中数国科 5G 终端安全接入网关

产品白皮书

（中数国科集团）

【中数国科】

■ 文档编号	■ 密　级
■ 版本编号	■ 日　期

■ 撰 写 人	■ 批 准 人
■	■ @2025 中数国科

■ 版权声明

目录

一、引言

在数字化浪潮加速推进的今天，企业及工业用户对网络安全的需求日益迫切。移动互联网和无线网络的广泛应用，虽然为业务开展带来了高效与便捷，但也伴随着数据泄露、非法接入等安全风险。如何确保终端设备的安全接入与数据传输的机密性、完整性，成为各行各业亟待解决的关键问题。

为此，我们推出终端安全接入网关——一款基于4/5G移动网络的高性能安全终端设备。该产品创新性地融合密码技术与网络通信技术，为用户提供入网身份认证、安全组网、传输数据加密等核心功能，并支持串口设备的远程安全接入与管理，全面满足企事业及工业场景的安全需求。

终端安全接入网关支持IPSec VPN、SSL VPN等多种安全接入协议，并集成SM2、SM3、SM4等国密算法，构建起符合国家密码管理体系的安全链路。无论是远程办公、工业物联网，还是跨区域数据传输，均可通过该产品建立高效、可靠的安全通道，确保数据在传输过程中的机密性与完整性，为用户打造坚不可摧的网络安全防线。

在网络安全威胁日益复杂的背景下，终端安全接入网关以技术创新为驱动，以用户需求为核心，助力企业实现安全、高效的数字化转型升级。

二、产品概述

2.1.产品简介

终端安全接入网关是基于4/5G通信网络的高性能终端设备，创新应用密码技术与网络通信技术融合，为企事业、工业用户提供入网身份认证、安全组网、传输数据加密等高性能安全服务。终端安全接入网关支持IPSec VPN、SSL VPN安全接入协议，支持SM2、

SM3、SM4 等多种国密算法，通过与安全接入网关的连接可实现基于国密体系的安全链路充分保证数据的安全性。

产品遵循国家密码管理局颁发的《GM/T 0022 IPSec VPN 技术规范》、《GM/T 0023 IPSec VPN 产品规范》、《GM/T 0024 SSL VPN 技术规范》和《GM/T 0025 SSL VPN 产品规范》，支持 SM2、SM3、SM4 国密算法；利用基于 SM2 算法的数字证书技术实现数据的传输加密和身份认证。

终端安全接入网关为行业客户提供高防护、高可靠性能力。主要面向的行业有交通行业，如港口、机场、高速公路；能源行业，如变电/配电站；制造业，如工厂、矿山及测绘行业、消防行业等。

终端安全接入网关针对电力配电网领域，产品内嵌国网电力专用密码 SE 安全芯片，自主研发针对配电自动化终端通信的加密模块，支持数据标准化封装解析、通信服务控制管理、双向身份认证、数据加密保护、终端证书管理等功能。终端安全接入网关在电力行业有着更广阔是应用。

2.2.标准规程

GM/T 0002《SM4 分组密码算法》

GM/T 0003《SM2 椭圆曲线公钥密码算法》

GM/T 0004《SM3 密码杂凑算法》

GM/T 0005《随机性检测规范》

GM/T 0009《SM2 密码算法使用规范》

GM/T 0010《SM2 密码算法加密签名消息语法规范》

GM/T 0015《基于 SM2 密码算法的数字证书格式规范》

GM/T 0018《密码设备应用接口规范》

GM/T 0022 《IPSec VPN 技术规范》

GM/T 0023 《IPSec VPN 网关产品规范》

GM/T 0024 《SSL VPN 技术规范》

GM/T 0025 《SSL VPN 网关产品规范》

GM/T 0034 《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》

GA/T686-2007 《信息安全技术 虚拟专用网安全技术要求》

三、典型应用场景

终端安全接入网关以其轻量便携、接口丰富、组网灵活、智能融合等特点，广泛应用于为移动设备、智能设备、工业设备、监控设备提供稳定、安全的网络通信服务，主要面向的行业有智慧城市建设：如智能监控、智慧停车场、户外宣传；交通行业：如港口、机场、高速公路；能源行业：如变电/配电站、智能电网、光伏新能源；制造业：如工厂、矿山及测绘行业、消防行业等。

