联网收费系统省域系统并网接入网络安全基本技术要求解读

贺文涛

交通运输部路网监测与应急处置中心

2019年10月24日

目　录

一、编制背景

按照取消高速公路省界收费站总体工作部署，在撤站工作网络安全专项工作组的领导下，为指导规范省域联网收费系统安全规划设计、设备选型、建设实施、并网接入安全检测，保障联网收费系统整体网络安全，为联网收费系统长期安全稳定运行奠定基础，制订了《联网收费系统省域系统并网接入网络安全基本技术要求》（以下简称“接入要求”）。

部路网中心负责并网接入网络安全管理，组织实施各级系统并网接入。

一、编制背景

一是 未严格落实国家等级保护制度要求，部分省级联网收费系统定级为二级，有的甚至只对系统的一部分进行了定级；

二是 网络安全管理体系不完善，责任主体不清晰，专业人才队伍严重不足；

三是 网络边界防护措施存在重大隐患，部分省份的收费站、分中心、省中心之间访问无限制措施；

四是 数据保护。技术防控措施不完善，部分省份数据明文传输和存储，存在数据泄露风险；

五是 联网收费系统及基础运行环境存在较严重的安全隐患，安全漏洞发现及处置机制不完善，多省仍然存在“永恒之蓝”漏洞。

二、编制原则

充分结合《取消高速公路省界收费站总体技术方案》提出的网络架构和系统组成，适应云计算、物联网、大数据等新技术，全面贯彻落实国家网络安全等级保护新制度、新标准，主要遵循六项基本原则：

