2023

智胜空天·安全护航

无人机现状观察及安全分析报告

NSFOCUS

CEPREI 中国赛宝实验室（工业和信息化部电子第五研究所）

关于绿盟科技

绿盟科技集团股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。公司于 2014 年 1 月 29 日在深圳证券交易所创业板上市，证券代码：300369。绿盟科技在国内设有 50 余个分支机构，为政府、金融、运营商、能源、交通、科教文卫等行业用户与各类型企业用户，提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。公司在美国硅谷、日本东京、英国伦敦、新加坡及巴西圣保罗设立海外子公司和办事处，深入开展全球业务，打造全球网络安全行业的中国品牌。

格物实验室
NSFOCUS GEWU LAB

绿盟科技格物实验室专注于工业互联网、物联网和车联网三大业务场景的安全研究。实验室以“格物致知”的问学态度，致力于以智能设备为中心的漏洞挖掘和安全分析，提供基于业务场景的安全解决方案。积极与各方共建万物互联的安全生态，为企业和社会的数字化转型安全护航。

中国赛宝实验室
（工业和信息化部电子第五研究所）
CEPREI

工业和信息化部电子第五研究所（国家无人机系统质量监督检验中心，智能制造装备通用质量技术及应用工业和信息化部重点实验室），1955 年成立，又名中国电子产品可靠性与环境试验研究所、中国赛宝实验室，作为中国最早专业从事可靠性研究与服务的专业机构，开创了中国相关研究领域的诸多先河。

电子五所作为工业和信息化部直属单位，受部的委托和授权，为部的行业管理和地方政府提供技术支撑，代表中国进行国际技术交流、标准和法规的制订；作为国家级科研院所，为国家、政府等相关单位提供专业支持；作为生产性服务业公共平台，为企业提供强有力的质量技术服务，服务领域涉及航空、航天、兵器、船舶、电子、机械、通信、交通、软件、能源、化工等众多行业。业务范围涵盖广泛，包括：体系认证、产品检验、计量校准、元器件检测、失效分析与 DPA、工艺与材料、环保技术、可靠性与环境试验、软件测评、信息安全、信息化监理、仪器设备与工具软件、标准与政策研究、技术培训等。

版权声明

前言

无人机是新一代电子信息技术与航空工业技术深度融合的产物，是自动化、智能化、网络化的重要载体，也是全球战略性新兴科技的热门发展方向之一。现代无人机综合了自动驾驶、人工智能、数据分析等高新技术，无论是在辅助交通、商业运作、物流运输，还是在航拍摄影、农业植保、深空探测，都展现出巨大的应用价值和发展潜力，受到了世界各国的重视。结合当前无人机的发展趋势，攻克技术难点，扩展服务领域，正成为制造强国竞争的新焦点。

作为航空产业中冉冉升起的新星，无人机产业不仅在社会生产生活中发挥了越来越重要的作用，更成为了新的经济增长点。其中，无人机安全既是保障产业高质量发展的基础，又是未来领域能力建设的刚性要求。目前，国内外纷纷采取各种措施以支持行业的蓬勃发展。在国际上，主要以欧美国家主导，包括：出台《欧盟委员会第 2019/945 号授权条例—关于无人驾驶航空器系统和无人驾驶航空器系统第三国运营人》、《美国 2016 年联邦航空管理局扩张、安全和安保法》等国家层面的政策法规；制定 ISO/IEC WD 22460、ISO/DIS 21384 等行业层面的技术标准；组织 ICUAS 等专题研讨会议；搭建 AUVSI、ArduPilot 等开源平台等，在多方的积极推动下，无人机产业呈现出良性发展态势。在国内，从法律层面的《民用航空法》，到行政法规层面的《无人驾驶航空器飞行管理暂行条例（意见征求稿）》，再到民航局出台的管理办法及运行规定《民用无人机系统空中交通管理办法》、《特定类无人机试运行管理规程（暂行）》，同样也为无人机产业发展注入了活力、明确了方向、提供了依据。

本白皮书从无人机的发展历程出发，系统分析了行业现状与领域相关政策，在梳理无人机安全风险和常见攻击面的基础上，总结了国内外无人机安全研究动态，提出了相关安全建议和加固防范措施，并展望了未来发展方向。在编写过程中，本白皮书集众人之智、采众家之长，是对新形势下无人机技术演进和安全实施的提炼和总结，希望能够为行业内相关人员提供参考。通过社会多方共同努力，为我国无人机的发展贡献力量。

工业和信息化部电子第五研究所

（国家无人机系统质量监督检验中心）

（智能制造装备通用质量技术及应用工业和信息化部重点实验室）

DRONE

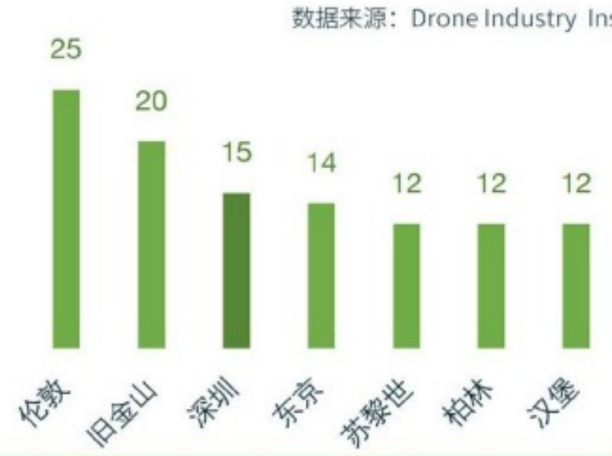
2022 无人机市场地图

1076 家无人机相关厂商提供各类硬件、软件及服务，近一半的厂商是无人机硬件制造商，其次是 404 家无人机服务提供商，占比最少的厂商是无人机软件制造商。

大多数厂商的总部位于**欧洲和北美**。尽管亚洲是全球领先的无人机市场区域，但由于只由少数公司主导，因此亚洲的厂商只占到了11.6%。

拥有超过 10 家厂商的城市依次是：伦敦、旧金山、深圳、东京等，虽然亚洲厂商总数低于欧洲和北美，但中国和日本的城市位于顶级枢纽之列这一事实充分证明了**亚洲市场的实力**

数据来源：Drone Industry Insights

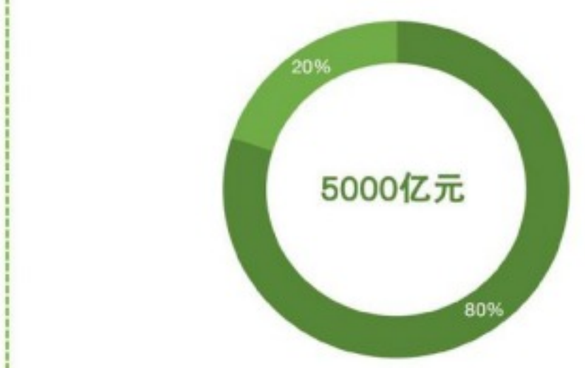


2022 无人机市场现状

2021年全球民用无人机市场规模超过**1600亿元**，同比增长**61.6%**，其中工业级无人机占 **60%** 左右。随着下游应用领域的不断扩大，未来将继续保持增长，预计2025年将达到**5000亿元**，工业级无人机市场规模占比将超过**80%**。

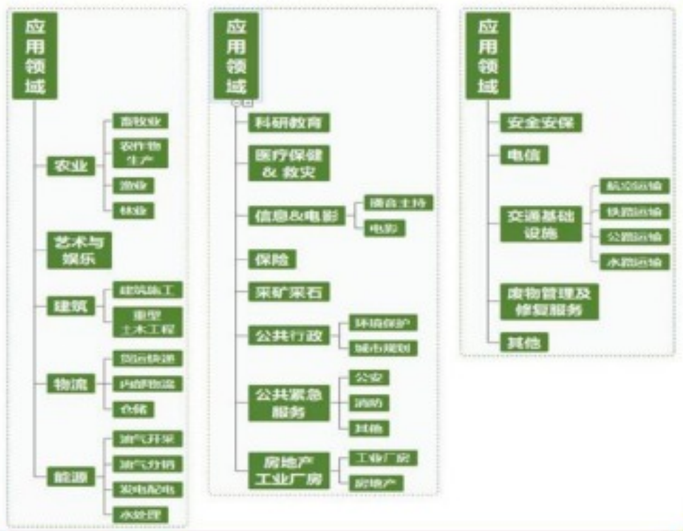
2021 年全球军用无人机市场规模为 **102.5 亿美元**，并预计将从 2022 年的 **117.3 亿美元**增长到 2029 年的 **308.6 亿美元**，预测期内的复合年增长率为 **14.82%** 。

数据来源：通用航空产业发展白皮书（2022）
Fortune Business Insights



产业链长

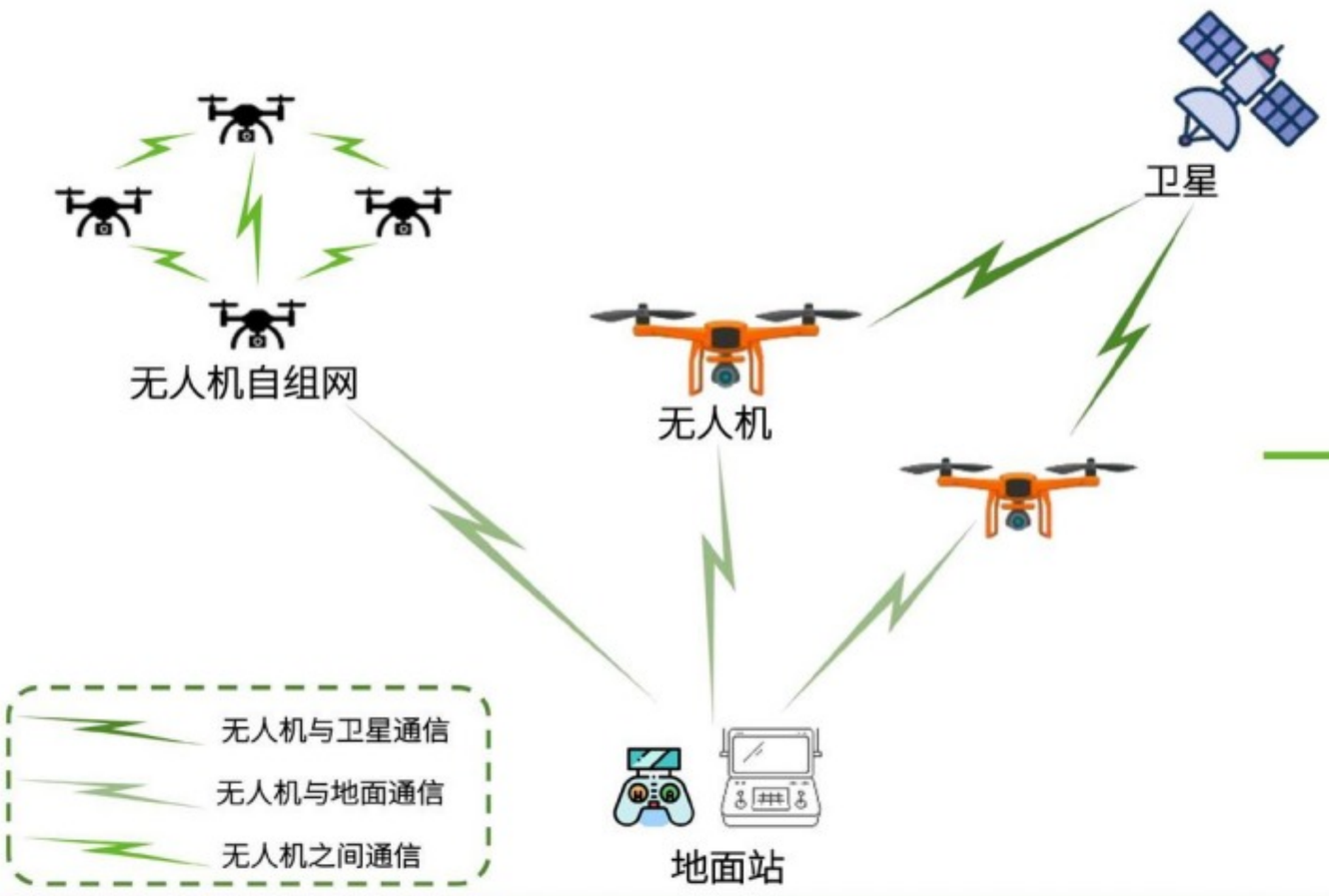
应用领域广



政策法规完善中

当前，还没有一个全球级的无人机管理框架，不过各国也都在制定并不断完善无人机相关的法规和标准，努力在**确保安全**和**推动发展**间寻找到一个平衡点。

无人机系统安全现状



通信链路
主要有卫星通信、电台通信、基站通信、Wi-Fi通信

飞控系统
核心部分，包括自动飞行控制系统、人工飞行控制系统和飞行控制计算机等

传感器
通常包括加速度计、陀螺仪、罗盘和气压计等

地面站
通常由遥控装置、显示器，电源系统，电台等设备组成

— 攻击应用场景 —

近源攻击

- 2022年，两架通过改装的无人机通过Wi-Fi入侵某金融公司内部网络；
- 《2020年网络威胁趋势展望》报告称，无人机可能成为主要的网络安全威胁，建议企业机构保护建筑物周围的空域。

情报获取

- 2022年，乌克兰对新型电子情报无人机进行二次试飞，基于无人机的电子情报系统将为军方打开一个全新的机会；
- 2022年8月，英国和挪威联手向乌克兰提供850架“黑蜂”微型侦察无人机。

武装攻击

- 2022年1月，阿布扎比无人机袭击导致油箱爆炸造成三人死亡；
- 2022年11月，阿曼海岸附近的一艘油轮遭携带炸弹的无人机袭击；
- 2019 年 9月，武装组组织袭击沙特阿拉伯境内炼油厂和油田，触发炼油厂大火。

实体战争

- 近年来军用无人机装备频繁出现在局部地区战场；
- 2022年2月爆发的俄乌战争战报中，屡见无人机的身影。俄主要参战无人机包括：猎户座、前哨-R等，乌参战无人机包括：“旗手”TB2、UJ-22“天空”等。

— 安全研究动态 —

无人机劫持攻击

- 2022年Black Hat大会，某议题展示了对无人机的劫持攻击；
- 研究员通过研究无人机的信号，分析出无人机的跳频规律以及无线协议格式，实现了一个伪造的地面控制器来劫持空中飞行的无人机。

针对无人机的模糊测试

- 乔治梅森大学的研究人员针对消费级无人机使用模糊测试方法进行安全评估；
- 发送变异数据报文到无人机的FTP等端口。测试过程中，监测到无人机的GPS性能、响应速度、传感器准确性均受到影响。

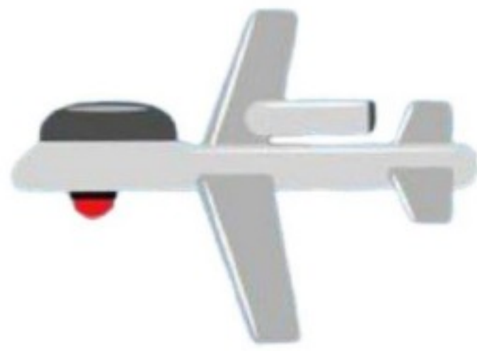
无人机渗透测试框架

- 一款专为无人机黑客量身定制，且类似Metasploit 的框架在2019年Black Hat 欧洲会议上被公开；
- 该无人机渗透测试框架名为DroneSploit，旨在发现无人机安全漏洞。

无人机攻击智能电视

- 2019 Defcon 大会上，某议题展示了如何利用无人机接管现代智能电视；
- 对于一些物理隔离或者有严格数据风险管控的机构来说，无人机是一个潜在的数据漏点。

无人机系统攻击面



固件

- **攻击面：**固件业务逻辑问题、升级机制漏洞、暴露服务和端口等
- **加固方法：**

1、通过Anti-rollback机制防止无人机回滚到有漏洞的版本；

2、对固件本身进行保护，用数字签名技术来验证固件的真实性，通过加密技术来保护其中的数据；

3、限制硬件调试接口SWD、JTAG的滥用，服务、端口最小化。

软件服务

- **攻击面：**飞控程序、FTP、SSH、ADB、TELNET、DHCP 等
- **加固方法：**

1、开源组件尽量使用最新版本以缓解 Nday 漏洞的利用；

2、关键端口服务尽量不直接对外暴露，特别是调试类服务；

3、核心飞行服务进程可考虑使用内存安全语言进行重写。

无线通信

- **攻击面：**无线信号干扰、嗅探、欺骗
- **加固方法：**

1、使用长度较长的跳频序列；

2、在上层设计更加安全的传输协议，包括使用数据加密以及签名技术；

3、分别从信号处理层面、信息处理层面检测欺骗，从协议设计上防止无线信号被简单的重放。

GPS

- **攻击面：**GPS 欺骗
- **加固方法：**

1、使用多种不同的定位技术校验GPS信号的准确性；

2、将依靠无人机自身传感器确定位置的自主定位技术作为备用措施；

3、当系统发现GPS信号存在异常时，自动切换到备用定位方式。

Wi-Fi

- **攻击面：**Wi-Fi 协议栈漏洞、Wi-Fi Deauth 攻击、Wi-Fi 密码可预测
- **加固方法：**

1、厂商做好漏洞管理，及时推送补丁对射频芯片以及无人机本身进行缓解；

2、使用增强型WPA或WPA2加密；

3、将Wi-Fi密码的设置权交给用户，并保证密码的强度。

应用协议

- **攻击面：**破坏Mavlink协议的保密性、完整性、可用性和真实性
- **加固方法：**

在开源的Mavlink基础上，加入协议加密，数据签名，访问认证的部分。

即使攻击者能攻破物理层协议，由于上层协议是加密签名的，依然可以保证无人机系统的通信安全。

传感器

- **攻击面：**陀螺仪、雷达、超声波、摄像头CMOS
- **加固方法：**

1、减少传感器对外部信号的暴露；

2、在不影响正常信号的情况下衰减恶意信号；

3、增加传感器的随机性；

4、改进组件质量；

5、融合多个或多种传感器在不同空间、时间或频率上的测量结果。

无人机未来发展趋势

技术发展方向

● 电池技术

电池是直接制约无人机发展与应用的关键因素，因此亟待大幅度提高电池的能量和功率密度以及安全性。

● 通信系统

公共无线电通信链路，抗干扰能力弱，尤其是同频干扰无法避免。民用无人机尤其消费级无人机受影响最大。

● 定位导航

无人机的定位功能是无人机自主导航的前提。未来有更多应用场景需要高精度、高可靠性、高抗干扰性的无人机，多种导航技术结合将是未来发展的方向。

● 避障技术

避障技术对确保公共安全至关重要，现有的解决方案仍处于探索阶段。主流的无人机避障技术有：超声波避障、红外避障、视觉避障和激光避障。

● 自动飞行

该技术的发展将在矿场采集、管道运输监控和建筑相关的场景中发挥极大作用。

● AI 算法应用

使用基于AI的路径规划和机器视觉技术，使无人机更加智能。

● 网联无人机

网联无人机采用多无人机协同工作的方式，能够实现更加高效和精确的作业。

反无人机

● 反无人机解决方案和措施

军民领域对反无人机的需求日益增加，反无人机解决方案可分为三种类型：检测、非交互措施和拦截；

检测：使用声学、热学、雷达、视觉等传感器或无线电频率 (RF) 发现无人机；

非交互措施：发出警报、关闭Wi-Fi、使用烟雾弹、干扰无人机摄像头等；

拦截：激光、捕捉导弹、捕捉网、射频/ GNSS干扰等；

● 发展方向

更具有针对性：对特定型号的无人机进行有针对性的信号压制及欺骗；

更加智能化：自动化发现、识别、跟踪无人机目标。

无人机防护

● 军用无人机

隐身化是目前军用无人机发展的重要方向之一，是高端无人机的重要技术瓶颈之一。隐身技术是对目标特征信号进行有效控制和抑制的技术，主要包括雷达隐身、红外隐身等。

● 民用无人机

防破解是目前民用无人机尤其消费级无人机防护的重点之一。遭破解后的无人机可绕过厂商本身的各种限制，尤其是绕过禁飞区限制。因此需要厂商及时对软件、固件存在的已知问题进行更新，并在未来从硬件层面使用诸如安全芯片等技术来保证无人机的安全。

