ICS 01.020
CCS A 00

团　　体　　标　　准

T/CAMC 00019-2025

低空装备飞行控制系统安全设计指南

Safety Design Guide for Low-Altitude Equipment Flight Control Systems

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：航空工业第一飞机设计研究院、天目山实验室、浙江众合科技股份有限公司、中航沈飞民用飞机有限责任公司、工业和信息化部电子第五研究所、成都智腾承启科技有限公司、北京国科标研科技有限公司。

本文件主要起草人：马佳驹、周尧明，林成浩、刘爱军、焦玉坤、陈平、于敏、杨亚楠、亢金涛、李威、尚尔钧、张林虎。

低空装备飞行控制系统安全设计指南

1 范围

本文件规定了低空装备飞行控制系统安全设计的术语和定义、总体要求、核心技术要求、验证与确认、数据安全与隐私保护、应急管理、维护与升级等。

本文件适用于低空装备（如无人机、eVTOL 等）飞行控制系统的安全设计，涵盖系统架构、容错机制、抗干扰能力、数据安全及验证验证等关键环节，旨在确保飞行器在复杂动态环境下的安全性与可靠性。

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 35018 民用无人驾驶航空器系统分类及分级
GB/T 38152 无人驾驶航空器系统术语
GB/T 38996 民用轻小型固定翼无人机飞行控制系统通用要求
GB/T 42862 民用大中型无人直升机飞行控制系统通用要求
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

飞行控制系统 flight control system

集成传感器、控制算法和执行机构，实现飞行姿态、动力分配及故障管理的核心系统。

3.2

容错控制 fault tolerant control

在部分系统失效时仍能维持安全飞行的能力。

3.3

智能算法 intelligent algorithm

基于 AI 的路径规划、故障诊断及动态决策模块。

4 总体要求

4.1 设计原则

4.1.1 冗余设计

在低空装备飞行控制系统的设计中，冗余设计是保障系统安全稳定运行的核心原则之一，重点针对关键传感器、执行器等模块展开。

a) 硬件层面，需为关键传感器（如惯性测量单元）配置双套或多套独立硬件设备，执行器（如电机驱动模块、舵机控制单元）则采用主备双路硬件架构；
b) 软件层面需开发独立的控制逻辑与数据处理程序，形成软硬件双重冗余机制；
c) 当主用模块出现故障时，系统可通过预设的故障检测算法快速识别异常，在毫秒级时间内自动切换至备用模块，确保飞行控制功能不中断，有效规避单点故障导致的系统失效风险。

4.1.2 抗干扰能力

抗干扰能力设计需从电磁、环境、数据安全三个维度构建全方位防护体系。

a) 电磁屏蔽方面，对飞行控制系统的核心电路板、信号传输线路采用金属屏蔽罩封装及双绞线布线，减少外界电磁辐射对信号的干扰；
b) 环境抗扰方面，集成抗风扰等算法，通过实时采集风速、风向数据，动态调整控制参数以抵消气流对装备姿态的影响；
c) 数据安全方面，对传感器采集数据、控制指令传输过程采用 AES 加密技术，防止数据被窃取或篡改，保障系统在复杂电磁环境与开放通信场景下的稳定运行。

4.1.3 实时性

实时性是决定低空装备飞行控制精度与响应效率的关键指标，需通过硬件选型与软件优化严格把控时间参数。

a) 硬件上选用高性能嵌入式处理器与高速数据总线，确保数据处理与指令传输的基础速率；软件上采用实时操作系统（RTOS），对控制任务进行优先级划分，保障核心控制指令优先执行。
b) 最终需实现两大关键指标：一是飞控指令响应时间应控制在≤50ms，即从传感器检测到姿态偏差到执行器做出调整动作的全过程耗时不超过 50 毫秒；二是飞控系统数据传输延迟应控制在≤10ms，即系统内部各模块间的数据交互延迟应控制在 10 毫秒以内。

