ICS 01.020
CCS A 00

团　　体　　标　　准

T/CAMC 0017-2025

低空智能网联系统 第 4 部分:信息安全体系建设指南

Low-Altitude Intelligent Connected System - Part four: Guidelines for Information Security System Construction

征求意见稿

202X-XX-XX 发布　　202X-XX-XX 实施

中国计算机自动测量与控制技术协会　发　布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1文件：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国计算机自动测量与控制技术协会提出并归口。

本文件起草单位：中国信息通信研究院、中移信息技术有限公司、上海东海职业技术学院、上海量讯物联技术有限公司、中电科大数据研究院有限公司、北京国科标研科技有限公司。

本文件主要起草人：王瑞、王弘毅、王改、陈刚、方玉园、支婷、蔡惠民、管桂林、王华、尚尔钧、张林虎。

低空智能网联系统第4部分：信息安全体系建设指南

1 范围

本文件规定了低空智能网联系统信息安全体系的总体要求、安全基础与公共性技术要求、不同层级信息安全要求、数据安全要求、安全运营与管理要求、重点领域信息安全要求、实施路径与建议等。

本文件适用于低空物流运输（无人机配送、货运无人机等）、低空公共服务（应急救援、消防灭火等）、低空交通管理（低空飞行器管控、航线规划等）、低空商业运营、低空科研教学等领域。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20274 信息安全技术 信息系统安全保障评估框架

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 38645 信息安全技术 数据安全分级指南

GB/T 44662 健康管理终端设备数据采集与传输协议

MH/T 2015 低空飞行服务系统技术要求

YD/T 4324 低空智联网通信安全技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

低空智能网联系统 low altitude intelligent connected system

由低空飞行器（无人机、垂直起降飞行器等）、地面控制设施、感知设备、通信网络、数据处理与存储平台、应用服务系统等组成，具备智能感知、自主决策、协同控制、数据交互能力，实现低空领域飞行器运行管理、任务执行与服务提供的综合系统。

3.2

信息安全 information security

为保护信息资产（包括数据、软件、硬件、服务等）免受未经授权的访问、使用、披露、修改、损坏、丢失或干扰，确保信息的机密性、完整性、可用性、真实性、不可否认性得到保障的状态和相关技术措施、管理过程的总和。

4 总体要求

4.1 信息安全目标

低空智能网联系统信息安全体系建设需围绕系统全生命周期的安全需求，实现以下安全目标：

4.1.1 保障数据机密性

防止低空智能网联系统中的敏感数据（如核心任务数据、系统关键配置参数、飞行计划等）被未授权主体获取或泄露。对于涉及国家秘密、商业秘密、个人隐私的数据，需通过加密、访问控制、数据脱敏等技术手段和管理措施，确保数据仅在授权范围内传输、存储和使用。

4.1.2 维护数据与系统完整性

可确保低空智能网联系统的硬件设备、软件系统、网络链路、各类数据在全生命周期过程中不被未授权篡改、破坏、伪造或损坏。飞行数据的实时传输、任务数据的处理分析、系统软件的运行、设备固件的更新等，均需通过校验、备份、冗余设计、防篡改技术（如数字签名、哈希算法等）等措施，保障数据内容的真实性、准确性和系统功能的正常实现。

4.1.3 确保系统与服务可用性

可保障低空智能网联系统在正常运行、面临网络攻击或遭遇突发故障（如设备损坏、通信中断、自然灾害等）时，核心功能（如飞行器控制、飞行状态监测、任务执行等）和服务不中断或可快速恢复。通过冗余部署（如关键设备冗余、灾备建设、故障快速定位与修复技术、抗干扰能力提升等措施，满足低空物流、应急救援、交通管理等关键领域对系统可用性的高要求。

4.1.4 保护用户隐私安全

严格遵循个人信息保护相关法律法规和标准要求，对低空智能网联系统中收集、存储、使用的用户个人信息进行合规管理。明确用户信息的收集范围和目的，获得用户授权，采取数据加密、匿名化处理、访问权限严格控制等措施防止用户隐私泄露，同时建立用户信息安全投诉与处理机制，保障用户对个人信息的知情权、查询权、更正权和删除权。