一是 结合总体技术方案

二是 充分全面贯彻落实等级保护2.0标准

三是 充分结合撤站任务实施安排

四是 坚决守住整体安全策略

五是 充分考虑方案的实施成本

六是 兼顾当前和长远的发展要求

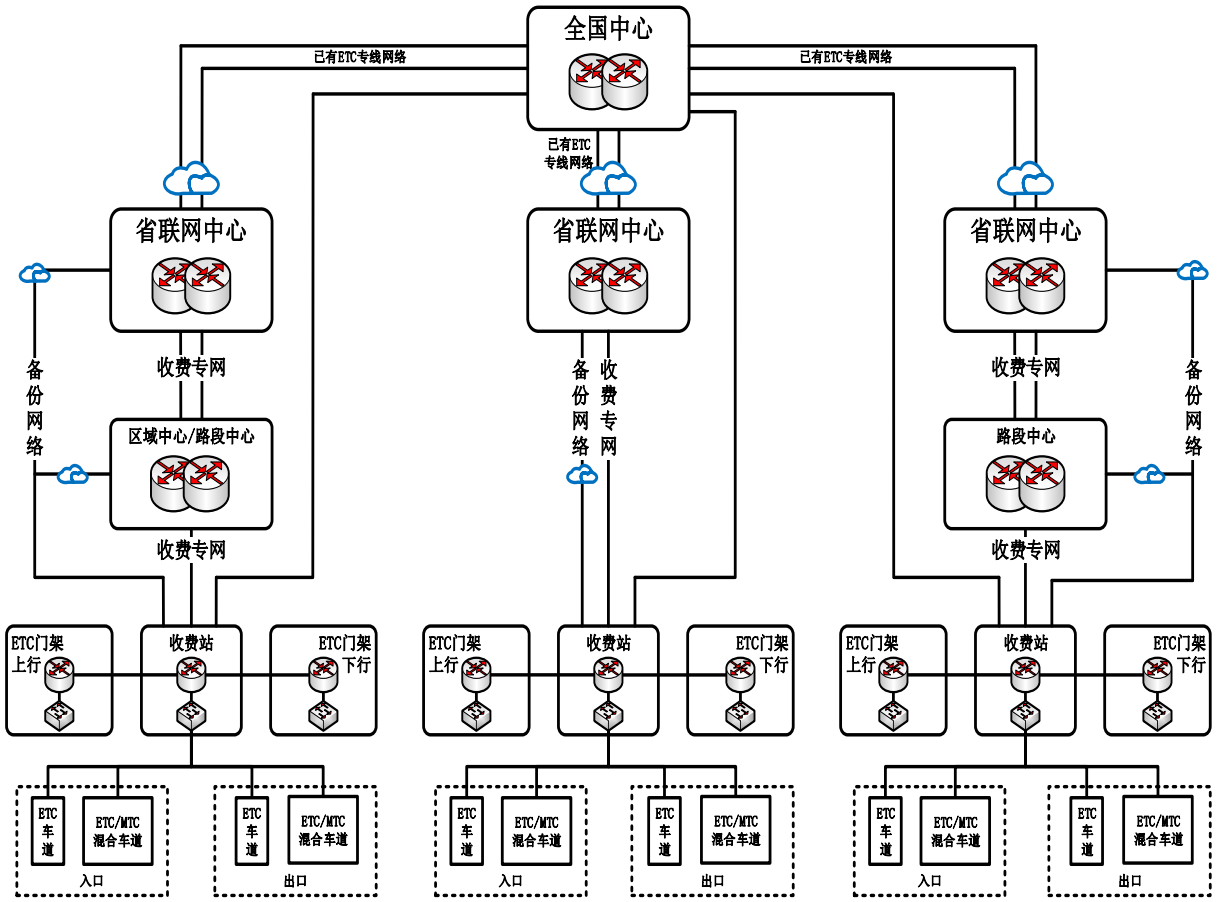
三、编制思路

针对联网收费系统安全保护对象，构建从外到内的纵深安全防御体系，从收费专网与互联网边界划分、收费专网应用分类分区、区域内部网络资源、计算环境等逐层提出要求；综合运用互补的安全措施，比如，对于通信传输的数据完整性、保密性要求，由于部站之间链路形态复杂、点多等困难，难以实现通信链路加密，接入要求中考虑提出使用应用层数据加密的方式来降低风险。

四、保护对象-通信网络架构

联网收费系统总体架构由全国收费公路联网结算管理中心（以下简称全国中心）、省（区、市）联网结算管理中心（以下简称省联网中心，含具有清分结算功能的区域及路段中心）、省内区域/路段中心、ETC门架、收费站、收费车道（MTC车道、ETC车道）等组成。

为保证数据实时传输，ETC门架和收费站到省联网中心、全国中心采用主备双链路，主用链路采用省内现有收费通信网络，备份通信链路可采用电信运营商专线网络（或现有全国高速公路信息通信干线传输系统网络）。省联网中心到全国中心复用已有跨省清分结算通信链路。为加强联网收费系统运行监测，建立联合稽查和信用管理体系，建立全国中心与收费站、ETC门架的直连链路。



四、保护对象-联网收费系统

联网收费系统由全国中心系统、省联网中心系统、ETC门架系统、收费站（ETC 车道系统、ETC/MTC 混合车道系统）、结算系统、ETC 发行系统、客服系统、稽查与信用管理系统、在线密钥管理系统组成。根据各业务模块功能特点，可将联网收费系统分为三大类：

业务数据处理类系统

对收费数据进行计算和存储的相关系统，主要包括：结算系统、在线密钥管理与服务系统等，该类系统对数据完整性、保密性和可用性具有较高的要求。

业务生产控制类系统

对车辆的通行进行管理控制的相关系统，主要包括： ETC门架系统、收费车道系统等，该类系统对控制类数据的完整性和业务连续性方面具有较高的要求。

业务辅助类系统

辅助支撑业务数据处理和业务生产控制的信息系统，主要包括：ETC发行系统、CPC卡发行与管理系统、客服系统、稽查与信用管理系统等，一般不对收费系统核心业务运行产生影响，但根据其系统特性，对数据完整性、保密性或业务连续性存在响应要求。

四、保护对象-重要数据

联网收费系统根据功能和数据特点，重要数据可以分为以下四类：

一是 鉴别数据

（验证用户身份的信息)