4.2 系统架构

4.2.1 分层设计

低空装备飞行控制系统采用“感知 - 决策 - 执行”三层递进式架构设计，各层级功能独立且协同联动，形成完整的控制闭环。

a) 在感知层作为系统“感知器官”，核心在于传感器融合技术的应用：通过集成惯性测量单元（IMU）、激光雷达、视觉摄像头、GPS/北斗双模定位模块等多类型传感器，利用卡尔曼滤波、联邦滤波等算法对多源数据进行冗余校验与信息融合，剔除噪声干扰，输出装备位置、姿态、速度及周边环境数据，为后续决策提供可靠依据。
b) 在决策层承担“大脑中枢”职能，应用经典控制方法（含增稳控制功能、飞行管理功能、平台管理功能等）保障基本飞行安全，同时结合智能算法（如强化学习、模型预测）对感知层传输的数据进行实时分析，结合预设飞行任务（如巡航、悬停、路径规划）与动态环境变化（如突发障碍、气流扰动），快速生成最优控制策略，且具备故障诊断与容错决策能力，可在组件异常时自动调整控制逻辑。
c) 在执行层作为“执行手脚”，以冗余执行机构为核心，包含多套独立的电机驱动模块、舵机控制单元及动力调节组件，严格遵循决策层下达的控制指令，通过调节装备动力输出与姿态角，实现对飞行轨迹的实时控制，且在单一执行机构故障时，可通过冗余切换保障执行功能不中断。

4.2.2 接口标准化

为实现低空装备与外部系统的高效协同，系统架构需构建标准化接口体系，重点支持与地面站、空域管理系统的实时通信，打破数据交互壁垒。

a) 在与地面站的接口设计上，采用符合航空领域标准的通信协议（如 Mavlink 协议、TCP/IP 协议），定义统一的数据交互格式（包括飞行状态数据、任务指令数据、故障报警数据等），确保地面站可实时接收装备飞行参数、下发任务指令，同时支持双向数据加密传输。

b) 在与空域管理系统的接口适配中，遵循低空交通管理相关规范（如国内 GB/T 标准），实现空域授权信息、禁飞区数据、周边飞行器动态等信息的实时同步，帮助系统提前规避空域冲突。

c) 标准化接口应具备良好的扩展性，可兼容未来新增的外部系统（如气象预警系统、应急救援调度系统），为系统功能升级与多场景应用提供灵活支撑。

5 核心技术要求

5.1 容错控制技术

容错控制技术是保障低空装备飞行安全的核心机制，通过多维度设计实现系统在故障状态下的稳定运行。

5.1.1 模式切换

在模式切换方面，系统需支持多模式智能切换功能，涵盖手动/自动控制模式及备用动力模式等关键场景：

a) 自动模式下，系统依托经典控制方法，结合智能算法自主完成飞行控制；

b) 当遭遇复杂环境或自动控制异常时，可无缝切换至手动模式；

c) 主动力系统出现故障时，备用动力模式将快速启动，通过冗余动力单元（如备用电池、辅助推进装置）维持装备基本飞行能力，为应急处置争取时间。

5.1.2 故障响应指标

系统需满足故障响应指标如下所示：

a) 故障检测率需满足≥99.9%，通过构建多层次故障检测网络（包括传感器数据校验、执行器状态监测、通信链路诊断等），确保微小故障、潜在隐患均能被精准识别；

b) 容错响应时间需满足≤200ms，在检测到故障后，系统需在 200 毫秒内完成故障定位、冗余切换或控制策略调整。

5.2 控制算法安全

控制算法作为飞行控制系统的“决策核心”，其安全性直接决定低空装备的运行可靠性，需从功能精度与鲁棒性两方面建立严格标准。

5.2.1 路径规划算法

在路径规划算法设计中，需满足动态避障与环境适应性双重要求：

a) 动态避障精度，通过融合激光雷达、视觉传感器等的实时环境数据，算法需在 100ms 内完成障碍物建模与安全路径重新规划，确保装备与障碍物（如建筑物、其他飞行器）的横向与纵向安全距离（如小型无人机需控制在≤0.5m 范围内）；

b) 需适应风速≤15m/s 的复杂环境，算法需内置气流扰动补偿模型，根据实时风速、风向数据动态调整路径曲率与飞行速度，避免强风导致的轨迹偏移，保障在中低强度风力条件下的路径执行精度。

5.2.2 深度学习模型

对于深度学习模型（如用于目标识别、姿态预测的神经网络模型），需通过系统性测试验证其安全鲁棒性：

a) 必须通过对抗样本测试，即对输入数据（如图像、传感器信号）加入微小扰动后，模型的识别准确率或预测误差需控制在预设阈值内，防止恶意攻击或噪声干扰导致的模型失效；

b) 鲁棒性验证覆盖率需满足≥95%，测试场景应涵盖极端光照、电磁干扰、传感器部分失效等边缘工况，通过蒙特卡洛模拟、故障注入等方法，确保模型可在95%以上的异常场景中仍能输出可靠结果，从算法层面筑牢系统安全防线。

