联网收费系统省域系统并网接入网络安全检测规程解读

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、编制目的

为加强高速公路联网收费系统网络安全、规范省域系统并网接入安全检测工作、有效核验安全建设合规达标情况、管控安全接入关口，依据《联网收费系统省域系统并网接入网络安全基本技术要求》等文件，制定本规程。

以检促建　以检促防　以检促安

二、适用范围

本规程用于取消高速公路省界收费站工作中新改建的省联网中心、收费站、ETC门架系统、区域/路段中心、ETC发行等系统并网接入全国联网收费系统专网时，对《联网收费系统省域系统并网接入网络安全基本技术要求》的符合性进行检测，旨在核验取消省界站中省域系统网络架构、安全策略、设备配备等是否具备并网接入安全条件。软件功能性的并网接入不适用本规程。

三、检测依据

并网安全检测主要依据以下标准和规范进行：

一．《联网收费系统省域系统并网接入网络安全基本技术要求》

二．《收费公路联网收费系统网络安全管理暂行办法》

四、检测要求

一是 时间要求。并网接入网络安全检测，省域系统应在接入全国中心生产系统前完成。

二是 检测机构要求。并网安全检测应由国家有关部门认可的网络安全等级保护测评或信息安全风险评估机构承担。

三是 安全保密要求。应符合《收费公路联网收费系统网络安全管理暂行办法》对第三方服务安全管理的有关要求。签署保密协议，明确安全责任，防止敏感信息泄露。

四是 等级保护要求。省联网中心、ETC发行系统应通过等级保护第三级测评。

五、检测方法

并网安全检测应对照《并网接入网络安全符合性检测细则》（见附录A）中“要求小项”逐项开展符合性检测。

检测方法可采用访谈、文档核查、配置核查、案例验证测试、漏洞扫描测试、渗透性测试等方式。

五、结果判定

1. 检测报告结论为“通过”和“不通过”；
2. 单个“要求小项”的检测结果分为“符合”、“视同符合”、“部分符合”、“不符合”、“不适用”；符合记1分，视同符合记1分，部分符合记0.8分，不符合记0分，不适用不纳入记分项；
3. 标“*”的“要求小项”为“单项否决项”，任一项不符合则检测结论为“不通过”；
4. 省联网中心、ETC发行系统符合率低于90%则检测结论为“不通过”；收费站、ETC门架系统、路段/区域中心符合率低于80%则检测结论为“不通过”。
5. 符合率：记分项得分之和除以记分总数（记分项数）。

六、检测组织及接入管理

各省（区、市）按照分级检测、抽测复核、核准实施、整体接入的方式开展检测及接入管理工作。

省域自检测---各省（区、市）

并网接入管理---部路网中心、各省（区、市）

六、省域自检测

1. 省联网中心、收费站、ETC门架、区域/路段中心、ETC发行等系统的等级保护测评、技术要求符合性检测，由各省（区、市）结合实际情况自行组织实施。
2. 对省联网中心系统、ETC发行系统、具备清分结算功能或与全国中心系统直连的区域/路段中心系统，应实现100%检测，对其余区域/路段中心系统可采用抽检方式检测。
3. 在设计单位相同且建设施工单位也相同的条件下，对收费站系统、ETC门架系统的检测，可采用抽检方式开展，结合实际确定检测数量，抽检比例不得低于10%，且抽检数量不得少于2个。
4. 等级保护测评报告、技术要求符合性检测报告，应留档备查。

六、并网接入管理

1. 在省域自检测完成后，由省联网中心或其上级单位向部路网中心提出省域系统整体并网接入申请。
2. 由部路网中心对申请接入的省域系统开展复核，方式包括不限于现场技术检测、调阅文档、询问有关工作人员等。
3. 如果复核通过，则组织省域系统整体接入；如果复核不通过，由部路网中心通知申请单位开展自查及整改，并重新提交并网接入申请。

