ICS 35.030
CCS L 80

DB65

新 疆 维 吾 尔 自 治 区 地 方 标 准

DB65/T 4728—2023

基于5G网络的电力业务系统安全防护评估规范

Evaluation specification for security protection of power business system based on 5G network

2023－XX－XX 发布　　2023－XX－XX 实施

新疆维吾尔自治区市场监督管理局　　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。

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。

本文件由国网新疆电力有限公司电力科学研究院提出。

本文件由新疆维吾尔自治区工业和信息化厅归口并组织实施。

本文件起草单位：国网新疆电力有限公司电力科学研究院、国网智能电网研究院有限公司、国网新疆电力有限公司、中国信息通信研究院、国网山东省电力公司电力科学研究院、国网新疆电力有限公司乌鲁木齐供电公司、国网新疆电力有限公司经济技术研究院、中国计量大学、国网福建省电力有限公司电力科学研究院、国网新疆电力有限公司信息通信公司、国网新疆电力有限公司喀什供电公司、国网新疆电力有限公司超高压分公司、国网新疆电力有限公司塔城供电公司、国网新疆电力有限公司巴州供电公司。

本文件主要起草人：邹振婉、张小建、李峰、冯泽冰、周文婷、陈涛、王齐、陈佳、王晓斌、刘冬兰、张建业、何碧舟、韩文婷、杨慧婷、王斌、樊树铭、王睿、费稼轩、黄秀丽、宋新甫、艾红、罗凤英、董文娟、马瑞龙、王宇晨、王昱洁、朱雪琴、陈莉佳、李明轩、张笑宇、高明、张昊、张朋越、张静、何金栋、郭江涛、王楷、李浩升、罗成、罗政邦、侯英洒、景佳佳、郭庆瑞、郭学让、何玲、马林、张强、叶波、黎玉娥、张庭祎、杨帆。

本文实施应用中的疑问，请咨询国网新疆电力有限公司电力科学研究院。

对本文件的修改意见建议，请反馈至新疆维吾尔自治区工业和信息化厅（乌鲁木齐市沙依巴克区友好南路179号）、国网新疆电力有限公司电力科学研究院（乌鲁木齐市高新技术产业开发区（新市区）恒达街200号）、新疆维吾尔自治区市场监督管理局（乌鲁木齐市天山区新华南路167号）。

新疆维吾尔自治区工业和信息化厅 联系电话：0991-4536153；传真：0991-4536153；邮编：830000

国网新疆电力有限公司电力科学研究院 联系电话:0991-2918563；传真：0991-2918015；邮编：830011

新疆维吾尔自治区市场监督管理局 联系电话：0991-2818750；传真：0991-2311250；邮编：830004

基于5G网络的电力业务系统安全防护评估规范

1 范围

本文件规定了基于5G网络的电力业务系统安全防护评估工作的总体要求、基本安全防护评估内容和增强安全防护评估内容。

本文件适用于自治区电力企业对基于5G网络的电力业务系统组织开展的安全防护评估工作。

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 20272—2019 信息安全技术 操作系统安全技术要求

DL/T 1757—2017 电子数据恢复和销毁技术要求

YD/T 3628—2019 5G移动通信网 安全技术要求

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

3 术语和定义

下列术语和定义适用于本文件。

3.1

自评估 self-assessment

由运行单位自身发起，依据国家有关法规与标准，对基于5G网络的电力业务系统及其安全管理组织实施的网络安全防护评估活动。

[来源：GB/T 20984,3.1.8,有修改]

3.2

检查评估 inspection assessment

由被评估单位的业务主管部门发起，依据国家有关法规与标准，对基于5G网络的电力业务系统及其安全管理组织实施的具有强制性的网络安全防护评估活动。

[来源：GB/T 20984,3.1.9,有修改]

3.3

上线安全评估 online implementation security assessment

基于5G网络的电力业务系统投运前及发生重大变更时，运行单位自行组织或委托评估机构对系统进行的安全评估。

注：重大变更包括，但不限于：

a） 增加新的应用或应用发生较大变更；

b） 网络结构和连接状况发生较大变更；

c） 技术平台大规模更新；

d） 系统扩容或改造；

e） 系统运行维护管理机构或人员发生较大规模调整。

［来源：GB/T 38318，3.3,有修改］

3.4

5G电力虚拟专网　power virtual private network of 5G

在电信运营商的5G网络中，基于网络切片、MEC、能力开放等技术，在接入、承载、核心网等环节虚拟出一张面向电力行业的专用网络，并与电力通信专网跨域融合，实现端到端的电力业务承载、高强度安全隔离以及资源管理。