4.1.5 抵御各类网络攻击

具备有效识别、防范和处置针对低空智能网联系统的各类网络攻击能力，包括但不限于恶意代码攻击、网络入侵攻击（端口扫描、SQL 注入、跨站脚本攻击、DDoS 攻击等）、无线通信干扰、身份伪造攻击（伪造控制指令、冒充授权设备或用户等）。通过部署防火墙、入侵检测/防御系统（IDS/IPS）、反恶意代码软件、无线通信加密与认证机制、异常行为分析系统等技术手段，结合安全策略优化、攻击特征库更新等管理措施，构建多层次的攻击防御体系。

4.1.6 实现安全事件可追溯

建立完善的低空智能网联系统安全日志记录与审计机制，对系统中的用户操作行为、网络通信活动（如数据传输源地址与目的地址、通信协议、传输流量等）、系统运行状态、安全事件进行全面、准确、不可篡改的记录。确保在发生安全事件后，能够通过日志审计追溯事件的发生时间、地点、涉及主体、操作过程、影响范围等关键信息。

4.2 基本原则

4.2.1 整体性原则

从低空智能网联系统的全局视角出发，将信息安全融入系统规划设计、建设实施、运行维护、退役报废的全生命周期，覆盖系统的硬件设备、软件系统、网络架构、数据资产、管理流程、人员组织等所有环节和要素，避免出现安全短板或漏洞。统筹还应考虑信息安全、网络安全、数据安全之间的协同关系，以及安全措施与系统功能、性能、成本之间的平衡，构建全方位、多层次、一体化的安全保障体系，确保系统整体安全能力的提升。

4.2.2 动态性原则

低空智能网联技术的快速发展、安全威胁的不断演变以及法律法规和标准要求的更新，信息安全体系建设需具备动态调整和持续优化的能力。定期开展安全风险评估，识别新的安全威胁和漏洞；及时更新安全技术措施和管理策略；根据系统升级、场景变化或安全事件经验，对安全体系进行迭代改进，确保安全防护能力始终与系统发展和威胁态势相匹配。

4.2.3 合规性原则

以国家法律法规、行业标准和相关政策要求为基本依据，将合规性要求贯穿于低空智能网联系统信息安全体系建设的全过程。

a) 在系统设计阶段，充分考虑合规性需求，确保安全方案符合相关规定；
b) 在建设实施阶段，选用符合安全标准的设备和软件，按照合规流程开展安全功能集成与测试；
c) 在运行维护阶段，定期开展合规性检查与评估，及时整改违规问题；
d) 在数据处理、用户信息管理等关键环节，严格遵循数据安全和个人信息保护相关法规，确保系统安全建设与运营活动合法合规。

4.2.4 风险导向原则

以安全风险评估为基础，针对低空智能网联系统面临的不同类型、不同等级的安全风险，采取差异化的安全防护措施。

a) 优先聚焦高风险领域（如核心控制系统、关键通信链路等），投入更多资源实施高强度的安全防护；
b) 对于低风险领域，在满足基本安全要求的前提下，合理控制安全成本，避免过度防护；
c) 建立持续的风险监测与预警机制，及时发现新的风险点，动态调整风险应对策略，实现以最低成本将安全风险控制在可接受范围内的目标。

4.2.5 责任明确原则

明确低空智能网联系统信息安全体系建设与运营过程中各相关方（如系统建设单位、设备供应商、运营管理单位、用户、维护服务提供商等）的安全责任，建立清晰的责任划分与追究机制。

a) 建设单位需对系统安全方案的科学性和可行性负责；
b) 设备供应商需提供符合安全标准的产品，并承担产品漏洞修复责任；
c) 运营管理单位需落实日常安全管理职责，包括系统监控、漏洞修复、应急响应等；
d) 用户需遵守系统安全使用规定，妥善保管个人账号与信息；
e) 维护服务提供商需按照安全规范开展维护操作，防止因维护不当引发安全事件。

4.2.6 技术与管理结合原则

应重视先进安全技术在低空智能网联系统中的应用，构建技术层面的安全防护屏障；加强安全管理体系建设，包括制定完善的安全管理制度（如安全审计制度）、建立规范的安全操作流程、开展全员安

全培训、实施有效的安全监督与考核机制。通过技术手段与管理措施的有机结合，实现“技术防护 + 管理保障”的双重安全防线。

5 安全基础与共性技术要求

5.1 术语和定义规范

5.1.1 术语与定义编写规则

a) 术语需覆盖低空智能网联系统安全领域的核心范畴，包括但不限于密码应用、漏洞管理、层级安全、安全技术等细分领域。
b) 定义需遵循“精准性、无歧义、关联性”原则：精准性要求明确术语的核心内涵与适用边界，避免模糊表述；无歧义要求避免同一术语对应多个定义或同一概念使用多个术语；关联性要求对相关术语明确逻辑关系，便于使用者理解技术链条。

