工业 5G LAN 网络安全技术报告

工业互联网产业联盟
中国联通研究院
联通数字科技有限公司
2024 年 10 月

声　　明

本报告所载的材料和信息，包括但不限于文本、图片、数据、观点、建议，不构成法律建议，也不应替代律师意见。本报告所有材料或内容的知识产权归工业互联网产业联盟、中国联通研究院、联通数字科技有限公司共同所有（注明是引自其他方的内容除外），并受法律保护。如需转载，需联系本联盟并获得授权许可。未经授权许可，任何人不得将报告的全部或部分内容以发布、转载、汇编、转让、出售等方式使用，不得将报告的全部或部分内容通过网络方式传播，不得在任何公开场合使用报告内相关描述及相关数据图表。违反上述声明者，本联盟将追究其相关法律责任。

工业互联网产业联盟

联系电话：010-62305887

邮箱：aii@caict.ac.cn

目 录

前　言

3GPP 在 R16 中启动 5G LAN 项目研究，意味着 5G 网络具备了广域局域网的能力，为 5G 网络在工业领域的应用提供了新的思路。5G LAN 可以为工业领域提供定制化的专属广域“局域网”，使得工业终端与企业云随时随地处于一个虚拟化局域网中。5G LAN 的优良特性使得 5G 网络在工业领域应用中发挥重要的作用，必将培育出新工业网络应用场景，促进工业企业数字化转型。

工业领域的数字化升级促进了 IT 和 OT 网络融合，也给工业网络带来了严峻安全挑战，如攻击暴露面扩大、攻击路径增多等，原来封闭的生产网络、业务系统开始向外界开放，工厂内部网络、系统等被攻击的概率增加。5G LAN 在继承 5G 网络安全能力的同时，结合局域网特点也诞生了一些独有的核心安全能力。面向工业领域千差万别的安全需求，不仅能形成统一了工厂设备的连接形式，而且能针对不同的业务场景形成有效的网络安全整体解决方案。

本报告考虑工业领域的网络安全需求，结合工业领域 5G LAN 技术的发展和应用情况，总结了 5G LAN 网络安全相关技术，以及有代表性的行业典型案例，为工业领域的 5G LAN 安全技术应用和推广提供参考依据和指导。

总策划：叶晓煜　谢　攀　李浩宇　张建荣

主编：周晓龙

副主编：柳　兴　荆　雷　鲁华伟　谢　云

编委会成员：

王　哲　陶耀东　冯冬芹　井　柯　刘　旸　俞一帆　文　宏

蒋美景　何　凯　陈丽萍　王新宇　李易凡　刘广祺　谢嘉宇

韩江雪　邱　晨　张博文　王竑达　王维治　傅成龙　葛　然

王宝栋　文　雯　范勇杰　徐乐西　吴　冬　崔莹莹　黄继烨

靳冰祎　谢　璟　田慧蓉　王　磊　刘　程　王　舒　乔思远

毛庆梅　李　艺　陈　昕　黄东华　徐书珩　赖羿明　白小愚

指导单位：中国联合网络通信有限公司政企客户事业群

中国联合网络通信有限公司网络与信息安全部

参与单位：中国信息通信研究院

深圳艾灵网络有限公司

奇安信科技集团股份有限公司

北京双湃智安科技有限公司

中智云物联网有限公司

杭州安恒信息技术股份有限公司

兰州兰石爱特互联科技有限公司

普天信息工程设计服务有限公司

天津市工业互联网研究院

浙江大学

北京交通大学

一、5G LAN 简介

5G LAN 是基于 5G 网络的私有移动局域网，由一组 5G 终端组成，通过 5G 网络连接实现相互通信。这种网络连接可以在同一办公区内，也可以在相隔遥远的不同工厂、园区之间。相较 Wifi、4G 等传统技术，5G LAN 可以提供更为安全、高效、灵活的无线局域网服务。

（一）5G LAN 的起源

5G 技术自 2019 年商用以来，正逐渐与工业制造、能源电力、交通、城市管理、教育等各个垂直行业深度融合，这一趋势已经得到广泛认可。目前，行业各方正在紧密合作，探索各种 5G 行业应用解决方案和服务流程，推动 5G 技术的规模商用和进一步发展。

与个人移动应用不同，各个垂直行业对 5G 网络有着各自独特的需求。一些应用场景需要低延时和高可靠性，也有一些应用则需要更大的带宽，还有一些应用场景要求专属网络以确保数据的安全性。因此，不同的应用场景需要不同的技术方案来满足其特定需求。此外，传统通信方式通常采用 TCP/IP 协议来实现终端之间的数据传输，但在垂直行业、特别是工业领域的终端可能缺乏对这些三层网络协议的充分支持，这将导致 5G 网络在垂直行业的应用阻力重重。出于这些需求考虑，5G LAN 的概念应运而生。

3GPP R16 首次提出了“5G LAN-type service”（5G LAN 类型业务），包含“5G Virtual Network group”、“5G LAN Virtual Network”等概念，涵盖了虚拟组管理、虚拟组成员管理、虚拟组会话管理以及

局域网数据交换管理等多项关键技术能力。通过这项技术，可以实现 5G 环境下的虚拟局域网分组管理，更好的应对不同垂直行业需求不同的现状，并且使垂直行业不支持二层通信的顽症得以解决。

（二）5G LAN 的发展

在定义了 5G LAN 的基本功能后，R17 版本又重点针对 5G LAN 的计费进行了研究，提出了组管理事件计费方案。该方案通过对虚拟组的组内、组间等不同计费场景进行计费配置，实现了更灵活的计费方案，为 5G LAN 进一步商用提供了有力支撑。

5G LAN 的标准发展也逐渐完善，其中 3GPP TS 23.501、3GPP TS 23.502、3GPP TS 23.503 分别从系统架构、程序与信息流和策略与计费控制对 5G LAN 进行了研究。IEEE 802 系列标准中 IEEE802.11ax（Wi-Fi 6）、IEEE 802.1Q（VLAN）、IEEE 802.3（以太网），虽不是 5G 标准，但可与 5G 结合形成更强大的网络解决方案，用于实现 5G LAN 的目标。

目前 R18 版本已经冻结。R18 完善了 5G LAN 管理方面的能力：

（1）组成员流量特征实时监控。通过该能力，可以让工业用户通过业务量获得更多的工控系统实时统计数据，从而更好地了解网络和业务的实时状态，监控系统运行状态，及时完成性能分析和故障排除。

（2）跨 SMF 管理 VN Group。该功能可以有效解决 R16“一个 VN Group 只能被一个 SMF 管理”的问题。在当前 SMF 出现故障时自动切

换到其他可用的 SMF 上，从而保证整个 VN Group 的运行不受影响，为工业用户带来更加可靠和高效的网络服务。

（3）跨 VN Group 通信。在 R16 中，跨组通信存在很大的局限性，R18 的方案可以解决该问题，帮助用户将多个群组连接起来，建立范围更大的网络。

（4）组管理和组状态上报增强。该特性可以帮助工业用户实现对组内用户和业务流的精细化管理，提高包括用户认证、权限管理、QoS 控制等方面的灵活性与可靠性。

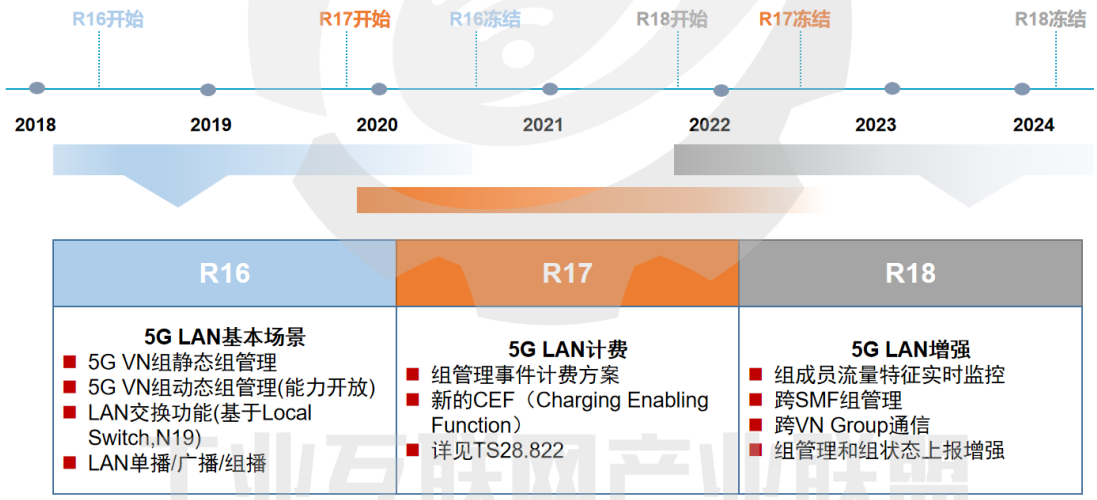

图 1.1 5G LAN 技术演进图

（三）5G LAN 的优势

5G LAN 兼顾移动通信网和无线局域网的优点，可满足复杂多变的通信需求，具体如下：

（1）良好的基础性能：5G LAN 以 5G 无线技术为基础，继承了 5G 无线技术大容量传输数据、大规模设备连接、超高可靠低延迟（uRLLC）可满足生产制造、远程控制等垂直行业对网络带宽、实时

性和精确性要求极高的应用场景。较工业 Wi-Fi，5G 的覆盖范围更广、小区间切换更流畅、运维服务更具标准体系化，可给用户带来更好的网络体验。

（2）优秀的工业适配：5G LAN 解决 5G 系统本身不支持二层通信的难题，具备直接进行二层通信的能力，可以与用户已有数据网络进行连接，实现即插即用和相互访问，省去了引入 AR 的步骤，大大降低了 5G 网络的改造难度，方便工业终端的 5G 无线接入。

