第 2 卷◆第 4 期◆版本 1.0◆2024 年
文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

智慧城市信息安全风险评估模型研究

苏颖　谷慧娟
中国网络安全审查认证和市场监管大数据中心
DOI:10.12238/acair.v2i4.10358

[摘　要] 本文探讨信息安全风险评估在智慧城市建设中的应用价值。并据此构建了一套适用于智慧城市的信息安全风险评估模型,该模型能够全面、系统地评估城市信息系统所面临的安全威胁和脆弱性,为城市管理者提供科学的风险决策依据。探讨了该评估模型在智慧城市实际场景中的应用,验证了其在识别和量化风险方面的有效性,为智慧城市的可持续发展提供了有力的安全保障。总结而言,本研究旨在构建一个适用于智慧城市的全面、有效的信息安全风险评估框架,为城市信息安全的精细化管理提供理论支持和技术参考,对推动智慧城市的健康发展具有重要的理论意义和实践价值。
[关键词] 信息安全；风险评估；智慧城市；模型构建；定量化方法
中图分类号：X820.4　**文献标识码：**A

Research on the Risk Assessment Model of Information Security in Smart Cities

Ying Su　Huijuan Gu
China Network Security Review Certification and Market Supervision Big Data Center

[Abstract] This article explores the application value of information security risk assessment in the construction of smart cities. And based on this, a specialized risk assessment model suitable for smart cities was constructed, which can comprehensively and systematically evaluate the security threats and vulnerabilities faced by urban information systems, providing scientific risk decision-making basis for urban managers. Explored the application of the evaluation model in practical scenarios of smart cities, verified its effectiveness in identifying and quantifying risks, and provided strong security guarantees for the sustainable development of smart cities. In summary, this study aims to construct a comprehensive and effective information security risk assessment framework applicable to smart cities, providing theoretical support and technical references for the refined management of urban information security. It has important theoretical significance and practical value for promoting the healthy development of smart cities.
[Key words] information security; Risk assessment; smart city; Model construction; Quantitative methods

前言

随着科技的飞速发展和城市化进程的加速,智慧城市作为未来城市发展的必然趋势,其信息安全问题日益凸显。智慧城市的信息基础设施如物联网、大数据、云计算等的广泛应用,不仅极大地提升了城市管理和服务的效率,但也使得城市面临更为复杂多样的信息安全风险。这些风险可能来自恶意攻击、内部失误、技术漏洞,甚至外部环境因素,对城市的正常运行构成严重威胁。因此,建立一个科学、全面、有效的信息安全风险评估模型,对于保障智慧城市的可持续发展具有至关重要的现实意义。

1 研究背景与意义

随着GB/T 20984-2022和ISO/IEC 27001:2022等国内外标准的发布,信息安全风险评估的理论体系和方法论日益完善。然而,这些通用标准在应用于智慧城市时,往往难以充分反映其特性和需求,因此,针对性地构建智慧城市信息安全风险评估模型成为当务之急。以往的研究大多侧重于单一技术层面的风险评估,忽视了智慧城市中多元因素的交互影响。本研究旨在填补这一空白,通过深入剖析智慧城市的信息安全特点,构建一套全面考虑技术、管理、法律等多维度风险因素的评估模型。

研究智慧城市信息安全风险评估模型,既是应对智能化、网络化时代信息安全挑战的必然选择,也是提升城市治理能力、推动智慧城市健康发展的战略需求。通过构建这样的评估模型,可以为城市管理者提供有力的决策支持,确保智慧城市在享受信息技术带来的便利的同时,能够有效应对各种安全风险,从而保障城市运行的稳定与安全,为智慧城市的可持续发展奠定坚实基础。

2 信息安全风险评估模型的构建

2.1信息安全风险评估模型的基本原理

信息安全风险评估模型是保障智慧城市建设中信息安全的关键工具。它构建了一个系统化的框架,用于识别、分析和评价可能影响城市信息系统安全的各种风险。基本原理可概括为三个核心阶段：风险识别、风险分析和风险评价。

在风险识别阶段,模型探究并确定智慧城市的信息资产,包括硬件、软件、数据、人员及其在城市运行中的重要性[1]。同时,评估潜在的威胁源,如黑客攻击、内部错误、自然灾害等,以及这些威胁如何通过已识别的脆弱性影响系统。

在风险分析阶段,模型聚焦于量化和定性分析识别出的威胁和脆弱性对系统安全的实际影响。这通常包括评估安全事件发生的可能性,即威胁发生的频率或可能性,以及其可能造成的损失,如数据泄露带来的财务损失、声誉损害或业务中断。这一阶段通常结合威胁和脆弱性评估的结果,使用数学模型和工具来计算风险值,如风险矩阵、概率影响图等[2]。