二是 关键业务数据

（交易和清分数据、拆分数据等）

三是 服务支持数据

（基础数据、费率数据、黑名单数据、稽查数据、 车辆图像数据等）

四是 公民个人信息

五、总体要求-安全技术框架

根据国家网络安全政策法规和技术标准体系的有关要求，落实网络安全等级保护制度，围绕联网收费三类系统的安全保护需求，针对联网收费系统重要数据和业务系统进行分级分类管理，从安全物理环境、安全通信网络、安全区域边界、安全计算环境及安全管理中心等五个方面提出通用安全要求以及云计算、大数据及物联网三个方面提出扩展安全要求，以建立联网收费系统网络安全技术防护体系，构建综合防御能力。

五、总体要求-整体安全保护要求

联网收费系统在整体上，应确保收费专网的专网属性，一是严格控制外部网络接入，明确联网收费系统与银行、公安等外部单位的边界保护规则，在统一安全策略下由全国中心或省中心统一提供出口，并在内部建立独立的接入区域，设置严格的逻辑隔离及安全审计措施。

收费专网内部合理划分网络安全区域，并通过有效技术措施对安全区域进行隔离，确保安全控制策略有效、安全风险影响范围最小，综合运用互补的安全措施，构建从外到内的网络安全纵深防御体系。

同时，充分考虑国家安全战略要求及新技术发展和应用，设备及应用有效支持IPv6，推进关键软硬件设备国产化，实现联网收费系统安全、稳定、高效运行。

五、总体要求-全国中心

联网收费系统整体严格落实国家网络安全等级保护要求，全国中心按照国家关键信息基础设施进行保护，全面落实等级保护第三级要求，并适当予以增强。

建立基于行为的安全管控措施，形成部省一体的全方位网络安全态势感知体系。

建立完善的联网收费系统密钥管理体系，支撑省联网中心、路段中心、收费站及ETC门架系统在身份鉴别、访问控制、数据安全等方面的密码技术应用需求，建立联网收费系统网络安全信任体系。

五、总体要求-省域系统

省联网中心整体按照等级保护第三级进行定级、备案、建设、测评、保护，运用云计算、大数据等技术时参照等级保护第三级扩展要求开展相关工作。

推动省联网中心逐步建立覆盖收费站及ETC门架系统的网络安全态势感知平台，与全国中心态势感知平台实现对接，能够按统一要求上报安全相关数据。

收费站及ETC门架系统参照网络安全等级保护中在安全通信网络、安全区域边界及安全计算环境等方面的三级安全保护要求，同时充分考虑外场设备的物联网属性，开展安全保护。

五、总体要求-省域系统

区域/路段中心系统与联网收费系统存在网络连接和数据交换，是全网系统的重要接入点和组成部分，参照网络安全等级保护中安全通信网络、安全区域边界及安全计算环境方面的三级安全保护要求开展安全保护。

ETC发行系统支撑联网收费业务开展，与联网收费系统存在网络连接和数据交互，应按照等级保护第三级要求进行定级、备案、测评、保护，严格管控其与其他网络区域的网络连接和数据交互，并按照国家相关标准重点加强对个人信息保护。

五、总体要求-接入检测要求

省域联网收费系统中，省联网中心系统接入全国中心须提供等级保护测评报告，并经过具有网络安全等级测评或信息安全风险评估等相关资质的第三方检测评估机构依据本技术要求进行安全接入检测，并出具技术要求符合性检测报告。

路段中心、收费站、ETC门架系统接入联网收费系统应经过具有网络安全等级测评或安全风险评估等相关资质的第三方检测评估机构，依据本技术要求进行安全接入检测，并出具技术要求符合性检测报告。

六、主要内容-省级联网中心安全要求

省联网中心系统包含省级清分结算系统等业务处理类系统，省级稽查与信用管理系统、密钥管理系统、客服系统等业务辅助系统，以及网络基础运行环境。具有清分结算功能的区域/路段中心以省联网中心安全要求为标准。

