• **Introduction and Vocabulary**

• **Software Modelling I**
  (i) views and viewpoints, the 4+1 view
  (ii) model-driven/-based software engineering
  (iii) **Modelling structure**
    a) (simplified) class diagrams
    b) (simplified) object diagrams
    c) (simplified) object constraint logic (OCL)
    d) Unified Modelling Language (UML)

• **Principles of Design**
  (i) modularity, separation of concerns
  (ii) information hiding and data encapsulation
  (iii) abstract data types, object orientation
  (iv) **Design Patterns**

• **Software Modelling II**
  (i) **Modelling behaviour**
    a) communicating finite automata
    b) Uppaal query language
    c) basic state-machines
    d) an outlook on hierarchical state-machines

• **Testing**: Introduction
CFA vs. Software
- a CFA model is software
- implementing CFA
- formal methods in the real world: case study

UML State Machines
- Core State Machines
- steps and run-to-completion steps
- Hierarchical State Machines
- Rhapsody

Unified Modelling Language
- Brief History
- Sub-Languages
- UML Modes
Recall: CFA, Queries, Model-Checking

**Example**

**ChoicePanel:** (simplified)

- **User:**
  - **WATER?**
  - **TEA?**
  - **SOFT?**
  - **HALF IDLE**

- **DOK?**
  - **OK!**
  - **water_enabled := false, soft_enabled := false, tea_enabled := false**

- **C50?**
  - **WATER!**
  - **TEA!**
  - **SOFT!**

- **E1!**

**Design Verification: Another Invariant**

- **Question:** Is it the case that, if there is money in the machine and water in stock, that the “water” button is enabled?

- **Approach:** Check

  - $N_{VAL} \models \forall (t, e) \left( \text{CoinValidator have } c_{50} \text{ or CoinValidator have } c_{100} \text{ or CoinValidator have } c_{150} \right)$

  imply water_enabled.

- **Query:**
  - $(\text{CoinValidator have } c_{50} \text{ or CoinValidator have } c_{100} \text{ or CoinValidator have } c_{150})$

  imply water_enabled.

**Satisfaction of Uppaal Queries by Configurations**

**Exists finally:**

- $(\tau; v_0) \models \exists \zeta \text{ path } \zeta$ of $N$ starting in $(\tau; v_0)$

- $\exists i \in \mathbb{N}_0 \cdot \zeta[i] \models \text{term}$

- “some configuration satisfying term is reachable”

**Example:**

- $(\tau; v_0) \models \exists \varphi$
CFA vs. Software
A CFA Model Is Software

Definition. **Software** is a finite description $S$ of a (possibly infinite) set $[[S]]$ of (finite or infinite) computation paths of the form

$$
\sigma_0 \xrightarrow{\alpha_1} \sigma_1 \xrightarrow{\alpha_2} \sigma_2 \cdots
$$

where

- $\sigma_i \in \Sigma$, $i \in \mathbb{N}_0$, is called **state** (or **configuration**), and
- $\alpha_i \in A$, $i \in \mathbb{N}_0$, is called **action** (or **event**).

The (possibly partial) function $[[ \cdot ]] : S \mapsto [[S]]$ is called **interpretation** of $S$.

- Let $C(A_1, \ldots, A_n)$ be a network of CFA.
- $\Sigma = \text{Conf}$
- $A = \text{Act}$
- $[[C]] = \{ \pi = \langle \vec{l}_0, \nu_0 \rangle \xrightarrow{\lambda_1} \langle \vec{l}_1, \nu_1 \rangle \xrightarrow{\lambda_2} \langle \vec{l}_2, \nu_2 \rangle \xrightarrow{\lambda_3} \cdots | \pi \text{ is a computation path of } C \}$.

**Note:** the structural model just consists of the set of variables and the locations of $C$. 

-
Customer 2

Mmmh, Software!

Requirements

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

Design

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

Implementation

\[ S_1 = \{\sigma_0^{\alpha_{1}} \rightarrow \sigma_1^{\alpha_{1}} \rightarrow \sigma_2^{\alpha_{2}} \ldots, \ldots\} \]

\[ S_2 = \{\sigma_0^{\alpha_{2}} \rightarrow \sigma_1^{\alpha_{2}} \rightarrow \sigma_2^{\alpha_{2}} \ldots, \ldots\} \]
Content I (Architecture & Design)

- CFA vs. Software
  - a CFA model is software
  - implementing CFA
  - formal methods in the real world: case study

- UML State Machines
  - Core State Machines
  - steps and run-to-completion steps
  - Hierarchical State Machines
  - Rhapsody

- Unified Modelling Language
  - Brief History
  - Sub-Languages
  - UML Modes
Implementing CFA
Implementing CFA

- Now that we have a CFA model $C(A_1, \ldots, A_n)$ (thoroughly checked using Uppaal), we would like to have executable software – an implementation of the model.

- This task can be split into two sub-tasks:
  
  (i) **implement** each CFA $A_i$ in the model by module $S_{A_i}$,

  (ii) **implement** the communication in the network by module $S_C$.

  (This has, by now, been provided implicitly by the Uppaal simulator and verifier.)

- **Fully distributed implementation** (without $S_C$): different story, possible for sub-class of CFA.
• Let $\mathcal{N} = \mathcal{C}(A_1, \ldots, A_n)$ with **pairwise disjoint variables**.

• Assume $B = B_{\text{input}} \cup B_{\text{internal}}$, where $B_{\text{input}}$ are **dedicated input channels**, i.e. there is no edge with action $a!$ and $a \in B_{\text{input}}$.