（3）灵活的组网方式：5G LAN 具备数据网络组网、本地组网和远程组网三种数据转发能力，既能满足同一个 PSA UPF 下的工厂终端通信，又能满足不同 PSA UPF 下的工厂终端通信，可以帮助工厂终端设备通信灵活组网，同时支持二层数据交换和三层数据交换，具有较高的数据转发效率。

（4）支持广播与多播：5G LAN 支持 UPF 的双检测转发机制，提供类似于以太交换机的数据处理与转发功能，实现终端间的数据转发，可以满足组播、广播的通信需求。UPF 通过检测终端的目的地址并添加路由，在传统上、下行数据转发的能力之上，实现单 UPF、跨 UPF 的终端间的广播、多播，可满足工业终端的多样性通信需求。

二、5G 网络安全关键技术

5G LAN 是建立在 5G 终端接入能力和 5G 网络之上的私有移动 LAN 服务，通过建立“群”，为企业内部终端提供灵活的通信服务，包括终端互通和终端隔离等。**5G LAN 技术是一种基于 5G 的局域网技术，它提供了高速、低时延和高可靠的网络连接，可以支持实时数据传输和网络控制。5G LAN 安全具备多项技术能力，不仅继承了 5G 本身的安全技术，更加具备增强的网络安全技术能力**。本章主要介绍 5G 本身的安全技术。

（一）5G 接入认证安全技术

1、统一安全认证框架

5G 支持多种接入技术，为了更好的支持不同应用场景、不同设备接入 5G 网络，使得用户可以在不同的接入网间实现无缝切换，5G 网络采用一种统一的认证框架，实现灵活、高效地支持各种应用场景下的双向身份鉴权，进而建立统一的认证体系。可扩展认证协议（EAP）认证框架，能够满足 5G 统一认证需求。EAP 认证框架，是一种支持多种认证方法的认证框架，框架本身不提供任何安全性，只规定了消息的封装格式，具体的安全目标依赖于使用的认证方法。

2、基于证书实现用户身份信息保护

在 5G 网络中，每个用户都有一个用户永久身份标识。如果该身份信息在空口暴露，可能出现固定用户进行位置跟踪等安全事件，从而侵犯用户隐私。5G 系统中引入了基于公钥体系的加密机制，对 SUPI

进行加密形成 SUCI，在空口中传递 SUCI 以全面保证用户的隐私在空口不泄露。为支持 SUCI 的计算，首先 SIM 卡需在生产过程中预置运营商公钥，需采用安全方式（如专线、VPN 等方式）将公钥数据传输给供卡商制卡；在用户开机登网等场景下，需要传递 SUPI 时，通过 SIM 卡中的归属网络公钥对 SUPI 进行加密生成密文 SUCI 用于在空口中传输，从而更加有效地保护用户的隐私。在产生 SUCI 时，需要利用 USIM 中预置的归属运营商公钥、采用 ECIES 对 SUPI 进行加密运算，并且根据算法原理，每次使用时产生的 SUCI 也不相同。因此攻击者无法根据 SUCI 推算出 SUPI，也无法利用 SUCI 长时间对用户进行探测，进而无法针对用户进行持续性的跟踪。

3、基于零信任的接入认证技术

零信任体系保障终端可信、通道可信、身份可信，并提供持续信任评估与行为监测能力。对于身份可信，可以通过 IAM 实现身份管理、认证鉴别、权限管理和访问控制，融合零信任智能多因子认证，支持多种认证模式，包括客户端私有密钥、设备指纹、IP 地址、生物身份等。IAM 通常采取集中部署模式，基于 5G LAN 的部署架构，可以按需实施分层部署。对于持续信任评估与行为监测，通过行为记录和审计等方式，持续监控用户行为。针对终端安全事件、违规越权行为、潜在威胁、文件泄露、系统漏洞等状态，及时调整身份认证和访问控制策略。

（二）5G 数据安全保护技术

1、5G 数据加密技术

5G 网络上面承载着很多用户的隐私和敏感信息，需要采用技术措施解决 5G 网络的隐私保护问题。数据加密是 5G 网络中保证数据隐私安全的常见手段，按照实现思路，可以分为静态加密技术和动态加密技术。在实现的层次上，可以分为存储加密，链路层加密、网络层加密、传输层加密等。采用加密技术可以有效保证 5G 网络数据的机密性、完整性和可用性。针对 5G 网络虚拟化和云化的新特点，可以引入一些新的加密技术来保证数据的隐私安全，如同态加密技术。同态加密技术对加密的数据处理得到输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的结果相同。

2、5G 数据防护技术

5G 网络在空口为用户面数据增加了可选的完整性保护功能。在用户需要新建会话时，由核心网根据用户配置信息中的用户安全策略向基站发送无线链路配置消息来告知终端是否启用用户面完整性保护。5G 使用 SEPP 设备进行网间安全保护。SEPP 间的安全传输定义了两种安全保护的机制：一种是基于传输层协议的安全保护机制，即 TLS。这种机制将会导致中间转接商 IPX 失去对信令调整的能力。另一种是基于应用层协议的安全保护机制。这种机制可以灵活的对多个应用层数据集合采用不同的安全保护策略，从而实现了在 SEPP 之间的安全传输，同时也为 IPX 获取相关信息或修改相关信息留下了空间。

3、5G 工业流量防护技术

针对工业应用，采集和分析工业协议的流量，针对加密流量采用非监督学习和监督学习结合的方式，从网络流量特征、协议、流量大小、业务时间、业务操作行为等多维度建立合规基线模型，然后实时对比、分析从而发现数据安全风险事件；针对非加密协议可对操作数据内容、传输文件内容进行还原，利用大数据分析、机器学习等技术建立用户画像、业务画像、数据安全合规基线等，实现批量传输敏感数据、数据跨境传输、接口异常访问敏感数据、接口未授权等安全场景的实时监测与风险事件溯源分析，确保 5G 智能制造行业的应用与数据安全。

（三）5G 网络切片安全技术

1、切片安全隔离技术

5G 网络切片是一组运行在通用物理硬件上的多个 NF 的编排组合，具有独立提供网络服务能力的端到端虚拟网络。由于网络切片共享相同的网络资源，因此切片之间的安全隔离非常重要，做好网络切片的端到端隔离，一方面可以避免切片之间发生资源相互竞争而影响切片的正常部署和运行，另一方面可以避免一个切片的异常（如遭受内部安全威胁或者攻击，影响其他切片的安全），有效防止攻击扩散、切片数据泄露等安全威胁。网络切片是端到端虚拟网络，是由无线接入、承载、核心网构成，因此网络切片端到端的隔离包括切片在接入网、承载网和核心网的隔离实现。

2、切片接入安全技术

用户接入切片的认证能力是在终端接入网络时由 5G 网络执行接入认证来保证接入 5G 网络用户的合法性的基础上，3GPP 还提供了运营商、切片客户配合完成切片认证和授权的机制，保证仅合法用户可接入切片，实现垂直行业对切片网络及资源使用的可控性。切片选择辅助信息及隐私保护能力时在 NSSAI 可以区分不同类型、不同用途的切片。在用户初始接入网络时，NSSAI 指示基站及核心网网元将其路由到正确的切片网元上。切片选择辅助信息对于垂直行业属于敏感信息，5G 网络提供标准的机制，可对传输中的 NSSAI 进行隐私保护。

3、切片管理安全技术

切片的管理安全包括两个部分，一是通过管理手段保证切片的可用性；二是保证切片管理过程的安全。针对切片的可用性，切片管理系统提供实时的切片安全监控、应急处置以及故障恢复能力，实时掌握切片的运行情况、可能的被攻击情况及故障状况，通过联动对应的安全设备进行处置，并及时对故障进行修复，从而保障系统的可用性。针对切片管理过程的安全，一方面是管理信令的安全保护；另一方面是切片生命周期管理和维护管理。为了保障切片管理的安全，要设置相应的安全保护机制。

（四）5G 网络安全增强技术

1、5G 网络安全态势感知

传统网络基于 IP 的单一化寻址路由机制已经难以适应目前 5G 网

络承载的多样化业务需求，缺乏数据传输安全能力以及对终端行为的感知能力。人工智能技术以 SDN 和 NFV 技术为基础，实现控制层面与传输层面的能力解耦。基于实时更新优化的智能路由模型，可实现对于网络整体态势的实时感知，配部署网络安全传输设备，建立智能化安全防护模型，形成针对用户的恶意访问行为的精确感知，从而构建一个集网络安全态势感知、数据安全智能路由、恶意行为告警及网络安全防护功能于一体的传输网络安全体系，从根源上杜绝如分布式拒绝服务攻击等恶意行为对 5G 网络造成的安全隐患。

2、5G 终端行为感知与管控

相比于传统网络，为满足物联网、车联网以及智慧城市等应用环节的网络能力需求，5G 网络在 mMTC 场景下需支持每平方千米 100 万用户的接入数量，超大规模的终端接入能力必定伴随着由挟持终端发起的 DDoS 攻击的风险。因此，终端行为的感知与管控能力是 5G 网络 mMTC 场景下必不可少的安全防护能力。通过在网络侧收集终端用户的行为信息，充分利用机器学习技术针对多源数据的辨识能力，训练一个具备识别用户实时状态的终端行为的管控模型，从而在网络侧形成针对终端异常或恶意行为的感知、识别、管控的一体化能力，进一步提升 5G 网络的运行效率，增强网络的可靠性。

3、区块链助力 5G 数据安全

5G 网络使得网络速度提升，数据量随之高速增长，对数据的安全性保护和隐私性提出了更高的要求。区块链的分布式、自组织特性，

可用于构建数据共享、分散协作、去中心化的松散的生态环境，其用密码学的手段为交易去中心化、隐私信息保护、历史记录防篡改、可追溯等提供技术支持，天然适用于对数据保护要求严格的场景，同时，区块链去中心化也为网络资源共享提供了新的解决思路。以区块链为代表的应用密码技术将为网络重构安全边界，建立设备间的信任域，实现安全可信互联。同时，终端去隐私化的关键行为信息上链后，即会分布式存储在区块链各节点中，保证数据的安全性和可用性，促进构建智能协同的数据安全防护体系。