NSFOCUS

中国赛宝实验室
CEPREI （工业和信息化部电子第五研究所）

CONTENTS

01

无人机发展现状

1.1 无人机概述

无人机最早出现于 20 世纪初期，它的出现与第一次世界大战有关，用于军事用途，当时指不需要驾驶员登机驾驶，而用无线电操纵的小型飞机。在经历了近一个世纪的发展后，正在军事和民用的广阔领域发挥日益重要、甚至是不可替代的作用。

随着技术的发展进步，无人机的名称也发生着变化，光典型的英文缩写就有 UA、UAV、UAS、RPA 等，中文名称则有无人机、遥控驾驶航空器、无人驾驶航空器等。中英文名的字面不同，带来的意义及内涵也略有不同，下面对不同中英文名称做简要说明，也借此进一步明确本文中无人机所指代的范围。根据 GB/T 38152-2019 《无人驾驶航空器系统术语》和 GB/T 41300-2022 《民用无人机唯一产品识别码》中的定义：

表 1.1 名称定义

无人驾驶航空器	UA，unmanned aircraft UAV，unmanned aerial vehicle	由遥控设备或自备程序控制装置操纵，机上无人驾驶的航空器 注 1：无人驾驶航空器包括遥控航空器、自主航空器和模型航空器等 注 2：遥控航空器和自主航空器统称无人机。
无人驾驶航空器系统	UAS，unmanned aircraft system	以无人驾驶航空器为主体，配有相关的遥控站、所需的指挥和控制链路以及设计规定的任何其他部件，能完成特定任务的一组设备。
遥控驾驶航空器	RPA，remotely piloted aircraft	由遥控站 (台) 操纵的无人驾驶航空器。
遥控驾驶航空器系统	RPAS，remotely piloted aircraft system	以遥控驾驶航空器为主体，配有相关的遥控站、所需的指挥和控制链路以及型号设计规定的任何其他部件，能完成特定任务的一组设备。
民用无人机	civil drone；civil unmanned aerial vehicle	从事民用领域飞行活动的遥控航空器和 / 或自主航空器。

本文中，无人机指遥控航空器和自主航空器的统称。

1.2 无人机分类

通常，无人机可按用途、平台构型、运行风险大小等方法进行分类。

1.2.1 无人机按照用途分类

从用途层面来看，无人机可分为军用无人机与民用无人机两大类。

军用无人机对于灵敏度、飞行高度、飞行速度、智能化等性能有着更高的要求，是技术水平最高的无人机，主要包括侦察、靶机、诱饵、电子干扰、战斗攻击和察打一体无人机等机型，全世界拥有军用无人机的国家数目从 2010 年的 60 个激增至 2020 年的 102 个。大型

无人机可以用来执行定点打击任务。对于情报和侦察任务，微型无人机的固有隐身性，模仿鸟类或昆虫，提供了秘密监视的潜力，并使它们难以被击落。

民用无人机一般又分为消费级无人机和工业级无人机，消费级无人机主要用于影视航拍和消费娱乐，着重拍摄功能和可操作性；工业无人机注重经济效益，追求巡航速度、续航能力等性能的平衡，对无人机的专业化应用要求高，工业无人机通过搭载不同的任务载荷实现多样化的功能，主要应用于农林植保、安防治安、科学探测以及物流运输等各行业各领域。

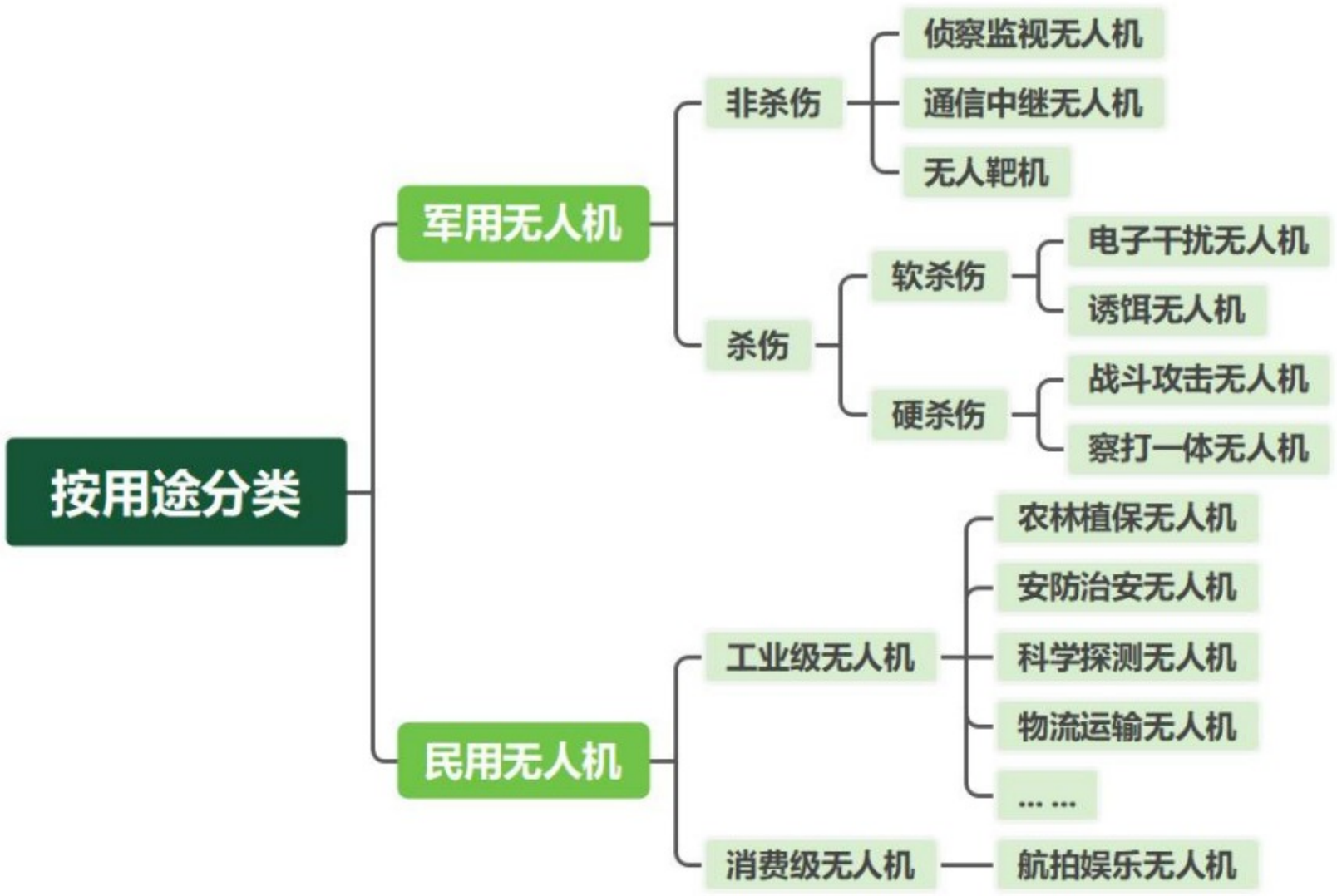


图 1.1　无人机按用途分类

1.2.2　无人机按照平台构型分类

按照不同平台构型来分类，无人机主要有固定翼无人机、多旋翼无人机和无人直升机三大平台，其它小种类无人机平台还包括伞翼无人机、扑翼无人机和无人飞艇等。

固定翼无人机看起来比较像常规飞机，是军用和部分民用无人机的主流平台，具有飞行速度快、载荷大、续航时间长等优点，因此在对航程、升限等有要求的领域应用更广泛，譬如农业植保、军事侦察、打击等。但是，固定翼无人机也有其局限性，那就是起降要求高，不具备垂直起飞能力，且不能悬停。

市面上的消费级无人机大多是多旋翼机型，常见为四旋翼，也有六旋翼甚至八旋翼机型，多旋翼式无人机的优势在于拥有垂直起降及精准悬停功能，同时体积小、操作灵活且成本低。

对环境要求很低，也可以用于很多工业领域，譬如管道检修、仓库清点等。但是由于大多数多旋翼无人机器只有不到一个小时的飞行时间，续航时间短、作业面积小、速度慢，使其在应用时受到一定的限制。

无人直升机的外形看起来和传统直升机很像，可以原地垂直起飞和悬停。相比于固定翼无人机在使用上更灵活机动，相比于多旋翼小型无人机，又能够承担更大的载荷，但因技术复杂度高，使用和维护成本也比较高。近年来，经常出现在军事侦察、海事巡逻，以及应急救援等场景中。

图 1.2　无人机按飞行平台构型分类

1.2.3　无人机按照运行风险大小分类

根据运行风险大小，民用无人机又可分为微型、轻型、小型、中型、大型。

图 1.3　民用无人机按运行风险大小分类

02

无人机市场现状

2.1　无人机供应链

无人机市场调研机构 Drone Industry Insights 在 10 月发布了 2022 年无人机市场地图，截止发布日期，共统计到全球 1076 家无人机相关的厂商，这些厂商提供各类硬件、软件及服务，各细分市场及对应厂商详见图 2.1[1]。

图 2.1　2022 年无人机市场地图

该无人机市场地图虽然并未能将世界上所有的无人机公司都囊括其中，但它突出了全球无人机行业的多样性，并展示在市场各个领域的领先无人机厂商。

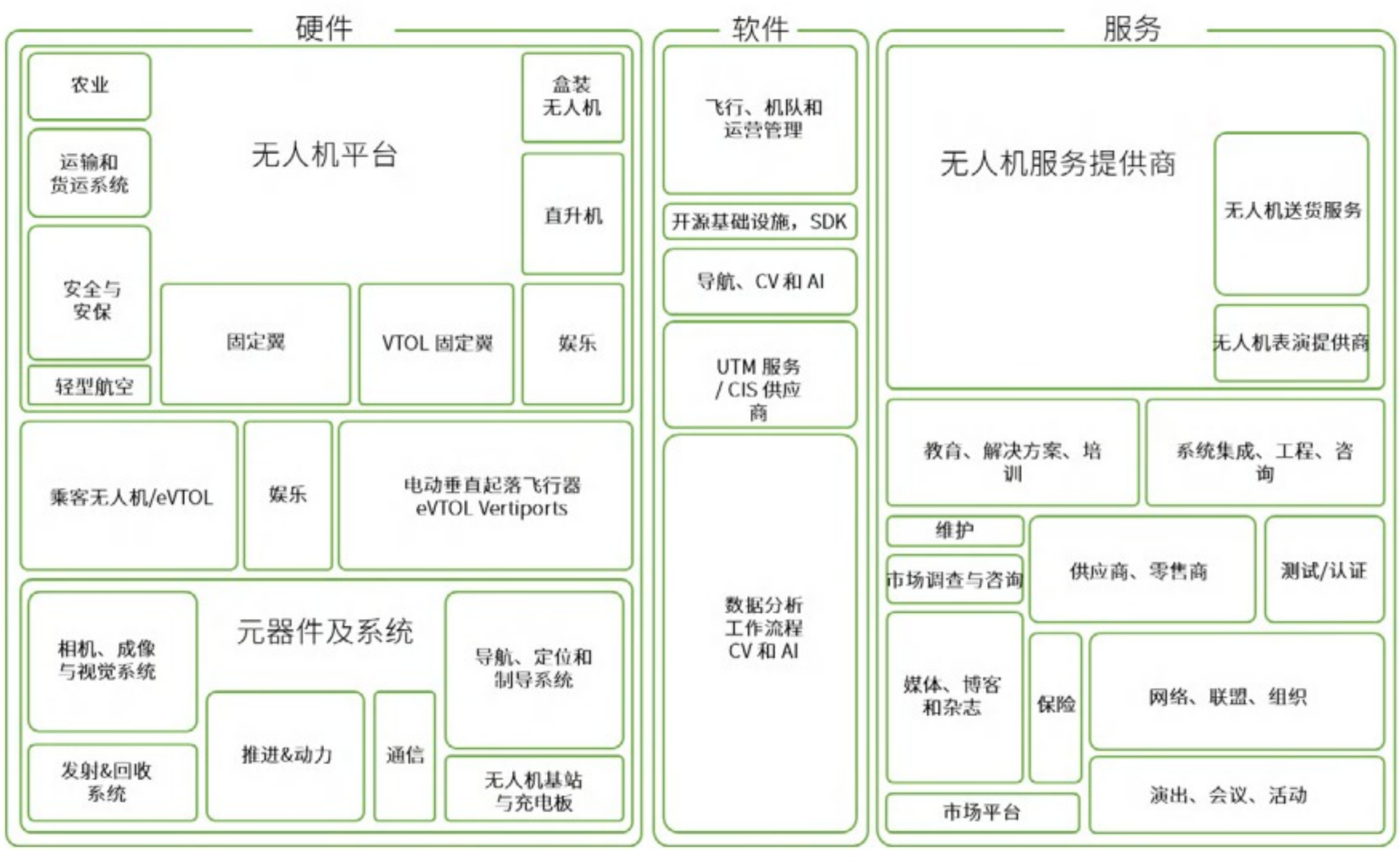


图 2.2　无人机厂商类型分区图

在所有被统计对象中，有将近一半的厂商都是无人机硬件制造商 (49.5%)，其次是 404 家无人机服务提供商 (37.6%)，占比最少的是无人机软件制造商 (12.9%)。

从地理区域上分析这些厂商可以发现，大多数厂商的总部位于欧洲 (40.3%) 和北美 (35.8%)。尽管亚洲是全球领先的无人机市场区域，但是由于只由少数公司主导，因此亚洲的厂商只占到了 11.6%。

从国家和城市层面来看，美国拥有最多的公司，共有 337 家（31.3%）。其次是英国（7.3%）、德国（6.6%）、法国（4.7%）和瑞士（4.7%）。拥有超过 10 家厂商的城市依次是：伦敦（25 家）、旧金山（20 家）、深圳（15 家）、东京（14 家）、苏黎世（12 家）、柏林（12 家）和汉堡（12 家）。虽然亚洲厂商总数低于欧洲和北美，但中国和日本的城市位于顶级枢纽之列这一事实充分证明了亚洲市场的实力。

此外，该市场地图也充分体现了无人机系统的复杂性，那么整个产业必然拥有较长的产业链。民用无人机产业上游企业主要提供关键原材料以及核心零部件的加工制造，其中关键原材料有金属材料和复合材料两大类，包括钛合金、铝合金、陶瓷基等特殊材料；零部件制造环节，一般包括芯片、电池、电机、发动机、机身结构件、陀螺仪、金属零件和复合零件等[2]。

产业链中游无人机各分系统、任务载荷和系统集成是无人机制造的核心部分。其中分系统又主要包括飞行平台系统和地面系统，飞行平台覆盖飞控、导航、动力、通信、图传和电气等；地面系统包含遥控检测、监控系统、数据处理、起降系统以及辅助设备等；任务载荷环节，一般包含航摄相机、激光雷达、高光谱成像仪等专业任务载荷。系统集成商多指只包含无人机系统集成，不涉及服务提供的厂商，但目前多数企业这两部分均已涉及，但还存在部分企业以提供服务为主，服务包括无人机飞行数据整合、技术支持、飞行培训、租赁、维修等。

下游为无人机应用领域，包括国防安保、农林植保、航空拍摄、物流运输、城市规划、环境监测、巡检应急等。

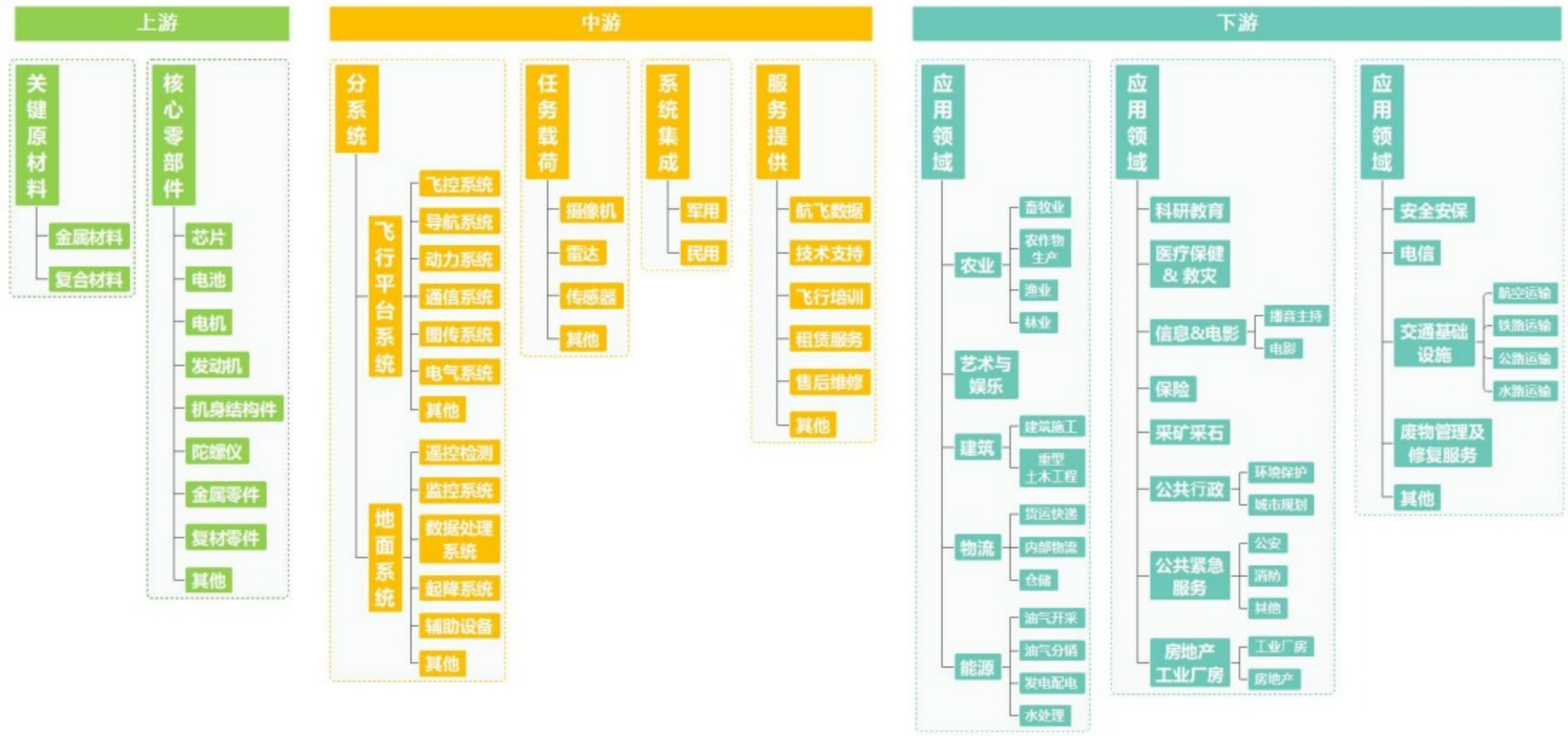


图 2.3　无人机产业链

无人机产业链上游原材料代表性企业主要包括炼石航空、宝钛股份、中国航天、泰和新材、会通股份、银禧科技等企业；无人机芯片厂家：Qualcomm（高通）、NXP（恩智浦半导体）、Intel（英特尔）、ST（意法半导体）、大唐电信联芯、TI（德州仪器）、SamSung（三星）、Atmel（爱特梅尔）、Nuvoton（新唐）、XMOS、NVIDIA（英伟达）、瑞芯微等；电池供应商：格瑞普、欣旺达、正方科技等；机体结构件代表性企业：中信海直、博云新材等；核心部件供应商：InvenSense（被日本 TDK 收购，研发、销售运动跟踪装置中的微机电系统陀螺仪）、MicroPilot（为无人机系统生产自动驾驶仪）、PolarPro（为运动相机专业生产过滤器等配件）、uAvionix（利用硬件产品识别、控制、协调空中、地面的所有飞行物）等[3]。

无人机产业链中游飞控系统代表性企业包括威海广泰、零度智控等；导航通信系统代表性企业：易瓦特、中海达、观典防务等；动力系统代表性企业：欣旺达、德赛电池、鹏辉能源、格瑞普、微光股份等；任务载荷系统代表性企业包括高德红外、华测导航、中海达、纵横股份、时代星光、大立科技、中信海直、赛为智能、臻迪科技等；地面系统代表性企业包括大疆、华科尔、易瓦特、华测导航、中信海直、中海达等企业。在系统集成环节，军用无人机代表性企业包括中航沈飞、航空工业、航天彩虹、洪都航空、北方导航、华力创通等；民用无人机代表性企业包括大疆、极飞科技、零度智控、极翼、易瓦特、赛为智能、顺丰控股等企业[4]。

