On Applying FMEA to SOAs

A Proposal and Open Challenges

Cristiana Areias <careias@dei.uc.pt>
PhD Student @ University of Coimbra

Nuno Antunes
João Cunha

Department of Informatics Engineering
University of Coimbra, Portugal
Outline

- Contextualization and Motivation
  - Service Oriented Architectures (SOA)
  - Verification and Validation (V&V)
  - Failure Mode and Effects Analysis (FMEA)

- **FMEA4SOA**

- Open Challenges to Runtime FMEA4SOA
Service Oriented Architectures

- Used in a wide range of scenarios
  - Support business processes
  - Increase business agility
  - Improve interoperability
  - Composed by Services

- Dynamic
- Complex

How to guarantee the quality of SOAs?
**V&V** is the process of assessing the quality of software systems throughout their lifecycle.

- **Verification**: Are we building the **product right?**
- **Validation**: Are we building the **right product?**

**Multiple Techniques Available:**
- Walkthroughs, Inspections
- Testing
- Formal Methods
- RAMS Analysis (**FMEA**, **FTA**, Hazard Analysis,...)
- ...

---

Cristiana Areias | SERENE | 15 October 2014, Budapest
Can we apply traditional V&V in SOAs?

V&V in Critical Systems
- Detailed checking prior to deployment
- Rigorous V&V forms

Service Oriented Architectures
- Multitude of services is being deployed, interconnected and updated in a dynamic fashion
- Uncertain boundaries and surrounding environment
- Extreme Dynamicity

Do not suit...
The solution is…

Runtime V&V

The Challenge: how to apply V&V techniques on SOAs at runtime?
- To continuously assure the required quality
- Thus, improve trustworthiness
Failure Modes and Effects Analysis

- Reliability analysis technique
  - Forestall failure modes
  - Mitigate potential risks
  - Assess the impact of failures on system

- Helps on anticipating **what, where** and **how** something might fail
  - Product, processes, system, services, etc.

- Identify the parts that should be improved
Why apply Software FMEA for SOAs?

- To allow the **systematic review** of the environment
  - Understand the most critical services...
  - ... their risks and effects of their failures

- To **prioritize** the services based on the needs to apply other V&V techniques

- To determine the services that must be **re-verified** and/or **re-validated**
Scope and boundaries definition

- Provider
- Service
- Operations

Type of control

- Under Control
- Partially Under Control
- Within-Reach
What could go wrong?
## FMEA4SOA Workflow (2)

### Scope and services for analysis

- Failures Modes

### Failure Modes

<table>
<thead>
<tr>
<th>Failure Modes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unavailable service or operation</td>
<td>The service is unavailable or the operation invoked does not exist.</td>
</tr>
<tr>
<td>Operation execution hangs</td>
<td>The service and operation execution hangs and should be ended by force.</td>
</tr>
<tr>
<td>Abnormal termination</td>
<td>The service execution stops abnormally once an unexpected exception is raised by the application.</td>
</tr>
<tr>
<td>No error output after timeout</td>
<td>There is no error indicating that an operation cannot be performed after a timeout.</td>
</tr>
<tr>
<td>Invalid error code</td>
<td>The error code returned by the service is not correct.</td>
</tr>
<tr>
<td>Slow service</td>
<td>The service executes the intended operation but the response is delayed.</td>
</tr>
<tr>
<td>Incorrect results</td>
<td>The service provides an incorrect output.</td>
</tr>
<tr>
<td>Incoherent results</td>
<td>The service provides incoherent results when it executes non-deterministic actions.</td>
</tr>
<tr>
<td>Outdated results</td>
<td>The service returns outdated results according to what was agreed upon in SLA and QoS.</td>
</tr>
</tbody>
</table>
What are the effects of such failure? Its impact?
FMEA4SOA Workflow (3)

Assess the severity of effects according to the impact as perceived by the user

<table>
<thead>
<tr>
<th>Effect</th>
<th>Severity Description</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No effect or the effect will not be perceived by the consumer.</td>
<td>1</td>
</tr>
<tr>
<td>Minor</td>
<td>Minor effects on the service operation performance but still working on the SLA threshold. The service operation does not require repair or an acceptable workaround or solution exists. The data were not corrupted.</td>
<td>2</td>
</tr>
<tr>
<td>Significant</td>
<td>The performance is highly degraded and the operation may not operate, affecting the consumer with frequent or continuous instabilities. SLA can be seriously compromised so the service operation requires repair.</td>
<td>3</td>
</tr>
<tr>
<td>Extreme</td>
<td>The service operation is unavailable or is providing incorrect results with critically impact on business consumers.</td>
<td>4</td>
</tr>
<tr>
<td>Hazardous</td>
<td>The failure involves outcomes that affects a bigger part of the SOA environment or even compromise the entire system.</td>
<td>5</td>
</tr>
</tbody>
</table>
What are the possible causes of the failure?

