



5G 安全知识库

IMT-2020(5G)推进组

中国信息通信研究院

2021 年 12 月

前 言

5G 是新一代科技革命和产业变革的代表性、引领性技术，是实现万物互联的关键信息基础设施、经济社会转型升级的重要驱动力。5G 商用两年来，在产业界各方共同努力下，5G 发展成效显著，技术产业能力不断提升，网络和用户规模全球领先，应用探索日益活跃，涌现了大批优秀案例，实现了从 0 到 1 的突破，我国已经迈入 5G 融合应用规模化发展的关键时期。

5G 融合应用在造福社会、造福人民的同时，也引发了新的网络安全风险。中国国家主席在第二届世界互联网大会上指出，维护网络安全是国际社会的共同责任。国际社会应该在相互尊重、相互信任的基础上，加强对话合作，共同构建和平、安全、开放、合作的网络空间。5G 安全是全球面临的共同问题，更需要倡导开放合作的网络安全理念，客观看待和应对 5G 安全风险，深化合作，增进互信，共同提高 5G 安全保障水平。

随着 5G 技术、产业、应用迈入无经验可借鉴的“无人区”，5G 与垂直领域深度融合引发的安全风险备受瞩目，IT、CT、OT 安全问题相互交织，构建与 5G 应用发展相适应的安全保障体系成为迫切需要。2021 年 7 月，工信部联合网信办、发改委等 9 部门印发《5G 应用“扬帆”行动计划（2021-2023 年）》，提出加强 5G 应用安全风险评估，开展 5G 应用安全示范推广，提升 5G 应用安全评测认证能力，强化 5G 应用安全供给支撑服务，计划到 2023 年底，打造 10-20 个 5G 应用安全创新示范中心，树立 3-5 个区域示范标杆。《5G 安全知识库》在 5G 应用“扬帆”发展的关键阶段发布，凝聚了电信行业关于 5G 网络安全建设的最佳实践经验，探索提出 5G+行业应用

安全最佳实践方案，将有力促进形成全行业共识。

《5G 安全知识库》梳理总结了 5G 终端、接入网、核心网、MEC、切片、数据、应用等安全最佳实践经验，制定面向 5G 网络基础设施和典型行业应用的最优安全措施集，并提出面向运营商、设备商、垂直行业等不同主体的 5G 安全措施落地部署方式，旨在成为全行业的 5G 安全最佳实践综合性技术指导文件，从 5G 网络和应用两个维度促进全行业在 5G 安全需求、安全能力和安全措施等方面形成共识，共同保障 5G 网络和应用安全、可靠、高质量发展。

目 录

1 引言	1
1.1 5G 网络简介	1
1.2 5G 网络安全特点	2
1.3 5G 应用安全特点	4
2 国内外相关情况简介	5
2.1 欧盟 5G 安全风险评估及工具箱	5
2.2 美国 NIST 5G 安全实践指南	6
2.3 GSMA 网络设备安全保障框架	6
2.4 国内相关工作	8
3 5G 网络安全知识库	10
3.1 5G 网络安全范围	10
3.2 面向的 5G 资产	11
3.3 描述方式	12
3.4 描述内容	13
4 5G 应用安全知识库	14
4.1 5G 融合应用安全特点	14
4.1.1 5G 融合应用安全需求	14
4.1.2 行业应用安全需求与 5G 安全能力的映射	14
4.2 面向行业的 5G 安全原子能力集	16
4.2.1 SeCAP-1 端到端网络切片隔离能力	16
4.2.2 SeCAP-2 网络边界安全防护能力	18
4.2.3 SeCAP-3 增强的终端接入认证能力	19
4.2.4 SeCAP-4 开放的网络管理和安全管控能力	20
4.2.5 SeCAP-5 边缘/本地园区的数据安全防护能力	22
4.2.6 SeCAP-6 面向行业应用的安全监测能力	23
4.2.7 SeCAP-7 基于蜜罐技术的 5G 安全防护能力	24
4.2.8 SeCAP-8 服务于多租户的虚拟专网能力	25
4.2.9 SeCAP-9 面向行业应用的 5G 安全测评能力	26

4.3 5G 应用安全最佳实践模板	27
4.3.1 ST-IIot 5G+工业互联网安全模板	27
4.3.2 ST-grid 5G+电力安全模板	29
4.3.3 ST-mine 5G+矿山安全模板	30
4.3.4 ST-port 5G+港口安全模板	31
4.3.5 ST-city 5G+智慧城市安全模板	33
4.3.6 ST-hospital 5G+医疗安全模板	34
4.3.7 ST-education 5G+教育安全模板	35
5 安全知识库使用方法	37
5.1 面向运营商、设备商的 5G 网络安全知识库使用方法	37
5.2 面向运营商、垂直行业的 5G 应用安全知识库使用方法	38
6 总结及展望	40
7 缩略语	42
附录 A: 5G 网络安全知识库措施	49
A.1 终端安全 (Mobile Terminal, MT)	49
A.1.1 MT-1 终端与 5G 网络数据和信令保护	49
A.1.2 MT-2 用户凭证的安全保护	50
A.1.3 MT-3 终端接入认证	51
A.1.4 MT-4 终端访问限制	52
A.2 接入网安全 (Radio Network, RN)	53
A.2.1 RN-1 基站用户数据和信令保护	53
A.2.2 RN-2 伪基站检测及防护	54
A.2.3 RN-3 基站可用性保护	55
A.2.4 RN-4 降低无线电干扰风险	56
A.2.5 RN-5 基站物理安全保护	57
A.3 多接入边缘计算安全 (Multi-access Edge Computing, MEC)	58
A.3.1 MEC-1 物理环境安全防护	58
A.3.2 MEC-2 组网安全防护	59
A.3.3 MEC-3 基础设施安全防护	61

A. 3. 4 MEC-4 虚拟化安全防护	64
A. 3. 5 MEC-5 边缘计算平台安全防护	66
A. 3. 6 MEC-6 应用安全防护	68
A. 3. 7 MEC-7 能力开放安全防护	69
A. 3. 8 MEC-8 通信安全防护	70
A. 3. 9 MEC-9 管理运维安全	71
A. 3. 10 MEC-10 数据安全防护	72
A. 4 核心网安全 (Core Network, CN)	74
A. 4. 1 CN-1 核心网资源可用性保护	74
A. 4. 2 CN-2 5GC NEF 安全保护	75
A. 4. 3 CN-3 核心网流量保护	76
A. 4. 4 CN-4 核心网内外边界隔离	77
A. 4. 5 CN-5 核心网网元合法身份保障	78
A. 4. 6 CN-6 虚拟化环境保护	79
A. 4. 7 CN-7 用户标识保护	80
A. 4. 8 CN-8 漫游安全	80
A. 5 网络切片安全 (Network Slice, NS)	81
A. 5. 1 NS-1 终端接入切片安全	81
A. 5. 2 NS-2 切片网络隔离	82
A. 5. 3 NS-3 切片数据隔离	83
A. 5. 4 NS-4 切片管理安全	84
A. 6 安全管理 (Security Management, SM)	85
A. 6. 1 SM-1 安全管理和编排	85
A. 6. 2 SM-2 安全可控	86
A. 6. 3 SM-4 人员管理	87
A. 6. 4 SM-4 安全审计	88
A. 7 运维管理 (Operation and Management, OM)	88
A. 7. 1 OM-1 5GC 安全运维	88
A. 7. 2 OM-2 云基础设施主机运维	89

A. 7. 3 OM-3 云基础设施虚拟化层运维.....	90
A. 7. 4 OM-4 云基础设施 PIM 运维.....	91
A. 7. 5 OM-5 云基础设施 MANO 运维.....	92
A. 7. 6 OM-6 云基础设施 SDN 运维.....	94
A. 7. 7 OM-7 安全应急响应.....	95
A. 8 数据安全 (Data, DAT)	96
A. 8. 1 DAT-1 数据识别与管理.....	96
A. 8. 2 DAT-2 数据安全防护.....	97
A. 8. 3 DAT-3 数据安全监测.....	98
致 谢.....	100

1 引言

1.1 5G 网络简介

2015 年，国际电信联盟（ITU）发布了《IMT 愿景：5G 架构和总体目标》，定义了增强移动宽带（eMBB）、超高可靠低时延（uRLLC）、海量机器类型通信（mMTC）三大应用场景，以及峰值速率、流量密度等八大关键性能指标。与 4G 相比，5G 将提供至少十倍于 4G 的峰值速率、毫秒级的传输时延和每平方公里百万级的连接能力。

5G 网络是一个复杂的组合体，传统移动通信网的结构主要分为接入网、传输网和核心网，核心网之后就是骨干网。5G 网络由于引入网络功能虚拟化、软件定义网络、多接入边缘计算等新技术，网络形态相比 4G 更加复杂。在网络参与主体上，除传统通信设备厂商、基础电信企业外，5G 时代由于新技术的引入，云、大数据、互联网数据中心等厂商加入到 5G 网络组成各个环节，多领域垂直行业主体也深度参与 5G 融合应用的发展。

中国 5G 正式商用近两年以来，在技术标准、网络建设、产业发展等方面已取得了世界领先的发展成就，5G 应用也实现了从“0”到“1”的突破，展现出了庞大的潜在市场空间和助力经济社会创新发展的巨大潜能。随着中国进入 5G 应用规模化发展的关键时期，5G 技术、产业、应用迈入无经验可借鉴的“无人区”，5G 与垂直领域深度融合引发的安全风险备受瞩目，IT（信息技术）、CT（通信技术）、OT（运营技术）安全问题相互交织，构建与 5G 应用发展相适应的安全保障体系，制定符合我国 5G 网络建设和应用发展特点的、指引全行业 5G 网络和应用安全最佳实践的技术文件成为迫切需要。

1.2 5G 网络安全特点

第五代通信（5G）是实现人、机、物互联的新型信息基础设施和经济社会数字化转型的重要驱动力量。5G 安全是 5G 高质量发展的重要基础和坚实保障，做好 5G 安全工作，需要客观认识 5G 安全特点，积极应对 5G 安全风险挑战。

（1）国际标准定义了增强的 5G 安全标准

5G 网络整体架构延续 2/3/4G 通信网络特征，仍采用接入层、核心网层和应用层三层架构，但在核心网层引入网络功能虚拟化、网络切片、边缘计算、服务化架构、网络能力开放等新技术，网络架构有了重大变化，比 4G 具有更高的性能指标，支持更多样化的业务场景。与网络演进相适应的，5G 网络安全也不断演进和增强。在继承 4G 网络分层分域的安全架构的基础上，3GPP R15 版本定义了比 4G 更强的安全能力：一是新增服务域安全，采用完善的注册、发现、授权安全机制及安全协议来保障 5G 服务化架构安全。二是采用统一认证框架，能够融合不同制式的多种接入认证方式，保障异构网络切换时认证流程的连续性。三是增强数据隐私保护，使用加密方式传送用户身份标识，支持用户面数据完整性保护，以防范攻击者利用空中接口明文传送用户身份标识来非法追踪用户的位置和信息，以及用户面数据被篡改。四是增强网间漫游安全，提供了网络运营商网间信令的端到端保护，防范外界获取运营商网间的敏感数据。

R16 和 R17 阶段对已有的安全基础架构进行了进一步优化，一方面是提供增强的安全能力，例如定义了 SBA 架构服务增强安全机制，包含更细粒度的网元间授权机制、更强的运营商间的用户面数据传输保护等，以保障核心网内部信令面及用户面数据传输安全。此外，3GPP 还将 5G SA 网络的用户面完整性保护机制引入到 5G

NSA 网络以及 4G 网络中，以进一步增强空口安全。另一方面是使能垂直行业安全。例如支持 IoT 设备小数据传输安全、支持 uRLLC 的冗余会话传输安全、支持切片的认证和授权、支持多种私网形态的灵活认证，以满足不同行业的多样性安全需求，并向第三方开放 3GPP 安全能力。

（2）5G 网络发展仍面临一定的安全挑战

5G 新技术、新应用的发展，带来了新的安全风险挑战，需要以发展、系统、客观、合作的理念看待，以实现 5G 安全与发展的协同推进。2020 年 2 月，中国 IMT-2020(5G)推进组编制发布《5G 安全报告》，对 5G 安全挑战进行了梳理和分析：

在 5G 关键技术方面，5G 由于引入虚拟化、网络切片、边缘计算等新技术带来诸多安全挑战：网络功能虚拟化和服务化架构技术使得原有网络中基于功能网元进行边界防护的方式不再适用，且其底层实现多使用开源软件，出现安全漏洞的可能性加大；网络切片基于共享硬件资源，在没有采取适当安全隔离机制情况下，低防护能力切片易成为攻击其他切片的跳板；边缘计算在网络边缘、靠近用户的位置上提供信息服务和计算能力，由于其设施通常会暴露在不安全环境中，受性能成本、部署灵活性等多种因素制约，易带来接入认证授权、安全防护等多方面安全风险；网络能力开放采用互联网通用协议，与之前相对较为封闭的通信网络相比，易将互联网现有的各类网络攻击风险引入 5G 网络。

在 5G 典型场景方面，其安全风险与融合应用行业和业务场景紧密结合：增强宽带（eMBB）场景超大流量、超高速率的特性使得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、链路覆盖等方面的安全防护能力面临较大挑战；超高可靠低时延

（uRLLC）场景需要提供高可靠低时延的服务质量保障，给业务接入认证、数据传输安全保护等环节安全机制部署带来挑战；海量机器类通信（mMTC）场景下接入终端数量庞大，同时接入给网络带来运行风险，且功耗低、计算和存储资源有限等情况，使得较强安全策略难以部署。从长远来看，各类 5G 应用将在网络规模部署后逐步涌现，其安全风险与垂直领域自身特点高度相关，需分行业、分场景结合 5G 垂直领域各自特点，细化安全措施。

1.3 5G 应用安全特点

5G 基于全新的架构，使传统的人与人通信延伸覆盖到人与物、物与物之间智能互联，应用场景从互联网拓展到工业互联网、车联网、物联网等更多领域。5G 为垂直行业带来了更大带宽、更低时延、更多接入的通信技术能力，将会深度与垂直行业业务融合，5G 行业应用面临以下安全需求：

（1）业务开放安全需求：一是垂直行业终端、业务系统等接入 5G 环境，增大了终端、业务系统的暴露风险，使其面临的攻击面更广；二是在垂直行业企业侧部署 MEC，运营商 MEC 平台上承载多个垂直行业应用，企业与运营商间的安全界限变得模糊。

（2）5G 新技术安全需求：5G 中使用了虚拟化、网络切片、MEC 等新技术，大量使用虚拟化等 IT 技术、互联网通用协议，进一步将互联网已有的安全风险引入到 5G 网络，导致业务也面临安全风险。

（3）数据安全需求：垂直行业业务数据通过公共 5G 网络环境传输，行业对自身的业务数据控制能力减弱，可能会带来数据泄露风险。

（4）安全运维管理需求：将原本较封闭的企业网络将变得较为

开放，且引入了大量新技术和新运维对象，对安全管理、运维管理都带来新的安全风险和挑战。

5G 网络与垂直行业深度融合的特点，导致 5G 一旦出现安全问题不仅会影响人和人之间的通信，还将会影响到各行各业，有些场景甚至可能威胁到人们的生命财产安全乃至国家安全。全行业应树立正确的网络安全观，统一 5G 安全认识，共同建设满足监管要求的安全可靠 5G 网络，打造 5G 安全管理与运营体系，构建覆盖端到端的 5G 安全测评能力，提供安全有保障的能力及服务，全面提升 5G 安全水平。

2 国内外相关情况简介

2.1 欧盟 5G 安全风险评估及工具箱

欧盟委员会于 2019 年 3 月 26 日通过了《5G 网络安全建议》，呼吁欧盟成员国根据各国需求和特点，开展 5G 网络基础设施风险评估并审查各国安全措施。欧盟网络安全局（ENISA）于 2019 年 10 月发布了《欧盟 5G 网络安全风险评估》报告详细分析了欧盟成员国可能面临的 5G 安全风险，为成员国制定管理措施、网络部署、运营维护和采购 5G 基础设施提供重要指导和参考。紧接着，ENISA 于 2019 年 11 月发布了《5G 网络安全图谱》，针对网络资产及其风险识别等技术进行详细分析，并作为工具箱的实施参考。

2020 年 1 月 29 日，欧盟网络信息安全合作组（NIS CG）发布了《欧盟 5G 网络安全风险消减措施工具箱》（以下简称工具箱），为欧盟和各成员国实施 5G 网络安全风险消减措施提供了指导和依据。工具箱提出了 8 项战略措施、11 项技术措施和 10 项支撑行动，明确了各成员国具体实施风险消减措施的流程和方式。其中战略措施用于增加监管机构审查网络采购和部署情况的监管权力的措施，以及

应对与非技术漏洞相关的风险的具体措施，技术措施用于提升 5G 网络和设备安全，具体包括网络安全基线措施、5G 相关措施、有关供应商流程及设备认证、韧性和可持续性；支撑行动从审查或制定最佳实践、支持 5G 标准化工作、制定安全措施实施指导意见、加强信息共享机制等方面，协助战略与技术措施的执行，以便风险消减措施有效落地。工具箱用于解决包括与非技术因素风险在内的所有已评估出的风险，对欧盟整个单一市场和欧盟的技术主权具有战略重要性。

为了促进工具箱的落实，基于欧盟电子通信准则（EECC），欧盟于 2020 年 12 月发布了《EECC 安全措施指南》和《5G 补充安全措施实施指南》，促进成员国在 5G 网络建设中立法落实工具箱措施的实施。

2.2 美国 NIST 5G 安全实践指南

2021 年 2 月，美国国家标准与技术研究院（NIST）发布《5G 网络安全实践指南》初步草案。这是 SP 1800-33 系列三册中的第一册，旨在定义底层基础设施、技术架构和组件等安全属性，利用现有网络安全产品、解决方案以及 NIST 其他系列网络安全标准指南，构建整体性的 5G 网络安全保障能力。目前 5G 网络安全实践指南(草案)处于设计和开发解决方案的早期阶段，随着 NIST 相关项目的进行，将对草案逐步更新，并将发布其他册以供行业参考。该实践指南旨在帮助使用 5G 网络运营商、设备供应商等参与者提升安全能力，对电信和公共安全也有较高参考价值。

2.3 GSMA 网络设备安全保障框架

为促进产业对网络设备的安全性达成共识，满足通信领域利益相关方在 5G 时代对安全评估的诉求，全球移动通信系统协会

(GSMA)联合第三代合作伙伴计划(3GPP)共同发布网络设备安全保障计划 (NESAS)，旨在制定业界认同的通用安全基线，推进通信领域全球产业界的安全合作互信，联合各国运营商、设备商等产业链利益相关方共同推进 5G 安全建设。NESAS 提供了统一、有效的通信行业网络安全评估标准，为运营商、设备商、政府监管机构、应用服务提供商等利益相关方保障 5G 网络安全提供了有价值的参考。

表 2.1 GSMA NESAS 标准文档体系

类别	标准	内容
GSMA FS 系列	FS.13	NESAS 总体概述
	FS.14	检测实验室认证需求及流程
	FS.15	设备商开发及产品全生命周期审计方法
	FS.16	设备商开发及产品全生命周期审计要求
3GPP SCAS 系列	TR 33.805	网络产品安全保障方法研究与选择
	TR 33.916	网络产品安全保障方法论
	TR 33.926	3GPP 网元产品威胁和重要资产
	TS 33.511	5G 基站 gNB 安全保障规范
	TS 33.512	AMF 网元（接入和移动性管理功能）安全保障规范
	TS 33.513	UPF 网元（用户面功能）安全保障规范
	TS 33.514	UDM 网元（统一数据管理功能）安全保障规范
	TS 33.515	SMF 网元（会话管理功能）安全保障规范
	TS 33.516	AUSF 网元（鉴权服务功能）安全保障规范
	TS 33.517	SEPP 网元（安全边缘保护代理功能）安全保障规范
	TS 33.518	NRF 网元（网络存储功能）安全保障规范
	TS 33.519	NEF 网元（网络开放功能）安全保障规范
	TS 33.520	N3IWF 网元（非 3GPP 互通功能）安全保障规范
	TS 33.521	NWDAF 网元（网络数据分析功能）安全保障规范
	TS 33.522	SCP 网元（服务通信代理功能）安全保障规范
	TS 33.326	NSSAAF 网元（网络切片特定认证和授权功能）安全保障规范
	TR 33.818	虚拟化网络产品安全保障方法和安全保障规范标准

GSMA NESAS 分为产品研发流程审计和 SCAS 产品安全功能测试，其中 NESAS 研发流程审计包括 4 个标准（见表 2.1）。SCAS 安全保障规范是 3GPP 推出的电信产品的安全要求和测试用例，分析

5G 网元的资产组成、威胁及相对应的保障措施，目前已有 4 项研究报告和 14 个技术规范（见表 2.1）。通过 NESAS 框架下的安全审计和检测，设备厂商可以对产品的安全能力进行证明，运营商符合标准安全基线要求的产品进行 5G 网络建设时，在一定程度上可以保障 5G 网络基础设施满足安全基线要求。

2.4 国内相关工作

在国际高度关注 5G 安全问题的同时，我国也积极推动 5G 网络安全工作，从政策、标准、技术等方面持续完善安全保障措施，统筹规划 5G 安全相关工作。

（1）制定 5G 安全政策促进产业发展。工业和信息化部于 2020 年 3 月印发《关于推动 5G 加快发展的通知》，在加速推进 5G 新基建、加大 5G 技术研发力度的同时，着力构建 5G 安全保障体系的指示，指导 IMT-2020(5G)推进组发布《5G 安全报告》，出台 5G 网络安全实施指南，全面梳理分析 5G 安全风险和应对措施，为 5G 产业链各环节客观认识和应对 5G 安全问题提供技术指引。此外，在 2021 年 7 月，工信部联合网信办、发改委等 9 部门印发《5G 应用“扬帆”行动计划（2021-2023 年）》，针对 5G 应用安全保障能力提出了目标和要求，明确指出要加快构建与 5G 应用发展相适应的安全保障体系。

