ICS 35.020
CCS M 10

YD

中 华 人 民 共 和 国 通 信 行 业 标 准

YD/T XXXXX—XXXX

5G 移动通信网虚拟化管理和编排安全防护要求

Security protection requirements for 5G mobile communication network virtualization management and orchestration

(点击此处添加与国际标准一致性程度的标识)

报批稿

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国工业和信息化部　　发 布

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、中兴通讯股份有限公司、亚信安全科技股份有限公司。

本文件主要起草人：孟楠、戴方芳、王晗、查选、周继华、薛辉。

5G 移动通信网虚拟化管理和编排安全防护要求

1 范围

本文件规定5G移动通信网虚拟化管理和编排按安全保护等级的安全防护要求，涉及应用安全、网络安全、设备安全、数据安全、物理环境安全和管理安全。

本文件适用于基础电信业务经营者独立或与第三方合作建设运营的5G移动通信网虚拟化管理和编排。

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 36637-2018	信息安全技术 ICT供应链安全风险管理指南
YD/T 1731-2008	电信网和互联网灾难备份及恢复实施指南
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 2698-2014	电信网和互联网安全防护基线配置要求及检测要求 网络设备
YD/T 2699-2014	电信网和互联网安全防护基线配置要求及检测要求 安全设备
YD/T 2700-2014	电信网和互联网安全防护基线配置要求及检测要求 数据库
YD/T 2701-2014	电信网和互联网安全防护基线配置要求及检测要求 操作系统
YD/T 2702-2014	电信网和互联网安全防护基线配置要求及检测要求 中间件
YD/T 2703-2014	电信网和互联网安全防护基线配置要求及检测要求 WEB应用系统

3 术语和定义

下列术语和定义适用于本文件。

3.1

虚拟化管理和编排 virtualization management and orchestration

管理基础设施和编排网络服务及虚拟网络功能所需资源的功能。

4 缩略语

下列缩略语适用于本文件。

BSS 业务支撑系统 Business Support System

MANO	管理和编排	Management and Orchestration
MFA	多因素认证	Multi-factor Authentication
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
NFV-MANO	网络功能虚拟化管理和编排	Network Functions Virtualization Management and Orchestration
NFVO	网络功能虚拟化编排器	Network Functions Virtualization Orchestrator
OSS	运营支撑系统	Operation Support System
VIM	虚拟化基础设施管理器	Virtualized Infrastructure Manager
VNF	虚拟化网络功能	Virtualised Network Function
VNFM	虚拟化网络功能管理器	Virtualised Network Function Manager

5 5G 移动通信网虚拟化管理和编排安全防护概述

5.1 5G 移动通信网虚拟化管理控制单元安全防护范围

本文件主要对基础电信业务经营者独立或与第三方合作建设运营的5G移动通信网虚拟化管理和编排提出安全防护要求，安全防护对象覆盖NFV-MANO以及其和外部网络间的交互等，如图1所示。

