《民用无人驾驶航空器数据链路网络安全要求》强制性国家标准

编制说明

（报批稿）

2026 年 10 月

目录

一、工作简况 1

（一）任务来源 1

（二）制定背景 1

（三）起草过程 2

二、编制原则、强制性国家标准主要技术要求的依据及理由 4

（一）标准编制原则 4

（二）主要技术要求及其确定依据 4

（三）修订前后技术内容的对比[仅适用于国家标准修订项目] 13

三、与有关法律、行政法规和其他强制性标准的关系 13

四、与国际标准化组织、其他国家或者地区有关法律法规和标准的比对分析 15

五、重大分歧意见的处理过程、处理意见及其依据 16

六、对强制性国家标准自发布日期至实施日期之间的过渡期（以下简称过渡期）的建议及理由 16

七、与实施强制性国家标准有关的政策措施 16

八、是否需要对外通报的建议及理由 16

九、废止现行有关标准的建议 16

十、涉及专利的有关说明 17

十一、强制性国家标准所涉及的产品、过程或者服务目录 17

十二、其他应当予以说明的事项 17

国家标准《民用无人驾驶航空器数据链路网络安全要求》（征求意见稿）编制说明

一、工作简况

（一）任务来源

根据国家标准化管理委员会2025年下达的国家标准制修订计划，强制性国家标准《民用无人驾驶航空器数据链路网络安全要求》由工业和信息化部和中国民用航空局联合提出并归口，委托全国网络安全标准化技术委员会组织制定，中国电子技术标准化研究院牵头起草，计划号：20256752-Q-339。

（二）制定背景

民用无人驾驶航空器数据链路在无人机飞行中扮演着至关重要的角色，它不仅是飞行器与地面系统间通信的桥梁，更是整个民用无人驾驶航空器能够高效运作的关键。民用无人驾驶航空器数据链路包含上行链路、前向链路、下行链路、反向链路等，涵盖控制指令、遥测数据、任务载荷等重要信息，数据链路通常使用蓝牙、WLAN、蜂窝网络、卫星等无线网络，容易受到敌手攻击，导致民用无人驾驶航空器劫持、数据泄露、指令篡改等安全问题，甚至会干扰民航飞行、危害人民群众生命财产安全和国家安全。

2023年5月，国务院、中央军委发布《无人驾驶航空器飞行管理暂行条例》（国令第761号）要求从事民用无人驾驶航空器系统的设计、生产、使用活动，应当符合国家网络信息安全相关规定。2023年12月，工业和信息化部发布《民用无人驾驶航空器生产管理若干规定》（工业和信息化部令第 66 号），要求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。

为落实《无人驾驶航空器飞行管理暂行条例》《民用无人驾驶航空器生产管理若干规定》等政策法规相关要求，切实维护国家安全和公共利益，制定本标准，对民用无人驾驶航空器数据链路网络安全要求提出规范。本标准对防范民用无人驾驶航空器数据链路网络安全风险，提升网络安全水平起到规范作用，促进低空装备行业高质量发展。

（三）起草过程

1、预研阶段

在标准立项之初，中国电子技术标准化研究院在行业主管部门的指导下，组织开展了大量的资料搜集和调研研讨工作。主编单位认真学习了《强制性国家标准管理办法》，确定了标准框架的大纲，并针对国内外无人机行业现状和安全基线进行了研讨。

2025 年 5 月，征集并组建标准预研团队，编制形成第一版草案。中国电子技术标准化研究院在北京组织召开了强制性国家标准编制启动会，成立了标准编制组。主编单位中国电子技术标准化研究院对强标背景、要求、总体方案等情况进行介绍。各编制单位按各自专业对现有的标准大纲进行了分工，并明确了强制性国家标准的编写要求，全面启动标准预研工作。

2025 年 6 月-2025 年 8 月，按强制性国家标准双归口管理，工业和信息化部和中国民用航空局听取了编制组关于《民用无人驾驶航空器数据链路网络安全要求》拟定标准范围、当前国内无人机运行困难与瓶颈、国内外标准适用性等方面的情况汇报，对标准适用范围，标准的科学性、合理性和可验证性进行了讨论。组织 30 余家无人驾驶航空器行业企业多次开展调研、召开 2 次线下研讨会，收集企业反馈材料，进一步完善标准草案。

