中国联通 China unicom

中国联通 5G 网联无人机

系统安全架构白皮书

中国联通研究院

2023 年 6 月

版权声明

目 录

前 言

近年来，无人机产业发展迅猛，已经呈现出高起点、高爆发、高成长等特性，作为朝阳产业，无人机数量与日剧增，随着无人机产业规模不断壮大，无人机安全事件不断增多，网络安全问题已成为限制无人机产业发展的障碍之一。本白皮书从无人机系统安全威胁与趋势出发，全面分析无人机产业面临的各维度安全风险，构建全体系无人机安全架构方案，并从政府监管、产业发展角度提出保障无人机系统安全健康发展方向及建议。

编写组成员（排名不分先后）：

魏进武、周晶、关蕾、杨双仕、张成岩、贾宝军。

一、概述

（一） 无人机产业发展情况

无人机行业是指从事无人机研发、生产、销售及售后服务等众多企业的集成组合。无人机产业链具体可分为上游、中游、下游。

无人机产业链上游是指无人机硬件和软件生产，主要包括电子元器件行业、电池、飞控系统开发、原材料等关键零部件生产，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。

无人机产业链中游主要是工业无人机生产与制造厂商，整机制造包括飞行系统、地面系统、任务载荷系统三个方面，是无人机制造的核心部分。

无人机产业链下游聚焦行业应用场景，主要应用于航空拍摄、灯光表演、农林植保、灾难救援、物流运输、电力巡检、公共安防、环境保护等领域。

目前，“无人机+行业应用”是民用无人机发展的主流方向，有着广阔的应用前景，在应用领域多元化的背景下，未来会有大量的企业进入无人机下游应用服务环节，向市场提供针对特定场景的专业化服务。从国内市场来看，随着无人机民用化进程的加快，我国无人机行业快速发展。据 Frost & Sullivan，2019 年中国民用无人机市场规模为 434 亿元，其中工业级无人机 151 亿元，消费级无人机 283 亿元，预计 2024 年民用无人机市场规模将超过 2000 亿元。根据工业和信息化部印发了《关于促进和规范民用无人机制造业发展的指导意见》预测，预计到 2025 年，民用

无人机产值达到 1800 亿元，年均增速 25%以上。

数据来源：工业和信息化部、Frost & Sullivan

（二）网联无人机简介

网联无人机是指接入低空移动通信网络的无人机，它与传统无人机最大的区别是采用了移动通信网络来承担无线数据通信工作，5G 蜂窝移动网数据链提供的高可靠、低时延、大带宽网络，取代了传统无人机数据通信链路点对点连接方式。5G 网联无人机在无线网状网络中，节点是互连的，通常可以直接在多个链路上进行通信，从而使无人机飞行范围更广，安全性和可靠性更高，成本更加低廉，无人机承载的业务范围变得更加广阔。

二、网联无人机安全发展现状

（一）网联无人机系统架构

网联无人机受到信息安全攻击与其系统架构有关。作为一个集传感器、控制器、通讯设备、业务载荷装置于一体、高度集成的信息物理系统，无人机系统架构与工业控制系统架构具有极高的相似性。网联无人机系统是指网联无人机及其配套的六大部分组成，包括飞行控制系统、通信导航系统、机载终端、任务载荷以及安全飞行管理系统。各系统间架构如下图：

图 1 网联无人机系统架构

无人机各子系统有以下特点：

1. **飞行控制系统。**结构微型化、轻量化，可靠性高，稳定性好，系统智能化，高效实用。
2. **通信和导航系统。**低时延、大带宽、超视距远程控制，路径规划、

自主导航，高精度定位，具有集群飞行能力。

3. **机载终端。**具有环境感知、智能识别及二级应用开发等能力。
4. **任务载荷。**载荷设备小型化、轻量化、多样化。具有载荷数据的实时联网传输、本地或云端的智能化分析能力。
5. **安全飞行管理系统。**适航认证，具备安全加密能力。

