ICS 03.220.20
R 85

中华人民共和国国家标准

GB/T 37378—2019

交通运输　信息安全规范

Transportation—Information security specification

2019-05-10 发布　　2019-12-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国智能运输系统标准化技术委员会(SAC/TC 268)提出并归口。

本标准起草单位:交通运输部公路科学研究院、北京中交国通智能交通系统技术有限公司、中关村中交国通智能交通产业联盟、国家计算机网络与信息安全管理中心、北京奇安信科技有限公司、恒安嘉新(北京)科技股份公司、北京信息科技大学、北京航空航天大学。

本标准主要起草人:孟春雷、武俊峰、梅新明、周洲、孙婧、宋向辉、陈晓光、郑新华、刘鸿伟、王永建、王立岩、赵童、吴秋新、王云鹏、余贵珍、马涛、赵云辉、王龑。

交通运输　信息安全规范

1　范围

本标准规定了交通运输信息安全技术体系架构和通用技术要求，包括构成交通运输信息系统的用户终端、载运装备单元、基础设施单元、计算中心、网络与通信各基本组成部分的信息安全通用和专项技术要求。

本标准适用于指导交通运输信息系统运营者针对非涉密系统的特定信息安全需求提出具体的信息安全标准、规范、实施指南等，也可用于指导开展信息安全技术体系规划、设计、建设、运维、评估等工作。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 20839—2007　智能运输系统　通用术语

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 20839—2007 和 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了 GB/T 20839—2007 和 GB/T 25069—2010 中的某些术语和定义。

3.1

交通运输信息系统　transport information system

交通运输领域由计算机或者其他信息终端及相关设备和网络组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。通常由终端、载运装备单元、基础设施单元、计算中心、网络和通信等全部或部分组成。

3.2

信息安全　information security

保护、维持信息的保密性、完整性和可用性，也可包括真实性、可核查性、抗抵赖性、可靠性等性质。

[GB/T 25069—2010，定义 2.1.52]

3.3

交通运输信息系统运营者　operators of transport information system

交通运输非涉密信息系统的所有者、管理者和服务提供者。

3.4

交通运输通用用户终端　general user terminal for transport

在交通运输业务中使用的通用桌面终端设备和移动智能终端设备，包括台式机、笔记本电脑、智能手机、平板电脑等。

3.5

交通运输专用用户终端　special user terminal for transport

在交通运输业务中使用的具备特定功能可实现人机交互操作的设备。

3.6

基础设施单元　infrastructure side unit

为实现交通运输信息系统功能，部署在路侧、岸侧的设备或模块等，包括通信设备、信息发布设备、状态监测设备、环境监测设备等。

3.7

载运装备单元　vehicle side unit

车辆、船舶、集装箱等交通运输装备中与基础设施单元、终端或计算中心实现通信的装置或通信模块等。

3.8

安全单元　security element；SE

含有中央处理单元的集成电路模块，负责通用和专用用户终端、载运装备单元和基础设施单元的访问许可、信息鉴别和加密保护等。

3.9

生命安全级应用　safety related application

紧急碰撞与伤害减弱，潜在碰撞与伤害减弱和防止，紧急事件通知（如前车急刹）等；紧急情况通知（如事故，急救车辆，突发性环境恶化通知）等应用。

3.10

行驶辅助级应用　driving aid application

基础设施侧单元向载运装备通知的高优先级的公共安全信息相关通知；安全相关道路状况紧急通知如红绿灯周期、急转弯等；行车辅助消息如自动驾驶、路侧周期广播、定位差分信号、交通信息播报等应用。

3.11

增值服务级应用　value-added service application

非优先类业务如在线支付充值、个性化导航服务、行车路线建议、电子商务等应用。

3.12

保密性　confidentiality

使数据不泄露给未授权的个人、实体、进程，或不被其利用的特性。

[GB/T 25069—2010，定义 2.1.1]

3.13

完整性　integrity

数据没有遭受以未授权方式所做的更改或破坏的特性。

[GB/T 25069—2010，定义 2.1.42]

