ICS 03.080

CCS A 16

DB21

辽 宁 省 地 方 标 准

DB21/T XXXX—XXXX

基于蜂窝网络的工业无线通信安全规范

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

辽宁省市场监督管理局　　发 布

目 次

前 言 IV
1 范围 1
2 规范性引用文件 1
3 术语和定义 3
3.1 3
3.2 3
3.3 4
4 缩略语 4
5 总体要求 5
6 物理环境安全 6
6.1 室外控制设备物理防护 6
6.2 蜂窝网络接入节点的物理位置 6
7 通信网络安全 6
7.1 网络架构 6
7.2 通信传输 6
8 区域边界安全 6
8.1 边界保护 7
8.2 访问控制 7
8.3 蜂窝网络使用控制 7
8.4 接入控制 7
8.5 入侵防范 7
9 计算环境安全 8
9.1 工业蜂窝网络控制设备安全 8
9.2 终端节点设备安全 8
9.3 网关节点设备安全 9
9.4 抗数据重放 9
9.5 边缘计算 9
10 建设运维安全 9
10.1 产品采购和使用 9
10.2 外包软件开发 9
10.3 运维 9
附 录 A 11
A.1 蜂窝网络要求 11
A.2 组网要求 11
A.3 接入认证 11
A.4 信息安全要求 11
A.5 服务分级要求 11
A.6 定位要求 11
A.7 传输要求 11
A.8 蜂窝网络设备的管理要求 12

A.9 性能指标 12
A.9.1 时延 12
A.9.2 支持最大蜂窝终端设备数量 12
A.9.3 吞吐量 12
A.9.4 非实时带宽 12
A.9.5 时间同步精度 12
A.9.6 非基于时间的同步精度 12
A.9.7 故障恢复时间 12
A.10 工业蜂窝网络访问子层要求 13
附 录 B 14
B.1 接入安全 14
B.2 5GC 安全 14
B.3 MEC 安全 5G 14
B.4 切片安全 15
B.5 服务安全要求 15
B.5.1 一般要求 15
B.5.2 认证要求 16
B.5.3 授权要求 16
B.5.4 身份管理要求 16
B.5.5 监管要求 17
B.5.6 欺诈保护要求 17
B.5.7 资源效率安全要求 18
B.5.8 数据安全和隐私要求 18
B.6 端到端核心网络安全要求 18
B.6.1 通用要求 18
B.6.2 数据传输安全 18
B.7 UE 安全要求 19
应满足 3GPP TS 33.501 中 5.2 中的要求。 19
B.8 gNB 安全要求 19
应满足 3GPP TS 33.501 中 5.3 中的要求。 19
B.9 ng-eNB 安全要求 19
应满足 3GPP TS 33.501 中 5.4 中的要求。 19
B.10 AMF 安全要求 19
应满足 3GPP TS 33.501 中 5.5 中的要求。 19
B.11 SEAF 安全要求 19
B.12 UDM 安全要求 19
B.13 AUSF 安全要求 19

B.14 核心网络安全要求 19
B.15 算法安全要求 19
参 考 文 献 20

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。

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。

本文件由辽宁省工业和信息化厅提出并归口。

本文件起草单位：东北大学、沈阳华睿博信息技术有限公司、沈阳工业大学、辽宁省先进装备制造业基地建设工程中心、鞍钢集团信息产业有限公司、沈阳鼓风机集团股份有限公司、国网辽宁省电力有限公司、宁波和利时信息安全研究院有限公司、恒安嘉新(北京)科技股份公司、三六零安全科技股份有限公司、北京神州绿盟科技有限公司、中国联合网络通信有限公司沈阳市分公司、北京理工大学、北京圣博润高新技术股份有限公司、南京佶合信息科技有限公司。

本文件主要起草人：姚羽、邵华、张晓玲、郭剑峰、陈莹、翟宝鹏、郝玉明、周小明、金阳、梁艳、苗向阳、黄晓波、李士炜、李冬妮、李小川、李昊、杨巍、李慧玲、刘可欣。

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函等方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

本文件起草单位通讯地址和联系电话：通讯地址：辽宁省沈阳市和平区文化路三巷11号，联系电话：024-83687392。

本文件归口部门通讯地址和联系电话：通讯地址：辽宁省沈阳市皇姑区北陵大街45-2号，联系电话：024-86913384。

基于蜂窝网络的工业无线通信安全规范

1 范围

本文件规定了工业蜂窝网络总体要求、物理环境安全、通信网络安全、区域边界安全、计算环境安全和建设运维安全等。

本文件适用于以应用场景为重点的工业蜂窝网络安全的建设运维和监督管理。

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 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 35673-2017 工业通信网络 网络和系统安全 系统安全要求和安全等级

