|  |  |
| --- | --- |
| 用例名 | 选课 |
| 简要描述 | 学生通过该用例选择要上的课程 |
| 参与者 | 学生 |
| 相关用例 | 无 |
| 前置条件 | 学生已正确登录到系统 |
| 后置条件 | 如果选课成功，则系统记录学生选课信息 |
| 基本事件流   1. 用例起始于学生需要选课 2. 学生查询可选学期（D-1） 3. 系统显示可选的学期信息（A-1）（D-2） 4. 学生选择某个可选的学期 5. 系统显示该可选学期的所有可选课程信息列表（A-2）（D-3） 6. 学生确认选择的课程 7. 系统保存学生的选课信息（B-1），显示选课成功（A-3），用例结束 | |
| 备选事件流  A-\* 学生在确认选课前，随时都可以中止该用例   1. 系统提醒学生当前所有操作都会被取消 2. 学生确认后，当前用例结束，也可选择取消，则继续后续操作   A-1 没有找到可选学期   1. 系统显示没有找到可选学期 2. 学生选择结束该用例   A-2 没有找到可选课程   1. 系统显示没有找到可选课程 2. 学生选择结束该用例   A-3 系统保存失败   1. 系统显示保存失败信息，并提醒学生重新提交 2. 学生可以重新提交本次选择的课程，也可以结束该用例 | |
| 补充约束-数据需求  D-1 无特定的查询条件  D-2 可选学期信息是学年-学期格式，例：22-23上  D-3 可选课程信息包括：课程名称、课程性质（必修/选修）、学时、学分、学院、学期、上课教师姓名、上课时间、上课教室  补充约束-业务规则  B-1 必修课程必须全部选择  B-2 所有选择课程的学分要满足该学期学分要求  B-3 所选择课程的上课时间不能冲突 | |
| 待解决问题  无 | |

|  |  |
| --- | --- |
| 用例名 | 注册 |
| 简要描述 | 学生通过学号注册系统 |
| 参与者 | 学生 |
| 相关用例 | 无 |
| 前置条件 | 学生学号输入正常 |
| 后置条件 | 注册成功在选课系统中录入该学生信息 |
| 基本事件流   1. 学生打开注册页面或应用程序。 2. 系统显示注册表单，包含必填字段和可选字段。 3. 用户填写注册表单，包括学号、密码、电子邮件地址等必填字段，以及可选的个人信息字段。 4. 学生提交注册表单。 5. 系统验证学生填写的表单信息，确保符合要求。 6. 系统检查学号和电子邮件地址是否已被使用。 7. 如果学号或电子邮件地址已存在，系统显示相应错误消息，提示用户选择其他用户名或电子邮件地址。 8. 如果学号和电子邮件地址可用，系统创建一个新账号，并将用户填写的信息保存到数据库中。 9. 系统生成一个确认链接或发送确认电子邮件给用户，要求学生验证其电子邮件地址。 10. 系统显示注册成功消息，并提示用户进行进一步操作，如登录或完善个人信息。 | |
| 备选事件流  步骤 5-7：如果用户填写的表单信息不符合要求，系统显示相应错误消息，并要求用户根据错误提示进行修改。  步骤 9：如果系统无法发送确认电子邮件给用户，系统显示相应错误消息，并提供其他方式供用户进行验证，如通过手机短信验证。 | |
| 补充约束-数据需求   1. 密码复杂度要求：系统可以设置密码复杂度要求，例如密码长度、包含特殊字符、数字或大写字母等要求。 2. 唯一性约束：用户名和电子邮件地址需要唯一，系统需要验证新注册的用户名和电子邮件地址是否已存在于数据库中。 3. 必填字段：注册表单中可能存在必填字段，如用户名、密码和电子邮件地址等，系统需要确保用户填写了这些必填字段。 4. 验证码验证：系统可以引入验证码功能，在注册过程中要求用户输入验证码以防止恶意注册。 5. 注册限制：系统可以设置注册限制，如限制每个IP地址或设备在一定时间内只能注册一个账号，以防止滥用和恶意注册。 6. 安全性考虑：注册过程应使用安全的传输协议（如HTTPS）来保护用户的个人信息，确保数据在传输过程中的机密性和完整性。 7. 合法性验证：系统应对用户提交的数据进行验证，确保输入的数据符合规范，如验证电子邮件地址格式是否正确。 8. 服务条款接受：用户注册过程中可能需要接受系统的服务条款和隐私政策。 | |

图表 1

|  |  |
| --- | --- |
| 用例名 | 学生登录 |
| 简要描述 | 学生通过输入正确的账号密码成功进入系统 |
| 参与者 | 学生 |
| 相关用例 | 无 |
| 前置条件 | 学生已注册成功到系统 |
| 后置条件 | 如果选课成功，则系统记录学生选课信息 |
| 基本事件流   1. 用户打开登录页面或应用程序。 2. 系统显示登录表单，包括用户名和密码字段。 3. 用户输入用户名和密码。 4. 用户点击登录按钮或按下回车键。 5. 系统验证用户输入的用户名和密码是否正确。 6. 如果用户名和密码正确，系统将用户标识为已登录状态，并允许用户访问相关功能。 7. 系统显示登录成功消息，并跳转到用户的个人首页或主界面。 | |
| 备选事件流  用户名或密码不正确：  在步骤 5，系统验证用户输入的用户名和密码后发现不匹配。  系统显示错误消息，提示用户输入正确的用户名和密码。  用户可以重新输入用户名和密码，然后点击登录按钮，重试登录。  或者用户可以选择重置密码选项，通过提供相关信息进行密码重置操作。  用户未填写用户名或密码：  在步骤 3，用户未填写用户名或密码字段。  系统显示错误消息，提示用户输入必填的用户名和密码。  用户补充完整用户名和密码，然后点击登录按钮，重试登录。  账号锁定：  在步骤 5，系统检测到用户连续多次输入错误的用户名或密码。  系统锁定用户的账号，禁止登录一段时间或需要进行解锁操作。  系统显示相应的锁定消息，并提供解锁账号的选项，如通过电子邮件或安全问题进行解锁。  双因素认证：  在步骤 5，系统启用了双因素认证功能。  系统要求用户进一步验证身份，例如通过手机短信、手机应用程序生成的验证码或指纹扫描等方式。  用户提供第二个因素的验证，系统验证通过后用户可以成功登录。 | |
| 补充约束-数据需求  步骤 5：如果用户输入的用户名或密码不正确，系统显示相应错误消息，并要求用户重新输入正确的用户名和密码。 | |