白皮书
2020-10

IMT-2020
IMT-2020 (5G) 推进组

面向行业的 5G 安全分级

目录

IMT-2020(5G)推进组于2013年2月由中国工业和信息化部、国家发展和改革委员会、科学技术部联合推动成立，组织架构基于原IMT-Advanced推进组，成员包括中国主要的运营商、制造商、高校和研究机构。推进组是聚合中国产学研用力量、推动中国第五代移动通信技术研究和开展国际交流与合作的主要平台。

引言

5G作为实现万物泛在互联、人机深度交互、智能引领变革的新型基础设施，应用场景从移动互联网拓展到工业互联网、车联网、医疗健康等更多领域，其价值将在垂直行业的应用中得到进一步体现。5G与行业深度融合发展的同时也带来新的安全风险和挑战，本白皮书致力于通过5G网络安全分级支撑垂直行业应对网络安全风险，指导垂直行业建设和部署符合自身需求的网络安全能力，提升垂直行业网络安全水平。

目前，5G安全架构和机制基本能满足行业通用安全需求，但面向垂直行业的差异化网络安全能力需求，还需进一步通过安全能力分级来实现。通过提供分级的5G安全能力，可支撑垂直行业网络遵从安全分级保护要求并实现行业5G网络快速部署。

5G承载行业应用发展概述

2.1 5G成为新基建之首，商用进程加速

当前，以数字化、网络化、智能化为特征的全球第四次工业革命孕育兴起。作为新一轮科技革命的核心通用技术，5G以其超大带宽、超广连接、超低时延三大特性，成为全球各国发展重点，对于推动经济转型、社会进步、民生改善具有重要意义。

国家和相关部委高度重视5G发展。2019年6月6日，工业和信息化部正式发放5G商用牌照；2020年3月，工业和信息化部印发《关于推动5G加快发展的通知》，要求全力加快5G网络建设部署、丰富应用场景、加大5G技术研发力度和着力构建5G安全保障体系；同月，国务院国有资产监督管理委员会明确提出加快以5G基建为首的七大“新基建”的政策要求，加快推动5G成为人工智能、大数据中心等其他新基建领域的信息联接平台，并于2020年“两会”期间被写入政府报告。

预计到2020年底，我国5G基站数量将超过60万个，覆盖全国所有地级以上城市。中国信通院2020年3月发布的《5G产业经济贡献》认为，预计2020至2025年，我国5G商用间接拉动的经济总产出约24.8万亿元。

2.2 5G驱动行业数字化，催生更多应用

自5G网络商用以来，远程教育、远程医疗、工业互联网、自动驾驶、智慧城市、智慧港口等5G场景应用如雨后春笋般层出不穷。特别是5G三大特性激发了新一轮规模创新，为各行各业带来新的商机，行业应用边界势必更加宽泛，另外，5G所带来的强大联接能力也是行业提升自身效率、进一步提升竞争力的契机，为行业数字化带来广阔的发展空间，加速推动各行各业的数字化转型。

与此同时，为全面加快企业数字化转型，国家和各部委也陆续出台了一系列政策。2019年9月起，发改委、工信部、交通部、农业部、商务部、卫健委等国家多部委发布20余项5G相关行业政策；全国多个省市也积极推动“百万企业上云”战略，“百行千业上5G”的探索成为时下各行业数字化转型的风潮。以5G+工业互联网为例，5G三大特性可有效满足工业业务苛刻的安全性、传输时延及可靠性要求，加快推动5G与工业互联网融合发展，将推动制造业从单点、局部的信息技术应用向数字化、网络化和智能化转变。

因此，5G网络与垂直行业业务的深度结合，势必会在扩大有效需求，优化投资结构、稳定增长速度、推动高质量发展等方面迸发出更多的化学反应，推进全产业链的深刻变革，从而有力支撑制

造强国、网络强国建设。

行业应用安全挑战及安全需求

3.1 行业应用安全挑战

3.1.1 垂直行业安全监管挑战

垂直行业高业务价值引发更多攻击风险，安全威胁以国家安全数据、商业机密等为目标，以操纵市场、取得战略优势，损害关键信息基础设施为出发点，由传统的个人黑客技术性单点攻击逐步向商业性、有组织的高级持续攻击转变。

面对严峻的行业安全形势，国家加强了对关键信息基础设施的监管。《网络安全法》第三十五条规定：关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。2020年4月，我国发布了《网络安全审查办法》，产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏，以及重要数据被窃取、泄露、毁损的风险成为审查重点，因此，为关键信息基础设施提供通信网络产品的设备商需要在产品设计、实现、运行、维护全生命周期构建可信设备能力，围绕应用场景，分析安全威胁和实施消减措施。

同时，在行业领域，业务数据通常涉及企业商业秘密、个人隐私等，一旦被非法获取、利用后，可能会对社会秩序、公共利益乃至国家安全带来严重损害，我国对于数据保护的意识和要求不断提升，即将出台《数据安全管理办法》。为了保障数据采集、传输、存储、处理、销毁全生命周期的安全，需要信息基础设施具有相应的安全能力。

3.1.2 行业安全需求差异化挑战

从信息安全三要素CIA（机密性、完整性和可用性）来看，应用各种通信技术的公共通信网络需要保障信息在网络中传输、交换和存储的信息的机密性、完整性，不被未经授权的篡改、泄露和破坏，同时，保障系统连续可靠地运行，不中断地提供通信服务。5G网络承载的行业应用，因业务需求的多样化，针对CIA三要素的安全策略也存在差异化需求，例如工业制造要求高可用性、数据不出园区，远程医疗要求高度的用户隐私数据保护，车联网要求匿名认证、防跟踪等。

3.1.3 新业务特征带来新安全挑战

在万物移动互联时代，5G 网络需要满足前所未有的联接场景需求，主要包括三大新业务场景：移

动增强宽带（eMBB）、超可靠低时延通信（URLLC）和大规模机器类型通信（mMTC）。新业务面临新的安全挑战：

- eMBB：该场景下的主要安全风险是超大流量对于现有网络安全防护手段形成挑战。由于5G数据速率较4G增长10倍以上，网络边缘数据流量将大幅提升，现有网络中部署的防火墙、入侵检测系统等安全设备在流量检测、链路覆盖、数据存储等方面将难以满足超大流量下的安全防护需求，传统安全边界设备面临较大挑战，边缘计算成为新的安全焦点。