• Then software $S_\mathcal{N}$ consists of $S_{A_1}, \ldots, S_{A_n}$ and the following $S_C$.

```plaintext
Set(Act) R_1 := R_{1,ini}, \ldots, R_n := R_{n,ini};  // initially enabled actions

void main() {
  do
  □ true: (α, snd, rcv) := select(R_1, \ldots, R_n);  // choose synchronisation
    □ rcv = 0 if α = τ,  // (rcv = 0 if α = τ,  // blocks on deadlock)

    for (k = 1 to n)
      if
        □ snd = k: R_k := take_action_k(α)  // sender
        □ rcv = k: R_k := take_action_k(\bar{α})  // receiver
      fi
  od  // snapshot
}
```
int w := 3;

typedef {Wi, dispense, W0} st_T;
st_T st := Wi;

Set⟨Act⟩ take_action( Act α ) {
    Set⟨Act⟩ R := ∅;
    if
        □ st = Wi :
            □ α = DWATER? :
                w := w - 1;
                st := dispense;
                if (w = 0) R := R ∪ {DOK!};
                if (w > 0) R := R ∪ {DOK!};
            □ α = FILLUP? :
                w := 3;
                st := Wi;
                R := R ∪ {FILLUP?, DWATER?};
            fi;
    fi;

    □ st = dispense :
        □ α = DOK! ∧ w = 0 :
            st := W0;
            R := R ∪ {FILLUP?};
        □ α = DOK! ∧ w > 0 :
            st := Wi;
            R := R ∪ {FILLUP?};
        fi;

    □ st = W0 :
        □ α = FILLUP? :
            w := 3;
            st := Wi;
            R := R ∪ {FILLUP?, DWATER?};
        fi;
    fi;
}

return R;
Translation Scheme...

... for \( A = (\{\ell_1, \ldots, \ell_m\}, B, \{v_1, \ldots, v_k\}, E, \ell_{ini}) \) with

\[
E = \{(\ell_1, \alpha_{1,1}, \varphi_{1,1}, \vec{r}_{1,1}, \ell_{1,1}), \ldots, (\ell_1, \alpha_{1,n_1}, \varphi_{1,n_1}, \vec{r}_{1,n_1}, \ell_{1,n_1}),
\ldots, (\ell_m, \alpha_{m,1}, \varphi_{m,1}, \vec{r}_{m,1}, \ell_{m,1}), \ldots, (\ell_m, \alpha_{m,n_m}, \varphi_{m,n_m}, \vec{r}_{m,n_m}, \ell_{m,n_m})\}:
\]

\[
T_1 v_1 := v_{1,ini}; \ldots T_k v_k := v_{k,ini};
\]

\textbf{typedef} \( \{\ell_1, \ldots, \ell_m\} \) \( \text{st}_T \);

\( \text{st}_T \) \( \text{st} := \ell_{ini}; \)

\( \textbf{Set}\langle\text{Act}\rangle \) \( \text{take\_action}(\text{Act} \, \alpha) \) \{ 

\( \textbf{Set}\langle\text{Act}\rangle \) \( R := \emptyset; \)

\( \textbf{if} \)

\( \ldots \)

\( \square \, \text{st} = \ell_i: \, \textbf{if} \)

\( \ldots \)

\( \square \, \alpha = \alpha_{i,j} \land \varphi_{i,j}: \, \vec{r}_{i,j}; \)

\( \text{st} := \ell_{i,j}; \)

\( \textbf{if} (\ell_{i,j} = \ell_{1,1}) \, R := R \cup \{\alpha_{1,1}\}; \)

\( \ldots \)

\( \textbf{if} (\ell_{i,j} = \ell_{m,1}) \, R := R \cup \{\alpha_{m,1}\}; \)

\( \ldots \)

\( \textbf{return} \, R; \)
\}
**Definition.** A network of CFA $\mathcal{C}$ with (joint) alphabet $B$ is called deterministic if and only if each reachable configuration has at most one successor configuration, i.e. if

$$\forall c \in \text{Conf}(\mathcal{C}) \text{ reachable} \forall \lambda \in B \cup \{\tau\} \forall c_1, c_2 \in \text{Conf}(\mathcal{C}) \bullet$$

$$c \xrightarrow{\lambda} c_1 \land c \xrightarrow{\lambda} c_2 \implies c_1 = c_2.$$ 

**Proposition.** Whether $\mathcal{C}$ is deterministic is decidable.

**Proposition.** If $\mathcal{C}$ is deterministic, then the translation of $\mathcal{C}$ is a deterministic program.
Model vs. Implementation

- Define $[S_N]$ to be the set of computation paths $\sigma_0 \xrightarrow{\alpha_1} \sigma_1 \xrightarrow{\alpha_2} \sigma_2 \cdots$ such that $\sigma_i$ has the values at ‘snapshot’ at the $i$-th iteration and $\alpha_i$ is the $i$-th action.
- Then $[S_N]$ bisimulates the behaviour $[C]$ of model $C(A_1, \ldots, A_n)$. 

\[ J(e) : \sigma_0 \xrightarrow{w=3} \cdots \xrightarrow{w=3} \sigma_1 \rightarrow \sigma_2 \rightarrow \sigma_3 \cdots \]

\[ L(S_e) : \tilde{\sigma}_0 \rightarrow \cdots \rightarrow \tilde{\sigma}_n \rightarrow \cdots \rightarrow \tilde{\sigma}_1 \rightarrow \cdots \]
Model vs. Implementation

- Define $[S_N]$ to be the set of computation paths $\sigma_0 \xrightarrow{\alpha_1} \sigma_1 \xrightarrow{\alpha_2} \sigma_2 \cdots$ such that $\sigma_i$ has the values at ‘snapshot’ at the $i$-th iteration and $\alpha_i$ is the $i$-th action.
- Then $[S_N]$ bisimulates the behaviour $[C]$ of model $C(A_1, \ldots, A_n)$.

