Document sequences of interactions in which the system satisfies some goals or fails to satisfy them.
Goal-Scenario coupling

... initiate and influence the definition of ...

... classify ...

... illustrate satisfaction ...

... lead to the identification of new ...

... lead to revision of ...
Scenarios

• Scenario Types
• Scenario presentation – Use Case
• Use Case Template
• Misuse case
• Rules for Documenting Scenarios
Scenarios

• **Scenario Types**
  • Scenario presentation – Use Case
  • Use Case Template
  • Misuse case
  • Rules for Documenting Scenarios
Scenarios as Means to Put Requirements in Context

Requirements exit in a specific context

- **Actors**
  - Persons or systems interacting with the system

- **Roles**
  - Specific class of actors

- **Goals**
  - Scenarios illustrate satisfaction of goals

- **Preconditions**
  - Conditions that must hold before executing the scenario in order to be able to execute the scenario

- **Postconditions**
  - Conditions that must hold either within the system or in the system context, after executing the scenario

- **Resources**
  - Special conditions that must hold so that a scenario can be executed

- **Location**
  - Place where the scenario is executed
Scenario Types

• Current state and desired state
• Positive and negative
• Misuse scenarios
• Descriptive, exploratory and explanatory
• Instance, type and mixed scenarios
• System-internal, interaction, and context scenarios
• Main, alternative, and exception scenario
Scenario Types

- Current state and desired state
  - Indicative scenarios
    - Used to document the current system usage.
  - Optative scenarios
    - Describe desired system usage, not yet implemented

- Positive and negative
- Misuse scenarios
- Descriptive, exploratory and explanatory
- Instance, type and mixed scenarios
- System-internal, interaction, and context scenarios
- Main, alternative, and exception scenario
Scenario Types

• Current state and desired state

• **Positive and negative**
  – Desired sequence of interactions leading to the satisfaction of a set of goals associated with the scenario
  – A sequence of interactions that fail to satisfy a goal or set of goals associated with the scenario
    • Can be **allowed** or **forbidden**

• Misuse scenarios

• Descriptive, exploratory and explanatory

• Instance, type and mixed scenarios

• System-internal, interaction, and context scenarios

• Main, alternative, and exception scenario
Scenario Types

- Current state and desired state
- Positive and negative
- **Misuse scenarios**
  - A sequence of interactions in which a hostile actor uses the system against the stakeholder intention
- Descriptive, exploratory and explanatory
- Instance, type and mixed scenarios
- System-internal, interaction, and context scenarios
- Main, alternative, and exception scenario
Scenario Types

- Current state and desired state
- Positive and negative
- Misuse scenarios

- Descriptive, exploratory and explanatory
  - Understanding the process operations, involved agents, triggering events, and other
    - Illustrate meaning of goals and requirements
  - Explore and evaluate possible, alternative solutions in order to support the selection of one alternative solution
    - Support decision making
  - Aims explaining a goal, an alternative solution or a sequence of interactions
    - Explain complex facts
Scenario Types

- Current state and desired state
- Positive and negative
- Misuse scenarios
- Descriptive, exploratory and explanatory
- **Instance, type and mixed scenarios**
  - Concrete sequence of interactions between concrete actors
  - Abstracts from the concrete actors, inputs, and outputs
- System-internal, interaction, and context scenarios
- Main, alternative, and exception scenario
Scenario Types

- Current state and desired state
- Positive and negative
- Misuse scenarios
- Descriptive, exploratory and explanatory
- Instance, type and mixed scenarios

- **System-internal, interaction, and context scenarios**
  - Only system-internal interactions; among different system parts
  - Interactions between the system and its actors
  - Interactions between the system and its actors as well as additional context that is relevant for the system usage or the system itself

- Main, alternative, and exception scenario
Scenario Types

- Current state and desired state
- Positive and negative
- Misuse scenarios
- Descriptive, exploratory and explanatory
- Instance, type and mixed scenarios
- System-internal, interaction, and context scenarios
  - Only system-internal interactions
  - Interactions between the system and its actors
  - Interactions between the system and its actors as well as additional context that is relevant for the system usage or the system itself
- Main, alternative, and exception scenarios
Scenario Types