- URLLC：该场景下的主要安全风险是低时延需求造成复杂安全机制部署受限。安全机制的部署，例如接入认证、数据传输安全保护、终端移动过程中切换、数据加解密等均会增加时延，过于复杂的安全机制不能满足低时延业务的要求。

- mMTC：该场景下的主要安全风险是泛在连接场景下的海量多样化终端易被攻击利用，对网络运行安全造成威胁。接入设备多、应用地域和设备供应商标准分散、业务种类多，大量功耗低、计算和存储资源有限的终端难以部署复杂的安全策略，一旦被攻击容易形成僵尸网络，将会成为攻击源，进而引发对用户应用和后台系统等的网络攻击，带来网络中断、系统瘫痪等安全风险。

3.2 行业安全需求

3.2.1 终端身份安全和访问授权

物联网终端安全能力普遍较低，如果合法终端身份被非法利用（如SIM卡被插拔），入侵物联网络设备或业务系统，将可能导致网络数据流量滥用、业务数据泄露、假冒或篡改，甚至可能被操控发起DDoS（分布式拒绝服务）攻击从而导致物联业务系统瘫痪。为防御终端身份盗用、伪造等威胁，需要：

- 终端设备内支持安全存储入网凭据。
- 终端设备接入网络时进行严格的双向访问认证。
- 基于用户注册业务的网络授权访问。
- 支持基于用户名/密码、SIM卡号、设备序列号或者MAC地址绑定认证、远程管理和异常告警等安全能力。

3.2.2 网络分域、安全隔离

5G网络面向千行百业，承载的业务类型多种多样。例如，承载各类电子政务应用时，有高机密性要求；承载工业生产网络时，有高可用要求；承载普通数据上网或者AR（增强现实）、VR（虚拟现实）娱乐类业务时，有QoS（服务质量）要求；而承载医疗业务时，要求数据不出医院。因此，服务于不同的业务类型，安全保障要求也不同，为保障网络安全，需要：

- 定义网络安全域，安全域间采用技术隔离手段，在信任边界实施严格的访问控制。
- 使用同一网络基础设施向具有不同安全需求的行业提供服务时，采用软件或物理等技术措施实现网络资源、数据传输通道的隔离。
- 对安全要求较高的场景，要求数据不出园区，保障数据传输通道和外界网络物理隔离。

3.2.3 数据机密性和完整性保护

行业应用对数据机密性和完整性提出更高要求。以工业场景为例，工业数据囊括了从客户需求到销售、订单、计划、研发、设计、工艺、制造等整个产品全生命周期的各类数据，这些数据具有的价值巨大，关系企业经营和生产安全，甚至关乎国家安全。5G网络作为承载工业应用的基础网络，应选择基于高强度的密码算法实施机密性和完整性保护：

- 无线接口：使用AES、ZUC或者Snow3G 128位以上的密码算法。
- 传输网络：使用IPSec/DTLS通道并选择128位安全强度以上的对称加密、非对称加密、摘要密码算法支持通信双方的身份认证和通道加密/完整性保护。
- 端到端加密：对于高度机密性防篡改要求的业务数据，使用高强度密码算法进行端到端加密和完整性保护。
- 抗量子算法：为防御使用量子计算破解对称或者非对称密钥算法可能导致的威胁，对特别重要的基础设施网络，采用抗量子算法。

3.2.4 无线接口通信保护

无线接口通信安全是保障垂直行业业务安全运行的重要一环，以工业场景为例，无线接口的开放性打破了原有工业网络通过物理边界保护生产网络的封闭性，为保障无线接口通信安全，需要：

- 防窃听、篡改：防御基于无线接口传输通道的数据嗅探、篡改等攻击，无线接口需支持信令面、数据面的加密和完整性保护。
- 无线接口防未授权无线设备（如伪基站）劫持：无线接口劫持可能导致合法终端接入非法网络，泄露敏感信息（身份信息、活动轨迹、上网凭据等），需要提供实时监测和检测定位伪基站能力。
- 防御无线接口(D)DoS攻击：在5G海量物联终端接入场景下，终端设备数量众多，在线时间长，漏洞更新周期长，易被攻击者利用发起(D)DoS攻击，需快速检测攻击行为、定位和排除攻击源。
- 无线接口抗干扰：高安全性要求的行业应用要求能够识别物理环境中未经授权的无线设备，报告未经授权试图接入或干扰控制系统的行为。另外，随着黑客能力的提升可能会演进出针对无线接口的新型攻击方式和形态，需要持续研究和增强5G无线接口攻击检测和防御技术。

3.2.5 隐私保护

5G网络中可能会传输大量敏感数据，例如用户生活轨迹、消费习惯、驾驶习惯、医疗数据等信息，这些信息比其他数据具有更高的价值，信息泄露带来的负面影响更大。5G网络应能在隐私数据的收集、传输、处理、存储、转移、销毁等过程中保证落实相关法律法规的要求。

3.2.6 网络韧性

垂直行业对业务的可用性和连续性也提出了更高的要求，比如，工业领域对可用性要求非常重视，要求工业系统能够承受一定规模的攻击并在被攻击时保持核心服务能力。随着垂直行业面临越来越多的复杂攻击，为了增强网络/系统安全性，抵御内外部攻击，对5G网络和网络设备提出了高可用要求，即网络韧性需求：

- 网络集中管理，上报安全告警、安全/操作日志支持审计等。
- 具备对未知威胁的主动检测和应急响应能力。
- 承载关键业务时，应具备态势感知和系统韧性能力。

3.2.7 网络设备安全可信

网络设备的安全可信是保障工控网络、远程医疗等业务高可用和连续性服务要求的重要基础。网络设备包括硬件设备、软件系统和应用程序等，面临近端攻击注入恶意代码、通过接口渗透实施非授权访问、窃取/篡改/破坏敏感数据或文件、针对网络设备的可用性攻击等一系列威胁。为了抵御以上威胁，网络设备需要：

- 保障设备本身及周围组网设施的物理安全，如配置电子门禁、配备烟雾、温度、红外传感器等。
- 保障系统、固件、应用软件包的完整性和来源合法性。
- 对关键设备文件提供机密性和完整性保护。
- 设置访问控制规则，对受控接口需实施重点保护。
- 接口协议健壮性保护，识别过滤异常报文、畸形报文。
- 高安全要求场景下，需要具备从硬件可信根开始构筑的安全可信链，保障从系统启动到动态运行的系统可信。