GB/T 41780.1-2022 物联网 边缘计算 第 1 部分：通用要求

YD/T 2910-2015 LTE/SAE 安全技术要求

IEC TS 62443-1-1:2009 工业通信网络 网络和系统安全 第 1-1 部分：术语、概念和模型（Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models）

IEC 62443-2-1:2010 工业通信网络 网络和系统安全 第 2-1 部分：工业自动化和控制系统建设安全程序（Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program）

IEC TR 62443-2-3:2015 工业自动化和控制系统安全 第 2-3 部分：IACS 环境补丁管理（Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment）

IEC 62443-2-4:2015 工业自动化和控制系统安全 第 2-4 部分：IACS 服务提供商安全程序要求（Security for industrial automation and control systems - Part 2-4: Security

program requirements for IACS service providers）

IEC 62443-2-4:2015+AMD1:2017 CSV 工业自动化和控制系统安全 第 2-4 部分：IACS 服务提供商安全程序要求（Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers）

IEC 62443-2-4:2015/AMD1:2017 修改件 1 工业自动化和控制系统安全 第 2-4 部分：IACS 服务提供商安全程序要求（Amendment 1 - Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers）

IEC 62443-2-4:2015/COR1:2015 勘误表 1 工业自动化和控制系统安全 第 2-4 部分：IACS 服务提供商安全程序要求(Corrigendum 1 - Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers）

IEC 62443-3-2:2020 工业自动化和控制系统安全 第 3-2 部分：系统设计安全风险评估（Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design）

IEC TR 62443-3-1:2009 工业通信网络 网络和系统安全 第 3-1 部分：工业自动化和控制系统安全技术（Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems）

IEC 62443-3-3:2013 工业通信网络 网络和系统安全 第 3-3 部分：系统安全要求和安全等级（Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels）

IEC 62443-3-3:2013/COR1:2014 勘误表 1 工业通信网络 网络和系统安全 第 3-3 部分：系统安全要求和安全等级（Corrigendum 1 - Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels）

IEC 62443-4-1:2018 工业自动化和控制系统的安全性 第 4-1 部分：安全产品开发生命周期要求（Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements）

IEC 62443-4-2:2019 工业自动化和控制系统安全 第 4-2 部分：IACS 部件技术安全要求

（Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components）

ISO/IEC 27001 信息技术 安全技术 信息安全管理系统要求（Information technology -- Security techniques -- Information security management systems -- Requirements）

ISO/IEC 27002 信息技术 安全技术 信息安全管理实践规范（Information technology—Security techniques—Code of practice for information security controls）

ISO/IEC 27005 信息技术 安全技术 信息安全风险管理（Information technology—Security techniques—Information security risk management）

3GPP TS 33.310 网络域安全性（NDS）；认证框架（AF）(Network Domain Security (NDS);Authentication Framework(AF))

3GPP TS 24.501 用于 5G 系统的非接入层(NAS)协议(5GS);阶段 3(Technical Specification Group Core Network and Terminals;Non-Access-Stratum (NAS) protocol for 5G System (5GS);Stage 3;)

3GPP TS 33.501 5G 系统安全架构和过程（5G;Security architecture and procedures for 5G System）

3 术语和定义

GB/T 22239-2019、GB/T 22240-2020、GB/T 35673-2017、GB/T 41780.1-2022界定的及以下术语和定义适用于本文件。

3.1

蜂窝网络 cellular network

又称移动网络（mobile network）是一种移动通信硬件架构，分为模拟蜂窝网络和数字蜂窝网络。由于构成网络覆盖的各通信基地台的信号覆盖呈六边形，从而使整个网络像一个蜂窝而得名。

3.2

工业蜂窝网络 industrial cellular network

基于蜂窝网络的工业无线通信网络。

3.3

网络切片 network slice

网络切片是一种按需组网的方式，可以让运营商在统一的基础设施上分离出多个虚拟的端到端网络，每个网络切片从无线接入网承载网再到核心网上进行逻辑隔离，以适配各种各样类型的应用。

