ICS ×××
CCS ×××

T/GDEIIA

团　体　标　准

T/GDEIIA ××—20××

无人机信息安全测试规范

UAV information security test specifications

（征求意见稿）

20XX–XX–XX 发布　　20XX–XX–XX 实施

广东省电子信息行业协会　　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。

本文件由工业和信息化部电子第五研究所提出。

本文件由广东省电子信息行业协会归口。

本文件起草单位：工业和信息化部电子第五研究所、广州大学、北京亚邦恒泰科技有限公司、中山大学。

本文件主要起草人：×××、×××、×××。

本文件为首次发布。

无人机信息安全测试规范

1 范围

本标准规定了无人机安全测试各阶段（阅读手册、硬件功能验证、硬件安全测试、固件测试、系统测试和测试报告）的流程、要求以及证实方法。

本文件适用于无人机安全测评人员、无人机生产厂家等开展的无人机安全测试活动。

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 32927-2016 《信息安全技术 移动智能终端安全技术要求及测试评价方法》

GB/T 36951-2018 《信息安全技术 物联网感知终端应用安全技术要求》

GB/T 37024-2018 《信息安全技术 物联网感知层网关安全技术要求》

GB/T 37025-2018 《信息安全技术 物联网数据传输安全技术要求》

GB/T 37044-2018 《信息安全技术 物联网安全参考模型及通用要求》

GB/T 37093-2018 《信息安全技术 物联网感知层接入通信网的安全要求》

GB/T 38152-2019 《无人驾驶航空器系统术语》

GB/T 41300-2022 《民用无人机唯一产品识别码》

YD/B 173-2017 《物联网终端嵌入式操作系统安全技术要求》

YD/T 2407-2013 《移动智能终端安全能力技术要求》

3 术语和定义

3.1 物联网 Internet of Things

根据GB/T 33745-2025《物联网 术语》中描述，物联网即基于感知控制设备，通过通信网络，使物理实体、人、系统和信息资源相连接，响应和处理物理和虚拟世界信息的基础设施。