（二）无人机安全事件

随着电子信息和无人系统技术的快速发展，无人机作为新兴的智能装备产品，广泛应用于农业植保、电力巡线、道路巡检、消防救援等行业应用领域。然而，在无人机应用领域不断扩展的同时，其深度融入各领域后面临的安全问题日益凸显。

- 2018 年 5 月西安无人机表演出现严重事故，1374 架无人机并没有成功组成完整图案。事后对无人机进行数据分析表明：部分无人机的定位及辅助定位系统在起飞后受到定向干扰，造成其位置和高度的数据异常。
- 2021 年 1 月 25 日晚间，重庆朝天门广场无人机编队飞行表演突然撞向了附近一幢大楼，导致约百架无人机坠落。分析显示控制飞行的主机死机导致了事故发生。
- 2021 年 10 月 1 日晚 9 时许，河南郑州高新区一广场无人机表演突发故障，集体“炸机”，多架无人机失控从高空坠落。

从上述比较引人注目的无人机安全事件可以看出，无人机在现在规模化使用过程中，正在暴露一系列的安全隐患和监管漏洞，这类安全问题对社会和个人都会造成一定影响，需要在政策层面在不断完善和加强管理，因此近年来，国内对无人机监管政策也更加趋于严格管理。

（三）无人机安全相关法律法规

国内无人机相关法律法规监管政策，整体趋严，彰显政府推进行业规范化发展的决心。但是在无人机系统网络安全、信息安全方面相关标准以及法律法规相对缺乏，必须加强探索，予以重视。

2013 年，《民用无人驾驶航空器系统驾驶员管理暂行规定》，由中国 AOPA 协会负责民用无人机的相关管理。

2014 年，《低空空域使用管理规定(试行)》征求意见稿，将低空空域分为管制空域、监视空域和报告空域，其中涉及监视、报告空域的飞行计划，企业需向空军和民航局报备。

2015 年，《轻小型无人机运行试行规定》，起飞全重 7 公斤以上无人机，必须接入“电子围栏”，不得在禁飞区使用无人机，无人机驾驶员需要持有操作执照。

2016 年 9 月，《民用无人驾驶航空器系统空中交通管理办法》，保障民用航空活动的安全，加强民用无人机飞行活动的管理，规范其空中交通管理的办法。

2019年12月,世界上第一个通过ISO认证的无人机安全标准公布。国际无人机系统安全和质量标准（UAS）的最终发布将对全球无人机行业的未来发展产生巨大影响，并且是多年合作和严格审问的产物来自社会各界。这些标准还试图解决公众对隐私和数据保护的关注，要求运营商必须拥有适当的系统来处理数据，以及在飞行时进行通信和控制计划。所有相关操作设备的硬件和软件也必须保持最新。重要的是，所有无人机飞行（包括自主运行）都需要人为干预的故障安全措施，以确保对无人机操作员负责。

2021 年 1 月，国家标准委下达了《民用无人机产品安全要求》等 55 项强制性国家标准制修订计划和 5 项强制性国家标准外文版计划。据了解，本标准规定了民用无人机的运行安全要求、整机安全要求、使用说明书要求等内容。本标准的基本要求主要对民用无人机的标志、标识、产品合格证进行了规定；运行安全要求主要从对运行过程中遇到的风险进行限制的角度，规定了空域保持要求、身份识别要求、地理围栏要求、感知与避让要求、应急处置要求等；其中整机安全中的无线电抗干扰要求提出了无人机无线电发射功率、频段、频率应满足国家规定的要求，不影响现有国家的通信安全，也不对操作者、附近相关人员造成电磁辐射伤害。

三、网联无人机安全威胁分析

（一）网联无人机安全风险原因

1. 系统安全漏洞

随着无人机技术的快速发展，无人机的系统组成和飞行机理正日益复杂，因此无人机的信息安全已经不仅仅存在于软件和网络层面，而是包含硬件、传感器、通信链路等多个方面。很多无人机以及地面站通常使用智能化的开源操作系统，无人机的载荷设备也大多都有自己的操作系统，这些系统可能会存在系统漏洞未修复的情况，攻击者会利用这些漏洞入侵无人机或者地面站，进行攻击、劫持或者盗取数据。

