城市交通信息化的安全保障系统设计

刘 硕
中公华通（北京）科技发展有限公司 北京 100088

摘 要：随着城市交通信息化的快速发展，城市交通信息化安全保障系统已成为城市发展中不可或缺的一部分。其设计方案的科学性与完整性将直接关系到城市交通信息系统的可靠性和安全性。本文深入分析城市交通信息化安全保障系统的设计方案，详细论述了关键问题及其解决方案。本文提出了通过制定完善的安全策略、适当的资源保护策略以及强化安全意识的措施来保障城市交通信息化安全。同时，针对安全测试与应急处理设计了对应的解决方案，并提出了重要的安全防护措施和安全意识教育。文章全面精准地指出了城市交通信息化安全保障系统设计方案中的问题，并给出了可靠的解决方案，对于保障城市交通的信息安全具有一定的指导意义。

关键词：城市交通信息化；安全保障；系统设计

引言：近年来，时代的发展与日益更新的科学技术，促使我国城市交通建设事业得到了快速发展，城市交通信息化成为必然趋势，围绕城市交通信息化安全保障系统的建设迫在眉睫。城市交通信息化安全保障系统是利用先进的信息技术手段，对城市交通信息系统进行监测、管理、运行和维护，确保城市交通信息的安全和可靠。城市交通信息系统的安全性一旦受到威胁，将对市民的出行、城市的运营和社会的稳定产生重大影响。因此，城市交通信息化安全保障系统的设计方案的合理性和完备性对于城市交通信息化的安全管理和保障意义重大。

1 城市交通信息化的安全保障系统的重要性

城市交通信息化系统的快速发展，为城市交通管理带来了巨大的便利和效益，同时也面临着诸多的安全风险。城市交通信息化系统中各种设备、网络、数据等多个环节都存在着被黑客攻击、破坏、篡改、泄露等多类安全问题，对城市交通安全和秩序带来了严重的隐患。对此，设计一个可靠的城市交通信息化安全保障系统是至关重要的。首先，城市交通是城市的重要基础设施之一，也是人民群众生命财产安全的重要保障。城市交通信息化系统的安全问题一旦出现直接影响到城市交通的顺畅运行和安全管理，甚至可能导致严重的交通事故和公共安全问题。通过建立可靠的城市交通信息化安全保障系统是保障城市交通安全、顺畅的重要手段之一。其次，城市交通信息化系统涵盖的内容极其繁杂，发生问题的概率非常高。城市交通信息化系统涉及的设备和软件很多，这其中任何一个环节出现问题，都可能导致安全事故。因此，城市交通信息化安全保障系统的设计需要考虑涉及到不同设备、软件、网络、运营管理等多方面因素。第三，城市交通信息化系统更需要保密与隐私保护。城市交通信息化系统中的数据，包括车辆和人员行踪、停车场管理、智能交通管理等很多内容，在不当的保护措施下，可能会导致个人私密信息泄露、商业机密被窃、计划和政策被破坏等多类安全问题。城市交通管理部门需根据实际情况制定明确的数据管理隐私政策，建立健全的数据安全保障系统，严格保护数据的安全性、机密性和完整性。最后，城市交通信息化系统的保障需要不断进行升级和改进，以适应安全环境的不断变化。犯罪分子的入侵手段变得越来越先进，攻击手法和黑客技术也在不断升级，因此城市交通信息化安全保障系统必须注重持续、主动的监测，以及随着时间的发展不断对应、完善安全策略。这需要城市交通管理部门投入足够的人员、技术和资源，开展各类漏洞测试和风险评估，并建立预警机制，实时排查、追踪和解决各种安全问题[1]。

2 城市交通信息化安全保障系统的设计原则

城市交通信息化安全保障系统的设计是城市交通信息化系统的关键组成部分。其主要的任务是保障城市交通信息化系统的安全稳定运行。因此，设计一套成熟可靠的安全保障系统变得尤为重要。本节将基于城市交通信息化安全保障系统的要求，探讨其设计原则，有助于实现有效的保障。

2.1 安全性优先原则

城市交通信息化安全保障系统的设计之初就要考虑安全性，保证系统的稳定性和完整性，避免系统被黑客侵犯。系统的安全性是城市交通信息化保障系统的核心，每一项功能的设计都必须考虑到安全因素，所有连接信息的虚拟通道必须进行统一监测，对异动信息或异常行为实现自动拦截和反馈。设备的购买和管理也要考虑设备本身的安全问题。

