ICS 35.020
CCS M 10

YD

中华人民共和国通信行业标准

YD/T XXXX—202X

互联网新技术新业务安全评估要求
基于 5G 场景的业务

The requirements of security assessment for new Internet technologies and new services — Applications for 5G services

（报批稿）

202x-xx-xx 发布　　202x-xx-xx 实施

中华人民共和国工业和信息化部 发布

目　　次

前　　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是“互联网新技术新业务安全评估体系”系列标准之一，该系列标准预计结构及名称如下：

— 《互联网新技术新业务安全评估指南》

— 《互联网新技术新业务安全评估实施要求》

— 《互联网新技术新业务安全评估要求 即时通信业务》

— 《互联网新技术新业务安全评估要求 互联网资源协作服务》

— 《互联网新技术新业务安全评估要求 大数据技术应用与服务》

— 《互联网新技术新业务安全评估要求 内容分发业务》

— 《互联网新技术新业务安全评估要求 移动应用商店业务》

— 《互联网新技术新业务安全评估要求 信息社区平台业务》

— 《互联网新技术新业务安全评估要求 信息搜索查询服务》

— 《互联网新技术新业务安全评估要求 信息发布与递送业务》

— 《互联网新技术新业务安全评估要求 基于 5G 场景的业务》（本文件）

— 《互联网新技术新业务安全评估第三方服务机构能力认定准则》

—

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：中国信息通信研究院、中国移动通信集团有限公司、中国移动通信集团设计院有限公司、北京神州绿盟科技有限公司、中国电信集团有限公司、北京亚鸿世纪科技发展有限公司、郑州信大捷安信息技术股份有限公司。

本文件主要起草人：郭建南、张琳琳、朱纯超、邱勤、赵蓓、李伟旗、王立超、赵锐、沈军、张蔚茵、丁沛、成海、于宝占、韩函、刘献伦、刘为华。

互联网新技术新业务安全评估要求 基于 5G 场景的业务

1 范围

本文件规定了基于5G场景的业务安全评估要求，包括评估框架和eMBB场景、uRLLC场景、mMTC场景、边缘计算、云化基础设施、网络切片的安全评估要求。

本文件适用于5G网络运营者、5G技术业务提供者和使用者的5G业务安全自评估，也可用于第三方机构等开展5G业务安全评估。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2022 信息安全技术 术语

