ICS 35.030
CCS L 80

中华人民共和国国家标准

GB XXXXX—XXXX

民用无人驾驶航空器数据链路网络安全要求

Cybersecurity requirements for data links of civil unmanned aircraft

（报批稿）

XXXX—XX—XX 发布　　XXXX—XX—XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 II
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 概述 2
5 安全要求 2
5.1 通用安全 2
5.2 上行链路和前向链路安全 3
5.3 下行链路和反向链路安全 4
6 试验方法 4
6.1 试验样机 4
6.2 通用安全要求试验方法 4
6.3 上行链路和前向链路安全要求试验方法 7
6.4 下行链路和反向链路安全要求试验方法 8
7 标准的实施 8
附录 A （资料性）民用无人驾驶航空器数据链路框架 9

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。

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专利的责任。

本文件由中华人民共和国工业和信息化部和中国民用航空局联合提出并归口。

民用无人驾驶航空器数据链路网络安全要求

1 范围

本文件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，描述了相应的试验方法。

本文件适用于民用无人驾驶航空器数据链路的设计、开发、制造与测试。本文件不适用于模型航空器与自备动力系统的飞行玩具，以及运行识别通信链路。

注 1：模型航空器也称航空模型，是指有尺寸和重量限制，不能载人，不具有自动的高度保持和位置保持飞行功能的无人驾驶航空器，包括自由飞、线控、直接目视视距内人工不间断遥控、借助第一视角人工不间断遥控的模型航空器等。模型航空器的技术规格为：总升力面积不超过 500dm^2，最大起飞重量不超过 25kg（含燃料、动力电池），活塞发动机气缸工作容积不超过 250cm^3，电动机电源空载电压不超过 72V，喷气发动机推力不超过 250N。

注 2：飞行玩具是最大飞行真高不超过 30m，最大起飞重量小于 0.25kg，最大飞行水平距离不超过 100m，最大飞行速度不超过 18km/h，且无线电发射设备符合微功率短距离技术要求，不搭载拍摄和测控设备，全程靠人工操作进行飞行的遥控玩具。

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 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

3 术语和定义

GB 42590—2023、GB 46750—2025、GB/T 25069—2022、GB/T 38152—2019界定的以及下列术语和定义适用于本文件。

3.1

数据链路 data link

用于无人驾驶航空器遥控、遥测和任务载荷信息传输的数据终端和数据通信协议与规程所建立的数据通信链路。

注：数据终端主要包括机载数据终端、中继数据终端、控制数据终端，数据通信协议与规程包括传输通道、通信协议、消息格式。

[来源：GB/T 38152—2019，8.1.1，有修改]

3.2

上行链路　uplink

从无人驾驶航空器控制信息输入到无人驾驶航空器控制信息输出之间的数据传输链路。

[来源：GB/T 38152—2019，8.1.9]

3.3

前向链路　forward link

从控制数据终端到中继数据终端、再从中继数据终端到机载数据终端的链路。

[来源：GB/T 38152—2019，8.1.11，有修改]

3.4

下行链路　downlink

从无人驾驶航空器遥测信息和任务载荷数据输入到无人驾驶航空器遥测信息和任务载荷数据输出之间的数据传输链路。

[来源：GB/T 38152—2019，8.1.10]

3.5

反向链路　reverse link

从机载数据终端到中继数据终端、再从中继数据终端到控制数据终端的链路。

[来源：GB/T 38152—2019，8.1.12，有修改]

3.6

私有协议　private protocol

专用的、非通用的协议。

[来源：GB 40050—2021，3.6]

4　概述

民用无人驾驶航空器数据链路包括上行链路、前向链路、下行链路、反向链路（见附录A）。基于数据链路的通信方向和网络安全特性，本文件中微型、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以下三类：