（2）建立健全与国际接轨的 5G 安全标准体系框架。同步 3GPP SA3，GSMA NESAS 等国际标准进展，依托 IMT-2020(5G)推进组安全工作组，在 TC260、TC485、CCSA 等国内标准化组织中积极布局 5G 安全标准，推动制定我国 5G 通信安全、边缘计算（MEC）安全、切片安全、设备安全保障等技术标准，发布《5G 移动通信网安全技术要求》等行业标准，建立健全 5G 安全标准体系，引导 5G 安全技

术、产品及产业健康发展。同时，对标 3GPP 等国际标准，制定我国 5G 移动通信设备安全保障系列规范，构建覆盖 5G 基站及核心网各项安全保障要求的安全测评体系，奠定与国际 5G 安全检测认证互认的基础。

(3) 构建 5G 安全评测能力并开展 5G 设备安全测试。在工业与信息化部的指导下，中国信息通信研究院成立“5G 安全测评中心”，构建与国际接轨的 5G 安全测评体系，搭建 5G 网络测试床，建设包括终端接入安全、基站/核心网设备安全、通信协议安全、网络切片安全等检测能力。牵头组织运营商、设备商共同开展 5G 网络设备安全评测工作，于 2021 年 5 月正式完成了对华为、中兴、大唐、爱立信、上海诺基亚贝尔 5 家国内外主流设备厂商的 5G 基站和核心网设备安全测试，测试结果在 IMT-2020（5G）推进组、GSMA 官方网站发布。

(4) 推动 5G 行业应用安全防护体系落地推广。连续举办两届“绽放杯”5G 应用安全专题赛，聚焦工业、能源、金融、交通等 5G 应用热点领域，面向全社会征集 400 多项 5G 应用安全实践案例，有效促进了 5G 应用安全解决方案、产品和服务供给，并在引导垂直行业 5G 应用安全需求、促进 5G 安全产业生态完善等方面发挥了显著作用。此外，工业和信息化部还组织开展了 5G 应用安全创新示范中心创建工作，引导基础电信企业、设备企业、安全企业及相关科研机构以“团体赛”模式加强 5G 安全能力建设和示范工作，推动标准化、模块化、可复制、易推广的 5G 应用安全解决方案和最佳实践在重点行业落地普及。

3 5G 网络安全知识库

3.1 5G 网络安全范围

5G 网络除了要满足 eMBB、uRLLC 和 mMTC 新形态的业务需求，也需要为各种应用场景提供差异化的安全服务。虚拟化、网络切片、边缘计算和 MIMO 等新技术的引入导致 5G 网络结构发生了很大的变化。从网络架构来看，5G 网络整体延续 4G 特点，包括接入网、核心网和上层应用。通常 5G 安全的范围大致分为以下几方面：

（1）基础设施安全：5G 网络基础设施安全主要包括终端、接入网、边缘、核心网和支撑管理平台等设施的安全，而端到端网络切片安全是 5G 网络的特色。网络切片通过对接入网、传输网、核心网进行资源编排、网络隔离以及网元功能划分等方式组成，也可以认为是基于 5G 网络基础设施形成虚拟专网提供网络服务的一种方式。

（2）数据安全：5G 数据通常包括与用户相关的身份标识信息、网络位置信息、业务数据，以及网络设备信息、管理运营等网络资产和管理数据。数据安全主要是指应用数据在 5G 网络基础设施内部采集、处理、存储、共享和销毁等生命周期的安全。

（3）运维安全：通过安全的运维管理提高 5G 网络的运行质量，实现设备资产清晰、网络运行稳定有序、事件处理及时合理和安全措施落实到位，从而提升网络支撑能力，提高网络管理水平。运维管理安全需要确保 5G 基站、网元、NFV 基础设施的硬件和软件运行的可靠性、保密性和完整性。5G 安全运维的对象主要为 NFV 基础设施、SDN、5G 网元、网络切片、MEC 的硬件和软件等。

（4）安全管理：5G 安全管理主要是对 5G 网络设备、人员、流程等进行安全管理，并按照“三同步”要求满足行业安全监管要求，包括安全风险评估、产品生命周期管理与检测、安全定级备案、威

胁与漏洞管理、应急响应等。

(5) 安全技术：安全技术通常用于支持上述安全内容的实现，包括网络隔离、密码算法、访问控制、隐私保护、态势感知以及安全检测等技术，这些安全技术也是知识库中安全措施的基础。



图 3-1 5G 安全范围视图

3.2 面向的 5G 资产

5G 网络安全知识库框架将围绕 5G 端到端网络资产类型，将安全措施划分为 L1、L2 和 L3 共 3 个层面。其中 L1 层主要面向 5G 网络基础软硬件设施，包括物理机/虚拟机、NFV、Hypervisor/K8s/docker、SDN、数据库以及安全组件，这些软硬件是支撑 L2 层 5G 网络功能部署的基础设施，主要由设备商、安全厂商和其他第三方服务商提供；L2 层主要包括 5G 终端、接入网、传输网、MEC、核心网、切片、安全管理、运维管理、互联互通等，主要资产由通信设备商提供，由运营商进行建设、运营和维护；L3 层主要关注上层 5G 应用安全，包括应用数据、应用 APP 以及应用平台等，相关应用由运营商、互联网服务提供商以及垂直行业提供。5G 网络安全知识库将重点对 L2 和 L3 层资产的安全防护措施进行描述，针对 L1 层资产的安全措施将融合在 L2 安全措施中进行描述，例如在 5G 核心网安全措施中会重点阐述 NFV 的安全防护措施。

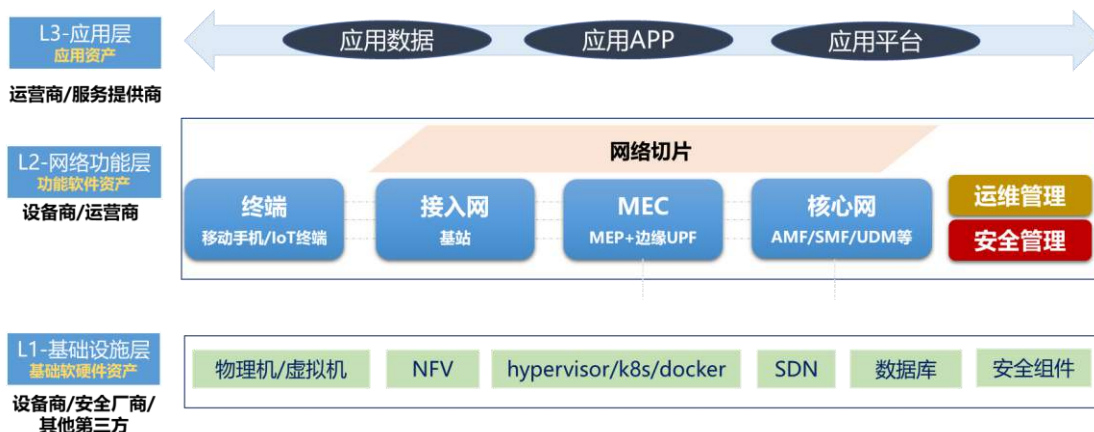


图 3-2 5G 知识库描述范围

3.3 描述方式

5G 网络安全知识库采用表 3-1 的方式进行描述，主要包括措施编号、措施名称、安全需求、措施作用（CIA）、措施详细描述、作用资产、实施主体、是否有标准要求以及实施难度等方面。

表 3-1 5G 网络安全知识库描述方式

措施编号	安全措施的缩略语—序号			
措施名称	安全措施的名称			
安全需求	描述该安全措施满足哪些 5G 安全需求			
措施作用（CIA）	描述安全措施措施在机密性（Confidentiality）、完整性（Integrity）和可用性（Availability）方面的安全作用。			
	机密性	完整性	可用性	
措施详细描述	措施编号+子序号：安全子措施的详细实施情况。			
作用资产	安全措施作用于哪些 5G 资产（具体资产参考图 3-2）。			
实施主体	运营商	措施编号+子序号		
	设备厂商	措施编号+子序号		
	服务提供商	措施编号+子序号		
	监管部门	措施编号+子序号		
	安全厂商	措施编号+子序号		
是否已有标准要求	是/否			
标准名称	国际和国内发布相关标准名称			
实施难度	通过 5 级区分本措施在相关资产实施的难以程度。灰色部分越多，措施实施难度越大，实施主体需要更多的 CAPEX 和 OPEX 投入。			

3.4 描述内容

5G 网络安全知识库采用表 3-1 的方式，重点针对图 3-2 中的 L2 层资产的安全措施进行描述，包括 8 大安全模块、45 项安全措施、188 项安全子措施，整体措施编号和名称如图 3-3 所示，详细安全措施见附录 A。

终端安全MT MT-1: 终端与5G网络数据和信令保护 MT-2: 用户凭证的安全保护 MT-3: 终端接入认证 MT-4: 终端访问限制	接入网安全RN RN-1: 基站用户数据和信令信息保护 RN-2: 伪基站检测及防护 RN-3: 网络可用性保护 RN-4: 降低无线电干扰风险 RN-5: 物理基站安全保护	边缘计算安全MEC MEC-1: 物理环境安全防护 MEC-2: 组网安全防护 MEC-3: 基础设施安全防护 MEC-4: 虚拟化安全防护 MEC-5: 边缘计算平台安全防护 MEC-6: 应用安全防护 MEC-7: 能力开放安全防护 MEC-8: 通信安全防护 MEC-9: 管理运维安全 MEC-10: 数据安全防护	核心网安全CN CN-1: 核心网资源可用性保护 CN-2: 5GC NEF安全保护 CN-3: 核心网流量保护 CN-4: 核心网内外边界隔离 CN-5: 核心网网元合法身份保障 CN-6: 虚拟机 (VM) 资源保护 CN-7: 用户标识符保护 CN-8: 漫游安全
网络切片安全NS NS-1: UE接入切片安全 NS-2: 切片网络隔离 NS-3: 切片数据隔离 NS-4: 网络切片管理安全	安全管理SM SM-1: 安全管理和编排 SM-2: 安全可控 SM-3: 人员管理 SM-4: 安全审计	数据安全DAT DAT-1: 数据发现识别及管理 DAT-2: 数据安全防护 DAT-3: 数据安全监测	运维管理OM OM-1: 5GC安全运维 OM-2: 云基础设施主机运维 OM-3: 云基础设施虚拟化层运维 OM-4: 云基础设施PIM运维 OM-5: 云基础设施MANO运维 OM-6: 云基础设施SDN运维 OM-7: 安全应急响应

图 3-3 5G 网络安全知识库措施描述内容

4 5G 应用安全知识库

4.1 5G 融合应用安全特点

4.1.1 5G 融合应用安全需求

为了保障 5G +行业应用的安全部署、运行和管理，IMT-2020（5G）推进组于 2020 年 10 月发布《面向行业 5G 安全分级白皮书》，深入分析和识别行业场景下对 5G 承载网络的差异化需求，主要包括基本需求和行业网络高级安全需求。其中基本需求主要是业务场景、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。高级安全场景是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，需提供更高的安全保障能力才能满足。安全需求主要包括终端身份安全和访问授权、网络安全隔离、数据机密性和完整性、无线接口通信安全、隐私安全、网络韧性、网络设备安全可信、技术自主可控和产品生命周期安全等九个方面，如表 4-1 所示。

4.1.2 行业应用安全需求与 5G 安全能力的映射

5G 网络安全知识库是为应用提供一张安全的基础网络，但 5G 网络承载的行业应用因业务场景特点、组网方式和安全要求不同，针对 CIA 三要素的安全策略也存在差异化需求，例如工业互联网场景要求高可用性、数据不出园区保护本地网络和数据安全，智慧医疗场景要求高度的用户隐私数据保护，车联网要求匿名认证、防跟踪等措施保护用户隐私，智慧电力场景要求严格的网络隔离确保生产业务安全。通常 5G+行业应用重点涉及以下几个维度的安全问题：

（1）5G 网络基础设施安全。垂直行业往往关注运营商的 5G 网络是否足够安全、可靠的承载应用业务，例如运营商是否能配置足够安全的网络切片供多垂直行业用户使用、本地边缘平台的数据防

护措施是否完善等。因此，需要通过 5G 网络安全知识库中的 8 项措施对 5G 接入网、边缘计算平台、核心网等网络基础设施进行保护，为承载垂直行业应用提供安全的“底座”和通道。

表 4-1 5G 融合应用安全需求

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保护	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	端到端业务数据传输机密性、完整性保护
无线接口通信保护	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、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	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(高级持续性威胁) 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

(2) 网络边界安全防护。5G 虚拟专网、共享切片、资源云化等行业应用的服务模式导致出现更多虚拟网络边界（例如边缘计算云平台上的虚拟资源之间、APP 之间等），运营商与垂直行业之间需要明确在混合组网、共享云平台等场景下的安全责任边界划分，并在物理边界和虚拟边界部署入侵检测、安全隔离等安全防护措施。

(3) 网络能力开放安全。3GPP 标准定义了 5G 网络能力开放功能，支持通过能力开放平台的 API 接口对外部提供调度、流控、监控、安全保障等管控能力，但网络能力开放也导致北向接口的管理和传输面临安全风险，需要通过认证鉴权、安全传输等防护措施对开放接口进行安全保护，确保合法的垂直行业用户访问 5G 网络。

(4) 端到端应用数据安全。从信息安全三要素 CIA（机密性、完整性和可用性）来看，5G 网络与其他公共通信网络一样，需要保障垂直行业的数据在网络中传输、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，不中断地为上层应用提供通信服务。

4.2 面向行业的 5G 安全原子能力集

为了满足 5G+行业应用的核心安全需求，需要对 5G 网络的安全能力（Security Capability, SeCAP）进行原子化分解，并通过灵活的管理和编排组成最佳安全能力集合，实现“对症下药”。5G 应用安全知识库总结了当前满足行业安全需求的 5G 网络 9 大安全能力，并细分为 53 项安全原子能力，为满足 5G+行业应用不同的应用场景的安全需求，提供细粒度、可定制、原子化、可编排的安全能力参考。

4.2.1 SeCAP-1 端到端网络切片隔离能力

安全能力编号	SeCAP-1
能力名称	端到端网络切片隔离能力

安全能力目标	5G 网络提供匹配垂直行业业务隔离安全需求的 5G 网络端到端切片隔离能力，从空口、传输、核心网等多个层面为行业应用提供安全的传输通道。																			
能力详细描述	<p>SeCAP-1-1: 5G RAN 为应用业务流提供无线资源分配机制，包括不限于专用无线资源分配、基于 SLA 服务等级的无线资源调度、共享的无线资源调度等方式。</p> <p>SeCAP-1-2: 5G 传输网为应用业务数据提供承载隔离机制，包括但不限于 Flex-E 硬隔离、VPN 软隔离等。</p> <p>SeCAP-1-3: 5G 核心网为行业用户提供网络功能切片隔离机制，包括不限于完全专用切片（NF 独享）、部分逻辑共享切片（共享部分 NF）、共享切片（共享所有 NF）。对于安全性和隔离性要求较高的切片，可单独部署 vDC 和主机组进行物理隔离，对于安全性和隔离性要求一般的切片，可规划单独的 vDC，共用主机组进行逻辑隔离。</p> <p>SeCAP-1-4: 5G 网络应根据行业应用场景的网络和安全需求，通过切片管理平台灵活配置相应的切片隔离机制，根据业务安全优先级不同，切片隔离方式可参考下表。</p> <table><tr><th>端到端位置</th><th>基本切片隔离 - 低安全需求场景</th><th>中等切片隔离 - 中安全需求场景</th><th>高级切片隔离 - 高安全需求场景</th></tr><tr><td>RAN</td><td>QoS 优先级、无线资源共享</td><td>高优先级 QoS+ 无线资源预留</td><td>载频独享的专用基站或小区</td></tr><tr><td>传输</td><td>VPN 隔离 + QoS 隔离调度</td><td>FlexE 接口隔离 + VPN 隔离</td><td>FlexE 接口隔离 + FlexE 交叉</td></tr><tr><td>5GC</td><td>To B 大网 NF 共享</td><td>SMF/UPF 逻辑资源独占专享 + 其他网元共享</td><td>SMF/UPF 物理资源独占专享</td></tr></table>				端到端位置	基本切片隔离 - 低安全需求场景	中等切片隔离 - 中安全需求场景	高级切片隔离 - 高安全需求场景	RAN	QoS 优先级、无线资源共享	高优先级 QoS+ 无线资源预留	载频独享的专用基站或小区	传输	VPN 隔离 + QoS 隔离调度	FlexE 接口隔离 + VPN 隔离	FlexE 接口隔离 + FlexE 交叉	5GC	To B 大网 NF 共享	SMF/UPF 逻辑资源独占专享 + 其他网元共享	SMF/UPF 物理资源独占专享
端到端位置	基本切片隔离 - 低安全需求场景	中等切片隔离 - 中安全需求场景	高级切片隔离 - 高安全需求场景																	
RAN	QoS 优先级、无线资源共享	高优先级 QoS+ 无线资源预留	载频独享的专用基站或小区																	
传输	VPN 隔离 + QoS 隔离调度	FlexE 接口隔离 + VPN 隔离	FlexE 接口隔离 + FlexE 交叉																	
5GC	To B 大网 NF 共享	SMF/UPF 逻辑资源独占专享 + 其他网元共享	SMF/UPF 物理资源独占专享																	
所需的安全措施	NS-2, NS-3, NS-4																			

垂直行业主体措施	VER-SeCAP-1-1: 明确 5G 行业应用场景, 以及行业应用场景的网络安全隔离要求 (如物理/逻辑网络隔离、单向隔离等), 并分析相应业务场景的隔离要求与 5G 切片安全隔离的对应关系, 选择合适的 5G 端到端切片隔离组合方案。
----------	--

4.2.2 SeCAP-2 网络边界安全防护能力

安全能力编号	SeCAP-2
能力名称	网络边界安全防护能力
安全能力目标	5G 网络提供运营商资产与垂直行业网络资产 (包括服务器、交换机等物理资产, 也包括在物理资源商的应用、数据等虚拟资产) 之间应安全边界防护能力, 保障网络边界安全。
能力详细描述	<p>SeCAP-2-1: 5G 网络数据面出口 (如 UPF 与垂直行业 DN) 之间部署边界防火墙和访问控制设备。</p> <p>SeCAP-2-2: 5G 网络对外开放功能 (如 NEF) 为垂直行业提供服务时, 其接口应采用鉴权认证机制。</p> <p>SeCAP-2-3: 运营商切片管理平台等如果对垂直行业开放, 在对外接口采用鉴权认证机制。</p> <p>SeCAP-2-4: 运营商 MEC 平台提供对垂直行业的访问接口时, 采用鉴权认证机制。</p> <p>SeCAP-2-5: 运营商信任域内的 UPF 和 MEP 与边缘垂直行业的内网之间通过物理防火墙进行隔离, 边缘 MEC 云内部的运营商 APP 与垂直行业 APP 之间通过虚拟防火墙进行隔离。</p> <p>SeCAP-2-6: MEC 平台内部应为服务于不同行业应用 APP 具备逻辑隔离措置 (如虚拟防火墙、边界访问控制机制等)。</p>
所需的安全措施	CN-2, CN-4, MEC-5, MEC-6, MEC-7, MEC-8

垂直行业主体措施	<p>VER-SeCAP-2-1: 明确垂直行业资产与 5G 网络的边界, 并在边界位置部署访问控制、网络隔离等安全防护措施, 如通过网闸、正反向隔离装置等对 CT 与 OT 域进行通信隔离。</p> <p>VER-SeCAP-2-2: 垂直行业在网络边界上部署流量监测和防护措施, 通过设置黑白名单、异常流量识别等机制对可能来自 5G 网络的非法访问和攻击流量进行识别和过滤。</p>
----------	---

4.2.3 SeCAP-3 增强的终端接入认证能力

安全能力编号	SeCAP-3
能力名称	增强的终端接入认证能力
安全能力目标	5G 网络提供满足行业需求的认证鉴权能力, 保障垂直行业终端接入 5G 网络的合法性。
能力详细描述	<p>SeCAP-3-1: 5G 网络提供 3GPP 定义的主认证机制, 并支持 EPS-AKA'和 5G-AKA 认证机制对终端接入进行认证。</p> <p>SeCAP-3-2: 5G 网络支持二次认证机制, 实现行业终端与外部 AAA 认证服务器的认证, 二次认证信令中包含的用户身份认证信息, 可通过 MPLS VPN 或 IPSec 专线进行保护。</p> <p>SeCAP-3-3: 5G 网络提供 GBA 认证机制, 智能终端或网关可通过 GBA 机制与外部 AAA 进行认证。</p> <p>SeCAP-3-4: 5G 网络提供 AKMA 认证机制, 通过 AUSF 与外部 AAA 生成 K_{AF}, 并使用密钥进行数据完整性和机密性保护。</p> <p>SeCAP-3-5: 5G 网络提供 SECAPIF 框架下的 5G 功能开放能力, 垂直行业调用 5G 网络开放 API 时, 需要进行认证鉴权。</p>

