Softwaretechnik / Software-Engineering

Lecture 8: Scenarios & Use Cases

Prof. Dr. Andreas Podelski, Dr. Bernd Westphal
Albert-Ludwigs-Universität Freiburg, Germany

Topic Area Requirements Engineering: Content

- Introduction
- Definition: Software & SW Specification
- Requirements Specification
  - Desired Properties
  - Kinds of Requirements
  - Analysis Techniques
- Documents
  - Dictionary, Specification
- Specification Languages
  - Natural Language
  - Decision Tables
    - Syntax, Semantics
    - Completeness, Consistency, ...
- Scenarios
  - User Stories, Use Cases
  - Live Sequence Charts
    - Syntax, Semantics
- Wrap-Up
Scenarios

• Scenarios: The Idea

• Use Cases
  • Use Case Diagrams

• User Stories

• Sequence Diagrams
  • A Brief History
  • Live Sequence Charts
    • LSC Body Syntax:
      • LSC Model Elements, Locations
      • Well-Formedness
    • Towards Semantics:
      • Cuts, Firedsets
      • Automaton Construction
    • Excursion: Symbolic Büchi Automata

Informatik III
(Automata Theory)
Recall: The Crux of Requirements Engineering

One quite effective approach:

try to approximate the requirements with positive and negative scenarios.

- Dear customer, please describe example usages of the desired system.
  Customer intuition: "If the system is not at all able to do this, then it’s not what I want."

- Dear customer, please describe behaviour that the desired system must not show.
  Customer intuition: "If the system does this, then it’s not what I want."

- From there on, refine and generalise:
  what about exceptional cases? what about corner-cases? etc.

Notations for Scenarios

- The idea of scenarios (sometimes without negative or anti-scenarios) (re-)occurs in many process models or software development approaches.

- In the following, we will discuss two-and-a-half notations:
  - Use Cases and Use Case Diagrams (OOSE)
  - User Stories (part of Extreme Programming)
  - Sequence Diagrams (here: Live Sequence Charts (Damm and Harel, 2001))

Use Cases
Use Case: Definition

*Use Case* — A sequence of interactions between an actor (or actors) and a system triggered by a specific actor, which produces a result for an actor. (Jacobson, 1992)

Use Case: More Precisely

- A use case has participants: the system and at least one actor.
- **Actor**: an actor represents what interacts with the system.
- An actor is a role, which a user or an external system may assume when interacting with the system under design.
- Actors are not part of the system, thus they are not described in detail.
- Actions of actors are non-deterministic (possibly constrained by domain model).
- A use case is triggered by a stimulus as input by the main actor.
- A use case is goal oriented, i.e. the main actor wants to reach a particular goal.
- A use case describes all interactions between the system and the participating actors that are needed to achieve the goal (or fail to achieve the goal for reasons).
- A use case ends when the desired goal is achieved, or when it is clear that the desired goal cannot be achieved.

<table>
<thead>
<tr>
<th>name</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>role</td>
<td>...</td>
</tr>
<tr>
<td>pre-condition</td>
<td>...</td>
</tr>
<tr>
<td>post-condition</td>
<td>...</td>
</tr>
<tr>
<td>post-cond. in exceptional case</td>
<td>...</td>
</tr>
<tr>
<td>actors</td>
<td>...</td>
</tr>
<tr>
<td>open questions</td>
<td>...</td>
</tr>
<tr>
<td>normal case</td>
<td>1. ...</td>
</tr>
<tr>
<td></td>
<td>2. ...</td>
</tr>
<tr>
<td></td>
<td>3. ...</td>
</tr>
</tbody>
</table>
Use Case Example: ATM Authentication

