低空经济-工业无人机网络安全防护解决方案

目录

什么是工业级无人机

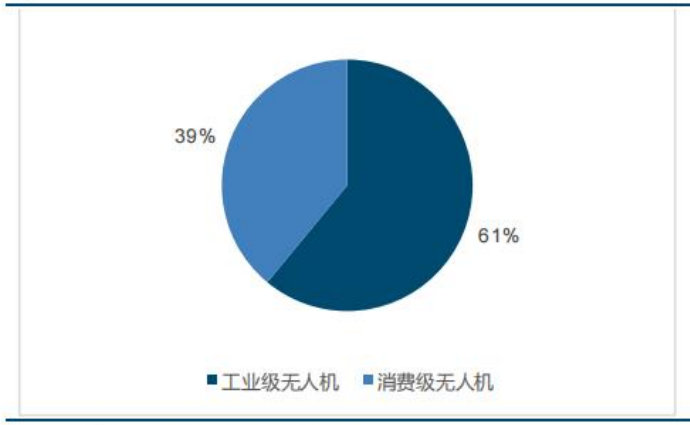
无人机产业快速发展，工业级无人机市场占比高

无人机产业是低空经济的主导产业，市场规模快速增长。工业级无人机是民用无人机市场主体，市场规模快速增长。随着无人机普及度提升，目前无人机向消费市场的扩张已经遇到门槛，未来工业级无人机将接力打开长期成长空间。工业无人机属于民用无人机的一种，主要用于协同或代替人工完成多种商业领域的任务，其通常搭载为完成作业飞行活动的装置或设备。据央视网报道，工业和信息化部赛迪研究院（CCID）预测 2025 年我国民用无人机产业规模将突破 2000 亿元，工业级无人机将成为主力机型。

工业级无人机应用领域逐步拓展，农林植保、地理测绘、巡逻巡检为目前主要应用场景。

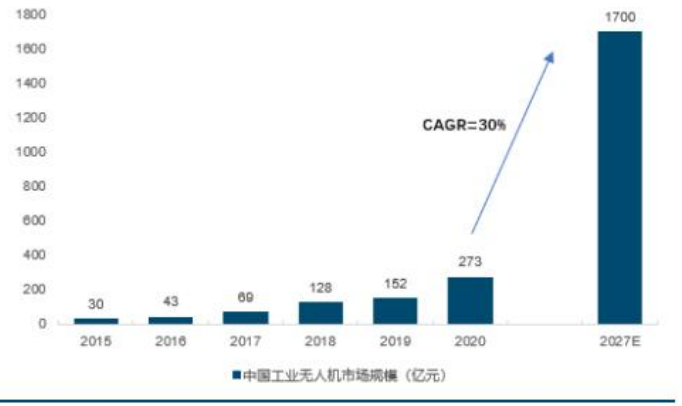
工业级无人机主要应用领域包括电力巡检、应急救援、航空摄影、水利应用、农药喷洒、航空测绘、国土资源、旅游业、管线巡查、医疗业、海事监察、农业林业、物流运输、交通管制、气象监测、反恐防暴等。且随着工业无人机技术水平的不断提升，各行各业对无人机应用需求的提升，工业无人机应用领域将更加深化、细化，应用领域将不断扩大。据研究机构分析，我国工业级无人机主要应用于农林植保、地理测绘、巡检领域，市场占比分别为 30.7%、22.6%、18.8%。