2025 年 8 月 28 日，按照“电子标准院关于召开第八批工业和信息化领域强制性国家标准立项评审会的通知”，编制组参加了《民用无人驾驶航空器数据链路网络安全要求》强制性国家标准项目立项评估汇报答辩，从立项必要性、可行性、通用范围、解决的关键问题、技术先进性创新性等方面进行了汇报，通过了《民用无人驾驶航空器飞行控制系统数据记录要求》的项目建议书和项目申报书。

2025 年 9 月-2025 年 10 月，标准牵头单位组织 30 余家行业企业开展标准文本编制，举办线下线上研讨会 11 次，累计收集并处理反馈意见 130 条（主管部门 8 条、生产制造企业 61 条、科研院所 38 条、其它单位 23 条），其中采纳 68 条、部分采纳 18 条、未采纳并沟通一致的 44 条，推动标准文本历经 14 轮迭代优化，形成了较为完善的标准草案。

（4）2025 年 11 月-2025 年 12 月，走访近十家低空装备制造企业，开展标准条款验证，提升标准内容的科学性与可行性。

2、起草阶段

（1）2025 年 12 月 22 日，国家标准化管理委员会下达本强制性国家标准的制定计划，标准正式立项。

（2）2026 年 1 月 16 日，受工业和信息化部、中国民用航空局委托，中国航空综合技术研究所在北京主持召开“《民用无人驾驶航空器数据链路网络安全要求》等三项强制性国家标准制定启动会（部委指导会）”。来自国家发展改革委低空司、国家市场监督管理总局标准技术司、工业和信息化部工业二司、中国民用航空局适航审定司、中国民用航空局空管行业管理办公室、中国标准化研究院、中国质量认证中心、工业和信息化部装备工业发展中心、国家无线电监测中心、民航二所，以及深圳大疆、道通智能、中航无人机、深圳美团、成都纵横、国网智能等政府有关部门、科研院所和企业的近 45 名代表参加会议。会议围绕三项强制性国家标准的编制情况、初稿框架和推进计划进行研讨，旨在强化部委指导、凝聚行业共识、明确标准研制路径。其中，《民用无人驾驶航空器数据链路网络安全要求》为本次启动的三项强制性国家标准之一。

（3）2026 年 1 月-2026 年 2 月，标准起草组召开 2 次线上会议，对标准内容进行研讨，收集并处理意见 108 条（生产制造企业 52 条、科研院所 34 条、其它单位 22 条），其中采纳 57 条、部分采纳 6 条、未采纳并沟通一致的 45 条，进一步推动标准草案的完善。

（4）2026 年 3 月 5 日，组织专家评审会，专家一致同意该项标准通过评审，根据专家意见修改完善后形成征求意见稿。

3、公开征求意见阶段

（1）2026 年 7 月 1 日-2026 年 8 月 31 日，通过工业和信息化部、国家标准化管理委员会网站、向社会公开征求意见，共收到意见 103 条。

（2）2026 年 8 月-2026 年 9 月，联合无人驾驶航空器制造企业，标准编制组组建标准验证团队，搭建标准验证环境，研发标准验证工具，在实机上对标准条款进行逐条验证，验证了相关标准条款的可行性和可操作性。

（3）2026 年 9 月 2026 年 10 月，标准编制组对征集到的 103 条意见逐条研究处理，其中采纳 45 条、部分采纳 41 条、不采纳 17 条；在此基础上形成标准送审稿。

二、编制原则、强制性国家标准主要技术要求的依据及理由

（一）标准编制原则

本标准的编制原则是：

1）通用性：民用无人驾驶航空器的生产者、使用者和测试服务提供者均可依据本标准，开展微型、轻型、小型、中型和大型民用无人驾驶航空器数据链路的设计、开发、制造与测试活动。

2）可行性：为确保标准中技术要求可验证、可操作，本标准编制过程中与科研机构、相关企业、专家进行了多轮研讨。

3）符合性：符合《无人驾驶航空器飞行管理暂行条例》《民用无人驾驶航空器生产管理若干规定》等法律法规和GB 42590-2023《民用无人驾驶航空器系统安全要求》等标准规范对于民用无人驾驶航空器数据链路网络安全的相关要求。

（二）主要技术要求及其确定依据

1、范围

本标准规定了民用无人驾驶航空器数据链路的网络安全技术要求和测试方法，适用于微型、轻型、小型、中型和大型民用无人驾驶航空器数据链路的设计、开发、制造与测试，不适用于模型航空器与自备动力系统的飞行玩具，不适用于运行识别通信链路。

