可定制的 5G+ 工业互联网安全能力

Customizable 5G + Industrial Internet Security Capabilities

王继刚 /WANG Jigang，王庆 /WANG Qing，滕志猛 /TENG Zhimeng
（中兴通讯股份有限公司，中国 深圳 518057）
(ZTE Corporation, Shenzhen 518057, China)

摘要： 5G+ 工业互联网安全以 5G 自身安全能力为基础，结合工业互联网的实际应用场景，参考网络安全等级保护相关指导，通过融合创新，将零信任、内生安全、微分段等前沿安全技术融入 5G 工业互联网场景安全方案中，以定制化的安全能力来满足工业互联网整体的安全防护需求。这些定制化的安全能力包括：差异化切片满足企业网络安全隔离需求，用户面功能（UPF）下沉 + 灵活以太网（FlexE）可靠地支持企业低时延业务需求，多重机制提供企业端到端数据安全保障，零信任架构增强企业自主控制接入安全策略，以及态势感知保障网络整体安全能力。

关键词： 5G；工业互联网；可定制安全能力；零信任网络；内生安全

Abstract: Based on the security capability of 5G network, 5G + industrial Internet security is deeply combined with the actual application scenarios of the industrial Internet. At the same time, it also complies with the relevant requirements of network security level protection. Zero trust networks, endogenous security, differential segment and other cutting-edge security technologies are integrated into the 5G industrial Internet scenario security scheme. Through customized security capabilities, security researchers can meet the overall security protection needs of the industrial Internet. These customized security capabilities include: The differential slicing meets the needs of enterprise network security isolation; the user port function (UPF) sinking + flexible Ethernet (FlexE) reliably supports the enterprise low latency business requirements; the multi-mechanism provides the enterprise end-to-end data security guarantee; the zero trust architecture enhances the enterprise independent control access security strategy, and the situation perception guarantees the network overall security ability.

Keywords: 5G; industrial Internet; customizable security capabilities; zero trust networks; endogenous security

DOI：10.12142/ZTETJ.202006005
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20201124.1844.005.html

网络出版日期：2020-11-25
收稿日期：2020-10-18

工业互联网是互联网和新一代信息技术与工业系统深度融合所形成的产业和应用生态，是工业智能化发展的关键信息基础设施。5G 将以其高带宽、低时延、海量连接等特性大幅提升工业互联网的信息化水平，逐步成为支撑工业生产的基础设施。同时，5G 网络提供的灵活定制、弹性部署、多层次隔离等智能网络能力与工业生产中既有的研发设计系统、生产控制系统及服务管理系统等相结合，可以全面推动工业系统的生产流程产生深刻变革。

5G 的引入，打破了工业互联网相对封闭、可信的制造环境：病毒、木马、高级持续性攻击等对工业生产的威胁日益加剧，一旦网络受到攻击，将会造成巨大的经济损失，并可能带来环境灾难和人员伤亡。在第 3 代合作伙伴计划（3GPP）标准中[1-3]，5G 网络的基础安全能力还不能完全契合不同业务场景下工业互联网对网络安全的要求。为此，需要在现有 5G 安全架构基础之上，结合工业互联网行业特征

与运营模式，构建 5G+ 工业互联网安全定制能力，从而满足企业安全技术体系对于 5G+ 工业互联网安全能力的要求。本文主要介绍 5 个方面的能力，即终端接入认证、网络切片隔离、高实时性业务保障、数据端到端安全、未知安全威胁防御。

