ICS 35.020
CCS 653

DB46

海 南 省 地 方 标 准

DB46/T XXXX—XXXX

无人驾驶航空器供应链管理 网络安全要求

UAS supply chain management—Cybersecurity requirements

（征求意见稿）

（本草案完成时间：2026.4.9）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

海南省市场监督管理局　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由海南省市场监督管理局提出并归口。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件起草单位：向数科技（海南）有限公司、海南临空产业发展集团有限公司、中国网络安全审查认证和市场监管大数据中心、海南正邦信息科技有限公司、海南警察学院、国铁新能源发展（北京）有限公司、郑州大学、海南省网络安全和信息化协会、海南师范大学。

本文件主要起草人：宋明秋、王海烨、李京春、封化民、陈世翔、林明瑜、张鲲、张大龙、肖凝、张大年、张建军、刘尚喜等。

无人驾驶航空器供应链管理 网络安全要求

1 范围

本文件给出了无人驾驶航空器系统所包含的数字要素产品和服务供应链的安全要求。

本文件适用于民用无人驾驶航空器系统中与数字要素相关的硬件、软件产品、接口和服务供应链安全属性的识别、检测和管理，可作为无人驾驶航空器系统运营方及所包含的数字要素产品供应商和服务提供方的供应链安全管理依据，也可作为第三方机构的测评依据。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 35018—2018 民用无人驾驶航空器系统分类及分级

GB 42590—2023 民用无人驾驶航空系统安全要求

GB/T 43698—2024 网络安全技术 软件供应链安全要求

GB 46750—2025 民用无人驾驶航空器系统运行识别规范

GB 46860—2025 民用无人驾驶航空器唯一产品识别码

3 术语和定义

GB/T 25069－2022界定的以及下列术语和定义适用于本文件。

3.1

无人驾驶航空器 unmanned aircraft

没有机载驾驶员、自备动力系统的航空器，简称“无人机”。

[来源：GB 42590—2023,3.1]

3.2

硬件物料清单 hardware bill of materials

硬件设备中所包含的所有组件的清单，以及硬件内外部依赖关系和安全信息的描述。

3.3

软件物料清单 software bill of materials

软件中所包含的所有组件、文件、开源代码片段的清单，以及软件内外部依赖关系和安全信息的描述。

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Program Interface）
CB：民用波段（Citizen’s Brand）
CDN：内容分发网络（Content Delivery Network）
FRS: 家庭无线电系统（Family Radio Service）
GCS：地面控制站（Ground Control Station）
GMRS：通用移动无线电服务（General Mobile Radio Service）
HBOM：硬件物料清单（Hardware Bill of Materials）
IPRS：个人应答系统（Personal Response System）
LOS：视距（Line of Sight）
MURS：多使用无线电服务（Multi-use Radio Service）
SBOM：软件物料清单（Software Bill of Materials）
SCA：软件成分分析（Software Composition Analysis）
SMI：系统管理接口（System Management Interface）
UA：无人驾驶航空器（Unmanned Aircraft）
UAS：无人驾驶航空器系统（Unmanned Aircraft System）

5 无人驾驶航空器系统供应链安全架构

5.1 无人驾驶航空器系统包含数字要素的产品和组件

本文件所描述的无人驾驶航空器系统中包含数字要素的产品和组件主要包括：

a) 无人机机身。包括：指示灯、高清摄像头、专业图像处理器、视觉定位传感器、电机、飞行控制器、加速传感器、陀螺仪、气压计、TF卡插口、电源等等。
b) 负载。负载可以内装，也可以外挂。包括：
   1) 装备，例如：光谱成像设备、测绘扫描设备，挂轨式巡检机器人和运营识别模块等；
   2) 货物。
c) 传感器
   1) 图像传感器，例如：光电传感器、红外传感器或雷达（包括：合成孔径雷达、逆向合成孔径雷达、海上搜索雷达）等；
   2) 地面、水面或海上移动目标指示器；
   3) 光检测器；
   4) 化学、生物、放射、核或爆炸物检测器；
   5) 自动化地识别、检测和标识信息和信号信息的传感器；
   6) 激光测距仪和/或激光制导能力（可选）；
   7) 未来，可能还包括环境、多光谱或超光谱的传感器。
d) 通信中继。可提供以下通信中继方式，允许用户跨越无线电、数据链路和网络之间进行通信，包括：
   1) 无线电通信；
   2) 音频通信；

3） 网络数据流；
4） 桥接、范围扩展和转换的能力。

e） 人员要素。尽管无人驾驶航空器本身是无人驾驶的、但无人驾驶航空器系统是有人的，包括：
1） 操作员；
2） 维护人员；
3） 任务控制员；
4） 智能分析员。

f） 控制要素。地面、海面、空中等多个方面处理与控制要素，包括：
1） 任务控制；
2） 命令与控制链接（C2）；
3） 负载控制；
4） 通信控制；
5） 控制基站。