考虑到模型航空器和自备动力系统的飞行玩具分别在《无人驾驶航空器飞行管理暂行条例》和《民用无人驾驶航空器生产管理若干规定》中有明确定义，且相关标准规范正在或规划制定，本文件不适用于模型航空器与自备动力系统的飞行玩具，其具体界定分别见标准正文注1、注2；运行识别通信链路的相关要求在GB 46750—2025《民用无人驾驶航空器系统运行识别规范》中另有规定，本文件亦不将其纳入适用范围。

需要说明的是，本文件技术要求和试验方法主要针对微型、轻型和小型无人驾驶航空器：第5章规定通用安全、上行链路和前向链路安全、下行链路和反向链路安全等安全要求要求，第6章规定相应试验方法。中型和大型无人驾驶航空器系统的相关要求和试验，将陆续在相关适航标准中予以规定。按照主管机关要求，本文件未在“范围”中排除中型和大型无人驾驶航空器系统，而是在第4章中，以“中型和大型无人驾驶航空器……另见相关适航标准”的方式作出衔接性

规定。

2、规范性引用文件

本文件第 2 章规范性引用文件共引用 4 项标准：GB 42590—2023《民用无人驾驶航空器系统安全要求》、GB 46750—2025《民用无人驾驶航空器系统运行识别规范》、GB/T 25069—2022《信息安全技术 术语》、GB/T 38152—2019《无人驾驶航空器系统术语》。其中，GB 42590—2023 规定了民用无人驾驶航空器系统的安全要求，本文件数据链路安全相关要求与其保持衔接；GB 46750—2025 规定了民用无人驾驶航空器系统运行识别要求，本文件不适用于运行识别通信链路；GB/T 25069—2022 和 GB/T 38152—2019 分别规定了信息安全技术和无人驾驶航空器系统术语，本文件相关术语引用其界定。为与现行有效版本保持一致，本文件引用文件均标注年代号。

3、术语和定义

本文件第 3 章共界定“数据链路”“上行链路”“前向链路”“下行链路”“反向链路”“私有协议”6 个术语。其中，“数据链路”“上行链路”“前向链路”“下行链路”“反向链路”引用 GB/T 38152—2019《无人驾驶航空器系统术语》相应条目（部分有修改）；“私有协议”引用 GB 40050—2021《网络关键设备安全通用要求》第 3.6 条。其余术语采用 GB 42590—2023、GB 46750—2025、GB/T 25069—2022、GB/T 38152—2019 界定的术语和定义。

4、安全要求的分类及确定依据

民用无人驾驶航空器数据链路涉及控制站（单元）、中继平台和无人驾驶航空器之间的双向通信，包括上行链路、前向链路、下行链路、反向链路等，面临数据窃取、非法接入、重放攻击等多种安全威胁。依据《无人驾驶航空器飞行管理暂行条例》（国令第 761 号）第八条“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，并采取有效措施减少大气污染物和噪声排放”，基于数据链路的通信方向和网络安全特性，本文件中民用无人驾驶航空器数据链路的网络安全要求分为以下三类：

通用安全要求：适用于所有类别的数据链路，包括实体鉴别、数据防伪造篡改、链路状态感知、抗重放攻击、安全更新、日志记录、密码及密钥安全；

其中，通信实体鉴别要求链路建立或重连时验证通信实体身份真实性，防范非法接入；数据防伪造篡改要求具备验证传输数据完整性和来源真实性的功能；链路状态感知与恢复要求具备感知链路连通、中断等状态及链路异常状态下的自恢复功能；抗重放攻击要求识别并拒绝执行或丢弃重放数据包；安全更新要求具备数据链路相关软件、固件或配置文件的安全更新功能，并验证更新数据完整性和来源真实性；日志记录要求记录数据链路时间信息、源标识及目的标识、安全事件等信息，存储在非易失性存储区域并具备完整性保护功能，无人驾驶航空器和控制站（单元）应存储不少于最近 3 个飞行架次的数据链路日志数据，采用网络存储方式时安全事件信息留存不少于 6 个月；密码及密钥安全要求密码算法、协议及密码模块（如有）符合密码相关标准，并具备防止数据链路相关密钥泄露、非授权读取和修改的安全功能。