3.5

终端　terminal

对电源、电网、负荷等的数据采集、数据处理及控制的装置，可集成内置通信模块或连接外置通信模块。

3.6

通信模块　communication module

将基带、射频、存储、电源管理等硬件进行封装，采用标准数据接口并嵌入在终端（或微型纵向加密装置）内部，对外提供网络连接功能的装置。

3.7

网络切片　network slice

提供特定网络能力和网络特征（如资源隔离、SLA保障特性等）、为客户提供多种业务属性的逻辑网络。依照资源隔离强度高低，网络切片可分为硬切片和软切片两种类型。

3.8

机卡绑定　equipment and SIM card bond

终端5G SIM卡与终端设备绑定，即某个SIM卡只允许在特定的终端设备上使用，在其他终端设备上不可用。

3.9

完整性保护　integrity protection

通过哈希算法形成需要传输数据的摘要，以在接收端实现鉴别传输数据是否被篡改等功能。

3.10

二次认证　secondary authentication

在通信模块初始化注册时的主认证之后、建立会话之前，通过电力专用认证服务器进行的辅助认证。

4　缩略语

下列缩略语适用于本文件。

128-NEA1：基于128位SNOW 3G加密算法（128-NR Encryption Algorithm 1）

128-NEA2：基于128位AES加密算法（128-NR Encryption Algorithm 2）

128-NEA3：基于128位ZUC加密算法（128-NR Encryption Algorithm 3）

128-NIA1：基于128位SNOW 3G完整性算法（128-NR Integrity Algorithm 1）

128-NIA2：基于128位AES完整性算法（128-NR Integrity Algorithm 2）

128-NIA3：基于128位ZUC完整性算法（128-NR Integrity Algorithm 3）

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

5G：第五代移动通信技术（5th Generation Mobile Networks）

5QI：5G QoS标识符（5G QoS Identifier）

AS：接入层（Access Stratum）

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

DNN：数据网络名称（Data Network Name）
eSIM：嵌入式SIM卡（Embedded-SIM）
FlexE：灵活以太网（Flex Ethernet）
HTTP2.0：超文本传输协议2.0（HyperText Transfer Protocol 2.0）
IP：网际互连协议（Internet Protocol）
IPSec：互联网安全协议（Internet Protocol Security）
L3VPN：第三层虚拟专用网络（Level3 Virtual Private Network）
MANO：管理和编排（Management and Orchestration）
MEC：多接入边缘计算（Multi-access Edge Computing）
N1：N1接口（N1 Interface）
N2：N2接口（N2 Interface）
N3：N3接口（N3 Interface）
N4：N4接口（N4 Interface）
NAS：非接入层（Non Access Stratum）
NF：噪声系数（Noise Figure）
PMU：电源管理单元（Power Management Unit）
RB：资源块（Resource Block）
RRC：无线资源控制（Radio Resource Control）
SDN：软件定义网络（Software Defined Network）
SIM：用户身份识别卡（Subscriber Identity Module）
SNMP：简单网络管理协议（Simple Network Management Protocol ）
SR：分段路由（Segment Routing）
SSL：安全套接层协议（Secure Socket Layer）
TLS：传输层安全（Transport Layer Security）
UDM：统一数据管理功能（Unified Data Management）
UPF：用户面功能（User Plane Function）
USIM：全球用户识别卡（Universal Subscriber Identity Module）
Uu：Uu接口（Uu Interface）
vCPU：虚拟处理器（Virtual Central Processing Unit）
VNF：虚拟网络功能（Virtual Network Feature）
VLAN：虚拟局域网（Virtual Local Area Network）
VPN：虚拟专用网络（Virtual Private Network）

5 总体要求

5.1 评估分级

基于5G网络的电力业务系统安全防护评估分为基本安全防护评估和增强安全防护评估。基本安全防护评估适用于5G无线公网承载的电力业务，增强安全防护评估适用于5G电力虚拟专网承载的电力业务，典型安全防护评估业务系统见附录A。

5.2 评估内容

基于5G网络的电力业务系统安全防护评估包括终端安全防护评估、网络安全防护评估、数据安全防护评估、业务系统安全防护评估和管理安全防护评估。基于5G网络的电力业务系统安全防护评估表见附录B。

5.3 评估要求

5.3.1 评估时间

基于5G网络的电力业务系统的安全防护评估工作应常态化、定期进行。系统的规划、设计阶段应进行安全审查，实施、运行维护和废弃阶段应进行安全评估，各阶段结合本阶段的实际情况开展安全防护评估工作。

5.3.2 评估角色和职责

5.3.2.1 运行单位

负责发起本单位的自评估工作，参加评估方案等文档的评审工作，配合检查评估实施工作，并根据安全防护评估结果开展问题整改。系统投运前及发生重大变更实施上线安全评估时，运行单位总体负责相关工作，可委托评估机构进行评估。

5.3.2.2 业务主管部门

负责组织开展管辖范围内的检查评估，根据安全防护评估结果督促运行单位整改。

5.3.2.3 系统供应商

负责配合完成系统上线安全评估，在运行维护阶段支持、配合安全防护评估工作，配合执行安全防护评估整改工作。

5.3.2.4 评估机构

负责编制安全防护评估实施方案，自行组织评审评估实施方案，实施安全防护评估，出具安全防护评估报告，提出整改建议。

宜选择国家或行业有丰富经验的稳定、可靠、可控的评估机构。

5.3.3 评估形式

5.3.3.1 自评估

运行单位对本单位的基于5G网络的电力业务系统定期组织开展自评估。

5.3.3.2 检查评估

业务主管部门根据实际情况对各运行单位的基于 5G 网络的电力业务系统组织开展检查评估。

5.3.3.3 上线安全评估

基于 5G 网络的电力业务系统投运前或发生重大变更时，由运行单位委托评估机构进行上线安全评估。

5.3.4 评估结果分析方法

评估结果分析是总结被评估系统整体安全防护能力的综合评价活动，根据评估结果，定位整个系统的安全防护现状与安全要求之间的差距，并分析这些差距导致被评估系统存在的安全问题，从而给出评估结论和安全建议，形成评估报告，按照附录C的定量或定性分析方法，给出分析结果。