六、并网接入网络安全检测

条件准备-部级

1. 系统建设：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，通过自检测试和第三方检测机构安全检测。
2. 并网接入复核：组建复核队伍，由国家有关部门认可的网络安全等级保护测评或信息安全风险评估机构配合开展省级并网接入复核工作。

六、并网接入网络安全检测

条件准备-省级

1. 系统建设：按照《联网收费系统省域系统并网接入网络安全基本技术要求》完成省域安全系统建设；基本完成省域系统网络安全态势的初步感知能力建设。
2. 并网接入安全自检测：自行组织开展并网接入安全自检测【网络安全等级保护测评或信息安全风险评估机构】。
3. 材料准备：网络安全管理制度、内部操作规程、应急预案、记录文件、资产信息登记表、网络拓扑图等。

六、并网接入网络安全检测

省域自检测

1 各省区市分组，每组指定最迟提出省域系统整体并网接入申请时间

2 各省区市完成自检测后分批次在指定时间点前提出申请

3 可提前提出并网接入申请

4 检测机构按照报告标准模板出具

六、现场技术检测

部路网中心复核省域接入

1 根据分组和各省实际申请情况开展复核

2 复核覆盖各省（区、市）省域联网收费系统

3 复核方式包括不限于现场技术检测、调阅文档、询问有关工作人员等

4 以抽检方式现场技术检测，覆盖省界ETC门架系统

5 原则上现场技术检测不抽检各省自测抽取的系统、同一省（区、市）省域联网收费系统自检测机构与现场技术检测机构应不同。

六、并网接入网络安全检测

现场技术检测准备

1. 省域系统应完成对重要数据进行备份，对系统及设备的运行状态进行确认，明确系统的测试的时间段，做好应急处置的人员和工具准备。
2. 提供现场检测的场所，配备电源插座、网络接口等必备条件
3. 至少配备1名总协调人员和1名专业技术人员全程陪同，接受问询和事务处理

七、其他要求

1. 全国中心系统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，等级保护测评报告应为“优”级别，由部公路局和科技司负责监督管理。
2. 对在技术检测过程中弄虚作假的第三方服务机构，要严肃追究责任，并向全行业通报。

七、检测细则要点

省联网中心通用要求62个，其中单项否决项14个；云安全扩展要求29个，其中单项否决项3个；大数据扩展要求8个，其中单项否决项2个。

收费站通用要求36个，其中单项否决项 10个；物联网安全扩展要求9个，其中单项否决项1个。

ETC门架通用要求38个，其中单项否决项 4个；物联网安全扩展要求9个，其中单项否决项3个。

区域/路段中心通用要求42个，其中单项否决项 12个。

ETC发行系统通用要求12个，其中单项否决项 4个。

七、省联网中心-单项否决项

1 通用要求-安全物理环境-机房物理访问控制

- 安全要求：*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。
- 不符合判例：

满足条件（任意条件）

1.机房无电子或机械门锁，机房入口也无专人值守。

2.办公或外来人员可随意进出机房，无任何管控、监控措施。

- 补偿措施：机房配备24小时专人值守或配备摄像头实时监控，可视同符合。

七、省联网中心-单项否决项

2 通用要求-安全通信网络-网络构架

安全要求：a) *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。

不符合判例：

满足条件（任意条件）：

1.收费业务应用（业务数据处理类、业务生产控制类）与其他业务应用（业务辅助类等）在同一网络区域。

2.联网收费业务应用和外部单位存在共享或交换的设备在同一网络区域。

3.运维管理和业务应用在同一区域。

4.未单独划分测试区域。

补偿措施：无。

七、省联网中心-单项否决项

4 通用要求-安全通信网络-网络构架

- 安全要求：c）*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。
- 不符合判例：

满足条件（任意条件）：

1.与互联网连接，未设置网闸或双防火墙隔离措施。

2.与互联网区域边界隔离设备本单位无管理权限。

3.与互联网区域边界隔离设备访问控制措施配置不当，存在较大安全隐患。

- 补偿措施：无。

七、省联网中心-单项否决项

7 通用要求-安全区域边界-边界保护

- 安全要求：a) *应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。
- 不符合判例：

满足条件（任意条件）：

1.网络边界无任何访问控制措施。

2.网络边界访问控制措施配置不当，存在较大安全隐患。

3.网络边界控制措施失效，无法起到访问控制功能。

- 补偿措施：边界访问控制设备不一定必须是防火墙，只要是能实现相关的访问控制功能。内部网络边界如通过路由器、交换机或者带ACL功能的负载均衡器等设备实现，可视同符合。。

