

团 体 标 准

T/CAMC 0010—2025

低空智能网联系统 第 5 部分：指挥调度平台 建设通用技术要求

Low-Altitude Intelligent Networking System – Part five: General
Technical Requirements for the Construction of Command and Dispatch
Platforms

征求意见稿

202X-XX-12 发布

202X-XX-12 实施

中国计算机自动测量与控制技术协会 发 布

目 次

前言.....III

1 范围.....1

2 规范性引用文件.....1

3 术语和定义.....1

4 总体技术要求.....2

4.1 架构设计原则.....2

4.1.1 分层协同.....2

4.1.2 弹性扩展.....2

4.1.3 智能驱动.....2

4.2 核心能力要求.....2

4.2.1 空域动态管控.....2

4.2.2 跨域协同调度.....2

4.2.3 应急响应服务.....2

5 技术架构要求.....2

5.1 基础设施层.....2

5.1.1 通信网络.....3

5.1.2 算力资源.....3

5.2 数据服务层.....3

5.2.1 数据融合.....3

5.2.2 数据安全.....3

5.3 应用支撑层.....3

5.3.1 智能决策引擎.....3

5.3.2 可视化系统.....3

6 功能模块要求.....3

7 性能与可靠性要求.....4

7.1 性能指标.....4

7.1.1 处理能力.....4

7.1.2 可靠性.....4

7.2 容灾备份.....4

8 安全与合规要求.....4

8.1 安全体系.....4

8.2 合规管理.....4

9 实施与运维要求.....5

9.1 建设流程.....5

9.2 运维管理.....5

10 测试与评估.....5

10.1 测试环境.....5

10.2 评估指标.....5

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：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：国防科技大学系统工程学院、航天时代低空科技有限公司、重庆大学、珠海中科慧智科技有限公司、汕头保税区联通工业有限公司、厦门兆翔智能科技有限公司、西安爱生技术集团有限公司、无锡凯美锡科技有限公司、北京国科标研科技有限公司。

本文件主要起草人：周鋈、李美璇、潘岩、潘超、杨青、韩青叶、郑建超、高四季、薛晓斌、王宝军、刘剑平、尚尔钧、张林虎

低空智能网联系统 第 5 部分：指挥调度平台建设通用技术要求

1 范围

本文件规定了低空智能网联系统指挥调度平台的总体技术要求、技术架构要求、功能模块要求、性能与可靠性要求、安全与合规要求、实施与运维、测试与评估等内容。

本文件适用于低空智能网联系统指挥调度平台的规划设计、开发部署、运行维护及评估改进，可覆盖空域管理、飞行服务、应急指挥等核心场景。

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 22239 信息安全技术 网络安全级保护基本要求
GB/T 37724 信息技术 工业云服务 能力通用要求
GB/T 38675 信息技术 大数据计算系统通用要求
GB/T 39612 低空数字航摄与数据处理规范
GB/T 39409 北斗网格位置码
T/CIE 131 信息技术 通用时空信息应用支撑平台参考架构
T/CITS 411 低空空域智能管控系统建设指南
T/CIET 828 低空空域数字孪生系统技术规范
T/CQRA 007 低空飞行综合管理服务系统技术规范
T/TDIA 00013 面向低空空域的集群通信平台建设技术规范
T/GXDSL 012 低空经济产业链数据共享与协同标准
MH/T 2015 低空飞行服务系统技术要求
MH/T 4055.1 低空飞行服务系统技术规范 第 1 部分：架构与配置
MH/T 4055.2 低空飞行服务系统技术规范 第 2 部分：技术要求
MH/T 4055.3 低空飞行服务系统技术规范 第 3 部分：测试方法

3 术语和定义

下列术语和定义适用于本文件。

3.1

动态空域网格 **Dynamic airspace grid**

动态空域网格可将空域进行精细划分与灵活管理，把特定空域，尤其是低空、中空等不同高度层的空域，按照一定规则及北斗网格位置码标准分割为众多网格状单元。网格大小会依据空域繁忙程度、飞行器类型及飞行任务需求等因素动态调整。

指挥调度平台 **Command dispatching system**

指挥调度平台是辅助指挥管理人员实施组织、指挥与协调的一类信息系统。

4 总体技术要求

4.1 架构设计原则

4.1.1 分层协同

分层协同是指挥调度平台的核心架构支撑，可采用“端-边-云”三级联动模式。终端设备（如飞行器传感器、地面终端）负责实时数据采集与基础感知；边缘节点（如低空基站、边缘服务器）承担本地化数据处理与即时响应；云端平台则进行全局资源统筹与深度分析。三级架构无缝衔接，支持空天地一体化通信覆盖与全域感知数据融合，实现任务从感知到决策的高效协同闭环。

4.1.2 弹性扩展

弹性扩展是指挥调度平台适配动态负载的关键能力，依托微服务架构实现核心功能的模块化拆分与独立部署。各服务模块可根据实际业务需求灵活增减，支持节点规模在 50 至 300 区间内动态扩容，保障系统在不同工况下的高效稳定运行。