3.2.8 技术自主可控

国家重要基础设施网络是国家级黑客重点攻击的对象，需要加强自主可控技术规划，保障关键技术以及核心部件的自主可控。

3.2.9 产品生命周期安全

对于承载关键业务的基础网络，需要对设备商和服务供应商提出产品生命周期安全要求，例如建立完备的产品开发过程管理制度，在产品需求分析、功能设计、实施开发、测试验证及上线发布等环

节进行质量及安全控制以实现可信的软件开发过程，建立全生命周期全量软件管理，实现严格符合业界标准的第三方（含开源软件）软件管理和更新制度，确保端到端变更可追溯。

3.2.10 行业安全需求总结

根据上述对行业场景分析，行业安全需求可分为如下两大类：

- 基本需求：工作场景、安全保障目标与传统公众通信网络相同的安全需求，通过继承当前通信网络安全保障技术可满足。

- 行业网络高级安全需求：为应对新的业务场景、高资产价值带来的安全风险，在基本需求基础之上的安全需求，需提供更高保障的安全能力才能满足。

需求分类	基本需求	行业网络高级安全需求
终端身份安全和访问授权	终端身份安全存储、和网络进行双向认证	终端身份和设备绑定
网络分域、安全隔离	安全域间技术隔离	数据不出园区 不同安全等级业务数据隔离
数据机密性和完整性	通过密码算法保障业务数据传输和敏感数据存储的机密性和完整性	E2E 业务数据传输机密性、完整性保护
无线接口通信安全	无线接口数据的机密性、完整性	抗量子算法保障机密性、完整性
	防御非法网络劫持	保障网络免受无线电干扰
	检测和识别未经授权的无线设备	检测和防御无线接口（D）DOS 攻击
隐私保护	在隐私数据收集、传输、处理和存储、转移、销毁等过程中保证相关法律法规中隐私保护要求的落实	无线接口隐私保护、防跟踪
网络韧性和安全态势感知	网络集中管理，检测攻击后上报安全告警、安全/操作日志支持审计等	对 APT 攻击、未知威胁的防御和态势感知；对于有业务连续性要求的关键业务，在攻击发生时需保持核心业务的运行，以及其他业务的快速恢复
网络设备安全可信	物理安全、接口访问控制、软件数字签名和关键文件完整性、机密性保护	具备基于硬件可信根的安全可信链，保障从系统启动到动态运行的系统可信
技术自主可控	满足 3GPP 标准、国家通信标准和设备准入标准	在关系国家安全的网络中，需使用国密算法等自主可控技术保护数据和网络安全
产品生命周期安全	满足 3GPP 标准、国家通信标准和设备准入标准	关键基础设施通信网络产品在产品设计、实现、运行、运维全生命周期构建可信设备能力

面向垂直行业提供5G安全分级能力

4.1 5G安全分级目标

4.1.1 支撑行业网络的安全分级要求

无论是在国家监管层面还是垂直行业自身安全保障层面，相关法律法规和行业标准均对信息网络和系统定义了分级要求，例如等级保护2.0、电信网和互联网网络安全防护分级相关标准等。垂直行业网络的运营者应当按照相关分级要求，履行法律法规和行业标准中规定的安全保护义务，部署与之匹配的安全能力，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

“电信网和互联网安全防护体系”系列标准针对电信网和互联网网络安全防护体系中的网络和系统，结合各类业务系统特点，根据社会影响力、规模和服务范围、所提供服务的重要性三个相互独立的定级要素将网络/系统单元划分为5个安全等级，并提出了针对性的安全防护要求。

等级保护2.0面向网络基础设施、重要信息系统、云计算平台、大数据系统、物联网系统、工业控制系统、采用移动互联技术的系统等，对信息网络，信息系统、网络上的数据和信息，按照重要性和遭受损坏后的危害性分成五个安全保护等级，从第一级到五级，逐级增高，分别是用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。

另外，国际电工委员会（IEC）的工控系统安全标准（IEC 62443），也定义了分级安全策略，将安全级别分为4个等级，分别是S1（抵御偶然的攻击，非主动泄密）、S2（抵御简单的故意攻击）、S3（抵御简单的调用中等规模资源的故意攻击）和S4（抵御复杂的调用大规模资源的故意攻击，对应持续的国家层面攻击），并对每个级别定义特定的安全要求，例如S2级要求如果行业网络部署公钥基础设施(PKI)，ICT设备需要对接行业的PKI系统，S3、S4级要求有硬件可信根。5G-ACIA联盟在工业系统安全防护中引用了该系列标准。

需满足分级要求的垂直行业网络如果使用5G网络承载，在保证行业自身的信息系统网络满足要求时，也需要作为基础网的5G网络能够提供支撑行业满足相应分级要求的安全能力。

4.1.2 使能行业网络快速安全部署

5G网络作为行业系统的网络基础设施，引入了开放的无线接口和灵活的部署及组网方式，同时，5G网络运营商向行业应用提供服务也存在多种共享方式（切片、移动边缘计算（MEC）、基础设施独享等）。5G安全分级有助于运营商和行业用户加强理解、拉通安全需求、在安全语言和安全能力上对

齐，有助于用最佳性价比的安全方案满足行业要求，有助于给行业提供模板化的安全能力集合，促进基础网络和业务系统安全地快速集成部署。

4.2 面向垂直行业的5G安全分级定义

4.2.1 5G安全能力分级映射

垂直行业网络的部署、运行和管理需要根据相关法律法规和行业标准进行定级、备案，按照安全分级保护的技术要求（例如等级保护2.0、电信网和互联网网络安全防护分级相关标准）进行安全建设和安全运行维护，并接受相关部门的监管。5G网络作为垂直行业网络基础，需要支持行业满足安全分级保护要求，同时结合行业业务特定安全需求，提供充分的安全保障能力。

基于分级安全框架和策略，对5G安全能力划分等级，以便提供符合行业需求的5G安全能力。同时，根据《网络安全法》第三十一条，对关键信息基础设施实行重点保护。因此，面向行业的5G网络安全能力可分为5个级别的安全能力集合，与安全等级1—4级形成映射关系，如图1所示：