3.1.物联网领域

针对物联网领域下的典型应用场景示例如图 3.1。

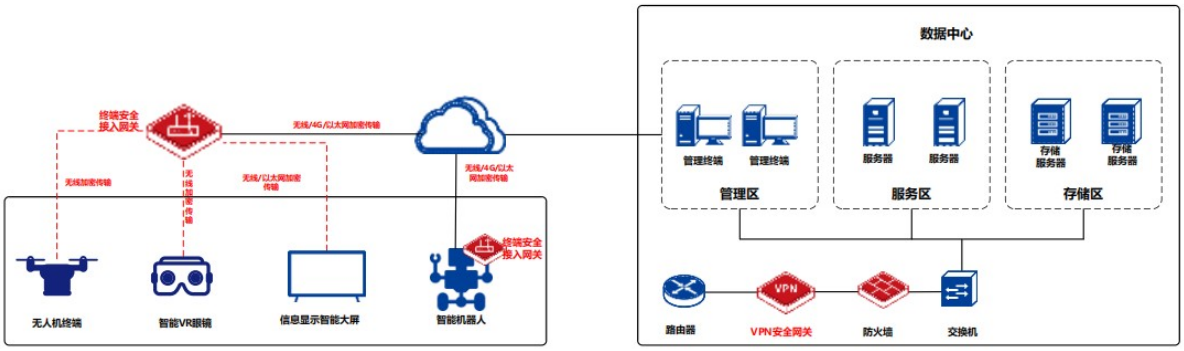

图 3.1 物联网领域典型应用场景示例

场景痛点：物联网设备接入存在安全问题，容易成为攻击者新目标入侵企业内部或物联网平台，数据容易被窃取和篡改。如高价值无人机设备容易成为攻击者目标，需实时监控飞行状态与数据传输。公共场所智能显示设备易被利用展示恶意内容或收集敏感信息。VR 设备用户数据与控制指令需保护，防止被窃取或篡改。自主导航与操作指令需安全保障，防止被远程控制或欺骗。

解决方案：在物联网设备接入终端安全接入网关，终端安全接入网关提供国密 VPN 接入服务，实现身份可信、数据安全、行为可控的物联网设备安全接入管理。可对物联网设备进行防护，为无人机提供数据加密与身份验证，为智能显示设备显示数据传输内容加密与访问控制，为 VR 设备用户数据加密与签名验签,为自主导航与操作指令加密与行为安全监控,可解决物联网设备存在的安全隐患问题。终端安全接入网关对访问控制，检测威胁，防止恶意设备入侵或数据窃取，可广泛应用于电力、能源、油田、管网、光伏、水利、交通、环保、广播站台、无人机等领域。

