161250041
软件学院 侯韵晗

Software Structured Design & Architecture

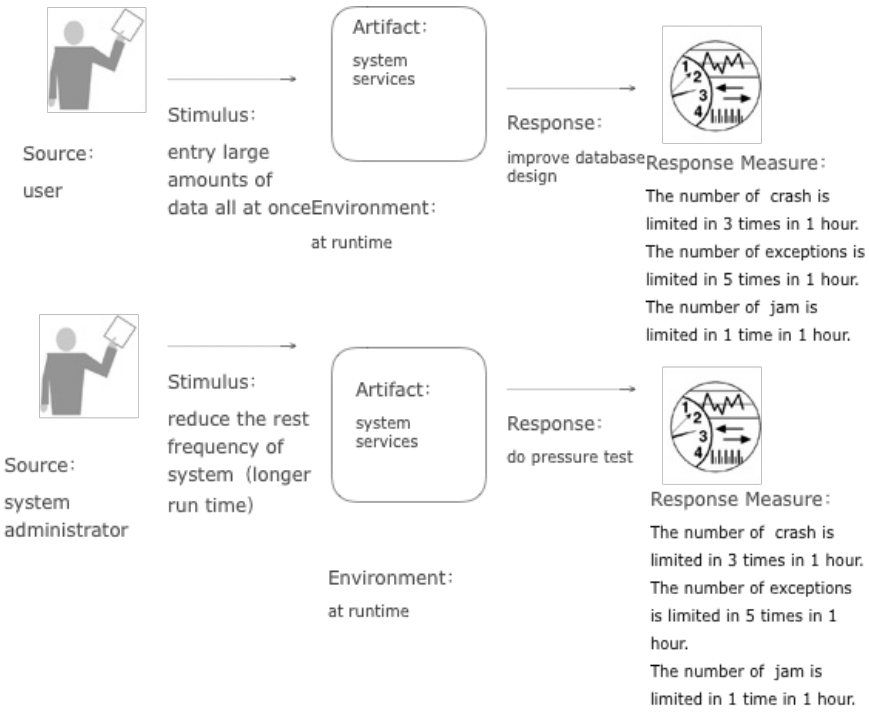
Assignment 1

stability vs. reliability

1. scenario
   a) stability
      i. General scenario

Portion of Scenario	Possible Values
Source	Internal and external sources
Stimulus	Some unstable factors： increased system business pressure or increased data volume or too long run time
Artifact	System services
Environment	At runtime
Response	Reduce the crash and ensure that no exceptions are thrown: improve system architecture improve database design do pressure test（do more test）
Response Measure	The number of exceptions and crash thrown

