# 需求分析

1 系统功能性需求

对门禁系统进行相关了解后，确定本系统所需要具备的功能，包括用户信息模块和访问控制模块。

1. 用户信息模块：主要用于记录用户信息，管理不同用户的角色和相应权限，让管理员通过用户信息进行相应的授权功能等。
2. 访问控制模块：用于确定哪些用户拥有访问门禁资源的权限，让系统根据用户的角色自动控制门禁的开启和关闭。

2 系统非功能需求

本系统非功能性需求主要从以下几个方面展现：

1. 是开放以及可拓展的：

本门禁系统允许管理员进行用户的增删改查，允许增加用户并授予门禁权限，从而对门禁系统进行拓展。

1. 使用性能简洁：

用更加简洁的界面简化用户操作流程，方便用户使用。

1. 具有可维护性：

系统中必将存在一定问题，在使用过程中，必须有管理员对系统进行时时地观察，以便在系统运行出现错误时，可以在第一时间内进行系统的修复，避免门禁系统停止运行，对用户造成困扰。

3 系统使用者

每个角色与门禁系统的交互方式和权限范围都是不同的，确保了系统的安全性和有效管理。管理员负责维护系统和用户信息，用户则通过系统进行日常的身份验证以进入授权区域，而非用户则被系统排除在外，以保障区域的安全。

以下是三个角色的职责、权限以及操作：

1. 管理员：

职责：管理员是门禁系统的最高权限持有者，负责系统的日常管理和维护工作。

权限：管理员可以添加或删除用户信息，分配或修改用户的访问权限，监控门禁系统的运行状态，以及在必要时进行系统设置的更改。

操作：管理员可能需要通过一个管理界面来执行操作，如用户账户管理、权限配置、审计日志审查、系统更新和故障排除等。

1. 用户

职责：用户是门禁系统授权允许进入特定区域的人员，通常是企业员工、居民或注册访客。

权限：用户拥有进入授权区域的权限，但通常只能进行与个人身份验证相关的操作。

操作：用户通过门禁系统进行身份验证，如输入密码、刷卡、指纹识别或面部识别，以获得进入权限。

3.非用户

职责：非用户是指那些没有获得门禁系统授权的人员，可能是未注册的访客、服务人员或其他未经授权的个体。

权限：非用户没有权限通过门禁系统进入特定区域。

操作：当非用户试图通过门禁时，系统会阻止他们进入，并可能触发安全警报或通知管理员。

4 系统用例分析

4.1系统概述：简单门禁系统是一个用于控制特定区域进出的安全系统，它通过识别和验证用户的身份来授权或拒绝访问。

4.2角色定义：

管理员：负责系统配置、用户权限管理、系统监控和维护。

用户：拥有进入特定区域权限的个体，需要通过身份验证。

非用户：未获得进入权限的个体，系统将拒绝其访问。

4.3用例列表：

用例1：用户身份验证

用例2：权限分配与修改

用例3：门禁监控

用例4：非用户访问尝试

4.4用例详细分析：

1.用例1：用户身份验证：

用例目标：允许授权用户通过身份验证进入特定区域。

活动者：用户。

前置条件：用户已被管理员授权并注册到系统中。

后置条件：用户成功通过身份验证并进入区域或被拒绝访问。

事件流：

1.1用户接近门禁点。

1.2用户提供身份验证信息（密码、刷卡、指纹或面部识别）。

1.3系统验证用户信息。

1.4系统根据验证结果开启或保持门锁关闭。

1.5系统记录验证事件。

2.用例2：权限分配和修改：

用例目标：管理员分配或修改用户访问权限。

活动者：管理员。

前置条件：管理员已登录到管理系统。

后置条件：用户权限更新成功。

事件流：

2.1管理员访问用户管理界面。

2.2管理员选择用户并编辑其权限。

2.3管理员保存权限更改。

2.4系统更新用户权限信息。

1. 用例3：门禁监控：

用例目标：管理员实时监控门禁状态和用户活动。

活动者：管理员。

前置条件：管理员已登录到监控系统。

后置条件：管理员获得当前门禁状态和用户活动信息。

事件流：

3.1管理员访问监控界面。

3.2系统显示实时门禁状态和用户活动日志。

3.3管理员监控并根据需要进行干预。

1. 用例4：非用户访问尝试：

用例目标：系统阻止非用户进入特定区域并记录尝试。

活动者：非用户。

前置条件：非用户接近门禁点。

后置条件：非用户的访问尝试被记录并可能触发警报。

事件流：

4.1非用户接近门禁点并尝试进入。

4.2系统识别非用户并拒绝访问。

4.3系统记录访问尝试并可能通知管理员。

4.5系统需求：

1.系统应支持多种身份验证方式。

2.系统应具备实时监控和日志记录功能。

3.系统应允许灵活的权限管理。

4.系统应保证数据的安全性和隐私性。

4.6 安全和隐私：

1.系统应采用加密技术保护用户数据。

2.系统应有防止未授权访问和数据泄露的措施。

通过这些用例分析，我们可以确保简单门禁系统的设计能够满足不同角色的需求，同时保障系统的安全性和有效性。