3.2.工业领域

针对工业领域下的典型应用场景示例如图 3.2。

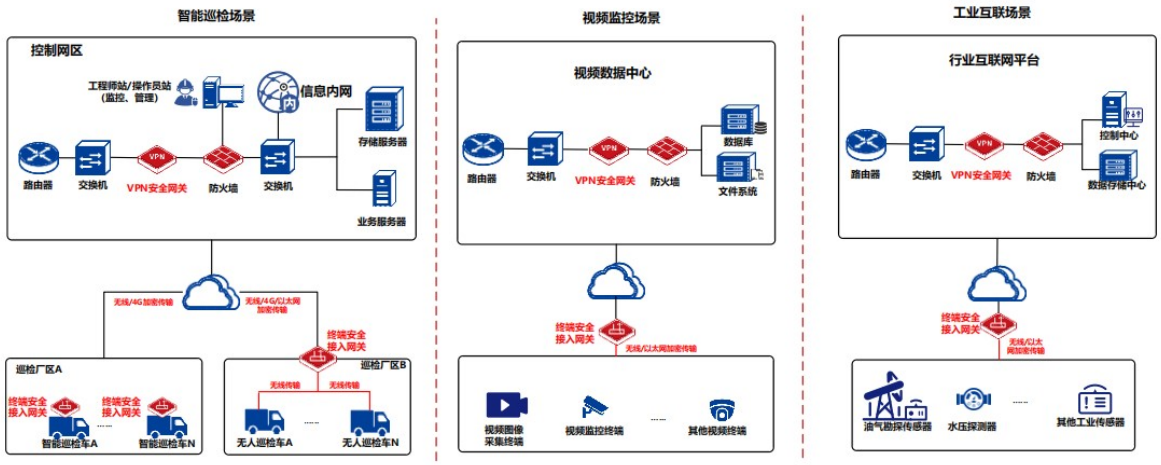

图 3.2 工业领域典型应用场景示例

场景痛点：工业设备（如智能巡检车、视频监控、工业传感器、工控设备）等　　终

端与数据中心进行数据交互，实时传输生产数据和控制指令过程中需要生产数据实时传输与监控，数据加密与完整性保护。

解决方案：在工业设备终端侧部署终端安全接入网关，通过运营商网络实现安全组网通过与内置 VPN 模块交互，实现与控制网的连接、数据加密传输及身份认证，保障设备身份可信及控制网接入安全。终端安全接入网关为工业传感器、控制器等关键设备提供安全接入与数据保护，确保电网监控、工业生产等关键业务的安全可靠运行，可广泛应用于智能变电站、工业控制系统、远程监控系统等场景中。

四、主要功能

中数国科 5G 终端安全接入网关功能列表		
功能	**细分项**	**说明**
移动网络	网络状态信息展示	丰富的移动网络连接状态信息展示。
	双 SIM 卡	支持双 SIM 卡切换。
	网络制式	支持 TD-LTE/FDD-LTE 制式和 NSA（非独立组网）和 SA（独立组网）组网。
	全网通	支持中国移动、中国电信、中国联通和中国广电，全网通的 3G/4G/5G 移动网络。
网络接入	网络接入方式	支持静态 IP、动态 IP、PPPoE、PPTP 等多种方式入网。
	NAT 地址转换	支持 NAT 地址转换和端口映射功能。
	网络诊断工具	为便于运维管理，提供完善的网络诊断工具 ping、traceroute、nslookup 等。
身份认证	算法支持	支持 SM2、SM3、SM4 国密算法。
	双证书支持	支持签名证书和加密证书的双证书认证体系。
网络防护	集成防火墙	基于包过滤的防火墙功能，支持网络访问控制，防止

		外部网络用户对 VPN 的攻击。
	防重放攻击	避免因中间人攻击，网络传输的数据包被非法用户修改后重放，接收方能识别并丢弃被非法篡改的数据包。
	攻击防御	实时防御 Synflood、Icmpflood、Udp Flood、Ping of death、Icmp-Smurf、Tcp-Land、Icmp-Unreachable、ARP Flood 等多种泛洪攻击。
工业协议	支持多种工业协议	Modbus RTU, MQTT
串口服务	串口服务	支持透明传输模式和 Modbus TCP 互转 Modbus RTU 模式，便于串口设备接入网络。
传输加密	IPSec VPN	支持基于国密算法和国密协议的 IPSec VPN。
	SSL VPN	支持基于国密算法和国密协议的 SSL VPN。
	链路加密	支持基于国密算法的净载荷链路加密。
	纵向加密	采用专用电力安全芯片，支持配电网系统中配网终端和主站的纵向加密传输功能。
系统监控	网络监控	支持指定时间端对网络宽带进行设备宽带流量监控显示，支持当前系统实时系统负载、流量、用户连接数等信息进行详细统计。
	SNMP 远程监控	支持 SNMP 远程监控，支持 V1/V2c/V3 版本，可设置共同体并可限制访问源。
统一监管	监测代理	支持设备统一监管检测系统实时状态及信息上报，服务端可查看最系统当前状态及上报信息。
	管理代理	支持设备统一监管远程管理获取设备信息状态，远程监控、版本升级、密钥更新下发。
系统管理	日志管理	支持系统日志、业务日志级、操作日志查看、导出以及日志外发功能。
	NTP 时间同步	支持本地时间和互联网时间校准。