GB/T 35273-2020 信息安全技术 个人信息安全规范

YD/T 3489-2019 SDN网络安全能力要求

YD/T 3962-2021 5G核心网边缘计算总体技术要求

YD/T XXXX-202X 网络功能虚拟化（NFV）安全技术要求

3 术语和定义

GB/T 25069-2022、GB/T 35273-2020界定的以及下列术语和定义适用于本文件。

3.1

增强移动宽带场景，enhanced mobile broadband，eMBB

5G 典型应用场景之一，支持超高的数据传输速率和广覆盖下的移动性保证。

3.2

可靠低时延通信场景，ultra-reliable low-latency communications，uRLLC

5G 典型应用场景之一，以无人驾驶、远程医疗、智能制造等关键通信为代表性应用场景，强调必须严格满足低时延和可靠性。

3.3

大规模机器类通信场景，massive machine type communication，mMTC

5G典型应用场景之一，支持密集环境下的海量机器通信，以大规模物联网为典型应用场景，使人与机器、机器与机器的大规模通信成为可能。

4 缩略语

下列缩略语适用于本文件。

5G	第五代移动通信技术	5th Generation Mobile Communication Technology
ACL	访问控制列表	Access-control List
AKMA	应用程序认证和密钥协议	Authentication and Key Agreement for Applications
AMF	接入和移动管理功能	Access and Mobility Management Function
API	应用程序接口	Application Programming Interface
DDoS	分布式拒绝服务	Distributed Denial of Service
eMBB	增强移动宽带	Enhanced Mobile Broadband
GBA	通用认证机制	GeneralBootstrappingArchitecture
GTP	GPRS 隧道协议	GPRS Tunneling Protocol
HMAC	基于哈希散列的消息认证代码	Hash-based Message Authentication Code
IPS	入侵防御系统	Intrusion Prevention System
L2TP	第二层隧道协议	Layer 2 Tunneling Protocol
mMTC	大规模机器类型通信	Massive Machine Type Communication
MANO	编排与管理	Management and Orchestration
MEC	多接入边缘计算	Multi-access Edge Computing
NF	网络功能	Network Function
NFV	网络功能虚拟化	Network Functions Virtualization
NFVI	网络功能虚拟化基础设施	Network Functions Virtualization Infrastructure
NRF	网络存储功能	Network Repository Function
SBA	基于服务的架构	Service Based Architecture
SDN	软件定义网络	Software Defined Network
UE	用户终端设备	User Equipment
uRLLC	超高可靠超低时延通信	Ultra Reliable Low Latency Communication
VLAN	虚拟局域网	Virtual Local Area Network

5 概述

5.1 评估需求

5G 更高带宽、更低时延、更大连接的特性及与各行业的融合渗透，在为经济社会发展带来变革的同时也带来不良信息治理、5G 安全监管和 5G 业务防护等方面的压力和挑战。同时，在实际业务开展过程中，5G 三大业务场景的通信需求各不相同，业务接入方式和网络服务方式存在较大差异，网络支持的业务交付方式也有所区别，5G 业务面临着差异化的场景安全需求，以及不同场景和不同 5G 技术组合应用带来的安全风险。

本文件围绕 eMBB、uRLLC、mMTC 三大 5G 典型应用场景的特点和风险，结合三大场景业务和安

全需求的差异性，提出基于 5G 场景业务的安全评估内容、评估要求和评估启动条件。

5.2 评估框架

本文件对 eMBB 场景下的 5G 业务、uRLLC 场景下的 5G 业务、mMTC 场景下的 5G 业务和涉及 5G 云化基础设施、5G 网络切片、5G 边缘计算的业务明确了安全评估的内容和要求，基于 5G 场景的业务安全评估框架见图 1。

