中国移动
China Mobile

低空智能网联网络与数据安全体系白皮书

（2025）

中国移动（成都）产业研究院 电子科技大学 中国电子科技集团 紫金山实验室

本白皮书参与编写单位包括（排名不分先后）：中国移动（成都）产业研究院，电子科技大学，中国电子科技集团，紫金山实验室，密码科技国家工程研究中心，中国电子科技集团有限公司总体院（特区），西北工业大学，中国信息通信研究院，广东为辰信息科技有限公司，北京启明星辰信息技术有限公司，信通数智量子科技有限公司，西安辰航卓越科技有限公司，中电科普华基础软件股份公司，国汽大有时空科技（安庆）有限公司，西部科学城智能网联汽车创新中心（重庆）有限公司，西部智车（重庆）科技有限公司。

主要参与编写人员（排名不分先后）：刘耕，苏郁，周剑，张小松，饶志宏，罗蕾，张帆，陈丽蓉，潘泉，兰盾，张愉菲，傅军，刘少勋，杜加玉，刘书勇，侯建宁，林晖，彭红，李华，王洪博，孙向前，李允，赵焕宇，罗建超，陈厅，汪小芬，童钰辉，汪珂丽，黄滟茹，杨文彬，林汲，程倩倩，韩雨亭，牛锐，徐晓东，郑文龙，何孝游，彭璐，邱裕鹤，何虎，何博，郭锐，詹海鹏，陈萧宇，尤景涛，王稀，赵一锋，吕洋，李扬，叶亮，刘晨晖，刘宏倩，肖堃，李庆建，韩建新，沈斌，张文滔，孔德聪。

目录

1. 引言

低空经济的发展依赖于高效、智能、可靠的信息基础设施，而网络与数据安全则是保障低空飞行器安全、高效运行的关键要素。在这种背景下，针对低空智联网开展网络与数据安全的建设已成为行业发展的迫切需求。

本白皮书旨在系统梳理低空智能网联网络与数据安全的现状与发展趋势，分析国内外标准体系建设情况，并提出标准体系建设的建议和框架。通过构建涵盖安全检测认证、运行监测、管理体系及防护技术的全生命周期安全体系，为行业提供系统性参考，推动低空经济的安全可持续发展。

标准体系的建立是推动行业规范化、透明化发展的必要基础。统一的技术标准为技术部署、运行监控与安全防护等关键环节提供明确依据，促进行业在统一框架下高效协同与规范运行。标准体系的建立应覆盖低空飞行器的设计、制造到运行的各个阶段，确保每一环节都能遵循相应的安全要求。此外，建设完备的标准体系，行业可构建全面的检测和管理能力，并通过对低空飞行器及基础设施进行实时监测和响应，保障低空经济在复杂的网络环境中能够稳定、安全地运行。

未来，通过持续的技术创新、标准化建设和政策支持，可以有效应对网络安全威胁和数据泄露风险，为低空经济产业提供更加安全、智能和可靠的保障。希望本白皮书能够为相关主管部门以及行业提供有价值的参考，促进低空智能网联体系的健康发展，共同开创低空经济更加安全、创新与可持续的新篇章。

2. 发展趋势

2.1. 低空经济发展的六要素

近年来，全球低空经济行业得到了快速发展，技术的突破和政策的支持为这一进程提供了强有力的推动力。无人机等低空经济相关产业的蓬勃发展，已成为推动经济增长的新引擎。低空经济的发展离不开六个关键要素：法规制度是保障，标准是依据，应用场景是根本，空域是关键，技术是支撑，安全是底线。依托“新技术+新标准”，打造“新模式+新产业”，孵化产业的新方向。

（1）法规是保障

各国纷纷出台无人机相关政策和法规，以保障低空经济有序发展。在我国，

《无人驾驶航空器飞行管理暂行条例》为低空经济的发展奠定了坚实的法律基础，并明确了国家主导、地方政府主责、市场运营的无人机业态框架。此外，相关部门还从行业监管的角度发布了一系列规范，涵盖无人机研发设计、生产制造、运行管理等多个领域，进一步保障了行业的规范化发展。

（2）标准是依据

低空经济的快速发展需要一套完善的标准体系，以确保行业的健康有序推进。制定统一的标准能够为低空经济参与者提供明确的合规框架，提升整体行业的运行效率，有助于提升产业链各环节的协同效能，减少资源浪费与市场混乱。同时，标准化将促进国内外低空经济领域的合作与交流，推动全球低空经济的协调发展。因此，制定符合行业需求的标准体系，对于确保低空经济的可持续发展至关重要。

（3）场景是根本

低空经济的腾飞离不开规模化、价值化的场景应用。只有通过针对不同客户主体的场景开发与应用，才能实现低空经济的规模化发展。目前，面向个人的载人运输、观光飞行及物流外卖配送等场景，已经展现出巨大的市场潜力；同时，面向企业和政府的巡检、监测等场景需求也在持续增长。除现有应用场景外，仍有许多新兴场景值得探索。通过创新应用场景的开发，可以更好地激发低空经济的潜力，推动产业的快速成长。

（4）空域是关键

开放的空域是低空经济规模化发展的关键，将空域开放与场景使用相结合，有助于提高空域资源的有效利用率，推动低空经济的快速增长。当前的目标是将低空打造成“可计算”的空域，构建低空飞行的“航路网”，支持具有“异构、高密度、高频次、高复杂性”特征的大容量融合低空飞行。因此，空域管理需要向智能化、精细化方向转型，以满足日益增长的无人机飞行需求，确保低空经济的安全高效发展。

（5）技术是支撑

低空经济的发展离不开强有力的技术支撑，尤其是在政策法规完善、空域进一步开放的过程中，必须依托有效的监管技术、运营技术和基础设施建设，确保低空活动安全和高效地开展。低空经济的开放与安全运行需要多领域技术的融合支撑，包括通信、导航、监视等。目前业内普遍认为，低空智联网将成为低空相

关技术应用和飞行活动承载的核心，因此，有必要加大低空智联网技术的研发和应用投入。通过技术的不断创新和完善，为低空经济的发展提供强有力的支撑。

（6）安全是底线

低空飞行的安全保障是低空经济可持续发展的基础。在无人机飞行过程中，涉及到空防安全、公共安全、飞行安全以及网络安全等多个层面。因此，必须建立完善的安全体系，确保低空经济的健康发展。安全体系的建设不仅需要从技术层面提供保障，还应从法规和标准层面加以完善。只有在确保安全的前提下，低空经济才能稳步前进，行业才能迎来更大的成长空间。

2.2. 政策总结

2023 年是低空经济政策全面完善的一年，无人机首部行政法规《无人驾驶航空器飞行管理暂行条例》出台，各部委集中发布涉及无人机全生命周期管理的相关政策。此外，各省市也纷纷发布低空经济发展的行动方案和若干措施。当前，国家及地方政策高度关注低空网络与数据安全，围绕技术攻关、产业支持和安全管理等方面提出了一系列要求，以促进行业的安全可持续发展。主要体现在以下几个方面：

安全责任与运行管理：政策对无人驾驶航空器的运行管理提出了明确要求，例如实名登记、飞行区域限制等。此外，还对无人机生产者的安全责任进行了规范，包括防止产品被恶意篡改、及时修复安全漏洞并按规定报告等。这些措施有助于提升行业的合规性和安全性，促进低空经济的有序发展。

技术创新与安全保障：多项政策鼓励企业和科研机构加强低空安全相关技术研究，如数据安全、通信链路安全等，以提升低空飞行器的安全性和稳定性。同时，政策支持应用商用密码技术、人工智能等前沿技术，以增强网络与数据安全防护能力。这些举措有助于提升行业的整体技术水平，为低空经济的发展奠定坚实基础。

数据管理与安全防护：在数据管理方面，提出应加强数据在采集、存储、传输和使用等环节的安全防护。此外，还要求相关运营主体遵循数据分类分级管理原则，强化低空飞行数据的合规存储，确保重要数据和个人隐私的安全。这些措施旨在平衡数据共享与安全保护，为行业提供稳健的数据治理体系。

低空运行监测与应急机制：针对低空飞行的安全管理，政策提出建立一体化

指挥体系，加强低空飞行动态监测和预警能力，并完善低空飞行应急处置机制，以提升运行安全性。这些举措有助于提高低空经济运行的安全管理能力，并增强对各类潜在风险的应对水平。

表 1 低空网络与数据安全相关要求

发布时间	发文方	发文名称	核心内容
2023-06-28	国务院、中央军委	《无人驾驶航空器飞行管理暂行条例》	➢ 从事民用无人驾驶航空器系统的设计、生产、使用活动，应当符合国家有关实名登记激活、飞行区域限制、应急处置、网络信息安全等规定。 ➢ 禁止利用无人驾驶航空器实施下列行为：非法获取、泄露国家秘密，或者违法向境外提供数据信息。
2023-12-18	工业和信息化部	《民用无人驾驶航空器生产管理若干规定》	➢ 民用无人驾驶航空器生产者不得在民用无人驾驶航空器中设置恶意程序；发现民用无人驾驶航空器存在网络或者数据安全缺陷、漏洞等风险时，应当立即采取补救措施，按照国家有关规定及时告知使用人，并向住所地的县级以上地方人民政府工业和信息化主管部门或者省级通信主管部门报告。 ➢ 国家鼓励民用无人驾驶航空器生产者依法使用商用密码等技术手段保护网络与信息安全。 ➢ 民用无人驾驶航空器生产者应当加强民用无人驾驶航空器生产过程的数据管理和安全防护。
2024-03-27	工业和信息化部、科学技术部、财政部、中国民用航空局	《通用航空装备创新应用实施方案（2024-2030 年）》	➢ 到 2030 年，以高端化、智能化、绿色化为特征的通用航空产业发展新模式基本建立，支撑和保障“短途运输+电动垂直起降”客运网络、“干-支-末”无人机配送网络、满足工农作业需求的低空生产作业网络安全高效运行。 ➢ 强化装备安全技术攻关，重点突破电池失效管理、坠落安全、数据链安全等技术，提升空域保持能力和可靠被监视能力。
2023-11-8	中国民用航空局	《中华人民共和国空域管理条例（征求意见稿）》	➢ 空域数据按照使用性质分为空域结构数据、空域环境数据和空域运行数据。空域数据管理包括空域数据采集汇聚、共享开放、开发应用、安全保障等活动。
2024-1-16	中国民用航空局	《民用微轻小型无人驾驶航空器运行识别最低性能要求（试行）》	➢ UAS 在设计时应提供相应的安全功能，以确保：防止对 UAS 固有信息的接口或功能的修改；减少运行识别模块及运行识别信息被人为篡改或破坏的可能。 ➢ 广播式运行识别信息接收及应用应符合国家用户隐私保护及数据安全等相关法律法规的要求。