4 缩略语

下列缩略语适用于本文件。

AKA：身份验证和密钥协议（Authentication and Key Agreement）

AMF：接入及移动性管理功能（Access and mobile management function）

API：应用编程接口（Application programming Interface）

AUSF：认证服务器功能（Authentication server function）

CPU：中央处理器（Central Processing Unit）

DDos：分布式拒绝服务攻击（Distributed Denial of Service）

DN：数据网络（Data Network）

EPS：演进分组系统（Evolved Packet System）

FTP：文件传输协议（File Transfer Protocol）

gNB：基站协议功能实体（gNodeB）

IP：互联网协议（Internet Protocol）

IPv4：互联网协议第4版（Internet Protocol version 4）

IPv6：互联网协议第4版（Internet Protocol version 6）

IoT：物联网（Internet of Things）

LAN：局域网（Local Area Network）

LAN-VN：局域网-虚拟网络（Local Area Network-Virtual Network）

MANO：管理和编排（Management and Orchestration）

MEC：多接入边缘计算（Multi-access Edge Computing）

NAS：非接入层（Non-Access Stratum）

PLMN：公共陆地移动网（Public Land Mobile Network）

QoS：服务质量（Quality of Service）

RAN：无线接入网络（Radio Access Network）

SEAF：安全锚功能（Safety anchor function）

SEPP：安全边缘保护代理（Security Edge Protection Proxy）

SLA：服务等级协议（Service Level Agreement）

TLS：传输层安全（Transport Layer Security）

UDM：统一数据管理（Unied Data Management）

UE：用户设备（User Equipment）

URLLC：超高可靠性与超低时延通信（Ultra Reliable & Low Latency Communication）

USB：通用串行总线（Universal serial bus）

USIM：全球用户识别卡（Universal Subscriber Identity Module）

3GPP：第三代合作伙伴计划（Third Generation Partnership Project）

5GC：5G核心网络（5G Core Network）

5 总体要求

工业蜂窝网络安全要求涉及工业蜂窝网络基本要求、蜂窝网络安全要求及工业蜂窝网络应用场景的安全要求。

工业蜂窝网络基本要求参考附录A；4G蜂窝网络安全应满足YD/T 2910-2015中的要求；5G蜂窝网络安全要求参考附录B。

工业蜂窝网络应用场景应首先满足工业网络信息安全的规定，如IEC TS 62443-1-1:2009，IEC 62443-2-1:2010，IEC TR 62443-2-3:2015，IEC 62443-2-4:2015，IEC 62443-2-4:2015+AMD1:2017 CSV，IEC 62443-2-4:2015/AMD1:2017，IEC 62443-2-4:2015/COR1:2015，IEC 62443-3-2:2020，IEC TR 62443-3-1:2009，IEC 62443-3-3:2013，IEC 62443-3-3:2013/COR1:2014，IEC 62443-4-1:2018，IEC 62443-4-2:2019，ISO 27001，ISO/IEC 27002，ISO/IEC 27005等标准中的要求，以及网络安全等级保护的要求，如GB/T 22240-2020、GB/T 22239-2019等标准中的要求。此外，还应满足本文件所提出的物理环境安全、通信网络安全、区域边界安全、计算环境安全以及建设运维安全等要求。

6 物理环境安全

6.1 室外控制设备物理防护

室外控制设备物理防护应满足如下要求：

a） 室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；

b） 箱体或装置具有透风、散热、防盗、防雨和防火能力等；

c） 室外控制设备放置应远离强电磁干扰、强热源等环境，如无法避免应及时做好应急处置及检修，保证设备正常运行。

6.2 蜂窝网络接入节点的物理位置

应为蜂窝网络接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

7 通信网络安全

7.1 网络架构

工业控制系统网络架构应满足如下要求：

a） 工业控制系统与企业其他系统之间应划分为不同区域，区域间应采用技术手段实现安全隔离；工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术手段实现安全隔离；

b） 涉及实时控制和数据传输的工业控制系统，应使用独立的网络设备组网，在物理层面上实现与其他数据网及外部公共信息网的安全隔离；

c） 对重要生产系统，应在无线蜂窝网络的边界采用屏蔽或干扰手段，隔离物理边界外对无线蜂窝网络的访问。

7.2 通信传输

在工业控制系统内使用工业生产网络进行控制指令或相关数据交换的应采用加密技术手段实现身份认证、访问控制和数据加密传输。

8 区域边界安全

8.1 边界保护

应保证有线网络与蜂窝网络边界之间的访问和数据流通过蜂窝网络接入网关设备。

8.2 访问控制

工业网络访问控制应满足如下要求：

a） 应在工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的E-Mail，Web、Telnet、Rlogin及FTP等通用网络服务；