<table>
<thead>
<tr>
<th>name</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>goal</td>
<td>the client wants access to the ATM</td>
</tr>
<tr>
<td>pre-condition</td>
<td>the ATM is operational, the welcome screen is displayed, card and PIN of client are available</td>
</tr>
<tr>
<td>post-condition</td>
<td>client accepted, services of ATM are offered</td>
</tr>
<tr>
<td>post-cond. in exception case</td>
<td>access denied, card returned or withheld, welcome screen displayed</td>
</tr>
<tr>
<td>actors</td>
<td>client (main actor), bank system</td>
</tr>
<tr>
<td>open questions</td>
<td>none</td>
</tr>
<tr>
<td>normal case</td>
<td>1. client inserts card</td>
</tr>
<tr>
<td></td>
<td>2. ATM reads card, sends data to bank system</td>
</tr>
<tr>
<td></td>
<td>3. bank system checks validity</td>
</tr>
<tr>
<td></td>
<td>4. ATM shows PIN screen</td>
</tr>
<tr>
<td></td>
<td>5. client enters PIN</td>
</tr>
<tr>
<td></td>
<td>6. ATM reads PIN, sends to bank system</td>
</tr>
<tr>
<td></td>
<td>7. bank system checks PIN</td>
</tr>
<tr>
<td></td>
<td>8. ATM accepts and shows main menu</td>
</tr>
<tr>
<td>exception case 2a</td>
<td>card not readable</td>
</tr>
<tr>
<td></td>
<td>2a.1 ATM displays &quot;card not readable&quot;</td>
</tr>
<tr>
<td></td>
<td>2a.2 ATM returns card</td>
</tr>
<tr>
<td></td>
<td>2a.3 ATM shows welcome screen</td>
</tr>
</tbody>
</table>

exc. case 2b: card readable, but not ATM card
exc. case 2c: no connection to bank system
exc. case 3a: card not valid or disabled
exc. case 5a: client cancels
exc. case 5b: client doesn't react within 5 s
exc. case 6a: no connection to bank system
exc. case 7a: first or second PIN wrong
exc. case 7b: third PIN wrong

(Ludewig and Lichter, 2013)

Once Again: Use Case Definition

*Use Case* — A sequence of interactions between an actor (or actors) and a system triggered by a specific actor, which produces a result for an actor. (Jacobson, 1992)
Use Case Diagrams

Use Case Diagrams: Basic Building Blocks

- Actor name ➔ (use case name)
- (use case name)
- Or: (use case name)

Diagram examples:

- Actor A ➔ Use case C
- Actor B ➔ Use case C
- Use case C ➔ Actor C
Use Case Example: ATM Authentication

**Name:** Authentication

**Goal:** The client wants access to the ATM

**Pre-condition:**
- The ATM is operational
- The welcome screen is displayed
- Card and PIN of client are available

**Post-condition:**
- Client accepted
- Services of ATM are offered

**Post-cond. in exceptional case:**
- Access denied, card returned or withheld, welcome screen displayed

**Actors:**
- Client (main actor)
- Bank system

**Open questions:**
- None

**Normal case:**
1. Client inserts card
2. ATM reads card, sends data to bank system
3. Bank system checks validity
4. ATM shows PIN screen
5. Client enters PIN
6. ATM reads PIN, sends to bank system
7. Bank system checks PIN
8. ATM accepts and shows main menu

**Exception cases:**

- **Exc. case 2a**
  1. Card not readable
  2a.1 ATM displays "card not readable"
  2a.2 ATM returns card
  2a.3 ATM shows welcome screen

- **Exc. case 2b**
  Card readable, but not ATM card

- **Exc. case 2c**
  No connection to bank system

- **Exc. case 3a**
  Card not valid or disabled

- **Exc. case 5a**
  Client cancels

- **Exc. case 5b**
  Client doesn’t react within 5 s

- **Exc. case 6a**
  No connection to bank system

- **Exc. case 7a**
  First or second PIN wrong

- **Exc. case 7b**
  Third PIN wrong

*(Ludewig and Lichter, 2013)*
Use Case Diagrams: More Building Blocks

More notation:

More notation:

Use Case Diagram: Bigger Examples

(Ludewig and Lichter, 2013)
User Stories
"A User Story is a concise, written description of a piece of functionality that will be valuable to a user (or owner) of the software."

Per user story, use one file card — proposed card layout (front side):

<table>
<thead>
<tr>
<th>priority</th>
<th>unique identifier, name</th>
<th>estimation</th>
</tr>
</thead>
</table>

As a [role] I want [something] so that [benefit].