5.3 抗干扰能力

抗干扰能力是低空装备在复杂环境中稳定运行的关键保障，需从电磁兼容与环境适应两方面构建防护体系。

5.3.1 电磁兼容性

在电磁兼容性（EMC）方面，系统需通过传导发射、辐射发射测试，确保自身电子元件运行时的电磁辐射不会对其他设备造成干扰；同时需通过静电放电、辐射抗扰度、电快速瞬变脉冲群等抗扰度测试，在遭遇外部电磁干扰（如雷达信号、通信基站、高压输电线路等产生的电磁环境）时，能保持传感器数据采集准确、控制指令传输稳定。

5.3.2 环境抗干扰

在环境抗干扰尤其是抗风扰性能上，系统需配备高性能抗风扰算法，确保飞行轨迹精度要求（如大型低空装备应在 6 级风况即风速 10.8-13.8m/s 下保持飞行轨迹偏差在≤1m）。算法需通过实时采集风速传感器、姿态传感器数据，建立气流扰动模型，动态调整舵机转角、电机转速等控制参数：当遭遇阵风时，快速输出补偿力矩抑制姿态晃动；在持续侧风环境中，通过微调飞行航向角抵消风场推力，确保实际飞行轨迹与规划路径的横向、纵向偏差满足要求（如大型低空装备应在 1m 以内）。

5.4 数据安全

数据安全是低空装备飞行控制系统稳定运行的基础保障，需从数据加密、指令验证及备份恢复三个维度构建全链条防护体系。

5.4.1 数据加密

在数据加密方面，飞行数据（包括位置信息、姿态参数、任务指令等）的存储与传输需采用国密 SM4 算法进行加密处理。算法具备高强度加密能力（如大型低空装备采用 128 位密钥长度），可有效防止数据在传输过程中被窃取、篡改或伪造，确保飞行数据的机密性与完整性。

5.4.2 指令验证

对于起飞、着陆、紧急返航等关键指令，需建立双重签名验证机制：指令需经地面控制站操作员与系统管理员双重数字签名，接收端通过验证签名的有效性确认指令来源的合法性，杜绝恶意指令注入风险。

5.4.3 备份恢复

在数据备份与恢复机制上，系统需具备完善的断点续传与快速恢复能力。

a) 飞行过程中产生的关键数据（如飞行日志、故障记录、任务参数等）需实时备份至本地存储与云端服务器，备份过程支持断点续传功能—当通信链路中断后，恢复连接时可从断点处继续传输未完成的备份数据。
b) 数据恢复时间需控制在≤5 分钟以内，通过采用增量备份、数据压缩及快速校验技术，确保在系统出现数据损坏或丢失时，能迅速从备份源恢复关键数据。

6 验证与确认

6.1 仿真验证

仿真验证是确保低空装备飞行控制系统可靠性的关键环节，需通过高保真场景模拟与全面功能测试构建多层级验证体系。

6.1.1 仿真平台

在仿真平台搭建方面，需构建高保真度的数字孪生仿真环境，整合气象模型、地理信息系统与物理引擎：

a) 气象模块可模拟暴雨、强风、雷暴等突变气象条件，精确复现风速骤变、能见度骤降等极端场景；
b) 地理环境模块则基于高精度三维地图，模拟城市建筑群、山地峡谷等复杂地形，并植入动态障碍物（如突发闯入的飞行器、飘落的异物），实现碰撞风险场景的数字化复现；
c) 通过多维度参数调节，可模拟从常规到极端的全谱系运行环境，验证系统在边界条件下的稳定性。

6.1.2 测试覆盖度

在测试覆盖度方面，需建立严格的验证指标体系：

a) 核心功能（含增稳控制功能、飞行管理功能、平台管理功能等）逻辑覆盖率需达到 100%，包括飞行模式切换、路径规划、故障容错等关键功能，通过自动化测试脚本遍历所有控制逻辑分支，确保无功能盲区；
b) 故障注入测试比例需满足≥20%，即从传感器失效、通信中断、执行器卡滞等数十种潜在故障模式中，选取不少于 20%的典型故障类型进行注入测试，通过模拟单点故障、多点并发故障等场景，验证系统的故障检测精度、容错响应速度及降级运行能力，确保在实际飞行中可能遭遇的故障场景均已通过仿真验证。