b） 应在工业控制系统内安全域和安全域之间的边界防护机制失效时，及时进行报警。

c） 蜂窝网络接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。

8.3 蜂窝网络使用控制

工业蜂窝网络使用控制应满足如下要求：

a） 应对所有参与蜂窝网络通信的用户（人员、软件进程或者设备）提供唯一性标识和鉴别；

b） 应对所有参与蜂窝网络通信的用户（人员、软件进程或者设备）进行授权以及执行使用进行限制；

c） 应对蜂窝网络通信采取传输加密的安全措施，实现传输报文的机密性保护；

d） 对采用蜂窝网络通信技术进行控制的工业控制系统，应能识别其物理环境中发射的未经授权的蜂窝网络设备，报告未经授权试图接入或干扰控制系统的行为。

8.4 接入控制

应保证只有授权的终端节点可以接入。

8.5 入侵防范

工业网络入侵防范应满足如下要求：

a） 终端节点应能够限制与终端节点通信的目标地址，以避免对陌生环境的攻击行为；

b） 终端节点应能够限制与网关节点通信的目标地址，以避免对陌生环境的攻击行为；

c） 应能够检测到非授权蜂窝网络接入设备和非授权移动终端的接入行为；

d） 应能够检测到针对蜂窝网络接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为；

e） 应能够阻断非授权蜂窝接入设备或非授权移动终端；

f） 对重要生产系统应采用探针和异常检测技术对网络行为进行实时检测；

g） 对重要生产系统宜部署态势感知及蜜罐系统进行持续监控，并对网络攻击行为进行捕获。

9 计算环境安全

9.1 工业蜂窝网络控制设备安全

工业蜂窝网络控制设备应满足如下要求：

a） 控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制；

b） 应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作；

c） 应关闭或拆除控制设备的软盘驱动、光盘驱动、USB 接口、串行口或多余网口等，确需保留的应通过相关的技术措施实施严格的监控管理；

d） 应使用专用设备和专用软件对控制设备进行更新；

e） 应保证控制设备在上线前经过安全性检测，避免控制设备固件中存在恶意代码程序。避免设备中存在未授权的无线网络通信模块。

9.2 终端节点设备安全

工业蜂窝网络终端节点设备应满足如下要求：

a） 终端节点设备应保证只有授权的用户可以对终端节点设备上的软件应用进行配置或变更；

b） 终端节点设备应具有对其连接的网关节点设备进行身份标识和鉴别的能力；

c） 终端节点设备应具有对其连接的其他终端节点设备进行身份标识和鉴别的能力；

d） 对重要生产系统，当终端节点设备通过非可信网络访问（例如远程访问）控制系统时，控制系统应为其提供多因子认证的能力；

e） 控制系统应具备对经由不可信网络访问控制系统的访问控制限制的方法，例如可限制未授权的 IP 地址接入。

9.3 网关节点设备安全

工业蜂窝网络网关节点设备应满足如下要求：

a） 网关节点设备应具备对合法连接设备进行标识和鉴别的能力；

b） 网关节点设备应具备过滤非法节点和伪造节点所发送的数据的能力；

c） 授权用户应能够在设备使用过程中对关键密钥进行在线更新；

d） 授权用户应能够在设备使用过程中对关键配置参数进行在线更新。

9.4 抗数据重放

工业蜂窝网络终端节点设备抗数据重放应满足如下要求：

a） 终端节点设备应能够鉴别数据的时效性，避免历史数据的重放攻击；

b） 终端节点设备应能够鉴别对历史数据的非法修改，避免数据的修改重放攻击。

9.5 边缘计算

边缘计算节点的设计、开发和应用应满足GB/T 41780.1-2022中的要求。

10 建设运维安全

10.1 产品采购和使用

工业控制系统重要设备应通过专业机构的安全性检测后方可采购使用。

10.2 外包软件开发

应在外包开发合同中规定针对开发单位、供应商的约束条款，包括设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专业等方面的内容。

