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

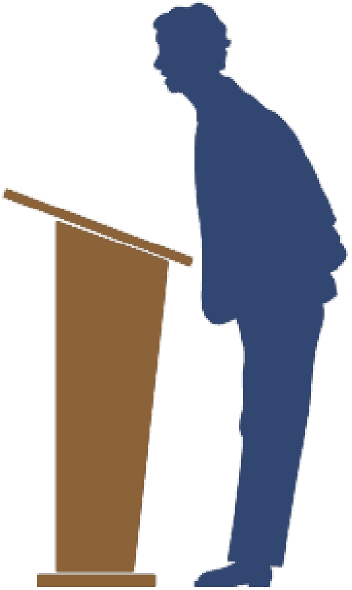
Department of Informatics Engineering
University of Coimbra, Portugal

Instituto Superior de Engenharia de Coimbra, DEIS
Polytechnic Institute of Coimbra, Portugal

SERENE 2014

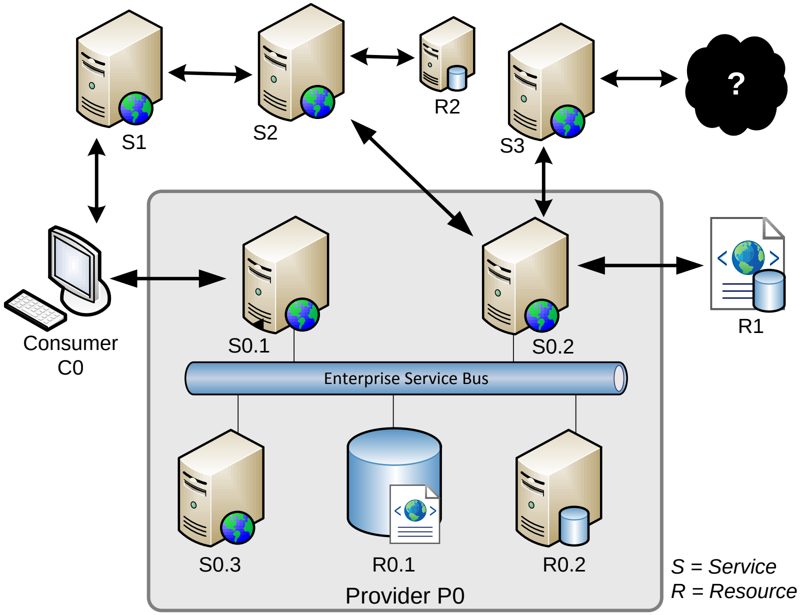
Outline

- 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

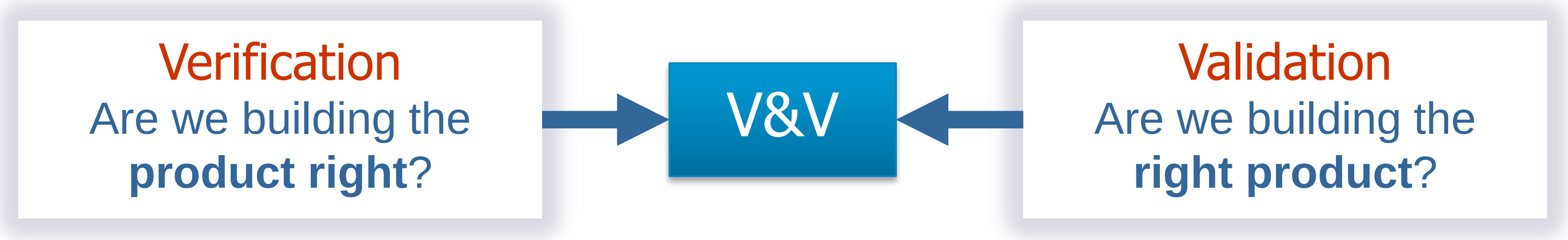


- Dynamic
- Complex

How to guarantee the quality of SOAs?

Verification and Validation

- **V&V** is the process of assessing the quality of software systems throughout their lifecycle



Verification
Are we building the **product right**?

V&V

Validation
Are we building the **right product**?

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

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

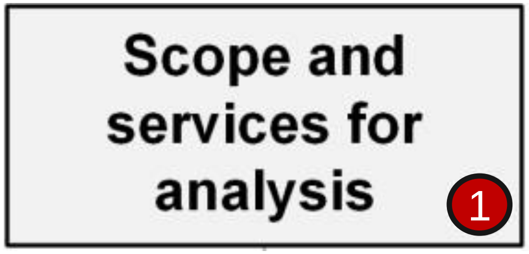
Why apply Software FMEA for SOAs?

- 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**

FMEA4SOA Workflow (1)

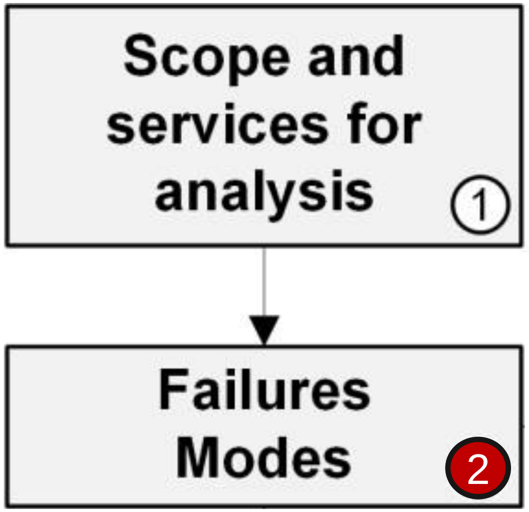


Scope and services for analysis

1

- Scope and boundaries definition
  - Provider
  - Service
  - Operations
  - Type of control
    - Under Control
    - Partially Under Control
    - Within-Reach

FMEA4SOA Workflow (2)