<table>
<thead>
<tr>
<th>risk</th>
<th>real effort</th>
</tr>
</thead>
</table>

with

- the user story, e.g. following the pattern:

As a [role] I want [something] so that [benefit].

and in addition:

- unique identifier (e.g. unique number),
- priority (from 1 (highest) to 10 (lowest)) assigned by customer,
- effort, estimated by developers,
- back side of file card: (acceptance) test case(s), i.e., how to tell whether the user story has been realised.

Natural Language Patterns

Natural language requirements can be (tried to be) written as an instance of the pattern "A (B) (C) (D) (E) (F)." (German grammar) where:

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>clarifies when and under what conditions the activity takes place</td>
<td>is MUST (obligation), SHOULD (wish), or WILL (intention), also: MUST NOT (forbidden)</td>
<td>is either &quot;the system&quot; or the concrete name of a (sub-)system</td>
</tr>
</tbody>
</table>

D | one of three possibilities:
|---|
| "does", description of a system activity,
| "offers", description of a function offered by the system to somebody, |
User Stories: Discussion

- ✔ easy to create, small units
- ✔ close contact to customer
- ✔ objective / testable: by fixing test cases early
- ✗ may get difficult to keep overview over whole system to be developed → maybe best suited for changes / extensions (after first iteration).
- ✗ not designed to cover non-functional requirements and restrictions
- ✗ agile spirit: strong dependency on competent developers
- ✗ estimation of effort may be difficult

(Balzert, 2009)

Customer and Developer Happy?

Use Case Example: ATM Authentication

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>goal</td>
<td>The client wants access to the ATM. The ATM is operational, the welcome screen is displayed, and PIN of client is available.</td>
</tr>
<tr>
<td>precondition</td>
<td>The ATM accepts valid card and PIN.</td>
</tr>
<tr>
<td>postcondition</td>
<td>The client is accepted, services of the ATM are offered.</td>
</tr>
</tbody>
</table>

Sample exception case:
- 1. Client inserts card.
- 2. ATM reads card, sends data to bank system.
- 4. ATM displays PIN screen.
- 5. Client enters PIN.
- 6. ATM reads PIN, sends to bank system.
- 7. Bank system checks PIN.
- 8. ATM accepts and shows main menu.

(Ludewig and Lichter, 2013)
Content

- Scenarios: The Idea
- Use Cases
  - Use Case Diagrams
- User Stories
- Sequence Diagrams
  - A Brief History
- Live Sequence Charts
  - LSC Body Syntax:
    - LSC Model Elements, Locations
    - Well-Formedness
  - Towards Semantics:
    - Cuts, Firedsets
    - Automaton Construction
  - Excursion: Symbolic Büchi Automata
A Brief History of Sequence Diagrams

- **Message Sequence Charts**, ITU standardized in different versions (ITU Z.120, 1st edition: 1993); often accused of lacking a formal semantics.

- **Sequence Diagrams** of UML 1.x (one of three main authors: I. Jacobson)

- **SDs of UML 2.x** address some issues, yet the standard exhibits unclarity and even contradictions (Harel and Maoz, 2007; Störrle, 2003)

- For the lecture, we consider **Live Sequence Charts** (LSCs) (Damm and Harel, 2001; Klose, 2003; Harel and Marely, 2003). LSCs have a common fragment with UML 2.x SDs: (Harel and Maoz, 2007).
The Plan: A Formal Semantics for a Visual Formalism

Concrete syntax
(diagram)

Abstract syntax

\((L, \preceq, \sim, I, \text{Msg},\newline Cond, \text{Lochn}, \Theta)\)

Semantics
(Büchi automaton)

Software

Does the software satisfy the LSC?

