Exercise Session 1: Quality Scenarios

Gregory Gay
DIT635 - January 29, 2021

Exercise Sessions

- Every Friday, 13:15 - 15:00
- Builds on the lectures with interactive activities.
    - This week: **quality scenarios**
    - We give introduction and an activity.
    - You work in groups.
    - Feel free to come and go, split off into breakout rooms.
- Professor + TAs will be here to answer questions.
    - Not graded - intended to build skills that will be helpful on assignments and in the future.
    - **This is also a good time to ask us homework questions too!**

Exercise - Airport Parking

- Fully automated parking system.
  - User can insert credit card into a reader at parking ramp entrance. Records time of entry.
  - User presents same card on exit.
  - User can also get a ticket on entry (with time of entrance) and pay by credit card or cash on exit.
- Interacts with: customers, police, emergency responders, managers, external card validation and payment systems, accounting system, physical gate and signage, personnel system

Exercise - Airport Parking

The system will be deployed within the physical architecture of the airport parking garage, incorporating:

- Entrance Kiosks
  - Card dispensers
  - Credit card reader for e-park
  - Card reader for contract parking
  - Entry gate
- Parking entrance
  - Signage {FULL / NOT FULL}

- Exit Kiosks
  - Signage: {OPEN / CLOSED}
  - Staffed kiosks
  - Automated kiosks
  - Exit gate
- Security Cameras
- Hardware for Parking System
  - Dual server w/failover (can switch in event of failure)
  - Clustered DB
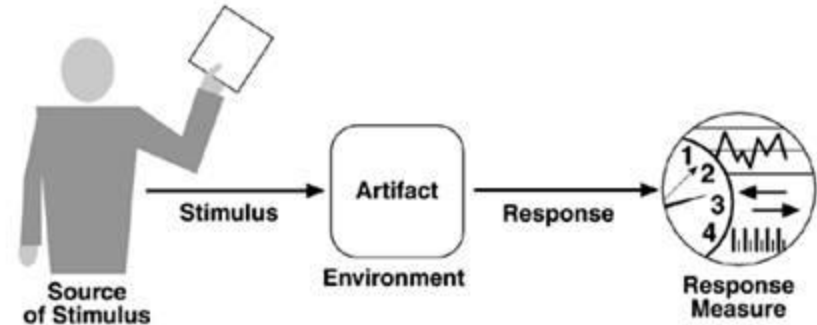 - Storage area network

Scenario Format

Overview:

Brief description of the scenario.

External Stimulus:

Input or environmental factors that initiate the scenario.

(e.g., user request, infrastructure changes or failures, security attacks)

Scenario Format

System State:

Aspects of internal state that affect quality (e,g., information stored in the system or database, current load)

System Environment:

Significant observations about the external environment (e.g., network connection, external system availability).

Source of Stimulus → Stimulus → Artifact Environment → Response → Response Measure
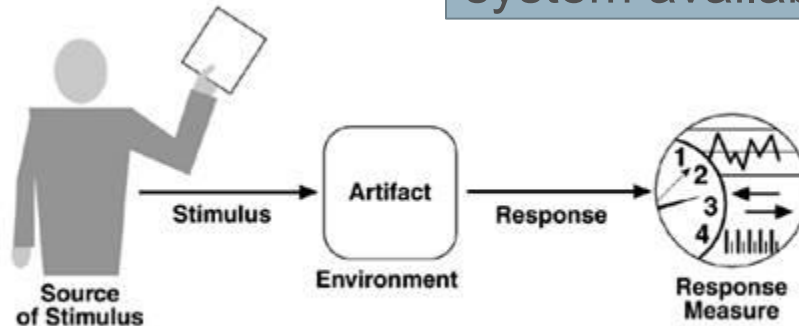
Scenario Format
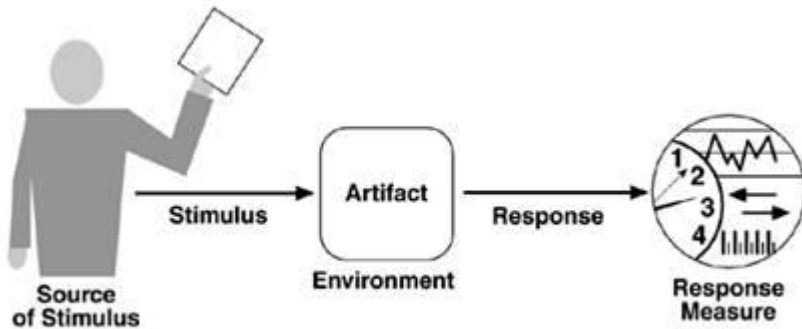
Required System Response:

How does the system respond and meet the quality goal?