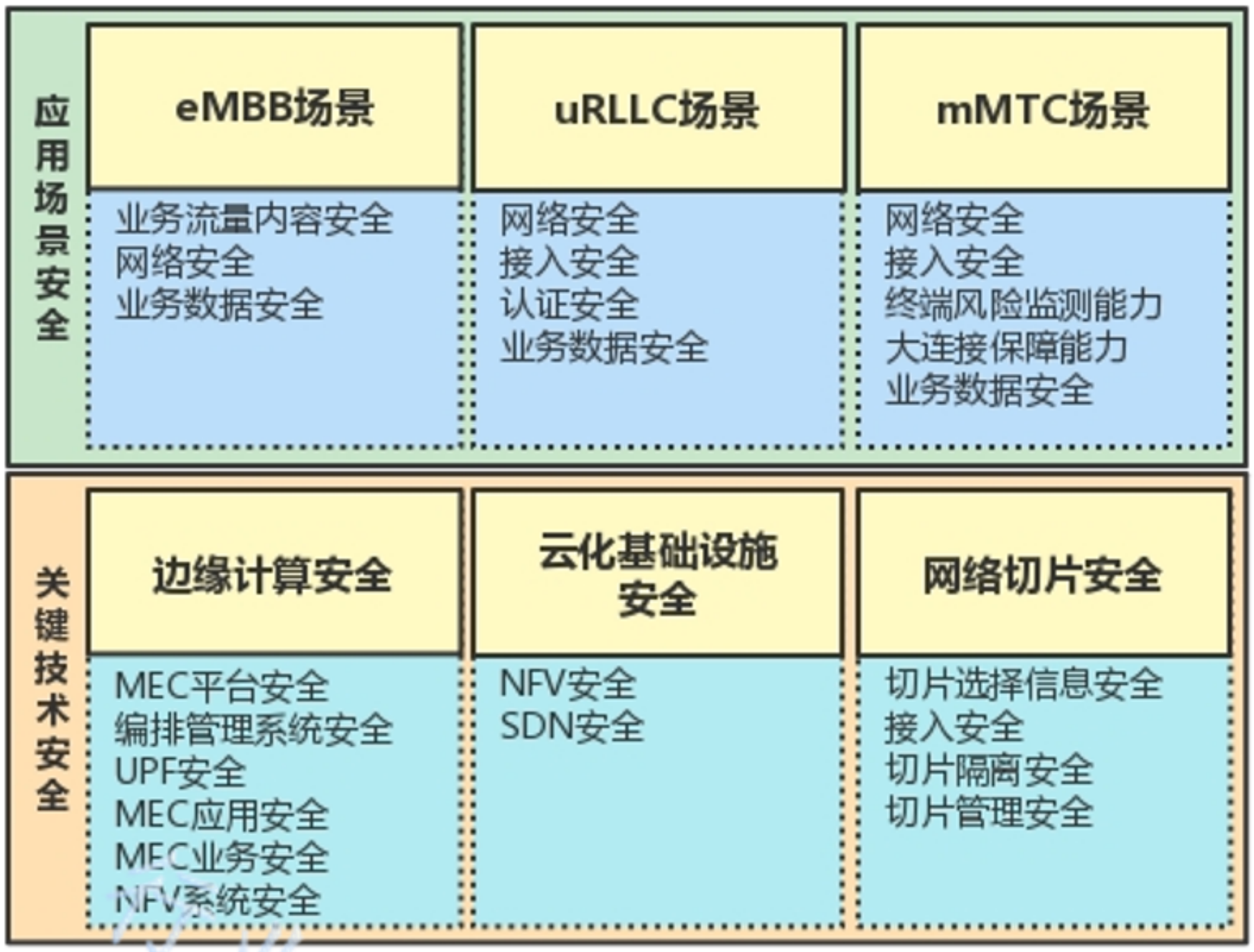

图 1 基于 5G 场景的业务安全评估框架

5.3 评估启动条件

当满足下列情形之一，应及时启动安全评估：

a) 基于 5G 场景的业务上线前（含合作推广、试点、试商用）应开展安全评估的；

b) 基于 5G 场景的业务运营阶段，其运营环境发生较大变化应开展安全评估的；

c) 行业主管部门要求进行安全评估的；

d) 满足国家法律法规有关情形，应开展安全评估的。

6 eMBB 场景安全评估要求

5G eMBB 业务具有大带宽、大流量和业务内容、形式多样化的特征，面临着不良信息管控难度加大、数据泄露/窃取风险点增多、用户隐私泄露风险增大和现有安全设备防护能力不足的风险。对 eMBB 场景下的业务开展安全评估，应重点考虑以下几个方面：

a) 是否具备 eMBB 业务流量内容监控、识别和处置能力，能否对判定的不良信息和违法违规内容、账户和业务及时进行过滤、关闭、下架等处置；

b) 是否部署抗 DDoS 设备或具备抗 DDoS 攻击能力，能否防止因 DDoS 攻击造成网络拥塞或者通信链路中断；对现有网络中的防火墙、入侵检测系统等安全设备是否定期升级并留存升级记录，能否满足流量检测、链路覆盖、数据存储等方面超大流量安全防护需求；

c) 是否具有高安全要求业务场景保障能力，能否通过物理隔离或加密措施保证网元之间用户数据传输安全，或在核心网与 eMBB 业务服务平台之间建立安全的数据传输通道，保证用户业务数据传输安全。

