Introduction

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

Definition: Software & SW Specification

Wrap-Up
Content

- LSCs: Automaton Construction
- Excursion: Symbolic Büchi Automata
- LSCs vs. Software
- Methodology
  - Requirements Engineering with scenarios
  - Strengthening scenarios into requirements
- Requirements Engineering Wrap-Up

Topic Area Architecture & Design

- Vocabulary
  - (software) system, component, module, interface
  - design, architecture

- Software Modelling
  - model
  - views & viewpoints, the 4+1 view
  - model-driven software engineering
"Only" construct the transitions' labels:

\[ \rightarrow = \{ (q, \psi_{\text{loop}}(q), q') \mid q \in Q \} \cup \{ (q, \psi_{\text{prog}}(q, q'), q') \mid q \xrightarrow{f} q' \} \cup \{ (q, \psi_{\text{exit}}(q), \mathcal{L}) \mid q \in Q \} \]

\[
\psi_{\text{loop}}(q) = \psi_{\text{Msg}}(q) \land \psi_{\text{LocInv,\ hot}}(q) \land \psi_{\text{LocInv,\ cold}}(q)
\]

\[
\psi_{\text{exit}}(q) = \left( \psi_{\text{hot}}(q) \land \neg \psi_{\text{LocInv,\ cold}}(q) \right) \lor \bigvee_{1 \leq i \leq n} \left( \psi_{\text{hot}}(q, q_i) \land \neg \psi_{\text{LocInv,\ hot}}(q, q_i) \land \neg \psi_{\text{Cond,\ cold}}(q, q_i) \lor \neg \psi_{\text{Cond,\ cold}}(q, q_i) \right)
\]

\[
\psi_{\text{prog}}(q, q_n) = \left( \psi_{\text{Msg}}(q, q_n) \land \psi_{\text{Cond,\ hot}}(q, q_n) \land \psi_{\text{LocInv,\ hot}}(q, q_n) \land \psi_{\text{LocInv,\ cold}}(q, q_n) \land \psi_{\text{Cond,\ cold}}(q, q_n) \right)
\]

\[
\psi_{\text{loop}}(q) = \psi_{\text{hot}}(q)
\]
**Loop Condition**

\[
\psi_{\text{loop}}(q) = \psi^\text{Msg}(q) \land \psi^\text{LocInv}_\text{hot}(q) \land \psi^\text{LocInv}_\text{cold}(q)
\]

- \(\psi^\text{Msg}(q) = \neg \bigvee_{1 \leq i \leq n} \psi^\text{Msg}(q, q_i) \land \text{strict} \implies \bigwedge_{\psi \in \mathcal{E}_? \cap \text{Msg}(\mathcal{L}) \land \neg \psi} \psi = : \psi_{\text{strict}}(q)\)

- \(\psi^\text{LocInv}_\theta(q) = \bigwedge_{\ell = (l, \iota, \phi, l', \iota') \in \text{LocInv}, \Theta(\ell) = \theta} \ell \text{ active at } q \phi\)

A location \(l\) is called **front location** of cut \(C\) if and only if \(\exists l' \in \mathcal{L} \cdot l < l'.\)

Local invariant \((l_0, \iota_0, \phi, l_1, \iota_1)\) is **active** at cut (!) \(q\) if and only if \(l_0 < l < l_1\) for some front location \(l\) of cut \(q\) or \(l = l_1 \land \iota_1 = \bullet.\)

- \(\text{Msg}(\mathcal{F}) = \{E_! \mid (l, E, l') \in \text{Msg, } l \in \mathcal{F}\} \cup \{E? \mid (l, E, l') \in \text{Msg, } l' \in \mathcal{F}\}\)

- \(\text{Msg}(\mathcal{F}_1, \ldots, \mathcal{F}_n) = \bigcup_{1 \leq i \leq n} \text{Msg}(\mathcal{F}_i)\)
Progress Condition

\[ \psi_{\text{hot}}^{\text{prog}}(q, q_i) = \psi_{\text{Msg}}^{\text{hot}}(q, q_i) \land \psi_{\text{hot}}^{\text{Cond}}(q, q_i) \land \psi_{\text{hot}}^{\text{LocInv}}(q, q_i) \]