1 差异化切片满足企业网络安全隔离需求

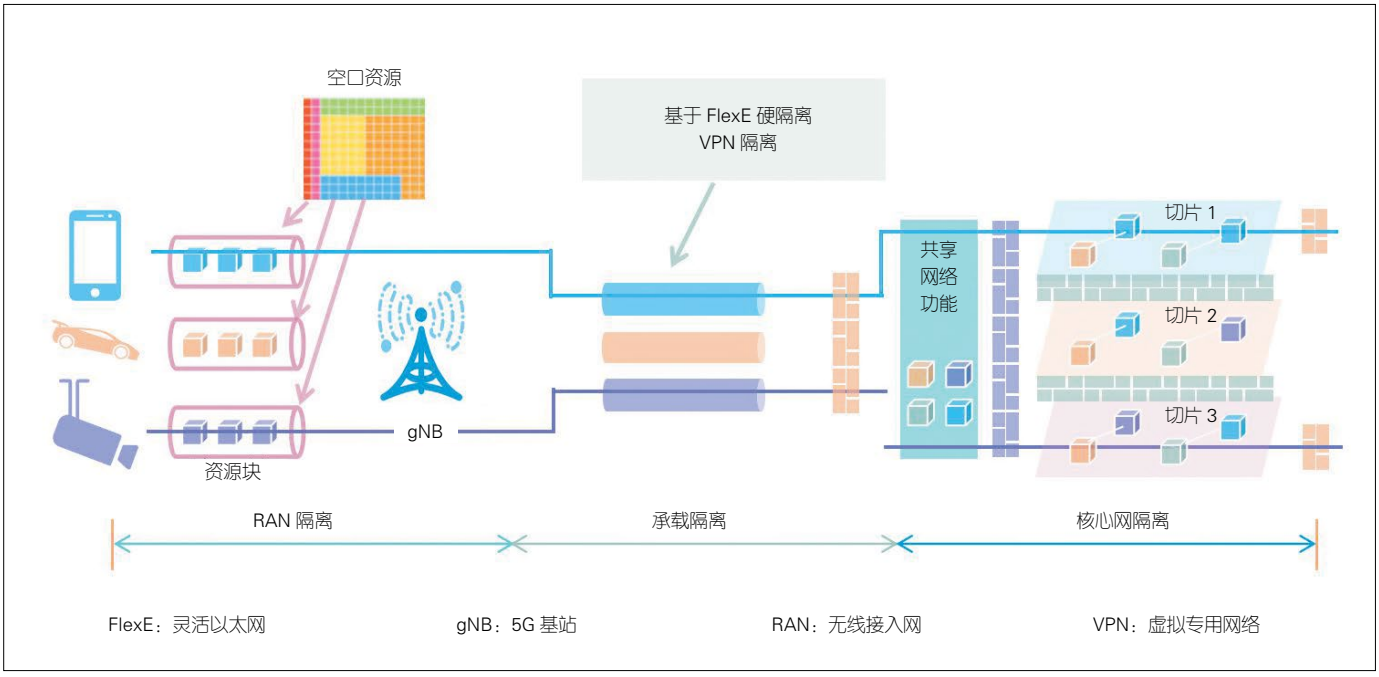
5G 网络切片是基于无线接入网、承载网与核心网基础设施，以及网络虚拟化技术构建的一个面向不同业务特征的逻辑网络。运营商可以为不同行业应用在共享的网络基础设施上，通过能力开放、智能调度等技术构建网络切片，提供差异化的网络服务。这对安全提出了新的挑战，带来了包括切片间非法访问、切片内不同安全域间的非法访问等多种安全威胁。

为了安全地支持各种差异化的业务场景，需要提供网络切片隔离（如图 1 所示），为不同业务提供差异化的安全服务。工业互联网切片隔离符合《网络安全等级保护 2.0》中对安全通信网络的要求，并通过一套参数配置，实现切片的资源隔离和业务质量保障。可以根据行业的安全隔离要求和需要保障的关键服务等级协议（SLA）选择不同类型的切片，并进行参数配置。从资源隔离和业务保障的角度，无线网络可以提供多种切片隔离技术。如表 1 所示，工业互联网切片隔离方案分为 4 类，分别对应等级保护中的 1—4 级，不同业务系统可以根据自身需求选择不同的网络隔离方案。

1.1 无线接入网（RAN）隔离

网络切片在 RAN 侧的隔离主要面向无线频谱资源以及基站处理资源。最高安全等级的工业控制类切片采用独立的基站或者频谱独享；其他类型切片则根据安全需求，通过物理资源承载（PRB）独享、数据资源承载（DRB）共享，以及 5G 服务质量特性（5QI）优先级调度等多种方式组合来实现。

（1）独立基站 / 频谱独享。部分



▲图 1 端到端网络切片隔离

▼表 1 工业互联网切片隔离方案

切片类别	隔离类别	RAN	TN	MEC	5GC
专用切片	完全独占	基站 / 频谱独享	FlexE 隔离	MEC/UPF 业务独享	CPF 全部独享
定制切片 1	部分共享	PRB 独享	VPN/VLAN 隔离	MEC/UPF 企业独享	CPF 部分独享
定制切片 2	部分共享	DRB 共享、5QI 优先级调度	VPN/VLAN 隔离、QoS 资源保障	MEC/UPF 企业独享	CPF 全部共享
普通切片	完全共享	DRB 共享	VPN/ VLAN 隔离	VLAN/ VxLAN 隔离	CPF 全部共享，UPF 独享

5GC：5G 核心网
5QI：5G 服务质量特性
CPF：控制面功能
DRB: 数据资源承载
FlexE：灵活以太网
MEC：移动边缘计算
PRB：物理资源承载
QoS：服务质量
RAN：无线接入网
TN：承载网
UPF：用户面功能
VLAN: 虚拟局域网
VPN: 虚拟专用网
VxLAN：虚拟扩展局域网