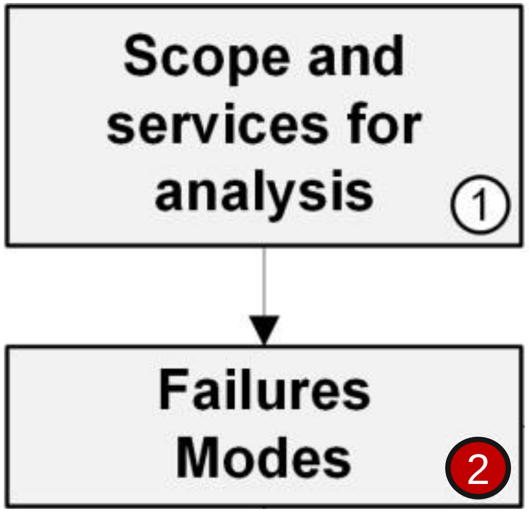


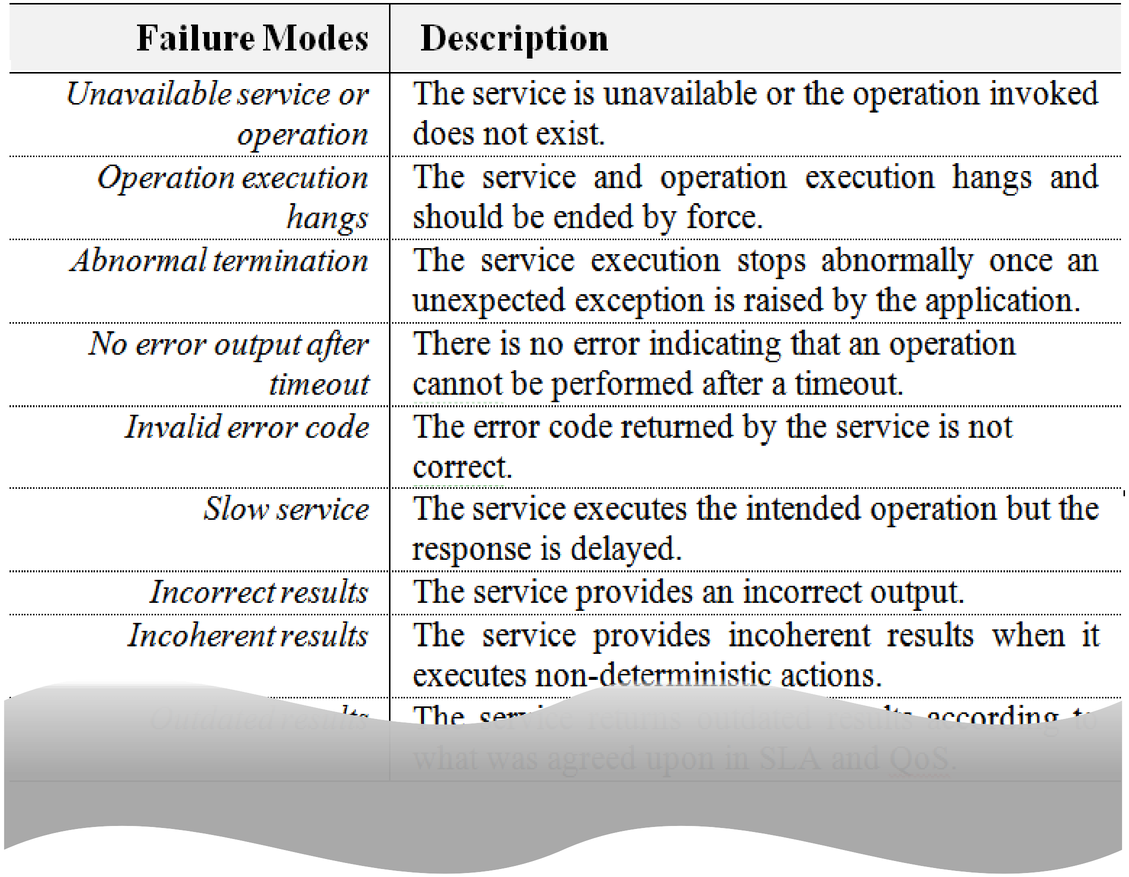
Scope and services for analysis 1

Failures Modes 2

What could go wrong?

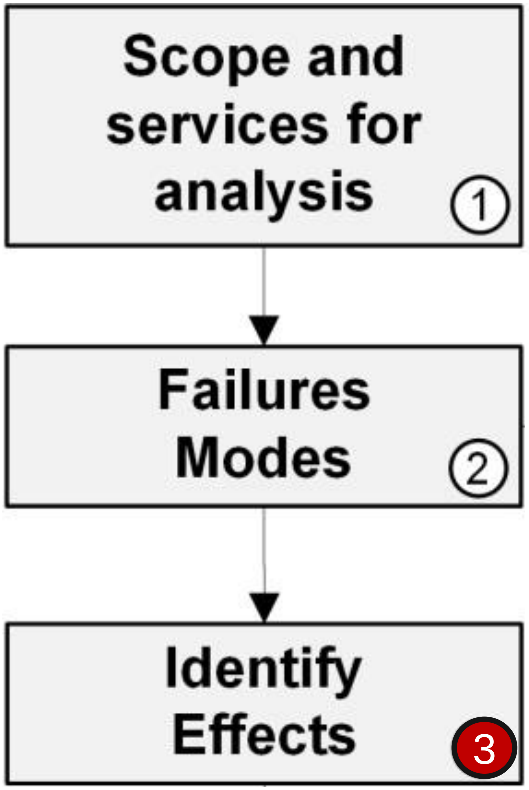
FMEA4SOA Workflow (2)