10.3 运维

运维应满足如下要求：

a） 应指定人员定期巡视终端节点设备、网关节点设备的部署环境，对可能影响终端节点设备、网关节点设备正常工作的环境异常进行记录和推护；

b） 应对终端节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理；

c） 应加强对终端节点设备、网关节点设备部署的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。

附 录 A

（资料性）

工业蜂窝网络通用要求

A.1 蜂窝网络要求

工业蜂窝网络需满足蜂窝网络通信行业标准规定的蜂窝网络通信功能要求。

A.2 组网要求

工业蜂窝网络组网应满足如下要求：

a） 应支持按需采用公共网络或非公共网络；

b） 应支持IP地址分配，宜支持IPv4和IPv6双栈；

c） 按需支持冗余组网；

d） 宜支持工业蜂窝网络和工业应用系统之间的安全防护措施。

A.3 接入认证

工业蜂窝网络接入认证应满足如下要求：

a） 应支持蜂窝终端设备的接入认证；

b） 宜支持蜂窝终端设备的二次接入认证。

A.4 信息安全要求

工业蜂窝网络应用场景应按照工业网络信息安全的规定。

A.5 服务分级要求

工业蜂窝网络服务分级应满足如下要求：

a） 应支持将工业应用映射为相应的服务等级；

b） 应支持提供满足SLA的分级网络。

A.6 定位要求

工业蜂窝网络应支持蜂窝终端设备的定位，可提供不同精度要求的位置信息。

A.7 传输要求

工业蜂窝网络传输应满足如下要求：

a） 应支持确定性传输的能力；

b） 应支持时间同步的能力；

c） 应满足工业应用对通信的可用性要求；

d） 应支持为通信双方的多个业务设置不同的传输优先级，支持按优先级进行通信；

e） 应保障蜂窝终端设备移动过程中的工业应用需求。

A.8 蜂窝网络设备的管理要求

蜂窝网络设备的管理应满足如下要求：

a） 应支持对蜂窝网络设备的操作和管理功能，可对工业蜂窝网络功能进行使能、禁用、配置、监控和故障排除；

b） 应支持对工业蜂窝网络的实时监控功能，包括关键应用的 QoS、蜂窝网络设备的通信和连接状态及一般服务可用性等；

c） 应支持和工业网络管理系统的对接，宜支持工业网络的故障告警、拓扑生成及设备管理等。

A.9 性能指标

A.9.1 时延

时延应指示将报文从一个终端设备的应用层（源）实时交付到另一个终端设备应用层（目的地）所需的时间。

对于以下两种情况，应规定最大时延，最大时延的计算应包括传输时间以及任何等待时间：

——无传输错误；

——帧丢失并恢复。

A.9.2 支持最大蜂窝终端设备数量

在工业应用的实时性要求情况下，可支持最大蜂窝终端设备的数量。

A.9.3 吞吐量

蜂窝终端设备应用层传输的吞吐量（单位：字节/秒）。

A.9.4 非实时带宽

带宽的百分比，可用于一个链路上的非实时性无线通信。此外，还应规定总链路带宽。

A.9.5 时间同步精度

任意两个终端设备时钟之间的最大偏差。

A.9.6 非基于时间的同步精度

任意两个终端设备循环行为的最大抖动，通过周期性事件的触发来建立循环行为。

A.9.7 故障恢复时间

单个故障的情况下，从故障出现到完全恢复的最长时间。

A.10 工业蜂窝网络访问子层要求

工业应用和工业蜂窝网络应通过工业蜂窝网络访问子层对接。工业蜂窝网络访问子层应实现工业应用在工业蜂窝网络上的透明的数据传输，见图 A.1。

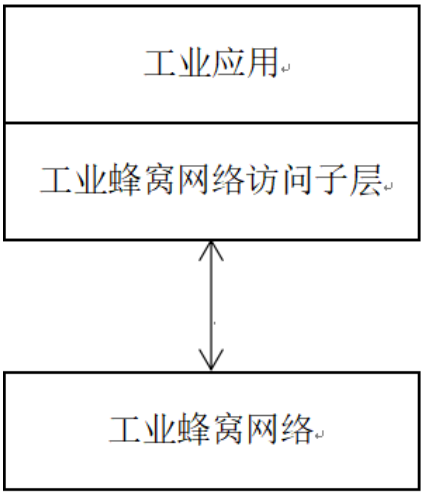

图 A.1 工业蜂窝网络访问子层示意图

工业蜂窝网络访问子层应具备满足下列工业应用需求的能力：