4.1.3 智能驱动

智能驱动是指挥调度平台提升决策精度的核心支撑，通过深度融合AI算法构建智能化管理体系。基于机器学习与深度学习模型，实时分析空域流量、飞行器轨迹及环境参数等数据，实现空域资源的动态优化分配，精准匹配不同飞行任务的需求。同时通过冲突检测算法提前识别潜在飞行冲突风险，生成预警信息与规避建议，可提升空域运行的安全性与效率。

4.2 核心能力要求

4.2.1 空域动态管控

空域动态管控是指挥调度平台的核心功能，需具备高强度空域管理能力。系统可支持每小时 500 架次以上混合航空器的实时路径规划，通过智能算法优化航线布局，构建毫秒级响应机制，冲突预警响应时间应严格控制在 200ms 以内。

4.2.2 跨域协同调度

跨域协同调度是指挥调度平台实现全域空域管理的核心支撑，通过标准化接口技术打通民航、军方、公安等关键系统的数据壁垒。系统构建统一数据交互框架，实现各领域空域信息、飞行计划及管控指令的秒级同步共享。跨域协同机制可消除信息孤岛，确保多方主体实时掌握空域动态，为联合决策、应急联动提供高效数据支撑，提升全域空域协同管理水平。

4.2.3 应急响应服务

应急响应服务是指挥调度平台保障空域安全的关键功能，聚焦突发事件的高效处置。当遭遇飞行险情、设备故障等紧急情况时，系统依托实时数据采集与三维建模技术，应在5分钟内快速生成多套包含三维态势推演的处置方案。内容涵盖风险评估、资源调配、法规条例及操作指引，为指挥人员提供可视化决策依据，助力快速响应、精准施策，最大限度降低突发事件影响。

4.2.4 统一功能与接口要求

统一功能与接口要求是在指挥调度平台中实现统一空域管理、飞行信息、飞行服务等模块接口，规范飞行申报、告警、联动处置等功能。

5 技术架构要求

5.1 基础设施层

5.1.1 通信网络

通信网络是指指挥调度平台高效运行的核心基础设施，构建多模态传输体系保障全域连接。系统全面支持 5G-A 通感一体化技术实现高精度感知与高速传输，融合低轨卫星通信突破地域限制，通过自组网电台强化复杂环境下的应急通信。多技术协同可确保数据传输无死角，端到端时延应严格控制在 100ms 以内。

5.1.2 算力资源

算力资源是指指挥调度平台系统高效运转的动力核心，采用边缘与云端协同的分布式架构。系统按需部署 15-50 个边缘计算节点，可就近处理终端实时数据，同时与中心云平台形成算力联动。通过动态资源调度机制实现算力弹性扩展，可支撑 10 万级终端设备的并发接入与数据处理需求。

5.2 数据服务层

5.2.1 数据融合

数据融合是指指挥调度平台构建精准空域画像的核心环节，通过一体化数据处理平台整合 ADS-B、雷达、气象等关键数据源。系统可采用多源数据清洗、关联分析与时空对齐技术，将分散的飞行轨迹、空域环境等信息深度融合，驱动空域数字孪生体实现亚秒级动态更新，可为态势感知、决策推演提供高保真数据底座。

5.2.2 数据安全

数据安全是指指挥调度平台稳定运行的重要保障，可构建多层次防护体系守护关键信息。针对核心坐标等敏感数据，采用国际公认的 AES-256 加密算法进行全链路加密；将系统操作日志纳入区块链存证，利用分布式记账与不可篡改特性，确保操作轨迹可追溯、责任可认定。

5.3 应用支撑层

5.3.1 智能决策引擎

智能决策引擎是指指挥调度平台实现精准管控的核心中枢，需要实现通信、感知、导航、管控一体化，为平台提供实时、可靠的飞行器监控与数据传输能力。通过可持续学习历史飞行数据、实时空域状态及环境因素，能动态优化预测逻辑，将空域拥堵预测准确率稳定控制在 85% 以上。

5.3.2 可视化系统

可视化系统是边指挥调度平台实现直观管控的重要载体，具备高性能三维态势展示能力。系统可支持 200 名以上并发用户同时进行空域态势查询、操作与分析，通过 LOD（细节层次）渲染技术动态优化画面精度，应将渲染延迟严格控制在 0.3 秒以内。

6 功能模块要求

低空智能网联系统指挥调度平台的核心功能如下表 1 所示：

表 1 功能模块要求表

模块名称	核心功能	技术指标
空域管理子系统	动态地理围栏设置、空域资源弹性分配、多源数据融合处理。	空域数字孪生体更新频率应控制在≤5 秒，网格划分粒度应在 50m-5km 可调。
飞行服务子系统	电子化审批全流程自动化、飞行计划动态优化、多无人机协同管理。	审批时效压缩至传统模式 1/5，应支持 1000+ 并发飞行计划冲突检测。
应急指挥子系统	突发事件三维推演、应急资源调度、避障方案生成。	应在 10 秒内生成避障方案，支持系留无人机至少 24 小时滞空通信保障。
监控管理子系统	实时飞行状态监控、异常行为识别、越界自动报警。	目标识别精度应≥95%，误报率≤0.1%。