2. 受到数据干扰易拦截

现代无人机通过地空间的通信链路提供的必要控制信息来实现飞行指挥和控制。因此，如针对这些通信链路进行干扰、窃听甚至是截获和篡改等信息安全攻击，则可以对无人机飞行产生直接的影响。在无人机通信中，通常在接收有用信号的同时，不可能完全抑制外部干扰，致使通信接收系统检测有用信号时必然存在着不确定因素。当前无人机地空通信链路普遍存在着频点公开、链路透明、缺乏保密措施等问题，极易成为各种攻击手段的目标。攻击者有机会对无人机进行数据拦截，恶意数据注入以及更改预设飞行路线等操作。

3. 飞行过程易被欺骗

无人机对卫星导航信号有着巨大的依赖性，其飞行控制一般都离不

开 GPS 等卫星导航系统提供的重要位置和速度数据，为此，如果对无人机所使用的导航信息进行欺骗，则有可能干扰无人机的正常飞行路径，通过 GPS 欺骗，可以轻松地捕获，修改或注入信息。数据通信传输链路中的这些漏洞可实现拦截和欺骗，从而使攻击者能够完全控制无人机。

4. 易受到外界条件影响

此类问题通常与缺乏稳定的连接有关，特别是在具有挑战性的自然原因下（寒冷、 潮湿、过热等）。同时在极端自然条件下，无人机电池寿命使用寿命会缩短，从而缩短飞行时间，并可能出现故障。

（二）网联无人机安全风险类型

1. 导航系统攻击

现代无人机对卫星导航信号有着巨大的依赖性，其飞行控制一般都离不开 GPS 等卫星导航系统提供的重要位置和速度数据，为此，如果对无人机所使用的导航信息进行欺骗，则有可能干扰无人机的正常飞行路径，迫使其在事先不知情的情况下偏离正常的飞行路线并出现在不应出现的区域，从而起到接管无人机的效果。原理是向无人机的控制系统发送虚假的地理位置坐标，从而控制导航系统，诱导无人机飞向错误的地点。由于无人机接收 GPS 信号总是以信号最强的信号源为准，因此在地面人造的 GPS 信号只要强度足够大，就可以覆盖真正的 GPS 信号，从而欺骗无人机的定位接收模块。

2. 飞控信号劫持

由于无线信号是无人机和控制者之间的主要通信方式，对无线信号的攻击可以直接影响无人机的正常运作，乃至获得无人机的控制权。攻击者利用干扰器产生无人机飞控干扰信号以及卫星定位干扰信号，通过对无人机的上行飞控信道和卫星定位信道进行阻塞式干扰，从而使其失去飞控指令和卫星定位信息，使之无法正常飞行，根据无人机的设计不同会产生返航、降落以及坠落的管控效果。

3. 飞行控制软件安全漏洞

无人机系统包含大量的软件平台，如指挥控制系统、飞控导航系统及与地面站联系的相关软件等，这些软件系统保证无人机的飞行、任务执行、信息采集和数据回传等功能正常运转，是无人机系统重要的组成部分。恶意攻击者可能通过邮件钓鱼、信息挖掘、供应链攻击等社会工程学手段对无人机系统进行攻击，或进行非授权软件安装执行、利用身份认证缺陷绕过认证机制进行越权攻击等。这些攻击方式都可能导致系统卡顿、崩溃、关键文件泄露甚至控制权被夺取等问题，给系统带来极大安全风险。

4. 通信链路攻击

网联无人机高度依赖地空通信链路提供的必要控制信息来实现飞行指挥和控制。因此，如针对这些通信链路进行干扰、窃听甚至是截获和篡改等信息安全攻击，则可以对无人机产生直接的打击后果。当前主要的无人机地空通信链路也普遍存在着频点公开、链路透明、缺乏保密措