上行链路和前向链路安全要求：包括加密传输、恢复与应急处置、访问控制和备份链路安全；

其中，加密传输要求具备保护传输数据机密性的加密功能，防范控制指令等上行数据被窃听、窃取；访问控制要求任一时间仅有 1 个控制站（单元）具有无人驾驶航空器的飞行控制权限，并防止飞行控制权限转移时未授权控制站（单元）接入。

下行链路和反向链路安全要求：包括加密传输和备份链路安全。

该要求对应标准正文 5.3，要求具备保护指挥和控制数据机密性的加密功能，并支持对任务载荷数据进行机密性保护，防范遥测信息和任务载荷数据被窃取。

需要说明的是，标准正文第 4 章基于数据链路的通信方向和网络安全特性，将微型、轻型和小型民用无人驾驶航空器数据链路的网络安全要求分为上述三类；中型和大型民用无人驾驶航空器相关要求另见适航审定相关标准。

5、试验方法

依据《强制性国家标准管理办法》（国家市场监督管理总局令第 25 号）第十九条、第二十条关于强制性国家标准技术要求应当可验证、可操作以及开展试验验证的相关要求，本文件第 6 章规定了与第 5 章安全要求相对应的试验方法，包括试验样机要求、通用安全要求试验方法、上行链路和前向链路安全要求试验方法、下行链路和反向链路安全要求试验方法，逐条规定试验步骤与合格判定，

确保标准条款可验证、可操作、可落地，为产品检测认证和市场监管提供依据。

6.1　试验样机

试验样机包含：

a）无人驾驶航空器、控制站（单元）和中继平台（如有）等数据链路相关设备，预留测试接口（如需）；

b）相关说明文档，包括但不限于网络安全技术文档、网络安全设计声明或其它等效文档；

c）其它安全材料（如有），包括但不限于密码产品检测或认证机构出具的检验报告或认证证书。

6.2　通用安全要求试验方法

6.2.1　通信实体鉴别试验方法

6.2.1.1　控制站（单元）和无人驾驶航空器通信实体鉴别试验方法

按照以下试验方法依次开展试验，判断数据链路是否满足 5.1.1 要求：

a）收集控制站（单元）与无人驾驶航空器间实体鉴别凭证；

b）使用有效凭证，在控制站（单元）与无人驾驶航空器间执行双向实体鉴别，验证数据链路能否正常建立或重连；

c）分别使用失效、伪造凭证，在控制站（单元）与无人驾驶航空器间进行双向实体鉴别，验证控制站（单元）与无人驾驶航空器能否有效识别并拒绝建立或重连数据链路。

6.2.1.2　中继平台通信实体鉴别试验方法

如有中继平台，按照以下试验方法依次开展试验，判断数据链路是否满足 5.1.1 要求：

a）收集控制站（单元）、无人驾驶航空器与中继平台间实体鉴别凭证；

b）使用有效凭证，在控制站（单元）与中继平台间进行双向实体鉴别，验证链路能否正常建立或重连；

c）使用有效凭证，在无人驾驶航空器与中继平台间进行双向实体鉴别，验证链路能否正常建立或重连；

d）分别使用失效、伪造的凭证，在控制站（单元）与中继平台间进行双向实体鉴别，验证控制站（单元）与中继平台能否有效识别并拒绝建立或重连数据

链路；

e）分别使用失效、伪造的凭证，在无人驾驶航空器与中继平台间进行双向实体鉴别，验证无人驾驶航空器与中继平台能否有效识别并拒绝建立或重连数据链路。

6.2.2　数据防伪造篡改试验方法

按照以下试验方法开展试验，判定数据链路是否满足 5.1.2 的要求：

a）若数据链路采用私有协议，查看数据链路传输数据完整性和来源真实性的证明文件。对传输中的数据包实施伪造、篡改攻击，观察无人驾驶航空器和控制站（单元）响应行为，并检查无人驾驶航空器和控制站（单元）的日志记录，验证其是否有效识别并拒绝执行或丢弃伪造、篡改的数据包。

b）若数据链路采用非私有协议，使用工具进行数据抓包，解析通信报文数据，检查数据链路数据传输是否采用传输数据完整性和真实性保护机制。对传输中的数据包实施伪造、篡改攻击，观察无人驾驶航空器和控制站（单元）响应行为，并检查无人驾驶航空器和控制站（单元）的日志记录，验证其是否有效识别并拒绝执行或丢弃伪造、篡改的数据包。