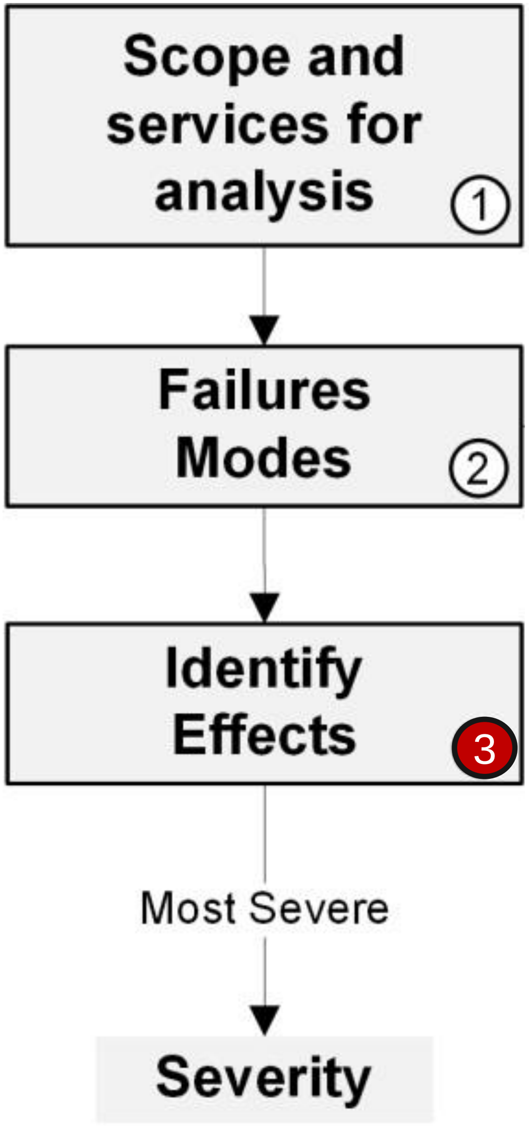
Failure Modes	Description
Unavailable service or operation	The service is unavailable or the operation invoked does not exist.
Operation execution hangs	The service and operation execution hangs and should be ended by force.
Abnormal termination	The service execution stops abnormally once an unexpected exception is raised by the application.
No error output after timeout	There is no error indicating that an operation cannot be performed after a timeout.
Invalid error code	The error code returned by the service is not correct.
Slow service	The service executes the intended operation but the response is delayed.
Incorrect results	The service provides an incorrect output.
Incoherent results	The service provides incoherent results when it executes non-deterministic actions.
Outdated results	The service returns outdated results according to what was agreed upon in SLA and QoS.

FMEA4SOA Workflow (3)

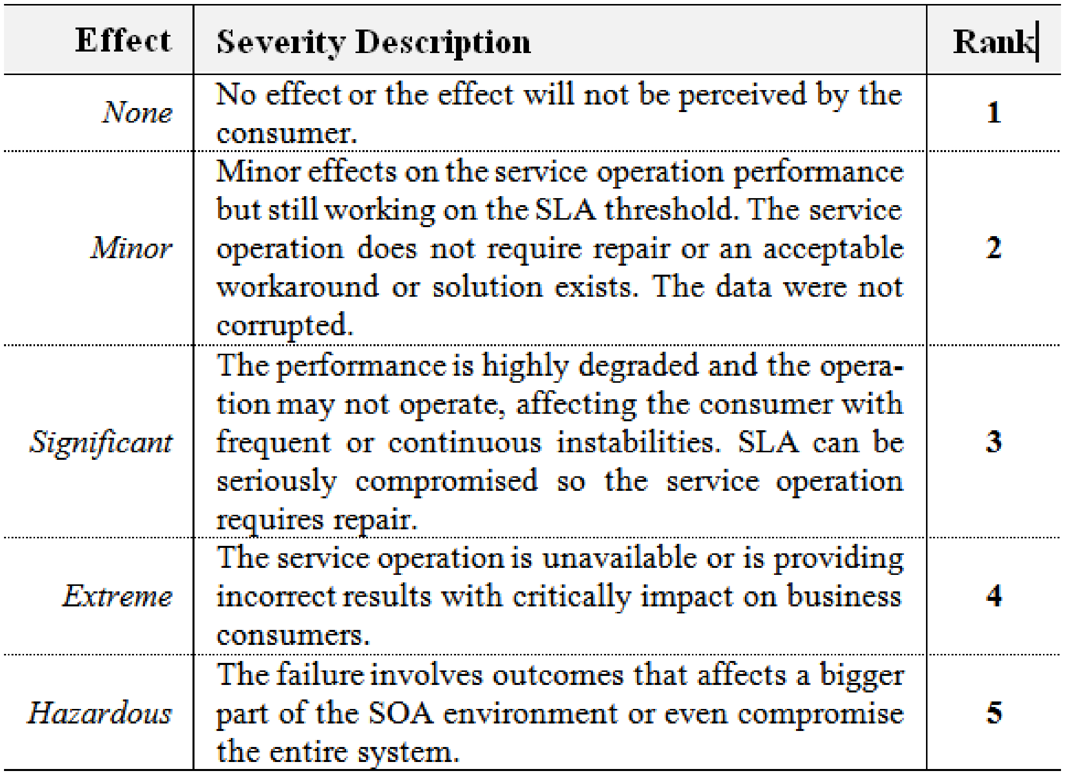


What are the effects of such failure?
Its impact?