风险评价阶段是将风险分析的结果与组织设定的风险接受准则进行比较,确定风险等级,判断是否需要采取进一步的控制措施。这可能涉及对风险的接受、转移、降低或避免。比如,对于高风险项目,可能需要增强系统的安全防护,改进安全策略,或者将部分风险转移给保险公司。此外,风险等级的确定还能帮助城市管理者确定资源分配的优先级,确保关键系统的安全得到充分保障。

构建智慧城市信息安全风险评估模型时,必须遵循相应标准和最佳实践,例如GB/T 20984-2022和ISO/IEC 27001:2022,以保证评估的标准化和有效性。这些标准提供了风险评估的结构化框架,指导如何在组织中实施有效的风险评估,确保所有关键步骤得到遵循。

信息安全风险评估模型的基本原理是通过结构化的过程,识别和量化智慧城市中的安全风险,为管理者提供科学的决策依据,确保城市信息系统在面临日益复杂和动态的威胁环境下能够保持安全稳定[3]。这不仅有助于建立一个综合、动态的风险管理体系,也有助于促进智慧城市的可持续发展,为城市居民提供一个安全、高效的生活和工作环境。

2.2定量化信息安全风险评估的方法与指标

定量化信息安全风险评估是风险评估模型的重要组成部分,它借助数学模型和工具,将抽象的风险转化为具体的数据,以便更准确地衡量和管理风险[4]。这种方法通常包括资产估值、威胁和脆弱性评估、风险计算和风险等级划分四个步骤。

资产估值是评估过程的基础,涉及识别信息系统中的关键资产,并为每个资产分配一个经济价值或业务重要性分数。资产的价值不应仅考虑其经济成本,还应考虑其对智慧城市运行的直接影响,例如关键数据的丢失可能导致的服务中断或业务损失。通过这种方式,可以确保评估过程更加全面,且能够反映资产在智慧城市中的实际价值[5]。

威胁和脆弱性评估是确定风险发生概率和潜在影响的关键。威胁评估旨在识别可能影响智慧城市的信息安全事件,如黑客攻击、内部失误等,同时量化这些威胁发生的可能性。而脆弱性评估则关注系统中存在的弱点,如软件漏洞、安全策略的不足等,以及这些弱点被威胁利用的可能性。在评估过程中,可利用多种方法,如威胁树分析、漏洞扫描工具,或者采用模糊逻辑、人工神经网络等技术进行评估。

在识别业务并对其重要性赋值、识别系统资产及其业务承载连续性后对资产价值赋值、识别系统组件和单元资产后对其资产价值赋值、识别威胁的能力和频率并对其威胁值赋值,识别安全措施和脆弱性后并对脆弱性被利用难易程度和影响程度赋值,采用适当的计算方法与工具确定安全事件发生的可能性和损失,并进行风险计算。一般采用安全事件发生的可能性以及安全事件造成的损失,计算系统资产风险值,即:风险值=R[安全事件发生的可能性,安全事件造成的损失]。风险值越大,表示该风险对系统的影响越严重。

风险等级划分是将计算出的风险值与预设的风险接受准则进行比较,将风险划分为高、中、低等不同等级。这样可以为城市管理者提供直观的风险轮廓,便于优先处理高风险项目,并根据资源分配和业务需求制定相应的安全策略。此外,风险等级划分也有助于定期回顾和调整风险接受准则,以适应不断变化的威胁环境。

定量化信息安全风险评估的方法与指标为智慧城市提供了量化风险的手段,使决策者能够以数据为依据,制定更精准、更有效的安全策略。通过这种方法,城市管理者能够对风险进行有重点的管理,优化资源分配,确保智慧城市的长时间安全运行,同时为未来可能面临的挑战提供有力的防护。这种方法的实施不仅符合国际标准如ISO/IEC 27001:2022的要求,也符合GB/T 20984-2022等国内规范,为风险评估提供了科学性和一致性。

3 智慧城市信息安全风险评估模型

3.1智慧城市应用的信息安全特点

智慧城市的信息安全特点在其高度集成和互联互通的基础上,构建出一个复杂且动态的网络环境。这些特点决定了其面临的信息安全风险具有独特性,需要专门的风险评估模型来全面、准确地识别和管理。

智慧城市的信息系统通常由众多子系统组成,如智能交通、智慧能源、智慧医疗等,它们之间紧密相连,形成一个整体。这种高度集成性意味着一个子系统的安全问题可能迅速扩散到整个系统,引发连锁反应,导致全局性的安全危机。