专网的应用（如工业控制类）或局部区域（如无人工厂、无人发电站、矿山等）的通信独立性和可控性要求很高，共享基站无法满足；因此，可以考虑采用独立基站的形式提供无线切片。另外，对于资源隔离和业务质量保障更高的应用，可以在运营商频谱资源中划分出一部分单独给该应用使用（如 5 MHz）。

（2）PRB 独享。在 5G 正交频分多址（OFDMA）系统中，无线频谱从时域、频域、空域维度被划分为不同的 PRB，用于承载终端和基站之间数据传输。对于一些要求资源隔离且对业务质量保障要求高的切片用户，可以为其配置一定比例的 PRB（如 5%）。此时，该小区 5% 的空口资源和带宽为该切片专用，不受其他用户影响。PRB 的正交性保证了切片的隔离性，PRB 专用也保证了业务质量的稳定性。

（3）DRB 共享。可以配置 DRB 接纳控制参数，以确保切片在该小区下能够接入的用户数不被其他业务抢占。DRB 接纳控制可以采用灵活的配置策略，既可以固定配置，也可以配置一个较小的比例，超过后还可以在资源池中抢占。

（4）5QI 优先级调度。对于不需要严格确保资源隔离和业务质量的切片，如视频监控类的增强移动宽带（eMBB）切片，可采用 5QI 优先级调度方式。该方式基于单一网络切片选择辅助信息（S-NSSAI）的不同优先级（可以依据切片业务需保障的程度进行配置）和业务，并能在一个调度周期内计算出不同业务的调度优先级。5QI 软切片的本质是基于调度，即以调度策略来实现业务质量，但当基站业务繁忙时并不能确保达到该目标。

1.2 承载网（TN）隔离

5G 网络依托数据中心部署，其跨越数据中心的物理通信链路需要承载多个切片的业务数据。网络切片在承载侧的隔离可通过软隔离、硬隔离和服务质量（QoS）资源保障等多种方案实现。

（1）虚拟专用网（VPN）/ 虚拟局域网（VLAN）隔离。软隔离方案基于现有网络机制，通过 VLAN 标签与网络切片标识的映射来实现。网络切片具备唯一的切片标识，能够根据切片标识为不同的切片数据映射封装不同的 VLAN 标签，再通过 VLAN 隔离实现承载隔离，从而保障 QoS。

（2）灵活以太网（FlexE）隔离。硬隔离方案引入了 FlexE 技术。FlexE 分片基于时隙调度，将一个物理以太网端口划分为多个以太网弹性管道（逻辑端口）。这使得承载网络既具备类似于时分复用（TDM）的隔离性好的特性，又具备以太网的网络效率高的特点。对于工业控制应用等对时延和安全保障较高的业务，可以在承载侧独占时隙，从而实现切片硬隔离。

1.3 核心网隔离

5G 核心网由多种不同的网络功能构成，有些网络功能为切片专用（工业控制），有些则在多个切片之间共享；因此，在核心网侧的隔离需要采用多重隔离机制。

（1）控制面功能（CPF）全部独享。核心网的所有控制面网元[4-5]，包括接入和移动管理功能（AMF）、统一数据管理功能（UDM）、鉴权服务功能（AUSF）、统一数据仓库功能（UDR）、策略控制功能（PCF）、会话管理功能（SMF），以及用户面网元功能（UPF）都需要新建。该模式适用于如工业控制、典型专网等对安全需求最高的应用场景。

（2）CPF 部分共享。核心网的部分控制面网元（包括 AUSF、UDR、PCF、SMF）需要新建，AMF 和 UDM 被多个切片共享。这种方式可根据容量、时延等要求，选择在核心机房或者边缘机房新建 UPF。对于希望数据隔离的大部分切片，或对部署位置有严格要求（比如工厂、园区）且有本地应用部署需求的切片用户，我们建议采用这种模式。