注：地面控制站（GCS）是一种陆基或海基控制中心，提供人为控制无人机的设施。

g） 数据链接
1） 数据链接包括所有UA、UAS控制要素、用户以及数据使用者之间的通信方式；
2） 数据链路将UA与GCS连接起来，使操作员能够远程控制UA并接收传输。数据链路既可以通过无线电建立，也可以通过卫星和网络节点建立，用于LOS通信；
3） UAS通常使用两个或多个天线来维持GCS和卫星之间的数据链路。接收来自GCS的信号的天线面朝下，可以是定向和/或全向的。接收卫星信号的天线面朝上，通常是定向的。由于全向LOS天线通常只用于发射和回收，因此干扰LOS数据链的时间框架相当短。特别是在着陆阶段，UAS非常容易受到可能的数据链路丢失的影响；
4） 数据可被直接传输到UAS操作员或传输到另一个网络，以进一步利用和分发；
5） UAS数据可以通过多种通信传输，例如：4G、5G、6G、卫星通信、地面电路、无线电信号、光电传输等。

h） 软件要素
1） 飞行控制系统；
2） 交通管理系统；
3） 无人值守监控系统；
4） 测控系统；
5） 信息传输系统；
6） 任务与设备系统；
7） 发射与回收系统。

i） 支持要素
1） 物流支持。包括部署、运输、维护、发射和回收UAS的所有预处理设备；
2） 大的UAS比小的UAS需要更多的支持要素。

注：本文件关注无人驾驶航空器系统（UAS），而不只是无人机（UA），二者的区别在于：无人机只关注飞行器本身，不包括地面控制或通信系统等辅助部件；而无人驾驶航空器系统，不仅包括无人机，还包括使空中任务成为可能的支持部件，包含地面控制站、通信与软件（例如各种无人机APP）、数据链接、有效载荷、运营管理团队等。

5.2 无人驾驶航空器系统供应链安全目标

UAS供应链比传统供应链面临更多安全风险，需加强UAS供应链安全风险管理，重点实现以下目标：

a） 合规性。遵守相关法律法规，遵守政府、行业主管部门政策、标准、规范和组织安全管理要求，包括《无人驾驶航空器飞行管理暂行条例》《网络安全法》《数据安全法》《个人信息保护法》《数据出境安全评估办法》等相关法律法规以及海南省相关管理规定。
b） 真实性。保证每一台UAS及其产品、组件和服务都具有唯一的真实身份或来源，并且其真实身份或来源是可识别的。
c） 完整性。保证UAS供应链所有环节中所包含的数据要素产品和服务及其组件、部件、元器件、数据等要素不被非法植入、篡改、替换和伪造，并且不存在已知漏洞。
d） 可用性。保证供应链中产品、服务的连续性，UAS中关键产品和服务供应链的业务连续性应达到行业规定的要求。
e） 机密性。保证UAS供应链上的信息不被非法泄露给未授权者。
f） 抗抵赖。保证UAS供应链上已发送或接收的信息或操作是真实、可记录、可审计的。
g） 韧性。即使因突发事件导致UAS供应链发生中断，仍能持续提供基本服务并快速恢复到正常供应状态的能力，即供应链韧性，包括硬件生存性和软件弹性。
h） 数据安全。保证UAS供应链中数据和个人信息安全得到妥善保护。涉及数据跨境的，应符合国家互联网信息办公室《数据出境安全评估办法》、《个人信息出境标准合同办法》、司法部《促进和规范数据跨境流动规定》以及海南省关于数据跨境安全相关规定。

6 硬件物料清单

6.1 概述

在UAS设计、生产和分销供应链过程中应引入硬件物料清单（HBOM），提高识别潜在硬件安全风险的能力，提高供应链管理的透明性。

6.2 HBOM 基本信息

HBOM基本信息包括HBOM头信息、供应商名称、产品详情、组件详细信息以及零部件的详细信息（表1）。

表1 硬件物料（HBOM）基本信息

数据类型	定义	示例
HBOM头信息	识别HBOM相关的信息（产品—描述信息和HBOM作者/日期）	作者、创建/修改日期，产品类型、名字、描述、供应商/OEM
供应商名称	HBOM中的供应商名称	（合同）供应商名字、集成&测试服务提供商、组件制造商/供应商
供应商地址	HBOM表中供应商单位地址	供应商单位地址的详细信息
硬件产品信息	硬件产品：技术信息	产品版本
产品详细信息	产品/操作/技术信息	供应商成分分析、前置时间、数量、技术节点
组件信息	组件描述信息	组件的版本
组件零部件的详细信息	组件零部件技术信息	零部件的技术说明书

6.3 依赖关系信息

识别UAS供应链的依赖关系，包括：

a） UAS中硬件产品和组件在供应链上下游中的位置；

b） UAS中硬件产品和组件之间的包含关系。

6.4 硬件安全性信息

6.4.1 合规性

评估硬件产品供应链符合国家法律法规（包括《无人驾驶航空器飞行管理暂行条例》《网络安全法》《数据安全法》《个人信息保护法》《数据出境安全评估办法》等相关法律法规以及海南省相关管理规定）、行业标准规范（例如无线电发射设备需符合无线电发射设备型号核准）、客户要求以及产品自身需求的情况，并确保UAS制造商了解基于UAS操作环境的风险。