- Current state and desired state
- Positive and negative
- Misuse scenarios
- Descriptive, exploratory and explanatory
- Instance, type and mixed scenarios
- System-internal, interaction, and context scenarios

- **Main, alternative, and exception scenario**
  - Normally executed
    - Satisfy a specific set of goals
  - Can be executed instead of the main scenario
    - Result in the satisfaction of the goals that are associated with the main scenario
  - Executed when an exceptional event occurs
    - Some goals of the main scenario cannot be satisfied
Scenarios

- Scenario Types
- **Scenario presentation** – Use Case
- Use Case Template
- Misuse case
- Rules for Documenting Scenarios
Narrative scenario

A driver assistance system includes a (sub-) system for avoiding rear-end collisions. This system comprises distance sensors, that permanently check the distance to the vehicle driving ahead in order to avoid an imminent rear-end collision. If the system detects that the distance falls below the safety distance yet is still outside the critical range, an acoustic warning signal sounds. Alternatively, a symbol or message maybe displayed on the driver display in the cockpit of the car. In the driver has not react to the warning after $2\text{ s}$ and the distance between two cars still decreases, the system reduces the speed of the car.

If the distance (in meters) falls below one quarter of the driving speed (in km/h) at any time, the system initiates emergency breaking.

• Sequence of interactions using natural language
A driver assistance system includes a (sub-) system for avoiding rear-end collisions. This system comprises (1) **distance sensors**, that (2) permanently check the distance to the vehicle driving ahead (3) in order to avoid an imminent rear-end collision. (4) If the system detects that the distance falls below the safety distance yet is still outside the critical range, an acoustic warning signal sounds. (5) Alternatively, a symbol or message maybe displayed on the driver display in the cockpit of the car. In the driver has not react to the warning after 2 s and the distance between two cars still decreases, (6) the system reduces the speed of the car. (7) If the distance (in meters) falls below one quarter of the driving speed (in km/h) at any time, the system initiates emergency breaking.
A driver assistance system includes a (sub-) system for avoiding rear-end collisions. This system comprises (1) **distance sensors**, that (2) permanently check the distance to the vehicle driving ahead (3) in order to avoid an imminent rear-end collision. (4) If the system detects that the distance falls below the safety distance yet is still outside the critical range, an acoustic warning signal sounds. (5) Alternatively, a symbol or message maybe displayed on the driver display in the cockpit of the car. In the driver has not react to the warning after 2 s and the distance between two cars still decreases, (6) the system reduces the speed of the car. (7) If the distance (in meters) falls below one quarter of the driving speed (in km/h) at any time, the system initiates emergency breaking.
Structured Scenario

• Enumeration of Scenario steps:

1. The driver activates the navigation system
2. The navigation system determines the current position of the car
3. The navigation system asks for the desired destination
4. The driver enters the destination
5. The navigation system identifies the relevant part of the map
6. The navigation system displays the map of the destination area
7. The navigation system asks for the routing options
8. The driver selects the desired routing option
9. The navigation system calculates the route
10....
Structured Scenario

- Tabular documentation of interaction sequence

<table>
<thead>
<tr>
<th>Driver</th>
<th>Navigation system</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The driver activates the navigation system</td>
<td>2. The navigation system determines the current position of the car</td>
</tr>
<tr>
<td>4. The driver enters the destination</td>
<td>3. The navigation system asks for the desired destination</td>
</tr>
<tr>
<td>5. The navigation system identifies the relevant part of the map</td>
<td>6. The navigation system displays the map of the destination area</td>
</tr>
<tr>
<td>7. The navigation system asks for the routing options</td>
<td>8. The driver selects the desired routing option</td>
</tr>
<tr>
<td>9. The navigation system calculates the route</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
Scenarios

• Scenario Types
  • Scenario presentation – **Use Case**
• Use Case Template
• Misuse case
• Rules for Documenting Scenarios