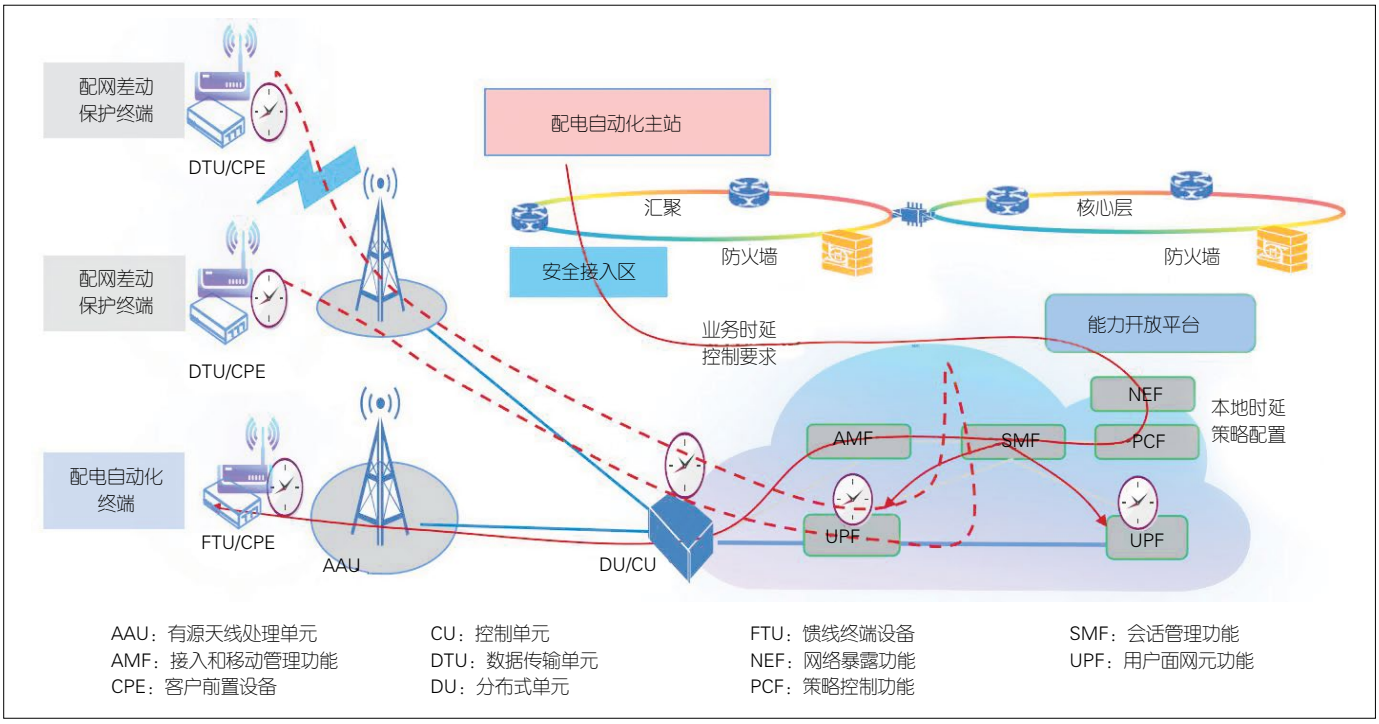
（3）CPF 全部共享，UPF 独享。核心网的控制面网元被多个切片共享，UPF 需要新建，切片通过 S-NSSAI 来区分，数据网络名称（DNN）也需要新建。该模式适用于管理信息网、视频监控等对于安全隔离有一定要求的业务场景。

2 UPF 下沉 +FlexE 可靠地支持企业低时延业务需求

智能车间内设备的互联，以及生产运营的数字化转型，使得工业系统对实时性、抗抖动性的无线网络需求变得迫切。传统无线网络无法满足该要求，而 5G 网络以其高带宽、低时延、大连接的特性获得工业生产系统的青睐[6-8]。

传统端到端移动通信，必须经过无线接入网、核心网、平台、应用层层处理，这导致端到端时延较长，无法满足对时延要求比较高的工业控制应用的要求。为了进一步降低端到端通信时延，可以将 5G 网络中 UPF 下沉到移动边缘计算（MEC）。图 2 中的架构就是将数据、应用、智能引入基站边缘侧，从而减少数据传输路由节点，降低端到端通信时延。

在网络传输方面，服务于工业控制的网络切片，对时延要求更高。传统分组设备对于客户业务报文采用的是逐跳转发策略，网络中每个节点设备都需要对数据包进行媒体接入控制（MAC）层和多协议标签交换（MPLS）层解析。这种解析耗费大量时间，单设备转发时延高达数十微秒。为此，