6.4.2 真实性

此项包括：

a） UA唯一身份标识。依据GB 46860—2025，每一台无人驾驶航空器产品都应在外包装表面、机身等位置明显标识其唯一产品机读码标识，保证其身份真实、且可采用目视法识别；

b） 供应链可溯源。保证UAS组件中包含数据要素的产品供应链清晰，可溯源。

6.4.3 完整性

此项包括：

a) 组件完整性。保证UAS硬件供应链中所包含的数据要素产品和服务及其组件、零部件等要素不被非法植入、篡改、替换和伪造，避免因非法改装而产生安全风险；

b) 漏洞管理。确保硬件设备不存在已知的硬件漏洞或缺陷，及时更新设备组件、零部件或固件，采取必要措施防止硬件漏洞被利用；

c) 风险场景下安全保障效果评估。评估硬件产品在面临漏洞被利用或不可信场景下的安全保障效果。

6.4.4 可用性

此项包括：

a) 评估重大事件对于硬件供应链的影响；

d) 评估供应链网络硬件的常见事件或单点失效可能导致的供应链中断风险，采取措施保证供应链的持续稳定运行。

6.4.5 生存性

6.4.5.1 手动操作

确保无人驾驶航空器具有手动操作模式，必要时通过人工干预的方式，保证航空器安全。

6.4.5.2 失效安全

参考ARP4761，采用FMEA等方法，识别UAS硬件失效模式，采取措施避免硬件失效带来的风险，确保即使发生UAS失效事件，也不会对对系统用户造成伤害。例如：

a） 在电源电能低于20%的情况下，无人机可自动返航；

b） 在一个传感器出现故障的情况下，可自动切换到另一套传感器，保证无人机对环境的正常感知能力；

c） UAS具有感知紧急事件的能力，必要时通过人工干预，实现UA的悬停、迫降或自动返航。

6.4.5.3 防故障

UAS应内置设备故障预防机制，保证及时识别和处理故障避免造成重大设备故障，并建立故障追溯机制。包括：

a) 故障类型
   1) 单点故障。因某个关键设备组件发生故障，导致UAS整体故障；
   2) 多点故障。多个设备组件发生组合故障，引发UAS整体功能失效；
   3) 潜在故障。在故障检测时间内未能被安全机制检测出来的、也未能被无人机驾驶员识别的故障；
   4) 残留故障。某个硬件单元中已被故障识别装置检测出来但未能及时修复的故障。
b) 故障识别
   1) 内置故障检测机制。UAS应内置安全故障识别装置或组件故障检测能力；
   2) 故障诊断。通过内置安全检测组件评估设备故障，并评估故障的检测或诊断覆盖率以及残余故障的情况。
c) 故障处理
   1) 故障暴露时间。设计设备的重启（手动、自动）或自我恢复机制，将事件暴露时间缩短到可接受的水平；
   2) 安全切换。应设计安全状态保持机制，或由故障状态安全地切换到安全状态的能力，特别是在故障缓解或容错时间内，设备应具备安全自我保护能力；
   3) 容错机制。设计故障容错机制，保证即使设备输入了错误信息，也能自动识别并纠正错误输出正确结果。
d) 建立故障追溯机制
   1) 建立故障发现、响应、处理、根因分析全过程的故障闭环复盘机制；
   2) 记录每次故障发生的时间、配置变更内容和操作人员，建立故障追溯机制。

6.4.6 数据和隐私安全

6.4.6.1 重要数据保护

采用可信的硬件设备，加强硬件安全，是UAS安全的基础。例如：采用可信硬件模块或专用硬件设备对重要数据进行加密，防止对硬件设备的攻击；或者为UAS提供受保护的容器，当重要代码被加载到受保护的容器中，将执行区域完整性检查，防止内存攻击。

6.4.6.2 隐私保护

采用硬件增强的计算环境，通过可信处理器、加密模块等，实现敏感数据的处理和传输。例如：采用隐私计算环境，避免个人敏感信息在数据处理的过程中被泄露。

6.5 映射关系

评估硬件设备及组件的安全状况，建立映射关系表，见表2。

表2 HBOM与安全性的映射关系表

安全属性		合规性			真实性		完整性			可用性		生存性			数据安全	
基本信息类型	子项	政策与法规	行业与用户需求	内部政策与质量管理	UA唯一身份标识	供应链可溯源	组件完整性	漏洞管理	风险场景安全保障效果	重大事件影响	常见问题及单点失效	手动操作	失效安全	防故障	重要数据保护	隐私保护
产品详细信息	产品1															
	产品2															
	产品3															
零部件详细信息	部件1															
	部件2															
	部件3															

7 软件物料清单

7.1 概述

提供详细的软件物料清单（SBOM），包括软件的基本信息、软件组成信息、依赖性信息、安全性信息、扩展信息、软件的签名信息等，提高对软件设计、开发、交付和部署整个生命周期中引入潜在安全风险的识别能力，提高软件供应链管理的透明性。