图表43：工业级无人机是我国民用无人机市场主要组成部分



来源：中商产业研究院，国金证券研究所

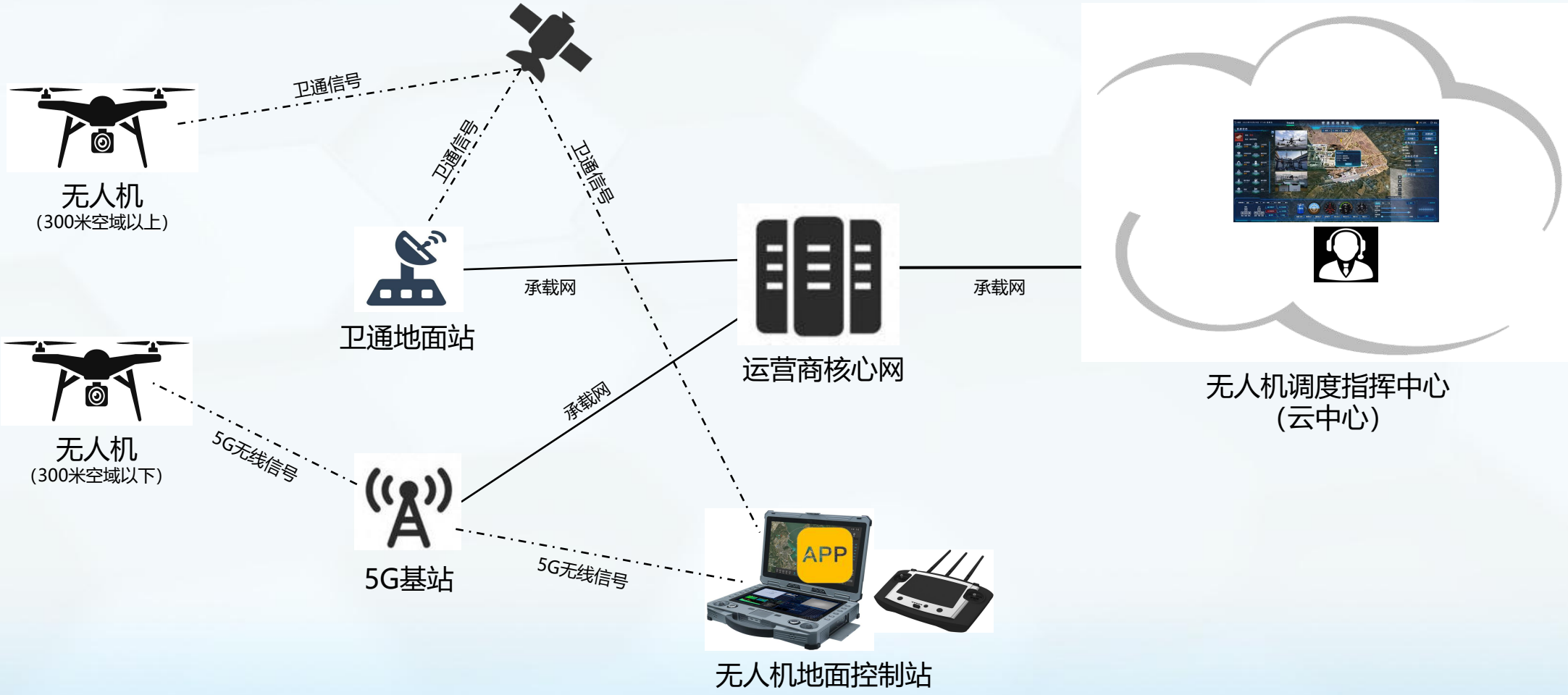
图表44：2027 年我国工业无人机市场规模有望达 1700 亿元



来源：前瞻产业研究院，国金证券研究所

工业级无人机的典型组网结构

典型工业无人机系统主要由**无人机飞行器、地面站、遥控装置及各类应用系统/平台**构成，核心组件包括飞控系统、导航系统、视频图传系统、操作系统、APP、管理平台、通信网络以及硬件和固件系统等。



上图根据行业标准：《无人机管理（服务）平台安全防护要求》（YD/T 4324-2023）中的概述定义整理绘制

典型无人机安全事件

- 随着电子信息和无人系统技术的快速发展，无人驾驶飞行器作为新兴的智能装备产品，广泛应用于政府监管、园区巡检、快递物流、消防救援、农业环保、电力巡线、道路巡检等行业应用领域。然而，在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,安全攻击手段多样，包括：导航系统劫持、飞控信号劫持、通信链路攻击、飞控软件及地面系统安全漏洞等。
- 低空经济领域安全事件时有发生，无人驾驶飞行器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， 需要在政策层面不断完善和加强管理。包括推动低空经济国家安全立法、推动低空经济国家安全监管、加强低空经济国家安全法制安全教育等。

2009年

事件描述：伊拉克武装分子从无人机的**通信链路**中拦截了视频流数据。
原因：美军无人机**遥控数据不加密**，被伊武装分子轻松劫持。使用软件仅26美元

2012年

事件描述：伊朗武装分子利用**GPS欺骗技术**劫持了美国的RQ-170“哨兵”无人机
原因：伊朗利用美国无人机GPS“信号微弱、易于操纵”的弱点，切断其与美国基地的通信线路，然后重构它的GPS坐标，引导它降落在伊朗境内。

2015年

事件描述：黑客利用大疆无人机的**无线通信安全漏洞**，通过逆向无人机控制终端芯片信息得到无人机通信链路参数，劫持了大疆精灵3的控制权。

2016年

事件描述：墨西哥边境毒贩企图使用**GPS欺骗技术**攻击美国巡逻无人机，以达到非法跨境的目的。
原因：利用欺骗式GPS干扰技术向这些无人机发送错误坐标，让GPS接收器得到错误的伪距

2024年

事件描述：天津滨海机场因无人机导致的公共安全原因，航班起降受到影响，航班延误29架次，取消8架次，有32架次备降外场，3000余名旅客出行受到影响。
原因：安全监管漏洞

2012年

事件描述：在美国安全部委托的一项实验中，美国奥斯汀德州大学的工程研究生们成功劫持了一架民用无人飞机。他们通过制造劫持用的“电子欺骗”设备，取代了GPS信号，从而完全控制了无人飞机。

