Topic Area Architecture & Design: Content

- **Introduction and Vocabulary**
- **Principles of Design**
  - (i) modularity
  - (ii) separation of concerns
  - (iii) information hiding and data encapsulation
  - (iv) abstract data types, object orientation
- **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)
  - (v) modelling behaviour
    - a) communicating finite automata
    - b) Uppaal query language
    - c) implementing CFA
    - d) an outlook on UML State Machines
- **Design Patterns**
- **Testing**: Introduction
Design Sanity Check: Drive to Configuration

- **Question**: Is it (at all) possible to have no water in the vending machine model? (Otherwise, the design is definitely broken.)

- **Approach**: Check whether a configuration satisfying
  \[ w = 0 \]

  is reachable, i.e. check

  \[ N_{VM} \Vdash \exists w. w = 0. \]

  for the vending machine model \( N_{VM} \).
Design Check: Scenarios

- **Question**: Is the following existential LSC satisfied by the model? (Otherwise, the design is definitely broken.)

  \[ \begin{align*}
  &\text{LSC: buy tea} \\
  &\text{AC: } \text{true} \\
  &\text{AM: initial } I: \text{permissive User} \\
  &\text{Choice Panel C} \\
  &\text{50} \\
  &\text{C} \\
  &\text{50} \\
  &\text{C} \\
  &\text{50} \\
  &\text{TEA} \\
  &\neg E_1
  \end{align*} \]

- **Approach**: Use the following newly created CFA 'Scenario' instead of User and check whether location end_of_scenario is reachable, i.e. check

  \[ \mathcal{N}'_{VM} \models \exists \text{Scenario.end_of_scenario} \]

  for the modified vending machine model \( \mathcal{N}'_{VM} \).

Design Verification: Invariants

- **Question**: Is it the case that the "tea" button is only enabled if there is €1.50 in the machine? (Otherwise, the design is broken.)

- **Approach**: Check whether the implication

  \[ \text{tea_enabled } \implies \text{CoinValidator.have_c150} \]

  holds in all reachable configurations, i.e. check

  \[ \mathcal{N}_{VM} \models \forall \text{tea_enabled } \implies \text{CoinValidator.have_c150} \]

  for the vending machine model \( \mathcal{N}_{VM} \).
**Design Verification: Sanity Check**

- **Question**: Is the “tea” button ever enabled? (Otherwise, the considered invariant $\text{tea\_enabled} \Rightarrow \text{CoinValidator.\ have\_c150}$ holds vacuously.)

- **Approach**: Check whether a configuration satisfying $\text{water\_enabled} = 1$ is reachable. Exactly like we did with $w = 0$ earlier.

**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

\[ \mathcal{N}_{\mathcal{M}} \models \forall \square (\text{CoinValidator.\ have\_c50} \lor \text{CoinValidator.\ have\_c100} \lor \text{CoinValidator.\ have\_c150}) \implies \text{water\_enabled}. \]
Recall: Universal LSC Example

Uppaal Architecture

Java

C++
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 [...].

\[ \bigwedge_{i \in C} \Box (FAIL = i \land \neg DET_i) \implies \ell \leq 300 \text{ s} \]

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

\[ \bigwedge_{i \in C} [ALARM_{i,1}] \implies \Box ([ALARM_i \land \neg DISP_i] \implies \ell \leq 10 \text{ s}) \]

Content

- CFA at Work continued
  - design checks and verification
  - Uppaal architecture
  - case study
- CFA vs. Software
  - a CFA model is software
  - implementing CFA
  - Recall MDSE
- UML State Machines
  - Core State Machines
  - steps and run-to-completion steps
  - Hierarchical State Machines
  - Rhapsody
- UML Modes
CFA vs. Software

A CFA Model Is Software

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

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

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 $S$.

- Let $\mathcal{C}(A_1, \ldots, A_n)$ be a network of CFA.
- $\Sigma = Conf$
- $A = Act$
- $\llbracket \mathcal{C} \rrbracket = \{ \pi = (\ell_0, \nu_0) \xrightarrow{\lambda_1} (\ell_1, \nu_1) \xrightarrow{\lambda_2} (\ell_2, \nu_2) \xrightarrow{\lambda_3} \ldots \mid \pi \text{ is a computation path of } \mathcal{C} \}$.