7.2 SBOM 信息

SBOM信息主要内容包括：

a） 基本信息：包含软件的名称、版本、标识、供应商、获取途径、许可证信息、完整性等信息；

b） 清单信息：包含软件物料清单的版本、标识、创建、获取或访问等信息。

7.3 基本信息

SBOM的基本信息包括：

a） 软件名称：SBOM 归属软件的名称；

b） 软件标识：在软件开发、生产、销售等环节中用来区分、识别和描述软件产品的信息，是确保软件唯一性和可追溯性的关键手段；

c） 软件版本：软件的版本编号，应为每个版本的软件生成一份 SBOM；

d） 哈希算法：对软件产品进行完整性保护的哈希算法名称；

e） 消息摘要：对软件产品通过哈希运算获取的摘要值；

f） 软件产品的供应商列表，每个供应商包括如下字段信息：

1） 供应商：软件供应商的注册名称；

2） 供应商类型：软件供应商的类别，包括开发商、集成商、代理商、其它；

3） 所属区域：软件供应商注册地所属国家省市名称，格式应为“国家-[省]-市”，最小区域至城市，例如：“中国-北京”和“中国-海南省-海口市”；

4） 开发商：编写软件的人员或组织的名称；

5） 供应商类型为集成商或代理商时，本字段应为必选项；

g） 获取途径：软件获取渠道，包括代码托管平台、第三方下载站点、开源社区等；

h） 许可证信息（授权）：软件许可证名称，应在许可证信息中提供软件许可证的详细字段数据，如不存在许可证应为 NULL 值；

i） 授权期限：软件授权使用的截止日期，日期格式应为“YYYY-MM-DD”；

表3 SBOM基本信息

信息项	信息子项	信息描述	字段类型（必选或可选）
软件名称			
标识			
版本号			
完整性	哈希算法		
	信息摘要		
供应商	开发商		
	集成商		
	代理商		
获取途径			
许可证信息			
授权期限			

7.4 清单信息

SBOM 清单信息包括：

a） 清单格式名称：SBOM 所采用格式标准的名称，可设为固定值，例如“SBOMDF”；

b） 格式版本：SBOM 遵循的数据格式的版本号；

c） 清单标识：每个生成的 SBOM 都应该有一个唯一的序列号；

d） 生命周期：一个 SBOM 生成时，软件所处生命周期的阶段，包括：开发阶段、交付阶段、运维阶段、废止阶段；

e） 时间戳：创建 SBOM 的日期和时间，例如“YYYY-MM-DDHH:mm:ss”；

f） 创建者：创建 SBOM 的实体组织或个人的名称；

g） 创建工具：创建 SBOM 的工具名称和版本；

h） 下载链接：获取 SBOM 的 URL 地址。

表4 SBOM软件物料清单信息

信息项	信息子项	类型	字段类型
清单格式名称			
格式版本			
生命周期阶段			
时间戳			
创建者			
创建工具			
下载链接			

7.5 组成信息

通过 UAS 软件组成信息分析来识别该软件组成成分的来源、版本、许可证等信息（表 5），识别其供应链依赖关系（例如某上游组件包含在某个软件中），识别和管理潜在的供应链安全风险。具体包括：

a） 来源。软件组成成分来源于开发商、集成商、代理商、自主开发或第三方开源代码库等；
b） 版本。组件的版本号信息；
c） 许可证信息。许可证全称、是否通过 OSI 认证等；
d） 覆盖率。每一种类型代码片段占总代码数量的百分比；
e） 签名信息。保存签名后的摘要信息的文件名称以及用于验证签名的数字证书的文件名称；
f） 获取途径。组件代码的采购、委托开发或在线下载；
g） 下载地址。软件代码下载的 URL 地址；
h） 归属信息。描述软件组件所属航空器子系统。

表5 SBOM软件组成成分清单信息

序号			信息项	来源	版本	许可证信息	覆盖率	签名信息	获取途径	下载地址	归属信息
1			软件名称								
	1-1		组件名称								
		1-1-1	代码片段信息								
		1-1-2	代码片段信息								
	1-2		组件名称								
		1-2-1	代码片段信息								
		1-2-2	代码片段信息								
		1-2-3	代码片段信息								
2			软件名称								

7.6 依赖关系信息

识别UAS软件供应链的依赖关系，包括：
c） UAS中软件产品或组件在供应链上下游中的位置；
d） UAS中软件产品和组件之间的包含关系。

7.7 软件安全性信息

7.7.1 合规性

确保UAS开发和操作符合适用的法律法规，确保UAS开发商了解UAS操作环境的合规风险，包括《网络安全法》《数据安全法》《个人信息保护法》《数据出境安全评估办法》等相关法律法规以及海南省相关管理规定。

7.7.2 真实性

此项包括：
a） 身份标识管理。依据GB 46860—2025，包括UA产品的身份标识编码规则、身份标识的产生、分发、使用、注销等全生命周期管理。并提供多种类型的身份标识，以识别不同供应商、不同服务提供商、不同用户类型等；
b） 识别身份标识。提供一种机制，使系统有能力确认和验证UA的身份标识，并确认其空域权限；
c） 运行识别过程保护。依据GB 46750—2025，为UAS运行识别全过程提供安全保护，有效防止对运行识别模块和数据的篡改、破坏和删除。