施等严重的问题，极易成为各种攻击手段的目标。

四、网联无人机安全技术策略

（一）网联无人机安全技术策略整体框架

由于无人机具有动态性、移动性等特点，因此网联无人机系统的安全体系要充分考虑无人机的特殊要求。网联无人机系统主要包括无人机终端、4/5G 网络、管理平台，无人机的安全技术策略框架要重点解决终端侧、网络侧、平台侧的安全问题，其中终端侧安全主要提供安全可信的无人机软硬件系统，抵御针对传感器、数据、系统等的恶意破坏；网络侧安全以轻量级密码认证为基础，构建从物理层到网络层的无人机网络可信互联，抵御窃听、假冒、篡改等网络攻击；平台侧安全通过软件可信、数据加密保护和鉴权认证等措施，防止非法软件滥用、数据窃取和非法终端接入；基础安全管理提供无人机设备、安全策略、密钥、漏洞、身份的管理，并可呈现无人机系统的整体安全态势。

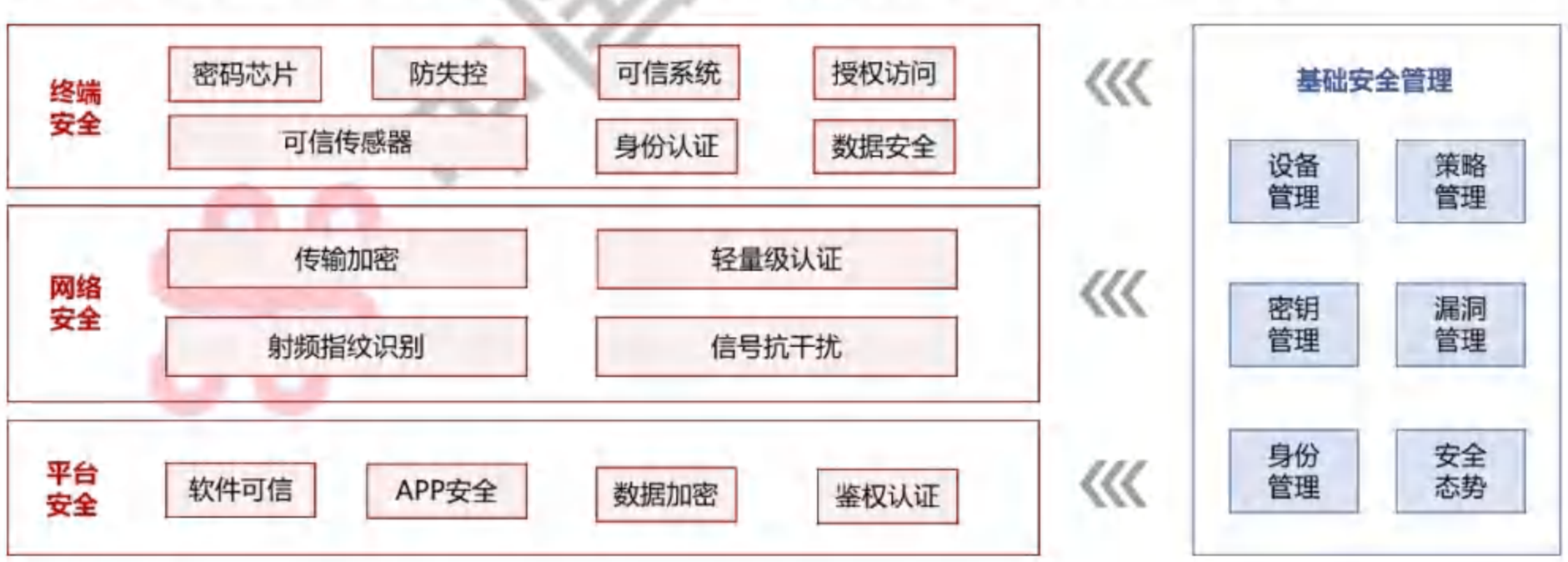

图 2 网联无人机安全技术策略框架

（二）终端侧安全防护技术策略

终端侧安全基于可信计算、数据安全等技术，以可信模块为基础，构

建可信软硬件系统，建立自底向上的可信链，确保无人机终端软硬件环境的安全可信，将可信度量结果与基线核查结果共同作为安全度量参数，为构建可信网络环境提供支撑。

1. 隐私计算

无人机终端在运行过程中会产生大量飞行数据，包括飞控数据、采集数据等重要敏感数据。终端在计算、处理这些敏感数据时，为了防止数据泄露，保护数据安全，必须进行安全防护。隐私计算主要是解决数据不出本地，在保护数据安全的同时实现运算的问题。隐私计算技术可以在不暴露数据本身的前提下，实现数据的互通、计算、建模，最终产生超出自身数据的价值，同时保障敏感数据信息的安全，实现数据“可用而不可见”。从技术实现原理上看，隐私计算主要技术选型分两类，第一类是以多方安全计算为代表的基于密码学的隐私计算技术；第二类是以可信执行环境为代表的基于硬件的隐私计算技术。无人机终端可以采用基于硬件的隐私计算技术，运算效率高，且安全性较高。

2. 可信评估

为了防止攻击者对无人机的恶意攻击，无人机可以运用可信评估机制对安装的硬件和软件进行识别度量。可信评估机制主要通过对无人机终端软硬件、操作系统、应用程序进行行为数据分析建模，实现可信度量识别，对无人机终端统一管控，防止恶意攻击。可信评估体系主要包括硬件可信度量、可信模块、可信引导、可信安全基线核查四部分内容，其中硬件可

