

城市景观照明控制系统的网络安全挑战与对策

朱龙龙

青岛市户外广告与亮化发展中心

摘要：随着城市化进程的不断推进，城市景观对于照明的要求也越来越高，为了实现高质量的景观照明，这就需要保障景观照明控制系统的安全运行。然而，在照明控制系统的运行过程中，往往会受到一系列网络安全挑战，威胁着系统的正常运行。本文旨在探讨城市景观照明控制系统所面临的网络安全挑战，并提出一系列对策来应对这些挑战。首先，论述了城市景观照明控制系统，研究了其系统构成、功能以及网络化特点，其次，分别从数据泄漏风险、远程控制漏洞以及恶意软件和病毒等方面分析了城市景观照明控制系统的网络安全挑战，最后，结合城市景观照明控制系统的特点，提出了硬件、软件以及数据安全等措施，进而为保障城市景观照明控制系统的正常运行提供技术支持。

关键词：景观照明；控制系统；网络安全

【DOI】10.12254/j.issn.2096-6539.2024.09.068

一、前言

城市景观照明在现代城市规划和建设中扮演着越来越重要的角色，不仅为城市夜晚增色添彩，还提升了城市形象和居民的生活质量。随着科技的不断发展，城市景观照明控制系统逐渐实现了智能化和网络化，以满足不同场景和时间的照明需求。然而，与此同时，城市景观照明控制系统也面临着越来越复杂和严峻的网络安全挑战。因此，进行城市景观照明控制系统的网络安全挑战与对策研究对于保障控制系统的安全稳定运行具有十分重要的现实意义。

二、城市景观照明控制系统概述

（一）控制系统的构成与功能

城市景观照明控制系统应搭建控制中心，建设综合管理系统，包含灯光效果控制系统、配电控制系统，配备视频监控、网络通信设施，可通过灯光手段为主对文字、图案和视频进行加工、存储、传输等处理，系统架构如图1。

首先，城市景观照明控制系统应能够实现灯光开关灯控制、实时灯光开关灯控制和离线本地控制，具备数据采集、数据管理、数据存储、故障检测、资产管理等功能。其次，对于演绎灯光，应有灯光效果编辑处理、下发、时控切换、实时切换及离线本地控制等功能。开关控制应同时具备手动、时控、远程控制功能。再次，城市景观照明控制系统还有节能和环保的功能。效果控制应能实现亮度调节、场景切换，根据使用要求设置平日、节日、重大活动及节能等不同亮灯模式。这有助于

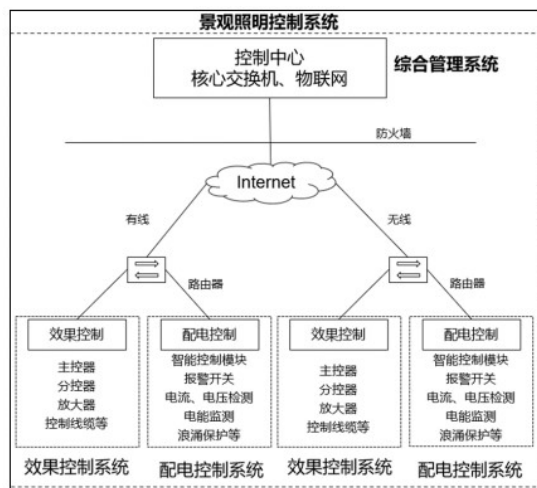


图1 景观照明控制系统架构

减少电能消耗，降低碳排放，对城市的环境可持续性产生积极影响。最后，城市景观照明控制系统通常还具备远程监控和管理功能。管理员可以通过远程访问系统，实时监测照明设备的状态和性能，及时发现问题并采取维修和维护。这有助于提高系统的可靠性和可用性。