7.7.3 完整性

7.7.3.1 不包含已知漏洞

此项包括：

a) UAS不能含有已知漏洞（基于现有的漏洞数据库），因为UAS的安全性影响通常很高，其应用软件产品应具有高安全等级；
b) 建立和执行针对UAS产品安全缺陷、漏洞的应急响应机制和流程，对发现的产品安全缺陷和漏洞采取修复或替代方案等措施，及时告知用户安全风险和可用的补救措施，并向有关主管部门报告。

7.7.3.2 补丁信息

此项包括：

a) 从UAS软件发布到生成SBOM期间，为修复问题和漏洞、优化性能，应发布UAS补丁列表，包含补丁名称、原厂标识、用途描述等信息；
b) 保护用户对UAS软件（包含固件）补丁安装和系统升级等的知情权和选择权，安装和升级时明确告知用户并获得用户同意。

7.7.3.3 安全更新

保证UAS及应用软件可以安全地更新和升级。

7.7.4 机密性

此项包括：

a) 加密机制安全。确保加密协议和算法是按照国家标准要求实现的；
b) 信任机制。通过软件、数据标识和访问控制实现信任机制；
c) 数据防泄露。采取加密通信信道等措施保证无人机控制信息和数据不会被泄露，避免勒索攻击。

7.7.5 抗抵赖

此项包括：

a) 信息抗抵赖。确保UAS发送的操作指令真实、有效，而不是假冒、伪造的，包括：
    1) 原发抗抵赖。确保信息的发起者不能成功地否认曾经发送过信息；
    2) 接收抗抵赖。确保信息的接收者不能成功地否认对信息的接收。
b) 可核查性。通过日志确保所发送的UAS操作指令及其数据操作可核查，保证日志数据的安全性，包括：
    1) 日志包括系统日志、登录日志、操作日志、接口访问日志等类型；
    2) 日志应记录必要的支持UAS运维程序执行过程和状态的信息，例如：监控警告、问题定位、容量预警、业务流程回放、恢复等提供支持数据，以及与安全攻击行为相关信息，例如登陆错误、异常访问等；
    3) 通过工具软件实现对于开启和关闭任何日志分析机制以及由于潜在的安全侵害而采取的动作的自动响应；
    4) 每一类日志都应记录事件发生的日期和时间，并采用校验机制保证日志数据的完整性、准确性、一致性，并严格控制对无人驾驶航空器日志的访问授权，保证日志一旦生成，其内容不能再被修改；
    5) 对日志数据中的个人信息进行去标识化处理；

6） 明确日志的保存期限，满足数据安全与个人信息保护的需求。

c） 可审计性。确保那些与安全相关活动有关的信息被识别、记录、存储和分析，例如：确保由于潜在侵害而产生的报警响应动作是可审计的。通过检查审计记录结果可确定发生了哪些安全相关活动以及哪个用户要对这些活动负责。

7.7.6 可靠性

UAS在预定条件或操作环境下持续正常运行的能力与在特定时间内无故障运行的概率。包括：

a） 自主可控。保证UAS在支持感知、避障、路径规划、导航和控制方面做出有保证的自主决策；

b） 失效安全。参考ARP4761，采用FMEA等方法，识别UAS软件失效模式，采取措施避免软件失效带来的风险。

c） 防故障。UAS宜内置自动检测组件，及时发现并处理系统功能故障，分析故障产生的原因，并建立故障追随机制，以便对已发生的故障追溯到硬件、软件、接口等；

d） 鲁棒性。采用冗余资源、路径冗余、反馈控制等方法，保障UAS在面临内部结构或外部环境变化时，仍能维持其功能稳定运行。

7.7.7 软件弹性

7.7.7.1 理解需求

依据GB/T 44862—2024，分析UAS软件可能面临的不利条件、压力、攻击和失效组件情况的预防、承受、恢复和适应的能力需求，特别是可能存在的极端场景，根据其对UAS运行的影响情况，对UAS软件的弹性能力进行优先级排序，做出最有利于保护UAS和用户的决策。

7.7.7.2 安全开发和集成

此项包括：

a） 软件开发商应理解UAS的设计、开发和集成过程中可能引入的安全风险，采取措施减少漏洞，保证所开发的软件产品不包含已知漏洞；

b） 根据需求分析，设计并实现软件弹性需求目标。

7.7.8 数据和隐私安全

7.7.8.1 重要数据保护

针对UAS中设备配置参数和数据收集、传输、终端设备本地或云端存储等场景，并采取措施保证重要数据不被泄露或/和篡改；

7.7.8.2 隐私安全

理解可能导致个人信息或隐私泄露的情况，或未经授权跟踪UAS数据的情况，采取措施减少个人信息和隐私安全风险。

7.8 映射关系

评估 UAS 所包含的软件及其组件的安全性，建立映射关系，见表 6。

表6　SBOM与安全性的映射关系

安全属性		合规性			真实性			完整性			机密性			抗抵赖			可靠性				弹性		数据安全	
信息项	子项	政策与法规	风险管理	质量管理	身份标识管理	身份标识识别	运行识别过程保护	不包含已知漏洞	补丁信息	安全更新	加密机制安全	信任机制	数据防泄漏	信息抗抵赖	可核查性	可审计性	自主可控	失效安全	防故障	鲁棒性	理解需求	安全开发与集成	重要数据保护	隐私和匿名性
软件产品详细信息	产品1																							
	产品2																							
	产品3																							
组件详细信息	1-1																							
	1-2																							
	2-1																							