Contains:
• **Context information**
• **Main scenario**
• **Alternative scenario**
• **Exceptional scenario**
Moving towards specification

• **What functions will the new system provide?**
  – How will people interact with it?
  – Describe functions from a user’s perspective

• **Use Cases**
  – Used to show:
    • the **functions** to be provided by the system
    • which **actors** will use which functions
  – Each Use Case is:
    • a pattern of behavior that the new system is required to exhibit
    • a sequence of related actions performed by an actor and the system via a dialogue

• **An actor:**
  – anything that needs to interact with the system:
    • a person
    • a role that different people may play
    • another (external) system
Use case diagram

- Capture the relationships between actors and Use Cases

- Campaign manager
  - Add a new client

- Staff contact
  - Change a client contact

- Accountant
  - Record client payment
Notation for Use Cases

Staff contact

Actor

Communication association

System boundary

Use case

Change client contact
Example

Financial Module

- Add new staff member
- Add new staff grade
- Change rate for the client
- Change grade for the staff member
- Calculate staff bonuses

Accountant
<<extends>> and <<includes>>

- **<<extends>>**: one use case adds behaviour to a base case
  - used to model a part of a use case that the user may see as optional system behavior
  - also models a separate sub-case which is executed conditionally

- **<<includes>>**: one use case invokes another (like a procedure call)
  - used to avoid describing the same flow of events several times
  - puts the common behavior in a use case of its own
Another example

Car System

Driver

Gas Attendant

Mechanic

Fill Up

Check Oil

Turn On Engine

Fix Car

Fix Car on the Road

«include»

«include»

«include»

«extend»

«include»
Identifying Actors

• **Ask the following questions:**
  – Who will be a **primary user** of the system? (primary actor)
  – Who will **need support** from the system to do her daily tasks?
  – Who will **maintain, administrate, keep the system working**? (secondary actor)
  – Which **hardware devices** does the system need?
  – With which **other systems** does the system need to interact with?
  – Who or what **has an interest** in the results that the system produces?

• **Look for:**
  – the users who directly use the system
  – also others who need services from the system
Finding Use Cases

• For each actor, ask the following questions:
  – Which **functions** does the actor require from the system?
  – What does the **actor need to do**?
  – Does the actor need to **read, create, destroy, modify, or store** some kinds of information in the system?
  – Does the actor **have to be notified** about events in the system?
  – Does the **actor need to notify** the system about something?
  – What do those events require in terms of system functionality?
  – Could the actor’s daily work be simplified or made more efficient through new functions provided by the system?
Scenarios

- Scenario Types
- Scenario presentation – Use Case
  - **Use Case Template**
  - Misuse case
- Rules for Documenting Scenarios
Documenting Use Cases

• For each use case:
  – prepare a “flow of events”
  – document from an actor’s point of view
  – describe what the system must provide to the actor when the use case is executed

• Typical contents
  – How the use case starts and ends
  – Normal flow of events
  – Alternate flow of events
  – Exceptional flow of events

• Documentation style
  – Textual use case description
  – Sequence diagrams
# Use case template

*(Wiegers, 2004)*

<table>
<thead>
<tr>
<th>Use Case ID:</th>
<th>Last Updated By:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Case Name:</td>
<td>Date Last Updated:</td>
</tr>
<tr>
<td>Created By:</td>
<td>Date Created:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actors:</th>
<th>Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Preconditions:</th>
<th>Postconditions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Flow:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alternative Flows:</th>
<th>Exceptions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Includes:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Priority:</th>
<th>Frequency of Use:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Rules:</td>
<td>Special Requirements:</td>
</tr>
<tr>
<td>Assumptions:</td>
<td></td>
</tr>
</tbody>
</table>

Notes and Issues:
Use case templates (2)
(Wiegers, 2004)

