安全性：场景1：阻止恶意抢火车票行为

|  |  |
| --- | --- |
| 场景组成部分 | 可能的值 |
| 源 | 外部恶意软件 |
| 刺激 | 以用户身份持续购票或者快速购票 |
| 制品 | 购票模块 |
| 环境 | 系统运行时 |
| 响应 | 系统冻结此用户的账号，阻止其购票行为 |
| 响应度量 | 当恶意软件发出恶意请求时，要在1s内检测。  在1s内冻结其账户操作。 |

安全性：场景2：阻止黑客攻击

|  |  |
| --- | --- |
| 场景组成部分 | 可能的值 |
| 源 | 对系统的攻击行为 |
| 刺激 | 黑客对系统的数据攻击、DOS攻击等 |
| 制品 | 系统 |
| 环境 | 系统运行时 |
| 响应 | 系统检测到攻击，同时采取相应保护措施，避免攻击范围扩大，消除攻击带来的影响 |
| 响应度量 | 在1s之内检测到正在进行的攻击。  在1s内采取安全措施。  在1s内消除攻击带来的影响。 |

可用性：场景1：应对系统错误

|  |  |
| --- | --- |
| 场景组成部分 | 可能的值 |
| 源 | 系统内部的运行或者是用户的操作 |
| 刺激 | 大量用户的操作导致系统压力增大或者是系统自身运行时出现错误 |
| 制品 | 系统 |
| 环境 | 系统运行时 |
| 响应 | 如果压力过大则将压力转移到一些设备上。如果是出错，那么快速修复错误。 |
| 响应度量 | 诊断异常状况的时间不超过2s  将请求压力转移到其他设备上的时间不超过3s  快速修复错误的时间不超过2s  错误修复成功率不低于90% |

可延展性：场景1：硬件升级

|  |  |
| --- | --- |
| 场景组成部分 | 可能的值 |
| 源 | 开发人员 |
| 刺激 | 系统硬件需要升级，如可能增加服务器数量，或者对单个服务器进行硬件的修改 |
| 制品 | 系统硬件 |
| 环境 | 系统在构建中或者已经上线 |
| 响应 | 对系统硬件进行淘汰或更新  修改项目使之适应新的硬件环境  测试更改对于系统造成的影响  发布维护变更 |
| 响应度量 | 升级时间不应超过8小时  升级所影响的代码量不应超过2% |

可延展性：场景2：服务器数据库升级

|  |  |
| --- | --- |
| 场景组成部分 | 可能的值 |
| 源 | 开发人员 |
| 刺激 | 服务器数据库需要进行扩容或者分布式处理 |
| 制品 | 服务器，数据库 |
| 环境 | 系统在构建中或者已经上线 |
| 响应 | 对数据库进行升级处理  修改服务端响应代码  测试修改后性能 |
| 响应度量 | 升级时间不应超过8小时  升级所影响的代码量不应超过3% |

互操作性：场景1：和第三方系统进行交互

|  |  |
| --- | --- |
| 场景组成部分 | 可能的值 |
| 源 | 系统 |
| 刺激 | 系统请求和第三方系统交互 |
| 制品 | 第三方系统 |
| 环境 | 系统运行时或构建时 |
| 响应 | 系统成功拿到第三方系统的服务 |
| 响应度量 | 交互请求成功率大于99.9% |

易用性：场景1：正常操作

|  |  |
| --- | --- |
| 场景组成部分 | 可能的值 |
| 源 | 终端用户 |
| 刺激 | 想要使用系统完成操作 |
| 制品 | 系统 |
| 环境 | 系统运行时 |
| 响应 | 能够正确引导用户完成操作  提供撤销或取消功能，在用户操作过程中识别并纠正用户错误  错误发生时的恢复 |
| 响应度量 | 用户完成单项操作的时间小于等于2min  用户操作成功率应该大于等于99%  错误恢复时间小于5min |

性能：场景1：系统运行

|  |  |
| --- | --- |
| 场景组成部分 | 可能的值 |
| 源 | 用户，第三方系统 |
| 刺激 | 非周期性的数据请求，操作请求 |
| 制品 | Broker模块，服务器模块，request bus |
| 环境 | 系统正常运行时，系统高负载时 |
| 响应 | 系统执行用户请求的操作；处理用户数据；返回数据 |
| 响应度量 | 请求响应延迟时间不超过5s  请求丢失的比例不超过0.001% |