8　硬件与软件接口规范

8.1　概述

在系统设计时制定软硬件接口规范，在硬软件开发时对接口规范进行进一步细化。接口规范规定了硬件与软件（包含组件）之间的交互方式，并与技术安全的概念一致。在UAS供应链安全场景下关注以下几种接口规范。

8.2　软硬件一体化场景下的接口规范

在软硬件一体化的场景下，例如智能视频/图像识别系统，软件和硬件之间需要紧密协作，才能达到更高的性能和效率，包括以下特征：

a)　工作模式。硬件设备的工作模式和相关的配置参数，硬件设备的操作模式，例如：缺省模式；
b)　配置参数。初始化、测试或高级模式下的配置参数，例如：增益控制、带通频率或时钟分频器；
c)　隔离。确保单元之间的独立性，支持基于软件分区的硬件特性；
d)　共享和专用硬件资源。例如：内存映射、寄存器、定时器、中断、I/O端口的分配；
e)　接口访问。硬件设备（例如：CPU、内存、主板、网卡、传感器等）的获取机制，包括串口、并口、主/从等；
f)　时序约束。技术安全要素执行的时间先后顺序。

8.3　硬件及加载的软件诊断功能场景下的接口规范

此项包括：

a)　诊断功能定义。定义对硬件的诊断功能，例如：检测过流、短路或过热；
b)　诊断功能实现。在软件中实现对硬件的诊断功能。

8.4　接口安全性信息

此项包括：

a)　安全的用户接口。识别UAS典型硬件与软件入口点或出口点，对入口点设置访问控制机制，或通过中介程序访问数据，实现三重访问控制；

b） 安全的应用程序接口API。采用安全的API，避免不安全的API被黑客利用对UAS进行攻击；
c） 安全管理接口SMI。对于那些用于配置和具有较高优先权的管理软件接口，需保证它们不会被破坏，避免对系统造成严重的影响；
d） 安全的带外管理接口。必须确保只有经过授权的人员和进程才可以访问UAS带外管理接口，调用必要的服务，避免UAS中硬件设备或计算组件处于关闭、睡眠或休眠模式等非活动或关闭状态下，仍能连接到网络；
e） 安全的日志接口。包括UAS日志的应用环境，可配置的事件记录类型、日志信息（状态、报警、完整的堆栈）、日志的可视化接口以及日志的访问控制机制（包括：日志的打开、关闭机制，日志只能增加记录，永远不要覆盖和删除日志的机制）等。

注1：日志记录的基本内容要求包括：支持系统运维的信息，包括反应系统运行状态的监控警告信息、为快速准确定位问题提供数据支持的问题定位信息、反映系统性能瓶颈或潜在风险的信息、为业务流程回放、为系统恢复提供支持的信息以及与安全相关的信息，例如系统登陆错误、异常访问等。

注2：为保证日志记录的真实有效性，日志记录时通常加上记录的日期和时间。

8.5 映射关系

建立UAS接口与安全性的映射关系，见表7。对于API使用需按业务需求最小化原则，防止数据过度传输。

表7 UAS接口与安全性的映射关系

安全性 / 接口类型	安全的用户接口	安全的API	安全的SMI	安全的带外管理接口	安全的日志接口
软硬件一体化场景下的接口					
硬件及加载的软件诊断功能场景下的接口					

9 外部服务清单

9.1 外部服务类型

此项包括：
a） 卫星通信服务；
b） 雷达及空中交通管制服务；
c） 无线电通信和数据传输服务，包括：CB，FRS，GMRS，IPRS和MURS等；
d） 光通信和数据传输服务；
e） 无线网络通信服务，包括：4G、5G、6G，蓝牙、Wifi等；
f） 应用层服务，包括：网络域名服务、CDN服务、邮件发送、短信发送、支付接口等。

9.2 外部服务安全

确定外部服务的供应链安全性指标，包括供应链恢复时间目标、恢复点目标以及最大可容忍中断时间等，保证UAS所涉及的各类外部服务安全稳定运行，保证UAS运行安全。

注：无人驾驶航空器信息通信、数据传输重要服务子系统恢复时间目标不得大于30毫秒，恢复点目标不得大于10分钟，最大可容忍中断时间不得大于30毫秒。

10 供应商管理

10.1 采购

此项包括：

a) 采购UAS及组件时，应采购符合国家安全标准、经过第三方机构测试合格的产品；
b) 采购UAS关键组件时，应参照关键设备采购清单；
c) 实行UAS供应商备案制度。