6.2.3　链路状态感知与恢复试验方法

6.2.3.1　链路状态感知试验方法

按照以下试验方法依次开展试验，判断数据链路是否满足 5.1.3 a）要求：

a）建立并维持数据链路，观察无人驾驶航空器或控制站（单元）的链路状态指示是否正常；

b）阻断数据链路，观察无人驾驶航空器或控制站（单元）的链路状态告警指示是否正常。

6.2.3.2　链路恢复试验方法

按照以下试验方法依次开展试验，判断数据链路是否满足 5.1.3 b）要求：

a）建立并维持控制站（单元）与无人驾驶航空器之间的数据链路；

b）触发中断、丢失、阻塞等数据链路异常状态，核查数据链路是否启动恢复机制；

c）停止触发数据链路异常，核查数据链路是否在制造商声明的时间内恢复正常状态或切换至备份链路。

6.2.4　抗重放攻击试验方法

按照以下试验方法依次开展试验，判断数据链路是否满足 5.1.4 要求：

a）建立并维持控制站（单元）与无人驾驶航空器之间的数据链路；

b）使用工具对数据包进行采集和重放；

c）观察无人驾驶航空器对重放数据包的响应行为，并查看无人驾驶航空器的日志记录，是否能识别并拒绝执行重放的数据包；

d）观察控制站（单元）对重放数据包的响应行为，并查看控制站（单元）的日志记录，是否能识别并丢弃重放的数据包。

6.2.5　安全更新试验方法

6.2.5.1　链路更新功能试验方法

按照以下试验方法依次开展试验，判断数据链路是否满足 5.1.5 a）要求：

a）记录更新前无人驾驶航空器数据链路相关软件、固件版本号或配置文件的信息，作为更新验证的比对基准；

b）更新完成且重启后，查看数据链路相关的软件、固件版本号或配置文件的信息，比对更新前版本，核查是否变更为新版本；

c）核查数据链路功能是否正常。

6.2.5.2　链路更新的来源真实性与数据完整性试验方法

按照以下试验方法开展试验，判断数据链路是否满足 5.1.5 b）要求：

a）若数据链路采用离线升级包更新方式，分别构造被伪造、被篡改的升级包，使用离线升级工具将该升级包下载或传输到无人驾驶航空器或控制站（单元），执行离线升级，观察其是否识别并拒绝被伪造、被篡改的升级包。

b）若数据链路采用在线更新方式，使用工具进行数据抓包，解析通信报文数据，核查无人驾驶航空器或控制站（单元）是否对在线升级服务器进行身份真实性验证并使用安全措施保护传输数据完整性；中断后再恢复与在线升级服务器的连接，使用工具进行数据抓包，解析通信报文数据，核查是否重新进行身份真实性验证。

6.2.6　日志记录试验方法

6.2.6.1　安全事件记录试验方法

按照以下试验方法依次开展试验，判断数据链路是否满足 5.1.6 a）要求：

a）校准控制站（单元）、无人驾驶航空器与中继平台（如有）等试验对象的系统时间；

b）分别执行实体鉴别、链路建立、链路断开、链路更新等操作，记录操作时间和内容；

c）导出日志数据，核查控制站（单元）、无人驾驶航空器与中继平台（如有）等日志是否记录时间信息、源标识及目的标识、安全事件等信息并与实际操作一致。

6.2.6.2　日志非易失性存储试验方法

按照以下试验方法依次开展试验，判断数据链路是否满足 5.1.6 b）要求：

a）建立数据链路，分别执行实体鉴别、链路建立、链路断开、链路更新等操作;在未断电前,通过日志查看工具验证相关日志是否已生成并可被正常读取，并记录其日志内容作为对照基准；

b）在日志生成后，对被测设备执行物理断电操作；等待设备完全放电后重新上电，待重启并运行稳定后，再次通过日志查看工具读取或导出日志。核查掉电前所触发的安全事件日志是否完整、准确地被记录和保存，是否发生丢失或损坏。