- \( \psi_{\text{Msg}}^{\text{hot}}(q, q_i) = \bigwedge_{\psi \in \text{Msg}(q_i \setminus q)} \psi \land \bigwedge_{j \neq i} \bigwedge_{\psi \in (\text{Msg}(q_j \setminus q) \setminus \text{Msg}(q_i \setminus q))} \neg \psi \land (\text{strict} \implies \bigwedge_{\psi \in (E_1 \cap \text{Msg}(L)) \setminus \text{Msg}(F_i)} \neg \psi) \]
  
  \[ =: \psi_{\text{strict}}^{\text{hot}}(q, q_i) \]

- \( \psi_{\text{Cond}}^{\text{hot}}(q, q_i) = \bigwedge_{\gamma = (L, \phi) \in \text{Cond}, \Theta(\gamma) = \theta, L \cap (q_i \setminus q) \neq \emptyset} \phi \)

- \( \psi_{\text{LocInv}}^{\text{hot}}(q, q_i) = \bigwedge_{\lambda = (l, \mu, l', \nu') \in \text{LocInv}, \Theta(\lambda) = \theta} \lambda \cdot \text{-active at } q_i \phi \)

Local invariant \((l_0, \mu_0, \phi, l_1, \nu_1)\) is \(\cdot\)-active at \(q_i\) if and only if

- \(l_0 < l < l_1\), or
- \(l = l_0 \land \mu_0 = \bullet\), or
- \(l = l_1 \land \nu_1 = \bullet\)

for some front location \(l\) of cut (!) \(q_i\).
Example

\[ l_1, 0, l_1, 1, l_2, 0, l_2, 1, l_3, 0, l_2, 2, l_2, 3, l_3, 1, l_3, 2, l_3, 3 \]

\[ q_1, q_2, q_3, q_4, q_5, q_6, q_7 \]

\[ \text{false} \rightarrow q_1 \rightarrow \neg E \wedge \neg (E \lor F \lor \ldots) \]

\[ E \wedge \neg (E \lor F \lor \ldots) \rightarrow q_2 \rightarrow \neg E \wedge \phi \]

\[ E \wedge \phi \rightarrow q_3 \rightarrow G \wedge G \]

\[ G \wedge G \rightarrow q_4 \rightarrow (F \lor G \lor G?) \]

\[ F \lor G \lor G? \rightarrow q_5 \rightarrow \neg G \wedge G \]

\[ \neg G \wedge G \rightarrow q_6 \rightarrow \neg (G \lor G?) \]

\[ G \lor G? \rightarrow q_7 \rightarrow \text{true} \]
Content

- LSCs: Automaton Construction
- Excursion: Symbolic Büchi Automata
- LSCs vs. Software
- Methodology
  - Requirements Engineering with scenarios
  - Strengthening scenarios into requirements
- Requirements Engineering Wrap-Up

Topic Area Architecture & Design

- Vocabulary
  - (software) system, component, module, interface
  - design, architecture

- Software Modelling
  - model
  - views & viewpoints, the 4+1 view
  - model-driven software engineering
Excursion: Symbolic Büchi Automata
From Finite Automata to Symbolic Büchi Automata

\( A: \qquad \Sigma = \{0, 1\} \)

\( \mathcal{L}(A) = 0 \cdot (1, 0)^* \)

\( \omega_1 = 010 \in \mathcal{L}(A) \)

\( \omega_2 = 111 \in \mathcal{L}(A) \)

\( B: \qquad \Sigma = \{0, 1\} \)

\( \mathcal{L}(B) = 0 \cdot (10)^\omega \)

\( \omega = 010101... \in \mathcal{L}(B) \)

\( \omega_2 = 111... \in \mathcal{L}(B) \)

\( A_{sym}: \qquad \Sigma = \{x\} \rightarrow \mathbb{N} \)

\( \mathcal{L}(A_{sym}) = \{(\sum_{x \in \{x\}} x \rightarrow \mathbb{N}) \}

\( \omega = (x \rightarrow 0)(x \rightarrow 2)(x \rightarrow 3) \in \mathcal{L}(A_{sym}) \)