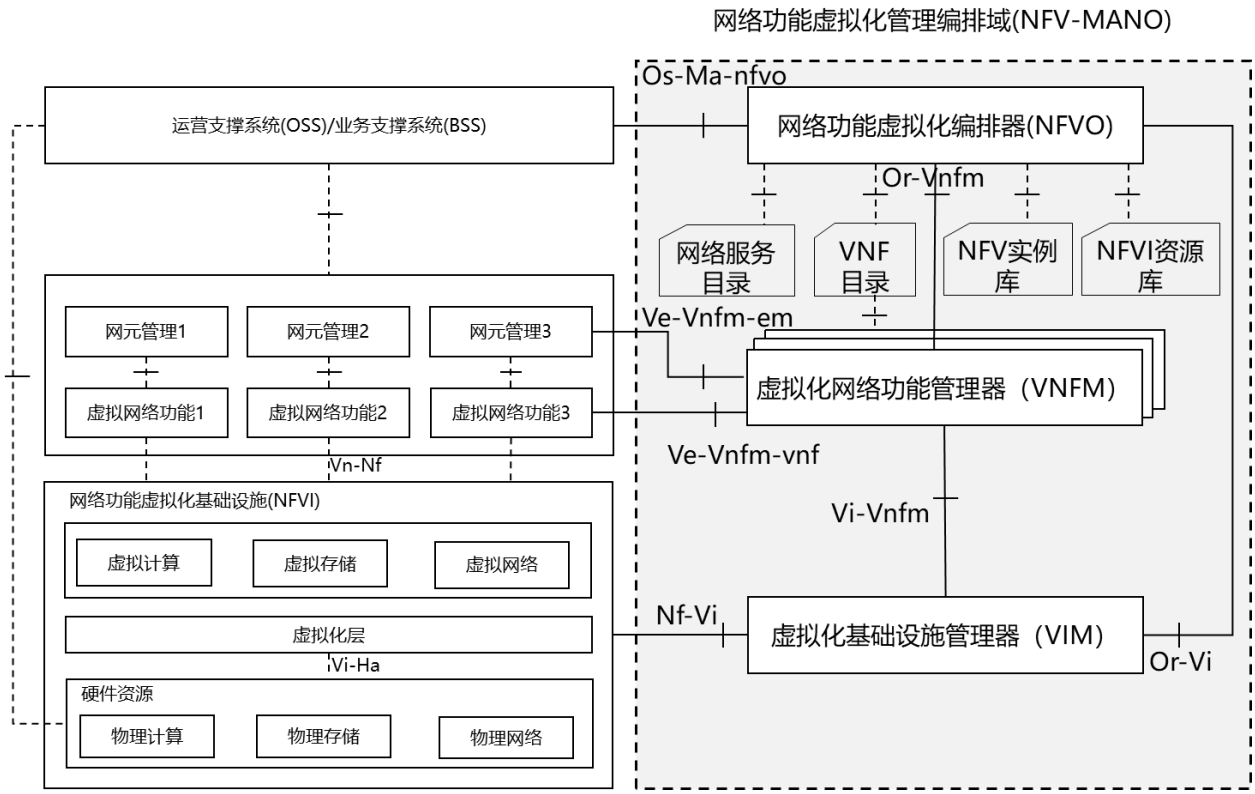

图1 5G 移动通信网虚拟化管理控制单元示意图

从外部看，NFV-MANO负责管理基础设施和编排网络服务和虚拟网络功能所需的资源，通过4个外部接口进行外部交互；从内部看，NFV-MANO包含网络功能虚拟化编排器（NFVO）、虚拟化网络功能

管理器（VNFM）和虚拟化基础设施管理器（VIM）三个功能模块，通过3个内部接口进行内部交互，其中：

——网络功能虚拟化编排器（NFVO）实现网络服务的生命周期管理，并协调 VNF 生命周期的管理（需要得到 VNFM 的支持）、协调 NFVI 各类资源的管理（需要得到 VIM 的支持），以此确保所需各类资源与连接的优化配置。包括服务编排与资源编排，实现控制新的网络服务并将 VNF 集成到虚拟架构中，验证并授权 NFVI 的资源请求等。

——虚拟化网络功能管理器（VNFM）是 VNF 管理系统，负责 VNF 生命周期管理，包括上线、下线，状态监控等。

——虚拟化基础设施管理器（VIM）实现对 NFVI 资源的管理、调度、编排和监控，主要功能包含分配、管理、释放虚拟化基础设施的虚拟化资源；接收和存储软件镜像；收集、上报虚拟化资源的性能和故障信息。

——内部接口：

——Or-Vnfm：NFVO 将配置信息发给 VNFM，进一步由 VNFM 控制 VNF 运行。同时收集 VNF 的信息，支撑 NFVO 进行网络服务生命周期管理。