3.2 无人机

本规范中，无人机特指中小型消费级无人机、自组装无人机和模块化定制无人机。

4 无人机安全测试流程

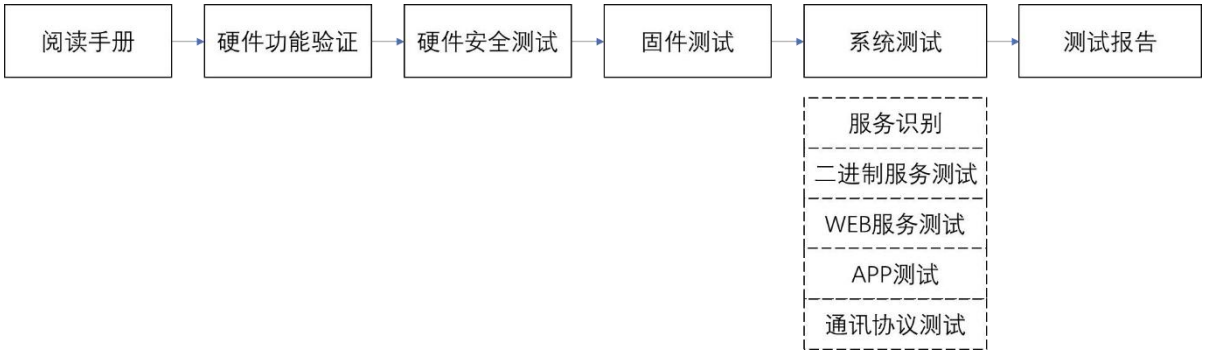

图1 无人机安全测试流程

无人机安全测试如图1包含以下阶段：

阅读手册：通过阅读厂商给出的无人机手册，了解无人机的相关参数、任务功能、通讯方式以及控制方式等。

硬件功能验证：安装无人机系统并进行试飞，保证无人机硬件功能均能够正常运行。

硬件安全测试：硬件功能正常后，硬件进行安全测试过程中，需要保证测试人员的人身安全以及无人机硬件功能的正常。

固件测试：针对无人机固件进行安全测试。

系统测试：针对无人机系统进行安全测试，此部分测试内容涉及服务识别、二进制服务测试、WEB 服务测试、APP 测试以及通讯协议测试。

测试报告：编写无人机安全测试报告，保证规范性、真实性、公正性。

无人机安全测试规范中的各个阶段的行为要求见第5章。

5 无人机安全测试要求

5.1 阅读手册

在无人机安全测试过程中，对阅读手册需要细心、认真，完成对如下内容的掌握：

a) 无人机软硬件参数。

b) 无人机的通讯方式，例如包括但不限于 WIFI、4G、GPS 等。

c) 无人机的控制方式，例如包括但不限于遥控器、手机、地面站等。

d) 无人机的任务功能，例如包括但不限于图传、表演等。

5.2 硬件功能验证

无人机各项功能正常时进行无人机安全测试的前提条件，无人机硬件功能验证包括如下内容：

a) 硬件功能验证需要合法的无人空旷区域进行，包括但不限于实验场所。

b) 无人机上电正常。

c) 无人机与控制设备连接正常。

d) 无人机通讯功能正常。

e) 无人机定位功能正常。

f) 无人机飞行控制功能正常。

g） 无人机载荷任务功能正常。

5.3 硬件安全测试

在进行硬件安全测试的过程中，需要遵守如下行为规范：

a） 拆除无人机螺旋桨，避免测试过程中无人机启动导致的人员伤害。
b） 无人机及其附属设备使用原厂充电器进行充电，充满电后及时移除充电器。
c） 拆解无人机的过程中，需要细心观察，小心拆解，避免结构物理损坏。
d） 观察无人机及附属设备电路板，拆解前先拍照，避免拆解后无法复原。
e） 寻找无人机的相关调试接口，接线测试的时候需要保证电压和电流安全，避免点击导致设备损坏。
f） 拆焊元器件时保证拆焊设备温度和焊接时间处于电路板和元器件可以承受的范围。
g） 焊接元器件后保证元器件管脚无虚焊和无连锡。
h） 元器件不宜频繁拆焊，避免元器件损坏和 PCB 掉点。
i） 拆焊的元器件需要归类存放。
j） 设备拆解操作台需要满足放静电要求，操作人员需要佩戴防静电环。
k） 设备拆解操作台不可存放影响设备拆解安全的任何物品。
l） 避免在强无线信号干扰的环境中进行硬件安全测试。

5.4 固件测试

固件安全测试过程中，应遵守如下行为规范：

a） 不允许使用非法手段进行固件获取，包括但不限于利用无人机厂商官网漏洞。
b） 无人机固件片级提取注意读写操作，避免误操作导致系统和数据丢失。
c） 无人机固件片级提取需要进行多次提取并比对，保证提取到的数据一致性。
d） 固件结构安全测试宜使用 linux 系统，包括但不限于 kali、parrot 等。
e） 安全测试过程中硬盘剩余空间不小于 80G。
f） 在使用打包固件命令时，打包的固件应该放在临时目录下。
g） 在获取到固件后要注意保密，不要随意上传到第三方固件分析平台。
h） 固件安全测试过程中尽量避免对固件以及数据的修改操作。
i） 固件安全测试过程需要对原始固件数据进行备份，必要时可以利用此备份数据进行系统恢复。

5.5 系统测试

5.5.1 服务识别

服务识别过程中，应遵守如下行为规范：

a） 在测试过程中，允许使用全端口扫描，但是严禁在无人机飞行时候进行扫描。
b） 使用的服务识别工具需要支持无人机常见的协议，如 MAVLink。
c） 使用扫描器应该断开不必要的网络接口，防止扫描到非预期的 IP 目标。
d） 服务识别过程中应严格控制数据量，避免出现设备拒绝服务导致识别失败。
e） 使用商用固件分析自动化工具发现对外服务程序。

