ICS 33.020
CCS M 14

团　　体　　标　　准

T/　　XXXXX—XXXX

跨域无人装备协同通信安全接入规范

Specification for communication security access of cross domain unmanned equipment collaboration

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

广东省质量检验协会　　发 布

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。

本文件由珠海云洲智能科技股份有限公司提出。

本文件由广东省质量检验协会归口。

本文件起草单位：

本文件主要起草人：

跨域无人装备协同通信安全接入规范

1 范围

本文件规定了跨域无人装备协同通信的连接框架、基本要求、通信连接安全。
本文件适用于跨域无人装备多成员协同作业。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

本文件没有需要界定的术语和定义。

4 通信连接框架

4.1 通信连接框架主要包括无人装备控制中心、通信网关、无线路由、无人装备终端、无线网络。
4.2 跨域无人装备无线连接示意图见图 1。
4.3 跨域无人装备有线连接示意图见图 2。

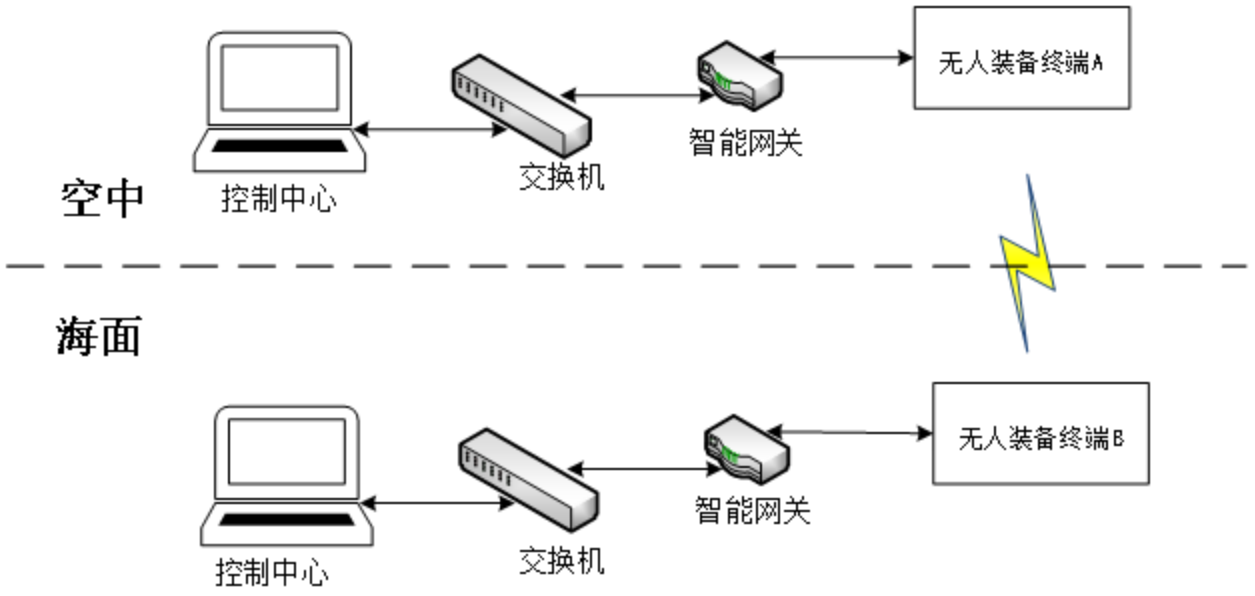

图1 跨域无人装备无线连接示意图

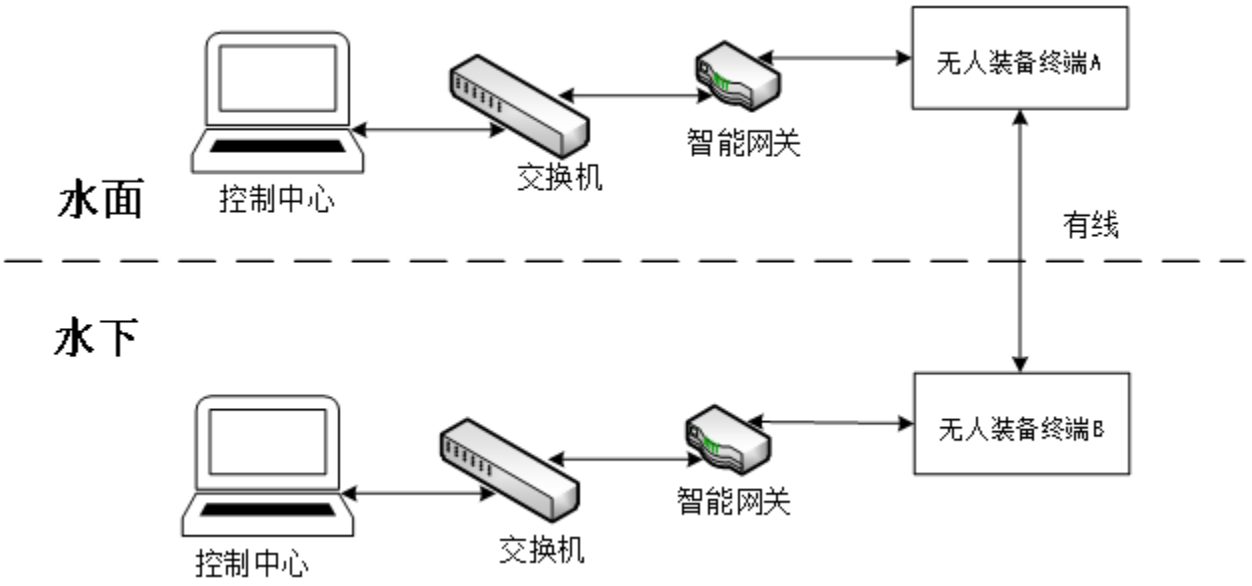

图2 跨域无人装备有线连接示意图

4.4 处于不同介质的无人装备终端 A 和无人装备终端 B，可通过有线或者无线连接的方式进行协同通信，交互信息通过无人装备终端、智能网关、交换机到达无人装备控制中心，实现跨域协同通信。

5 基本要求

无人装备终端应按国家规定使用无线电频段，并具有电磁兼容和抗电磁干扰能力。

6 通信连接安全

6.1 网络接入认证

无人装备终端在接入网络中具有唯一的网络身份标识，并可以对所连接的通信节点设备进行身份验证，至少支持以下身份鉴别机制之一：

a) 基于网络身份标识的鉴别；
b) 基于 MAC 地址的鉴别；
c) 基于通信协议的鉴别；
d) 基于通信端口的鉴别；
e) 基于秘钥机制的鉴别。

6.2 网络访问控制

无人装备终端应设置网络访问控制策略，限制对另一终端的网络访问。终端的网络访问控制功能要求如下：