Yes, and…?

- If Uppaal reports that $\mathcal{N}_{VM} \models \exists \diamond w = 0$ holds, then $w = 0$ (should be) reachable in $[S_{\mathcal{N}_{VM}}]$.
- If Uppaal reports that $\mathcal{N}_{VM} \models \forall \square \text{tea\_enabled}$ imply CoinValidator.have_c150 holds, then $[S_{\mathcal{N}_{VM}}]$ (should be) correspondingly safe.

In General: If Uppaal reports that
- a desired configuration is not reachable in the model, or
- an invariant does not hold in the model,
then there is an issue with the model, or the requirement (or the checking tool) to be investigated.
Model-Driven Software Engineering

- (Jacobson et al., 1992): “System development is model building.”
- Model **based** software engineering (MBSE): *some* (formal) models are used.
- Model **driven** software engineering (MDSE): *all artefacts* are (formal) models.
Content I (Architecture & Design)

- CFA vs. Software
  - a CFA model is software
  - implementing CFA
  - formal methods in the real world: case study

- UML State Machines
  - Core State Machines
  - steps and run-to-completion steps
  - Hierarchical State Machines
  - Rhapsody

- Unified Modelling Language
  - Brief History
  - Sub-Languages
  - UML Modes
Formal Methods in the Real World: Case Study
(R1) The **loss of the ability** of the system to transmit a signal from a component to the central unit is **detected** in less than 300 seconds [...].

\[ \forall i \in C \quad (\text{FAIL} = i \land \lnot \text{DET}_i) \implies \ell \leq 300 \text{s} \]

(R2) A **single alarm event** is **displayed** at the central unit within 10 seconds.

\[ \forall i \in C \quad \left( \overline{\text{ALARM}}_i \right) \implies \square \left( \text{ALARM}_i \land \lnot \text{DISP}_i \implies \ell \leq 10 \text{s} \right), \]
**Figures (Arenis et al., 2016)**

<table>
<thead>
<tr>
<th>Monitoring</th>
<th>Templates</th>
<th>Instances</th>
<th>Total Locations</th>
<th>Clocks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensors as slaves</td>
<td>9</td>
<td>137</td>
<td>1040</td>
<td>6</td>
</tr>
<tr>
<td>Repeaters as slaves</td>
<td>9</td>
<td>21</td>
<td>82</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Query</th>
<th>Sensors as slaves, N = 126.</th>
<th>Repeaters as slaves, N = 10.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>seconds</td>
<td>MB</td>
</tr>
<tr>
<td>Q1 Detection possible</td>
<td>10,205.13</td>
<td>557.00</td>
</tr>
<tr>
<td>E&lt;&gt; switcher.DETECTION</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q2 No message collision</td>
<td>12,895.17</td>
<td>2,343.00</td>
</tr>
<tr>
<td>A[] not deadlock</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q3 Detect&lt;sub&gt;T&lt;/sub&gt;</td>
<td>36,070.78</td>
<td>3,419.00</td>
</tr>
<tr>
<td>A[] (switcher.DETECTION imply switcher.timer &lt;= 300*Second)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q4 NoSpur&lt;sub&gt;T&lt;/sub&gt;</td>
<td>97.44</td>
<td>44.29</td>
</tr>
<tr>
<td>A[] !center.ERROR</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Verification of the final design (Opteron 6174 2.2Ghz, 64GB, Uppaal 4.1.3 (64-bit), options -s -t0 -u).

<p>| | Model | Model | Model | Measured |</p>
<table>
<thead>
<tr>
<th></th>
<th>sequential</th>
<th>optimized</th>
<th>test scenario</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Alarm</td>
<td>3.26s</td>
<td>2.14s</td>
<td>3.31s</td>
<td>2.79s ± 0.53s</td>
</tr>
<tr>
<td>All 10 Alarms</td>
<td>29.03s</td>
<td>27.08s</td>
<td>29.81s</td>
<td>29.65s ± 3.26s</td>
</tr>
</tbody>
</table>

Predicted alarm transmission times vs. Measurements on real hardware.
Process Model

- Requirements Engineering
  - Grounding
  - Formalization
  - Elicitation
  - Validation

- Design
  - Design Capturing
  - Modeling
  - Validation

- Verification
  - Validation
  - Modeling & Verification
  - Identify Abstractions, Assumptions, Decomposition

- Model
  - Formalized Requirements
  - Glossary
  - Formal Specifications
  - Detailed Models

- Certification Authority
  - Finished Product
  - Verification Results
Case Study: Wireless Fire Alarm System

(R1) The loss of the ability of the system to transmit a signal from a component to the central unit is detected in less than 300 seconds [...].

\[ \bigwedge_{i \in C} \square (\text{FAIL} = i \wedge \text{DET}_i) \implies \ell \leq 300s \]

(R2) A single alarm event is displayed at the central unit within 10 seconds.

\[ \bigwedge_{i \in C} [\text{ALARM}_i] \implies \square (\text{ALARM}_i \wedge \text{DISP}_i) \implies \ell \leq 10s \]