<table>
<thead>
<tr>
<th>Use Case ID:</th>
<th>Last Updated By:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Case Name:</td>
<td></td>
</tr>
<tr>
<td>Created By:</td>
<td></td>
</tr>
<tr>
<td>Date Created:</td>
<td>Date Last Updated:</td>
</tr>
</tbody>
</table>

- **Use Case ID**: a unique integer sequence number identifier
- **Use Case Name**: a concise, results-oriented name for the use case
- **Created By**: the name of the person who initially documented this use case
- **Date Created**: the date on which the use case was initially documented
- **Last Updated By**: the name of the person who performed the most recent update to the use case description
- **Date Last Updated**: the date on which the use case was most recently updated
Use case templates (3)

(Wiegers, 2004)

<table>
<thead>
<tr>
<th>Use Case ID:</th>
<th>Last Updated By:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Case Name:</td>
<td>Date Last Updated:</td>
</tr>
<tr>
<td>Created By:</td>
<td></td>
</tr>
<tr>
<td>Date Created:</td>
<td></td>
</tr>
</tbody>
</table>

- **A**ctors: a person or other entity external to the software system being specified who interacts with the system and performs use cases to accomplish tasks
- **Description**: the reason for and outcome of this use case, the sequence of actions and the outcome of executing the use case
- **Trigger**: the event that initiates the use case
- **Pre-condition**: list any activities that must take place, or any conditions that must be true, before the use case can be started
- **Post-condition**: the state of the system at the conclusion of the use case execution
Use case templates (4)

(Wiegers, 2004)

<table>
<thead>
<tr>
<th>Use Case ID:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Case Name:</td>
<td></td>
</tr>
<tr>
<td>Created By:</td>
<td>Last Updated By:</td>
</tr>
<tr>
<td>Date Created:</td>
<td>Date Last Updated:</td>
</tr>
</tbody>
</table>

- **Normal flow**: a detailed description of the user actions and system responses that will take place during execution of the use case under normal, expected conditions
- **Alternative flows**: other, legitimate usage scenarios that can take place
- **Exceptions**: any anticipated error conditions that could occur during execution of the use case
- **Includes**: any other use cases that are included (“called”) by this use case
- **Priority**: the relative priority of implementing the functionality required to allow this use case
Use case templates (5)
(Wiegers, 2004)

| Use Case ID: |
| Created By: | Last Updated By: |
| Date Created: | Date Last Updated: |

- **Frequency of use**: the number of times this use case will be performed by the actors per some appropriate unit of time
- **Business rules**: any business rules that influence this use case
- **Special Requirements**: any additional requirements (e.g., quality) for the use case that may need to be addressed during design or implementation
- **Assumptions**: any assumptions that were made in the analysis that led to accepting this use case
- **Notes and Issues**: any additional comments
Scenarios

• Scenario Types
• Scenario presentation – Use Case
• Use Case Template
• **Misuse case**
• Rules for Documenting Scenarios
Misuse cases

• **A modeling technique** – use cases
  – Normal actors and wanted functionality +
  – Mis-users, harmful acts

• **Makes it possible to discuss**
  – Security requirements together with functional requirements.
  – With a technique that is
    • In normal use
    • Relatively easy to understand for end-users

• **As with use-cases, there are two possibilities:**
  – Diagrams
  – Textual descriptions
Misuse cases

• **A modeling technique – use cases**
  – Normal actors and wanted functionality +
  – Mis-users, harmful acts

• **Makes it possible to discuss**
  – Security requirements together with functional requirements.

• **Diagrams**
  – Textual descriptions
Security risk management process
1. Context and Assets Identification
2. Security Objectives Determination

- Description of organisation and its environment
  - sensitive activities related to information security
3. Risk Analysis

Diagram showing the process of risk analysis and assessment, including context and asset identification, determination of security objectives, risk analysis and assessment, risk treatment, security requirements definition, and control selection and implementation.
3. Risk Analysis
3. Risk Analysis

- **Basic path:**
  - actions that the misuser(s) and the system go through to harm the proposed system

- **Mitigation points:**
  - actions in a basic or alternative path where misuse can be mitigated