			➢ 网络式运行识别服务提供者要求：应符合国家用户隐私保护及数据安全等相关法律法规的要求。
2024-07-23	中国民用航空局	《中型民用无人驾驶航空器系统适航标准及符合性指导材料（试行）》	➢ 指挥和控制数据链路安全符合性说明报告：可说明无人驾驶航空器系统满足 2.2.4（a）（1）的指挥和控制数据链路安全防护设计 （如加密设计）。
2023-03-29	交通运输部、国家铁路局、中国民用航空局、国家邮政局、中国国家铁路集团有限公司	《加快建设交通强国五年行动计划(2023—2027年）》	➢ 推进智慧邮政建设：建设一批智慧网点，支持推广无人车、无人机运输投递和无人仓建设。 ➢ 开展网络和数据安全能力提升行动。 ➢ 实现部三级系统等级测评全覆盖，网络监测预警系统完成迭代升级。 ➢ 完善行业网络安全信息通报机制，及时共享漏洞信息和威胁情报。 ➢ 加强数据分类分级保护 ➢ 组织实施网络安全实网攻防演练，加强商用密码应用推广。 ➢ 加强邮政快递业重要数据和个人信息保护。
2024-01-01	交通运输部	《民用无人驾驶航空器运行安全管理规则》	➢ 民用无人驾驶航空器航行服务提供方应当妥善保管民用无人驾驶航空器飞行活动数据记录，确保记录不会遭到破坏、篡改和盗窃。 ➢ 飞行动态数据记录应当至少保存 12 个月，飞行活动申请数据记录应当至少保存 15 个月。

表 2 各省市低空安全要求总结

地区	发文名称	核心内容
北京市	《房山区低空经济产业发展行动方案（2024—2027年）（征求意见稿）》《关于促进丰台区低空经济产业高质量发展的指导意见（2024—2026年）》《北京市促进低空经济产业高质量发展行动方案	➢ 加强高效氢能与储能、航空电池控制与管理等关键技术攻关，强化电池安全、数据链安全等技术突破。 ➢ 联合京津冀有空域条件的地区提供应用场景实践，开展低空安防反制、数据安全与信息安全防护技术验证，构建低空安全防范体系的典型示范应用。 ➢ 加强无人机及新型低空飞行器数据安全、网络安全攻防演练，着力确保信息安全。 ➢ 建立健全低空数据管理制度，强化数据分类分级管理，加强数据生产、传输、处理和使用全流程安全管理。 ➢ 瞄准复杂环境适应性及高安全防控，加快长距离、高

	（2024-2027 年）》	可靠、抗干扰、反劫持、防破解的飞控系统研制。
四川省	《成都市加快提升低空飞行服务能力培育低空经济市场的若干措施（征求意见稿）》	➢ 提升低空安全监管效能。支持建立一体化指挥体系架构，提升快速预警、精准识别、有效处置的低空安防能力，加强飞行活动、数据信息、公民隐私等安全管理。
山东省	《山东省通用航空装备创新应用实施方案（2024-2030 年）》《济南市低空经济高质量发展实施方案》	➢ 围绕电池失效管理、坠落安全、数据链安全等技术，强化装备安全技术攻关，提升空域保持能力和可靠被监视能力。 ➢ 加强安全管控。加强飞行活动、数据信息、公民隐私等安全管理，强化低空飞行应急处置能力。
广东省	《广州市低空经济发展条例》《深圳经济特区低空经济产业促进条例》	➢ 机关、企业、行业组织等建设运行的低空飞行运营平台应当符合标准要求并接入市级低空飞行综合管理服务平台，确保接入平台数据的真实性、完整性、准确性和及时性。 ➢ 从事低空飞行以及相关活动的单位和个人不得非法采集和处理数据。 ➢ 在发生或者可能发生国家安全数据以及个人隐私数据泄露、篡改、丢失和损毁的情况时，相关单位和个人应当立即采取补救措施，按照规定及时履行告知义务并向相关主管部门报告。
安徽省	《安徽省加快培育发展低空经济实施方案（2024—2027 年）及若干措施》《芜湖市低空经济高质量发展行动方案（2023—2025 年）》	➢ 围绕低空感知管控体系和低空信息安全关键技术开展研究，有序推进要地防御技术创新迭代。 ➢ 积极运用人工智能、大数据等新一代信息技术，提高低空飞行服务系统的响应速度和各项飞行数据处理能力，采用加密技术、访问控制等手段防止数据泄露或篡改，保护数据的安全性和隐私性，确保飞行活动安全。 ➢ 建立健全风险防范机制，严厉打击威胁生产安全、信息安全、飞行安全的违法违规行为，加大查处和惩罚

		力度。
江苏省	《加快推进低空制造产业高质量发展行动方案》	➢ 支持网络安全防控系统发展，保障低空网络安全和数据安全。 ➢ 引导优势企业和研究机构持续深化合作，重点突破低空航空器整机制造及关键配套、低空飞行管理、探测感知、电磁频谱管理、北斗应用、装备安全和网络数据安全等领域关键核心技术，提升低空航空器产品性能及飞行服务保障能力。
内蒙古自治区	《内蒙古自治区低空经济高质量发展实施方案（2024—2027年）》	➢ 加强低空空域应用监管，健全风险防范机制，严厉打击威胁生产安全、信息安全、飞行安全、扰乱公共秩序或危及公共安全的违法违规行为。
上海市	《上海市信息通信业加快建设低空智联网助力我市低空经济发展的指导意见》	➢ 探索低空经济网络和数据安全合规制度建设。加强低空经济领域网络和数据安全法律法规宣贯以及防护能力提升指导，鼓励、引导低空飞行器生产者和运营使用者采取相应技术手段保护网络和数据安全。开展低空经济相关产品的安全技术和标准研究。
浙江省	《绍兴市人民政府关于推进低空经济高质量发展的实施意见》 《关于支持民航强省低空经济发展加强自然资源要素保障的通知》	➢ 围绕低空感知管控体系和低空信息安全关键技术开展研究，有序推进要地防御技术创新迭代。 ➢ 加快推进实景三维浙江建设，打造全省低空三维可持续更新的数字孪生空间，夯实基础数据资源底板，为航线规划、航路管理、低空基础设施建设、低空经济应用场景提供地理信息服务保障，做好低空经济相关地理信息安全应用监管。
海南省	《海南省低空经济发展三年行动计划（2024-2026年）》	➢ 加强对低空无人机测绘、航空摄影和地理信息数据的安全监管，规范高精度实景三维地图的安全使用。
江西省	《江西省关于促进低空经济高质量发展的	➢ 深化军民航协作，促进各类数据汇聚互通，为监管方、管理方、产业方、运行方等各方面赋能。着力在网络

	意见(征求意见稿)》	安全、数据安全、恶意攻击防护、通信链路安全、飞行器飞控安全以及非合作目标的反制等方面，强化低空安全数字化保障。
辽宁省	《大连市低空经济高质量发展行动方案（2024-2026 年）》	➢ 建立健全风险防范机制，严厉打击威胁国防安全、生产安全、信息安全、飞行安全及扰乱公共秩序、危及公共安全的违法违规行为，加大反制、查处和惩罚力度。建立健全低空飞行应急处置机制，针对低空飞行过程可能出现的各类风险和问题做好应急预案，确保低空飞行安全有序。
湖北省	《湖北省加快低空经济高质量发展行动方案（2024—2027 年）》	➢ 筑牢安全防线。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。建立健全风险防范机制，严厉打击威胁生产安全、信息安全、飞行安全的违法违规行为。

3. 标准体系

3.1. 标准体系建设必要性与目标

低空智能网联体系涉及云、网、端多层级，涵盖各种丰富的业务场景，随着无人机、eVTOL、相关基础设施和各类管控服务平台等要素在网联化、智能化方面的交融发展，各种安全风险交织叠加，面临复杂且日益严峻的网络安全和数据安全问题。建立健全面向低空智能网联体系网络和数据安全的标准体系，对其涉及的安全技术、试验测试和管理进行体系性地规划，提出系统性的要求、方法及指南，将有利于指导低空智能网联设备、系统、平台的安全相关研发、准入合规及安全运营，为低空智能网联产业的安全健康发展提供支撑。

面向低空智能网联体系，建立其网络安全和数据安全标准体系，主要目标是防止敏感数据泄露和抵御各种网络攻击，确保系统的可用性及用户隐私的保护。低空智能网联体系的运行包含海量信息与数据，极易成为网络攻击的重点目标，同时也面临不同程度的数据泄露风险，需要设计不同层次的网络安全体系保障低空智能网联体系的稳定运行。参考智能网联汽车行业标准体系的建设经验，定义

并研制形成行业领先的网络与数据安全标准。

到 2027 年底，初步构建起低空智能网联的网络安全和数据安全标准体系。重点研究安全总体与基础、机载设备与系统安全、基础设施安全、平台与通信安全、数据安全、安全运营与监测等标准，完成急需标准的研制。