\( B_{sym}: \qquad \Sigma = \{x\} \rightarrow \mathbb{N} \)

\( \mathcal{L}(B_{sym}) = \{(\sum_{x \in \{x\}} x \rightarrow \mathbb{N}) \}

\( \omega = 10000... \in \mathcal{L}(B_{sym}) \)

\( \mathcal{L}(B_{sym}) = (01)^* \cdot 1 \cdot 0^\omega \)
Symbolic Büchi Automata

Definition. A Symbolic Büchi Automaton (TBA) is a tuple

\[ B = (C_B, Q, q_{ini}, \to, Q_F) \]

where

- \( C_B \) is a set of atomic propositions,
- \( Q \) is a finite set of states,
- \( q_{ini} \in Q \) is the initial state,
- \( \to \subseteq Q \times \Phi(C_B) \times Q \) is the finite transition relation. Each transition \((q, \psi, q') \in \to\) from state \( q \) to state \( q' \) is labelled with a formula \( \psi \in \Phi(C_B) \).
- \( Q_F \subseteq Q \) is the set of fair (or accepting) states.
Definition. Let $B = (C_B, Q, q_{ini}, \rightarrow, Q_F)$ be a TBA and

$$w = \sigma_1, \sigma_2, \sigma_3, \ldots \in (\Phi(C_B) \rightarrow B)^\omega$$

an infinite word, each letter is a valuation of $\Phi(C_B)$.

An infinite sequence

$$\rho = q_0, q_1, q_2, \ldots \in Q^\omega$$

of states is called run of $B$ over $w$ if and only if

- $q_0 = q_{ini}$,
- for each $i \in \mathbb{N}_0$ there is a transition $(q_i, \psi_i, q_{i+1}) \in \rightarrow$ s.t. $\sigma_i \models \psi_i$.

**Example:**

$B_{sym}$:

$$\Sigma = (\{x\} \rightarrow \mathbb{N})$$
The Language of a TBA

Definition.
We say TBA $B = (C_B, Q, q_{ini}, \rightarrow, Q_F)$ accepts the word

$$w = (\sigma_i)_{i \in \mathbb{N}_0} \in (\Phi(C_B) \to B)^\omega$$

if and only if $B$ has a run

$$\varphi = (q_i)_{i \in \mathbb{N}_0}$$

over $w$ such that fair (or accepting) states are visited infinitely often by $\varphi$, i.e., such that

$$\forall i \in \mathbb{N}_0 \exists j > i : q_j \in Q_F.$$

We call the set $Lang(B) \subseteq (\Phi(C_B) \to B)^\omega$ of words that are accepted by $B$ the language of $B$.

Example:

$B_{sym}$:

$$\Sigma = \{x\} \to \mathbb{N}$$

$$q_1 \xrightarrow{\text{even}(x)} q_2 \xrightarrow{\text{odd}(x)}$$
LSCs vs. Software
A software $S$ is called \textbf{compatible} with LSC $\mathcal{L}$ over $C$ and $E$ is if and only if
\begin{itemize}
  \item $\Sigma = (C \rightarrow B)$, i.e. the states are valuations of the conditions in $C$,
  \item $A \subseteq E! ?$, i.e. the events are of the form $E!$, $E?$ (viewed as a valuation of $E!$, $E?$).
\end{itemize}

A computation path $\pi = \sigma_0 \xrightarrow{\alpha_1} \sigma_1 \xrightarrow{\alpha_2} \sigma_2 \ldots \in \llbracket S \rrbracket$ of software $S$ \textit{induces} the word $w(\pi) = (\sigma_0 \cup \alpha_1), (\sigma_1 \cup \alpha_2), (\sigma_2 \cup \alpha_3), \ldots,$
we use $W_S$ to denote the set of words induced by $\llbracket S \rrbracket$.