信度量是通过对终端芯片、GPS、陀螺仪等硬件可信度量，实现对传感器硬件的可信管控；可信模块作为软硬件可信度量的信任基础，通过可信软件栈为上层应用实现可信度量提供支撑；可信引导通过建立贯穿硬件模块、操作系统及应用的信任链，实现对硬件启动和软件引导过程的完整度量；可信安全基线核查对终端的软硬件综合可信度量，形成对终端的综合安全度量结果。

（三）网络侧安全防护技术策略

网络侧安全主要保障无线空口机密性、完整性和可用性，通过射频指纹识别、轻量级认证、无线传输加密、信号抗干扰等安全防护，从物理层、链路层和网络层等各个层面保障合法终端入网，抵御窃听、假冒、篡改等网络攻击。

1. 射频指纹识别

针对网联无人机系统，无人机终端通过通信网络接入平台系统之前，需进行信号识别和授权，确保无人机的合法性，无人机系统可以通过射频指纹识别技术实现对通信信号进行鉴权。射频指纹识别技术通过信号处理手段，提取采集到的无线信号特征，建立无人机终端射频指纹库，通信双方利用射频指纹识别与检测方法，从而实现对无人机终端的识别，实现辐射源设备个体识别，发现和阻断非法终端连接。近年来,辐射源个体识别技术相关理论与实践应用不断完善,指纹特征提取方法的研究取得了较大的进展。

2. 轻量级认证

针对网联无人机动态变化、通信带宽窄的特点，使用轻量级认证协议可以实现无人机的安全认证，防止非法和假冒用户的接入。轻量级认证协议重点研究的是轻量级的认证算法，主要目的在于简化认证交互次数、交互数据量，同时兼顾通信的机密性、完整性及不可否认性，协议主要是实现无人机密钥管理、身份认证等功能。轻量级认证方式主要分为有中心的无人机网络认证和无中心的无人机网络认证，其中有中心的无人机网络认证是管理中心为无人机分发密钥，并提供无人机身份认证功能；无中心的无人机网络认证是利用门限密钥技术，由网络中多个节点共同参与密钥生成和身份认证。

3. 无线传输加密

由于无人机终端与平台系统之间传输大量的重要敏感数据，因此需要对通过无线网络传输的敏感数据进行链路层、网络层等加密处理，包括使用国密 SM、祖冲之算法等，实现无人机终端和平台系统之间进行端到端加密，确保数据在无线网络传输的机密性和完整性。重要数据经过加密模块或软件进行加密传输到网络，在整个网络传输过程中，数据包始终处于加密状态，平台系统解密模块或软件解密出对端的数据信息后进行存储，以此实现数据在空中传输的安全保密功能。