2018年5月

事件描述：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

事件描述：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。

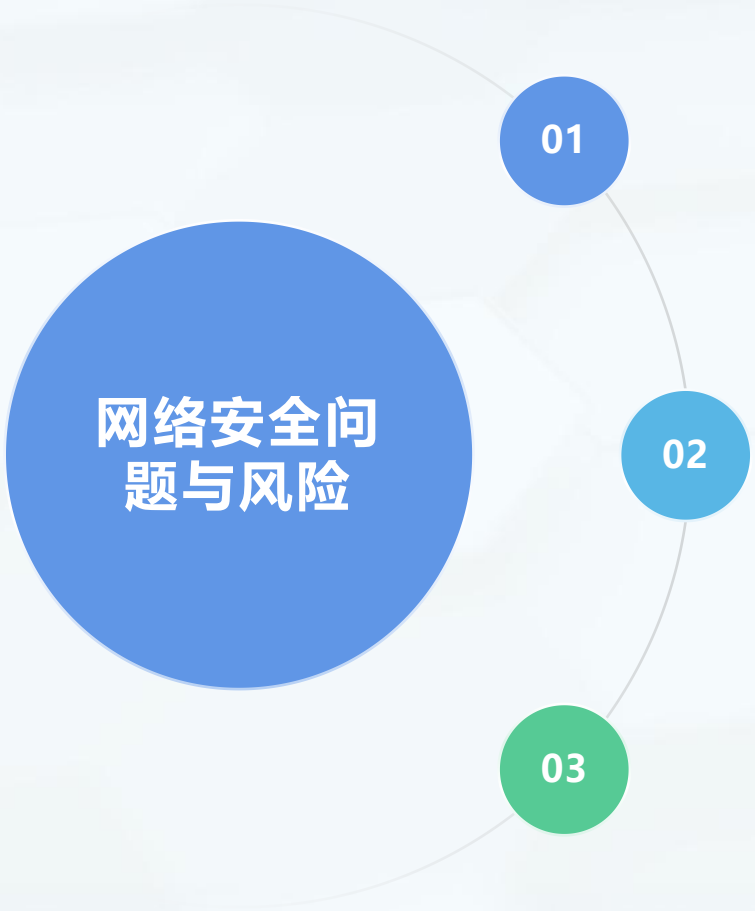
2024年

事件描述：无人机在四川乐山嘉定中学上空非法飞行，被警方成功挡获
原因：该事件反映了无人机“黑飞”现象的普遍性，以及安装无人机反制设备的紧迫性和重要性。

2024年

事件描述：俄罗斯“反无人机小组”在扎波罗热前线截获了一架美制RQ-20“美洲狮”无人机，并成功诱使其着陆。通过技术手段**破解了无人机的空地数据链**，接管了控制权。

工业级无人机面临的主要安全问题与风险



访问控制与身份鉴别

(1)目前工业无人机系统普遍缺乏合规、高安全的身份标识及鉴别机制，存在弱口令、被伪造、窃取后仿冒接入的风险。
(2)云端的管理调度平台是无人机系统的关键组件，云平台存在的安全漏洞及暴露面，通过未经授权的外部违规访问及非法接入会对无人机系统机构成严重威胁，导致系统被攻陷或遭受拒绝服务攻击。
(3)各类应用系统、APP、固件等普遍存在身份验证不当、签名验证绕过、任意代码执行等安全漏洞，本质上还是在系统安全设计方面缺乏精细化的权限管控机制，未遵循最小化权限管控原则，容易导致正常接入的无人机违规访问权限外的服务或被利用发起横向攻击。

数据安全

在工业无人机的飞行作业过程中，大量的敏感数据需要被收集、传输、处理和存储，如飞行器的位置信息、航路信息、图像和作业信息、用户身份信息等。如果数据没有得到安全保护，极易面临数据隐私泄露的风险，对个人隐私、企业商业秘密造成损害，严重的甚至会危害国家安全。

供应链安全风险

工业无人机系统中的各类固件系统、控制系统、应用系统、操作系统和通信系统都是由供应链企业研发生产，从当前无人机存在安全漏洞和风险问题来看，供应链安全是非常关键的环节，目前针对飞行器及遥控设备的风险监测机制还不够健全，对飞行调度管理安全、APP安全、固件安全、通信安全缺乏相应的安全监测及管理能力。

无人驾驶飞行器身份鉴别及访问控制风险

- 无人驾驶飞行器作为低空经济应用场景中实际的信息采集及接入主体，其可直接发起与平台侧交互。其身份的唯一性、真实性标识及可靠的鉴别技术是保障系统安全稳定运行的前提。在真实可信身份的基础之上，构建精细化、动态的访问控制机制，是确保低空经济场景化安全保障的前提和基石。
- 将先进的安全技术、密码技术与业务融合，形成内生安全机制，可更有效的实现安全防护保障。

①身份伪造、终端仿冒接入

- 缺乏合规、高安全的身份标识及鉴别机制，导致无人驾驶飞行器身份存在弱口令、被伪造、窃取后仿冒接入的风险
- 缺乏飞行器及遥控等设备风险监测机制，不具备监测APP运行状态、刷机、固件状态监测能力，导致非法终端接入平台侧，造成信息泄露或安全事故

②平台系统存在漏洞或隐蔽端口

- 平台侧存在系统漏洞及严格的访问控制机制，导致未经授权的外部终端可非法接入
- 平台侧存在暴露面，未经授权的外部终端可在未经身份认证之前与平台建立连接
- 可导致平台被攻陷或遭受拒绝服务攻击

③越权访问风险

- 缺乏精细化的权限管控机制，未遵循最小化权限管控原则，导致正常接入的无人驾驶飞行器可访问正常权限外的服务或发起横向攻击
- 越权访问多来自于权限设置不当；或缺乏微隔离防护手段；或身份凭证被冒用等

④静态访问控制风险

- 缺乏基于实时全域风险监测的动态访问控制机制，导致攻击发生后，仅能通过事后审计的方式，定位及追溯问题
- 静态访问控制机制，将导致合法用户的非正常访问行为无法发现以及及时阻断，造成严重的安全事件

数据安全风险

- 在低空经济中，大量的敏感数据需要被收集、传输、处理和存储，如飞行器的位置信息、用户身份信息等。如果数据没有得到安全保护，就可能面临数据隐私泄露的风险。将会造成对个人隐私造成侵犯，同时也可能为企业带来法律风险和声誉损失。
- 基于体系化、服务化低空全域密码算力实现数据全生命周期安全防护，是安全合规且最经济有效的手段。

①预置飞行数据泄露及篡改风险

- 飞行速度限制、稳定性参数、预设飞行轨迹、通信频率及协议参数、返航点设置等预置飞行数据，缺乏安全防护，存在被篡改或泄露风险
- 可导致飞行安全及使用体验，严重可导致撞机、坠机

②数据传输被劫持及篡改风险

- 控制信号、空管信号、导航数据、气象数据等通过不安全的网络传输，存在被窃听或篡改风险
- 飞行器采集数据通过不安全的网络传输，存在被窃听及任务被篡改风险
- 可导致飞行器被劫持或数据丢失，严重可导致无法控制、炸机等