到 2030 年，形成较为完善的低空智能网联的网络安全和数据安全标准体系。提升标准对细分领域的覆盖程度，加强标准服务能力，提高标准应用水平支撑低空智能网联产业安全健康发展。

3.2. 低空智能网联网络与数据安全相关标准现状

3.2.1. 国际标准

- ETSI EN 303 645：随着物联网设备的普及，网络安全和隐私保护问题日益突出。许多物联网设备存在默认密码、未加密通信、软件漏洞等安全问题。ETSI EN 303 645 《Cyber Security for Consumer Internet of Things:Baseline Requirements》是由欧洲电信标准化协会（ETSI）发布的一项关于消费类物联网（IoT）设备网络安全的通用标准，旨在为物联网设备制造商提供一套基本的安全要求，以保护用户隐私和数据安全。标准内容涵盖漏洞报告、软件更新、安全通信等 13 个大类，并且高度重视用户隐私，要求提供用户数据易于删除功能、明确告知用户数据的收集存储和使用方式、确保数据不被非法窃取等。
- ISO/IEC 22460：该系列标准旨在规范无人机（UAS）执照和安全模组的设计，考虑了较高的安全性。通过解决物理特性、数据存储、加密功能和逻辑数据结构等问题，维护 UAS 驾驶人员信息的标识的完整性和安全性，保护了涉及无人机操作的数据和用户。该系列包含三个主要部分：

  a)第 1 部分规定了无人机执照的物理特性、基本数据元素、视觉布局及物理安全特性，为整个系列奠定了基础术语和物理要求；

  b)第 2 部分聚焦于无人机/UAS 安全模组的数据存储和加密功能，强调模组的灵活性，以适应不同类型的加密需求；

  c)第 3 部分则涉及逻辑数据结构、访问控制、认证和完整性验证，为执照的安全性设计提供详细指导。
- DO-326A / ED-202A：由 RTCA（美国航空无线电技术委员会）和 EUROCAE

（欧洲民用航空设备组织）同步制定的航空安全标准，全称均为《Airworthiness Security Process Specification》（适航安全流程规范），是航空领域首个针对机载系统安全的权威标准集。DO-326A / ED-202A 旨在确保航空系统的网络安全和信息安全，用于指导航空系统从开发到部署的整个生命周期中的信息安全。DO-326A / ED-202A 主要有七步适航安全认证流程，包括认证安全方面计划、安全范围定义、安全风险评估、风险可接受性确定、安全开发、安全有效性保证和证据交流。通过遵循 DO-326A / ED-202A，航空系统开发和运营者可以有效管理网络安全风险，确保系统的安全性和可靠性。

3.2.2. 国内标准

- **GB 42590-2023 民用无人驾驶航空器系统安全要求:**我国首部针对民用无人机的强制性国家标准，于 2023 年 5 月发布，2024 年 6 月 1 日正式实施。适用于除航模外的微型、轻型和小型无人驾驶航空器，覆盖研制、生产、交付、使用全环节，涵盖电子围栏、远程识别、应急处置、机体结构、数据链保护等 17 个方面的强制性技术要求，标准中还对每一项安全要求规定了相应的试验方法，包含试验条件、试验步骤，为低空安全提供有力保障。
- **YD/T 4324-2023 无人机管理（服务）平台安全防护要求：**该标准于 2023 年 7 月 28 发布，2023 年 11 月 1 日实施。规定了无人机管理（服务）平台按安全保护等级的安全防护要求，涉及业务应用安全、网络安全、设备安全、物理环境安全和管理安全。本标准对无人机管理（服务）平台面临的安全风险进行了分析，并在此基础上指出安全防护的主要内容，并分 5 级提出防护要求。
- **民用航空行业标准体系(征求意见稿)：**该征求意见稿于 2023 年 12 月 8 日发布，提出了民用航空网络安全和数据安全标准子体系的内容，其中网络安全类主要包括涉及网络安全的安全管理体系、安全防护、检测评估等方面内容。数据安全类主要包括涉及数据安全的安全管理体系、安全保护、检测评估等方面内容。
- **MH/T 2015-2024 基于区块链的民用无人驾驶航空器飞行数据存证技术要求:**该标准于 2024 年 1 月 10 日发布，2024 年 2 月 1 日开始实施。标准适用于民

用无人驾驶航空器运行中与飞行活动有关数据的生成、处理、传输、存储、应用和管理工作。标准的一般性要求涵盖数据的追溯性、有效性、隐私性和时效性。其区块链技术应用基本要求涉及应用架构的基础设施层、核心功能层、数据接口层、应用服务层和监控管理层。同时，规定了飞行数据存证模型，明确了运行业务相关方和存证支持相关方，对存证技术规则与过程方面提出了具体要求，并对存证数据及其格式进行了规范。

- **中型民用无人驾驶航空器系统适航标准及符合性指导材料（试行）:**该标准于 2024 年 7 月发布，适航标准涵盖设计特征、整机、系统与设备、使用限制和资料等方面要求。符合性指导材料包括工程评估验证、试验室验证、飞行试验验证和耐久性与可靠性试验等，提供多种验证方法和要求。其中网络安全主要涉及防止电子干扰、保障数据链路稳定和加密设计等方面；数据安全侧重于关键数据的可靠完整传输以及稳定监控等。

小结：当前，低空网络与数据安全的标准较为离散，需进一步在体系性、安全要求的完备性等方面进行系统性地规划和加强，以赋能日新月异的低空经济发展。行业已充分认识到这一问题，加快了相关标准的研制步伐，目前已有数项标准进入公开征求意见阶段，包含一项强制性国家标准，推动无人机产业朝着更加有序、健康、繁荣的方向迈进。

3.3. 标准体系建设建议

3.3.1. 标准体系框架

网络与数据安全标准体系的设计基于低空智能网联体系的参考架构进行考虑，覆盖“云”、“网”、“端”、“场景”等层级：“云”即包括安全运营与监测方面；“网”主要涉及通信安全；“端”重点以微、轻、小型无人机为主，包括无人机整机网络安全（无人机设备制造与准入）、无人机分系统安全、基础设施安全。将数据安全作为独立的标准分类进行考虑，而“场景”维度主要与数据安全有关，例如基于场景定义数据的分类分级。另外，还需要基础与共性类标准。因此，整个低空智能网联的网络安全与数据安全标准体系如下图所示。技术类安全标准的内容一般包含技术要求和检测方法，管理类安全标准的内容一般包含管理要求和检查方法，检测或检查的内容基于要求制定，与后者相对应。

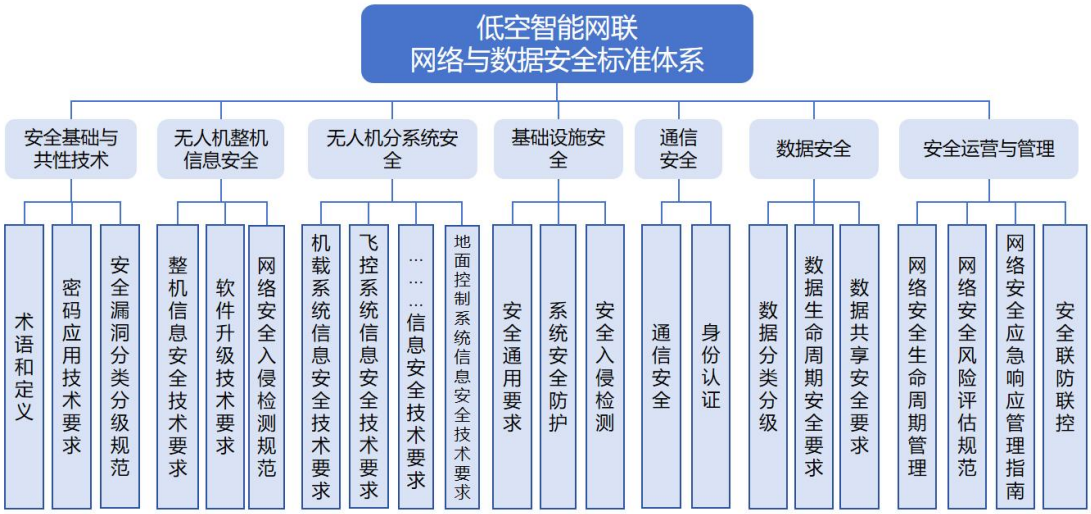

图 1 低空智能网联网络与数据安全标准体系

3.3.2. 安全基础与共性技术

包含术语和定义（包含图形与符号）、密码应用技术要求、安全漏洞分类分级规范等标准。

- 术语和定义：对低空智能网联网络与数据安全标准体系中涉及的术语、定义、各种图形与符号给出清晰、准确的描述。
- 密码应用技术要求：密码技术作为网络与数据安全的基础性、支撑性技术，在整个低空智能网联体系中将得到广泛应用，以满足各种维度（机密性、完整性、可鉴别、抗抵赖等）的安全要求，针对不同应用场景、设备及系统中的应用具有一些共性要求。
- 安全漏洞分类分级规范：给出低空智能网联体系中可能存在的各种漏洞的分类及分级方法，为实现漏洞的分类分级管理提供依据。

3.3.3. 无人机整机信息安全

针对无人机整机的制造与准入，其网络安全标准涵盖整机信息安全技术要求、软件升级技术要求、网络安全入侵检测规范等标准。

- 整机信息安全技术要求：
  - ❖ 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；
  - ❖ 整机信息安全基本要求：包括遵循无人机信息安全管理体系要求、供应