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|}
\hline
\text{\textbf{\(\Theta_{\mathcal{L}}\)}} & \text{am = initial} & \text{am = invariant} \\
\hline
\text{\textbf{\textsc{cold}}} & $\exists w \in W_S \bullet w^0 \models ac \land \neg \psi_{\text{exit}}(C_0)$ & $\exists w \in W_S \exists k \in \mathbb{N}_0 \bullet w^k \models ac \land \neg \psi_{\text{exit}}(C_0)$ \\
& $\land w^0 \models \psi_{\text{prog}}(\emptyset, C_0) \land w/1 \in \text{Lang}(\mathcal{B}(\mathcal{L}))$ & $\land w^k \models \psi_{\text{prog}}(\emptyset, C_0) \land w/k + 1 \in \text{Lang}(\mathcal{B}(\mathcal{L}))$ \\
\hline
\text{\textbf{\textsc{hot}}} & $\forall w \in W_S \bullet w^0 \models ac \land \neg \psi_{\text{exit}}(C_0)$ & $\forall w \in W_S \forall k \in \mathbb{N}_0 \bullet w^k \models ac \land \neg \psi_{\text{exit}}(C_0)$ \\
& $\implies w^0 \models \psi_{\text{prog}}(\emptyset, C_0) \land w/1 \in \text{Lang}(\mathcal{B}(\mathcal{L}))$ & $\implies w^k \models \psi_{\text{cond}}^{\text{hot}}(\emptyset, C_0) \land w/k + 1 \in \text{Lang}(\mathcal{B}(\mathcal{L}))$ \\
\hline
\end{tabular}
\end{table}

Software $S$ satisfies \textbf{a set of LSCs} $\mathcal{L}_1, \ldots, \mathcal{L}_n$ if and only if $S \models \mathcal{L}_i$ for all $1 \leq i \leq n$. 
Example: TBA vs. Computation Path

$$\Pi_1 = \sigma_0 \xrightarrow{E!} \sigma_1 \xrightarrow{E!} \sigma_2 \xrightarrow{F!} \sigma_3 \xrightarrow{F! \land E! \land G!} \ldots \in \text{Lang}(\mathcal{L})$$

$$\Pi_2 = \sigma_0 \xrightarrow{E?} \ldots \in \text{Lang}(\mathcal{L})$$

$$\Pi_3 = \sigma_0 \xrightarrow{E? \land \phi} \ldots \notin \text{Lang}(\mathcal{L})$$
A full LSC \( \mathcal{L} = (PC, MC, ac, am, \Theta_\mathcal{L}) \) actually consists of

- **pre-chart** \( PC = ((\mathcal{L}_P, \preceq_P, \sim_P), I_P, Msg_P, Cond_P, LocInv_P, \Theta_P) \) (poss. empty),
- **main-chart** \( MC = ((\mathcal{L}_M, \preceq_M, \sim_M), I_M, Msg_M, Cond_M, LocInv_M, \Theta_M) \),
- **activation condition** \( ac \in \Phi(C) \), and **mode** \( am \in \{\text{initial, invariant}\}, \)
- **strictness flag** \( \text{strict} \), chart mode existential (\( \Theta_\mathcal{L} = \text{cold} \)) or universal (\( \Theta_\mathcal{L} = \text{hot} \)).

A set of words \( W \subseteq (C \to B)^\omega \) is accepted by \( \mathcal{L} \), denoted by \( W \models \mathcal{L} \), if and only if