- **Trigger:**
  - states or events in the system or its environment that may initiate the misuse case

- **Assumption**
  - states in the system’s environment that make the misuse case possible

- **Precondition**
  - system states that make the misuse case possible

- **Mitigation point**
  - guaranteed outcome of mitigating a misuse case

- **Stakeholder and risks:**
  - major risks for each stakeholder involved in the misuse case
## 3. Risk Analysis

<table>
<thead>
<tr>
<th>Name</th>
<th>Intercept transfer of game report</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>A violator establishes himself as man in the middle and captures the game report. He reads and keeps game report for later use.</td>
</tr>
<tr>
<td><strong>Basic path</strong></td>
<td><strong>bp1</strong>: Violator establishes himself as man-in-the-middle; <strong>bp2</strong>: Umpire submits game report to ERIS; <strong>bp3</strong>: Game report is transferred; <strong>bp4</strong>: Attacker intercepts transfer of game report; <strong>bp5</strong>: Attacker reads and keeps game report for later use (extension point ext1)</td>
</tr>
<tr>
<td><strong>Mitigation points</strong></td>
<td><strong>mp1</strong>: Use secure communication</td>
</tr>
<tr>
<td><strong>Extension points</strong></td>
<td><strong>ext1</strong>: Includes to misuse case Read and keep game report for later use.</td>
</tr>
<tr>
<td><strong>Trigger</strong></td>
<td>Game report is submitted.</td>
</tr>
<tr>
<td><strong>Assumption</strong></td>
<td><strong>as1</strong>: Transmission can be intercepted.</td>
</tr>
<tr>
<td><strong>Precondition</strong></td>
<td><strong>pr1</strong>: Game report is not hidden (e.g., is not encrypted).</td>
</tr>
<tr>
<td><strong>Worst case threat</strong></td>
<td>Confidentiality of game report is negated; game report is not updated; transfer of game report is not reliable.</td>
</tr>
<tr>
<td><strong>Mitigation guarantee</strong></td>
<td>Use secure communication.</td>
</tr>
<tr>
<td><strong>Related business rules</strong></td>
<td>Game report is required to finalise the results of the game.</td>
</tr>
<tr>
<td><strong>Misuser profile</strong></td>
<td>Skilled. Knowledge of how to perform man-in-the-middle attack, knowledge of how to intercept transferred messages. Motivated by some reward.</td>
</tr>
<tr>
<td><strong>Stakeholder and risks</strong></td>
<td><strong>Umpire</strong>: Change of the confidentiality of the game report. Not able to received the game in time. Respectability of the Football Federation is lost.</td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td>Business environment</td>
</tr>
<tr>
<td><strong>Abstraction level</strong></td>
<td>Confidentiality of game report</td>
</tr>
<tr>
<td><strong>Precision level</strong></td>
<td>Focussed</td>
</tr>
</tbody>
</table>
## 4. Risk Treatment Decisions

<table>
<thead>
<tr>
<th>Risk treatment decisions</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avoiding risk</td>
<td>Decision not to be involved in, or to withdraw from a risk</td>
</tr>
<tr>
<td>Transferring risk</td>
<td>Sharing with another party the burden of loss for a risk</td>
</tr>
<tr>
<td>Retaining risk</td>
<td>Accepting the burden of loss from a risk</td>
</tr>
<tr>
<td>Reducing risk</td>
<td>Action to lessen the probability, negative consequences, or both, associated with a risk</td>
</tr>
</tbody>
</table>
5. Security Requirements Definition

- Context and asset identification
- Determination of security objectives
- Risk analysis and assessment
  - [assessment satisfactory]
  - [assessment unsatisfactory]
- Risk treatment
- Security requirements definition
- Control selection and implementation

Diagram:
- ERIS
  - Intercept transfer of game report
  - Use secure communication
  - Read and keep game report for later use
  - Collect info about accessing game report
  - Obtain umpire’s login name
  - Check game storage access repeatedly
- Umpire
  - Submit game report
  - Transfer game report
  - Update game report
  - Check umpire’s login and password
  - Check umpire’s ID card
- Violator
Scenarios