5.4 评估流程

基于5G网络的电力业务系统安全防护评估流程分为启动准备、现场实施、安全分析三个阶段。基于5G网络的电力业务系统安全防护评估流程见图1。

图 1 基于 5G 网络的电力业务系统安全防护评估流程

5.5 评估方法

5.5.1 文档检查

检查被评估单位提交的有关文档（如系统配置文档、安全防护方案、自评估报告等）是否符合相关标准和要求。

5.5.2 人工核查

根据评估方案和评估指导书，核查各项安全功能和防护能力是否与提交文档一致，是否符合相关标准和要求。

5.5.3 工具检查

根据评估方案，在被评估单位授权的前提下，选择适用的评估工具实施评估，如网络评估工具、主机评估工具、资产识别工具等。

5.6 评估注意事项

5.6.1 保密管理

应对评估资料和评估结果做好保密工作，可采取签订保密协议、最小接触原则、职业道德评估、人员保密管理、设备保密管理、文档保密管理等控制措施，明确问责和追责等处理办法，保证评估过程中产生、接触的所有记录、数据评估结果的安全、保密。

5.6.2 风险控制

应对评估过程进行风险控制，可采取严格的申请和监护、操作时间控制、制定应急预案、搭建运行系统模拟环境、关键业务系统采用人工评估、评估人员选取、评估现场安全培训等风险控制手段，防止评估过程中引入的风险。

6 基本安全防护评估内容

6.1 终端安全

防护评估内容应包括：

a) 是否采用机卡绑定、SIM 卡防拔插或 eSIM 卡等物理安全保障措施；
b) SIM 卡是否被分配固定 IP 地址，不同切片的终端 SIM 卡间是否禁止相互访问；
c) 通信模块是否能够根据签约的 5G 网络切片信息在网络注册时进行切片选择；
d) 通信模块是否支持 YD/T 3628—2019、3GPP TS 33.501 等标准中要求的机密性和完整性保护算法，如：128-NEA1、128-NEA2、128-NEA3、128-NIA1、128-NIA2 和 128-NIA3；
e) 退役时是否删除配置参数及证书，解绑 SIM 卡并回收。

6.2 网络安全

6.2.1 接入网安全

防护评估内容应包括：

a) 终端 SIM 卡是否仅允许接入一个 DNN 网络；
b) 基站是否具备防 DDos 攻击措施；
c) N1、N2、Uu 接口是否具备机密性保护、完整性保护和抗重放保护机制；
d) 空口 5QI 等级和业务签约参数是否一致；
e) 空口 AS 信令是否支持对 RRC 信令进行机密性和完整性保护，是否支持机密性保护和完整性保护算法优先级配置，且完整性保护算法配置不能为 NIA0；
f) 空口 NAS 信令是否支持对 NAS 信令进行机密性和完整性保护，是否支持机密性保护和完整性保护算法优先级配置，且完整性保护算法配置不能为 NIA0。

6.2.2 承载网安全

防护评估内容应包括：

a) 是否支持 VLAN 方式实现软隔离，VLAN 标签是否能够与网络切片标识进行映射；
b) 网络切片是否支持通过不同的 VPN 通道，实现电力业务与非电力业务的隔离。

6.2.3 核心网安全

防护评估内容应包括：

a) 是否建立切片隔离管理机制，是否支持多种隔离手段，是否支持端到端切片隔离和网络分段管理；
b) NF 间服务化接口是否支持 3GPP 标准要求的 HTTP2.0 协议及参数配置；
c) 切片管理接口、切片内部网元是否支持双向身份认证和访问控制机制；
d) 是否具备过载保护功能，是否设置最大连接限制；
e) 和基站之间是否建立双向鉴权机制，以鉴别基站或者核心网是否为伪造网元；
f) MEC 平台是否部署抗 DDos 攻击、入侵检测等措施；
g) MEC 平台是否关闭不必要的端口和服务，是否存在安全漏洞；
h) MEC 平台是否划分不同的安全域并部署域间安全隔离措施，包括物理隔离、虚拟机隔离、网元隔离、网络隔离、数据隔离、流量隔离等；
i) UPF 所在机房是否部署物理防护措施；
j) UPF 与核心网通信接口是否支持双向认证、传输加密机制；
k) UPF 与 MEC 平台等应用平台间是否部署安全隔离和访问控制措施。

6.3 数据安全

防护评估内容应包括：

a) 针对 5G 虚拟化设施，MANO 中的证书、私钥、VNF 访问口令、SNMP 口令等敏感数据是否部署相应数据保护措施，SDN 控制器是否对口令、私钥、流表、策略等敏感数据部署相应的数据保护措施；
b) 虚拟机在迁移或弹性扩缩过程中，是否能实现其存储数据的有效销毁，确保数据不可恢复和防止滥用误用，是否对数据销毁操作过程进行日志记录以支持安全审计；
c) 不同虚拟机之间共享同一存储资源时，是否进行数据隔离，确保虚拟机不能直接或间接访问其它虚拟机的数据；
d) 在 MANO 各实体间、以及 SDN 控制器南向和北向接口等进行数据传输时，是否采用传输通道或数据加密模式，如采用 TLS/SSL 协议进行数据加密传输，或建立 VPN 加密传输通道方式进行行安全传输；
e) 5G 核心网（如 UDM）存储、处理的个人数据是否依据数据最小化原则，采用访问控制、匿名化、加密保护以及用户许可等技术手段对个人敏感信息的请求、存储、传输、使用等操作进行隐私保护；
f) 核心网与外部业务系统之间存在的网络开放接口，是否采用双向认证、数据传输加密和完整性校验、数据安全日志审计等措施；
g) MEC 平台与 APP 之间是否建立访问控制及数据传输安全机制，如机密性、完整性保护及防重放攻击机制等；
h) MEC 平台的安全域和非安全域之间或不同安全域之间进行互联访问、数据流转时，是否在安全边界进行访问控制，是否采用接入鉴权、接入策略设置等手段；
i) 存储于互联网大区的企业重要数据是否遵循最小化原则，是否加密。