三、5G LAN 安全防护关键技术

5G LAN 的二层组网功能可以提供更加灵活、高效和安全的网络连接方式，符合工业领域对网络的要求。它可以使用虚拟局域网（VLAN）来实现逻辑隔离和网络划分，从而满足不同的应用需求。此外，5G LAN 还可以支持多个广播域和多个网段的划分，以便更好地管理和控制网络。5G LAN 安全防护关键技术在网络中的位置具体如下图：

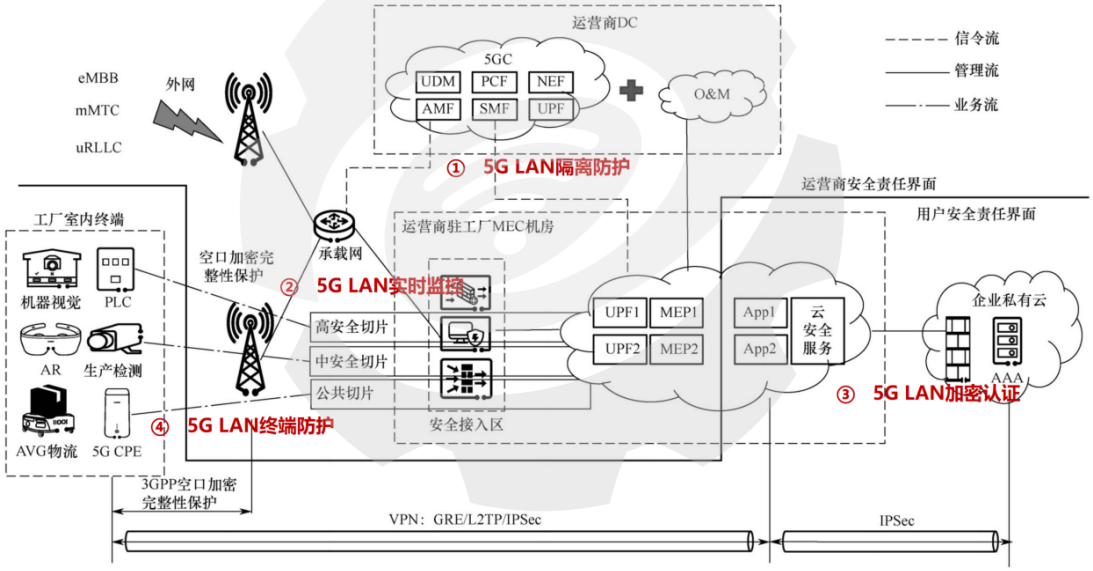

图 3.1 5G LAN 安全关键技术全景图

（一）5G LAN 隔离防护技术

跨 SMF 管理 VN Group 可以有效地解决一个 VN Group 只能被一个 SMF 管理的问题，该问题会导致容灾能力不足，一旦该 SMF 出现问题，整个 VN Group 都会受到影响。跨 SMF 管理 VN Group 能够使得多个 SMF 可以同时管理一个 VN Group，从而提高了系统的可用性、容灾能力和稳定性。在 SMF 出现故障时自动切换到其他可用的 SMF 上，从而保证整个 VN Group 的运行不受影响，为工业用户带来更加可靠和高效的网络服务。

基于 5G LAN 的工业互联网承载多个业务系统，应按照业务相对隔离、信息按需互通的原则进行各子网的设计。在网络层面，保证不同的业务系统部署在独立的 VLAN 中，同时划分不同的安全域，各安全域之间采取边界防护措施，保证各业务系统和子网的独立；在应用和数据层面，各业务系统采取身份认证、访问控制等措施阻止非法访问，保持应用和数据的独立性。

5G LAN 边缘组网隔离包含三平面隔离和安全域划分。三平面隔离是指服务器和交换机等应支持管理、业务和存储三平面物理/逻辑隔离。对于业务安全要求级别高并且资源充足的场景，应支持三平面物理隔离；对于业务安全要求不高的场景，可支持三平面逻辑隔离。安全域划分是指 UPF 和通过 MP2 接口与 UPF 通信的 MEP 应部署在可信域内，和自有 APP、第三方 APP 处于不同安全域，根据业务需求实施物理/逻辑隔离。 另外，可通过特定的技术确保网络安全，如 N4 流量采用 IPSec 等技术建立安全通道、开启防地址欺骗策略防止 UPF 上、下行流量中的地址欺骗、在物理端口执行 ACL 过滤策略、通过 URL 黑名单方式对 WAP 推入的恶意消息拦截过滤、通过 GRE 等隧道对不同业务类别流量进行控制和隔离、在 UPF 公网侧部署抗 DDoS 设备等。

（二）5G LAN 实时监控技术

组成员流量特征和性能监控对于工业用户来说非常重要，因为他们对网络和业务的运行状态更加关注。这意味着在 5G 网络中，工业用户可以获得更多的业务流和性能统计数据，从而更好地了解网络和

业务的实时状态。此外，5G LAN 还支持实时性能监控和告警，以及高级的日志分析和故障排除功能，这些功能可以提高网络的可靠性和稳定性。总的来说，5G LAN 为工业用户提供了强大的网络管理和监控工具，以确保他们的业务能够顺利运行。

性能监控和告警功能可以及时发现网络中的异常行为或安全威胁。5G LAN 提供高级的日志分析和故障排除功能，帮助管理员深入了解网络的运行情况和潜在的安全问题。通过分析日志数据，可以发现潜在的安全漏洞或攻击行为，从而采取相应的防范措施。

通过设置部署网络安全态势感知探针，实时监测网络安全状态，识别异常流量，及时发现网络攻击行为，提供实时的预警和报警信息，帮助用户及时采取安全措施，保障信息系统的安全。还可通过安全管理中心进行全系统安全态势的集中统一管理，及时识别网络攻击，采取有效的应对措施。

（三）5G LAN 加密认证技术

5G LAN 借助于 5G 技术的加密与认证机制，能够提供更高级别的安全保障。这包括使用强加密算法对数据进行加密传输，以及使用认证机制对终端进行身份验证，确保只有授权终端可以接入网络。

对于接入 5G LAN 网络的终端设备采用接入认证，防止 5G 公网终端非法接入 5G LAN 网络。可采用的措施包括：独立建设用户 AAA 设备，让企业自行管理 5G LAN 的用户，只有在企业 AAA 设备中的合法用户才能接入 5G LAN 网络；在 5G LAN 网络中对接入终端进行二次

认证，采用企业自主可控的二次认证方案和设备，只有通过二次认证的终端才能接入 5G LAN 网络，防止非法用户接入。

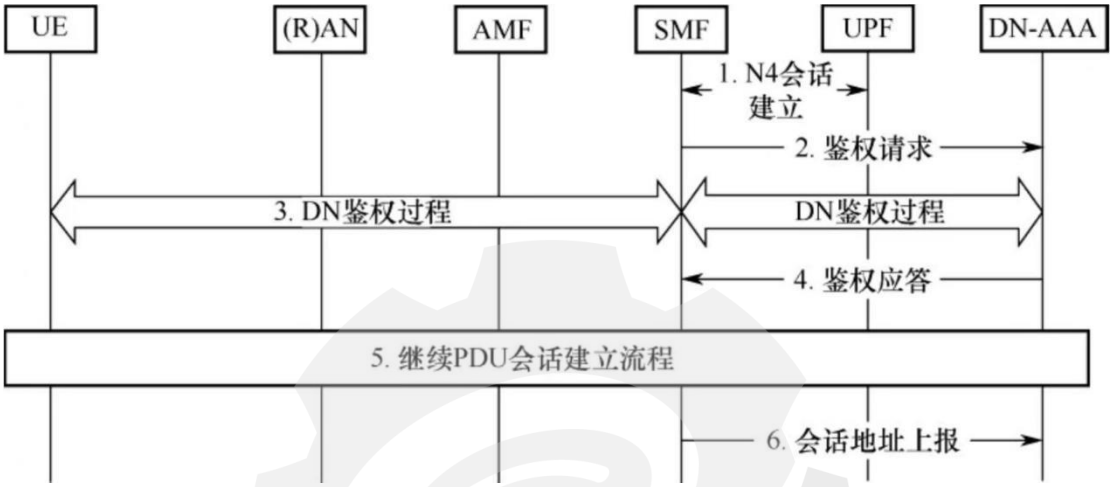

图 3.2　5G LAN 的二次认证流程

（四）5G LAN 终端防护技术

5G LAN 技术允许在 LAN 内为 5G 终端提供终端互通或终端隔离等灵活的通信服务。通过设置访问控制策略，可以限制不同终端之间的通信，减少潜在的安全风险。在基于 5G LAN 建立的工业互联网系统中，各种设备需采用安全措施提升自身的安全。