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

——上行链路和前向链路安全，包括加密传输、访问控制；

——下行链路和反向链路安全，包括加密传输。

中型和大型无人驾驶航空器相关要求另见适航审定相关标准。

5　安全要求

5.1　通用安全

5.1.1　通信实体鉴别

通信实体鉴别安全要求如下：

a）控制站（单元）、无人驾驶航空器和中继平台（如有）应具备通信实体鉴别功能；

b）链路建立或重连时，应验证通信实体身份真实性。

5.1.2 数据防伪造篡改

应具备验证传输数据完整性和来源真实性的功能。

5.1.3 链路状态感知与恢复

链路状态感知与恢复安全要求如下：

a）应具备感知数据链路连通、中断等状态的功能；

b）应具备链路异常（中断、丢失、阻塞等）状态下的自恢复功能。

5.1.4 抗重放攻击

应具备识别并拒绝执行或丢弃重放数据包的功能。

5.1.5 安全更新

安全更新安全要求如下：

a）应具备数据链路相关软件、固件或配置文件的安全更新功能，更新后数据链路应可用；

b）应具备验证更新数据完整性和来源真实性的功能。

5.1.6 日志记录

数据链路日志记录安全要求如下：

a）应记录数据链路时间信息、源标识及目的标识、安全事件（包括但不限于实体鉴别、链路建立、链路断开、链路更新）等信息；

b）应存储在非易失性存储区域中；

c）应具备数据完整性保护功能，防止数据链路日志被篡改和非授权删除；

d）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；

注：飞行架次是指完成一次从起飞或发射到着陆或回收的完整飞行过程，作为飞行活动统计的基本计量单位，仅地面滑行、未离地或未完成起飞的不计入飞行架次。

e）若采用网络存储方式，数据链路日志的安全事件信息应留存不少于 6 个月。

5.1.7 密码及密钥安全

数据链路密码及密钥要求如下：

a）密码算法、协议及密码模块（如有）应符合密码相关标准；

b）应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，对存储在数据终端中的密钥进行保护。

5.2 上行链路和前向链路安全

5.2.1 加密传输

应具备保护传输数据机密性的加密功能。

5.2.2 访问控制

访问控制安全要求如下：

a）任一时间应仅有1个控制站（单元）具有无人驾驶航空器的飞行控制权限；

b）应具备防止飞行控制权限转移时未授权控制站（单元）接入的功能。

5.3 下行链路和反向链路安全

应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。

6 试验方法

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。

7　标准的实施

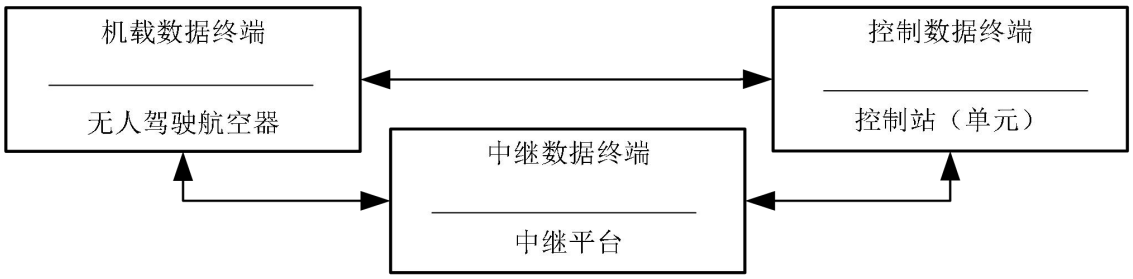
在本文件实施之日前出厂或者进口的产品，可在本文件实施之日起一年内销售。

附 录 A

（资料性）

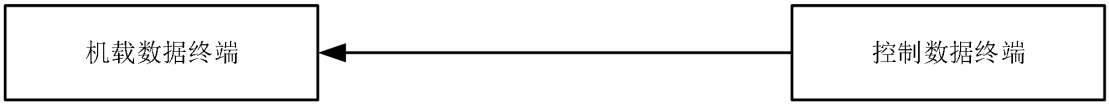
民用无人驾驶航空器数据链路框架

机载数据终端、中继数据终端与控制数据终端，是分别部署于无人驾驶航空器、中继平台与控制站（单元）用于实现数据链路通信的功能模块，如图A.1。



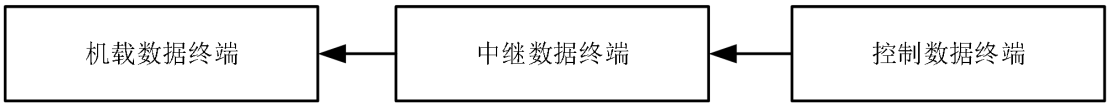
图A.1 数据终端示意图

上行链路示意图见图A.2。



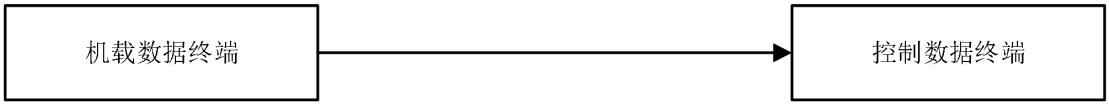
图A.2 上行链路示意图

前向链路示意图见图A.3。



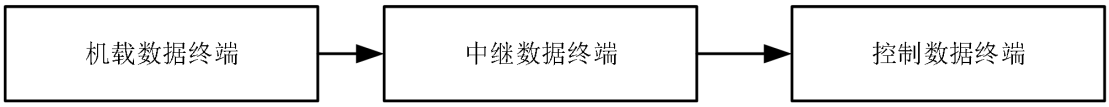
图A.3 前向链路示意图

下行链路示意图见图A.4。



图A.4 下行链路示意图

反向链路示意图见图A.5。



图A.5 反向链路示意图