- **Scope and services for analysis**
- **Failures Modes**
- **Identify Causes**
- **Identify Effects**
- **Most Severe**
- **Severity**

### Identify Causes

<table>
<thead>
<tr>
<th>Class</th>
<th>Cause</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>Network problem</td>
<td>The network adapters are having trouble to perform as expected or are making the server unreachable.</td>
</tr>
<tr>
<td></td>
<td>Machine reboots</td>
<td>The machine that supports the applications rebooted.</td>
</tr>
<tr>
<td></td>
<td>Application server crash</td>
<td>The application server crashed and needs to be restarted to resume its activity.</td>
</tr>
<tr>
<td></td>
<td>Resource exhaustion</td>
<td>The resources that are needed to perform the action (e.g. memory, storage) were entirely consumed.</td>
</tr>
<tr>
<td></td>
<td>Server overload</td>
<td>The server is receiving more requests than it can handle.</td>
</tr>
<tr>
<td>Development</td>
<td>Incorrect requirements</td>
<td>The functional requirements are not well specified so the service does not perform as expected.</td>
</tr>
<tr>
<td></td>
<td>specification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incorrect Design</td>
<td>The service/operation was incorrectly designed.</td>
</tr>
<tr>
<td></td>
<td>Codification Error</td>
<td>The service/operation had a function, assignment, interface, timing or algorithm codification error.</td>
</tr>
<tr>
<td></td>
<td>Service description incorrect or missing</td>
<td>The service is well implemented but its description is not clear or is described incorrectly causing a wrong invocation.</td>
</tr>
<tr>
<td></td>
<td>Service requirement changed</td>
<td>The service requirements changed and the interface is inconsistent.</td>
</tr>
<tr>
<td>Exceptions</td>
<td>Incorrect SLA</td>
<td>The SLA that supports the service is incorrect or is outdated due to the changes in the service.</td>
</tr>
<tr>
<td></td>
<td>Attacks</td>
<td>Attacks targeting the service implementations, infrastructure or transactions.</td>
</tr>
</tbody>
</table>
How could this failure be prevented?

Which controls exist in the SOA system?
For each of the possible causes, assess the probability of occurrence.
What is the likelihood that such failure is detected before affecting other components of the system or its user?
FMEA for SOA Workflow (6)

1. Scope and services for analysis
2. Failures Modes
3. Identify Effects
4. Identify Causes
5. Current Controls
   - Prevention
   - Detection
6. Risk Priority Number

Severity × Occurrence × Detection = RPN

Most Severe

For each cause

For each control

Cristiana Areias | SERENE | 15 October 2014, Budapest
Identify corrective actions and re-calculate RPN
FMEA4SOA Workflow (7)

1. Scope and services for analysis
2. Failures Modes
3. Identify Effects
4. Identify Causes
5. Current Controls
   - Prevention
   - Detection
6. For each control
   - X Occurrence
   - X Detection
7. Corrective Actions

Challenges to Runtime FMEA4SOA

Identify corrective actions and re-calculate RPN

Severity X Occurrence X Detection = RPN
Challenges to Runtime FMEA4SOA (1)

- Lack of knowledge on environment and services
  - Historical data of the used services helps, but it may be insufficient for a deep analysis
    - Explore cooperation between partners, share information to perform the FMEA

- Environment evolves and failure impact also
  - Fault injection is a possible solution but...
    - Running services cannot be stopped
    - How to avoid the failure propagation?
  - For third-party services virtualization cannot be applied
    - There is no access to the environment
Challenges to Runtime FMEA4SOA (2)

- **SOA complexity**
  - FMEA at runtime for all components can be expensive
    - In terms of time, resources and cost
  - Establish criteria to select services to be analyzed

- **Occurrence, severity and detectability**
  - A set of scales may not fit every scenario
  - Diff. teams/orgs rank differently the same conditions
  - *How to select the adequate values during runtime?*

- **Quickly outdated FMEA analysis**
  - Adapt to new requirements at runtime, and provide up-to-date information timely
Challenges to Runtime FMEA4SOA (3)

- Define RPN adapted for SOA
  - Traditional RPN is ambiguous
  - New metrics should be created
    - Taking into account the SOA characteristics

- Dynamic Services Composition
  - SOA evolves with dynamic discovery/use of new services
    - Frequently without knowledge of their quality and risks
  - We can define and use Risk Graphs to
    - Demonstrate the effects of the failures
    - When SOA changes, determine the parts to be re-V&Ved
    - Provide a common format for information sharing by partners
      - In a collaborative world 😊
Questions

On Applying FMEA to SOAs

A Proposal and Open Challenges

Thank you for your attention!

Cristiana Areias | careias@dei.uc.pt
PhD Student
University of Coimbra, Portugal

Nuno Antunes | João Cunha