6.2.6.3　日志数据完整性试验方法

按照以下试验方法依次开展试验，判断数据链路是否满足 5.1.6 c）要求：

a）按照无人驾驶航空器、控制站（单元）和中继平台（如有）的数据链路日志文件存储地址，通过测试接口，修改数据链路日志文件，核查是否能修改数据链路日志文件；

b）按照无人驾驶航空器、控制站（单元）和中继平台（如有）的数据链路日志文件存储地址，通过测试接口，核查是否能在非授权状态下删除数据链路日志文件。

6.2.6.4　数据终端日志存储试验方法

按照以下试验方法依次开展试验，判断数据链路是否满足 5.1.6 d）要求：

a）通过有效方式使日志存储空间达到饱和状态；

b）在正常工作负载下，使用无人驾驶航空器完成 3 个飞行架次；

c）导出无人驾驶航空器和控制站（单元）的日志数据，核查无人驾驶航空

器、控制站（单元）是否完整、准确记录最近 3 个飞行架次的数据链路日志。

6.2.6.5　网络日志存储试验方法

若支持网络日志存储，按照以下试验方法依次开展试验，判断数据链路是否满足 5.1.6 e）要求：

a）构建并触发数据链路运行状态和安全事件，检查是否按照网络日志存储机制记录安全事件信息；

b）检查是否具备留存日志不少于 6 个月的能力。

6.2.7　密码及密钥安全试验方法

6.2.7.1　密码安全试验方法

按照以下试验方法依次开展试验，判断数据链路是否满足 5.1.7 a）要求：

a）核查数据链路中使用的密码算法及协议的名称、用途、何处使用及其实现方式（软件、硬件或固件）；

b）使用检测工具核查密码算法及协议是否符合密码相关标准。

6.2.7.2　密码模块安全试验方法

如有密码模块，按照以下试验方法依次开展试验，判断数据链路是否满足 5.1.7 a）要求：

a）通过读取模块标识、版本信息或核查模块清单及说明文档，与实际使用的密码模块进行一致性比对；

b）检查密码模块是否具备认可的密码产品检测或认证机构出具的检验报告或认证证书。

6.2.7.3　密钥存储安全试验方法

按照以下试验方法开展试验，判断数据链路是否满足 5.1.7 b）要求：

a）若采取安全访问技术保护存储密钥，在未获得授权的条件下，通过测试接口尝试读取、导出密钥，核查是否有效拒绝密钥非授权访问和获取。

b）若采取硬件安全模块或安全软件保护存储密钥，通过文件访问等方式获取密钥存储介质（软件、硬件）中的内容，核查密钥是否以密文或受保护形式存储。

6.3　上行链路和前向链路安全要求试验方法

6.3.1　加密传输试验方法

按照以下试验方法开展试验，判断数据链路是否满足 5.2.1 要求：

a）若采用信道加密方式且数据链路采用私有协议，查看通信通道机密性保护证明文件，通过构造数据等方式，核查通信报文机密性保护机制是否有效。

b）若采用信道加密方式且数据链路采用非私有协议，使用工具进行数据抓包，解析通信报文数据，核查是否采用密码技术对通信报文进行机密性保护，并核查通信报文机密性保护机制是否有效。

c）若采用信源加密方式，查看信源机密性保护证明文件，通过构造数据等方式，核查通信报文机密性保护机制是否有效。

6.3.2　访问控制试验方法

6.3.2.1　访问控制机制试验方法

按照以下试验方法开展试验，判定数据链路是否满足 5.2.2 a）的要求：

a）若无人驾驶航空器仅支持接受 1 个控制数据终端的控制，准备 2 个同型号控制站（单元），授权其中 1 个控制站（单元）与无人驾驶航空器建立数据链路并赋予其控制权限，核查其通信正常且控制指令被正确响应。使用未授权的控制站（单元）向同一无人驾驶航空器发起数据链路建立请求，核查未授权的控制站（单元）发起的连接请求是否被拒绝。

b）若无人驾驶航空器支持同时接受 2 个及以上控制数据终端的控制，操作无人驾驶航空器同时与 2 个具备获取飞行控制权限能力的控制站（单元）建立数据链路；同时操作 2 个控制站（单元）向无人驾驶航空器发送不同的飞行控制指令，核查任一时间是否仅有 1 个控制站（单元）对无人驾驶航空器拥有飞行控制权限。

6.3.2.2　飞行控制权限转移试验方法

按照以下试验方法开展试验，判断数据链路是否满足 5.2.2 b）要求：

a）若无人驾驶航空器仅支持接受 1 个控制数据终端的控制，准备 2 个同型号控制站（单元），授权其中 1 个控制站（单元）与无人驾驶航空器建立数据链路并赋予其控制权限，触发对无人驾驶航空器的控制权限在不同控制站（单元）间发生转移，核查是否对获得飞行控制权限的控制站（单元）的身份真实性进行验证。

b）若无人驾驶航空器支持同时接受 2 个及以上控制数据终端的控制，操作

无人驾驶航空器同时与2个具备获取飞行控制权限能力的控制站（单元）建立数据链路，触发对无人驾驶航空器的控制权限在不同控制站（单元）间发生转移，核查是否对获得飞行控制权限的控制站（单元）的身份真实性进行验证。