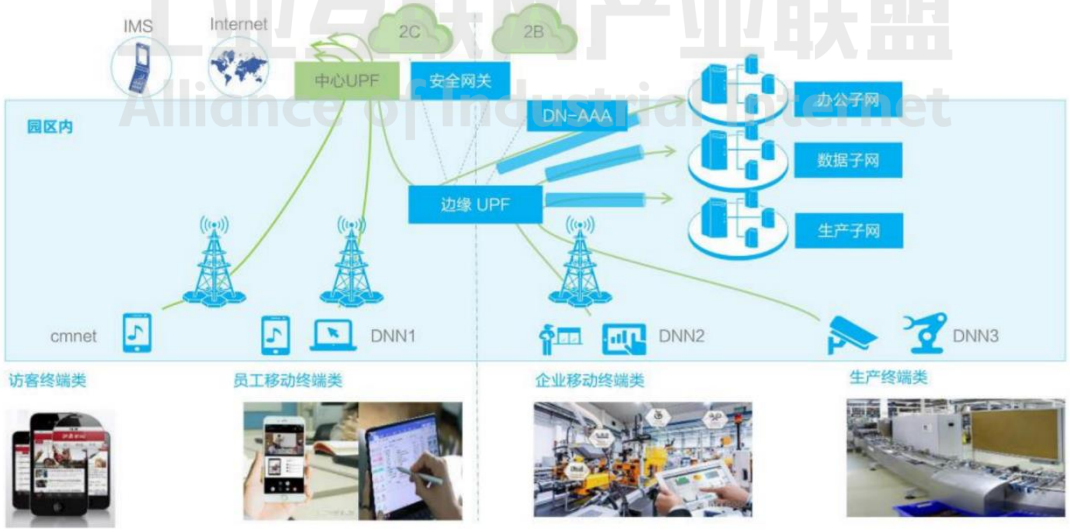

图 3.3　5G LAN 基于用户的终端隔离防护

安全防护的重点是数量众多的终端设备，以防止病毒、木马通过终端设备侵入系统为主要保护目标，采取的主要措施：减少不必要的功能和应用，操作系统和应用软件都遵循系统最小化原则；应用基于“白名单”和“黑名单”相结合的防护技术，在系统稳定运行后通过规则匹配、深度学习等方法自主建立合法的“白名单”，在没有特征库的情况下也能发现病毒和网络攻击等异常情况；使用端口管控工具控制外部移动设备的接入，并对所有接入的移动存储设备进行审计。

四、典型案例

（一）工业 5G LAN 数据安全管理应用案例

1、背景

工业控制网络是工业生产的“核心大脑”，用于监控、管理工业生产过程中的智能终端设备，确保生产的稳定性和可靠性，提升生产效率，在关键信息基础设施领域得到广泛应用。为适应新时期工业控制系统网络安全形势，进一步指导企业提升工控安全防护水平，夯实新型工业化发展安全根基，2024 年工信部印发《工业控制系统网络安全防护指南》，使用、运营工业控制系统的企业适用本指南，防护对象包括工业控制系统以及被网络攻击后可直接或间接影响生产运行的其他设备和系统。

5G 与工业互联网的深度融合，大量工业设备接入网络，由于工控设备安全防护相对薄弱，存在被非法访问控制的风险，导致生产中断或设备损坏。需进一步提升工业企业的工控安全保证能力，保护工业设施免受攻击，在石油化工、汽车、智能制造等工业领域，满足工业 5G LAN 网络中数据加密传输、身份认证、数据安全等需求。

中国联通联合中智云物联网打造工业 5G LAN 数据安全测试床，面向工业领域由于工控系统老旧、系统性能低、无法与互联网通讯、无有效的安全维护人员和体系等情况导致在 IT 领域使用的身份认证技术措施无法直接应用到工业控制领域的问题。针对 5G+工业互联网场景对工业数据安全的迫切需求，提出了一套针对工业领域全链路数

据安全防护的技术方案。

2、应用场景与需求

在工业互联网场景下，数据在采集、传输和存储过程中面临着安全风险。如果数据被恶意获取或泄露，可能导致用户隐私曝光，损害用户信任和企业声誉。若第三方机构或合作伙伴参与数据共享和处理，一旦数据共享失控或处理出现错误，可能会引发法律责任和用户隐私泄露的风险。

工业企业在数字化转型过程中面临的数据泄露风险，恶意攻击风险、数据传输风险、安全防护能力不足等数据安全问题。工业互联网领域中的数据安全保护涉及多个关键环节。首先，访问控制与身份验证构成确保仅授权端到端能够接触数据。其次，数据加密与隐私保护技术构成保障端到端数据机密性和隐私安全。最后，采用高级加密手段对信息实施安全编码，确保数据在传输和存储过程中不会被未授权访问或篡改。

本案例通过工业 5G LAN 满足云、管、端数据传输安全、身份认证等方面的安全需求，提升主机身份鉴别、网络设备安全接入、用户认证、传输加密等安全能力。

3、解决方案

5G-LAN 功能场景:网络规划方案 5G-LAN 组网架构支持二层组网，不同的 UPF 进行 5G-LAN 组网后，相互之间可直接进行通信，完成 5G-LAN 组网架构后，可实现如下功能：