商安全风险管理、风险评估与管理、专用环境、信息安全措施有效性测试、攻击威胁漏洞监测及数据取证能力、密码算法与密码模块、默认安全设置、数据安全要求等；

- ❖ 信息安全技术要求：包括无人机的外部连接安全要求、通信安全要求、软件升级安全要求、数据安全要求等。其中外部连接安全要求包括远程控制、外部接口的安全要求；通信安全要求包括身份真实性验证、证书验证、无线通道完整性、数据操作访问控制、关键指令数据有效性唯一性、个人信息保密、零部件身份识别、防止非授权特权访问、边界防护与最小化授权、识别拒绝服务攻击、识别恶意数据、安全日志等内容；软件升级安全要求包括在线升级安全要求、离线升级安全要求等；数据安全要求包括密钥存储安全保护、敏感个人信息保护、无人机身份识别数据保护、关键数据保护、安全日志保护等。
- ❖ 检查与试验方法：针对信息安全管理体系以及技术要求，提供相应的检查或试验的方法。

- 软件升级技术要求：对无人机软件升级的管理体系的过程、安全保障、无人机端的升级功能要求等作出规定，并对相应的试验方法进行描述，包括升级包的真实性、完整性、防篡改、软件版本号管理等。
- 网络安全入侵检测规范：对无人机核心系统与部件的网络安全入侵检测（安全监控）功能、以及相应的处置措施等提出要求。

3.3.4. 无人机分系统安全

无人机核心系统与部件的安全标准内容包括硬件安全、安全启动、操作系统、中间件、应用软件、外部连接、通信安全等方面，分别对飞控系统、机载系统、地面指挥控制系统等提出信息安全防护技术要求。

3.3.5. 基础设施安全

低空智能网联系统基础设施的安全标准包括安全通用要求、系统安全防护、安全入侵检测等。

- 安全通用要求：给出对低空智能网联体系相关的基础设施的通用安全要求。
- 系统安全防护：对低空智能网联基础设施的系统安全防护技术提出要求，包括硬件安全、安全启动、操作系统、中间件、应用软件、外部连接、通信安

全等方面的安全技术要求。

- 安全入侵检测：对低空智能网联基础设施自身的安全监控（即入侵检测）功能、以及所能够采取的处置措施等提出要求。

3.3.6. 通信安全

包含通信安全、身份认证等标准。

- 通信安全标准：主要规范应用于低空智能网联的蜂窝移动通信（4G/5G）、卫星通信、无线射频识别、蓝牙低能耗（BLE）、紫蜂（Zigbee）、超宽带（UWB）等通信的安全技术与检测要求。
- 身份认证标准：主要规范低空智能网联系统数字身份认证相关的证书应用接口、证书管理系统、安全认证技术及测试方法、关键部件轻量级认证等技术要求。

3.3.7. 数据安全

包含数据分类分级、数据生命周期安全要求、数据共享安全要求等标准。

- 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（包括机载设备系统、基础设施、服务/运营/监管平台及它们之间通信等）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；
- 数据生命周期安全要求：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；
- 数据共享安全要求：低空智能网联系统涉及跨域、跨平台的数据共享、协同联动需求，该标准对数据共享的安全提出要求。

3.3.8. 安全运营与管理

安全运营的方面主要包括网络安全生命周期管理、安全风险评估、安全应急响应、安全联防联控等。

- 网络安全生命周期管理：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。
- 安全风险评估：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，并给出典型示例。

- 安全应急响应：围绕低空智能网联体系的安全应急响应的过程，给出低空信息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。
- 安全联防联控：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。

3.3.9. 重点领域与实施路径

随着无人机等低空相关系统、产品在军事、民用和商业领域的广泛应用，其网络与数据安全问题日益突出，例如恶意入侵可能导致航线篡改或敏感影像数据外泄，威胁公共安全与个人权益。低空智能网联体系网络与数据安全标准的研制是确保低空智能网联相关系统安全可靠运行的关键。

一、重点关注领域

标准研制重点关注的是要能够覆盖无人机生命周期的各个阶段，包括研制阶段的安全防护与监控措施的实现、生产阶段的供应链管控、运行阶段的安全运营等，确保其全生命周期的安全；在数据安全方面，重点关注数据的安全合规，即规范数据的采集、存储、传输环节的匿名化与加密要求。最终通过“设计即安全”原则和迭代式标准更新，平衡技术创新与风险管控，支撑无人机及整个低空智能网联产业的可持续发展。

二、相关标准研制的实施路径

1. 标准研制的总体思路

- 以需求为导向：根据无人机应用场景（如工业、消费）和安全需求，制定针对性的标准。
- 分层分类：将标准分为基础标准、技术标准、管理标准等，形成完整的标准体系。
- 动态更新：随着技术发展和安全威胁的变化，及时更新和完善标准。

2. 标准研制的主要步骤

- 需求调研与分析：调研无人机网络与数据安全的需求，分析现有标准的不足。
- 标准框架设计：设计标准框架，明确标准的适用范围、技术要求和测试方法。

- 关键技术研究：研究无人机网络与数据安全的关键技术，为标准的制定提供技术支撑。
- 标准草案编制：编制标准草案，明确具体的技术要求、测试方法和评估指标。
- 征求意见与修改：向行业专家、企业和研究机构征求意见，修改完善标准草案。
- 标准发布与实施：发布标准，并推动其在行业中的应用和实施。
- 标准评估与更新：定期评估标准的实施效果，根据技术发展和安全需求更新标准。

3. 标准研制的实施路径

- 国际合作：参考国际标准（如 ISO、IEC、ITU 等），参与国际标准的制定，提升国内标准的国际影响力。
- 行业协作：联合无人机企业、研究机构和行业协会，共同制定标准，确保标准的实用性和可操作性。
- 政策支持：争取政府在资金、技术和政策方面的支持，推动标准的研制和实施。
- 试点应用：在典型应用场景中试点应用标准，验证标准的可行性和有效性。
- 培训与推广：开展标准培训，提高行业对标准的认知和应用能力。

总结：低空智能网联体系的网络与数据安全标准的研制需要重点关注将安全的需求、设计、实现、验证融入到无人机研制的各个阶段和过程中，并开展持续的安全运营以确保其全生命周期的安全。通过需求调研、标准框架设计、关键技术研究、标准草案编制、征求意见与修改、标准发布与实施、标准评估与更新等步骤，制定出科学、实用的标准。同时，国际合作、行业协作、政策支持、试点应用和培训推广也是标准成功研制的重要因素。

4. 全生命周期安全体系

参考车联网成熟的安全管控模式，从一台无人机的研发设计之初就将网络安全进行同步规划、同步研发、同步生产及运营监测，不论是整机还是安全相关零部件，逐步建立起完善的标准和流程，具备端到端的、覆盖全生命周期各阶段（包括概念阶段、需求阶段、设计阶段、实现阶段、集成阶段、验证阶段、发布和运

行阶段）的安全体系。

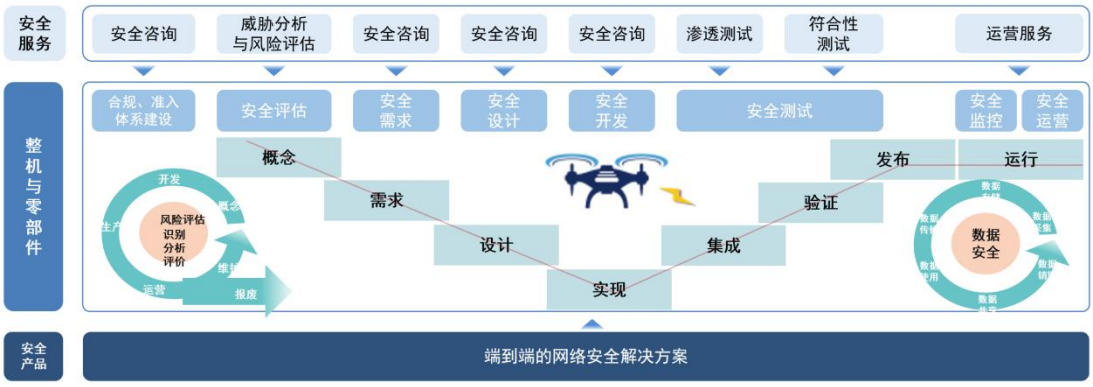

图 2 全生命周期安全体系

4.1. 安全检测认证

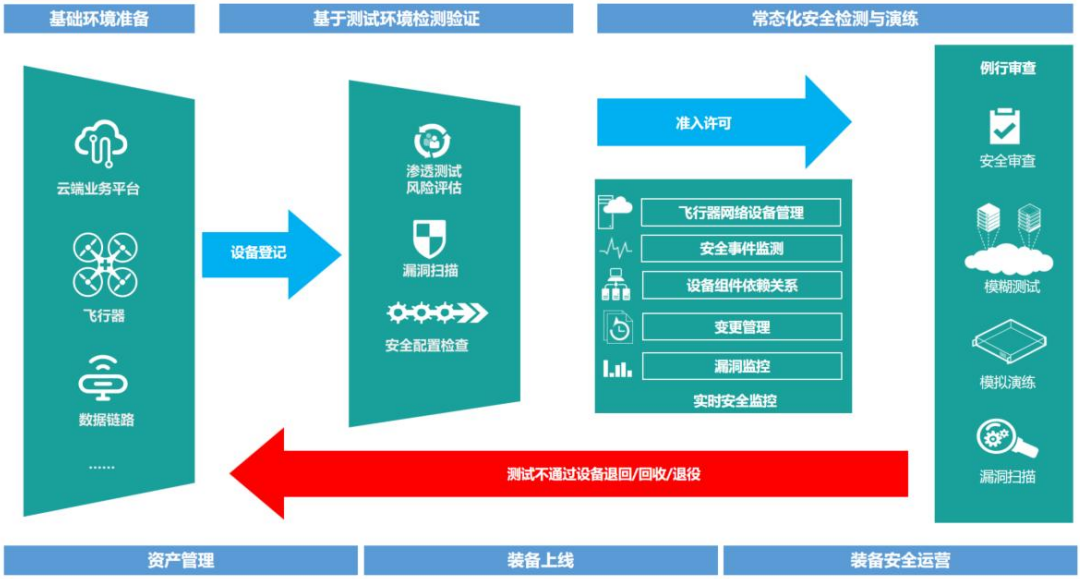

图 3 安全检测认证

低空智能网联安全检测认证能力是保障无人驾驶航空器、机载终端与基础设施安全运行、满足法律法规要求、提升行业竞争力以及推动技术创新的重要手段。随着低空经济产业的快速发展，加强网络数据安全检测认证工作已成为行业发展不可或缺的一部分。未来，应基于逐步完善的低空安全标准，推动技术突破，构建全面的安全生态体系，以应对日益复杂的网络安全挑战。