▲图 2 5G 工业应用延时保证

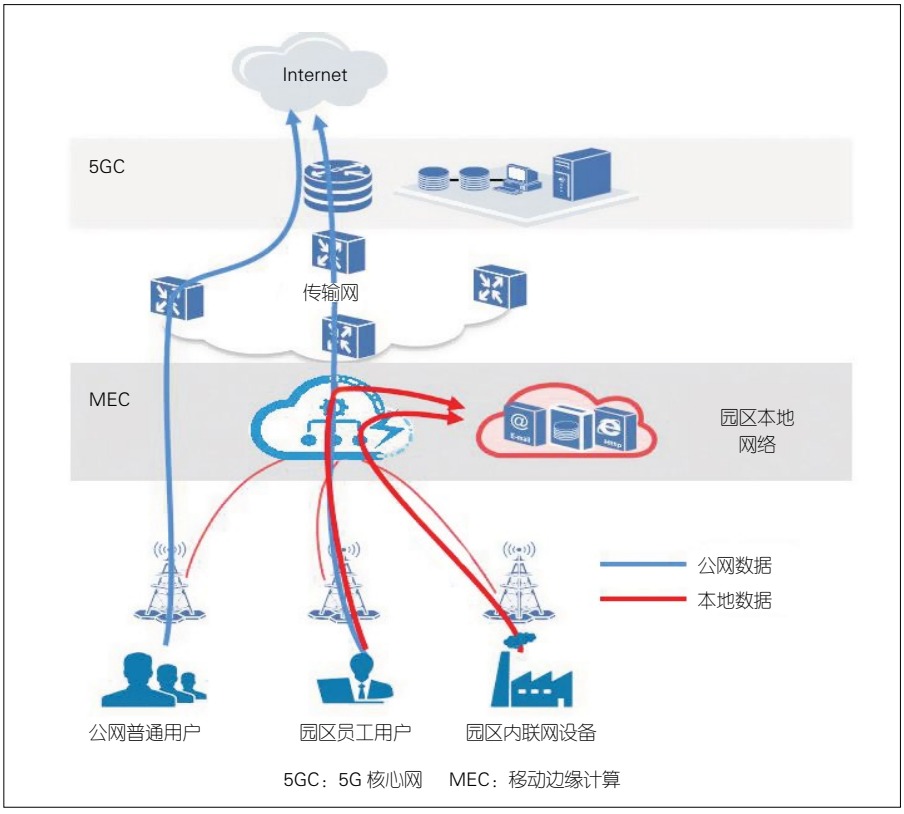
可以采用 FlexE 交叉技术，来实现网络设备之间的信息传递。这种方式可以实现基于物理层的用户业务流转发，用户报文在网络中间节点无须解析，业务流交叉过程近乎瞬间完成，实现单跳设备转发时延 1~10 μs，可有效解决时间报文的模拟、欺骗。

3 多重机制提供企业端到端数据安全保障

用户数据在传输过程中存在被窃听、篡改、泄露等安全威胁。为降低行业应用中数据安全风险，5G 提供了更强大的数据安全保护方法，如图 3 所示。

3.1 接入认证

在为高安全等级工业系统提供定制化服务过程中，5G 网络采用的是切片二次认证机制，即在用户接入网络并做了认证之后，为接入特定业务建立数据通道而进行的认证。在该认证过程中，使用了非运营商控制的信任



▲图 3 5G 工业园区数据安全

状要求，即用户通过接入认证后并不能直接与业务系统建立连接，而是利用业务相关的信任状与用户终端进行认证，并在认证通过的情况下才允许

5G 网络为用户建立与业务系统间的通信链路，从而保证企业对安全策略自主可控。

3.2 访问控制

访问控制遵循最小权限授权原则。系统为不同用户分配不同的数据操作权限。访问者未经授权不能访问用户信息，以防止非法访问、越权访问等手段获取用户的数据。

为避免不可靠来源用户的接入，系统提供选择多种访问控制方式。系统不允许时间、来源、登录方式等访问控制条件不满足的用户登录系统并建立会话。另外，关键敏感数据采用 SHA256、AES256 等加密算法进行加密存储。

3.3 数据传输安全

在机密性保护方面，5G 网络采用的高级加密标准（AES）、3GPP 流密码（SNOW 3G）、祖冲之密码（ZUC）等算法。这些算法采用 128 位密钥长度，被证明是安全的。

数据传输安全机制为工业互联网中的数据产生、处理、使用等环节提供了安全保护。首先，在数据产生和处理过程中，数据根据敏感度进行分类，建立不同安全域间的加密传输链路，并根据不同的安全级别采用差异化的数据安全技术。其次在数据使用过程中，数据管理者对使用者进行授权和验证，保证数据使用的目的和范围符合安全策略，并对重要业务数据的使用进行审计，最终为行业用户提供数据的机密性和完整性保护。

