ICS 03.100.30

CCS L 70

团 体 标 准

T/CIITA 201.4-2021

城市轨道交通 自动售检票系统

第 4 部分：网络安全规范

Urban rail transit — automatic fare collection system —

part 4:Information security specifications

2021-11-09 发布

2021-12-08 实施

中国信息产业商会 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专利的责任。

T/CIITA 201 《城市轨道交通 自动售检票系统》由六个部分组成，本文件是第4部分。T/CIITA 201已经发布如下部分：

——第1部分：系统架构、业务规则及软件要求；

——第2部分：终端设备；

——第3部分：系统测试与检测；

——第4部分：网络安全规范；

——第5部分：互联互通要求；

——第6部分：安装施工规程。

本文件由中国信息产业商会团体标准委员会提出并归口。

本文件起草单位：北京中软万维网络技术有限公司、上海中软华腾软件系统有限公司、南京熊猫信息产业有限公司、上海华虹计通智能系统股份有限公司、方正国际软件（北京）有限公司、普天轨道交通技术（上海）有限公司、北京地铁科技发展有限公司、 深圳地铁建设集团有限公司、深信服科技股份有限公司、长春光华科技发展有限公司、青岛博宁福田智能交通科技发展有限公司、上海中铁通信信号测试有限公司、广州地铁设计研究院股份有限公司、北京东土科技股份有限公司、深圳市三旺通信股份有限公司、广州广电运通智能科技有限公司、北京天地和兴科技有限公司、北京尊冠科技有限公司、天津南大通用数据技术股份有限公司、苏州雷格特智能设备股份有限公司。

本文件主要起草人：杨巍、胡佳乐、唐晓闯、闫学文、黄亮哓、杨波、马涛、许翔、戴华、闫雷雷、钱鸣、赵玉军、张然、胡冰、陈鑫、王健、马怀清、吴博、李白、岳峰、余从海、冯秀波、陈鑫、张森、李沁龙、李铁根、邓顺义、陈波洲、高炜丽、金光宇、田雄军、马岚、金尚柏、陈峤、李道全、徐健洲、林杨。

本文件为T/CIITA 201.4的第一次修订。

引　言

新技术、新产品和业务需求的快速发展，为城市轨道交通自动售检票系统不断提出新的要求。为规范城市轨道交通自动售检票系统的新建、扩建、改建工作，特制定本文件。其深度和颗粒度高于国标《地铁设计规范》（GB50157-2013）、《城市轨道交通自动售检票系统技术条件》（GB/T20907-2007）的内容及要求，对新技术、新产品及业务需求的发展做了必要的补充和要求。目标是根据不同城市的实际情况，在实现AFC基本功能和性能要求的基础上，为智慧交通和智慧城市建设需要，制定保障运营业务需求和发展所需的技术条件和要求。补充的新兴技术应用内容，着力在产品化标准化方面做重点表述，以期促进AFC产品化、标准化进程。本文件拟由6部分构成。本分册是第4部分。

——第4部分：网络安全规范。目的在于根据国家网络安全等级保护原则结合AFC系统构成及运营管理要求，对AFC系统各部分的系统建设、运营管理做出网络安全规范性要求。

城市轨道交通 自动售检票系统

第 4 部分：网络安全规范

1 范围

本文件规定了城市轨道交通自动售检票系统网络安全架构、网络安全等级保护技术要求、网络安全等级保护管理要求、网络安全运营管理、网络安全测评功能要求和性能要求。

本文件适用于指导城市轨道交通自动售检票系统的新线建设、既有线路扩建、改建和运营。

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 信息安全技术信息系统安全等级保护定级指南；

GB/T 32399-2015 信息技术 云计算 参考架构

GB/T 35273 信息安全技术 个人信息安全规范

3 术语和定义

3.1

自动售检票系统 automatic fare collection

基于计算机、通信、网络、自动控制等技术，实现轨道交通售票、检票、计费、收费、统计、清分、管理等全过程的自动化系统。自动售检票系统，以下简称系统或简称AFC。

[来源：GB/T 50381-2018]

3.2

AFC 云平台 automatic fare collection cloud platform

为AFC软件提供云计算资源的平台。

3.3

自动售检票清分中心系统 AFC central clearing system

用于发行和管理城市轨道交通车票，对线网内不同线路的票、款进行结算和清算，并具有与城市轨道交通线网内乘用消费的其他付费卡进行清算功能的系统。

[来源：GB/T 50381-2018 有修改]

3.4

城市互联清分中心系统 urban interconnection AFC central clearing system

用于城市间轨道交通线网融合互联互通后，对不同票、款进行结算和清算的系统。

3.5

互联网票务系统 Internet Ticketing Platform

城市轨道交通企业在互联网票务使用、运营过程中提供各种管理功能的信息系统。

3.6

多线路中心系统 multiple line central system

用于管理和控制城市轨道交通多条线路自动售检票系统的计算机系统。

3.7

线路计算机系统 line computer system

用于监控和管理城市轨道交通单线路自动售检票系统的计算机系统。

[来源：GB/T 50381-2018 有修改]

3.8

车站计算机系统 station computer system

用于车站级票务管理、运行管理和客流统计的计算机系统。

[来源：GB/T 50381-2018]

3.9

车站终端设备 station level equipment

安装在城市轨道交通线路各车站，进行车票发售、进站检票、出站检票、充值、验票分析等交易处理的设备。

[来源：GB/T 50381-2018 有修改]

3.10

乘车凭证 riding pass

乘客乘坐轨道交通的凭证载体。

3.11

云计算 cloud computing

一种通过网络将可伸缩、弹性的共享物理和虚拟资源池以按需自服务的方式供应和管理的模式。

[来源：GB/T 32400-2015]

3.12

云服务 cloud service

通过云计算已定义的接口提供的一种或多种能力。

[来源：GB/T 32400-2015]

3.13

微服务 microservice

一种云原生架构方法，其中单个应用程序由许多松散耦合且可独立部署的较小组件或服务组成。

3.14

容器化 containerization

以统一的方式打包应用程序以及依赖包到一个可移植的容器中。

3.15

敏捷开发 agile development

以用户的需求进化为核心，采用迭代、循序渐进的方法进行软件开发。

3.16

银联ODA清算中心系统 unionpay oda central clearing system

负责银联IC卡联机ODA交易的收单、支付、清算业务的系统。

3.17

自动检票机 automatic gate machine

对车票进行自动检验和处理，放行或阻挡乘客出入付费区的设备。自动检票机分进站检票机、出站检票机和双向检票机三种类型。

[来源：GB/T 50381-2018 有修改]

3.18

多功能自助票务终端 multi function self service ticketing terminal

具备票务自助处理、票务查询、信息咨询服务、开具电子发票功能，用于部分替代车站票务客服人员工作。

3.19

读写器 ticket reader-writer

安装在自动售票机、自动补票机、半自动售票机、自动检票机、边门闸机、移动检票机、自动查询机、便携式检验票机、多功能自助票务终端、智慧客服等设备中，用于对车票的发售、检票、充值、验票分析作读写处理的设备。

3.20

黑名单 blacklist

根据管理要求对挂失车票和异常车票进行特殊控制的数据列表。

[来源：GB/T 50381-2018]

3.21

互联网票务 internet ticketing

基于各种新型的媒体（二维码、NFC虚拟卡、生物特征等），利用互联网实现的虚拟化、数字票种（或乘车凭证）。

3.22

互联网票务系统 internet ticketing system

城市轨道交通企业在互联网票务使用、运营过程中提供各种管理功能的信息系统。

3.23

生物特征识别 biometric recognition

基于个人的行为特征和生物学特征，对该个体进行的自动识别。

[来源：GB/T 26238-2010]

3.24

密钥 key

一种用于控制密码变换操作（如加密、解密、密码校验函数计算、签名产生或签名验证）的符号序列。

[来源：GB/T 17901.1-2020]

3.25

安全存取模块 security access module

一种能够提供必要的安全机制，以防外界对终端所储存或处理的安全数据进行非法攻击的硬件加密模块，简称SAM。

[来源：GB/T 50381-2018]

3.26

初始化 initialization

在车票投入运行前，为保证其在本系统内正常使用，需对其进行初始格式、发行及应用信息写入的过程。

[来源：GB/T 50381-2018]

3.27

进站 entry

从非付费区到付费区通过的行为。

[来源：GB/T 50381-2018]

3.28

出站 exit

从付费区到非付费区通过的行为。

[来源：GB/T 50381-2018]

3.29

单程票 single journey ticket

在限定时间内一次性使用的车票。

[来源：GB/T 50381-2018]

3.30

储值票 storage value ticket

具有储值功能，可重复充值使用的车票。

[来源：GB/T 50381-2018]

4 缩略语

下列缩略语适用于本文件。

ACC:自动售检票的清分中心(AFC Clearing Center)

ACL：访问控制列表（Access Control List）

AD：活动目录（Active Directory）

AFC：自动售检票系统(Automatic Fare Collection)

AP：无线访问接入点（Wireless Access Point）

API：应用程序编程接口（Application Programming Inteface）

APP：手机的应用软件（Application）

APT：高级持续性威胁（Advanced Persistent Threat）

ARP：地址解析协议（Address Resolution Protocol）

AV：防病毒（Anti Virus）

CA：数字证书认证中心（Certificate Authority）

CPU：中央处理器（Central Processing Unit）

DDoS：分布式拒绝服务（Distributed Denial of Service）

DF：设备错误（Device Fault）

DNS：域名系统（Domain Name System）

EC：纠删码（Erasure Coding）

FTP：文件传输协议（File Transfer Protocol）

GRE：通用路由封装（Generic Routing Encapsulation）

HA：高可用性（High Availability）

IO：输入/输出（Input/Output）

IP：互联网协议（Internet Protocol）

IPS：入侵防御系统（Intrusion Prevention System）

IT：信息技术（Information Technology）

LTE：长期演进（Long Term Evolution）

MAC：媒体访问控制（Media Access Control）

NAS：网络附属存储（Network Attached Storage）

ODBC：开放数据库连接（Open DataBase Connectivity）

Oday：已经被发现而官方还没有相关补丁的漏洞

PXE： 预启动执行环境(Preboot eXecution Environment)

RTP：实时传输协议（Real-time Transport Protocol）

SaaS：软件即服务（Software as a Service）

IaaS：基础设施即服务（Infrastructure as a Service）

PaaS：平台即服务（Platform as a Service）

SDN：软件定义网络（Software Defined Network）

SQL：结构化查询语言（Structured Query Language）

SSD：固态盘（Solid State Drives）

SSL：安全套接字协议（Secure Sockets Layer）

TB：太字节（TeraByte）

UE：用户设备（User Equipment）

USB：通用串行总线（Universal Serial Bus）

VDC：虚拟数据中心（Virtual Data Center）

VLAN：虚拟局域网（Virtual Local Area Network）

VM：虚拟机（Virtual Machine）

VPC：虚拟专有云（Virtual Private Cloud）

VPN：虚拟专用网（Virtual Private Network）

PPI：像素每英寸（Pixel Per Inch）

5 一般规定

基本原则：

城市轨道交通自动售检票系统兼容创新系统设计的原则包括：

a) 系统设计需要满足“数据自主、技术自主、风险可控”的基本原则。必须不断完善自主可控产业体系，积极推进国产基础软硬件的集成适配和解决方案研发，联合产业内合作伙伴打造安全可控产业生态体系；

b) 应按自动售检票系统的安全需求，构建保证信息系统可用性、完整性和保密性的平台和安全保证体系，确保自动售检票系统的业务安全；

c) 遵循“系统自保、平台统保、边界防护、等保达标、安全确保”的策略，以网络安全等级保护为基础，分级分类建立安全保护措施；

d) 应采用带外管理技术构建安全管理域，支持对自动售检票系统的安全集中管控；

e) 应实现自动售检票系统的安全态势感知，可对车站、多线路中心/单线路中心系统、清分清算中心系统设备进行持续监控；

f) 自动售检票系统安全审计日志留存期不少于六个月；

g) 应部署时钟同步服务系统，开启时钟同步服务；

h) 自动售检票系统设备使用应优先选择国产自主产品，使用前应通过第三方检测机构的安全性检测。

6 系统网络架构

6.1 AFC 系统网络架构

城市轨道交通AFC系统架构应包含五层，第第一层为线网中心（清分中心）系统（ACC）和互联网票务系统（ITS），第二层为多线路中心/单线路中心系统（MLC/LC），第三层为车站系统（SC），第四层为终端设备（SLE），第五层为乘车凭证。AFC系统架构示意见图 1。