5.5.2 二进制服务测试

二进制程序包括系统中的驱动程序，二进制服务程序以及二进制用户程序，针对无人机的二进制服务测试包含以上三种程序的的测试，测试过程中应符合如下规范：

a) 测试人员需要了解 ARM、MIPS、x86、x64 等CPU 的汇编语言。
b) 测试人员需要具备 C 语言的阅读能力，能够准确的掌握模块/函数的功能。
c) 测试人员需要具备双机调试以及测试用例构建的能力。
d) 使用逆向工具对二进制程序进行逆向并进行静态分析，发现安全风险点，逆向工具包括但不限于 IDA Pro，JEB，Ghidra，dnSpy 等。
e) 使用商用固件分析自动化工具发现安全风险点。
f) 安全测试可以在虚拟化环境中进行，虚拟化环境包括但不限于 Qemu，qiling 框架等。
g) 安全用例测试验证需要在无人机实体设备中进行，保证真实有效。

5.5.3 WEB 服务测试

在测试无人机相关WEB服务应用过程中，应遵守如下规范：
a) 在测试过程中，应该获取无人机厂商的授权，严禁非授权测试。
b) 在测试过程中，实现非授权访问或用户权限越权，在完成非授权逻辑、越权逻辑验证时，不应再获取和留存用户信息和信息系统文件信息。
c) 不允许对线上相关业务进行大规模，大流量扫描，防止造成业务系统瘫痪。
d) 测试中如果需要对数据库操作，应该只对本人的数据进行操作，不允许修改其他用户测正常数据。
e) 严禁对内网进行横向渗透，使用 SSRF 这类漏洞只有证明存在即可，不允许携带恶意PayLoad。
f) 在挖掘到数据库相关漏洞时候，严禁进行脱库，也不允许对数据的增删改。
g) 禁止执行可导致拒绝服务危害的技术验证测试。
h) 在挖掘命令注入这类 RCE 漏洞，只需证明漏洞存在即可，不允许利用漏洞获取主机上的敏感信息，也禁止利用该主机进行进一步渗透。

5.5.4 APP 测试

在分析IOS 以及安卓等移动平台上的应用时，测试过程中应符合如下规范：
a) 测试人员应该了解 IOS、安卓等移动平台相关安全技术，包括逆向工程、脱壳、漏洞分析等知识。
b) 专注于测试 APP 本身的安全性，除非获取授权，否则不能对APP 对应的云服务器发起渗透测试。
c) 通过反编译得到的源码或者敏感信息在测试完成后应该及时删除，防止泄露。
d) 在测试过程中应该使用真实的手机设备，不建议使用模拟器，保证漏洞的真实有效性。

5.5.5 通讯协议测试

在对无人机进行通信协议方面的测试过程中，应遵守如下规范：
a) 在测试过程中，采用无线电方式测试时，应不影响民用正常使用，如果需要全频段测试时，需远离闹市区从而避免影响民用生活。
b) 在测试过程中，采用无线电方式测试时，应不在重大会议及军事重要设施附近进行。
c) 在测试过程中，采用无线电方式测试时，应先探测频段后在进行测试，防止干扰其它正常通信。
d) 在测试过程中，采用通信协议模糊测试时，应将无人机的桨叶卸下测试，防止造成混乱飞行引发事故。
e) 在测试过程中，采用通信协议模糊测试时，应将配套零件固定，防止飞行掉落。
f) 在测试过程中，采用通信协议业务测试时，应远离闹市区测试，不要做快速灵敏操作，尽可能缓慢操作测试。

g） 在测试过程中，在降落功能相关测试时，应在软质地面进行，防止摔坏设备。
h） 在测试过程中，在起飞功能相关测试时，应在开阔地面测试。
i） 在测试过程中，应在满电量进行模糊测试，防止电量不足导致的测试不完全。
j） 在测试过程中，对于漏洞验证应在开阔少人地面测试，同时做好防护。
k） 在测试过程中，图传通信协议测试时，应与飞控测试分开进行。
l） 在测试过程中，飞控漏洞应单个功能测试，防止多功能导致飞行状态紊乱。

5.6 测试报告

有关测试报告的处置规范如下：
a） 在测试报告编写时，应客观、真实地对安全问题进行描述。
b） 无人机安全测试报告流转需要满足密级要求。

6 证实方法

在无人机安全测试过程中，相关个人或组织应确定漏洞管理活动是否符合第 5 章的要求，并应随着无人机安全测试阶段的推进及时进行更新。

参 考 文 献

[1] GB/T 38152-2019 无人驾驶航空器系统术语
[2] GB/T 41300-2022 民用无人机唯一产品识别码