

# 高速公路机电工程联网收费系统网络安全研究

莫广全

广西交通投资集团崇左高速公路运营有限公司 广西崇左 532200

**摘要:** 研究高速公路机电工程联网收费系统的网络安全问题,这类收费系统是基于互联网形成的应用,它包含许多关键信息,如用户身份和交易记录。因此,确保系统的安全性至关重要。首先介绍了高速公路机电工程联网收费系统的概述,然后分析了高速公路联网收费系统的优点,接着阐述了高速公路联网收费系统网络安全保障需求,然后又探讨了高速公路联网收费系统网络安全方案,最后从两个方面分析了高速公路机电工程联网收费系统网络安全管理。

**关键词:** 高速公路; 机电工程联网收费系统; 网络安全研究

## Research on Network Security of Network Toll Collection System of Expressway Mechanical and Electrical Engineering

Guangquan Mo

Guangxi Transportation Investment Group Chongzuo Expressway Operation Co., LTD Chongzuo, Guangxi 532200

**Abstract:** To study the network security problem of expressway electromechanical engineering network toll collection system, which is based on the Internet, which contains many key information, such as user identity and transaction records. Therefore, it is crucial to ensure the safety of the system. First introduces the overview of highway mechanical and electrical engineering network charging system, and then analyzes the advantages of the highway network charging system, then expounds the highway network toll system network security requirements, and then discusses the highway network toll system network security scheme, finally from two aspects analyzed the highway mechanical and electrical engineering network charging system network security management

**Keywords:** Expressway; Network toll system of mechanical and electrical engineering; Research on network security

### 1 高速公路联网收费系统的优点

#### 1.1 提高了通行效率

采用联网收费系统可以实现快速的收费处理和车辆通行,从而提高了通行效率。例如,以往传统的人工收费方式需要车辆停下来等待收费员开闸放行,容易造成车辆排队等待的情况,而联网收费系统采用电子支付方式,车辆不需要停下来等待收费员开闸,直接通过收费站,缩短了车辆等待时间,提高了通行效率。

#### 1.2 降低了交通拥堵

由于联网收费系统能够快速处理收费,避免了传统收费方式中人工收费带来的拥堵现象,从而降低了交通拥堵。例如,在高峰时段,人工收费的车辆排队等待时间长,易造成交通拥堵,而采用联网收费系统,车辆通过收费站的时间极大缩短,减少了车辆排队等待的情况,降低了交通拥堵。

#### 1.3 方便了用户缴费

联网收费系统采用电子支付方式,用户可以通过网上银行、手机支付等方式缴费,方便快捷,避免了人工收费中存在的找零问题。例如,以往在人工收费中,如果车辆支付的金额和实际收费不符,需要找零,而采用联网收费系统,用户可以通过电子支付方式自动扣款,不需要找零,避免了找零问题。

#### 1.4 提高了收费管理效率

联网收费系统具有集中管理、自动计费、数据分析等功能,可以提高收费管理的效率和精度,降低管理成本。例如,采用联网收费系统可以实现收费数据的自动记录和处理,无需人工干预,从而降低了人工成本和错误率。

#### 1.5 增强了安全保障

联网收费系统采用先进的计算机、通信和网络技术,实现了对车辆信息和交易数据的保密和安全性控制,有效

防止了欺诈和非法行为的发生。例如，采用联网收费系统可以实现车辆通行信息和支付数据的实时监控和记录，如果发现异常情况，可以及时报警和处理，提高了安全保障。

## 2 高速公路联网收费系统网络安全保障需求

### 2.1 数据加密

数据加密技术是通过将数据进行加密和解密，以保证数据的机密性和完整性，防止数据被非法获取和篡改。在高速公路联网收费系统中，需要采用加密技术对用户的隐私数据进行保护，如车辆信息、个人信息等。其中，对于车载电子标签（ETC）中的车辆信息，需要采用高强度的加密算法对其进行加密，确保其信息的机密性和完整性。例如，AES（Advanced Encryption Standard）加密算法就是一种常用的加密算法，在车载电子标签中常用于保护车辆信息的安全。