4. 信号抗干扰

目前，国内外对无人机网络抗干扰技术的研究方向主要集中在跳扩频、

频谱资源分配优化等方面。跳频扩频技术主要通过快速切换频率载波来积极躲避干扰攻击，长期被用来提高无线通信的抗干扰能力。频谱资源优化技术是通过对可用频谱资源的最佳使用实现抗干扰，利用自适应方法达到最优资源分配效果。另外，还可以利用针对干扰攻击的“蜜罐”欺骗机制，将网络中的空闲节点伪装成传输节点，通过诱骗干扰方对其进行干扰，以此来提高网络中传输对的传输性能。

（四）平台侧安全防护技术策略

平台侧安全通过鉴权认证确保合法用户能够访问和使用控制软件；软件可信和 APP 安全实现应用软件运行控制，防止非法软件的运行；对存储在管理平台的敏感数据进行加密存储，防止攻击者窃取。

1. 应用可信

可信就是一个实体在实现给定目标时，其行为与结果总是可以预期的，如果软件应用总是与用户的预期相符，即使在运行过程中出现一些特殊情况，这样的应用就是应用可信。在无人机管理平台中会安装大量的应用类软件和程序，为了保证所安装应用程序的合法性和安全性，无人机管理平台可以基于软件白名单和数字签名机制，为应用软件运行提供安全保证，实现软件的来源可信、运行可控，并提供软件的发布、更新等管理功能。

2. APP 安全

无人机管理平台运用特定的 APP 软件，实现管理操作的便利性。在 2012 年，Gartner 引入了“Runtime application self-protection”一

词，简称为 RASP，这种技术可以和应用程序绑定在一起，像“疫苗”一样注入到应用程序里，将安全防御功能整合到正在运行的应用程序中，实时检测和阻断安全攻击，当应用程序遭受到实际攻击伤害，就可以自动对其进行防御，使应用程序在运行时实现自我安全保护，有效防护已知和未知攻击。为了确保 APP 应用程序的安全性，无人机管理平台可以利用 RASP 安全保护技术。

3. 数据存储加密

无人机管理平台需要存储大量重要敏感数据，主要包括：采集数据、飞控数据、身份数据等。数据存储加密技术的目的是防止在存储环节上的数据失密。数据存储加密技术分为密文存储、存取控制两种，密文存储技术是通过加密算法、附加密码、加密模块等方法实现；存取控制技术是对用户资格、权限加以审查和限制，防止非法用户存取数据或合法用户越权存取数据。无人机管理平台可以对存储在管理平台内的重要数据，采用国密 SM 等加密技术，进行分级分类加密存储，防止攻击者破坏或窃取。

4. 鉴权认证

针对接入管理平台的终端用户，可以采用“零信任”机制进行用户动态鉴权和识别认证。零信任模型表明，默认情况下，任何用户（即使允许进入网络）都不应受信任，因为它们可能会受到损害。在整个网络中需要标识和设备身份验证，而不仅仅是在边界进行身份验证。授予的访问权限

应保证是完成任务所需的最小权限，并对访问行为进行记录和审计，实现数据资源访问的安全管控，保证合法的用户访问合法的数据。

（五）基础安全管理技术策略

基础安全管理主要是通过设备管理、策略管理、密钥管理、漏洞管理、身份管理和安全态势，实现无人机终端状态监控、安全策略的调整与分发、无人机密钥管理与分发、系统漏洞修复、用户认证以及无人机安全态势分析与呈现。

1. 设备管理

设备管理主要提供资产管理、补丁管理、软件管理、资产状态管理、监控审计、存储介质管理、等功能，解决平台和终端的各种安全管理问题和满足各种合规需求。无人机管理平台的设备管理模块主要提供无人机终端设备的管理和监控功能，主要包括：终端上下线管理、软件版本升级管理、运行状态监控、运行数据统计分析等，并对管理平台设备运行状态进行监控分析。

2. 策略管理

策略管理能够对涉及的无人机终端设备的策略进行全面的梳理和优化，及时发现安全策略的各类异常并通知维护人员，以保证无人机终端设备以最优状态运行，提升用户的便利性和安全性。策略管理模块主要是依据实际情况对无人机终端进行运行策略的制定和管理，通过对无人机终端制定