3.14

可用性　availability

已授权实体一旦需要就可访问和使用的数据和资源的特性。

[GB/T 25069—2010，定义 2.1.20]

3.15

数据新鲜性　data freshness

防止已成功接收的历史数据再次被接收处理，或超出数据接收时间的数据被接收，或超出数据合法性范围的数据被接收的特性。

3.16

辅助驾驶　driving assistance

利用传感探测、自动控制、通信等技术，通过载运装备单元和基础设施单元的智能探测、载运装备-载运装备和载运装备-基础设施通信等方法，为驾驶员提供信息服务与支持、紧急情况下的预警和控制干预支持等功能，提高驾驶员出行安全和效率。

[GB/T 20839—2007，定义 7.2]

4 缩略语

下列缩略语适用于本文件。

RFID:射频识别(Radio Frequency Identification)

T-BOX:远程信息处理器(Telematics BOX)

TPMS:轮胎压力监测系统(Tire Pressure Monitoring System)

USB:通用串行总线(Universal Serial Bus)

VIN:车辆识别码(Vehicle Identification Number)

5 交通运输信息系统安全技术体系架构

交通运输信息安全技术体系架构由用户终端安全、载运装备单元安全、基础设施单元安全、计算中心安全、网络和通信安全、安全通用技术六部分构成,安全通用技术是对其余五部分的共性要求。

交通运输信息系统运营者应确保所运营的信息系统满足用户终端安全、载运装备单元安全、基础设施单元安全、计算中心安全、网络和通信安全五个体系组成部分的专项安全技术要求,同时还要满足安全通用技术要求。

采用网络和通信安全技术要求时,应根据不同交通运输信息系统的特征,参考用户终端、载运装备单元、基础设施单元、计算中心的安全技术要求,采用合理的技术措施,确保交通运输信息系统各组成部分安全防护机制之间的协调性和互补性,形成纵深防护能力。交通运输信息安全体系架构见图 1。