### 2.2 访问控制

访问控制是通过将系统的不同部分进行权限控制，防止未经授权人员访问系统。在高速公路联网收费系统中，需要对不同的用户进行身份认证，并根据其权限对系统进行访问控制。例如，对于收费站的工作人员，需要通过身份证明和密码认证，方可进入系统并操作计费设备，而普通用户则只能在ETC车道通过系统自动缴费，无法进入系统操作计费设备。

### 2.3 安全监测

安全监测是指对系统进行实时监测，及时发现系统的异常情况，并采取相应的应对措施。在高速公路联网收费系统中，需要对系统的网络通信情况、系统运行状态等进行实时监测，并在发现异常情况时，及时进行报警和处理。例如，如果发现有恶意攻击行为，系统应该立即对攻击行为进行阻拦，并记录相关信息，以便后续分析和处理。

### 2.4 防病毒攻击

防病毒技术是指通过对系统进行病毒扫描和杀毒，防止病毒攻击对系统造成破坏。在高速公路联网收费系统中，需要对系统进行定期的病毒扫描和杀毒，确保系统的安全。例如，采用常见的杀毒软件，如360杀毒软件、卡巴斯基等，对系统进行定期的病毒扫描和杀毒操作，防止病毒攻击对系统造成影响。

### 2.5 应急响应

应急响应是指在系统安全事件发生时，采取应急措施，防止安全事件对系统造成较大的影响。在高速公路联网收费系统中，需要建立完善的应急响应机制，及时发现和处理安全事件。例如当系统出现安全漏洞或攻击事件时，高

速公路联网收费系统需要采取应急响应措施，例如：立即通知安全管理人员和技术支持团队，组织专业人员对系统进行调查和修复；关闭受攻击的系统和网络设备，避免攻击扩散和造成更大的损失；对攻击者的IP地址进行封锁和追踪，收集攻击者的信息，保留相关日志和数据，为后续追究责任提供证据；对系统进行安全加固，修补漏洞，更新补丁，加强防火墙和入侵检测系统的保护能力；对受影响的用户进行通知，并提供相关的安全建议和措施。

## 3 高速公路联网收费系统网络安全方案

### 3.1 网络架构安全

针对高速公路联网收费系统的网络架构安全，可以采用以下技术：边界防火墙，对外部网络进行过滤和限制，避免不必要的流量进入系统，保障网络通信的安全。入侵检测系统，对系统的网络流量进行实时监测和分析，检测和阻止入侵行为，提高系统的安全性。VPN，建立虚拟专用网，加密通信内容，确保数据传输的安全。安全网关，对系统的网络通信进行安全管理和控制，过滤和拦截非法流量，保障系统的安全。例如，高速公路联网收费系统可以采用边界防火墙和入侵检测系统对系统进行防护。当外部攻击或入侵行为发生时，边界防火墙可以拦截攻击流量，而入侵检测系统可以及时发现入侵行为，防止攻击扩散。

### 3.2 数据传输安全

高速公路联网收费系统需要采用安全传输协议，如HTTPS等，对用户的隐私数据进行加密传输。同时，需要对用户隐私数据进行加密存储，保护数据的安全。例如，系统可以使用HTTPS协议对用户隐私数据进行加密传输，使用AES等加密算法对用户隐私数据进行加密存储。

### 3.3 认证与授权安全

高速公路联网收费系统需要采用多种身份认证技术，如用户名和密码认证、指纹认证、智能卡认证等，确保系统的安全。同时，需要对用户的权限进行控制，对不同用户进行不同的授权设置。例如，系统可以使用用户名和密码认证技术对用户进行身份认证，并使用访问控制技术对用户的权限进行控制。

### 3.4 应用程序安全

高速公路联网收费系统需要采用多种安全技术，如安全编码规范、代码审查、漏洞扫描等，保护系统的应用程序安全。例如，系统可以采用安全编码规范，对开发人员进行安全培训和指导，确保应用程序的安全性。同时，对应用程序进行代码审查和漏洞扫描，及时发现和修复安全漏洞。

### 3.5 安全管理与监控

高速公路联网收费系统需要采用安全管理和监控系统,对系统的网络通信情况、系统运行状态等进行实时监测,并在发现异常情况时及时发出警报和采取应对措施,确保系统的安全。例如,系统可以采用安全信息和事件管理系统,对系统进行实时监控和管理。当发现异常情况时,系统会自动发出警报,管理员可以及时采取应对措施,确保系统的安全。