5.1.2 图形与符号规范

a) 统一低空智能网联系统安全相关的图形符号，包括但不限于安全状态标识、网络拓扑符号、操作流程符号。
b) 图形符号需满足“易识别、易传播、兼容性”要求：易识别要求图形简洁直观，避免复杂设计；易传播要求符号可适配不同载体（纸质文档、电子屏幕、系统界面），在不同分辨率下不失真；兼容性要求符号设计参考 GB/T5465.2《电气设备用图形符号第 2 部分：图形符号》等通用标准。

5.1.3 术语与符号管理机制

a) 建立术语与符号的动态更新机制，由标准制定机构定期（建议每 1-2 年）收集低空智能网联技术发展带来的新术语、新符号需求，组织专家评审后纳入标准附录，确保术语体系与技术发展同步；对已过时的术语进行标注或删除。
b) 明确术语与符号的使用场景规范，在安全检测报告中需使用标准图形符号（如漏洞等级需用“红/黄/绿”三色星级符号标注），在用户操作手册中需对专业术语（“轻量级认证”）进行通俗解释，兼顾专业性与易用性。

5.2 密码应用技术要求

通过规范密码技术的应用，可为低空智能网联系统的机密性、完整性、可鉴别性、抗抵赖性提供核心技术支撑，同时确保密码应用符合国家密码管理相关法规。具体要求如下：

5.2.1 密码技术选型原则

需根据低空智能网联系统的不同场景、设备性能、安全需求选择适配的密码技术：

a) 实时通信场景（如无人机与地面控制站的指令传输）：优先选用轻量级对称加密算法（如 SM4、AES-128），兼顾加密效率与安全性，避免因算法复杂导致通信延迟；同时采用哈希算法保障数据完整性，防止指令被篡改。
b) 身份认证场景（如无人机接入地面基站）：采用非对称加密算法（如 SM2、RSA-2048）实现数字签名与密钥交换，确保身份可鉴别与抗抵赖；对于算力受限的终端（如微型无人机），可采用基于椭圆曲线的轻量级非对称算法，降低资源消耗。

c）数据存储场景（如云端飞行数据归档）：采用对称加密算法（如 SM4）对数据加密存储，同时使用密钥加密密钥（KEK）机制管理存储密钥，避免密钥泄露导致批量数据泄露；对于敏感数据，需采用国家商用密码算法，禁止使用未经国家密码管理部门认可的境外算法。

5.2.2 密码应用共性要求

a）密钥管理：建立全生命周期密钥管理体系，包括密钥生成、分发、存储、使用、更新、销毁（通过物理粉碎、多次覆写等方式彻底销毁，防止密钥残留）。

b）密码模块要求：低空智能网联系统中使用的密码模块至少达到二级及以上安全等级；对于部署在户外的设备，密码模块需具备抗物理攻击能力（如防拆报警、电磁屏蔽），防止模块被拆解或侧信道攻击。

c）合规性验证：密码应用需通过国家密码管理部门认可的检测机构检测，取得《商用密码产品认证证书》或《密码应用安全性评估报告》；涉及国家关键信息基础设施（如低空交通管理云平台）的密码应用，需按照《关键信息基础设施安全保护条例》要求开展密码应用安全性评估（CAE），确保合规性。

5.3 安全漏洞分类分级规范

5.3.1 漏洞分类方法

a）按漏洞所在对象分类：硬件漏洞、软件漏洞、网络漏洞、管理漏洞等。

b）按漏洞利用方式分类：远程可利用漏洞、本地可利用漏洞等。

5.3.2 漏洞分级方法

采用“CVSS（通用漏洞评分系统）4.0”作为基础分级框架，结合低空智能网联系统的特殊性，从“基础评分”和“环境评分”两个维度确定漏洞等级，分为四级：

a）高危漏洞（评分≥9.0）：指可能直接导致低空智能网联系统瘫痪、飞行事故、敏感数据大规模泄露的漏洞；

b）中危漏洞（评分 6.0-8.9）：指可能导致系统部分功能异常、局部数据泄露、权限被滥用的漏洞；

c）低危漏洞（评分 3.0-5.9）：指利用难度高、危害范围小的漏洞；

d）无危漏洞（评分＜3.0）：指几乎无利用价值或利用后无实际危害的漏洞。

5.3.3 漏洞分类分级管理流程

明确漏洞发现后的管理流程：漏洞发现→漏洞分类→漏洞分级→处置优先级排序（高危＞中危＞低危＞无危）→漏洞处置（修复、封堵、替代方案）→ 验证测试（确认漏洞已消除）→ 漏洞上报→复盘总结（分析漏洞成因，优化漏洞管理机制）。

