ICS 33.060,99
CCS M 36

T/EJCCCSE

团　　体　　标　　准

T/EJCCCSE XXX—2024

5G 通信基站运维系统

5G communication base station operation and maintenance system

（征求意见稿）

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。

2024－XX－XX 发布　　2024－XX－XX 实施

中国商业股份制企业经济联合会　　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这些专利的责任。

本文件由中国商业股份制企业经济联合会提出并归口。

本文件起草单位：苏州泰坦智能科技有限公司、昆山小橙物联网科技有限公司。

本文件主要起草人：赵永良 刘瑞瑞 刘伟凡。

本文件为首次制定。

5G 通信基站运维系统

1 范围

本文件规定了5G通信基站运维系统(以下简称:系统)运维的基本要求、安全运维要求及运维应急管理等。

本文件适用于5G通信基站运维系统的安全运维。

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 3628 5G移动通信网 安全技术要求

YD/T 3807 移动通信网络设备安全保障通用要求

3 术语和定义

本文件没有需要界定的术语和定义。

4 缩略语

下列缩略语适用于本文件。

MANO 管理和编排 Management and Orchestration

NFVO 网络功能虚拟化协调器 Network Functions Virtualization Orchestrator

OMC 运维管理中心 Operation Management Center

PIM 物理基础设施管理器 Physical Infrastructure Manager

SDN 软件定义网络 Software Defined Networking

SSH 安全外壳 Secure Shell

MEC 移动边缘计算 Mobile Edge Computing, MEC

NFV 网络功能虚拟化，Network Function Virtualization

HTTPS 超文本传输安全协议 Hypertext Transfer Protocol Secure

SFTP 安全文件传送协议 Secure File Transfer Protocol

Hypervisor 虚拟机监视器virtual machine monitor，缩写为 VMM

UPF 用户端口功能 User Port Function

5 基本要求

5.1 入网安全验收

5.1.1 5G 通信基站网络设备应符合 YD/T 3807 的要求。入网设备安全检查项目包括但不限于以下：

a) 不应存在无主帐号设备。

b) 所有开放端口对应的应用软件和功能应列表登记，不允许存在非必要的开放端口。

c) 设备的系统层、数据库和应用层应具备用户越权访问、权限升级、更改口令、新建用户、非正常时间登录、多次错误登录、审计策略更改或其他异常事件日志记录功能。

d) 采用静态口令认证的设备，口令至少由 8 位及以上、且至少含大小写字母、数字及特殊符号中的 3 种组成。不应以姓名、电话号码等作为口令或口令的组成部分。

e) 使用评估工具对网络结构、网络设备、服务器主机、数据库、中间件和用户帐号/口令等进行安全扫描，不应存在严重风险、高风险以及中风险漏洞。
f) 安装通用操作系统的设备应安装指定授权的防病毒软件，且病毒库应可时时更新至最新。
g) 网元业务流程和通信协议不应存在漏洞。

5.1.2 5G 通信基站网络技术应符合 YD/T 3628 的要求，网络架构安全检查项目包括但不限于以下:

a) 网络资产、拓朴、安全域、防火墙、路由器等的配置应符合建设方案，防火墙应具备双向访问控制功能且已按最小化权限的原则配置了防火墙策略。
b) 渗透测试应由具备渗透经验的安全运维人员使用扫描工具、漏洞验证、脚本等方式对网络中存在的安全风险点做进一步检查。

5.2 安全资产管理

5.2.1 应编制网络安全资产清单，并维护资产清单的准确性与完整性。资产清单应包括但不限于资产名称、所处位置、所属系统、资产责任人、设备类型、设备厂商、iP 地址、系统信息、端口信息、服务信息、中间件信息、程序应用框架信息、应用软件信息、资产分类、安全级别等。