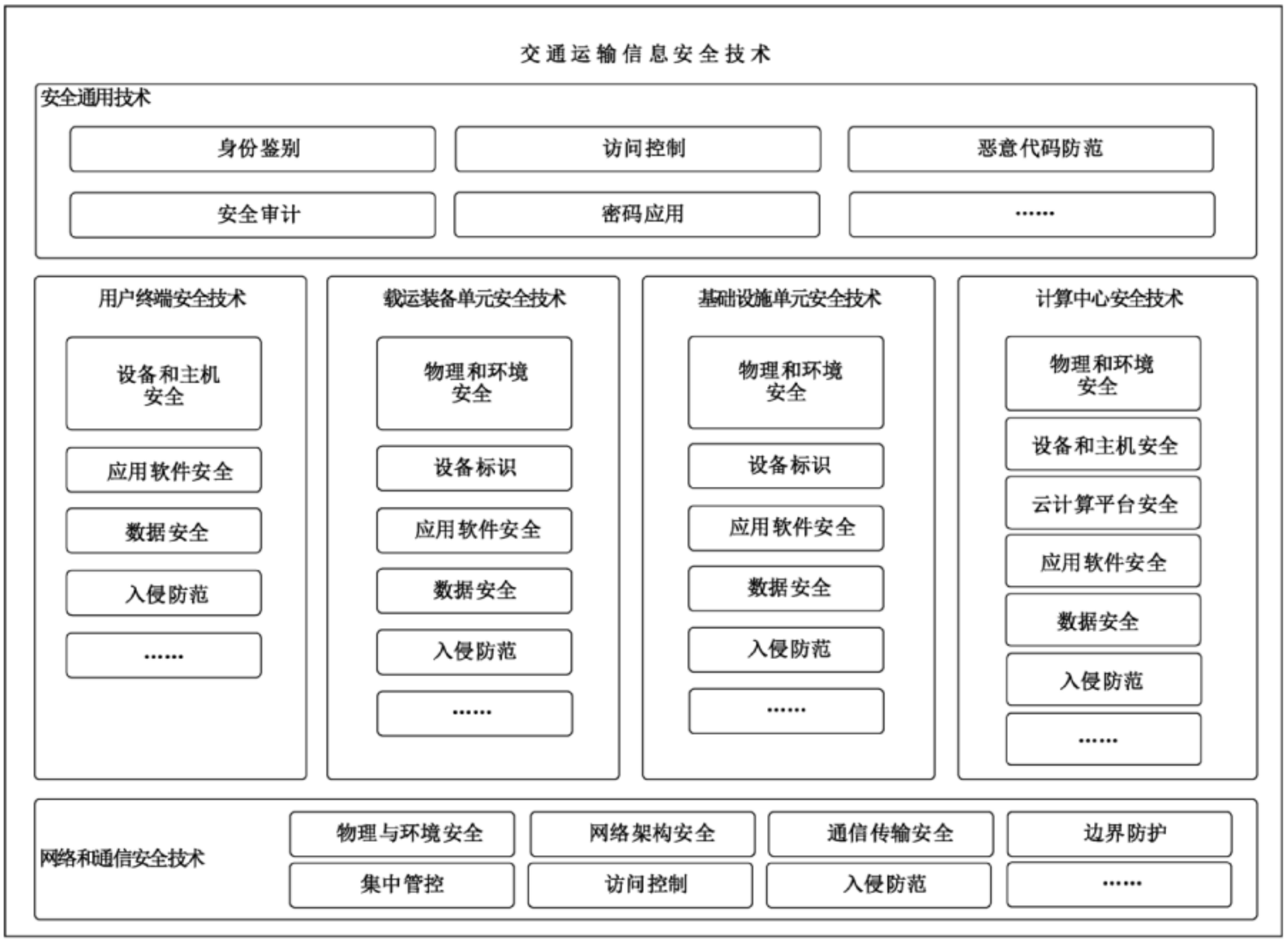

图 1 交通运输信息安全体系架构图

6 交通运输信息系统安全通用技术要求

6.1 身份鉴别

身份鉴别技术要求包括：

a) 应对登录的用户进行身份标识和鉴别，用户的身份标识应具有唯一性，身份鉴别信息具有复杂度要求；

b) 用户首次登录时应修改系统设置的初始口令，并定期更换；

c) 宜采用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应使用密码技术来实现；

d) 当进行远程管理时，应采取必要措施，避免鉴别信息明文传输；

e) 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必要的保护措施；

f) 用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全；

g) 按照“后台实名、前台自愿”的原则，要求用户在各类交通运输应用中进行实名身份(基于姓名、身份证号、VIN 号、移动电话号码等)注册，系统应对实名情况进行校验。

6.2 访问控制

访问控制技术要求包括：

a) 应提供访问控制功能，对登录的用户分配账号和权限；

b) 应重命名或删除默认账号，修改默认账号的默认口令；

c) 应及时删除多余的、过期的账号；

d) 应授予不同账号为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；

e) 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；

f) 访问控制的粒度应达到主体为用户级，客体至少为文件级；

g) 应对敏感信息资源设置安全标记，并控制主体对有安全标记信息资源的访问。

6.3 恶意代码防范

恶意代码防范技术要求包括：

a) 应具备对病毒、蠕虫、木马等恶意代码进行检测和清除的能力；

b) 应具备维护恶意代码防护机制的升级和更新的能力，交通运输专网、局域网等应采取技术手段及时升级恶意代码防护机制。

6.4 安全审计

安全审计技术要求包括：

a) 应对交通运输信息系统中的关键节点进行安全审计，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、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) 应确保审计记录的留存时间符合法律法规要求，存储时间不少于 6 个月；