6.4　下行链路和反向链路安全要求试验方法

按照以下试验方法开展试验，判断数据链路是否满足5.3要求：

a）若采用信道加密方式且数据链路采用私有协议，查看通信通道机密性保护证明文件，通过构造数据等方式，核查指挥和控制以及任务载荷数据机密性保护机制是否有效。

b）若采用信道加密方式且数据链路采用非私有协议，使用工具进行数据抓包，解析指挥和控制以及任务载荷数据，核查是否采用密码技术进行机密性保护且保护机制是否有效。

c）若采用信源加密方式，查看信源机密性保护证明文件，通过构造数据等方式，核查指挥和控制以及任务载荷数据机密性保护机制是否有效。

6、标准的实施

本文件第7章规定，在本文件实施之日前出厂或者进口的产品，可在本文件实施之日起一年内销售。该规定按照不溯及既往、合理过渡和减少资源浪费的原则，为企业有序消化既有库存、稳定市场供应预留时间，避免对已出厂、已进口产品造成不必要的资源浪费；自本文件实施之日起，新生产、新进口的产品以及过渡期届满后继续销售的产品，均应符合本文件要求。

为落实《无人驾驶航空器飞行管理暂行条例》《民用无人驾驶航空器生产管理若干规定》等相关要求，切实维护国家安全和公共利益，在有关主管部门的指导下，编制组广泛调研民用无人驾驶航空器生产企业、科研院所和检测机构，编制组成员分工合作，积极开展技术可行性分析与技术条款符合性验证工作，确保了标准的可落地、可实施。

（三）修订前后技术内容的对比[仅适用于国家标准修订项目]

不涉及。

三、与有关法律、行政法规和其他强制性标准的关系

习近平总书记在中共中央政治局第十六次集体学习时指出“要做好国家空中

交通管理工作，促进低空经济健康发展。”

一是《中共中央关于制定国民经济和社会发展第十五个五年规划的建议》的要求。该文件第十三章（推进国家安全体系和能力现代化，建设更高水平平安中国）提出“加强网络、数据、人工智能、生物、生态、核、太空、深海、极地、低空等新兴领域国家安全能力建设。”

二是《2025 年国务院政府工作报告》的要求。该报告第三章（2025 年政府工作任务）提出“开展新技术新产品新场景大规模应用示范行动，推动商业航天、低空经济、深海科技等新兴产业安全健康发展。”

三是国务院、中央军委《无人驾驶航空器飞行管理暂行条例》（国令第 761 号）的要求。该条例第八条提出：“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，并采取有效措施减少大气污染物和噪声排放。”该条例第二十三条提出：“空中交通管理机构和民用航空、公安、工业和信息化等部门、单位按照职责分工采集无人驾驶航空器生产、登记、使用的有关信息，依托无人驾驶航空器一体化综合监管服务平台共享，并采取相应措施保障信息安全。”

四是工业和信息化部《民用无人驾驶航空器生产管理若干规定》（工业和信息化部令第 66 号）的要求。该规定第十条提出：“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。”

五是中国民用航空局《民用无人驾驶航空器运行安全管理规则》（民航规章 CCAR-92）的要求。该规则第 92.679 条提出“指挥和控制链路（C2 链路）(a)民用无人驾驶航空器指挥和控制链路（C2 链路）应当符合与运行相适合的通信业务处理时间、连续性、可用性和完好性要求。”

六是与 GB 42590-2023《民用无人驾驶航空器系统安全要求》强制性国家标准的相关要求一致。该标准“4.11 数据链保护”提出“轻型和小型无人驾驶航空器应采用信息安全技术手段进行防护，防止链路非授权访问。”

四、与国际标准化组织、其他国家或者地区有关法律法规和标准的比对分析

1、有关国际标准化组织的相关标准情况、主要内容

美国标准协会（ANSI）和加拿大标准委员会（CAN）2018 年 9 月发布标准《ANSI/CAN/UL 3030-2018 安全无人机系统标准（第一版）》要求“应评估无人驾驶航空器系统通信的有效性或飞行期间无人驾驶航空器系统通信丢失的影响。”