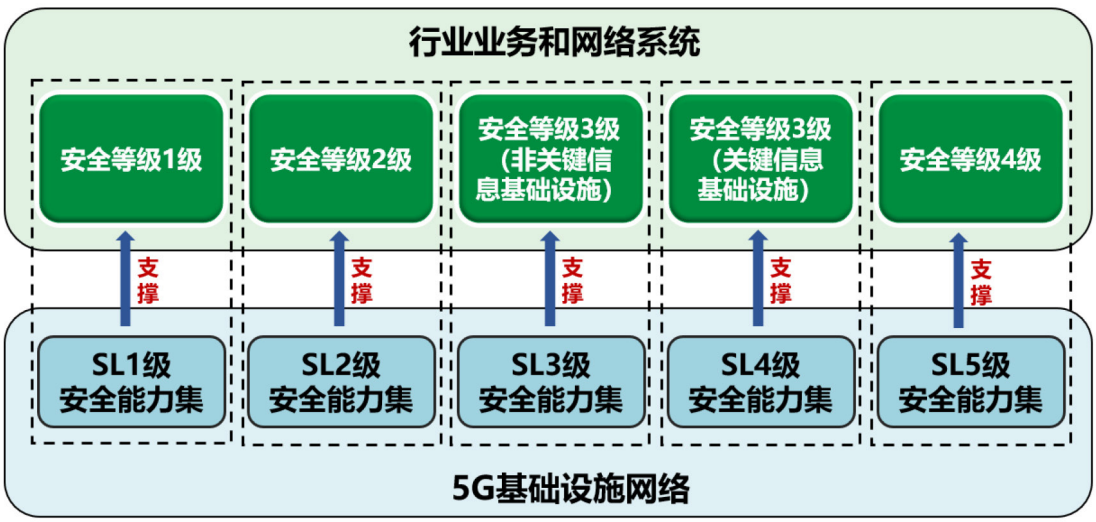

图1 5G网络安全能力分级映射

面向行业的5G承载网络的定级要求，建议遵循原则：作为基础设施的5G网络安全要求不低于承载的行业网络定级。例如对于定级为安全等级三级及以下的网络，可以通过提供5G SL3安全能力集承

载；定级为安全等级三级同时是关键信息基础设施网络，需要提供5G SL4安全能力集，定级为安全等级四级的行业网络，相应的是5G SL5安全能力集以满足其安全要求。

对于定级为安全等级三级以上的行业网络，包括三级网络（非关键信息基础设施）、三级网络（关键信息基础设施）和四级网络这三种网络，使用5G网络承载时在硬件安全、设备可信、密码安全、安全隔离、安全管理等方面支持提供更高级的安全保障能力。

4.2.2 5G安全能力分级策略

根据安全等级的分级安全设计要求，制定对行业5G网络安全能力集的分级策略，具体如下：

- 一级（SL1）：提供基本信息安全能力，具备初步的认证授权和访问控制措施，提供基本的安全入侵检测能力，采取多种方式保护系统和数据的信息安全属性，避免未经授权的访问、破坏信息完整性、系统可用性的攻击行为。

- 二级（SL2）：在一级基础上，增强安全事件监测和审计、以及根据监测审计结果进行处置的能力，增加数据保护基本能力。

- 三级（SL3）：在二级的基础上，增加覆盖产品全生命周期的基本安全要求，构建较为完善的集中管理系统和态势感知系统，支持未知威胁检测，具备以硬件可信根为基础的可信执行环境，采用包括高强度密码算法在内的增强技术措施，构建较为完备的可信、安全的5G安全体系，支撑行业在网络设备、网络传输及数据保护等多方面的CIA安全保障目标。

- 四级（SL4）：在三级的基础上，全面覆盖面向行业的5G安全能力需求，以高可用为目标，加强安全技术的有效性和可靠性，提升无线接口安全检测能力，增加支持行业可控的认证管理和访问权限控制，增加防近端攻击能力，提升安全威胁自动化检测和响应水平，确保在面对多种安全威胁和攻击的情形下，网络服务降级后仍可维持核心功能的运行。

- 五级（SL5）：在四级的基础上，强化技术自主可控要求，增加运行期应用动态可信和网络隔离强度要求，完善包括硬件安全在内的各项安全需求，全面保障关键行业网络安全目标达成，面临潜在的APT安全攻击，可通过对威胁实现动态关联感知、主动分析决策和联动响应，保障网络关键业务在攻击发生时仍然能够按照预期的方式工作，对上层行业系统提供连续网络服务。

5G安全能力分级模型

5.1 5G安全需求模型

通信行业标准定义5G网络通信安全、设备安全等要求，等级保护规定对行业应用网络系统的通用分级安全能力要求，垂直行业标准体现基于业务特点以及行业安全风险态势实施重点防护的安全原则和安全能力需求。

因此，在国家相关安全法律法规框架内，基于成熟的通信标准体系，综合考虑安全分级保护要求和行业特定安全需求，基于网络运行保障、生命周期保障、核心技术自主可控保障三个维度，将5G安全需求分为5G网络安全、产品开发和生命周期安全、技术自主可控三大类，其中5G网络安全根据信息系统需要具备的基础安全能力（CIA）、数据保护能力和面对攻击的业务保持/业务恢复能力细分为基础安全、数据安全和网络韧性，由此形成面向行业的5G安全能力需求模型，如图2所示。