e) 审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性；

f) 应对审计进程进行保护，防止未经授权的中断。

6.5 密码应用

密码应用技术要求包括：

a) 交通运输重要信息系统应采用交通运输行业规划的密钥和数字证书；

b) 交通运输重要信息系统采用密码技术保证应用系统实现身份鉴别、访问控制等安全功能，确保审计记录、数据存储和通信安全；

c) 应优先采用 SM 系列密码算法；

d) 应采用经国家密码主管部门认可的密码产品；

e) 同时运行在互联网和专网的信息系统，须使用密码技术保证网络系统实现安全访问路径、访问控制、身份鉴别功能；

f) 应采用密码技术保证主机设备、网络设备实现身份鉴别、访问控制、审计记录、数据传输安全、数据存储安全和程序安全；

g) 应采用密码技术实现专用终端、载运装备单元和基础设施单元的接入认证。

7 用户终端安全技术要求

7.1 设备和主机安全

设备和主机安全技术要求包括：

a) 专用用户终端应具备与工作环境相适应的物理防护措施，具备必要的防挤压、防水等能力；

b) 专用用户终端的身份标识装置应具备防物理拆卸、逻辑破坏和伪造等功能，发现标识异常时，应停止服务并发出和上传警示信息；

c) 专用移动终端、卡证读写设备等应具有可寻址的唯一性标识，发起信息传输时应进行自身身份标识；

d) 应对专用用户终端的启用、维护、弃置等进行全生命周期管理；

e) 专用用户终端在启动前应进行安全检测；

f) 专用用户终端应拆除或封闭不必要的数据传输物理接口；

g) 对于能够接入外部设备的专用用户终端，应具有防恶意软件和入侵防护能力，对临时接入设备采取病毒查杀等安全预防措施。

7.2 应用软件安全

应用软件安全技术要求包括：

a) 应用软件应经过信息系统运营者自身授权和安全评估，能够支持实现载运装备侧设备和移动应用软件安全防护需求（如密钥管理、身份认证管理、远程升级管理、安全监控、数据安全、恶意代码防护等），形成载运装备侧、移动应用软件和服务平台的一体化防御体系；

b) 移动应用软件在上线前，应经过安全检测；

c) 移动应用软件在启动前，应具有安全检测机制并提供版本更新功能；

d) 移动应用软件在运行中，宜具有通信数字证书安全性校验功能；

e) 移动专用用户终端上的应用软件应经过单位自身授权和专业评估单位的安全评估。

7.3 数据安全

数据安全技术要求包括：

a) 专用移动终端、卡证读写设备等应采用安全单元或者达到同样安全等级的方式存储密钥和敏感信息；

b) 应具备定期备份关键业务数据的能力；
c) 经用户同意或接纳服务条款的，服务提供者可以采集、存储、传输和使用用户信息（包括载运装备所有者与使用者，载运装备基础信息等）。

7.4 入侵防范

入侵防范技术要求包括：
a) 用户终端应关闭不需要的系统服务、默认共享和高危端口；
b) 专用用户终端操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序。

8 载目装备单元次全技术要求

8.1 物理和环境次全

物理和环境安全技术要求包括：
a) 应具有在特定使用环境中正常运行的能力；
b) 载运装备运行状态控制或辅助驾驶等载运装备单元应具备监测并拒绝非法物理接入的能力；
c) 为生命安全级、行驶辅助级应用提供逻辑计算基础数据的载运装备单元，应具备抗通信干扰和物理破坏等能力，并具备异常状态监测和报警的能力。

8.2 载目装备单元设备标识

载运装备单元设备标识技术要求包括：
a) 载运装备单元应具有可寻址的唯一性标识，发起信息传输时应进行自身身份标识；
b) 载运装备单元与计算中心系统、基础设施单元、专用用户终端、卡证读写设备、卡证之间应实现安全注册和基于密钥或证书的身份认证等功能；
c) 载运装备单元的身份标识装置应具备防逻辑破坏和伪造等功能，发现标识异常时，应上传警示信息，当不影响交通安全时，应停止其服务。

8.3 应用软件次全

应用软件安全技术要求包括：
a) 载运装备单元应用应经过相关的授权和安全评估，并选择具有相应安全措施（如安全启动、安全升级、安全通信、安全存储、安全监控、恶意代码防护等）的软件；
b) 载运装备单元应用软件应根据功能和操作需求确定应用优先级，包括生命安全级、行驶辅助级和增值服务级，生命安全级包括紧急碰撞与伤害减弱、潜在碰撞与伤害减弱和防止、紧急事件通知、紧急情况通知等应用；
c) 生命安全级、行驶辅助级的应用软件应进行安全性的专项测试，增值服务级应用软件按需进行安全性专项测试；
d) 生命安全级、行驶辅助级和增值服务级的资源占用优先级应逐级降低。