低空智能网联安全检测认证旨在打造面向低空安全准入、覆盖检测/认证/仿真验证的一体化能力体系，提升低空智能网联网络数据安全保障水平。安全检测中心应当全面覆盖低空智能网联体系内的全要素，涵盖飞行器、网络、设备、平

台、应用和数据等防护对象，支持整体安全架构、设备与系统安全、网络与传输安全、应用与平台安全、数据全生命周期等多层级，通过深入研究其网络数据安全测试评估技术，创新性地构建覆盖全要素的安全测试评估标准规范和流程方法，研发适配不同低空装备架构的自动化测试工具装备，实现低空智能网联全方位安全测试与能力评价能力。可支撑行业主管部门对相关企业开展入网前安全检测评估、安全产品评测、周期性安全评估、攻防演练、安全众测、新技术验证、人才培养、安全运营应急响应验证等应用场景，打造闭环式虚实安全验证环路。

4.2. 安全运行监测

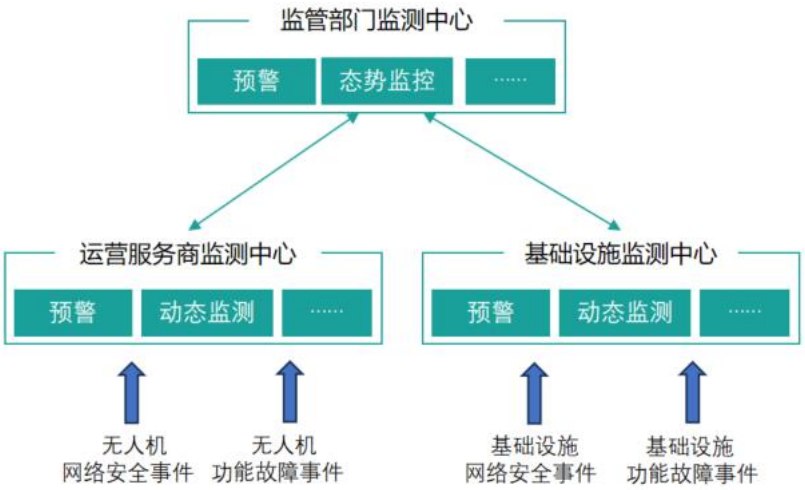

图 4 安全运行监测

低空智能网联系统存在的安全漏洞若被恶意利用，将严重威胁系统的安全稳定运行，如何有效发现和应对不断出现的网络安全事件是关键。因此，需要在保障低空智能网联系统安全的基础上，建立一体化的网络安全监测与运营管理体系，对低空智能网联系统运行安全风险进行管控。为保障无人机系统运行的安全可靠，同时满足相关安全合规与监管要求，需要构建一体化的网络安全监测与运营管理体系，对无人机运行安全风险进行管控，实现系统安全态势的“可见、可管、可控、可信”。

低空运营安全监测可构建自下而上的监测、预警、态势分析的体系架构。无人机运营服务商安全监测中心负责所运营无人机的网络安全事件采集、告警分析研判、资产信息管理、入侵检测规则策略配置与更新管理、安全漏洞管理、安全运维审计、安全态势感知、应急响应等功能。同理建设基础设施安全监测中心，

监测低空基础设施安全态势。中心通过采集无人机设备/基础设施的网络安全事件与日志，基于对安全事件进行分析、统计以及可视化呈现，实现系统的实时安全监控，及早发现安全风险，根据不同的威胁等级触发风险预警、开展溯源分析、漏洞验证和策略更新等安全管控，有效治理无人机系统和基础设施的网络安全问题。与此同时，安全风险数据可同步上报到监管部门。监管部门安全监测中心汇总辖区内无人机和基础设施安全监测中心上报的数据，通过对安全事件/漏洞进行分析、统计以及可视化呈现，实现对低空智能网联系统的实时安全态势监控与管理。

4.3. 安全管理体系

为应对网络与数据安全合规要求，需要建立安全管理体系，分四个层次进行建设，第一层次为组织的安全手册，包括网络安全方针政策与目标；第二层次为组织的管理程序，包括网络安全的各项管理制度；第三层次为组织的工作指导，包括网络安全管理活动的各项指南以及实施管理活动的所需要的表格表单等；第四层次为组织的实施记录，包括依据体系文件运行而产生的各项符合法规、标准要求的客观运行记录。

（1）安全手册编制

根据组织的网络安全方针政策及目标，依据法规、标准的要求，结合差距分析的结果及组织的现状，制定组织的网络安全管理组织架构和安全管理策略与方针。通过设立专门的网络安全管理机构，明确各部门和人员在网络安全管理中的职责和权限，确保网络安全工作得到有效的组织和协调。

（2）管理程序制定

根据安全手册的要求，进行顶层的管理程序拆分，制定组织在网络安全领域的活动过程和程序，包括安全建设管理、人员管理、供应商管理、安全运维管理等方面的流程制度文件。

安全建设管理贯穿系统整个生命周期，在系统审批、建设、安全定级与备案、安全方案设计、软件开发与实施、验收与测试、系统交付与等级测评等过程均需要进行安全管理。

人员管理是对员工定期开展网络安全培训，提高员工的网络安全意识和技能，使其能够在日常工作中遵循安全规范，识别和防范网络安全威胁。

供应商管理是对供应商进行严格的网络安全评估和管理，确保供应商提供的产品和服务符合企业的网络安全要求，签订包含网络安全条款的合同，明确双方的责任和义务。

安全运维管理是整个系统安全运营的重要环节，其内容涵盖机房环境管理、资产管理、介质管理、设备管理、漏洞和风险管理、网络及系统安全管理、恶意代码防范、配置管理、密码管理、变更管理、备份与恢复管理、安全应急处置以及安全服务管理工作等内容。

（3）作业指导书制定

作业指导书是组织活动开展的详细描述，涉及到组织现有体系中具体的业务运行，需要根据组织的现状，依据法规和标准的要求，制定相关作业指导书和用于流程活动开展的表格、表单。

（4）运行记录实施

运行记录是基于组织整个管理体系运行后产生的结果、记录。需要按网络安全体系要求开展覆盖系统建设与运营全生命周期的安全管理措施落地。

4.4. 安全防护关键技术

由于低空智能网联系统的开放性，导致其面临严峻的信息安全风险，一旦其安全性遭受破坏，将可能影响人身财产安全、交通安全，严重时甚至会对社会安全和国家安全造成影响。为保障低空智能网联系统运行的安全可靠，同时满足相关安全合规与监管要求，需要构建多维度纵深防御的安全防护体系。

4.4.1. 内生安全

4.4.1.1. 内生安全概念内涵

1.内生安全问题

低空智联网是低空经济发展的基石和助推器，随着智能化、网联化的融合发展促使低空智联网成为典型的复杂信息物理系统(CPS)，构成的复杂性使其难免在无人机（端）、通信网络（网）、监控服务管理平台（云）等方面存在漏洞后门或缺陷。低空智联网作为 CPS，其自身存在漏洞后门或设计缺陷，且在外部复杂环境下容易遭受不确定扰动或人为蓄意攻击。自身固有缺陷加之外部条件触发，容易引发内生安全问题。

在端侧，无人机系统面临攻击面多、资源受限、安全机制薄弱等问题，开源软件漏洞、无线通信易受攻击等威胁突出。网侧存在通信制式多样、网络协议不统一，数据链路开放易被干扰，无法互联互通等状况。云侧的监控服务管理平台则面临黑飞等异常情况难以管控，AI 算法存在不可解释性等难题。同时，复杂环境中的随机干扰和人为蓄意攻击，如障碍物遮蔽、电离层活动、电磁干扰、网电攻击、样本攻击等，严重威胁低空智联网安全，可能导致无人机飞行失控、数据泄露等后果。

图 5 CPS 漏洞后门或设计缺陷示意

2.内生安全防护增益

内生安全理论是一种创新的安全范式，能一体化解决网络安全、功能安全和信息/数据安全交织的问题。内生安全基于动态异构冗余（DHR）架构，不排斥传统安全技术，而且与传统安全技术结合可以获得非线性的防御增益。比如，在部分或全部可重构的执行体中差异化地部署入侵隔离、检测、预防等传统手段，或者采用防火墙、蜜罐、沙箱、杀毒软件、查补漏洞等多样化技术措施，或者应用动态化、虚拟化迁移以及加密认证等主动防御技术，其作用都是提高执行体之间的异构度，给非配合环境下的协同攻击带来更大的不确定性，提高 DHR 架构发现攻击的概率。

通过系统设计和架构创新，内生安全理论从根本上提升系统的安全性和可靠性，将安全能力融入系统基因，实现从“被动防御”到“主动免疫”的跨越。它能够不依赖先验知识，有效防御未知网络攻击，为解决低空智联网安全难题提供了新

思路，对推动低空经济安全发展意义重大。

4.4.1.2. 低空智联网内生安全关键技术

在低空经济迅猛发展的当下，构建一套完善的安全架构设计方案对于保障低空智联网的安全性和可靠性至关重要。该方案涵盖无人机飞控系统、通信与数据安全、感知与导航技术以及网络弹性设计等多个关键领域，通过整合各种安全技术和措施，构成一个有机整体，全面提升低空智联网在复杂环境中的鲁棒性。