七、省联网中心-单项否决项

10 通用要求-安全区域边界-边界保护

- 安全要求：d）*收费专网应严格禁止无线局域网络的使用。
- 不符合判例：

满足条件：

存在和收费专网互联的无线网络。

- 补偿措施：无。

七、省联网中心-单项否决项

19 通用要求-安全区域边界-安全审计

- 安全要求：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。
- 不符合判例：

满足条件：

未部署网络审计系统、日志审计系统，从而在网络边界、重要网络节点无法对重要的用户行为和重要安全事件进行日志审计。

- 补偿措施：无。

七、省联网中心-单项否决项

22 通用要求-安全区域边界-安全审计

- 安全要求：d) *审计记录留存6个月以上。
- 不符合判例：

满足条件（任意条件）：

1.审计记录未留存6个月。

2.审计记录存储空间不足以存储6个月。

- 补偿措施：无。

七、省联网中心-单项否决项

26 通用要求-安全计算环境-身份鉴别

- 安全要求：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。
- 不符合判例：

满足条件（同时）：

1.可通过远程登录。

2.对连续登录失败无任何处理措施。

3.攻击者可利用登录界面进行口令猜测。

- 补偿措施：无。

七、省联网中心-单项否决项

29 通用要求-安全计算环境-访问控制

- 安全要求：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分配账户和权限。
- 不符合判例：

可通过直接访问URL等方式，在不登录系统的情况下，非授权访问系统重要功能模块。

- 补偿措施：无。

七、省联网中心-单项否决项

33 通用要求-安全计算环境-访问控制

- 安全要求：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。
- 不符合判例：

系统访问控制策略存在缺陷，可越权访问系统功能模块或查看、操作其他用户的数据。如存在平行越权漏洞，低权限用户越权访问高权限用户所能访问的功能模块等。

- 补偿措施：无。

七、省联网中心-单项否决项

35 通用要求-安全计算环境-安全审计

- 安全要求：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。
- 不符合判例：

满足条件（同时）：

1.业务数据处理类、业务生产控制类等应用系统无任何日志审计功能，重要核心网络设备、安全设备、操作系统、数据库等未开启任何审计功能，无法对用户的重要行为进行审计。

2.无其他技术手段对重要的用户行为和重要安全事件进行溯源。

- 补偿措施：使用堡垒机或其他第三方审计工具进行日志审计，能有效记录用户行为和重要安全事件；通过其他技术或管理手段能对事件进行溯源的;视同符合。

七、省联网中心-单项否决项

38 通用要求-安全计算环境-安全审计

- 安全要求：d) *审计记录留存6个月以上。
- 不符合判例：

满足条件（任意条件）：

1.审计记录未留存6个月。

2.审计记录存储空间不足以存储6个月。

- 补偿措施：无。

七、省联网中心-单项否决项

40 通用要求-安全计算环境-入侵防范

- 安全要求：b) *应关闭不需要的系统服务、默认共享和高危端口。
- 不符合判例：

满足条件：

操作系统上的多余系统服务/默认共享/高危端口存在可被利用的高风险漏洞或重大安全隐患。

- 补偿措施：通过防火墙、入侵防御等防护设备关闭、阻断对默认共享和高危端口，可视同符合。

七、省联网中心-单项否决项

42 通用要求-安全计算环境-入侵防范

- 安全要求：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。
- 不符合判例：

满足条件：

应用系统存在如存在SQL注入、跨站脚本、上传漏洞等可导致敏感数据泄露、篡改、服务器被入侵等安全事件。

- 补偿措施：无。

七、省联网中心-单项否决项

1 云安全扩展要求-基本要求-基础设施位置

- 安全要求：a) *应确保云计算基础设施位于中国境内。
- 不符合判例：

满足条件：

云计算基础设施位于中国境外。

- 补偿措施：无。

七、省联网中心-单项否决项

2 云安全扩展要求-基本要求-基础设施位置

- 安全要求：b）*应确保业务数据处理类系统不得部署于公有云平台。
- 不符合判例：

满足条件：

业务数据处理类系统部署于公有云平台。