Content I (Architecture & Design)

- **CFA vs. Software**
  - a CFA model is software
  - implementing CFA
  - formal methods in the real world: case study

- **UML State Machines**
  - Core State Machines
  - steps and run-to-completion steps
  - Hierarchical State Machines
  - Rhapsody

- **Unified Modelling Language**
  - Brief History
  - Sub-Languages
  - UML Modes
UML State Machines
\[ \text{annot} ::= \left[ \langle \text{event} \rangle \cdot \langle \text{event} \rangle \right]^* \left[ [ \langle \text{guard} \rangle ] \right] [ / \langle \text{action} \rangle ] \]

with

- \( \text{event} \in \mathcal{E} \), (optional)
- \( \text{guard} \in \text{Expr}_\mathcal{F} \) (default: \( \text{true} \), assumed to be in \( \text{Expr}_\mathcal{F} \))
- \( \text{action} \in \text{Act}_\mathcal{F} \) (default: \( \text{skip} \), assumed to be in \( \text{Act}_\mathcal{F} \))
Event Pool and Run-To-Completion

\[ u_1 : C \]
state: \{s_1, s_2\}
stable: Bool

\[ u_2 : D \]
\[ x = 27 \]
state: \{s_1, s_2, s_3\}
stable: Bool

<table>
<thead>
<tr>
<th>step</th>
<th>state</th>
<th>stable</th>
<th>x</th>
<th>state</th>
<th>stable</th>
<th>event pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>s_1</td>
<td>1</td>
<td>27</td>
<td>s_1</td>
<td>1</td>
<td>( E ) ready for ( u_1 )</td>
</tr>
</tbody>
</table>
Event Pool and Run-To-Completion

\[ E/\text{its}D!F \]

\[ F[x > 0] \]

\[
\begin{array}{c|c|c|c|c|c}
\text{step} & \text{state} & \text{stable} & \text{state} & \text{stable} & \text{event pool} \\
0 & s_1 & 1 & s_1 & 1 & E \text{ ready for } u_1 \\
1 & s_2 & 1 & s_1 & 1 & F \text{ ready for } u_2 \\
\end{array}
\]
Event Pool and Run-To-Completion

\[ u_1 : C \]
\[
\text{state} : \{s_1, s_2\}
\]
\[
\text{stable} : \text{Bool}
\]

\[ u_2 : D \]
\[
\text{state} : \{s_1, s_2, s_3\}
\]
\[
\text{stable} : \text{Bool}
\]

\[ E / \text{itsD} ! F \]
\[ G \]

\[ F[x > 0] \]
\[ /x := 0 \]

<table>
<thead>
<tr>
<th>step</th>
<th>state</th>
<th>stable</th>
<th>( x )</th>
<th>state</th>
<th>stable</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>( s_1 )</td>
<td>1</td>
<td>27</td>
<td>( s_1 )</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>( s_2 )</td>
<td>1</td>
<td>27</td>
<td>( s_1 )</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>( s_2 )</td>
<td>1</td>
<td>27</td>
<td>( s_2 )</td>
<td>0</td>
</tr>
</tbody>
</table>

Event pool:

- \( E \) ready for \( u_1 \)
- \( F \) ready for \( u_2 \)
Event Pool and Run-To-Completion

\[ u_1 : C \]
\[
\text{state} : \{s_1, s_2\} \\
\text{stable} : \text{Bool}
\]
\[ u_2 : D \]
\[
\text{state} : \{s_1, s_2, s_3\} \\
\text{stable} : \text{Bool}
\]

<table>
<thead>
<tr>
<th>step</th>
<th>state</th>
<th>stable</th>
<th>( x )</th>
<th>state</th>
<th>stable</th>
<th>event pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>( s_1 )</td>
<td>1</td>
<td>27</td>
<td>( s_1 )</td>
<td>1</td>
<td>( E ) ready for ( u_1 )</td>
</tr>
<tr>
<td>1</td>
<td>( s_2 )</td>
<td>1</td>
<td>27</td>
<td>( s_1 )</td>
<td>1</td>
<td>( F ) ready for ( u_2 )</td>
</tr>
<tr>
<td>2</td>
<td>( s_2 )</td>
<td>1</td>
<td>27</td>
<td>( s_2 )</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>( s_2 )</td>
<td>1</td>
<td>27</td>
<td>( s_3 )</td>
<td>0</td>
<td>( G ) ready for ( u_1 )</td>
</tr>
</tbody>
</table>
Event Pool and Run-To-Completion

\[ u_1 : C \]
\[
\text{state: } \{s_1, s_2\} \\
\text{stable: } \text{Bool}
\]

\[ u_2 : D \]
\[
\frac{x = 27}{x := 0}
\]
\[
\text{state: } \{s_1, s_2, s_3\} \\
\text{stable: } \text{Bool}
\]

<table>
<thead>
<tr>
<th>step</th>
<th>state</th>
<th>stable</th>
<th>( x )</th>
<th>state</th>
<th>stable</th>
<th>event pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>( s_1 )</td>
<td>1</td>
<td>27</td>
<td>( s_1 )</td>
<td>1</td>
<td>( E ) ready for ( u_1 )</td>
</tr>
<tr>
<td>1</td>
<td>( s_2 )</td>
<td>1</td>
<td>27</td>
<td>( s_1 )</td>
<td>1</td>
<td>( F ) ready for ( u_2 )</td>
</tr>
<tr>
<td>2</td>
<td>( s_2 )</td>
<td>1</td>
<td>27</td>
<td>( s_2 )</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>( s_2 )</td>
<td>1</td>
<td>27</td>
<td>( s_3 )</td>
<td>0</td>
<td>( G ) ready for ( u_1 )</td>
</tr>
<tr>
<td>4.a</td>
<td>( s_2 )</td>
<td>1</td>
<td>0</td>
<td>( s_1 )</td>
<td>1</td>
<td>( G ) ready for ( u_1 )</td>
</tr>
</tbody>
</table>
**Event Pool and Run-To-Completion**

