Automated mode Coverage Analysis for Hybrid Automata using OpenModelica

Johan Eddeland
Javier Gil Cepeda
Rick Fransen
Sajed Miremadi
Martin Fabian
Knut Åkesson

Chalmers University of Technology

OpenModelica Workshop
2017
Outline

Introduction
- Model-based testing
- Coverage criteria
- Hybrid automata

Mode coverage
- Definition
- Why mode coverage and not MC/DC?

Use case from Volvo Cars
- The model
- Generating the modes
- Mode coverage results
Introduction
  Model-based testing
  Coverage criteria
  Hybrid automata

Mode coverage
  Definition
  Why mode coverage and not MC/DC?

Use case from Volvo Cars
  The model
  Generating the modes
  Mode coverage results
• An industrial Cyber-Physical System (CPS) is typically safety-critical.

• The *continuous dynamics* makes the system impossible to test efficiently using standard software testing methods.
From software testing, we know of different (code) coverage criteria, for example:
From software testing, we know of different (code) coverage criteria, for example:

- Statement coverage
From software testing, we know of different (code) coverage criteria, for example:

- Statement coverage
- Branch coverage
From software testing, we know of different (code) coverage criteria, for example:

- Statement coverage
- Branch coverage
- Condition coverage
From software testing, we know of different (code) coverage criteria, for example:

- Statement coverage
- Branch coverage
- Condition coverage
- Mixed Condition/Decision coverage (MC/DC)
\[
\begin{align*}
\text{if } u_1 > 0 \text{ then } & \quad \dot{x}_1 = -2u_1u_2x_1 \\
\text{else } & \quad \dot{x}_1 = -5u_1u_2x_1 \\
\text{end if } & \\
\text{if } u_2 > 0 \text{ then } & \quad \dot{x}_2 = -7u_1u_2x_1 \\
\text{else } & \quad \dot{x}_2 = -u_1u_2x_1 \\
\text{end if }
\end{align*}
\]

Table: Test input that gives full MC/DC.

<table>
<thead>
<tr>
<th>time</th>
<th>( u_1 )</th>
<th>( u_2 )</th>
<th>Stability</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>stable</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>stable</td>
</tr>
</tbody>
</table>
Hybrid automata

Example

\[
\text{if } u_1 > 0 \text{ then } \quad \dot{x}_1 = -2u_1 u_2 x_1 \\
\text{else} \quad \dot{x}_1 = -5u_1 u_2 x_1 \\
\text{end if}
\]

\[
\text{if } u_2 > 0 \text{ then } \quad \dot{x}_2 = -7u_1 u_2 x_1 \\
\text{else} \quad \dot{x}_2 = -u_1 u_2 x_1 \\
\text{end if}
\]
if \( u_1 > 0 \) then
\[
\dot{x}_1 = -2u_1u_2x_1
\]
else
\[
\dot{x}_1 = -5u_1u_2x_1
\]
end if

if \( u_2 > 0 \) then
\[
\dot{x}_2 = -7u_1u_2x_1
\]
else
\[
\dot{x}_2 = -u_1u_2x_1
\]
end if
Hybrid automata

Example

if \( u_1 > 0 \) then
\[
\dot{x}_1 = -2u_1 u_2 x_1
\]
else
\[
\dot{x}_1 = -5u_1 u_2 x_1
\]
end if

if \( u_2 > 0 \) then
\[
\dot{x}_2 = -7u_1 u_2 x_1
\]
else
\[
\dot{x}_2 = -u_1 u_2 x_1
\]
end if
Hybrid automata

Example

if \( u_1 > 0 \) then
\[
\dot{x}_1 = -2u_1u_2x_1
\]
else
\[
\dot{x}_1 = -5u_1u_2x_1
\]
end if

if \( u_2 > 0 \) then
\[
\dot{x}_2 = -7u_1u_2x_1
\]
else
\[
\dot{x}_2 = -u_1u_2x_1
\]
end if
Hybrid automata

Example

if $u_1 > 0$ then
   $\dot{x}_1 = -2u_1u_2x_1$
else
   $\dot{x}_1 = -5u_1u_2x_1$
end if

if $u_2 > 0$ then
   $\dot{x}_2 = -7u_1u_2x_1$
else
   $\dot{x}_2 = -u_1u_2x_1$
end if
Hybrid automata