- 补偿措施：无。

七、省联网中心-单项否决项

12 云安全扩展要求-安全计算环境-访问控制

- 安全要求：a) *应保证当虚拟机迁移时，访问控制策略随其迁移。
- 不符合判例：

满足条件：

迁移虚拟机时访问控制策略无法随其迁移。

- 补偿措施：无。

七、省联网中心-单项否决项

5 大数据安全扩展要求

- 安全要求：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。
- 不符合判例：

满足条件：

未提供静态脱敏和去标识化能力。

- 补偿措施：无。

七、省联网中心-单项否决项

7 大数据安全扩展要求

- 安全要求：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。
- 不符合判例：

满足条件：

对重要操作未提供访问控制措施。

- 补偿措施：无。

七、收费站-单项否决项

1通用要求-安全物理环境-机房物理访问控制

- 安全要求：*机房出入应对外来人员进行身份核实，并记录下外来人员身份信息、联系电话、接待人、时间等详细情况。
- 不符合判例：

满足条件（任意条件）：

1.机房无电子或机械门锁，机房入口也无专人值守。

2.办公或外来人员可随意进出机房，无任何管控、监控措施。

- 补偿措施：机房配备24小时专人值守或配备摄像头实时监控，可判定为部分符合。

七、收费站-单项否决项

2通用要求-安全通信网络-网络构架

- 安全要求：a) *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。
- 不符合判例：

满足条件（任意条件）：

1.收费业务和设备接入在同一网络区域。

2.收费业务和运维管理在同一区域。

3.未单独划分ETC门架系统接入区域。

- 补偿措施：无

七、收费站-单项否决项

4 通用要求-安全通信网络-网络构架

- 安全要求：c）*严禁在收费站区域内开展收费专网与互联网数据交互的业务应用。
- 不符合判例：

满足条件（任意条件）：

存在收费专网与互联网数据交互的业务应用，无论是否采用双防火墙、网闸等隔离措施。

- 补偿措施：无。

七、收费站-单项否决项

7 通用要求-安全区域边界-边界保护

- 安全要求：a)*应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。
- 不符合判例：

满足条件（任意条件）：

1.网络边界无任何访问控制措施。

2.网络边界访问控制措施配置不当，存在较大安全隐患。

3.网络边界控制措施失效，无法起到访问控制功能。

- 补偿措施：边界访问控制设备不一定要是防火墙，只要是能实现相关的访问控制功能，形态为专用设备，且有相关功能能够提供相应的检测报告，可视为等效措施，判符合。如通过路由器、交换机或者带ACL功能的负载均衡器等设备实现，可根据系统重要程度，设备性能压力等因素，可视同符合。

七、收费站-单项否决项

10 通用要求-安全区域边界-边界保护

- 安全要求：d) *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。
- 不符合判例：

满足条件（同时）：

a)存在和收费专网互联的无线网络。

b)未采用有效认证技术确保移动设备的可信接入。

- 补偿措施：无。

七、收费站-单项否决项

14 通用要求-安全区域边界-入侵防范

- 安全要求：b) *应在网络中进行检测从内部发起的网络攻击行为。
- 不符合判例：

关键网络节点（如核心服务器区与其他内部网络区域边界处）未采取任何防护措施，无法检测从内部发起的网络攻击行为。

- 补偿措施：如网络设备设置较严格的访问控制策略，且发生内部网络攻击可能性较小，可判定为部分符合。

七、收费站-单项否决项

17 通用要求-安全计算环境-身份鉴别

- 安全要求：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。
- 不符合判例：

满足条件（同时）：

1.可通过远程登录。

2.对连续登录失败无任何处理措施。

3.攻击者可利用登录界面进行口令猜测。

- 补偿措施：无。

七、收费站-单项否决项

23 通用要求-安全计算环境-安全审计

- 安全要求：a)*启用网络、服务器、中间件、数据库、终端及应用等计算设备安全审计功能，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。
- 不符合判例：