相应的安全策略，并在无人机执行任务之前下发至对应无人机终端，同时可在线调整无人机终端的安全策略。

3. 密钥管理

密钥管理是指管理加密密钥的密码系统，主要包括处理密钥的生成、交换、存储、使用、加密粉碎（销毁）和替换，它还包括密码协议设计、密钥服务器、用户程序和其他相关协议，成功的密钥管理对于密码系统的安全性至关重要。无人机管理平台密钥管理模块主要通过密钥的生成、分发、存储、销毁等功能，支撑对数据、账号、网络等资产的加密、认证、消息完整性保护等处理，并能根据无人机终端执行不同任务动态调整密钥分发策略。

4. 漏洞管理

漏洞管理以安全漏洞全生命周期管理为核心理念，从网络产品安全漏洞的识别、确认、修复、复查等全流程建立技术支撑手段，快速发现和处置网络产品安全漏洞，形成常态化、规范化漏洞管理机制。无人机管理平台的漏洞管理模块提供对无人机终端、管理平台软硬件系统的定期漏洞扫描、安全加固等功能。通过定期安全巡检，评估漏洞情况，对于新公布的漏洞，开展应急检测。同时，优先修复风险较高的漏洞，结合修复对于业务影响的程度，制定合适的整改方案。

5. 身份管理

身份管理可防止对系统和资源的未经授权的访问，帮助防止企业或受保护数据的泄露，并在未经授权的人员或程序进行访问尝试时发出警报和警报。无人机管理平台的身份管理模块提供无人机用户、设备的身份识别和统一管理功能，并提供无人机系统身份认证支撑。无人机管理平台通过创建、存储和管理无人机终端和使用用户的帐户和身份记录，实现对无人机终端或使用用户名下的服务、资源接入控制统一管理。

6. 安全态势

安全态势感知是一种基于环境的、动态、整体地洞悉安全风险的能力，是以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的一种方式，最终是为了决策与行动，是安全能力的落地。网络态势感知（Cyberspace Situation Awareness，CSA）旨在大规模网络环境中对能够引起网络态势发生变化的安全要素进行获取、理解、显示以及最近发展趋势的顺延性预测，进而进行决策与行动。无人机管理平台通过在线或离线方式收集无人机终端的安全事件、系统日志、状态监控、策略参数等数据，对收集到的数据进行综合分析，形成无人机系统的安全态势。

五、网联无人机安全发展展望

近年来，无人机产业蓬勃发展，但是安全问题也在逐渐爆发。无人机、外挂设备、地面站、通信网络等无人机系统各主要环节大量存在网络安全管理问题。其中包括缺乏安全检测认证工作、缺乏有效的安全防护技术、传统安全防护不适用、安全防护防御体系未构建、安全生态未建立等诸多问题。

展望未来，网联无人机系统发展应当着眼于无人机的实际安全需求，考虑即将面临的网络安全新形势新风险，未来无人机的安全研发工作可以从以下几个方面来展开：

（一）传感器安全

传感器是无人机获取外界数据的重要组件，当传感器受到干扰或者欺骗，无人机则无法获取自己当前的真实状态信息，很有可能会因此做出错误的反应，这很有可能会影响无人机的飞行安全。所以，不仅要继续发掘传感器存在的安全隐患，同时也要设计相应的算法来规避这些安全隐患所带来的不利影响。

（二）通信安全

无人机与地面站的通信方式包括无线电、无线数传、WiFi 和无线图传等，无人机在不同的通信链路上都存在不同程度的安全威胁。除了避免使用比较脆弱的通信方式外，设计出高效加密的通信协议将是未来的一项重要的研究工作。

（三）软件安全

软件安全主要是指无人机和地面站的控制软件安全。在软件设计和编码时，应将其放入到整个运行系统中进行分析，考虑软件、操作人员和系统之间的相互影响，尽量避免产生漏洞、采用更加安全的加密技术和协议。同时，对于无人机飞控系统植入木马的安全问题也将继续加强研究。