8.4 数据次全

数据安全技术要求包括：
a) 载运装备单元与计算中心系统、基础设施单元、专用用户终端、卡证读写设备、卡证之间的网络传输和通信应确保数据的保密性、完整性和可用性；
b) 载运装备单元与计算中心系统、基础设施单元、专用用户终端、卡证读写设备之间的网络传输和通信应能辨识数据的有效性和新鲜性等，并具有数据过滤功能；

c) 对范运术语(包括车考、车辆使范者、车辆技体术语、车辆文行数据等)元采集、存储、传件性使范,应经过范运元明确授权。

8.5 义系和运

入侵防前略规交通包括:

a) 息文系统安全操作和定应遵循最小义系原基,计具统相应元恶意代码防前设力;

b) 应对息文系统实现远程访问元信算进行严格控制,络闭不必交元信算;

c) 应对息文系统元缩心访问点(如蓝牙、USB、光驱、诊断接算、调试接算、引中和定、TPMS 射频用术、车钥匙射频用术、RFID 等)进行配置、访问控制(如白名安、数据流向、数据内容等);

d) 息文系统络键端载边界架统(如 T-BOX、端络等)需施供边界义缩防护功设;

e) 息文系统安全装外心用术采范义缩接入方式,计根据应范优先级,用过不同元用术和定义缩接入端载;

f) 应采范逻辑隔离或其他略规措构,实现生命义缩级、行驶辅助级、增值服务级应范元边界防护;

g) 承息生命义缩级、行驶辅助级应范元息文系统安全应具统入侵防护功设性相应元报警设力,遵循故障义缩原基。

9 全规范围性引交通件息术语

9.1 统营安者户交通

物与性环境义缩略规交通包括:

a) 应具统防盗、防献、防火、防水等物与义缩防护设力性报警功设;

b) 应设保证持续元电力供应;

c) 应在中置选择时避免强光、电磁等辐射源元干扰;

d) 应具统抵御电磁、用术等干扰元设力;

e) 重交元技体架构安全应用过冗余或其他措构确保和定可范言,应设够监测架统状态计在和定不可范时报警。

9.2 全规范围性引范用终端

技体架构安全架统备识略规交通包括:

a) 应具网可寻址元唯一言备识,发础术语传件时应进行自身身参备识;

b) 技体架构安全元身参备识系置应具统防物与拆卸、逻辑破坏性伪造等功设,发现备识异常时,应上传警示术语或停止服务;

c) 技体架构安全装要求户终和定、息文系统安全或专范范运输信、卡证读写架统、卡证之间应实现义缩注册性技于密钥或证书元身参认证等功设。

9.3 文输定信交通

应范软围义缩略规交通包括:

a) 技体架构安全应范软围应经过相络元授权性义缩评估,计选择具网相应义缩措构(如义缩启动、义缩升级、义缩用术、义缩存储、义缩监控、恶意代码防护等)元软围;

b) 技体架构安全应范软围应根据功设性操作需通确引应范优先级,包括生命义缩级、行驶辅助级性增值服务级;

c) 生命义缩级、行驶辅助级元应范软围,应进行义缩言元专项测试,增值服务级应范软围单需进行义缩言专项测试;