1)同一 UP 下的两个 UE(5G CPE 路由器)可以直接进行二层交互；

2）不同 UPF 可以通过 N19 直接进行交互；

3）不处于同一个 5G-LAN 用户组的 UE(5G CPE 路由器）不能相互通信，如图 4.1 中 UE31 不可访问其他 5G-LAN 用户组；

4）企业可以自主分配 IP 优化网络规划，如图 4.1 中生产车间、生产厂房或生产园区 1 所示，企业可以自主搭建 DHCP 服务器实现 IP 动态分配。

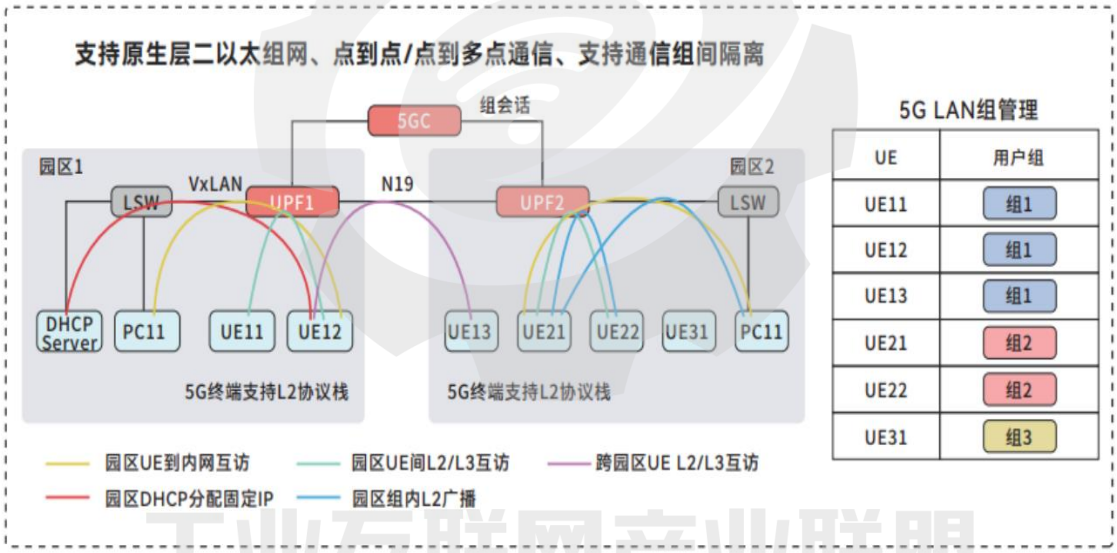

图 4.1 5G LAN 组网架构

使用 5G-LAN 组网，不同工业 5G CPE 路由器可以直接进行二层数据交换，无需部署 CE。使用 5G-LAN 的生产车间组网架构如图 4.2-2 所示：

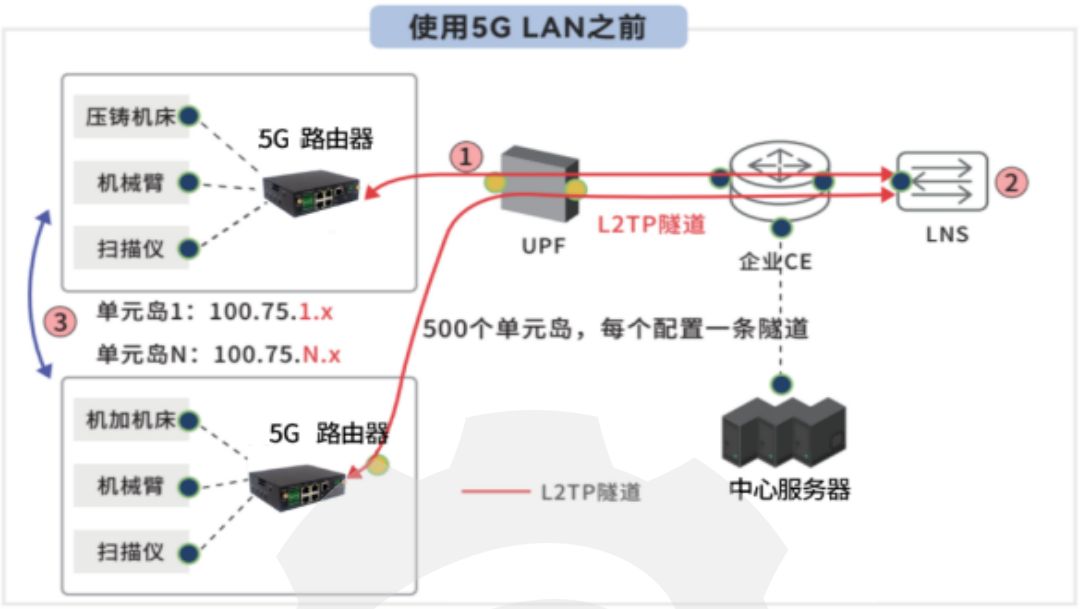

图 4.2-1 未使用 5G-LAN 生产车间组网架构

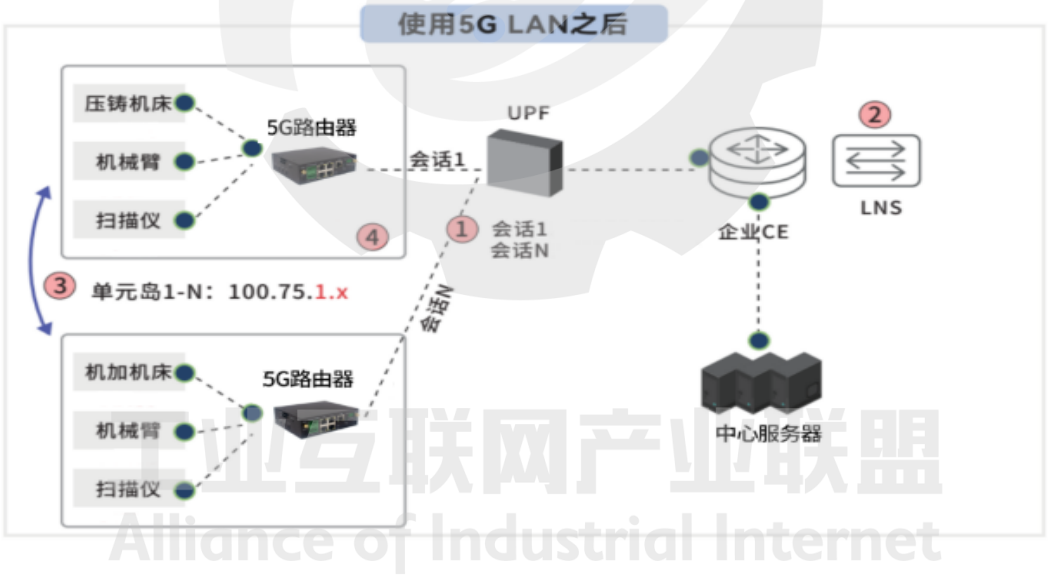

图 4.2-2 使用 5G-LAN 生产车间组网架构

使用 5G-LAN 生产车间组网架构优势如下：

1）在工业互联网中降低建网成本，无需额外建立隧道设备；

2）支持二层组网，可以使用工业协议报文；

3）降低延迟和网络负荷。

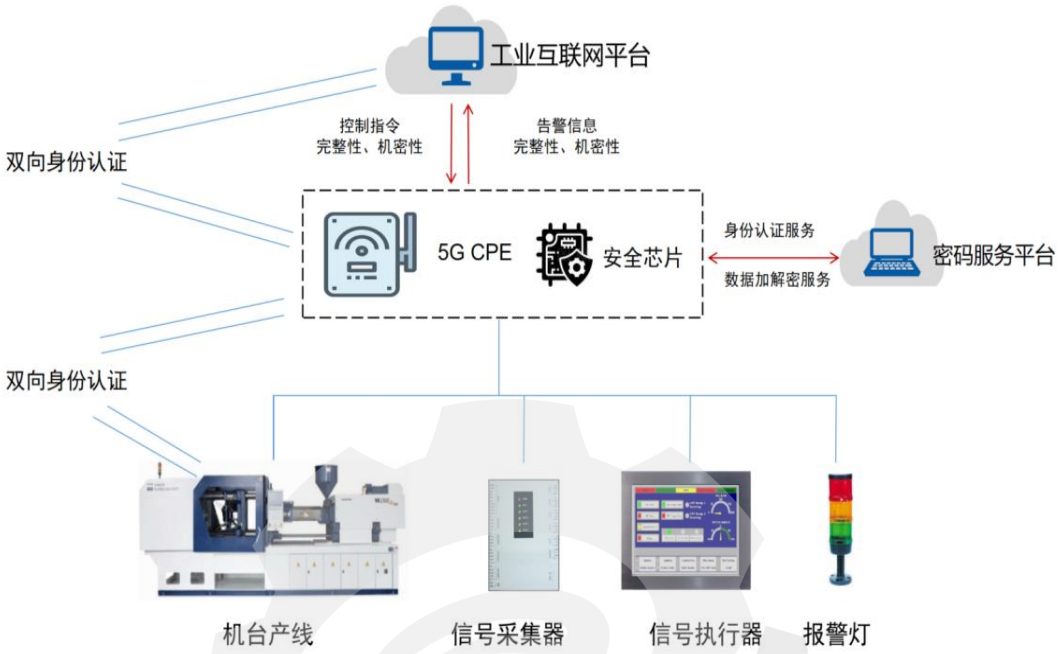

图 4.3 5G LAN 数据安全测试床总体架构

测试床组网架构如图 4.3 所示，主要包括工业互联网平台、5G CPE 工业网关/边缘网关、SEC 安全芯片、智能终端设备等部分。主要包括端到端全链路加密、设备身份认证、安全通信等技术方案。

(1)端到端全链路加密技术方案

本测试床项目依托 5G CPE 进行数据加密实现端到端的全链路加密传输方案，可确保数据在传输过程中即使被拦截也无法被读取或篡改。工业领域数据传输及设备通信的端到端加密是确保设备之间的通信数据安全性的重要组成部分。通过选择合适加密算法，保证设备的效率、适用性和可扩展性，对于提升安全能力至关重要。

利用 5G CPE 或模组的 eSIM 安全芯片卡作为应用载体，结合运营商 ID 和网络可信身份 ID，为用户提供一种安全、可信且便捷的身份认证服务。该服务以 eSIM 安全芯片卡为核心，为持卡用户提供身份

验证服务。这个网络身份凭证是与用户的实体身份证芯片唯一对应的电子映射文件，确保身份信息的准确性和安全性。

(2)安全通信技术方案

依托 5G 安全通信的数据加解密与数据加密传输技术，对工业互联网平台和智能终端设备的数据传输进行加解密。在外部接入数据和内部数据流转两种场景中设置不同参数的加解密算法，可达到系统外部和系统内部交换数据时数据无法泄露的效果，可保证数据安全以及设备安全。工业互联网平台增加数据安全存储能力，5G CPE 网关加密传输能力，降低工业生产数据的泄露风险。

4、应用效果

通过运用基于商用国密服务、PKI/CA 数字证书服务、SEC 安全芯片、5G LAN 切片安全服务等工业互联网数据安全信创体系综合协同服务。为各类设备接入访问提供安全认证、访问控制，解决业务应用在身份鉴别、数据传输机密性、完整性等安全问题。

本方案通过全链路数据安全体系的构建，帮助用户打破安全数据交互壁垒，统筹安全能力，从而形成安全防护合力。建设以密钥管理、数据加解密管理、数据安全传输、设备身份认证为功能的全链路加密技术框架，通过全链路技术加密框架传输安全数据，挖掘数据真正价值，全面提高安全处置效率，赋能工业企业数据安全防护。促使用户信息安全效率提升。

（二）电力 5G LAN 终端认证和身份管理应用案例

1、背景

电力是国家的支柱能源和经济命脉，发展工业互联网是电力行业数字化转型的必然过程。根据工信部印发的《工业互联网创新发展行动计划（2021-2023 年）》的相关内容要求，电力行业将进一步加快工业互联网创新发展步伐，持续推动工业数字化转型。电力行业的安全稳定运行关系到国家的经济发展。随着电网规模的逐渐扩大，安全事故的影响范围越来越大，安全问题越来越突出。

当前 IT 和 OT 融合发展趋势加速，电力行业智慧转型离不开新兴的云计算、大数据、物联网、人工智能等技术的支撑，传统的安全威胁和新技术带来的新型安全风险将交织扩散，给风力发电、光伏发电造成巨大安全威胁。电网面临各种攻击，如勒索攻击、蠕虫病毒、远程操纵等定向攻击。在基础结构安全方面则表现为典型的物理安全、设备运行数据安全、远程运维网络安全等突出问题。

某光伏电厂引入 5G 网络，支持了多样化应用及海量的终端接入。随着智能化发展，传统的终端身份接入认证机制难以实现细粒度的访问控制，因此不论是对身份管理的能力需求上，还是实现网络和业务的深度融合机制上，都需要构建新的多元认证和身份管理体系。为电力行业网络安全提供安全可靠的终端认证能力。

2、应用场景与需求

5G 网络支持各种设备终端接入，电力行业的终端也接入了 5G 专

网。依照电力行业相关规定，在安全分区、网络专用、横向隔离、纵向加密、分级综合防护的基础上，需要进一步对终端设备的身份认证格式、登录和绑定协议等进行标准化，实现设备身份的可追溯性。

在光伏电厂应用环境下,SIM 卡会被非法使用,一旦终端内的 SIM 卡被非法移至其他设备用来进行大数据流量的传输,将会使行业用户蒙受损失。内外横向攻击，恶意终端随办公网接入容易进一步引发行业内网横向攻击，导致生产事故，危害极大。出于对终端安全和用户卡安全角度的考虑，需要通过技术手段限定 SIM 卡和终端的绑定关系。

伴随着移动终端和各种智能设备的普及,接入网络的终端设备更多的是位置会发生变化的移动终端。电力行业的终端地理位置分布广、涉及管理部门层级多，终端归口管理细。为了确保接入安全，需要对终端接入位置进行管控，防止数据泄露等安全风险。因此，需要基于身份管理系统结合网络空间测绘技术进行准确的地理定位和细粒度管理。

3、解决方案

本案例主要包括终端接入二次认证、终端机卡绑定接入认证、终端接入位置认证、终端零信任接入认证等技术方案。

（1）终端接入二次认证技术方案

5G 网络中,终端必须具备身份验证的能力,终端接入首先由运营商核心网实现对终端基于 5G AKA 或 EAP-AKA’的主认证，如果启用

了切片，还包括接入切片的过程。但主认证仅由运营商对终端身份进行了验证，仅在运营商侧无法彻底解决行业客户的前述终端接入风险，因此除了运营商主认证，还需要提供行业用户自主可控的终端二次认证能力。二次认证接入图如下图所示：