ii. Typical concrete scenario

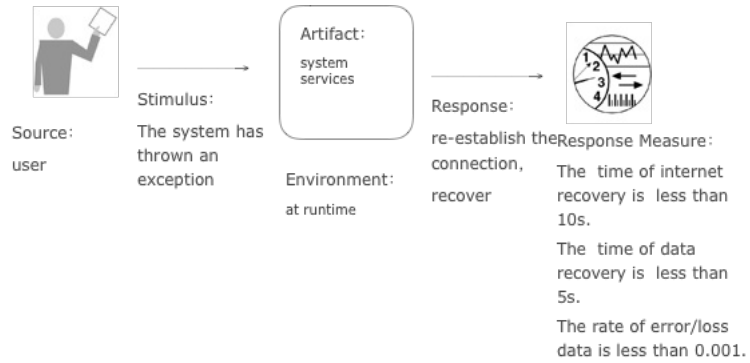


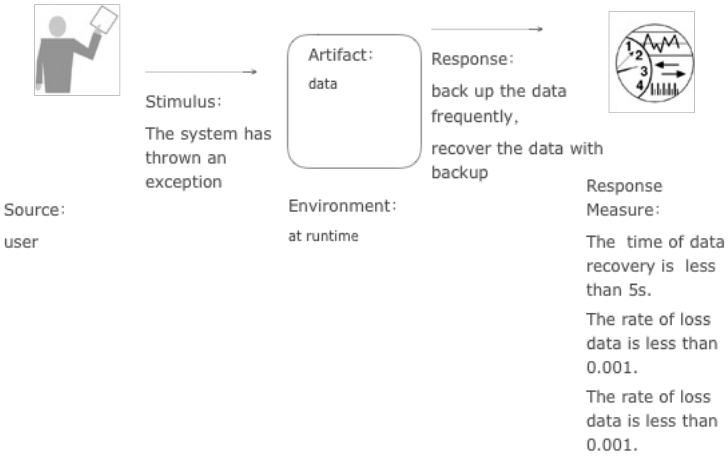
b) reliability

i. General scenario

Portion of Scenario	Possible Values
Source	Internal and external sources
Stimulus	The system has thrown an exception
Artifact	System services, data
Environment	At runtime
Response	Reduce data loss and data errors, ensure data accuracy: re-establish the connection as soon as possible back up the data recover quickly
Response Measure	Fault tolerance of data, the rate of recovery

ii. Typical concrete scenario





2. relationships and differences

a) relationships:

1. Their goals are both to ensure no mistakes when using the system.

2. They both reflect the system's ability to adapt to unstable phenomena.

b) differences:

1. Stability means that the system can run without crash, jam, or exception.

2. Reliability means that after a system failure, such as a network connection is interrupted, or the system is disconnected, data and network can still be restored to their original state without causing errors.

3. Reliability is that some faults have occurred in the system but the data is guaranteed to be error-free; the stability is guaranteed not to fail but the data is not necessarily correct.

c) examples:

1. If the system fails and the system can quickly recover the correct data and network connections.It has reliability.

2. If the system can guarantee as few failures, jams, and anomalies as possible.It has stability.

3. strategies and tactics

QA	Strategy	Tactic	Impact
stability	Improve system architecture design	improve code architecture	more excellent code style, more stable system architecture
		improve database design	enhance the stability in the face of large data access and storage
	plan the test reasonably	do 7*24 pressure test	strengthen the system's compressive resistance to long-term work
		do the edge test	ensure system stability on boundary issues
reliability	back up the date	back up the data of usage	ensure the correctness of the data
		back up the configuration information	ensure the correctness of the configuration information
	reduce the time to recover	Improve code to detect accidents	reduce the time to find an accident
		improve	reduce the time to re-establish

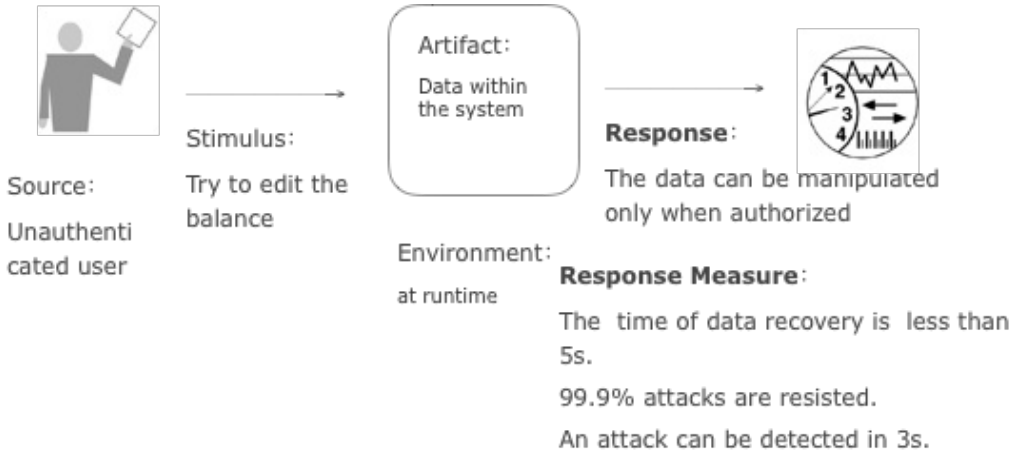
		reconnection mechanism	the connection

security vs. safety

1. scenario
   a) stability
      i. General scenario

Portion of Scenario	Possible Values
Source	Malicious attackers, destructive forces, unauthorized users
Stimulus	Attack (or exploit), the action taken to harm the system/data.
Artifact	System services, data within the system, a component or resouces of the system, data produced or consumed by the system.
Environment	The system is either online or offline; either connected to or disconnected from a network;either behind a firewall or open to a network; fully operational,partially operational, or not operational.
Response	The data/services can be accessed, manipulated only when authorized and will be available for legitimate use. Parties to a transaction are identified with assurance. The parties to the transaction cannot repudiate their involvement.
Response Measure	The rate of recover.The time passed before an attack was detected. How many attacks were resisted. How much data is vulnerable to a particular attack. How much of a system is compromised when a particular component or data value is compromised.