——应支持获取工业应用的需求，工业应用需求包括但不限于收发工业蜂窝终端设备标识、通信关系、发送周期、数据包大小、时延、时间同步精度、生存时间和传输可用性；

——宜支持工业蜂窝网络与工业应用进行需求的协商；

——宜支持将工业应用的需求发送给工业蜂窝网络；或工业蜂窝网络访问子层宜支持将工业应用的需求映射为工业蜂窝网络的 QoS 参数，并发送给工业蜂窝网络。

附 录 B

（资料性）

5G 蜂窝网络安全要求

B.1 接入安全

5G蜂窝网络接入应满足如下安全要求：

a） 应采用终端接入认证、终端访问控制和安全数据传输设计；

b） 应采用多重接入认证、切片认证、数据网络认证、信息加密方式；

c） 应针对不同业务，灵活配置不同级别的认证策略或策略组合；

d） 针对安全等级高的工业系统提供定制化的服务过程，应采用切片二次认证机制；

e） 应提供多种访问控制方式，以避免不可靠来源访问；

f） 应对关键敏感数据采用加密算法进行加密存储。

B.2 5GC 安全

5GC应满足如下安全要求：

a） 应针对 5GC 功能虚拟化特点，划分不同的安全等级，并设置不同的安全域；

b） 每个安全域应分配专用的硬件资源池；

c） 域间访问应通过虚拟安全设备做防护；

d） 域内应根据网元种类、归属地区等划分子域；

e） 安全资源池应提供防火墙、虚拟专用网络、web 应用防护系统以及入侵防御系统等安全服务，并进行 MANO 统一编排。

B.3 MEC 安全 5G

MEC安全5G应满足如下要求：

a） 应满足 5G 业务本地化、差异化、低延时的要求；

b） 应根据 MEC 自身业务特点，从物理安全、基础设施安全、系统及平台安全、业务及数据安全、管理与运维安全等端到端的安全解决方案，构建“放心”的边缘计算平台；

c） 应采用安全隔离手段；

d） 应参考虚拟层安全要求和容器安全要求，采用安全措施实现虚拟 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间的隔离；

e） 应保证平台镜像仓库具有完整性、机密性和访问控制的安全保护。

B.4 切片安全

切片安全应满足如下要求：

a） 应建立在共享资源之上的虚拟化专用网络；

b） 应提供传统移动网络安全机制；

c） 应提供网络切片之间端到端安全隔离机制，包括端到端切片隔离、切片与用户间安全隔离、切片与 DN 间安全隔离；

d） 针对面向无线频谱资源以及基站处理资源应采用 RAN 侧隔离；

e） 最高安全等级的工业控制类切片应采用独立的基站或者频谱独享；

f） 应通过软隔离、硬隔离和 QoS 资源保障等多种方案，实现网络切片在承载侧的隔离；

g） 应采用多重隔离机制，实现核心网侧的隔离。

B.5 服务安全要求

B.5.1 一般要求

蜂窝通信系统应满足如下安全要求：

a） 蜂窝通信系统应支持存储缓存数据的安全机制；

b） 蜂窝通信系统应支持接入内容缓存应用程序的安全机制；

c） 蜂窝通信系统应支持接入服务或运营商服务托管环境中的应用程序的安全机制；

d） 蜂窝通信系统应支持接入独立安全框架；

e） 蜂窝通信系统应支持运营商授权其他 PLMN 的用户接收临时服务的机制；

f） 蜂窝通信系统应能够为没有接入到其本地网络的授权用户提供临时服务；

g） 根据第三方与网络运营商之间的协议，蜂窝通信系统应允许运营商授权第三方创建，修改和删除网络片；

h） 蜂窝通信系统应支持一种安全机制，以保护中继数据不被中继 UE 拦截；

i） 根据 HPLMN 政策及其服务和运营需求，任何能够使用接入 EPS 而不是蜂窝网络 USIM 的 USIM 可用于根据用户的用户在 5G 蜂窝系统中对接入支持的服务进行身份验证；