6.2 硬件在环（HIL）测试

硬件在环测试是连接仿真验证与实际飞行的关键环节，通过将物理硬件嵌入虚拟仿真环境，实现对系统真实运行状态的精准验证。

a) 测试核心聚焦于控制模块的实时性与稳定性，需构建包含真实飞行控制单元（FCU）、传感器硬件、执行器组件的闭环测试系统—将实际硬件接入高保真仿真平台，通过信号接口模拟传感器数据输入（如姿态角数据、速度数据），并将控制模块输出的指令反馈至虚拟执行器模型，形成“硬件决策-虚拟执行-数据回传”的完整闭环。
b) 测试需满足时长要求，连续测试周期应满足≥72 小时：在不间断运行中，需模拟多场景切换（如从自主巡航到手动操控的模式转换、从低空悬停到高速飞行的状态切换），同步监测控制模块的指令响应延迟（需稳定在设计阈值内）、数据处理吞吐量及长时间运行后的性能衰减情况。
c) 测试过程中需动态注入电磁干扰、传感器噪声等干扰因素，验证控制模块在复杂工况下的稳定性，确保其在连续 72 小时高强度运行中无死机、无数据溢出、无控制失准等异常。

6.3 环境适应性测试

环境适应性测试是验证低空装备飞行控制系统在极端工况下可靠性的核心环节，通过模拟极端自然环境与机械应力条件，检验系统硬件的物理耐受性与功能稳定性。

6.3.1 极端自然环境测试

在高低温循环测试中，系统需经过宽温域循环考验（如大型低空装备温域为-40℃~70℃）：测试舱内温度将按预设程序交替在极低温（-40℃）与高温（70℃）间切换，建议每个循环包含 8 小时恒温暴露与 2 小时温度剧变过程，累计循环次数应不少于 10 次。测试期间需持续监测核心部件（如处理器、传感器、电源模块）的工作状态，确保在低温下无电路冻结、信号漂移，高温下无元件过热、性能衰减，且温度恢复后系统能快速重启并恢复正常控制功能，满足在寒区、沙漠、高温机舱等极端温度环境中的使用需求。

6.3.2 震动测试

振动测试需覆盖 5-2000Hz 的全频段机械振动环境，模拟装备在运输、起飞、湍流飞行等场景中承受的振动应力：

a) 建议测试将按 GJB150 规定的振动等级，先以 5-200Hz 低频段进行正弦振动测试，验证结构抗共振能力；
b) 建议以 200-2000Hz 高频段进行随机振动测试，模拟气流扰动产生的高频振动。
c) 测试过程中需通过加速度传感器监测关键部件的振动响应，确保电路板焊点无脱落、连接器无松动、光学元件无位移，且振动环境下的传感器数据采集精度、控制指令输出稳定性仍符合设计标准。

7 数据安全与隐私保护

7.1 数据分类

数据分类是构建分层防护体系的基础，需根据数据敏感度与影响范围精准划分等级。

a) 飞行数据归为公开级，这类数据包括装备常规飞行轨迹（已剔除精准坐标、任务关联信息）、飞行时长、平均速度等非敏感内容，主要用于行业数据统计、公共飞行态势公示等场景，虽无需高强度加密，但需通过校验机制确保数据完整性，避免被篡改导致公共信息误导。
b) 控制指令划分为机密级，涵盖起飞授权指令、紧急规避指令、动力系统调节参数等直接决定飞行安全的核心数据，一旦泄露或被篡改可能引发坠机、空域冲突等严重事故，必须采用国密算法加密存储与传输，且仅限核心运维人员通过专用终端访问。
c) 用户信息属于隐私级，包含操作人员身份证号、登录账号密码、个人任务规划记录等私人信息，若泄露可能导致身份盗用、个人隐私曝光，需严格遵循《个人信息保护法》，采用脱敏存储、访问审计等措施，杜绝非法收集与滥用。