<table>
<thead>
<tr>
<th>( \Theta_\mathcal{L})</th>
<th>( am = \text{initial} )</th>
<th>( am = \text{invariant} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \Theta_\mathcal{L} = \text{cold} )</td>
<td>( \exists w \in W \exists m \in \mathbb{N}<em>0 \cdot ) ( \wedge w^0 \models ac \land \neg \psi</em>{\text{exit}}(C^P_0) \land \psi_{\text{prog}}(\emptyset, C^P_0) ) ( \wedge w/1, \ldots, w/m \in \text{Lang}(B(PC)) ) ( \wedge w^{m+1} \models \neg \psi_{\text{exit}}(C^M_0) ) ( \wedge w^{m+1} \models \psi_{\text{prog}}(\emptyset, C^M_0) ) ( \wedge w/m + 2 \in \text{Lang}(B(MC)) )</td>
<td>( \exists w \in W \exists k &lt; m \in \mathbb{N}<em>0 \cdot ) ( \wedge w^k \models ac \land \neg \psi</em>{\text{exit}}(C^P_0) \land \psi_{\text{prog}}(\emptyset, C^P_0) ) ( \wedge w/k + 1, \ldots, w/m \in \text{Lang}(B(PC)) ) ( \wedge w^{m+1} \models \neg \psi_{\text{exit}}(C^M_0) ) ( \wedge w^{m+1} \models \psi_{\text{prog}}(\emptyset, C^M_0) ) ( \wedge w/m + 2 \in \text{Lang}(B(MC)) )</td>
</tr>
<tr>
<td>( \Theta_\mathcal{L} = \text{hot} )</td>
<td>( \forall w \in W \forall m \in \mathbb{N}<em>0 \cdot ) ( \wedge w^0 \models ac \land \neg \psi</em>{\text{exit}}(C^P_0) \land \psi_{\text{prog}}(\emptyset, C^P_0) ) ( \wedge w/1, \ldots, w/m \in \text{Lang}(B(PC)) ) ( \wedge w^{m+1} \models \neg \psi_{\text{exit}}(C^M_0) ) ( \implies w^{m+1} \models \psi_{\text{prog}}(\emptyset, C^M_0) ) ( \wedge w/m + 2 \in \text{Lang}(B(MC)) )</td>
<td>( \forall w \in W \forall k \leq m \in \mathbb{N}<em>0 \cdot ) ( \wedge w^k \models ac \land \neg \psi</em>{\text{exit}}(C^P_0) \land \psi_{\text{prog}}(\emptyset, C^P_0) ) ( \wedge w/k + 1, \ldots, w/m \in \text{Lang}(B(PC)) ) ( \wedge w^{m+1} \models \neg \psi_{\text{exit}}(C^M_0) ) ( \implies w^{m+1} \models \psi_{\text{prog}}(\emptyset, C^M_0) ) ( \wedge w/m + 2 \in \text{Lang}(B(MC)) )</td>
</tr>
</tbody>
</table>

where \( C^P_0 \) and \( C^M_0 \) are the minimal (or instance heads) cuts of pre- and main-chart.
How to Prove that a Software Satisfies an LSC?

- Software $S$ satisfies **existential** LSC $\mathcal{L}$ if there exists $\pi \in \llbracket S \rrbracket$ such that $\mathcal{L}$ accepts $w(\pi)$. Prove $S \models \mathcal{L}$ by demonstrating $\pi$.

- Note: **Existential** LSCs* may hint at **test-cases** for the **acceptance test**!
  (*: as well as (positive) scenarios in general, like use-cases)
How to Prove that a Software Satisfies an LSC?

- Software $S$ satisfies **existential** LSC $\mathcal{L}$ if there exists $\pi \in \llbracket S \rrbracket$ such that $\mathcal{L}$ accepts $w(\pi)$. Prove $S \models \mathcal{L}$ by demonstrating $\pi$.

- Note: **Existential** LSCs* may hint at test-cases for the acceptance test! (*: as well as (positive) scenarios in general, like use-cases)

- **Universal** LSCs (and negative/anti-scenarios!) in general need an **exhaustive analysis**! (Because they require that the software never ever exhibits the unwanted behaviour.)

Prove $S \not\models \mathcal{L}$ by demonstrating one $\pi$ such that $w(\pi)$ is not accepted by $\mathcal{L}$.
Pushing Things Even Further

(Harel and Marelly, 2003)
Requirements Engineering with Scenarios
One quite effective approach:

(i) **Approximate** the software requirements: ask for positive / negative existential scenarios.

(ii) **Refine** result into universal scenarios (and validate them with customer).

That is:

- **Ask** the customer to describe example usages of the desired system.
  
  In the sense of: “If the system is not at all able to do this, then it’s not what I want.”
  
  (→ positive use-cases, existential LSC)

- **Ask** the customer to describe behaviour that must not happen in the desired system.
  
  In the sense of: “If the system does this, then it’s not what I want.”
  
  (→ negative use-cases, LSC with pre-chart and hot-false)

- **Investigate** preconditions, side-conditions, exceptional cases and corner-cases.
  
  (→ extend use-cases, refine LSCs with conditions or local invariants)

- **Generalise** into universal requirements, e.g., universal LSCs.