ISO/IEC 22460-2:2024《ISO 无人机执照和无人机安全模组-第 2 部分:无人机安全模组》提出“本文件规定了无人机/无人机系统（UAS）安全模块的加密功能要求。该安全模块作为专用安全设备，用于安全存储与承载无人机/UAS 飞行员执照、操作员执照及其他相关身份凭证，同时提供可选数据的存储空间。其加密功能主要包括完整性验证、身份认证与数据加密，以确保存储信息与传输过程的安全可靠。”

ITU-T Y.4421-2021《使用 IMT-2020 网络的无人机和无人机控制器的功能架构》要求“7.3 安全能力要求 IMT-2020 的安全能力（包括用户数据传输加密与完整性保护）可在网络层及以下的协议栈中被复用。”“9 安全考虑 IMT-2020 网络的安全能力（包括用户数据传输加密与完整性保护）可在网络层及以下协议栈复用，并可支持应用层、服务层等更高层次的安全要求。”

IEEE P1937.16《民用无人驾驶航空器系统网络安全框架标准》草案“拟规定民用无人机系统（UAS）的参考网络安全框架，包括空域安全、设备安全、通信和网络安全、数据安全、隐私保护和运营管理安全。”

标准制定过程参考了上述标准。

2、有关国家或地区技术法规情况、主要内容。

欧盟委员会 2018/1139 号条例《关于民航领域的共同规则和建立欧盟航空安全机构》要求“考虑到航空安全不同领域之间以及航空安全、网络安全和其他航空监管技术领域之间的相互依存关系。”2019/945 号条例《关于无人驾驶航空器系统和无人驾驶航空器系统非成员国运营者》要求“无人驾驶航空器在数据链路丢失的情况下，有可靠和可预测的方法让 UA 恢复数据链路或终止飞行，以减少对空中或地面第三方的影响；C2 级（重量在 900 克-4 千克）和 C3 级（重量在 4 千克-25 千克）无人驾驶航空器数据链路配备安全措施，防止未经授权访问指挥和控制功能。”2019/947 号条例《关于无人驾驶航空器运行规则和程序》要求

“根据联盟法律进行公共安保或隐私和个人数据保护，要求无人驾驶航空器的运行满足特定的条件”。

美国国土安全部网络安全和基础设施安全局跨部门安全委员会2020年发布《防范无人机系统的威胁》要求“为保护个人信息或环境安全、国家安全、隐私，应对无人机进行安全认证，并建立和维护注册系统管理无人机运营商。”美国联邦航空管理局2022年发布的《无人机系统（UAS）安全》要求“支持无人机系统安全可靠地集成到美国国家空域系统（NAS）。”

五、重大分歧意见的处理过程、处理意见及其依据

本标准制定过程中无重大分歧。

六、对强制性国家标准自发布日期至实施日期之间的过渡期（以下简称过渡期）的建议及理由

建议本文件批准发布后12个月实施。考虑到产品升级涉及复杂技术和较高成本，对既有库存产品不再做溯及要求。

本文件自实施之日起，无人机产品的设计、生产、销售、使用维护、检验检测和管理的政府部门、企业、检测机构等单位需严格参照使用本标准。

七、与实施强制性国家标准有关的政策措施

本标准的实施监督管理部门是国家市场监督管理总局、工业和信息化部、民用航空局。强制性国家标准《民用无人驾驶航空器数据链路网络安全要求》发布实施后，由行业大规模开展新的国家标准宣贯工作，让产品生产企业、经销商企业和广大消费者了解和掌握新的国家标准，鼓励和支持企业进行产品结构调整升级，提高产品竞争力；由各地市场监督管理部门实施监督管理，对违反执行国家标准《民用无人驾驶航空器数据链路网络安全要求》的行为，可以依据《中华人民共和国标准化法》第二十五条、第三十六条、第三十七条进行处置。

八、是否需要对外通报的建议及理由

建议对外通报。

本文件未采用国际标准，且对世界贸易组织（WTO）其他成员的民用无人机贸易有重大影响，因此建议对外通报。

九、废止现行有关标准的建议

不涉及。

十、涉及专利的有关说明

在标准制修订过程中广泛征求意见，未发现涉及专利问题。

十一、强制性国家标准所涉及的产品、过程或者服务目录

本文件涉及的产品包括：民用微型、轻型、小型、中型和大型无人驾驶航空器。

十二、其他应当予以说明的事项

无。

标准编制组

2026 年 10 月 15 日