7.2 访问控制

访问控制需依托基于角色的权限管理（RBAC）机制实现精细化权限管控，避免越权操作引发安全风险。系统先根据岗位职能划分角色，如系统管理员、一线操作员、审计人员等，为每个角色配置专属权限：

a) 系统管理员可进行权限分配、系统配置等核心操作；一线操作员仅能查看所属装备的飞行数据、下发常规控制指令；
b) 审计人员仅可调取操作日志，无数据修改权限，通过角色边界隔离实现“最小权限原则”；

c）所有操作需生成详细日志，记录操作人员 ID、操作时间、操作内容、访问数据类型等信息，且日志留存时间≥6 个月。

7.3 隐私保护

隐私保护需重点防范语音通信和数据链路的信息泄露风险。其中，防范语音通信的核心措施是抑制人耳可听频段（20Hz-20kHz）的干扰信号。语音通信是操作人员与地面站、协同装备间的关键沟通渠道，可能涉及任务目标、应急处置方案等敏感内容，系统需在语音传输模块集成自适应滤波技术，实时识别并抑制可听频段内的杂波干扰，同时搭配语音加密算法对传输内容进行编码，即使干扰信号未被完全消除，第三方也无法还原有效语音信息。

8 应急管理

8.1 故障预案

故障预案是保障低空装备在突发故障时安全运行的关键，需针对高频风险场景制定完善应对策略。对于动力失效、通信中断等典型故障场景，要预设精细化自动恢复策略：

a）动力失效时，系统需在检测到异常的瞬间启动动力源切换程序，若主动力完全失效则触发备用动力激活逻辑，同时结合预设的迫降航线规划算法，引导装备向安全空旷区域降落；

b）通信中断时，系统自动切换至备用通信频段（如卫星通信、备用无线电频段），若仍无法恢复，则执行预存的“失联应急程序”，维持当前飞行状态或按预设航线返航。

c）对于有人低空装备，需配备降落伞、冗余动力等应急装置，且装置触发响应时间≤3 秒—从故障检测到应急装置启动的全过程需控制在 3 秒内。

8.2 黑飞防控

黑飞防控作为低空装备飞行安全的重要要求，需依托高性能地面感知系统构建全天候监测防线，杜绝非法飞行器入侵管控空域。地面感知系统需具备 24 小时不间断监测能力，通过融合多类型监测设备实现全方位覆盖：

a）白天依托高清光学摄像头捕捉空域目标，夜间启用红外热成像设备识别低可见度飞行器，同时搭配雷达系统（如低空补盲雷达）探测远距离、小目标飞行器，确保在暴雨、大雾、夜间等复杂环境下仍能稳定监测。

b）系统的非法飞行器识别准确率需控制在≥98%，通过训练基于深度学习的目标识别模型，对飞行器的外形特征、飞行轨迹、信号频率等多维度数据进行分析，精准区分合法作业装备与非法飞行器（如未备案无人机），并在识别到非法目标后快速触发预警机制。

9 维护与升级

9.1 OTA（空中下载）更新

OTA 更新是保障低空装备飞行控制系统持续优化与安全防护的重要手段，需建立严格的安全机制。

a）授权和验证机制：安全补丁作为 OTA 更新的关键内容，必须通过数字签名验证环节—系统会对补丁文件附带的数字签名进行合法性校验，确认补丁来源于官方授权渠道且未被篡改，防止恶意第三方注入含有漏洞或病毒的虚假补丁，避免更新过程中引发系统故障或数据泄露。

b）需设计更新失败自动回滚机制：若更新过程中出现网络中断、文件损坏等问题导致更新失败，系统会立即触发回滚程序，自动恢复至更新前的稳定版本，且回滚过程中需保障装备核心控制功能正常运行，不影响当前飞行任务或装备待机状态，确保 OTA 更新的安全性与可靠性。

9.2 故障诊断日志

故障诊断日志是实现装备精细化维护的核心依据，需全面记录关键部件运行状态。

a) 日志内容应涵盖传感器（如惯性测量单元、视觉摄像头）的实时数据偏差、执行器（如电机、舵机）的输出响应时间、核心处理器的负载率等关键参数，同时记录部件异常触发的告警信息（如故障代码、发生时间、持续时长），确保每一项潜在故障都有可追溯的原始数据。

b) 日志需支持远程分析功能，地面维护人员可通过加密通信链路调取日志，结合故障诊断算法定位问题根源；更能为预测性维护提供数据支撑，通过分析日志中部件性能的变化趋势，提前预判可能出现的故障（如传感器精度衰减），实现“提前维护”替代“事后维修”。