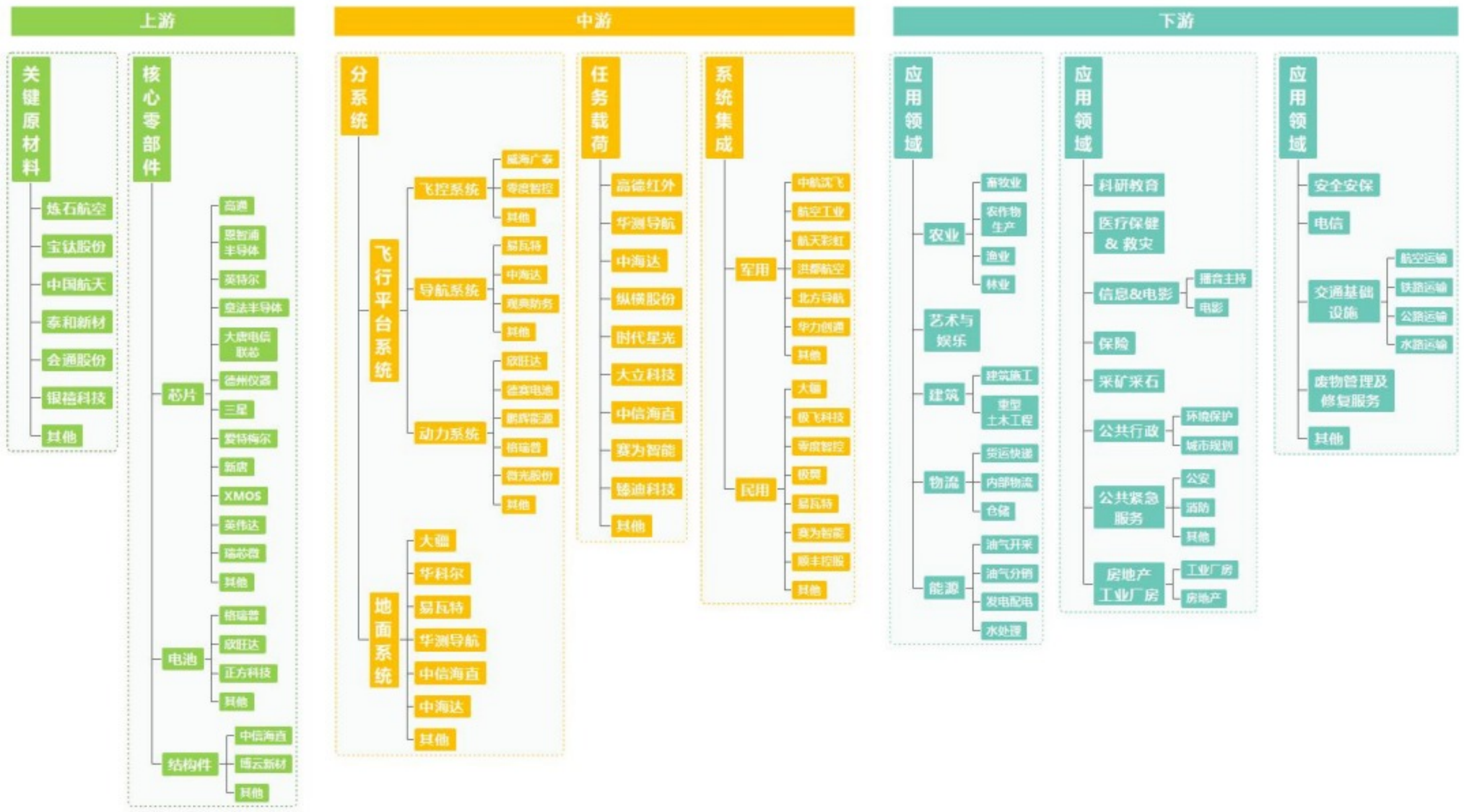


图 2.4　无人机产业链对应公司

无人机产业链下游的应用领域可谓是相当的广泛，据 Drone Industry Insights 于 2022 年 4 月发布的统计资料显示，在图 2.4 列出的 17 个行业中，能源、建筑和农业是当前无人机技术应用的前三大行业 [5]。

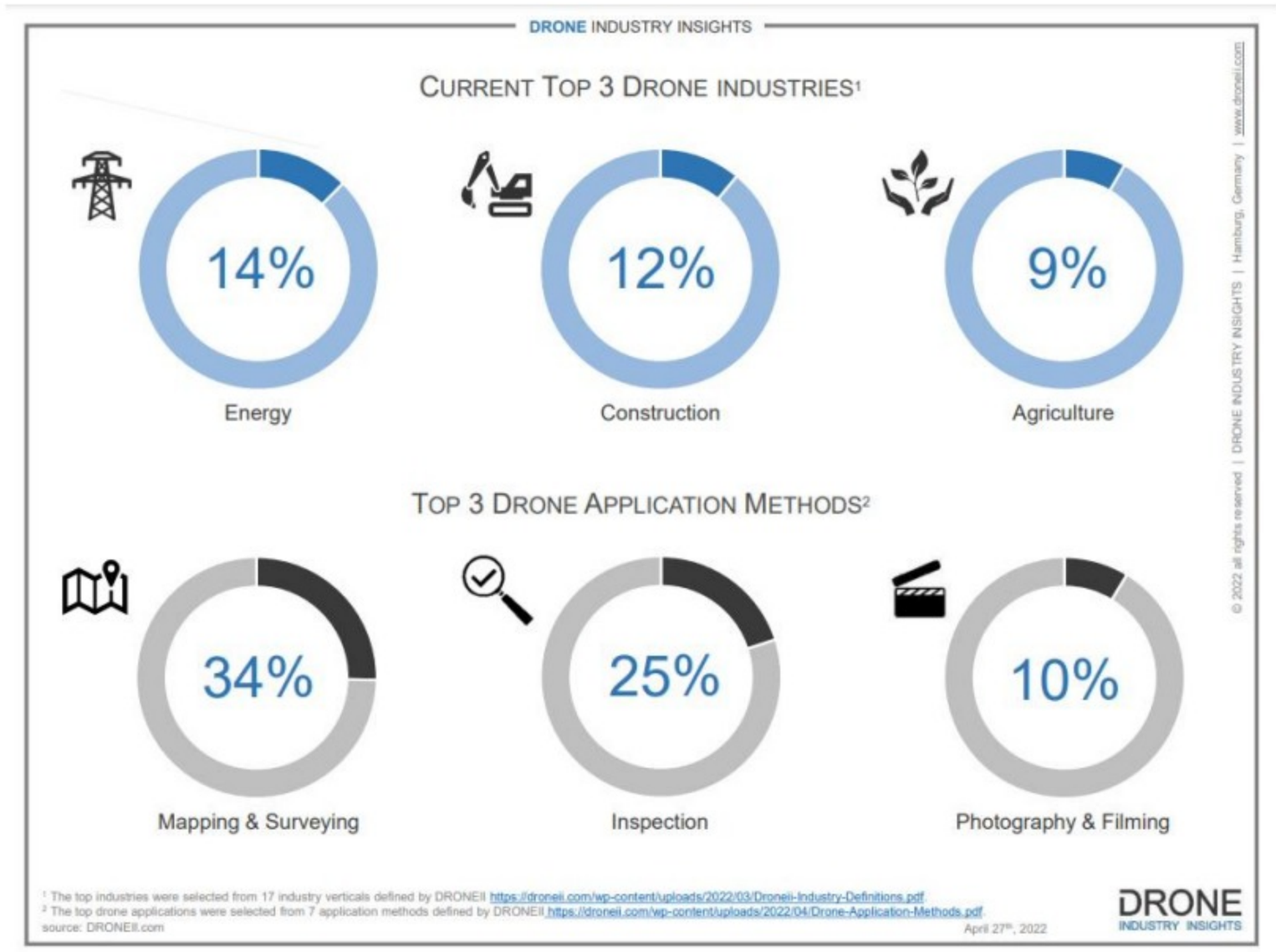


图 2.5　无人机应用领域前三大行业

其中，14% 的无人机应用发生在能源行业，其次是建筑业 12%，农业领域 9%，这 3 个行业加起来占无人机总应用的三分之一以上 （注意：图中显示的百分比是衡量无人机在上述 17 个行业中应用的指标，而不是衡量每个行业中无人机采用率的指标）。

能源领域的一些主要应用包括对炼化厂区、油气管道、电网等进行安全巡检和故障排查，使用无人机代替人员进入危险区域时，被检查的设备和系统等通常不必关闭，这意味着生产能够继续运行并产生收益。建筑业中无人机能担负前期的现场勘测与实景采集，施工阶段的现场实时监控，后期设施运维阶段的监测等任务，很大程度上节省了人力和物力。农业领域无人机应用的一些案例包括对农作物或植物进行数字化精准管理、精准喷洒作业等，因为可以更好地监测作物并以更有针对性的方式进行处理，使生产力得到大幅度提高。

图 2.5 中还显示出，无人机的主要应用方法是测绘 (34%)、勘察 (25%) 以及摄影和拍摄 (10%)，其他常见应用方法详见图 2.6[6]。

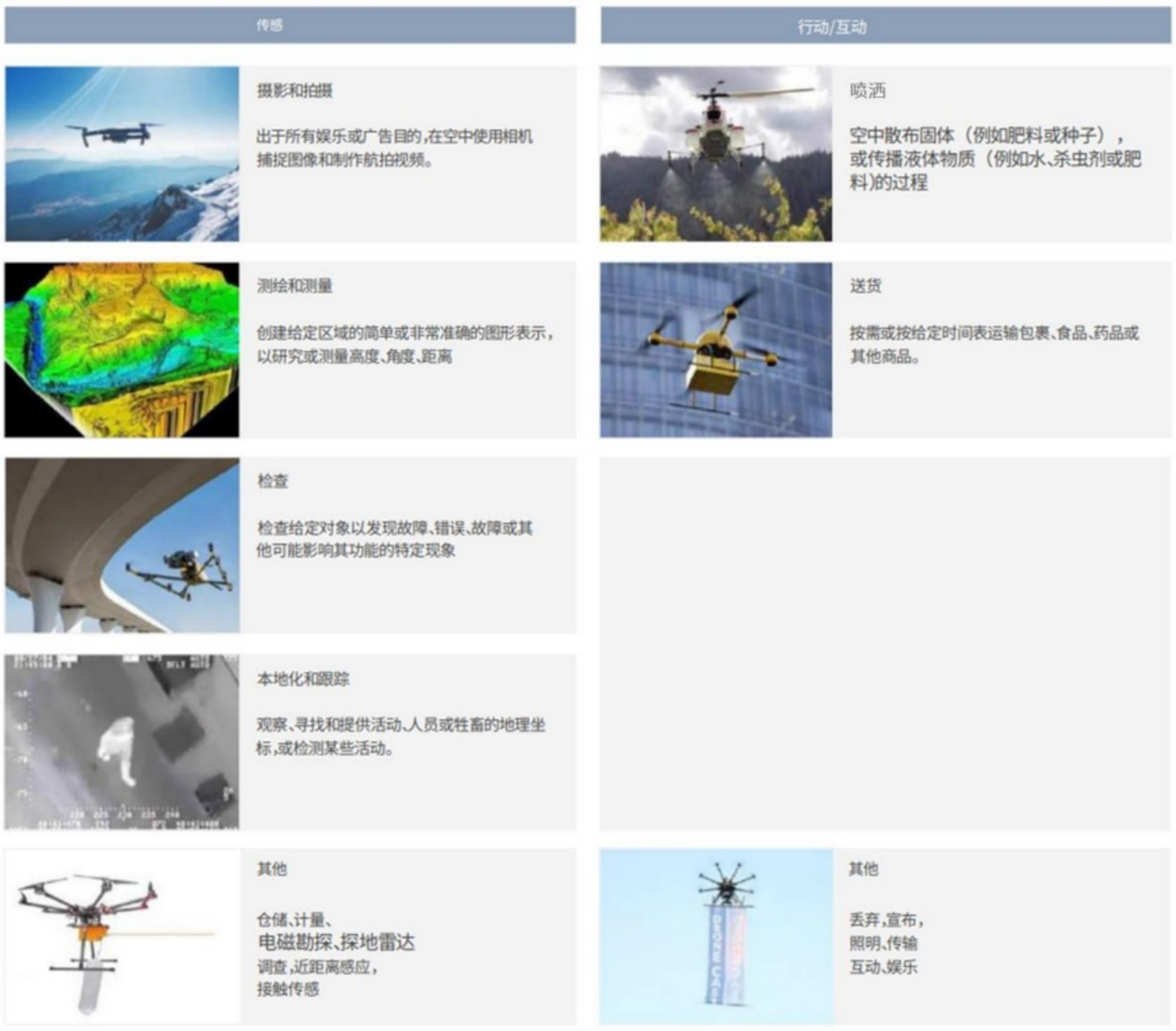


图 2.6　无人机主要应用方法

2.2 民用无人机市场现状

据中国航空工业集团有限公司在今年 11 月发布的《通用航空产业发展白皮书（2022）》显示，2021 年全球民用无人机市场规模超过 1600 亿元，同比增长 61.6%，其中工业级无人机占 60% 左右。随着下游应用领域的不断扩大，未来将继续保持增长，预计 2025 年将达到 5000 亿元。值得注意的是，随着更多高价值的工业级无人机应用到生产生活中，曾主导市场的消费级无人机市场份额会逐年降低，预计到 2025 年工业级无人机市场规模占比将超过 80%。

据行业主管部门统计，2020 年我国民用无人机研制企业已超过 1300 家，其中民营企业占据绝大多数，销售额在 1 亿元以上的企业超过 10 家。截至 2021 年底，我国获得通用航空经营许可证的无人机通用航空企业超过 1.2 万家。

民用市场的增长是由多种因素推动的，主要驱动力之一是无人机技术的进步。尤其是传感器相关的科技更是极大促进了工业级和消费级领域无人机的高速发展，随着无人机变得越来越复杂，它们能够执行更广泛的任务并在更具挑战性的环境中运行。这促使无人机在各种应用中的使用量增加，包括测绘和测量、检查和维护以及搜索和救援行动。

推动民用无人机市场增长的另一个因素是对航空数据和成像的需求不断增加。无人机能够从各种角度收集高质量的数据和图像，使其成为一系列行业的宝贵工具。例如，无人机正在农业中用于收集有关作物健康和生长的数据，在建筑中用于监测进度和识别潜在问题，以及在石油和天然气中用于检查管道和其他基础设施。

总体而言，民用无人机市场的发展受到技术进步、航空数据和成像需求增加以及无人机在各行业应用范围不断扩大的推动，未来民用无人机市场很可能会继续增长并扩展到新的领域。

再参考民航局近年来持续发布的《民航行业发展统计公报》，其中对无人机拥有者、注册无人机数、无人机有效驾驶员执照、和无人机飞行活动时长均有统计。

图 2.7　《民航行业发展统计公报》关于无人机的统计

从图 2.7 中数据可以看出，2021 年中国全行业无人机注册数量达 83.2 万架，较 2020 年增加了 31.5 万架，同比增长 60.93%。

随着无人机注册数量的增加，用户数量也随之增长，2021 年国内全行业无人机拥有者注册用户数量达 78.1 万个，较 2020 年增加了 22.3 万个，同比增长 39.96%。其中个人无人机用户连年占据无人机拥有者注册用户总数的 85% 以上。

随着在各应用领域的普及，无人机进入持证上岗时代，2021 年中国全行业无人机有效驾驶员执照数量达 12.08 万本，较 2020 年增加了 3.18 万本，同比增长 35.74%。

2021 年，共有 8 家无人机云系统加入交换系统进行数据交换和共享，它们分别是 U-Cloud 优云、U-Care 优凯、北斗云、无忧云、知翼云、极飞云、拓攻云和中科天网 [7]，其中北斗云由于其无人机运行量较少，2021 年下半年暂停数据交换，中科天网第四季度由于其系统升

级，没有数据上报。最终统计得到数据显示，参与民航局无人机云交换系统的无人机飞行时间在 2020 年达到了 183 万小时，较 2019 年增加了 58 万小时，同比增长 46.4%，2021 年较 2020 年有所下滑，2021 年飞行时间为 143.6 万小时，较 2020 年减少了 39.4 万小时，同比减少 21.53%，但仍然高于 2019 年同期水平，可见，在经历 2020 年初爆发的疫情后，2021 年度无人机的运行量已趋于正常[8]。

2.3 军用无人机市场现状

根据市场调研机构 Fortune Business Insights 于今年 6 月发布的军用无人机市场报告显示，2021 年全球军用无人机市场规模为 102.5 亿美元，并预计将从 2022 年的 117.3 亿美元增长到 2029 年的 308.6 亿美元，预测期内的复合年增长率为 14.82%[9]。

军用无人机市场的快速增长是由多种因素推动的，包括技术进步、军费开支增加以及无人机的军事采购增加。市场增长的主要驱动力之一是无人机技术的进步，这使得无人机能够在各种军事活动中胜任更多种类的任务，而军事组织也越来越认识到无人机在作战中的潜力。

促成军用无人机市场增长的另一个因素是全球不断增加的军费开支。根据斯德哥尔摩国际和平研究所 (SPIRI) 的报告，2021 年全球军事支出总额按实际价值计算增长了 0.7%，达到 21130 亿美元的历史新高。2021 年支出最大的五个国家是美国、中国、印度、英国和俄罗斯，共占支出总额的 62%[10]。

图 2.8 全球军费开支统计（1988-2021）

另一方面，信息技术在战场中发挥着越来越重要的作用，而无人机在信息对抗领域中独特的能力使其在现代局部战争中发挥重要作用。军用无人机的发展，正由单一的情报收集、通信中继、高空侦察等支援任务，向火力打击等主战任务转变。对无人机装备有需求的国家越来越多，但全球具备自主生产高性能军用无人机能力的国家较少，相较传统武器装备，无人机全球军贸市场较为活跃。根据 SIPRI 统计，2010 至 2020 年，以色列、美国和中国在无人机军贸市场出口份额分别为 30%、28% 和 17%，其他国家无人机系统军贸出口规模合计占比约 25%[11]。

03

无人机相关政策 & 标准 & 组织

在大力推动无人机产业迅速发展的过程中，各国政府及主管部门其实面临着诸多挑战。这首先来源于无人机带来的航空与公共安全、公众隐私侵犯等问题。与民航客机相比，无人机的飞行活动具有较强的不可控性，实现全面监管的难度更大， 因而可能对航空与公共安全造成重大威胁。此外，现有的民航管理体系难以直接套用在无人机上，因此，需要制定专门适用于无人机的登记、空中管理、遥控驾驶员管理等相关规定。

当前，还没有一个全球级的无人机管理框架，但不同国家和地区都在制定并不断完善无人机相关的法规和标准，努力在确保安全和推动发展间寻找到一个平衡点。本节将对国内外遵循的相关法律法规、规范标准、组织和会议进行简单介绍。

3.1 国内外政策

1. 欧盟

2018 年 8 月欧盟修订的《欧洲议会和理事会第 2018/1139 号法规—关于民用航空领域的共同规则和建立欧洲航空安全局》（以下简称《第 2018/1139 号法规》）将欧盟管理权限扩展至除国家航空器以外的所有的无人机，而不仅限于最大起飞重量大于 150 千克的无人机。在此上位法的基础之上，2019 年 6 月，欧洲航空安全局（EASA）发布了两部欧盟无人机通用条例，即《欧盟委员会第 2019/945 号授权条例—关于无人驾驶航空器系统和无人驾驶航空器系统第三国运营人》（以下简称《第 2019/945 号授权条例》）和《欧盟委员会第 2019/947 号实施条例—关于无人驾驶航空器运行规则和程序》（以下简称《第 2019/947 号实施条例》）。两部条例自 2020 年 7 月 1 日开始实施 [12]。

欧盟这一新近立法包含以下内容：以运行风险为基础，对无人机进行分类管理；建立注册登记系统、远程识别系统及地理感知系统，为“优空域”（U-Space）奠定基础；规定了两部条例对于第三国无人机系统运营人的适用性。

2. 美国

在国会立法层面，关于无人机的规则主要包含于民航相关法律中，通常无人机作为其中一个单独章节存在。已通过的涉及无人机的法律包括《2012 年联邦航空管理局现代化与改革法》(FAA Modernization and Reform Act of 2012) 和《2016 年联邦航空管理局扩张、安全和安保法》(FAA Extension, Safety, and Security Act of 2016)。前者明确规定将无人机纳入国家空域系统 (National Airspace System)，以实现对无人机和有人驾驶航空器的统一协调管理，后者主要关注民航信息系统、空中交通管理系统及国家空域系统的安全问题。