FMEA4SOA Workflow (3)



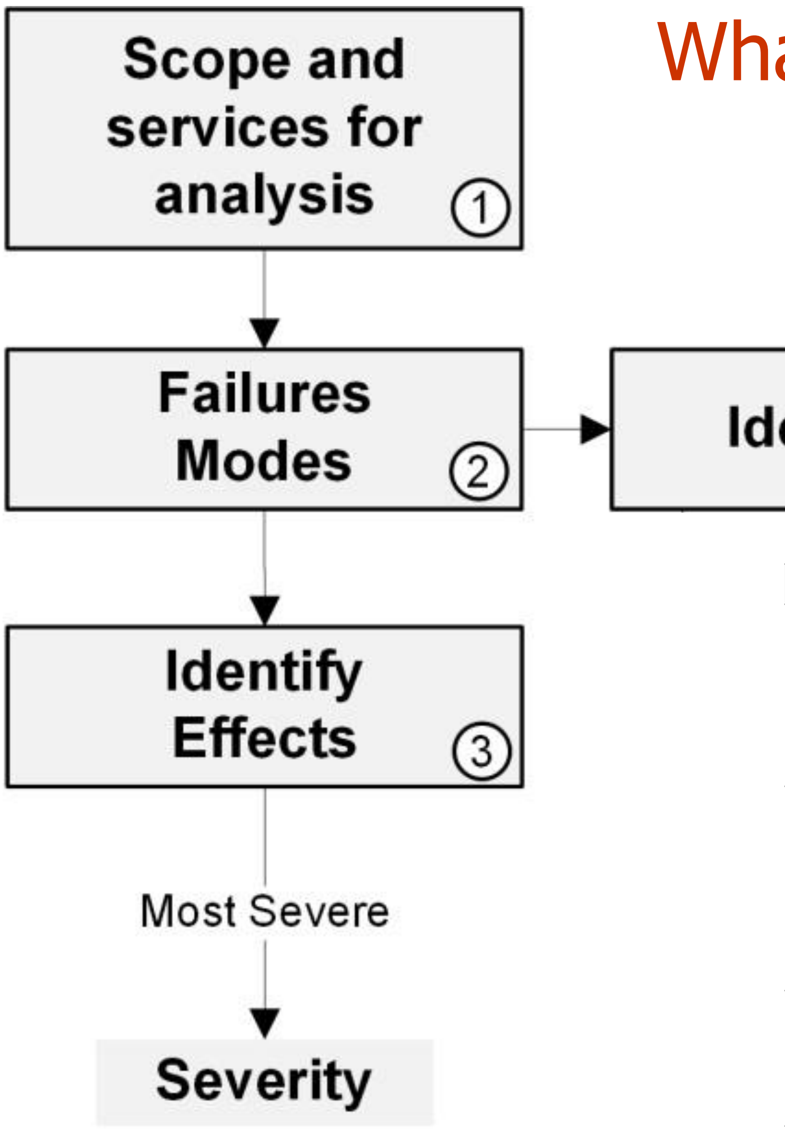
Assess the **severity** of effects according to the impact as perceived by the user



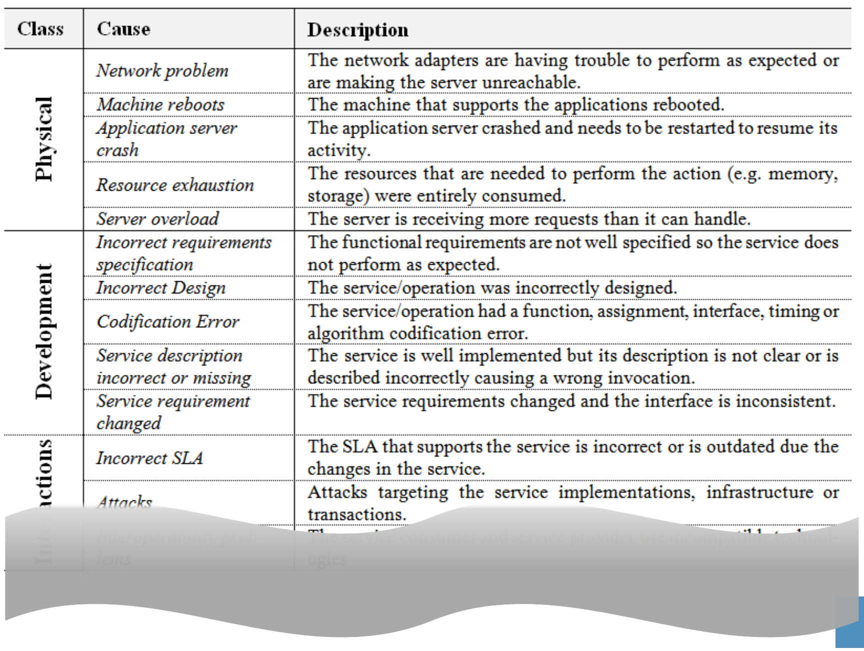
Effect	Severity Description	Rank
None	No effect or the effect will not be perceived by the consumer.	**1**
Minor	Minor effects on the service operation performance but still working on the SLA threshold. The service operation does not require repair or an acceptable workaround or solution exists. The data were not corrupted.	**2**
Significant	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.	**3**
Extreme	The service operation is unavailable or is providing incorrect results with critically impact on business consumers.	**4**
Hazardous	The failure involves outcomes that affects a bigger part of the SOA environment or even compromise the entire system.	**5**

FMEA4SOA Workflow (4)

What are the possible causes of the failure?