6.4 业务系统安全

防护评估内容应包括：

a) 与终端间是否部署安全接入网关，实现加密传输和双向认证；

b) 是否通过具备国家检测资质的第三方权威机构的安全检测，是否具备检测报告；
c) 操作系统、数据库、中间件等基础软件，是否满足 GB/T 20272—2019 中 6.3 和 6.4 的要求，身份鉴别、访问控制、安全审计等安全功能和策略是否已启用并配置合理；
d) 操作系统及数据库是否遵循最小安装的原则，仅安装必要的组件和应用程序，并及时更新系统补丁；
e) 操作系统及数据库是否定期开展安全漏洞扫描和加固；
f) 操作系统是否定期更新防病毒软件和恶意代码库；
g) 数据库是否按照最小权限原则，仅授予管理用户所需的最小权限；
h) 是否部署网络安全监视措施，实现主机设备、网络设备、安全设备等的信息采集、安全审计、实时监视告警等功能。

6.5 管理安全

防护评估内容应包括：
a) 运行单位是否对业务系统制定日常运维和安全防护的相关管理制度、操作规程等管理措施，并依照执行，定期修订；
b) 运行单位是否对业务系统制定安全防护方案，并指定相关系统、设备接入技术方案，安全防护措施是否有效；
c) 运行单位是否定期开展业务系统安全防护自评估工作，实现隐患排查整改闭环；
d) 运行单位是否对业务系统配备安全管理员、系统管理员和安全审计员，是否明确岗位职责、分工和技能要求；
e) 运行单位是否与安全管理员、系统管理员和安全审计员等关键岗位人员签署保密协议；
f) 运行单位是否取消离岗人员相关系统访问权限、回收软硬件设备；
g) 运行单位是否对业务系统制定厂家维护、评估检测等第三方人员访问管理制度或相关规范。

7 增强安全防护评估内容

7.1 终端安全

防护评估内容应包括6.1及以下：
a) 是否部署支持国密通用算法或电力专用算法的安全模块，实现身份认证和数据加解密；
b) 退运的安全模块是否进行物理销毁；
c) 涉控终端是否部署可信验证模块，在系统引导、操作系统加载、应用程序加载等阶段进行静态度量和校验；
d) 是否禁止同时连接 5G 电力虚拟专网和其他公共网络。

7.2 网络安全

7.2.1 接入网安全

防护评估内容应包括6.2.1及以下：
a) 空口是否选择和业务系统安全等级相适应的 RB 资源预留方式；
b) 基站是否通过 5QI 保障切片内不同业务承载的优先级。

7.2.2 承载网安全

防护评估内容应包括6.2.2及以下：

a) 是否支持 FlexE 等，是否提供通道隔离和多端口绑定功能，实现硬切片隔离；
b) 是否支持 SR 和 L3VPN，实现硬切片内不同电力业务的软切片隔离。

7.2.3 核心网安全

防护评估内容应包括6.2.3及以下：

a) 基站与核心网间的用户面接口（N3 口）是否采用加密认证、访问控制等技术措施，保障通信数据的机密性、完整性；
b) UPF 与核心网间的信令接口（N4 口）是否采用加密认证、访问控制等技术措施，保障通信控制信令的机密性、完整性；
c) 是否能够配合业务系统进行终端二次认证。

7.3 数据安全

防护评估内容应包括6.3及以下：

a) 终端在传输鉴别信息、电力敏感数据、控制数据等数据时是否进行加密保护；
b) 终端是否具备防审计记录非法读取、防恶意篡改、防恶意删除等数据安全保护措施；
c) MEC 平台是否支持动态身份标识、匿名化等技术削弱 MEC 平台计算节点标识和地理位置的映射关系，防止第三方根据 MEC 平台节点位置推断用户的地理位置；
d) MEC 平台是否具备对电力业务不同应用资源进行隔离的能力，防止应用越权访问其他应用数据，如 vCPU 调度安全隔离、内存资源安全隔离；
e) NFV/SDN 是否对数据传输安全策略变更进行审核和监控，是否对通道安全配置、密码算法配置、密钥管理等保护措施进行审核及监控；
f) 对于重点防护的调度中心、发电厂、变电站，是否设置经过国家指定部门检测认证的电力专用纵向加密认证装置或加密认证网关及相关设施；发电厂、变电站关键设备是否定期对数据进行备份，备份策略是否合理，是否按照策略执行备份操作；
g) 针对数据泄露、勒索攻击等数据安全威胁，业务系统是否部署数据分级分类、敏感数据加密、流量监测等措施；
h) 存储过企业重要数据的各类存储介质在报废、返厂维修、内部再利用等转作他用之前，是否采用符合 DL/T 1757—2017 规定的设备及方法对存储介质进行有效处理，并做记录。

7.4 业务系统安全

安全防护评估内容应包括6.4及以下：

a) 与终端间是否设置安全接入区；
b) 终端和安全接入区之间是否建立通信隧道，支持终端安全接入认证及通信加密；
c) 安全接入区内是否部署隔离装置，实现安全隔离；
d) 系统服务器、汇聚服务器以及安全接入区中的服务器是否部署安全自主可控操作系统；
e) 下发控制指令的系统服务器、汇聚服务器和安全接入区中的服务器是否部署可信验证模块，对系统引导程序、系统程序、应用程序和重要配置参数等进行可信验证；
f) 使用 5G 电力虚拟专网承载控制类业务时，是否采用具备安全认证机制的通信规约，是否使用加密机或加密卡等硬件加密设施进行加解密和签名验签运算，是否使用签名验签技术实现控制指令的完整性保护。