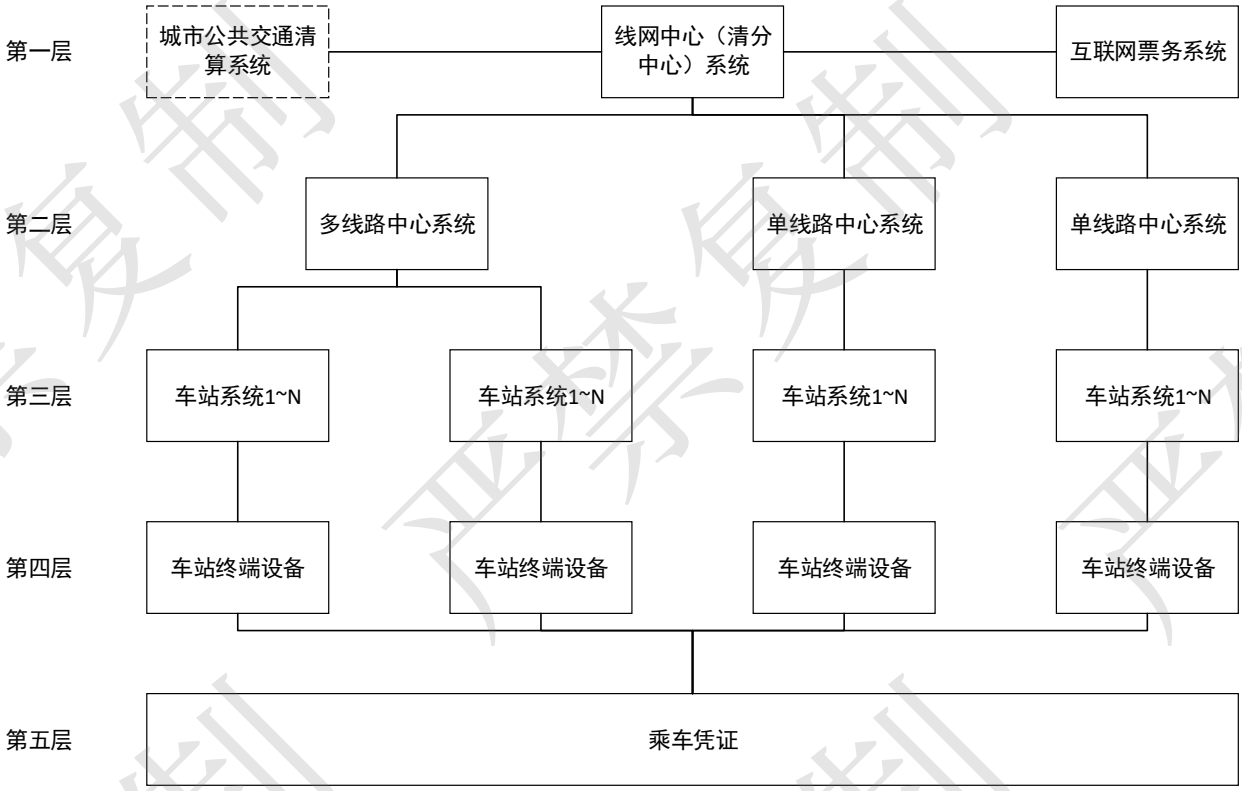

图1　AFC 系统架构示意图

自动售检票系统分为车票、终端、车站系统、多线路中心/单线路中心系统、清分中心5层架构。基于传统的5层架构，应按车站、多线路中心/单线路中心系统、清分清算中心构建安全域，建立纵向防护机制。互联网售票平台应与各个子系统进行物理隔离，独立构建安全域。线网中心系统（清分中心系统）和互联网平台应按照等保三级要求建设；多多线路中心/单线路中心系统（单多线路中心/单线路中心系统）系统宜按照等保三级要求建设；车站系统宜按照等保二级要求建设。

6.2　AFC 云平台系统架构

当轨道交通 AFC 系统需新建或迁移至云计算平台时，宜将第一层、第二层系统部署在云计算平台，车站系统可在云计算平台部署，也可保留在车站本地部署。AFC 系统云部署架构分为两类：1、第一、二层部署于 AFC 云平台；2、第一、二、三层部署于 AFC 云平台。AFC 系统云部署架构示意如图 2。

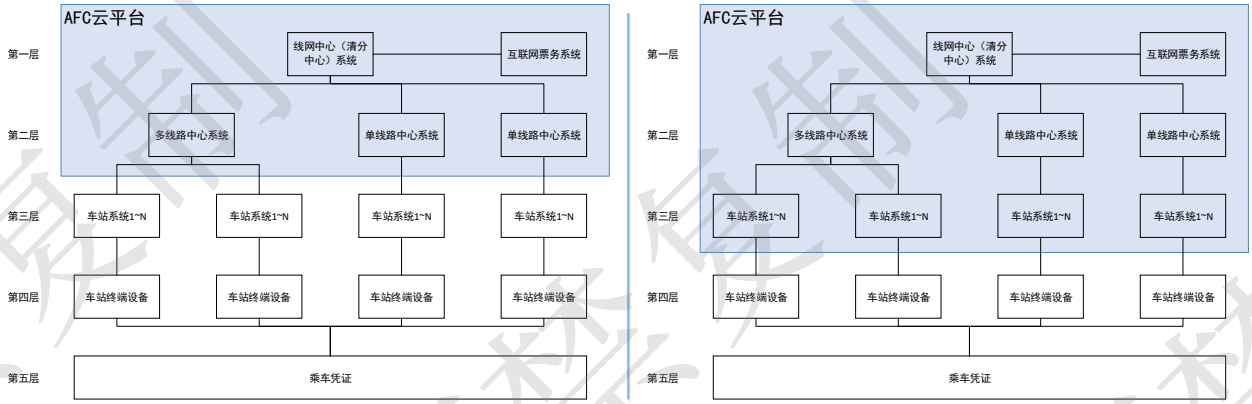

图2　AFC 系统云部署架构示意图

当轨道交通AFC系统需新建或迁移至云计算平台时，则整体AFC系统建设统一的安全防护体系，并且设计中心云化部分与车站非云化部分的网络安全边界，整体网络安全管理需在云上部署。建设中心云化部分按照等保三级进行网络安全建设，车站非云化部分按照等保二级进行建设。可将要求包括：

a) 采用云平台的自动售检票系统，车站级的自动售票机、自动检票机、半自动售票机及车票编码分拣等设备应独立部署；

b) 应为互联网售检票系统设置独立的安全域，与车站系统、清分清算系统进行数据交互时应通过物理隔离设备进行数据传输；

c) 云平台是云计算基础设施及其上的服务软件的集合。自动售检票系统可以采用云平台；

d) 云平台主要由服务器、磁盘阵列、交换机、防火墙等硬件及配套的软件及服务组成；

e) 云平台的边界主要包括内部的防火墙、交换机、服务器及互联的传输等硬界面及平台内部虚机之间、容器之间、业务或服务之间的软界面和外部的业务安全、访问安全、服务安全、授权安全、系统安全等服务面；

f) 云平台宜采用双活、主备等灾备机制宜增加相应的接口扩展及必要的切换过程的安全机制和安全界面。同时宜根据相关标准辅以物理安全等必要的安全边界。

7　网络安全技术要求

7.1　清分中心线网络安全保护要求

7.1.1　清分中心网络安全等级保护要求

7.1.1.1　总则

清分中心的网络安全建设符合GB/T 22239—2019 第三级系统的要求及结合AFC系统的特点

7.1.1.2　安全物理环境

7.1.1.2.1　物理位置的选择

清分中心机房场地应远离产生粉尘、油烟、有害气体以及生产或贮存危险品的场所。

7.1.1.2.2　物理访问控制

外部人员访问清分中心主机房前应发起申请，经过审批后由机房管理人员全程陪同并保留相关审批、访问记录。

7.1.1.2.3　防盗窃和防破坏

应在必要情况下对主机房出入人员携带的物品进行检查。

7.1.1.2.4　防静电

辅助区内的工作台面可采用导静电或静电耗散材料。

7.1.1.2.5　温湿度控制

应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。冷通道或机柜进风区域的温度应不高于27℃，相对湿度不大于60%。在停机时，主机房环境温度应不高于45℃，相对湿度应不高于80%。

7.1.1.2.6　电磁防护

电磁防护要求如下：

a)　可采用屏蔽布线系统、光缆布线系统或建筑屏蔽等技术手段实现，当采用屏蔽布线系统时，应保证链路全程屏蔽以及屏蔽层可靠接地；

b) 可对清分中心机房中关键设施实施电磁屏蔽。

7.1.1.3 安全通信网络

7.1.1.3.1 网络架构

网络架构要求包括：

a) 应保证网络设备的业务处理能力满足业务高峰期的需要，应保证关键网络设备（如核心交换机、清分中心与多线路中心/单线路中心系统，互联网票务系统之间的路由器）等资源使用率不超过60%；

b) 应保证网络各个部分的带宽满足业务高峰期需要，应保证清分中心与多线路中心/单线路中心系统之间、清分中心与互联网票务系统之间链路带宽使用率不超过70%；

c) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址，至少应划分不同的区域并为每个区域划分独立的VLAN；

d) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；

e) 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。应保证清分中心与多线路中心/单线路中心系统之间、清分中心与互联网票务系统之间网络设备冗余部署。

7.1.1.3.2 通信传输

通信传输要求包括：

a) 应对清分中心与多线路中心/单线路中心系统之间通信在网络层传输过程中进行完整性保护；

b) 应对清分中心与多线路中心/单线路中心系统、互联网票务系统之间通信在网络层传输过程中采用密码技术保证数据的保密性。

7.1.1.4 安全区域边界

7.1.1.4.1 边界防护

边界防护要求包括：

a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信，应对清分中心与多线路中心/单线路中心系统、清分中心与互联网票务系统之间交互仅通过通信前置机，同时应对上述边界设备接口状态进行检测；

b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制，应关闭网络设备、安全设备、计算设备的闲置端口，同时应采用如802.1x等方式对接入设备进行认证；