- Scenario Types
- Scenario presentation – Use Case
- Use Case Template
- Misuse case

**Rules for Documenting Scenarios**
Documenting Scenario

- Identifier
- Name
- Interaction
- Scenario type
- Scenario
- Postcondition
- Precondition
- Source
- Stakeholder
- Document
- System
- Actor

- has scenario step
- is of
- has
- has author
- has
- participates in
Documenting Scenario

1. Each scenario has a unique identifier and a unique name

2. For each scenario, one or multiple scenario steps of the type interaction have to be defined

3. For each scenario, arbitrary number of pre- and post-conditions must be defined

4. Exactly one scenario type is assigned to each scenario

5. Exactly two actors participate in each interaction
Rule 1: Use the present tense when documenting scenario

- The user entered his name and password into the system. The system checked the correctness of the entered data
- The user enters his name and password into the system. The system checks the correctness of the entered data
Rule 2:
Use the active voice when documenting scenario

- The user name and password are entered and validated
- The user enters his user name and password into the system. The system validates the correctness of the entered data
Rule 3:
Use the subject-predicate-object sentence structure

• By the means of the user database, the system validates the user data
• The system validates the user data by the means of the user database
Rule 4:
Avoid modal verb

• The system **should** check the user data
• The system **checks** the user data
Rule 5:
Clearly separate each interaction from other interactions

Rule 6:
Number each scenario step

• The user submits a search query to the online shop, selects an item from the list of search results, and adds the item to the shopping cart.

1. The user submits a query to the online shop.
2. The systems displays a list of search results.
3. The user selects an item from the list.
4. The user adds the item to his shopping cart.
5. The user iterates steps 1-4 until he has finished shopping.
Rule 7: Only one interaction sequence per scenario

10. The user enters his data into the system
11. The user data is incorrect -> continue with step 41.
11. System displays “incorrect user data, please retry”
   …
31. System displays “incorrect user data – transaction cancelled”
32. System returns credit card
41. System displays “user data correct”.
   …

Alternative scenario:
If 10. is unsuccessful:
11a.1. System displays “incorrect user data, please retry”.
11a.2. System asks the user for entering his data.
11a.3. The user enters his user data into the system
Rule 8:
Describe scenario from the perspective of an outsider

1. The system receives the user name and password
2. The system encrypts the user data
3. The system logs on to the user server
4. The system transfers the user data to the user server
5. The user server decrypts the user data
6. The user server checks the user data by means of the user database
7. The user server transmits that the user data is correct
8. The system logs off from the user server
9. The system informs the user that the login was successful

1. The user logs on with his user data
2. The system checks the data
3. The system informs the user about the successful login
Rule 9:
Explicit name of the actor involved

1. The user logs on to the system
2. The system reports that there is no connection to the network
3. The system restarts
4. The connection to the network is re-established
5. The user logs on to the system

1. The user logs on to the system
2. The system reports that there is no connection to the network
3. The user reboots the system
4. The system establishes the connection to the network
5. The user logs on to the system
Rule 10:
Explicitly state the goal of the scenario

1. An unauthorised user boots the system
2. The system displays status reports about the boot procedure
3. The system displays a successful boot on the screen
4. The system asks the user to enter his user name and password
5. The unauthorised user enters different, random chosen user names an passwords
6. After 5 unsuccessful login attempts, the system logs the login functionality for 30 min.

Goal: Protecting the system against the unauthorised access

The unauthorised user tries to log on to the system with a randomly chosen user name and password
After five unsuccessful login attempts, the system locks the login functionality for 30 min.
Rule 11:
Focus on illustrating how the goal is satisfied by the scenario
Message to Take Home

- Scenario Types
- Use Case
- Use Case Template
- Misuse case
- Rules for Documenting Scenarios
Goal-Scenario coupling

... initiate and influence the definition of ...

... classify ...

... illustrate satisfaction...

... lead to the identification of new ...

... lead to revision of ...