六、省级联网中心-安全通用要求

5.1.1 安全物理环境

5.1.1.1机房物理位置选择

a)机房和办公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；

c)机房场地应当避开强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区。

5.1.1.2 机房物理访问控制

a) 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。

5.1.1.8 温湿度控制

a)机房应设置温湿度自动调节设施，使机房内的温度和湿度的变化在设备运行所允许的范围内，机房温度范围为 23±1℃，湿度范围为40%-55%。

六、省级联网中心-安全通用要求

5.1.2 安全通信网络

5.1.2.1网络架构

a)应保证核心交换机、核心路由器、出口防火墙等网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；

b) 应保证部省连接、下级单位接入等线路网络的带宽满足业务高峰期需要；

c) 应根据业务职能、重要性和所涉及信息的重要程度等因素，根据需要至少划分收费业务应用、其他业务应用、数据服务、传输接入、运维管理等不同的网络区域，单独划分测试区域，应通过有效措施对各网络区域进行技术隔离，并按照便捷管理和集约管控的原则为各网络区域分配地址，采用白名单固定IP方式（由全国中心统一划分，原则上不超过10个）与全国中心通信;

d) 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，与全国中心通信应采用双机热备;

e)联网收费系统不得直接提供互联网服务，如与互联网应用存在数据交换，应通过设置网闸或者双防火墙方式实现隔离

六、省级联网中心-安全通用要求

5.1.2 安全通信网络

5.1.2.2通信传输

a)应至少采用校验技术保证部省、省站通信过程中数据的完整性，不宜使用UDP、FTP协议，根据需要还可采用符合国家密码主管部门要求的密码技术，保证通信过程中数据的完整性。

b) 应应采用符合国家密码主管部门要求的密码技术，保证部省、省站通信过程中的保密性。

c)密码算法应符合国家密码管理局相关规范要求。

5.1.3 安全区域边界

5.1.3.1 边界防护

a) 保证跨越网络区域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；

b) 应能够对非授权设备私自联到收费专网的行为进行检查或限制，能够对收费专网终端或用户非授权连接到外部网络的行为进行检查或限制，阻止非授权访问；

c) 收费专网应严格禁止无线局域网络的使用。

六、省级联网中心-安全通用要求

5.1.3 安全区域边界

5.1.3.2访问控制

a) 应在5.1.2.1划定的网络区域边界防护设备上（如防火墙）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) 优化防火墙等安全设备的访问控制列表，删除多余或无效的访问控制规则，使访问控制规则数量最小化；

c) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为传输层端口级，对源地址、目的地址、源端口、目的端口和协议等进行检查，确定是否允许数据包进出该区域边界。

六、省级联网中心-安全通用要求

5.1.3 安全区域边界

5.1.3.3入侵防范

a) 应在核心交换机等关键网络节点处部署具备入侵检测功能的设备，检测从内部/外部发起的网络攻击行为；

b) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；

c) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警，通过人工阻断方式或配置相应入侵防御设备，防止或限制从内部和外部发起的网络攻击行为。

六、省级联网中心-安全通用要求

5.1.3 安全区域边界

5.1.3.5安全审计

a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要的安全事件进行审计，能对远程访问的用户行为单独进行行为审计和数据分析；

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) 审计记录留存6个月以上。

六、省级联网中心-安全通用要求

5.1.4 安全计算环境

5.1.4.1 身份鉴别

a) 应对登录网络、服务器、中间件、数据库、终端及应用等计算环境的用户进行身份标识和鉴别，且保证用户名具有唯一性；

b) 应采用口令、密码技术、生物技术等鉴别技术对用户进行身份鉴别，并对鉴别数据进行保密性和完整性保护，对管理员、运维人员、重要业务系统（业务数据处理类）用户应采取两种或两种以上组合的鉴别技术；

