ICS 33.040
CCS M 10

YD

中华人民共和国通信行业标准

YD/T 1734—2024
代替 YD/T 1734—2009

移动通信网安全防护要求

Security protection requirements for mobile telecommunication network

（报批稿）

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。

本文件代替YD/T 1734-2009《移动通信网安全防护要求》。

本文件对YD/T 1734-2009的具体修订内容如下：

a) 第1章“范围”，修改为“本文件规定了IPv4、IPv6、双栈环境下的移动通信网的安全防护要求，包括业务安全、网络安全、设备安全、物理环境安全和管理安全等方面”；
b) 删除原第5章“移动通信网安全定级对象和安全等级确定”内容；
c) 删除原第6章“移动通信网资产、脆弱性、威胁分析”内容；
d) 第5章“移动通信网安全防护概述”下内容修改为“移动通信网运营者应根据YD/T 3799中确定安全等级的方法确定移动通信网的安全等级，并依据安全等级开展包括业务安全、网络安全、设备安全、物理环境安全和管理安全等五个层面的安全防护工作。”，主要涉及5.2；
e) 第6章“移动通信网安全等级保护要求”下，增加6.2.2.2.7 接入LTE/EPC网络安全和6.2.2.2.8接入5G网络安全，主要涉及6.2.2.2；
f) 第6章“移动通信网安全等级保护要求”下增加6.2.2.3.4 LTE/EPC网络域安全和6.2.2.3.5 5G网络域安全，最主要涉及6.2.2.3；
g) 第6章“移动通信网安全等级保护要求”下修改题目为“网元设备和基础设施安全要求”，增加6.2.3.1 网元设备和基础设施通用安全，6.2.3.4 LTE/EPC网络，6.2.3.5 5G网络，主要涉及6.2.3；
h) 第6章“移动通信网安全等级保护要求”下增加6.3.2.1.5 LTE/EPC网络拓扑结构和6.3.2.1.6 5G网络拓扑结构，主要涉及6.3.2.1；
i) 第6章“移动通信网安全等级保护要求”下增加6.3.2.3.4 LTE/EPC网络域安全和6.3.2.3.5 5G核心网安全域与隔离，主要涉及6.3.2.3；
j) 第6章“移动通信网安全等级保护要求”下修改章节题目为“网元设备和基础设施安全要求”，增加6.3.3.1 网元设备和基础设施通用安全，6.3.3.2 5G网元设备和基础设施安全，主要涉及6.3.3。

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、中国电信集团公司、中国移动通信集团公司、中国联合网络通信集团有限公司。

本文件主要起草人：贺倩、戴方芳、孟楠、黄维龙、袁琦、曹一生、刘申建、杨恒。

本文件于2008年首次发布，2009年第一次修订，本次为第二次修订。

移动通信网安全防护要求

1 范围

本文件规定了IPv4、IPv6、双栈环境下的移动通信网的安全防护要求，包括业务安全、网络安全、网元设备和基础设施安全、物理环境安全和管理安全等方面。

本文件适用于指导移动通信网安全防护工作开展和推进。

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。

YD/T 1754-2008	电信网和互联网物理环境安全等级保护要求
YD/T 1756	电信网和互联网管理安全等级保护要求
YD/T 3799	电信网和互联网网络安全防护定级备案实施指南
YD/T 4694	5G 独立组网（SA）架构核心网安全防护要求
YD 5098	通信局（站）防雷与接地工程设计规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

移动通信网 mobile communication network

通过无线接入技术为公众用户提供移动通信业务的网络。

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
AAA	认证、授权、计费	Authentication, Authorization, and Accounting
AC	鉴权中心	Authentication Center
AKA	鉴权和密钥协商	Authentication and Key Agreement
AMF	接入和移动性管理功能	Access Management Function
AN	接入网	Access Network
AN-AAA	接入网认证、授权、计费	Access Network-Authentication, Authorization, and Accounting
API	应用程序编程接口	Application Programming Interface
ARP	地址解析协议	Address Resolution Protocol
AUC	鉴权中心	Authentication Center
AUSF	认证服务器功能	Authentication Server Function
BG	边界网关	Border Gateway
BGP	边界网关协议	Border Gateway Protocol
BSF	绑定支持功能	Binding Support Function

BTS	基站收发信站点	Base Transceiver Station
CDMA	码分多址	Code Division Multiple Access
CG	计费网关	Charging Gateway
CPU	中央处理器	Central Processing Unit
CSCF	呼叫会话控制功能	Call Session Control Function
CSMF	通信服务管理功能	Communication Service Management Function
DDoS	分布式拒绝服务	Distributed Denial of Service
DMZ	隔离区	Demilitarized Zone
DNS	域名服务器	Domain Name Server
EAP	扩展认证协议	Extensible Authentication Protocol
eNB	演进型基站	Evolved Node B
ESP	封装安全负载	Encapsulating Security Payload
EPC	分组核心网	Evolved Packet Core
FTP	文件传送协议	File Transfer Protocol
GGSN	网关 GPRS 支持节点	Gateway GPRS Support Node
GMSC	网关移动交换中心	Gateway Mobile Switching Center
GMSCe	网关移动交换中心元件	Gateway Mobile Switching Center element
gNB	下一代基站	next Generation Node B
GPRS	通用分组无线业务	General Packet Radio Service
GSM	全球移动通信系统	Global System for Mobile communications
GW-C	控制面网关	Gateway-Control
GW-U	用户面网关	Gateway -User
HLR	归属位置寄存器	Home Location Register
HRPD	高速分组数据	High Rate Packet Data
HTTPS	超文本传输安全协议	Hypertext Transfer Protocol Secure
HSS	归属用户服务器	Home Subscriber Sever
HSS-FE	归属用户服务器前端	Home Subscriber Sever- FrontEnd
HSS-BE	归属用户服务器后端	Home Subscriber Sever- BackEnd
IBCF	互联边界控制功能	Interconnection Border Control Function
ICMP	互联网控制消息协议	Internet Control Message Protocol
I-CSCF	查询呼叫会话控制功能	Interrogating Call Session Control Function
IKE	互联网密钥交换协议	Internet Key Exchange
IMS	互联网多媒体子系统	IP Multimedia Subsystem
IMSI	国际移动用户识别码	International Mobile Subscriber Identity
I/O	输入输出	Input/Output
ISIM	互联网多媒体服务身份模块	IP Multimedia Service Identity Module
IS-IS	中间系统到中间系统	Intermediate System to Intermediate System
IP	互联网协议	Internet Protocol
IPSec	互联网安全协议	Internet Protocol Security
IPv4	互联网协议第四版	Internet Protocol Version 4
IPv6	互联网协议第六版	Internet Protocol Version 6
LTE	长期演进项目	Long Term Evolution
MSC	移动交换中心	Mobile Switch Center
MSCe	移动交换中心元件	Mobile Switch Center element
MS	移动台	Mobile Station
MME	移动管理节点	Mobility Management Entity
NF	网络功能	Network Functions
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
NFVO	网络功能虚拟化编排器	Network Functions Virtualization Orchestrator