Example

- $X = \mathbb{R}^2$ and $V(X) = \{x_1, x_2\}$,
- $Q = \{1, 2, 3, 4\}$,
- $U = \mathbb{R}^2$ and $V(U) = \{u_1, u_2\}$,
- $E$: Arrows,
- $F$: Equations,
- $G$: Arrow labels,
- $R$: The set of identity functions.

```
\begin{align*}
\dot{x}_1 &= -2u_1u_2x_1 \\
\dot{x}_2 &= -7u_1u_2x_2
\end{align*}
```

```
\begin{align*}
\dot{x}_1 &= -5u_1u_2x_1 \\
\dot{x}_2 &= -7u_1u_2x_2
\end{align*}
```

```
\begin{align*}
\dot{x}_1 &= -2u_1u_2x_1 \\
\dot{x}_2 &= -u_1u_2x_2
\end{align*}
```

```
\begin{align*}
\dot{x}_1 &= -5u_1u_2x_1 \\
\dot{x}_2 &= -u_1u_2x_2
\end{align*}
```
Introduction
  Model-based testing
  Coverage criteria
  Hybrid automata

Mode coverage
  Definition
  Why mode coverage and not MC/DC?

Use case from Volvo Cars
  The model
  Generating the modes
  Mode coverage results
A test case \( \xi(t) = (u(t), q(t), x(t)) \) is the time-varying signal containing the input \( u(t) \) applied to the hybrid system, together with the resulting hybrid states.

A test suite \( \Xi = \{\xi_1, \xi_2, \ldots, \xi_N\} \) is a set of test cases executed on the hybrid system.
The **set of visited modes** \( Q_{\text{case}} \subseteq Q \) for a **test case** \( \xi \) is defined as

\[
Q_{\text{case}}(\xi) = \{ q(t) | (\exists t \in [0, T]) [(q(t), x(t)) \in \xi] \}
\] (1)

The **set of visited modes** \( Q_{\text{suite}} \subseteq Q \) for a **test suite** \( \Xi = (\xi_1, \xi_2, \ldots, \xi_N) \) is defined as

\[
Q_{\text{suite}}(\Xi) = \bigcup_{i=1}^{N} Q_{\text{case}}(\xi_i)
\] (2)
The **mode coverage** of a test suite $\Xi$ of the hybrid automaton containing $Q$ is defined as

$$
Coverage(\Xi) = \frac{|Q_{suite}(\Xi)|}{|Q|}.
$$

(3)

Let $c_q(\xi)$ be the total time spent in mode $q$ in $\xi$, and let $C(\xi)$ denote the total time spent in all modes in $\xi$. The **relative mode coverage** $\eta$ of the mode $q \in Q$ in the test suite $\Xi = (\xi_1, \xi_2, \ldots, \xi_N)$ is defined as

$$
\eta = \frac{\sum_{i=1}^{N} c_q(\xi_i)}{\sum_{j=1}^{N} C(\xi_j)}
$$

(4)
Why mode coverage and not MC/DC?

Example

<table>
<thead>
<tr>
<th>time</th>
<th>$u_1$</th>
<th>$u_2$</th>
<th>Stability</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>stable</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>stable</td>
</tr>
</tbody>
</table>
Why mode coverage and not MC/DC?

Example

<table>
<thead>
<tr>
<th>time</th>
<th>$u_1$</th>
<th>$u_2$</th>
<th>Stability</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>stable</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>stable</td>
</tr>
</tbody>
</table>

$$\xi = \Xi = \left( \begin{bmatrix} 1 \\ -1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right), \begin{bmatrix} 1 \\ 4 \end{bmatrix}, \left( \begin{bmatrix} x_1(0) \\ x_1(1) \end{bmatrix}, \begin{bmatrix} x_2(0) \\ x_2(1) \end{bmatrix} \right)$$
Why mode coverage and not MC/DC?

Example

<table>
<thead>
<tr>
<th>time</th>
<th>$u_1$</th>
<th>$u_2$</th>
<th>Stability</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>stable</td>
</tr>
<tr>
<td>1</td>
<td>−1</td>
<td>−1</td>
<td>stable</td>
</tr>
</tbody>
</table>

$$\xi = \Xi = (\begin{bmatrix} 1 \\ -1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix}), \begin{bmatrix} 1 \\ 4 \end{bmatrix}, (\begin{bmatrix} x_1(0) \\ x_1(1) \end{bmatrix}, \begin{bmatrix} x_2(0) \\ x_2(1) \end{bmatrix})$$

- $Q_{case} = Q_{suite} = \{1, 4\}$,
Why mode coverage and not MC/DC?