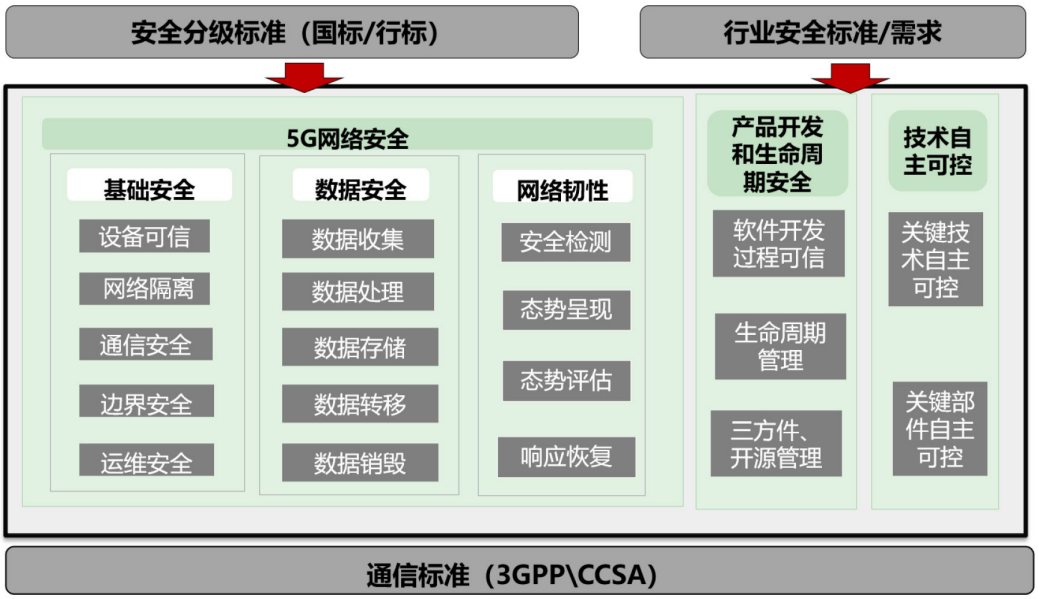

图2 5G网络安全需求模型

1　5G网络安全

（1）基础安全：以保障5G基础网络的机密性、完整性、可用性和可追溯性为安全目标，包括设备安全可信、不同网络信任域的隔离、通信的机密性和完整性保护、跨边界通信的访问控制机制、支持行为可追溯的网络运维安全等。

- 设备可信：主要包括硬件安全、系统可信保障和设备接口保护三个方面。硬件安全包括从硬件接口的安全防护、防近端攻击到独立硬件安全模块等多个层次的保障；系统可信保障包括基于硬件信任根的系统或软件的静态可信验证，应用程序执行环境的动态可信验证，以及关键文件的机密性和完整性保护；设备接口防护包括以最小权限原则设置访问控制策略和规则，增强接口协议健壮性保护等。

- 网络隔离：划分不同的网络区域，跨越边界的访问和数据流通过边界设备提供的受控接口进行通信，重要网络区域与其他网络区域之间采取可靠的技术隔离手段，特别的，基于共享基础设施多制式、多业务网络共部署场景下通过技术隔离手段防御跨制式、跨业务网络攻击能力，最高支持物理隔离。

- 通信安全：使用密码技术进行机密性、完整性验证，保障无线接口和传输网络通信安全，高安全要求场景下支持提供基于硬件密码模块对重要通信过程进行密码运算和密钥管理。

- 边界安全：网络边界根据访问控制策略设置访问控制规则，无线接口访问控制包括基于可信凭据的无线接口双向认证、切片认证或二次认证等多种能力支持行业需求。

- 运维安全：支持登录用户身份管理、权限管理、安全审计等，对于高安全要求行业提供用户权限管理（如，基于角色的访问控制）、多因素认证、管理分权分域等安全能力。

（2）数据安全：在5G时代，数据将成为物联网、人工智能等新兴技术的核心，数据的生产采集、处理和分析、分享和迁移等各个环节都在日臻完善的数据安全法律法规的框架保护之下。5G网络数据保护目标是在数据的收集、传输、处理和存储、转移、销毁等过程中保证相关法律法规的隐私保护要求的落实。

（3）网络韧性

- 安全检测：能够检测、分析和防御从外部、内部发起的主机、网络、无线接口攻击行为，主动防范各种已知威胁或进一步提供高级别的未知新型威胁检测。

- 态势呈现和评估：安全态势可视化，态势发展情况的预测评估和影响评估。

- 响应恢复：包括安全事件可视、事件响应、事件恢复，攻击溯源以及自适应动态协同防御能力，同时提供应急响应和业务恢复支持。对有高可用要求的行业提供韧性增强能力，支持系统在遭遇攻击时通过降级、恢复并适应攻击的方式保障关键任务达成，以保持在有定义的运行状态。

2　产品开发和生命周期安全

安全目标是从需求分析、设计、开发、发布、部署运行、升级维护等全生命周期过程保障产品的透明、可追溯、可审核。

- 软件开发过程可信：防御软件开发漏洞被攻击者利用，导致栈溢出、恶意注入等风险，提供安全设计/开发/测试流程保障。

- 生命周期管理：防御软件开发、发布、部署过程中被恶意注入后门、恶意功能，待上线后发起攻击。

- 三方件、开源管理：确保软件的网络安全、来源可靠、合法合规、修改和使用可追溯性、归一化、生命周期的漏洞与补丁管理、变更管理等风险可控。

3　技术自主可控

安全目标是面向高安行业要求保障核心技术、部件自主可控。

- 关键技术自主可控：密码算法、操作系统。

- 关键部件自主可控：处理器、安全芯片等。

基于安全需求模型，构建SL1−SL5的分级安全能力集。如表1所示。

表1　安全需求能力集

安全能力集			SL1	SL2	SL3	SL4	SL5
需求		子需求					
5G网络安全	基础安全	网络隔离	★	★	★★	★★★	★★★★
		运维安全	★	★★	★★★	★★★★	★★★★★
		通信安全	★	★	★★	★★★	★★★★
		边界安全	★	★★	★★★	★★★★	★★★★★
		设备可信	★	★★	★★★	★★★★	★★★★★
	数据安全	数据收集	★	★	★	★	★
		数据处理	---	★	★★	★★★	★★★
		数据存储	---	★	★	★★	★★
		数据转移	---	★	★★	★★★	★★★
		数据销毁	---	---	★	★★	★★
	网络韧性	安全检测	★	★★	★★★	★★★★	★★★★★
		态势呈现	---	---	★	★★	★★★
		态势评估	---	---	★	★★	★★★
		响应恢复	---	★	★★	★★★	★★★★
产品开发和生命周期安全		软件开发过程可信	---	---	★	★★	★★★
		生命周期管理	---	---	★	★★	★★★
		三方件、开源管理	---	---	★	★★	★★★
技术自主可控		关键技术自主可控	---	---	---	★	★★
		关键部件自主可控	---	---	---	★	★★