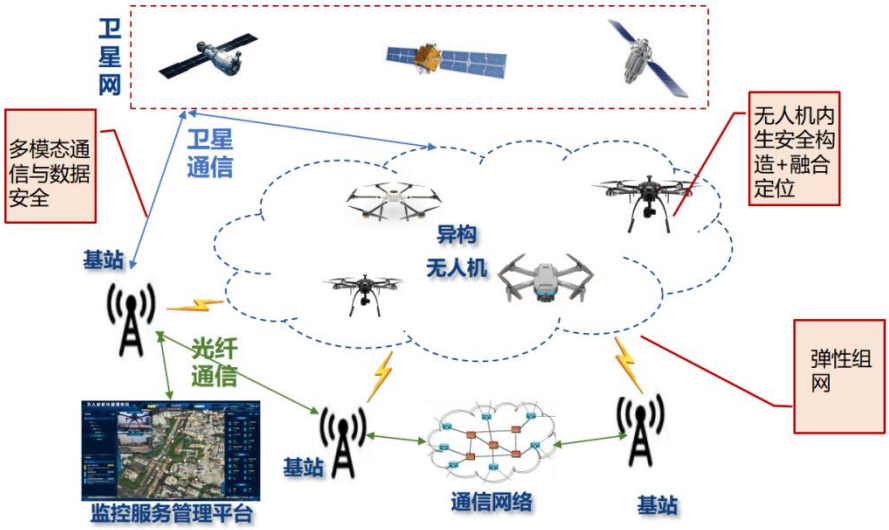

图 6 低空智联网内生安全关键技术

1.无人机内生安全构造

无人机作为低空经济核心终端载体，其主机系统面临攻击面多、资源受限、安全机制薄弱等问题。采用内外兼修的纵深防御机制，建立起“内生安全、检测控制、认证加密”三道防线，构建轻量化、灵活化、体系化的纵深安全防御解决方案，实现对已知威胁的有效检测，对未知威胁的主动防御。

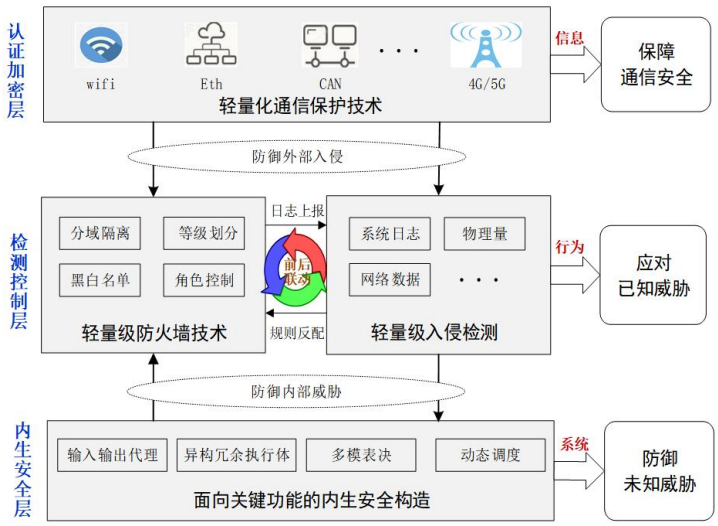

图 7 纵深安全防御解决方案

在硬件层面，飞控系统作为无人机核心控制中枢，直接决定着无人机任务执行的稳定性和可靠性。飞控系统不仅搭载多个异构处理器，例如同时采用基于 ARM 架构和 x86 架构的处理器，更配备冗余设计的传感器、电源模块及通信模块。飞控系统还集成了先进的故障诊断模块，实时监测各组件和软件模块的运行状态，通过分析传感器数据和通信信号强度等信息，及时识别潜在故障和异常，快速定位问题节点并启动修复机制，为低空设备的稳定运行筑牢防线。此外，针对飞控系统数据链通信模块等关键节点，进行拟态化改造强化安全防护，同时运用虚拟化容器技术实现轻量化部署，大幅降低对主机资源的占用，提升系统整体运行效率。

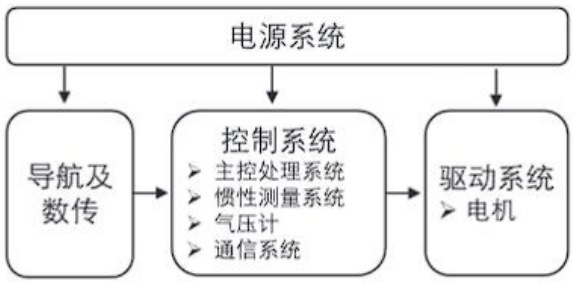

图 8 典型无人机飞控系统组成示意图

在应用层面，无人机安装多个版本的飞行控制软件和任务执行软件。这些软件在功能上等价，但在代码实现、算法逻辑和数据结构等方面存在差异。例如，不同版本的飞行控制软件可能采用不同的路径规划算法、姿态控制算法和避障算法。在无人机运行期间，一旦侦测到飞控软件的某个版本存在漏洞或遭受攻击，

系统能够实时切换至另一版本的飞行控制软件，确保飞行安全。

在通信策略上，无人机支持多种通信方式共存，包括卫星通信、蜂窝网络通信、自组网通信以及无线局域网通信等多种技术。不同的通信方式具有各自的特点和适用场景。例如在拒止环境下，无人机之间的自组网通信可以在缺乏基础设施或者基础设施被破坏的情况下保障设备之间的通信。通过多种通信方式融合，无人机能够根据不同的环境条件和任务需求，选择最适合的通信方式，确保稳定可靠通信。

2.多模态通信与数据安全

通信与数据安全是保障低空智联网稳定运行的关键要素，构建“多模通信+安全防护”体系至关重要。在通信层，卫星通信、5G/6G、自组网等多种通信链路协同发力：卫星通信以广域覆盖优势，支撑偏远地区或超视距场景通信；5G/6G凭借高带宽、低时延特性，精准满足实时业务需求；自组网则为无人机集群自主协同作业提供通信支撑。通过实时监测链路信号强度、带宽等关键指标，结合任务需求与环境感知结果，系统可以智能切换链路，确保数据传输连续稳定。

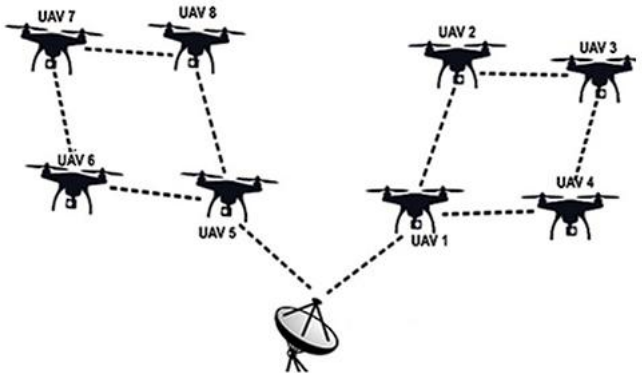

图 9 无人机自组网示意图

在数据安全防护方面，采用加密传输和数据签名认证技术，从源头保障控制指令和业务数据在传输中的完整性与真实性。同时，通过监测数据流动，识别异常流量并分析数据内容，结合威胁情报与模型预判攻击行为，实现安全风险及时预警。配套数据安全存储机制，最终形成覆盖通信与数据采集、传输、存储、处理全生命周期的安全管理闭环，为低空智联网筑牢安全屏障。

3.多源异构传感器融合定位

在低空智联网中，感知与导航技术是提升低空设备自主运行能力的核心。根据内生安全理论，构建“多传感器融合+智能算法+自定位导航”体系。基于现有多

源定位传感器，构建无人机的异构冗余定位信息集合，突破多源定位信息动态调度、多模裁决、负反馈控制及弹性融合关键技术，为低空经济中复杂场景下的无人机任务执行提供更精确和全面的环境信息。

基于内生安全动态冗余理念，多传感器融合技术融合处理激光雷达、毫米波雷达、视觉传感器、超声波传感器等异构传感器数据，构建统一的传感器数据融合模型，对各类数据进行时间同步和综合分析，最终输出更准确全面的环境信息，有效降低单一传感器失效风险。

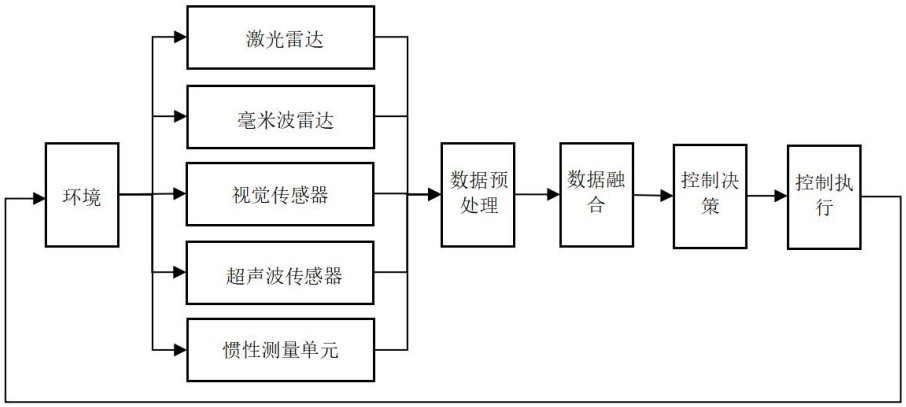

图 10 多传感器融合示意图

智能导航算法紧密结合低空环境约束（如禁飞区、交通规则等），通过学习历史数据持续优化升级路径策略。自定位技术则融合卫星定位（北斗、GPS 等）、惯性导航、视觉定位，构建数据交叉验证机制，实时校验各定位源数据。例如，当惯性导航数据出现异常突变时，系统自动调用视觉定位数据进行比对分析，剔除错误信息；在卫星定位易受干扰区域，通过惯性导航与视觉定位的融合结果，反向验证卫星定位数据可信度。凭借先进的智能导航算法与自定位技术，低空设备得以在复杂场景下实现最优路径规划与动态调整，显著提升抗干扰导航能力。

