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

Outline

Model-based testing

- 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.

Coverage criteria

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

Coverage criteria

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

- Statement coverage

Coverage criteria

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

- Statement coverage
- Branch coverage

Coverage criteria

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

- Statement coverage
- Branch coverage
- Condition coverage

Coverage criteria

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

- Statement coverage
- Branch coverage
- Condition coverage
- Mixed Condition/Decision coverage (MC/DC)

Coverage criteria

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

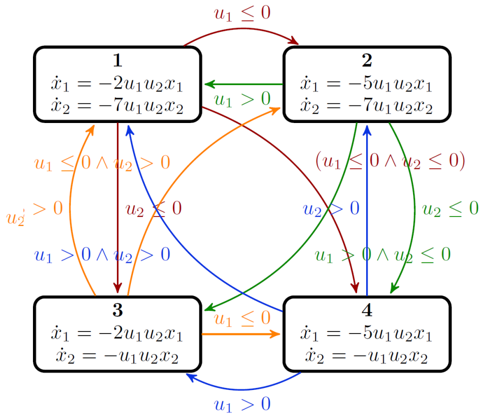
Table: Test input that gives full MC/DC.

time	u_1	u_2	Stability
0	1	1	stable
1	-1	-1	stable

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

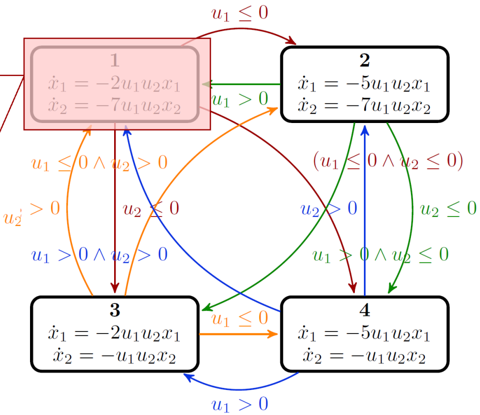
if $u_2 > 0$ **then**
    $\dot{x}_2 = -7u_1u_2x_1$
else
    $\dot{x}_2 = -u_1u_2x_1$
end if



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

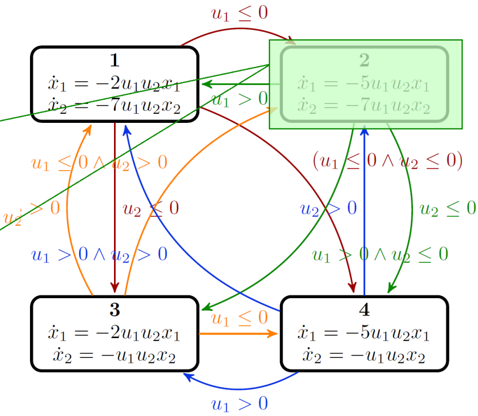
if $u_2 > 0$ **then**
$\dot{x}_2 = -7u_1u_2x_1$
else
$\dot{x}_2 = -u_1u_2x_1$
end if