5.2.2 应参照网络安全等级保护、关健信息基础设施保护、网络数据安全等要求确定网络安全资产管理系统的安全级别，并实施相应后安全保护措施。

5.3 定级备案

5.3.1 应对所维护系统或网元进行定级备案。

5.3.2 应全量、真实填报定级备案信息。

5.3.3 应按相关要求定期完成符合性评测和风险评估工作。

5.4 账号口令

5.4.1 应明确账号的生命周期、账号分配原则、口令配置规则。

5.4.2 维护人员应对所管理维护的系统、软硬件设备的账号口令加强管理，不允许使用弱口令、易猜解口令。

5.4.3 应定期修改口令并妥善保管账号口令。

5.5 数据安全

5.5.1 应做好数据的分级分类管理，数据访问权限管理，并应形成网络数据资产清单。

5.5.2 应做好数据的操作行为管理，实施账号管理、认证管理、授权管理和安全审计措施。

5.5.3 对于涉及高价值信息的操作应由两人及以上有相应权限的人员共同协作完成。

5.5.4 应做好数据的全生命周期管理，在数据采集、传输、存储、使用、共享和销毁环节，应严格实施安全管控措施。

5.5.5 数据的共享应严格按照分级审批、合理授权的原则进行。

5.5.6 维护人员不应以任何方式违规获取、保存、复制、修改和删除 5G 基站的各类数据。

5.5.7 应制定数据安全应急预案，发生网络数据安全事件时应及时采取补救措施。

5.5.8 应建立完善的数据备份与恢复机制，定期执行灾难备份恢复能力检测，更新备份关健数据。

5.5.9 应使用安全的随机数生成器产生公私密钥对，并对私钥进行加密存储和备份。禁止私钥以明文形式导出专用密码设备。

5.6 安全补丁管理

5.6.1 应通过漏洞扫描及时发现存在的安全漏洞以及需要安装的漏洞补丁。

5.6.2 对发现存在严重安全预警或高危漏洞的系统，以及有互联网暴露面的端口或服务，应在规定时限内完成安全处理。

5.6.3 对于无补丁的漏洞，应做好访问控制策略，并应加强安全监测。

5.6.4 应根据安全影响严重程度以及对业务影响程度进行评估，对系统和设备更新补丁。

5.6.5 应对补丁进行兼性测试，通过后方可进行批量化下发和安装操作。

5.7 系统变更与配置管理

5.7.1 应建立数据备份与恢复机制，制定系统变更方案及流程。
5.7.2 应支持文件级的全量备份或增量备份，支持虚拟机及文件级的热备份及冷备份。
5.7.3 应定期执行灾难备份恢复能力检测，更新备份关键数据。

5.8 证书管理

5.8.1 应使用安全的随机数生成器产生公私密钥对。
5.8.2 应对私钥进行加密存储、备份，以加密方式从专用密码设备导入到 5G 网元中，禁止私钥以明文形式导出专用密码设备。
5.8.3 证书应设置合理有效期，并对已过期或即将过期证书进行提醒。

5.9 安全监测

5.9.1 应开展网络安全资产属性采集，建立资产档案并定期进行核查。
5.9.2 应定期对 5G 网元进行合规配置检查。
5.9.3 应定期通过扫描工具、漏洞验证、脚本等方式检测安全风险。
5.9.4 应将部置在 5G 网络安全域边界的安全月志、安全事件通过接口统一上报感知平台，进行集中安全监测及告警处置。

6 安全运维要求

6.1 5G 网元安全运维

5G网元安全运维要求应包括：
a) 5G 虚拟化网元进行升级、部署等操作时应对软件包的合法性和完整性进行校验。
b) 应禁止对 5G 网元的非授权访问；
c) 应设置 5G 网元的信令或数据流量门限，丢弃超过门限的流量或降低处理流量的速度；
d) 应及时关闭不必要的端口和服务。应支持通过 OMC 对网元进行证书配置、 安全基线核查等。

6.2 网络切片安全运维

网络切片安全运维要求应包括:
a) 网络切片管理系统与所有网络切片之间的访问应进行认证、授权；
b) 网络切片管理系统应对操作人员进行认证、授权，并对操作行为进行日志记录和安全审计；
c) 网络切片管理系统应支持按照租户设置分权分域，并对租户的管理权限进行控制；
d) 网络切片管理系统应使用 HTTPS、 SFTP、 SSHv2 等安全协议与 NFV 编排和管理系统等进行通信；
e) 网络切片终止使用的，应释放该网络切片使用的相关资源，将相关数据按需进行彻底删除；
f) 应对网络切片进行安全监控，实时掌握网络切片运行情况、可能的攻击及故障状况，并在出现故障后采用恢复网络切片措施；
g) 网络切片的基础设施安全运维要求应参考 NFV 基础设施的安全运维要求。