6 不同层级信息安全要求

6.1 安全运营与监测

a）应对低空飞行器、基础设施等的研发测试、制造、检测认证、流通、维保和注销等各个环节的网络安全相关过程/活动提出要求。

b）应对面向低空智能网联体系的信息安全风险评估方法、流程给出一般要求，包括信息安全相关资产的识别与赋值、威胁识别与攻击可行性评估、风险评估等环节。

c) 围绕低空智能网联体系的安全应急响应的过程，给出安全应急响应的组织架构与职责、每个响应阶段的具体要求、信息安全事件的分类分级与处置策略、应急响应预案与演练等。
d) 对低空智能网联系统网络安全、数据安全事件的运营管理、应急响应等过程中涉及的联防联控过程、方法、以及信息共享、协同管理等内容作出规定。

6.2 网络层安全要求

6.2.1 通信安全

6.2.1.1 蜂窝移动通信（4G/5G）安全

a) 数据传输加密，采用 3GPP 定义的加密算法，对用户面数据（如飞行监测数据）和控制面数据（如飞行指令)进行端到端加密，禁止明文传输；核心网与基站之间的传输需采用 IPsec VPN 加密。
b) 抗干扰与防切换攻击，支持 5G 的抗干扰技术（如跳频通信、波束赋形），减少电磁干扰对通信的影响；防范切换攻击，需验证目标基站的数字证书，切换前需二次确认基站身份。
c) 流量控制与异常监测，基站需对无人机的通信流量进行实时监测，识别异常流量，对异常终端采取限流、断连措施；支持流量溯源，记录无人机的 IMSI、IP 地址、通信时间、数据量，便于事件追溯。

6.2.1.2 卫星通信安全

a) 信号加密，采用国家商用密码算法（如 SM4）对卫星通信信号进行加密，防止信号被截获后破解；卫星终端需内置硬件加密模块，密钥存储于安全载体（如 TPM 芯片）。
b) 身份认证，卫星终端接入卫星网络前，需向地面卫星站提交数字证书（由卫星运营商颁发），地面站验证证书有效性（有效期、签名完整性）后，方可允许接入；禁止未认证终端接入卫星网络。
c) 抗欺骗攻击，卫星终端需具备星历校验功能，验证卫星播发的星历数据是否与预设值一致，防止攻击者通过伪造星历数据误导无人机定位；支持多卫星星座融合（如北斗 +GPS），当单一星座信号异常时，自动切换至其他星座。

6.2.1.3 短距离通信（RFID、BLE、Zigbee、UWB）安全

a) RFID 安全，采用超高频 RFID（UHF）技术时，需开启标签加密功能（如 ISO 18000-6C 的加密协议），禁止明文传输标签数据（如无人机设备编号、状态信息）；阅读器需验证标签的访问权限，防止未授权读取或修改标签数据。
b) BLE（蓝牙低能耗）安全，采用 BLE 5.0 及以上版本，开启 AES-CCM 加密功能，对蓝牙连接进行加密；配对时需采用 “数字密码 + 生物识别”的双重认证，防止蓝牙被暴力破解后接管无人机。
c) Zigbee 安全，启用 Zigbee 的 AES-128 加密功能，对网络层、应用层数据进行加密；采用集中式密钥管理，密钥可每 30 天更新一次；禁止非信任节点加入 Zigbee 网络（需协调器验证节点证书)。
d) UWB（超宽带）安全，利用 UWB 的高精度定位特性，结合加密算法（如 SM4）对定位数据进行加密，防止定位信息被篡改导致无人机碰撞；UWB 设备需具备抗干扰能力，在多设备共存环境下，定位精度误差需≤0.3 米。