智慧城市的信息系统依赖于物联网、大数据和云计算等技术,这些技术的广泛应用带来前所未有的数据处理和交互能力,但也暴露出大量的脆弱点。例如,物联网设备的固件更新困难、云服务的安全配置复杂,以及大数据处理过程中隐私保护的挑战,都可能成为攻击者的切入点。风险评估模型必须涵盖这些技术特有的风险因素,确保评估的针对性。

智慧城市的信息安全风险还与管理、法规和公众行为等因素交织。例如,政策法规的更新可能影响安全标准的执行,公众

对网络安全的意识可能影响系统的使用行为,这些间接风险同样需要纳入评估模型,以确保整体风险的全面覆盖。通过构建这样的模型,城市管理者可以更精确地识别和管理风险,确保智慧城市在享受现代科技带来的高效与便利的同时,能够抵御各种安全威胁,为城市居民提供一个安全、稳定的信息环境。

3.2智慧城市信息安全影响因素分析

在智慧城市的信息安全风险评估中,影响因素的深入分析是构建有效评估模型的关键。这些因素包括技术层面的风险、管理与组织层面的挑战、法规遵从问题以及社会环境与公众行为的影响。

技术层面的影响因素主要包括智慧城市的基础设施即服务,如物联网设备、大数据平台和云计算服务。物联网设备因其数量庞大且分布广泛,往往成为攻击者易于渗透的目标,它们的固件更新困难和安全防护措施不足增加了安全风险。大数据平台由于处理海量信息,对隐私保护和数据安全提出了更高要求,而云计算服务的安全配置复杂性可能导致安全漏洞。因此,评估模型需要特别关注这些技术特性,为每个因素设计合适的量化指标。

管理与组织层面的风险主要涉及内部流程、人员培训和安全策略。智慧城市的信息系统通常涉及众多部门和机构,如何确保所有参与者都遵循统一的安全标准,避免内部失误和疏漏,是评估过程中的重要考虑。此外,员工的安全意识和技能不足也可能成为安全威胁的来源,因此,定期的培训和教育也是风险评估模型需要关注的部分。

法规遵从性则是评估智慧城市信息安全风险时不可忽视的环节。智慧城市的发展受到一系列国家和地方政策法规的约束,如数据保护法、网络安全法等,这些法规对信息系统的安全要求和责任划分都有明确的规定。评估模型需要考虑这些法规的要求,确保评估结果能帮助城市管理者满足合规性,降低因法规违反带来的潜在风险。

社会环境与公众行为对信息安全的影响不容小觑。经济活动、社会变革、公众对网络安全的认知水平,甚至敌对国家或组织的意图,都可能成为智慧城市面临的安全威胁。评估模型需要考虑这些动态因素,建立环境感知机制,以便在必要时实时调整风险评估策略。

智慧城市信息安全风险评估模型在构建时,必须充分考虑技术、管理、法规和外部环境等多方面的影响因素。通过深入分析这些因素,模型能提供更加全面、准确的风险评估,帮助城市管理者制定科学的决策,确保智慧城市的可持续发展和公众的信息安全。

4 结束语

综上所述,智慧城市的健康发展离不开健全的信息安全风险评估体系。研究者和实践者应继续探索更有效的定量与定性评估方法,以及如何将评估结果融入城市规划和管理决策中。同时,强化公众的网络安全意识,推动相关法律法规的完善,以及促进跨部门、跨行业的风险信息共享,也将是保障智慧城市安全的重要途径。通过这些努力,我们期待能够构建一个更加完善、智慧的信息安全风险评估框架,为智慧城市的可持续发展提供坚实的保障。

[参考文献]

[1]宋豪杰,刘铭,查鹏皓,等.面向智慧城市的网络信息安全管理平台建设研究[J].项目管理技术,2024,22(10):122-128.

[2]胡柳.智慧城市网络信息安全风险评估模型及应用研究[J].科技创新与生产力,2024,45(09):70-72.

[3]陈月华,陈发强,王佳实.新型智慧城市网络安全发展探析[J].信息安全研究,2022,8(09):947-951.

[4]高凯,邹凯,蒋知义,等.智慧城市信息安全风险评估指标体系构建[J].现代情报,2022,42(04):110-119.

[5]张文德,蔡均益,卫西宁,等.改进FMEA模型在智慧城市信息安全风险评估的应用[J].情报探索,2021,(07):1-8.

作者简介：

苏颖(1998--),女,汉族,河南人,本科,研究方向:信息安全认证。

谷慧娟(1984--),女,汉族,山西人,本科,研究方向:信息安全认证。