**Note:** the structural model just consists of the set of variables and the locations of $\mathcal{C}$. 
Model-Driven Software Engineering

- (Jacobson et al., 1992): “System development is model building.”
- Model driven software engineering (MDSE): everything is a model.
- Model based software engineering (MBSE): some models are used.
Implementing CFA

- Now that we have a CFA model $C(A_1, \ldots, A_n)$ (thoroughly checked using Uppaal), we would like to have software — an implementation of the model.
- This task can be split into two sub-tasks:
  1. implement each CFA $A_i$ in the model by module $S_{A_i}$.
  2. implement the communication in the network by module $S_C$.

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

Example

$st : \{ (); W0, dispense \}$

$W1 : w = 3$

$st = W1 \cup (\alpha = \text{DWATER}) ;
  w := w - 1 ;
  st = \text{dispense};$

else ($w = \text{FILLUP}$)

$w := 3$;
Example

```
int w := 3;
type st_T := {W0, dispense, W1};

Set(Act) take_action(Act α) {
  Set(Act) R := Ø;
  if □ st = W0:
    if □ α = DWATER?:
      w := w - 1;
      st := dispense;
    if □ w > 0:
      R := R∪{DOK!};
    if □ w = 0:
      R := R∪{DOK!};
      st := W0;
    R := R∪{FILLUP?, DWATER?};
  if □ st = dispense:
    if □ α = DOK! ∧ w = 0:
      R := R∪{DOK!};
      st := W0;
    if □ w > 0:
      R := R∪{FILLUP?};
      st := W0;
      R := R∪{DOK!};
    R := R∪{FILLUP?, DWATER?};
  if □ st = W0:
    if □ α = FILLUP?:
      w := 3;
      st := W1;
      R := R∪{FILLUP?, DWATER?};
  return R;
}
```

Translation Scheme...

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

$E = (\{\ell_1, \alpha_{1,1}, \varphi_{1,1}, r_{1,1}, \ell_{1,1}\}, \ldots, (\ell_m, \alpha_{m,1}, \varphi_{m,1}, r_{m,1}, \ell_{m,1}),$

$(\ell_m, \alpha_{m,1}, \varphi_{m,1}, r_{m,1}, \ell_{m,1}), \ldots, (\ell_m, \alpha_{m,n_m}, \varphi_{m,n_m}, r_{m,n_m}, \ell_{m,n_m})) :$

```
T x v1 := v_{1,ini} ... Tx x vn := v_{n,ini};
type st_T := st_{ini};
Set(Act) take_action(Act α) {
  Set(Act) R := Ø;
  if □ st = \ell_i:
    if □ α = \alpha_{i,j} ∧ \varphi_{i,j}:
      r_{i,j}:
        if (\ell_{i,j} = \ell_{1,1} ∧ \alpha_{1,1}) R := R∪{\alpha_{1,1}};
        if (\ell_{i,j} = \ell_{m,1} ∧ \alpha_{m,1}) R := R∪{\alpha_{m,1}};
      fi;
    fi;
  fi;
  return R;
}
```
**Deterministic CFA**

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

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

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

**Proposition.** Whether $C$ is deterministic is decidable.

**Proposition.** If $C$ is deterministic, then the translation of $C$ is a deterministic program.

---

**Putting It All Together**

- Let $\mathcal{N} = C(A_1, \ldots, A_n)$ 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 $S_N$ consists of $S_{A_1}, \ldots, S_{A_n}$ and the following $S_C$.