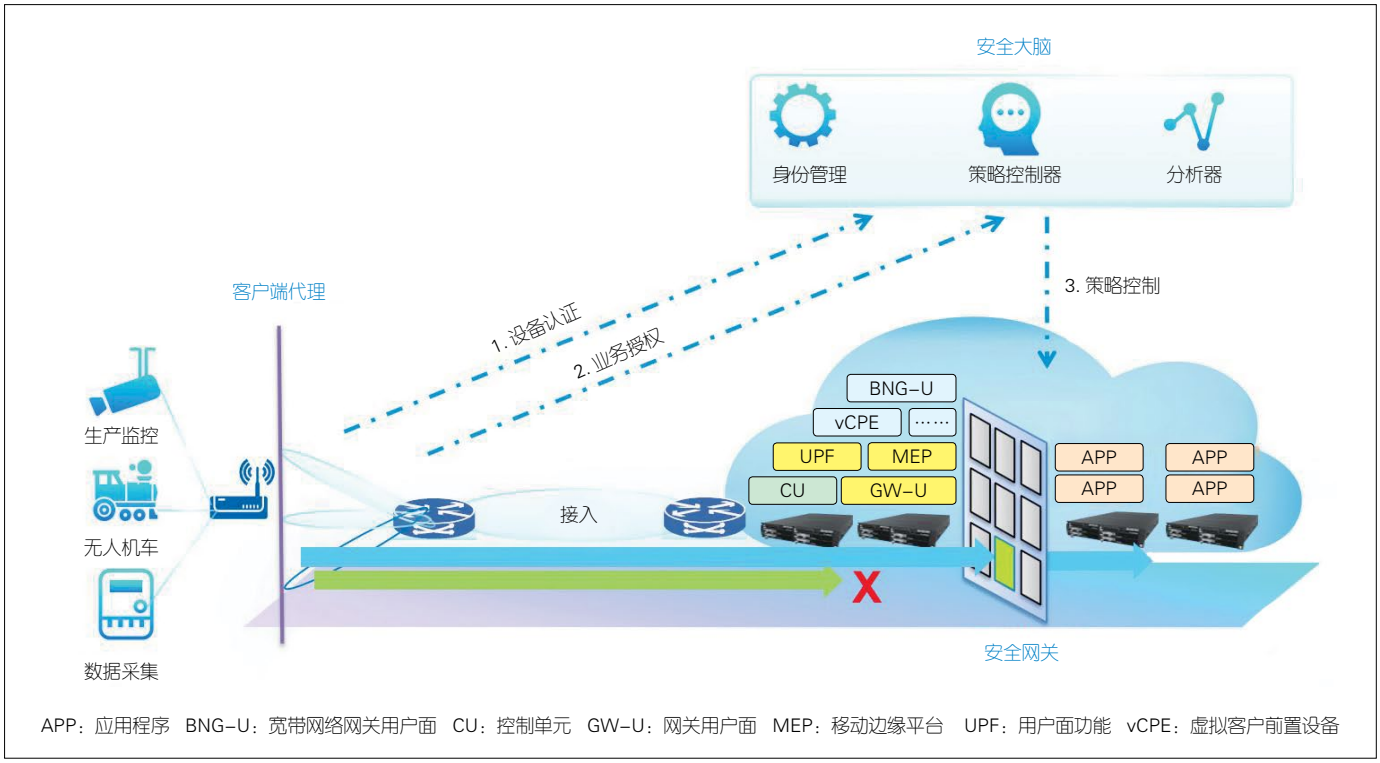
另外，采用基于会话的加密机制，需要按需配置加密算法与密钥强度。采用数据加密、完整性校验能够保证数据在空口、用户设备（UE）和 MEC 之间的安全传输。例如，建立互联网协议安全（IPSec）/ 安全套接字协议（SSL）VPN 隧道，可以预防数据被嗅探窃取、篡改等威胁，同时结合 UPF 分流技术及内部边界安全隔离，能够实现数据不出园区。

4 零信任架构增强企业自主控制接入安全策略

随着安全边界下沉，5G 网络架构中的身份验证凭据成为了新的核心安全边界。一旦 5G+ 工业互联网场景下海量的工业生产终端被入侵利用，将会产生非常严重的后果。

传统边界安全模型中的信任是来自网络地址的，即在网络边界验证终端身份，确定用户是否被信任。如果终端的 IP 地址可信，用户被认定为可信，并通过验证进入内网。随着攻击方式和威胁多样化，传统网络接入安全架构凸显出很大的局限性。为此，5G+ 工业互联网安全架构引入基于零信任安全理念，并启用新型身份验证管理模式，充分利用身份验证凭据、设备、网络、应用等多种资源的组合安全边界 [9]。

如图 4 所示，零信任安全系统包



APP：应用程序 BNG-U：宽带网络网关用户面 CU：控制单元 GW-U：网关用户面 MEP：移动边缘平台 UPF：用户面功能 vCPE：虚拟客户前置设备

▲图 4 基于 5G 的工业零信任安全系统

括控制器、可信网关、分析器 3 大组件。控制器作为安全控制面的核心组件，为可信网关提供自适应认证服务、动态访问控制和集中管理能力。控制器对所有的访问请求进行权限判定。权限判定不再基于简单的静态规则，而是基于身份库、权限库和信任库的上下文属性、信任等级和安全策略等。