（二）控制系统的网络化特点

城市景观照明控制系统的网络化特点包括以下几个方面：

首先，灯光秀系统根据其网络部署情况可分为局域网、运营商虚拟专用网，如与其他外部网络有信息交换，应增加安全边界防护。在控制中心的网络边界，部署防火墙设备是确保网络安全的基础。通过启用访问控制功能，可以按用户和系统之间的允许访问规则，决定用户对受控系统进行资源访问的权限。控制粒度为单个用户，这意味着可以对每个用户进行精细的权限控制，保障系统的安全性。以上策略有助于防范未经授权的访问和恶意攻击，提高网络的防护能力。部署物联网设备身份鉴别系统是保障系统整个生存周期设备标识的唯一性的关键一步。这个系统要求对接入网络边界的所有传感器、控制器等物联网设备进行设备类型及型号识别，并使用唯一ID进行标识。同时，通过实时监控检测网络边界接入行为，对合法接入终端进行接入健康检查，保证接入的安全性。采用自动化识别和注册机制，对网络中所有设备进行实时监控，有助于快速发现并处理违规设备。综合的身份鉴别系统有助于确保系统对物联网设备的可控性和合规性^[1]。

三、城市景观照明控制系统的网络安全挑战分析

(一) 数据泄漏风险

数据泄漏指的是系统中存储的敏感信息，如配置数据、操作日志、用户身份验证信息等，被未经授权的人或实体访问、获取或披露。这种泄漏可能发生在多个层面，包括系统本身、网络传输、以及用户或管理员的不当行为。

首先，如果城市景观照明控制系统的软件或固件存在安全漏洞，攻击者可能会利用这些漏洞来访问系统中存储的敏感数据。这些数据可能包括有关照明设备和配置の詳細信息，以及操作日志记录了系统的使用情况。攻击者可以利用这些数据来了解系统的运行方式，进而发起更有针对性的攻击或泄漏数据。其次，数据泄漏风险也可能发生在数据传输过程中。如果通信通道不受足够的加密保护，攻击者可能会拦截传输的数据包，然后解密并获取其中的敏感信息。这种情况可能会在数据从系统发送到远程服务器或用户设备时发生，尤其是在不安全的公共网络上。最后，用户或管理员的不当行为也可能导致数据泄漏。如果他们共享了敏感信息、密码或访问权限，或者在未经授权的情况下将数据导出到不安全的存储设备，就会存在泄漏的风险。同时，弱密码、未及时更改密码或共享访问凭证也可能导致未经授权的访问和数据泄漏^[2]。

(二) 远程控制漏洞

远程控制漏洞通常是由于系统中的软件或硬件漏洞而导致的。攻击者可以通过利用这些漏洞，远程访问控制系统，执行未经授权的操作，常见的漏洞类型如下所示：

(1) 软件漏洞。照明控制系统通常依赖于特定的软件来管理设备和执行操作。如果这些软件存在漏洞，攻击者可能通过远程方式进入系统，篡改设置、关闭照明或干扰正常运行。

(2) 通信漏洞。控制系统通常使用网络连接进行远程控制和监控。如果网络通信协议或设备存在漏洞，攻击者可能会通过网络入侵系统，从而获得对照明设备的控制权。

(3) 未经授权的访问点。如果系统的远程访问点未经适当保护，攻击者可能会通过未经授权的途径访问系统，例如通过默认密码、弱密码或未加密的通信。

远程控制漏洞可能对城市景观照明系统带来多种风险。首先，攻击者可能通过关闭照明或改变照明模式来制造混乱，影响城市的安全性和美观。其次，攻击者可能利用漏洞来获取系统中的敏感信息，如配置数据、访问权限和操作日志，这可能导致隐私泄漏和安全问题。