NEA	5G 加解密算法	Encryption Algorithm for 5G
NIA	5G 完整性保护算法	Integrity Algorithm for 5G
NRF	网络存储功能	Network Repository Function
NSA	非独立组网	Non-Standalone
NSD	网络服务描述符	Network Service Descriptor
NSMF	网络切片管理功能	Network Slice Management Function
NSSF	网络切片选择功能	Network Slice Selection Function
NSSMF	网络切片子网管理功能	Network Slice Subnet Management Function
OAM	操作管理和维护	Operation Administration and Maintenance
OMC-R	无线接入网网元统一管理平台	Operation & Management Center-Radio
OSPF	开放式最短路径优先	Open Shortest Path First
PDSN	分组数据业务节点	Packet Data Serving Node
PCF	分组控制功能	Packet Control Function
PCRF	策略和计费规则功能	Policy and Charging Rules Function
PCRF-FE	策略和计费规则功能前端	Policy and Charging Rules Function- FrontEnd
PCRF-BE	策略和计费规则功能后端	Policy and Charging Rules Function- BackEnd
P-CSCF	代理呼叫会话控制功能	Proxy Call Session Control Function
RNC	无线网络控制器	Radio Network Controller
RIPng	下一代路由信息协议	Routing Information Protocol next generation
RRC	无线资源控制	Radio Resource Control
SAE	独立设备	Stand Alone Equipment
SAE-GW	独立设备网关	Stand Alone Equipment-Gateway
S-CSCF	服务呼叫会话控制功能	Serving Call Session Control Function
SDN	软件定义网络	Software Defined Network
SEPP	安全边缘保护代理	Security Edge Protection Proxy
SGSN	服务 GPRS 支持节点	Serving GPRS Support Node
S-GW	服务网关	Serving GateWay
SIP	会话初始协议	Session initialization Protocol
SMF	会话管理功能	Session Management Function
SNMP	简单网络管理协议	Simple Network Management Protocol
SSH	安全外壳协议	Secure Shell
TD-SCDMA	时分同步码分多址	Time Division Synchronous Code Division Multiple Access
TLS	传输层安全协议	Transport Layer Security
TLCP	传输层密码协议	Transport Layer Cryptography Protocol
TMSI	用户临时识别码	Temporary Mobile Subscriber Identity
TMSC	汇接移动交换中心	Time Multiplexed Switched Crossbar
TMSCe	汇接移动交换中心元件	Time Multiplexed Switched Crossbar element
UE	用户设备	User Equipment
UDM	统一数据管理	Unified Data Management
UDM-FE	统一数据管理前端	Unified Data Management- FrontEnd
UPF	用户平面功能	User-Plane Function
UPS	不间断电源	Uninterruptible Power Supply
VIM	虚拟化基础设施管理器	Virtualised Infrastructure Manager
VLAN	虚拟局域网	Virtual Local Area Network
VxLAN	虚拟扩展局域网	Virtual eXtensible Local Area Network
VLR	拜访位置寄存器	Visitor Location Register
VM	虚拟机	Virtual Machine
VNF	虚拟网络功能	Virtual Network Function
VNFD	虚拟网络功能描述符	Virtual Network Function Descriptor

VNFM	虚拟化网络模块功能管理器	Virtualised Network Function Manager
VPN	虚拟专用网	Virtual Private Network
WAF	网络应用程序防火墙	Web Application Firewall
WCDMA	宽带码分多址	Wideband Code Division Multiple Access

5 移动通信网安全防护概述

5.1 移动通信网安全防护范围

移动通信网的安全防护范畴包括 GSM/GPRS/WCDMA/TD-SCDMA 网、cdma2000/HRPD 网、LTE/EPC 网络、5G 网络以及与这些网络运行和业务提供相关的传送网、IP 承载网、信令网、同步网、支撑网等相关系统。

本文件仅对移动通信网中的 GSM/GPRS/WCDMA/TD-SCDMA 网、cdma2000/HRPD 网、LTE/EPC 网络、5G 网络提出安全防护要求。传送网、IP 承载网、信令网、同步网、支撑网等安全防护的具体要求应遵循各自的安全防护要求标准。

5.2 移动通信网安全防护内容

移动通信网运营者应根据YD/T 3799中确定安全等级的方法确定移动通信网的安全等级，并依据安全等级开展包括业务安全、网络安全、网元设备和基础设施安全、物理环境安全和管理安全等五个层面的安全防护工作。其中：

a） 业务安全：主要包括移动通信网业务接入、业务连续方面的要求；
b） 网络安全：主要包括移动通信网结构拓扑、接入安全、网络域安全等方面内容和要求；
c） 网元设备和基础设施安全：主要包括移动通信网中各网元设备和基础设施安全方面的内容和要求；
d） 物理环境安全：主要包括移动通信网所在的物理环境的安全要求；
e） 管理安全：主要包括移动通信网风险评估、应急预案等方面内容和要求。