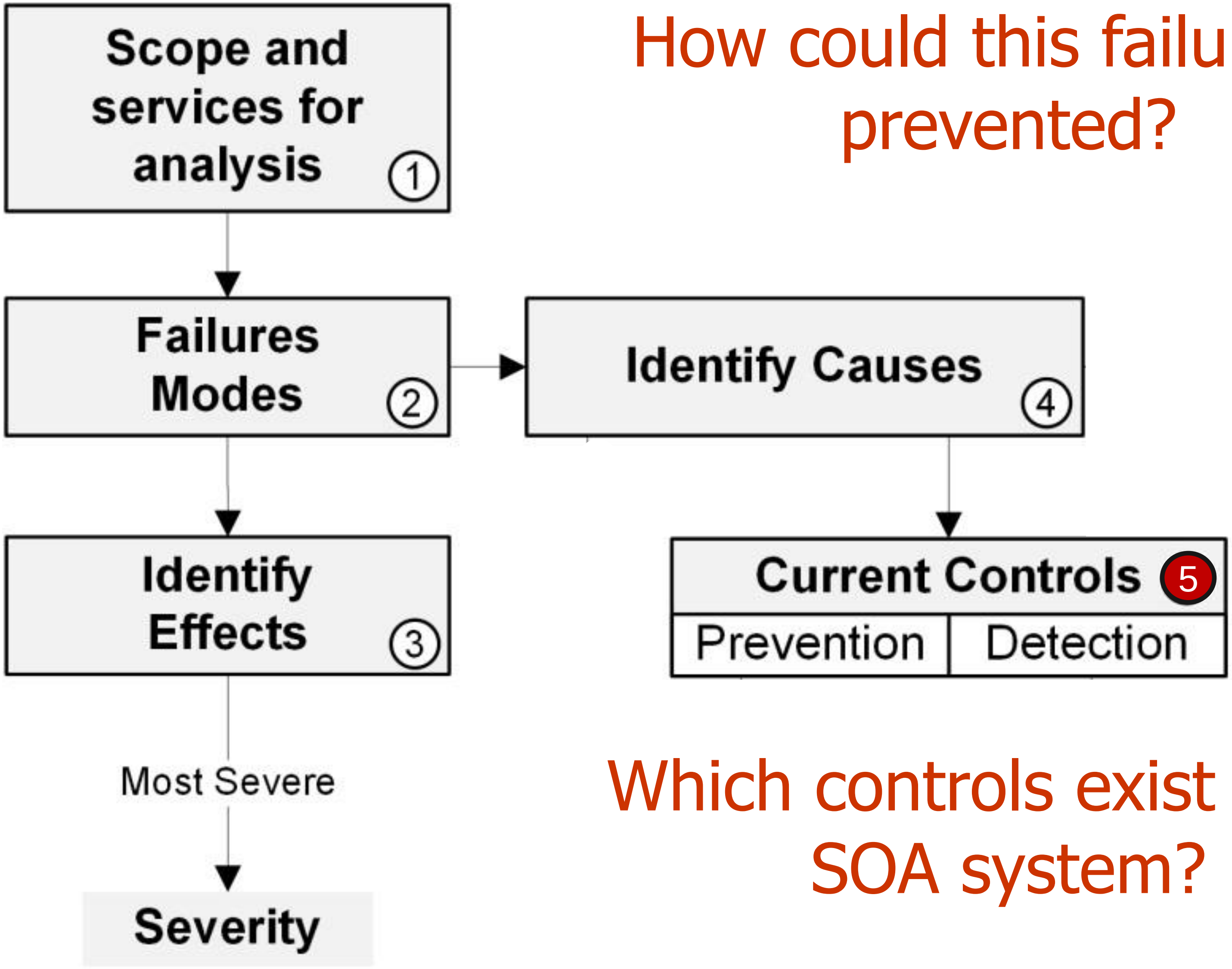


Identify Causes 4



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

FMEA4SOA Workflow (5)



Scope and services for analysis ①

Failures Modes ②

Identify Effects ③

Most Severe

Severity

Identify Causes ④

Current Controls 5

Prevention

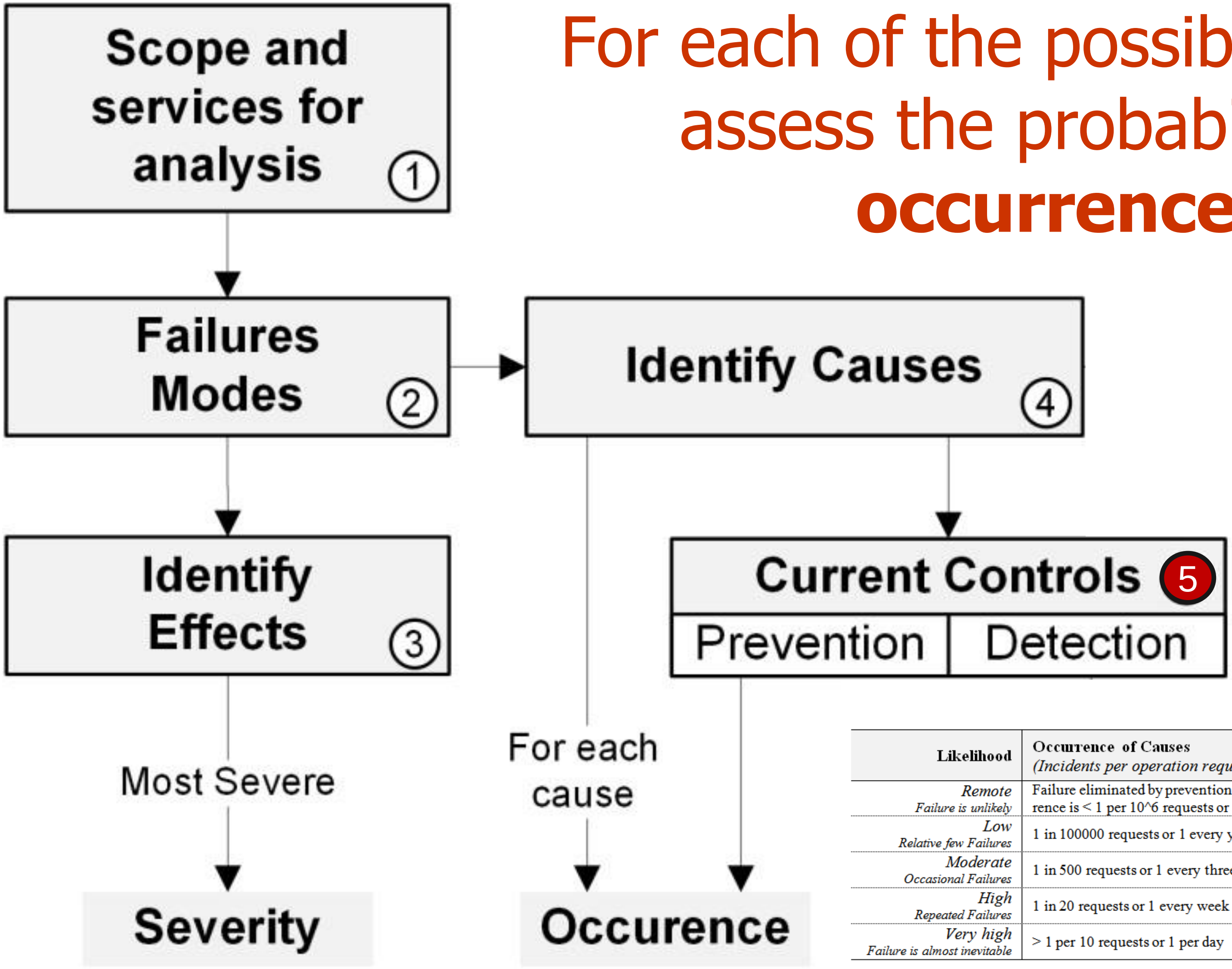
Detection

How could this failure be prevented?