	<p>SeCAP-3-6: 5G 网络提供 UDM 定制化能力，在专网场景下实现对行业特定用户的认证鉴权过程。</p> <p>SeCAP-3-7: 5G 网络支持定制 DNN 及切片，终端号码签约行业定制 DNN+切片，UPF 仅支持该 DNN 及切片接入，实现仅允许授权用户接入用户网络功能。</p> <p>SeCAP-3-8: 终端内置专用安全芯片、SIM 卡、SDK 等，实现终端与 5G 应用之间的安全认证与数据传输加密。</p> <p>SeCAP-3-9: 支持基于电子围栏的终端安全接入能力，通过对 AMF 进行小区 TA 和终端绑定配置，实现专网只允许合法授权终端接入。</p> <p>SeCAP-3-10: 通过部署零信任安全网关进行终端接入统一的认证管理，避免非法设备接入进行攻击、窃听，建立基于环境和行为感知的持续动态认证和权限控制。</p>
所需的安全措施	MT-3, MT-4, RN-3, MEC-5, CN-5, CN-7, CN-8, NS-1
垂直行业主体措施	<p>VER-SeCAP-2-1: 垂直行业终端设备支持二次认证、GBA 认证、AKMA 机制等增强安全接入认证能力，并具备符合 AKA 的二次认证机制的外部 AAA 服务器。</p> <p>VER-SeCAP-2-2: 垂直行业根据其接入认证算法、流程、参数需求，与运营商确定增强认证机制的实现方案，例如 5G 网络是否支持定制化的认证算法和流程、电子围栏位置粒度、安全 SIM 卡的算法和密钥长度等。</p>

4.2.4 SeCAP-4 开放的网络管理和安全管控能力

安全能力编号	SeCAP-4
能力名称	开放的网络配置和安全管控能力

安全能力目标	5G 网络通过集中化对外管理开放平台，为垂直行业提供开放的网络管理、配置和管控能力，垂直行业能对其行业用户的业务情况进行监测和流量策略进行管理，并能共享运营商提供的安全服务。
能力详细描述	<p>SeCAP-4-1: 5G 网络支持 3GPP 定义的 CAPIF 框架，提供对垂直行业的开放能力。</p> <p>SeCAP-4-2: 5G 网络切片管理系统提供对外的切片管理开放能力，为行业用户提供切片编排、资源分配以及切片运行状态监控等能力。</p> <p>SeCAP-4-3: 5G 网络提供业务服务开放能力，提供行业用户的资源使用情况、流量使用情况、计费情况、QoS 服务质量等。</p> <p>SeCAP-4-4: 5G 网络提供行业用户的流量策略管理开放能力，能基于行业用户的策略对特定终端进行接入控制和流量路由（如路由到本地）。</p> <p>SeCAP-4-5: 5G 网络向行业用户提供安全即服务的能力，将 DDoS 安全检测、恶意域名/URL 检测、行业终端异常接入、异常流量使用、安全攻击事件检测及告警（如 DoS）、安全漏洞和威胁情况等结果开放给垂直行业，帮助 5G 垂直行业提升安全事件响应和处置能力。</p> <p>SeCAP-4-6: 5G 基于 NWDAF 网元能力通过 NEF/CAPIF 向 5G 垂直行业开放终端异常行为分析的服务，如位置异常、异常唤醒、频繁切换、流量突发异常等。</p> <p>SeCAP-4-7: 为垂直行业提供操作系统、数据库和路由器的口令、账号权限、身份鉴别、访问控制、安全审计的基线检查能力，帮助垂直行业识别安全风险。</p>
所需的安全措施	MEC-7, CN-2, CN-4, NS-4

垂直行业主体措施	<p>VER-SeCAP-4-1: 与运营商沟通开放能力需求, 约束各方的能力调用方法和安全责任。</p> <p>VER-SeCAP-4-2: 参与制定开放能力的技术标准, 明确开放接口的安全要求。</p>
----------	---

4.2.5 SeCAP-5 边缘/本地园区的数据安全防护能力

安全能力编号	SeCAP-5
能力名称	本地园区/边缘平台的数据安全防护能力
安全能力目标	针对行业园区数据安全防护需求, 5G 网络边缘云平台提供基础的安全网络环境, 通过差异化的访问控制和可靠的数据安全保护措施, 保护园区专网安全, 确保业务数据不出园区。
能力详细描述	<p>SeCAP-5-1: 5G 网络提供对边缘平台的访问控制、态势感知、边界隔离等安全防护措施, 支持过滤链路层、网络层、传输层非法报文,防止边缘平台业务被非法访问。</p> <p>SeCAP-5-2: 5G 园区 UPF 应提供通过安全的传输链路与垂直行业网络连接, 例如专线、L2TP/IPSec 隧道传输、VxLAN 等。</p> <p>SeCAP-5-3: 5G MEP 采用微服务隔离、VLAN 隔离、vFW 等机制, MEC 平台上部署 vFW, 实现行业 APP 间的按需安全隔离, 提供 MEC 内部东西向流量的安全防护。</p> <p>SeCAP-5-4: 5G 边缘 UPF 应支持面向垂直行业用户的独立部署, 提供不同业务类别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。</p> <p>SeCAP-5-5: 行业应用 APP 支持与 MEP、UPF 使用虚拟防火墙实施隔离。</p> <p>SeCAP-5-6: 边缘 MEP 应提供对 APP 数据的安全存</p>

	<p>储，涉及行业 5G 用户的位置、标识等信息应在 MEP 中加密存储。</p> <p>SeCAP-5-7: 5G RAN 至边缘 UPF 通过 IPSec 传输通道保护行业本地数据传输安全。</p> <p>SeCAP-5-8: 支持采用独享式 UPF，网络侧配置数据 ULCL 分流策略，本地做分流规则自检与 IP/FQDN 一致性检查，保证本地分流数据不出企业。</p> <p>SeCAP-5-9: 建议园区部署 2 套及以上 UPF，多链路对接企业内网，实现网络资源冗余能力提高，确保企业数据冗余安全。</p> <p>SeCAP-5-10: 在园区与外网之间通过防火墙 DPI 能力识别流量业务类型，监控所有出园区的数据流量是否包括业务数据，若发现数据出园区则产生告警事件，并能快速隔离阻断、恢复。</p>
所需的安全措施	MEC-2, MEC-3, MEC-4, MEC-5, MEC-6, MEC-7, MEC-8, CN-3, CN-4, NS-2, NS-3, DAT-1, DAT-2, DAT-3
垂直行业主体措施	<p>VER-SeCAP-4-1: 构建园区行业内网 DNN，通过专线、L2TP/IPSec 隧道传输、VxLAN 等与运营商 UPF 进行网络连接。</p> <p>VER-SeCAP-4-2: 依赖运营商 5G 网络开放能力，从运营商 MEC 侧获取网络开放数据，实现对垂直行业数据流量和终端情况的安全监测。</p>

4.2.6 SeCAP-6 面向行业应用的安全监测能力

安全能力编号	SeCAP-6
能力名称	面向行业应用的安全监测能力
安全能力目标	5G 网络提供对行业应用的安全监测和预警能力，能够对行业应用数据的安全、行业平台通过开放 API 访问 5G 网络等情况进行安全监测。

能力详细描述	<p>SeCAP-6-1: 5G 网络提供对 UPF 数据面攻击流量的实时特征进行检测，识别 UPF 与外部 DN 的可疑流量。</p> <p>SeCAP-6-2: 5G 网络提供对开放 API 接口的安全监测，识别外部网络通过开放 API 接口进行非法访问的行为。</p> <p>SeCAP-6-3: 对 MEP 关键数据进行监测审计，对 API 接口行为监控，支持 MEC 边缘流量常见攻击行为的监测，例如漏洞利用、非授权访问攻击、拒绝服务攻击等。</p> <p>SeCAP-6-4: 提供 5G 场景下的用户行为分析 UEBA，通过模式识别、深度学习等手段发现 5G 网络用户和网络节点的异常行为，实现对未知威胁的发现和监测。</p> <p>SeCAP-6-5: 5G 网络能将安全监测的结果通过自动化的方式开放给垂直行业。</p>
所需的安全措施	MEC-9, NS-4, INT-4, OM-7, DAT-3
垂直行业主体措施	<p>VER-SeCAP-6-1: 构建应用安全监测平台，通过网络能力开放，与运营 5G 商网络进行互通，对关键资产、数据和应用情况进行安全监测。</p> <p>VER-SeCAP-6-2: 使用运营商安全监测平台能力，监控应用安全风险和事件。</p>

4.2.7 SeCAP-7 基于蜜罐技术的 5G 安全防护能力

安全能力编号	SeCAP-7
能力名称	基于蜜罐技术的 5G 安全防护能力
安全能力目标	5G 网络提供蜜罐防御技术，通过对攻击者的诱骗实现攻击行为的精确感知和深度分析，以便及时调整安全防护措施，防患攻击者对 5G 网络的渗透攻击。
能力详细描述	SeCAP-7-1: 在 5G 核心网、MEC 等节点部署探针，

	<p>将异常访问流量重定向至与探针关联的蜜罐服务中，实现网络层欺骗。</p> <p>SeCAP-7-2: 在 5G 网络中部署蜜罐节点（如核心网网元、MEC APP 等），针对捕获到的网络攻击者的异常流量，结合大数据分析、云计算、AI 智能等技术，从而精确的感知攻击者行为，通过欺骗技术发现攻击者，收集和捕获攻击行为，追溯攻击来源，方便安全员做出及时的安全响应。</p>
所需的安全措施	RN-3, MEC-9
垂直行业主体措施	VER-SeCAP-7-1: 与运营商合作构建蜜罐安全模型，并通过 SeCAP-6 相关能力，对面向行业应用的安全攻击等进行识别发现和处理应对。

4.2.8 SeCAP-8 服务于多租户的虚拟专网能力

安全能力编号	SeCAP-8
能力名称	服务于多租户的虚拟专网能力
安全能力目标	针对多行业客户的服务需求，在 5G 基础网络上搭建 5G 虚拟专网，为不同客户提供隔离的安全通道，并通过统一的安全管控能力为不同客户提供安全管控服务。
能力详细描述	<p>SeCAP-8-1: 5G 网络支持多租户分权分域管理机制，能对客户进行不同级别的访问权限划分。</p> <p>SeCAP-8-2: 通过配置网段、NAT 支持多租户之间网络和流量隔离。支持 IPSec over VxLAN 隧道的建立，多客户网络之间可通过建立隧道进行数据传输隔离。</p> <p>SeCAP-8-3: 5G 网络支持统一安全资源池管理，对安全能力通过服务化方式提供给提供垂直行业客户，如抗 DDOS，NDR、IDS、AAA 等。</p> <p>SeCAP-8-4: 5G 网络支持 DNN 专线，采用专用 APN</p>

	<p>接入点接入垂直行业内网，与公网隔离，确保网络传输通道安全、可靠。</p> <p>SeCAP-8-5: 5G 网络支持统一的安全管理中心，整合和集中管理 5G 安全资源，提供满足多租户的主机漏扫、防病毒、堡垒机、安全态势共享、安全审计服务等服务能力。</p>
所需的安全措施	MEC-3, MEC-4, CN-6, SM-1, OM-3, OM-4, OM-5, OM-6
垂直行业主体措施	<p>VER-SeCAP-4-1: 根据垂直行业内网隔离与权限访问策略，与运营商进行 5G 专网安全隔离和边界防护规划，明确垂直行业使用 SeCAP-8 能力的具体方式。</p> <p>VER-SeCAP-4-2: 根据垂直行业对网络安全管理的需求，向运营商订购 SeCAP-8 中相应的安全服务。</p>

4.2.9 SeCAP-9 面向行业应用的 5G 安全测评能力

安全能力编号	SeCAP-9
能力名称	面向行业应用的 5G 安全测评能力
安全能力目标	重点对涉及业务应用安全风险、业务平台安全风险等风险点和安全方案的保障能力进行评估，重点发现存在安全风险，对安全方案进行完善。
能力详细描述	<p>SeCAP-9-1: 依据国际和国内相关标准（包括 ISO/IEC 27005、SP-800 等）和模型（如 805.X、STRIDE 等），对 5G 网络和应用安全风险情况进行评估，评估 5G 应用面临的安全风险。</p> <p>SeCAP-9-2: 5G 网络基于 GSMA NESAS 和 3GPP SCAS 体系的设备安全保障测试。</p> <p>SeCAP-9-3: 针对 5G 网络和应用业务特点，制定符合行业应用通信安全、网络隔离和数据安全需求的测试评估文档，常见的测评场景包括海量终端连接造成的信令风暴冲击、网络抗 DDoS 攻击、终端仿冒身份</p>

	<p>非法接入、信令面/用户面数据安全传输、UPF 流量安全、切片隔离安全等。</p> <p>SeCAP-9-4: 提供针对 5G 行业专网的安全渗透和攻防测试, 验证 5G 网络能为行业终端接入、信令交互、网络和切片隔离、应用数据传输等过程保证足够的安全性。</p>
所需的安全措施	SM-4
垂直行业主体措施	<p>VER-SeCAP-9-1: 与运营商、设备厂商等合作制定垂直行业应用安全需求的测试评估文档, 对各场景下的 5G 端到端安全能力进行测试验证。</p> <p>VER-SeCAP-9-2: 如果垂直行业建设自己的 5G 行业专网, 可以参考 SeCAP-9-2 的措施对其采购的设备进行安全保障测试。</p>

4.3 5G 应用安全最佳实践模板

5G 安全能力能够为垂直行业提供差异化的安全保障, 通过不同的安全原子能力组合, 可以构建出符合垂直行业业务需求的安全最佳实践模板, 这些模板具有可复制性, 可以应用于不同行业的业务场景, 在边界防护、数据隐私保护、访问控制等方面提供一定的安全保障能力。本章节参考了“绽放杯”5G 应用安全专题赛优秀案例, 对目前 5G 安全方案较为成熟的行业进行分析, 并总结出较为普适性的安全模板 (Security Template, ST), 为运营商、垂直行业等开展 5G 应用安全建设部署提供参考。

4.3.1 ST-IIoT 5G+工业互联网安全模板

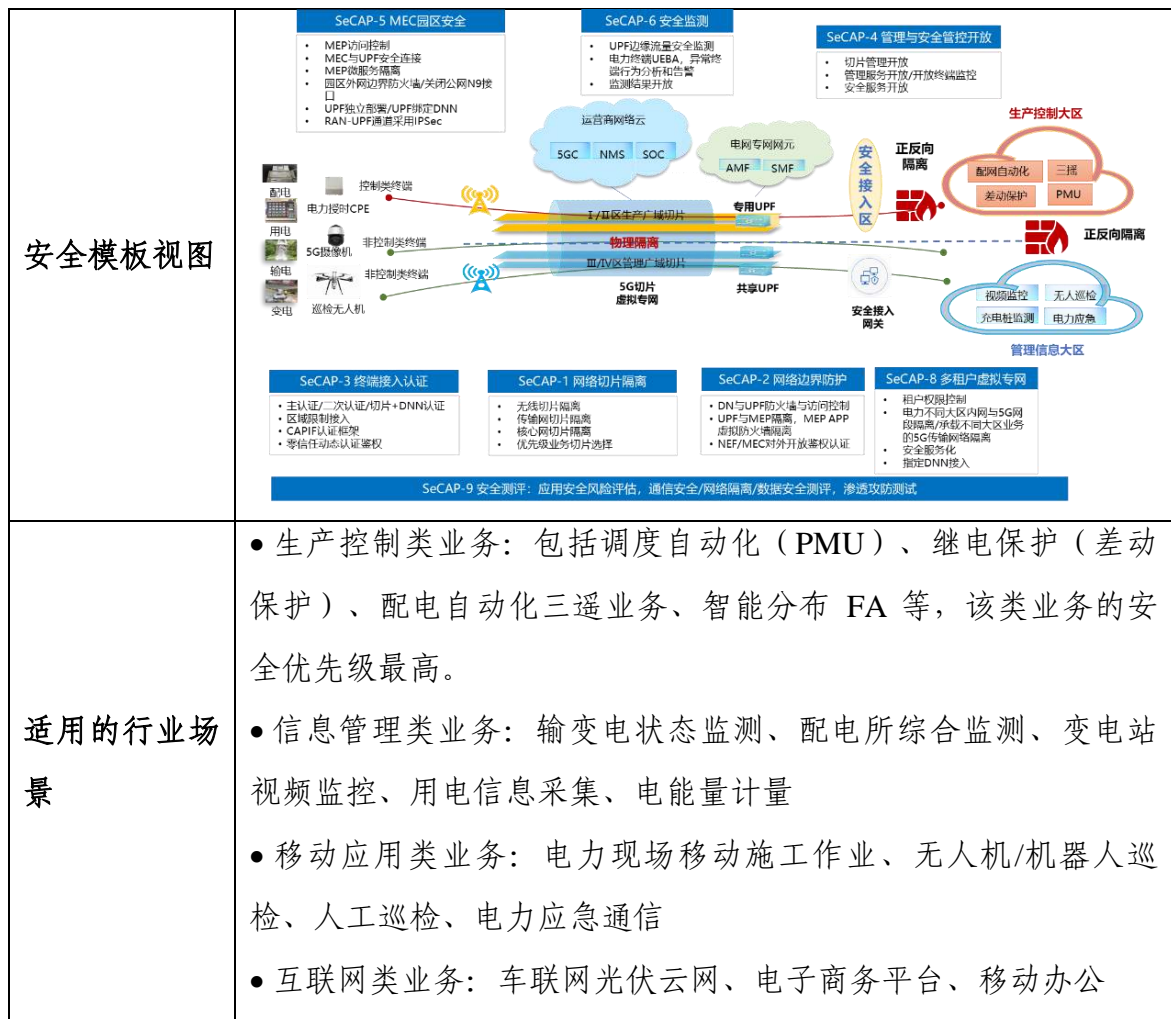
模板编号	ST-IIoT (Security Template for Industrial IoT)
模板名称	5G+工业互联网安全模板
核心安全需求	1. 工业接入终端类型多、数量大, 需要防范大量终端仿冒接入引起 DDoS 攻击、终端被伪基站吸附导致数据泄露、终端跨地域/超

	<p>阈值异常使用等安全问题。</p> <p>2. 工业生产数据（尤其是本地园区数据）的安全防护。</p> <p>3. CT、IT、OT 网络具有相互独立的安全体系，三类网络融合组网环境下，需要通过精细化的网络安全隔离对网络边界和数据通道进行保护。</p> <p>4. 工业互联网协议复杂多样，需要支持适配多种协议的安全监测能力，实现对协议攻击、网络渗透等事件行为的监测。</p>
模板介绍	<p>本模板为 5G+工业互联网提供安全能力集合，通过网络隔离能力、安全监测能力、终端接入能力等保障防止外部入侵攻击园区内部网络和数据，确保业务数据不出园区，实现对工业互联网安全监测和入侵防御。</p>
最佳安全原子能力集合	<ul style="list-style-type: none"> • SeCAP-1-1; SeCAP-1-2; SeCAP-1-3; SeCAP-1-4; • SeCAP-2-1; SeCAP-2-5; SeCAP-2-6; • SeCAP-3-1; SeCAP-3-2; SeCAP-3-7; SeCAP-3-9; SeCAP-3-10; • SeCAP-5-1; SeCAP-5-2; SeCAP-5-3; SeCAP-5-4; SeCAP-5-5; SeCAP-5-7; SeCAP-5-8; SeCAP-5-9; SeCAP-5-10 • SeCAP-6-1; SeCAP-6-3; SeCAP-6-4; • SeCAP-8-1; SeCAP-8-2; SeCAP-8-3; SeCAP-8-4; • SeCAP-9-1; SeCAP-9-3; SeCAP-9-4
安全模板视图	 <p>该图展示了5G+工业互联网安全模板的架构。中心是一个“端到端切片”管道，连接了“终端”、“接入网”、“传输网”和“用户面UPF”。终端侧包含“物联网终端”、“生产线”、“MES”和“企业管理网”。接入网侧包含“5G CPE”和“MEC”。传输网侧包含“UPF”和“MEP”。用户面UPF侧包含“工厂园区MEC”，其中包含“VM11”、“VM1n”、“VM21”、“VM2n”和“业务系统”。工厂园区MEC下方标注有“Hardware + FS”。右侧展示了“5GC”核心网，包含“AMF”、“SMF”、“UDM”和“SMF”。图中还包含多个安全能力集合的说明框：</p> <ul style="list-style-type: none"> SeCAP-6 安全监测： <ul style="list-style-type: none"> • UPF边缘流量安全监测 • 工业终端UEBA，异常终端行为分析和告警 SeCAP-5 MEC园区安全： <ul style="list-style-type: none"> • MEP访问控制 • MEC与UPF安全连接 • MEP微服务隔离 • 园区外网边界防火墙/关防公网N9接口 • UPF独立部署/UPF绑定DNN • RAN-UPF通道采用IPSec • UPF冗余 SeCAP-3 终端接入认证： <ul style="list-style-type: none"> • 主认证/二次认证/切片+DNN认证 • 区域限制接入 • 零信任动态认证鉴权 SeCAP-1 网络切片隔离： <ul style="list-style-type: none"> • 无线切片隔离 • 传输网切片隔离 • 核心网切片隔离 SeCAP-2 网络边界防护： <ul style="list-style-type: none"> • DN与UPF防火墙与访问控制 • UPF与MEP隔离，MEP APP虚拟防火墙隔离 SeCAP-8 多租户虚拟专网： <ul style="list-style-type: none"> • 租户权限控制 • OT、IT、CT网段隔离 • 安全服务化 • 指定DNN接入 <p>底部蓝色条标注：SeCAP-9 安全测评：应用安全风险评估，通信安全/网络隔离/数据安全测评，渗透攻防测试</p>
适用的行业场景	<ul style="list-style-type: none"> • 大带宽业务场景：VR/AR 检测 • 大连接业务场景：PLC 控制、工业传感 • 低时延、高可靠业务场景：远程机器人控制、CNC 数控机床控制