6 移动通信网安全等级保护要求

6.1 第 1 级要求

不作要求。

6.2 第 2 级要求

6.2.1 业务安全要求

业务安全应满足以下要求：

a) 在业务开始时对用户进行认证，防止未授权用户接入业务。
b) 在网络发生拥塞或设备发生单点故障时，应保证业务的连续性。
c) 应能够记录操作维护人员对网络进行的操作，对发布、修改、删除等操作行为进行记录，并且可以按时间、操作方式、操作人员来查询。

6.2.2 网络安全要求

6.2.2.1 网络拓扑结构

网络拓扑结构应满足以下要求：

a) 网络设备处理能力应具备冗余空间，满足流量高负荷时需求，不能由于设备配置不够而导致网络全部或者局部瘫痪。

b) 网络拓扑设计合理（如不存在单点瓶颈、支持不停网的扩容等），应绘制与当前运行情况相符合的网络拓扑图。

6.2.2.2 接入安全

6.2.2.2.1 接入 GSM 网络安全

GSM网络接入安全应满足以下要求：

a) 对接入的用户身份发起鉴权认证，验证用户身份的合法性，保证只有授权用户能够接入网络。

b) 应提供用户身份的保密措施。在用户初次接入网络或在网络丢失用户的TMSI和IMSI同步时，才会请求用户发送IMSI。

c) 应在MS和BTS之间提供数据的加密机制，保证数据在无线链路上的传输安全。（在国家未对算法作出具体规定之前，对此功能不做要求）

6.2.2.2.2 接入 GPRS 网络安全

GPRS网络接入安全应满足以下要求：

a) 对接入的用户身份发起鉴权认证，验证用户身份的合法性，保证只有授权用户能够接入网络。

b) 应提供用户身份的保密措施。在用户初次接入网络或在网络丢失用户的TMSI和IMSI同步时，才会请求用户发送IMSI。

c) 应在MS和SGSN之间提供用户数据的加密机制，保证用户数据在链路上的传输安全。（在国家未对算法作出具体规定之前，对此功能不做要求）

6.2.2.2.3 接入 WCDMA/TD-SCDMA 网络安全

WCDMA/TD-SCDMA网络接入安全应满足以下要求：

a) 支持双向鉴权认证功能。对接入的用户身份发起鉴权认证，验证用户身份的合法性，保证授权用户能够接入网络。用户对接入的网络发起鉴权认证，验证网络的合法性，保证用户能够接入合法网络。

b) 应提供用户身份的保密措施。在用户初次接入网络的时候IMSI才被发送，仅在无线信道上发送移动用户相应的TMSI。

c) 应支持用户和网络之间的密钥协商机制。

d) 应在MS和RNC之间提供数据的加密机制，保证数据在链路上的传输安全。（在国家未对算法作出具体规定之前，对此功能不做要求）

e) 应该支持对层三RRC消息的完整性保护，用于维护信令的完整性。

6.2.2.2.4 接入 cdma2000 网络安全

cdma2000网络接入安全应满足以下要求：

a) 对接入的用户身份发起鉴权认证，验证用户身份的合法性，保证只有授权用户能够接入网络。

b) 在空中接口的层三提供鉴权和加密的服务。

c) 应在MS和基站系统之间提供数据的加密机制，保证数据在无线链路上的传输安全。（在国家未对算法作出具体规定之前，对此功能不做要求）

6.2.2.2.5 接入 cdma2000 HRPD 网络安全

cdma2000 HRPD网络接入安全应满足以下要求：

a) 应支持AN-AAA对移动台进行无线接入网的认证和授权。
b) 对接入的用户身份发起鉴权认证，验证用户身份的合法性，保证授权用户能够接入网络。
c) 应支持空中接口安全层的密钥交换、鉴权和加密服务，安全层使用密钥交换协议、鉴权协议、加密协议和安全协议提供这些功能。
d) 应在MS和基站系统之间提供数据的加密机制，保证数据在无线链路上的传输安全。（在国家未对算法作出具体规定之前，对此功能不做要求）

6.2.2.2.6 接入 IMS 网络安全

IMS网络接入安全应满足以下要求：

a) 提供用户和IMS网络之间的双向认证。HSS负责产生密钥和挑战，委托S-CSCF执行用户认证的操作。认证基于由ISIM和HSS共享的密钥和算法。
b) UE与P-CSCF之间的SIP信令消息使用IPSec ESP提供机密性和完整性保护。
c) 应提供用户身份的保密措施。在用户初次接入网络或在网络丢失用户的TMSI和IMSI同步时，才会请求用户发送IMSI。

6.2.2.2.7 接入 LTE/EPC 网络安全

LTE/EPC网络接入安全应满足以下要求：

a) 应支持用户和LTE/EPC网络之间的双向认证。
b) 应支持对用户数据的加密和完整性保护，支持根据需要启用或关闭对用户数据的加密及完整性等保护机制。

6.2.2.2.8 接入 5G 网络安全

5G网络接入安全应满足以下要求：

a) 应支持通过5G网络AMF、AUSF、UDM网元实现用户UE和5G网络的双向认证。
b) 应支持并开启UE和基站之间信令数据的机密性和完整性保护措施，其中除了未经认证的紧急服务以外，完整性保护禁止使用空完整性保护算法（NIA0算法）。
c) 应支持UE和基站之间用户面数据的机密性保护措施，UE的用户面安全策略能够激活UE的用户面机密性保护。
d) 应支持并开启UE和基站之间用户面数据的完整性保护，其中除了未经认证的紧急服务以外，完整性保护禁止使用空完整性保护算法（NIA0算法）。
e) 对于未经认证的紧急服务，5G网络应仅支持法律法规要求支持的服务类型。例如，限制终端在未经认证的情况下使用紧急服务时，仅能发起110、119等紧急呼叫服务。
f) 应支持基于IPsec ESP和IKEv2证书，对gNB的Xn/Xx、N2、N3、S1-U等外部接口的通信提供认证保护，以及机密性、完整性和抗重放保护。其中，Xx接口指NSA组网下gNB和eNB之间的直联接口，S1-U接口指NSA组网下gNB和EPC的S-GW之间的直联接口。