(三) 恶意软件和病毒

恶意软件和病毒是一类被精心设计用来破坏、感染或控制计算机系统的恶意程序，可能导致系统的不稳定

性、数据丢失和隐私泄漏等严重问题，这些恶意程序可以通过多种途径进入城市景观照明控制系统。

首先，恶意软件和病毒可能通过恶意下载进入系统。用户或管理员可能会在不知情的情况下下载了恶意软件或病毒，这些恶意程序常常伪装成合法的软件或文件，一旦运行，就会感染系统，破坏其正常运行。其次，恶意附件也是一种常见的传播途径。攻击者可能会通过电子邮件或其他通信方式发送包含恶意软件或病毒的附件给系统用户或管理员。一旦这些附件被打开，恶意程序就会进入系统，并开始破坏、感染或控制系统。最后，外部攻击也可能导致系统感染恶意软件或病毒。黑客或攻击者可以通过网络入侵城市景观照明控制系统，然后在系统中注入恶意代码或病毒，以获取对系统的控制权，从而造成损害。

一旦恶意软件或病毒进入城市景观照明控制系统，可能会导致多种问题。首先，这些恶意程序可以干扰系统的正常运行，导致照明设备的异常操作，从而影响城市的景观和安全性。其次，可能会窃取系统中的敏感信息，如访问权限、操作日志和配置数据，这可能会导致隐私泄漏和安全隐患^[3]。

四、城市景观照明控制系统的网络安全对策

(一) 落实网络安全等级保护制度

景观照明控制系统应根据设施规模、重要性、功能等确定安全保护等级，制定安全策略，使其网络安全保护能力应满足现行国家标准《信息安全技术 网络安全等级保护基本要求》(GB/T 22239)的要求，避免系统遭受未经授权的访问，防止重要数据泄漏或者被盗窃、篡改。

(二) 硬件安全措施

硬件安全措施主要涉及网络设备与通信协议的安全性，具体如下所示：

首先，确保网络设备的物理安全性。这包括将网络设备放置在安全的物理位置，以防止未经授权的人员物理访问或破坏设备。设备通常应放置在锁定的机柜或机房中，只有经过授权的人员才能进入。同时，设备上应安装物理防护措施，如摄像头监控、门禁系统等，以进一步增强物理安全性。其次，对网络通信采用安全的通信协议和加密技术。网络通信是城市景观照明控制系统的关键组成部分，因此必须确保数据在传输过程中不被窃取或篡改。采用安全的通信协议，如HTTPS、SSH等，可以加密数据传输，防止中间人攻击。此外，采用强大的加密技术，如AES（高级加密标准），可以确保数据在传输和存储时的安全性。最后，对网络设备进行定期的安全审计和漏洞扫描。网络设备可能会受到安全漏洞的威胁，因此需要定期对设备进行安全审计和漏洞扫描，以识别并解决潜在的安全问题。这包括更新设备的固件和操作系统，以修补已知的漏洞，并采取限制

不必要的服务和端口的访问^[4]。

（三）软件安全措施

软件安全措施主要关注系统软件与应用程序的安全性，具体如下所示：

首先，确保软件及应用程序的及时更新和补丁管理。系统的软件和应用程序应定期更新到最新版本，以确保已知的漏洞和安全问题得到修复。同时，应建立有效的补丁管理流程，及时应用新的安全补丁和更新，以减少系统受到已知漏洞攻击的风险。其次，进行安全编码实践。在开发和维护软件 and 应用程序时，应遵循安全编码实践，以减少常见的安全漏洞，如SQL注入、跨站脚本（XSS）等。应该定期对代码进行审查和测试，以发现潜在的漏洞并进行修复。最后，建立日志和监控系统。记录系统的活动和事件，包括登录尝试、异常操作和安全事件，以便及时检测和应对潜在的安全问题。建立监控系统来监视系统的性能和安全性，并在发现异常情况时触发警报和响应。

（四）数据安全措施

在城市景观照明控制系统中，数据安全是至关重要的一环。数据包括了关于照明设备状态、运行日志、用户信息以及城市景观照明方案等重要信息。为了应对网络安全挑战，需要采取一系列数据安全措施，包括数据加密、备份和恢复策略。