c) 若只采用“用户名+口令”的方式进行身份鉴别，口令须满足大小写英文字母、数字、特殊字符3种以上组成、长度不少于8位，每90天更换；

d) 应启用登录失败处理功能，登录失败后采取结束会话、限制非法登录次数和自动退出等措施，连续5次登录失败至少锁定10分钟；

e) 当进行远程管理时，应采取SSH、HTTPS等方式防止管理数据、鉴别信息在网络传输过程中被窃听；

f) 应为与全国中心之间进行通信的计算设备、安全防护设备实现双向身份标识认证，保障部省传输的安全。

六、省级联网中心-安全通用要求

5.1.4 安全计算环境

5.1.4.6 数据完整性

a) 采用校验码技术或密码技术保证重要数据在传输和存储过程中的完整性，并在检测到完整性错误时采取必要的恢复措施，包括但不限于鉴别数据、关键业务数据（交易和清分数据、拆分数据等）、服务支持数据（基础数据、费率数据、黑名单数据、稽查数据、车辆图像数据等）和公民个人信息等；

b) 密码算法应符合国家密码管理局相关规范要求。

5.1.4.7 数据保密性

a) 采用密码技术保证重要数据在传输和存储过程中的保密性，包括但不限于鉴别数据和公民个人信息等；

b) 密码算法应符合国家密码管理局相关规范要求。

六、省级联网中心-安全通用要求

5.1.4 安全计算环境

5.1.4.8 数据备份恢复

a) 应提供关键业务数据（交易和清分数据、拆分数据等）、服务支持数据（基础数据、费率数据、黑名单数据、稽查数据、车辆图像数据等）等的本地数据备份与恢复功能，每周至少进行一次全备份，每天进行增量备份；

b) 应提供异地备份功能，利用通信网络将关键业务数据（交易和清分数据、拆分数据等）备份至备份场地，有条件的可提供异地实时备份功能；

c) 应提供关键业务数据（交易和清分数据、拆分数据等）处理系统的热冗余，保证系统的高可用性。

六、省级联网中心-安全通用要求

5.1.5 安全计算环境

5.1.5.2 集中管控

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，并保证审计记录的留存时间符合法律法规要求；

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。

六、省级联网中心-云安全扩展要求

省联网中心如有部分系统部署在私有云平台（含虚拟化资源池）或公有云平台（含专属云平台，不得为业务数据处理类系统）应遵循云安全扩展要求。使用公有云平台应确保其云计算基础设施位于中国境内，并提供等级保护第三级备案证明。--对使用的云平台提出的要求

云平台（云管平台+安全组件）配合密码技术实现安全通信网络、安全区域边界、安全计算环境、安全管理中心相关要求。

5.2.3.4 镜像和快照保护

a) 针对收费系统、稽查与信用管理系统等部署在云中的联网收费业务系统提供加固的操作系统镜像；

b) 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。

六、省级联网中心-大数据安全扩展要求

a) 大数据平台应对数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别；
b) 大数据平台应为大数据应用提供管控其计算和存储资源使用状况的能力；
c) 大数据平台应对其提供的辅助工具或服务组件，实施有效管理；
d) 大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行；
e) 大数据平台应提供静态脱敏和去标识化的工具或服务组件技术；
f) 大数据平台应提供数据分类分级安全管理功能，供大数据应用针对不同类别级别的数据采取不同的安全保护措施；
g) 涉及重要数据接口、重要服务接口的调用，应实施访问控制，包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作；
h) 应在数据清洗和转换过程中对重要数据进行保护，以保证重要数据清洗和转换后的一致性，避免数据失真,并在产生问题时能有效还原和恢复。

六、主要内容-收费站安全要求

收费站系统主要包括：ETC车道系统、ETC/MTC混合车道系统、站级管理系统及有关网络基础运行环境。收费站安全要求主要包括两方面内容，分别是：安全通用要求和物联网安全扩展要求；综合上述两方面构建具备其相应安全保护能力的网络安全综合防御体系。收费站在省联网中心要求的基础上，降低了部分安全要求，不再提出安全管理中心的要求，重点关注通用安全要求中通信网络和计算环境的相关要求。