c) 应能够对内部用户非授权联到外部网络的行为进行检查或限制，应限制计算设备利用多余网卡、USB网卡访问外部网络；

d) 清分中心不应设置无线网络。

7.1.1.4.2 入侵防范

入侵防范要求包括：

a) 应在清分中心与多线路中心/单线路中心系统、清分中心与互联网票务系统边界处部署能够检测、防止或限制从外部发起的网络攻击行为的设备，并对攻击源进行限制；

b) 应在清分中心内部署具有能够检测、防止或限制从内部发起网络攻击行为的设备，并对攻击源进行限制；

c) 应在清分中心安全运维区域部署抗APT系统、安全态势感知等基于流量或设备日志对网络行为进行分析的设备，实现对网络攻击特别是新型网络攻击行为的分析。

7.1.1.4.3 恶意代码和垃圾邮件防范

恶意代码和垃圾邮件防范要求包括：

应在关键网络节点处部署基于流量进行分析恶意代码行为并限制的设备，并维护恶意代码防护机制的升级和更新。

7.1.1.5 安全计算环境

7.1.1.5.1 身份鉴别

身份鉴别要求包括：

a) 计算设备应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换，相关安全策略不应低于以下要求：

1) 用户口令长度不少于8位，应包含字母、数字、特殊符号混合排列；

2) 用户口令更换周期不大于180天；

3) 用户首次登录计算设备时应强制修改默认口令。

b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施，相关安全策略不应低于以下要求：

1) 非法登录次数应不超过5次；

2) 超过非法登录次数后应采取锁定账户或IP的措施，锁定时间应不少于5min；

3) 登录连接超时时间应不超过30min,超过后应采取强制注销等措施；

c) 应用系统或未提供多种鉴别技术的计算设备应仅通过开启两种或两种以上组合的鉴别技术的运维审计系统进行各类操作。

7.1.1.5.2 访问控制

访问控制要求包括：

应定期检查账户及权限的分配情况，并及时删除或停用多余的、过期的账户。

7.1.1.5.3 入侵防范

入侵防范要求包括：

a) 操作系统、网络设备、安全设备应遵循最小安装的原则，仅安装需要的组件和应用程序；

b) 操作系统、网络设备、安全设备应关闭不需要的系统服务、默认共享和高危端口；

c) 操作系统、网络设备、安全设备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；

d) 业务应用系统应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

e) 应定期对清分中心内计算设备进行检查，能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；

f) 操作系统、网络设备、安全设备应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警；

g) 清分中心中应部署时钟服务器，同时对NTP协议启用验证功能。

7.1.1.5.4 恶意代码防范

操作系统应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。同时应每月更新恶意代码库。

7.1.1.5.5 数据完整性

数据完整性要求包括：

a) 业务应用系统、数据库管理系统、中间件应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

b) 业务应用系统、数据库管理系统、中间件应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

7.1.1.5.6 数据保密性

数据保密性要求包括：

a) 业务应用系统、数据库管理系统、中间件应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；

b) 业务应用系统、数据库管理系统、中间件、操作系统应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

7.1.1.5.7 剩余信息保护

剩余信息保护要求包括：

a) 操作系统、业务应用系统、数据库管理系统、中间件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；

b) 操作系统、业务应用系统、数据库管理系统、中间件应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

7.1.1.5.8 个人信息保护

个人信息保护要求包括：

a) 业务应用系统和数据库管理系统应仅采集和保存用户个人信息；

b) 业务应用系统和数据库管理系统应禁止未授权访问和非法使用用户个人信息。

7.1.1.6 安全管理中心

清分中心安全系统应该独立设置安全管理中心。在清分系统网络中新建安全管理域，选型部署安全管理平台，实现网络设备、安全设备、服务器等系统的运行状态进行集中监测，安全系统配置集中管理、安全事件识别、报警、分析与可视化，安全策略、恶意代码、补丁升级等安全相关事项

的集中管理；选型部署日志审计系统，实现全网主机系统告警日志与审计日志的集中收集、存储，保留时间不少于六个月。通过堡垒主机系统部署解决清分系统网络中各系统管理员、审计管理员、安全管理员通过统一方式登录系统时进行身份鉴别与操作行为安全审计。

集中管控：

a) 划分特定的管理区域，在保证信息传输路径安全可靠的前提下，对网络中的设备、系统、资源进行集中管控，实时监测、分析网络的运行情况，能及时对各种网络安全事件进行处理；

b) 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；

c) 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；

d) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；

e) 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；

f) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；

g) 应能对网络中发生的各类安全事件进行识别、报警和分析。

7.1.2 清分中心网络安全建设要求

7.1.2.1 清分中心边界防护建设要求

清分中心边界防护建设要求如下：

a) 清分中心与互联网票务系统边界处应具备以下功能：链路负载均衡功能；通信链路加密功能；基于五元组、数据流、应用协议的访问控制；入侵检测与防御功能；基于流量和日志的未知威胁检测；流量清洗功能；

b) 清分中心与互联网票务系统边界建议部署以下产品或服务：链路负载均衡设备、使用软件定义边界技术的产品、防火墙、入侵检测/防御设备、WEB 应用防火墙、态势感知平台、抗DDoS 产品或服务；

c) 互联网票务系统互联网票务系统清分中心与多线路中心/单线路中心系统应具备以下功能：基于五元组、数据流、应用协议的访问控制；入侵行为检测与防御功能；基于流量和日志的未知威胁检测；

d) 清分中心与多线路中心/单线路中心系统边界建议部署以下产品或服务：防火墙、入侵检测/防御设备、态势感知平台；

e) 清分中心的业务区域与其他区域的边界应具备以下功能：应用负载均衡功能；应用传输加密功能；基于五元组、数据流、应用协议的访问控制；入侵行为检测与防御功能；基于流量和日志的未知威胁检测；

f) 清分中心的业务区域与其他区域的边界建议部署以下产品或服务：应用负载均衡设备、SSL安全网关、防火墙、Web应用防火墙、入侵检测/防御设备、态势感知平台；

g) 清分中心与其他区域的边界应对串行接入设备采用冗余部署。

7.1.2.2 清分中心安全计算环境建设要求

清分中心安全计算环境建设要求如下：

a) 清分中心应具备针对应用的数据库进行安全审计的能力，应部署数据库审计设备；

b) 清分中心应具备针对终端设备恶意代码防范和终端管控的能力，部署终端安全管理设备及终端防病毒设备；

c) 清分中心应具备保证应用数据传输过程中完整性和保密性的能力，应部署SSL安全网关类设备；

d) 清分中心应具备对应用中数据安全管理的能力，对重要数据及敏感数据进行管控，应在安全管理中心部署数据库脱敏设备和数据库加密设备。

7.1.2.3 清分中心安全管理中心建设要求

清分中心安全管理中心建设要求如下：

a) 安全管理中心应具备安全运维管理的能力，应在安全管理中心部署运维堡垒机；

b) 安全管理中心应具备漏洞管理的能力，能够针对全网脆弱性问题等进行扫描发现和跟踪管理，应在安全管理中心部署漏洞扫描设备；

c) 安全管理中心应具备安全态势管理、事件管理、分析风险、计算风险、应对风险的能力，应在安全管理中心部署安全态势感知平台；

d) 安全管理中心应具备针对各类终端进行授权、识别、认证、管控的能力，应在安全管理中心部署终端准入管控设备；

e) 安全管理应具备用户身份管理能力，应具备针对用户进行授权、认证、管控、审计功能，应在安全管理中心部署统一身份认证管理平台，相关组件应满足国家密码管理部门的相关要求。

7.2 多线路中心/单线路中心系统信息安全保护要求

7.2.1 多线路中心/单线路中心系统网络安全等级保护要求

7.2.1.1 总则

多线路中心/单线路中心系统的网络安全建设将按照GB/T 22239-2019 中第三级系统的要求及结合AFC系统的特点

7.2.1.2 安全物理环境

7.2.1.2.1 物理位置的选择

多线路中心/单线路中心机房场地应远离产生粉尘、油烟、有害气体以及生产或贮存危险品的场所。

7.2.1.2.2 物理访问控制

外部人员访问多线路中心/单线路中心机房前应发起申请，经过审批后由机房管理人员全程陪同并保留相关审批、访问记录。

7.2.1.2.3 防盗窃和防破坏

应在必要情况下对主机房出入人员携带的物品进行检查。

7.2.1.2.4 防静电

辅助区内的工作台面可采用导静电或静电耗散材料。

7.2.1.2.5 温湿度控制

应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。冷通道或机柜进风区域的温度应不高于27℃，相对湿度不大于60%。在停机时，主机房环境温度应不高于45℃，相对湿度应不高于80%。

7.2.1.2.6 电磁防护

电磁防护要求如下：

c) 可采用屏蔽布线系统、光缆布线系统或建筑屏蔽等技术手段实现，当采用屏蔽布线系统时，应保证链路全程屏蔽以及屏蔽层可靠接地；

d) 可对多线路中心/单线路中心机房机房中关键设施实施电磁屏蔽。

7.2.1.3 安全通信网络

7.2.1.3.1 网络架构

网络架构要求包括：

f) 应保证网络设备的业务处理能力满足业务高峰期的需要，应保证关键网络设备（如核心交换机、多线路中心/单线路中心系统与车站系统的路由器）等资源使用率不超过60%；

g) 应保证网络各个部分的带宽满足业务高峰期需要，应保证多线路中心/单线路中心系统与车站系统之间链路带宽使用率不超过70%；

h) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址，至少应划为不同区域并为每个区域划分独立的VLAN；

i) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；

j) 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。应保证多线路中心/单线路中心系统与车站系统之间网络设备冗余部署。

7.2.1.3.2 通信传输

应对多线路中心/单线路中心系统与车站系统之间通信传输在网络层进行完整性保护。

7.2.1.4 安全区域边界

7.2.1.4.1 边界防护

边界防护要求包括：

a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信，应对多线路中心/单线路中心系统与车站系统之间交互仅通过通信前置机，同时应对上述边界设备接口状态进行检测；

b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制，应关闭网络设备、安全设备、计算设备的闲置端口，同时应采用如802.1x等方式对接入设备进行认证；

c) 应能够对内部用户非授权联到外部网络的行为进行检查或限制，应限制计算设备利用多余网卡、USB网卡访问外部网络；

d) 多线路中心/单线路中心系统不应设置无线网络。

7.2.1.4.2 入侵防范

入侵防范要求包括：

a) 应在多线路中心/单线路中心系统与车站系统边界处部署能够检测、防止或限制从外部发起的网络攻击行为的设备，并对攻击源进行限制；

b) 应在多线路中心/单线路中心系统内部署具有能够检测、防止或限制从内部发起网络攻击行为的设备，并对攻击源进行限制；

c) 应在多线路中心/单线路中心系统安全运维区域部署抗APT系统、安全态势感知等基于流量或设备日志对网络行为进行分析的设备，实现对网络攻击特别是新型网络攻击行为的分析。

7.2.1.4.3 恶意代码和垃圾邮件防范

应在关键网络节点处部署基于流量进行分析恶意代码行为并限制的设备，并维护恶意代码防护机制的升级和更新。

7.2.1.5 安全计算环境

7.2.1.5.1 身份鉴别

身份鉴别要求包括：

a) 计算设备应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换，相关安全策略不应低于以下要求:

1) 用户口令长度不少于8位，应包含字母、数字、特殊符号混合排列；

2) 用户口令更换周期不大于180天；

3) 用户首次登录计算设备时应强制修改默认口令。

b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施，相关安全策略不应低于以下要求：

1) 非法登录次数应不超过5次；

2) 超过非法登录次数后应采取锁定账户或IP的措施，锁定时间应不少于5min；

3) 登录连接超时时间应不超过30min，超过后应采取强制注销等措施。

c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

7.2.1.5.2 入侵防范

入侵防范要求包括：

a) 操作系统、网络设备、安全设备应遵循最小安装的原则，仅安装需要的组件和应用程序；

b) 操作系统、网络设备、安全设备应关闭不需要的系统服务、默认共享和高危端口；

c) 操作系统、网络设备、安全设备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；

d) 业务应用系统应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

e) 应定期对清分中心内计算设备进行检查，能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。

7.2.1.5.3 恶意代码防范

操作系统应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。同时应每月更新恶意代码库。

7.2.1.5.4 数据完整性

数据完整性要求包括：

a) 业务应用系统、数据库管理系统、中间件应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；

b) 业务应用系统、数据库管理系统、中间件、操作系统应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

7.2.1.5.5 剩余信息保护

剩余信息保护要求包括：

a) 操作系统、业务应用系统、数据库管理系统、中间件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；

b) 操作系统、业务应用系统、数据库管理系统、中间件应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

7.2.1.5.6 个人信息保护

个人信息保护要求包括：

a) 业务应用系统和数据库管理系统应仅采集和保存用户个人信息；

b) 业务应用系统和数据库管理系统应禁止未授权访问和非法使用用户个人信息。

7.2.1.6 安全管理中心

AFC系统线路安全系统应该独立设置安全管理中心。各线路的多线路中心/单线路中心系统应与本线路的各个车站共同建立统一的安全管理中心。在AFC系统网络中新建安全管理域，选型部署安全管理平台，实现网络设备、安全设备、服务器等系统的运行状态进行集中监测，安全系统配置集中管理、安全事件识别、报警、分析与可视化，安全策略、恶意代码、补丁升级等安全相关事项的集中管理；选型部署日志审计系统，实现全网主机系统告警日志与审计日志的集中收集、存储，保留时间不少于六个月。通过堡垒主机系统部署解决AFC系统网络中各系统管理员、审计管理员、安全管理员通过统一方式登录系统时进行身份鉴别与操作行为安全审计。