——Vi-Vnfm：VNFM 控制 VNF 资源的接口，同时也收集虚拟化资源的配置和状态信息，供 VNF 使用。

——Or-Vi：NFVO 连接到 VIM 的接口，用于资源的分配和保留，收集虚拟化资源的配置和状态信息。

——外部接口：

——Nf-Vi：具体的虚拟资源分配接口，同时收集虚拟化资源的配置和状态信息。

——Os-Ma-nfvo：与 OSS/BSS 进行交互的接口。

——Ve-Vnfm-vnf 和 Ve-Vnfm-em：VNFM 管理 VNF 的接口，包括配置管理、收集 VNF 状态信息，支撑网络服务生命周期管理。

从资产的角度看，5G移动通信网虚拟化管理和编排防护范畴涵盖构建管理和编排的通用/专用设备、软件、数据、文档和资料、人员、物理环境等，具体见附录A中表A.1。

5.2 5G 移动通信网虚拟化管理和编排安全风险分析

5.2.1 概述

以5G移动通信网虚拟化管理和编排的资产为核心，可从技术脆弱性和管理脆弱性两个方面识别5G移动通信网虚拟化管理和编排脆弱性。5G移动通信网虚拟化管理和编排的脆弱性分析应包括但不限于附录A中表A.2所列范围。表A.3列举出5G移动通信网虚拟化编排管理主要面临的威胁。结合5G移动通信网虚拟化管理和编排技术架构和运行模式，可能面临的安全风险主要包括以下几个方面。

5.2.2 应用安全风险

5G移动通信网虚拟化管理和编排将能力等开放给运营支撑系统（OSS）/业务支撑系统（BSS），涉及的软件安全风险包括但不限于：

——**应用安全隔离风险：**软件模块与软件模块、软件模块与网元间的隔离不当，可能导致用户访问权限越界、数据丢失和泄露等安全风险。

——**应用管理和编排不当：**软件过度授权或权限滥用，或因应用的调用、编排、协作管理等策略设置不当，导致应用对下层基础资源的过度消耗或滥用。

——**安全漏洞：**包括 5G 移动通信网虚拟化管理和编排应用、API 接口等在开发、部署、更新等过程中可能引入的安全漏洞，serverless、service mesh、容器技术、虚拟化技术、微服务框架等技术架构安全漏洞，监控工具、调试工具等组件安全漏洞等。