六、收费站-安全通用要求

6.1.2 安全通信网络

6.1.2.1 网络架构

a) 应保证通信设备的业务处理能力具备冗余空间，以满足业务高峰期需要；

b) 应保证收费站与全国中心、省联网中心、路段中心等传输线路网络带宽满足业务高峰期需要；

c) 应通过交换机或防火墙等设施至少划分收费业务、运维管理、设备接入等不同的网络区域，并为ETC门架系统接入单独设置网络区域，按照便捷管理和集约管控的原则为各网络区域分配地址，通过有效措施对各网络区域进行技术隔离；

d) 收费站和全国中心、省联网中心、区域/路段中心的通信传输应提供链路冗余，主干链路的通信和安全防护等关键设备应采用双机备份。

六、收费站-安全通用要求

6.1.3 安全区域边界

6.1.3.1 边界防护

a) 应保证跨越网络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；

b) 应能够对非授权设备私自联到收费网络的行为进行检查或限制，能够对收费网终端或用户非授权连接到外部网络的行为进行检查或限制；

c) 收费专网一般应禁止无线局域网络的使用，如使用，应采用证书认证技术确保移动设备的可信接入。

6.1.3.2访问控制

a) 在网络区域边界上配置访问控制策略，默认情况下除允许通信外，受控接口拒绝所有通信；

b) 优化安全设备的访问控制列表，删除多余或无效的访问控制规则，使访问控制规则数量最小化；

c) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为传输层端口级，对源地址、目的地址、源端口、目的端口和协议等进行检查，确定是否允许数据包进出该区域边界。

六、收费站-物联网安全扩展要求

6.2.1安全物理环境

a) 应具备防水、防潮、防尘设计，防护等级应不低于IP55。

6.2.2 安全区域边界

6.2.2.1接入控制

a) 应提供设备认证能力，保证只有授权的设备可以接入，与全国中心之间连接实现双向身份标识认证。

6.2.2.2 入侵防范

a) 应能够限制与设备通信的目标地址，以避免对陌生地址的攻击行为。

6.2.3 安全计算环境

6.2.3.1 设备安全

a) 应保证只有授权的用户可以对设备上的软件应用进行配置或变更；

b) 设备应支持远程集中管控。

六、主要内容-ETC门架系统安全要求

ETC门架系统主要包含ETC门架收费软件，车道控制器、RSU、车牌图像识别等设施设备及有关网络基础运行环境。

ETC门架系统业务数据通过收费站与省联网中心和全国中心建立连接，收费站内为门架系统服务的设备，按照收费站安全要求进行保护；多个门架系统共用收费站部署的一套计算环境和网络环境，可统筹考虑安全防护。同时，门架系统可视情况复用、共用收费站的网络安全物理环境、网络环境和计算环境。