	制、AGV 控制、自动配送
--	---------------

4.3.2 ST-grid 5G+电力安全模板

模板编号	ST-grid (Security Template for Grid)
模板名称	5G+电力安全模板
核心安全需求	<ol style="list-style-type: none"> 1. 5G 网络提供的安全能力符合电网 “安全分区、网络专用、横向隔离、纵向认证” 的原则。 2. 多样化电力业务安全隔离需求不同，需要 5G 网络灵活划分切片承载，特别是生产类业务需要严格的切片隔离措施（如物理隔离）。 3. 防范非法终端通过 5G 专网接入电力系统，窃取或篡改电力系统敏感信息。 4. 电力业务数据端到端的安全机密性和完整性保护。 5. 5G 网络开放安全管控能力，对电力终端的状态进行监控和安全管理。
模板介绍	本模板为 5G+电力业务提供安全能力集合，通过网络隔离能力、安全监测能力、终端接入能力、管理和安全开放能力、多租户专网服务能力等重点解决电力差异化业务对 5G 网络切片隔离安全需求，并增强电力终端接入认证和边缘平台数据保护能力。
最佳安全原子能力集合	<ul style="list-style-type: none"> • SeCAP-1-1; SeCAP-1-2; SeCAP-1-3; SeCAP-1-4 • SeCAP-2-1; SeCAP-2-2; SeCAP-2-3; SeCAP-2-4; SeCAP-2-5; SeCAP-2-6 • SeCAP-3-1; SeCAP-3-2; SeCAP-3-5; SeCAP-3-7; SeCAP-3-9; SeCAP-3-10 • SeCAP-4-1; SeCAP-4-2; SeCAP-4-3; SeCAP-4-4; SeCAP-4-5 • SeCAP-5-1; SeCAP-5-2; SeCAP-5-3; SeCAP-5-4; SeCAP-5-5; SeCAP-5-6; SeCAP-5-7; SeCAP-5-8 • SeCAP-6-1; SeCAP-6-2; SeCAP-6-3; SeCAP-6-4; SeCAP-6-5 • SeCAP-8-1; SeCAP-8-2; SeCAP-8-3; SeCAP-8-4; SeCAP-8-5 • SeCAP-9-1; SeCAP-9-2; SeCAP-9-3; SeCAP-9-4

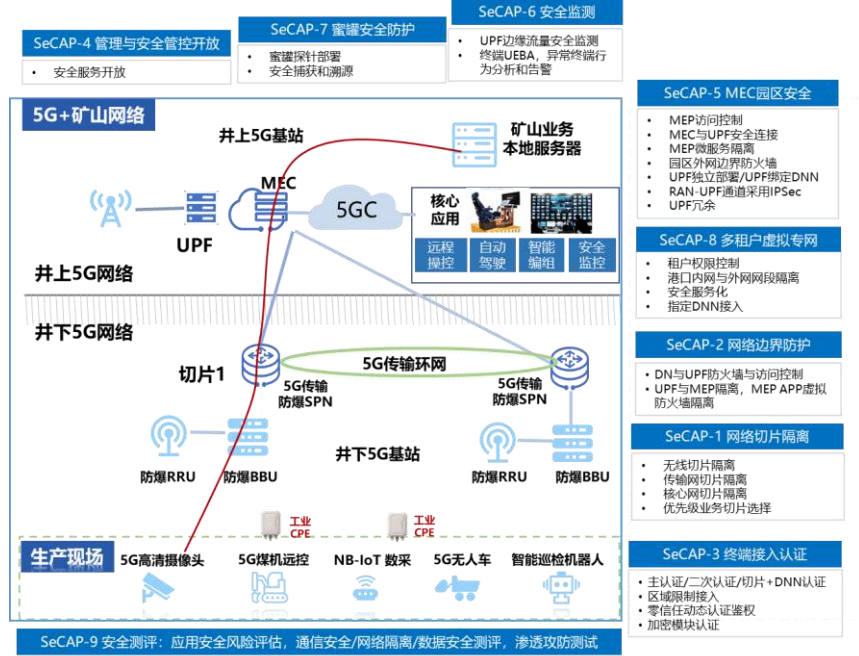


适用的行业场景

- 生产控制类业务：包括调度自动化（PMU）、继电保护（差动保护）、配电自动化三遥业务、智能分布 FA 等，该类业务的安全优先级最高。
- 信息管理类业务：输变电状态监测、配电所综合监测、变电站视频监控、用电信息采集、电能量计量
- 移动应用类业务：电力现场移动施工作业、无人机/机器人巡检、人工巡检、电力应急通信
- 互联网类业务：车联网光伏云网、电子商务平台、移动办公

4.3.3 ST-mine 5G+矿山安全模板

模板编号	ST-mine（Security Template for Mine）
模板名称	5G+矿山安全模板
核心安全需求	<ol style="list-style-type: none"> 1. 矿山业务涉及人员生命安全，对 5G 基础网络设施的安全性依赖极高，需要通过严格的安全评估测试保障 5G 网络安全可靠。 2. 矿山终端类型多样，需要防范终端弱加密导致数据泄露、被劫持发起 DDoS 攻击和终端非法接入等安全问题。
模板介绍	本模板为 5G+矿山提供安全能力集合，通过网络隔离能力、安全监测能力、终端接入能力、管理和安全开放能力、蜜罐防护能力、安全评测能力等，保障 5G+矿山基础网络设施的安全性。
最佳安全原子能力集合	<ul style="list-style-type: none"> • SeCAP-1-1; SeCAP-1-2; SeCAP-1-3; SeCAP-1-4 • SeCAP-2-1; SeCAP-2-5; SeCAP-2-6

	<ul style="list-style-type: none"> SeCAP-3-1; SeCAP-3-2; SeCAP-3-7; SeCAP-3-8; SeCAP-3-9; SeCAP-3-10 SeCAP-4-1; SeCAP-4-5 SeCAP-5-1; SeCAP-5-2; SeCAP-5-3; SeCAP-5-4; SeCAP-5-5; SeCAP-5-6; SeCAP-5-7; SeCAP-5-8; SeCAP-5-9; SeCAP-5-10 SeCAP-6-1; SeCAP-6-3; SeCAP-6-4; SeCAP-7-1; SeCAP-7-2 SeCAP-8-1; SeCAP-8-2; SeCAP-8-3; SeCAP-8-4; SeCAP-8-5 SeCAP-9-1; SeCAP-9-3; SeCAP-9-4
安全模板视图	
适用的行业场景	<ul style="list-style-type: none"> 大连接业务场景：传感器信息采集 低时延、高可靠业务场景：矿卡远程驾驶、电铲远程操控、井下远程控制、井下定位 大带宽业务场景：井下监控、AI智能识别、井下人员视频通信

4.3.4 ST-port 5G+港口安全模板

模板编号	ST-port (Security Template for Port)
模板名称	5G+港口安全模板
核心安全需求	1. 5G MEC 承载港口本地大量控制业务，需要 MEC 安全防护措施防范通过攻击者通过 MEC 渗透进入港口内网 IT 系统，也需要数

	<p>据防护措施保证港口边缘平台敏感信息安全。</p> <p>2. 防范港口 AVG/龙门吊等终端通过 5G 网络非法接入业务系统窃取或篡改港口业务敏感信息。</p> <p>3. 自动驾驶、龙门吊等控制类业务安全要求较高，需要通过资源和切片有效隔离防止网络资源抢占或非法跨切片攻击导致业务不可用。</p>
模板介绍	<p>本模板为 5G+港口提供安全能力集合，通过端到端网络切片隔离、增强的终端接入认证、边缘数据防护、安全监测能力等，重点解决港口业务的终端安全接入、MEC 平台和数据保护问题，并实现港口不同 SLA 业务的切片认证和切片隔离。</p>
最佳安全原子能力集合	<ul style="list-style-type: none"> • SeCAP-1-1; SeCAP-1-2; SeCAP-1-3; SeCAP-1-4 • SeCAP-2-1; SeCAP-2-5; SeCAP-2-6 • SeCAP-3-1; SeCAP-3-2; SeCAP-3-7; SeCAP-3-9; SeCAP-3-10 • SeCAP-4-1; SeCAP-4-5 • SeCAP-5-1; SeCAP-5-2; SeCAP-5-3; SeCAP-5-4; SeCAP-5-5; SeCAP-5-6; SeCAP-5-7; SeCAP-5-8; SeCAP-5-9; SeCAP-5-10 • SeCAP-6-1; SeCAP-6-3; SeCAP-6-4; • SeCAP-8-1; SeCAP-8-2; SeCAP-8-3; SeCAP-8-4; • SeCAP-9-1; SeCAP-9-3; SeCAP-9-4
安全模板视图	 <p>该图详细展示了5G+港口安全模板的架构。左侧为“码头现场”，包含“港机远控”、“智能理货”、“视频监控”等应用，通过“5G CPE”接入“5G RAN”。5G RAN包含“AAU”和“BBU”，并连接到“MEC”（边缘计算平台）。MEC通过“接入SPN”和“汇聚SPN”连接到“承载网”。承载网包含“FlexE专用通道”（VLAN1, VLAN2, VLAN3）和“FlexE数据流”。承载网通过“SecGW”（安全网关）连接到“5GC”（5G核心网）。5GC包含“AMF”、“NRF”、“UDMF”、“SMF”、“UPF”、“AUSF”、“NEF”等网元。5GC通过“安全网关”连接到“Internet”。图中还标注了“SeCAP-5 MEC安全”、“SeCAP-6 安全监测”、“SeCAP-4 管理与安全管控开放”、“SeCAP-3 终端接入认证”、“SeCAP-1 网络切片隔离”、“SeCAP-2 网络边界防护”、“SeCAP-8 多租户虚拟专网”等安全能力集合。底部有“SeCAP-9 安全测评”说明。</p>
适用的行业场景	<ul style="list-style-type: none"> • 大带宽业务场景：视频监控、龙门吊、桥吊等视频辅助、无人机/机器人巡检 • 大连接业务场景：传感采集

	<ul style="list-style-type: none"> • 低时延、高可靠业务场景：港机实施操控、集卡无人驾驶、自动理货
--	--

4.3.5 ST-city 5G+智慧城市安全模板

模板编号	ST-city (Security Template for City)
模板名称	5G+智慧城市安全模板
核心安全需求	<p>1. 海量异构终端接入 5G 网络，需要通过增强的接入认证措施防范弱终端被劫持，非法接入窃取平台业务数据，或大量终端对网络发起信令风暴或 DDoS 攻击。</p> <p>2. 5G 网络传输交通信息、消防信息、安防信息等多类敏感数据，需要对数据进行安全保护。</p> <p>3. 需要建设统一的安全管理平台对异构设备安全事件进行态势监控，并能对终端非法接入、异常访问行为等情况及时监测和响应。</p>
模板介绍	<p>本模板为 5G+智慧城市提供安全能力集合，通过网络隔离能力、安全监测能力、终端接入能力、边缘数据防护能力等增强智慧城市多行业终端的安全接入，实现行业敏感数据保护和安全态势监测。</p>
最佳安全原子能力集合	<ul style="list-style-type: none"> • SeCAP-1-1; SeCAP-1-2; SeCAP-1-3; SeCAP-1-4 • SeCAP-2-1; SeCAP-2-5; SeCAP-2-6 • SeCAP-3-1; SeCAP-3-2; SeCAP-3-5; SeCAP-3-7; SeCAP-3-8 • SeCAP-4-5 • SeCAP-5-1; SeCAP-5-2; SeCAP-5-3; SeCAP-5-4; SeCAP-5-5; SeCAP-5-6; SeCAP-5-7; SeCAP-5-8 • SeCAP-6-1; SeCAP-6-3; SeCAP-6-4 • SeCAP-8-1; SeCAP-8-2; SeCAP-8-3; SeCAP-8-4; SeCAP-8-5 • SeCAP-9-1; SeCAP-9-3

安全模板视图	
适用的行业场景	<ul style="list-style-type: none"> • 电子政务：政务服务 • 智慧安防：巡逻机器人、VR 安防监控 • 智慧交通：车辆调度、智能调度、客流疏导 • 智慧消防：智慧作战、智慧管理 • 智慧执法、智慧旅游、智慧农业等

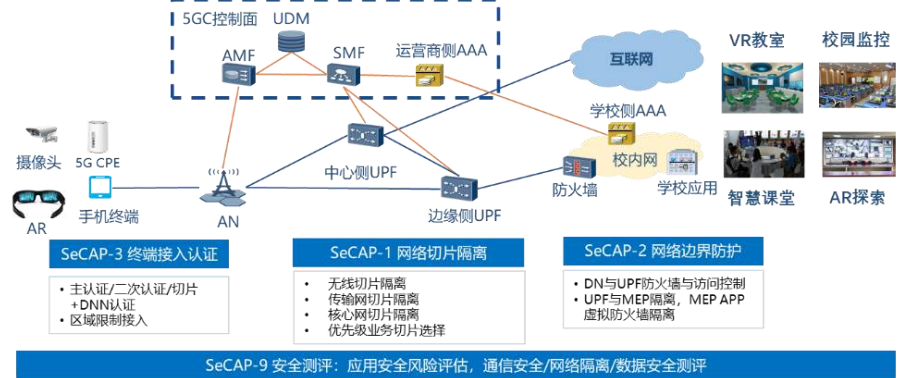
4.3.6 ST-hospital 5G+医疗安全模板

模板编号	ST-hospital (Security Template for Hospital)
模板名称	5G+医疗安全模板
核心安全需求	<p>1. 医疗数据高度敏感，需要通过数据安全防护措施对流经 5G 基站和 MEC 的医疗数据进行精准分流，对 MEC 平台的医疗数据进行保护。</p> <p>2. 5G 虚拟专网同时连接医院内网络与院外互联网，需要通过严格的网络隔离措施防止非法数据流入院内网络。</p>
模板介绍	本模板为 5G+医疗提供安全能力集合，通过端到端网络切片隔离、增强的终端接入认证、边缘数据防护等实现 5G+医疗院内院外网络隔离，并对医疗业务数据进行安全保护。
最佳安全原子能力集合	<ul style="list-style-type: none"> • SeCAP-1-1; SeCAP-1-3 • SeCAP-2-1; SeCAP-2-5; SeCAP-2-6 • SeCAP-3-1; SeCAP-3-2; SeCAP-3-7; SeCAP-3-9 • SeCAP-5-1; SeCAP-5-2; SeCAP-5-3; SeCAP-5-4 SeCAP-5-5; SeCAP-5-6; SeCAP-5-7; • SeCAP-8-1; SeCAP-8-2; SeCAP-8-4;

	<ul style="list-style-type: none"> SeCAP-9-1; SeCAP-9-3
安全模板视图	<p>医院内网</p> <p>HIS PACS EMR DB</p> <p>院内医疗应用系统</p> <p>院内医疗数据流</p> <p>院前急救</p> <p>远程超声</p> <p>远程会诊</p> <p>移动查房</p> <p>5G基站, 院区覆盖</p> <p>传输</p> <p>5GC</p> <p>AMF UDM SMF</p> <p>Internet</p> <p>院外公网流量</p> <p>院内专网流量</p> <p>SeCAP-5 MEC院区数据安全</p> <ul style="list-style-type: none"> MEP访问控制 MEC与UPF安全连接 MEP微服务隔离 院区外网边界防火墙 UPF独立部署/UPF绑定DN RAN-UPF通道采用IPSec <p>SeCAP-3 终端接入认证</p> <ul style="list-style-type: none"> 主认证/二次认证/切片+DN认证 区域限制接入 <p>SeCAP-1 网络切片隔离</p> <ul style="list-style-type: none"> 无线切片隔离 核心网切片隔离 <p>SeCAP-2 网络边界防护</p> <ul style="list-style-type: none"> DN与UPF防火墙与访问控制 UPF与MEP隔离, MEP APP虚拟防火墙隔离 <p>SeCAP-8 多租户虚拟专网</p> <ul style="list-style-type: none"> 租户权限控制 院内/5G与院外网段划分 指定DN接入 <p>SeCAP-9 安全测评: 应用安全风险评估, 通信安全/网络隔离/数据安全测评</p>
适用的行业场景	<ul style="list-style-type: none"> 大带宽业务场景: 远程会诊、远程示教、移动查房 低时延、高可靠业务场景: 远程超声、远程手术、院前急救 (急救车)

4.3.7 ST-education 5G+教育安全模板

模板编号	ST-education (Security Template for Education)
模板名称	5G+教育安全模板
核心安全需求	<ol style="list-style-type: none"> 通过部署软硬件隔离措施, 保障校园专网与校外网络的安全隔离, 实现一张专网对校内校外业务场景全覆盖。 通过增强的安全认证机制, 保障终端接入校园网络的安全。
模板介绍	本模板为 5G+教育提供电力模板, 通过端到端网络切片隔离、增强的终端接入认证、边缘数据防护等实现校园专网隔离, 防范非法终端通过 5G 网络接入对校园网站进行攻击。
最佳安全原子能力集合	<ul style="list-style-type: none"> SeCAP-1-1; SeCAP-1-2; SeCAP-1-3; SeCAP-1-4 SeCAP-2-1; SeCAP-2-5; SeCAP-2-6 SeCAP-3-1; SeCAP-3-2; SeCAP-3-7; SeCAP-3-9 SeCAP-5-2; SeCAP-5-3; SeCAP-5-4; SeCAP-5-5; SeCAP-5-7 SeCAP-9-1; SeCAP-9-3

<p>安全模板视图</p>	 <p>The diagram illustrates a 5G network security architecture for a campus scenario. It shows the 5G control plane (5GC) including UDM, AMF, and SMF, along with the operator's AAA server. The network is divided into three security domains: SeCAP-3 (Terminal Access Authentication), SeCAP-1 (Network Slice Isolation), and SeCAP-2 (Network Boundary Protection). The SeCAP-3 domain includes main/secondary authentication, DNN authentication, and area restriction access. The SeCAP-1 domain includes radio slice isolation, transport network slice isolation, core network slice isolation, and priority-based slice selection. The SeCAP-2 domain includes DN and UPF firewall and access control, UPF and MEPI isolation, MEPI APP, and virtual firewall isolation. The network also includes a central UPF and an edge UPF. The campus scenario includes various applications such as VR classrooms, campus surveillance, 5G online courses, smart classrooms, and AR exploration, all connected to the campus network and the Internet.</p> <p>SeCAP-3 终端接入认证</p> <ul style="list-style-type: none"> 主认证/二次认证/切片+DNN认证 区域限制接入 <p>SeCAP-1 网络切片隔离</p> <ul style="list-style-type: none"> 无线切片隔离 传输网切片隔离 核心网切片隔离 优先级业务切片选择 <p>SeCAP-2 网络边界防护</p> <ul style="list-style-type: none"> DN与UPF防火墙与访问控制 UPF与MEPI隔离, MEPI APP 虚拟防火墙隔离 <p>SeCAP-9 安全测评: 应用安全风险评估, 通信安全/网络隔离/数据安全测评</p>
<p>适用的行业场景</p>	<ul style="list-style-type: none"> 大带宽业务场景: VR 教室、智慧课堂、校园监控、5G 网课

5 安全知识库使用方法

知识库为运营商、设备商和垂直行业提供了一套完整的安全措施落地实施方法，在实际使用过程中，相关责任主体需要明确具体的网络和应用业务场景，通过安全风险分析确定特定业务场景的安全需求和 5G 安全能力的映射关系，参考知识库选择最佳的安全能力和措施组合，满足特定的安全需求。

5.1 面向运营商、设备商的 5G 网络安全知识库使用方法

图 5-1 描述了运营商、设备商使用 5G 网络安全知识库的方法，主要过程如下：

1) 根据具体的网络场景（例如无线接入场景、边缘计算场景等），梳理明确哪些 5G 资产存在安全风险，需要进行安全保护；

2) 对资产进行安全威胁分析，通过威胁建模等方式，明确该资产和该场景下面临的安全威胁问题；

3) 将安全威胁映射为具体的安全需求，从而确定需要开展网络资产安全保护的范围（见 3.1）；

4) 从信息安全 CIA 指标角度，分析需要在机密性、完整性和可用性等方面对资产进行进行安全保护；

5) 结合安全需求+CIA 指标能力，从附录 A 5G 网络安全知识库中选定满足条件的安全措施子集；

6) 参考附录 A 安全措施的责任主体和安全子措施内容，结合已有的安全标准规范，将选定的安全措施部署在相关的资产上；

7) 通过效果评价机制（包括风险消除评估、安全能力测试验证等），对安全措施的效果进行效果评价，并根据评价结果对安全措施进行重新选定或更新完善。

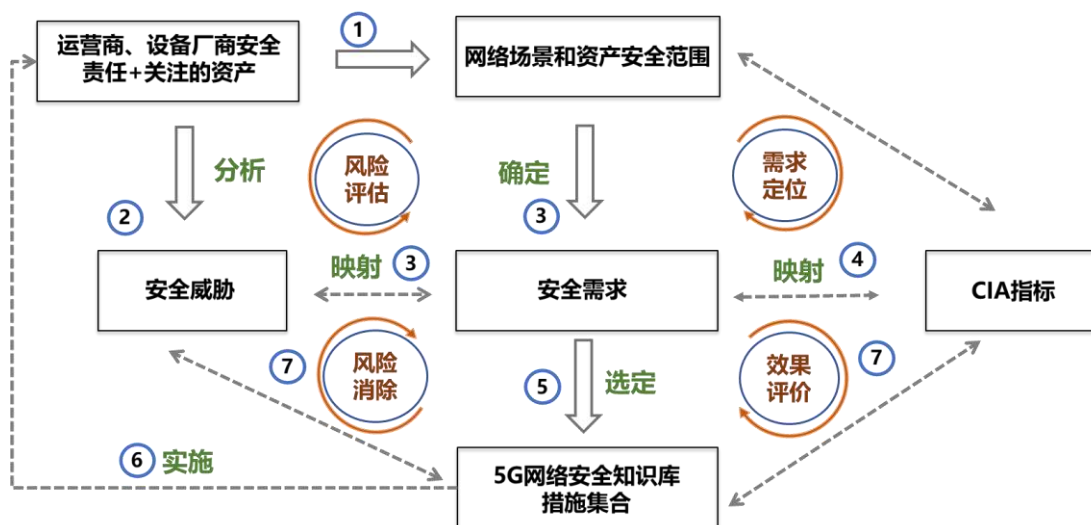


图 5-1 5G 网络安全知识库使用方法

5.2 面向运营商、垂直行业的 5G 应用安全知识库使用方法

图 5-2 描述了运营商、垂直行业合作使用 5G 安全知识库的方法，主要过程如下：

1) 运营商、垂直行业沟通明确 5G 行业应用的具体场景和资产，例如参考 4.3 应用安全模板中的业务场景；

2) 根据具体的应用场景，通过威胁建模、风险评估等方法，分析应用场景下 5G 网络和应用面临的安全风险和威胁；

3) 将安全风险和威胁映射为具体的安全需求，从而明确 5G 行业应用的安全目标和核心安全需求；

4) 根据安全需求内容，匹配 4.3 应用安全知识库中的安全模板，如果安全模板适用于相关场景，可以参考 4.3 中的最佳实践模板中的安全原子能力；如果有定制化的安全需求，可参考 4.2 中总结的安全原子能力，形成自定义的安全原子能力集合；