10.2 供应链风险管理

此项包括：

a) 确保UAS供应链的完整性。通过识别、评估和减轻与信息技术产品和服务相关的风险，包括可信性、资质和假冒等，改善公司的安全实践。包括相关利益相关方的参与、数据安全保护以及将供应链安全实践整合到公司的决策、预算和运营流程中；
b) 供应商多样性。保证UAS关键组件供应商的多样性，避免单一供应源而存在潜在的供应链中断风险；
c) 供应商的可见性。通过HBOM和SBOM表，实现UAS全生命周期的供应商管理；
d) 供应链运营管理平台服务中断风险。在供应链管理服务平台和相关企业落实安全管理和技术，保证UAS供应链服务持续稳定运行；
e) 知识和技能。建立、实施和管理供应链安全相关知识、技能和经验，为UAS供应链安全提供重要保证；
f) 实施保证。企业领导、管理层应充分理解UAS供应链安全管理对业务风险的影响，在组织范围内培养UAS供应链安全管理意识和文化，使UAS供应链安全管理实践能够为企业提供保护，保护企业的资产、员工和客户的安全。

10.3 供应商管理

参考GB/T43698—2024，确定UAS供应商管理要求，包括：

a) 分类分级建立合格的UAS供应商目录,对供应商目录及相关信息进行集中管理,并定期或按照实际需求进行更新维护；
b) 优先选择UAS供应商目录中满足条件的供应商；
c) 对于公务用途UAS可探索白名单机制，减少UAS产品及组件供应链安全重复检测评估的工作量；
d) 根据UAS软件供应链中供应关系、供应活动的不同,供应商应符合本文件10.2的安全要求；
e) 制定UAS供应商选择策略和制度,对供应商进行风险分析,包括但不限于背景、资质、能力以及能否持续安全地提供产品或服务等方面的风险；
f) 要求UAS供应商开展软件供应链安全检测和风险评估工作,明确相关内容和范围;确需第三方服务机构的,应明确对第三方服务机构的能力、资质等要求；
g) 要求UAS供应商配合相关部门开展UAS供应链安全审查、监督和检查；
h) 在UAS供应关系、供应商股权等信息发生变更时,应对变更带来的安全风险进行评估,并采取相应的风险控制措施；

i） 建立UAS供应商替代方案或具备UAS供应链的自主维护能力,防范供应链中断风险；

j） 对供应商的信息应设置安全保护机制，保证供应商信息安全。可对HBOM、SBOM等供应链技术性文档设置适当的保留期限，例如10年。

11 UAS 供应链安全等级划分与安全等级要求

11.1 安全等级划分

本文件依据GB/T 35018—2018，并考虑应用场景和技术指标，将UAS供应链安全等级从低到高依次划分为2级：基本级、增强级，各安全等级的定义见表8。

表8 UAS供应链安全等级

UAS 供应链安全等级	基本级	增强级	
UAS类型	开放类 （满足兴趣爱好）	特许经营类 （满足特殊行业需求）	审定类 （保障重大活动安全）
应用场景	低空旅游、航空体育、消费娱乐、面向个人的消费级无人机、农业植保、农林牧渔等	GB/T 35018—2018所列的应用场景	除军用、警用、海关之外的全类型应用场景
技术指标	微型无人机: 最大设计使用高度≤120m 最大空机重量≤0.25kg 农业植保无人机的最大起飞重量≤150kg	除微型以外的无人驾驶航空器: 120m<最大设计使用高度≤300m 0.25kg<最大空机重量≤116kg 最大起飞重量≤150kg 农业植保无人机的最大起飞重量可>150kg	25公斤以上中型、大型无人机

注：此表中无人机类型和技术指标来源于《无人驾驶航空器飞行管理暂行条例》和GB/T 35018—2018。

11.2 安全等级要求

根据11.1节UAS安全等级的划分，参照GB/T 18336-2—2015中功能安全要求和等保2.0,提出UAS供应链安全等级要求，见表9。其中，用于科学研究或自己组装的非商业用途无人机在适飞空域内可不受本文件要求的限制。

表9 UAS供应链安全等级要求

UAS 供应链安全要素			UAS 供应链安全等级要求	
			基本级	增强级
硬件	合规性	政策与法规	✓	✓
		行业与用户需求	✓	✓
		内部政策与质量管理	✓	✓
	真实性	UA 唯一身份标识	✓	✓
		供应链可溯源		✓
	完整性	组件完整性	✓	✓

		漏洞管理	✓	✓
		风险场景安全保障效果		✓
	可用性	重大事件影响		✓
		常见问题及单点失效		✓
	生存性	手动操作	✓（可人工介入）	✓
		失效安全		✓
		防故障		✓
	数据安全	重要数据保护		✓
		隐私安全	✓	✓
软件	合规性	政策法规	✓	✓
		风险管理	✓	✓
		质量管理	✓	✓
	真实性	身份标识管理	✓	✓
		身份标识识别	✓	✓
		运行识别过程保护	✓	✓
	完整性	不包含已知漏洞	✓	✓
		补丁信息	✓	✓
		安全更新	✓	✓
	机密性	加密机制安全		✓
		信任机制		✓
		数据防泄漏		✓
	抗抵赖	信息抗抵赖		✓
		可核查性		✓
		可审计性		✓
	可靠性	自主可控		✓
		失效安全		✓
		防故障		✓
		鲁棒性		✓
	软件弹性	理解需求		✓
		开发和集成		✓
	数据安全	重要数据保护		✓
		隐私安全	✓	✓
接口	接口类型与安全性	安全的用户接口		✓
		安全的应用程序接口		✓
		安全管理接口		✓
		安全的带外管理接口		✓
服务	无线网络及通信服务安全			✓
	卫星通信服务安全			✓
	雷达及空中交通管制服务			✓
	无线电通信和数据传输服务			✓
	光通信和数据传输服务			✓
	应用层服务			✓