在法规层面，美国政府各部门主要是联邦航空局所颁布的关于无人机的法规主要集中于美国《联邦法规》(Code of Federal Regulations) 第 14 编 (Title 14)“航空与航天”中，主要包括该编第 1 部分关于无人机的定义、第 21 部分关于航空器产品和部件适航认证程序、第 91 部分一般作业与飞行规则以及根据《2012 年联邦航空管理局现代化与改革法》所制定的专门关于小型无人机规则的第 107 部分“小型无人机系统”等[13]。

3. 中国

法律层面2018年修订的《民用航空法》中增加了第214条作了原则性授权规定，即国务院、中央军事委员会对无人驾驶航空器的管理另有规定的，从其规定[14]。

行政法规层面，国务院、中央军委空管委办公室于 2018 年组织起草了《无人机飞行管理暂行条例（征求意见稿）》，征求意见稿重点在民用无人机分级分类、空域划设、计划申请等管理措施上实现突破，对产品质量、登记识别、人员资质、运行间隔等关键环节做出了详细规定。

规章层面，2018 年修订实施的《民用航空空中交通管理规则》，开了规章对无人机做出规定的先河，直接将“无人机”写入条文，在第 18 章第 2 节对无人机的飞行活动进行了原则性规定。

规范性文件层面，近年来，民航局针对无人机运行、空中交通管理、登记、驾驶员、经营性飞行活动以及适航管理等，先后出台了《轻小无人机运行规定（试行）》、《民用无人机系统空中交通管理办法》、《民用无人机实名制登记管理规定》、《民用无人机驾驶员管理规定》、《民用无人机经营性飞行活动管理办法（暂行）》、《特定类无人机试运行管理规程（暂行）》、《民用无人机产品适航审定管理程序（试行）》和《民用无人机系统适航审定项目风险评估指南（试行）》等一系列规范性文件。通过上述规范性文件以及相关的标准、程序，民航局搭建了无人机管理的基本框架，为无人机的进一步法律规制打下了基础。

3.2 标准与最佳实践

除了各个国家发布的无人机相关法律法规，全球范围内还有不少官方和非官方的针对无人机的工业设计标准、安全标准以及最佳实践等。

早在 2019 年底，国际标准化组织 (ISO) 就批准了无人机系统 (UAS) 的新国际安全和质量标准。新标准是与无人机专业人士、学者、企业和公众进行为期 12 个月磋商的结果，将对全球无人机行业的未来发展产生巨大影响。以下是 ISO 关于无人机的部分标准：

- ISO/IEC WD 22460 ISO License and Drone Identity Module for Drone(Ultra Light Vehicle or Unmanned aircraft system)
- ISO/IEC AWI 22460-3 ISO license and drone identity module for drone (Ultra Light Vehicle or unmanned aircraft system) — Part 3: Logical data structure, access control, authentication and integrity validation for drone licence
- ISO/IEC AWI 22460-2 ISO license and drone identity module for drone (Ultra light vehicle or unmanned aircraft system) — Part 2: Drone identity module (DIM)
- ISO/IEC CD 22460-1.2 ISO license and drone identity module for drone (Ultra light vehicle or unmanned aircraft system) — Part 1: Physical characteristics and basic data sets for drone licence
- ISO/TC 20/SC 16 - Unmanned aircraft systems
- ISO/DIS 21384-3 Unmanned aircraft systems — Part 3: Operational procedures
- ISO/DIS 21384-1 Unmanned aircraft systems — Part 1: General specification

除了 ISO 标准外，还有民间组织联合制定的业内最佳实践或安全操作标准，例如 SAFIR（Safe and Flexible Integration of Initial U-space Services in a Real Environment）。

SAFIR 是指在真实环境中安全、灵活地集成初始 U-space 服务。SAFIR 财团由 unily 领导，由 13 个公共和私营组织组成。SAFIR 项目证明了在具有挑战性的环境中，综合无人机交通的安全性和经济可行性。三家 U-space 服务提供商 (USSP) 和一家空中导航服务提供商共同控制了空域。可互操作、统一和标准化的 U-space 服务可以安全可靠地部署在整个欧洲。SAFIR 用例首次在位于 Sint-Truiden 的最先进的安全测试环境 DronePort 中成功测试。

还有其他一些非官方的民间无人机研究组织，会根据行业发展和现实应用场景中的问题，整理并发布一些测试评估标准或是最佳实践。例如 DroneSec 领头发布的 CUAS 标准和测试框架，该框架旨在帮助组织测试和评估反无人机系统的真正有效性和能力。该框架可以被视为一个基本的 OT&E 工具，在一个不受控制的环境中单独运行，以扩展和测试系统规格的极限，而不受供应商影响。

3.3 研究组织

全球范围内也有很多专注于无人机领域报道和深度分析的组织，除了在安全方面为无人机保驾护航外，还积极参与到无人机相关法规和条例的制定中，并且联合组织召开无人机主题大会，旨在促进无人机在非军用的民用消费级领域快速稳定地发展，并尽快被民众所接受，建立安全完善的无人机飞行环境。

1. The Drone Girl

图 3.1 The Drone Girl 标志

The Drone Girl[15] 是一个专注于无人机的新闻网站，由记者萨莉·芬奇运营，是《市场观察》和《华尔街日报》以及其他几家新闻网站的定期撰稿人。创建的目的是探索无人机以及如何通过它们产生的图像来帮助世界，通过发布航拍照片、视频和故事来展示无人机的发展情况。

2. Drone Industry Insights

图 3.2 Drone Industry Insights 标志

Drone Industry Insights[16] 是一家无人机行业研究组织，发布报告、信息图表和白皮书。普及无人机市场情报、当前趋势和未来潜力是他们的核心理念。他们还提供咨询服务和定制无人机市场研究，为客户提供商业情报。

3. DroneSec

图 3.3　DroneSec 标志

DroneSec[17] 创建网络安全和威胁情报解决方案，以保护合法无人机并防御恶意无人机。他们通过无人机保障未来的移动、运输和配送，从而实现创新。DroneSec 有每周的无人机资讯可以进行订阅，并且会追踪行业内最新的无人机信息，发布相关的分析报告和预测报告等内容，并且联合多个安全研究者共同发布无人机的安全分析和解决方案。

4. JARUS

图 3.4　JARUS 标志

无人系统规则制定联合体（Joint Authorities for Rulemaking on Unmanned Systems）作为全球航空领域最具领导力、影响力和增长潜力的新型国际组织（合作机制），致力于无人航空监管规则制定，促进全球无人航空安全、健康、持续发展。JARUS 既同国际民航组织（ICAO）等政府间国际组织保持密切合作，也同国际化标准组织（ISO）等非政府间国际组织和产业保持积极互动，并因其灵活性、专业性，以及对于成员国监管需求的精准响应一直走在无人航空规则制定的前沿。JARUS 秘书处由我国国家空管法规标准研究中心、中国民用航空局第二研究所、加拿大交通部和葡萄牙民航局四方支持。JARUS 还会定期举办全球大会，一般持续一周，数十个国家和国际组织的航空管理机构官员、专家学者，以及波音、空客、谷歌、顺丰、迅蚁等国内外无人航空产业代表参加。共同探讨无人航空系统规则制定，促进全球无人航空安全、健康、持续的发展。

5. AUVSI

图 3.5　AUVSI 标志

国际无人系统协会（AUVSI）是世界上无人系统领域最大的非营利组织，致力于推动无人系统和机器人技术的发展。AUVSI 成员在国防，民用和商业市场工作。AUVSI 会员资格对所有类型的无人系统和机器人公司以及服务于该行业的专业人士开放。

6. ArduPilot 国际开源者组织

图 3.6　ArduPilot 标志

ArduPilot 国际开源者组织是全球最知名的无人机开源社区，它在功能更新、硬件发展、工业集成、数据传输等方面发挥着重要的影响力。ArduPilot 提供多功能、可信度高和开放性强的无人机开源软件项目。

3.4　相关会议

参加无人机相关的会议可以提供广泛的好处和学习机会，并能与该领域其他研究人员和专家建立联系，掌握最前沿的资讯。无人机相关的主要会议有：

1. AUVSI XPONENTIAL

图 3.7　AUVSI XPONENTIAL 标志

由 AUVSI 主办的 AUVSI XPONENTIAL 通过汇集商业和国防应用的交集问题捕捉行业潜能。思想领袖和行业专家将探索怎样用新兴技术在各个市场领域创造商机。XPONENTIAL 拥有行业内顶尖演说家、结构化的追踪、最优的网络机会，这也使它成为了那些想与快速发展的无人系统产业并肩前行的专业人士的第一选择。

2. 世界无人机大会

图 3.8　2022 世界无人机大会现场

世界无人机大会 [18] 的目标是将大会打造成全球无人机行业领袖探讨交流技术、创新产品应用的平台，深入分析无人机产业发展中面临空中交通管理、数据安全与隐私保护的风险问题，提出具有可靠性的解决方案，推动无人机行业可持续发展。会间各国代表对无人机、无人系统的发展现状、技术创新，空域管理、教育培训、标准建设，以及无人机、无人车、无人船、无人化装备、安保机器人、人工智能产品技术在治安、疫情防控、国土、海事、消防、环保、农业、电力、铁路、贸易、遥感、气象、测绘、林业及灾害防治和公共安全等领域的应用议题进行深度交流与探讨。

3. 国际无人机系统会议（ICUAS）

图 3.9　ICUAS 会议

ICUAS 是关于无人机的重要会议，汇集了行业专家、研究人员和政策制定者，讨论无人机技术和应用的最新发展。ICUAS 有一系列会议和研讨会，主题包括无人机设计和开发、无人机在各行业的应用、无人机监管和政策，以及无人机行业的新兴技术和趋势。会议还设有展览厅，与会者可以看到来自领先制造商和供应商的最新无人机产品和服务。

4. Commercial UAV Expo Americas

图 3.10　Commercial UAV Expo Americas 标志

Commercial UAV News 主办的商业无人机博览会是领先的国际贸易展览和会议，专注于特定垂直市场中商用 UAS 的集成和运营。与会者能够了解在建筑、能源和公用事业、无人机交付、基础设施和运输、采矿和集料、公共安全等方面利用无人机的机会，培养无人机的应用。

5. 全球无人机应用及防控大会暨无人机产业博览会

2022全球无人机应用及防控大会
暨无人机产业博览会
2022 GLOBAL CONFERENCE ON UAV APPLICATION AND ANTI-UAV
& UAV INDUSTRY EXPOSTION

图 3.11　全球无人机应用及防控大会暨无人机产业博览会标志

该会议致力于将会、展、赛相结合，打造一场高规格、高水平的无人机产业应用国际盛会，聚集了行业应用，链接无人机全产业链，助推中国无人机产业健康、有效发展。会议汇集无人机行业顶级专家，加强无人机区域国际交流合作，探索国际无人机产业创新发展之路。

04

无人机系统安全性现状

4.1 无人机系统

无人机系统主要由三大部分组成，包含无人机机体、地面站以及传输信息的通信链路。地面控制系统负责接收地面站的控制命令，并将命令发送给无人机，以控制无人机的飞行。无人机接收到地面控制系统的控制命令后，通过飞行控制系统对电机和舵机进行控制，从而实现飞行。同时，无人机的传感器负责收集无人机的运动状态信息，并将信息传递给地面控制系统。地面控制系统接收到无人机的运动状态信息后，将信息传递给地面站，地面站则根据无人机的运动状态信息，进行相应的处理，并向地面控制系统发送新的控制命令，以指导无人机的飞行。这样，无人机系统就能够通过地面站对无人机进行远程控制，实现无人机的飞行。

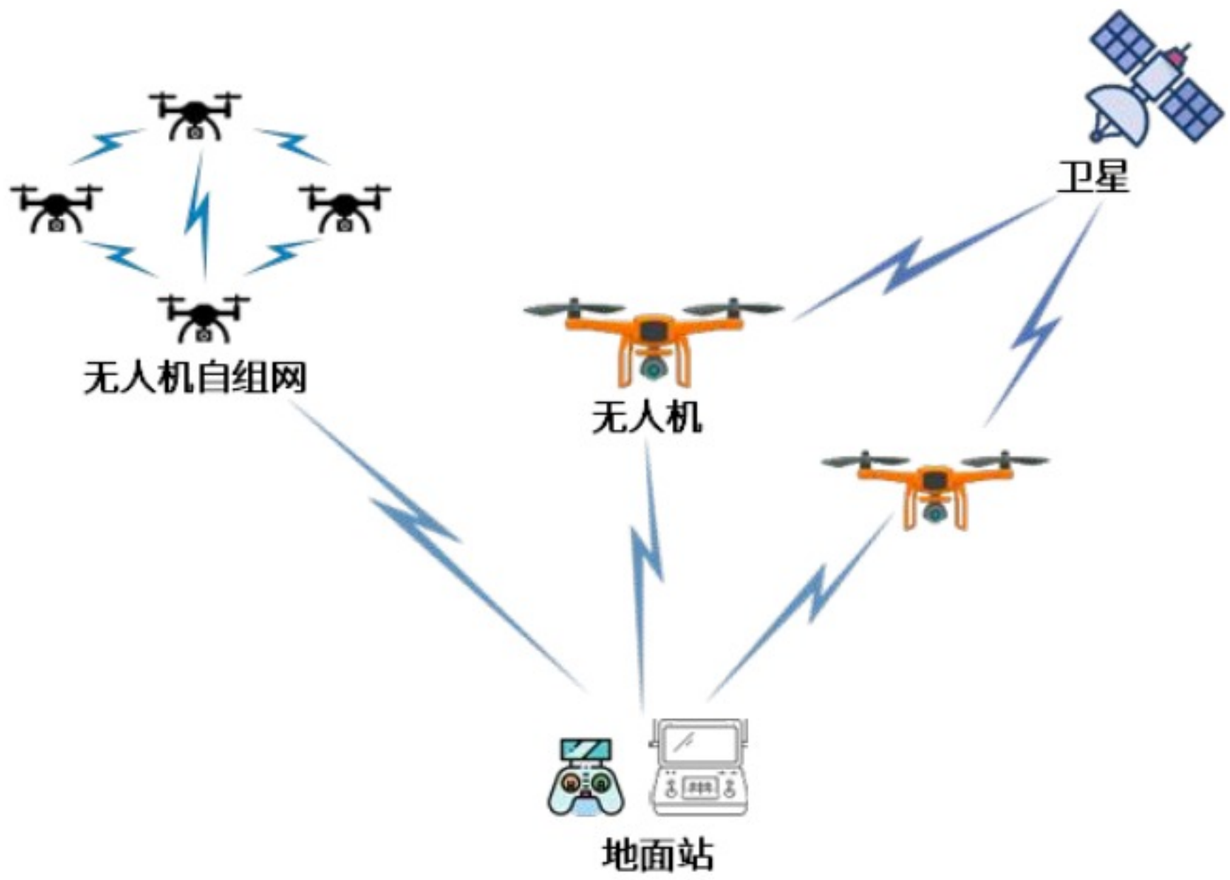


图 4.1 无人机系统结构

4.1.1 无人机机体

无人机由飞行器机架、推进系统、飞行控制系统和传感器等部件组成。飞行器机架负责支撑无人机，推进系统负责提供动力，飞行控制系统则负责控制无人机的飞行。传感器则负责收集无人机的运动状态信息，并将信息传递给飞行控制系统。

1. 飞控系统

无人机的飞行控制系统是无人机的核心部分，它负责控制无人机的飞行。无人机的飞行控制系统通常由多个部分组成，包括自动飞行控制系统、人工飞行控制系统和飞行控制计算机等。自动飞行控制系统负责接收无人机的运动状态信息，并基于一组预定义的控制规则，

自动控制无人机的飞行；人工飞行控制系统则允许操作人员直接控制无人机的飞行，并能够实时监测无人机的飞行状态；飞行控制计算机则负责处理飞行控制系统的数据，并根据飞行控制系统的要求，对无人机的电机和舵机进行控制。目前市面上中低端的无人机大多数使用开源的飞控系统，例如 PX4、ArduPilot 等。

1）PX4

PX4 是平台无关的自动驾驶仪软件，由苏黎世理工大学（ETH）的科研团队研发并开放，可以驱动无人机或无人车。它可以被烧写在某些硬件（如 Pixhawk v2），并与地面控制站一起组成一个完全独立的自动驾驶系统。

图 4.2　PX4 标志

2）ArduPilot

ArduPilot 支持多种平台，包括固定翼、多旋翼、转子飞行器和车载应用。该飞控系统采用 C++ 语言编写，并提供丰富的功能和可扩展性。ArduPilot 可以用于控制各种无人机和机器人，并支持多种传感器，包括 GPS、陀螺仪、加速度计、气压计、罗盘和摄像头等。它提供了丰富的功能，包括飞行控制、导航、图像处理、遥控器接入、地面站接入和固件更新等。

图 4.3　ArduPilot 标志

3）Pixhawk

Pixhawk 是世界上著名的开源飞控硬件厂商 3DR 推出的开源飞控硬件平台，它同时支持 Ardupilot 和 PX4 飞控系统，基于 STM32F427（180MHZ）主控及 STM32F100 协处理器，可以提供完整的飞行控制功能，包括姿态控制、导航和避障。它还提供了丰富的接口，方便用户接入各种外部设备，实现更多功能。

图 4.4　Pixhawk 硬件

2. 传感器

无人机的传感器负责收集无人机的运动状态信息，并将信息传递给飞行控制系统。无人机的传感器通常包括加速度计、陀螺仪、罗盘和气压计等。加速度计负责检测无人机的加速度；陀螺仪则负责检测无人机的角速度；罗盘则负责检测无人机的航向；气压计则负责检测无人机的高度。通过这些传感器，无人机的飞行控制系统能够实时获取无人机的运动状态信息，从而控制无人机的飞行。

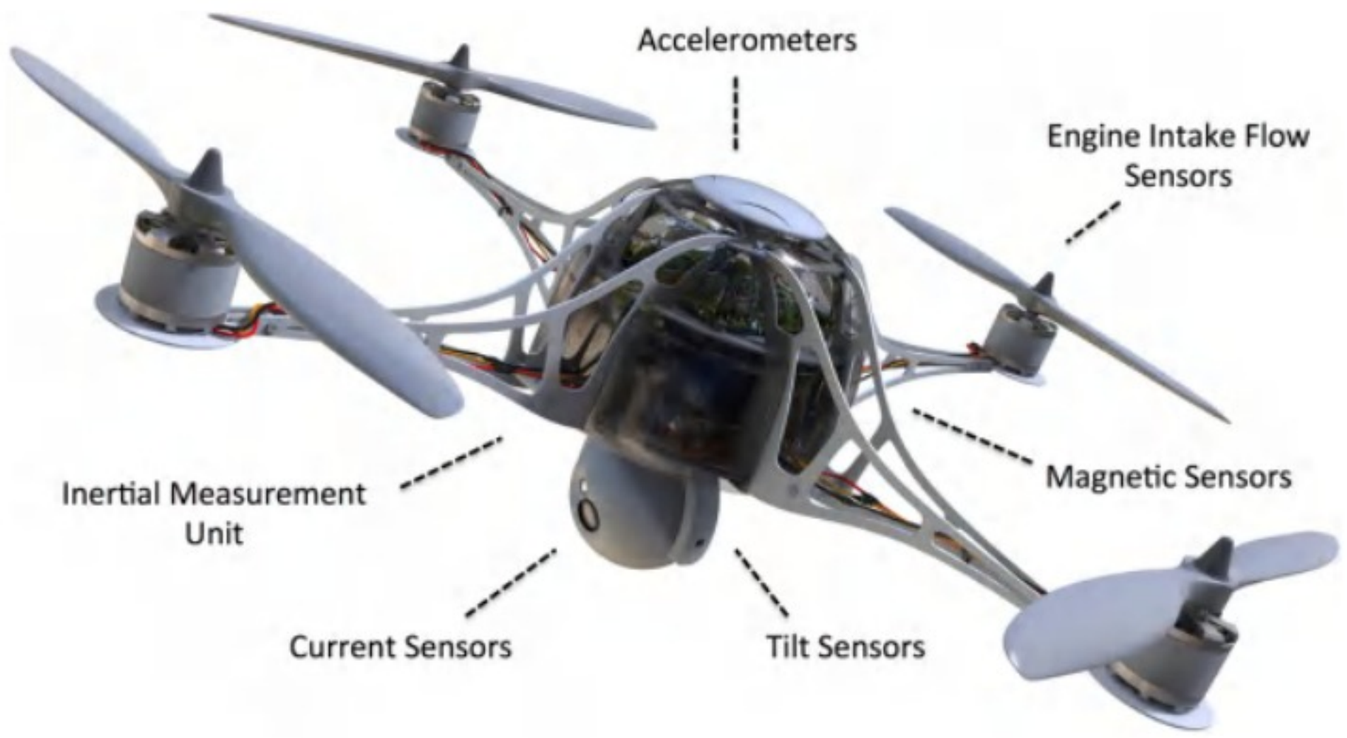


图 4.5　无人机传感器

4.1.2　地面站

无人机地面站是整个无人机系统的指挥控制中心。通常地面站由遥控装置、显示器，电源系统，电台等设备组成，地面站上装有控制飞机的软件，无人机的飞行路线通过路线规划工具进行安排，并设置飞行高度、飞行速度和飞行位置等。常用民用无人机的地面控制站相对简单，尤其是消费级无人机的控制站实际主要是控制手柄或者安装了配套软件的平板电脑、智能手机。