③平台侧数据被拖库或篡改风险

- 平台侧核心配置文件、飞行器用户数据、数据库文件等，缺乏必要的机密性及完整性保护措施，导致被拖库、恶意篡改或现场拷贝
- 可导致核心敏感数据丢失，核心数据被篡改，造成个人隐私泄露，或飞控事故，给个人、组织机构带来极大的损失

固件、系统及基础设施安全风险

- 无人驾驶飞行器固件，飞控系统及地面系统，低空通讯网、感知网及算力网等基础设施，如果存在安全漏洞，一旦遭受恶意攻击，将影响低空经济体系的安全性。
- 可引入固件签名机制，硬件隔离和防护机制，以抵御物理攻击和侵入。确保硬件元件的可信度，防范硬件级别的攻击。
- 可基于代码审计、安全扫描、安全体检、安全靶场的技术手段，对低空经济系统进行针对性及体系化安全检测，知攻知防，尽早查缺补漏，防范于未然；并对地面系统开展体系化密码建设及等级保护，确保系统合规安全运行

①固件更新身份验证不当风险

- 该类风险发生在固件更新过程中，固件更新程序在下载更新包时，未使用安全协议对站点TLS 证书的有效性进行验证。
- 攻击者可能会利用中间人技术，如 DNS 投毒、 ARP 欺骗或控制路由节点等手段，诱导系统安装恶意固件更新。一旦得逞，便可能获取底层操作系统的管理权限。

②固件签名验证绕过风险

- 无人驾驶飞行器固件包中的配置文件缺乏数字签名或加密技术保护。而引导加载程序会依据文件中的内容对固件进行修改，而且改动发生在验证固件签名之后。
- 通过该漏洞，攻击者通过构造特殊的配置文件就可能对固件代码进行任意更改。

③恶意代码执行风险

- 问题源于无人驾驶飞行器系统中某些字段的设置可被用户输入控制，但程序未对输入字符串进行合理的清理过滤。
- 通过该漏洞，攻击者通过精心构造的输入，在绕过长度检查后能够注入任意代码，进而实现对无人机的完全控制。

③基础设施安全风险

- 低空经济发展依赖各种基础设施，如低空通信网、低空感知网、低空算力网等。这些基础设施如果存在安全漏洞或被恶意攻击，就可能影响低空经济的整体安全。
- 例如，通信网络的瘫痪可能导致无人机无法正常飞行或通信，感知网络的不准确可能导致飞行冲突或事故。

目录

关键安全痛点

技术复杂性

1. 资源受限与安全防护的矛盾
工业级无人机通常受限于计算能力、存储容量和电池续航，传统的安全防护措施难以部署，亟需解决如何在资源受限条件下实现轻量化安全防护的同时，不显著影响飞行性能和稳定性。

2. 异构系统整合的复杂性
无人机系统涉及飞控、通信、载荷等多个子系统，且可能由不同厂商提供，存在协议兼容性和接口通用性问题。

3. 动态环境下的实时威胁响应
无人机在飞行中面临动态网络环境，传统静态防御策略（防火墙、固定规则）难以应对。

交叉合规与风险监测

1. 多法规交叉与合规建设成本高
工业级无人机系统需同时满足网络安全、航空安全、行业规范等多重法规，企业合规建设成本较高。

2. 风险监测范围和机制不健全
无人机的安全风险监测既要包含运行期间的动态风险，也需要涵盖供应链存在的潜在风险，无人机的供应链较长，行业复杂性较高，目前缺乏统一的供应链安全评估标准，且一般企业很难对供应商进行深度安全审计。

隐私与数据安全保护

1. 隐私保护与数据安全
无人机采集和使用的敏感数据及隐私信息，如何实现有效保护的同时兼顾数据效用。

2. 操作员身份管理的实践挑战
户外环境下如何确保操作员的身份认证以及无人机及相关设备的有效监测和控制。

核心安全需求分析

■ **工业级无人机主要是商业化应用场景，运营主体是政府机构和企业，因此，其核心安全需求的出发点还是以运营主体和应用场景为主。**

运营企业视角

安全合规与系统防护

一、安全合规

需要满足等级保护、关基保护等合规要求以及民航、物流、农业等行业领域的相关安全标准和规范

二、有效的系统防御能力

需要从企业运营角度建设完整的无人机系统安全防御能力体系

三、供应链安全管理

建立面向供应链安全的评估机制，对无人机系统相关的各类系统和代码存在的安全漏洞进行风险管控。

业务场景视角

场景化风险应对

巡检、测绘、运输作业是工业级无人机在商用业务场景的典型应用，这些场景中最关键的安全需求是保障无人系统的业务连续性以及应用过程中的敏感信息保护，如：

1. 电力/油气管道巡检和监控过程中，无人机被劫持后撞击关键基础设施或窃取敏感设施坐标数据；
2. 物流运输过程中被截获或路径规划被篡改，造成高价值货物损失；
3. 还有农林地理测绘过程中对测绘数据的安全保护等。

用户视角

隐私与操作安全

一、隐私保护需求

需要采取数据安全保护措施，保护无人机飞行过程中采集的各类人脸、车牌以及建筑物等数据以及操作用户的隐私信息的安全。

二、操作员安全需求

1. 无人机访问控制

确保无人机控制链路的安全，需要采取包括无人机认证与准入控制、控制链路加密等防护措施；

2. 用户身份管理

采取强身份认证和授权机制，避免未授权人员通过仿冒身份操控无人机。

解决方案设计思路

- 由于当前工业级无人机的大多数场景还处于试验或试商用性质，对于网络安全的建设**需求相对模糊**，一方面**缺乏规范化的标准**指引，另一方面在风险应对方面的需求还主要以**功能安全**为主，网络和信息安全方面的需求相对滞后。基于此，本方案的设计思路将从用户需求视角出发，综合考虑**安全投入成本和方案的弹性可扩展**，以解决关键痛点和重要风险为核心，突出无人机的场景化安全，确保方案的可落地性和实用性。