注：标识本级别不需要考虑需求，★的数目递增标识安全技术能力增强。

表中，纵向是安全需求，横向是基于每个级别安全目标，描述对于该需求的安全能力强度。

5.2 5G安全能力分域定义

5G终端从接入网络进入5G网络，通过5G网络的传输实现到因特网或者企业应用的端到端连接。

5G安全能力范围从终端通信模块出发，经过5G接入网、承载传输网到达5G核心网的通信基础网络，包括边缘计算（MEC）平台安全和边缘网元安全，但不含MEC平台上部署的应用软件。5G网络端到端安全分域架构如图3所示。

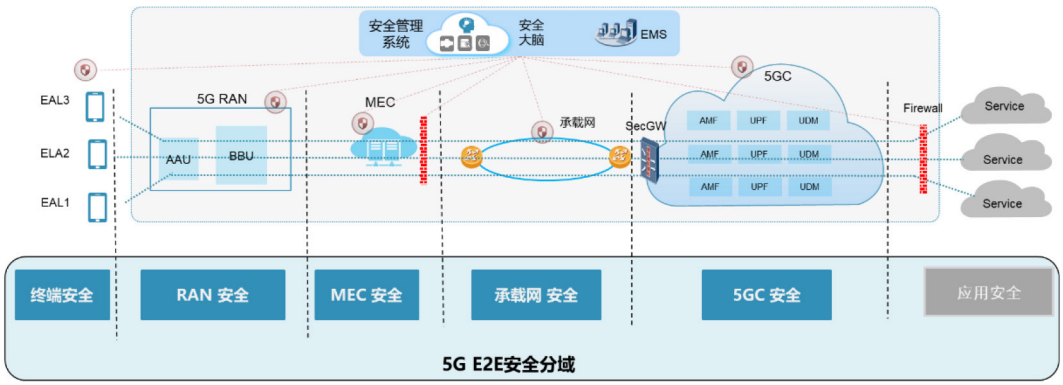

图3 5G网络端到端安全分域架构

图中，终端、5G接入网（RAN）、MEC、承载网、5G核心网的安全作为独立的五个域。以上五个域由于所处位置、业务能力不同，支撑行业网络安全分级要求需要提供的安全能力也有所不同。在构建5G安全分级能力集合时，需要分域依据安全分级保护框架进行定义。

5.3 行业5G网络分级分域能力集示例

5.3.1 终端安全

5G终端种类和形态丰富，包括面向个人用户的手机终端、VR/AR 终端，以及面向垂直行业的工控终端、车载终端、移动医疗终端和各种传感器等，同时数量众多、分布区域广，易成为不法攻击者的攻击目标，终端应在软硬件方面做好安全加固与安全防护，防御物理攻击、信息泄露或篡改以及非授权访问或恶意控制等安全风险。

鉴于5G终端面临的安全风险，综合考虑不同的5G终端在形态、系统架构存在的较大差异，企业在根据安全分级要求选择终端安全能力时可采用相应终端行业标准。

5.3.2 5G RAN安全

5G网络作为承载行业应用的基础网络，需要依据行业网络安全等级目标分析提供分级安全保障技术能力。由于无线网络域和有线网络的技术和架构区别显著，5G RAN作为无线管道，将终端的数据/信令从无线接口透明转发至网络侧，不涉及用户数据的处理，对外的接口包括：

- 通过无线接口和终端进行数据和信令交互
- 通过NG-C、NG-U接口和5GC/MEC交互信令、数据
- 通过管理接口和运维网元对接，接收配置数据，上报日志、告警、性能信息等

根据行业5G安全需求模型和能力分级策略，对承载行业应用的5G网RAN域的分级安全能力集进行定义，重点关注基础安全能力、网络韧性能力、产品开发及生命周期安全和技术自主可控。以下选取典型安全需求为例描述RAN域能力分级：

需求模型		子类	SL1	SL2（在SL1的基础上）	SL3（在SL2的基础上）	SL4（在SL3的基础上）	SL5（在SL4的基础上）
5G网络RAN域安全	基础安全	设备可信	系统程序可信验证、告警	可信验证上报	应用程序可信验证、支持可信执行环境	应用程序关键环节动态可信	应用程序所有执行环节动态可信
			公开接口安全防护	内部调测接口关闭	硬件可信根	防近端攻击	硬件密码模块
		网络隔离	边界接口受控	同SL1	通过边界设备访问核心网络	支持2B、2C网络技术隔离	支持2B、2C网络物理隔离
		通信安全	使用校验码支持的完整性	同SL1	基于密码算法的机密性/完整性；传输支持TLS/IPSEC	空口用户面全速率完整性保护	使用硬件密码模块保护密钥
		边界安全	---	---	网元间接口和管理通道双向安全认证、基站侧支持多协议层次的ACL报文过滤	基站支持使用802.1x接入网络认证	使用证书白名单校验增强访问控制
		运维安全	用户访问控制	权限分离、支持安全审计	强访问控制、基于RBAC的用户管理	多因素认证，管理分权分域	同SL4
	网络韧性	安全检测	主机检测（已知威胁）	网络检测（已知威胁）	未知威胁检测、空口DDOS检测&防御	空口伪基站检测&防御	空口防御DOS、干扰检测增强&防御
		响应恢复	---	安全事件可视化	安全事件响应、安全配置基线核查	安全事件恢复、攻击定位溯源及影响评估	自适应动态协同防御
技术自主可控		技术自主可控	---	---	---	算法自主可控（国密算法）	操作系统自主可控
产品开发和生命周期安全		生命周期安全	---	---	安全设计/开发/测试流程保障、配置管理、自动化构建	二进制级完整性、一致性	全量软件管理，双向可追溯

（1）基础安全

- 设备可信

设备可信验证能力根据安全防护等级的防护要求，SL1-5分别提供从系统引导程序、系统程序到应用程序的可信验证，提供从加载阶段的可信、关键环节动态可信到所有执行环节动态可信和动态关联的安全能力。

此外，从硬件可信维度，提供不同级别的安全能力保障：SL1支持公开接口安全防护，SL2支持内部调测接口关闭，SL3支持基于硬件可信根构建系统可信链，SL4提供防近端攻击的物理安全保障，SL5面向安全等级4级要求提供硬件密码模块能力。