满足条件（同时）：

1.重要核心网络设备、安全设备、操作系统、数据库等未开启任何审计功能，无法对用户的重要行为进行审计。

2.无其他技术手段对重要的用户行为和重要安全事件进行溯源。

- 补偿措施：a) 如使用堡垒机或其他第三方审计工具进行日志审计，能有效记录用户行为和重要安全事件；通过其他技术或管理手段能对事件进行溯源的；可视同符合。

七、收费站-单项否决项

26 通用要求-安全计算环境-安全审计

- 安全要求：d) *审计记录留存6个月以上。
- 不符合判例：

满足条件（任意条件）：

1.审计记录未留存6个月。

2.审计记录存储空间不足以存储6个月。

- 补偿措施：无。

七、收费站-单项否决项

28 通用要求-安全计算环境-入侵防范

- 安全要求：b) *应关闭不需要的系统服务、默认共享和高危端口。
- 不符合判例：

满足条件：

操作系统上的多余系统服务/默认共享/高危端口存在可被利用的高风险漏洞或重大安全隐患。

- 补偿措施：通过防火墙、入侵防御等防护设备关闭、阻断对默认共享和高危端口访问，可判定为部分符合。

七、收费站-单项否决项

7 物联网安全拓展要求-安全计算环境-设备安全

- 安全要求：d) *具有登录失败和登录超时处理功能，连续5次登录失败至少锁定10分钟。
- 不符合判例：

满足条件（同时）：

1.可通过远程登录。

2.对连续登录失败无任何处理措施。

3.攻击者可利用登录界面进行口令猜测。

- 补偿措施：无。

七、ETC门架-单项否决项

28 通用要求-安全计算环境-访问控制

- 安全要求：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。
- 不符合判例：

满足条件：

网络内非授权终端可对门架系统设备进行管理或操作。

- 补偿措施：无。

七、ETC门架-单项否决项

6 物联网扩展要求-安全计算环境-设备安全

- 安全要求：c) *若只用“用户名+口令”的鉴别方式进行身份鉴别，则应使用具有一定复杂度的用户口令（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），90天进行更新。
- 不符合判例：

满足条件（同时）：

一、网络设备、安全设备、服务器、中间件、数据库、终端及应用系统。

1.未采用密码技术。

2.存在空口令或弱口令帐户。

二、应用系统：

通过渗透测试或常用/弱口令尝试，发现应用系统中存在可被登录弱口令帐户。

- 补偿措施：如采用双因素认证等管控手段，恶意用户使用该空/弱口令帐号无法直接登录相关设备，可判定为部分符合。

七、ETC门架-单项否决项

7 物联网扩展要求-安全计算环境-设备安全

- 安全要求：d）*具有登录失败和登录超时处理功能，连续5次登录失败至少锁定10分钟。
- 不符合判例：

满足条件（同时）：

1.可通过远程登录。

2.对连续登录失败无任何处理措施。

3.攻击者可利用登录界面进行口令猜测。

- 补偿措施：无。

七、ETC门架-单项否决项

8 物联网扩展要求-安全计算环境-设备安全

- 安全要求：e）*当进行远程管理时应启用SSH、HTTPS等管理方式，加密管理数据、鉴别信息，防止被网络窃听。
- 不符合判例：

满足条件（同时）：

1.通过不可控网络环境远程进行管理。

2.管理帐户口令以明文方式传输。

3.使用截获的帐号可远程登录。

- 补偿措施：1-2-3-4

谢谢聆听