Hybrid automata
Example

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

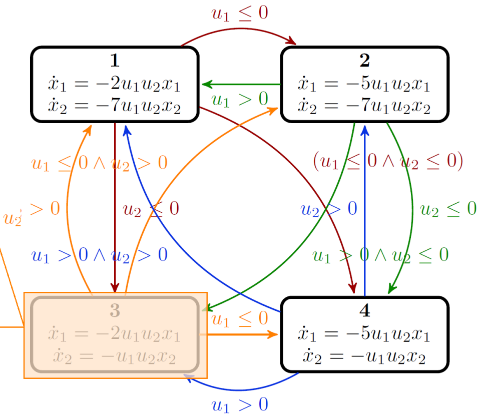


Hybrid automata

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

if $u_1 > 0$ **then**

$\dot{x}_1 = -2u_1u_2x_1$

else

$\dot{x}_1 = -5u_1u_2x_1$

end if

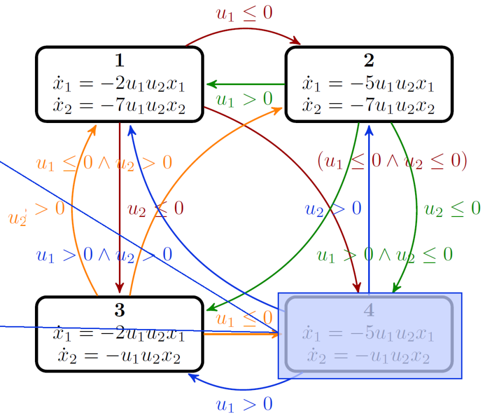
if $u_2 > 0$ **then**

$\dot{x}_2 = -7u_1u_2x_1$

else

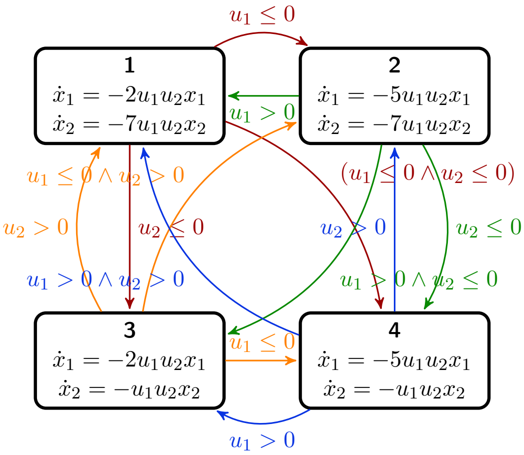
$\dot{x}_2 = -u_1u_2x_1$

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.



Outline

Definition

Test case, test suite

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.

Definition
Set of visited modes

The ***set of visited modes*** $Q_{case} \subseteq Q$ for a *test case* ξ is defined as

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

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

$$Q_{suite}(\Xi) = \bigcup_{i=1}^{N} Q_{case}(\xi_i) \tag{2}$$

Definition

Mode coverage, relative mode coverage

The ***mode coverage*** of a test suite Ξ of the hybrid automaton containing Q is defined as

$$Coverage(\Xi) = \frac{|Q_{suite}(\Xi)|}{|Q|}. \tag{3}$$

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

$$\eta = \frac{\sum_{i=1}^{N} c_q(\xi_i)}{\sum_{j=1}^{N} C(\xi_j)} \tag{4}$$

Why mode coverage and not MC/DC?

Example

time	u_1	u_2	Stability
0	1	1	stable
1	-1	-1	stable

Why mode coverage and not MC/DC?

Example

time	u_1	u_2	Stability
0	1	1	stable
1	-1	-1	stable

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

Why mode coverage and not MC/DC?

Example

time	u_1	u_2	Stability
0	1	1	stable
1	-1	-1	stable

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

- $Q_{case} = Q_{suite} = \{1, 4\}$,

Why mode coverage and not MC/DC?

Example

time	u_1	u_2	Stability
0	1	1	stable
1	-1	-1	stable

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

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

Why mode coverage and not MC/DC?

Example

time	u_1	u_2	Stability
0	1	1	stable
1	-1	-1	stable

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

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

Why mode coverage and not MC/DC?

Example

time	u_1	u_2	Stability
0	1	1	stable
1	-1	-1	stable

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

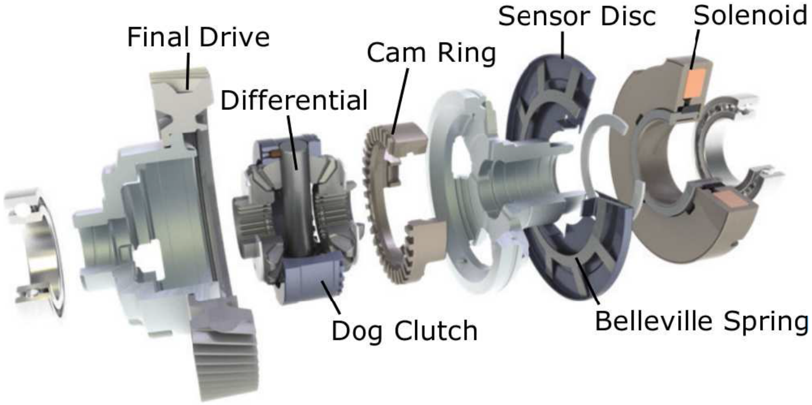
- $Q_{case} = Q_{suite} = \{1, 4\}$,
- $Coverage(\Xi) = \frac{|\{1,4\}|}{|\{1,2,3,4\}|} = \frac{2}{4} = 0.5$,
- $\eta_1 = \eta_4 = \frac{1}{2} = 0.5$,
- $\eta_2 = \eta_3 = 0$.

Why mode coverage and not MC/DC?