Read out relevant information

Apply construction procedure
LSC Body Syntax

LSC Body Building Blocks

instance line head
exclusive
(cold) local invariant
inclusive
(hot) line segment
coregion
(cold) line segment
(cold) condition
(hot) instantaneous message
(hot) condition
instance line/
life line
(cold) asynchronous message
Definition. [LSC Body]
Let $E$ be a set of events and $C$ a set of atomic propositions, $E \cap C = \emptyset$.
An LSC body over $E$ and $C$ is a tuple $((L, \preceq, \sim), I, \text{Msg}, \text{Cond}, \text{LocInv}, \Theta)$ where

- $L$ is a finite, non-empty set of locations with
  - a partial order $\preceq \subseteq L \times L$,
  - a symmetric simultaneity relation $\sim \subseteq L \times L$ disjoint with $\preceq$, i.e. $\preceq \cap \sim = \emptyset$,
- $I = \{I_1, \ldots, I_n\}$ is a partitioning of $L$; elements of $I$ are called instance line,
- $\text{Msg} \subseteq L \times E \times L$ is a set of messages with $(l, E, l') \in \text{Msg}$ only if $(l, l') \in \preceq \cup \sim$; message $(l, E, l')$ is called instantaneous if $l \sim l'$ and asynchronous otherwise,
- $\text{Cond} \subseteq (2^L \setminus \emptyset) \times \Phi(C)$ is a set of conditions with $(L, \phi) \in \text{Cond}$ only if $l \sim l'$ for all $l \neq l' \in L$,
- $\text{LocInv} \subseteq L \times \{\circ, \cdot\} \times \Phi(C) \times L \times \{\circ, \cdot\}$ is a set of local invariants with $(l, \iota, \phi, l', \iota') \in \text{LocInv}$ only if $l \prec l'$, $\circ$: exclusive, $\cdot$: inclusive,
- $\Theta : L \cup \text{Msg} \cup \text{Cond} \cup \text{LocInv} \rightarrow \{\text{hot, cold}\}$ assigns to each location and each element a temperature.
LSC Body: Abstract Syntax

Definition. [LSC Body]
Let $\mathcal{E}$ be a set of events and $\mathcal{C}$ a set of atomic propositions, $\mathcal{E} \cap \mathcal{C} = \emptyset$.

An LSC body over $\mathcal{E}$ and $\mathcal{C}$ is a tuple

$$((\mathcal{L}, \preceq, \sim), \mathcal{I}, \text{Msg}, \text{Cond}, \text{LocInv}, \Theta)$$

where

- $\mathcal{L}$ is a finite, non-empty set of locations with
  - a partial order $\preceq \subseteq \mathcal{L} \times \mathcal{L}$,
  - a symmetric simultaneity relation $\sim \subseteq \mathcal{L} \times \mathcal{L}$ disjoint with $\preceq$, i.e. $\preceq \cap \sim = \emptyset$,
- $\mathcal{I} = \{I_1, \ldots, I_n\}$ is a partitioning of $\mathcal{L}$; elements of $\mathcal{I}$ are called instance line,
- $\text{Msg} \subseteq \mathcal{L} \times \mathcal{E} \times \mathcal{L}$ is a set of messages with $(l, e, l') \in \text{Msg}$ only if $(l, l') \in \preceq \cup \sim$; message $(l, e, l')$ is called instantaneous if $l \sim l'$ and asynchronous otherwise,
- $\text{Cond} \subseteq (2^\mathcal{L} \setminus \emptyset) \times \Phi(\mathcal{C})$ is a set of conditions with $(I, \Phi) \in \text{Cond}$ only if $I \sim I'$ for all $I \neq I' \in \mathcal{I}$,
- $\text{LocInv} \subseteq \mathcal{L} \times \{\circ, \bullet\} \times \Phi(\mathcal{C}) \times \mathcal{L} \times \{\circ, \bullet\}$ is a set of local invariants with $(l, \circ, \Phi, l', \bullet) \in \text{LocInv}$ only if $l \sim l'$, $\circ$ exclusive, $\bullet$ inclusive,
- $\Theta : \mathcal{L} \cup \text{Msg} \cup \text{Cond} \cup \text{LocInv} \to \{\text{hot}, \text{cold}\}$ assigns to each location and each element a temperature.
From Concrete to Abstract Syntax