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

void main() {
    do
        if (true) {
            if (true) {
                (\alpha, snd, rcv) := select(R_1, \ldots, R_n);  // choose synchronisation
            } else {
                (\alpha, snd, rcv) := read_input();  // or read input (snd = 0)
            }
        } else {
            for (k = 1 to n) if (snd = k) R_k := take_action_k(\alpha);  // sender
            for (k = 1 to n) if (rcv = k) R_k := take_action_k(\bar{\alpha});  // receiver
            // snapshot
        }
    od
}
```
Model vs. Implementation

- Define $[S_N]$ to be the set of computation paths $\sigma_0 \overset{\alpha_1}{\longrightarrow} \sigma_1 \overset{\alpha_2}{\longrightarrow} \sigma_2 \cdots$ 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 $T(C(A_0, A_1, \ldots, A_n))$ where $A_0$ has one location $l$ and edges $E_0 = \{(l, \alpha!, true, (), l) \mid \alpha \in B_{input}\}$.

\[
B_{input} = \{\text{C50, WATER, FILLUP}\} = \{\text{C50, WATER, FILLUP}\}.
\]

$A_0:$

\[
\begin{array}{c}
\text{CSO} \\
\text{WATER!} \\
\text{FILLUP!} \\
\end{array}
\]

$A_1:$

\[
\begin{array}{c}
\text{idle} \\
\text{have_c50} \text{ WATER}! \\
\text{water_selected} \\
\text{halt_idle} \\
\end{array}
\]

$T(\mathcal{E})$

\[
\mathcal{E}:
\begin{array}{c}
\sigma_0 \overset{\alpha_1}{\longrightarrow} \sigma_1 \overset{\alpha_2}{\longrightarrow} \sigma_2 \cdots \\
\end{array}
\]

$\mathcal{L}[S_N]$:

\[
\begin{array}{c}
\sigma_0 \overset{\alpha_1}{\longrightarrow} \sigma_1 \overset{\alpha_2}{\longrightarrow} \sigma_2 \cdots \\
\end{array}
\]

\[
\begin{array}{c}
\text{CSO} \\
\text{WATER!} \\
\text{FILLUP!} \\
\end{array}
\]

Model vs. Implementation

- Define $[S_N]$ to be the set of computation paths $\sigma_0 \overset{\alpha_1}{\longrightarrow} \sigma_1 \overset{\alpha_2}{\longrightarrow} \sigma_2 \cdots$ 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 $T(C(A_0, A_1, \ldots, A_n))$ where $A_0$ has one location $l$ and edges $E_0 = \{(l, \alpha!, true, (), l) \mid \alpha \in B_{input}\}$.

\[
B_{input} = \{\text{C50, WATER, FILLUP}\} = \{\text{C50, WATER, FILLUP}\}.
\]

Yes, and...?

- If Uppaal reports that $\mathcal{N}_{VM} \models \exists w = 0$ holds, then $w = 0$ is reachable in $[S_{N_{VM}}]$.
- If Uppaal reports that
  \[
  \mathcal{N}_{VM} \models \forall \text{tea_enabled \ imply CoinValidator.have_c150}
  \]
  holds, then $[S_{N_{VM}}]$ is correspondingly safe.
Model-Driven Software Engineering

- (Jacobson et al., 1992): “System development is model building.”
- Model driven software engineering (MDSE): everything is a model.
- Model based software engineering (MBSE): some models are used.

Content

- CFA at Work continued
  - design checks and verification
  - Uppaal architecture
  - case study

- CFA vs. Software
  - a CFA model is software
  - implementing CFA
  - Recall MDSE

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

- UML Modes
UML Core State Machines

annot ::= [(event)\* \{guard\}] \{action\} 

with
- event ∈ E
- guard ∈ Expr(S)
- action ∈ Act(S)

(default: true, assumed to be in Expr(S))
(default: skip, assumed to be in Act(S))
### Event Pool and Run-To-Completion

<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>
</tbody>
</table>

**Diagram:**

- $E$ ready for $u_1$