——**虚拟化安全风险：**应用共享下层基础资源，若某个软件模块被攻击将会波及其他模块。由网络虚拟化致使大量采用开源和第三方软件，引入安全漏洞的可能性增大。

5.2.3 网络安全风险

5G移动通信网虚拟化管理和编排涉及的网络安全风险包括但不限于：

——**非授权访问安全风险：**包括底层设备、网络功能、服务遭到不安全的通信协议接入、非法接入的安全风险。

——**网络攻击安全风险：**攻击者入侵网络发动 IP 攻击、DDoS 攻击等网络攻击安全风险。

——**网络配置错误：**包括网络连接配置不当、资源分配配置不当、访问控制策略配置不当、底层设备系统补丁未及时更新而带来的网络安全风险。

5.2.4 设备安全风险

5G移动通信网虚拟化管理和编排主要涉及通用服务器、网络设备、安全设备等实体，负责承载虚拟化管理和编排核心能力等，其涉及的安全风险包括但不限于：

——**设备配置缺陷：**包括各类设备基线配置不当、设备登录和访问控制策略配置不当、设备资源管理策略配置不当等引发的非法用户登录、非授权攻击等安全问题。

——**设备管理安全：**包括因设备维护的管理通道缺乏双向认证或匹配的加密算法引发的窃听、劫持和篡改攻击，设备安全漏洞更新不及时导致的安全隐患等。

——**设备安全漏洞：**包括设备涉及的硬件漏洞、软件漏洞，以及容器、数据库开发等第三方组件漏洞等。

5.2.5 数据安全风险

5G移动通信网虚拟化管理和编排可收集、存储与其外部接口交互的数据，包括配置信息、状态信息等，其涉及的数据安全风险包括但不限于：

——**数据损毁风险：**包括因 5G 移动通信网虚拟化管理和编排底层硬件设备毁坏、设备遭受攻击、重要数据未备份、未具备数据恢复机制等造成的数据损毁风险。

——**数据泄露风险：**因未实施数据分级分类管理，未部署敏感数据加密、脱敏手段，或开展不合规的数据开放共享等，可能导致数据泄露等安全风险。

——**数据篡改风险：**包括因 5G 移动通信网虚拟化管理和编排涉及的数据未进行机密性、完整性保护、以及系统脆弱性等造成的数据篡改风险。

5.2.6 物理环境安全风险

5G移动通信网虚拟化管理和编排可根据基础电信企业不同方案，部署在大区、省级机房等位置，其涉及的物理环境安全风险包括但不限于：

——**机房环境安全风险：**包括因机房位置、电力供应、防火、防水、防静电、温湿度控制等设置不合规而引发的设备断电、网络断连等安全风险。

5.2.7 管理安全风险

5G移动通信网虚拟化管理和编排的管理安全风险包括涉及平台自身的管理安全风险，以及与其他相关方合作过程中的管理安全风险等，包括但不限于：

——**网络安全管理风险：**包括缺少对管理人员身份与权限、安全策略配置、安全事件应急恢复、网络云容器安全、安全局划分和访问控制、安全审计等技术管理手段造成的安全风险隐患。

——**运维管理安全风险：**未采取安全风险监测和处置、安全事件应急预案管理和响应、人员管理等方面的措施，造成运行故障、数据泄露等安全隐患。

——**供应链安全风险：**包括因设备整机、关键芯片、核心部件、软件功能等断供引发的供应链完备性问题，以及引入第三方组件/工具时，被植入了后门或者木马，从而导致系统瘫痪或中断的安全风险。

5.3 5G 移动通信网虚拟化管理和编排安全防护内容

从5G移动通信网虚拟化管理和编排的资产和脆弱性分析看，5G移动通信网虚拟化管理和编排的安全防护内容具体包括：

a） 应用安全

应用安全主要包括5G移动通信网虚拟化管理和编排相关应用在身份鉴别、访问控制、资源管控、业务连续性、安全审计、虚拟化安全、能力开放安全等方面的安全要求。

b） 网络安全

网络安全主要包括5G移动通信网虚拟化管理和编排层面的结构拓扑、网络攻击防范、冗余保护与灾备恢复、安全审计等方面的安全防护要求。

c） 设备安全

设备安全主要包括5G移动通信网虚拟化管理和编排所涉及的通用服务器、数据库、相关设备等通用主机设备，在身份鉴别、访问控制、安全审计、入侵防范、资源控制等方面的安全防护要求。

d） 数据安全

数据安全主要包括5G移动通信网虚拟化管理和编排所涉及的在数据加密、数据存储、敏感数据处理、数据传输等方面的安全防护要求。

e） 物理安全

物理安全主要包括5G移动通信网虚拟化管理和编排基础设施所处的物理环境在机房位置、电力供应、防火、防水、防静电、温湿度控制等方面的安全防护要求。

f） 管理安全

管理安全主要包括管理制度、人员和技术支持能力、运行维护管理能力、灾难恢复预案等方面的安全防护要求。

6 5G 移动通信网虚拟化管理和编排安全防护要求

6.1 第 1 级要求

本项要求包括：

a） 操作系统的安全基线配置应满足 YD/T 2701—2014 的安全要求。

b） 数据库的安全基线配置应满足 YD/T 2700—2014 的安全要求。

c） WEB 应用系统的安全基线配置应满足 YD/T 2703—2014 的安全要求。

d） 中间件的安全基线配置应满足 YD/T 2702—2014 的安全要求。

e） 网络设备的安全基线配置应满足 YD/T 2698—2014 的安全要求。

f） 安全设备的安全基线配置应满足 YD/T 2699-2014 的安全要求。

g） 用户个人电子信息保护应满足 YD/T 2692—2014 的安全要求。

6.2 第 2 级要求

6.2.1 应用安全要求

6.2.1.1 身份鉴别

本项要求包括：

a) 应对登录 NFVO、VNFM 的用户进行身份标识和鉴别，身份标识具有唯一性，口令等身份鉴别信息应有复杂度及强度要求并定期更换。
b) 应用的登录过程应启用登录连接超时自动退出功能，应启用登录失败处理功能，可采取结束会话、限制非法登录次数等措施。
c) 应强制用户首次登陆时修改初始口令。
d) 用户身份鉴别信息丢失或失效时，应采用技术措施确保鉴别信息重置过程的安全。
e) 应提供集中账号管理，建立基于唯一身份标识的全局实名制管理。
f) 当对业务系统进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。
g) 应使用密码技术对用户身份鉴别信息进行保密性和完整性保护。