d) 生命安全级、行驶辅助级和增值服务级的资源占用优先级应逐级降低。

9.4 数据通信安全

数据通信安全技术要求包括：

a) 基础设施单元一般不应存储关键业务数据，确需存储的应存储于安全单元或者达到同样安全等级的芯片中；

b) 基础设施单元与计算中心系统、载运装备单元或专用用户终端、卡证读写设备、卡证之间的网络传输和通信应确保数据的保密性、完整性和可用性；

c) 基础设施单元与计算中心系统、载运装备单元或专用用户终端、卡证读写设备之间的网络传输和通信应能辨识数据的有效性和新鲜性等，并具有数据过滤功能；

d) 视频监控设备应具有数据签名功能；

e) 语音、视频等发布类系统应采用校验码技术、特定的文件格式协议或等同强度手段保证数据完整性。

9.5 入侵防范

入侵防范技术要求包括：

a) 应拆除或封闭不必要的 USB、光驱、无线等接口。若确需使用，应通过技术手段实施严格访问控制；

b) 应具抵御远程非法控制的能力；

c) 应能监测到广播、电子指示等基础设施侧设备的非法接入并报警；

d) 承载照明控制、通风控制、消防控制、船闸控制等系统运行的网络，应和其他网络实现物理隔离。

10 计算中心安全技术要求

10.1 物理和环境安全

物理和环境安全技术要求包括：

a) 机房应选择在具有防震、防风和防雨等能力的建筑内；

b) 机房应具备访问控制、防盗窃和防破坏等措施；

c) 机房应设置避雷、火灾自动消防、防静电、防水和防潮等装置；

d) 机房应设置温、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；

e) 应用确保系统电力的持续供应；

f) 应采用电磁防护措施，防止外界电磁干扰、设备寄生干扰和线路相互干扰等；

g) 确保云计算服务器、承载云租户账户信息、鉴别信息、系统信息及运行关键业务和数据的物理设备均位于中国境内。

10.2 设备和主机安全

设备和主机安全技术要求包括：

a) 应满足交通运输信息系统安全通用技术要求；

b) 应具备系统的资源控制能力，对重要节点进行监视，包括监视 CPU、硬盘、内存等资源的使用情况；

c) 应能够对重要节点的服务水平降低到预先规定的最小值进行检测和报警；

d) 应采取必要的措施对重要节点的设备和主机的安全漏洞和隐患进行检测、报警和修补；

e) 应具备维护漏洞管理机制的升级和更新的能力，交通运输专网、局域网等应采取技术手段及时升级漏洞管理机制；
f) 应提供重要节点设备的硬件冗余。

10.3 云计算平台安全

云计算平台架构安全技术要求包括：

a) 实现不同云租户虚拟网络之间的隔离；
b) 保证云计算平台管理流量与云租户业务流量分离；
c) 云租户能根据业务需求自主设置安全策略集并加载安全服务；
d) 确保只有在云租户授权下，云服务方或第三方才具有云租户数据的管理权限；
e) 保证分配给虚拟机的内存空间仅供其独占访问；
f) 能够对应用系统的运行状况进行监测，并在发现异常时进行告警；
g) 能监测到虚拟机与宿主机之间的异常流量，并进行告警；
h) 提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
i) 针对重要业务系统提供加固的操作系统镜像；
j) 当进行远程管理时，管理终端和云计算平台边界设备之间应建立双向身份验证机制；
k) 保证云服务方对云租户系统和数据的操作可被云租户审计；
l) 能监测到云租户的网络攻击行为，并能记录攻击源地址、攻击目标地址、攻击时间、攻击流量等信息；
m) 虚拟机所使用的内存和存储空间回收时，应实现不可恢复清除。

10.4 应用软件安全

应用软件安全技术要求包括：

a) 应用软件上线前，均应通过软件安全性测试；
b) 应用软件应及时升级到最新版本，在软件升级前应进行必要的验证；如需远程升级，需在具有系统安全保障的条件下进行，并记录升级过程的相关信息；
c) 重要应用软件应具备相应的抗应用层攻击和渗透入侵能力；
d) 应用软件应能监测、记录软件自身的运行状态和安全事件，留存相关的日志不少于 6 个月；
e) 重要应用软件在故障发生时，应自动保存易失性数据和所有状态，保证系统能够进行恢复；
f) 重要应用软件在故障发生时，应能够继续提供一部分功能，确保能够实施必要的措施。

