Verification of fault tolerant safety I&C systems using model checking

Antti Pakonen\textsuperscript{1}, Igor Buzhinsky\textsuperscript{2}

\textsuperscript{1}VTT Technical Research Centre of Finland Ltd.
\textsuperscript{2}Aalto University, Finland

20th IEEE International Conference on Industrial Technology (IEEE-ICIT2019)
Feb 13-15, 2019, Melbourne, Australia
I&C application logic verification

Model checking

100% exhaustive verification
VTT customer projects

**stuk**

Olkiluoto 3 (under construction)
- Evaluation of NPP I&C system designs 2008-2011
- Evaluation of Olkiluoto 3 Protection System 2015
- Evaluation of Olkiluoto 3 PACS 2015

**fortum**

Lovisa 1 & 2 I&C modernization
- Verification of nuclear automation 2009
- Verification of nuclear I&C in the LARA project 2012-2014
- Verification of nuclear I&C in the ELSA project 2016-2017

**FENNOVOIMA**

Hanhikivi 1 (decision-in-principle)
- Model checking of functional, architecture-level I&C 2016, 2018
Customer feedback

- “…a very effective method…”
- “…truly beneficial…”
- “…design changes have been made…”
- “The results are so remarkable…”
MODCHK

a graphical tool for I&C model checking

- Structural, composite models
- Verification with NuSMV 2.6.0
- Counterexample animation
Hardware + software verification
Case example: U.S. EPR PS

https://www.nrc.gov/docs/ML1326/ML13261A544.html
U.S. EPR PS architecture simplified
### SW+HW modelling efforts in 2014

<table>
<thead>
<tr>
<th>Hardware Components</th>
<th>Failure Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor module</td>
<td>Hang</td>
</tr>
<tr>
<td></td>
<td>Communication dropout</td>
</tr>
<tr>
<td></td>
<td>Delayed signal</td>
</tr>
<tr>
<td></td>
<td>Random behaviour</td>
</tr>
<tr>
<td>Analog Input Module</td>
<td>Signal fails high/low</td>
</tr>
<tr>
<td></td>
<td>Signal drifts</td>
</tr>
<tr>
<td></td>
<td>Signal hangs/freeze</td>
</tr>
<tr>
<td>Analog Input Module, Single channel</td>
<td>Signal fails high/low</td>
</tr>
<tr>
<td></td>
<td>Signal drifts</td>
</tr>
<tr>
<td></td>
<td>Signal hangs/freeze</td>
</tr>
<tr>
<td>Analog Output Module</td>
<td>Signal fails high/low</td>
</tr>
<tr>
<td></td>
<td>Signal drifts</td>
</tr>
<tr>
<td></td>
<td>Signal hangs/freeze</td>
</tr>
<tr>
<td>Analog Output Module, Single channel</td>
<td>Signal fails high/low</td>
</tr>
</tbody>
</table>

![Diagram showing different divisions (Div 1, Div 2, Div 3, Div 4) with various hardware components (APU 1, APU 2, APU 3, APU 4, ALU 1, ALU 2, ALU 3, ALU 4) and failure modes highlighted.](image)
MBSE: Related attempts

- The system model has to be kept very abstract.
  - Models based on "specified behavior", "functional model", etc.

- Typical model scales: $10^6 - 10^9$ states
- VTT’s SW-only models: $10^{20} - 10^{30}$ states
New approach in 2018

- Idea 1:
  - Focus on single failure

- Idea 2:
  - Utilise symmetry

- Idea 3:
  - Non-deterministic failures
Case example logic

SW-only model: $7,3 \cdot 10^{31}$ reachable states in NuSMV
### Case study results

Below is a table showing the model checking time (s) for different failure scenarios:

<table>
<thead>
<tr>
<th>Failure Scenario</th>
<th>LTL</th>
<th>CTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>No failure</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Single failure</td>
<td>38</td>
<td>7</td>
</tr>
</tbody>
</table>
## Case study results (cnt’d)

<table>
<thead>
<tr>
<th></th>
<th>BMC</th>
<th>LTL</th>
<th>CTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>No failure</td>
<td>98</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>No failure + comm. delay</td>
<td>117</td>
<td>--*</td>
<td>--*</td>
</tr>
<tr>
<td>Single failure</td>
<td>25125</td>
<td>38</td>
<td>7</td>
</tr>
<tr>
<td>Single failure + comm. delay</td>
<td>138</td>
<td>--*</td>
<td>--*</td>
</tr>
</tbody>
</table>

* Model checking time (s)

* terminated after 8 hours
Future research needs

- Communication delay, asynchrony?
- Automatic tool support?
- How to express properties?
Model checking – a well-established and integral I&C verification method in the Finnish nuclear industry!

https://www.vttresearch.com/modelchecking/