- 网络隔离

SL1和SL2级满足安全分级要求实现边界访问受控，包括无线接口和陆地传输接口；SL3级RAN网元支持通过安全网关设备实现核心网网元间的安全隔离和访问控制；SL4级支持网络间技术隔离；SL5级提供多个网络之间的物理隔离（例如处理资源、传输通道物理隔离）。

- 通信安全

SL1和SL2级支持基于校验码的完整性验证，SL3支持基于密码算法保障无线接口和数据传输机密性、完整性和防御重放攻击，支持TLS/IPSec机制实现管理通道和回传通道安全，SL4支持无线接口用户面全速率完整性保护，SL5支持基于硬件密码模块的密钥保护。

- 边界安全

针对SL3级，N2/N3/Xn接口和管理面接口支持双向认证，同时基站支持过滤链路层、网络层、传输层的非法报文；针对SL4级，在基站接入网络前提供接入认证；针对SL5高安全级别，可在双向认证的基础上使用证书白名单校验增强访问控制。

- 运维安全

SL1基本能力支持用户访问控制，包括用户身份和权限管理、口令防暴力破解等，SL2支持安全审计和管理用户的权限分离，SL3基于强访问控制要求支持用户权限管理，SL4提供多因素认证和管理权限分权分域。

（2）网络韧性

- 安全检测

SL1支持面向已知威胁的主机检测，SL2支持面向已知威胁的网络检测，SL3要求支持面向未知威胁的主机、网络检测，提供(D)DoS检测和流量阻断（面向海量物联终端），SL4提供伪基站检测，SL5支持无线接口抗干扰、(D)DoS的增强检测和防御能力。另外，由于5G无线接口复杂性和攻击成本很高，攻击者需要具备蜂窝专业领域知识并借助专业工具才能实现攻击，因此，从SL3级开始提供无线接口入侵检测能力。

- 响应和恢复

响应和恢复作为态势感知能力的重要组成部分，SL2提供安全事件的集中管理和可视化，SL3增加了安全事件响应和面向行业的安全配置基线核查能力，SL4支持安全事件恢复、攻击定位溯源和影响评估，SL5级以动态关联感知能力为重点，实现自适应动态协同防御，保障系统能够承受中高强度攻击，支撑行业关键业务系统连续运行。

（3）产品开发和生命周期安全

从技术角度侧重对设备软件的生命周期可信要求，SL3提供配置管理、自动化构建、安全设计/开发/测试流程保障等能力，确保正确性、可重复性和高效性，SL4增强二进制一致性和完整性，提高防篡改能力，在SL5安全集合中实现全量的软件管理，包括开源和第三方件的管理策略和机制，支持端到端可追溯。

（4）技术自主可控

SL4级需支持使用国密算法对承载的行业数据进行机密性完整性保护，SL5级建议提供自主可控的操作系统、高强度国密算法。

5.3.3 5GC安全

（1）基础安全

- 网络隔离

SL3级提供不同网络切片共用同一个网元实例，切片内网元与多切片共享网元间部署虚拟防火墙实施访问控制；SL4级提供不同切片网络间的虚拟局域网（VLAN）/虚拟扩展局域网（VXLAN）技术隔离，可部署虚拟防火墙实施访问控制；SL5级提供不同切片网络间的物理隔离，可部署物理防火墙实施访问控制。

- 通信安全

针对SL3及以上级别，5G可提供行业用户的信令面、数据面数据加密性、完整性保护；针对SL4,5GC在SBA(服务化架构)下可通过TLS(传输层安全协议)实现网元之间传输层认证及信息传输保护，应用层引入IETF定义的OAuth 2.0授权框架，确保只有被授权的网络功能才有权访问提供服务的网络功能，提供切片认证或者二次认证能力；SL4级对于有安全要求的企业提供对接企业PKI的能力，实现企业对终端接入网络的可控要求。

- 边界安全

针对SL3及以上级别，核心网内部分网元提供VLAN或防火墙进行隔离，用于各网元间互访流量隔离，核心网网元与RAN的N2、N3接口传输网络将提供专网或IPSec传输通道，各网元间均要通过认证

实现相互访问；针对SL4及以上级别，在N6接口提供安全缓冲区（DMZ）、异构防火墙、抗DDoS、入侵检测系统（IDS）等安全防护。

- 运维安全

SL3基于强访问控制要求支持基于RBAC（基于角色的访问控制）的用户管理，SL4提供多因素认证和管理权限分权分域。

（2）数据保护

针对SL3，5G可提供行业用户的信令面、数据面数据加密性、完整性保护；针对SL4，5GC在SBA架构下可通过TLS协议实现网元之间传输层认证及信息传输保护；针对SL3及以上级别，提供切片选择辅助信息（NSSAI）的隐私保护。

（3）网络韧性

针对SL3及以上级别，可以为行业用户提供订购相应切片和切片服务；针对SL4及以上级别，可以为行业应用提供所管理切片资源、告警、性能和运行状态数据；针对SL4及以上级别，在N6接口提供DMZ、异构防火墙、抗DDoS、IDS等安全防护。

（4）产品生命周期安全

SL3提供配置管理、自动化构建、安全设计/开发/测试流程保障等能力，确保正确性，可重复性和高效性；SL4增强二进制一致性和完整性，提高防篡改能力；在SL5安全集合中实现全量的软件管理，包括开源和第三方件的管理策略和机制，支持E2E可追溯。

（5）技术自主可控

SL4级可提供使用国密算法对承载的行业数据进行机密性完整性保护；SL5级可提供高强度国密算法对承载的行业数据进行机密性完整性保护。

5.3.4 MEC安全

（1）基础安全

- 设备可信

针对SL4及以上级别，可提供可信的UPF、MEP等网元与运行环境。

- 网络隔离

针对SL3、SL4，服务器、交换机应支持管理、业务和存储三平面实施逻辑隔离；针对SL5，服务器、交换机应支持管理、业务和存储三平面实施物理隔离。

针对SL3，第三方应用间以及第三方应用与运营商自有应用间支持VLAN隔离，应与MEP(移动边缘计算平台)、UPF(用户面功能)使用防火墙实施隔离；针对SL4，第三方应用间支持VLAN隔离，应与