5) 垂直行业根据安全最佳实践模板+自定义原子能力集合，一方面向运营商订购相应的安全能力要求，运营商参考 4.2 章节能力表中的“所需安全措施”选定附录 A 的安全措施满足相应的安全能力，

另一方面垂直行业可参考 4.2 安全能力表格中的“行业主体措施”选定自己的安全措施；

6) 运营商和垂直行业分别参考附录 A 和 4.2 章节将选定的安全措施部署在具体的应用场景和 5G 资产上；

7) 运营商和垂直行业对安全原子能力满足安全需求的情况进行效果评估（包括风险消除评估、安全能力测试验证等），并根据评价结果对安全原子能力和安全措施进行重新选定或更新完善。

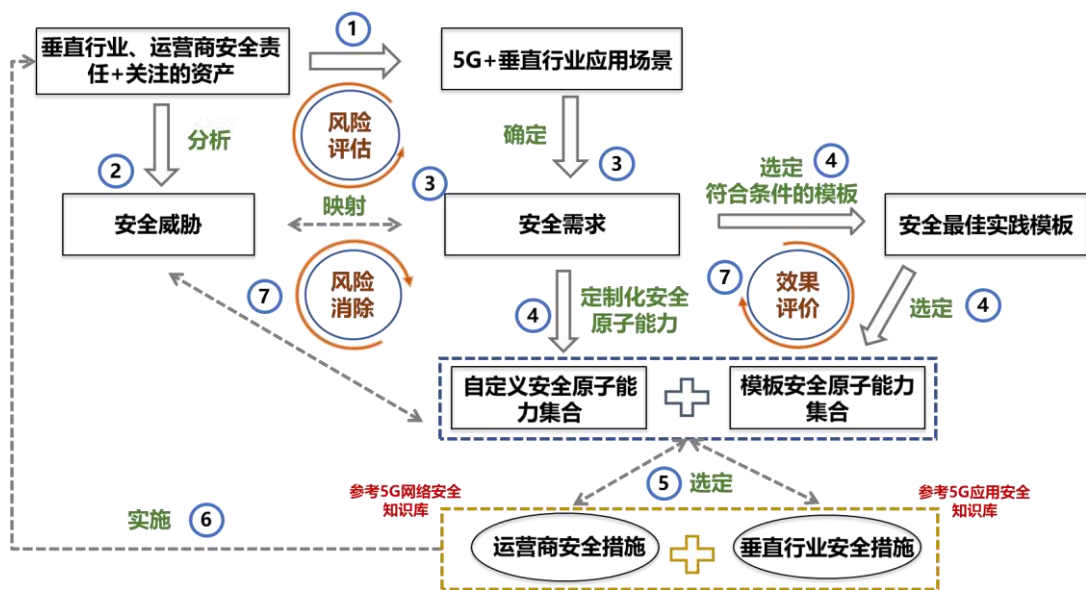


图 5-2 5G 应用安全知识库使用方法

6 总结及展望

当前，加快 5G 应用部署，赋能垂直行业，培植应用生态，已成为业界各方共同探索的重要方向。5G 与各垂直行业的融合应用打破了经济社会各领域的边界，网络安全与工业、交通等领域安全问题相互交织，给 5G 安全工作提出了更高要求。在此新形势下，

《5G 安全知识库》的发布将为 5G 网络和应用产业上各环节的参与方提供了参考，对于保障和促进 5G 应用快速发展有着积极和重要的价值和意义。

在 5G 发展中各方既有共同关切，也有不同诉求，应当在尊重彼此核心利益的前提下，共同合作开展 5G 安全措施的实施，形成对 5G 安全的共识，促进 5G 技术更好的造福行业。

（1）知识库措施将持续更新迭代。一方面，5G 网络正在逐步向更智能、更开放的架构演进，零信任、内生安全、主动防御等网络安全技术也在不断发展，知识库将随着 5G 网络技术的演进、融合应用的发展、以及新型安全技术的成熟，持续迭代更新，适应 5G 网络和应用的发展形势，保障 5G 安全能力不断提升。

（2）多方合作才能发挥最大价值。虽然知识库列出了各主体在参与 5G 网络建设、运营和维护以及部署 5G 行业应用中可参考采取的最佳安全实践措施，但是 5G 网络是一个整体，不能割裂地对待安全问题。各参与方应加强合作，在各环节将安全措施进行有机关联和落实到位，避免出现安全薄弱点，形成 5G 网络和应用的整体防护能力，发挥知识库中安全措施的最大效果。

（3）精确平衡安全供需是关键。运营商和垂直行业要从具体的 5G 应用场景出发，准确评估网络和应用面临的安全风险，充分沟通 5G+行业场景下的安全需求内容和供给能力，形成符合双方彼此共

识的安全实践措施，在供需平衡中不断优化供需关系，在实践过程中持续增强合作互信。

（4）在实践中不断检验和优化。知识库中的安全措施在实际执行中会有交织，各参与主体要从实际出发，在实践过程中不断检验措施的适用性、合理性和有效性，逐步完善和优化知识库中各个安全措施的内容，促进最佳安全实践经验在实践中不断迭代完善，持续适应 5G 网络和应用安全高质量发展。

7 缩略语

3GPP	3rd Generation Partnership Project	第三代合作伙伴计划
5G-AKA	5G - Authentication and Key Agreement	5G 认证与密钥协商
5GC	5G Core	5G 核心网
AAA	Authentication, Authorization and Accounting	认证、授权与计费
ACL	Access Control Lists	访问控制列表
AES	Advanced Encryption Standard	高级加密标准
AF	Authentication Framework	认证框架
AGV	Automated Guided Vehicle	自动导航车
AI	Artificial Intelligence	人工智能
AKA	Authentication and Key Agreement	认证与密钥协商
AKMA	Authentication and Key Management for Applications	应用层认证和密钥管理
AMF	Access and Mobility Management Function	接入与移动性管理功能
API	Application Programming Interface	应用程序接口
APP	Application	应用程序
AS	Access Stratum	接入层
AUSF	Authentication Server Function	鉴权服务功能
CAPIF	Common API Framework	通用 API 开放框架
CCSA	China Communications Standards Association	中国通信标准化协会
CIA	Confidentiality, Integrity and Availability	机密性、完整性和可用性
CN	Core Network	核心网
CPU	Central Processing Unit	中央处理器
CSA	Cybersecurity Act	网络安全法
CSG-ID	Closed Subscriber Group Identity Document	闭合用户组身份标识

CT	Communication Technology	通信技术
DAT	Data	数据
DDoS	Distributed Denial of Service	分布式拒绝服务
DMZ	Demilitarized Zone	隔离区
DN	Data Network	数据网络
DNN	Data Network Name	数据网络名称
DOS	Denial of Service	拒绝服务
DTLS	Datagram Transport Layer Security	数据包传输层安全性协议
EAS	Edge Application Service	边缘应用服务
eMBB	Enhanced Mobile Broadband	增强移动宽带
ENISA	European Union Agency for Cybersecurity	欧洲网络与信息安全局
eNodeB	Evolved Node B	4G 基站
EPS	Evolved Packet System	演进分组系统
EPS-AKA	Evolved Packet System - Authentication and Key Agreement	4G 认证与密钥协商
ETSI	European Telecommunications Standards Institute	欧洲电信标准化协会
EU	European Union	欧盟
Flex-E	The Flexible Ethernet	柔性以太网
FQDN	Fully Qualified Domain Name	全限定域名
FTP	File Transfer Protocol	文件传输协议
GBA	General Bootstrapping Architecture	通用认证机制
gNB	NR NodeB	5G 基站
gNodeB	NR NodeB	5G 基站
GPS	Global Positioning System	全球定位系统
GPSI	Generic Public Subscription Identifier	通用公共用户标识

GSMA	Global System for Mobile Communications Assembly	全球移动通信协会
GTP	GPRS Tunnel Protocol	GPRS 隧道协议
GUTI	Globally Unique Temporary UE Identity	全球唯一临时 UE 标识
HTTPS	Hyper Text Transfer Protocol over Secure Socket Layer	超文本安全传输协议
I/O	Input and Output	输入输出
ICT	Information and Communications Technology	信息与通信技术
IDS	Intrusion Detection System	入侵检测系统
IEC	International Electro technical Commission	国际电工委员会
IMEI	International Mobile Equipment Identity	国际移动设备识别码
IMSI	International Mobile Subscriber Identification Number	国际移动用户识别码
IMT	International Mobile Telecommunications	国际移动通信
INT	Inter-Network	互联互通
IP	Internet Protocol	网间互联协议
IPS	Intrusion Prevention System	入侵防御系统
IPsec	Internet Protocol Security	互联网安全协议
IPX	Internetwork Packet Exchange protocol	互联网分组交换协议
ISO	International Organization for Standardization	国际标准化组织
IT	Information Technology	信息技术
ITU	International Telecommunication Union	国际电信联盟
ITU-T	ITU Telecommunication Standardization Sector	国际电信联盟电信标准分局

K8S	Kubernetes	开源容器集群管理系统
KPI	Key Performance Indicator	关键绩效指标
L2TP	Layer 2 Tunneling Protocol	第二层隧道协议
LAC	Location Area Code	位置区域码
LTE	Long Term Evolution	长期演进
MAC	Media Access Control	介质访问控制
MANO	Management and Orchestration	管理和编排
MEC	Multi-access Edge Computing	多接入边缘计算
MEP	Multi-access Edge Platform	多接入边缘平台
mMTC	Massive Machine Type Communication	大规模机器类通信
MNO	Mobile Network Operator	移动运营商
MT	Mobile Terminal	移动终端
MVNO	Mobile Virtual Network Operator	移动虚拟网络运营商
NAS	Non Access Stratum	非接入层
NAT	Network Address Translation	网络地址转换
NDR	Network Detection and Response	网络检测与响应
NDS	Network Domain Security	网络域安全
NE	Net Element	网元
NEA	NR Encryption Algorithm	5G 加密算法
NEF	Network Exposure Function	网络开放功能
NESAS	Network Equipment Security Assurance Scheme	网络设备安全保障方案
NF	Network Function	网络功能
NFV	Network Virtualization Function	网络功能虚化
NFVI	Network Virtualization Function Infrastructure	网络功能虚拟化基础设施
ng-eNB	Next Generation Evolved NodeB	下一代演进基站
NG-RAN	Next Generation Radio Access Network	下一代无线接入网

NIA	NR Integrity Protection Algorithm	5G 完整性保护算法
NIST	National Institute of Standards and Technology	美国国家标准与技术研究院
NRF	Network Repository Function	网络存储功能
NS	Network Slice	网络切片
NSI	Network Slice Instance	网络切片实例
NSSAI	Network Slice Selection Assistance Information	网络切片选择辅助信息
OM	Operation and Management	运维管理
OS	Operating System	操作系统
OT	Operational Technology	运营技术
OWASP	Open Web Application Security Project	开放 Web 软体安全项目
PC	Personal Computer	个人计算机
PDP	Packet Data Protocol	分组数据包协议
PDU	Protocol Data Unit	协议数据单元
PIM	Physical Infrastructure Manager	物理基础设施管理器
PKI	Public key infrastructure	公钥基础设施
PLMN	Public Land Mobile Network	公共陆地移动网
QoS	Quality of Service	服务质量
RAN	Radio Access Network	无线接入网
RB	Resource Block	资源块
RN	Radio Network	无线网络
RRC	Radio Resource Control	无线资源控制
SAEGW-U	SAE GateWay User Plane	SAE 用户面网关
SBA	Service-based Architecture	服务化架构
SCAS	Security Assurance Specification	安全保障规范
SDK	Software Development Kit	软件开发工具包
SDN	Software Defined Network	软件定义网络

SeCAP	Security Capability	安全能力
SEAF	Security Anchor Function	安全锚定功能
SEPP	Security Edge Protection Proxy	安全边缘保护代理
SFTP	Secure File Transfer Protocol	安全文件传输协议
SIEM	Security Information Event Management	安全信息和事件管理
SIM	Subscriber Identity Module	用户身份识别模块
SLA	Service Level Agreement	服务等级协议
SM	Security Management	安全管理
SMF	Session Management Function	会话管理功能
SMS	Safety Management System	安全管理系统
SNMP	Simple Network Management Protocol	简单网络管理协议
SS7	Signaling System #7	7号信令系统
SSH	Secure Shell	安全协议
SSL	Secure Sockets Layer	安全套接字协议
ST	Security Template	安全模板
ST-city	Security Template for City	智慧城市安全模板
ST-education	Security Template for Education	教育安全模板
ST-grid	Security Template for Grid	电力安全模板
ST-hospital	Security Template for Hospital	医疗安全模板
ST-IIot	Security Template for Industrial Iot	工业互联网安全模板
ST-mine	Security Template for Mine	矿山安全模板
ST-port	Security Template for Port	港口安全模板
SUCI	Subscription Concealed Identifier	隐藏性用户标识符
SUPI	Subscription Permanent Identifier	用户永久标识符
TA	Tracking Area	跟踪区
TLS	Transport Layer Security	传输层安全协议
UDM	Unified Data Management	统一数据管理
UE	User Equipment	用户设备

UEBA	User and Entity Behavior Analytics	用户和实体行为分析
UICC	Universal Integrated Circuit Card	通用集成电路卡
ULCL	Uplink Classifier	上行分类器
UPF	User Plane Function	用户面功能
uRLLC	Ultra Reliable Low Latency Communication	超可靠低时延通信
vFW	Virtual Firewall	虚拟防火墙
VIM	Virtual Infrastructure Management	虚拟基础架构管理
VLAN	Virtual Local Area Network	虚拟局域网
VM	Virtual Machine	虚拟机
VPC	Virtual Private Cloud	私有网络
VPN	Virtual Private Network	虚拟专用网络
VR	Virtual Reality	虚拟现实
VRF	Virtual Routing Forwarding	虚拟路由转发
VxLAN	Virtual Extensible Local Area Network	虚拟扩展局域网

附录 A：5G 网络安全知识库措施

A.1 终端安全（Mobile Terminal, MT）

A.1.1 MT-1 终端与 5G 网络数据和信令保护

措施编号	MT-1			
措施名称	终端与 5G 网络间的数据和信令保护			
安全需求	保护终端与 5G 网络之间的用户面数据和控制面信令传输被非法篡改和窃取。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓		
措施详细描述	<p>MT-1-1: 终端采取加密措施，对终端和 gNB/5GC 之间控制面信令（包括 AS 和 NAS 层）进行加密。</p> <p>MT-1-2: 终端采取完整性保护措施，对终端和 gNB 之间用户面数据和控制面信令（包括 AS 和 NAS 层）进行完整性保护。</p> <p>MT-1-3: 终端应支持 3GPP 标准中要求的机密性和完整性保护算法，包括 NEA0, 128-NEA1, 128-NEA2, 128-NEA3, 128-NIA1, 128-NIA2 和 128-NIA3。</p> <p>MT-1-4: 如果终端支持通过 ng-eNB 连接到 5GC，应支持 LTE 网络的 RRC 和 NAS 完整性和机密性算法。</p> <p>MT-1-5: 除 3GPP 规定的未经认证的紧急会话等场景，终端与 5G 网络之间的 RRC 和 NAS 信令完整性保护算法不得使用 NIA0。</p>			
适用的资产	终端			
设施主体	设备厂商（主要是终端厂商）		MT-1-1, MT-1-2, MT-1-3, MT-1-4, MT-1-5	
是否已有标准要求	是			
标准名称	3GPP TS 33.501: Security architecture and procedures for 5G System			

	YD/T 3628-2019 《5G 移动通信网 安全技术要求》				
实施难度					

A.1.2 MT-2 用户凭证的安全保护

措施编号	MT-2			
措施名称	用户凭证的安全保护			
安全需求	保护终端存储、处理和传输 5G 网络中凭证的安全性，保障终端唯一凭证的合法性。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓		
措施详细描述	<p>MT-2-1: 终端使用防篡改的安全硬件组件，对终端内的用户凭证进行完整性保护。</p> <p>MT-2-2: 终端内用户凭证的认证算法应在防篡改安全硬件组件内执行。</p> <p>MT-2-3: 终端内用户凭证的长期密钥（即 K 值）使用防篡改安全硬件组件进行机密性保护，如采用加密存储、通过 HTTPS/SFTP 安全协议传输等。</p> <p>MT-2-4: 终端在与 5G 网络的通信过程中采用 SUCI 和 5G-GUTI，对 SUPI 信息进行保护，除未经认证的紧急呼叫等场景，终端不能在 NG-RAN 传输 SUPI 明文。</p> <p>MT-2-5: 归属网络公钥和 SUPI 保护方案应存储在终端 UICC 中，标识应存储在 UICC 中。</p> <p>MT-2-6: UICC 配置和更新归属网络公钥、UICC 开启 SUPI 隐私保护机制应由归属运营商网络控制。</p> <p>MT-2-7: 通过尝试访问次数限制等措施防止物理 UICC 被暴力攻击访问。</p> <p>MT-2-8: 终端具备 GSMA 安全规则定义的唯一合法 IMEI 标识。</p>			

适用的资产	终端				
实施主体	运营商		MT-2-6		
	设备厂商（终端厂商）		MT-2-1, MT-2-2, MT-2-3, MT-2-4, MT-2-5, MT-2-7, MT-2-8		
是否已有标准要求	是				
标准名称	3GPP TS 33.501: Security architecture and procedures for 5G System YD/T 3628-2019 《5G 移动通信网 安全技术要求》 GB/T 35278-2017 《信息安全技术 移动终端安全保护技术要求》				
实施难度					

A.1.3 MT-3 终端接入认证

措施编号	MT-3			
措施名称	终端接入认证			
安全需求	终端通过接入认证机制接入 5G 网络，防范恶意终端非法接入 5G 网络使用 5G 网络服务或发起 DoS 等网络攻击。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓	✓	
措施详细描述	MT-3-1：终端应支持 3GPP 网络的主认证机制，支持 EPS-AKA’和 5G-AKA 认证机制。 MT-3-2：在特定场景下，终端支持主认证之外的二次认证机制，可与外部 AAA 进行二次认证。 MT-3-3：在特定场景下，终端支持 GBA 认证或 AKMA 认证机制，与外部 AAA 进行认证，并使用衍生的密钥（如 K _{AF} ）进行数据完整性和机密性保护。			
适用的资产	终端			

实施主体	设备厂商（终端厂商）	MT-3-1, MT-3-2, MT-3-3, MT-3-4
是否已有标准要求	是	
标准名称	3GPP TS 33.501: Security architecture and procedures for 5G System YD/T 3628-2019 《5G 移动通信网 安全技术要求》	
实施难度	<div></div> <div></div> <div></div> <div></div> <div></div>	

A.1.4 MT-4 终端访问限制

措施编号	MT-4			
措施名称	终端访问限制			
安全需求	通过限制黑名单或行为异常的特定终端接入 5G 网络，防范终端被非法劫持使用 5G 网络服务或发起 DoS 等网络攻击。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓	✓	
措施详细描述	MT-4-1: 5G 网络基于终端的 IMSI/SUPI、CGI、TAI 等用户标识和位置标识，对终端做 5G 网络限制接入。 MT-4-2: 5G 网络对非法 IMEI（如 IMEI 黑名单）的终端进行 5G 网络访问限制。 MT-4-3: 通过流量限制、机卡绑定等措施，对终端接入 5G 网络进行限制。			
适用的资产	终端			
实施主体	运营商		MT-4-1， MT-4-2 ， MT-4-3	
是否已有标准要求	是			
标准名称	3GPP TS 33.501: Security architecture and procedures for 5G System YD/T 3628-2019 《5G 移动通信网 安全技术要求》			

实施难度						
------	--	--	--	--	--	--

A.2 接入网安全（Radio Network, RN）

A.2.1 RN-1 基站用户数据和信令保护

措施编号	RN-1			
措施名称	基站用户数据和信令保护			
安全需求	保护经过 5G 基站的用户数据和信令流量的机密性和完整性，防止未经授权的信息窃听和篡改。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓		
措施详细描述	<p>RN-1-1: gNB 与终端之间的空口应支持 AS 层的 RRC 控制面信令和用户面的完整性和机密性保护机制。</p> <p>RN-1-2: 保护 gNodeB 和核心网之间的 N2/N3 接口传输安全，如在适当的情况下部署 IPsec，提供控制面和用户面数据的完整性和机密性保护。</p> <p>RN-1-3: 保护 eNodeB 和 gNodeB 之间的 X2 接口，gNodeB 之间的 Xn 接口，如在适当的情况下部署 IPsec，提供控制面和用户面数据的完整性和机密性保护。</p> <p>RN-1-4: 基站的加密算法机制采用 3GPP 国际标准中要求的最强机制，支持禁用 NIA0 算法。</p> <p>RN-1-5: 基站采取抗重放保护机制，对重放的 RRC 信令 and 用户面数据进行识别和丢弃。</p> <p>RN-1-6: 基站采用访问限制、加密存储等机制，对基站侧的密钥信息（如 K_{gNB}, K_{RRC}, K_{UP} 等）进行安全存储。</p>			
作用资产	gNodeB			
实施主体	设备厂商		RN-1-1, RN-1-2, RN-	