6.3 虚拟化层安全运维

虚拟层的安全运维要求应包括：
a) 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；
b) 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；
c) Hypervisor 的管理接口流量应该和其它网络流量物理隔离；
d) Hypervisor 应满足安全配置、合规账号口令管理的安全要求。

6.4 PIM 安全运维

PIM安全运维要求应包括：
a) PIM 应采用安全协议和算法、设置访问控制，开启鉴权认证，实现限制对管理端口的访问；

b) 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 和分布式存储服务器之间传输的数据的机密性和完整性；
c) 应做好日常监测及处置工作。

6.5 MANO 安全运维

MANO安全运维要求应包括：
a) 应使用安全通信协议，并进行 web 安全加固；
b) 在创建角色和用户时应分配最小权限；
c) MANO 中不应包含明文敏感信息，并应支持会话超时退出功能；
d) 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；
e) 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；
f) 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；
g) 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；
h) 应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。

6.6 SDN 安全运维

SDN安全运维要求应包括：
a) SDN 控制器应启用识别异常流量/报文，并通过限速等机制，防止(D) DoS 攻击；
b) SDN 控制器应启用检测配置及策略冲突，并在检测到冲突后进行提示；
c) 远程登录 SDN 控制器时，应使用 SSHv2 等安全协议；
d) 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，保证接口传输数据的机密性和完整性；
e) SDN 控制器应支持集群方式部署。

6.7 MEC 安全运维要求

MEC安全运维要求应包括：
a) 应提供安全审计功能，并根据运营商和 MEC 平台用户的职责划分，对各自部分的用户行为和安全事件进行审计；
b) 应确保运营商对 MEC 应用的操作可被 MEC 平台用户审计，并应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等，保证审计数据的真实性和完整性；
c) 应对下沉至园区的 UPF 中的敏感数据进行加密存储，严格限制访问人员，禁止非授权用户访问，敏感用户数据页面显示应进行脱敏处理，禁止本地数据导出；
d) 应限制园区用户访问下沉至园区的 UPF；
e) 下沉至园区的 UPF 与运营商大网核心网、 园区网络应建立安全通道进行数据传输， 并做好安全隔离，配置 IP 白名单互访；
f) 当位于客户机房的运营商设备采用远程运维方式时，应禁掉设备本地运维的所有接口，并能够检测本地运维接口是否打开，进行报警；
g) 应支持通过加密安全通道进行远程运维，并限制远程访问 IP 白名单和远程操作类型，且设备的所有操作均应进行日志记录和审计。

7 运维应急管理

7.1 总体要求

应制定安全应急管理要求，至少应包括安全应急预案管理、安全事件监测、安全事件预警以及安全事件处置。当突然发生由网络攻击、网络入侵、恶意程序等造成或可能造成严重社会危害或影响时，应采取应急处置措施应对网络中断、系统瘫痪、数据丢失 、病毒传播等事件。

7.2 应急预案管理

7.2.1 系统应制定详细的安全应急预案，系统发生变更调整时，安全应急预案相关部分应同步更新，系统下线时安全应急预案及时清理。
7.2.2 系统应制定详细的应急演练计划并提交给网络安全部门备案，定期开展安全应急演练，且应急演练记录应包含但不限于：演练目标、演练时间、参演人员、演练内容及与应急预案的一致性、演练过程记录等。

7.3 安全事件监测

7.3.1 应建立和完善安全风险监测手段，提供各类安全风险的主动监测与感知能力。
7.3.2 应开展 7*24 小时安全监控，监控范围包括但不限于：安全设备运行实时情况监控，网络安全设备安全状况实时情况监控。
7.3.3 针对监控发现的安全问题应进行记录并形成监控日志。

7.4 安全事件预警

7.4.1 应根据安全事件等级对接到正式预警后采取临时防护措施、完成处置的时限进行要求。
7.4.2 应根据预警信息对系统的影响情况调高预警级别。

7.5 安全事件处置

应根据安全事件等级对处置时限进行要求，并在进行风险处置的同时及时对风险处置情况进行上报。