可参考的标准

- **国标：**
  - ✓ 《民用无人驾驶航空器系统安全要求》（GB 42590-2023）
- **行标：**
  - ✓ 《无人机管理（服务）平台安全防护要求》（YD/T 4324-2023）
  - ✓ 《网络空间安全仿真 无人机系统信息安全仿真平台接入技术要求》（YD/T 4597-2023）

安全事件成因

- APP安全漏洞
- 固件安全漏洞
- 通信链路被截获或干扰
- 账号密码被破解提权
- 身份认证机制被绕过
- 数据无加密或权限管理机制被绕过

效能平衡的场景化设计

- 以无人机典型应用场景为方案设计基础，每个场景要有独立的解决方案
- 满足合规要求的同时避免贪大求全，综合考虑成本投入
- 从整体规划角度出发，方案需具备弹性可扩展空间，满足用户循序渐进、逐步完善的建设步骤。

工业级无人机网络安全整体解决方案

- 方案围绕工业级无人机在实际应用中的关键痛点，以网络安全防护技术和网络安全信任技术的能力基础，针对工业级无人机在商业化应用场景中“云、地、端”三个层面的安全要素和防护要点，提出基于无人机全域安全监测与管理的场景化解决方案，充分覆盖无人机系统在云平台防护、无人机安全运行以及重要数据保护方面的核心要求，方案基于成熟技术设计，具备较强的可落地性和实施性。

云

- 无人机全域安全监测与管理平台
- 无人机密码安全管理服务平台
- APP及应用安全监测
- 无人机管理（服务）平台安全防护

地

- 无人机安全访问控制中心
- 终端信任评估
- 数据安全传输

端

- 终端安全检测
- 无人机/终端安全接入
- 可信安全组件（SDK）

整体方案部署拓扑示意图

云中心

无人机全域安全监测与管理平台

- 无人机态势安全监测
- 无人机应用安全画像
- 控制站终端信任评估
- 安全漏洞与威胁管理

无人机密码安全管理中心

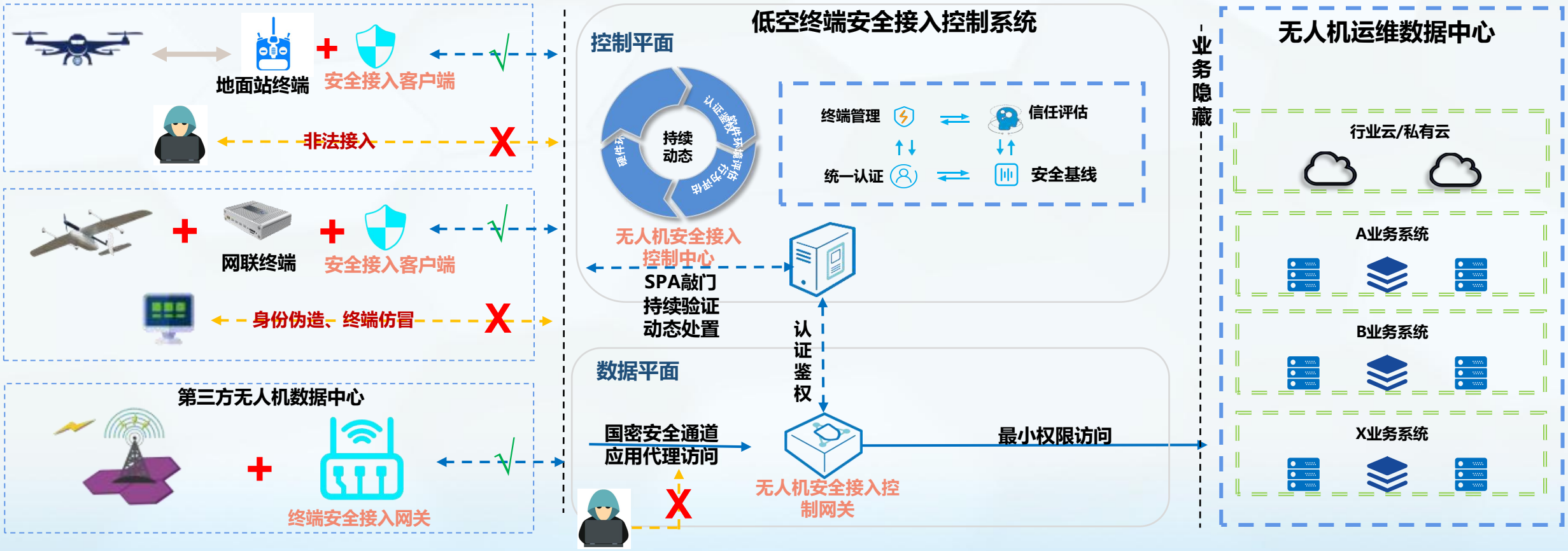
- 密码应用安全态势预警
- 密码应用安全服务分析
- 密码应用安全合规监管
- 高安全密钥管理