首先，数据加密是保护数据安全的关键手段。对于城市景观照明控制系统中的敏感数据，如用户信息、控制命令和照明计划等，应采用强大的加密算法进行加密存储和传输。这可以防止未经授权的访问者或黑客窃取敏感信息。同时，确保数据在传输过程中使用安全的通信协议，如TLS/SSL，以保障数据在传输中的安全性。其次，建立有效的数据备份与恢复策略。数据备份是在数据丢失或受损时的重要保障。应定期备份系统中的所有重要数据，并将备份数据存储在安全的位置，以防止数据丢失。同时，确保备份数据的完整性和可访问性，以便在需要时能够迅速进行数据恢复。恢复策略包括灾难恢复计划，以确保系统在面临灾难性事件时能够迅速恢复运行。最后，加强数据监控和审计。建立数据监控系统，跟踪数据访问和操作，以便及时发现异常活动。定期进行数据审计，以确保数据的完整性和合规性。监控和审计可以帮助识别潜在的数据安全问题，并采取相应的措施来解决它们。

（五）认证与授权

认证与授权有助于确保只有经过身份验证的用户可以访问系统，并限制他们的权限，以保护系统的安全性。

首先，用户身份验证是确保只有合法用户可以登录和使用系统的关键步骤。城市景观照明控制系统应该实施强大的身份验证机制，例如多因素身份验证，以确保

用户是其声称的人物。这可以包括使用用户名和密码结合生物识别信息、智能卡或手机验证等方法。同时，要求用户定期更改密码以提高安全性，同时记录和监控登录尝试，以便及时检测和响应潜在的安全威胁。其次，权限管理是控制用户对系统资源和功能的访问的关键。每个用户应根据其职责和需要被授予适当的权限。这可以通过分配角色和权限组来实现，以简化权限管理。例如，系统管理员和普通用户可能具有不同的权限级别，只有管理员才能进行系统配置和更改关键设置。此外，应实施严格的最小权限原则，即用户只能获得完成其工作所需的最低权限，以减少潜在的滥用权限的风险。最后，系统应定期审查和更新用户权限，以反映他们的当前职责和需求。当用户的职位发生变化或他们不再需要某些权限时，及时取消或降低其权限级别，以减少潜在的安全风险^[5]。

（六）规范安全管理机制

景观照明控制系统网络安全管理，应从安全管理机构、责任制度、安全策略、操作规程、定期检查及应急保障等方面，规范提升管理机制^[6]。首先，应制定安全运维管理责任制度，明确安全责任人，明确系统、网络、安全管理等岗位和职责。其次，应建立网络安全教育培训制度，对工作人员培训网络安全管理相关法规、规定、标准等。再次是强化应急保障，制定网络安全突发事件应急预案，定期开展应急演练，模拟不同事件报告、处置内容。

五、结语

综上所述，城市景观照明控制系统的网络安全挑战是一项综合性的系统问题，落实网络安全等级保护制度，通过硬件和软件的升级、采取有效的数据保护和严格的访问控制等技术防范措施，并规范提升管理机制，才能够更好地保护系统的网络安全。在未来，还需要不断改进和完善这些对策，以适应不断演化的网络威胁，从而确保城市景观照明系统的安全运行。

参考文献

- [1] 房晓峰. 智能控制系统在园林景观照明工程中的应用[J]. 工程建设与设计, 2022(22): 84-86.
- [2] 李磊. LED景观照明及其智能控制系统的应用[J]. 光源与照明, 2022(08): 13-15.
- [3] 冯健, 周强. 智能控制系统在室外景观照明中的应用研究[J]. 光源与照明, 2022(07): 1-3.
- [4] 邓建凯. 园林景观照明智能控制系统设计[J]. 光源与照明, 2022(06): 32-34.
- [5] 奚圣鑫. 基于物联网技术的景观照明控制系统的设计与实现[D]. 苏州大学, 2022.
- [6] 全国信息安全标准化技术委员会. 信息安全技术 网络安全等级保护基本要求GB/T 22239-2019[S]. 北京: 中国标准出版社, 2019.