10.5 数据安全

数据安全技术要求包括：

a) 应采用校验码技术或密码技术保证交通运输重要数据在传输过程和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、重要个人信息等；
b) 应采用密码技术保证交通运输重要数据在传输过程和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、重要审计数据、重要个人信息等；
c) 交通运输信息系统运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内安全存储；
d) 应提供交通运输重要数据的备份与恢复功能，定期备份重要数据；
e) 交通运输关键信息基础设施等应提供异地备份功能；
f) 应仅采集和保存业务必需的用户个人信息（姓名、交通工具编号等），并对其用户信息严格保密，建立健全用户信息保护制度；

g) 应采取技术手段防止未经授权访问和非法使用用户个人信息；
h) 应采取技术手段保证存有敏感数据的存储空间被释放或重新分配前实现不可恢复清除；
i) 应定期备份关键业务数据；
j) 云租户应在本地保存其业务数据的备份；
k) 应提供查询云租户数据及备份存储位置的方式；
l) 应具备将业务系统及数据迁移到其他云计算平台和本地系统的技术手段。

10.6 入侵防范

入侵防范技术要求包括：
a) 应能检测和阻止从外部发起的对计算中心的攻击行为；
b) 应能检测和阻止从内部发起的对计算中心的攻击行为；
c) 当检测到攻击行为时，应能记录攻击源地址、攻击目标地址、攻击时间等信息，并能够提供报警功能。

11 网络与通信安全技术要求

11.1 物理和环境安全

物理和环境安全技术要求包括：
a) 网络与通信设备应具备防盗、防雷、防火、防水等物理安全防护能力和报警功能；
b) 网络与通信设备应能保证持续的电力供应；
c) 网络与通信设备应具备抵御电磁、通信等干扰的能力。

11.2 网络架构安全

网络架构安全技术要求包括：
a) 交通运输专网应采取技术措施与互联网实现逻辑隔离；
b) 应保证网络设备的处理能力和带宽资源满足交通运输业务信息通信高峰期的需要；
c) 应提供通信线路、关键网络设备的硬件冗余，保证信息系统的可用性；
d) 应合理划分安全域、子网或网段，通过采用可靠的技术隔离措施等方式保证网络结构安全；
e) 应避免将重要交通信息系统部署在网络边界处且没有边界防护措施。

11.3 通信传输安全

通信传输安全技术要求包括：
a) 应能够采用密码技术保证交通运输信息通信过程中数据的完整性；
b) 应采用密码技术保证交通运输信息通信过程中敏感信息或整个报文的保密性；
c) 应能够在通信前基于密码技术对交通运输信息通信的双方进行验证或认证；
d) 应可按照业务服务的重要程度为交通运输数据设置优先级并据此分配带宽，优先保障高优先级的重要业务。

11.4 边界防护

边界防护技术要求包括：
a) 应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信；
b) 应能够对非授权设备私自连到交通运输业务专网的行为进行限制或检查，并对其进行有效阻断；

c) 应能够对交通运输业务内部用户非授权连到互联网的行为进行限制或检查，并对其进行有效阻断；
d) 应确保有线网络与无线网络边界之间的通信经过无线接入网关设备；
e) 宜禁用无线接入设备和无线接入网关等存在风险的功能。

11.5 集中管控

集中管控技术要求包括：

a) 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；
b) 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；
c) 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；
d) 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；
e) 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；
f) 应能对网络中发生的各类安全事件进行识别、报警和分析。

11.6 访问控制

访问控制技术要求包括：

a) 进行网络或通信设备的远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；
b) 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，默认情况下受控接口除允许的通信外，拒绝所有通信；
c) 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；
d) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
e) 应能根据会话状态信息为进出的交通运输数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。

11.7 入侵防范

入侵防范技术要求包括：

a) 应在关键网络节点处检测、防止或限制从外部发起的对交通运输信息网络的攻击行为；
b) 应在关键网络节点处检测和限制从内部发起的对交通运输信息网络的攻击行为；
c) 应采取技术措施对交通运输信息系统的网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析；
d) 当检测到攻击行为时，记录攻击源地址、攻击目标地址、攻击时间等，并能够提供报警功能；
e) 应能够对非授权用户终端接入的行为进行检测、记录和定位；
f) 应具备对无线接入设备的网络扫描、拒绝服务攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录、分析和定位的能力。

参 考 文 献

[1] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求