- **Validate** with customer using new positive / negative scenarios.
**Strengthening Scenarios Into Requirements**

- Needs!
- Solution!

Customer announcement (Lastenheft) → Customer offer (Pflichtenheft) → Customer developer software contract (incl. Pflichtenheft) → Developer customer software delivery

**Needs!**

- Need 1
- Need 2
- Need 3

**Solution!**

- Customer Developer
- Announcement (Lastenheft)
- Offer (Pflichtenheft)
- Software contract (incl. Pflichtenheft)
- Software delivery

**Customer Developer software contract** (incl. Pflichtenheft)
- Ask customer for (pos./neg.) scenarios, note down as existential LSCs:

```
Button Controller Motor Sensor
- down pressed
  position ≠ bottom
  move down
  bottom reached
  stop

Button Controller Motor Sensor
- down pressed
  position ≠ bottom
  move down
  bottom reached
  stop

Button Controller Motor Sensor
- down pressed
  position = bottom
  move down
  false
  position = bottom
```
**Strengthening Scenarios Into Requirements**

- **Ask customer for (pos./neg.) scenarios**, note down as existential LSCs:

- **Strengthen into requirements**, note down as universal LSCs:

- **Re-Discuss** with customer using example words of the LSCs’ language.
Requirements on Requirements Specifications

A requirements specification should be

- **correct** – it correctly represents the wishes/needs of the customer.
- **complete** – all requirements (existing in somebody’s head, or a document, or …) should be present.
- **relevant** – things which are not relevant to the project should not be constrained.
- **consistent, free of contradictions** – each requirement is compatible with all other requirements; otherwise the requirements are not realisable.
- **neutral, abstract** – a requirements specification does not constrain the realisation more than necessary.
- **traceable, comprehensible** – the sources of requirements are documented, requirements are uniquely identifiable.
- **testable, objective** – the final product can objectively be checked for satisfying a requirement.

**Correctness** and completeness are defined relative to something which is usually only in the customer’s head.

→ is difficult to be sure of correctness and completeness.

“Dear customer, please tell me what is in your head!” is in almost all cases not a solution!

It’s not unusual that even the customer does not precisely know…!

For example, the customer may not be aware of contradictions due to technical limitations.

**Definition.** [LSC Consistency] A set of LSCs \( \{ \mathcal{L}_1, \ldots, \mathcal{L}_n \} \) is called **consistent** if and only if there exists a set of words \( W \) such that \( \bigwedge_{i=1}^n W \models \mathcal{L}_i \).
Requirements Engineering Wrap-Up
Introduction

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

Definition: Software & SW Specification

Wrap-Up
Tell Them What You’ve Told Them...

- A **Requirements Specification** should be
  - correct, complete, relevant, consistent, neutral, traceable, objective.
- **Requirements Representations** should be
  - easily understandable, precise, easily maintainable, easily usable.
- **Languages / Notations** for Requirements Representations:
  - Natural Language Patterns
  - **Decision Tables**
  - User Stories
  - Use Cases
  - **Live Sequence Charts**
- **Formal representations**
  - can be very **precise**, objective, testable,
  - can be **analysed** for, e.g., completeness, consistency
  - can be **verified** against a formal design description.

  (Formal) inconsistency of, e.g., a decision table **hints at** inconsistencies in the requirements.
Requirements Analysis in a Nutshell

- Customers **may not know** what they want.
  - That's in general not their “fault”!
  - Care for **tacit** requirements.
  - Care for **non-functional** requirements / constraints.

- For **requirements elicitation**, consider starting with
  - **scenarios** (“positive use case”) and **anti-scenarios** (“negative use case”) and elaborate corner cases.

  Thus, **use cases** can be **very useful** – use case **diagrams** not so much.

- Maintain a **dictionary** and high-quality descriptions.

- Care for **objectiveness / testability** early on.

  Ask for each requirements: what is the **acceptance test**?

- **Use formal notations**
  - to **fully understand requirements** (precision),
  - for **requirements analysis** (completeness, etc.),
  - to communicate with your developers.

- If in doubt, **complement** (formal) **diagrams with text** (as safety precaution, e.g., in lawsuits).
Example: Software Specification

Alphabet:

- $M$ – dispense cash only,
- $C$ – return card only,
- $MC$ – dispense cash and return card.