7.5 管理安全

增强防护评估内容应符合6.5的规定。

附 录 A
（资料性）
典型安全防护评估业务系统

A.1 典型基本安全防护评估业务系统参见表A.1,包括但不限于表A.1中所列业务系统。

表A.1 典型基本安全防护评估业务系统

序号	业务系统名称
1	电力市场交易
2	车联网
3	电子商务
4	移动办公

A.2 典型增强安全防护评估业务系统参见表A.2,包括但不限于表A.2中所列业务系统。

表A.2 典型增强安全防护评估业务系统

序号	业务系统名称
1	调度生产管理系统
2	用电信息采集系统
3	输变电状态监测系统
4	电能质量监测系统
5	无人机/机器人巡检
6	精准负荷控制
7	配电自动化系统
8	用电负荷需求侧响应
9	配网PMU
10	配网差动保护
11	光伏电站运行监控系统

附 录 B
（资料性）
基于 5G 网络的电力业务系统安全防护评估表

基于5G网络的电力业务系统基本安全防护评估表参见表B.1、增强安全防护评估表参见表B.2，运行单位或评估机构可根据实际需求在表B.1、表B.2的基础上删减评估内容。

表 B.1 基于 5G 网络的电力业务系统基本安全防护评估表

序号	评估类别		评估项	是否符合要求	问题描述
1	终端安全		是否采用机卡绑定、SIM 卡防拔插或 eSIM 卡等物理安全保障措施	是□ 否□	
2			SIM 卡是否被分配固定 IP 地址，不同切片的终端 SIM 卡间是否禁止相互访问	是□ 否□	
3			通信模块是否能够根据签约的 5G 网络切片信息在网络注册时进行切片选择	是□ 否□	
4			通信模块是否支持 YD/T 3628—2019、3GPP TS 33.501 等标准中要求的机密性和完整性保护算法，如：128-NEA1、128-NEA2、128-NEA3、128-NIA1、128-NIA2 和 128-NIA3	是□ 否□	
5			退役时是否删除配置参数及证书，解绑SIM卡并回收	是□ 否□	
6	网络安全	接入网安全	终端 SIM 卡是否仅允许接入一个 DNN 网络	是□ 否□	
7			基站是否具备防 DDos 攻击措施	是□ 否□	
8			N1、N2、Uu 接口是否具备机密性保护、完整性保护和抗重放保护机制	是□ 否□	
9			空口 5QI 等级和业务签约参数是否一致	是□ 否□	
10			空口 AS 信令是否支持对 RRC 信令进行机密性和完整性保护，是否支持机密性保护和完整性保护算法优先级配置，且完整性保护算法配置不能为 NIA0	是□ 否□	
11			空口NAS信令是否支持对NAS信令进行机密性和完整性保护，是否支持机密性保护和完整性保护算法优先级配置，且完整性保护算法配置不能为NIA0	是□ 否□	
12		承载网安全	是否支持 VLAN 方式实现软隔离，VLAN 标签是否能够与网络切片标识进行映射	是□ 否□	
13			网络切片是否支持通过不同的VPN通道，实现电力业务与非电力业务的隔离	是□ 否□	
14		核心网安全	是否建立切片隔离管理机制，是否支持多种隔离手段，是否支持端到端切片隔离和网络分段管理	是□ 否□	

表 B.1（续）

序号	评估类别		评估项	是否符合要求	问题描述
15	网络安全	核心网安全	NF 间服务化接口是否支持 3GPP 标准要求的 HTTP2.0 协议及参数配置	是□ 否□	
16			切片管理接口、切片内部网元是否支持双向身份认证和访问控制机制	是□ 否□	
17			是否具备过载保护功能，是否设置最大连接限制	是□ 否□	
18			和基站之间是否建立双向鉴权机制，以鉴别基站或者核心网是否为伪造网元	是□ 否□	
19			MEC 平台是否部署抗 DDos 攻击、入侵检测等措施	是□ 否□	
20			MEC 平台是否关闭不必要的端口和服务，是否存在安全漏洞	是□ 否□	
21			MEC 平台是否划分不同的安全域并部署域间安全隔离措施，包括物理隔离、虚拟机隔离、网元隔离、网络隔离、数据隔离、流量隔离等	是□ 否□	
22			UPF 所在机房是否部署物理防护措施	是□ 否□	
23			UPF 与核心网通信接口是否支持双向认证、传输加密机制	是□ 否□	
24			UPF 与 MEC 平台等应用平台间是否部署安全隔离和访问控制措施	是□ 否□	
25	数据安全		针对 5G 虚拟化设施，MANO 中的证书、私钥、VNF 访问口令、SNMP 口令等敏感数据是否部署相应数据保护措施，SDN 控制器是否对口令、私钥、流表、策略等敏感数据部署相应的数据保护措施	是□ 否□	
26			虚拟机在迁移或弹性扩缩过程中，是否能实现其存储数据的有效销毁，确保数据不可恢复和防止滥用误用，是否对数据销毁操作过程进行日志记录以支持安全审计	是□ 否□	
27			不同虚拟机之间共享同一存储资源时，是否进行数据隔离，确保虚拟机不能直接或间接访问其它虚拟机的数据	是□ 否□	
28			在 MANO 各实体间、以及 SDN 控制器南向和北向接口等进行数据传输时，是否采用传输通道或数据加密模式，如采用 TLS/SSL 协议进行数据加密传输，或建立 VPN 加密传输通道方式行安全传输	是□ 否□	