4.低空智联网络弹性组网

在网络弹性设计方面，以网络弹性理论框架为设计遵循，基于内生安全理论，构建包含主动威胁感知、实时威胁响应和自主修复重构的自适应安全防御体系，实现“预防-防御-恢复-适应”四维能力的闭环，提升低空智联网络持续服务能力。

弹性网络拓扑结构设计是低空智联网络建设中的关键一环。该结构支持网络根据环境变化与任务需求，自动调整拓扑形态，从源头规避单点故障对全网的影响。同时，部署先进的入侵检测与防御系统，对智联网络流量、行为模式展开实时监测，精准识别抵御异常流量、恶意攻击及未授权访问尝试。

故障恢复与自愈机制的建立，为低空智联网络安全运行再加砝码。当网络出现故障或遭受攻击时，系统可以迅速定位并隔离问题节点，自动触发恢复程序，借助备份链路和节点切换，恢复网络正常运行。此外，面对复杂的电磁干扰和网络负载波动，网络能够自动调整通信频率、功率和调制方式，动态分配资源、优化性能。

在弹性网络拓扑中，低空设备可以结合任务需求和临近设备状态，自主决定加入或离开网络群组，灵活调整网络结构。借助智能策略的裁决和执行体的调度，网络实现自我演进，如同生物体般自动规避攻击，持续强化环境适应能力。

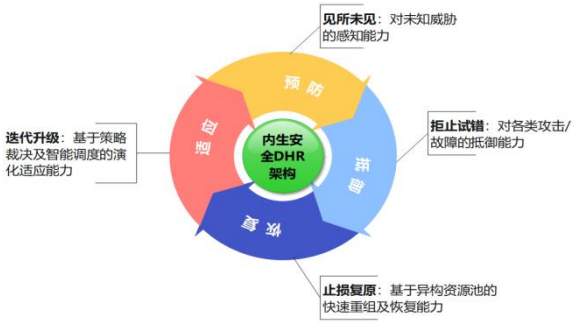

图 11 内生安全赋能网络弹性的四个目标

通过实施上述安全架构设计方案，低空智联网将能够有效应对复杂多变的威胁环境，构建起具有自主免疫能力的安全体系，为低空经济的持续健康发展提供坚实保障。

4.4.2. 密码技术

密码技术是维护低空网络空间安全的核心技术和基础支撑，在通信链路安全防护、网络空间可信身份认证、数据全生命周期管控等方面发挥重要作用，充分保障航路规划、空域审批、运行监管等业务安全。

1.可信身份认证

构建基于密码技术的低空智联网统一身份认证体系，为航路规划审批、空域资源分配、飞控指令安全下达等核心业务开展，低空智联网可信接入及通信安全，提供数字身份凭证。

- **公钥基础设施。**建立符合国家密码管理要求的低空智联网数字证书服务，为飞行器、信息系统、操作人员等提供数字证书的生成、注册、签发、存储、动态更新及撤销管理服务。
- **可信安全接入。**基于零信任安全理念，在相关设备中内置零信任密码安全组

件，飞行器在不泄露自身位置、所有者身份等敏感信息的前提下完成身份验证和安全接入，实现低空智联网的身份接入安全可信。

- **跨域身份认证。**采用基于证书的安全可信根及区块链技术，实现飞行器跨城市、跨专业应用系统、跨管理部门间身份互认。

2.通信安全防护

采用基于符合国家密码管理要求的密码算法混合加密机制对 5G-A 网络、卫星互联网和飞行器自组织网络通信链路进行端到端加密，确保飞行指令、实时监测数据等关键信息在通信传输过程中的机密性和完整性。采用 TLS/IPSec 等协议保障飞行器与业务系统间、以及业务系统与监管系统等不同平台之间通信安全。针对小微型飞行器运算资源受限特点，可采用短证书、标识公钥算法、无证书密码技术实现签名验签；利用轻量化密码算法、安全协议保证通信安全同时降低密码运算对飞行器计算资源、带宽资源的占用。

3.数据全生命周期安全

在低空智联网数据分类分级基础上，利用基于密码技术的访问控制、机密计算、数据脱敏等技术对不同安全等级和应用需求数据进行差异化的保护，保障低空智联网数据采集、传输、存储、处理、使用、销毁、备份等全生命周期的安全。

- **数据采集阶段。**基于数字签名等技术实现采集数据来源的真实性验证，确保来源真实合法；针对不同等级数据采取不同的加解密和密钥保护措施，尤其加强地理信息、人脸、用户声音等数据的安全保护。
- **数据传输阶段。**采用信源、信道多重加密措施，保证数据传输过程中的机密性、完整性。通过同态加密技术保障隐私信息在传输过程中的安全性。
- **数据存储阶段。**基于属性基加密等技术对数据的访问使用进行细粒度控制，针对不同类别、不同级别的数据执行相应机密性、完整性保护措施，做好容灾备份数据的保护。
- **数据处理阶段。**基于硬件可信技术（如机密计算）保障数据处理过程中机密性、完整性，防止未经授权访问。
- **数据流通阶段。**基于哈希计算等技术对数据流通环节的各主体进行身份鉴别，保障身份合法性；利用多方安全计算协议保护各方的数据隐私安全；利用数字签名、版权保护、安全共享交换技术实现数据确权，按需共享；采用审计

溯源技术对数据流通中流通过程操作进行审计追踪。

- **数据销毁阶段。**采用密码技术对销毁记录完整性进行保护，对销毁前数据进行随机数覆盖、加密等预处理，验证数据销毁过程的完整性，以确保数据真正被合法销毁。同时，基于密钥全生命周期管理措施，对数据加密密钥进行销毁。
- 加强数据全生命周期中的安全审计。

4.密码融合应用

加强低空智联网密码应用顶层设计，实现密码技术与低空智联网业务应用的深度融合，根据不同应用场景选配适当的密码算法及安全协议实现机制，形成安全可靠、经济适用双向闭环，为低空经济发展构建自主可控的安全基座。

- **司法存证。**基于电子签章、数字水印等技术对航路规划、空域资源审批进行司法存证，使空域管理记录具备司法效力，提升纠纷处理效率与司法保障效果。
- **关键操作记录不可篡改。**采用签名验签、区块链等技术实现禁飞区设置、飞控指令下达等关键业务操作记录进行密码技术固化，为审计溯源提供技术基础。
- **固件安全及可信启动。**基于密码技术对飞行器固件中包含合法飞行及政策技术监管业务逻辑实现可信保障，如采用数字签名、信源加密等技术加强对固件升级制作、上传、下发、存储、升级等全过程实现可信跟踪；基于密码芯片的可信验证技术，确保飞行器程序从启动到运行的完整可信，确保业务逻辑不被篡改，满足监管需求。

5.前沿安全技术

- **抗量子计算密码技术**

据国际普遍预测，2033 年前后量子计算机可具备破解现有密码算法的能力，届时现行经典密码算法及常规长度密钥面临失效风险。可通过在有条件场景中部署量子熵源生成量子密钥、应用量子密钥分发技术，显著提升密钥安全性；同时，推动现行国密算法与抗量子密码算法在低空智联网领域的兼容应用和平滑升级。为低空智联网在数据传输、设备认证等环节筑牢安全防线，还为后量子时代密码迁移技术路线奠定坚实基础，确保低空智联网在量子计算时代持续安全、稳定运

行。

量子通信是指利用量子比特作为信息载体进行信息交互的通信技术，可在确保信息安全等方面突破经典信息技术的极限。量子密钥分发（QKD）是量子通信的典型应用之一，可以让空间分开的用户共享无法破解的密钥，是抗量子计算攻击的主要技术路线之一。QKD 已率先进入实用化阶段，其安全性由量子力学的不确定性原理、量子不可克隆定理和量子不可再分的性质来保证，并已得到严格证明。我国量子保密通信技术及产业化应用已经具有国际先进水平。经过多年的技术积累和项目实践，我国已经形成了以量子密钥分发（QKD）技术为核心的较为完整的量子保密通信产业链。

由于无人机与管理平台之间的数据传输过程中存在窃听、身份伪造等风险，通过量子加密技术与无人机的技术融合，增强多类型终端及管理平台之间数据传输防护能力，满足设备、用户的身份认证、数据传输安全等需求，防止非授权访问、数据窃取篡改，解决现场数据采集、视频直播、控制指令下达等场景下的数据安全需求，通过量子保密通信技术在无人机中的应用，确保无人机整体系统的安全运行。

- **基于统一标识的认证与保密通信（UMIAN）技术**

统一多域标识认证与网络保密通信（Unified Multi-domain Identifier Authentication & Network-secure- communication，UMIAN），也称由密安。其底层是统一标识下的无证书公钥认证技术（UMIA），而 UMIAN 是在认证的同时，进行密钥协商，建立安全的通信信道，实现实时保密通信，即集成了“统一标识下的无证书公钥管理+跨域标识认证+实时保密通信”。UMIAN 在密码上基于国密标准算法，在通信上仅基于 IP 协议，适用于多种裁减版或嵌入式物联网终端系统。由于任一终端可快速计算出另一终端的公钥，无需公钥证书，故终端公、私钥可自主管理，不依赖第三方 CA，成本低、效率高，跨域认证时延小。在多层次多域结构下的海量物联网终端低时延标识认证和实时保密通信上具有显著优势，尤其适用于网联无人机、车联网等场景。

UMIAN 技术在顶层统一规划、统一标识、统一参数、统一部署、统一监管；在基层域进行实际的终端管理，密钥自主分发和更新，且各域独立，分域而治，无需证书却又能跨域互认，不依赖于其它网络安全协议又能实时保密通信，实现