无人机管理（服务）平台安全防护能力

- 业务应用安全
- 网络安全
- 设备安全
- 数据安全
- 物理环境安全
- 管理安全

工业级无人机身份及访问控制防护设计

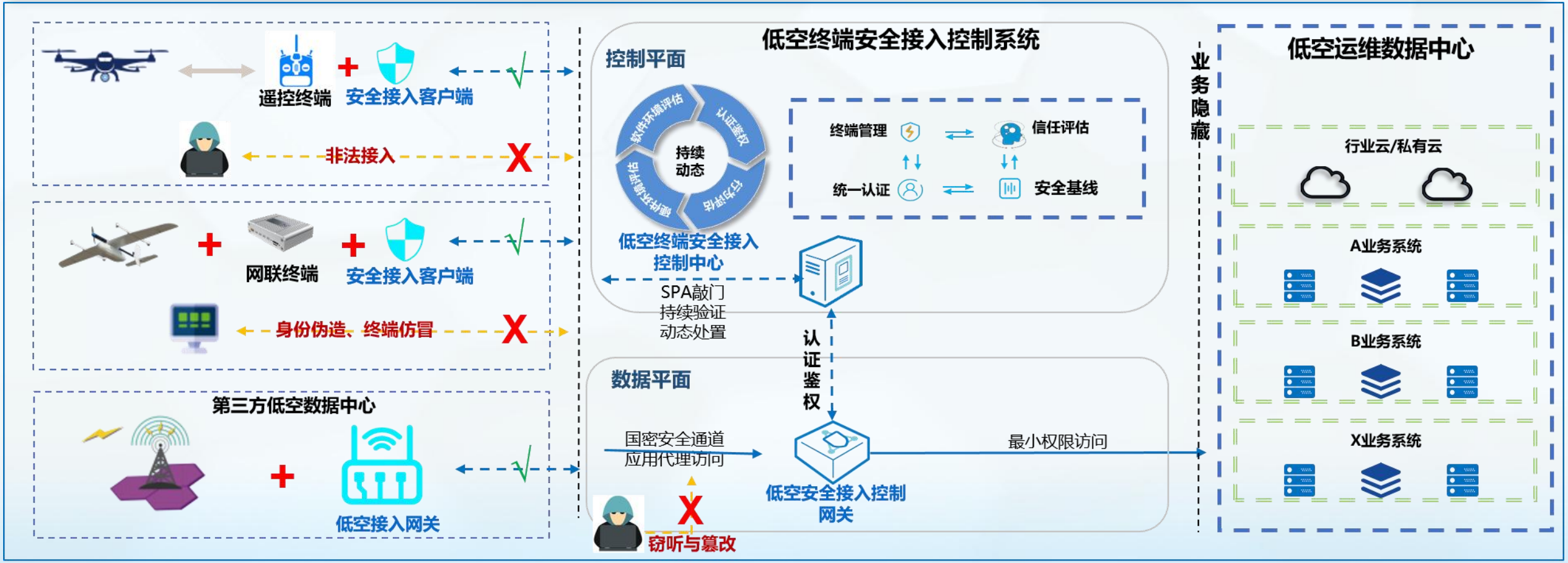
- 针对无人机监管及租赁单位面临的HVV安全需求，在云数据中心部署安全接入控制系统，提供通用化工业无人机身份及访问控制的防护能力。
- 对于强访问控制需求，可以通过对具有智能操作系统且的可改造智能终端进行定制开发，集成安全接入客户端组件，加配SIM/TF卡，实现零信任安全接入。可实现国密数字证书认证及国密安全通道，零信任敲门，有效收敛中心侧网络暴露面。
- 对于软硬件系统均无法定制改造终端，具备网络通讯接口。定制终端安全接入网关串接实现安全接入防护。