- From our toy example, we get full MC/DC coverage but only 50% mode coverage
- Mode coverage can give additional insight for complex models

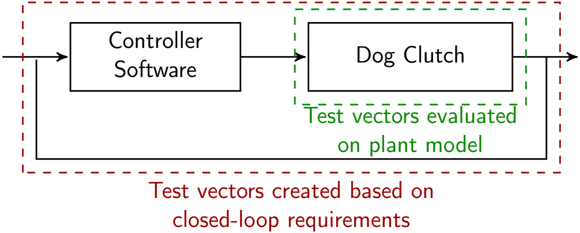
Outline

The model


Final Drive
Differential
Cam Ring
Sensor Disc
Solenoid
Dog Clutch
Belleville Spring

The model

- We use mode coverage to analyze previously created test vectors
- 175 test vectors
  - 25 created manually by engineers
  - 150 created automatically using Testweaver

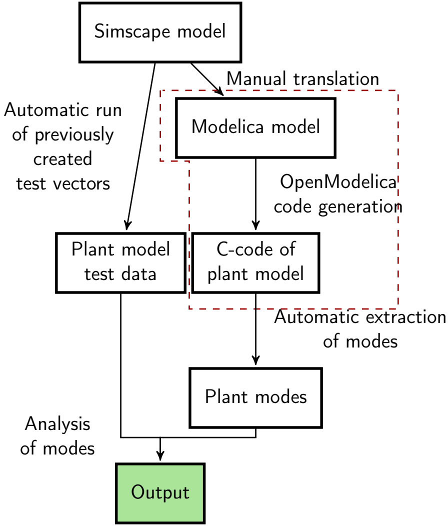


Generating the modes
Using an SMT solver

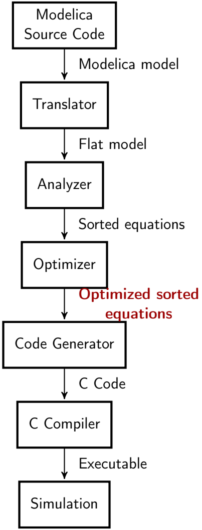
- The conditions for equations to be executed can be formulated using first-order logic
- Conflicting conditions lead to unreachable modes
- These unreachable modes are removed by an SMT Solver

Generating the modes

Overview of approach

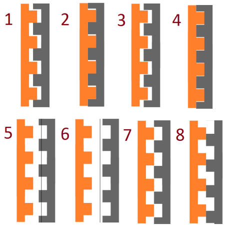


Generating the modes
OpenModelica's role

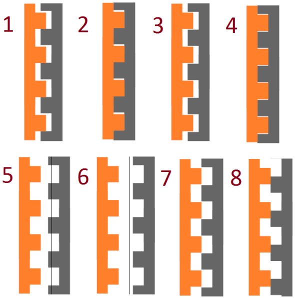


Generating the modes
Characteristics of generated modes

- 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

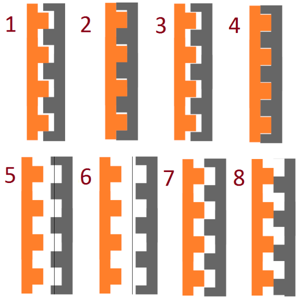


Mode coverage results



Physical configuration	η_{man}	η_{auto}	η_{tot}
1	0.336%	0%	0.228%
2	0.066%	0%	0.045%
3	1.111%	0.623%	0.954%%
4	0.103%	2.988%	1.031%
5	97.814%	96.386%	97.356%
6	0%	0%	0%
7	0%	0.003%	0.001%
8	0.570%	0%	0.385%
Mode coverage:	75%	50%	87.5%

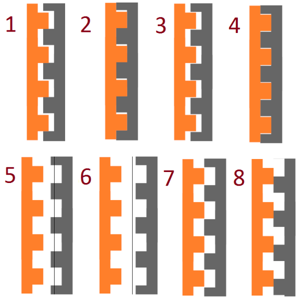
Mode coverage results



Physical configuration	η_{man}	η_{auto}	η_{tot}
1	0.336%	0%	0.228%
2	0.066%	0%	0.045%
3	1.111%	0.623%	0.954%%
4	0.103%	2.988%	1.031%
5	97.814%	96.386%	97.356%
6	0%	0%	0%
7	0%	0.003%	0.001%
8	0.570%	0%	0.385%
Mode coverage:	75%	50%	87.5%

- Configuration 6 is never visited

Mode coverage results



Physical configuration	η_{man}	η_{auto}	η_{tot}
1	0.336%	0%	0.228%
2	0.066%	0%	0.045%
3	1.111%	0.623%	0.954%%
4	0.103%	2.988%	1.031%
5	97.814%	96.386%	97.356%
6	0%	0%	0%
7	0%	0.003%	0.001%
8	0.570%	0%	0.385%
Mode coverage:	75%	50%	87.5%

- Configuration 6 is never visited
- System spends large amount of time in configuration 5

Mode coverage results
Conclusions

- 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.