Which controls exist in the SOA system?

FMEA4SOA Workflow (5)

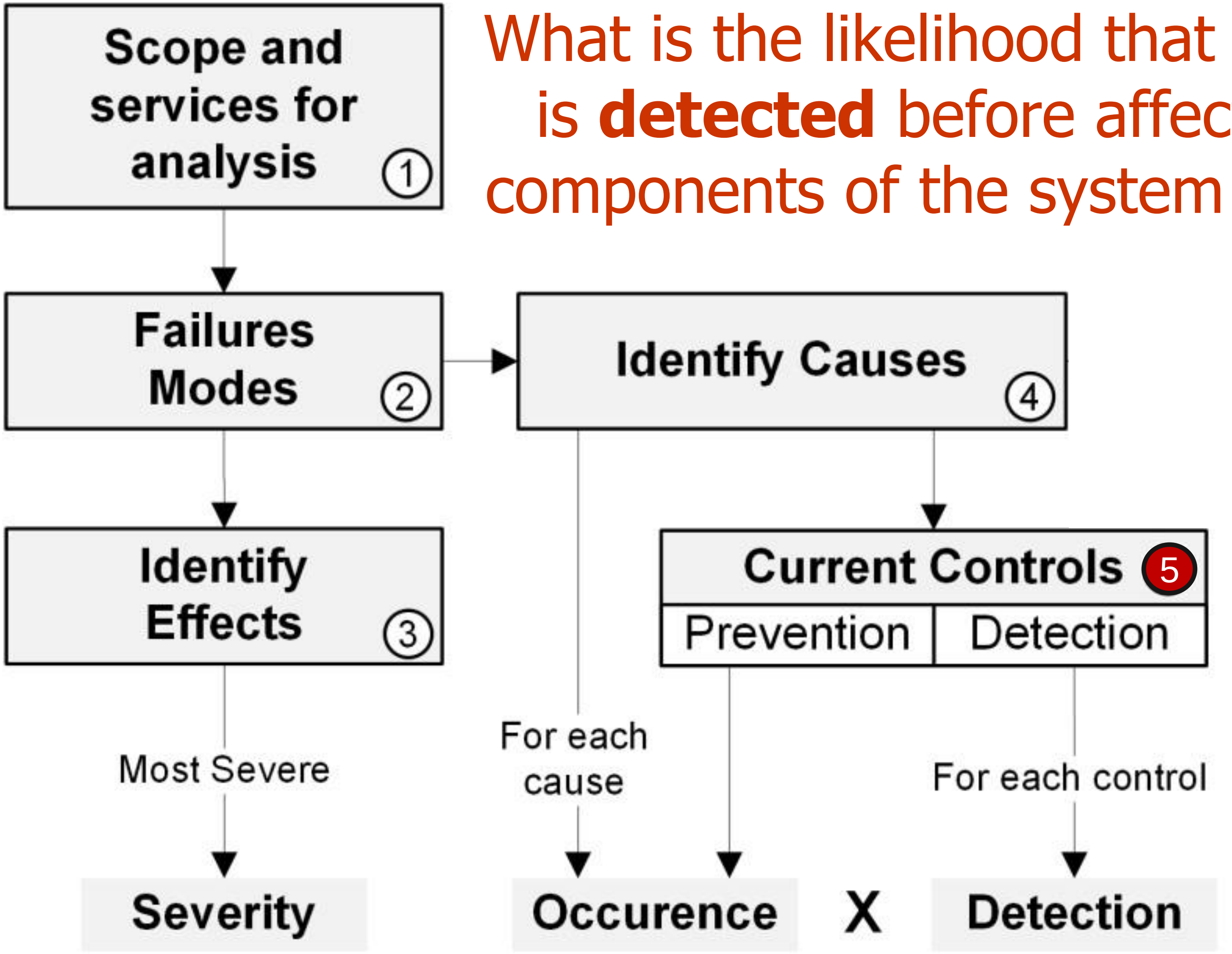
For each of the possible causes, assess the probability of **occurrence**