6.2.2.3 网络域安全

6.2.2.3.1 GPRS/WCDMA/TD-SCDMA 网络域安全

GPRS/WCDMA/TD-SCDMA网络域应满足以下要求：

a) 在分组域与外部 IP 网络之间应设置防火墙进行隔离，禁止外部网络对内部网络的配置操作，并严格管理内部网络数据。
b) 不同分组域之间互连时应在 BG 处设置防火墙进行隔离。

6.2.2.3.2 cdma2000 HRPD网络域安全

在PDSN与外部IP网络之间应设置防火墙进行隔离，禁止外部网络对内部网络的配置操作，并严格管理内部网络数据。

6.2.2.3.3 IMS网络域安全

IMS网络域应满足以下要求：

a) 通过选择网络隐藏机制提供对其他网络运营单位隐藏网络拓扑的能力，包括隐藏S-CSCF的数量、S-CSCF的能力以及网络能力，归属网络中的所有I-CSCF将共享一个加密和解密密钥。
b) 与外部IP网络之间应设置防火墙进行隔离，禁止外部网络对内部网络的配置操作，并严格管理内部网络数据。
c) 在两个网络运营单位域间进行互连的IBCF处应设置防火墙进行隔离。

6.2.2.3.4 LTE/EPC网络域安全

LTE/EPC网络域应满足以下要求：

a) 应采用VPN单独组网，与其它网络在逻辑上进行隔离。
b) 与外部IP网络之间应设置防火墙进行隔离。
c) 与外部IP网络互联互通时或者设备间通信途径外部网络时可采用IPSec机制，提供消息机密性、完整性保护安全。
d) 应对可疑的连接、非法访问进行监控，对未经防火墙的登录和口令爆破的行为进行告警。

6.2.2.3.5 5G网络域安全

5G核心网除满足YD/T 4694第2级要求外，还应满足以下要求：

a) 核心网服务化NF之间、NF与NRF之间、NRF之间均应支持使用基于证书的TLS建立安全会话，并进行双向认证。
b) 应具备网络流量检测与防护能力，支持用户面、信令面与管理面安全检测与防护能力。
c) 与外部IP网络之间应设置防火墙进行隔离。
d) 与跨境网络运营单位对接时，应部署SEPP网关进行信令流量的保护。

6.2.3 网元设备和基础设施安全要求

网元设备和基础设施应满足以下要求：

a) 移动通信网网元、网络设备、基础设施、配套管理系统和安全设备均应支持IPv4、IPv6的单栈、双栈环境。
b) 网元接口、安全设备应支持基于IPv6的访问控制策略，且遵循访问控制最小化原则。
c) 网络设备应支持IPv6路由协议安全功能，支持OSPFv3、RIPng路由协议的认证；支持IS-ISv6、BGP4+的认证，支持BGP4+路由振荡抑制。
d) 网元设备应满足设备技术规范、设备入网管理相关要求，设备退网时应将相关配置数据全部清除。

6.2.4 物理环境安全要求

6.2.4.1 机房、办公场地物理环境安全

除满足YD/T 1754-2008中第2级的安全要求外，还应满足以下要求：

a) 机房整体抗震能力应不低于里氏7级，相关楼层承重能力不低于750公斤/平方米。
b) 机房应具备防虫防鼠等相关措施，以有效防范鼠虫蚁害。

6.2.4.2 室外无线接入设备场地物理环境

6.2.4.2.1 物理位置的选择

除满足6.2.4.1要求外，室外无线接入设备场地还应选择在具有防震、防风和防雨等能力的建筑内。

6.2.4.2.2 防盗窃和防破坏

应满足以下要求：

a) 将主要设备放置在物理受限的范围内。
b) 对设备或主要部件进行固定，并设置明显的不易除去的标记。
c) 将通信线缆铺设在隐蔽处，如铺设在地下或管道中等。

6.2.4.2.3 防雷击

除满足YD 5098中 “通用规定”、“综合通信大楼的防雷与接地”、“有线通信局（站）的防雷与接地”的要求外，还应满足以下要求：

a) 室外无线接入设备建筑设置避雷装置。
b) 应设置交流电源地线。

6.2.4.2.4 防火

应设置灭火设备，并保持灭火设备的良好状态。

6.2.4.2.5 防水和防潮

应满足以下要求：

a) 应采取措施防止雨水通过屋顶和墙壁渗透。
b) 应采取措施防止室内水蒸气结露和地下积水的转移与渗透。

6.2.4.2.6 温湿度控制

应设置温、湿度自动调节设施，使室外无线接入设备场地温、湿度的变化在设备运行所允许的范围之内。

6.2.4.2.7 防尘

应采取必要的对室外无线接入设备场地的防尘措施，出入室外无线接入设备场地要求使用鞋套，有专人定期对室外无线接入设备场地进行除尘工作。

6.2.4.2.8 电力供应

应满足以下要求：

a) 应设置稳压器和过电压防护设备。
b) 应提供短期的备用电力供应（如UPS设备）。

6.2.5 管理安全要求

应满足YD/T 1756中第2级的安全要求。

6.3 第 3 级要求

6.3.1 业务安全要求

应满足6.2.1的要求。

6.3.2 网络安全要求

6.3.2.1 网络拓扑结构

6.3.2.1.1 GSM/GPRS/WCDMA/TD-SCDMA 网络拓扑结构

除满足6.2.2.1要求外，还应满足以下要求：

a) GMSC 或 GMSC Server 应当采用 1+1 方式配置，并通过负荷分担方式来保证业务安全，避免单一 GMSC 或 GMSC Server 瘫痪时导致业务全阻。
b) TMSC 或 TMSC Server 应当采用 1+1 方式配置，并通过负荷分担方式来保证业务安全，避免单一 TMSC 或 TMSC Server 瘫痪时导致业务全阻。
c) MSC 或 MSC Server 至关口局和汇接局之间应当具备双路由或多路由。
d) HLR 应当采用 1+1 或 N+1 备份，具有负荷分担的能力。
e) GGSN 要求采用负荷分担的工作方式，或者采用 N+1 备份的工作方式。
f) DNS 和 CG 设备应当采用 1+1 备份的工作方式，具有负荷分担的能力。
g) 网络域至无线接入系统应当采用物理上的多路由方式配备，在不同的传输设备和传输线路上相互保护，确保传输路径的安全，避免单一传输通道阻断时导致业务全阻。