7 性能与可靠性要求

7.1 性能指标

7.1.1 处理能力

处理能力是指调度平台高效运转的核心保障，需具备海量数据处理与高并发接入能力。系统每日可稳定处理不少于 10TB 的空域数据，涵盖飞行轨迹、环境监测、设备状态等多类信息，确保数据及时分析与应用；同时支持 10 万级以上终端设备的并发接入，可保障资源动态调度与负载均衡技术。

7.1.2 可靠性

可靠性是指调度平台持续稳定运行的关键特质，通过关键业务双活中心部署构建高可用架构。两套独立的中心系统同步运行核心业务，实时保持数据与状态一致性，当主中心遭遇故障时，可自动切换至备用中心，且故障切换时间严格控制在 10 秒以内。双活机制可有效避免单点故障导致的业务中断，确保空域调度、数据处理等关键功能连续运行。

7.2 容灾备份

容灾备份是指调度平台抵御极端风险的重要防线，依托分布式存储与计算架构构建全方位数据保护体系。系统将核心数据分散存储于多个节点，并通过跨地域灾备机制实现异地数据同步备份，确保在本地系统遭遇严重故障或自然灾害时，关键数据不丢失。同时优化数据恢复流程，通过自动化恢复技术将数据恢复时间严格控制在 1 小时以内。

8 安全与合规要求

8.1 安全体系

- a) 安全体系是指调度平台筑牢安全防线的核心支撑，应严格遵循等保 2.0 三级标准构建全方位防护体系。通过建立网络边界防护、主机加固、应用白名单、数据脱敏四层防御架构，实现从网络入口到数据应用的全链条安全管控。网络边界防护应阻挡非法入侵，主机加固提升系统抗攻击能力，应用白名单规范程序运行，数据脱敏保障敏感信息安全，多维度防护为系统营造安全可靠的运行环境。
- b) 系统支持基于 UMIAN 等协议的远程身份认证机制，对远程接入设备进行严格身份核验，确保接入主体的合法性与安全性。通过动态认证与权限管控，有效防止非法设备接入系统窃取数据或干扰运行。

8.2 合规管理

a) 合规管理是指挥调度平台融入空域管理生态的关键基础，严格遵循 RTCADO-365C 标准构建数据交互规范。通过标准化接口设计与协议适配，实现与现有空管系统的无缝数据互通，确保飞行计划、空域状态等关键信息在不同系统间准确传输、高效共享。

b) 为适应空域通信技术的迭代升级，系统预留 15% 的冗余字段用于协议扩展，可灵活支持 5G-AURC 等新协议的平滑接入，可避免因协议更新导致的系统大规模改造，降低技术升级成本，同时确保系统能快速响应行业技术标准变化，持续保持与新兴通信技术的兼容性。

9 实施与运维要求

9.1 建设流程

建设流程采用分期递进实施的策略推进指挥调度平台系统落地。首年可聚焦基础能力搭建，完成边缘计算节点、通信网络等核心基础设施部署，同步落地空域动态分配、冲突检测等核心算法，构建系统运行的技术底座；次年重点强化智能决策能力，通过算法迭代优化与数据积累训练，将 AI 预警准确率提升至 95% 以上，显著增强系统对空域风险的预判能力。

9.2 运维管理

a) 运维管理是保障指挥调度平台持续稳定运行的关键环节，通过建立全链路自动化监控平台实现精细化运维。平台实时监测系统硬件状态、软件性能及业务流程，自动预警潜在故障并触发修复机制，将系统可用性严格控制在 99.99% 以上，最大限度减少因设备故障或性能波动导致的业务中断。

b) 为强化系统安全防御与应急处置能力，定期开展红蓝对抗演练模拟真实网络攻击场景，检验防御体系的有效性并优化防护策略；同时将应急响应演练频次设定为每年不少于 2 次，通过模拟飞行冲突、系统故障等突发状况，提升团队的快速响应与协同处置能力。

10 测试与评估

10.1 测试环境

测试环境是指挥调度平台功能验证与迭代优化的重要支撑，具备高度仿真的环境构建能力。通过自动化配置与镜像技术，可快速克隆生产环境的硬件架构、软件配置及数据场景。同时将功能迭代周期严格控制在 2 周以内，借助标准化测试流程与自动化验证工具，加速新功能从开发到上线的全流程效率。

10.2 评估指标

评估指标是衡量指挥调度平台运行质量与安全水平的重要标尺，采用安全能力成熟度模型（CMMC）进行系统化分级评估。通过对系统安全策略、技术防护、应急响应等维度的全面测评，精准定位安全能力短板并推动持续优化；应将核心场景故障率严格控制在 0.01% 以内，通过常态化监测与优化改进，最大限度降低关键业务环节的故障风险。