6.2.1.2 访问控制

本项要求包括：

a) 应在应用边界部署访问控制设备，并启用访问控制功能。
b) 应对使用应用的用户依据最小授权原则为各用户分配账户及相应的访问操作权限，对不同的访问行为分配相应的读取、写入等资源访问权限。
c) 应防止在未经授权的情况下对 VNF 进行操作。
d) 应重命名或删除默认账户，修改默认账户的默认登录口令，禁用共享账户，及时删除或停用多余、过期账户。
e) 应基于最小权限原则授予应用管理用户所需的权限。
f) 应删除多余的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。
g) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，根据会话状态信息为数据流提供明确的允许/拒绝访问能力。

6.2.1.3 应用安全部署

本项要求包括：

应对应用提供日常安全扫描和基线核查等安全机制，在上线前进行代码审计和基线核查，以确保代码未遗留已知中危及以上安全漏洞。

6.2.1.4 攻击防范

本项要求包括：

a) 应配置虚拟 WAF 或物理 WAF、主机安全（如防病毒、EDR 等）攻击防范机制，对应用进行安全隔离和攻击防范。
b) NFVO、VNFM 的镜像文件应存储在安全的环境中，防止非授权访问。并进行镜像安全漏洞扫描和病毒扫描、基线核查，保证镜像的存储安全、防篡改和传输安全等。
c) 应支持通过第三方接口或内置工具等方式对应用容器镜像进行漏洞扫描，发现已知漏洞并及时进行修复。
d) 应对应用容器实例进行进程监控，对异常进程行为进行告警。
e) 根据应用重要程度，对关键应用所在虚拟机宜采用独占服务器方式进行部署运行。应支持微分段，可以按照应用类型对虚拟机进行隔离，避免非授权访问和不同应用间相互影响。

6.2.1.5 安全审计

本项要求包括：

a) 应对相关应用启用安全审计功能，审计范围应覆盖到每个用户的关键操作，审计内容应包括对用户的重要行为、资源使用情况等重要事件。
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息，并确保审计记录的留存时间符合有关法律法规要求。
c) 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，并对审计数据进行定期备份。
d) 审计记录中应避免明文记录敏感数据，如用户口令等。
e) 应通过集中安全审计，对用户从登录到退出的全程操作行为进行审计。

6.2.1.6 资源安全管控

本项要求包括：

a) 应能够对业务系统最大并发会话连接数进行限制。
b) 应能够对单个账户的多重并发会话进行限制。
c) 应保证虚拟机的资源使用不受周边虚拟机的影响，能够实现同一物理机上不同虚拟机之间的资源隔离。

6.2.2 网络安全要求

6.2.2.1 结构安全

本项要求包括：

a) 应绘制与 NFV-MANO 运行情况相符的网络拓扑结构图，维护网络设备、虚拟化网络资源、网络配置等资产清单，并能够对网络拓扑结构图和资产清单进行及时更新。
b) 应划分不同的安全域，安全域之间应采用物理隔离或逻辑隔离的技术隔离手段。
c) 重要系统、网络关键设备、通信链路的设计部署等方面应实施冗余备份。

6.2.2.2 访问控制

本项要求包括：

a) 应在网络边界或安全域之间等根据访问控制策略设置访问控制规则，严格控制 NFV-MANO 内部不同组件间、OSS/BSS 对 NFV-MANO 等的访问。
b) 应及时对访问控制规则进行更新，删除多余的访问控制规则，优化访问控制列表。
c) 应对接入 NFV-MANO 的用户身份发起鉴权认证，验证用户身份的合法性，保证授权用户接入。

6.2.2.3 安全审计

本项要求包括：

a) 应对网络操作、关键网络设备的日志、重要安全事件等进行审计。
b) 审计记录应包括事件的日期和事件、用户、事件类型、事件是否成功及其他与审计相关的信息。
c) 应对审计记录进行保护，定期备份，避免受到未经授权的删除、修改或覆盖等，审计记录的留存时间应符合相关法律法规要求。
d) 应通过中央日志服务器等专用设备或系统提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