		1-3, RN-1-4, RN-1-5, RN-1-6
是否已有标准要求	是	
标准名称	3GPP TS 33.501: Security architecture and procedures for 5G System 3GPP TS 33.511: Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class YD/T 3628-2019 《5G 移动通信网 安全技术要求》	
实施难度		

A.2.2 RN-2 伪基站检测及防护

措施编号	RN-2		
措施名称	伪基站检测及防护		
安全需求	对 5G 伪基站进行检测，防止因伪基站向终端发送虚假信息造成的终端拒绝服务、隐私信息泄露以及用户欺诈等后果。		
措施作用（CIA）	机密性	完整性	可用性
			✓
措施详细描述	RN-2-1: 使用网管或信令监控系统，通过以下方式检测和定位伪基站是否存在： <ul style="list-style-type: none"> •客户投诉：根据客户的欺诈呼叫或消息相关的投诉，结合掉话发生的地理位置信息，确定伪基站可能运行的区域。 •蜜罐技术：通过专用的终端设备检测伪基站，例如 SnooopSnitch 应用程序。 •无线电检测：通过无线电设备监测以下参数来检测来自伪基站的无线电信号，以识别不寻常的模式。 1) DBE 连续性		

	<p>2) LAC/Cell ID 连续性</p> <p>3) 周边基站</p> <p>4) 信号强度</p> <p>5) 静默消息的存在</p> <p>6) 毫微微蜂窝基站的存在</p> <p>7) 使用较弱的算法（如 A5/1、A5/2 和 A5/0 空）</p> <p>8) 手机发送到网络的测量报告异常。</p> <p>RN-2-2：配置网络监控系统，识别并标记网络地理区域中的异常流量波动，查看是否有不明信号/基站迫使用户 UE 驻留。持续监控物理网络的异常、死点、服务中断区域，以帮助识别网络是否正在使用虚假基站进行攻击。</p> <p>RN-2-3：使用终端设备向基站和网络发送测量报告，参考 3GPP TS 33.501 中的附录 E，检测基站的签名判断是否为虚假基站。</p> <p>RN-2-4：国家当局和运营商应依据《中华人民共和国无线电管理条例》等，起诉和惩罚未经授权使用受管制无线电频谱的罪犯。</p>				
作用资产	gNodeB，终端				
实施主体	运营商			RN-2-1 ， RN-2-2 ， RN-2-3	
	监管部门			RN-2-4	
是否已有标准要求	是				
标准名称	YD/T 3167-2016《移动伪基站网络侧监测技术要求》				
实施难度					

A.2.3 RN-3 基站可用性保护

措施编号	RN-3
措施名称	基站可用性保护

安全需求	保护基站的可用性及用户体验，防止大量空口异常链接请求，消耗网络资源，导致网络服务拒绝。				
措施作用（CIA）	机密性	完整性	可用性		
			✓		
措施详细描述	RN-3-1：通过网管监控 5G 基站的 KPI，如 RRC 连接建立成功率/阻塞率、E-RAB 建立成功率/阻塞率、掉话率等，发现和检测可能的恶意连接等情况。 RN-3-2：在基站设备中启用访问控制，对发现得异常终端连接和流量进行过滤控制。				
作用资产	gNodeB				
实施主体	运营商		RN-3-1		
	设备厂商（终端厂商）		RN-3-2		
是否已有标准要求	是				
标准名称	YD/T 3167-2016 《移动伪基站网络侧监测技术要求》				
实施难度					

A.2.4 RN-4 降低无线电干扰风险

措施编号	RN-4			
措施名称	降低无线电干扰风险			
安全需求	避免 5G 基站空口因无线电干扰导致正常用户无线信号无法被基站识别，从而影响正常用户无法使用 5G 网络。			
措施作用（CIA）	机密性	完整性	可用性	
			✓	
措施详细描述	RN-4-1：通过部署 RN-2-1 中的伪基站检测解决方案来检测和定位干扰设备。 RN-4-2：通过干扰源定位技术，对 5G 基站授权频段带内和带外的信号干扰源进行定位。			

	RN-4-3: 使用设备发送到网络（用于切换和自组织网络等目的）的测量报告来检测 RN-2-2 3GPP 33.501 附录 E 中所述的虚假基站的签名。				
作用资产	gNodeB				
实施主体	运营商			RN-4-1, RN-4-2, RN-4-3	
是否已有标准要求	是				
标准名称	YD/T 3167-2016《移动伪基站网络侧监测技术要求》				
实施难度					

A.2.5 RN-5 基站物理安全保护

措施编号	RN-5			
措施名称	基站物理安全保护			
安全需求	对基站进行物理安全防护，确保基站免受物理破坏或近端入侵。			
措施作用（CIA）	机密性	完整性	可用性	
			√	
措施详细描述	<p>RN-5-1：确保实施物理站点安全控制，包括：</p> <p>1）采用生物识别门禁、视频监控、入侵告警、关闭物理端口等技术手段组合加强物理安全防护，定期对设备安全状态进行巡检，降低设备被物理入侵的风险。</p> <p>2）为设备物理维护建立访问记录，并定期进行审计。</p> <p>3）严格落实机房出入安全管理、网络接入安全管理制度。</p> <p>RN-5-2：确保基站的接口、管理通道安全，包括：</p> <p>1）部署硬件端口加固措施，对未使用的端口默认关闭，端口状态更改向网管上报告警信息，禁用远程端</p>			

	<p>口等。</p> <p>2) 部署操作系统加固措施，禁用非必要的服务，设置文件或目录的访问权限，对基站访问记录审计。</p> <p>RN-5-3: 基站部署安全环境技术（例如安全启动、安全运行、安全存储等），防范软硬件被篡改和敏感信息被窃取。</p> <p>RN-5-4: 政府及管制机构依据保护运营商基础设施的法律法规，对非法破坏、入侵运营商基础设施的行为进行打击和惩罚。</p>					
作用资产	gNodeB					
实施主体	运营商			RN-5-1, RN-5-2		
	设备厂商（终端厂商）			RN-5-3		
	监管部门			RN-5-4		
是否已有标准要求	是					
标准名称	<p>YDT/5202-2015 《移动通信基站安全防护技术暂行规定》</p> <p>YD/T 1754-2008 《电信和互联网物理环境安全等级保护要求》</p>					
实施难度						

A.3 多接入边缘计算安全 (Multi-access Edge Computing, MEC)

A.3.1 MEC-1 物理环境安全防护

措施编号	MEC-1
措施名称	物理环境安全防护
安全需求	通过部署安全防护措施，保护MEC物理环境安全。物理安全主要包括5G MEC平台基础设施所处的物理环境在机房位置、电力供应、防盗窃、防火、防水、防静电、温湿度控制、电磁防护等方面的安全防护要求。

措施作用（CIA）	机密性	完整性	可用性	
			✓	
措施详细描述	MEC-1-1：部署于 MEC 平台的机房环境，在机房位置、电力供应、防火、防水、防静电、温湿度控制、防雷击、防盗窃和防破坏、电磁防护、人员进出等方面应满足 YD/T 1754-2008《电信和互联网物理环境安全等级保护要求》中的第 3.1 和 3.2 级要求。 MEC-1-2：MEC 系统机房出入口配置电子门禁系统，控制、鉴别和记录进入的人员，机柜部署电子防拆封功能，并记录、审计打开和关闭机柜的行为。边缘计算设备应是可信设备，应防止非法设备接入系统。			
适用的资产	MEC			
实施主体	安全厂商		MEC-1-1, MEC-1-2	
是否已有标准要求	是			
标准名称	YD/T 1754-2008 《电信和互联网物理环境安全等级保护要求》			
实施难度				

A.3.2 MEC-2 组网安全防护

措施编号	MEC-2			
措施名称	组网安全防护			
安全需求	通过组网安全防护措施，保护UPF、MEC平台与5G网络之间的组网安全，防止攻击者从外部网络（如互联网）入侵MEP，造成MEP应用被非法访问，或者进一步攻击与MEC连接的UPF和核心网。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓	✓	
措施详细描述	MEC-2-1：通过物理或逻辑隔离的方式，对组成MEC系统的服务器、交换机等设备的管理、业务和存储三			

	<p>平面进行隔离（隔离方式应根据业务应用安全需求来选择）。</p> <p>MEC-2-2: 通过物理或逻辑隔离的方式，对行业用户应用与运营商 MEC 应用、MEP、UPF 进行安全隔离，对行业应用之间、运营商自有应用之间进行安全隔离（隔离方式应根据业务应用安全需求来选择）。</p> <p>MEC-2-3: 对于有 Internet 访问需求的场景，根据业务访问需求设置 DMZ 区（如 IP 地址暴露在 Internet 的管理入口等部署在 DMZ 区），并在边界部署抗 DDoS 攻击、入侵检测、访问控制、Web 流量检测等安全能力，实现边界安全防护。</p> <p>MEC-2-4: 设置 UPF 白名单规则，针对 N4、N6、N9 接口分别设置专门的 VRF，在 UPF 的 N6 接口部署网络防火墙进行流量安全控制。</p> <p>MEC-2-5: 对于 MEC 部署在广域场景下，MEC 和 UPF 部署在运营商边缘汇聚机房，行业应用部署在运营商 MEP，可通过 MEC-2-1/MEC-2-2/MEC-2-3/MEC-2-4 的措施进行安全防护。</p> <p>MEC-2-6: 对于 MEC 部署在园区的场景下，除 MEC-2-1/MEC-2-2/MEC-2-3/MEC-2-4 措施外，园区 UPF 和 MEP 均与 MEC 应用之间进行安全隔离，通过 VLAN 等方式对 MEC 应用之间进行隔离，对 UPF 和 SMF 的 N4 接口流量进行安全访问控制，并在园区 MEC 与核心网之间部署网络防火墙进行安全流量控制。</p> <p>MEC-2-7: 针对 MEC 专网部署场景，UPF 仅作转发，行业 MEC 应用部署在自己或第三方 MEP 中，MEP 和</p>
--	---

	UPF 根据广域或园区部署方式采取 MEC-2-5 和 MEC-2-6 的措施。					
适用的资产	MEP、MEC APP、UPF					
实施主体	运营商		MEC-2-1, MEC-2-2, MEC-2-3, MEC-2-4, MEC-2-5, MEC-2-6, MEC-2-7			
	设备厂商		MEC-2-4, MEC-2-5, MEC-2-6, MEC-2-7			
	垂直行业		MEC-2-7			
是否已有标准要求	暂未发布					
标准名称	/					
实施难度						

A.3.3 MEC-3 基础设施安全防护

措施编号	MEC-3			
措施名称	基础设施安全防护			
安全需求	通过部署安全防护措施，保护MEC基础设施安全，防范由于基础设施存在漏洞、配置缺陷、防护措施不当或故障造成MEC服务不可用。MEC基础设施主要是为上层MEC应用和服务运行提供计算、存储、网络等资源的底层基础设施，包括计算服务器、存储服务器、硬件加速卡等设备和硬件实体，以及NFVI等虚拟化基础设施。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓	✓	
措施详细描述	MEC-3-1: MEC基础设施具备身份鉴别机制，包括： <ul style="list-style-type: none">对MEP登录用户进行身份标识和鉴别，身份标识具有唯一性，口令等身份鉴别信息应有复杂度要求			

	<p>并定期更换，具备限制登录次数等登录失败处理措施，通过通道加密保护鉴别信息传输安全；</p> <ul style="list-style-type: none"> • 对系统进行管理的人机接口以及跨信任网络的接口都需具备接入认证机制。 • 登录访问界面支持主动退出选项，当用户退出时，服务器清除该用户的会话信息。设置会话超时机制，在超时过后清除该会话信息。用户登录认证通过后必须更换会话标识，以防止会话固定（Session Fixation）漏洞。 <p>MEC-3-2: MEC 平台应具备访问控制措施，对用户进行访问权限控制，包括：</p> <ul style="list-style-type: none"> • 根据管理用户的角色授予其所需的最小权限，实现管理用户的权限分离。 • 通过设定终端接入方式、网络地址范围等对合法访问终端的对象进行限制。 • 配置程序中连接数据库系统的帐号不能是数据库系统最高权限的帐号，对程序产生的关键信息文件、配置只能被相应权限的用户访问。 • 在MEC应用用户授权下，MEC平台或第三方才具有MEC用户数据的管理权限。 • 配置MEP平台的服务只监听所需的网络接口、IP地址和端口。 <p>MEC-3-3: MEC 应具备入侵防范措施，包括最小化安装软件原则、关闭不需要的系统服务/端口、支持漏洞监测和及时修补、部署防恶意代码软件/入侵监测系统、对设备进行安全基线配置、支持敏感数据（如口令）的加密传输和存储、支持软件包校验等。</p> <p>MEC-3-4: 对连接 MEC 的 UPF 进行安全防护，包括：</p> <ul style="list-style-type: none"> • UPF 对上行和下行流量进行防地址欺骗检查，
--	---

	<p>若报文的源地址或目的地址与终端用户地址不匹配，UPF 丢弃该报文。</p> <ul style="list-style-type: none"> • UPF 对没有匹配 PDP 上下文/承载的下行流量进行丢弃，UPF 将 GTP 解封装后的流量仅转发至外部指定的数据网络。 • UPF 支持 ACL 过滤功能，拦截配置的网络地址和端口，对拦截次数进行统计。在采用隧道封装情况时，对解封装后的 IP 包进行 ACL 过滤。 • UPF 具备告警能力，例如出现上下行流量地址欺骗，没有匹配 PDU 会话/承载的下行流量等情况时，UPF 报告告警信息。 • UPF 支持 L2TP 和 IPSec 隧道配置，支持安全启动技术，保证设备启动链的完整性，防止被植入后门。 <p>MEC-3-5: 对 MEC 进行安全审计，对用户行为、系统资源的异常使用、系统命令的使用和安全事件进行审计，审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。审计记录应按有关法律法规要求进行留存，并进行审计记录防篡改和防窃取保护。</p> <p>MEC-3-6: MEC 应具备资源管理机制，保证虚拟机仅能使用为其分配的计算资源，限制单个用户或进程对系统资源的最大使用限度，并通过资源预留等方式确保某个虚拟机崩溃后不影响虚拟机监视器及其他虚拟机运行。</p>	
适用的资产	MEC NFVI、UPF	
实施主体	运营商	MEC-3-1, MEC-3-2, MEC-3-3, MEC-3-4, MEC-3-5, MEC-3-6

	设备厂商	MEC-3-1, MEC-3-2, MEC-3-4, MEC-3-6
是否已有标准要求	是	
标准名称	ETSI GS MEC 009: Multi-access Edge Computing (MEC); General principles, patterns and common aspects of MEC Service APIs 3GPP TS 33.513: 5G Security Assurance Specification (SCAS); User Plane Function (UPF)	
实施难度	<div style="display: flex; width: 100%; height: 20px; border: 1px solid black;"> <div style="width: 25%; background-color: #cccccc;"></div> <div style="width: 25%; background-color: #cccccc;"></div> <div style="width: 25%; background-color: #cccccc;"></div> <div style="width: 25%; background-color: #cccccc;"></div> </div>	

A.3.4 MEC-4 虚拟化安全防护

措施编号	MEC-4			
措施名称	虚拟化安全防护			
安全需求	容器或虚机是 MEC 的主要部署方式，通过部署虚拟化安全防护措施，防范攻击者利用 Host OS 或虚拟化软件漏洞篡改容器或虚机镜像，或针对容器或虚机发起容器逃逸、DDoS 等攻击。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓	✓	
措施详细描述	<p>MEC-4-1: 禁止使用不必要的宿主机外接设备，禁止安装不必要的系统组件，禁止启动不必要的应用程序，禁止弱口令登录，配置宿主机资源访问控制权限，对 Host OS、虚拟化软件、Guest OS 进行安全加固。</p> <p>MEC-4-2: 开启镜像完整性校验，使用安全的传输通道上传镜像，使用经过安全校验和安全存储的镜像来创建虚拟机和容器。</p> <p>MEC-4-3: Hypervisor 设置 VM 的操作权限及每个 VM 使用资源的限制，对同一物理主机上不同虚拟机之间的资源进行隔离，并对资源使用情况进行监控。</p> <p>MEC-4-4: 容器开发阶段应要求开发者对容器镜像及中</p>			

	<p>间过程镜像进行漏洞扫描，同时对第三方甚至自有应用/代码进行安全检查。部署阶段应由 MEC 平台对镜像仓库进行安全监管，对上传的第三方/自有容器镜像进行漏洞扫描，控制有高危漏洞的容器镜像的运行使用。运行阶段首先应支持容器实例跟宿主机之间的内核隔离。</p> <p>MEC-4-5: 在容器环境内部使用防火墙机制防止容器之间的非法访问，对环境内的第三方进程进行监控，发现容器实例运行中的非法或恶意行为；在虚拟化平台层面部署 API 安全网关来对容器管理平台的 API 调用情况进行安全监控，防止非法恶意 API 调用。</p> <p>MEC-4-6: 虚拟化编排管理实体进行安全加固，登录需要进行认证授权。编排管理实体与被管理实体间应进行认证授权，防止管理面被攻击。</p>	
适用的资产	MEC NFVI、MEAO、VNFM、NFVO、Hypervisor、Docker/Kubernetes 等	
实施主体	运营商	MEC-4-1, MEC-4-2, MEC-4-3, MEC-4-4, MEC-4-5, MEC-4-6
	设备厂商（终端厂商）	MEC-4-4
是否已有标准要求	是	
标准名称	<p>ETSI GS NFV-SEC 013: “Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification</p> <p>ETSI GS NFV-SEC 012: Network Functions Virtualisation (NFV) - Release 3; Security; System architecture specification for execution of sensitive NFV components</p> <p>ETSI GS NFV-SEC 022: Network Functions Virtualisation (NFV) Release 2; Security; Access Token Specification for API Access</p>	

	ETSI GS NFV-SEC 023: Network Functions Virtualisation (NFV); Security; Container Security Specification - Release 4 ETSI GS NFV-SEC 026: Network Functions Virtualisation (NFV) Release 4; Security; Isolation and trust domain specification - Release 4
实施难度	<div><div></div><div></div><div></div><div></div><div></div></div>

A.3.5 MEC-5 边缘计算平台安全防护

措施编号	MEC-5			
措施名称	边缘计算平台安全防护			
安全需求	5G 边缘计算平台 MEP 本身是基于虚拟化基础设施部署，对外提供应用的发现、通知的接口。通过实施安全防护措施保护 MEP，防止攻击者或者恶意应用对 MEP 的服务接口进行非授权访问，拦截或者篡改 MEP 与 APP 等之间的通信数据，防止攻击者通过恶意应用访问 MEP 上的敏感数据，窃取、篡改和删除用户的敏感隐私数据。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓	✓	
措施详细描述	<p>MEC-5-1: 通过安全措施保障 MEP 对外提供应用的发现、通知的 API 接口安全，包括：</p> <ul style="list-style-type: none">• 对 MEP 的访问需要进行认证和授权，防止恶意的应用对 MEP 的非授权访问。MEP 应支持防(D)DoS 攻击，MEP 的敏感数据应启用安全保护，防止非授权访问和篡改等。• 为防止 MEP 与 APP 等之间的通信数据被拦截、篡改，MEP 与 APP 等之间的数据传输应启用机密性、完整性、防重放保护。			

	<ul style="list-style-type: none"> • 边缘计算系统中的标准接口应支持通信双方之间的相互认证，并在认证成功后，使用安全的传输协议保护通信内容的机密性和完整性。边缘计算系统应使用安全的标准通信协议，如 SSHv2，TLS v1.2 及以上版本 SNMP v3 等，禁止使用 Telnet，FTP，SSHv1 等。 <p>MEC-5-2: MEC 应对终端用户使用边缘计算服务进行授权，只有具备合法授权的用户才能使用对应的边缘计算服务。</p> <p>MEC-5-3: 终端用户在 MEC 应用服务器发生切换时，安全上下文应从源 MEC 服务器传递到其他 MEC 服务器，以保证用户服务连续性。</p> <p>MEC-5-4: 对接入到运营商核心网络、边缘计算节点的终端进行身份识别，并根据事先确定的策略确定是否允许接入。</p> <p>MEC-5-5: 对于接入关键核心业务的终端，考虑基于零信任理念进行动态持续的安全与信任评估，一旦发现安全与信任异常，应采取合适的管控策略限制终端访问。</p>	
适用的资产	MT、MEP	
实施主体	运营商	MT-5-1, MEC-5-2, MEC-5-3, MEC-5-4, MEC-5-5
	设备厂商	MEC-5-1, MEC-5-5
	安全厂商	MEC-5-5
是否已有标准要求	暂未发布	
标准名称	/	