ETC门架系统安全要求主要包括两方面内容，对站级服务器等设备提出通用安全要求，ETC门架系统选取的摄像头、天线等终端设备参考物联网安全要求。

六、ETC门架-安全通用要求

7.1.1 物理防护

7.1.1.1物理位置选择

a) ETC门架系统应将计算设备和通信设备布设在具有温湿度控制、防盗防破坏的环境，并通过有线通信网络与门架设备连接。

b) 应远离强电磁干扰环境，避免对ETC门架系统设备的正常工作造成影响。

7.1.1.2物理访问控制

a) 布设RSU、高清车牌视频识别等终端设备的ETC门架严禁非授权人员攀登。

7.1.1.3防盗和防破坏

a) 应将ETC门架系统的车道控制器、通信设备、供电设备等放置在机柜内，设备及主要部件须进行固定，并设置明显的不易除去的标记；

b) 室外机柜应具备硬件防盗设计，柜体无裸露可拆卸部件，保障柜体难以从外部撬开；

c) 应通过电子门锁、视频监控、设备状态监测等手段对箱体开启情况进行监控记录，及时发现设备的丢失、损坏等异常状态。

六、ETC门架-安全通用要求

7.1.1.4防雷击

a) 室外机柜内部应集成防雷和接地保护装置，具备防雷击和防浪涌冲击的能力。

7.1.1.5防火

a) 室外机柜应布设剩余电流式电气火灾监控探测器、测温式电气火灾监控探测器等监测设备；

b) 室外机柜柜体应采用铁皮或其他防火材料。

7.1.1.6 防尘和防水（防潮）

a) 室外机柜应具备防尘、防水（防潮）设计，防护等级应不低于IP55，部分地区可根据气候地理条件，采用更高的防护标准。

7.1.1.7 温湿度控制

a) 室外机柜应集成空调，支持柜内温度自动调节，保障柜内设备运行在所允许的范围内；

b) 室外机柜应具备温湿度传感器，ETC门架系统室外设备工作温度范围应至少应满足-20℃~+55℃（寒区-35℃~+40℃），湿度范围应满足5%~95%（无凝露），各地区可根据气候地理条件，进行温湿度适应范围调整。

7.1.1.8 电力供应

a) 应配备备用电力供应，保证ETC门架系统的持续电力供应，确保ETC门架系统 24 小时不间断工作。

六、ETC门架-安全通用要求

7.1.2 安全通信网络

7.1.2.1 网络架构

a) 应保证ETC门架系统相关通信设备的业务处理能力具备冗余空间，满足业务高峰期需要。

b) 应保证与全国中心、省联网中心等的传输线路网络带宽满足业务高峰期需要。

c) 应根据需要至少划分通信设备、计算设备等不同的网络区域，并按照便捷管理和集约管控的原则为各网络区域分配地址，应通过有效措施对各网络区域进行技术隔离；

d) ETC门架系统和省中心、部中心的通信传输应提供链路冗余，主干链路的通信和安全防护等关键设备应采用双机备份。

7.1.2.2 通信传输

a) 应至少采用校验技术保证与全国中心、省联网中心通信过程中数据的完整性，根据需要可采用密码技术，保证与全国中心、省联网中心通信过程中数据的完整性。

b) 应采用密码技术保证与全国中心、省联网中心通信过程中的保密性。

c) 密码算法应符合国家密码管理局相关规范要求。

六、ETC门架-安全通用要求

7.1.3 安全区域边界

7.1.3.1 边界防护

a) 通过边界防护设备，保证跨越网络区域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；

b) 应能够对非授权设备私自联到收费专网的行为进行检查或限制，能够对收费专网终端或用户非授权连接到外部网络的行为进行检查或限制，阻止非授权访问；

7.1.3.2访问控制

a) 可在网络区域边界上配置访问控制策略，默认情况下除允许通信外，受控接口拒绝所有通信；

b) 优化安全设备的访问控制列表，删除多余或无效的访问控制规则，使访问控制规则数量最小化；

c) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为传输层端口级，对源地址、目的地址、源端口、目的端口和协议等进行检查，确定是否允许数据包进出该区域边界。

六、ETC门架-安全通用要求

7.1.3 安全区域边界

7.1.3.3 入侵防范

a) 应在关键网络节点处检测网络攻击行为。

7.1.4 安全计算环境

7.1.4.1身份鉴别

a) ETC门架系统布设的RSU终端设备、车牌图像识别终端设备、服务器和计算机终端等设施的管理员进行身份标识和鉴别，且保证在系统整个生存周期用户名具有唯一性；

b) 身份鉴别可采用密码技术实现，若只采用“用户名+口令”鉴别方式，用户口令须由大小写英文字母、数字、特殊字符3种以上组成用户口令须由大小写英文字母、数字、特殊字符3种以上组成、长度不少于8位，每90天更换；

c) 启用登录失败处理功能，登录失败后采取结束会话、限制非法登录次数和自动退出等措施，连续5次登录失败至少锁定10分钟；

d) 当进行远程管理时，应采取SSH、HTTPS等方式防止鉴别信息在网络传输过程中被窃听。

六、ETC门架-安全通用要求

7.1.4.2 访问控制

a) 设定特定终端或网络地址范围，对通过网络进行管理的终端进行限制；

7.1.4.3 安全审计

a) 应启用安全审计功能，审计覆盖到每个远程连接管理的用户，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) 对审计进程进行保护，防止未经授权的中断。