- **Customer 1**: “don’t care”
  \[ S_1 = (M.C \mid C.M \mid \frac{M}{C})^\omega \]

- **Customer 2**: “you choose, but be consistent”
  \[ S_2 = (M.C)^\omega \text{ or } (C.M)^\omega \]

- **Customer 3**: “consider human errors”
  \[ S_3 = (C.M)^\omega \]
Customer 2

Mmmh, Software!

**Formal Methods in the Software Development Process**

**Requirements**

\[ [\mathcal{S}_1] = \{(M.C, [\cdot ]_1), (C.M, [\cdot ]_1)\} \]

**Design**

\[ [\mathcal{S}_2] = \{(M.T_M.C, [\cdot ]_1), (C.T_C.M, [\cdot ]_1)\} \]

\[ [S_1] = \{\sigma_0^1 \xrightarrow{\alpha_1^1} \sigma_1^1 \xrightarrow{\alpha_2^1} \sigma_2^1 \ldots , \ldots \} \]

**Implementation**

\[ [S_2] = \{\sigma_0^2 \xrightarrow{\alpha_1^2} \sigma_1^2 \xrightarrow{\alpha_2^2} \sigma_2^2 \ldots , \ldots \} \]
Literature Recommendation

(Rupp and die SOPHISTen, 2014)
Introduction and Vocabulary

Software Modelling

(i) views and viewpoints, the 4+1 view
(ii) model-driven/-based software engineering
(iii) Unified Modelling Language (UML)

(iv) Modelling structure
   a) (simplified) class diagrams
   b) (simplified) object diagrams
   c) (simplified) object constraint logic (OCL)

Principles of Design

a) modularity
b) separation of concerns
c) information hiding and data encapsulation
d) abstract data types, object orientation

Modelling behaviour

a) communicating finite automata
b) Uppaal query language
c) basic state-machines
d) an outlook on hierarchical state-machines

Design Patterns
Survey: Previous Experience

- Project Management
- Requirements Engineering
- Programming
- Design Modelling
- Software Quality Assurance
Content

- LSCs: Automaton Construction
- Excursion: Symbolic Büchi Automata
- LSCs vs. Software
- Methodology
  - Requirements Engineering with scenarios
  - Strengthening scenarios into requirements
- Requirements Engineering Wrap-Up

Topic Area Architecture & Design

- Vocabulary
  - (software) system, component, module, interface
  - design, architecture
- Software Modelling
  - model
  - views & viewpoints, the 4+1 view
  - model-driven software engineering
Introduction
IEEE Standard Glossary of Software Engineering Terminology

Sponsor
Standards Coordinating Committee of the Computer Society of the IEEE

Approved September 28, 1990
IEEE Standards Board


Keywords: Software engineering; glossary; terminology; definitions; dictionary


Copyright © 1990 by
The Institute of Electrical and Electronics Engineers
345 East 47th Street, New York, NY 10017, USA

No part of this document may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.
**Vocabulary**

**system**— A collection of components organized to accomplish a specific function or set of functions.  
*IEEE 1471 (2000)*

**software system**— A set of software units and their relations, if they together serve a common purpose. 
This purpose is in general complex, it usually includes, next to providing one (or more) executable program(s), also the organisation, usage, maintenance, and further development. 
*Ludewig and Lichter, 2013*

**component**— One of the parts that make up a system. A component may be hardware or software and may be subdivided into other components.  
*IEEE 610.12 (1990)*

**software component**— An architectural entity that  
(1) encapsulates a subset of the system’s functionality and/or data,  
(2) restricts access to that subset via an explicitly defined interface, and  
(3) has explicitly defined dependencies on its required execution context.  
*(Taylor et al., 2010)*
Vocabulary Cont’d
**module**— (1) A program unit that is discrete and identifiable with respect to compiling, combining with other units, and loading; for example, the input to, or output from an assembler, compiler, linkage editor, or executive routine.
(2) A logically separable part of a program.  
*IEEE 610.12 (1990)*

**module**— A set of operations and data visible from the outside only in so far as explicitly permitted by the programmers. *(vs. interface)*  
*(Ludewig and Lichter, 2013)*

**interface**— A boundary across which two independent entities meet and interact or communicate with each other.  
*(Bachmann et al., 2002)*

**interface (of component)**— The boundary between two communicating components. The interface of a component provides the services of the component to the component's environment and/or requires services needed by the component from the requirement.  
*(Ludewig and Lichter, 2013)*
Even More Vocabulary
**design**—
(1) The process of defining the architecture, components, interfaces, and other characteristics of a system or component.
(2) The result of the process in (1).