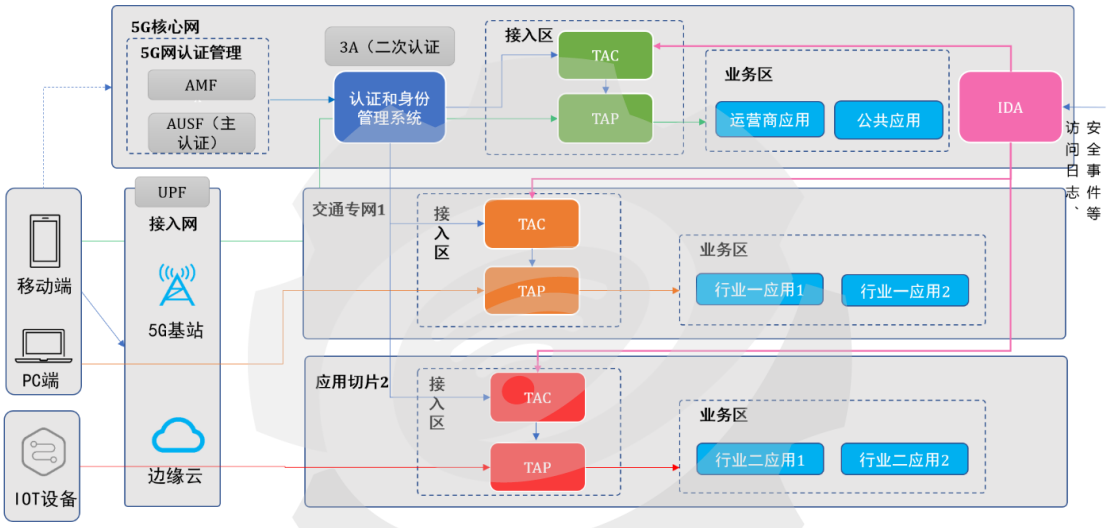

图 4.4 终端二次认证接入示意图

二次认证即 UE 设备向核心网认证，而 UE 的应用向业务系统认证。将二次认证进行统一，可以绑定设备与应用，并增强行为分析能力，构建用户、终端、网络、服务之间统一的信任体系，对于运行在可疑设备上的业务应用进行重点监控。

（2）终端机卡绑定接入认证技术方案

出于对终端安全和用户卡安全角度的考虑，需要通过技术手段限定 SIM 卡和终端的绑定关系。在二次认证的基础上同时对 SIM 卡和终端信息进行认证，做到先认证再访问。

对于高安全场景，需要部署 AAA 服务器基于安全 SIM 卡技术（基于 USIM 卡，内置 USB key 功能，基于 PKI 的数字证书体系，密钥存

储在 SIM 卡安全芯片中，不可复制、不可抵赖、不可篡改，具有高安全级别的身份认证能力）进行认证。

（3）终端接入位置认证技术方案

一般来说，电力客户内网设备数目庞大，且地理位置分散，如果日常的终端入网授权及设备信息维护都集中管理，将会带来极大的压力。通过采用设备指纹扫描技术和指纹库，能够对设备进行扫描和特征内容获取、判别，从而对接入内网的终端设备进行识别并归类。

利用接入层交换机到终端的网络拓扑管理模型，能够对全网终端进行直观拓扑展示，实时掌握全网终端网络位置分布信息、设备运行和安全状况。在拓扑展示图上，还可以进一步向下细化定位，直至每台终端设备。也可以通过终端设备向上检索，找到其连接的交换机，利用交换机管理功能协助用户精确定位终端接入位置，提高运维效率。

（4）终端零信任接入认证技术方案

电力行业基于零信任理念，模块化构建零信任动态授权平台，将应用、用户的身份鉴别、细粒度授权访问、统一动态策略管控形成零信任数据保护解决方案，做到“访问主体身份可信、行为操作合规、实现对被访问应用和数据的有效防护”。

方案建立了以身份为基础的动态访问行为管控，遵循“内生、主动、安全”原则，形成灵活扩展的身份管理和访问控制架构，实现多元用户的身份管理、终端安全管理、身份鉴别、访问授权、凭证管理与访问控制策略管理，提升整体安全水平。

4、应用效果

本方案通过增加二次认证和零信任技术，大大提高了系统的安全性，防止未授权访问和潜在的网络攻击。本方案的透明接入能够让用户使用终端接入时，无需额外操作，提升用户体验。尽管初期实施需要投入一定成本，但通过减少安全事件的发生和应对安全事件的费用，长期来看具有良好的成本效益，降低了由于安全事件导致的品牌损失。

本方案通过应用机卡绑定技术，能够确保只有授权设备和卡片才能访问系统和网络，减少因设备丢失或被盗而导致的安全风险。能够提供可靠的身份认证机制，进一步增强身份认证的可靠性和安全性。绑定技术使得设备和卡片之间形成紧密的关联，防止设备被篡改或替换。提高了系统的可管理性，减少了因设备丢失或被盗导致的经济损失。有效提高了系统的安全性和可靠性，为企业提供了坚实的安全保障。

本方案通过应用位置认证技术，能够确保终端设备只能在指定的物理位置范围内访问系统或执行特定操作，提升系统的整体安全性。企业可以更有效地管理和分配资源，优化工作流程，帮助企业进行资源调度和管理。用户也可在预期位置快速访问系统，无需繁琐的额外认证步骤，提升用户体验。所以，有效提升了系统的安全性和管理效率，为企业的业务运营提供了坚实的安全保障。

（三）智能制造 5G LAN 网络隔离应用案例

1、背景

2022 年 9 月，工信部印发《5G 全连接工厂建设指南》，支持企业建设产线级、车间级、工厂级等不同类型 5G 全连接工厂。基于 5G LAN 的二层通信能力，5G 可以实现与工厂传统有线车间生产网络同样的网络拓扑架构，实现工业级的组网，从而实现与传统有线车间生产网络无缝对接和平滑替代。在实际项目中，基于 5G LAN 的组网技术，形成标杆案例，实现工业智能化升级。

对于智能制造行业，存在现场无线网络的可靠性不足的痛点，提高网络的可靠性以保证安全的生产是非常必要的。5G LAN 技术支持工业海量数据的传输，且延时性低，可靠性高，端到端时延最低可降到接近 5 毫秒，可为工业生产制造实现高精度工业控制。因此，利用 5G 网络的优势，可不改变现有组网，提高网络的可靠性。

智能制造企业面临不同的生产区域之间为了连接的便利性未做有效的区域划分的问题。亟需针对 5G+工业互联网场景对网络隔离的迫切需求，提出了一套基于网络隔离的安全技术方案。

2、应用场景与需求

在传统的架构中，由于信息是逐层传递的，信息无法跨层进行交互。同时，由于工业网络协议众多，不同协议之间信息也难以互通，限制了信息的横向流转。而要实现智能制造，就需要实现数据的动态、实时采集，数据的高效可靠流转和智能化处理。为了实现数据的高效

流转和共享，就需要打破传统的架构，网络向扁平化方向转变。

生产网与管理网融合是无线与有线融合的统一网络，由于数据的流转和系统的开放，也带来安全性的风险。比如生产网与管理网混用，传统的 IT 网络威胁向生产网蔓延。工控网通讯协议较多，单一的隔离设备无法满足多样的网络通讯及安全隔离要求，难以保障工控网络隔离有效性，易感染病毒及恶意程序，同时也可能导致工业控制系统内不同安全域之间的边界防护机制失效。所以需要从网络的隔离和防护构建端到端的安全防护体系，为新的架构保驾护航。

针对工控系统中，存在缺少混合组网隔离、分区分域网络隔离、数据隔离防护措施及恶意代码防范措施等问题。本案例依托 5G LAN 实现横向安全域隔离，纵向边界防护的解决方案。通过在 5G 网络不同域间增加有效的安全隔离措施，实现纵深防御工控网络与企业资源网的打通，保证两网融合后原有隔离网络的独立安全性，使其能应对各种未知信息安全风险。同时部署相应工控信息安全产品以实现横向安全区域间的隔离、生产数据单向采集及监控。

3、解决方案

本案例通过5G LAN整合工控网络组网、工控网络边界隔离技术，实现工业网络横向安全域隔离和纵向边界防护能力。

（1）工控网络组网技术方案

工业5G LAN网络在东西向打通条件下，在部署防护措施的时候，应做好网络隔离安全，划分不同的网络区域，并按照方便管理和控制

的原则为各网络区域进行隔离，工业防火墙、工业隔离网闸、5G 安全 CPE 等作为工业控制边界安全防护设备和安全组网设备，可在工业控制系统网络安全区域之间提供逻辑隔离安全防护。具体如下图：

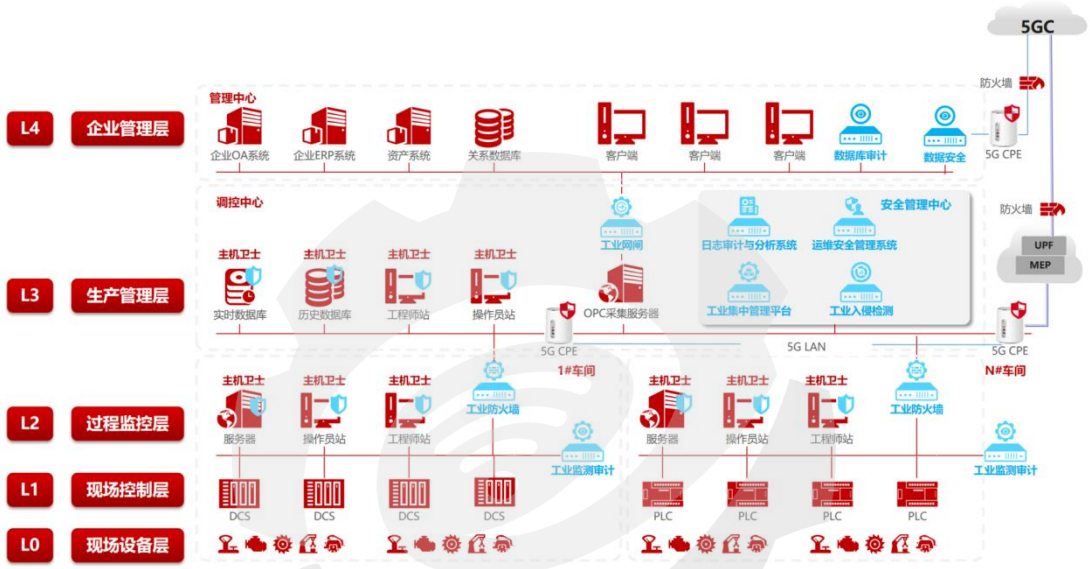

图 4.5 工控网络组网图

5G LAN 主要用于 L2 层网络，在 L2 部署 5G CPE 形成工业局域网，不同车间独立组网形成子网，各子网络用工业防火墙进行隔离。内部安全域划分上，按 IP 地址为生产网划分 VLAN，并设置子网地址。采用 VLAN 提供的安全机制，可以限制特定用户的访问，甚至锁定网络成员的 MAC 地址，这样，就限制了未经安全许可的用户和网络成员对网络的使用。