### Event Pool and Run-To-Completion

#### u₁ \( C \)
- **state**: \( \{s₁, s₂\} \)
- **stable**: Bool

#### u₂ \( D \)
- **state**: \( \{s₁, s₂, s₃\} \)
- **stable**: Bool

#### x = 27

#### 0
- **step**: 0
- **state**: \( s₁ \)
- **stable**: 1
- **event pool**: \( E \) ready for \( u₁ \)

#### 1
- **step**: 1
- **state**: \( s₂ \)
- **stable**: 1
- **event pool**: \( F \) ready for \( u₂ \)

#### 2
- **step**: 2
- **state**: \( s₂ \)
- **stable**: 1
- **event pool**: \( G \) ready for \( u₁ \)

#### 3
- **step**: 3
- **state**: \( s₂ \)
- **stable**: 1
- **event pool**: \( G \) ready for \( u₁ \)

#### 4.a
- **step**: 4.a
- **state**: \( s₂ \)
- **stable**: 1
- **event pool**: \( G \) ready for \( u₁ \)

#### 5.a
- **step**: 5.a
- **state**: \( s₁ \)
- **stable**: 1
Event Pool and Run-To-Completion

\[
\begin{align*}
E/\text{itsD!F} & \quad \text{s}_1 \quad \text{G} \quad \text{s}_2 \\
F[x > 0] & \quad \text{s}_1 \quad \text{s}_2 \\
/\text{x := 0} & \quad \text{s}_2 \quad \text{s}_3 \quad /\text{itsC!G}
\end{align*}
\]

\[
\begin{array}{c|c|c|c|c|c|c}
\text{step} & \text{state} & \text{stable} & \text{x} & \text{state} & \text{stable} & \text{event pool} \\
0 & \text{s}_1 & 1 & 27 & \text{s}_1 & 1 & E \text{ ready for } u_1 \\
1 & \text{s}_2 & 1 & 27 & \text{s}_1 & 1 & F \text{ ready for } u_2 \\
2 & \text{s}_2 & 1 & 27 & \text{s}_2 & 0 & G \text{ ready for } u_1 \\
3 & \text{s}_2 & 1 & 27 & \text{s}_3 & 0 & G \text{ ready for } u_1 \\
4.a & \text{s}_2 & 1 & 0 & \text{s}_1 & 1 & G \text{ ready for } u_1 \\
5.a & \text{s}_1 & 1 & 0 & \text{s}_1 & 1 & \\
4.b & \text{s}_1 & 1 & 27 & \text{s}_3 & 0 & \\
\end{array}
\]
Event Pool and Run-To-Completion

\[
\begin{align*}
E \text{itsD}! F &\rightarrow G \\
F[x > 0] &\rightarrow / \text{itsC}! G
\end{align*}
\]

\[
\begin{array}{|c|c|c|c|c|c|}
\hline
\text{state : } \{s_1, s_2\} & \text{stable : } \text{Bool} \\
\hline
u_1 : C & \text{itsD} & \text{itsC} & u_2 : D & x = 27 & \text{state : } \{s_1, s_2, s_3\} \\
\hline
\text{state : } \{s_1, s_2, s_3\} & \text{stable : } \text{Bool} \\
\hline
\end{array}
\]

<table>
<thead>
<tr>
<th>step</th>
<th>state</th>
<th>stable</th>
<th>( x )</th>
<th>state</th>
<th>stable</th>
<th>event pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>( s_1 )</td>
<td>1</td>
<td>27</td>
<td>( s_1 )</td>
<td>1</td>
<td>( E ) ready for ( u_1 )</td>
</tr>
<tr>
<td>1</td>
<td>( s_2 )</td>
<td>1</td>
<td>27</td>
<td>( s_1 )</td>
<td>1</td>
<td>( F ) ready for ( u_2 )</td>
</tr>
<tr>
<td>2</td>
<td>( s_2 )</td>
<td>1</td>
<td>27</td>
<td>( s_2 )</td>
<td>0</td>
<td>( G ) ready for ( u_1 )</td>
</tr>
<tr>
<td>3</td>
<td>( s_2 )</td>
<td>1</td>
<td>27</td>
<td>( s_3 )</td>
<td>0</td>
<td>( G ) ready for ( u_1 )</td>
</tr>
<tr>
<td>4.a</td>
<td>( s_2 )</td>
<td>1</td>
<td>0</td>
<td>( s_1 )</td>
<td>1</td>
<td>( G ) ready for ( u_1 )</td>
</tr>
<tr>
<td>5.a</td>
<td>( s_1 )</td>
<td>1</td>
<td>0</td>
<td>( s_1 )</td>
<td>1</td>
<td>( )</td>
</tr>
<tr>
<td>4.b</td>
<td>( s_1 )</td>
<td>1</td>
<td>27</td>
<td>( s_3 )</td>
<td>0</td>
<td>( )</td>
</tr>
<tr>
<td>5.b</td>
<td>( s_1 )</td>
<td>1</td>
<td>0</td>
<td>( s_3 )</td>
<td>0</td>
<td>( )</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( )</td>
</tr>
</tbody>
</table>

