置硬件安全模块（HSM），为每台设备生成唯一、不可篡改的去中心化标识（DID）。针对多品牌设备HSM接口与加密算法不统一的问题，提出“统一接口封装+算法兼容适配”方案，通过鸿蒙软总线屏蔽硬件差异，兼容RSA、SM2等主流算法。针对低配置终端认证延迟高，引入“轻量化认证优先”策略，区分设备类型实施差异化认证流程。设备接入时提交DID与凭证，由可信根节点验证后动态生成任务密钥用于通信加密，并结合鸿蒙安全状态感知能力实时监测设备是否被越权或植入恶意程序，一旦发现风险立即注销密钥并隔离设备。相比传统固定密钥或密码认证方式，本方案实现三大跃升：①身份认证从“静态授权”升级为“动态可信校验”，防伪造；②设备安全从“被动忽视”转为“主动感知+实时响应”；③通信密钥由“长期固定”变为“临时动态”，限制单点泄露影响范围，显著提升联盟整体抗攻击能力。

3.2 时空标签绑定技术：赋予数据全生命周期“可信身份证”

在数据生成瞬间，基于鸿蒙数据安全服务框架自动嵌入包含“数据DNA+生产者+时间+地点+安全等级”的五元组时空标签。为解决高速采集下标签生成延迟问题，采用“轻量化哈希+局部SHA-256加密”混合方案，效率提升45%；通过“双副本备份+实时校验”机制防止极端环境下标签丢失。标签在可信执行环境（TEE）中生成，确保不可篡改[3]。安全等级依据采集区域属性（如禁飞区、敏感区）自动分级（公开/内部/秘密/绝密），并与数据深度绑定，支持策略引擎按标签动态执行管控规则（如禁止跨设备传输、强制脱敏等）。突破传统“外挂标签”易篡改、易分离的缺陷，实现：①数据来源精准追溯，责任可

锁定；②安全等级动态适配，防高敏数据误用；③“数据自带策略”，支撑精细化、自动化访问控制，解决“无防护数据”流转失控难题。

3.3 端云协同的智能情境化访问控制：实现数据共享“可控可审计”

融合HarmonyOS端云协同能力与属性基访问控制（ABAC）模型，构建“云端决策+端侧执行”架构。为应对云端决策延迟（曾达8秒），在端侧增加“策略缓存与本地轻决策”模块，高频请求本地处理，平均延迟降至0.5秒内。通过“安全状态优先于身份权限”的权重机制解决多维情境冲突。访问时，端侧采集用户身份、设备状态、时间、场景、数据等级等情境信息，加密上传至云端策略引擎；引擎结合空域法规、行业标准与数据标签实时生成细粒度授权指令（如“只读1小时”“禁止下载”），端侧在TEE中执行并同步上报审计日志，形成闭环管控。相较传统基于角色（RBAC）的静态授权，本方案实现：①授权从“静态角色”转向“动态情境驱动”，适配应急协作等复杂场景；②权限从“粗放全量”细化为“最小必要”，降低泄露风险；③控制与审计深度融合，全程留痕、不可篡改，兼顾共享效率与合规安全。

4 应用场景与综合价值分析

4.1 应用场景

本系统在多元场景中展现出显著的安全与效能协同价值：（1）电网智慧巡检：自动规划合规航线，从飞控底层锁定作业范围；巡检数据端侧实时加密，授权班组“按需解密、全程留痕”，效率提升50%以上。（2）精准农林管理：通过分布式数字身份明确“农业数字资产”所有权；数据共享采用动态权限（只读、有效期可控），破解“共享难、保护难”痛点。（3）紧急医疗救援：搭建低时延、高安全的“绿色空中通道”，加密传输飞行路径与生命体征数据；任务结束后自动脱敏归档，兼顾效率与隐私[4]。（4）智慧城市综合治理：实现多部门设备无缝互联与数据格式统一；违规事件数据自动分类，并通过ABAC策略精准推送至对应执法部门，提升协同处置效率。（5）重大活动安保：实现多机统一编队协同与态势共享；监控数据端到端加密，访问权限与人员等级、任务时段动态绑定；任务结束自动集中擦除数据并生成审计凭证。

4.2 综合价值

综合价值体现在三个层面：技术层面初步验证了分布式架构在低空经济安全管控中的优势，缓解了“数据孤立”“管控空白”等难题。产业层面提供定制化解决方案，降低各行业安全合规成本，并通过跨设备协同提升作业效率，助力实体经济智能化转型。行业发展层面形成可复制、可推广的安全管理实践模式，有助于规范行业秩序，为国家低空经济战略的安全落地提供技术支撑。

5 结语

本研究完成了基于HarmonyOS的无人机低空经济内生安全协同系统的设计与实践。其核心贡献在于：尝试突破传统“被动防护”范式，初步构建了“分布式架构-内生安全-全生命周期管控”的理论框架；研发了具备可落地潜力的多场景安全解决方案，测试中实现效率提升40%-60%、风险下降80%以上；在研究视角、技术路径和核心目标上实现了对前人研究的三重跨越。研究也存在局限性，如老旧设备适配、未知威胁自适应防御能力不足、中小企业接入成本较高等。未来工作将聚焦于：联合各方推动基于鸿蒙生态的安全标准共建；深化区块链在审计日志存证中的应用；并挖掘小艺智能体的潜力，发展异常行为智能预警能力，推动系统从“被动合规”向“主动智能风控”进化。

参考文献

[1]华为技术有限公司.HarmonyOS开发者文档[EB/OL].[出版年].https://developer.harmonyos.com/.

[2]任卓,刘建伟,王帅.无人机集群协同控制技术研究进展[J].自动化学报,2021,47(1):1-17.

[3]任磊,贾晓辉,杜军平.面向智能无人系统的自然语言交互技术综述[J].计算机研究与发展,2020,57(9):1833-1851.

[4]张永生,刘军,王涛.智能时代地理信息安全:挑战与对策[J].测绘科学,2020,45(10):1-8.