分析器为控制器提供信任等级评估。分析器持续接收可信网关、控制器的日志信息，结合身份库、权限库数据，并基于大数据和人工智能技术，对身份进行持续画像，对访问行为进行持续分析，对信任进行持续评估，最终生成和维护信任库，为动态访问控制引擎提供决策依据。

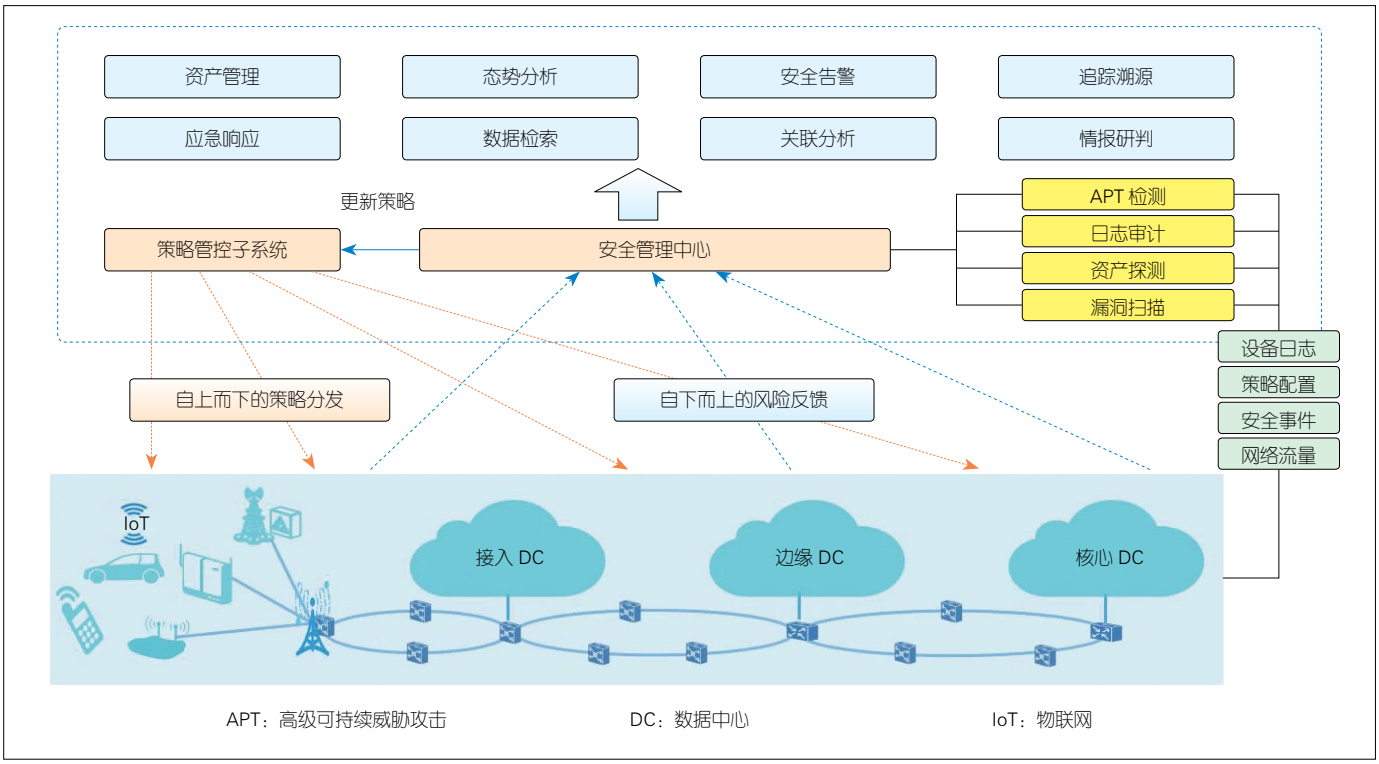
可信网关作为 5G 网络 MEC 用户面的网络控制节点，是确保业务安全访问的第一道关口，是动态访问控制能力的策略执行点。根据应用终端访问控制规则，可信网关拦截访问请求后，通过控制器对访问主体进行认证，对访问主体的权限进行动态判定。只有认证通过并且具有访问权限的访问请求才予以放行。

5G 工业互联网零信任安全架构下的终端安全接入不再以网络边界为限，这使得原来的被动防御向主动防御转变，边界防御向内生安全转变。

5 态势感知保障网络整体安全能力

5G 网络的应用，有力地推动了有线工业控制向无线接入工控自动化转型 [10-12]。云虚拟现实（VR）/ 增强现实（AR）技术的大量应用，工业可穿戴、远程操控的普及，使得传统工业系统势必与 5G 移动互联网产生大量信息和数据交互。这也给工业互联网行业安全防护提出了更高的挑战，原有的被动式防御已不可靠，无法有效防止有组织的规模性攻击。