- \( s_1 \) \rightarrow \text{E/itsD}! F \\
- \( s_2 \) \rightarrow \text{F}[x > 0] \\
- \( s_3 \) \rightarrow / \text{itsC}! G
Rhapsody Architecture
“D just stepped from $s_1$ to $s_2$ by transition $t$”
Composite (or Hierarchical) States

- Composite states are about abbreviation, structuring, and avoiding redundancy.
Would be Too Easy…

→ “Software Design, Modelling, and Analysis with UML” in some winter semesters.
Content I (Architecture & Design)

- CFA vs. Software
  - a CFA model is software
  - implementing CFA
  - formal methods in the real world: case study

- UML State Machines
  - Core State Machines
  - steps and run-to-completion steps
  - Hierarchical State Machines
  - Rhapsody

- Unified Modelling Language
  - Brief History
  - Sub-Languages
  - UML Modes
● Boxes/lines and finite automata are used to visualise software for ages.

● **1970’s, Software Crisis™**
  – Idea: learn from engineering disciplines to handle growing complexity.
  Modelling languages: Flowcharts, Nassi-Shneiderman, Entity-Relation Diagrams

● Mid **1980’s**: Statecharts (Harel, 1987), StateMate™ (Harel et al., 1990)

● Early **1990’s**, advent of Object-Oriented-Analysis/Design/Programming
  – Inflation of notations and methods, most prominent:
- Boxes/lines and finite automata are used to visualise software for ages.

- **1970’s, Software Crisis\textsuperscript{TM}**
  - Idea: learn from engineering disciplines to handle growing complexity.
  - Modelling languages: Flowcharts, Nassi-Shneiderman, Entity-Relation Diagrams

- **Mid 1980’s:** Statecharts (Harel, 1987), StateMate\textsuperscript{TM} (Harel et al., 1990)

- **Early 1990’s,** advent of Object-Oriented-Analysis/Design
  - Inflation of notations and methods, most prominent:
    - Object-Modeling Technique (OMT) (Rumbaugh et al., 1990)
A Brief History of the Unified Modelling Language (UML)

- Boxes/lines and finite automata are used to visualise software for ages.

- **1970’s, Software Crisis™**
  - Idea: learn from engineering disciplines to handle growing complexity.
  - Modelling languages: Flowcharts, Nassi-Shneiderman, Entity-Relation Diagrams

- **Mid 1980’s**: Statecharts (Harel, 1987), StateMate™ (Harel et al., 1990)

- **Early 1990’s**, advent of Object-Oriented-Analysis/Design/Programming
  - Inflation of notations and methods, most prominent:
    - Object-Modeling Technique (OMT) (Rumbaugh et al., 1990)
    - Booch Method and Notation (Booch, 1993)
• Boxes/lines and finite automata are used to visualise software for ages.

• **1970’s, Software Crisis™**
  – Idea: learn from engineering disciplines to handle growing complexity.
  Modelling languages: Flowcharts, Nassi-Shneiderman, Entity-Relation Diagrams

• Mid 1980’s: Statecharts (Harel, 1987), StateMate™ (Harel et al., 1990)

• Early 1990’s, advent of Object-Oriented—Analysis/Design/Programming
  – Inflation of notations and methods, most prominent:
    • **Object-Modeling Technique** (OMT) (Rumbaugh et al., 1990)
    • **Booch Method and Notation** (Booch, 1993)
    • **Object-Oriented Software Engineering** (OOSE) (Jacobson et al., 1992)

Each “persuasion” selling books, tools, seminars…
A Brief History of the Unified Modelling Language (UML)

- Boxes/lines and finite automata are used to visualise software for ages.

- **1970’s, Software Crisis**
  - Idea: learn from engineering disciplines to handle growing complexity.
  - Modelling languages: Flowcharts, Nassi-Shneiderman, Entity-Relation Diagrams

- Mid **1980’s**: Statecharts (Harel, 1987), StateMate™ (Harel et al., 1990)

- Early **1990’s**, advent of Object-Oriented-Analysis/Design/Programming
  - Inflation of notations and methods, most prominent:
    - Object-Modeling Technique (OMT) (Rumbaugh et al., 1990)
    - Booch Method and Notation (Booch, 1993)
    - Object-Oriented Software Engineering (OOSE) (Jacobson et al., 1992)

  Each “persuasion” selling books, tools, seminars…

- Late **1990’s**: joint effort of “the three amigos” UML 0.x and 1.x
  - Standards published by Object Management Group (OMG), “international, open membership, not-for-profit computer industry consortium”. Much criticised for lack of formality.

- Since **2005**: UML 2.x, split into infra- and superstructure documents.
Figure A.5 - The taxonomy of structure and behavior diagram

Dobing and Parsons (2006)
UML Modes
Recall: definition “model” (Glinz, 2008, 425):

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

**Examples for context/purpose:**

**Floorplan as sketch:**

![Floorplan sketch image]

**Floorplan as blueprint:**

![Floorplan blueprint image]

**Floorplan as program:**

![Floorplan program image]
The last slide is inspired by Martin Fowler, who puts it like this:

“ [...] people differ about what should be in the UML because there are differing fundamental views about what the UML should be.

I came up with three primary classifications for thinking about the UML: UmlAsSketch, UmlAsBlueprint, and UmlAsProgrammingLanguage.