6.2.2.4 攻击防范

本项要求包括：

a) 应具备在关键节点处监测网络攻击行为的能力。
b) 应能对面向虚拟网络节点的攻击行为进行检测，并应记录攻击源 IP、攻击类型、攻击目标、攻击时间等攻击信息。
c) 应在网络边界处部署 IDS 等同类安全检测设备、防火墙等同类访问控制设备、抗 DDoS 设备、防病毒系统等。

6.2.2.5 资源安全管控

本项要求包括：
a) 应能监测识别虚拟机与宿主机、虚拟机与虚拟机之间的异常流量，并在监测到异常流量时及时告警。
b) 应具备网络流量的监测分析能力，识别异常流量，并在监测到异常流量时及时告警。
c) 应能监控网络连接配置不当、资源分配配置不当、访问控制策略配置不当、底层设备系统补丁未及时更新等网络安全风险隐患，并及时告警。

6.2.2.6 通信安全

本项要求包括：
a) 应支持与 OSS/BSS（用户）建立安全的通信信道/路径，保障通信数据的保密性、完整性。
b) 基础通信协议应满足通信协议健壮性要求，防范异常报文攻击。
c) MANO 内外部交互接口应支持双向认证。
d) MANO 内外部交互的通信内容，如资源状态信息、业务信息，配置信息等应采用校验码技术进行机密性、完整性以及防重放保护。对外提供服务的 API 接口均采用安全的数据传输协议。
e) MANO 内部组件之间通信应采用消息队列机制并承载在数据传输协议之上，保证通信的完整性和机密性。
f) NFVO、VNFM 收到来自 VNF 的弹性请求时，应验证请求方的身份，只允许处理来自合法身份的请求。
g) NFVO、VNFM 与客户端通信应采用 SSH、SFTP、HTTPS 等安全通信机制；NFVO、VNFM、VIM 之间通信应采用 HTTPS 等安全通信机制；VNFM 与 VNF 之间通信应采用 HTTPS、SSH 等安全通信机制。

6.2.2.7 安全声明

本项要求包括：
a) 供应商应提供设备支持的所有协议，不应存在未声明的私有协议。
b) 供应商应承诺不存在未声明或告知的非公开功能、隐蔽链接和协议端口。

6.2.3 设备安全要求

6.2.3.1 身份鉴别

本项要求包括：
a) 应对登录用户进行身份标识和鉴别，身份标识具有唯一性，口令等身份鉴别信息应有复杂度要求并定期更换。
b) 应启用登录连接超时自动退出功能，应启用登录失败处理功能，可采取结束会话、限制非法登录次数等措施。退出时，服务器端必须清除该用户的会话信息。
c) 应支持限制用户会话连接的数量，以防范资源消耗类拒绝服务攻击。
d) 在支持基本的管理功能时，应支持安全的管理协议。

6.2.3.2 访问控制

本项要求包括：

a) 应根据管理用户的角色授予其所需的最小权限，实现管理用户的权限分离。
b) 应重命名或删除默认账户，修改默认账户的默认口令（需要满足口令复杂性的要求）。并及时删除或停用多余的、过期的账户，并避免共享账户的存在。
c) 应支持基于 IPv4/v6 源地址、源端口、协议类型等的访问控制列表功能。
d) 当远程管理设备时，管理终端和设备之间应建立双向身份验证机制。
e) 应保证当发生虚拟设备迁移时，访问控制策略随之迁移。
f) 应对包含敏感信息的文件（包括程序运行时产生的静态文件和临时文件）进行权限控制，确保文件只能被相应权限的用户访问。
g) 资产的通信矩阵应清楚地记录其正确操作所需的所有接口、服务、端口（源和目的地）和协议，包括任何可选的接口、服务、端口和协议，并明确服务与所需的网络接口、IP 地址和端口的对应关系。
h) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。