Example

<table>
<thead>
<tr>
<th>time</th>
<th>$u_1$</th>
<th>$u_2$</th>
<th>Stability</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>stable</td>
</tr>
<tr>
<td>1</td>
<td>−1</td>
<td>−1</td>
<td>stable</td>
</tr>
</tbody>
</table>

$$\xi = \Xi = \left( \left( \begin{bmatrix} 1 \\ -1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right), \begin{bmatrix} 1 \\ 4 \end{bmatrix}, \left( \begin{bmatrix} x_1(0) \\ x_1(1) \end{bmatrix}, \begin{bmatrix} x_2(0) \\ x_2(1) \end{bmatrix} \right) \right)$$

- $Q_{case} = Q_{suite} = \{1, 4\}$,
- $Coverage(\Xi) = \frac{|\{1,4\}|}{|\{1,2,3,4\}|} = \frac{2}{4} = 0.5,$
Why mode coverage and not MC/DC?

Example

<table>
<thead>
<tr>
<th>time</th>
<th>$u_1$</th>
<th>$u_2$</th>
<th>Stability</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>stable</td>
</tr>
<tr>
<td>1</td>
<td>−1</td>
<td>−1</td>
<td>stable</td>
</tr>
</tbody>
</table>

$$\xi = \Xi = \left(\left(\begin{bmatrix} 1 \\ -1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix}\right), \begin{bmatrix} 1 \\ 4 \end{bmatrix}, \left(\begin{bmatrix} x_1(0) \\ x_1(1) \end{bmatrix}, \begin{bmatrix} x_2(0) \\ x_2(1) \end{bmatrix}\right)\right)$$

- $Q_{case} = Q_{suite} = \{1, 4\}$,
- $Coverage(\Xi) = \frac{|\{1, 4\}|}{|\{1, 2, 3, 4\}|} = \frac{2}{4} = 0.5$,
- $\eta_1 = \eta_4 = \frac{1}{2} = 0.5$, 

$\eta_2 = \eta_3 = 0$.5.
Why mode coverage and not MC/DC?

Example

<table>
<thead>
<tr>
<th>time</th>
<th>$u_1$</th>
<th>$u_2$</th>
<th>Stability</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>stable</td>
</tr>
<tr>
<td>1</td>
<td>−1</td>
<td>−1</td>
<td>stable</td>
</tr>
</tbody>
</table>

$$\xi = \Xi = \left( \begin{bmatrix} 1 \\ -1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right), \begin{bmatrix} 1 \\ 4 \end{bmatrix}, \left( \begin{bmatrix} x_1(0) \\ x_1(1) \end{bmatrix}, \begin{bmatrix} x_2(0) \\ x_2(1) \end{bmatrix} \right) \right)$$

- $Q_{case} = Q_{suite} = \{1, 4\}$,
- $Coverage(\Xi) = \frac{|\{1, 4\}|}{|\{1, 2, 3, 4\}|} = \frac{2}{4} = 0.5$,
- $\eta_1 = \eta_4 = \frac{1}{2} = 0.5$,
- $\eta_2 = \eta_3 = 0$. 
• From our toy example, we get full MC/DC coverage but only 50% mode coverage
• Mode coverage can give additional insight for complex models
Outline

Introduction
Model-based testing
Coverage criteria
Hybrid automata

Mode coverage
Definition
Why mode coverage and not MC/DC?

Use case from Volvo Cars
The model
Generating the modes
Mode coverage results
• We use mode coverage to analyze previously created test vectors
• 175 test vectors
  • 25 created manually by engineers
  • 150 created automatically using Testweaver
Generating the modes
Using an SMT solver

- The conditions for equations to be executed can be formulated using first-order logic
- Conflicting conditions lead to unreachable modes
- These unreachable modes are removed by an SMT Solver
Generating the modes
Overview of approach

Simscape model

Manual translation

Automatic run of previously created test vectors

Modelica model

OpenModelica code generation

Plant model test data

C-code of plant model

Automatic extraction of modes

Plant modes

Analysis of modes

Output
Generating the modes
OpenModelica’s role

Modelica Source Code

Modelica model

Translator

Flat model

Analyzer

Sorted equations

Optimizer

Optimized sorted equations

Code Generator

C Code

C Compiler

Executable

Simulation

Use case from Volvo Cars — Generating the modes

Johan Eddeland et al. OpenModelica Workshop 2017 24/27
Generating the modes
Characteristics of generated modes