6.2.2 身份认证

a) 为保障低空智能网联系统安全运行，需从多维度规范数字身份认证技术要求。在证书应用接口层面，应统一接口协议标准，明确数据交互格式与加密传输机制，确保无人机、通信基站、地面控制终端等多端设备间证书调用的兼容性与安全性；证书管理系统需构建全生命周期管理流程，涵盖证书生成、分发、更新、吊销等环节，同时具备权限分级管控与操作日志溯源功能，防范证书滥用风险。
b) 安全认证技术及测试方法方面，需制定基于国密算法的身份鉴别技术规范，明确认证流程的合规性要求，并建立覆盖数据完整性校验、抗中间人攻击、抗重放攻击等场景的测试评估体系，量化安全性能指标。针对无人机飞控模块、通信模组等关键部件，应研发适配其算力与功耗限制的轻量级认证技术。

6.3 端层安全要求

6.3.1 无人机整机信息安全

a) 整机信息安全管理体系要求：包括管理无人机信息安全的过程、风险管理和评估、无人机信息安全测试过程、漏洞监测、响应及上报过程、管理无人机信息安全依赖关系的过程等；强化包容审慎监管，认真落实低空领域法律法规、规章制度和监管责任，加强对低空飞行器设计、生产、进口、飞行和维修等活动的规范化管理。
b) 软件升级技术要求：规定无人机软件升级的安全要求和流程，确保软件升级过程中的信息安全。
c) 网络安全入侵检测规范：明确无人机整机网络安全入侵检测的方法和标准。

6.3.2 无人机分系统安全

无人机各分系统的信息安全至关重要，直接关系到其整体运行的安全性与可靠性。

a) 飞控系统作为核心，需采用冗余设计，如多套惯性测量单元和卫星导航模块，配合先进软件诊断算法实时监控数据，一旦传感器异常能迅速切换，保障飞行姿态稳定。系统应具备权限分级管理，不同人员操作权限明确。
b) 动力系统方面，要实时监测电池电量、电机转速等关键参数，对异常波动及时预警，避免因动力故障引发事故。通信系统需采用高强度加密算法，防止数据传输被窃听或篡改，建立可靠身份认证机制。

6.4 基础设施安全要求

低空智能网联系统的基础设施，其信息安全关乎系统整体稳定运行。

a) 在物理安全上，地面基站机房选址要避开灾害频发区与人员嘈杂处，配备坚固门禁，仅授权人员可入；安装全方位监控与温湿度监测设备，保障环境适宜。
b) 网络安全方面，地面基站要采用防火墙阻挡非法网络访问，定期更新系统补丁；数据中心构建多层网络防护体系，对不同区域设置访问权限，防止数据泄露。
c) 数据安全方面，地面基站传输数据全程加密，数据中心存储数据采用先进加密算法，定期备份并异地存储，以防数据丢失或被恶意篡改，全方位守护低空智能网联系统的信息安全。

7 数据安全要求

7.1 数据分类分级

依据国家数据安全法规的要求，对低空智能网联系统中的数据定义分类分级的规范，明确一般数据、重要数据、敏感数据的划分依据及相应通用的安全要求，以及基于不同应用场景对数据分类分级的要求。

7.2 数据生命周期安全要求

需对低空智能网联系统涉及的数据的生成、采集、存储、传输、访问、处理和使用等过程或活动提出安全要求。

a) 数据生成阶段需确保源头合规，机载设备、基站等生成的飞行数据、设备状态数据需附带时间戳与设备标识，避免数据伪造；
b) 采集时遵循“最小必要”原则，如采集操作员信息仅获取身份核验必需字段，敏感区域影像需经审批后采集，禁止超范围采集；
c) 存储环节需按数据级别分级防护，一般数据可存于普通加密服务器，重要与敏感数据需用 SM4 等算法加密并存储于三级及以上等保设备；
d) 传输需用 TLS1.3 或 IPsecVPN 加密，敏感数据额外加硬件加密保护；
e) 访问、处理与使用需落实权限管控，敏感数据仅授权人员经多因素认证后操作，处理后数据需留存操作日志，使用中禁止篡改或违规共享。

7.3 数据共享安全要求

针对低空智能网联系统跨域、跨平台数据共享与协同联动的需求，需构建多维度安全防护体系。

a) 数据传输环节，需采用国密算法（如 SM4）对共享数据全程加密，搭配 VPN 专用通信通道，防止数据在跨域传输中被窃取或篡改；
b) 跨平台共享时，要建立统一的身份认证机制，各参与方需通过数字证书验证身份合法性，避免非法平台接入；
c) 需明确数据共享边界，仅开放协同联动必需的最小数据子集（如飞行态势基础数据），禁止敏感数据随意共享；
d) 需留存完整的数据共享日志，记录共享对象、时间、数据类型及用途，便于后续审计追溯。