- $F$ ready for $u_2$

- $u_1 : C, u_2 : D$
- $x = 27$
- $u_1 \in \text{itsD}$
- $u_2 \in \text{itsC}$
- $x > 0$

**Events:**
- $E$ ready for $u_1$
- $F$ ready for $u_2$

**State Transitions:**
- $s_1 \xrightarrow{G} s_2$
- $s_1 \xrightarrow{F} s_3$
- $s_2 \xrightarrow{G} s_1$
- $s_3 \xrightarrow{F} s_1$

**Conditions:**
- $x := 0$
- $u_1 \in \text{itsD}$
- $u_2 \in \text{itsC}$
Event Pool and Run-To-Completion

<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>s₁</td>
<td>1</td>
<td>27</td>
<td>s₁</td>
<td>1</td>
<td>E ready for u₁</td>
</tr>
<tr>
<td>1</td>
<td>s₂</td>
<td>1</td>
<td>27</td>
<td>s₁</td>
<td>1</td>
<td>F ready for u₂</td>
</tr>
<tr>
<td>2</td>
<td>s₂</td>
<td>1</td>
<td>27</td>
<td>s₂</td>
<td>0</td>
<td>G ready for u₁</td>
</tr>
<tr>
<td>3</td>
<td>s₂</td>
<td>1</td>
<td>27</td>
<td>s₁</td>
<td>0</td>
<td>G ready for u₁</td>
</tr>
</tbody>
</table>

Event Pool and Run-To-Completion

<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>s₁</td>
<td>1</td>
<td>27</td>
<td>s₁</td>
<td>1</td>
<td>E ready for u₁</td>
</tr>
<tr>
<td>1</td>
<td>s₂</td>
<td>1</td>
<td>27</td>
<td>s₁</td>
<td>1</td>
<td>F ready for u₂</td>
</tr>
<tr>
<td>2</td>
<td>s₂</td>
<td>1</td>
<td>27</td>
<td>s₂</td>
<td>0</td>
<td>G ready for u₁</td>
</tr>
<tr>
<td>3</td>
<td>s₂</td>
<td>1</td>
<td>27</td>
<td>s₁</td>
<td>0</td>
<td>G ready for u₁</td>
</tr>
<tr>
<td>4a</td>
<td>s₂</td>
<td>1</td>
<td>0</td>
<td>s₁</td>
<td>1</td>
<td>G ready for u₁</td>
</tr>
<tr>
<td>4b</td>
<td>s₁</td>
<td>1</td>
<td>27</td>
<td>s₁</td>
<td>0</td>
<td>H ready for u₂</td>
</tr>
<tr>
<td>5a</td>
<td>s₁</td>
<td>1</td>
<td>0</td>
<td>s₁</td>
<td>1</td>
<td>G ready for u₁</td>
</tr>
<tr>
<td>5b</td>
<td>s₁</td>
<td>1</td>
<td>0</td>
<td>s₁</td>
<td>1</td>
<td>H ready for u₁</td>
</tr>
</tbody>
</table>
generate → build / make → run

C.h → D.h → C.cpp → D.cpp → MainDefaultComponent.cpp → DfltCmp.exe

generate
build / make (compiler)
r

E!
got

“D just stepped from s1 to s2 by transition i”
generate → build / make → run

C.h → D.h → C.cpp → D.cpp → MainDefaultComponent.cpp → DfltCmp.exe

generate
build / make (compiler)
r

“D just stepped from s1 to s2 by transition i”
Composite (or Hierarchical) States

- Composite states are about abbreviation, structuring, and avoiding redundancy.

Example
“Software Design, Modelling, and Analysis with UML” in the winter semester.

UML Modes
**UML and the Pragmatic Attribute**

**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:**

<table>
<thead>
<tr>
<th>Floorplan as sketch:</th>
<th>Floorplan as blueprint:</th>
<th>Floorplan as program:</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Floorplan sketch" /></td>
<td><img src="image2.png" alt="Floorplan blueprint" /></td>
<td><img src="image3.png" alt="Floorplan program" /></td>
</tr>
</tbody>
</table>

**With UML it’s the Same** [http://martinfowler.com/bliki](http://martinfowler.com/bliki)

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.

**ProgrammingLanguage**
If you can detail the UML enough, and provide semantics for everything you need in software, you can make the UML be your programming language. 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.

**UML-Mode of the Lecture: As Blueprint**
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.

References
References