图 4.6　无人机地面站和遥控器

4.1.3　通信链路

无人机的通讯方式是指无人机与地面站之间通信的方式。目前，无人机的通讯方式主要有如下 4 通信方式，通过电台、WiFi 方式近距离通信，通过基站或者卫星进行远距离通信。

卫星通信：卫星通信主要利用卫星网络来实现无人机与地面站之间的通信。在无人机上，需要安装有卫星通信模块，能够通过卫星网络与地面站进行通信。在地面站上，需要安装有卫星天线和卫星通信模块。卫星通信的优点是能够实现地面站与无人机之间的远距离通信，能够满足无人机的远程控制需求。另外，卫星通信的安全性和可靠性也比较高，适用于各种各样的环境。缺点是卫星通信设备较为复杂，成本相对较高。

电台通信：电台通信主要利用无线电波来实现无人机与地面站之间的通信，是目前使用较为广泛的通讯方式。一般工作频段在 2.4GHz 或者 5.8GHz,，同时为了防止信号干扰还会使用跳频通信的方法，无人机电台通信的范围取决于天线的增益和功率以及周围的电波干扰情况，一般来说，无人机电台通信的范围在几公里到几十公里不等。

基站通信：无人机基站通信指的是无人机使用 4G/5G 通信方式进行远距离通信，由于通信是基于基站的，所以从理论上来说，只要有基站信号的地方就没有距离限制。当然，飞行距离也受电池因素的影响，同时，飞行路线应该选择有基站信号覆盖的地方，防止无人机失去控制。

WiFi 通信：WiFi 是一个相对成熟的通信技术，可以实现无人机和地面控制站、手机、平板电脑等设备之间的连接。WiFi 通信的传输距离一般较短，一般在几十米左右。此外，WiFi 通信易受到电波干扰，信号容易中断，不太适用于远距离的无人机通信。

在无人机的通讯方式中，电台通信和 WiFi 通信是目前比较主要的方式，但是基站通信和卫星通信也正在不断发展，未来可能会成为无人机通讯的重要方式。

4.2 无人机攻击应用场景

无人机攻击可能会用于许多不同的场景，例如将无人机用于近源攻击中，入侵目标系统的无线网络，无人机攻击还可能用于进行情报获取，进行监视和目标识别，或者用于实体战争中，特别是今年的俄乌战争，双方都将无人机作为军事斗争的重要手段。总之，无人机攻击可能会用于各种不同的场景，具体取决于攻击者的意图和目标。

4.2.1 近源攻击

2022 年夏天的一天，美国东海岸一家专注于私人投资的金融公司的工作人员发现其 Atlassian Confluence 内部页面出现了一些反常现象，安全人员发现大楼的楼顶有两架无人机。经过分析，黑客正是利用两台无人机搭载的一些电子设备，通过 WiFi 入侵了公司的内部网络。据海外媒体 theregister 报道，两架无人机分别是 Matrice 600 和 Phantom，不过都进行了改装。Phantom 无人机状况良好，并配备了经过改进的 Wi-Fi Pineapple 设备，用于网络渗透测试；Matrice 无人机携带一个箱子，里面装有一个 Raspberry Pi、几块电池、一个 GPD 迷你笔记本电脑、一个 4G 调制解调器和另一个 WiFi 设备 [19]。

美国规模最大的国防情报承包商之一的博思艾伦咨询公司（Booz Allen Hamilton）在《2020 年网络威胁趋势展望》报告中称，随着小型无人机正从新颖的物品演变为“无处不在的商业工具”，从 2020 年开始，无人机可能成为主要的网络安全威胁，建议企业机构保护建筑物周围的空域。

4.2.2 情报获取

2022 年初，乌克兰 Infozahyst 公司对其可能具有革命性的无人机进行了新的飞行测试，名为 “Gekata” 的无人机是一款新型电子情报无人机。该公司于 2 月 18 日宣布了该无人机的第二次试飞，其主要目的是确定综合设施的关键运行条件，以确保在复杂条件下无人机的性能。

图 4.7　乌克兰测试情报收集无人机

新的无人机系统以 PD-2 无人机系统为基础，设计用于搜索、探测、分类和识别来自雷达站、反舰战和飞机的信号脉冲。Gekata 系统的主要部件是一个 10 公斤重的无线电侦察设备套件，安装在 PD-2 无人机上。据开发人员称，整个综合体包括一个地面控制站和 6 架无人机，配备 Gekata 电子情报 / 通信情报套件。Gekata 可以在实时模式下探测和识别来自地面目标、空中目标 (包括超视距目标) 的无线电信号。根据该公司官员的说法，新的基于无人机的电子情报系统将为军方打开一个全新的机会。

2022 年 8 月，据外媒报道，英国和挪威联手向乌克兰提供 850 架“黑蜂”微型无人机，无人机由挪威制造。挪威开发的这款无人机用于侦察、监视和目标识别，并在包括美国、英国和其他几个北约成员国在内的许多国家执行任务。

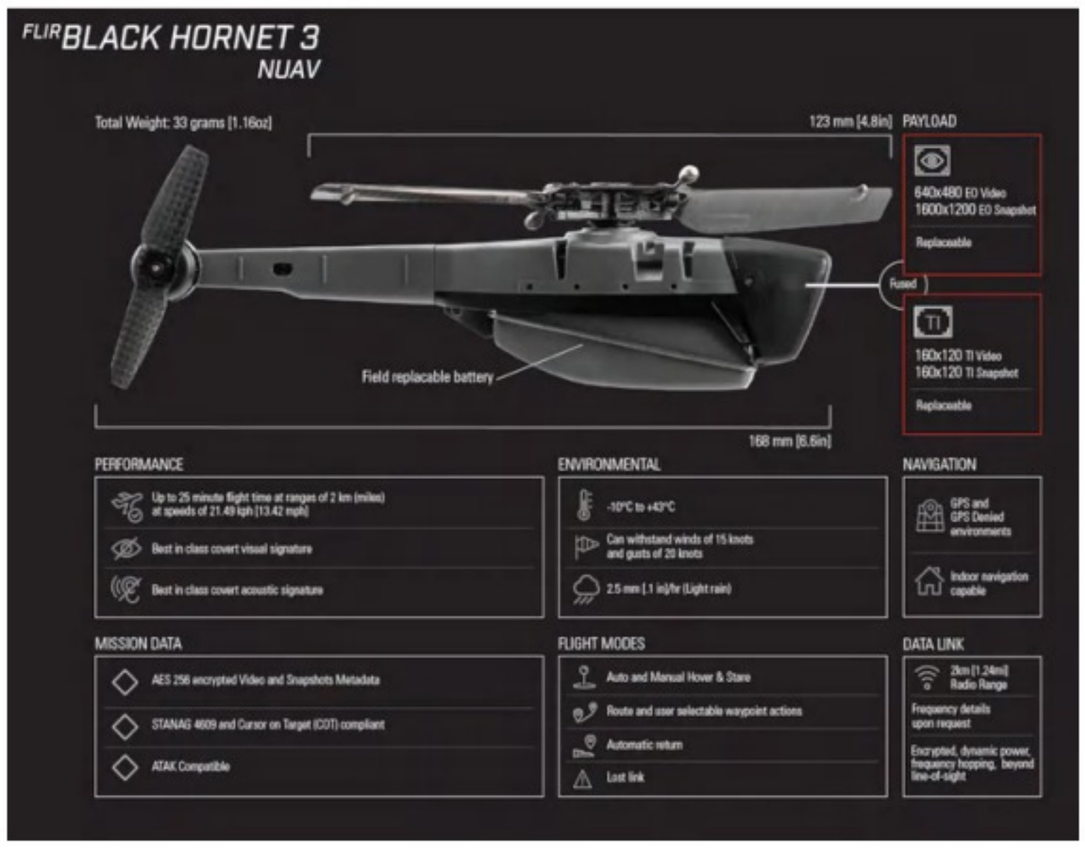


图 4.8　“黑蜂”微型无人机

在基本配置方面，黑蜂装有三个光学摄像头，可以无死角观测周边环境，并将现场所拍摄的视频与图像实时传回后方指挥部。值得一提的是，黑蜂无人机如此受欢迎，不仅仅是因为体型小，也与其续航时间长、上手快离不开关系。一套标准配备中包含两架无人机和一个配套的基站，平均每架无人机可以飞行 25 分钟，在 20 分钟里即可完成 90% 充电，两架飞机在正常的侦查任务中可以采取交替作战的方式，进一步延长侦查时间，获取更多有效情报。而在无人机充电的 20 分钟时间里，一名新手士兵完全能够在接受培训后学会如何使用。

4.2.3 武装袭击

2022 年 1 月 17 日，当地时间周一在阿布扎比，一起无人机袭击导致的油箱爆炸事故造成三人死亡。在也门胡塞反政府武装宣布在阿联酋展开“军事行动”几小时后，该组织声称对此次袭击负责，并警告称，它可能会针对更多设施发动袭击。

2022 年 11 月，据一名驻中东的国防官员表示，阿曼海岸附近的一艘油轮遭携带炸弹的无人机袭击，所幸没有人员伤亡，船体受到轻微损伤，但并未污染周围海域。

2019 年 9 月 14 日，也门胡塞武装证实，这一反政府武装当天清晨动用 10 架无人机袭击沙特阿拉伯境内一家炼油厂和一座油田，袭击触发炼油厂大火。胡塞武装针对沙特石油设施发动的袭击源于沙特介入也门战事。

4.2.4 实体战争

使用无人机作战，早在越战和中东战争中就已出现。2001 年，美国首次使用“捕食者”无人机发射反坦克导弹进行实战，开创了无人机对地打击先河。此后，军用无人机应用越来越广泛，并朝着察打一体化、攻防一体化方向发展。据斯德哥尔摩国际和平研究所的一项统计数据，1980 年至 2020 年，国际市场上共有 43 款无人机，其中大中型、长航时、固定翼作战无人机共 35 款，占比达 82%[20]。

近年来，军用无人机装备频繁出现在局部地区战场，应用潜力不断提升。在今年 2 月爆发的俄乌战争战报中，屡见无人机的身影，以下参考《战术导弹技术》期刊以及其他开源情报的信息，对俄乌双方在本次冲突中投入的无人机进行简单汇总 [21]。

表 4.1　俄参战主要无人机

无人机代号	简介	主要功能、战时表现
猎户座	俄最新研制的**大型察打一体无人机**，设计参数优于其现役同类型无人机装备	由于服役时间较短、列装数量有限，实战测试尚不充分，因此在此次冲突中并未大量部署运用，而是以能力展示为主。
前哨 -R	俄罗斯在以色列 Searcher 2 无人机的基础上改造而来的一款**察打一体无人机**	本次冲突中，俄军使用该型无人机挂载精确制导弹药打击了乌武装据点。
海鹰 -10	俄研发的中程**多功能无人机**	主要执行侦察监视和火炮校射等任务。可同时携带 3~4 种任务载荷，在复杂气候环境下和交通不便地区进行大范围侦察监视任务。
海鹰 -30	“海雕 -10”无人机的**升级版本**	主要特点与“海雕 -10”无人机基本相同，挂载光电侦察吊舱，具备激光测距和激光指示能力，可为重型迫击炮发射的激光制导武器进行目标照射。
KUB-BLA(立方体)	卡拉什尼科夫集团下属的俄罗斯国防公司扎拉航空研发制造的**新型巡飞弹无人机系统**	该机由电动发动机驱动，声学特征小，可携带多种战斗部，本次冲突中使用了钢珠杀爆战斗部。

表 4.2　乌参战主要无人机

无人机代号	简介	主要功能、战时表现
“旗手”TB2	土耳其研制的**中空长航时察打一体无人机**	本次冲突中，该无人机摧毁俄“山毛榉”防空导弹系统以及多辆加油车、地面输油设施和装甲车等目标。
UJ-22“天空”	乌克兰研制的**多用途小型无人机**	可在昼夜及多种气象条件下执行侦察监视、火炮校射、目标指示和搜救等多种任务。
莱莱卡 -100	乌克兰研制的**小型战术侦察无人机**	该机可按照地面终端在电子地图上规划的路线和高度自主飞行，且具备通信受阻下自主返航功能。
惩罚者	乌克兰研制的**小型武器化平台**	本次冲突中主要打击俄油料储存设施、弹药补给节点和电子战基站等目标。
弹簧刀	美国向乌克兰提供的**陆射巡飞弹**	主要用于执行精确打击任务，可协助小规模作战部队在无空地火力支援的情况下打击固定或移动目标。
RQ-20“美洲狮”	美国向乌克兰提供的**小型侦察无人机**	可手抛发射，执行情监侦、目标定位等任务。
量子侦察	美国向乌克兰提供的**小型侦察无人机**	可对战场上偏远、难以接近的区域进行准确和快速侦察。
凤凰幽灵	美国向乌克兰提供的**战术无人机**	性能与“弹簧刀”相似，主要定位为打击目标，但可携带光学器件，提供必要的侦察定位能力。

4.3 国内外安全研究动态

1. 无人机劫持攻击

2022 年，Black Hat 欧洲大会上，来自韩国的安全研究员在议题《Grand Theft Drone: Reaching Breaking Point in Drone Proprietary RF Link Security》中展示了对无人机的劫持攻击，研究员通过研究无人机的信号，分析出无人机的跳频规律以及无线协议格式，实现了一个伪造的地面控制器来劫持空中飞行的无人机。

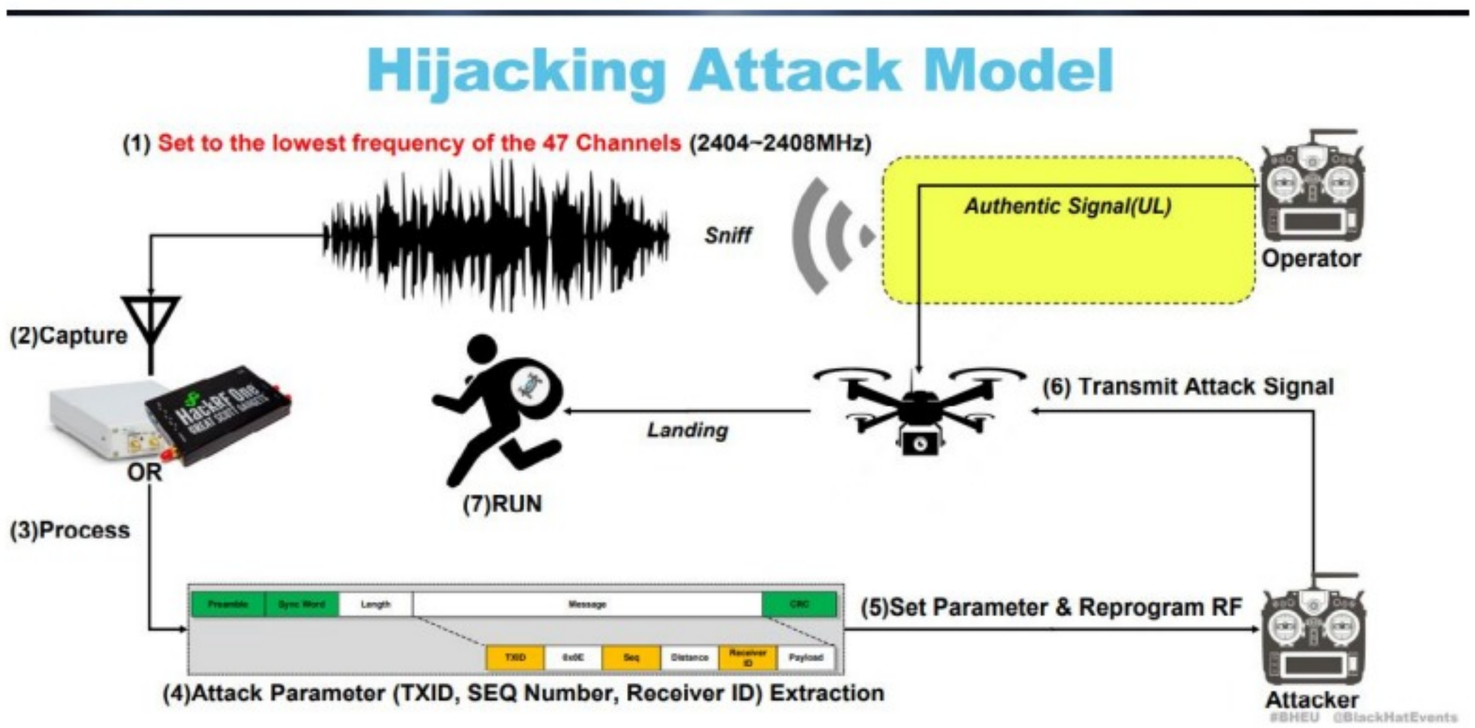


图 4.9　劫持攻击模型

2. 针对无人机的模糊测试

2020 年 8 月份，乔治梅森大学的研究人员针对消费级无人机使用模糊测试方法进行网络安全评估，在其研究成果中作者探讨了一个新的无人机漏洞，并给出了相应的安全保护措施。作者使用模糊测试的方法发送变异数据到无人机的 FTP 端口，并向无人机的其他端口也发送了大量数据报文。在测试中，持续监测无人机相关性能，以确定特定故障的模式和漏洞影响。这个模型被应用于 Parrot Bebop 2，在测试过程中，Parrot Bebop 2 的 GPS 性能下降、视频速度、无人机对地面站的响应速度、无人机传感器数据的准确性均受到相应影响。图 4.10 为在 Parrot Bebop 2 上进行 InviteFlood 模糊测试的 bash 脚本。

```
port=1
while [ "$port" -le 100 ]
do
   inviteflood wlan0 john.doe local.example 192.168.42.1 20000 -D $port
   port=$((port+1))
   if [ "$port" -eq 100 ]
   then
        port=1 #Multiple iterations without restarting
   fi
done
```

图 4.10　模糊测试脚本

3. 无人机渗透测试框架 DroneSploit

2019 年，Black Hat 欧洲大会上 Alexandre D’Hondt 和 Yannick Pasquazzo 展示了一款针对无人机的渗透测试工具“DroneSploit”，这是为无人机黑客量身定制的一个类似 Metasploit 的框架。据介绍，DroneSploit 只针对 WiFi 控制的无人机（例如 AR Drone、DJI Tello、Mavic Mini），但不支持基于射频（RF）的无人机（如 DJI Phantom 4、Mavic Pro 等）。该工具旨在帮助发现无人机安全漏洞 [22]。

图 4.11　DroneSploit 界面

4. 无人机攻击智能电视

2019 年，Defcon 大会上，独立安全研究员 Pedro Cabrera 展示了如何利用无人机攻击现代智能电视。在其公布的一段视频中，他使用 DJI 四轴飞行器悬挂一个配备有软件装置的无线电信号放大器，靠近邻居房屋顶部的电视接收天线，由于无人机携带的设备信号压制了智能电视原有的合法信号，很快，邻居家的电视屏幕上出现了 Defcon 字样的画面。很显然，无人机接管了邻居家的智能电视。

由于在无人机上搭载一个树莓派或者 WiFi Pineapple （俗称“大菠萝”，是无线安全审计公司 Hak5 开发并售卖的一款无线安全测试神器）就可使其变成 “黑客无人机”，因此对于一些有严格数据风险管控的机构来说，无人机也是一个潜在的数据漏点。针对日益增长的无人机空中威胁，IEEE 还专门发布了一篇题为《无人机黑客：物联网的安全和隐私威胁》的报告讨论此事。