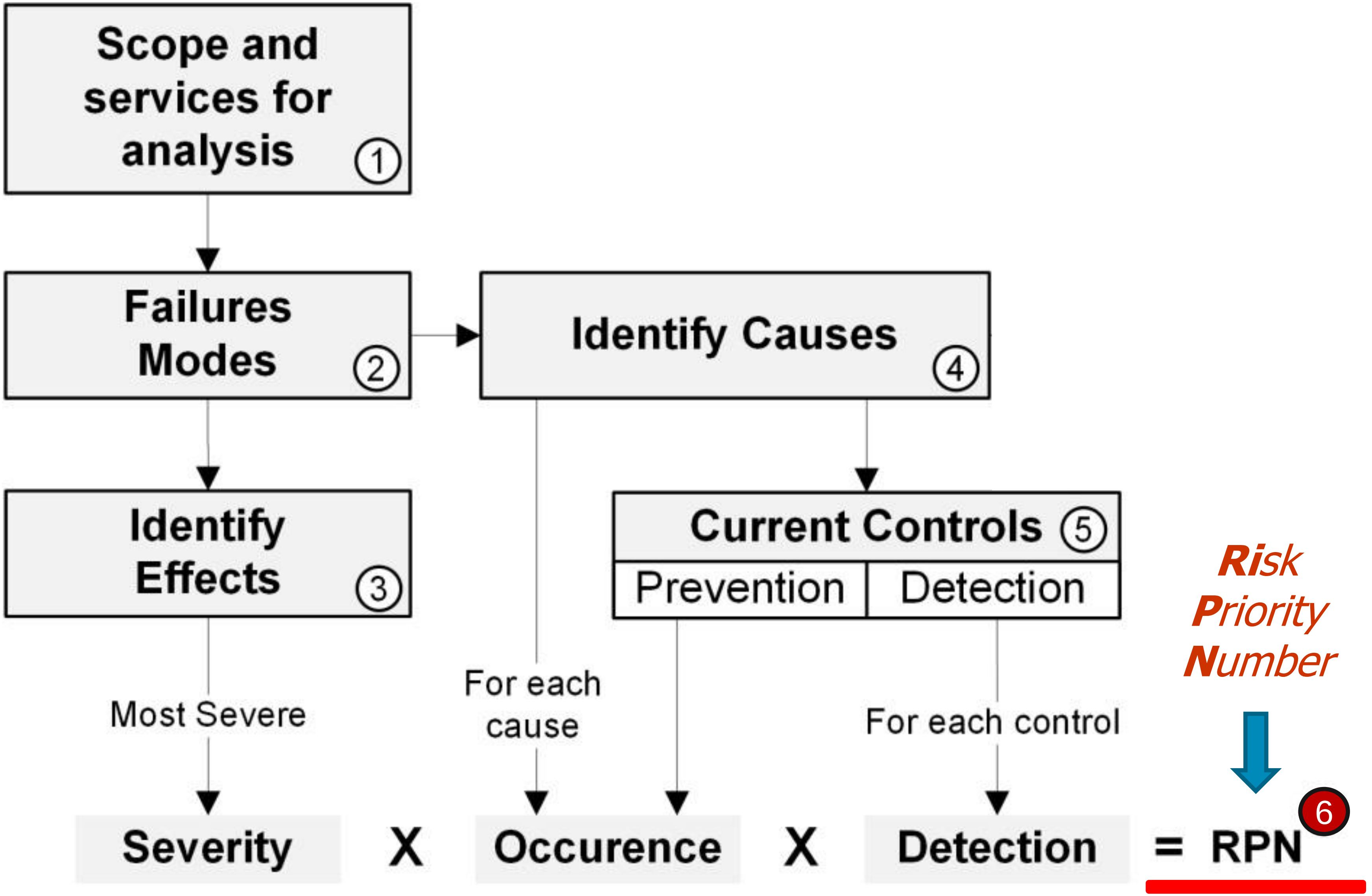
Likelihood	Occurrence of Causes *(Incidents per operation requests or Incidents on lifetime)*	Rank
Remote *Failure is unlikely*	Failure eliminated by prevention control or the probability of occurrence is < 1 per 10^6 requests or 1 occurrence in more than 3 years	1
Low *Relative few Failures*	1 in 100000 requests or 1 every year.	2
Moderate *Occasional Failures*	1 in 500 requests or 1 every three months	3
High *Repeated Failures*	1 in 20 requests or 1 every week	4
Very high *Failure is almost inevitable*	> 1 per 10 requests or 1 per day	5

FMEA4SOA Workflow (5)

What is the likelihood that such failure is **detected** before affecting other components of the system or its user?