2.2 实时监控和反应能力原则

城市交通信息化系统具有贯穿城市整个道路交通信息流通的特性，因此，城市交通信息化系统需要具备实时监测和反应能力，能够快速进行故障诊断、追踪和解决。如果一旦发现任何关键数据的异常或安全事件，城市交通管理部门应设法尽快启动报警联动机制，并且应该能够很快地针对任何的安全事件进行应急指挥，遏制事态扩大化。

2.3 数据隐私和保护原则

城市交通信息化系统中存在大量敏感性高、涉及隐私的数据，如车辆定位、人员行踪等。因此城市交通信息化安全保障系统的设计还必须考虑到数据隐私和保护原则。保护数据隐私是这个系统的重中之重。系统必须通过数据分类、身份验证、密钥管理等标准来保护所有数据的访问和使用[2]。

3 城市交通信息化安全保障系统设计方案

3.1 风险评估和安全策略制定

风险评估和安全策略制定涵盖了识别和评估系统的安全风险、准确区分每个安全风险的影响等级和风险等级、针对每个风险等级制定相应的安全策略和风险处理措施。以下为风险评估和安全策略制定的关键步骤

3.1.1 安全风险评估的基础分析

这个阶段是实现风险评估和安全策略制定的基础，其核心是识别可能存在的风险，包括人为因素、设备因素和管理因素。通过具体的意外事件、互联网攻击等类型进行危险场景的刻画，以及评估不同的风险类型和安全问题的影响程度和等级。

3.1.2 相关安全策略的制定

根据风险评估的分析结果，设计出相应的安全策略，随之制定风险管理计划。相关的安全策略设计需考虑系统的管理、网络可能面临的威胁、数据保护等多方面因素。安全策略的内容包括：记录和核实所有问题，制定突发事件应对计划，维持全部部门的安全意识和协调，开始建立有效的安全管理机制，并保证执行力度。

3.1.3 安全责任制度的建立

系统安全的保障是承担方内部相互展开的，需要明确安全责任和安全任务。其核心内容包括制定体系内部相关管理责任体系，并更新有效的安全规章制度，确保所有的员工都得知和执行防范措施，并真实了解其对应的安全责任。

3.1.4 安全方案的实施和维护

安全策略制定后需要及时进行实施并不断地对其进行维护。初步的反应岗位建立、信息的共享和员工的安全性培训，并通过主动监测与推动持续改进，来提高安全措施和安全效果[3]。

3.2 设备选择和配置

合适的设备选择和配置可以有效地确保系统的稳定性和可扩展性，并有利于保障系统的安全性。以下是设备选择和配置的关键步骤.

3.2.1 确定系统的需求

首先需要明确城市交通信息化安全保障系统的需求，了解系统的规模、功能和安全保障需要等方面，确定系统所需的设备类型和数量，并综合考虑性能和价格等因素。

3.2.2 设备选型

在设备选型中，需要充分考虑设备的稳定性、性能和扩展性等因素。可以通过用户反馈、行业标准、成本和维护费用等因素来选择设备。

3.2.3 设备配置

在设备配置方面，需要根据城市交通信息化安全保障系统的功能需求、业务模型和技术特性来进行设备配置。此时应注意使用合适的设备组件，如磁盘、内存、CPU等，并确保所选设备的性能和可靠性等质量问题。

3.2.4 设备部署和测试

设备部署和测试是系统设计方案中非常重要的一步，需要将配置好的设备组装安装到系统中，并进行组件间的联通测试、功能测试和性能测试等环节。在测试时，根据系统部署方案，可以进行多种角度的测试，如系统的安全性测试、数据流量测试、扩展性测试和容错性测试等，以确保系统的安全性和稳定性。

3.3 线路选择和隔离

线路是城市交通信息化系统中信息交互和数据传输的关键点，而线路选择和隔离可以有效地防止对系统的非法访问和攻击。以下是线路选择和隔离的关键步骤

3.3.1 线路选择

首先需要根据系统设计方案中要求的信息交互和数据传输的需求，选择合适的线路类型。在选择线路时，需要考虑线路的带宽、距离、传输速度、安全性等多方面因素，以确保选定的线路可靠性和稳定性。

3.3.2 线路隔离

在城市交通信息化系统中，应该采取线路隔离措施，避免非法访问和攻击，从而保护系统的安全性。通过使用物理隔离、逻辑隔离、安全加密等策略来增强系统的安全性，减少信息的泄露，避免线路感染等网络威胁。