**architecture**— The fundamental organization of a system embodied in its components, their relationships to each other and to the environment, and the principles guiding its design and evolution.

**software architecture**— The software architecture of a program or computing system is the structure or structures of the system which comprise software elements, the externally visible properties of those elements, and the relationships among them.

**architectural description**— A model – document, product or other artifact – to communicate and record a system’s architecture. An architectural description conveys a set of views each of which depicts the system by describing domain concerns.
Software Architecture

– The software architecture of a program or computing system is the structure or structures of the system which comprise software elements, the externally visible properties of those elements, and the relationships among them. (Bass et al., 2003)
Goals and Relevance of Design

- The **structure** of something is the set of **relations between its parts**.
- Something not built from (recognisable) parts is called **unstructured**.

**Design...**

(i) **structures** a system into **manageable** units (yields software architecture),

(ii) **determines** the approach for realising the required software,

(iii) provides **hierarchical structuring** into a **manageable** number of units at each hierarchy level.

Oversimplified process model “Design”:

```
req. (design) arch. (design) 
|  |  |
designer design
```

```
module (impl.) spec. (impl.) code
|  |  |
programmer implementation
```
Content

- LSCs: Automaton Construction
- Excursion: Symbolic Büchi Automata
- LSCs vs. Software
- Methodology
  - Requirements Engineering with scenarios
  - Strengthening scenarios into requirements
- Requirements Engineering Wrap-Up

Topic Area Architecture & Design

- Vocabulary
  - (software) system, component, module, interface
  - design, architecture

- Software Modelling
  - model
  - views & viewpoints, the 4+1 view
  - model-driven software engineering
Software Modelling
**Model**

**Definition. (Folk)** A model is an abstract, formal, mathematical representation or description of structure or behaviour of a (software) system.

**Definition. (Glinz, 2008, 425)**

A model is a concrete or mental image (Abbild) of something or a concrete or mental archetype (Vorbild) for something.

Three properties are constituent:

(i) the **image attribute** (Abbildungsmerkmal), i.e. there is an entity (called original) whose image or archetype the model is,

(ii) the **reduction attribute** (Verkürzungsmerkmal), i.e. only those attributes of the original that are relevant in the modelling context are represented,

(iii) the **pragmatic attribute**, i.e. the model is built in a specific context for a specific purpose.
Example: Process Model

From Building Blocks to Process (And Back)
1. Requirements

- Shall fit on given piece of land.
- Each room shall have a door.
- Furniture shall fit into living room.
- Bathroom shall have a window.
- Cost shall be in budget.

2. Designmodel

3. System
Example: Design-Models in Construction Engineering

1. Requirements

- Shall fit on given piece of land.
- Each room shall have a door.
- Furniture shall fit into living room.
- Bathroom shall have a window.
- Cost shall be in budget.

2. Designmodel

3. System

Observation (1): Floorplan abstracts from certain system properties, e.g., …

- kind, number, and placement of bricks,
- subsystem details (e.g., window style),
- water pipes/wiring, and
- wall decoration

→ architects can efficiently work on appropriate level of abstraction
Example: Design-Models in Construction Engineering

1. Requirements

- Shall fit on given piece of land.
- Each room shall have a door.
- Furniture shall fit into living room.
- Bathroom shall have a window.
- Cost shall be in budget.

2. Designmodel

3. System

Observation (2): Floorplan preserves/determines certain system properties, e.g.,

- house and room extensions (to scale),
- presence/absence of windows and doors,
- placement of subsystems (such as windows).

→ find design errors before building the system (e.g. bathroom windows)
A Better Analogy is Maybe Regional Planning

References
References