实施难度						
------	--	--	--	--	--	--

A.3.6 MEC-6 应用安全防护

措施编号	MEC-6			
措施名称	应用安全防护			
安全需求	对 MEP 上的 APP 进行安全保护，防止 APP 之间的非法访问，防止第三方 APP 通过恶意消耗 MEC 系统资源造成系统服务不可用。通过有效的数据备份、恢复、以及审计措施，防止攻击者修改或删除用户在边缘节点上的数据。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓	✓	
措施详细描述	<p>MEC-6-1：对不同业务类型应用之间的隔离和互访过程做安全监控。</p> <p>MEC-6-2：对 MEC 应用的生命周期管理，防止 MEC APP 被非法创建、修改及删除。</p> <p>MEC-6-3：对 MEC APP 之间的网络做安全隔离，MEC APP 之间的访问启用授权机制。</p> <p>MEC-6-4：对 MEC APP 访问 MEP 的资源情况进行实时监控，并对 APP 资源消耗做限制。</p> <p>MEC-6-5：对第三方 MEC 应用进行漏洞扫描及加固，对其镜像进行病毒查杀。</p> <p>MEC-6-6：当 MEC 应用以虚拟机或容器部署时，相应的虚拟化基础设施应支持 MEC 应用使用的虚拟 CPU、虚拟内存以及 I/O 等资源与其它虚拟机或容器使用的资源进行隔离。对 MEC APP 的镜像和镜像仓库进行完整性和机密性、访问控制保护等，具体可参考 MEC-4 容器和镜像安全要求。</p>			
适用的资产	MEC APP			

实施主体	运营商				MEC-6-1, MEC-6-2, MEC-6-3, MEC-6-4, MEC-6-5, MEC-6-6
	设备厂商				
	安全厂商				
是否已有标准要求	暂未发布				
标准名称	/				
实施难度					

A.3.7 MEC-7 能力开放安全防护

措施编号	MEC-7			
措施名称	能力开放安全防护			
安全需求	MEC 为用户提供开放 API，允许用户访问 MEC 相关的数据和功能。需要通过 API 进行安全防护，防止攻击者通过仿冒终端接入、漏洞攻击、侧信道攻击等手段，达到非法调用 API、非法访问或篡改用户数据等恶意攻击目的。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓	✓	
措施详细描述	MEC-7-1：参考 3GPP TS 23.222 定义的 CAPIF 框架，对 API 进行安全的管理、发布和开放，对 API 调用方进行认证和授权，从而保证边缘网络能力开放的安全性。 MEC-7-2：边缘应用服务器需要调用运营商网络的能力开放，获取终端用户的敏感信息（如位置信息）时，需要获取客户同意，且客户需要掌握哪些 MEC 应用以何种频率获取终端用户的指定信息。			
适用的资产	MEP			
实施主体	运营商		MEC-7-1， MEC-7-2	
	设备厂商		MEC-7-1	
是否已有标准要求	是			

标准名称	3GPP TS 23.222: Common API Framework for 3GPP Northbound APIs				
实施难度					

A.3.8 MEC-8 通信安全防护

措施编号	MEC-8			
措施名称	通信安全防护			
安全需求	MEC通信主要包括MEC内部通信（如应用、MEP之间以及核心网元之间的通信）和MEC间的通信（如用户移动切换中的用户上下文转发、EAS重分配等交互过程）。需要通过通信安全措施，对MEC内部和MEC之间服务访问和数据转发等通信过程进行保护。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓	✓	
措施详细描述	<p>MEC-8-1：对MEC之内或之间的数据传输部署安全通道，例如使用NDS/IP或TLS（参考协议3GPP TS 33.210和3GPP TS 33.310）进行认证和保护。</p> <p>MEC-8-2：MEC之内或之间的服务访问需要进行认证授权，可选的方案有部署Oauth或基于CAPIF进行认证和授权。</p> <p>MEC-8-3：MEC和5GC之间部署可部署防火墙隔离进行边界防护，防火墙能识别N4消息，仅信令及OM相关的数据流量才能通过防火墙。</p>			
适用的资产	UPF、SMF、MEC			
实施主体	运营商		MEC-8-1, MEC-8-2, MEC-8-3	
	设备厂商		MEC-8-1, MEC-8-2	
	安全厂商		MEC-8-3	
是否已有标准要求	是			
标准名称	3GPP TS 33.210: Network Domain Security (NDS); IP			

	network layer security 3GPP TS 33.310: Network Domain Security (NDS); Authentication Framework (AF)					
实施难度						

A.3.9 MEC-9 管理运维安全

措施编号	MEC-9			
措施名称	管理运维安全			
安全需求	边缘计算节点分布式的部署方式为运营商管理和运维带来挑战。通过安全管理运维措施，有效防止恶意内部人员非法访问，使用弱口令或漏洞进行攻击，并对 MEC 安全状态进行监控，及时进行安全措施调整和响应。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓	✓	
措施详细描述	<p>MEC-9-1: 通过收集物理安全设备、虚拟安全设备、应用层安全设备相关告警日志，上报至态势感知系统进行分析，进行安全事件预警。</p> <p>MEC-9-2: 针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程。</p> <p>MEC-9-3: 通过统一接入门户对宿主机、虚拟机、云管理平台、MEC 管理平台以及虚拟网元、第三方应用的用户进行统一管理。记录其登录/登出以及相关的命令操作。</p> <p>MEC-9-4: 通过 UEBA 技术绘制用户行为肖像并生成相应安全策略。当用户出现异常操作时，发生告警并阻止相关操作。</p>			

	<p>MEC-9-5: 对用户信息、配置信息、镜像信息、软件包等关键数据的流转进行记录，形成数据流转路径。当发生数据泄露事件时，为事件追溯提供证据。</p> <p>MEC-9-6: 对宿主机、虚拟机、物理网络设备、虚拟网络设备、镜像、应用软件包（网元、第三方应用）进行基线核查，确保平台本身以及上层应用的安全性。</p> <p>MEC-9-7: 对接入到 MEC 的设备进行生命周期管理，定期远程更新所有边缘设备和节点，维护管理补丁升级和固件升级，及时修补漏洞。</p> <p>MEC-9-8: 通过统一的安全态势感知、协同防御能力建设，实现边云协同态势感知，对恶意软件、恶意攻击等行为进行检测。</p>					
适用的资产	MEC					
实施主体	运营商		MEC-9-1, MEC-9-2, MEC-9-3, MEC-9-4, MEC-9-5, MEC-9-6, MEC-9-7, MEC-9-8			
	设备厂商		MEC-9-4, MEC-9-5, MEC-9-6 , MEC-9-7			
	安全厂商		MEC-9-1, MEC-9-4, MEC-9-6, MEC-9-8			
是否已有标准要求	暂未发布					
标准名称	/					
实施难度						

A.3.10 MEC-10 数据安全防护

措施编号	MEC-10
措施名称	数据安全防护

安全需求	5G 边缘计算平台可收集、存储与其连接设备的数据，包括应用数据、用户数据等。需要通过数据安全保护措施，对 5G MEC 的各类数据进行保护，防止数据损毁、数据泄露、数据篡改等安全风险。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓	✓	
措施详细描述	<p>MEC-10-1: 对于存储的大量数据，需要识别保障业务运行的重要数据并进行安全备份和恢复，避免因数据损毁导致正常业务无法进行。例如，提供异地备份功能，通过安全的通信网络将重要数据备份到异地，支持备份数据一致性检验、备份位置查询等。</p> <p>MEC-10-2: 将涉及用户隐私的数据信息加以标识，在每个 MEC 节点的数据入口通过防火墙进行隔离，按照最小化原则关掉所有不必要的服务及端口，对于增加标识的重要数据进行完整性、机密性及防复制的保护。</p> <p>MEC-10-3: 将入侵检测技术应用于 MEC 节点，对 API 接口的使用者进行检测，防止攻击者获取用户的隐私数据信息。</p> <p>MEC-10-4: 对用户数据中的隐私（如身份信息、位置信息和私密数据等关联到个人的数据）和身份（如智能卡、生物特征等）进行保护，进行加密（如对称加密、非对称加密等）或脱敏（如匿名或假名等），并且加强存储以防数据丢失，保障用户数据的机密性和完整性。</p>			
适用的资产	MEC			
实施主体	运营商		MEC-10-1, MEC-10-2, MEC-10-3, MEC-10-4	
	设备厂商		MEC-10-1, MEC-10-2,	

		MEC-10-4
	安全厂商	MEC-10-1, MEC-10-2, MEC-10-3, MEC-10-4
是否已有标准要求	是	
标准名称	YD/T 3802-2020 《电信网和互联网数据安全通用要求》	
实施难度	<div></div>	

A.4 核心网安全(Core Network, CN)

A.4.1 CN-1 核心网资源可用性保护

措施编号	CN-1			
措施名称	核心网资源可用性保护			
安全需求	保障核心网资源的可用性及用户体验，防止终端用户、漫游接口、基站和传输设备短时间内向网络节点发送大量异常消息，消耗网络资源，导致网络服务拒绝。			
措施作用（CIA）	机密性	完整性	可用性	
			✓	
措施详细描述	CN-1-1: 在 gNodeB 与核心网之间、核心网与互联网之间部署抗 DDoS 设备。 CN-1-2: 在核心网控制平面部署 SEPP，过滤来自漫游网络的攻击信令报文。 CN-1-3: 在核心网设备、抗 DDoS 设备内提供流量控制和 DDoS 攻击模式包过滤机制，对攻击流量进行识别的过滤。			
适用的资产	5GC			
实施主体	运营商		CN-1-1, CN-1-2, CN-1-3	
	设备厂商		CN-1-3	
	安全厂商		CN-1-1	

是否已有标准要求	是					
标准名称	3GPP SCAS Series Specifications(TS 33.117, TS 33.511-522)					
实施难度						

A.4.2 CN-2 5GC NEF 安全保护

措施编号	CN-2			
措施名称	5GC NEF 安全保护			
安全需求	5GC NEF 使用 SECAPIF 框架开放统一 API，API 通过软件实现，有存在漏洞的可能性。通过对 NEF 进行安全防护，防止攻击者通过开放 API 进行数据窃取、篡改、欺骗和拒绝服务攻击。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓	✓	
措施详细描述	<p>CN-2-1：参考行业标准和最佳实践（如 OWASP API Security Top 10），在 NEF 开发过程中对可能存在的 API 漏洞已经进行渗透测试，测试应涵盖主流 API 攻击方式。</p> <p>CN-2-2：制定应急响应计划，在发现 API 漏洞时及时通知受影响客户，并提供补丁和其他缓解措施快速修复漏洞。</p> <p>CN-2-3：使用防火墙、入侵检测等专用安全设备对关键 API 进行外部加固和安全防护。</p> <p>CN-2-4：依据通信行业管理办法，对第三方 APP 的恶意行为（如非法数据收集）进行法律监管。</p>			
适用的资产	5GC			
实施主体	运营商		CN-2-1， CN-2-2, CN-2-3， CN-2-4	
	设备厂商		CN-2-1， CN-2-2	

	安全厂商	CN-2-3
	监管部门	CN-2-4
是否已有标准要求	是	
标准名称	3GPP TS 33.117: Catalogue of general security assurance requirements 3GPP TS 33.519: 5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class	
实施难度	<div> <div></div> <div></div> <div></div> <div></div> <div></div> </div>	

A.4.3 CN-3 核心网流量保护

措施编号	CN-3			
措施名称	核心网流量保护			
安全需求	保护核心网各接口的流量的机密性和完整性，防止用户面和信令面数据被窃听和篡改。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓		
措施详细描述	CN-3-1: gNodeB 和核心网之间的 N2/N3 接口，采用 IPsec（N2/N3）和 DTLS（N2）防护措施。 CN-3-2: 核心网 SBA 接口传输和认证采用 HTTPS 机制。 CN-3-3: 在 N6 接口部署防火墙以隔离 5GC 与互联网之间的数据流量。 CN-3-4: 在 N4 接口部署防火墙，对 N4 信令进行保护。 CN-3-5: 漫游接口 N32 部署 SEPP，并使用 TLS（传输层）或应用层（PRINS）保护机制。			
适用的资产	5GC			
实施主体	运营商		CN-3-1, CN-3-2, CN-3-3, CN-3-4, CN-3-5	

	设备厂商		CN-3-1, CN-3-2, CN-3-5			
	安全厂商		CN-3-3, CN-3-4			
是否已有标准要求	是					
标准名称	3GPP TS 33.501: Security architecture and procedures for 5G System 3GPP TS 33.310: Network Domain Security (NDS); Authentication Framework (AF)					
实施难度						

A.4.4 CN-4 核心网内外边界隔离

措施编号	CN-4			
措施名称	核心网内外边界隔离			
安全需求	在 5GC 部署安全隔离措施，将 5GC 与外部网络、5GC 内部各域之间进行网络隔离，降低入侵横向带来的安全风险。			
措施作用（CIA）	机密性	完整性	可用性	
	✓		✓	
措施详细描述	<p>CN-4-1：对 5GC 进行安全域划分和域间隔离，强化管理面安全方案，通过 VM 隔离、VPC、防火墙等技术实现 5GC 与外部网络的安全隔离。</p> <p>CN-4-2：构建边界、内网、网元入侵检测和态势感知能力，对边界攻击入侵进行监测和发现，并及时调整边界防护策略，对攻击者的网络地址、端口等进行限制。</p> <p>CN-4-3：网元创建时定义访问矩阵，明确安全域内安全组间的访问策略，严格限制安全域内网元之间的访问。</p> <p>CN-4-4：使用安全组技术（如对虚拟机等进行安全分组）和 SIEM 解决方案，实现精细化控制和对横向</p>			

	攻击的持续监控。				
适用的资产	5GC				
实施主体	运营商			CN-4-1, CN-4-2, CN-4-3	
	设备厂商			CN-4-4	
是否已有标准要求	否				
标准名称	/				
实施难度					

A.4.5 CN-5 核心网网元合法身份保障

措施编号	CN-5			
措施名称	核心网网元合法身份保障			
安全需求	5G 核心网采用 SBA 架构，NF 通过在 NRF 中注册进行 NF 发现和访问授权，使用服务化接口进行通信。通过部署通过身份认证机制确保 NF 身份合法，防止 NF 被仿冒带来的安全风险，如信息泄露、篡改等。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓	✓	
措施详细描述	CN-5-1: 开启 NRF 动态授权，通过网元间流量白名单功能限制 NF 之间的访问权限。 CN-5-2: 严格管理 NF 证书发放流程，并定期严格审查证书的合法性和有效性。 CN-5-3: 基于 3GPP 标准，提供并开启核心网网元间的证书认证、动态授权、传输加密等功能。			
适用的资产	5GC			
实施主体	运营商		CN-5-1, CN-5-2	
	设备厂商		CN-5-3	
是否已有标准要求	是			
标准名称	3GPP TS 33.501: Security architecture and procedures for			

	5G System				
实施难度					

A.4.6 CN-6 虚拟化环境保护

措施编号	CN-6			
措施名称	虚拟化环境保护			
安全需求	5GC 部署在虚拟化基础设施上，需要通过虚拟化安全防护措施，保障虚拟化环境的正常服务，防止网络窃听、拦截、数据泄露和越权访问等攻击影响 NF 正常服务。			
措施作用（CIA）	机密性	完整性	可用性	
	✓		✓	
措施详细描述	<p>CN-6-1: 建议指定一个主集成商对 5G 核心网的虚拟化组件的整体安全解决方案进行部署。</p> <p>CN-6-2: 通过 HASH 校验等措施验证 VNF 包和 VNF 映像是否完整，确保仅有正确签名的 VNF 镜像才能实例化 VNF。</p> <p>CN-6-3: VNF 与 VNFM 之间的通信进行 HTTPS 双向认证，VNF 采用 OAuth 机制对 VNFM 进行授权访问。</p> <p>CN-6-4: 对虚拟机或容器进行物理机资源访问的权限控制，虚拟化层能对 VNF 的异常内存访问进行拒绝，防止虚拟机或容器逃逸。</p> <p>CN-6-5: 使用业界认可的虚拟化组件，并对虚拟化组件进行安全加固，并及时更新补丁。</p>			
适用的资产	Core Network			
实施主体	运营商		CN-6-1, CN-6-2, CN-6-3	
	设备厂商		CN-6-1, CN-6-3, CN-6-4, CN-6-5	

是否已有标准要求	是					
标准名称	3GPP TS 33.501: Security architecture and procedures for 5G System ETSI GG NFV-SEC Series Specifications					
实施难度						

A.4.7 CN-7 用户标识保护

措施编号	CN-7				
措施名称	用户标识保护				
安全需求	使用用户标识匿名化技术以保护核心网中用于识别和跟踪单个用户的标识，包括 SUPI、GPSI 等，防止用户身份信息泄露。				
措施作用（CIA）	机密性	完整性	可用性		
	✓	✓			
措施详细描述	CN-7-1: 核心网 NF 对终端进行认证之后，为终端分配 3GPP 标准中定义的临时标识符（如 GUTI），以保护用户真实身份标识。 CN-7-2: 核心网 UDM 在鉴权过程中网元应能对用户 SUPI 和 SUCI 之间进行加解密，对用户 SUPI 进行保护。				
适用的资产	5GC				
实施主体	运营商			CN-7-1, CN-7-2	
	设备厂商			CN-7-1, CN-7-2	
是否已有标准要求	是				
标准名称	3GPP TS 33.501: Security architecture and procedures for 5G System				
实施难度					

A.4.8 CN-8 漫游安全

措施编号	CN-8
------	------

措施名称	漫游安全				
安全需求	在 5G 网络漫游接口上部署安全防护措施，保护 5G 与其他网络之间、不同运营商 5G 网络之间的漫游和互连消息及用户免受窃听、篡改等攻击，防范漫游和互连互通网元被非授权访问。				
措施作用（CIA）	机密性	完整性	可用性		
	✓	✓			
措施详细描述	<p>CN-8-1：在国内跨网络/跨运营商、国际信令的漫游接口上部署信令防火墙（如 SEPP），提供外部网络的访问认证能力，对漫游信令消息进行加密和完整性保护，并对网络外部的攻击流量进行识别和阻断。</p> <p>CN-8-2：在属于不同运营商网络的 UPF 之间、以及拜访地与归属地 UPF 之间的 N9 接口上开启 IPsec 等通信加密功能。</p> <p>CN-8-3：对属于不同网络域的互联互通网元（如 SMF、AMF）分配不相交的 IP 地址段，禁用从互联网或终端 IP 地址访问漫游和互连网元。</p> <p>CN-8-4：在连通漫游网络之间的路由器或交换机上配置独立的虚拟路由或 VLAN 保持网络隔离。</p>				
适用的资产	5GC				
实施主体	运营商			CN-8-1, CN-8-2, CN-8-3, CN-8-4	
是否已有标准要求	是				
标准名称	3GPP TS 33.501: Security architecture and procedures for 5G System				
实施难度					

A.5 网络切片安全(Network Slice, NS)

A.5.1 NS-1 终端接入切片安全

措施编号	NS-1				
措施名称	终端接入切片安全				
安全需求	通过部署切片安全认证措施，保证合法的 UE 接入网络切片。				
措施作用（CIA）	机密性	完整性	可用性		
	✓	✓			
措施详细描述	NS-1-1：对切片选择辅助信息（NSSAI）进行隐私保护传输，使用安全上下文对携带 NSSAI 的信令进行加密。 NS-1-2：通过切片签约校验、切片选择、授权和分组数据单元会话机制防止终端对切片的未授权访问。				
适用的资产	5GC、MT				
实施主体	设备厂商			NS-1-1，NS-1-2	
是否已有标准要求	是				
标准名称	3GPP TS 33.501: Security architecture and procedures for 5G System				
实施难度					

A.5.2 NS-2 切片网络隔离

措施编号	NS-2			
措施名称	切片网络隔离			
安全需求	通过部署切片之间、切片专属部分或切片共享部分间在网络层面的隔离控制措施，防止运行在统一的基础设施资源上的切片之间相互影响。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓	✓	
措施详细描述	NS-2-1：采用 TLS 等认证机制，实现切片内 NF 与切片外公共 NF 间可信访问。 NS-2-2：在 AMF 或 NRF 做访问频率监控或者部署防			

	防火墙，防止恶意用户通过(D)DoS 将切片公有 NF 的资源耗尽。				
	NS-2-3: 为终端接入不同切片的通信配置不同的安全策略，为不同安全级别的切片设置不同的共用 NF。				
	NS-2-4: 在切片内 NF 与外网设备之间部署虚拟防火墙或物理防火墙，保护切片内网与外网的安全。				
	NS-2-5: 通过网络划分、资源隔离、启用 SBA 访问控制来保证切片间 NF 的访问隔离。				
适用的资产	切片 NF、MT				
实施主体	运营商		NS-2-2, NS-2-3, NS-2-4, NS-2-5		
	设备厂商		NS-2-1		
是否已有标准要求	是				
标准名称	3GPP TS 33.501: Security architecture and procedures for 5G System GSMA 5GJA NG.116: Generic Network Slice Template 3GPP TR 23.740: Study on enhancement of network slicing				
实施难度					

A.5.3 NS-3 切片数据隔离

措施编号	NS-3			
措施名称	切片数据隔离			
安全需求	通过部署切片之间、切片专属部分或切片共享部分间在数据访问层面的隔离控制措施，防止运行在统一的基础设施资源上的切片之间非法访问数据。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓	✓	
措施详细描述	NS-3-1: NF 对存储资源访问时进行基于切片的数据访问控制，例如根据 NF 所属的切片标识进行数据资			

	<p>源访问控制。</p> <p>NS-3-2: 切片中的 NF 支持根据数据安全级别，采用相应的存储加密机制（具体可参考 A.9 DAT-2）。</p> <p>NS-3-3: 应通过 SBA 认证和 Oauth2.0 等授权机制，对不同切片的 NF 之间进行数据访问控制。</p>					
适用的资产	切片 NF、MT					
实施主体	运营商			NS-3-1, NS-3-2, NS-3-3		
	设备厂商			NS-3-1, NS-3-3		
是否已有标准要求	是					
标准名称	3GPP TS 33.501: Security architecture and procedures for 5G System					
实施难度						