05

无人机系统攻击面

5.1 概述

无人机系统安全方面主要关注数据机密性、信息完整性和系统可用性，能够直接或者间接影响到这三个方面的风险因素会被视为攻击面。

1. 数据机密性

机密性是指保护信息不被未授权方访问。换句话说，只有被授权的人才能访问数据。攻击者可以利用不同的攻击矢量，通过各种方式，如假扮为无人机数据的授权接收方等，来危害无人机系统的保密性。无人机不可避免地需要在各种场景中传输数据，包括军事和民用环境。因此，任何未经授权的实体都不应获取无人机传输的数据信息，也不能直接对传输包中的数据进行解密。

2. 信息完整性

完整性保证了信息的真实性，攻击者可能通过通信链路、地面通信系统或受损的无人机修改或伪造无人机系统的信息，如收集的数据、发出的命令等，并劫持修改无人机控制数据使得接收的命令信息不完整，而直接导致无人机实施任务失败。如攻击视觉传感器或 GPS 传感器，使无人机得到错误的图像或地理位置信息，可能导致无人机漂移或坠毁。无人机通信需要保证数据的完整性，特别是用于控制无人机的命令数据，使无人机能够可靠地运行，不会受到干扰、错误感知数据和入侵的影响。显然，信息完整性是必不可少的无人机群系统安全需求。

3. 系统可用性

可用性确保无人机系统携带的服务和相关数据按预期运行，并可被授权用户访问。攻击者可能对无人机系统执行 DoS（拒绝服务）攻击，如淹没通信链路、过载处理单元或耗尽电池。无人机系统应严格按照其合法用户的命令执行任务或收集数据。有些攻击的主要目的不是获取无人机传输的数据，而是以较小的开销阻碍无人机的正常运行，例如，泛洪攻击使无人机无法响应用户的命令，黑洞攻击使无人机群网络中的无人机无法接收来自地面站的命令。这些攻击使无人机系统无法正常操作，甚至导致无人机坠落。因此，必须保证无人机系统的可用性。

总的来说，无人机面临的攻击面非常多，可能涉及到电子、网络和物理攻击，因此应该采取相应的措施来保护无人机免受攻击。

5.2 无人机常见攻击面及加固建议

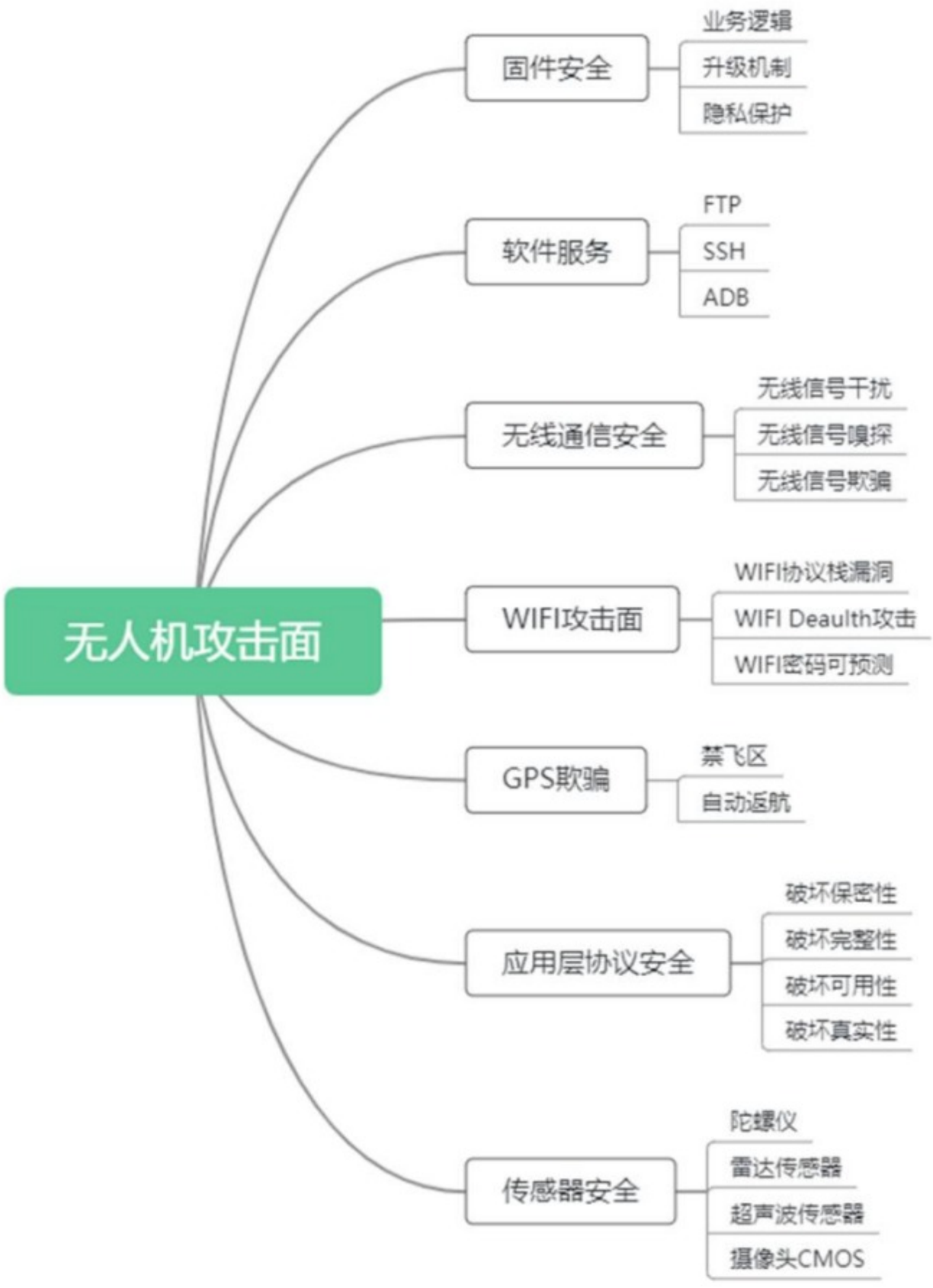


图 5.1 无人机攻击面

5.2.1 固件

无人机固件的安全风险很多，下面列举了部分常见内容。

1. 固件业务逻辑问题

无人机固件业务逻辑问题涉及到诸多方面。例如：飞机序列号和重要部件编号是否存在未授权修改，特别是序列号，修改序列号可导致伪造其他用户的无人机，造成安全问题。还有一些无人机，会内置固件类型，一般分为：开发、维修、发行，正常用户使用的是发行版本，但是如果可以被篡改成开发模式，那么固件就会开启一些远程调试服务。总的来说，这些关键的无人机参数应该存放到可信区，使用硬件的手段去保护这些参数不易受攻击者修改。

2. 升级机制

大部分无人机的固件升级需要通过 USB 或 WiFi 将 PC/ 手机与无人机连接。例如 DJI，需要将智能手机连接到遥控器，并确保智能手机有一个稳定的 WiFi 连接。一旦无人机完成了远程连接，应用程序将显示固件更新提示，需要用户允许应用程序下载和安装新的固件。整个过程中存在恶意修改固件升级包的可能性，进而给无人机引入漏洞或后门。

除了常见的固件的解包和重新打包（有部分固件是加密的），还有下面一些攻击方法：

通过固件 MODDING，在固件升级的过程中，将修改过的恶意固件安装到无人机系统中。这种攻击方式虽然不是远程攻击，需要物理接触，但是攻击者使用该漏洞可以完全获取无人机的控制权限，不仅可以接触到无人机中的敏感信息，例如飞行日志、操作日志等，同时也可以开启无人机的禁飞区以及限高等限制，威胁空中安全。幸运的是，该漏洞可以通过 Anti-rollback 机制来避免，防止无人机回滚到有漏洞的版本。

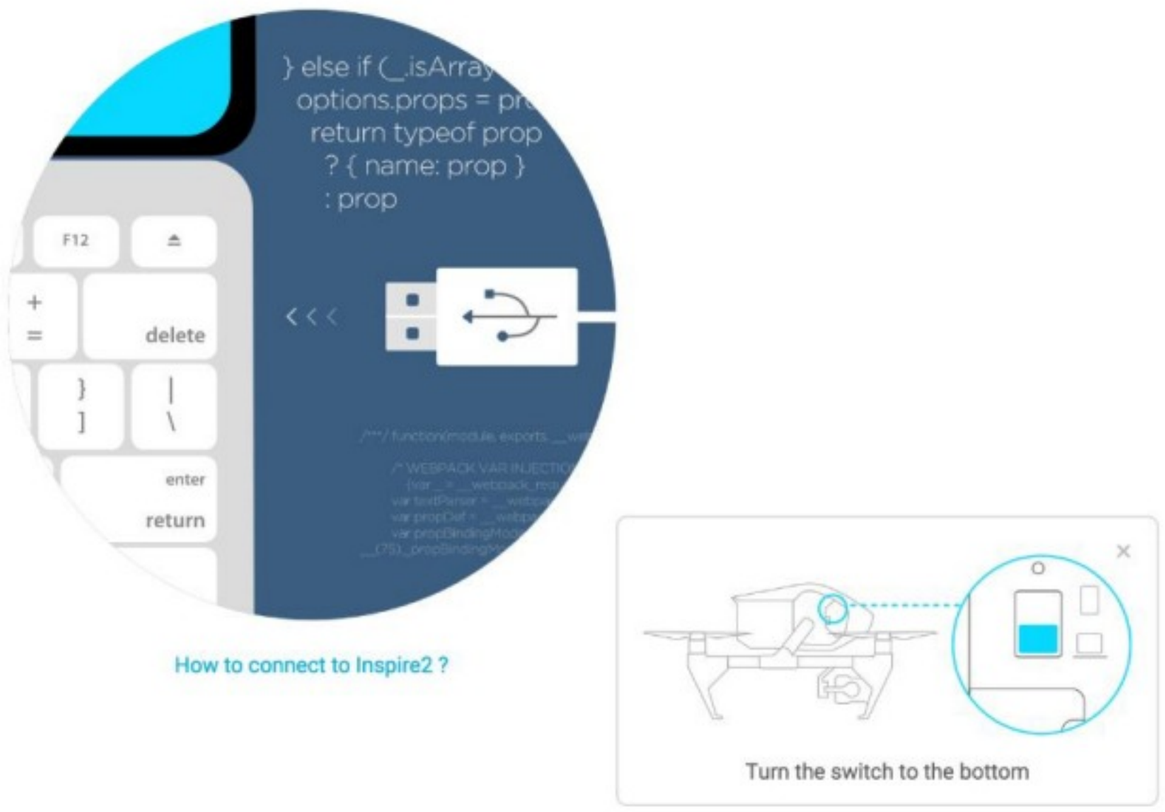


图 5.2　无人机升级工具

3. 固件隐私保护问题

近年来，无人机隐私保护的话题也越来越多了。

无人机飞行的地理位置和飞行时间等纪录，涉及到客户的隐私。

为了方便监管，起飞超过一定高度要登录用户的账户。例如：某公司无人机设计成必须登录账户才能解锁 30 米以上的飞行高度。

4. 固件安全测试

固件静态分析：一般用开源或内部定制的软件，对固件进行解包和扫描。发现的一些安全问题包括固件使用的操作系统存在漏洞，或使用到的开源软件有漏洞，还发现明文的密钥和证书等风险信息。当然，也可以分析二进制文件发现潜在的安全风险。

动态模拟执行：QEMU 是一个开源的模拟器和虚拟机，可以运行在多种操作系统平台上。它支持动态模拟执行，即在运行时进行模拟执行，可以用来模拟计算机系统的运行状态，从而对软件进行测试和调试。QEMU 的动态模拟执行功能可以用来测试固件的安全性，检查固件是否存在漏洞，并对固件进行安全测试。

有部分无人机操作系统采用了安卓，主要原因是使用的 AI 芯片原生态支持的就是安卓系统。在其上开发后，也延续了安卓操作系统。某些机型上可以对安卓进行 ADB 调试口激活和 root 系统，达到完全控制无人机的效果，这也是当前存在的一个安全风险。

固件安全加固

无论是为了防止攻击者获取到固件还是出于保护无人机知识产权的原因，厂商都应该对固件本身进行保护，防止第三方能直接访问固件。可以考虑采用数字签名技术来验证固件的真实性，数字签名是一种密码学技术，可以用来证明文件的完整性和真实性。通过使用数字签名，可以确保固件在传输和存储过程中不被篡改，并且只能由拥有合法私钥的实体进行签名。此外，固件还可以通过加密来保护其中的数据。加密可以使用密钥来对固件数据进行加密，升级程序将加密的固件传输到无人机中，无人机使用内置密钥进行解密。这样，即使无人机固件被拦截并篡改，攻击者也无法访问其中的数据。

为了阻止攻击者通过硬件手段获取到无人机系统的固件，针对嵌入式的 MCU，一般都会提供读写保护的功能，通过开启保护功能，限制硬件调试接口 SWD，JTAG 的滥用，保证片内数据不被提取。针对片外 FLASH，一般会将固件加密存放，而解密的 BootLoader 可以存放在不容易被破解的片内系统中，例如 BootROM 中。BootLoader 主要进行固件签名校验，成功后解密固件并且执行。

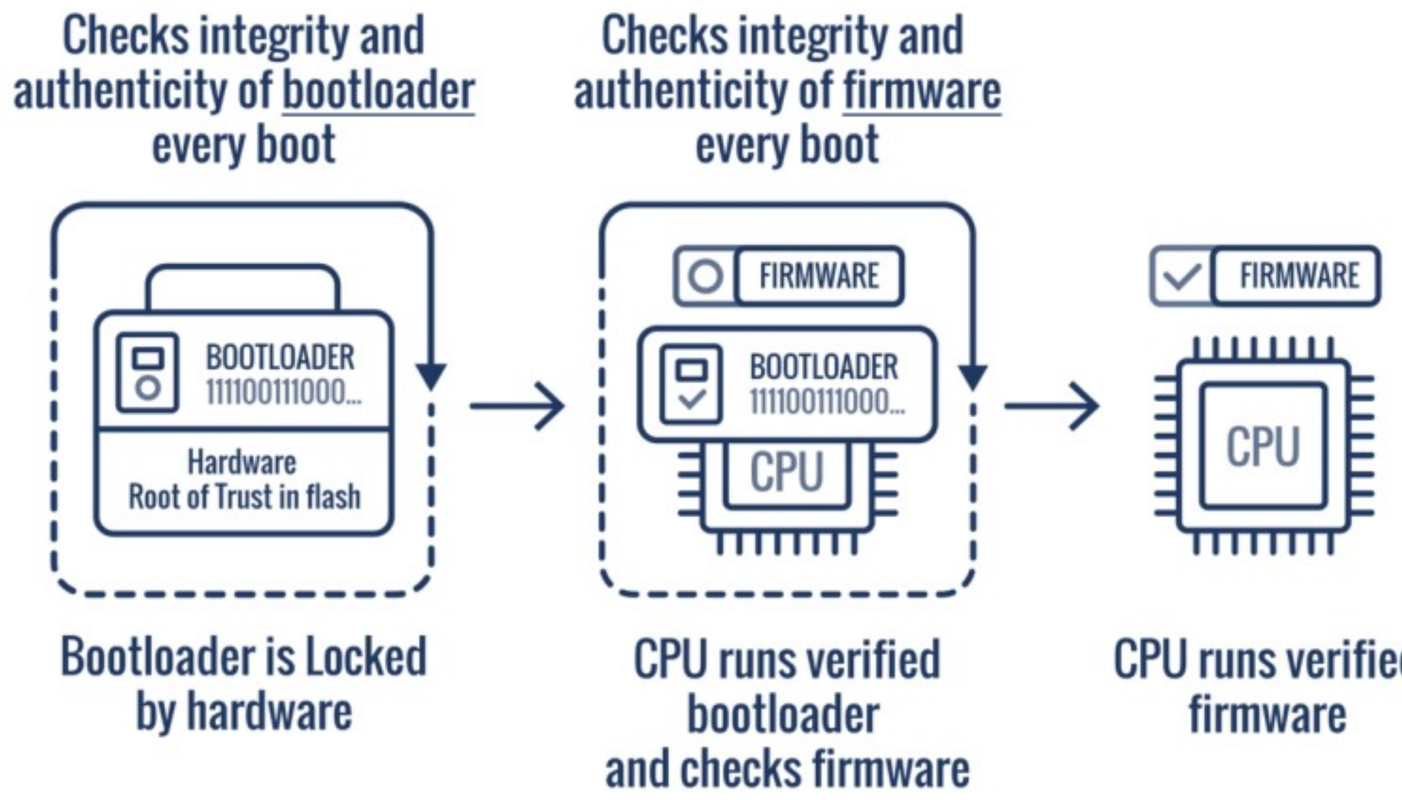


图 5.3　安全启动机制

5.2.2　软件服务

无人机的特殊性导致其软件的漏洞可能造成信息泄露、用户数据被任意读写。更严重的情况，漏洞可能被用于控制无人机的飞行功能，导致资产损失，甚至获得系统权限，突破禁飞、禁高等限制，并被用作从事危险活动，如运送毒品、地理测绘和军事行为[23]。

无人机上搭载的服务可以分为四种级别，根据它们对无人机系统的影响程度。这四种服务分别是：飞行控制程序、飞行支撑服务、调试服务和网络服务。

飞行关键服务，例如无人机飞行控制程序。该程序负责解析遥控器发送的指令，并进行状态反馈，执行智能飞行任务，进行主动避障等。如果该程序不提供服务，无人机将失去飞行功能，可能直接坠毁。

飞行支撑服务，包括 FTP 文件传输服务和 RTP 实时视频传输服务。FTP 服务负责无人机上的数据到手机 APP 控制端的数据传输服务，如果它不提供服务，无人机的状态就无法反馈。RTP 服务负责传输无人机的实时图像，如果它不提供服务，一方面智能避障算法可能失效，无人机可能被障碍物挂住；另一方面用户无法在手持遥控器上获取实时图像信息，可能导致误判无人机位置和飞行姿态，并产生危险的飞行行为。

调试服务，包括 ADB、TELNET 和 SSH 服务。这三种服务主要给无人机开发人员提供命令行窗口，以便输入指令和编写代码。虽然这些服务对无人机的飞行行为影响较小，但它们仍然是调试无人机的必备工具。

网络服务，包括 DHCP 和 mDNS 服务。DHCP 服务负责给连接到无人机上的终端提供动态地址分配的服务。如果 DHCP 服务不提供服务，控制端和无人机将失去连接，并触发失联

返航或原地降落算法。mDNS 服务提供主机发现服务，如果它不提供服务，连接到无人机的设备将无法互相发现，无法进行正常通信。

软件服务加固方法

除了提高代码质量外，也不能忽视第三方组件引入的风险，开源组件并不意味着一定安全，但使用稳定的最新版本能缓解 Nday 漏洞的利用。同时尽量减少软件服务的暴露面，关键端口服务尽量不直接暴露在外部，特别是 telnet、adb、ssh 这类调试服务，在发行版本不应该开启这些服务，防止攻击者通过暴露的软件端口攻击软件服务。另外，对于核心飞行服务进程可以考虑使用内存安全的 rust、golang 之类的语言进行重写，保证软件不出现内存安全相关漏洞。

5.2.3 无线通信

无人机基于无线网络进行通信，而在网络协议中存在的缺陷将导致非常严重的漏洞，攻击者可以利用这些漏洞通过网络发起远程攻击，夺取无人机的控制权。尤其是在协议的设计以及实现中，没有充分考虑其安全性，导致出现安全漏洞。

1. 无线信号的干扰

目前，地面遥控器和无人机之前通信已经普遍采用跳频、扩频技术，而且跳频参数还可以自适应，具有一定的抗干扰能力。对于这类信号的干扰思路是使用大功率设备对无人机控制信号进行全频段的噪声干扰。但是这类方法往往需要的信号功率比较强，同时会“误伤”同一频段的合法信号。因此为了尽可能让干扰更有针对性，一般会对无人机信号的频率特征、跳频参数、调制方式进行分析，进行更有针对性的干扰。目前针对无人机的信号干扰已经应用到反无人机系统中，如下图 5.4 就是一款反无人机枪，只需要将其对准无人机，该设备就会发射高功率的干扰信息，让无人机的通信系统瘫痪。