六、ETC门架-安全通用要求

7.1.4.4 入侵防范

a) 遵循最小安装原则，所有设备仅安装需要的组件和应用程序，关闭不必要的系统服务、默认共享和高危端口；

b) 通过统一管理系统等手段，发现可能已知漏洞，并在经过充分测试评估后，及时修补漏洞。

c) 通过入侵检测、监测预警等监测手段，发现对ETC门架系统的入侵行为，发生严重入侵事件时提供报警。

d) 应严格对U盘、移动光驱等外来存储设备的管控，并对各类硬件设备的外接存储接口进行移除或限制。

7.1.4.5 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防御机制及时识别入侵和病毒行为，并将其有效阻断。

b) 对ETC门架系统服务器、终端设备进行统一恶意代码防范，支持防恶意代码的统一升级和管理。

六、ETC门架-安全通用要求

7.1.4.6数据完整性

a) 采用校验码技术或密码技术保证重要数据（指令数据、交易数据、费率数据、车辆图像数据等）在传输和存储过程中的完整性，并在检测到完整性错误时采取必要的恢复措施；

7.1.4.7数据保密性

a) 应采用密码技术保证ETC门架系统重要数据（指令数据、业务数据）在传输和存储过程中的保密性；

b) 可对发送方和接受方进行身份认证，在建立连接前，利用密码技术进行初始化会话验证，必要时采用专用传输协议或安全协议服务，避免来自基于协议的攻击破坏保密性；

c) 密码算法应符合国家密码管理局相关规范要求。

7.1.4.8数据可用性

a) 提供重要数据（指令数据、交易数据、费率数据、车辆图像数据等）的本地数据存储。

六、ETC门架-物联网安全扩展要求

7.2.1安全物理环境

a) 应具备防水、防潮、防尘设计，防护等级应不低于IP55。

7.2.2 安全区域边界

7.2.2.1接入控制

a) 应提供设备认证能力，保证只有授权的设备可以接入，与全国中心之间连接实现双向身份标识认证。

7.2.2.2 入侵防范

a) 应能够限制与设备通信的目标地址，以避免对陌生地址的攻击行为。

7.2.3 安全计算环境

7.2.3.1 设备安全

a) 应保证只有授权的用户可以对设备上的软件应用进行配置或变更；

b) 设备应支持远程集中管控。

六、主要内容-区域/路段中心系统安全要求

区域/路段中心系统包含：ETC门架系统的运行监测与预警系统、收费稽查管理系统等业务辅助类系统及有关网络基础运行环境，同时包含省联网中心与收费站的通信网络传输系统。区域/路段中心系统一般不承担联网收费业务生产控制、业务数据处理等核心业务，但其存在与省联网收费系统和收费站间的网络连接和数据交换。

区域/路段中心只规范通用安全要求，建立收费公路联网收费系统网络安全技术保护措施，构建具备其相应安全保护能力的网络安全综合防御体系。如区域中心具备清分结算功能的区域中心按省联网中心安全要求。

区域/路段中心在省联网中心系统安全要求的基础上，降低了部分安全要求，重点关注通用安全要求中通信网络和计算环境，以及对所辖范围内收费站的安全管理的相关要求。

六、主要内容-ETC发行系统安全要求

ETC发行系统主要包含发行中心系统、网点发行系统、互联网发行系统、便携式发行系统等。ETC发行系统不承担联网收费业务生产控制核心功能，但其与联网收费系统存在网络连接和数据交互，且存有大量公民个人信息。

ETC发行系统应按照等级保护第三级要求进行定级、备案、测评、保护，同时应通过严格的网络访问控制策略管控其与省联网中心系统的网络连接和数据交互，同时，针对互联网访问边界进行严格管控，并应按照《信息安全技术 个人信息安全规范》（GB/T 35273-2017）等有关国家标准重点加强个人信息保护。

谢谢聆听