A.5.4 NS-4 切片管理安全

措施编号	NS-4			
措施名称	切片管理安全			
安全需求	通过网络切片安全管理措施, 对网络切片实例 NSI 的生命周期 (如创建、修改、终止等) 进行安全管理, 确保 NSI 的可用性。			
措施作用 (CIA)	机密性	完整性	可用性	
			✓	
措施详细描述	<p>NS-4-1: 支持切片租户的分权分域, 不同租户对其拥有管理权限的切片的管理操作、信息查看等行为应互相隔离。</p> <p>NS-4-2: 切片管理服务使用双向认证、授权机制, 切片管理系统与切片网络间通信需做完整性、机密性保护以及防重放攻击。</p> <p>NS-4-3: 在切片生命周期管理中, 切片模板、配置需</p>			

	要具备检查与校验机制，避免由于错误模板、错误人工配置，导致切片的访问控制失效、数据传输与存储存在安全风险等。 NS-4-4：切片去激活或终止后，遵照数据隔离要求做好数据清除工作。					
适用的资产	切片 OSS					
实施主体	运营商			NS-4-1, NS-4-2, NS-4-3, NS-4-4		
	设备厂商			NS-4-1, NS-4-2, NS-4-3		
是否已有标准要求	是					
标准名称	3GPP TS 33.501: Security architecture and procedures for 5G System					
实施难度						

A.6 安全管理(Security Management, SM)

A.6.1 SM-1 安全管理和编排

措施编号	SM-1			
措施名称	安全管理和编排			
安全需求	通过合理的安全资源管理和编排措施，配置有效的安全策略，对 5G 网络中的资产进行安全防护。			
措施作用（CIA）	机密性	完整性	可用性	
			✓	
措施详细描述	<p>SM-1-1：针对边缘计算、基站、5GC 等资产构建原子化安全资源池，安全能力包括虚拟化安全、OS 安全、攻击监测、纵深防御、安全巡检、数据处理、安全加固、应用加固、安全管理编排、威胁情报、边缘资产清点 and 安全管理。</p> <p>SM-1-2：通过部署安全管理能力，实现对 5GC、边缘计算等业务的安全资源编排，安全防护能力镜像下</p>			

	发、安全策略集中管理和下发、告警集中展现、运行状态监控等功能。				
适用的资产	路由器、交换机、服务器、存储类设备、安全类设备、基站、MEC、5GC 等				
实施主体	运营商			SM-1-1, SM-1-2	
是否已有标准要求	是				
标准名称	3GPP TS 33.501: Security architecture and procedures for 5G System GB/T 25068.1-2012 《信息技术 安全技术 IT 网络安全 第 1 部分：网络安全管理》				
实施难度					

A.6.2 SM-2 安全可控

措施编号	SM-2			
措施名称	安全可控			
安全需求	保证 5G 网络中的关键设备和关键功能安全可控。			
措施作用（CIA）	机密性	完整性	可用性	
			√	
措施详细描述	<p>SM-2-1: 在 5G 网络部署建设前，确保 5G 网络路由器、交换机、服务器、存储设备、安全设备（如防火墙、IDS/IPS、抗 DoS 等）、基站、核心网等设备满足安全可控标准要求。</p> <p>SM-2-2: 5G 基站等设备的传输同步方式主用 GPS、北斗等安全可控技术。</p> <p>SM-2-3: 5G 网络基站、核心网等关键功能具备切换能力。</p>			
适用的资产	路由器、交换机、服务器、存储类设备、安全类设备、基站等			

实施主体	运营商	SM-2-1, SM-2-2, SM-2-3
是否已有标准要求	是	
标准名称	GB/T 25068.1-2012 《信息技术 安全技术 IT 网络安全 第 1 部分：网络安全管理》 GB/T 36630 系列 《信息安全技术 信息技术产品安全可控评价指标》	
实施难度	<div> <div></div> <div></div> <div></div> <div></div> <div></div> </div>	

A.6.3 SM-4 人员管理

措施编号	SM-4			
措施名称	人员管理			
安全需求	对参与 5G 网络建设、运行、维护等过程中的人员进行严格管理，确保人员操作符合安全管理制度规定。			
措施作用（CIA）	机密性	完整性	可用性	
措施详细描述	SM-3-1：制订关键岗位人员和第三方人员安全管理制度。 SM-3-2：基于相关制度，与关键岗位人员和第三方人员签订保密协议。 SM-3-3：基于相关制度，对第三方远程接入、网元访问等行为进行审核。			
适用的资产	路由器、交换机、服务器、存储类设备、安全类设备、基站等			
实施主体	运营商		SM-3-1, SM-3-2, SM-3-3	
是否已有标准要求	是			
标准名称	3GPP TS 33.501: Security architecture and procedures for 5G System			

	GB/T 25068.1-2012 《信息技术 安全技术 IT 网络安全 第1部分：网络安全管理》					
实施难度						

A.6.4 SM-4 安全审计

措施编号	SM-4					
措施名称	安全审计					
安全需求	对 5G 网络资产和供应商进行安全审计，确保产品和服务满足相关标准安全要求。					
措施作用（CIA）	机密性	完整性	可用性			
措施详细描述	SM-4-1: 对 5G 供应商及其产品和服务进行 NESAS 合规性检查，以确保其设备在设备交付前具有基线安全级别。 SM-4-2: 制订安全审计相关规章要求，对 5G 网络运行中的安全告警、安全事件等进行安全审计，针对安全审计结果暴露的问题进行整改。					
适用的资产	路由器、交换机、服务器、存储类设备、安全类设备、基站等					
实施主体	运营商			SM-4-1, SM-4-2		
是否已有标准要求	是					
标准名称	GB/T 25068.1-2012 《信息技术 安全技术 IT 网络安全 第 1 部分：网络安全管理》 GSMA FS.16 NESAS Development and Lifecycle Security Requirements v.2.0					
实施难度						

A. 7 运维管理 (Operation and Management, OM)

A.7.1 OM-1 5GC 安全运维

措施编号	OM-1
------	------

措施名称	5GC 安全运维				
安全需求	在 5GC 运维管理中部署相应的安全保护措施，确保 5GC 安全机制和策略正常运行，保护 OM 系统访问 5GC 的安全。				
措施作用（CIA）	机密性	完整性	可用性		
	✓	✓	✓		
措施详细描述	<p>OM-1-1: 5GC 运维开启空口和/或终端到核心网之间的信令面和用户面加密和完整性保护机制。</p> <p>OM-1-2:OM 系统应建立双向认证机制、IPSec/SSL VPN 隧道，采取完整性验证、权限认证和重放保护，防范通信安全威胁，保证数据传输安全。</p> <p>OM-1-3: OM 建立日志分析，确保安全事件取证，建立事后回溯机制。</p> <p>OM-1-4: 对 OM 系统进行安全加固，包括病毒查杀、病毒库升级、防火墙等。</p> <p>OM-1-5: 对 OM 系统划分安全域，根据运营需求和网元功能，将网元进行安全等级划分，为不同等级设置不同安全域，每个功能网元和管理网元仅能归属其中一个安全域，实现域间隔离。</p>				
适用的资产	OM、5GC 组网设备、5GC NF				
实施主体	运营商		OM-1-1, OM-1-2, OM-1-3, OM-1-4, OM-1-5		
	设备厂商		OM-1-2, OM-1-4		
是否已有标准要求	是				
标准名称	GB/T 36626-2018 《信息安全技术 信息系统安全运维管理指南》				
实施难度					

A.7.2 OM-2 云基础设施主机运维

措施编号	OM-2				
措施名称	云基础设施主机运维				
安全需求	对云化基础设施实施安全运维措施，保护云基础设施主机运维安全。				
措施作用（CIA）	机密性	完整性	可用性		
	✓		✓		
措施详细描述	OM-2-1：5G 网络中的 Host OS（Hypervisor）、GuestOS、中间件、数据库、应用软件等，应满足安全合规配置、漏洞风险管理、账号口令管理、安全补丁管理等通用的安全要求。				
适用的资产	OM、物理主机、操作系统（Host OS）、中间件、数据库等				
实施主体	运营商		OM-2-1		
	设备厂商		OM-2-1		
是否已有标准要求	是				
标准名称	GB/T 36626-2018 《信息安全技术 信息系统安全运维管理指南》				
实施难度					

A.7.3 OM-3 云基础设施虚拟化层运维

措施编号	OM-3			
措施名称	云基础设施虚拟化层运维			
安全需求	对云化基础设施实施安全运维措施，保护云基础设施虚拟化层运维安全。			
措施作用（CIA）	机密性	完整性	可用性	
		✓	✓	
措施详细描述	OM-3-1: Hypervisor 的安全管理和安全配置应采取服务最小原则，禁用不必要的服务。			

	<p>OM-3-2: Hypervisor 的虚拟化软件接口，应严格限定为管理虚拟机所需的 API，应采用安全协议和算法、设置访问控制规则及开启鉴权认证实现限制对管理端口的访问，原则上仅允许 VIM、4A 堡垒机、应急终端的访问。</p> <p>OM-3-3: Hypervisor 的管理接口流量应该和其他（例如业务、存储）网络流量物理隔离。</p> <p>OM-3-4: Hypervisor 应满足安全配置合规、漏洞风险管理、账号口令管理的安全要求。</p>				
适用的资产	OM、虚拟化平台（Hypervisor、K8S、Docker 等）、虚拟机、Guest OS、容器				
实施主体	运营商		OM-3-1, OM-3-2,		
	设备厂商		OM-3-3, OM-3-4		
是否已有标准要求	是				
标准名称	GB/T 36626-2018 《信息安全技术 信息系统安全运维管理指南》 YD/T 3054-2016 《云资源运维管理功能技术要求》				
实施难度					

A.7.4 OM-4 云基础设施 PIM 运维

措施编号	OM-4			
措施名称	云基础设施 PIM 运维			
安全需求	对云化基础设施实施安全运维措施，保护云基础设施 PIM 运维安全。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓	✓	
措施详细描述	<p>OM-4-1: PIM 对物理硬件有较高管理及控制权限制（例如开关机等），应采用安全协议和算法、设置访问控制规则及开启鉴权认证实现限制对管理端口的访</p>			

	<p>问，原则上仅允许 MANO、4A 堡垒机、应急终端的访问。</p> <p>OM-4-2: PIM 应启用对分布式存储服务器的证书认证，并建立安全通道，保护 PIM 和分布式块存储服务之间传输的数据的机密性和完整性。</p> <p>OM-4-3: 应对 PIM 纳管物理硬件的告警信息，做好日常监测及处置工作。</p>					
适用的资产	OM、PIM、组网设备、存储设备、计算资源					
实施主体	运营商			OM-4-1, OM-4-2, OM-4-3		
是否已有标准要求	是					
标准名称	GB/T 36626-2018 《信息安全技术 信息系统安全运维管理指南》 YD/T 3054-2016 《云资源运维管理功能技术要求》					
实施难度						

A.7.5 OM-5 云基础设施 MANO 运维

措施编号	OM-5			
措施名称	云基础设施 MANO 运维			
安全需求	对云化基础设施实施安全运维措施，保护云基础设施 MANO 运维安全。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓	✓	
措施详细描述	<p>OM-5-1: 对提供 Web 访问界面的 MANO，应使用安全通信协议（如 TLS v1.2 以上）。</p> <p>OM-5-2: 在创建角色和用户时根据需要分配最小权限。</p> <p>OM-5-3: MANO 中不应包含明文敏感信息，敏感信息应加密保存，并支持会话超时退出功能。</p>			

			<p>OM-5-4: 账号口令应严格遵循账号口令管理要求, 防止暴力破解。</p> <p>OM-5-5: 需开启日志审计, 包括所有对系统状态有影响的操作, 所有安全相关操作的日志 (如创建用户、登入登出等), 系统自身重要事件的日志 (如定时触发的任务等), 用户普通操作的日志 (如业务上下线等)。</p> <p>OM-5-6: 应对虚拟机系统定期进行安全评估, 严格遵从补丁管理流程进行补丁更新。</p> <p>OM-5-7: 应启用 IP/MAC 防欺诈, 防止用户通过修改虚拟网卡的 IP、MAC 地址发起 IP、MAC 仿冒攻击。</p> <p>OM-5-8: 在进行迁移或弹性扩缩过程中, 应根据业务需求做好迁移和扩缩过程中的数据保护, 防止敏感信息泄露。虚拟机的性能应限制在特定的安全集群内, 安全集群应能与虚拟系统安全架构的安全域相对应。</p> <p>OM-5-9: 虚拟机镜像及模板上线前, 要进行全面的安全评估, 并进行安全加固。</p> <p>OM-5-10: 上传镜像时, 应约束镜像上传到固定的路径, 避免用户在上传镜像时随意访问整个系统的任意目录。</p> <p>OM-5-11: 对虚拟机镜像仓库及快照开启口令鉴权访问, 防止损坏、非授权访问、篡改、泄露。</p>
适用的资产			OM、MANO
实施主体	运营商	OM-5-4, OM-5-6, OM-5-8, OM-5-9, OM-5-10, OM-5-11	
	设备厂商	OM-5-1, OM-5-2, OM-5-3, OM-5-5, OM-5-7	
是否已有标准要求			是

标准名称	GB/T 36626-2018 《信息安全技术 信息系统安全运维管理指南》 YD/T 3054-2016 《云资源运维管理功能技术要求》				
实施难度					

A.7.6 OM-6 云基础设施 SDN 运维

措施编号	OM-6			
措施名称	云基础设施 SDN 运维			
安全需求	对云化基础设施实施安全运维措施，保护云基础设施 SDN 运维安全。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓	✓	
措施详细描述	<p>OM-6-1: SDN 控制器应启用识别来自南向接口或者北向接口的异常流量/报文，通过限速等机制，防止 (D)DoS 攻击。</p> <p>OM-6-2: SDN 控制器应启用检测配置及策略冲突，如 VLAN 冲突、流表冲突、成环等会造成网络安全隐患的问题，并在检测到冲突后进行提示。</p> <p>OM-6-3: 远程登录 SDN 控制器进行维护操作时，应使用 SSHv2 等安全协议，并且登录时不提示敏感信息，应接入 4A 进行操作维护。</p> <p>OM-6-4: SDN 控制器应启用对敏感数据（如密码、私钥、流表、策略等）进行加密存储、防篡改和安全访问控制。</p> <p>OM-6-5: SDN 控制器应满足安全配置合规、漏洞风险管理、账号口令管理的安全要求，对开放的不必要的、未使用的端口和服务进行关闭。</p> <p>OM-6-6: SDN 网关应开启对 SDN 控制器的认证，并和 SDN 控制器建立安全通道，保证南向接口传输数</p>			

	据的机密性和完整性。 OM-6-7: SDN 网关应满足安全配置合规、漏洞风险管理、账号口令管理的安全要求。				
适用的资产	OM、SDN				
实施主体	运营商	OM-6-3, OM-6-5			
	设备厂商	OM-6-1,	OM-6-2,	OM-6-4,	OM-6-6,
		OM-6-7			
是否已有标准要求	无				
标准名称	/				
实施难度					

A.7.7 OM-7 安全应急响应

措施编号	OM-7			
措施名称	安全应急响应			
安全需求	对 5G 网络系统上存在或传播的、可能或已经对公众造成危害的包括网络外部及内部的威胁、脆弱性、安全隐患或已发生的安全事件进行应急响应，采取紧急措施和行动，恢复业务到正常服务状态。			
措施作用（CIA）	机密性	完整性	可用性	
		✓	✓	
措施详细描述	<p>OM-7-1: 建立完善安全风险监测手段。参考运维故障告警标准化机制，提供各类安全风险主动监测与感知能力，开展 7*24 小时安全监控，包括但不限于反域名劫持、反网页篡改、反流量攻击等各类安全事件，记录形成监控日志。</p> <p>OM-7-2: 开展安全风险处置。参考运维故障告警标准化机制，对不同级别的风险采取相对应的安全防护措施，并对风险处置情况在规定时间内进行上报。</p>			

	<p>OM-7-3: 实施安全预警管理, 遵循对不同等级的风险采取分级管理, 并在限定的时间内完成临时防护措施以及闭环处置。应跟踪预警项进展, 预警内容出现变化应及时上报, 必要时调高预警级别并采取更严格防范措施。</p> <p>OM-7-4: 制定安全应急预案。规范化管理安全应急预案, 系统交付和运维时应具备详细的应急预案。在系统发生变更调整时, 应急预案应当同步进行更新, 系统下线时安全应急预案及时清理。</p> <p>OM-7-5: 制定本系统的安全应急演练计划, 并提交给网络安全部门备案, 并定期开展安全应急演练。</p>	
适用的资产	OM、5GC、云基础设施主机、云基础设施虚拟化层、云基础设施 PIM、云基础设施 MANO、云基础设施 SDN、gNB	
实施主体	运营商	OM-7-1, OM-7-2, OM-7-3, OM-7-4, OM-7-5
是否已有标准要求	是	
标准名称	<p>1、GB/T 24363-2009 《信息安全技术 信息安全应急响应计划规范》</p> <p>2、GB/T 38645-2020 《信息安全技术 网络安全事件应急演练指南》</p>	
实施难度	<div> <div></div> <div></div> <div></div> <div></div> <div></div> </div>	

A.8 数据安全(Data, DAT)

A.8.1 DAT-1 数据识别与管理

措施编号	DAT-1
措施名称	数据识别与管理

安全需求	建立数据安全管理制度，对 5G 网络中的资产信息、网络运维数据等进行发现识别，建立数据安全管理制度，明确掌握 5G 网络数据态势。					
措施作用（CIA）	机密性		完整性		可用性	
	✓		✓			
措施详细描述	DAT-1-1: 建设 5G 网络资产、运维管理等数据发现功能，建设数据资源清单管理，建立数据资源备案管理，对 5G 数据的分布情况进行综合呈现。 DAT-1-2: 建立数据识别策略、分类分级策略、对外接口数据监测策略、生产运维数据监测策略，实现 5G 数据态势可视。					
适用的资产	DAT					
实施主体	运营商			DAT-1-1, DAT-1-2		
是否已有标准要求	是					
标准名称	YD/T 3802-2020 《电信网和互联网数据安全通用要求》					
实施难度						

A.8.2 DAT-2 数据安全防护

措施编号	DAT-2			
措施名称	数据安全防护			
安全需求	保护 5G 网络中的业务数据和个人信息在数据全生命周期过程中的安全，防止发生数据泄露、未经授权访问等安全问题。			
措施作用（CIA）	机密性	完整性	可用性	
	✓	✓		
措施详细描述	DAT-2-1：采取加密措施，针对需进行加密处理的业务场景，对业务数据和个人信息进行加密。 DAT-2-2：采取完整性保护措施，利用防篡改技术对			

	<p>传输和存储过程中的数据进行完整性保护。</p> <p>DAT-2-3: 采取敏感数据保护措施，利用脱敏技术保护敏感数据在存储、使用过程中的安全性。</p> <p>DAT-2-4: 采取访问控制措施，限制用户对数据信息的访问能力及范围。</p> <p>DAT-2-5: 采用数据访问控制措施，对设备网元间的接口、网管接口等限制每类网元可访问的数据类型，采用严控数据导出操作、禁用特权操作等措施保障数据安全。</p> <p>注：以上数据安全防护措施是通用安全措施，适用于5G 网络基站、MEC、核心网、云化基础设施等各类资产，在具体实施过程中有一定差异性，具体见各章节措施描述。</p>				
适用的资产	DAT				
实施主体	运营商		DAT-2-4		
	服务提供商		DAT-2-6		
	安全厂商		DAT-2-1, DAT-2-2, DAT-2-3, DAT-2-5		
是否已有标准要求	是				
标准名称	YD/T 3802-2020 《电信网和互联网数据安全通用要求》				
实施难度					

A.8.3 DAT-3 数据安全监测

措施编号	DAT-3
措施名称	数据安全监测
安全需求	掌握数据资产的安全态势, 防止业务数据和个人信息以违反安全策略规定的形式流出 5G 网络, 并对数据进行安全管控, 实现数据溯源和数据风险监测。

措施作用（CIA）	机密性		完整性		可用性	
	✓		✓			
措施详细描述	DAT-3-1：采取恶意数据流量监测安全防护措施，在5G网络与其他网络的边界处部署IDS等设备，对进入5G网络的恶意攻击流量进行监测和阻断。 DAT-3-2：采取数据防泄漏措施，采用身份认证管理、进程监控、日志分析和安全审计等技术手段，对网元中重要数据的违规使用进行警告和控制。 DAT-3-3：采用数据集中管理措施，对网元、MANO、切片管理系统的数据创建操作、数据导入行为、操作日志等进行监测，分析操作账号、操作时间、操作行为、涉及的数据量等。 DAT-3-4：采取数据安全评估措施，通过文档查验、测评验证、系统演示等方式对5G资产的数据安全能力进行评估。 注：以上数据安全防护措施是通用安全措施，适用于5G网络基站、MEC、核心网、云化基础设施等各类资产，在具体实施过程中有一定差异性，具体见各章节措施描述。					
适用的资产	5G网元、网管系统、网络云					
实施主体	运营商				DAT-3-1， DAT-3-2, DAT-3-3, DAT-3-4	
是否已有标准要求	是					
标准名称	YD/T 3802-2020 《电信网和互联网数据安全通用要求》 YD/T 3801-2020 《电信网和互联网数据安全风险评估实施方法》					
实施难度	<div><div></div><div></div><div></div><div></div><div></div><div></div></div>					

致 谢

《5G 安全知识库》是在工业和信息化部网络安全管理局指导下，由中国信息通信研究院、中国移动通信集团有限公司、中国电信集团有限公司、中国联合网络通信集团有限公司、华为技术有限公司、中兴通讯股份有限公司、中国南方电网有限责任公司共同编制完成。

指导组： 王志勤 魏亮 张滨 谢玮 林美玉 张峰

编写组： 杨红梅 冯泽冰 邱勤 刘雅君 吴荣 江为强 焦杨 朱兵
于乐 崔洋