      ii. Typical concrete scenario



Source:

Malicious intruder

Stimulus:

Attempt to edit the system configuration

Artifact:

system configuration , system service

Environment:

at runtime

Response:

The service can be accessed only when authorized and will be available for legitimate use.

Reject the request.

Response Measure:

99.9% attacks are resisted.

0.01% is compromised when a particular component or data value is compromised.

The time of data recovery is less than 5s.

b) safety

i. General scenario

Portion of Scenario	Possible Values
Source	Authorized users, system administer, developer.
Stimulus	Unintentional accidents in normal use.
Artifact	System services, data within the system, a component or resouces of the system, data produced or consumed by the system.
Environment	The system is either online or offline; either connected to or disconnected from a network;either behind a firewall or open to a network; fully operational,partially operational, or not operational.
Response	**Design**: Software safety requirements analysis Software safety design analysis Software safety test analysis Software safety change analysis Software security and various software protection technologies should be used in the system. **Runtime**: Back up the data in time The data/services can be accessed, manipulated only when authorized. **Deal with the accidents**: Reduce the data/service losses/error: ignore(if the incident doesn't affect the system) pause->repair and continue/(if can't be repair)stop
Response Measure	The rate of recover.The time passed before an attack was detected. How many accidents were resisted. How much data is vulnerable to a particular attack.

ii. Typical concrete scenario

Source:

Authenticated user(but not the system administer)

Stimulus:

Attempt to edit the system configuration

Artifact:

system configuration , system service

Environment:

at runtime

Response:

The service can be manipulated only when authorized and will be available for legitimate use.

Reject the request.

Response Measure:

99.9% attacks are resisted.

0.01% is compromised when a particular component or data value is compromised.

The time of data recovery is less than 5s.

Source:

Authentica ted user

Stimulus:

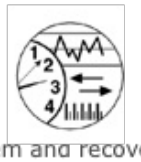
Succeed to pay the bill which is larger than the balance

Artifact:

Data within the system

Environment:

at runtime



Response:

Repair the system and recover the data in time

Response Measure:

The time of data recovery is less than 4s.

This accident can be detected in 3s.

The service can be repaired in 5s.

2. relationships and differences

a) relationships:

1. Their goals are both to ensure the safe when using the system.

2. They both reflect the system's ability to adapt to the unsafe situation, whether the accident is cause intentionally or unintentionally.

b) differences：

1. Safety refers to the loss of system prevention caused by **unintentional** actions by **non-malicious** users.

2. Security refers to the loss of system prevention caused by **malicious** operators due to **intentional** actions.

c) examples：

1. The **authenticated** user(not the system administer) doesn't have the permission to modify the system configuration.If he submits the request to modify the system configuration **unintentionally**, the system will refuse his request.This attributes is called Safety.

The **malicious** intruder attempts to modify the system configuration **intentionally**, the system will refuse his request.This attributes is called Security.

3．strategies and tactics

QA	Strategy	Tactic	Impact
security	regulate the authority to obtain and modify data	Configuration information is only available to administrators to modify	ensure the security of the configuration file
		The normal user authenticated also cannot perform operations beyond the authority.	regulate user behavior better.
	strengthen the management of users‘ rights	Users must log in first.	strengthen the system's compressive resistance to long-term work
		detecting the user's operating environment	reduce the risk
safety	back up the date	back up the data of usage	ensure the correctness of the data
		back up the configuration information	ensure the correctness of the configuration information
	deal with the accidents quickly	judge the impact of the accident on the process	do more efficient processing
		Improve code to increase the rate of process repair	reduce the time to re-establish the connection
	improve the software safety design	do software safety test analysis	make system design more reasonable and enhance system security

		do software safety design analysis	make system design more reasonable and enhance system security