6.2.3.3 攻击防范

本项要求包括：

a) 应对 MANO 实体进行安全加固，实现安全服务最小化原则，如关闭不必要的服务和端口等。
b) 在 NFVO、VNFM 基于虚拟机方式部署时，应以仅满足该服务器基本业务可正常运行为目的，对 Guest OS 进行最小化定制，限制操作系统开放的端口、访问权限和运行服务。
c) 对于存在较多版本的远程管理协议，应默认关闭安全性较低的版本。
d) 应遵循最小安装的原则（安全软件除外），仅安装需要的组件和应用程序，并保持系统补丁及时得到更新。
e) 应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞。
f) 应安装防病毒软件，并定期检查、查杀病毒以及升级病毒库。
g) 应部署板卡、内存等相关硬件校验措施，防止插入恶意板卡读取内存信息、硬件被刷新恶意系统镜像等硬件篡改攻击。
h) 应对关键网络设备、服务器等设备定期进行安全基线检查，并支持安全基线的管理、配置、更新，对违反安全基线配置要求的问题进行告警。

6.2.3.4 安全审计

本项要求包括：

a) 应对用户关键操作，如增/删账户、修改鉴权信息、修改关键配置、用户登录/注销、用户权限修改、重启/关闭设备、软件更新等行为进行记录。
b) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识、事件描述、结果等。
c) 审计记录应按有关法律法规要求进行超过一定期限的留存，定期备份并采取安全保护措施，避免在有效期内受到非授权的访问、篡改、覆盖或删除等。
d) 不应在日志中明文或弱加密记录敏感数据，如用户口令、未经脱敏处理的会话 ID 以及私钥等。

6.2.3.5 资源安全管控

本项要求包括：

a) 应限制单个用户或进程对系统资源的最大使用限度。
b) 应能够屏蔽虚拟资源故障，确保某个虚拟机崩溃后不影响虚拟机监视器及其他虚拟机运行。

c） 应保证虚拟机仅能使用为其分配的计算资源。
d） 当 VNFM 和 VIM 运行在虚拟机上时，应保证虚拟机的安全隔离。
e） VIM 不应与 VIM 管理的 NFVI 共享硬件和虚拟资源。
f） MANO 系统所在虚拟机和其他系统所在虚拟机应实现物理隔离，或根据安全需求采用独占模式。

6.2.4 数据安全要求

6.2.4.1 数据保护

本项要求包括：
a） 应保证重要数据在传输、虚拟机迁移等过程中的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。
b） 应采用数据加密技术，对传输的业务数据进行加密。
c） 应具备依据不同的传输信息，采用不同等级的加密保护能力。
d） 应采取技术措施保护业务相关数据安全，避免相关数据被篡改和破坏。
e） 应具备数据加密存储、数据加密传输模块，采用加密等安全方式存储和传输用户口令等身份鉴别信息，防止用户鉴别认证信息泄露而造成身份冒用。
f） 应对重要、敏感数据行分级分类处理，相关要求参考 2019-0216T-YD《基础电信企业数据分类分级方法》中的相关要求。
g） 针对不同网络域、不同用户、不同 VNF 和不同 VIM 之间的数据，应采取技术措施保证数据隔离。应支持基于虚拟内存等技术的内存隔离，为用户态进程提供完整的虚拟地址空间，防止攻击者劫持内核控制流。对于重要业务，应支持内存加密技术，对不同用户及业务采用不同加密算法或密钥进行信息保护。
h） 应具备身份认证机制和访问控制等安全机制保证数据库的安全访问；采取设置复杂的账户及口令，设置数据库安全白名单，拒绝匿名访问等加固措施。
i） 应具备数据加密能力，对重要敏感数据进行加密存储。
j） 应记录数据库操作日志。
k） 应具备技术手段，可以及时地发现针对数据库的违规操作行为并进行记录、报警。

6.2.4.2 数据备份恢复

本项要求包括：
a） 应提供重要业务及软件数据的本地数据备份与恢复功能，提供异地备份功能，可通过通信网络将重要数据备份到异地。
b） 应支持数据备份与恢复的配置，包括备份策略、备份数据一致性检验、备份位置查询等，且备份数据应采取与原数据保护强度一致的安全措施。

6.2.4.3 个人信息保护

本项要求包括：
a） 应遵循国家法律法规及有关部门对个人信息保护的相关规定。
b） 应仅采集和保存业务必需的用户个人信息。
c） 应禁止未授权访问和非法使用用户个人信息。

6.2.4.4 剩余信息保护

本项要求包括：
a） 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。