表 B.1（续）

序号	评估类别	评估项	是否符合要求	问题描述
29	数据安全	5G 核心网（如 UDM）存储、处理的个人数据是否依据数据最小化原则，采用访问控制、匿名化、加密保护以及用户许可等技术手段对个人敏感信息的请求、存储、传输、使用等操作进行隐私保护	是□ 否□	
30		核心网与外部业务系统间之间存在的网络开放接口，是否采用双向认证、数据传输加密和完整性校验、数据安全日志审计等措施	是□ 否□	
31		MEC平台与APP之间是否建立访问控制及数据传输安全机制，如机密性、完整性保护及防重放攻击机制等	是□ 否□	
32		MEC 平台的安全域和非安全域之间或不同安全域间进行互联访问、数据流转时，是否在安全边界进行访问控制，是否采用接入鉴权、接入策略设置等手段	是□ 否□	
33		存储于互联网大区的企业重要数据是否遵循最小化原则，是否加密	是□ 否□	
34	业务系统安全	与终端间是否部署安全接入网关，实现加密传输和双向认证	是□ 否□	
35		是否通过具备国家检测资质的第三方权威机构的安全检测，是否具备检测报告	是□ 否□	
36		操作系统、数据库、中间件等基础软件，是否满足 GB/T 20272—2019 中 6.3 和 6.4 的要求，身份鉴别、访问控制、安全审计等安全功能和策略是否已启用并配置合理	是□ 否□	
37		操作系统及数据库是否遵循最小安装的原则，仅安装必要的组件和应用程序，并及时更新系统补丁	是□ 否□	
38		操作系统及数据库是否定期开展安全漏洞扫描和加固	是□ 否□	
39		操作系统是否定期更新防病毒软件和恶意代码库	是□ 否□	
40		数据库是否按照最小权限原则，仅授予管理用户所需的最小权限	是□ 否□	
41		是否部署网络安全监视措施，实现主机设备、网络设备、安全设备等的信息采集、安全审计、实时监视告警等功能	是□ 否□	
42	管理安全	运行单位是否对业务系统制定日常运维和安全防护的相关管理制度、操作规程等管理措施，并依照执行，定期修订	是□ 否□	

表 B.1（续）

序号	评估类别	评估项	是否符合要求	问题描述
43	管理安全	运行单位是否对业务系统制定安全防护方案，并指定相关系统、设备接入技术方案，安全防护措施是否有效	是□ 否□	
44		运行单位是否定期开展业务系统安全防护自评估工作，实现隐患排查整改闭环	是□ 否□	
45		运行单位是否对业务系统配备安全管理员、系统管理员和安全审计员，是否明确岗位职责、分工和技能要求	是□ 否□	
46		运行单位是否与安全管理员、系统管理员和安全审计员等关键岗位人员签署保密协议	是□ 否□	
47		运行单位是否取消离岗人员相关系统访问权限、回收软硬件设备	是□ 否□	
48		运行单位是否对业务系统制定厂家维护、评估检测等第三方人员访问管理制度或相关规范	是□ 否□	

表 B.2 基于 5G 网络的电力业务系统增强安全防护评估表

序号	评估类别	评估项	是否符合要求	问题描述
1	终端安全	是否采用机卡绑定、SIM 卡防拔插或 eSIM 卡等物理安全保障措施	是□ 否□	
2		SIM 卡是否被分配固定 IP 地址，不同切片的终端 SIM 卡间是否禁止相互访问	是□ 否□	
3		通信模块是否能够根据签约的 5G 网络切片信息在网络注册时进行切片选择	是□ 否□	
4		通信模块是否支持 YD/T 3628—2019、3GPP TS 33.501 等标准中要求的机密性和完整性保护算法，如：128-NEA1、128-NEA2、128-NEA3、128-NIA1、128-NIA2 和 128-NIA3	是□ 否□	
5		退役时是否删除配置参数及证书，解绑SIM卡并回收	是□ 否□	
6		是否部署支持国密通用算法或电力专用算法的安全模块，实现身份认证和数据加解密	是□ 否□	
7		退运的安全模块是否进行物理销毁	是□ 否□	
8		涉控终端是否部署可信验证模块，在系统引导、操作系统加载、应用程序加载等阶段进行静态度量和校验	是□ 否□	
9		是否禁止同时连接 5G 电力虚拟专网和其他公共网络	是□ 否□	

表 B.2（续）

序号	评估类别		评估项	是否符合要求	问题描述
10	网络安全	接入网安全	终端 SIM 卡是否仅允许接入一个 DNN 网络	是□ 否□	
11			基站是否具备防 DDos 攻击措施	是□ 否□	
12			N1、N2、Uu 接口是否具备机密性保护、完整性保护和抗重放保护机制	是□ 否□	
13			空口 5QI 等级和业务签约参数是否一致	是□ 否□	
14			空口 AS 信令是否支持对 RRC 信令进行机密性和完整性保护，是否支持机密性保护和完整性保护算法优先级配置，且完整性保护算法配置不能为 NIA0	是□ 否□	
15			空口NAS信令是否支持对NAS信令进行机密性和完整性保护，是否支持机密性保护和完整性保护算法优先级配置，且完整性保护算法配置不能为 NIA0	是□ 否□	
16			空口是否选择和业务系统安全等级相适应的 RB 资源预留方式	是□ 否□	
17			基站是否通过 5QI 保障切片内不同业务承载的优先级	是□ 否□	
18		承载网安全	是否支持 VLAN 方式实现软隔离，VLAN 标签是否能够与网络切片标识进行映射	是□ 否□	
19			网络切片是否支持通过不同的VPN通道，实现电力业务与非电力业务的隔离	是□ 否□	
20			是否支持 FlexE 等，是否提供通道隔离和多端口绑定功能，实现硬切片隔离	是□ 否□	
21			是否支持 SR 和 L3VPN，实现硬切片内不同电力业务的软切片隔离	是□ 否□	
22		核心网安全	是否建立切片隔离管理机制，是否支持多种隔离手段，是否支持端到端切片隔离和网络分段管理	是□ 否□	
23			NF 间服务化接口是否支持 3GPP 标准要求的 HTTP2.0 协议及参数配置	是□ 否□	
24			切片管理接口、切片内部网元是否支持双向身份认证和访问控制机制	是□ 否□	
25			是否具备过载保护功能，是否设置最大连接限制	是□ 否□	
26			和基站之间是否建立双向鉴权机制，以鉴别基站或者核心网是否为伪造网元	是□ 否□	
27			MEC 平台是否部署抗 DDos 攻击、入侵检测等措施	是□ 否□	
28			MEC 平台是否关闭不必要的端口和服务，是否存在安全漏洞	是□ 否□	