- The automatically generated modes are interpreted as physical configurations.
- Automatically generate 34 modes, our modelling gives 8 physical configurations.
- The difference is mainly due to Boolean variables defining the system state more precisely without changing physical appearance.
Use case from Volvo Cars — Mode coverage results

<table>
<thead>
<tr>
<th>Physical configuration</th>
<th>$\eta_{man}$</th>
<th>$\eta_{auto}$</th>
<th>$\eta_{tot}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.336%</td>
<td>0%</td>
<td>0.228%</td>
</tr>
<tr>
<td>2</td>
<td>0.066%</td>
<td>0%</td>
<td>0.045%</td>
</tr>
<tr>
<td>3</td>
<td>1.111%</td>
<td>0.623%</td>
<td>0.954%</td>
</tr>
<tr>
<td>4</td>
<td>0.103%</td>
<td>2.988%</td>
<td>1.031%</td>
</tr>
<tr>
<td>5</td>
<td>97.814%</td>
<td>96.386%</td>
<td>97.356%</td>
</tr>
<tr>
<td>6</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>7</td>
<td>0%</td>
<td>0.003%</td>
<td>0.001%</td>
</tr>
<tr>
<td>8</td>
<td>0.570%</td>
<td>0%</td>
<td>0.385%</td>
</tr>
</tbody>
</table>

Mode coverage: 75% 50% 87.5%
Use case from Volvo Cars — Mode coverage results

<table>
<thead>
<tr>
<th>Physical configuration</th>
<th>$\eta_{man}$</th>
<th>$\eta_{auto}$</th>
<th>$\eta_{tot}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.336%</td>
<td>0%</td>
<td>0.228%</td>
</tr>
<tr>
<td>2</td>
<td>0.066%</td>
<td>0%</td>
<td>0.045%</td>
</tr>
<tr>
<td>3</td>
<td>1.111%</td>
<td>0.623%</td>
<td>0.954%</td>
</tr>
<tr>
<td>4</td>
<td>0.103%</td>
<td>2.988%</td>
<td>1.031%</td>
</tr>
<tr>
<td>5</td>
<td>97.814%</td>
<td>96.386%</td>
<td>97.356%</td>
</tr>
<tr>
<td>6</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>7</td>
<td>0%</td>
<td>0.003%</td>
<td>0.001%</td>
</tr>
<tr>
<td>8</td>
<td>0.570%</td>
<td>0%</td>
<td>0.385%</td>
</tr>
</tbody>
</table>

**Mode coverage:**
- 75%
- 50%
- 87.5%

- Configuration 6 is never visited
Mode coverage results

<table>
<thead>
<tr>
<th>Physical configuration</th>
<th>$\eta_{\text{man}}$</th>
<th>$\eta_{\text{auto}}$</th>
<th>$\eta_{\text{tot}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.336%</td>
<td>0%</td>
<td>0.228%</td>
</tr>
<tr>
<td>2</td>
<td>0.066%</td>
<td>0%</td>
<td>0.045%</td>
</tr>
<tr>
<td>3</td>
<td>1.111%</td>
<td>0.623%</td>
<td>0.954%</td>
</tr>
<tr>
<td>4</td>
<td>0.103%</td>
<td>2.988%</td>
<td>1.031%</td>
</tr>
<tr>
<td>5</td>
<td>97.814%</td>
<td>96.386%</td>
<td>97.356%</td>
</tr>
<tr>
<td>6</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>7</td>
<td>0%</td>
<td>0.003%</td>
<td>0.001%</td>
</tr>
<tr>
<td>8</td>
<td>0.570%</td>
<td>0%</td>
<td>0.385%</td>
</tr>
</tbody>
</table>

Mode coverage: 75% 50% 87.5%

- Configuration 6 is never visited
- System spends large amount of time in configuration 5
• Analysis of mode coverage and relative mode coverage can give insights into how well a system is exercised by a test suite.

• In some ways, mode coverage is more detailed than e.g. MC/DC.

• We can generate modes automatically thanks to OpenModelica and the Z3 SMT solver.

This work has been performed with support from the Swedish Governmental Agency for Innovation Systems (VINNOVA) under project TESTRON 2015-04893.