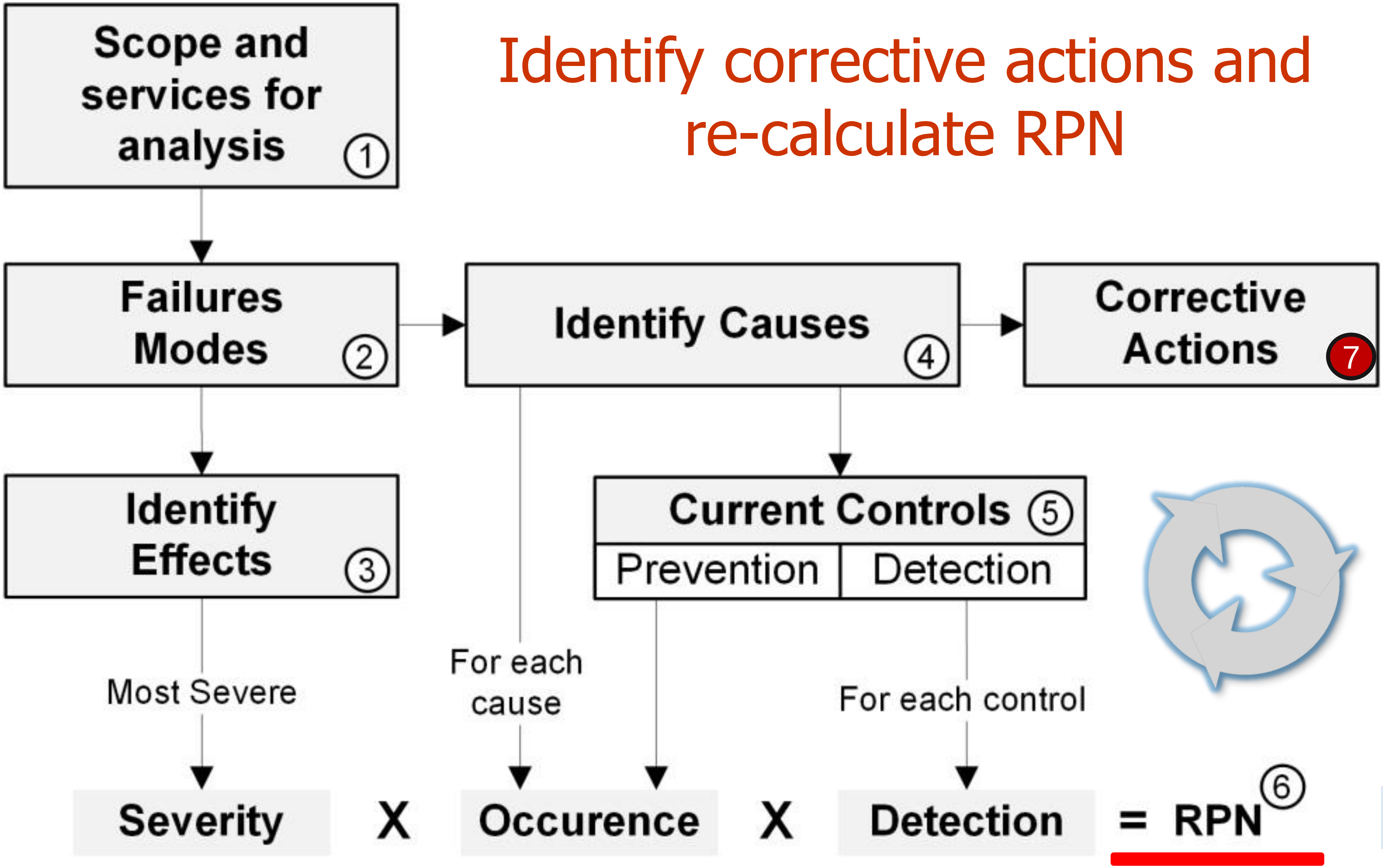


FMEA4SOA Workflow (6)



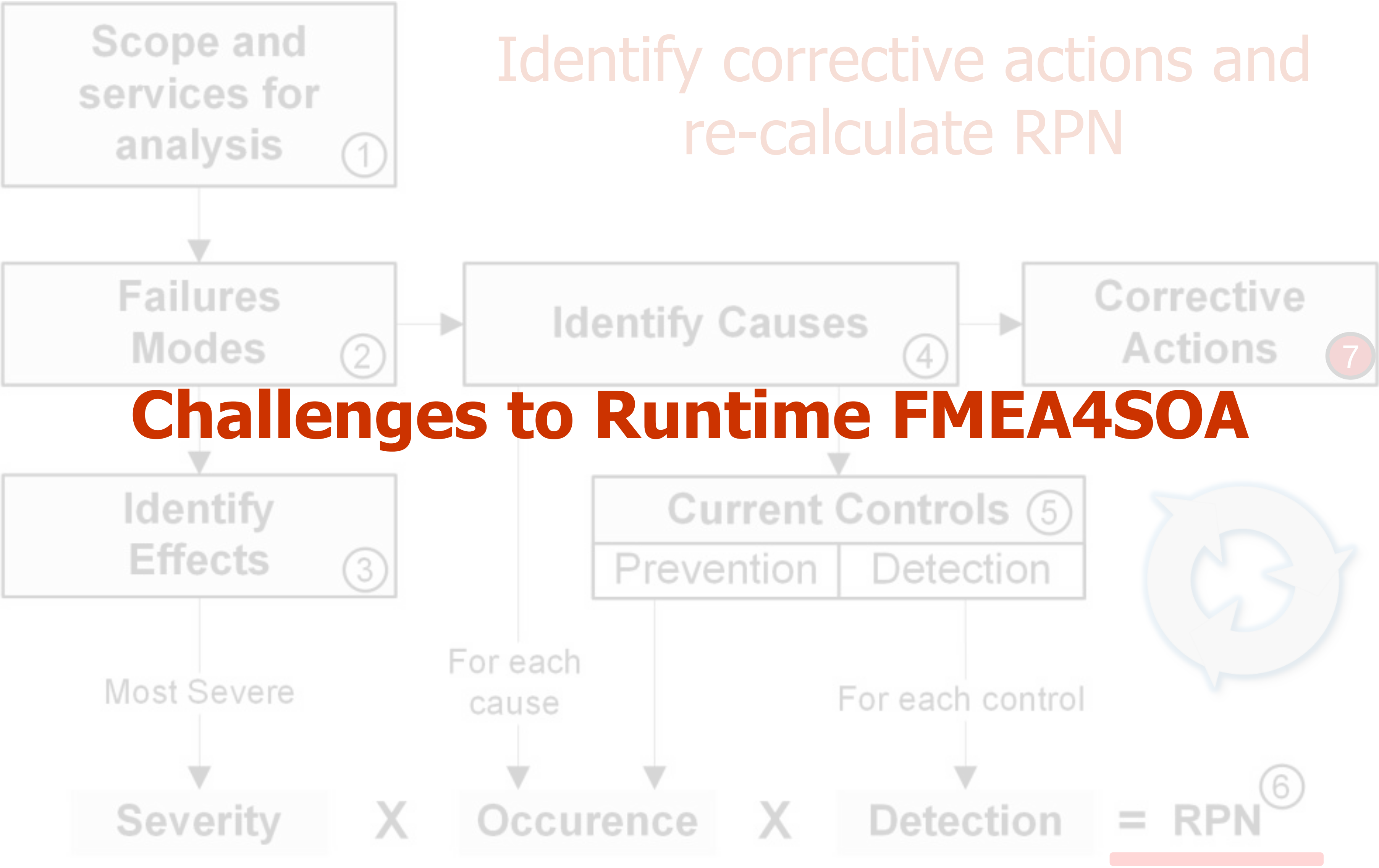
FMEA4SOA Workflow (7)

Identify corrective actions and re-calculate RPN



FMEA4SOA Workflow (7)

Challenges to Runtime FMEA4SOA



Identify corrective actions and re-calculate RPN

Scope and services for analysis (1)

Failures Modes (2)

Identify Causes (4)

Corrective Actions (7)

Identify Effects (3)

Current Controls (5)

Prevention | Detection

Most Severe

For each cause

For each control

Severity X Occurence X Detection = RPN (6)

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