目录

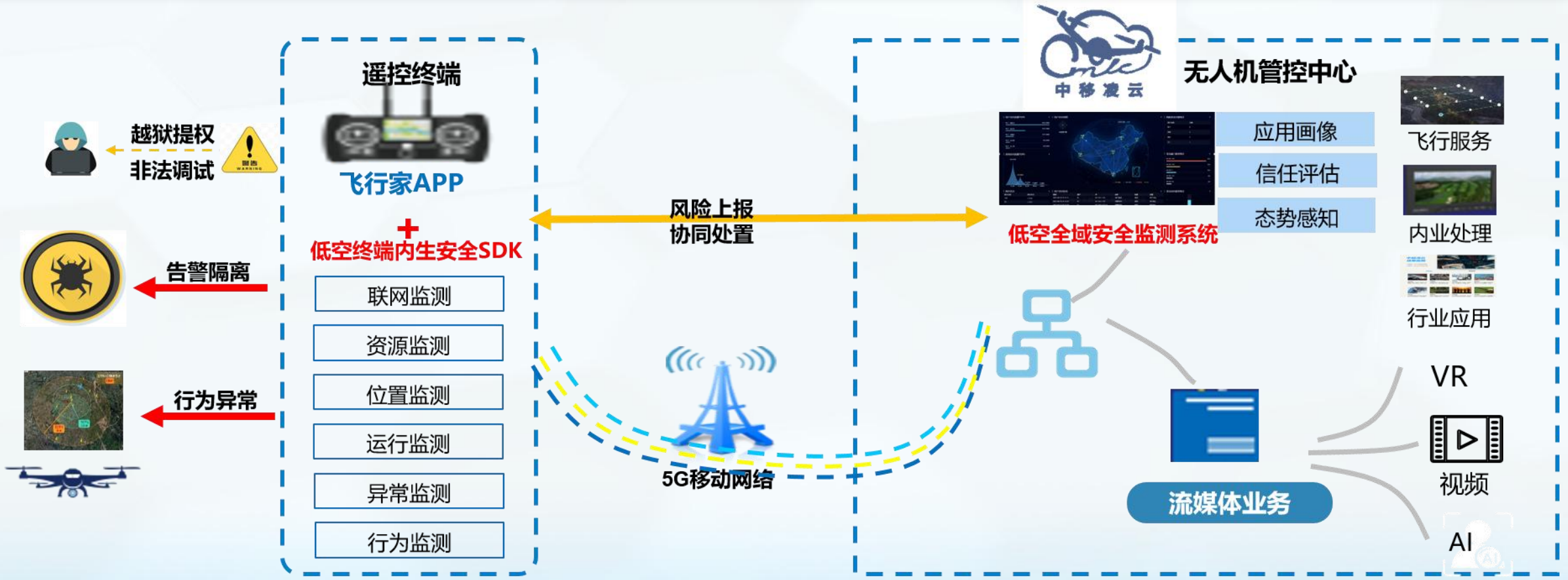
典型实践1：网联终端及遥控终端安全接入控制应用场景

- 针对无人机监管及租赁单位面临的HVV安全需求，数据中心部署安全接入控制系统，提供通用化网联终端及遥控终端安全接入防护能力。
- 具有智能操作系统且的可改造智能终端。集成安全接入客户端组件，加配SIM/TF卡，实现零信任安全接入。可实现国密数字证书认证及国密安全通道，零信任敲门，有效收敛中心侧网络暴露面。
- 硬件及软件系统均无法定制改造终端，具备网络通讯接口。定制低空接入网关串接实现安全接入防护。



典型实践2：低空遥控终端APP安全监测

- 针对主流无人机制造企业及无人采购及使用单位，提供内生安全SDK与飞控APP集成，实现APP安全监测及云测研判协同处置。
- 以端侧SDK作为风险感知触手，通过云测监测与分析系统评估，实时发现端侧安全风险，及时告警及应急处置。
- 安全监测系统还可以与飞控风险系统协同联动进行多维风险分析，发现潜在飞行安全威胁，提升全域飞控安全预警能力。



典型实践3：低空全域密码算力及数据加密管控系统应用场景

- 通过“终端轻量数据加密模块+分布式密钥管控系统+融合式密码算力设备”集成的私有化部署或云侧部署方式，采用密码技术分段处理不同阶段的数据安全问题，最大程度保障低空经济应用场景中的数据安全，解决因指令篡改、密钥或敏感参数泄露导致的无人机恶意劫持、隐私泄露等风险。
- 终端轻量数据加密模块可通过SDK和独立APP方式，内置在遥控终端或网联终端内，作为内生密码算力引擎；分布式密钥管控系统部署在边缘节点侧实现密钥安全分发和细粒度管控；超融合密码算力专用设备部署在云数据中心实现中心化密码算力。