附 录 A
（参考性）
海南省无人驾驶航空器系统供应链安全风险分析

海南省UAS丰富的应用场景，为低空经济的发展带来了新的发展机遇，但也带来了巨大的安全风险隐患。海南省UAS供应链安全风险分析见表A.1。各类风险要素的严重性、高发性和风险水平均为高，使海南省UAS供应链安全管理成为亟待解决的问题。

表A.1 海南省无人驾驶航空器系统供应链安全风险分析

供应链风险类型	风险要素	潜在影响	严重性	高发性	风险水平
硬件供应链风险	a) 硬件供应链不符合国家法律法规 b) 物理设备不存在身份标识、身份标识未被识别、被篡改或破坏 c) 物理设备或组件被非法篡改，完整性被破坏 d) 物理设备或组件不可信 e) 缺少HBOM，无法识别硬件供应链风险来源	a) UAS产品不合规导致系统不可控 b) 存在黑飞、未备案飞行等情况，存在无人机高空坠落、抛物、航空器被物理劫持、走私的可能性 c) 无人机被非法改装，导致无人机不可控 d) 系统设备不可控、重要数据被盗窃 e) 硬件故障无法追溯，无法确定事件责任	高	较高	高
软件供应链风险	a) UAS软件及组件的安全漏洞被利用 b) UAS软件缺少安全性保证措施，导致UAS软件被非法控制、被劫持 c) 硬件、软件之间的接口缺少安全保证措施，增加了攻击面 b) 缺少SBOM，无法识别软件供应链风险来源	a) 复杂的软件操作环境和供给面的扩大，导致UAS系统被攻击、被非法控制，无人驾驶航空器被劫持 b)软件故障无法追溯，导致无法确定事件责任	高	较高	高
供应链中断风险	UAS中各种硬件、软件、产品组件和服务发生中断，包括网络、微信通信、雷达、无线电等服务中断	特殊的社会、经济、地理环境，使海南UAS供应链中断带来的影响具有极大的不确定性，一旦发生供应链中断事件，造成的潜在损失或影响巨大	高	较高	高
供应商风险	政策风险	海南自贸岛封关运作，海南成为中国高水平对外开放的新篇章，世界各地的政策、制度、标准、技术、产品和服务在这里汇集，政策的理解和交叉应用变得高度复杂，给UAS供应链安全管理带来挑战。政策变化导致供应链中断风险，使UAS无法运维，产品及组件无法更新	高	高	高
	市场风险	海南省汇聚了全球的供应商，产品采购谈判、合同签订、供应商背景调查难度加大，影响采购进度，市场风险高	高	高	高
	信用风险	海南自贸岛是国际大市场环境，合同欺诈、合同陷阱、合同执行、违反合同等损失、合同结算等都存在较高风险	高	高	高
	物流风险	海南物流来源广泛、运行环境复杂，不仅包括境内的物流也包括境外的物流以及境内外交汇的转口物流；海南自然环境多热带风暴和台风等特点，都给UAS供应商物流管理带来挑战	高	高	高

参考文献

[1]. GB/T 18336.2—2024 网络安全技术 信息技术安全评估准则 第2部分：安全功能组件
[2]. GB/T 18336.3—2024 网络安全技术 信息技术安全评估准则 第3部分：安全保障组件
[3]. GB/T 36637—2018 信息安全技术 ICT供应链安全风险管理指南
[4]. GB/T 38931—2021 民用轻小型无人机系统安全性通用要求
[5]. GB 42250—2022 信息安全技术 网络安全专用产品安全技术要求
[6]. GB/T 42581-2023 信息技术服务 数据中心业务连续性等级评价准则
[7]. MH/T 4064—2026 民用无人驾驶航空器航行服务系统数据安全技术要求
[8]. SAE ARP4761A-2023 民用航空器、系统和设备安全评估过程指南
[9]. T/ISC 0035—2023 软件成分分析（SCA）知识库总体技术要求.
[10]. YD/T 6330.1-2025 信息通信行业质量管理体系分级认证评价准则 第1部分：生产服务组织质量管理体系分级认证评价准则
[11]. ISO 21384—2:2021 Unmanned aircraft systems — Part 2: UAS components.
[12]. ISO 26262—2018 Road vehicles—Functional safety—Part 2:Management of functional safety.
[13]. ISO 28000:2022 Security and resilience — Security management systems — Requirements
[14]. ISA/IEC 62443 Security of industrial automation and control systems.