（2）工控网络边界隔离技术方案

工控网络的边界防护主要涉及管理网与工控网边界、生产子网边界、5G CPE 组网隔离边界和未知边界，需针对不同边界采取安全隔离防护措施。

管理网与工控网边界：在管理网与工控网之间均采用工业网闸进行网络隔离。能够阻止不必要的流量进入工控网。仅定义必要的工控应用服务器与管理网的业务服务器允许通信，其他通信都被禁止。满足等保 2.0“安全网络通信”中：保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信的合规要求。

各生产子网的边界：在网络之间采用工业防火墙进行隔离。阻止生产子网以外的数据包或恶意程序进入生产子网，限制子网内的允许跨网通信的主机数量，除非必要，否则将禁止子网间的通信。同时防止一个子网感染病毒后向其他子网或上层安全域传播的可能。

5G CPE 组网隔离边界：5G 网络使用网络切片为业务提供网络服务。切片包含的所有网络功能都使用运营商电信云中独立的服务器加载，以实现业务与外界业务的物理隔离。CPE 上的 SIM 卡上签约上述两类业务对应的网络切片标识（NSSAI）。当 CPE 注册到 5G 网络时，需要携带 NSSAI。5G 网络为 CPE 选择对应的网络切片。CPE 同时接入多张网络切片，且分别建立分组数据单元会话连接，实现两类业务的逻辑隔离。

未知边界管理：由于工控网络的物理边界范围太大，给管理带来非常大的难度，随身 WIFI 设备、无线路由私接、手机热点等都随时可能破坏网络边界的完整性，使得用户在网络边界上的努力和投入化为乌有。在网络核心处部署边界完整性检查产品，快速网络检测、定位与阻断控制破坏网络边界行为，保护边界安全。

边界防护无法防御来自内部的“攻击”或“人为误操作”，边界防护无法阻止工程师以物理的方式突破网络上的边界。 针对这种问题，可根据区域、通道及深度包检测概念，通过在每个通道都部署支持工业协议的防火墙，并且只允许事先定义过的数据流通过（即白名单的方式）该通道的方式来实现深度安全防护。

4、应用效果

本案例中 5G LAN 网络隔离边界防护通过划分不同的网络区域，可以有效隔离潜在的威胁，防止内部网络受到外部攻击。它能够识别和阻止未经授权的访问，确保网络内部资源的安全。通过网络隔离和边界防护，可以对不同区域的设备和用户进行细粒度的访问控制。这意味着只有被授权的用户和设备才能访问特定的网络资源，从而减少安全风险。

5G LAN 使得工控网络稳定性和可靠性进一步提升。5G LAN 一张网络替代多张物理网络，便可简化网络架构，高效提升网络效率与产线可用性，从而降低组网成本和维护成本。不仅如此，5G LAN 技术的加持下深入工业互联网应用场景，支持外挂设备的即插即用、跨阈组网、双发选收等功能，解决了传统工业企业网络布线繁琐、网络调配难度大、网络适配灵活性差等问题。

（四）钢铁制造 5G LAN 网络安全智能感知应用案例

1、背景

在钢铁企业转向以质量型、差异化竞争为主的背景下，将 5G 技术、大数据、云计算、人工智能等先进技术与钢铁工业融合，在资源利用、节能减排、产品结构调整等方面，实现通过降本增效，来达到提高钢铁行业竞争力、培育钢铁行业增长新动力的目的。

钢铁企业的工业控制系统具有多个生产工艺流程混合、控制网络组网复杂、多种通信方式并存的问题，使得可以被黑客利用的漏洞大量存在。对于这样的工业 5G LAN 网络，需要根据实际情况，从不同角度和层次应用多种策略进行综合防护。

工控安全知识图谱是网络安全领域专用知识图谱，也是知识图谱应用于安全业务的重要工业尝试。当前，工业安全领域中存在大量的业务数据，通过了解钢铁行业工业网络建模需求以及应用需求，能够在工控网络态势感知、泛终端内生安全能力感知等场景进行应用，对 5G LAN 网络安全能力提供进一步的增强。

2、应用场景与需求

工业 5G LAN 网络产生的大量实时数据需要高效、准确的处理和分析，以支持安全态势感知。然而，目前的数据处理技术往往存在数据质量不高、处理效率不足等问题，难以满足实时性和准确性要求。因此，需要利用大数据、机器学习、人工智能等技术对网络的安全状况进行深度感知。

工业 5G LAN 网络主要的风险主要是来自于内网、终端层面，因此需要建立在生产工艺流程基础之上，结合网络流量、安全设备、主机及业务应用构建安全分析模型，感知网络威胁，实现通报预警，联防联控。基于安全知识图谱的事件风险画像、攻击路径调查、响应策略推荐，能够提供丰富的、具有安全语义的上下文，有效支撑动态事件的研判和策略部署，降低安全运营对专家经验与知识的依赖。

3、解决方案

某钢铁园区内建设的工业 5G LAN 网络过程中的打造的网络安全智能感知关键技术及应用的解决方案，覆盖了端、管、云、边下的应用场景的网络安全解决方案，实现了可信端、可监管、可控云、可防边的部署架构，具体网络安全场景包括：5G LAN 泛终端内生安全能力感知、切片流量安全检测、5G LAN 网络的用户行为分析、5G 安全编排与自动化运营能力开放等。

（1）5G LAN 泛终端内生安全能力感知技术

通过在 5G LAN 智能终端内部配置可信轻量级 SDK 软件，完成 5G LAN 泛终端的安全监测、内核级进程文件防护、数据采集、数据加密、异常分析和 5G LAN 泛终端大数据智能分析和态势感知等。利用数据驱动（基于算法）方法，把各种智能终端日志所描述行为作为多维向量，利用机器学习算法进行分析，根据分析结果来发现异常。

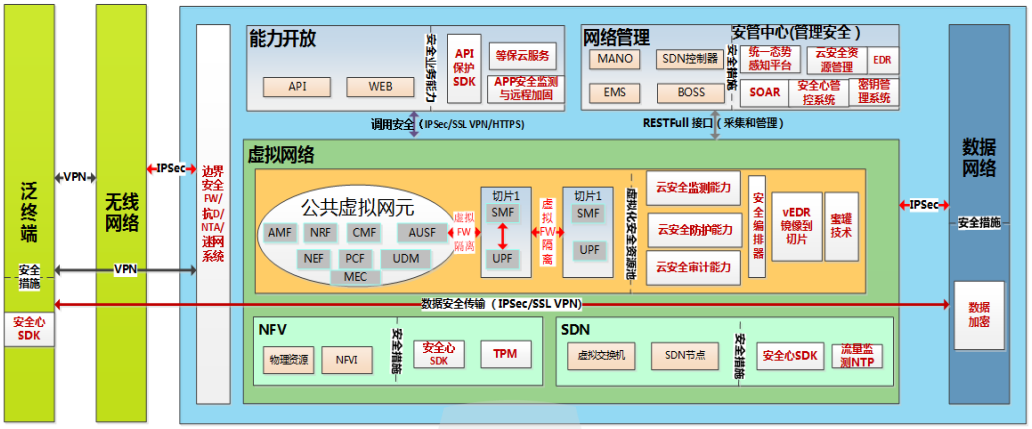

图 4.6 5G LAN 泛终端内生安全感知平台

（2）无人驾驶、实时监控和故障诊断等业务切片流量安全监测

通过对 5G LAN 网络切片中多种网络协议解析和监测泛终端设备异常流量威胁事件，详细清晰的记录系统发现的异常安全威胁日志，且保存 6 个月以上。采用旁路部署模式，监听异常流量，且支持多组逻辑隔离的切片网络流量分析检测。全流量多协议威胁检测基于主动和被动结合的检测机制。对僵尸网络、数据泄露、远程控制、DDOS 攻击等各类安全威胁进行实时深度检测、智能分析，感知并定位网络中存在的安全威胁，提供全面的检测能力。

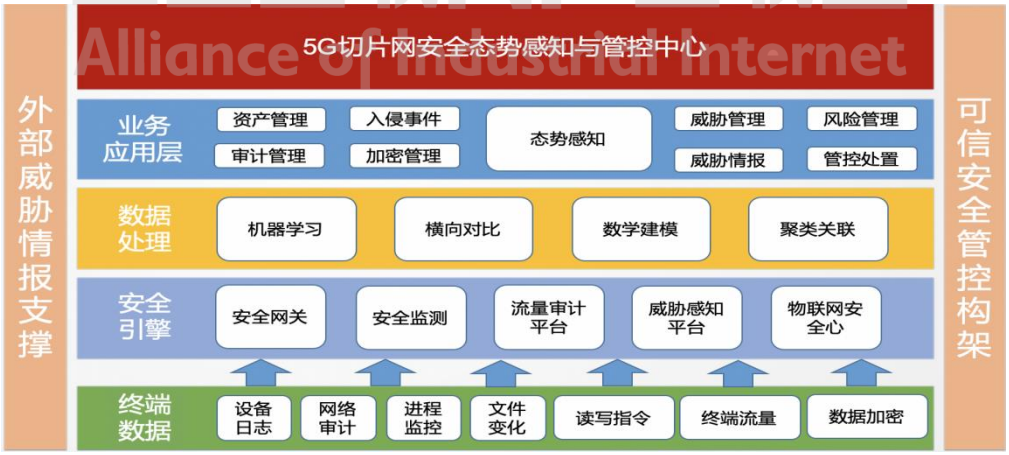

图 4.7 5G 切片流量检测平台

(3)5G LAN 网络下的用户行为异常检测

利用异常驱动（线索）方法，即将告警（APT、工业安全网关、工业防火墙等设备上的告警)和错误信息(系统件发送失败、登录失败、Web 访问错误、APP 访问失败等）作为线索，从中提取涉事主体的信息（IP 地址或域名），再从行为日志中找到涉事主体的通讯对端（IP 地址或域名），并进一步分析这些通讯对端的属性（数量、分布的连续性、公有私有、注册时间等等）以及它们通讯过程的情况。