7 uRLLC 场景安全评估要求

5G uRLLC 业务具有低时延、高精度、高可靠性的特征，其超低时延的需求致使该场景下的业务受 DDoS 攻击影响更大，数据传输可靠性保障难度更高，并且复杂的高级别安全机制也难以部署。对 uRLLC 场景下的业务开展安全评估，应重点考虑以下几个方面：

a) 是否部署抗 DDoS 设备或具备抗 DDoS 攻击能力，能否防止被 DDoS 攻击造成网络拥塞或者通信链路中断；

b) 是否具有面向低时延需求的安全机制，能否统筹业务接入认证、数据加解密等环节的安全需求和时延需求；

c) 是否具有高安全需求场景保障能力，能否在用户终端及业务服务器之间建立应用层双向身份认证机制（例如在应用层预置数字证书、共享密钥，或基于运营商网络开放的安全能力采用 AKMA、GBA 等安全机制），防止假冒用户/业务服务器建立合法的业务连接；

d) 是否具有数据完整性保护、时间戳、序列号等机制，能否防止业务数据被篡改、伪造或重放，保证数据传输可靠，是否根据数据分类分级进行静态存储和动态传输数据保护，明确行业关键数据，定期备份。

8 mMTC 场景安全评估要求

5G mMTC 业务具有接入设备数量庞大、种类繁多以及安全需求和安全能力差异巨大的特征，该场景下的业务面临假冒终端接入、数据窃听、数据篡改、能力风暴、病毒攻击、设备俘获、物理入侵等诸多风险。对 mMTC 场景下的业务开展安全评估，应重点考虑以下几个方面：

a） 能否及时检测并防止海量物联网设备被控制及设备资源被恶意使用，如采用分布式身份管理和接入认证，避免单个网络节点 DDoS 攻击；

b） 是否考虑网络负载能力，能否缩短认证链条实现快速安全接入（如采用分布式身份管理和接入认证），能否规避信令风暴以及认证节点高度集中带来的瓶颈风险，避免单个网络节点被海量终端同时攻击；

c） 是否具备终端安全风险监测能力，能否对异常终端进行控制，如设备及时下线；

d） 是否具备针对海量连接特性的安全保障能力，如采用轻量级的安全算法、简单高效的安全协议来实现物联网终端与网络间的双向认证、数据机密性及完整性保护；

e） 是否具备物联网终端、应用层业务数据保护能力，如进行机密性及完整性保护，防止窃听、篡改、伪造、重放，或基于安全凭据进一步协商产生会话密钥。

9 边缘计算安全评估要求

边缘计算业务可定制化、低成本、低时延以及隐私性等特征，面临着数据泄露、数据篡改、非授权访问、病毒及网络攻击等风险，进而引发网络延迟、服务中断乃至影响基础设施运行等危害，对边缘计算业务开展安全评估，应重点考虑以下几个方面：

a）边缘计算编排管理系统安全是否满足 YD/T XXXX-202X 第 7 章要求；

b）边缘计算平台系统安全是否满足 YD/T 3962-2021 7.2 要求。

c）是否对边缘计算应用进行安全加固，是否使用 HMAC 等机制对边缘计算应用软件或者镜像进行完整性保护，是否对敏感数据加密存储和完整性保护，是否对访问边缘计算应用的用户进行认证；

d）UPF 安全是否具备上下行流量防地址欺骗检查及告警能力，能否对没有匹配 PDP 上下文/承载的下行流量执行丢弃及告警；是否具备针对 GTP 协议恶意报文攻击的防御能力；是否具备 GTP 解封装后的流量只流向内部数据网络的能力；是否支持 ACL 过滤功能；是否支持 L2TP 隧道、IPSec 隧道、安全启动技术等灵活的终端互访策略；