7.2.1.6.1 系统管理

系统管理要求包括：

a) 应对AFC多线路中心/单线路中心系统管理员进行身份鉴别，只允许其通过

b) 应通过清分中心管理员对清分中心的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、 系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

7.2.1.6.2 审计管理

a) 只允许审计管理员对审计记录进行分析、管理等操作，并对审计管理员进行身份鉴别，对其执行的操作进行管理与审计；

b) 应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略 对审计记录进行存储、管理和查询等。

7.2.2 线路网络安全建设要求

7.2.2.1 多线路中心/单线路中心系统边界防护建设要求

多线路中心/单线路中心系统边界防护建设要求如下：

a) 清分中心与多线路中心/单线路中心系统应具备以下功能：基于五元组、数据流、应用协议的访问控制；入侵行为检测与防御功能；基于流量和日志的未知威胁检测；

b) 清分中心与多线路中心/单线路中心系统边界建议部署以下产品或服务：防火墙、入侵检测/防御设备、态势感知平台；

c) 多线路中心/单线路中心系统与车站系统边界应具备以下功能：基于五元组、数据流、应用协议的访问控制；入侵行为检测与防御功能；基于流量和日志的未知威胁检测；

d) 多线路中心/单线路中心系统与车站系统边界建议部署以下产品或服务：防火墙、入侵检测/防御设备、态势感知平台；

e) 多线路中心/单线路中心系统的业务区域与其他区域的边界应具备以下功能：应用负载均衡功能；应用传输加密功能；基于五元组、数据流、应用协议的访问控制；入侵行为检测与防御功能；基于流量和日志的未知威胁检测；

f) 多线路中心/单线路中心系统的业务区域与其他区域的边界建议部署以下产品或服务：应用负载均衡设备、SSL安全网关、防火墙、Web应用防火墙、入侵检测/防御设备、态势感知平台；

g) 多线路中心/单线路中心系统的边界宜对串行接入设备采用冗余部署。

7.2.2.2 多线路中心/单线路中心系统安全计算环境建设要求

多线路中心/单线路中心系统安全计算环境建设要求如下：

a) 多线路中心/单线路中心系统应具备针对应用的数据库进行安全审计的能力，应部署数据库审计设备；

b) 多线路中心/单线路中心系统应具备针对终端设备恶意代码防范和终端管控的能力，部署终端安全管理设备及终端防病毒设备；

c) 多线路中心/单线路中心系统应具备保证应用数据传输过程中完整性和保密性的能力，应部署SSL安全网关类设备；

d) 多线路中心/单线路中心系统应具备对应用中数据安全管理的能力，对重要数据及敏感数据进行管控，应在安全管理中心部署数据库脱敏设备和数据库加密设备。

7.2.2.3 多线路中心/单线路中心系统安全管理中心建设要求

多线路中心/单线路中心系统安全管理中心建设要求如下：

a) 安全管理中心应具备安全运维管理的能力，宜在安全管理中心部署运维堡垒机；

b) 安全管理中心应具备漏洞管理的能力，能够针对全网脆弱性问题等进行扫描发现和跟踪管理，宜在安全管理中心部署漏洞扫描设备；

c) 安全管理中心应具备安全态势管理、事件管理、分析风险、计算风险、应对风险的能力，宜在安全管理中心部署安全态势感知平台。宜能够与清分中心的安全态势感知平台对接；

d) 安全管理中心应具备针对各类终端进行授权、识别、认证、管控的能力，宜在安全管理中心部署终端准入管控设备；

e) 安全管理应具备用户身份管理能力，宜具备针对用户进行授权、认证、管控、审计功能，应在安全管理中心部署统一身份认证管理平台，宜能够与清分中心的统一身份认证管理平台对接，相关组件应满足国家密码管理部门的相关要求。

7.3 车站系统信息安全保护要求

7.3.1 车站系统网络安全等级保护要求

7.3.1.1 总则

车站系统作为AFC系统的一部分，在AFC系统的网络安全建设中一般作为系统的一部分开展。在本规范中，车站系统的网络安全建设将参照GB/T 22239-2019《网络安全技术 网络安全等级保护基本要求》中第二级系统的要求及AFC系统的特点。

7.3.1.2 安全物理环境

7.3.1.2.1 物理位置选择

物理位置选择要求包括：

a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；

b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。

7.3.1.2.2 物理访问控制

物理访问控制要求包括：

机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。

7.3.1.2.3 防盗窃和防破坏

防盗窃和防破坏要求包括：

a） 应将设备或主要部件进行固定，并设置明显的不易除去的标识；

b） 应将通信线缆铺设在隐蔽安全处；

c） 应设置机房防盗报警系统或设置有专人值守的视频监控系统。

7.3.1.2.4 防雷击

防雷击要求包括：

a） 应将各类机柜、设施和设备等通过接地系统安全接地；

b） 应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。

7.3.1.2.5 防火

防火要求包括：

a） 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；

b） 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；

c） 应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。

7.3.1.2.6 防水和防潮

防水和防潮要求包括：

a） 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

b） 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；

c） 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

7.3.1.2.7 防静电

防静电要求包括：

a） 应采用防静电地板或地面并采用必要的接地防静电措施；

b） 应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。

7.3.1.2.8 温湿度控制

应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

7.3.1.2.9 电力供应

电力供应要求包括：

a) 应在机房供电线路上配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，至少满足设备在断电情况下的正常运行要求；

c) 应设置冗余或并行的电力电缆线路为计算机系统供电。

7.3.1.2.10 电磁防护

电磁防护要求包括：

a) 电源线和通信线缆可隔离铺设，避免互相干扰；

b) 可对关键设备实施电磁屏蔽。

7.3.1.3 安全通信网络

7.3.1.3.1 网络架构

网络架构要求包括：

a) 应保证 SC 层网络设备的业务处理能力满足业务高峰期（上班高峰期、节假日等）需要；

c) 应保证 SC 层网络各个部分的带宽满足业务高峰期需要；

d) 应划分不同的网络区域，建议分为 PC 操作站域、SC 服务器域、SLE 终端域，并按照方便管理和控制的原则为各网络区域分配地址，建议固定 IP 地址，便于后期管理；

e) 应保证 SC 层局域网通过入侵检测系统、威胁检测探针等技术手段，对汇集核心交换机的流量进行实时监测，发现潜伏的安全风险能够联动安全管理中心进行预警、评估和处置的闭环；

f) 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。

7.3.1.3.2 通信传输

通信传输要求包括：

a） 应采用校验技术或密码技术保证通信过程中数据的完整性；

b） 应采用密码技术保证通信过程中数据的保密性。

7.3.1.4 安全区域边界

7.3.1.4.1 边界防护

边界防护要求包括：

a） 应保证跨越边界的访问和数据流通过边界防护设备（如：防火墙、网闸）提供的受控接口进行通信；

b） 应能够对非授权设备私自联到内部网络的行为进行检查或限制；

c） 应能够对内部用户非授权联到外部网络的行为进行检查或限制；

d） 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络；

e） 应保证 SC 层局域网与 MLC/LC 层通过边界防护设备（如：防火墙）提供的受控接口进行通信。

7.3.1.4.2 访问控制

访问控制要求包括：

a） 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；

b） 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

c） 应基于实时网络安全状态进行态势分析和研判，对于突发性攻击或 0day 攻击，访问控制系统可以联动安全管理中心实现安全策略的智能匹配，及时阻断；

d） 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。

7.3.1.4.3 应用层防护

应用层防护要求包括：

a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；

b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；

c) 应用层防护功能应集成融合多个功能模块，包括 ACL、入侵防御系统、恶意代码和垃圾邮件防范、防病毒等，融合安全，节省硬件投入成本。

7.3.1.5 安全计算环境

7.3.1.5.1 身份鉴别

身份鉴别要求包括：

a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

c) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

7.3.1.5.2 访问控制

访问控制要求包括：

a) 应对登录的用户分配账户和权限；

b) 应授予管理用户所需的最小权限，实现管理用户的权限分离；

c) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；

d) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。

7.3.1.5.3 安全审计

安全审计要求包括：

a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

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；

c） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

d） 应对审计进程进行保护，防止未经授权的中断。

7.3.1.5.4 入侵防范

入侵防范要求包括：

a） 应遵循最小安装的原则，仅安装需要的组件和应用程序；

b） 应关闭不需要的系统服务、默认共享和高危端口；

c） 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；

d） 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

e） 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；

f） 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

7.3.1.5.5 恶意代码防范

a） 应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断；

b） 应在 PC 操作站、SC 服务器、SLE 终端均需要安装防病毒或恶意代码防范系统，基于病毒扫描、进程白名单、U 盘白名单等技术手段做好终端侧的安全防范；防病毒或恶意代码防范系统应采用轻量级代理，不宜加载全量的病毒库文件，应采用后端管理平台统一管理、升级及病毒更新。

7.3.1.6 安全管理中心

安全管理中心要求包括：

结合 6.2.5 安全管理中心要求，车站系统应与多线路中心/单线路中心系统建立统一的安全管理系统。

7.3.2 车站网络安全建设要求

7.3.2.1 车站系统边界防护建设要求

多线路中心/单线路中心系统边界防护建设要求如下：

a) 多线路中心/单线路中心系统与车站系统边界应具备以下功能：基于五元组、数据流、应用协议的访问控制；入侵行为检测与防御功能；基于流量和日志的未知威胁检测；

b) 多线路中心/单线路中心系统与车站系统边界建议部署以下产品或服务：防火墙、入侵检测/防御设备、态势感知平台；

c) 车站系统的边界应对串行接入设备采用冗余部署。

7.3.2.2 车站系统安全计算环境建设要求

车站系统安全计算环境建设要求如下：

a) 车站系统应具备针对终端设备恶意代码防范和终端管控的能力，部署终端安全管理设备及终端防病毒设备。

7.4 互联网票务系统网络安全保护要求

7.4.1 互联网票务系统互联网票务系统网络安全等级保护要求

7.4.1.1 总则

本规范中，互联网票务系统的网络安全建设将参照GB/T 22239-2019 中第三级系统的要求及结合AFC系统的特点

7.4.1.2 安全物理环境

7.4.1.2.1 物理位置的选择

物理位置的选择要求包括：

互联网票务系统机房场地应远离产生粉尘、油烟、有害气体以及生产或贮存危险品的场所。

7.4.1.2.2 物理访问控制

物理访问控制要求包括：

外部人员访问互联网票务系统主机房前应发起申请，经过审批后由机房管理人员全程陪同并保留相关审批、访问记录。

7.4.1.2.3 防盗窃和防破坏

防盗窃和防破坏要求包括：

应在必要情况下对主机房出入人员携带的物品进行检查。

7.4.1.2.4 防静电

防静电要求包括：

辅助区内的工作台面可采用导静电或静电耗散材料。

7.4.1.2.5 温湿度控制

温湿度控制要求包括：

应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。冷通道或机柜进风区域的温度应不高于27℃，相对湿度不大于60%。在停机时，主机房环境温度应不高于45℃，相对湿度应不高于80%。