事事认证，端端保密，形成一种统域分治的新型零信任架构。

4.4.3. 人工智能安全

1.数据安全技术

在低空领域，人工智能广泛应用于飞行控制、目标识别、路径规划等关键环节，其运行高度依赖高质量数据的支持与算法模型的稳定性。然而，在人工智能应用过程中，数据易遭受泄露、污染、投毒等安全威胁，导致模型性能退化甚至行为异常，严重影响低空飞行器的运行安全。因此，保障数据安全，确保数据的质量和可靠性，已成为提升人工智能技术安全性的重要任务。

首先，数据隐私保护是确保人工智能系统安全的关键措施之一。在训练数据的采集、存储、使用、处理、传输及删除等环节中，必须严格遵守相关法律法规，保障用户的控制权、知情权和选择权。通过采用联邦学习和同态加密等隐私保护技术，人工智能系统可以在不损害个人隐私的前提下对加密数据进行处理，从而有效规避数据泄露风险。

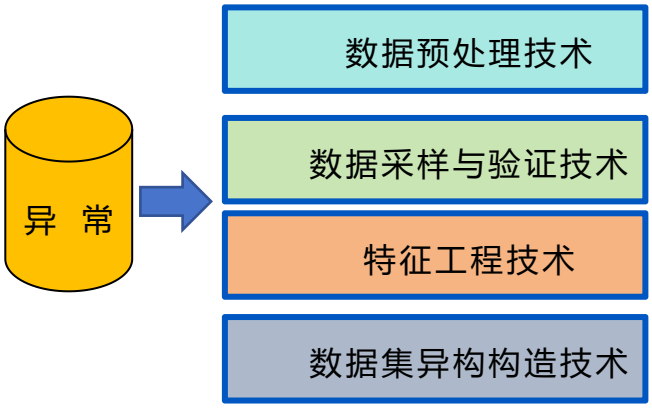

图 12 数据安全技术思路

为了消除潜在的质量问题并降低对人工智能系统安全的影响，数据预处理、数据采样与验证、特征工程等环节的优化至关重要。在数据预处理阶段，异常值检测是首要任务，利用统计方法、聚类分析或深度学习技术来识别并排除可能含有恶意样本的异常数据点。在数据采样和验证方面，分层采样有助于确保每个类别的数据平衡，防止通过数据注入进行攻击，同时通过交叉验证来评估模型的泛化能力，从而减少恶意样本的影响。

特征工程和数据集异构构造也是提升数据安全性的重要技术手段。特征工程通过提取语法、图像纹理等特征来帮助识别异常样本，同时引入统计特征如平均

值和方差，可以进一步提高模型的抗干扰能力。数据集异构则通过内生安全拟态化构造，使得模型在面对对抗样本攻击时展现出更强的鲁棒性。通过数据增强技术引入对抗样本、差异性样本和扰动样本，可以有效提高多模型的鲁棒性，降低数据被投毒的风险。

2.模型安全技术

为保障人工智能应用的安全，除了数据本身的防护之外，还可以从人工智能模型本身入手，采取模型结构改造和模型训练改造方式进行内生安全加固。

模型结构改造模块通过修改模型的内部结构，得到不同的网络模型并实现集成模型具有更好的内生安全效应。其中可以使用的方法包括但不限于：①内生安全网络结构优化技术，通过修改模型内部结构如层数的深度与宽度，层的类型与结构构件不同架构的网络模型。使得不同宽度与深度能够达成最佳的异构效果。②神经网络模型异构裁剪技术，通过对进行模型的针对性裁剪，直接从整体上衍生不同架构的模型，利用裁剪获得不同结构的模型。裁剪过程中的选择可以基于特定的度量方法来判定裁剪对象，例如权重值大小、激活值大小等。③网络连接方式异构调整技术，通过调整模型层与层直接的连接关系，得到不同的异构子模型，如利用随机或定向的 dropout 来使得不同模型对产生对数据特征的差异化反馈。

训练改造可以根据任务目标的需求选择不同的训练方法，以达到对目标模型的改造目的。针对于训练的优化已经被证实是一种可以增强模型安全性的有效策略。通过调整模型在训练过程中的方式和策略，使得模型发生差异最终得到不同的异构模型。使用不同的训练方法来获得具有足够差异性的模型，以提高整个系统的鲁棒性和抗攻击能力，其中使用的技术包括但是不限于：①正则化训练技术，该技术通过添加不同的反馈正则项调节模型的训练方向，以实现模型的差异化。通过正则化方法人为改变了模型对不同数据特征的关注程度并限制模型行为，从而使得不同的模型产生异构。②异构化参数调整技术，通过修改训练参数以调控每一训练轮次的训练结果。通过调整学习率、损失函数等参数，可以影响每一轮训练的结果，进而产生差异化的模型。③集成训练技术与对比学习技术。在训练过程中，并行或串行训练多个模型，并在训练过程中通过让多个模型之间互相学习、互相制约彼此远离，达成获得多个异构模型的目的。④预训练模型异构化微

调技术。针对于复杂任务与大模型，使用异构的数据集与辅助模型进行预训练模型的微调，服务于不同的下游任务。

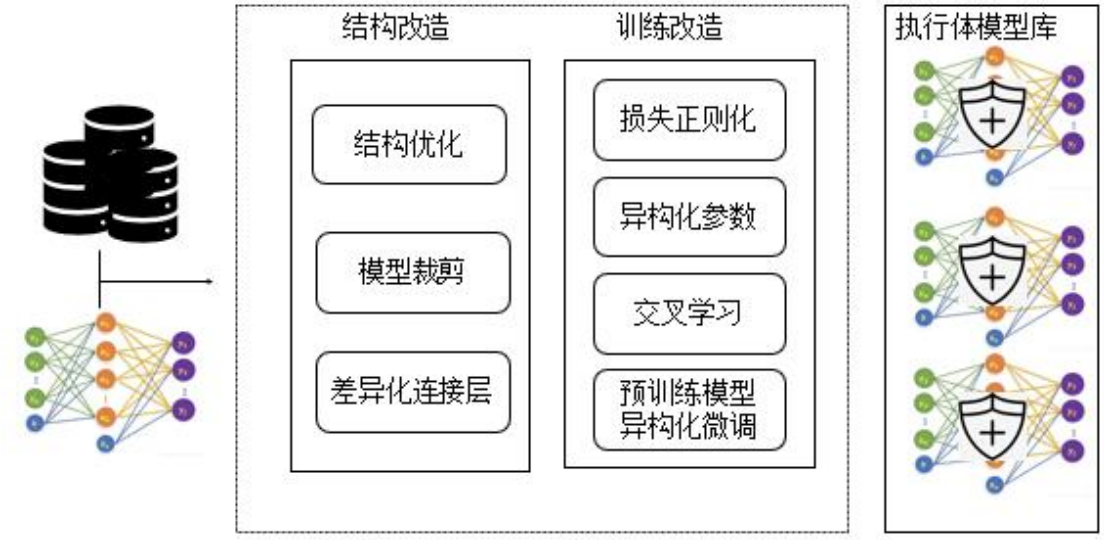

图 13 模型安全技术思路

5. 总结与展望

随着低空经济的快速发展，低空智能网联网络与数据安全的重要性日益凸显。面对潜在的安全威胁和挑战，构建完善的安全标准体系已成为行业可持续发展的关键。本白皮书从政策分析、标准体系建设、全生命周期安全体系等多个角度，对低空智能网联网络与数据安全的现状和发展方向进行了系统性分析，并提出了针对性的建设建议。

标准体系的建立是推动低空智能网联网络与数据安全治理的核心基础。当前，国际国内标准体系仍处于初步发展阶段，缺乏统一规范，导致产业协同度不足，安全风险难以系统性防控。因此，亟需加快制定覆盖数据安全、通信安全、基础设施安全、无人机整机及分系统安全等多个维度的标准体系，并通过标准的落地实施推动行业安全能力的提升。

基于标准体系，建立低空智能网联的全生命周期安全保障体系同样至关重要。从安全检测认证、运行监测到安全管理和防护，各环节均需形成闭环管理，确保低空智能网联的安全可控。同时，借助密码技术、人工智能安全防护、内生安全等关键技术，进一步提升低空智能网联的安全韧性，防范潜在的网络攻击、数据泄露及供应链安全风险。

未来，低空智能网联网络与数据安全体系的构建需要政府、行业组织、企业和科研机构的协同推进。法规体系和安全监管机制的完善将为行业发展提供方向指引，标准化建设与合规管理的强化有助于提升企业自主安全技术能力，而关键核心技术的持续攻关将为行业提供稳定的安全创新支撑。

本白皮书呼吁行业各方积极参与低空智能网联网络与数据安全体系建设，共同推进标准化工作，建立健全全生命周期安全管理机制，形成安全、可持续的低空经济发展生态。在未来的发展进程中，只有通过协同创新与系统治理，才能真正实现低空经济的高质量、安全发展，为全球低空产业的繁荣奠定坚实基础。

附件：缩略语

缩略语	英文全称	中文名称
eVTOL	electric Vertical Takeoff and Landing	电动垂直起降飞行器
BLE	Bluetooth Low Energy	蓝牙低能耗
UWB	Ultra Wide Band	超宽带
CPS	Cyber-Physical Systems	信息物理系统
DHR	Dynamic Heterogeneous Redundancy	动态异构冗余
GPS	Global Positioning System	全球定位系统
UMIAN	Unified Multi-domain Identifier Authentication & Network-secure-communication	统一多域标识认证与网络保密通信
CA	Certificate Authority	认证机构
IP	Internet Protocol	互联网协议
IPsec	Internet Protocol Security	互联网安全协议
TLS	Transport Layer Security	传输层安全性