j） 蜂窝通信系统应为使用蜂窝网络 LAN 类型服务的授权 UE 之间的通信提供完整性和机密性保护；

k） 蜂窝网络 LAN-VN 应能够验证请求加入特定私人通信的 UE 的身份；

l） 蜂窝通信系统应提供合适的 API，以允许在私有片服务的任何 UE 与该私有片中的核心网络实体之间使用受信任的第三方提供的加密。

B.5.2 认证要求

蜂窝通信系统认证应满足如下要求：

a） 蜂窝网络应支持用于认证 IoT 设备组的资源有效机制；

b） 蜂窝通信系统应支持向 IoT 设备验证用户的有效手段；

c） 蜂窝通信系统应能够使用 3GPP 凭证支持非 3GPP 接入技术的认证；

d） 对于隔离部署方案中的物联网设备，蜂窝通信系统应支持运营商控制的替代认证方法（即，替代 AKA），其具有用于网络接入的不同类型的凭证；

e） 蜂窝通信系统应支持合适的框架，允许具有非 3GPP 身份和凭证的替代认证方法用于非公共网络中的 UE 网络接入认证；

f） 根据移动网络运营商与第三方之间的协议，蜂窝通信系统应支持 PLMN 对托管的非公共网络和与托管的 PLMN 相关联的私有片的接入进行认证和授权的机制；

g） 蜂窝网络应支持 3GPP 支持的机制，以对蜂窝网络 LAN-VN 接入的传统非 3GPP 设备进行身份验证。

B.5.3 授权要求

蜂窝通信系统授权应满足如下要求：

a） 蜂窝通信系统应允许运营商授权物联网设备使用仅限于物联网设备的一个或多个蜂窝通信系统功能；

b） 蜂窝通信系统应允许运营商授权/取消授权 UE 使用蜂窝网络 LAN 类型的服务；

c） 基于运营商策略，在使用非 3GPP 接入技术建立直接设备连接之前，IoT 设备可以使用 3GPP 凭证来确定它们是否被授权参与直接设备连接；

d） 根据运营商政策，蜂窝通信系统应提供一种方法来验证 UE 是否被授权为特定服务使用优先级网络接入。

B.5.4 身份管理要求

蜂窝通信系统身份管理应满足如下要求：

a） 蜂窝通信系统应为运营商提供一种机制，允许 UE 使用隐藏其用户身份的临时标识符来进行接入；

b） 蜂窝通信系统应为运营商提供一种机制，允许接入来自使用隐藏其用户身份的临时标识符在间接网络连接中连接的 UE；

c） HPLMN 应能够将临时标识符与 UE 的用户标识相关联；

d） 蜂窝通信系统应能够保护用户身份和其他用户识别信息免受被动攻击；

e） 根据地区或国家监管要求，蜂窝通信系统应能够保护用户身份和其他用户识别信息免受主动攻击；

f） 在需要时，无论 UE 的用户界面如何，蜂窝通信系统都应允许合法实体收集设备标识符；

g） 蜂窝通信系统应能够独立于设备识别而支持识别用户；

h） 蜂窝通信系统应支持收集系统信息的安全机制，同时保障最终用户和应用程序隐私安全；

i） 根据地区或国家监管要求，蜂窝通信系统应能够提供蜂窝网络定位服务，同时保护 UE 用户或所有者的隐私，包括尊重 UE 用户对定位服务的同意；

j） 对于使用蜂窝网络技术的专用网络，蜂窝通信系统应使用由第三方提供和管理并由 3GPP 支持的身份、凭证和身份验证方法来支持网络接入。

B.5.5 监管要求

蜂窝通信系统监管应满足如下要求：

a） 蜂窝通信系统应支持所有支持的接入网络的区域或国家监管要求；

b） 蜂窝通信系统应支持合法拦截，但须符合地区或国家监管要求；

c） 连接到多个国家的蜂窝核心网络的通信卫星接入网络应能够满足这些国家的相应监管要求；

d） 蜂窝通信系统应支持蜂窝网络LAN类型服务的监管要求。

B.5.6 欺诈保护要求

蜂窝通信系统欺诈保护应满足如下要求：

a） 根据地区或国家监管要求，蜂窝通信系统应支持一种安全机制，允许授权实体禁止报告为被盗的 UE 的正常运行；

b） 根据地区或国家监管要求，蜂窝通信系统应支持一种安全机制，允许授权实体将恢复的被盗 UE 重新启用至正常运行；

c） 蜂窝通信系统应能够保护用户位置信息免受被动攻击；

d） 根据地区或国家监管要求，蜂窝通信系统应能够保护用户位置信息免受主动攻击；

e） 根据地区或国家监管要求，蜂窝通信系统应支持保护用户位置信息和用户定位相关数据的生成以防止篡改和欺骗的机制；

f） 根据地区或国家监管要求，蜂窝通信系统应支持检测用户位置信息和用户位置相关数据生成的

篡改和欺骗尝试的机制。

B.5.7 资源效率安全要求

蜂窝通信系统资源效率应满足如下要求：