表 B.2（续）

序号	评估类别		评估项	是否符合要求	问题描述
29	网络安全	核心网安全	MEC 平台是否划分不同的安全域并部署域间安全隔离措施，包括物理隔离、虚拟机隔离、网元隔离、网络隔离、数据隔离、流量隔离等	是□ 否□	
30			UPF 所在机房是否部署物理防护措施	是□ 否□	
31			UPF 与核心网通信接口是否支持双向认证、传输加密机制	是□ 否□	
32			UPF 与 MEC 平台等应用平台间是否部署安全隔离和访问控制措施	是□ 否□	
33			基站与核心网间的用户面接口（N3 口）是否采用加密认证、访问控制等技术措施，保障通信数据的机密性、完整性	是□ 否□	
34			UPF 与核心网间的信令接口（N4 口）是否采用加密认证、访问控制等技术措施，保障通信控制信令的机密性、完整性	是□ 否□	
35			是否能够配合业务系统进行终端二次认证	是□ 否□	
36	数据安全		针对 5G 虚拟化设施，MANO 中的证书、私钥、VNF 访问口令、SNMP 口令等敏感数据是否部署相应数据保护措施，SDN 控制器是否对口令、私钥、流表、策略等敏感数据部署相应的数据保护措施	是□ 否□	
37			虚拟机在迁移或弹性扩缩过程中，是否能实现其存储数据的有效销毁，确保数据不可恢复和防止滥用误用，是否对数据销毁操作过程进行日志记录以支持安全审计	是□ 否□	
38			不同虚拟机之间共享同一存储资源时，是否进行数据隔离，确保虚拟机不能直接或间接访问其它虚拟机的数据	是□ 否□	
39			在 MANO 各实体间、以及 SDN 控制器南向和北向接口等进行数据传输时，是否采用传输通道或数据加密模式，如采用 TLS/SSL 协议进行数据加密传输，或建立 VPN 加密传输通道方式行安全传输	是□ 否□	
40			5G 核心网（如 UDM）存储、处理的个人数据是否依据数据最小化原则，采用访问控制、匿名化、加密保护以及用户许可等技术手段对个人敏感信息的请求、存储、传输、使用等操作进行隐私保护	是□ 否□	
41			核心网与外部业务系统间之间存在的网络开放接口，是否采用双向认证、数据传输加密和完整性校验、数据安全日志审计等措施	是□ 否□	

表 B.2（续）

序号	评估类别	评估项	是否符合要求	问题描述
42	数据安全	MEC平台与APP之间是否建立访问控制及数据传输安全机制，如机密性、完整性保护及防重放攻击机制等	是□ 否□	
43		MEC 平台的安全域和非安全域之间或不同安全域间进行互联访问、数据流转时，是否在安全边界进行访问控制，是否采用接入鉴权、接入策略设置等手段	是□ 否□	
44		存储于互联网大区的企业重要数据是否遵循最小化原则，是否加密	是□ 否□	
45		终端在传输鉴别信息、电力敏感数据、控制数据等数据时是否进行加密保护	是□ 否□	
46		终端是否具备防审计记录非法读取、防恶意篡改、防恶意删除等数据安全保护措施	是□ 否□	
47		MEC 平台是否支持动态身份标识、匿名化等技术削弱 MEC 平台计算节点标识和地理位置的映射关系时，防止第三方根据 MEC 平台节点位置推断用户的地理位置	是□ 否□	
48		MEC 平台是否具备对电力业务不同应用资源进行隔离的能力，防止应用越权访问其他应用数据，如 vCPU 调度安全隔离、内存资源安全隔离	是□ 否□	
49		NFV/SDN 是否对数据传输安全策略变更进行审核和监控，是否对通道安全配置、密码算法配置、密钥管理等保护措施进行审核及监控	是□ 否□	
50		对于重点防护的调度中心、发电厂、变电站，是否设置经过国家指定部门检测认证的电力专用纵向加密认证装置或加密认证网关及相关设施；发电厂、变电站关键设备是否定期对数据进行备份，备份策略是否合理，是否按照策略执行备份操作	是□ 否□	
51		针对数据泄露、勒索攻击等数据安全威胁，业务系统是否部署数据分级分类、敏感数据加密、流量监测等措施	是□ 否□	
52		存储过企业重要数据的各类存储介质在报废、返厂维修、内部再利用等转作他用之前，是否采用符合 DL/T 1757—2017 规定的设备及方法对存储介质进行有效处理，并做记录	是□ 否□	
53	业务系统安全	与终端间是否部署安全接入网关，实现加密传输和双向认证	是□ 否□	