MEP、UPF使用防火墙实施隔离；针对SL5，第三方应用可与MEP、UPF位于不同的物理服务器。

- 通信安全

针对SL3及以上级别，可提供独享的UPF等设备，并在边界处进行网络隔离；提供不同业务类别(Traffic class)的流量控制和隔离能力，防止局部业务种类受到攻击影响所有业务；针对SL3及以上级别提供RAN至UPF的IPSec传输通道，UPF至行业用户侧可提供专线、L2TP/IPSec隧道传输。

- 边界安全

针对SL3及以上级别，在N6接口提供防火墙，实现边界安全防护，当短时间内有大量终端访问应用程序时，5G可在RAN、UPF访问流量异常情况下开启流控机制，防止终端向MEC发起攻击。

针对SL3，第三方应用支持与MEP、UPF使用虚拟防火墙实施隔离；针对SL4，第三方应用支持与MEP、UPF使用虚拟防火墙实施隔离；针对SL5，第三方应用支持与MEP、UPF使用物理防火墙实施隔离。

- 运维安全

SL3基于强访问控制要求支持基于RBAC的用户管理，SL4提供多因素认证和管理权限分权分域。

（2）数据保护

针对SL3及以上级别提供RAN至UPF的IPSec传输通道，UPF至行业用户侧可提供专线、L2TP/IPSec隧道传输；针对SL4及以上级别提供支持国密算法的用户数据完整性保护。

（3）网络韧性

针对SL3及以上级别，行业应用自有的APP可提供MEC运营管理平台对运行状态进行监控；针对SL3级以上级别可在MEC侧提供安全能力资源池，为行业应用提供防火墙、WAF(Web应用防火墙)、抗DDoS、IDS/IPS(入侵防御系统)等安全防护。

（4）产品生命周期安全

SL3提供配置管理、自动化构建、安全设计/开发/测试流程保障等能力，确保正确性，可重复和高效；SL4增强二进制一致性和完整性，提高防篡改能力；在SL5安全集合中实现全量的软件管理，包括开源和第三方件的管理策略和机制，支持端到端可追溯。

（5）技术自主可控

SL4级可提供使用国密算法对承载的行业数据进行机密性完整性保护；SL5级可提供高强度国密算法对承载的行业数据进行机密性完整性保护。

5.3.5 承载网络安全

（1）基础安全

- 网络隔离

承载网提供光纤、SPN(切片分组网)等方案构建端到端网络进行承载；针对SL3级别，可提供VPN(虚拟专用网络)隧道方式保证数据逻辑隔离传输，针对SL4级别，可提供FlexE(灵活以太网)方式保证数据物理隔离传输。

- 通信安全

提供光纤、SPN等方案构建端到端网络进行承载。

- 边界安全

提供防火墙、IDS等防护设备进行边界访问控制。

（2）数据保护

针对SL3级别，可提供VPN隧道方式保证数据逻辑隔离传输，针对SL4级别，可提供FlexE方式保证数据物理隔离传输。

行业应用5G网络安全分级能力建议

6.1 安全等级三级以上的行业系统

以运营商部署的5G网络为例，面向垂直行业安全等级三级要求分析如下：

（1）网络部署和通信设备安全要求：遵循安全通用技术要求实现对网络架构、接口（无线接口、陆地接口等）和通信过程等的安全防护，满足网络通信的CIA要求和集中安全管控要求。

（2）通信设备安全保障要求：网络通信设备经过NESAS（GSMA提出的网络设备安全保障计划）/SCAS(3GPP发布的安全保障规范)测评认证，实现安全分级要求的设备可信要求。

（3）运营商安全管理要求：具有安全信息管理、安全审计、安全事件响应机制，并部署态势感知系统实施主动检测、智能分析和安全态势可视化。

运营商5G网络基础设施满足如上要求，即覆盖了5G网络安全SL3级能力，能够直接支撑行业系统满足安全等级三级要求。

对于基于关键信息基础设施承载的安全等级三级的行业应用系统，建议考虑根据具体行业场景要求，参考5G网络安全SL4级安全能力集进行增强，例如对于工业互联高端制造业务，提供安全配置基线核查能力，避免安全相关配置被篡改后导致安全能力下降。

安全等级四级的行业业务系统，建议使用5G网络安全SL5级能力集进行保障，重点增强网络隔离、基于硬件的密码运算和密钥管理以及安全可信能力（系统动态可信验证、动态关联感知等），以便及时识别并有效阻断入侵。

6.2 安全等级一级和二级的行业系统

完善的安全保障能力在保障系统安全的同时也不可避免地带来开销增长，例如IPSec安全网关、PKI等基础设施的部署，高强度密码算法要求的计算能力和功耗提升，物理隔离要求的资源开销。针对某些物联场景没有强安全管控要求的业务系统（安全等级一级和二级网络），需要考虑业务属性要求和安全能力的平衡，运营商网络对其进行承载时，可以对安全能力进行裁剪，使用SL1或者SL2级能力集实现供给，例如，降低隔离的要求，使用资源共享策略；物联终端（不涉及自然人信息）在无线接口不进行SUPI/SUCI的隐私保护；不开启无线接口数据面完整性保护；面向低功耗物联网数据传输的轻量化密码算法等。

6.3 和现有安全认证标准的协同（NESAS/SCAS）

GSMA提出的NESAS统一了通信设备的安全能力基线，对于将5G设备的安全能力统一提升到高安全水平有非常重要的意义，在面向行业的5G安全分级体系中，中高级的安全等级（SL3级以上）的测评可以直接参考和引用NESAS/SCAS认证。

结束语

5G作为“新基建”的领跑基础设施，将驱动行业加快数字化转型。而保障5G行业网络的安全需要运营商、垂直行业和设备提供商协同合作共建安全生态，遵从安全分级保护相关规范对行业系统的安全要求，构建覆盖全面、分级分域的5G行业安全分级能力模型，面向行业提供分级的5G安全能力集和建立测评基线，贯穿行业5G网络建设、部署和运行的全生命周期，应对行业安全挑战，保障安全建设、安全运行、安全管理，为5G+行业的结合创造更大的价值保驾护航。

主要贡献单位

本白皮书起草单位：中国信息通信研究院、中国移动通信集团公司、华为技术有限公司、上海飞机制造有限公司

本白皮书起草人：杨红梅、吴君怡、焦杨、王晓晴、吴荣、张夕夜、汪顺利、陈智超

联系方式
电话：+86-10-62300155
邮箱：imt2020@caict.ac.cn