a） 蜂窝通信系统应在不影响3GPP系统安全级别的情况下最小化安全信令开销；

b） 蜂窝通信系统应支持有效的安全机制，将相同的数据发送到多个UE。

B.5.8 数据安全和隐私要求

蜂窝通信系统数据安全和隐私应满足如下要求：

a） 蜂窝通信系统应支持为URLLC和能量受限设备提供服务的数据完整性和机密性保护方法；

b） 蜂窝通信系统应支持一种机制来验证消息的完整性以及消息发送者的真实性；

c） 蜂窝通信系统应支持在请求的端到端延迟内对URLLC服务进行加密。

B.6 端到端核心网络安全要求

B.6.1 通用要求

端到端核心网络应满足如下要求：

a) 解决方案应支持应用层机制，用于由中间节点添加、删除和修改消息元素，本文件中描述的特定消息元素除外；

注：这种情况的典型例子是 IPX 运营商修改消息以用于路由目的。

b) 解决方案应为源和目的网络之间特定消息元素提供端到端机密性和/或完整性保护；在源 PLMN 和目的 PLMN 的两个 SEPP 之间提供消息元素的机密性和/或完整性保护；

c) 目的网络应能够确定发送由前一个项目保护的特定消息元素的源网络的真实性；为满足此要求，目的网络中专用于处理端到端核心网互连安全的 SEPP 应能确定源网络的真实性；

d) 该解决方案应该对 3GPP 定义的网络元素产生最小的影响；

e) 解决方案应使用标准的安全协议；

f) 解决方案应涵盖用于漫游目的的接口；

g) 解决方案应考虑性能和开销因素；

h) 解决方案应包括抗重放攻击保护；

i) 解决方案应包括算法协商和防降级攻击；

j) 解决方案应考虑密钥管理的操作方面。

B.6.2 数据传输安全

端到端核心网络数据传输应满足如下安全要求：

a） 应采用 5G 网络的加密算法，以保护数据传输的机密性；

b） 应建立 TLS 安全传输通道，对需要保护的信息进行机密性和完整性保护，有效防止数据在网间传输时被篡改或窃听；

c） 应提供工业互联网中的数据产生、处理、使用等环节的安全保护；

d） 应采用基于会话的加密机制，按需配置加密算法与密钥强度。

B.7 UE 安全要求

应满足 3GPP TS 33.501 中 5.2 中的要求。

B.8 gNB 安全要求

应满足 3GPP TS 33.501 中 5.3 中的要求。

B.9 ng-eNB 安全要求

应满足 3GPP TS 33.501 中 5.4 中的要求。

B.10 AMF 安全要求

应满足 3GPP TS 33.501 中 5.5 中的要求。

B.11 SEAF 安全要求

应满足 3GPP TS 33.501 中 5.6 中的要求。

B.12 UDM 安全要求

应满足 3GPP TS 33.501 中 5.8 中的要求。

B.13 AUSF 安全要求

应满足 3GPP TS 33.501 中 5.8a 中的要求。

B.14 核心网络安全要求

应满足 3GPP TS 33.501 中 5.9 中的要求。

B.15 算法安全要求

应满足 3GPP TS 33.501 中 5.11 中的要求。

参 考 文 献

[1] GB/T 22239-2019 网络安全技术 网络安全等级保护基本要求

[2] GB/T 51278-2018 数字蜂窝移动通信网 LTE 工程技术标准

[3] GB/T 25068.1-2020 信息技术 安全技术 网络安全 第 1 部分：综述和概念

[4] GB/T 25068.2-2020 信息技术 安全技术 网络安全 第 2 部分：网络安全设计和实现指南

[5] GB/T 37934-2019 信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求

[6] GB/T 37955-2019 信息安全技术 数控网络安全技术要求

[7] GB/T 38318-2019 电力监控系统网络安全评估指南

[8] GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

[9] YD/T 3615-2019 5G 移动通信网 核心网总体技术要求

[10] YD/T 3628-2019 5G 移动通信网 安全技术要求

[11] YD/T 5263-2021 数字蜂窝移动通信网 5G 核心网工程技术规范

[12] YD/T 5264-2021 数字蜂窝移动通信网 5G 无线网工程技术规范