([...] S. Mellor independently came up with the same classifications.)

So when someone else’s view of the UML seems rather different to yours, it may be because they use a different UmlMode to you.”

Claim:

- This not only applies to UML as a language (what should be in it etc.?),
- but at least as well to each individual UML model.
The last slide is inspired by Martin Fowler, who puts it like this:

### Sketch

In this UmlMode developers use the UML to help communicate some aspects of a system. [...] Sketches are also useful in documents, in which case the focus is communication rather than completeness. [...] The tools used for sketching are lightweight drawing tools and often people aren’t too particular about keeping to every strict rule of the UML. Most UML diagrams shown in books, such as mine, are sketches. Their emphasis is on selective communication rather than complete specification. Hence my sound-bite “comprehensiveness is the enemy of comprehensibility”

### Blueprint

[...] In forward engineering the idea is that blueprints are developed by a designer whose job is to build a detailed design for a programmer to code up. That design should be sufficiently complete that all design decisions are laid out and the programming should follow as a pretty straightforward activity that requires little thought. [...] Blueprints require much more sophisticated tools than sketches in order to handle the details required for the task. [...] Forward engineering tools support diagram drawing and back it up with a repository to hold the information. [...] Tools can take the UML diagrams you draw and compile them into executable code.

The promise of this is that UML is a higher level language and thus more productive than current programming languages. The question, of course, is whether this promise is true. I don’t believe that graphical programming will succeed just because it’s graphical. [...]
The “mode” fitting the lecture best is **AsBlueprint**.

**Goal:**

- be precise to **avoid misunderstandings**.
- allow formal analysis of consistency/implication on the **design level** – find errors early.

Yet we tried to be consistent with the (informal semantics) from the standard documents OMG (2007a,b) as far as possible.

**Plus:**

- Being precise also helps to work in mode **AsSketch**:
  - Knowing “the real thing” should make it easier to
  - (i) “see” which blueprint(s) the sketch is supposed to denote, and
  - (ii) to ask meaningful questions to resolve ambiguities.
Tell Them What You’ve Told Them...

- We can use tools like Uppaal to
  - check and verify CFA design models against requirements.

- CFA (and state charts)
  - can easily be implemented using the translation scheme.

- Wanted: verification results carry over to the implementation.
  - if code is not generated automatically, verify code against model.

- UML State Machines are
  - principally the same thing as CFA, yet provide more convenient syntax.

- Semantics uses
  - asynchronous communication,
  - run-to-completion steps

  in contrast to CFA.
  (We could define the same for CFA, but then the Uppaal simulator would not be useful any more.)

- Mind UML Modes.
Code Quality Assurance
Introduction and Vocabulary
- Test case, test suite, test execution.
- Positive and negative outcomes.

Limits of Software Testing
- Glass-Box Testing
  - Statement-, branch-, term-coverage.

Other Approaches
- Model-based testing,
- Runtime verification.

Software quality assurance in a larger scope.

Program Verification
- partial and total correctness,
- Proof System PD.

Review
Content (Part II)

- Introduction
  - quotes on testing,
  - systematic testing vs. ‘rumprobieren’.

- Test Case
  - definition,
  - execution,
  - positive and negative.

- The Specification of a Software

- Test Suite

- More Vocabulary
Testing: Introduction
“Testing is the execution of a program with the goal to discover errors.”
(G. J. Myers, 1979)

“Testing is the demonstration of a program or system with the goal to show that it does what it is supposed to do.”
(W. Hetzel, 1984)

“Software testing can be used to show the presence of bugs, but never to show their absence!”
(E. W. Dijkstra, 1970)

Rule-of-thumb: (fairly systematic) tests discover half of all errors.
(Ludewig and Lichter, 2013)
Recall:

**Definition.** Software is a finite description $S$ of a (possibly infinite) set $\llbracket S \rrbracket$ of (finite or infinite) computation paths of the form $\sigma_0 \xrightarrow{\alpha_1} \sigma_1 \xrightarrow{\alpha_2} \sigma_2 \cdots$ where

- $\sigma_i \in \Sigma, i \in \mathbb{N}_0$, is called state (or configuration), and
- $\alpha_i \in A, i \in \mathbb{N}_0$, is called action (or event).

The (possibly partial) function $\llbracket \cdot \rrbracket : S \mapsto \llbracket S \rrbracket$ is called interpretation of $S$.

- From now on, we assume that states consist of an input and an output/internal part, i.e., there are $\Sigma_{in}$ and $\Sigma_{out}$ such that
  $$\Sigma = \Sigma_{in} \times \Sigma_{out}.$$  

- Computation paths are then of the form
  $$\pi = \left( \begin{array}{c} \sigma_0^i \\ \sigma_0^o \end{array} \right) \xrightarrow{\alpha_1} \left( \begin{array}{c} \sigma_1^i \\ \sigma_1^o \end{array} \right) \xrightarrow{\alpha_2} \cdots$$ 

- We use $\pi \downarrow \Sigma_{in}$ to denote $\pi = \sigma_0^i \xrightarrow{\alpha_1} \sigma_1^i \xrightarrow{\alpha_2} \cdots$, i.e. the projection of $\pi$ onto $\Sigma_{in}$. 
**Definition.** A test case $T$ over $\Sigma$ and $A$ is a pair ($In$, $Soll$) consisting of

- a description $In$ of sets of finite input sequences,
- a description $Soll$ of expected outcomes,

and an interpretation $[\cdot]$ of these descriptions:

- $[In] \subseteq (\Sigma_{in} \times A)^*$, $[Soll] \subseteq (\Sigma \times A)^* \cup (\Sigma \times A)^\omega$ 

**Examples:**

- Test case for procedure `strlen`: $String \rightarrow \mathbb{N}$, $s$ denotes parameter, $r$ return value:

  $$T = (s = \text{"abc"}, r = 3)$$

  $$[s = \text{"abc"}] = \{\sigma_0^i \xrightarrow{\tau} \sigma_1^i \mid \sigma_0(s) = \text{"abc"}\}, \quad [r = 3] = \{\sigma_0 \xrightarrow{\tau} \sigma_1 \mid \sigma_1(r) = 3\},$$

  **Shorthand notation:** $T = (\text{"abc"}, 3)$.

- “Call `strlen()` with string "abc", expect return value 3.”
Test Case

Definition. A test case $T$ over $\Sigma$ and $A$ is a pair $(In, Soll)$ consisting of
- a description $In$ of sets of finite input sequences,
- a description $Soll$ of expected outcomes,
and an interpretation $[\cdot]$ of these descriptions:
- $[In] \subseteq (\Sigma_{in} \times A)^*$, $[Soll] \subseteq (\Sigma \times A)^* \cup (\Sigma \times A)^\omega$

Examples:
- Test case for vending machine.

\[ T = (C50, WATER; DWATER) \]

\[ [C50, WATER] = \{ \sigma_0 \xrightarrow{C50} \sigma_1 \xrightarrow{\tau} \cdots \xrightarrow{\tau} \sigma_{j-1} \xrightarrow{WATER} \sigma_j \} , \]

\[ [DWATER] = \{ \sigma_0 \xrightarrow{\alpha_1} \cdots \xrightarrow{\alpha_k} \sigma_{k-1} \xrightarrow{DWATER} \sigma_k \mid k \leq 10 \} , \]

- “Send event $C50$ and any time later $WATER$, expect $DWATER$ after 10 steps the latest.”
Definition. A test case $T$ over $\Sigma$ and $A$ is a pair $(In, Soll)$ consisting of

- a description $In$ of sets of finite input sequences,
- a description $Soll$ of expected outcomes,

and an interpretation $\llbracket \cdot \rrbracket$ of these descriptions:

- $\llbracket In \rrbracket \subseteq (\Sigma_{in} \times A)^*$, $\llbracket Soll \rrbracket \subseteq (\Sigma \times A)^* \cup (\Sigma \times A)^\omega$

Note:

- **Input sequences** can consider
  - input data, possibly with timing constraints,
  - other interaction, e.g., from network,
  - initial memory content,
  - etc.

- **Input sequences** may leave degrees of freedom to tester.
- **Expected outcomes** may leave degrees of freedom to system.
Executing Test Cases

- A computation path
  \[ \pi = \left( \begin{array}{c} \sigma^i_0 \\ \sigma^o_0 \end{array} \right) \xrightarrow{\alpha_1} \left( \begin{array}{c} \sigma^i_1 \\ \sigma^o_1 \end{array} \right) \xrightarrow{\alpha_2} \ldots \]
  from \([S]\) is called **execution** of test case \((In, Soll)\) if and only if
  - there is \(n \in \mathbb{N}\) such that \(\sigma_0 \xrightarrow{\alpha_1} \ldots \xrightarrow{\alpha_n} \sigma_n \downarrow \Sigma_{in} \in [In]\).

  ("A prefix of \(\pi\) corresponds to an input sequence").

Execution \(\pi\) of test case \(T\) is called
- **successful** (or **positive**) if and only if \(\pi \notin [Soll]\).
  - Intuition: an an error has been discovered.
  - Alternative: test item \(S\) **failed to pass the test**.
  - Confusing: "test failed".
- **unsuccessful** (or **negative**) if and only if \(\pi \in [Soll]\).
  - Intuition: no error has been discovered.
  - Alternative: test item \(S\) **passed the test**.
  - Okay: "test passed".
Consider the test case

\[ T = (\"\", 0) \]

for procedure `strlen`.

(“Empty string has length 0.”)

A tester observes the following software behaviour:

\[ \pi = \{ s \mapsto \text{NULL}, r \mapsto 0 \} \xrightarrow{\tau} \text{program-abortion} \]

Test execution **positive** or **negative**?
High quality software should be aware of its specification. and “complain” if operated outside of specification, e.g.

- throw an exception,
- abort program execution,
- (at least) print an error message,
- etc.

Not: “garbage in, garbage out”

Example: `strlen(3)` (C standard)

- Allowed inputs are C-strings, return value is an integer,
- `NULL` is not a C-string!
- Thus, on input `NULL`, “complain” instead of just return an arbitrary number.
Test Suite

- A test suite is a finite set of test cases \( \{T_1, \ldots, T_n\} \).

- An execution of a test suite is a set of computation paths, such that there is at least one execution for each test case.

- An execution of a test suite is called positive if and only if at least one test case execution is positive. Otherwise, it is called negative.
**Tell Them What You’ve Told Them…**

- **Testing** is about
  - finding errors, or
  - demonstrating scenarios.

- A **test case** consists of
  - input sequences and
  - expected outcome(s).

- A test case **execution** is
  - positive if an error is found,
  - negative if no error is found.

- A **test suite** is a set of test cases.

- Distinguish (among others),
  - **glass-box test**: structure (or source code) of test item available,
  - **black-box test**: structure not available.
References


References