e）对于边缘计算节点部署在用户侧的业务，是否建立隔离措施，防止边缘计算节点向核心网发起攻击；

f）是否采取措施保障 NFV 系统安全，包括 NFVI、业务通信系统和管理系统安全。

10 云化基础设施安全评估要求

10.1 SDN 安全

SDN 网络框架包括应用层、控制层、资源层、通道层（北向接口、南向接口），面临着拒绝

服务攻击、数据库漏洞等传统网络威胁，也面临 SDN 设备、协议及接口所带来的自身安全漏洞威胁。对 SDN 开展安全评估，应重点考虑以下几个方面：

a) 应用层安全是否满足 YD/T 3489-2019 6.1 要求；

b) 控制层安全是否满足 YD/T 3489-2019 6.2 要求；

c) 资源层安全是否满足 YD/T 3489-2019 6.3 要求；

d) 北向接口安全是否满足 YD/T 3489-2019 6.4 要求；

e) 南向接口安全是否满足 YD/T 3489-2019 6.5 要求。

10.2 NFV 安全

NFV 技术具有配置灵活性、架构易拓展性等特征，为 5G 网络切片实施提供了技术基础。NFV 架构主要包括 VNFI、MANO、VNFs 三部分，面临着虚拟机、硬件资源、管理和编排系统、接口攻击及滥用等安全威胁。对 NFV 开展安全评估，应重点考虑以下几个方面：

a) NFVI 硬件服务器及其承载的虚拟化软件、宿主机及虚拟机操作系统是否进行了加固，并在虚拟机间进行安全隔离；

b) 业务通信系统是否使用安全可靠的标准化通信协议，是否对通信的数据进行机密性、完整性和防重放保护；

c) MANO 安全是否满足 YD/T XXXX-202X 第 7 章要求；

d) 是否对管理、控制和存储流量使用独立网卡进行物理隔离，是否划分安全域，并在不同安全等级的安全域之间使用 VLAN 进行隔离；

e) 是否对管理系统的网元进行安全加固，是否对管理系统内部接口和管理系统与外部其它系统之间的接口上的数据进行机密性、完整性和防重放保护。

11 网络切片安全评估要求

11.1 选择信息安全

在安全上下文建立之后，是否对切片选择信息进行机密性保护。

11.2 接入安全

接入安全主要面临非法认证和授权风险，对切片数据机密性和完整性造成严重威胁。对切片接入开展安全评估，应重点考虑以下两个方面：

a) 切片接入时是否执行认证以保证终端的合法性，是否通过切片选择、授权和分组数据单元会话机制来防止对切片的未授权访问；

b) 在已有的用户认证鉴权基础上，是否对移动网络和行业应用共同完成切片用户端设备的接入认证和授权，以保证接入合法切片以及行业对切片网络及资源使用的可控性。

11.3 切片隔离安全

切片隔离技术实现了不同用户类型和应用场景下端到端的隔离，主要面临着切片内外及切片之间的非法认证授权、漏洞攻击、切片攻击等风险，导致切片故障、切片间资源挤占等问题。对切片隔离开展安全评估，应重点考虑以下两个方面：

a) 是否采用认证机制，实现切片内 NF 与切片外公共 NF 间相互可信，是否在 AMF 或 NRF 做频率监控或者部署防火墙，是否为 UE 到不同切片的通信设置不同的安全策略，是否为不同安全级别的切片设置不同的公用 NF；

b) 在切片内 NF 与外网设备间是否部署防火墙、IPS 等设备，能否抵御来自移动互联网的网络攻击；

c) 不同切片间是否采取网络划分、资源隔离、SBA 访问控制等，保证切片间 NF 隔离；

d) 是否具有数据安全保障措施，能否确保在数据发生丢失或破坏时利用备份进行数据恢复，能否防止数据被非法恢复，能否确保虚拟机不能直接或间接访问其它虚拟机的数据。

11.4 切片管理安全

切片管理架构主要包括网络切片子网管理功能、网络切片管理功能、通信服务管理功能等方面，面临着认证鉴权防护不足、恶意代码注入、接口攻击等风险，导致切片被非法删除及篡改等操作。对切片管理开展安全评估，应重点考虑以下几个方面：

a) 切片管理接口是否提供认证及授权机制；

b) 切片模板及相应软件镜像在上传和存储时是否做完整性保护；

c) 切片管理系统及切片网络间通信是否做完整性和机密性保护；

d) 切片终止后切片相关的资源是否做好释放和清理。