- locations $\mathcal{L}$,
- $\leq \subseteq \mathcal{L} \times \mathcal{L}$, $\sim \subseteq \mathcal{L} \times \mathcal{L}$
- $\mathcal{I} = \{I_1, \ldots, I_n\}$
- $\text{Msg} \subseteq \mathcal{L} \times \mathcal{E} \times \mathcal{L}$
- $\text{Cond} \subseteq (2^{\mathcal{L}} \setminus \emptyset) \times \Phi(\mathcal{C})$
- $\text{LocInv} \subseteq \mathcal{L} \times \{\text{hot, cold}\} \times \mathcal{E} \times \mathcal{L} \times \{\text{hot, cold}\}$
- $\Theta : \mathcal{L} \cup \text{Msg} \cup \text{Cond} \cup \text{LocInv} \rightarrow \{\text{hot, cold}\}$

Concrete vs. Abstract Syntax

- $\mathcal{L} = \{l_{1,0}, l_{1,1}, l_{1,2}, l_{1,3}, l_{1,4}, l_{2,0}, l_{2,1}, l_{2,2}, l_{2,3}, l_{3,0}, l_{3,1}, l_{3,2}, l_{3,3}\}$
- $l_{1,0} \prec l_{1,1} \prec l_{1,2} \prec l_{1,3}$, $l_{1,2} \prec l_{1,4}$, $l_{2,0} \prec l_{2,1} \prec l_{2,2} \prec l_{2,3}$, $l_{3,0} \prec l_{3,1} \prec l_{3,2} \prec l_{3,3}$,
  $l_{1,1} \prec l_{2,1}$, $l_{2,2} \prec l_{2,3}$, $l_{3,2} \prec l_{1,3}$, $l_{2,3} \prec l_{1,4}$, $l_{2,1} \sim l_{3,1}$, $l_{2,2} \sim l_{3,2}$,
- $\mathcal{I} = \{(l_{1,0}, l_{1,1}, l_{1,2}, l_{1,3}, l_{1,4}), (l_{2,0}, l_{2,1}, l_{2,2}, l_{2,3}), (l_{3,0}, l_{3,1}, l_{3,2}, l_{3,3})\}$
- $\text{Msg} = \{(l_{1,1}, A, l_{1,2}), (l_{2,2}, B, l_{1,2}), (l_{2,2}, C, l_{3,2}), (l_{2,3}, D, l_{1,3}), (l_{3,3}, E, l_{1,4})\}$
- $\text{Cond} = \{(\{l_{2,1}, l_{3,1}\}, c_4), (\{l_{2,2}\}, c_1)\}$
- $\text{LocInv} = \{(l_{1,1}, \mathcal{I}, c_2 \land c_3, l_{1,2})\}$
Well-Formedness

**Bondedness/no floating conditions:** (could be relaxed a little if we wanted to)

- For each location \( l \in L \), if \( l \) is the location of
  - a condition, i.e. \( \exists (L, \phi) \in \text{Cond} : l \in L \), or
  - a local invariant, i.e. \( \exists (l_1, i_1, \phi, l_2, i_2) \in \text{LocInv} : l \in \{l_1, l_2\} \),

  then there is a location \( l' \) simultaneous to \( l \), i.e. \( l \sim l' \),
  which is the location of
  - an instance head, i.e. \( l' \) is minimal wrt. \( \preceq \), or
  - a message, i.e.
    \[
    \exists (l_1, E, l_2) \in \text{Msg} : l \in \{l_1, l_2\}.
    \]

**Note:** if messages in a chart are cyclic, then there doesn’t exist a partial order (so such diagrams don’t even have an abstract syntax).
**LSC Semantics: It’s in the Cuts!**

**Definition.** Let \( \langle L, \preceq, \sim, I, \text{Msg}, \text{Cond}, \text{LocInv}, \Theta \rangle \) be an LSC body.