7.4.1.2.6 电磁防护

电磁防护要求包括：

可采用屏蔽布线系统、光缆布线系统或建筑屏蔽等技术手段实现，当采用屏蔽布线系统时，可保证链路全程屏蔽以及屏蔽层可靠接地。

7.4.1.3 安全通信网络

7.4.1.3.1 网络架构

网络架构要求包括：

a) 应保证网络设备的业务处理能力满足业务高峰期的需要，应保证关键网络设备（如互联网票务系统与AFC各个架构以及互联网票务系统与外部系统之间的路由器）等资源使用率不超过60%；

b) 应保证网络各个部分的带宽满足业务高峰期需要，应保证互联网票务系统与AFC各个架构系统以及互联网之间路带宽使用率不超过70%；

c) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址，应为互联网售票系统划分独立的区域，每个区域划分独立的VLAN；

d) 应避免将重要网络区域部署在边界处，重要网络区域（如XXX区域、XXX区域）与其他网络区域之间应采取可靠的技术隔离手段；

e) 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。应保证互联网票务系统之间网络设备冗余部署。

7.4.1.3.2 通信传输

通信传输要求包括：

a) 应对互联网票务系统与 AFC 各个架构系统之间、互联网售票平台与外部网络通信在网络层传输过程中进行完整性保护；

b) 应对互联网票务系统与 AFC 各个架构系统之间、互联网售票平台与外部网络通信在网络层传输过程中采用密码技术保证数据的保密性。

7.4.1.4 安全区域边界

7.4.1.4.1 边界防护

边界防护要求包括：

a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信，应对互联网票务系统与 AFC 各个架构系统之间交互仅通过通信前置机，同时应对上述边界设备接口状态进行检测；

b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制，应关闭网络设备、安全设备、计算设备的闲置端口，同时应采用如 802.1x 等方式对接入设备进行认证；

c) 应能够对内部用户非授权联到外部网络的行为进行检查或限制，应限制计算设备利用多余网卡、USB 网卡访问外部网络；

d) 互联网票中心应该与 AFC 其他接口部署如数据百度技术实现的物理隔离。

7.4.1.4.2 入侵防范

入侵防范要求包括：

a) 应在互联网票务系统与外部系统之间部署能够检测、防止或限制从外部发起的网络攻击行为的设备，并对攻击源进行限制；

b) 应在互联网票务系统署具有能够检测、防止或限制从内部发起网络攻击行为的设备，并对攻击源进行限制；

c) 应在互联网票务系统安全运维区域部署抗APT系统、安全态势感知等基于流量或设备日志对网络行为进行分析的设备，实现对网络攻击特别是新型网络攻击行为的分析。

7.4.1.4.3 恶意代码和垃圾邮件防范

应在关键网络节点处部署基于流量进行分析恶意代码行为并限制的设备，并维护恶意代码防护机制的升级和更新。

7.4.1.5 安全计算环境

7.4.1.5.1 身份鉴别

身份鉴别要求包括：

a) 计算设备应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换，相关安全策略不应低于以下要求:

1) 用户口令长度不少于8位，应包含字母、数字、特殊符号混合排列；

2) 用户口令更换周期不大于180天；

3) 用户首次登录计算设备时应强制修改默认口令。

b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施，相关安全策略不应低于以下要求：

1) 非法登录次数应不超过5次；

2) 超过非法登录次数后应采取锁定账户或IP的措施，锁定时间应不少于5min；

3) 登录连接超时时间应不超过30min,超过后应采取强制注销等措施。

c) 应用系统或未提供多种鉴别技术的计算设备应仅通过开启两种或两种以上组合的鉴别技术的运维审计系统进行各类操作。

7.4.1.5.2 访问控制

访问控制要求包括：

应定期检查账户及权限的分配情况，并及时删除或停用多余的、过期的账户。

7.4.1.5.3 入侵防范

入侵防范要求包括：

a) 操作系统、网络设备、安全设备应遵循最小安装的原则，仅安装需要的组件和应用程序；

b) 操作系统、网络设备、安全设备应关闭不需要的系统服务、默认共享和高危端口；

c) 操作系统、网络设备、安全设备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；

d) 业务应用系统应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

e) 应定期对互联网票务系统内计算设备进行检查，能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；

f) 操作系统、网络设备、安全设备应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警；

g) 互联网票务系统中应部署时钟服务器，同时对NTP协议启用验证功能。

7.4.1.5.4 恶意代码防范

操作系统应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。同时应每月更新恶意代码库。

7.4.1.5.5 数据完整性

数据完整性要求包括：

a) 业务应用系统、数据库管理系统、中间件应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

b) 业务应用系统、数据库管理系统、中间件应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

7.4.1.5.6 数据保密性

数据保密性要求包括：

a) 业务应用系统、数据库管理系统、中间件应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；

b) 业务应用系统、数据库管理系统、中间件、操作系统应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

7.4.1.5.7 剩余信息保护

剩余信息保护要求包括：

a) 操作系统、业务应用系统、数据库管理系统、中间件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；

b) 操作系统、业务应用系统、数据库管理系统、中间件应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

7.4.1.5.8 个人信息保护

个人信息保护要求包括：

a) 业务应用系统和数据库管理系统宜仅采集和保存用户个人信息；

b) 业务应用系统和数据库管理系统应禁止未授权访问和非法使用用户个人信息。

7.4.1.6 安全管理中心

7.4.1.6.1 总则

互联网票务系统安全系统应该独立设置安全管理中心。在互联网票务系统清分系统网络中新建安全管理域，选型部署安全管理平台，实现网络设备、安全设备、服务器等系统的运行状态进行集中监测，安全系统配置集中管理、安全事件识别、报警、分析与可视化，安全策略、恶意代码、补丁升级等安全相关事项的集中管理；选型部署日志审计系统，实现全网主机系统告警日志与审计日志的集中收集、存储，保留时间不少于六个月。通过堡垒主机系统部署解决清分系统网络中各系统管理员、审计管理员、安全管理员通过统一方式登录系统时进行身份鉴别与操作行为安全审计。

7.4.1.6.2 集中管控

集中管控要求包括：

a) 划分特定的管理区域，在保证信息传输路径安全可靠的前提下，对网络中的设备、系统、资源进行集中管控，实时监测、分析网络的运行情况，能及时对各种网络安全事件进行处理；

b) 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；

c) 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；

d) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；

e) 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；

f) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；

g) 应能对网络中发生的各类安全事件进行识别、报警和分析。

7.4.2 互联网票务系统安全建设要求

7.4.2.1 互联网票务系统边界防护建设要求

清分中心边界防护建设要求如下：

a) 清分中心与互联网票务系统边界处应具备以下功能：链路负载均衡功能；通信链路加密功能；基于五元组、数据流、应用协议的访问控制；入侵检测与防御功能；基于流量和日志的未知威胁检测；流量清洗功能；

b) 清分中心与互联网票务系统边界建议部署以下产品或服务：链路负载均衡设备、使用软件定义边界技术的产品、防火墙、入侵检测/防御设备、WEB 应用防火墙、态势感知平台、抗 DDoS 产品或服务；

c) 互联网票务系统与互联网边界处应具备以下功能：链路负载均衡功能；通信链路加密功能；基于五元组、数据流、应用协议的访问控制；入侵检测与防御功能；基于流量和日志的未知威胁检测；流量清洗功能；

d) 互联网票务系统与互联网边界处建议部署以下产品或服务：链路负载均衡设备、使用软件定义边界技术的产品、防火墙、入侵检测/防御设备、WEB 应用防火墙、态势感知平台、抗 DDoS 产品或服务；

e) 互联网票务系统与第三方机构边界应具备以下功能：基于五元组、数据流、应用协议的访问控制；入侵行为检测与防御功能；基于流量和日志的未知威胁检测；

f) 互联网票务系统与第三方机构边界建议部署以下产品或服务：防火墙、入侵检测/防御设备、态势感知平台；

g) 互联网票务系统的业务区域与其他区域的边界应具备以下功能：应用负载均衡功能；应用传输加密功能；基于五元组、数据流、应用协议的访问控制；入侵行为检测与防御功能；基于流量和日志的未知威胁检测；

h) 互联网票务系统的业务区域与其他区域的边界建议部署以下产品或服务：

i) 互联网票务系统与其他区域的边界应对串行接入设备采用冗余部署。

7.4.2.2 互联网票务系统安全计算环境建设要求

互联网票务系统安全计算环境建设要求如下：

a) 互联网票务系统应具备针对应用的数据库进行安全审计的能力，应部署数据库审计设备；

b) 互联网票务系统应具备针对终端设备恶意代码防范和终端管控的能力，部署终端安全管理设备及终端防病毒设备；

c) 互联网票务系统应具备保证应用数据传输过程中完整性和保密性的能力，应部署SSL安全网关类设备；

d) 互联网票务系统应具备对应用中数据安全管理的能力，对重要数据及敏感数据进行管控，应在安全管理中心部署数据库脱敏设备和数据库加密设备。

7.4.2.3 互联网票务系统安全管理中心建设要求

互联网票务系统安全管理中心建设要求如下：

a) 安全管理中心应具备安全运维管理的能力，应在安全管理中心部署运维堡垒机；

b) 安全管理中心应具备漏洞管理的能力，能够针对全网脆弱性问题等进行扫描发现和跟踪管理，应在安全管理中心部署漏洞扫描设备；

c) 安全管理中心应具备安全态势管理、事件管理、分析风险、计算风险、应对风险的能力，应在安全管理中心部署安全态势感知平台。应能够与清分中心的安全态势感知平台对接；

d) 安全管理中心应具备针对各类终端进行授权、识别、认证、管控的能力，应在安全管理中心部署终端准入管控设备；

e) 安全管理应具备用户身份管理能力，应具备针对用户进行授权、认证、管控、审计功能，应在安全管理中心部署统一身份认证管理平台，应能够与清分中心的统一身份认证管理平台对接，相关组件应满足国家密码管理部门的相关要求。

7.5 AFC 云平台网络安全保护要求

7.5.1 总则

云平台作为AFC系统的云化模式。当AFC云化后产生的架构变化时，无论五层架构变为二层或者三层架构，都将AFC云平台作为统一的安全域进行规划。

在本规范中，云平台的网络安全建设将参照GB/T 22239-2019 《网络安全技术 网络安全等级保护基本要求》中第三级系统的要求及AFC系统的特点。

7.5.2 云平台网络安全等级保护要求

7.5.2.1 安全物理环境

7.5.2.1.1 物理位置的选择

物理位置的选择要求包括：

a) 云平台基础设备应保证云计算基础设施位于中国境内；

b) 机房场地应远离产生粉尘、油烟、有害气体以及生产或贮存危险品的场所。

7.5.2.1.2 物理访问控制

外部人员访问云平台主机房前应发起申请，经过审批后由机房管理人员全程陪同并保留相关审批、访问记录。

7.5.2.1.3 防盗窃和防破坏

防盗窃和防破坏要求包括：

应在必要情况下对主机房出入人员携带的物品进行检查。

7.5.2.1.4 防静电

防静电要求包括：

辅助区内的工作台面可采用导静电或静电耗散材料。

7.5.2.1.5 温湿度控制

应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。冷通道或机柜进风区域的温度应不高于27℃，相对湿度不大于60%。在停机时，主机房环境温度应不高于45℃，相对湿度应不高于80%。

7.5.2.1.6 电磁防护

电磁防护要求包括：

a) 应采用屏蔽布线系统、光缆布线系统或建筑屏蔽等技术手段实现，当采用屏蔽布线系统时，应保证链路全程屏蔽以及屏蔽层可靠接地；

b) 应对AFC云平台机房中关键设施实施电磁屏蔽。

7.5.2.2 安全通信网络

7.5.2.2.1 网络架构

网络架构要求包括：

a) 应保证网络设备的业务处理能力满足业务高峰期的需要，应保证关键网络设备（如云平台与各个接口的路由器）等资源使用率不超过60%；

b) 应保证网络各个部分的带宽满足业务高峰期需要，应保证云平台与各个非云化部分以及外部出口之间链路带宽使用率不超过70%；

c) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址，将不同的业务区域划分独立的VLAN；

d) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；

e) 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。应保证清分中心与多线路中心/单线路中心系统之间、清分中心与互联网票务系统之间网络设备冗余部署；

f) 应具有根据云上 AFC 系统业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略；

g) 应具有根据云上 AFC 系统业务需求提供通信传输、边界防护、入侵防范等安全机制的能力。

7.5.2.2.2 通信传输

通信传输要求包括：

a) 应对云平台与各个非云化部分以及外部出口之间通信在网络层传输过程中进行完整性保护；

b) 应对云平台与各个非云化部分以及外部出口之间通信在网络层传输过程中采用密码技术保证数据的保密性；

c) 应实现不同云上 AFC 系统虚拟网络之间的隔离。

7.5.2.3 安全区域边界

7.5.2.3.1 访问控制

访问控制要求包括：

a) 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；比如 AFC 云平台外部的网络边界、AFC 云平台与互联网售票系统的边界、AFC 云平台与车站局域网的边界等；