图 5.4　反无人机枪

应对建议

就无人机来说，使用长度较长的跳频序列可以很好的解决正常使用过程中的信息干扰问题，但是随着技术的发展，全频段干扰的设备变得非常普及，换句话说，针对信号的干扰是不可完全避免的。为了防止无人机信号被干扰后出现的意外，例如被捕获，可以设置无人机信号丢失后立刻返航。

2. 无线信号的嗅探

无人机无线信号常见的调制方式有 GFSK、QPSK、OFDM 等，要想对调制方式进行研究，除了可以分析信号波形特征外，还可以使用硬件手段，获取到无人机系统（包括地面遥控器以及无人机本体）的射频芯片型号。例如常见的 NRF24 系列芯片，使用 GFSK 的调制方式，工作在 2.4GHZ 无线频段，使用 GNU Radio 很方便进行解调。

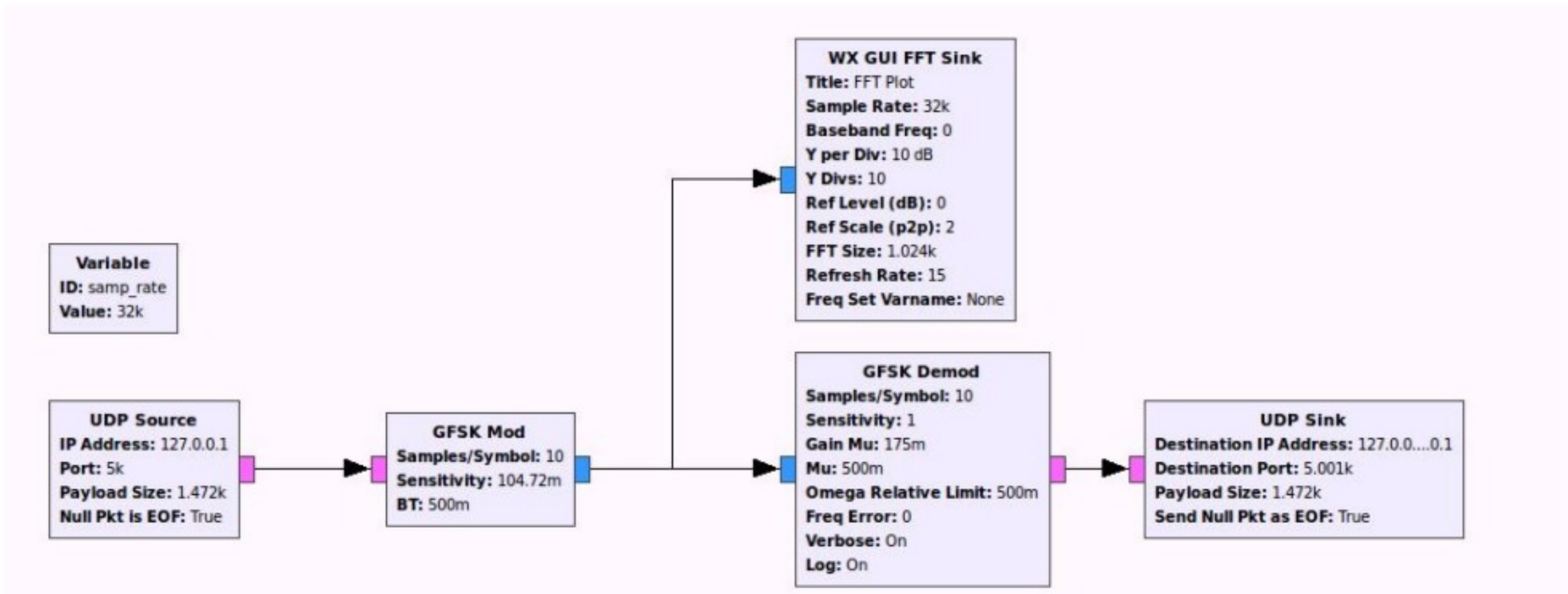


图 5.5　使用 GNU Radio 进行解调

无人机系统为了抗干扰，还会使用跳频技术来减少信号干扰，如果只在某个信道进行监听，会导致漏掉数据包，为了获取跳频序列，首先可以使用逆向手段对无人机固件进行分析，获取到其跳频参数设置，也可以使用逻辑分析仪嗅探 MCU 与射频芯片的通信来截获设置的参数。值得注意的是，一般来说跳频序列会在无人机出厂时进行写入，不同的无人机有不同的跳频序列，但是在无人机和遥控器对码的时候有可能在同一信道传输跳频序列，这就导致攻击者可能在空中截获该跳频序列。

应对建议

由于大多数无人机会使用现成的无线传输解决方案，无线信号的调制以及解调都是在射频芯片中完成，普通的无人机厂商无法对这一部分进行修改。为了让无线信号传输尽可能安

全，避免因为无线芯片带来安全问题，厂商应该在上层设计更加安全的传输协议，包括使用数据加密以及签名技术，并保证加密和签名密钥不被泄露。对于有能力自主设计射频芯片的厂商，尤其是军用级无人机，在设计射频芯片时应在无线传输过程中加入扰码，使用快速跳频且保证跳频序列的随机性，提高在物理层的可靠性以及安全性。

3. 无线信号的欺骗

在对无人机控制协议逆向的基础上，如果攻击者获取无人机的关键跳频参数，就可以对无人机信号进行调制，并发送到无人机中，这时，无人机系统在没有开启任何访问保护的情况下，会导致无人机被攻击者劫持，执行攻击者的任意指令，包括下降、起飞、方向控制等指令。好的设计不仅要在物理层考虑安全，在上层的协议设计中也应该加入访问管理，数据加密以及签名。

应对建议

无人机的 GPS 和遥控信号容易被欺骗，有几种潜在的技术方法可以防止。常用的有功率检测、到达角检测、多天线，这几种技术是在信号处理层面上检测欺骗干扰，需要额外的硬件开销，而且健壮性不高。一致性检测、加密认证应用于信息处理层面的技术，其中加密认证被认为是最具健壮性的一种技术，在防止无线信号被嗅探的基础上，进一步从协议设计上防止无线信号被简单的重放攻击，加强在身份验证上的保护。此外，使用多个冗余通信通道可以提供额外的安全性并有助于防止信号欺骗。

4. WiFi 攻击面

民用无人机经常使用 WiFi 网络在控制器和无人机之间进行通信，这很容易受到各种恶意攻击 [24]。

1）WiFi 协议栈漏洞

众所周知，WiFi 设备的网络协议安全性相当脆弱。对于无人机系统，会使用现有的无线解决方案来完成数据传输，尤其是以博通为代表的无线芯片厂商，这类芯片使用范围广，一旦出现安全问题经常无法通过简单升级固件来完成漏洞修复。在 2018 年安全研究人员就发现了 BroadPwn 漏洞，并使用该漏洞对智能设备完成了 RCE，而在 2021 年，国外研究员发现了 FragAttacks 系列漏洞，通过这一系列漏洞可以窃取用户的敏感信息，例如账号和密码，这说明 WiFi 协议实现仍然是一个巨大的风险点。

2）WiFi Deauth 攻击

Deauth 攻击全称为取消身份验证洪水攻击或验证阻断洪水攻击，通常被简称为 Deauth 攻击，是无线网络拒绝服务攻击的一种形式。Deauth 攻击的原理是 WiFi 管理数据帧没有被加密，导致攻击者可以伪造管理帧，从而让攻击者可以任意发送“取消认证”数据包来强行切断 AP 与客户端的连接。如果无人机的地面控制器和飞控之间使用 WiFi 进行数据交换，使用该攻击可以将地面控制器和飞控之间的链接断开，导致无法正常控制无人机。

3）WiFi 密码可预测

在基于 WiFi 控制协议的无人机系统中，正确的安全设计是让用户自己设置足够长度的密码去保证无人机不被非法访问，然而有一部分不安全无人机系统是使用无人机广播的 MAC 以及 SSID 动态生成密码进行连接，虽然这样表面上方便了用户使用，但是毫无疑问带来了安全问题，这样导致攻击者可以直接获取这些信息，并通过同样的密码生成算法获取连接密码来对飞控系统进行非法连接。

加固建议

厂商应及时做好漏洞管理，出现相关漏洞时应该及时推送补丁对射频芯片以及无人机本身进行缓解，同时使用增强型 WPA 或 WPA2 加密，这些加密方式可以有效防止攻击者伪造管理帧；做好安全设计，将 WiFi 密码的设置权交给用户，并保证密码的强度。另外，用户应该确保定期更新无人机的固件，以保证其具有最新的安全功能。

5. GPS 欺骗

民用无人机使用 GPS 进行导航时，暴露了一个可以执行 GPS 欺骗攻击的入口点。由于 GPS 信号未加密，因此很容易被欺骗或干扰，通过发送一个虚假的 GPS 信号覆盖来自卫星的真实 GPS 信号，从而有可能让无人机跟随攻击者想要的路径，这将有效地让攻击者完全控制无人机。

通过 GPS 欺骗攻击无人机可能有如下方式：

1. 欺骗无人机处在禁飞区内，如果无人机接收到伪造的 GPS 信号，并误以为自己正处在禁飞区内，根据无人机内部的工作机制，一旦处在禁飞区就会无法起飞，正在飞行的无人机会直接降落。

2. 欺骗无人机的“自动返航”的功能，有些无人机失去了信号，或者电量不足的时候，会执行“自动返航”的功能，那么通过发送虚假的 GPS 信号使得无人机认为自己已经处在返航点，那么无人机就会在当前位置降落。

应对建议

防止 GPS 欺骗的方法包括使用多种不同的定位技术（例如北斗定位系统、GLONASS 等）来校验 GPS 信号的准确性，并采用抗干扰技术来抵抗 GPS 欺骗。另外，在设计无人机时也可以考虑采用自主定位技术，这种技术可以通过无人机自身的传感器来确定位置，不依赖于 GPS 信号。另外，系统的安全措施也可以设计为当发现 GPS 信号存在异常时，自动切换到备用定位方式，以确保无人机的安全。

5.2.4 应用协议

Mavlink 是一种非常轻量级的消息传输协议，用于地面站与无人机（以及机载无人机组件之间）进行通信，在各种消费级无人机中应用非常广泛。但是 MavLink 在协议设计之初就没有实现安全访问功能，MavLink 的安全性依赖于底层协议，例如 WiFi 安全，无线跳频通信等。攻击者只要攻破了底层协议的安全性，那么 Mavlink 协议就毫无安全性可言。

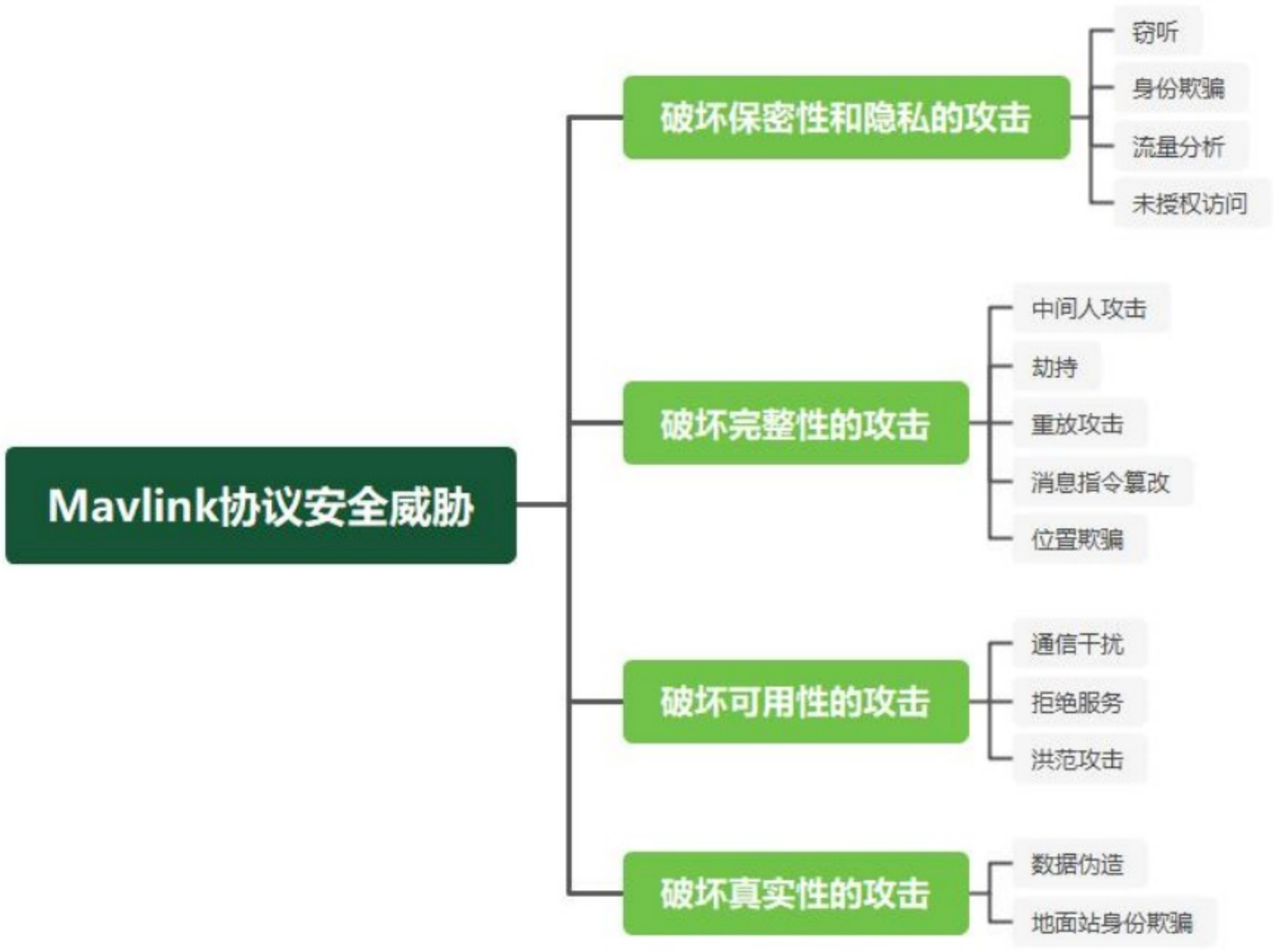


图 5.6　MavLink 协议安全威胁

加固建议：

由于 MavLink 是开源的，因此开发者可以直接在 MavLink 协议的基础上进行扩展，例如加入协议加密、数据签名、访问认证的部分，通过这样的方法进行加固后，即使攻击者能攻破物理层协议，但由于上层协议是加密签名的，依然可以保证无人机系统的通信安全。

5.2.5 传感器

1. 干扰陀螺仪

陀螺仪主要用于保证无人机机身平衡，一旦陀螺仪无法正常工作，很有可能导致无人机坠毁。在 2015 年，韩国先进科学技术研究院的研究人员，对无人机中的一个关键组件陀螺仪进行了共振测试，发现可利用声波使陀螺仪发生共振，输出错误信息，从而导致无人机坠落。为了保证无人机陀螺仪不受超声波干扰，厂商在研发产品时可对设备增加缓冲层，如增加一些覆盖材料，让外界声音进入不了陀螺仪，来防止由于传感器的声波或超声波干扰所造成的安全威胁，并为造成威胁的声音频率提供声音消除的功能；或者在设备上加装降噪装置，通过主动发射反向声音，抵消进行干扰的超声波，实现防干扰 [25]。

2. 攻击雷达传感器

毫米波雷达的原理与超声波的类似，但是电磁波传播速度更快，因此需要在发射端对其进行调制，在接收端对其进行解调。毫米波雷达主要用于无人机避障及测高，通过干扰雷达传感器，可以使无人机无法识别障碍物，造成飞行事故。即使用发射干扰的无线电波，输出干扰波形来干扰雷达传感器的检测。

3. 干扰超声波传感器

利用声波遇到物体会反射的原理，超声波传感器有助于无人机的着陆、悬停以及地面跟踪，将无人机保持在高于地面的恒定高度。通过向无人机发射精心构造的的超声波信号，可能会导致超声波测距输出 0 值或者最大值，甚至可以伪造任意数值。同时也可以使用消音装置，吸收传感器发送过来的超声波，利用这种方式，可以欺骗超声波传感器，使其产生错误的输出，导致无人机在测距时发生故障。

4. 攻击摄像头

摄像头作为无人机的“眼睛”，一旦失去了作用，就可以让无人机完全无法正常飞行。通过使用不同波长的光源可以致盲摄像头，主要原理是通过恶意的光束输入干扰 CCD/CMOS

传感器，使其无法识别图像，例如激光致盲，高强度的激光可以让 CCD/CMOS 传感器产生不可逆转的永久性损坏。

传感器加固建议：

传感器安全的重要性在于，传感器通常都会收集、处理和传输大量敏感信息，如果这些信息被非法获取，或者传感器被恶意篡改，都会导致无人机受到威胁。为了保证无人机传感器的安全，可以使用如下措施 [26]：

屏蔽：通过减少传感器对外部信号的暴露来抵御恶意攻击，主要包括物理隔离和攻击面缩减。物理隔离的目的是衰减进入传感器的外部物理干扰，例如电磁屏蔽、隔音、光屏蔽等。

滤波：在不影响正常信号的情况下衰减恶意信号。例如通过设计合适的低通滤波器去除高频攻击信号，避免交调失真或混叠的发生。当简单的滤波器不足时，防御者可以捕获环境中的攻击信号并使用自适应滤波有针对性地去除恶意信号。

随机化：增加传感器的随机性通常可以弱化攻击的影响。输入随机化将随机性增加在传感器输入信号流的控制上，例如将模数转换器的采样率进行随机变化，由于随机参数对于传感器来说是已知的，因此不会影响传感器的正常测量。输出随机化利用相似的思路增加传感器探测波形的随机性，适用于主动式传感器。

改进组件质量：通过重新设计传感器硬件，改进传感器中有缺陷的组件质量可以从根本上抵御一些外部攻击。例如，使用具有足够动态范围的放大器可以避免攻击者利用饱和现象；重新设计 MEMS 陀螺仪可以缩减共振频率的范围，降低其影响，从而避免声波注入。

传感器融合：由于攻击者难以同时攻击所有的传感器，因此通过融合多个或多种传感器在不同空间、时间或频率上的测量结果可以在一定程度上抵御攻击的影响。

5.3 无人机产品通用加固建议

1. 代码加固

无人机系统代码是由开发人员编写的，为了提高代码的安全性，必须提高开发人员的安全意识，遵守代码安全编写规范，严格杜绝危险函数的使用，尤其是在 C/C++ 开发中，特别容易引入内存安全问题，所以在开发无人机应用时，应该逐渐使用内存安全的开发语言 (go、rust、python) 逐步替换 c/c++。另一方面，无人机产品的很多的安全问题是使用了过时的依赖库引入的，例如过时的 OpenSSL 库、FTP 库等，为了不引入这些过时的版本，应该在保证兼容性的情况下，使用最新版本的依赖库以及操作系统。

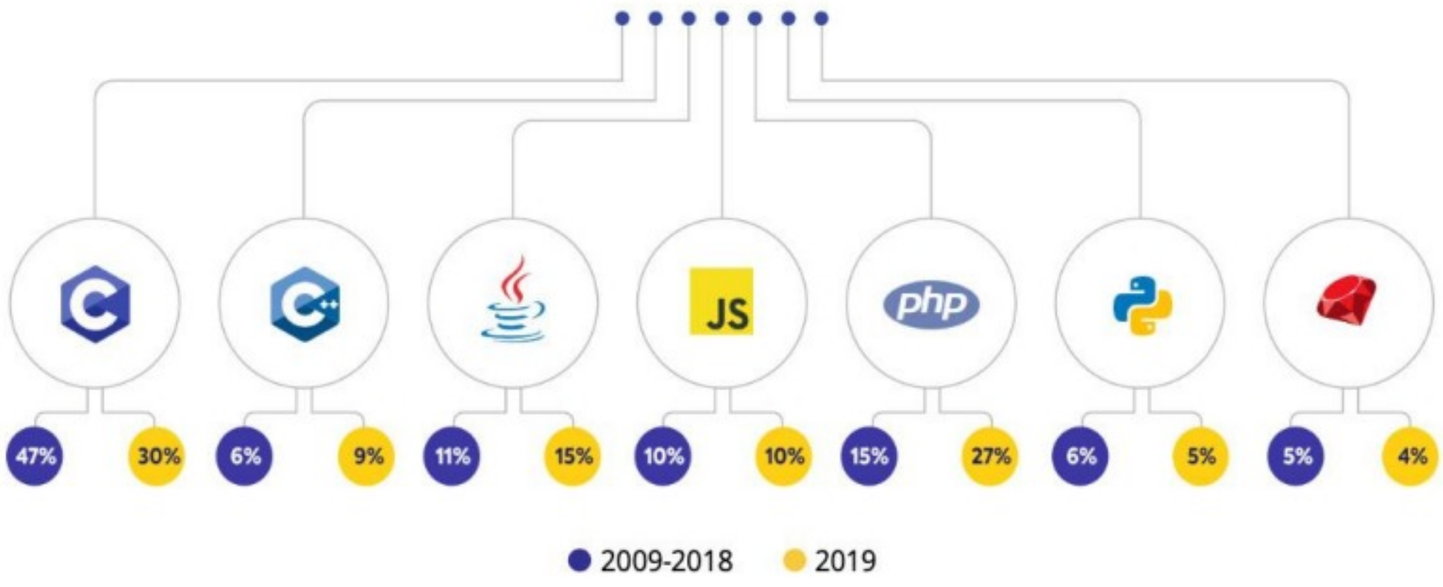


图 5.7　2019 年与 2009-2018 年每种语言的开源漏洞数对比图

2. 安全测试

在无人机产品开发过程中，不仅要进行功能性测试，还应该加入安全测试流程，例如使用自动化的源代码安全审计工具，这类审计功能往往可以支持多种开发语言，例如 c、c++、java、python 等，帮助开发人员发现产品中潜在的安全性问题。同时，也可以借助开源的模糊测试工具，编写 FUZZ 工具测试协议栈、解析库等代码的健壮性，模糊测试往往能发现静态审计工具发现不到的漏洞点。