6.3.2.1.2 cdma2000 网络拓扑结构

除满足 6.2.2.1 外，还应满足以下要求：

a) GMSC 或 GMSCe 应当采用 1+1 方式配置，并通过负荷分担方式来保证业务安全，避免单一 GMSC 或 GMSCe 瘫痪时导致业务全阻。
b) TMSC 或 TMSCe 应当采用 1+1 方式配置，并通过负荷分担方式来保证业务安全，避免单一 TMSC 或 TMSCe 瘫痪时导致业务全阻。
c) MSC 或 MSCe 至关口局和汇接局之间应当具备双路由或多路由。
d) 网络域至无线接入系统应当采用物理上的多路由方式配备，在不同的传输设备和传输线路上相互保护，确保传输路径的安全，避免单一传输通道阻断时导致业务全阻。
e) HLR 应当采用 1+1 或 N+1 备份，具有负荷分担的能力。
f) PDSN 设备应具有负荷分担的能力。
g) AAA 设备应采用 1+1 或 N+1 备份配置，具有负荷分担的能力。

6.3.2.1.3 cdma2000 HRPD 网络拓扑结构

除满足 6.2.2.1 外，还应满足以下要求：

a) PDSN 设备应具有负荷分担的能力。
b) AN-AAA、AAA 设备应采用 1+1 或 N+1 备份配置，具有负荷分担的能力。
c) 网络域至无线接入系统应采用物理上的多路由方式配备，在不同的传输设备和传输线路上相互保护，确保传输路径的安全，避免单一传输通道阻断时导致业务全阻。

6.3.2.1.4 IMS 网络拓扑结构

除满足6.2.2.1要求外，还应满足以下要求：

a） HSS的设置应采用N+1或1＋1的配置方式，支持对HSS上保存的用户信息相关的数据备份，发生故障时能够实现自动倒换或进行系统再配置。

b） S/I-CSCF应采用N+1方式配置，并通过负荷分担方式来保证业务安全，避免单一S/I-CSCF瘫痪时导致业务全阻。

c） 应支持应用服务器的N+1方式冗余备份配置，在主用应用服务器出现故障的情况下控制S-CSCF和备用应用服务器交互。

6.3.2.1.5 LTE/EPC 网络拓扑结构

除满足6.2.2.1要求外，还应满足以下要求：

a） MME、SAE-GW应采用Pool（资源池）方式的备份配置，具有负荷分担的能力。

b） HSS的设置应采用1+1互备的备份配置方式，支持对HSS上保存的用户信息相关的数据备份，发生故障时能够实现自动倒换或进行系统再配置。

c） PCRF应采用N+1主备方式的备份配置。

6.3.2.1.6 5G 网络拓扑结构

除满足6.2.2.1要求外，还应满足以下要求：

a） 5G核心网的所属资源池、控制面网元、配套支撑系统应支持异址双数据中心部署。

b） 5G核心网AMF、SMF/GW-C应采用N+1 Pool（资源池）方式的备份配置，具有负荷分担的能力。

c） UDM-FE、HSS-FE、PCF/PCRF-FE、UPF/GW-U应采用N+1备份配置，具有负荷分担的能力。

d） BSF应采用1+1备份配置，具有负荷分担的能力。

e） UDM/HSS-BE、PCF/PCRF-BE、NRF、NSSF应采用1+1主备的备份配置。

6.3.2.2 接入安全

同6.2.2.2要求。

6.3.2.3 网络域安全

6.3.2.3.1 GPRS/WCDMA/TD-SCDMA 网络域安全

同 6.2.2.3.1 要求。

6.3.2.3.2 cdma2000/HRPD 网络域安全

同 6.2.2.3.2 要求。

6.3.2.3.3 IMS 网络域安全

除满足6.2.2.3.3要求外，还应满足以下要求：

a） 网络域内CSCF和HSS之间应采用IPSec机制，提供消息机密性、完整性保护。

b） 相同网络内的CSCF之间应采用IPSec机制，提供消息机密性、完整性保护。

c） 应支持对S-CSCF上保存的和用户注册状态信息相关的数据备份（包括用户注册路由信息Path头域、用户注册的Contact地址、P-Visited-Network-ID、终端的鉴权方式等信息），当为注册用户提供服务的S-CSCF出现故障时，这些数据能够下载到重新为用户分配的服务S-CSCF上。

d） I-CSCF应能够根据负载均衡、能力集和可用性选择S-CSCF，并支持S-CSCF的重新分配。

e） 当第三方应用服务器请求接入IMS核心网络域时，需要对第三方应用服务器进行认证和鉴权，只有合法且认证通过的服务器才能接入的核心网络域中，而且I-CSCF应当对第三方应用服务器隐藏网络运营单位网络拓扑信息。

6.3.2.3.4 LTE/EPC 网络域安全

同 6.2.2.3.4 要求。

6.3.2.3.5 5G 核心网安全域与隔离

5G核心网除满足YD/T 4694第3级要求外，还应满足以下要求：

a) 应对控制平面、转发平面、OAM 管理平面实施资源隔离。
b) 5G 核心网应在平面资源隔离基础上，划分控制域、转发域、管理域等安全域。控制域网元应根据其功能特性和安全级别，以及与互联网连接和暴露程度进行安全子域的划分，至少划分可信区与 DMZ 区。
c) 5G 核心网应在 5G 核心网控制面出口部署控制与管理面防火墙，实施流量访问控制。
d) 5G 核心网应在 5G 核心网网络出口部署用户面防火墙，公网访问 UPF 的流量应经该防火墙进行访问控制。应具备行业客户内网对下沉 UPF 的访问控制能力，以及能够结合行业要求对行业客户内网的访问控制。
e) 应单独划设承载 VPN，并通过防火墙或应用层网关实施安全隔离，保障 5G 核心网安全。
f) 应支持根据业务重要程度，进行企业用户与个人用户网络切片间及企业用户与企业用户网络切片间的逻辑隔离，或采用独立物理机资源、独立网络设备等实现物理隔离。
g) 应只允许相关业务流访问基站所处的接入域，只允许核心控制域 AMF、核心转发域 UPF，以及支撑管理域的设备网管 OMC-R 访问接入域的基站。