b) 应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则；

c) 应在 AFC 云平台内部划分出应用系统域、数据存储域、终端接入域，云平台内要分级做好边界防护；

d) 应将 AFC 云平台上的业务系统与非云化业务系统统一考虑安全防护。

7.5.2.3.2 入侵防范

入侵防范要求包括：

a) 应能检测到云上 AFC 系统发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

b) 应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

c) 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量；

d) 应在检测到网络攻击行为、异常流量情况时进行告警；

e) 宜在 AFC 云平台外部的网络边界部署入侵防范系统，双冗余部署，并设置访问控制规则。

7.5.2.3.3 安全审计

安全审计要求包括：

a) 应对 AFC 云平台服务商和云上 AFC 系统在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启；

b) 应保证 AFC 云平台服务商对云上 AFC 系统和数据的操作可被审计。

7.5.2.4 安全计算环境

7.5.2.4.1 身份鉴别

当远程管理AFC云平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。

7.5.2.4.2 访问控制

a) 应保证当虚拟机迁移时，访问控制策略随其迁移；

b） 应允许云服务客户设置不同虚拟机之间的访问控制策略。

7.5.2.4.3 入侵防范

a） 应能检测虚拟机之间的资源隔离失效，并进行告警；

b） 应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警；

c） 应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。

7.5.2.4.4 镜像和快照保护

a） 应针对 AFC 系统提供加固的操作系统镜像或操作系统安全加固服务；

b） 应提供 AFC 云化的虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；

c） 应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问；

d） 在虚拟机、容器、物理机、PC 工作站中均部署轻量级终端杀毒代理，基于安全管理中心的病毒管理平台统一监控、升级、更新病毒库等保。

7.5.2.4.5 数据完整性和保密性

a） 应确保 AFC 系统云上数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；

b） 应确保只有在线路 AFC 业务的管理端授权下，AFC 云平台运营方才具有单个 AFC 数据的管理权限；

c） 应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；

d） 应支持云上 AFC 系统部署密钥管理解决方案，保证云上 AFC 系统自行实现数据的加解密过程。

7.5.2.4.6 数据备份恢复

a） 云上 AFC 系统应在本地保存其业务数据的备份；

b） AFC 云平台宜搭建双活数据中心，当主数据中心故障，可以在用户无感知的前提下进行业务和数据的实时切换，保障 AFC 的正常运行；

c） 应提供查询云上 AFC 系统数据及备份存储位置的能力；

d） AFC 云平台服务商的云存储服务应保证云上 AFC 系统数据存在若干个可用的副本，各副本之间的内容应保持一致；

e） 应为云上 AFC 系统将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。

7.5.2.4.7 剩余信息保护

a） 应保证虚拟机所使用的内存和存储空间回收时得到完全清除；

b） 云上 AFC 系统删除业务应用数据时，云计算平台应将云存储中所有副本删除。

7.5.2.5 安全管理中心

a） 应能对物理资源和虚拟资源按照策略做统一管理调度与分配；

b） 应保证 AFC 云平台管理流量与云上 AFC 系统流量分离；

c） 应根据 AFC 云平台服务商和云上 AFC 系统的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；

d） 应根据 AFC 云平台服务商和云上 AFC 系统的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。

7.5.3 云平台网络安全拓展建议要求

7.5.3.1 云安全南北向防护

a） 在云环境中，南北向主要是指互联网到业务、内网用户到业务的方向。需要对进出业务的虚拟化边界流量、请求或者认证做有效管控，实现南北向的安全防护；

b） 宜能够为云平台、云租户运维人员和移动办公人员，提供 VPN 服务；保障安全远程接入，并具备双向验证功能；

c） 宜能够提供针对租户远程运维人员的运维安全管理服务，包括能够对运维操作日志进行回放、溯源和审计取证；

d） 宜能够提供针对网络攻击的安全检测服务，包括但不限于病毒检测、僵木蠕检测、攻击检测

等；

e） 宜能够提供针对云租户应用系统的异常检测服务，包括但不限于应用负载检测、应用负载均衡、木马、网页篡改检测等；

f） 宜保障跨越南北向虚拟化边界的访问或者流量通过安全资源进行管控；

g） 宜保障对非授权的用户或者访问进行有效检查和控制；

h） 宜进行虚拟化关键网络节点的网络入侵防范、木马病毒防范、恶意代码防范、DDoS 攻击防范建设；

i） 宜在虚拟化网络边界进行全面审计，审计内容需要覆盖时间、用户信息、事件类型、事件结果和详细的日志信息。

7.5.3.2 云安全东西向防护

a） 在云环境中，东西向主要是指租户之间、VPC 之间、虚拟化实例之间的通讯方向。应在东西向流量和东西向请求做好网络和访问控制管控，实现云上东西向安全防护；

b） 宜能够提供 VPC 间、业务系统间、VM 间的边界安全防护服务，包括但不限于边界访问控制、病毒过滤和入侵防御；

c） 宜能通过 ACL、安全组、防火墙等机制实现租户之间的流量隔离；

d） 宜保障安全资源对虚拟化底层存储、计算、网络调用的隔离；

7.5.3.3 云安全资源池与云管理平台的关系

a） 安全资源池与云管理平台相互独立部署，之间通过接口方式实现必要的租户、网络、虚机信息、订单信息的共享同步，同时适应多厂商云平台；

b） 宜能够提供开放的南向接口，可以按需扩展安全能力；

c） 宜能够按照多种方式进行安全资源分配，如自助申请、统一分配等；

d） 宜支持通过横向扩容资源池服务器或者在资源池服务器中增加安全能力进行横向扩容且不影响客户业务网络架构变更；

e） 宜支持对防御类型的安全资源进行统一的策略下发和配置如：封堵策略、解封策略等；

f） 宜将策略处置相关的信息以通告的方式同步给相关业务责任人；

g） 安全资源池应能满足上层业务需要，通过 API 提供对安全资源安全策略的集中管理能力，安全能力不限于防护类设备、检测类设备、扫描类设备；策略包括创建、下发、状态、报表等；

h） 宜面向云管理平台提供标准接口服务，便于云管理平台能够统一纳管、有序分配安全资源；

i） 宜能够利用云管理平台提供的标准接口服务，完成安全资源的调配和应用安全保障，如同步云租户业务网段、下发引流策略；

j） 宜能够利用 SDN、策略路由等方式，将云环境中南北向流量牵引至云安全资源池。

7.5.4 云平台网络安全建设要求

7.5.4.1 云平台边界防护建设要求

云平台边界防护建设要求如下：

a） 云平台与物理网络边界应具备以下功能：链路负载均衡功能；通信链路加密功能；基于五元组、数据流、应用协议的访问控制；入侵检测与防御功能；基于流量和日志的未知威胁检测；流量清洗功能；

b） 云平台与物理网络边界边界建议部署以下产品或服务：链路负载均衡设备、使用软件定义边界技术的产品、防火墙、入侵检测/防御设备、WEB 应用防火墙、态势感知平台、抗 DDoS 产品或服务；

c） 云平台内部各个租户之间边界应具备以下功能：基于五元组、数据流、应用协议的访问控制；入侵行为检测与防御功能；基于流量和日志的未知威胁检测；

d） 云平台内部各个租户之间边界建议部署以下产品或服务：防火墙、入侵检测/防御设备、态势感知平台；

e） 云平台内部租户内部不同区域边界应具备以下功能：基于五元组、数据流、应用协议的访问控制；入侵行为检测与防御功能；基于流量和日志的未知威胁检测；

7.5.4.2 云平台安全计算环境建设要求

云平台安全计算环境建设要求如下：

a) 云平台应具备针对应用的数据库进行安全审计的能力，应部署数据库审计设备；

b) 云平台应具备针对终端设备恶意代码防范和终端管控的能力，部署终端安全管理设备及终端防病毒设备；

c) 云平台应具备保证应用数据传输过程中完整性和保密性的能力，应部署SSL安全网关类设备；

d) 云平台应具备对应用中数据安全管理的能力，对重要数据及敏感数据进行管控，应在安全管理中心部署数据库脱敏设备和数据库加密设备。

7.5.4.3 云平台安全管理中心建设要求

云平台安全管理中心建设要求如下：

a) 安全管理中心应具备安全运维管理的能力，宜在安全管理中心部署运维堡垒机；

b) 安全管理中心应具备漏洞管理的能力，能够针对全网脆弱性问题等进行扫描发现和跟踪管理，宜在安全管理中心部署漏洞扫描设备；

c) 安全管理中心应具备安全态势管理、事件管理、分析风险、计算风险、应对风险的能力，宜在安全管理中心部署安全态势感知平台；

d) 安全管理中心应具备针对各类终端进行授权、识别、认证、管控的能力，应在安全管理中心部署终端准入管控设备；

e) 安全管理应具备用户身份管理能力，应具备针对用户进行授权、认证、管控、审计功能，宜在安全管理中心部署统一身份认证管理平台，相关组件应满足国家密码管理部门的相关要求。

8 网络安全等级保护管理要求

8.1 安全管理制度

安全管理制度要求包括：

a) 应制定网络安全工作的总体方针和安全策略，阐明安全工作的总体目标、范围、原则和安全框架等；

b) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系；

c) 应制定或授权专门的部门或人员负责安全管理制度的制定，经过评审通过后，通过正式、有效的方式发布；

d) 应进行版本管控，定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

8.2 安全管理机构

安全管理机构要求包括：

a) 应成立指导和管理网络安全工作领导小组，其最高领导由单位主管领导担任或授权；

b) 管理机构应负责批准网络安全策略，协调系统范围内的安全策略落地实施；

c) 应在各车站、多线路中心/单线路中心系统、清分清算中心设立系统管理员、安全管理员，并定义工作岗位职责；

d) 应定期进行网络安全检查，检查内容包括系统安全日志审计、系统漏洞情；

e) 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。

8.3 安全管理人员

a) 应对被录用人员的专业资格或资质等进行审查，对其技术技能进行考核合格后上岗；

b) 应定期对线路所辖人员进行安全意识教育和岗位技能培训；

c) 应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议，明确操作规范和惩戒措施；

d) 应及时终止离岗人员的所有访问权限，对于在组织内部进行岗位调动的工作人员，应根据新岗位的工作需要，修改其访问权限；

e) 应确保外部人员物理访问受控区域时由专人全程陪同，接入网络进行系统维护前应提出书面申请，批准后由专人开设账号、分配权限，离场后及时清除外部人员所有的访问权限，并登记备案。

8.4 安全建设管理

安全建设管理要求包括：

a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；

b) 应组织相关部门和相关安全技术专家对定级结果的合理性和正确性进行论证和审定；

c) 应保证定级结果经过相关部门的批准，并将备案材料报主管部门和相应公安机关备案；

d) 应根据保护对象的安全保护等级进行安全方案设计，且安全方案应在相关部门和安全专家对其合理性和正确性论证和审定后，方可批准正式实施；

e) 应确保网络安全产品采购和使用符合国家的有关规定；

f) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制，在软件安装前对可能存在的恶意代码进行检测；

g) 应在软件交付前检测其中可能存在的恶意代码，并由开发单位提供软件设计文档和使用指南。

h) 应制定或授权专门的部门或人员负责工程实施过程的管理；

i) 应制定测试验收方案，根据验收方案进行上线前的安全性测试，并形成验收报告；

j) 应根据交付清单对所接的设备、软件和文档等进行清点；

k) 应对负责运行维护的技术人员进行相应的技能培训；

l) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；

m) 应在发生重大变更或级别发生变化时进行等级测评；

n) 应确保测评机构的选择符合国家有关规定；

o) 应确保服务供应商的选择符合国家的有关规定，并与选定的服务供应商签订与安全相关的协议，明确整个服务供应链各方需履行的网络安全相关义务。

8.5 安全运维管理

安全运维管理要求包括：

a) 应建立机房安全管理制度，指定专人负责机房安全，对物理访问和环境安全等方面进行管理，并定期对机房电源、温湿度、消防等设施进行维护；

b) 应对各车站、多线路中心/单线路中心系统、清分清算中心进行资产清单编制，并根据资产的重要程度对资产进行标识管理；

c) 应定期对各车站、多线路中心/单线路中心系统、清分清算中心的设备进行维护，并建立设备维护方面的管理制度，对维护进行有效的管理；

d) 应定期对各车站、多线路中心/单线路中心系统、清分清算中心开展安全检查，及时对安全漏洞和隐患进行修补，并形成安全检查报告；

e) 应建立网络和系统安全管理制度，设立不同的管理员角色对安全策略、账户管理、日志管理等方面进行运维管理；

f) 应提高员工的防恶意代码意识，定期检查恶意代码库的升级情况，并对检测的恶意代码进行分析；

g) 应根据各车站、多线路中心/单线路中心系统、清分清算中心的数据重要性，制定重要业务信息、系统数据和软件系统等方面的数据备份策略、数据恢复策略；

h) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；

i) 应建立重要事件的应急预案，包括应急处理流程、系统恢复流程等内容，并定期对相关员工进行应急预案培训和应急预案的演练；

j) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

9 网络安全运营管理

9.1 规划阶段

9.1.1 安全咨询

现场服务、远程联机服务、远程非联机服务，或者不同形式的组合。

典型的网络安全咨询服务，包括网络安全管理体系咨询和安全培训。

网络安全管理体系咨询主要是依照国家网络安全法律、法规、国际或国家网络安全管理体系相关标准，基于业务风险方法，通过定义范围和方针、业务分析、风险评估、设计、实施等步骤，面向组织建立、实施、运行、监视、评审、保持和改进网络安全的体系。网络安全管理体系是一个组织整个管理体系的一部分，应包括组织结构、方针策略、规划活动、职责、实践、规程、过程和资源等多个方面。可符合网络安全管理体系GB/T 22239（管理部分）。