A non-empty set \( \emptyset \neq C \subseteq L \) is called a cut of the LSC body iff \( C \)

- is downward closed, i.e.
  \[ \forall l, l' \in L : l' \in C \land l \preceq l' \Rightarrow l \in C, \]

- is closed under simultaneity, i.e.
  \[ \forall l, l' \in L : l' \in C \land l \sim l' \Rightarrow l \in C, \] and

- comprises at least one location per instance line, i.e.
  \[ \forall I \in I : C \cap I \neq \emptyset. \]

The temperature function is extended to cuts as follows:

\[
\Theta(C) = \begin{cases} 
\text{hot} & \text{if } \exists I \in I : (\exists l' \in C : l \prec l') \land \Theta(l) = \text{hot} \\
\text{cold} & \text{otherwise}
\end{cases}
\]

that is, \( C \) is hot if and only if at least one of its maximal elements is hot.
\( \emptyset \neq C \subseteq \mathcal{L} \) — downward closed — simultaneity closed — at least one loc. per instance line

\[
\begin{array}{c}
\phi \\
\leq \\
\subseteq \text{LSC: none}
\end{array}
\]

\[
\begin{array}{c}
\text{AM: invariant} \\
\|= \text{strict}
\end{array}
\]
$\emptyset \neq C \subseteq \mathcal{L}$ — downward closed — simultaneity closed — at least one loc. per instance line
Cut Examples

$\emptyset \neq C \subseteq \mathcal{L}$ — downward closed — simultaneity closed — at least one loc. per instance line
Cut Examples

$\emptyset \neq C \subseteq \mathcal{L}$ — downward closed — simultaneity closed — at least one loc. per instance line
A Successor Relation on Cuts

The partial order "\( \preceq \)" and the simultaneity relation "\( \sim \)" of locations induce a **direct successor relation** on cuts of an LSC body as follows:

Definition.
Let \( C \subseteq L \) be a cut of an LSC body \( ((L, \preceq, \sim), I, \text{Msg}, \text{Cond}, \text{LocInv}, \Theta) \).
A set \( \emptyset \neq F \subseteq L \) of locations is called **fired-set** \( F \) of cut \( C \) if and only if

- \( C \cap F = \emptyset \) and \( C \cup F \) is a cut, i.e. \( F \) is closed under simultaneity,
- all locations in \( F \) are direct \( \preceq \)-successors of the front of \( C \), i.e.
  \[ \forall l \in F \exists l' \in C \cdot l' \prec l \wedge (\not\exists l'' \in L \cdot l' \prec l'' \prec l), \]
- locations in \( F \) that lie on the same instance line are **pairwise unordered**, i.e.
  \[ \forall l \neq l' \in F \cdot (\exists I \in I \cdot \{l, l'\} \subseteq I) \implies l \not\preceq l' \wedge l' \not\preceq l, \]
- for each asynchronous message reception in \( F \), the corresponding sending is already in \( C \),
  \[ \forall (l, E, l') \in \text{Msg} \cdot l' \in F \implies l \in C. \]

The cut \( C' = C \cup F \) is called **direct successor of \( C \)** via \( F \), denoted by \( C \leadsto F C' \).

Successor Cut Example

\( C \cap F = \emptyset \rightarrow C \cup F \) is a cut — only direct \( \preceq \)-successors — same instance line on front pairwise unordered — sending of asynchronous reception already in.
Successor Cut Example

\[ C \cap F = \emptyset - C \cup F \text{ is a cut — only direct } \leftarrow \text{successors — same instance line on front pairwise unordered — sending of asynchronous reception already in} \]

Content

- Scenarios: The Idea
- Use Cases
  - Use Case Diagrams
- User Stories
- Sequence Diagrams
  - A Brief History
- Live Sequence Charts
  - LSC Body Syntax:
    - LSC Model Elements, Locations
    - Well-Formedness
  - Towards Semantics:
    - Cuts, Firedsets
    - Automaton Construction
  - Excursion: Symbolic Büchi Automata
• **Use-Cases**:
  - interactions between system and actors,
  - be sure to elaborate exceptions and corner cases,
  - in particular effective with customers lacking technical background.
• **Use-Case Diagrams**:
  - visualise which participants are relevant for which use-case,
  - pretty useless without the underlying use-case.
• **User Stories**: simple example of scenarios
  - **strong point**: naming tests is necessary,
  - **weak point**: hard to keep overview; global restrictions.
• **Sequence Diagrams**:
  - a visual formalism for interactions, i.e.,
    - precisely defined syntax,
    - precisely defined semantics
      (construct automaton from abstract syntax)
  - Can be used to precisely describe the interactions of a use-case.


