附件 1

ICS 35.240.99

A90

T/GXTB

广 西 中 小 企 业 联 合 会 标 准

T/GXSME xxx—xxx

基于 5G 技术的虚拟仿真警务训练平台传输链路技术

Technical standard for transmission link of virtual simulated police training platform based on 5G Technology

（征求意见稿）

xxxx-xx-xx 发布　　xxxx-xx-xx 实施

广西中小企业联合会　　发 布

目　次

前言

本标准依据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。

本标准由广西警察学院提出。

本标准起草单位：广西警察学院大数据应用研究中心　广西北部湾国际港务集团有限公司　广西博文教育科技有限公司　广西中小企业联合会

本标准主要起草人：侯文雷 吴海斌　罗春华　何娇

基于5G技术的虚拟仿真警务训练平台传输链路技术标准

1 范围

本标准介绍了基于5G技术的虚拟仿真警务训练平台传输链路类型及其承载网络，规定了5G技术传输链路的建设标准。

本标准适用于基于5G技术的虚拟仿真警务训练平台的建设、以及虚拟现实头戴式显示设备安全接入。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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。

YD/T 4011-2022 5G网络管理技术要求 总体要求

GB/T 38259-2019 信息技术 虚拟现实头戴式显示设备通用规范

3 术语和定义、缩略语

3.1 术语和定义

GB/T 36639、GB/T 37935、GB/T 38638及下列术语和定义适用于本文件。

3.1.1

传输链路 transmission link

公网、共网、专网等承载网络提供的系统接入的无线传输链路。

3.1.2

警务训练平台 Police training system

由MIS（多人交互系统）操作平台及射击训练实训场景内容，构建实战化训练场景、实战化训练科目、实战化训练体验的系统。

[GA/T 1561-2019，定义3.1.1]

3.1.3

虚拟现实头戴式显示设备 wear -type virtual reality equipment

利用仿真技术与计算机图形学人机接口技术多媒体技术传感技术网络技术等实现人机交互的终端设备。

3.1.4

5G技术 5th Generation Mobile Communication Technology

第五代移动通信技术。是具有高速率、低时延和大连接特点的新一代宽带移动通信技术。

3.2 缩略语

下列缩略语适用于本文件。

B-TrunC：宽带集群通信（Broadband Trunking Communication）

3GPP：第三代伙伴计划（Third Generation Partnership Project）

SIM：订阅者身份模块（Subscriber Identity Module）

IDS：入侵检测系统（Intrusion Detection System）

SNMP：简单网络管理协议（Simple Network Management Protocol）

BGP：边界网关协议（Border Gateway Protocol）

4 基于 5G 技术的虚拟仿真警务训练平台传输链路承载网络

虚拟现实头戴式显示设备通过无线专用传输链路接入警务训练局域网，无线专用传输链路的承载网络主要分为四类：公网、专网、共网和其它网络。

5 基于 5G 技术的虚拟仿真警务训练平台传输链路建设规范性要求

5.1 公网链路

a) 公网无线专用传输链路建设应结合运营商网络架构进行。建设 5G 专线/专网时应考虑进行 UPF 专属或下沉。

b) 公网无线专用传输链路建设应考虑向下兼容性原则，建设 5G 专线/专网时，必须考虑兼容 4G、3G 等用户的接入。

c) 公网无线专用传输链路应实现端到端逻辑隔离和物理隔离，宜通过切片技术确保警务训练人员的优先接入和调度，重点区域需要通过带宽资源预留或独立频谱等技术确保警务训练的高可用性。

5.2 专网链路

a) 设备频率使用应符合工信部发布的无线电管理规范，终端设备需要根据相关要求过检，并取得型号核准证。

b) 对于安全性较高的场景，警务训练局域网应采用完全自主可控的技术建设，其它场景也可以在标准 IEEE 802.11 WLAN 网络的基础上叠加可控的安全防护措施和控制机制进行建设。

c) 宽带专网建设应符合 LTE 宽带集群（B-TrunC）标准要求。

5.3 共网链路

a) 政府共网建设需要符合 LTE 宽带集群（B-TrunC）标准要求。

b) 运营商共网建设需要符合 LTE 宽带集群（B-TrunC）标准进行建设，采用 5G 建设共网时，不同行业用户之间可通过智能切片技术进行隔离。

5.4 其它网络链路

a) 微波设备频率使用应符合工信部发布的无线电管理规范，且只能用于点对点链路，应急场景下作为有线链路的替代。

6 基于 5G 技术的虚拟仿真警务训练平台传输链路安全接入要求

移动警务无线链路接入要求分为链路接入控制要求、安全防护要求和网络接入控制要求。

6.1 链路接入控制要求

6.1.1 公网链路

a) 应基于 SIM 卡等标识、通过 RADIUS、TACAS 等认证技术对专线/专网用户进入平台的权限进行控制。

b) 采用 5G 专线/专网链路时，应能够对专线/专网用户使用的联网通道进行管理和监测，如用户数、用户状态、终端位置、切片签约信息、上下行速率、丢包率等。

c) 采用 5G 专线/专网链路时，应提供部分通信服务接口，便于与管控系统和网络接入控制设备进行联动，更有效地进行无线通信管控。

d) 终端 IP 地址应规划为动态 IP，建议由运营商进行规划，并在 LNS 路由器上进行路由发布，避免采用默认路由的方式进行路由发布。

6.1.2 专网链路

a) 应基于 IP 地址、MAC 地址等标识对终端进入平台的权限进行控制。

b) 应支持基于协议白名单进行过滤，仅允许 SIP、RTP、HTTP 等协议通过。

6.1.3 共网链路

a) 应基于 SIM 卡等标识、通过 RADIUS、TACAS 等认证技术对专线/专网用户进入平台的权限进行控制。

b) 采用 5G 技术建设的共网，需要符合 6.1.1 b)、c)、d)要求。

6.1.4 其它网络链路

目前的两种其它网络链路指的是 ka 波段卫星链路和微波链路，这两种网络链路的链路接入控制满足 6.1.2 要求。

6.2 安全防护要求

a) 应具备威胁检测的能力。采集流量、日志、元数据等信息，通过防病毒、IDS、威胁情报、关联分析等技术进行建模分析，识别网络攻击和恶意代码。

b) 应对接入控制区内所有网元设备进行日志记录，并可通过 SSH 等协议实现安全的运维管理。

c) 防火墙默认安全策略应全部禁止，仅以白名单的形式对特定 IP、端口、协议等特征的流量进行放行。

d) 威胁检测设备应支持与防火墙设备联动，根据分析结果对流量进行阻断或放行。

6.3 网络接入控制要求

a) 应基于数字证书、生物特征等标识、采用安全性强的认证技术完成虚拟现实头戴式显示设备接入控制，禁止只采用安全性较弱的密码口令等方式进行接入控制。

b) 应采用两种以上异构的认证技术完成设备入网认证，应支持根据认证结果对虚拟现实头戴式显示设备进行接入控制。

c) 应支持基于黑名单对虚拟现实头戴式显示设备进行接入控制，黑名单策略生成来源包括但不限于威胁情报、政策合规性要求、日志分析和流量分析的结果。

d) 应支持基于终端环境持续监测结果对虚拟现实头戴式显示设备进行接入控制，监测项包括但不限于互联网联网监测、终端密码模块的状态、证书状态、安全监控组件状态、操作系统版本、安全监控组件版本。

e) 应支持基于终端或用户身份进行最小权限的授权控制，禁止默认为终端或用户开放平台所有业务系统的访问权限。