a) 默认状态下应仅开启必要的服务和对应端口,应明示所有默认开启的服务、对应的端口及用途；
b) 应能关闭默认开启的服务和对应的端口；
c) 非默认开放的端口和服务,应在用户知晓同意后才可启用；
d) 可设置为默认状态下拒绝所有外部主机/网络对本主机的网络访问；
e) 应能基于应用程序的白名单,对本主机访问外部网络进行访问控制；

f） 应能基于 IP 地址、端口号进行网络访问控制；
g） 应能基于源 IP 地址、目的 IP 地址、目的端口号、协议进行网络访问控制。

6.3 网络防护

禁止无人装备终端与网络之间进行全局路由协议交互，只能与网关进行点对点数据交互。在未授权外部移动设备接入时应能告警,并生成审计日志。

6.4 数据加密传输

应至少采用一种对称密码算法（如 SM4、ZUC等） 和数字信封分发对称密钥的方式的检验技术和密码技术保证重要数据在传输和存储过程中的保密性，如对传输身份鉴别信息、隐私数据和重要业务数据等敏感信息进行加密保护。加密算法应符合国家密码相关规定。

6.5 数据传输完整性校验

6.5.1 应采用杂凑密码算法（如 SM3） 和数字签名算法（如 SM2） 的检验技术和密码技术保证重要数据在传输和存储过程中的完整性， 包括鉴别数据、 重要业务数据、 重要配置数据等。
6.5.2 应具有并启用通信完整性校验机制，如:采用校验码、消息摘要、数字签名等，实现鉴别信息、隐私数据、数字签名和重要业务数据等数据传输的完整性保护。
6.5.3 应具有通信延时和中断的处理机制。

6.6 外围接口安全

外围接口分为有线外围接口和无线外围接口，有线外围接口包括USB接口、SD、RJ45接口等，无线外围接口包括无线专网空口、公网空口、蓝牙接口、WLAN接口和NFC接口等，以外围接口接入时应满足以下要求：

a） 应具备开关，可关闭/开启相应的外围接口；
b） 当应用软件调用开启外围接口时，终端应给用户相应提示，当用户确认后连接方可开启；
c） 应禁用终端闲置的外部设备接口；
d） 应禁用终端的外接存储设备自启动功能；
e） 已建立无线连接，应在相应的输出设备上有明确的连接状态显示；
f） 只在某种特定状态下接受外来通信连接请求，并对连接设备进行认证授权操作。非该状态时，仅允许已通过认证授权的设备连接。

6.7 抗数据重放

应能够采用时间戳或缓存队列等方式鉴别数据的新鲜性， 避免历史数据的重放攻击， 应能够鉴别历史数据的非法修改，避免数据的修改重放攻击。