表 B.2（续）

序号	评估类别	评估项	是否符合要求	问题描述
54	业务系统安全	是否通过具备国家检测资质的第三方权威机构的安全检测，是否具备检测报告	是□ 否□	
55		操作系统、数据库、中间件等基础软件，是否满足 GB/T 20272—2019 中 6.3 和 6.4 的要求，身份鉴别、访问控制、安全审计等安全功能和策略是否已启用并配置合理	是□ 否□	
56		操作系统及数据库是否遵循最小安装的原则，仅安装必要的组件和应用程序，并及时更新系统补丁	是□ 否□	
57		操作系统及数据库是否定期开展安全漏洞扫描和加固	是□ 否□	
58		操作系统是否定期更新防病毒软件和恶意代码库	是□ 否□	
59		数据库是否按照最小权限原则，仅授予管理用户所需的最小权限	是□ 否□	
60		是否部署网络安全监视措施，实现主机设备、网络设备、安全设备等的信息采集、安全审计、实时监视告警等功能	是□ 否□	
61		与终端间是否设置安全接入区	是□ 否□	
62		终端和安全接入区之间是否建立通信隧道，支持终端安全接入认证及通信加密	是□ 否□	
63		安全接入区内是否部署隔离装置，实现安全隔离	是□ 否□	
64		系统服务器、汇聚服务器以及安全接入区中的服务器是否部署安全自主可控操作系统	是□ 否□	
65		下发控制指令的系统服务器、汇聚服务器以及安全接入区中的服务器是否部署可信验证模块，对系统引导程序、系统程序、应用程序和重要配置参数等进行可信验证	是□ 否□	
66		使用 5G 电力虚拟专网承载控制类业务时，是否采用具备安全认证机制的通信规约，是否使用加密机或加密卡等硬件加密设施进行加解密和签名验签运算，是否使用签名验签技术实现控制指令的完整性保护	是□ 否□	
67	管理安全	运行单位是否对业务系统制定日常运维和安全防护的相关管理制度、操作规程等管理措施，并依照执行，定期修订	是□ 否□	

表 B.2（续）

序号	评估类别	评估项	是否符合要求	问题描述
68	管理安全	运行单位是否对业务系统制定安全防护方案，并指定相关系统、设备接入技术方案，安全防护措施是否有效	是□ 否□	
69		运行单位是否定期开展业务系统安全防护自评估工作，实现隐患排查整改闭环	是□ 否□	
70		运行单位是否对业务系统配备安全管理员、系统管理员和安全审计员，是否明确岗位职责、分工和技能要求	是□ 否□	
71		运行单位是否与安全管理员、系统管理员和安全审计员等关键岗位人员签署保密协议	是□ 否□	
72		运行单位是否取消离岗人员相关系统访问权限、回收软硬件设备	是□ 否□	
73		运行单位是否对业务系统制定厂家维护、评估检测等第三方人员访问管理制度或相关规范	是□ 否□	

附 录 C
（规范性）
评估结果分析方法

基于5G网络的电力业务系统安全防护评估结果分析方法包括定性分析方法和定量分析方法，运行单位或评估机构可根据实际需求选择。

C.1 定性分析

定性分析从安全问题发生的可能性、对系统的影响程度两个方面进行综合分析，评价安全问题等级。定性分析方法如下：

a) 判断安全问题发生的可能性，可能性等级为高、中和低，见表C.1；

表C.1 安全问题发生的可能性取值

等级	定义
高	安全问题出现的频率较高；或在大多数情况下很有可能会发生；或可以证实多次发生过；或其实现条件较容易被攻击者获得
中	安全问题出现的频率中等；或在某种情况下可能会发生；或可以证实曾经发生过；或其实现条件难以被攻击者获得
低	安全问题出现的频率较小；或一般不太可能发生；或没有被证实发生过；或其实现条件很难被攻击者获得

b) 判断安全问题被利用后，对基于5G网络的电力业务系统安全造成的影响程度，影响程度等级为高、中和低，见表C.2；

表C.2 安全问题对基于5G网络的电力业务系统安全造成的影响程度取值

等级	定义
高	如果安全问题出现，将对基于5G网络的电力业务系统造成重大损害
中	如果安全问题出现，将对基于5G网络的电力业务系统造成一般损害
低	如果安全问题出现，将对基于5G网络的电力业务系统造成较小或轻微损害

c) 结合a）和b）的结果，利用安全问题评价矩阵，对基于5G网络的电力业务系统存在的安全问题进行评价，等级为高、中和低，见表C.3。

表C.3 安全问题评价矩阵

影响程度	可能性		
	高	中	低
高	高	高	中
中	高	中	低
低	中	低	低

C.2 定量分析

根据基于5G网络的电力业务系统安全防护实际情况是否符合评估项的描述，为评估项赋予量化值（P_{ij}），P_{ij}取值标准参见表C.4，评估结果量化值（ISL）由式（C.1）计算求得。

$$ISL = \sum_{i=1}^{n}\left(\sum_{j=1}^{m} P_{ij}\right) \quad (C.1)$$

式中：

ISL——评估结果量化值；

P_{ij}——评估项量化值；

n——评估类别个数；

m——第 i 个评估类别中评估项的个数。

表 C.4　P_{ij}取值标准

序号	系统安全防护情况是否符合要求	P_{ij}取值
1	是☑　　否☐	P_{ij}=1
2	是☐　　否☑	P_{ij}=0

参 考 文 献

[1] GB/T 20984 信息安全技术 信息安全风险评估方法
[2] GB/T 22239 信息安全技术 网络安全等级保护基本要求
[3] GB/T 36047 电力信息系统安全检查规范
[4] GB/T 38318 电力监控系统网络安全评估指南
[5] GB/T 39204 信息安全技术 关键信息基础设施安全保护要求
[6] 电力监控系统安全防护规定 国家发展和改革委员会令 2014 年第 14 号
[7] 电力监控系统安全防护总体方案 国能安全〔2015〕36 号