安全培训提供网络安全意识、技术、管理、体系、工程、法律、政策和标准等方面的培训内容，以满足提高网络安全意识、完善网络安全知识、掌握网络安全技能的需求，从而提高相关人员的网络安全能力水平。具体还可包括针对网络安全专业人员的资质培训、针对服务需求方特定要求的定制培训等。

依据组织整体的使命和业务，以人力的方式提供相关咨询、意见、建议，服务交付物通常是一些文档。

9.2 建设阶段

9.2.1 安全集成

安全集成是按照信息系统建设的安全需求，采用信息系统安全工程的方法和理论，将安全单元、产品部件进行集成的行为或活动。典型的安全集成包括：

a) 网络安全设计；

b) 网络安全产品验收；

b) 网络安全产品部署；

c) 网络安全检查和测试。

9.2.2 安全监理

现场服务、远程联机服务、远程非联机服务，或者不同形式的组合。

具有相关资质的监理单位受网络安全工程建设单位的委托，依据国家批准的信息化工程项目建设文件、有关工程建设的法律法规和工程建设监理合同及其他工程建设合同，尤其是依据网络安全方面的标准和要求，在工程建设各阶段向建设单位提供相关咨询，并协助建设单位对承建单位在工程建设中的网络安全实施服务，实施控制和管理的一种专业化服务活动。网络安全监理还可以包括对信息系统运维阶段的其他网络安全实施服务进行监理。

依据组织整体的使命和业务，以人力的方式提供相关意见、建议、计划、方案，服务交付物通常是现场的人力监理活动和一些文档。

9.3 运营阶段

9.3.1 安全运营

现场服务、远程联机服务、远程非联机服务，或者不同形式的组合。

安全运维是为满足信息系统运行的安全需求，综合采用检查、测试、监控、应急等手段，维持信息系统安全保障水平的行为或活动。典型的安全运维包括：

a）网络安全检查和测试；

b）网络安全监控；

c）网络安全应急处理。

依据组织整体的使命和业务，以人力的方式提供相关咨询、意见、建议以及驻场的保障，服务交付通常是以派驻的人员的阶段服务为主。

9.3.2 风险评估

现场服务、远程联机服务、远程非联机服务，或者不同形式的组合。

风险评估主要是依据有关目前网络安全技术与管理法规、标准，从风险管理角度，对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程，通过评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响，并提出有针对性的抵御威胁的防护对策和整改措施。网络安全风险评估应贯穿于信息系统的规划、设计、实施、运行维护以及废弃各个阶段。

依据组织整体的使命和业务，以人力的方式提供相关咨询、意见、建议，服务交付物通常是一些文档。

9.3.3 应急响应

现场服务、远程联机服务、远程非联机服务，或者不同形式的组合。

网络安全应急处理主要是根据组织网络安全应急管理体系，针对各类突发网络安全事件，提供实施层面的应急响应和应急演练。应急响应是对已发生的各类网络安全事件作出快速响应，及时而有效进行事件处理，最大程度上减少损失和该事件造成的消极影响，响应的方式可以按事件特点和级别，可以分为现场和远程两种。

应急演练是根据组织已有的应急预案，在设备、系统、业务、组织等不同层面进行测试和演练，从而提高组织的应对各类突发网络安全事件的能力，演练的方式可分为桌面演练、模拟演练和实战演练。

依据组织整体的使命和业务，以人力的方式提供相关咨询、意见、建议、方案、演习脚本，服务交付物通常是一些文档以及专家、技术人员的人力服务。

9.3.4 灾难恢复

现场服务、远程联机服务、远程非联机服务，或者不同形式的组合。

容灾备份和恢复是为了防止信息系统及其应用和数据等，因网络安全事件或灾难而造成的丢失或损坏，从而在原文中独立出来单独存储的程序或文件副本，并在系统出现故障或瘫痪时，能够及时恢复系统及其应用和数据，将信息系统从故障或瘫痪状态恢复到可正常运行状态、并将其支持的业务功能从不正常状态恢复到可接受状态。容灾备份和恢复还应包括对备份介质和链路的定期测试、恢复的定期演练。

依据组织整体的使命和业务，以人力的方式提供相关意见、建议和方案，服务交付物通常是一些文档。

9.3.5 安全培训

现场服务、远程联机服务、远程非联机服务，或者不同形式的组合。

服务提供方提供网络安全意识、技术、管理、体系、工程、法律、政策和标准等方面的培训内容，以满足提高网络安全意识、完善网络安全知识、掌握网络安全技能的需求，从而提高相关人员的网络安全能力水平。

基于培训目的，结合培训规模、人员基础知识、培训时间、培训条件等情况，对培训内容、培训方式、考核方式等作出针对性的培训计划，并通过授课、实操、考核等方式予以实施。

依据组织整体的使命和业务，以人力的方式提供相关意见、建议和知识传递，服务交付物通常是一些文档、讲义、课件及专业授课、教学。

10 网络安全测评

10.1 安全物理环境

安全物理环境要求包括：

a) 核查是否有建筑物抗震设防审批文档，核查是否有雨水渗漏的痕迹，核查是否有可灵活开启的窗户，若有窗户，是否做了封闭、上锁等防护措施，

核查屋顶、墙体、门窗和地面等是否有破损开裂的情况，核查机房是否在顶层或地下室，若是，核查机房是否采取了防水和防潮措施；

b) 核查出入口是否配置电子门禁系统，核查电子门禁系统是否开启并正常运行，核查电子门禁系统是否可以鉴别、记录进入的人员信息；

c) 核查机房内设备或主要部件是否固定，核查机房内设备或主要部件上是否设置了明显且不易除去的标记；

d) 核查机房内通信线缆是否铺设在隐蔽安全处；

e) 核查是否配置防盗报警系统或专人值守的视频监控系统，核查防盗报警系统或视频监控系统是否开启并正常运行；

f) 核查机房内机柜、设施和设备等是否进行接地处理，通常黄绿色相间的电线为接地用线；

g) 核查机房内是否设置防感应雷措施，核查防雷装置是否通过验收或国家有关部门的技术检测；

h) 核查机房内是否设置火灾自动消防系统，核查火灾自动消防系统是否可以自动检测火情、自动报警并自动灭火，核查火灾自动消防系统是否通过验收或国家有关部门的技术检测；

i) 核查机房验收文档是否明确所用建筑材料的耐火等级；

j) 核查是否进行了区域划分，核查各区域间是否采取了防火隔离措施；

k) 核查窗户、屋顶和墙壁是否采取了防渗漏的措施；

l) 核查是否采取了防止水蒸气结露的措施，核查是否采取了排水措施，防止地面产生积水；

m) 核查是否安装了对水敏感的检测装置，核查防水检测和报警装置是否开启并正常运行；

n) 核查是否安装了防静电地板，核查是否采用了防静电接地措施；

o) 核查机房内是否配备了静电消除设备；

p) 核查机房内是否配备了专用空调，核查机房内温湿度是否在设备运行所允许的范围之内；

q) 核查供电线路上是否配置了稳压器和过电压防护设备，核查是否配备不间断电源(UPS)等备用供电系统，核查不间断电源(UPS)等备用供电系统的运行切换记录和检修维护记录，核查是否设置了冗余或并行的电力电缆线路为计算机系统供电；

r) 核查机房内电源线缆和通信线缆是否隔离铺设，核查机房内是否为关键设备配备了电磁屏蔽装置。

10.2 安全通信网络

安全通信网络要求包括：

a) 应访谈网络管理员业务高峰时期为何时，核查边界设备和主要网络设备的处理能力是否满足业务高峰期需要，询问采用何种手段对主要网络设备的运行状态进行监控，在业务高峰期主要网络设备的CPU内存最大使用率不宜超过70%，也可以通过综合网管系统查看主要网络设备的CPU、内存的使用情况；

b) 应访谈网络管理员，是否依据部门的工作职能、等级保护对象的重要程度和应用系统的级别等实际情况和区域安全防护要求划分了不同的VLAN,并核查相关网络设备配置信息，验证划分的网络区域是否与划分原则一致；

c) 应核查重要网络区域与其他网络区域之间，例如应用系统区、数据库系统区等重要网络区域边界是否采取可靠的技术隔离手段，是否部署了网闸、防火墙和设备访问控制列表(ACL)等；

d) 应核查系统的出口路由器、 核心交换机、安全设备等关键设备是否有硬件冗余和通信线路冗余，保证系统的高可用性；

e) 应核查是否在数据传输过程中使用校验技术或密码技术来保证其完整性；

f) 应测试验证设备或组件是否保证通信过程中数据的完整性。例如使用File ChecksumIntegrity Verifier、SigCheck 等工具对数据进行完整性校验；

g) 应核查是否基于可信根对设备的系统引导程序、系统程序、重要配置参数和关键应用程序等进行可信验证。

10.3 安全区域边界

安全区域边界要求包括：

a) 应核查网络拓扑图与实际的网络链路是否一致，是否明确了网络边界，且明确边界设备端口，应核查路由配置信息及边界设备配置信息，确认是否指定物理端口进行跨越边界的网络通信；

b) 应核查设备中访问控制策略是否明确设定了源地址、目的地址、源端口、目的端只和协议等相关配置参数；

c) 应核查相关系统或设备是否能够检测到从内部发起的网络攻击行为，应核查相关系统或设备的规则库版本是否已经更新到最新版本，应核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点，应测试验证相关系统或设备的安全策略是否有效；

d) 应访谈网络管理员和检查网络拓结构，查看在网络边界处是否部署了防恶意代码产品。如果部署了相关产品，则查看是否启用了恶意代码检测并查看白志记录中是否有相关阻断信息，应访谈网络管理员，是否对防恶意代码产品的特征库进升级及具体的升级方式，并登录相应的防恶意代码产品，核查其特征库升级情况，当前是否为最新版本，应测试验证相关系统或设备的安全策略是否有效；

e) 应核查是否基于可信根对设备的系统引导程序、系统程序、重要配置参数和关键应用程序等进行可信验证，应核查是否应用程序的关键执行环节进行动态可信验证3)应测试验证当检测到设备的可信性受到破坏后是否进行报警，应测试验证结果是否以审计记录形式送至安全管理中心。