（四）网络安全

无人机的无线自组网络是一种比传统有线、无线网络更加灵活的网络组织形式，最大的安全问题在于其动态的拓扑结构，没有中央基站提供约束，所以路由安全在整个网络安全中起着重要的作用。因此，有必要设计新的高效安全的路由协议，妥善解决这些高流动性的特点带来的安全隐患。

（五）自身抗干扰能力

抗干扰技术对无人机的数据链路传输系统是十分必要的，特别是在军事领域发展过程当中，可能会对整个的任务完成将会起到决定性的作用，伴随着各个领域在对电子技术应用中的不断提升，无人机抗干扰水平也得到了进一步的展现与提高。抗干扰技术主要采用扩频应用技术、跳频应用技术等进行不断的发展与运用，使得无人机系统的干扰能力得到进一步的增强，从而更好的保障无人机作业的安全和稳定。

（六）相关法律制度建设与完善

当前无人机的使用频率在不断的增加，所以我们一定要建立更加完善法律制度，使得整个的行业规范性能够得到进一步的完善。促使相关的数据连接传输，导航控制以及相关的电磁设备等，都能够达到规范化的要求。进行科学合理的无线电频谱设计，保证使用的频率能够更加的科学合理，使其不会出现与其他通讯系统相互干扰的现象。

总体来说，随着制造成本的降低和技术发展和成熟，无人机在给人们生活带来便利的同时，也面临日益严峻的安全问题。而随着信息技术的不断发展，无人机受到的安全威胁也在不断变化，因此安全防护措施也必须根据趋势变化及时更新，需要不断地对无人机系统安全进行实时评估，找到新的应对措施。

六、结语

未来，无人机产业链各方需着眼于无人机产业未来发展趋势，提前进行无人机系统安全技术预研，以应对未来的无人机系统网络安全需求。当前无人机市场在网联环境下，构建安全机制可令网联无人机产品更具竞争力，而无人机产业链各方也应将对安全机制的关注重点从成本增加转向价值创造。

中国联通 5G 无人机应用凭借联通 5G 资源禀赋，承诺了更好的数据隐私性、更安全的隔离度、更灵活的自管理能力和更高效稳定的连接性能，是中国联通响应国家号召，持续践行新基建，面向行业客户提供的基于新一代信息通信技术的精准供给。未来，中国联通将发挥 5G 网络资源、网络安全建设及运维等优势，积极拓展定制化 5G 无人机业务，与行业用户共同探索智能化、安全化网络与 5G 无人机应用的融合与创新，为行业客户提供专属的精品网络服务，推动生产方式与治理模式向更智能高效的方向发展。中国联通愿意与产业链合作伙伴携手共进，合力推动网联网人机安全体系建立，安全产品合作研发，构建无人机系统安全的健康可持续发展，共同打造无人机安全生态，共谋发展，联合共赢。

中国联通研究院是根植于联通集团（中国联通直属二级机构），服务于国家战略、行业发展、企业生产的战略决策参谋者、技术发展引领者、产业发展助推者，是原创技术策源地主力军和数字技术融合创新排头兵。联通研究院以做深大联接、做强大计算、做活大数据、做优大应用、做精大安全为己任，按照4+1+X 研发布局，开展面向 CUBE-Net 3.0 新一代网络、大数据赋能运营、端网边业协同创新、网络与信息安全等方向的前沿技术研发，承担高质量决策报告研究和专精特新核心技术攻关，致力于成为服务国家发展的高端智库、代表行业产业的发言人、助推数字化转型的参谋部，多方位参与网络强国、数字中国、智慧社会建设。联通研究院现有员工近 700 人，平均年龄 36 岁，85%以上为硕士、博士研究生，以“三度三有”企业文化为根基，发展成为一支高素质、高活力、专业化、具有行业影响力的人才队伍。

战略决策的参谋者
技术发展的引领者
产业发展的助推者

态度、速度、气度

有情怀、有格局、有担当

中国联合网络通信有限公司研究院
地址：北京市亦庄经济技术开发区北环东路 1 号
电话：010-87926100
邮编：100176

中国联通研究院

中国联通泛终端技术