8 安全运营与管理要求

8.1 网络安全生命周期管理

需对低空飞行器、基础设施等的研发测试、制造、检测认证、流通、维保和注销等各个环节的网络安全相关过程、活动提出要求。

a) 研发测试环节，需将网络安全融入设计，开展漏洞扫描与渗透测试；
b) 制造环节，禁止硬件植入恶意芯片，软件预装前安全检测，出厂设备重置默认密码并禁用冗余接口；
c) 流通环节，建立设备溯源机制，记录序列号、流向，禁止销售未修复高危漏洞的产品；
d) 维保需由资质人员操作，留存操作日志，禁止泄露敏感数据；
e) 注销环节，彻底销毁设备内数据，拆除存储介质单独处理，注销信息上报监管机构。

8.2 安全风险评估

a) 资产识别与赋值需梳理硬件、软件、数据等资产，按机密性、完整性赋值，如飞行控制数据赋值“高”；威胁识别需覆盖黑客攻击、设备故障等，评估攻击可行性。
b) 风险评估采用定性与定量结合法，分析资产、威胁、脆弱性叠加风险，形成风险清单与等级。

8.3 安全应急响应

a) 组织架构设国家、省、市、运营单位四级，国家级统筹重大事件，运营单位初处置；

b) 响应分监测预警、事件处置、恢复总结阶段，预警需设四级，处置时先遏制风险，恢复后 72 小时内复盘；
c) 事件分特别重大、重大、较大、一般四级，红色事件 24 小时恢复核心服务；
d) 预案需含资源清单与上报路径，运营单位每季度演练，演练后评估效果并整改问题。

8.4 安全联防联控

a) 联防联控过程需建立多方协同机制，运营单位、厂商、监管机构等定期召开联席会议；运营单位发现威胁后，1 小时内同步至厂商与监管机构，厂商提供漏洞补丁，监管机构协调资源。
b) 信息共享需搭建加密平台，分类分级共享威胁与事件信息，绝密信息仅共享至国家级；协同管理中，跨主体事件由监管机构牵头，明确各方职责。

9 重点领域信息安全要求

针对低空智能网联系统的重点领域，如军事应用、民用应用、商业应用等，可提出相应的信息安全要求，详细内容如下所示：

a) 军事应用领域，需采用军用加密标准保护低空监测数据、飞行控制指令，存储设备需物理隔离且经军工级认证，仅授权且背景审查合格人员可操作，禁止接入民用网络，数据销毁需按军事保密流程执行；
b) 民用应用（如城市巡检、应急救援）需保障公共数据安全，巡检影像脱敏处理，救援数据优先保障可用性并实时备份，设备需接入统一监管平台；
c) 商业应用（如低空物流）需加密用户隐私与订单数据，建立数据共享审批机制，定期开展漏洞扫描，确保业务合规与用户权益。

10 实施路径与建议

10.1 实施路径

a) 规划阶段需组建跨领域团队，梳理系统资产与安全需求，结合军事、民用等领域特性制定分阶段目标，明确资源投入与时间节点，形成信息安全体系建设规划方案并报监管部门备案。
b) 设计阶段依据规划方案，开展安全架构设计，如军事应用侧重物理隔离与军用加密，商业应用强化数据加密与访问控制；
c) 建设阶段按设计方案部署硬件（加密存储设备）、部署软件（入侵检测系统）；
d) 测试阶段通过渗透测试、压力测试验证安全功能；
e) 运行阶段建立日常监测与定期审计机制，确保体系持续有效。

10.2 建议与措施

a) 加强人员培训，针对不同岗位开展专项培训，如运维人员学习漏洞修复技术，管理人员掌握安全制度执行要点，定期组织考核与应急演练，提升全员安全意识与实操能力；
b) 提高技术水平，鼓励引入 AI 监测、量子加密等新技术，与科研机构合作攻克低空场景安全技术难题，建立技术迭代机制，及时将新技术融入安全体系；
c) 完善管理制度，制定数据分级、应急响应等专项制度，明确各环节责任主体，建立奖惩机制，对违规行为严肃追责，保障标准落地执行。