10.4 安全计算环境

安全计算环境包括：

a) 应核查系统是否采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户身份进行鉴别，应核查是否配置并启用了登录失败处理功能:如果网络中部署堡垒主机，先核查堡垒主机是否具有登录失败处理功能，如果没有部署堡垒主机，则设置默认登录失败3次，退出登录界面，应核查是否配置并启用了限制非法登录达到一定次数后实现账户锁定功能，应核查是否配置并启用了远程登录连接超时并自动退出功能；

b) 应核查是否进行角色划分，如划分为网络管理员，安全管理员、系统管理员等角色，应核查访问控制策略，查看管理用户的权限是否已进行分离，应核查管理用中权限是否为其工作任务所需的最小权；

c) 访谈审计记录的存储、备份和保护的措施，是否将交换机日志定时发送到日志服务器上等，并使用syslog方式或SNMP方式将日志发送到日志服务器，如果部署了日志服务器,登录日志服务器查看被测交换机的日志是否在收集的范围内；

d) 应访谈系统管理员是否定期对系统服务进行梳理，关闭了非必要的系统服务和默认共享，应核查是否不存在非必要的高危端口；

e) 应进行漏洞扫描，核查是否不存在高风险漏洞，应访谈系统管理员，核查是否在经过充分测试评估后及时修补漏洞；

f) 应核查防火墙是否有入侵检测功能，查看入侵检测功能是否正确启用，应核查在发生严重入侵事件时是否提供报警，报警方式般包括短信、邮件等；

g) 无论是Windows主机还是Linux主机，都面临木马、蠕虫等病毒的破坏。因此一般的主机为防范病毒，均会安装反病毒软件，或者采用可信验证机制对系统程序、应用程序等进行可信执行验证；

h) 核查服务器的启动，是否实现可信验证的检测过程，查看对那些系统引导程序、系统程序或重要配置参数进行可信验证，修改其中的重要系统程序之一和应用程序之一，核查是否能够检测到并进行报警，是否将验证结果形成审计记录送至安全管理中心；

i) 询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据；

j) 询问系统管理员,该系统采集了用户的哪些个人信息,询问系统管理员,系统中采集的用户个人信息是否是业务应用必需的，询问系统管理员，哪些系统账户可以访问个人信息，且系统采取了什么措施控制可访问个人信息的系统账户对个人信息的访问。

10.5 安全管理中心

安全管理中心要求包括：

a) 应核查是否对系统管理员进行身份鉴别，应核查是否只允许系统管理员通过特定的命令或操作界面进行系统管理操作，应核查是否对系统管理操作进行审计；

b) 应核查是否对审计管理员进行身份鉴别，应核查是否只允许审计管理员通过特定的命令或操作界面进行安全审计操作，应核查是否对安全事代操作进行审计；

c) 应核查是否通过安全管理员对系统中的安全策略进行配置，包括安全参数、主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等；

d) 应核查是否划分出单独的网络区域用于安全管理，应核查是否各个安全设备或安全组件的配置等管理均由管理区的设备进行；

e) 验证时钟同步功能，数据的管理和分析在时间上的一致性。

10.6 安全管理制度

安全管理制度要求包括：

a) 核查是否具有总体方针和策略文件，核查该文件是否明确了机构安全工作的总体目标，范围、原则和各类安全策略，该策略文件中可以明确网络安全管理活动的责任部门或人员、也可覆盖到等级保护对象生命周期中所有关键的安全管理活动。其中安全管理框架应包括组织机构及岗位职责，人员安全管理、环境和资产安全管理、

系统安全建设管理 系统安全运行管理、事件处置和应急响应等方面，明确各个方面的职责分工，需要关注的管理活动、管理活动的控制方法等；

b))核查是否具有总体方针策略文件、管理制度，操作规程和记录表单等，核查管理体系各要素之间是否具有连贯性，一套全面的安全管理制度体系最常见的为4层架构，即由网络安全工作的总体方针策略，各种安全管理活动的管理制度、日常操作行为的操作规程和安全配置规范和各类记录表单；

c) 核查制度制定和发布要求管理文档是否说明安全管理制度的制定和程序，格式要求及版本编号等相关内容，核查安全管理制度的收发登记记录是否通过正式、有效的方式收发，如正式发文、领导签署和单位盖章等，是否注明发布范围；

d) 访谈信息/网络安全主管是否定期对安全管理制度体系的合理性和适用性进行审定，核查是否具有安全管理制度的审定或论证记录，如果对制度做过修订，核查是否有修订版本的安全管理制度，安全管理制度体系涉及从上层方针到管理制度再到操作规程等整个单位等保护对象安全相关的所有文件，这里的定期一般可以为一年，具体可根据组织情况进行约定，但是，一旦发生可能引起安全管理制度不适用的事件时应该主动对安全管理制度进行检查和审定，发现不足及时修订。

10.7 安全管理机构

安全管理机构要求包括：

a) 访谈信息/网络安全主管是否成立了指导和管理网络安全工作的委员会或领导小组，核查部门职责文档是否明确了网络安全工作委员会或领导小组构成情况和相关职责，核查相关委任授权文件是否明确其最高领导由单位主管领导委任或授权；

b) 访谈信息/网络安全主管是否设立了系统管理员、网络管理员和安全管生员等岗位，核查岗位职责文档是否明确了各岗位职责；

c) 访谈信息/网络安全主管，是否设立了网络安全管理职能部门和各方面负责人(如机房负责人、系统运维负责人，系统建设负责人等)，)核查部门职责文档是否明确网络安全管理工作的职能部门和各负责人职责，安全主管“一般是一个单位安全管理工作的主要责任人，全面负责等级保护对象安全规划、建设、运行维护等安全管理

工作，一般由单位的高层或某一部门的主管担任。“安全管理各方面的负责人”一般包括物理安全负责人(其是保护等级保护对象物理进行环境和办公环境安全的责任人），系统建设方面负责人(其是保证等级保护对象安全规划、建设、工程实施过程的责任人)和系统运行维护方面的责任人(其是保证等级保护对象日常运行安全的责任人)等；

d) 访谈信息/网络安全主管是否定期进行了常规安全核查，核查常规安全核查记录是否包括了系统日常运行|系统漏洞和数据备份等情况；

e) 访谈信息/网络安全主管，是否定期进行了全面安全核查，核查内容都有哪些，核查全面安全核查记录类文档， 是否包括了现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

f) 核查人员安全管理文档是否说明录用人员应具备的条件(如学历要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等），核查是否具有人员录用时对录用人身份、背景、专业资格和审查的相关文档或记录，是否记录审查内容和审查结果等，核查人员录用时的缺技能考核文档或记录，是否记录考核内容和考核结果等；

g) 核查人员离岗的管理文档是否规定了人员调离手续和离岗要求，核查是否具有按照离岗程序办理调离手续的记录，核查保密承诺文档是否有调离人员的签字；

h) 核查外部人员访问管理文档，是否明确允许外部人员访问的范围，外部人员进入的条件、外部人员进入的访问控制措施等，核查外部人员访问重要区域的书面申请文档是否具有批准人允许访问的批准签字等，核查外部人员访问重要区域的登记记录是否记录了外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等。

10.8 安全建设管理

安全建设管理要求包括：

a) 核查定级文档是否明确测评系统的安全保护等级，核查是否给出了定级的方法和理由；

b) 核查是否对测评系统组织相关部门或相关专家对定级结果进行了认证和审定，核查是否有定级结果的评审和论证记录文件，核查是否获得了相关主管部门的批准；

c) 核查是否有定级结果的审批文件，核查是否向主管部门备案，查是否有备案证明证书；

d) 核查是否根据系统等级选择相应的安全保护措施，核查是否根据风险分析的结果补充安全措施；

e) 核查设计类文档是否根据系统等级或风险分析结果采取相应的安全保护措施，这里的安全规划设计类文档要求根据等级保护对象的安全保护 ，判断等级保护对象现有的安全保护水平与国家等级保护管理规范和技术标准之间的差距，提出等级保护对象的基本安全保护需求；

f) 管理内容是否覆盖开发环境和运行环境分开的规定以及测试数据是否受控，开发人员和测试人员分离，即开发人员不能做测试人员，测试数据和测试结果受到控制，是指它们应该与软件设计相关档文一起有专人管理，并且对他们的使月和访问进行严格限制；

g) 访谈建设负责人是否做恶意代码检测，核查是否有恶意代码检测报告；

h) 访谈建设负责人，工程实施是否指定专门部门或人员进行工程实施过程的管控，核查部门或岗位职责文档；

i) 访谈建设负责人是否对测试验收进行管控，核查是否有调试验收方案和测试验收报告；

j) 访谈建设负责人是否对系统交付建立管控流程以及交付清单，核查交付清单内容；

k) 访谈建设负责人是否对运行维护人员进行技能培训，核查培训记录相关记录文档；

l) 访谈等级测评负责人是否每年定期开展等级测评，核查等级测评报告和整改记录；

m) 访谈测评系统是否发生过重大变更或开级，核查重大升级变更或改造的文件；

n) 访谈测评负责人是否选择了具有测评资质的测评机构，到www.djbh.net上核查该机构是否符合要求；

o) 访谈建设负责人对服务供应商的管控措施，核查服务供应商的服务内容和协议。

10.9 安全运维管理

安全运维管理要求包括：

a) 访谈物理安全负责人是否指定部门和人员负责机房安全管理工作，如对机房的出入进行管理、对基础设施(如空调、供配电设备、灭火设备等)进行定期维护，核查来访人员登记记录，来访人员记录内容是否包括了来访人员、来访时间、离开时间，携带物品等，核查设施维护记录，设施维护记录内容是否包括了维护日期、维护人、维护设备、故障维护结果等；

b) 核查资产清单,资产清单内容是否包括了资产范围(含设备设施、软件、文档等）、资产责任部门、重要程度和所处位置等；

c) 核查安全管理制度中是否明确了对信息进行分类与标识的原则和方法，核查安全管理制度中是否明确了对不同类信息的使用、传输和存储等操作的要求；

d) 核查运维管理制度中对于发现安全弱点和可疑事件后的汇报要求，核查以往发现过的安全弱点和可疑事件对应书面报告或记录；

e) 访谈运维负责人指派哪个部门或人员进行账户管理，含网络层面、系统面、数据库层面、 业务应用层面，核查账户管理记录，记录内容是否包括了账户申请、建立、停用、删除、重置等相关的审批情况；

f) 核查提升员工防恶意代码意识的培训或宣传记录，核查恶意代码防范管理制度，核查外来计算机或存储设备接入系统前进行恶意代码检查记录；

g) 核查是否有数据备份策略、备份程序，核查是否具有数据恢复策略、恢复程序；

h) 核查配置变更审批程序，如对改变连接、安装系统组件或调整配置参数的审批流程，核查配置变更审计日志，核查配置变更记录，核查配置信息库更新记录；

i) 核查应急预案框架，内容是否包括了启动应急预案的条件、应急组织构成、应急资源保障、事后教育和培训等；

j) 检查外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

参 考 文 献

[1] GB/T 22239-2019 信息安全技术网络安全等级保护基本要求
[2] GB/T 22240 信息安全技术信息系统安全等级保护定级指南；
[3] GB/T 32399-2015 信息技术 云计算 参考架构
[4] GB/T 35273 信息安全技术 个人信息安全规范
[5] GB/T 25070-2019 信息安全技术网络安全等级保护安全设计技术要求；
[6] GB/T 25058 信息安全技术信息系统安全等级保护实施指南；
[7] GB/T 31168 信息安全技术云计算服务安全能力要求
[8] GB/T 50157-2013 地铁设计规范
[9] GB/T 28448 信息安全技术网络安全等级保护测评要求
[10] GB/T 28449 信息安全技术网络安全等级保护测评过程指南；
[11] T/CAMET 11001.3-2019 智慧城市轨道交通信息技术架构及网络安全规范第3部分：网络安全
[12] JT/T 18-2020 交通运输标准制定、修订程序和要求
[13] 交通运输部关于推动交通运输领域新型基础设施建设的指导意见
[14] 中国城市轨道交通智慧城轨发展纲要
[15] 中共中央、国务院：交通强国建设纲要
[16] 交通运输部：数字交通发展规划纲要
[17] 交通运输部：城市轨道交通设施设备运行维护管理办法
[18] 交通运输部：城市轨道交通运营管理规定
[19] 交通运输部：交通运输标准化管理办法
[20] 国家认监委：交通一卡通产品认证实施规则通用要求
[21] 交通运输部：城市轨道交通初期运营前安全评估技术规范 第1部分 地铁和轻轨
[22] 国务院：关键信息基础设施安全保护条例
[23] 国家：个人信息保护法