(e.g., how should it handle a defined increase in requests?)

Response Measure:

How we judge whether the system meets the quality goal.

(e.g., throughput, timing, availability)

Activity

- Scenarios centered around the following:
  - Reliability (POFOD, ROCOF, MTBF)
  - Availability
  - Performance
  - Scalability
  - Security
- Remember to include both a response and a response measure (with acceptable threshold)!

Reliability Example

- **Overview:** A user attempts to enter the ramp, using the credit card option.
- **System State:** System is operating normally.
- **Environment State:** The garage is not empty or full (0 < N < 100). All physical devices are functioning properly.
- **External Stimulus:** The user inserts their credit card into the reader at an entrance kiosk.
- **Required Response:** The system authenticates the card. If accepted, the system sends the command to raise the physical gate. If the garage is now full, the ramp sign is updated to FULL.
- **Response Measure:** The ROCOF must be less than 2/day on average, with MTBF of at least 16 hours.

Availability Example

- **Overview:** System recovery when connection to entry gate is disrupted.
- **System State:** System is operating normally.
- **Environment State:** Connectivity is normal. Garage is not empty or full ($0 < N < 100$). All physical equipment is functioning.
- **External Stimulus:** The system fails to connect to an entry gate for a sustained length of time (over two minutes, or 100 missed heartbeat messages).

Availability Example

- **Required Response:**
  - The system will update the sign to CLOSED for that kiosk. The screen at the kiosk will display an error message, and no credit cards will be accepted or tickets dispensed. The system will send a notification to managers and personnel.
  - The system will continue to send heartbeat messages until a sustained connection is established.
  - When a connection is established, the entrance will be reopened and resume normal operations.
- **Response Measure:** The entrance must be closed within 30 seconds of detecting the loss of connection (95% of the time), within 45 seconds 99% of the time. On establishing a connection again, it must be reopened within 30/45 seconds (95/99% of the time).

Performance Example

- **Overview:** Ensure that system can handle cars exiting garage at rush hour (high throughput).
- **System State:** System is operating under heavy load (> 1000 exit requests per hour).
- **Environment State:** All 10 exit kiosks are occupied, with additional cars waiting to exit at each.
- **External Stimulus:** A large number of card processing/exit requests come within a short window of time (10 within a one minute window).

Performance Example

- **Required Response:** All card payments are posted successfully (unless a card is invalid). All cars are released (system lifts gate and recloses it once car leaves).
- **Response Measure:** 95% of the time, all 10 kiosks release the waiting car within 30 seconds of the request. 99% of the time, all kiosks release within 45 seconds of the request.

Security Example

- **Overview:** An attacker disrupts the security cameras of the garage.
- **System State:** The system is operating normally.
- **Environment State:** The environment is operating normally. All hardware is functioning. The garage is not empty or full ($0 < N < 100$).
- **External Stimulus:** An attacker disrupts the network connection to the security cameras (either a physical or software-based attack).

Security Example

- **Required Response:**
    - The system will detect the loss of connection to the cameras (sustained missed heartbeat messages, > 15 missed messages or > 30 seconds).
    - All entrance and exit kiosks will be closed (gates will not raise, signs switch to closed, error message displayed), except to security personnel.
    - Security personnel will be notified, and must send "OK" message to the system to resume normal operations.
- **Response Measure:** All kiosks are closed within 30 seconds of detection. Notifications are sent within 45 seconds of detection.

Some Starting Ideas

- Performance
  - Time to exit ramp
- Availability
  - Exit Kiosk Malfunction
  - Loss of Connection to Credit Card Processing
- Scalability
  - Addition of more entrance/exit kiosks.
- Security
  - DDOS attack on a public API of the parking system (does one exist?) or external dependencies (payment systems)