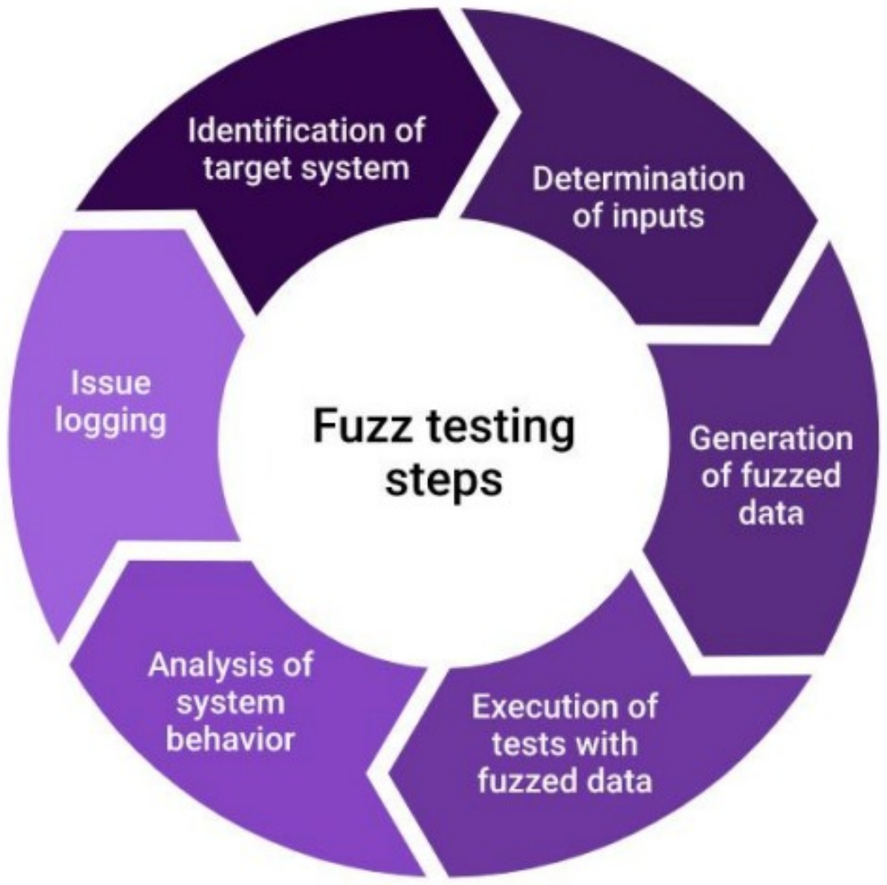


图 5.8　Fuzz 测试步骤

3. 漏洞管理

漏洞管理是指组织对无人机的软件和硬件系统中存在的漏洞进行管理和处理的过程。漏洞管理包括漏洞识别、分类、跟踪、修复等多个环节。漏洞管理的目的是防止漏洞被恶意利用，

保护无人机的安全。虽然在开发过程中加入了各种安全措施来提高代码质量，防止出现安全问题，但是仍旧不能保证无人机一定不会出现漏洞，所以无人机厂商应该鼓励安全研究个人和组织提交安全漏洞，一旦无人机出现了安全问题，厂商应该在合理的时间内完成漏洞修复，并且向用户推送最新版本的固件或软件。

图 5.9　漏洞生命周期管理

另外，可以采取最佳实践来提高无人机的安全性：

- 定期更新无人机的固件。当新的安全威胁出现时，主要的无人机制造商会发布补丁，所以定期更新有助于抵御黑客。
- 使用强密码。混合使用字母、数字和特殊字符来创建强密码可以阻止黑客非法访问无人机，避免不法分子入侵无人机信号。
- 如果使用智能手或笔记本电脑作为无人机控制器，请确保其安全，不要让它们受到恶意软件的感染。启用杀毒软件，不要下载安装来源不明的应用程序。
- 为可以连接到无人机的设备数量设置一个限制，这将防止黑客劫持信号来控制其他设备。
- 确保无人机有“返回家园”(RTH) 模式。一旦设置了返回点，在它失去信号、电池耗尽的情况下，将使无人机原路返回。但是，由于 RTH 依赖 GPS 工作，所以它不能免疫 GPS 欺骗。

06

未来发展

6.1 无人机技术发展方向

不论什么类型的无人机，都会在以下几个关键技术上寻求更进一步的突破：

1. 电池技术

聚合物锂电池作为无人机目前主要的动力来源，是直接制约无人机发展与应用的关键因素。近年来，锂电池等无人机零部件的价格持续下降，削减了无人机的整体成本，但不可否认的是，无人机锂电池续航时间短，仍是限制无人机行业发展的一块短板，也是世界各国发展无人机亟待攻克的技术性难题。

在今年 11 月召开的中国 (遂宁) 国际锂电产业大会暨新能源汽车及动力电池国际交流会上，中国科学院院士孙世刚表示，我国锂电产业现有的发展面临着资源、能量、安全、使用环境等四方面重大挑战，要从材料、界面、传输、系统等四个层面解决当前存在的问题。锂离子电池的能量密度限制了多场景的应用，要提高无人机等装备的航速和航程，都需要大幅度提高电池的能量和功率密度。对下一代非锂电池的展望中，钠离子电池被看好，钠离子电池的发展需要在储钠新材料、新型电解液方面有所突 [27]。

另一个重要的发展趋势是，电池充电速度正在加快，使电池能够在较短的时间内完成充电。电池效率提升意味着续航和稳定性的提升，将会拓宽更多无人机应用场景。

2. 通信系统

无人机通信系统，目前主要使用 900MHz、1.4GHz、2.4GHz 无线电频段，其中 1.4GHz 主要作为数据通讯频段，2.4GHz 主要作为图像传输频段，900MHz 不建议使用。工信部已经制定无线电相关使用准则，规范无人机行业的无线电频段使用。公共无线电通信链路，抗干扰能力弱，尤其是同频干扰无法避免。

军用无人机受干扰的影响会相对较小，首先军用无人机从设计之初就有抗强干扰的考虑，为此会采用抗干扰能力更强的电台，此外，军用无人机的飞控系统和传感器也会采用军用标准，这些都有助于提高抗干扰能力，未来军用无人机抗干扰的技术仍将持续精进。但是对于民用无人机尤其是消费级无人机，要在软件和硬件方面投入大量的精力与成本来获得更强的抗干扰能力，消费者未必愿意为此买单，因此随着消费级无人机的数量指数级增长，其通信系统干扰的问题将日渐突出 [28]。

3. 定位导航

无人机的定位功能是无人机自主导航的前提，常见的定位技术包括以卫星定位 GNSS 为代表的信号定位、以激光雷达定位为代表的环境特征匹配定位，以及惯性导航定位。这三种方式各有优劣[29]。

表 6.1　定位技术优缺点对照

定位技术	优点	缺点
信号定位	全天候、全天时、位置准确	依赖卫星信号，在信号丢失时，无法定位，易受电磁环境干扰
环境特征匹配定位	可获得周围环境的 3D 信息	传感器受天气、环境、光线影响大
惯性导航定位	不依赖于外部信息，强自主性，数据更新频率高	存在累计误差

一个完整的可在各种环境下稳定悬停的无人机，安装了 GNSS、惯性测量单元 (IMU)、指南针、气压计和辅助定位系统。GNSS 通过卫星定位系统提供了最基础的位置信息，民用 GNSS 的定位精度通常在 1 到 5 米之间；辅助定位系统包括但不限于视觉里程计、红外和超声测距仪、激光雷达、定位基站等，在卫星定位信号弱甚至完全没有卫星定位的复杂环境下帮助飞机确定位置和高度。在消费级无人机身上，最常用的就是视觉里程计，它包含了下视视觉定位和视觉避障两大部分。

未来，使用到无人机障碍回避、物资投放、自动进场着陆等功能的场景会越来越多，需要高精度、高可靠性、高抗干扰性能，因此多种导航技术结合将是未来发展的方向。

4. 避障技术

避障技术对于无人机来说至关重要，因为它能够帮助无人机避开障碍物，确保公共安全。目前，现有的避障解决方案仍处于探索阶段，需要不断改进传感器、算法和无人机设计来确保效果。主流的无人机避障技术有四套解决方案：超声波避障、红外避障、视觉避障和激光避障，每种方案都有其优点和局限性，需要根据实际需求来进行选择。

5. 自动飞行

这项技术的目的是使无人机能够自主地完成一定的飞行任务，而无需人工干预。为了实现自主飞行，无人机通常会装备一系列的传感器，例如高度计、罗盘、GPS 定位器、雷达等，

并利用这些传感器来收集周围环境的信息系统，进行故障响应、动态路线制定和校准。这些技术的发展将在矿场采集、管道运输监控以及建筑相关的场景中发挥极大作用。

6. AI 算法应用

随着无人机技术的发展，无人机的算力提高，将更复杂的 AI 算法放在无人机本体成为了可能，使用基于 AI 的路径规划和机器视觉技术，使得无人机更加智能。此外，人工智能算法还可以用于无人机的图像识别，通过分析无人机拍摄的图像，来识别周围环境中的物体、地标等。在农业、森林监测等领域，人工智能算法还可以用于无人机的作物健康监测和病虫害检测。

7. 网联无人机

未来无人机不再作为一个单一节点运行，会连接到互联网中，使用 5G、6G 技术链接到云上，通过网联技术，无人机能够在互联网的信息指令下，实现联合任务的执行。网联无人机通常采用多无人机协同工作的方式，能够实现更加高效和精确的作业。例如，在军事领域，网联无人机可以实现多架无人机协同执行搜索和攻击任务；在商业物流配送领域，网联无人机可以实现多架无人机协同执行配送任务，提高配送效率。总之，网联无人机是一种拥有广泛应用前景的新型无人机技术。

6.2 反无人机技术发展趋势

近年来各国纷纷推出应对无人机威胁的策略。美国军方将无人机列为最具破坏力的空中威胁之一，并制定出《反无人机系统战略》予以应对。俄罗斯军方将无人机防御作为重要任务，并在叙利亚战场上演练反无人机技术。英国则将应对蜂群无人机列为重中之重，探索使用射频抑制器干扰蜂群无人机链路的方法。在民用领域，由无人机造成的个人隐私泄露、危害民航飞行安全等事件也日益增多。因此，对反无人机技术的需求也在持续增加。

从广义上讲，反无人机解决方案和措施可分为三种类型：检测、非交互措施和拦截[30]。

应对无人机威胁的第一步是利用声学、热学、雷达、视觉等传感器或无线电频率 (RF) 检测到无人机的存在。由于这些属于非侵入式检测工具，因此通常不仅对政府机构、警察和军队开放，而且也对公司和个人开放。一旦识别出恶意无人机并认为其正前往受限或易受攻击的区域，可以采取两种方法来应对威胁：1) 采用非交互式措施来减少无人机对设施的影响；2) 立即采用拦截方法，将无人机移除。

图 6.1　反无人机解决方案和措施

考虑到拦截工具的法律限制和昂贵程度，许多场景下通常首先采用非交互式反无人机措施，包括发出警报或遮挡窗户以中止间谍活动、关闭 WiFi 以避免网络攻击等。在拦截措施中，向无人机发射大功率射频信号，可扰乱通信，使其无法执行任务或坠机；由传统防空火炮、导弹组成的拦截火力网，是目前应对无人机作战的主要手段之一；激光束在应对“低慢小”无人机时，展现出快速、灵活、精准、效费比高等优势。

上述提到拦截方法各有利弊，未来反无人机技术预计会在以下两个方面进一步发展。

1. 更加具有针对性

目前对无人机的信号干扰一般是针对指定频段进行信号干扰，例如消费级无人机大多数都工作在 2.4GHZ 频段，不同国家频段不同。这种攻击手段容易干扰正常工作的 WiFi 及蓝牙信号，甚至是合法飞行的无人机。为了克服这些缺点，首先需要针对特定型号无人机的信号特征进行分析来获取到相关信息，如频率特征、跳频参数、导航类型等，在完成分析之后可以对某种型号的无人机进行有针对性的信号压制及欺骗，甚至劫持无人机。

2. 更加智能化

地面的反无人机武器使用激光或者导弹直接打击无人机使其坠毁，但是由于无人机技术不断发展，无人机的速度和操作范围也在不断增大，这就需要反无人机武器有能力对快速移

动的无人机进行有效攻击，未来的发展方向必然是自动化的发现、识别、跟踪无人机目标，包括使用光学传感器或雷达来侦测和跟踪无人机，并有针对性地攻击无人机。

6.3 无人机防护发展方向

隐身化是目前军用无人机发展的重要方向之一，是高端无人机的重要技术瓶颈之一。隐身技术是对目标特征信号进行有效控制和抑制的技术，主要包括雷达隐身、红外隐身等。针对高空、长航时察打一体无人机，具有隐身设计能够应对更复杂的战场情况，具备穿透敌方防御系统而不被发现的能力，可潜入敌方区域，开展情报监视侦察活动，并利用携带的武器实施打击。同时具有隐身性能的无人机可以配合有人作战飞机，担任有人作战飞机的僚机，执行目标指引、前出探测、干扰诱骗及武器投放等协同任务，从而更好地提升其实战能力。

表 6.2 隐身技术分类

隐身技术	分类
雷达隐身	外形隐身
	吸波材料隐身
红外隐身	降低材料温度及其红外发射率
	遮挡技术

在消费级别，部分使用者不仅仅满足于正常操控无人机，而是想要对无人机进行“破解”从而绕过厂商本身的各种限制，尤其是绕过禁飞区的限制，无人机的破解一般指的是使用漏洞获取无人机的 Root 操作权限。这就使得无人机厂商不得不对无人机进行加固，除了定期更新无人机的软件和固件，以消除已知的安全漏洞外，还需要从硬件层面着手进行防护。目前有相当多无人机的硬件保护缺失，尤其是在中低端无人机市场，由于开发人员缺少安全意识，导致黑客可以使用硬件手段攻击无人机，例如重新刷入恶意固件，通过故障注入绕过 MCU 的读写保护机制，直接获取无人机的最高权限。而随着国家对无人机安全的重视，未来厂商需要在硬件层使用诸如安全芯片等技术来保证无人机的安全。另外，为了防止针对消费级无人机的劫持攻击，可以在软件层面使用账号绑定技术，防止不法分子直接使用无人机。

参考文献

[1] DRONE MARKET MAP: THE DRONE WORLD IN AN INFOGRAPHIC
https://droneii.com/drone-market-map-2022-drone-world-infographic

[2] 无人机行业深度报告：市场空间、竞争格局、商业模式分析
https://finance.sina.com.cn/stock/stockzmt/2022-07-22/doc-imizirav4994824.shtml

[3] 如果你关注无人机，那么你有必要对这 100 家公司做个了解
http://www.zytln.com/news-about.asp?id=191

[4] 预见 2023：《2023 年中国无人机行业全景图谱》
https://www.qianzhan.com/analyst/detail/220/221111-d56f7f77.html

[5] WHAT ARE THE TOP DRONE APPLICATIONS?
https://droneii.com/top-drone-applications

[6] DRONE APPLICATION CATEGORIES AND METHODS
https://droneii.com/wp-content/uploads/2022/04/Drone-Application-Methods.pdf

[7] 2021 无人机云数据统计报告
https://www.163.com/dy/article/HELBLUHO0553BLNF.html

[8] 2022 年中国民用无人机行业发展现状及未来发展趋势分析
https://www.chyxx.com/industry/1112353.html

[9] The global military drone market is projected to grow from $11.73 billion in 2022 to $30.86 billion by 2029, at a CAGR of 14.82% in forecast period, 2022-2029
https://www.fortunebusinessinsights.com/military-drone-market-102181

[10] World military expenditure passes $2 trillion for first time
https://www.sipri.org/media/press-release/2022/world-military-expenditure-passes-2-trillion-first-time

[11] 航空装备深度报告：军用无人机
https://pdf.dfcfw.com/pdf/H3_AP202208051576939822_1.pdf?1659726441000.pdf

[12] 欧盟无人机立法的新近发展与启示
https://finance.sina.com.cn/jjxw/2022-03-31/doc-imcwiwss9110142.shtml

[13] 美国无人机立法新动态及其启示
http://html.rhhz.net/BJHKHTDXXBSKB/20190116.htm

[14] 民用无人机法律规制研究
http://att.caacnews.com.cn/zsfw/ysfw/202201/t20220117_60581.html

[15] The Drone girl

https://www.thedronegirl.com/

[16] DRONE INDUSTRY INSIGHTS

https://droneii.com/

[17] Threat Intelligence for Drones

https://dronesec.com/

[18] 2022 第六届世界无人机大会

http://www.droneworldcongress.com/mobile-cn/

[19] 黑客改装大疆无人机，飞到金融公司楼顶通过 WiFi 入侵内部系统

https://www.secrss.com/articles/47921

[20] 反无人机空防作战新特点

http://military.people.com.cn/n1/2022/0726/c1011-32485825.html

[21] 俄乌冲突中的无人机运用

https://mp.weixin.qq.com/s/sZhP7-vJWIIXNG3EeuFXYw

[22] Drone Hacking Tool Analysis: DroneSploit

https://dronesec.com/blog/drone-hacking-tool-analysis-dronesploit

[23] 基于模糊测试的无人机软件系统漏洞挖掘研究

[24] Drones for Smart Cities: Issues in Cybersecurity,Privacy, and Public Safety

https://eps.fiu.edu/wp-content/uploads/2017/12/drones.pdf

[25] 利用声波和激光笔干掉无人机

https://www.aqniu.com/hack-geek/22654.html

[26] 传感器换能攻击方法和安全防护方法简介

https://www.163.com/dy/article/GDDQL04V0511SD1E.html

[27] 中科院院士孙世刚：现有锂离子电池的能量密度已接近理论极限

https://wallstreetcn.com/articles/3674558

[28] 无人机发展的痛点及技术瓶颈

http://k.sina.com.cn/article_7517400647_1c0126e4705901ddxu.html

[29] 2020 年中国惯性导航行业概览

https://pdf.dfcfw.com/pdf/H3_AP202010191422327550_1.pdf?1603126124000.pdf

[30] Anti-Drone Solutions: Possibilities and Challenges

https://droneii.com/anti-drone-solutions-possibilities-and-challenges

NSFOCUS

CEPREI 中国赛宝实验室（工业和信息化部电子第五研究所）

THE EXPERT BEHIND GIANTS

巨人背后的专家

扫描绿盟科技官微二维码
可在手机端直接观看报告电子书

东西智库 | 专注中国制造业高质量发展

东西智库，专注于中国制造业高质量发展研究，主要涵盖新一代信息技术、数控机床和机器人、航空航天、船舶与海工、轨道交通、节能与新能源汽车、电力装备、农机装备、新材料、医疗器械等制造强国战略十大领域，并提供战略咨询、规划编制、项目咨询、产业情报、品牌宣传等服务。

欢迎加入东西智库小密圈，阅览更多制造业精选信息