6.3.2.4 网络攻击防范（TDM 方式的电路域网络不适用）

网络攻击防范应满足以下要求：

a） 网络应采取安全措施检测和发现网络攻击，安全措施包括入侵防御、防病毒、网络隔离、访问控制、系统加固，安全措施应支持IPv4和IPv6网络环境。
b） 应对网络中关键的系统、设备和网络定期执行安全检查作业，以检查出网络弱点和策略配置上的问题。安全检查作业手段可以包括漏洞扫描、脆弱性扫描、安全基线配置检查等，应支持IPv4和IPv6环境。

6.3.2.5 用户数据存储

用户数据存储应满足以下要求：

a) 应保证重要设备中用户数据、系统配置等相关数据的存储安全性。
b) 应支持对重要设备保存的用户信息、系统配置等相关的数据备份，发生故障时能够实现自动倒换或进行系统再配置。

6.3.3 网元设备和基础设施安全要求

6.3.3.1 网元设备和基础设施通用安全

6.3.3.1.1 网元加固

除满足6.2.3的要求外，还应满足以下要求：

a) 应为不同用户分配不同的账号，避免账号共享，避免用户账号和网元间通信使用的账号共享。应删除或锁定与网元运行、维护等工作无关的账号。根据业务需求建立多个账号组，分配不同的权限。将账号划入某个具体账号组。
b) 网元应启用口令复杂度策略，启用对口令的校验功能，确保对所有口令在设置时即实施复杂度检查。对使用静态口令进行认证的网元或其组件，应设置其静态口令生存期不长于 90 天。
c) 在网元配置能力内，应根据账号需要，为其配置所需最小权限。

d) 当在创建新文件或目录时应屏蔽新文件或目录不应有的访问允许权限，防止同属于该组的其它账号及其他账号组的账号修改该账号的文件。
e) 应确保只有得到授权的用户才能修改文件、数据、文件夹或文件系统。
f) 使用 root 用户或同等最高权限用户账号应仅限于使用系统控制台直接登录的场景，禁止使用 root 用户和同等最高权限用户账号远程登录系统或网元，禁用或重命名默认账号。
g) 网元设备应使用 SSH 等加密协议进行远程维护。
h) 网元应禁用系统内核中与业务无关的网络功能。以下功能应默认关闭：IP 数据包在当前网络设备的不同网口间的转发、代理 ARP、定向广播、IPv4 多播处理、ARP 漫游消息、ICMP 广播的响应。
i) 网元应仅运行其操作所需要的协议处理程序和服务。网络产品的部分服务应由设备商默认初始配置为禁用，除了部署过程中需要的服务，这些服务在部署完成后应按照设备商的操作指南设置为禁用。
j) 网元应禁止安装与业务无关的软件或软件模块，包括缺省的网页、样例数据库文件、样例数据等，如在部署时需要使用的，在部署完成后立即卸载。
k) 在保证网元正常运行的前提下，网元及其组件应安装最新的补丁，或更新至没有安全漏洞的版本。安装更新前应对其进行稳定性测试。
l) 如网元支持，应启用输入限制功能，检查授权用户或程序对网元的输入信息，限制其输入范围，使其不影响网元安全稳定运行。
m) 网元应启用日志记录功能，主要包括系统运行状态、日常操作、故障维护、远程运维等日志，且记录安全事件的时间和内容，所有日志应均能远程上传到日志服务器，且数据留存时间不少于 6 个月。
n) 网元应启用日志文件的访问控制机制，并且只向特定管理员用户授予日志文件访问权限。

6.3.3.1.2 接口安全

接口安全应满足以下要求：

a) 网元应具备在任何 IP 接口上过滤传入的 IP 数据包的机制，并且启用丢包操作的日志记录。
b) 当网元从另一个网元接收到被操纵或不符合标准的数据包时，其可用性或健壮性不应受影响，即这些无效数据包应被检测到且应被丢弃。检测和丢弃过程不应影响网络产品的正常性能，针对大量无效数据包，网络产品健壮性应能保持和单个或少量无效数据包同样的效果。

6.3.3.2 5G 网元设备和基础设施安全

6.3.3.2.1 云化基础设施安全

6.3.3.2.1.1 虚拟化层安全

虚拟化层安全应满足以下要求：

a) 虚拟化管理器（Hypervisor）应实现同一物理机上不同虚拟机之间的计算、存储和网络等资源隔离，包括：虚拟 CPU 调度安全隔离、内存资源安全隔离、硬盘 I/O 安全隔离、内部网络安全隔离，并运行各自的操作系统和应用。
b) 用户使用虚拟机时，仅能访问属于自己虚拟机的资源（如硬件、软件和数据），不能访问其他虚拟机的资源，保证虚拟机隔离安全，并确保其无法探测其他虚拟机的存在。
c) 虚拟化管理器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。
d) 虚拟化管理器应支持设置 VM 的操作权限及每个 VM 使用资源的限制，如最小或最大的虚拟 CPU 数量，内存等，并监控资源的使用情况。

e) 虚拟化管理器管理接口流量应该和其它（如业务、存储等）网络接口流量物理隔离。

6.3.3.2.1.2 计算资源安全

计算资源应满足以下要求：

a) 应支持物理节点中的容器或虚拟机的资源配额限制方式，保护容器或虚拟机的性能不受其他容器或虚拟机资源消耗的影响。

b) 应支持容器或虚拟机仅能迁移至相同安全保护等级的资源池。

6.3.3.2.1.3 存储资源安全

存储资源应满足以下要求：

a) 应支持根据承载的云化应用类型及安全级别，具有虚拟化存储安全隔离的措施和存储位置分配的能力。

b) 应支持容器/虚拟机镜像文件完整性保护的能力，在镜像文件执行前验证镜像签名，确保来自可信源且未被篡改。

6.3.3.2.1.4 网络资源安全

网络资源应满足以下要求：

a) 应支持根据安全域划分原则，通过 VLAN/VxLAN 隔离不同租户南北向和东西向的网络资源；

b) 根据最小访问原则，应仅开放必需对外部 IP 及端口，禁止默认端口直接对外开放；

c) 应具备容器/虚拟机端口流量限速功能，实现端口级别的流量控制。

6.3.3.2.2 SDN 安全

6.3.3.2.2.1 集中控制平面安全

集中控制平面应满足以下要求：

a) 应支持对 SDN 控制器等集中控制平面提供流量控制或多控制器等手段，防止过度消耗流表资源导致控制器服务不可用；

b) 应支持通过加密方式访问控制器，对网络设备和控制器进行身份认证，交换机和控制器支持采用 TLS/TLCP 加密协议的安全版本进行通信，防止假冒控制器非法控制交换机等设备；