技术亮点

轻量级数据加密

高安全密钥管理

超融合密码算力设施

高性能、高可用、高容错的密码算力调度服务

自定义、可编排的密码业务镜像/密钥服务模版

…

方案成效

密码应用安全态势预警

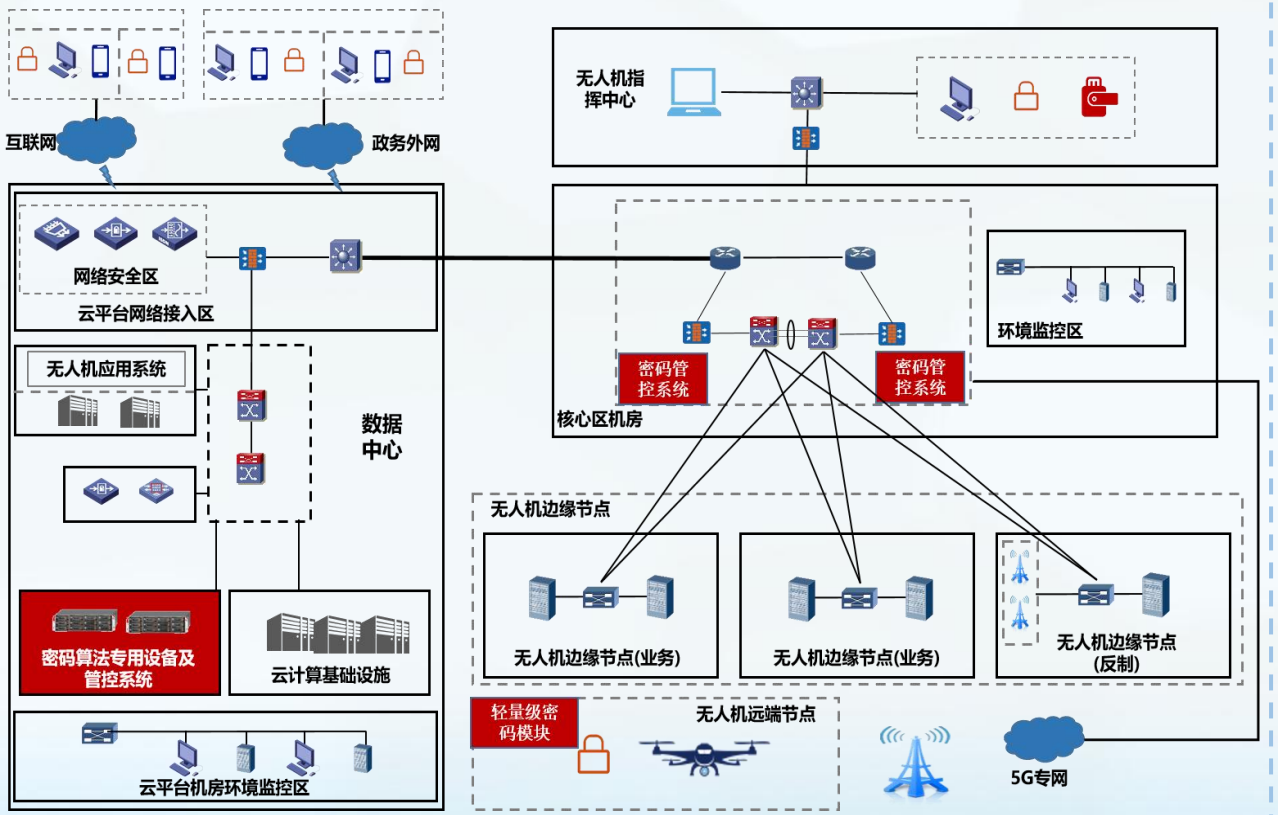
密码应用安全合规监管

密码应用安全服务分析

密码应用算力资源监控

超融合密码算力供给

部署方案



典型实践4：低空飞行服务站专网安全等级保护服务

■ **依托于等级安全保护要求，对湖南省长沙某飞行服务站专网实施等级保护安全保障，实现对地面系统合规体系化安全防护。**

案例背景

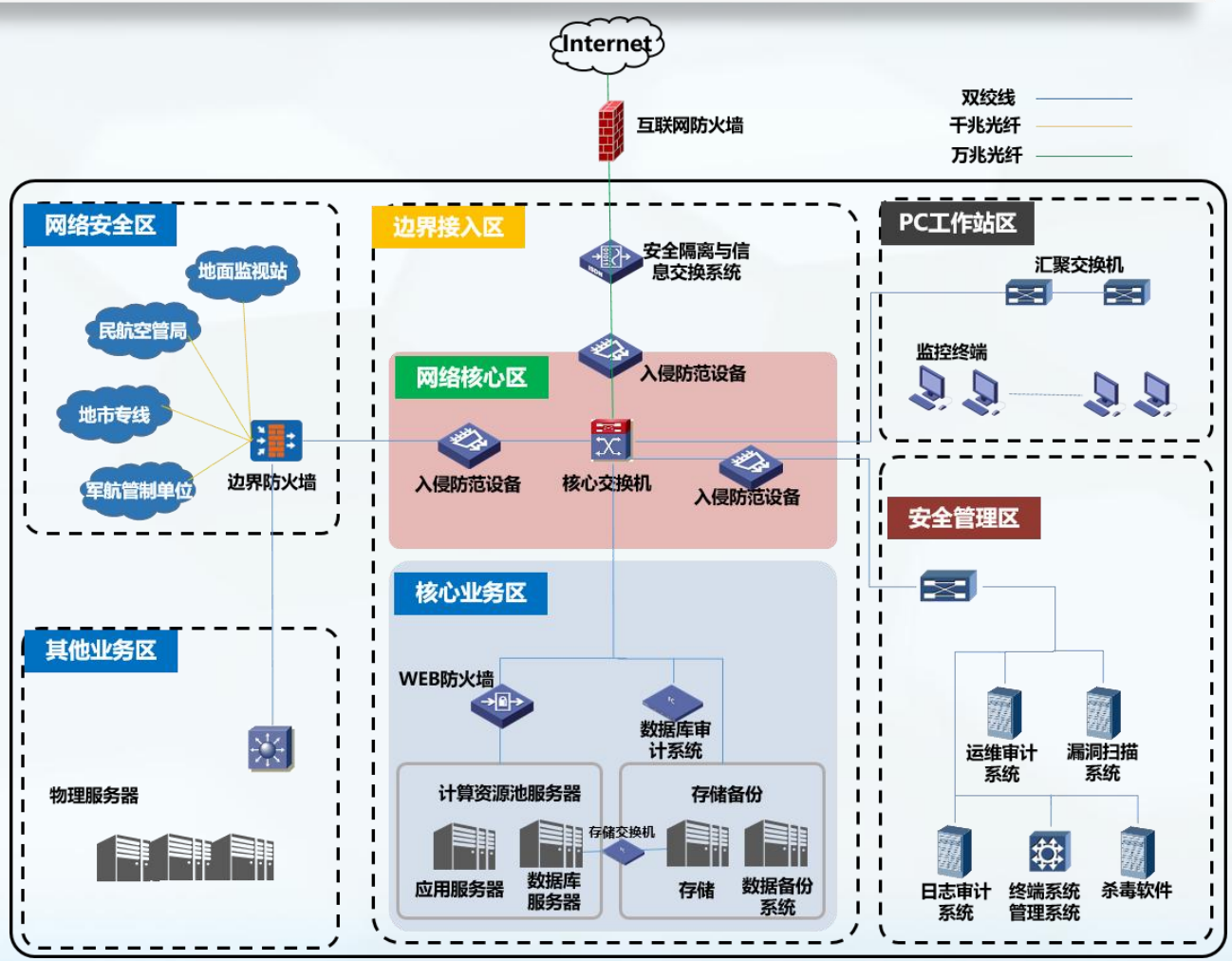
随着国家低空空域改革的不断深入，信息化应用水平的不断提高，对信息安全的要求也越来越高，低空飞行服务站专网建设需要确保符合有关信息安全主管部门的检查要求，同时符合实际安全防护需求与适用性。

建设内容

本项目主要对飞行服务站系统、空间地理信息系统、北斗低空监视通信系统开展等保二级差距评估、整改和辅助测评等工作，并完成机房网络安全部分的改造，针对现有信息系统进行安全合规建设，满足等保及民航行业安全标准要求。

建设价值

满足民航行业主管单位网络安全合规要求，增强安全防护体系建设能力，助力国产化替代安全建设实践落地。



感　谢　聆　听　！