SAUNA
Integrated safety assessment and justification of nuclear power plant automation

SAFIR2018 Final seminar
21.-22.3., Hanasaari, Espoo
Challenge: Overall plant safety of I&C
Defence-in-Depth assessment?

- Complex, cross-disciplinary relationships

- Complex chains of failures
Common Systems Engineering models
Integration and co-use of methods
Finding novel methods
Highlight: Model checking

SYSTEM → SYSTEM MODEL → MODEL CHECKING
Does the model satisfy the property?

FORMAL PROPERTY

→ YES

→ NO

COUNTER EXAMPLE
VTT customer projects

**stuk**
- **OL3**
  - Evaluation of NPP I&C system designs 2008-2011
  - Evaluation of Olkiluoto 3 PACS 2015
  - Evaluation of Olkiluoto 3 Protection System 2015, 2019

**fortum**
- **ELSA**
  - 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**
- **FH-1**
  - Model checking of functional, architecture-level I&C 2016, 2018
Hardware + software verification
Hardware + software verification

Model checking time (s)

<table>
<thead>
<tr>
<th></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>
Model checking in SAUNA 2015-2018

https://github.com/igor-buzhinsky/nusmv_counterexample_visualizer

https://github.com/igor-buzhinsky/synthesis-aided-basic-block-assurance
Other highlights – see the Final Report!
Dissemination 2015-2018

- 1 doctoral thesis
- 2 master’s theses
- 3 journal articles
- 40 conference papers
- 17 research reports
- 6 workshops
Thank you SAFIR2018!