3.3.3 网络安全设备部署

网络安全设备的部署是网络隔离的基础。网闸、防

火墙、入侵检测系统、入侵防御系统等具有防御和防范网络安全威胁的网络安全设备应根据系统的要求，在网络结构的主要位置上布置或配置，以取得最佳的安全保护效果。

3.3.4 隔离措施管理

线路隔离措施的管理和维护同样是设计城市交通信息化安全保障系统方案的重要环节。为了保障线路隔离措施的有效性，必须注意对接入设备的状态及设备的管理手段、管理内容、管理成效进行实时管控与反馈。

3.4 软件与系统的开发和测试

软件与系统的开发和测试是城市交通信息化安全保障系统设计方案中的关键环节，它们直接关系到系统的安全和可靠性。软件与系统的开发和测试的关键步骤包含如下内容

3.4.1 需求分析

在软件与系统开发之前，需要进行需求分析。需求分析阶段是确定软件功能、性能和接口的重要阶段，对后续的开发和测试工作具有重要意义。

3.4.2 系统设计

系统设计是指根据需求分析阶段的结果，设计符合需求的可实现方案。在这一阶段，需要综合考虑系统的功能、性能、可靠性、安全性和可扩展性等因素，设计出符合需求和标准的系统架构。

3.4.3 编码及测试

在编码阶段，会根据系统设计及相应的开发流程，进行代码编写。在这个过程中，需要注重编码风格、代码可维护性和可读性，并且进行单元测试，在代码编写完毕后还需要进行集成测试和系统测试，以确保系统的功能和安全性能。

3.4.4 安全测试

安全测试是保证城市交通信息化安全保障系统的安全性和可靠性的重要环节。主要包括漏洞扫描、安全审计、攻击模拟等多个方面的测试。

3.4.5 上线和维护

在通过测试确保系统的稳定性和安全性后，可以将系统上线，开始实际生产和应用。然而，这并不代表系统始终如一，需要不断迭代优化，始终保持系统的可靠性和稳定性。

3.5 安全团队的建立和培训

建立一支专业的安全团队，可以提高城市交通信息化安全保障系统抵御攻击和保障安全的能力，同时也能够发现和修复安全风险。从如下几方面可以有效建立和培训合格的安全团队.

3.5.1 建立安全团队

建立安全团队需要明确组织架构和人员配备等。目标是明确安全团队的职能职责，制定明确的工作目标和职责分工。

3.5.2 招聘安全人员

招聘安全人员是安全团队建设的重要一环。需要寻找有相关知识和经验的专业人士，如网络安全工程师、信息安全咨询师等，以确保团队的专业性和适用性。

3.5.3 安全团队培训

安全团队培训是建立和完善安全团队的重要基础。可以通过网络安全技术培训、信息安全知识体系培训、安全标准培训等多种方式来提升安全团队的专业知识、技能和素养，并加强团队的协作和协调能力。

3.5.4 确定工作计划和应急预案

安全团队应该根据城市交通信息化安全保障系统的设计方案，制定相应的工作计划和应急预案。随着安全形势的不断变化，应急预案可以随时协调调整，以适应实际情况。

3.5.5 随时监测和分析风险

安全团队可以通过捕获和分析网络数据流量、监测各类威胁漏洞、策略的执行细节等多项工作来实时监测和分析风险，进而做出相应的安全举措，以提高城市交通信息化安全保障系统的安全性。

结束语

城市交通信息化安全保障系统是保障城市交通信息安全的重要手段，而系统设计方案则直接关系到系统的稳定性和可靠性。设计方案的优劣会直接影响到危害程度及影响范围、日常运行维护，系统的漏洞修复升级等工作。因此，该系统的设计方案必须严谨、科学、可靠。在设计方案中应重视安全策略、网络隔离、安全测试等环节，建立专业的安全团队，实现对系统安全状况的实时监测和预警，及时采用有效措施进行攻击应对和预防。为确保城市交通信息化系统的安全性，必须严格遵循信息安全法律法规，及时升级更新防护设备和软件，加强信息安全系统建设，促进城市交通信息化的不断创新与发展。

参考文献

[1]王慧青,杨德峰.城市交通信息化安全保障系统研究[J].交通科技创新导刊,2019,(23):49-51.

[2]韩健,周建华.基于哈希链技术的城市交通信息化安全保障系统[J].哈尔滨理工大学学报,2019,24(3):46-50.

[3]秦艳霞,陈晓慧,翟晓光,等.城市交通信息化安全保障系统设计与实现[J].科学技术与工程,2019,19(8):194-197.