	恢复出厂设置	系统具有恢复默认设置功能，方便使用。
	系统备份与修复	在系统正常工作时，可以备份设备的配置和管理信息。在系统故障后或用户有需求的情况下，可将配置和管理信息恢复。此功能可减少用户的管理开销。系统支持 Web 方式的固件升级。
	网络诊断工具	为便于运维管理，提供完善的网络诊断工具 ping、traceroute、nslookup 等。
	运维终端	支持页面运维终端，便于终端登录设备运维管理。
	串口管理	提供串口管理来远程控制电子设备，监控电子设备的环境。
高可用性	故障检测	设备开机过程中进行关键部件的安全自检以及设备运行过程中的周期性安全自检。
	无人值守	支持网络监测，实现设备外网接入长期不掉线。

五、产品规格

产品型号		**ST1000**		
整体说明		4G 终端安全接入网关	5G 终端安全接入网关	三防终端安全网关
性能参数		低端	中低端	中低端
VPN 性能	加解密吞吐率	20Mbps	50Mbps	50Mbps
	加解密时延	小于 1ms	小于 1ms	小于 1ms
硬件配置	主频	580MHz	1GHz	1GHz
	内存	DDR2 128MB	DDR2 512MB	DDR2 512MB
	硬盘	Flash 32MB	eMMC 8GB	eMMC 8GB

接口配置	管理网口	百兆	千兆	千兆
	业务网口	百兆	千兆	千兆
	串口	RS232*1、RS485*1	RS232*1、RS485*1	RS232*1、RS485*1
	USB接口	1个USB2.0	无	无
	移动网路	4G通信模组	5G通信模组	无
	SIM卡槽	1个	2个	无
安全配置	复位初始化	支持	支持	支持
	开盖销毁	支持	不支持	不支持
	手动销毁	支持	支持	支持
显示配置	指示灯	1个电源灯，1个报警灯，1个系统灯，3个工作灯，4个信号灯	1个电源灯，1个报警灯，1个系统灯，5个工作灯，4个信号灯	1个电源灯，1个报警灯，1个系统灯，1个工作灯
	蜂鸣器	支持	支持	支持
	RTC时钟	支持	支持	支持
电源	插电自启	支持	支持	支持
	是否冗余	支持	支持	支持
	整机功耗	<8W	<13W	<85W
	额定工作电压	端子宽压DC7V-35V	冗余宽压，DC9V-48V	宽压，DC9V-24V
机箱	尺寸(长x宽x高(mm))	110×94×29（不含无线及天线座）	146.0×122.0×41.0（不含电源端子，无线及天线座）	210.0×210.0×55.0（不含航插8芯接头、航插16芯接头）
	净重	0.26g	0.85Kg	2.75Kg
工作环境	工作温度	-20~75℃	-40~70℃	-50℃~80℃
	工作相对湿度	5%~95%RH	5%~95%RH	5%~95%RH

	大气压力	86～106KPa	86～106KPa	86～106KPa

六、特点优势

6.1.安全合规

6.1.1.标准规范

综合网关符合《GM/T 0024 SSL VPN 技术规范》、《GM/T 0025 SSL VPN 网关产品规范》、《GM/T 0022 IPSec VPN 技术规范》、《GM/T 0023 IPSec VPN 网关产品规范》《GM/T 0028 密码模块安全技术要求安全二级》，全面符合国家密码管理法规，确保产品的安全性与合规性，满足政府、金融、能源等关键行业需求。

6.1.2.物理防护

终端安全接入网关外壳等级 IP30 防护，三防版本外壳等级 IP67，可做到防低温、高温、震动、抗击等物理防护特点。紧急情况下支持手动立即销毁密钥等密码资源，支持物理防护体系，保障密码设备硬件与数据安全。

6.1.3.身份认证

通过硬件级加密通道构建零信任运维体系：采用基于智能密码身份鉴别，确保远程运维场景中管理员身份真实性及管理指令传输安全，有效防御中间人攻击与数据窃取，满足等保 2.0 三级远程管控要求。

