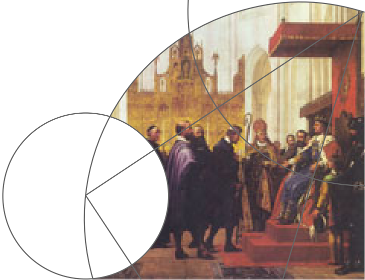
Towards Automatic Program Specification Using SME Models

Communicating Process Architectures 2018 – Technische Universität Dresden

Alberte Thegler
Niels Bohr Institute, University of Copenhagen, Denmark



Why should we verify hardware?

Ariane-5

4th June 1996

Why should we verify hardware?

Ariane-5

4th June 1996

Total failure on launch

Why should we verify hardware?

Ariane-5

4th June 1996

Total failure on launch

Converting a 64-bit floating point number to signed 16-bit integer.

Why should we verify hardware?

Ariane-5

4th June 1996

Total failure on launch

Converting a 64-bit floating point number to signed 16-bit integer.

Overflow caused the self-destruct mechanism in both primary and backup computer

Why should we verify hardware?

Ariane-5

4th June 1996

Total failure on launch

Converting a 64-bit floating point number to signed 16-bit integer.

Overflow caused the self-destruct mechanism in both primary and backup computer

No people where harmed

Why should we verify hardware?

The Patriot Missile Failure

25th February 1991 in the Persian Gulf war

Why should we verify hardware?

The Patriot Missile Failure

25th February 1991 in the Persian Gulf war

A Patriot missile failed to intercept an incomming ”Scud” which struck a U.S Army barracks, killing 28 soldiers.

Why should we verify hardware?

The Patriot Missile Failure

25th February 1991 in the Persian Gulf war

A Patriot missile failed to intercept an incomming ”Scud” which struck a U.S Army barracks, killing 28 soldiers.

A bug in the system’s weapons control computer caused an inaccurate tracking calculation. Conversion of time since last boot from an integer to a real number was performed using a 24 bit register.

Why should we verify hardware?

The Patriot Missile Failure

25th February 1991 in the Persian Gulf war

A Patriot missile failed to intercept an incomming ”Scud” which struck a U.S Army barracks, killing 28 soldiers.

A bug in the system’s weapons control computer caused an inaccurate tracking calculation. Conversion of time since last boot from an integer to a real number was performed using a 24 bit register.

Inaccurate results == missile misses target

What can SME do?

The SME model builds on the CSP algebra

SMEIL

You have just been introduced to SMEIL in the previous presentation

SMEIL

You have just been introduced to SMEIL in the previous presentation

We transpile from SMEIL to CSP$_M$
And then verify it in FDR4

SMEIL

You have just been introduced to SMEIL in the previous presentation

We transpile from SMEIL to CSP_M
And then verify it in FDR4

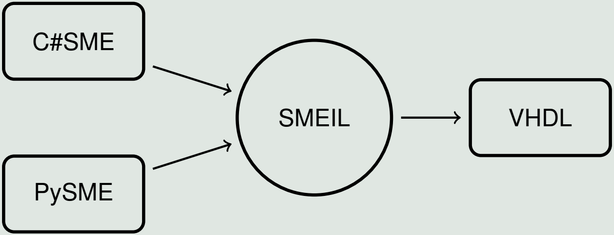


Figure. SMEIL transpiler structure.

Simple example

Seven Segment Display

Figure (Truls or something else?)

Seven Segment Display example

Write the seven segment circuit in SMEIL

Seven Segment Display example

Write the seven segment circuit in SMEIL

Transpile it to CSP_M

Seven Segment Display example

Write the seven segment circuit in SMEIL

Transpile it to CSP$_M$

Verify in FDR4

Simple example

What are we verifying

One seven segment example can only display the numbers 0-9.
4 bits can represent the data, but also more than needed.

Simple example

What are we verifying

One seven segment example can only display the numbers 0-9.
4 bits can represent the data, but also more than needed.

We can verify that the values communicated to the seven segment displays does not exceed the expected values.

Simple example

Seven Segments SMEIL Structure

SMEIL code

Simple example

Seven Segments SMEIL Structure

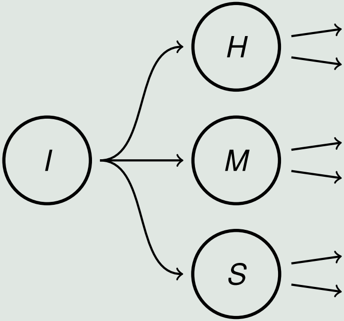


Figure. SMEIL network for a seven segment display clock. Each SMEIL process is represented by a cicle with a letter corresponding to the processes Input, Hours, Minutes and Seconds respectively.

CSPm process structure

Code example

Monitor process

Code example

Example continued

Run

All of the following CPU examples have been run on a Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz.

The GPGPU examples are run on GeForce GTX 680 (OpenCL C 1.1).

All examples were run 10 times and the average was measured.

Results - time to verify in FDR4?

The seven segment example have been run on a ...

The example were run x times and the average was measured.

Conclusion

Productivity and performance

....

Future work

DSL

....

Questions?

Comments?

Feel free to ask anything.