c) 应支持 SDN 控制器和虚拟化系统集成的用户访问控制策略冲突检测手段，保障访问控制策略的一致性。

d) SDN 控制器应支持对操作系统、数据库和中间件进行安全加固配置，满足安全基线要求。SDN 控制器上线前应对所有已知漏洞进行风险管控，运行过程中应定期接受漏洞扫描和端口扫描，并对检测出的漏洞进行风险管控，对开放的不必要的、未使用的端口和服务进行关闭。

e) SDN 控制器应支持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 DDoS 攻击。

f) SDN 控制器支持基于证书认证 VIM，以及使用 HTTPS 保证北向传输数据的机密性、完整性。

g) SDN 控制器应支持对北向 VIM 的访问进行授权。

h) SDN 控制器应支持对交换机和 SDN 网关进行认证，并和交换机/SDN 网关建立安全通道，保证南向接口传输数据的机密性和完整性。

6.3.3.2.2.2 开放 API 安全

开放API应满足以下要求：

a) 应支持对通过集中控制器的 API 接口下发的应用层策略进行规则检查，检测下发的规则是否有

冲突，是否符合安全策略、业务逻辑和行为特征，检测规则下发后是否导致网络发生异常；

b) 应支持对 SDN 控制器、VNF 等的开放 API 进行身份认证和细粒度的权限控制，防止越权的接口调用；

c) 启用 API 白名单，对发往 API 网关的请求进行过滤，禁止非授权访问。

6.3.3.2.2.3 数据平面安全

数据平面应满足以下要求：

a) 应具备对保存的敏感信息的防护手段，防止流表等敏感信息泄露；

b) 应支持对云化 VNF 调用用户身份、移动轨迹、位置信息等涉及用户敏感数据服务进行严格授权，同时支持对信息的使用进行严格限制，在数据外发前应对敏感数据进行脱敏操作。

6.3.3.2.3 云化 VNF 安全

云化VNF应满足以下要求：

a) 应支持云化 VNF 的上线、运行和下线的生命周期安全管控。

b) 应支持根据云化 VNF 的重要程度配置不同的流控策略，保障重要业务的稳定运行。

c) 应对云化 VNF 进行权限控制，避免云化 VNF 权限过高产生容器/虚拟机逃逸，导致非法提权；

d) 应支持企业自身 VNF 和第三方 VNF 的物理或逻辑隔离。

e) VNF 在安装、升级过程中应对软件进行完整性验证。

6.3.4 物理环境安全要求

6.3.4.1 机房、办公场地物理环境安全

除满足6.2.4.1和YD/T 1754-2008中第3.1级的安全要求外，还应满足以下要求：

a) 机房整体抗震能力应不低于里氏8级，相关机架及设备需进行必要的抗震加固，相关楼层承重能力不低于1000公斤/平方米。

6.3.4.2 室外无线接入设备场地物理环境

6.3.4.2.1 物理位置的选择

除满足6.2.4.2.1要求外，还应满足以下要求：

a) 室外无线接入设备场地应当避开强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区。

b) 室外无线接入设备场地整体抗震能力应不低于里氏8级，相关机架及设备需进行必要的抗震加固，承重能力不低于1000公斤/平方米。

6.3.4.2.2 防盗窃和防破坏

除满足6.2.4.2.2要求外，还应设置室外无线接入设备场地的防盗报警系统，以防进入室外无线接入设备场地的盗窃和破坏行为。

6.3.4.2.3 防雷击

除了满足6.2.4.2.3的要求，场地还应设置防雷保安器，防止感应雷。

6.3.4.2.4 防火

除了满足6.2.4.2.4的要求，场地房间还应采用具有耐火等级的建筑材料。

6.3.4.2.5 防水和防潮

应满足6.2.4.2.5的要求。

6.3.4.2.6 温湿度控制

应满足6.2.4.2.6的要求。

6.3.4.2.7 防尘

应满足6.2.4.2.7的要求。

6.3.4.2.8 电力供应

除满足6.2.4.2.8要求外，还应满足以下要求：

a) 应设置冗余或并行的电力电缆线路，或采用其他手段保证不间断供电。
b) 应建立备用供电系统（如备用发电机），以备常用供电系统停电时启用。

6.3.5 管理安全要求

应满足6.2.5和YD/T 1756中第3级的安全要求。

5G网络运维管理安全还应满足以下要求：

a) 应对业务系统的认证、授权、账号、审计进行管控，对资产的安全属性、风险进行管控。网络运营单位应定期支持 5G 核心网相关网络系统的日志安全记录，主要包括系统运行状态、日常操作、故障维护、远程运维等日志。
b) 网络运营单位应定期对 5G 核心网相关网络系统开展安全审计，应基于各类应用资源及系统资源的日志信息、账号信息、权限信息、工单信息以及纸质凭证等有效审计证据开展，审计结论必须获得审计证据支持。
c) 应通过漏洞情报采集分析、漏洞检测分析进行漏洞检查，需要将 NFV 资产纳入安全漏洞核查范围。
d) 应进行周期性漏洞扫描，并切实做好补丁管理。
e) 网络云中的虚拟化管理器、子操作系统、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、安全补丁管理等相关通用的安全要求。
f) 虚拟化网元部署采用的操作系统、数据库、中间件等应满足安全合规基线配置要求。
g) 虚拟化网元进行升级、部署等操作时，应在 NFVO 和 VNFM 中对软件包（VNFD、NSD）的合法性和完整性进行校验。
h) 虚拟机及镜像应开展安全管理。
i) 应建立完善安全资产管理手段、网络安全态势感知和风险监测手段，提供各类安全风险的主动监测与感知能力。
j) 建立网络及业务容灾备份机制，实现重要系统和网络数据的异地备份，保障业务连续性。
k) 网络运营单位间的网络切片运营管理系统（如 CSMF、NSMF、NSSMF）应实现网络切片需求与策略信息的传递，以及网络切片运营管理能力共享。