采用基于密码算法融合用户名口令的挑战强身份认证方式，从根本上解决弱口令爆破

风险，提升认证强度。

6.1.4.密钥安全

构建多层级密钥防护体系：支持用户自主定义设备业务工作密钥及会话密钥的更换周期，确保密钥全生命周期的动态安全。支持密钥备份恢复，保障密钥全生命周期安全。

6.1.5.网络防护

综合网关集成防火墙功能，实时阻断 Synflood、Icmpflood、Udp Flood、Ping of death、Icmp-Smurf、Tcp-Land、Icmp-Unreachable、ARP Flood、Udp-Teardrop 等多种攻击，保障业务连续性。

6.1.6.日志安全

采用国密 SM2 算法对管理员操作日志实施数字签名，确保日志完整性、操作不可抵赖性及司法取证有效性，符合《网络安全法》审计留存要求。

6.2.智能融合

6.2.1.国密 VPN 终端

终端安全接入网关智能融合国密 VPN 终端功能：支持 IPSecVPN、 SSLVPN 等多种 VPN 协议，实现安全远程接入，保障数据传输安全。

6.2.2.链路加密终端

终端安全接入网关智能融合链路加密终端功能：支持国密算法的净载荷加密，提供端

到端数据加密保护，确保通信安全。

6.2.3.5G CPE 终端

终端安全接入网关智能融合 5G CPE 终端功能：支持 4/5G 全网通移动网络，提供高速稳定的移动网路连接能力。

6.2.4.工业路由器

终端安全接入网关智能融合工业路由器功能：支持宽温运行、满足 IP30 防护等级，支持 4/5G 全网通，兼容电力 101/104 规约、工业 Modbus RTU 等协议。

6.2.5.配网加密终端

终端安全接入网关智能融合配网加密终端功能：支持国密算法，支持非对称加密认证主站指令，对称加密隧道保障实时数据安全传输适配电力标准通信规约（如 IEC 101/104）。

6.2.6.串口服务器

终端安全接入网关智能融合串口服务器功能：支持工业串口通信，实现串口设备的远程安全接入与管理。

6.3.组网灵活

6.3.1.接口丰富

终端安全接入网关接口丰富，包含一个 WAN(千兆)、一个 LAN(千兆)、一个工业串

RS232、一个RS485工业串口、两个支持5G安装的SIM卡槽，支持静态IP、动态IP、PPPoE、 PPTP等多种接入方式。

6.3.2.轻巧便捷

终端安全接入网关采用轻量化设计，支持导轨、挂壁及桌面多种安装方式，即插即用快速部署，让安全接入更灵活高效。

6.3.3.网络适应

终端安全接入网关具备卓越的网络适应性，支持移动/无线/有线/串口多模接入，提供二层安全组网与GOOSE防护，智能NAT穿越与地址转换，桥接模式零改造部署，轻松应对各类复杂网络环境。

6.4.稳定可靠

6.4.1.强环境适应性

终端安全接入网关备对环境适应能力强，可在恶劣条件下稳定运行，工作温度可在-40C°~ 70°C、存储环境温度可在-40°C ~ 125°C、工作相对湿度可在5% ~ 95% RH范围内长期稳定运行，具有外壳IP30防护等级，三防版本可达IP67。防低温、防高温、防尘、防震、防冲击，可在恶劣环境下长期稳定运行。

6.4.2.物理级密钥防护

终端安全接入网关采用硬件加密芯片保护密钥安全，配备有电力配网专用加密芯片、国密认证安全SE加密芯片/随机数芯片、提供有硬件级密钥存储与保护、防篡改设计。

6.4.3.硬件看门狗

终端安全接入网关支持硬件看门狗。硬件看门狗可在异常情况自动复位与恢复，提高系统稳定性和可靠性，避免因系统卡死导致的业务中断。

6.4.4.无人值守

终端安全接入网关设备具备自动化运维能力。支持远程管理与运维自动化，设备状态实时监控与报警，配置备份与恢复功能，适应长期无人值守场景需求。