利用数据驱动（基于算法）方法，即:把各种智能终端日志所描述行为作为多维向量，利用机器学习算法进行分析，根据分析结果来发现异常。

4、应用效果

建设一体化的钢铁 5G LAN 安全解决方案，协助推动了企业的网络安全建设，从关键信息基础设施的梳理，到持续的安全监测，及时的 0day 预警，快速的应急通报及处置工作，满足了《中华人民共和国网络安全法》和等级保护 2.0 以及中央网信办、国资委、公安部、工信部等国家部委对网络安全的监管要求。提供预见性安全维护，有助于减少 5G 泛智能终端的意外停机、改善生产运营动态。该方案帮助维护了一个智能制造架构网络安全的集中运营中心，以创建智能的、按优先级排列的自动+人工的维护作业顺序。同时，可以将检测潜在不良网络安全现象、未知威胁等提供潜在网络攻击警示。实时监测各种数据（如设备数据、检查数据、历史、日志文本等）通过分析和评估来预防运营问题的出现，可以有效提高预见性维护与修复性维护的

比率。通过减少意外停机时间，将资产可用率提高 3-5%。库存需求减少 10-20%。

该方案采用无监督的算法对数据进行智能判断，并在分析结果上打上标记。通过数据的聚能和态势感知形成该行业的安全大脑，具备自适应安全防御能力、学习能力、威胁情报的赋能能力和不同场景下的思考能力、管控能力。在工业互联网系统中，实现对工业控系统全方位、全天候的网络安全态势感知，及时发现各类网络安全风险等，赋能企业快速实现数字化、网络化、智能化转型。

五、未来展望

随着 5G LAN 在工业领域的规模化应用，围绕着工业生产安全运行的 5G LAN 相关安全技术、组织制度建设、产业链协同均会得到持续性的发展，具体如下：

5G 技术演进和新兴安全技术融合，将推动 5G LAN 在工业领域更大规模应用。随着 5G 技术的迭代更新，特别是 R18 等标准的冻结，5G LAN 的功能和性能将得到进一步的增强和完善。这将有助于推动 5G LAN 在不同行业和场景中的广泛应用。5G LAN 继承了 5G 网络的高安全性特点，通过加密与认证机制确保数据传输的安全性和完整性，结合区块链、人工智能等新兴技术，可实现更加严格的安全防护策略，提高网络安全的可靠性和效率。随着技术的不断进步、标准化进程的推进、应用领域的拓展以及安全性的提升，5G LAN 在工业领域的应用将发挥更加重要的作用，推动工业企业数字化转型和智能化发展。

5G LAN 在工业领域的应用使得工业网络融通，将重构工业企业组织管理机制。5G LAN 网络的大规模应用使得 IT 与 OT 网络深度融合，安全措施必须覆盖两类场景，才能实现对各种漏洞和风险的有效防控。在工业领域，IT 与 OT 隶属两个部门，在组织架构、制度管理、技术背景等方面存在居多差异，这些差异是工业制造企业实现网络安全协同防御面临的主要问题。5G LAN 网络在促进工业网络融通的同时，必然也会促进 IT 和 OT 相关工作人员的沟通协作。面对不可避免的变化，为了提升工厂网络安全相关管理效率和工作效率，工业企业

必然会重构相关组织管理机制，实现组织形式、管理制度、应急处置等方面的协调。

产业链各方协同推进 5G LAN 安全技术，共同构建工厂 5G LAN 安全生态。产业链各方应积极参与国际、国内标准，推动业界完成统一的 5G LAN 安全测评标准与流程，从源头强化 5G LAN 自身安全性。传统工业网络安全厂商、信息安全厂商、通信设备商等将以各自的优势技术为基础，以点及面，开展工业 5G LAN 网络安全实践，推广优秀安全方案。产业链上下将共同促进产业链、价值链、创新链的有机衔接，推动合作模式升级，践行合作机制落地，实现互惠互利、合作共赢，共同打造工业 5G LAN 的安全护城河。

电信运营商持续深耕工厂 5G LAN 网络运营，赋能工厂安全生产运营。电信运营商在工业 5G LAN 中发挥着基础网络提供者、技术标准化推动者、创新应用模式探索者、网络安全保障者和专业服务与支持提供者等多重作用。运营商作为维护网络信息安全的主力军，应继续发挥网络信息安全领域的独特优势，面对复杂严峻的网络安全环境形势，进一步加大 5G LAN 网络安全领域的建设力度，提供更加丰富的 5G LAN 安全技术服务，通过 5G LAN 安全技术，保障工业网络安全，筑牢工业生产安全可信的“安全堤坝”。

附录 A 缩略语

缩写	英文全称	中文名称
3GPP	3rd Generation Partnership Project	第三代合作伙伴计划
5G LAN	5G Local Area Network	5G 本地局域网
AAA	Authentication-Authorization-Accounting	鉴权、授权、计费
ACL	Access Control Lists	访问控制列表
AKA	Authentication and Key Agreement	认证和密钥协商
API	Application Programming Interface	应用程序接口
CPE	Customer Premises Equipment	客户终端设备
DDoS	Distributed Denial of Service	分布式拒绝服务
EAP	Extensible Authentication Protocol	可扩展认证协议
ECIES	Elliptic Curve Integrated Encryption Scheme	椭圆曲线加密算法
GRE	Generic Routing Protocol	通用路由封装
IAM	Identity and Access Management	身份识别与访问管理
IP	Internet Protocol	互联网协议
IPSec	Internet Protocol Security	互联网安全协议
MEC	Multi-access Edge Computing	多接入边缘计算
NFV	Network Functions Virtualization	网络功能虚拟化
NSSAI	Network Slice Selection Assistance Information	网络切片选择辅助信息
PSA	PDU Session Anchor	PDU 会话锚点
QoS	Quality of Service	服务质量
SDN	Software Defined Network	软件定义网络
SEPP	Security Edge Protection Proxy	安全边缘保护代理
SMF	Session Management Function	会话管理功能
SUCI	Subscription Concealed Identifier	用户隐藏标识

SUPI	Subscription Permanent Identifier	用户永久标识
TCP	Transmission Control Protocol	传输控制协议
TLS	Transport Layer Security	传输层安全协议
UE	User Equipment	用户设备
UPF	User Plane Function	用户面功能
VLAN	Virtual Local Area Network	虚拟局域网
VPN	Virtual Private Network	虚拟专用网
WAP	Wireless Application Protocol	无线应用协议

附录 B 参考文献

[1] 3GPP. Security architecture and procedures for 5G system. TS 33.501 v15.4.0. 2019

[2] 李静,李福昌,张涛.5G LAN 的应用需求与拓展研究[J].通信世界,2023(6):46-49.

[3] IMT-2020(5G)推进组.5G 零信任安全技术研究

[4] 施耐德电气,中国联通.5G+PLC 深度融合解决方案白皮书

[5] 国家工业信息安全发展研究中心.2022 年工业信息安全态势报告

[6] 刁敬源,曾子芸,刁兆坤, 等.5G LAN 技术分析及工业互联未来发展展望[J].通信世界,2023(6):42-45.

[7] 陈玉玺,赵鹏宇,李颖,等. 面向行业专网的 5G LAN 技术应用研究 [J].数字通信世界,2023(8):136-138.

[8] 陈福莉,蒋耀辉,汪超,等.5G LAN 应用及安全探讨[J]. 通信技术,2024,57(2):193-199.

[9] 刘霞,陈礼波,王运付,等. 工业物联网终端 5G LAN 组网方案研究[J].邮电设计技术,2024(1):83-87.

[10] 中国通信学会.5G 数据安全防护白皮书

[11] 工业互联网产业联盟.工业互联网典型安全解决方案案例汇编 （2022）

[12] 新华三.工业互联网技术白皮书（2022）

[13] 强奇, 武刚, 黄开枝, 等. 5G 安全技术研究与标准进展. 中国科学: 信息科学, 2021, 51: 347 - 366.

[14] 中通服咨询设计研究院.5G 网络安全白皮书

[15] 未来移动通信论坛.5G 信息安全白皮书

[16] IMT-2020(5G)推进组.5G 电力行业应用安全需求与架构白皮书

[17] 未来移动通信论坛.5G 信息安全白皮书

[18]工业和信息化部关于印发《工业控制系统网络安全防护指南》工信部网安〔2024〕14 号，工业和信息化部网站，2024,01.19.

[19]中智云物联网技术中心.内部参考技术资料[J].中智云物联网有限公司.SEC/eSIM，2024,03.11.

[20]王小军.基于国产密码的数字家庭安全解决方案[J].住建部.SAC/TC 426,2024,03.27.全国智标委广州.研究课题推进会.

[21]王钢.为数字家庭保驾护航.国产密码安全解决方案[J].住建部.SAC/TC 426，2024,06.20.张家港.全国智标委第三届第五次工作会议.