#### 4 高速公路机电工程联网收费系统网络安全管理

##### 4.1 对设备的管理

###### 4.1.1 设备的配置管理

设备的配置管理是指管理员对设备的初始配置进行规划和设置,并定期检查和修正设备的配置,以确保设备的合规性和安全性。管理员可以通过限制设备的访问权限来控制系统的安全性。

###### 4.1.2 设备的监控管理

设备的监控管理是指管理员采用实时监控、日志审计等方式对设备的运行情况进行监控,及时发现异常情况并处理。可以使用网络监控系统对设备的运行状态进行实时监测,以及对网络流量进行监测和分析等。

###### 4.1.3 设备的维护管理

设备的维护保养是确保设备长期安全运行的必要条件。管理员应当定期对设备进行维护和修复,包括软件更新、漏洞修补、硬件维修等方面。应当定期检查设备的硬件组件,及时更换老化和损坏的设备。

###### 4.1.4 设备的更新管理

设备的更新管理是保证设备安全性的重要环节。管理员应当定期检查设备的软件版本,及时进行软件升级和漏洞修补。管理员可以定期检查设备上的操作系统和应用程序的版本,并及时安装最新的更新。此外,还应当定期更新防病毒软件、防火墙等安全软件,以提高系统的安全性。

###### 4.1.5 设备的备份管理

设备的备份管理是指管理员对设备的重要数据和配置文件进行备份,并建立备份策略和恢复方案,以防止设备数据的丢失和破坏。例如,管理员可以定期对设备的配置文件和日志文件进行备份,并存储在安全的地方。在设备出现故障或攻击事件时,可以通过备份文件进行快速恢复,从而保证设备的安全运行。

##### 4.2 对人员的管理

###### 4.2.1 权限管理

权限管理是指管理员根据人员的角色和职责设置相应的访问权限,控制人员对系统资源的访问和操作。管理员需要根据业务需求,合理分配权限,避免人员拥有过高或

过低的权限,从而确保系统的安全性和稳定性。例如,系统管理员需要拥有最高权限,能够对系统的所有功能进行管理和控制,而普通用户则只能访问系统的部分功能。在权限管理过程中,管理员需要注意授权粒度,确保权限的控制不会过于细致或过于宽松,避免授权不当引发的安全问题。

###### 4.2.2 安全意识教育

安全意识教育是指管理员对人员进行安全意识培训和教育,提高人员的安全意识和安全素养,帮助他们了解各种安全威胁和安全防范措施。例如,管理员可以定期组织安全培训和演练,教授人员如何避免社会工程学攻击、如何识别和防范恶意软件等安全问题。在安全意识教育过程中,管理员需要注意及时更新教育内容,确保人员了解最新的安全威胁和防范措施。

###### 4.2.3 访问控制

访问控制是指管理员通过技术手段控制人员的访问权限,防止未经授权的人员访问系统,从而确保系统的安全性。例如,管理员可以使用IP白名单、用户认证等方式对人员的访问进行控制,避免来自未知来源的攻击。在访问控制过程中,管理员需要注意授权管理,及时删除无用账号和权限,避免因权限过度累赘或过期而引发的安全问题。

#### 5 结语

在本文中,我们对高速公路机电工程联网收费系统的网络安全问题进行了深入的研究和分析。我们认为应该加强系统的网络安全监控和日志记录,及时发现和应对任何异常行为和攻击事件。此外,我们建议对系统的访问控制和身份验证进行进一步的改进和加强,以确保只有授权用户可以访问系统和敏感数据。最后,我们认为高速公路机电工程联网收费系统的网络安全是一个长期而复杂的问题,需要各方面的持续努力和不断创新。我们希望本文的研究能够为该系统的网络安全提供一些有益的思路和启示,为保障用户的信息安全和系统的可靠运行做出贡献。

#### 参考文献:

- [1]高原.高速公路机电工程联网收费系统网络安全管理研究[J].交通世界,2022(34):174-176.
- [2]江孔顺.高速公路机电工程联网收费系统网络安全[J].电子技术与软件工程,2019(18):203-204.
- [3]徐超.高速公路机电工程联网收费系统网络安全研究[J].交通世界,2018(33):164-165+173.