6.4 第 4 级要求

暂不规定。

6.5 第 5 级要求

暂不规定。

参 考 文 献

[1] GF 015.1-1995 900MHz TDMA 数字蜂窝移动通信系统设备总技术规范 第一分册 交换子系统(SSS)设备技术规范 YDN 065-1997
[2] GF 015.2-1995 900MHz TDMA 数字蜂窝通信系统设备总技术规范 第二分册 基站子系统(BSS)设备技术规范
[3] YD/T 1057-2000 900/1800MHz TDMA 数字蜂窝移动通信网基站子系统设备测试规范
[4] YD/T 1110-2001 900/1800MHz TDMA 数字蜂窝移动通信网通用分组无线业务（GPRS）设备技术规范：基站子系统
[5] YD/T 1216-2002 900/1800MHz TDMA 数字蜂窝移动通信网通用分组无线业务（GPRS）设备测试方法：基站子系统
[6] YD/T 1105-2001 900/1800MHz TDMA 数字蜂窝移动通信网通用分组无线业务（GPRS）设备技术规范：交换子系统
[7] YD/T 1242-2002 900/1800MHz TDMA 数字蜂窝移动通信网通用分组无线业务(GPRS）设备测试方法：交换子系统
[8] YD/T 1365-2006 2GHz TD-SCDMA 数字蜂窝移动通信网 无线接入网络设备技术要求
[9] YD/T 1366-2006 2GHz TD-SCDMA 数字蜂窝移动通信网 无线接入网络设备测试方法
[10] YD/T 1410-2007 2GHz TD-SCDMA/WCDMA 数字蜂窝移动通信网核心网设备技术要求(第一阶段)
[11] YD/T 1411-2007 2GHz TD-SCDMA/WCDMA 数字蜂窝移动通信网核心网设备测试方法(第一阶段)
[12] YD/T 1505-2007 2GHz TD-SCDMA/WCDMA 数字蜂窝移动通信网媒体网关设备技术要求（第二阶段）
[13] YD/T 1506-2007 2GHz TD-SCDMA/WCDMA 数字蜂窝移动通信网媒体网关设备测试方法（第二阶段）
[14] YD/T 1507-2007 2GHz TD-SCDMA/WCDMA 数字蜂窝移动通信网移动软交换服务器设备技术要求（第二阶段）
[15] YD/T 1508-2007 2GHz TD-SCDMA/WCDMA 数字蜂窝移动通信网移动软交换服务器设备测试方法（第二阶段）
[16] YD/T 1552-2007 2GHz WCDMA 数字蜂窝移动通信网无线接入网络设备技术要求（第一阶段）
[17] YD/T 1553-2007 2GHz WCDMA 数字蜂窝移动通信网无线接入网络设备测试方法（第一阶段）
[18] YDC 014-2003 800MHz CDMA 1X 数字蜂窝移动通信网设备技术要求：基站子系统
[19] YDC 022-2003 800MHz CDMA 1X 数字蜂窝移动通信网设备测试方法：基站子系统
[20] YDC 016-2003 800MHz CDMA 1X 数字蜂窝移动通信网设备技术要求：分组设备
[21] YDC 025-2003 800MHz CDMA 1X 数字蜂窝移动通信网设备测试方法：分组设备
[22] YD/T 1048-2000 800MHz CDMA 数字蜂窝移动通信网设备总技术规范：交换子系统部分
[23] YD/T 1049-2000 800MHz CDMA 数字蜂窝移动通信网设备总测试规范：交换子系统部分
[24] YD/T 1556-2007 2GHz cdma2000 数字蜂窝移动通信网设备技术要求：基站子系统
[25] YD/T 1573-2007 2GHz cdma2000 数字蜂窝移动通信网设备测试方法：基站子系统
[26] YD/T 1568-2007 2GHz cdma2000 数字蜂窝移动通信网设备技术要求：交换子系统
[27] YD/T 1569-2007 2GHz cdma2000 数字蜂窝移动通信网测试方法：交换子系统
[28] YD/T 1557-2007 2GHz cdma2000 数字蜂窝移动通信网设备技术要求：分组设备
[29] YD/T 1574-2007 2GHz cdma2000 数字蜂窝移动通信网设备测试方法：分组设备
[30] YD/T 1561-2007 2GHz cdma2000 数字蜂窝移动通信网设备技术要求：高速分组数据（HRPD）（第一阶段）接入网（AN）

[31] YD/T 1566-2007 2GHz cdma2000 数字蜂窝移动通信网设备测试方法：高速分组数据 HRPD）（第一阶段）接入网（AN）
[32] YD/T 1579-2007 2GHz cdma2000 数字蜂窝移动通信网设备技术要求：高速分组数据（HRPD）（第一阶段）AN-AAA 设备
[33] YD/T 1564-2007 2GHz cdma2000 数字蜂窝移动通信网设备测试方法：高速分组数据（HRPD）（第一阶段）AN-AAA 设备
[34] YD/T 1677-2007 2GHz cdma2000 数字蜂窝移动通信网设备技术要求：高速分组数据（HRPD）（第二阶段）接入网（AN）
[35] YD/T 1678-2007 2GHz cdma2000 数字蜂窝移动通信网设备测试方法：高速分组数据（HRPD）（第二阶段）接入网（AN）
[36] YD/T 1557-2007 2GHz cdma2000 数字蜂窝移动通信网设备技术要求：分组设备
[37] YD/T 1574-2007 2GHz cdma2000 数字蜂窝移动通信网设备测试方法：分组设备