首先，5G 工业互联网态势感知技术，可以覆盖 5G 资产（包括 5GC 网元、切片、虚机、物理机、中间件等），能先将各层级资产进行关联，然后根据关联关系来判断漏洞、脆弱性与攻击事件等威胁事件对业务的影响，并在大量的安全事件中寻找事件之间的因果关系。通过这样的方式，态势感知技术能够追踪攻击链定位威胁发生的源头，并分析可能的波及范围，根据资产价值及业务影响来确定处置方式与手段。其次，态势感知技术可以对网络攻击事件深度挖掘，结合网络的基础设施情况和运行状态，对网络安全态势做出评估，从而对未来可能遭受的网络攻击进行预测，并提供针对性的预防建议和措施。另外，在工业互联网业务与 5G 移动互联网交互的关键路径上，态势感知技术可以对网络中的流量和各种日志信息持续地收集分析，对网络异常流量（包括攻击流量特征、威胁文件传输等）进行解析，从而发现网络流量异常行为或者用户异常行为，以便主动对未知威胁提前干预。图 5 为 5G 安全态势感知架构。



▲图 5 5G 安全态势感知架构

6 结束语

在 5G 与工业互联网融合的过程中必然会出现安全问题，目前的 5G 工业互联网安全防护发展尚处起步阶段。随着 5G 融入工业互联网的广度和深度持续增强，有必要引入新的安全理念、安全技术，不断完善 5G 工业互联网安全防护体系，以支撑工业数字化转型升级行稳致远 [13–15]。

可定制的 5G+ 工业互联网安全能力，贴合工业互联网应用场景，通过引入主动式、智能化的威胁检测与安全防护技术，构建全面的预测、基础防护、响应和恢复能力，同时利用机器学习、深度学习等人工智能技术分析处理安全大数据，从而不断改善安全防御体系。可定制的 5G+ 工业互联网安全能力可以有力保障 5G 行业应用的安全，为后续更多的 5G 行业应用落地创造了安全的网络环境。

参考文献

[1] 3GPP. Security architecture and procedures for 5G system: 3GPP TS 33.501 [S]. 2019
[2] 3GPP. System architecture for the 5G system: 3GPP TS 23.501 [S]. 2019
[3] 杨红梅，赵勇 . 5G 安全风险分析及标准进展 [J]. 中兴通讯技术，2019, 25(4): 2–5.
[4] 3GPP. 5G security assurance specification (SCAS); access and mobility management function (AMF): 3GPP TS 33.512 [S]. 2018
[5] 3GPP. 5G security assurance specification (SCAS); user plane function (UPF): 3GPP TS 33.513 [S]. 2018
[6] 工业互联网园区网络白皮书 [R]. 工业互联网产业联盟，2020
[7] 工业互联网安全框架 [R]. 工业互联网产业联盟，2019
[8] 陆平，李建华，赵维铎 . 5G 在垂直行业中的应用 [J]. 中兴通讯技术，2019, 25(1): 67–74.
[9] Zero trust architecture: NIST, draft special publication (SP) 800–207 [R]. NIST 2019
[10] 许书彬，甘植旺 . 5G 安全技术研究现状及发展趋势 [J]. 无线电通信技术，2020, 46(2): 133–138.
[11] 5G 网络安全需求与架构白皮书 [R]. IMT–2020, 2017
[12] 5G–ENSURE_deliverable D2.7 security architecture (Final) [R]. 5GPPP, 2017
[13] 基于 SDN/NFV 的电信网安全技术白皮书 [R]. SDN/NFV 产业联盟，2018
[14] 5G security white paper: security makes 5G go further [R]. GSMA, 2019
[15] 5G 行业应用安全白皮书 [R]. 中兴通讯股份有限公司，2019

作 者 简 介

王继刚，中兴通讯股份有限公司网络安全与操作系统首席专家；主要研究领域为网络安全、操作系统、云计算；先后主持和参加基金项目 10 余项，获得多项科研成果奖；已发表论文 30 余篇，其中被 SCI/EI 检索 20 余篇。

王庆，中兴通讯股份有限公司网络安全规划部部长；主要研究领域为 5G 及垂直行业网络安全；已发表论文 20 余篇。

滕志猛，中兴通讯股份有限公司网络安全产品线总工；主要研究领域为网络安全；发表论文 30 余篇、国际标准组织提案 20 余篇。