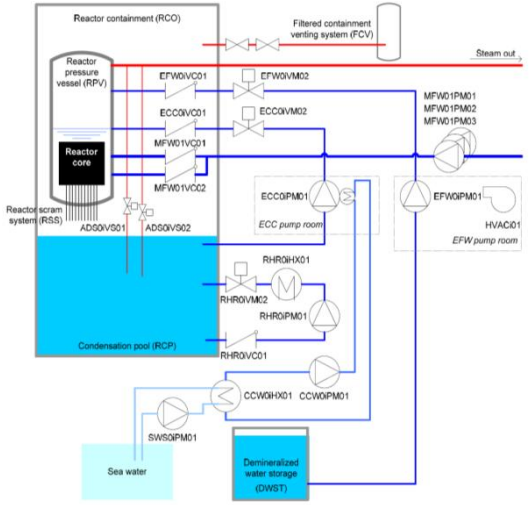


Safety evaluation and reliability analysis of nuclear automation (SARANA)

SAFIR2014 Final seminar 19.3.2015

Janne Valkonen, Kim Björkman, Jussi Lahtinen, Tero Tyrväinen, Antti Pakonen, Markus Porthin

VTT Technical Research Centre of Finland

Keijo Heljanko, Tuomas Kuismin, Kari Kähkönen, Antti Vanhala, Olli Saarikivi, Hernan Ponce de Leon, Siert Wieringa

Aalto University
School of Science

SARANA – Safety evaluation and reliability analysis of nuclear automation

- The objective of the SARANA project was to develop methods and tools for safety and reliability analysis of digital systems and utilize them in practical case studies
  - Four year project
  - Total volume (2011-2014): 1010,7 k€
  - VYR funding 576 k€
- Partners:
  - VTT, Aalto University
  - Through NKS DIGREL project:
    - Risk Pilot, Lloyd's Register

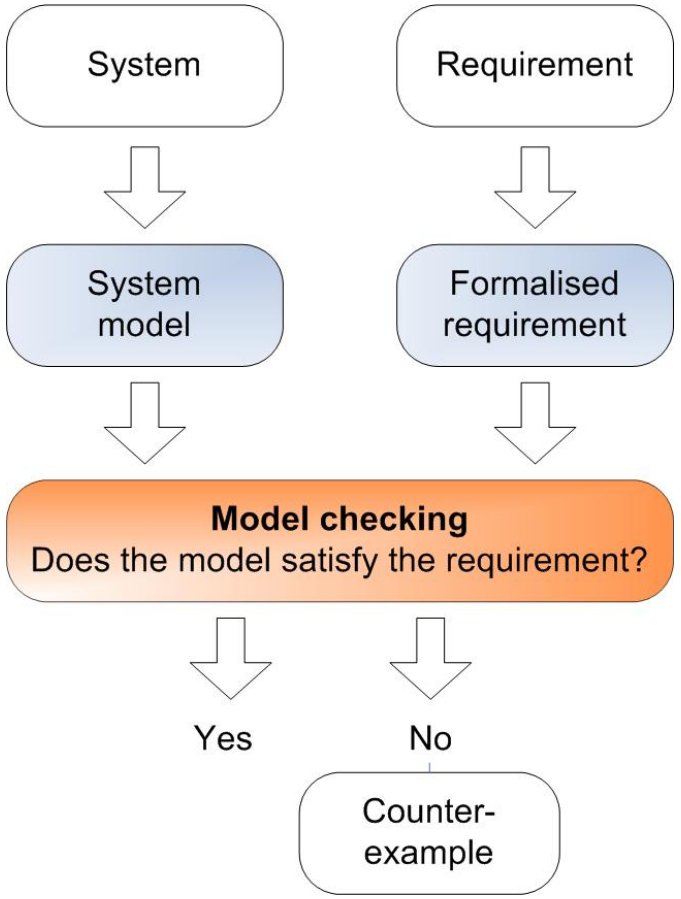
SARANA objectives

1. Reliability analysis:
   - Probabilistic risk assessment (PRA) of digital I&C
   - Dynamic flowgraph modelling
   - Finding synergy between reliability analysis methods and model checking

2. Extending the scope and scalability of the model checking method:
   - Larger systems and models
   - Hardware failures
   - Asynchronous system behaviour
   - Improving confidence

Model checking

- Model checking is an efficient formal method for the verification of critical systems.
- Can be applied to hardware / software. Our scope has been mainly in the design logic of systems.
- Models similar to simulation models
- Requirements formalised in temporal logic
- Unlike simulation or testing the model checking tool covers all behaviours of the model



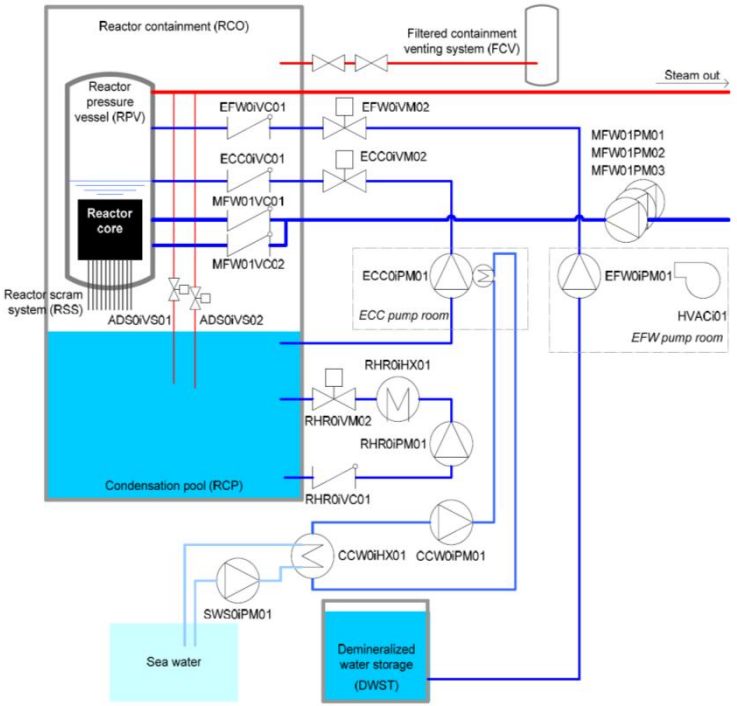
Aalto University
School of Science

SARANA – Main results

Reliability analysis of digital systems in PRA context

- International effort in developing guidelines to analyse and model digital systems in PRA context for nuclear power plants
- Main results:

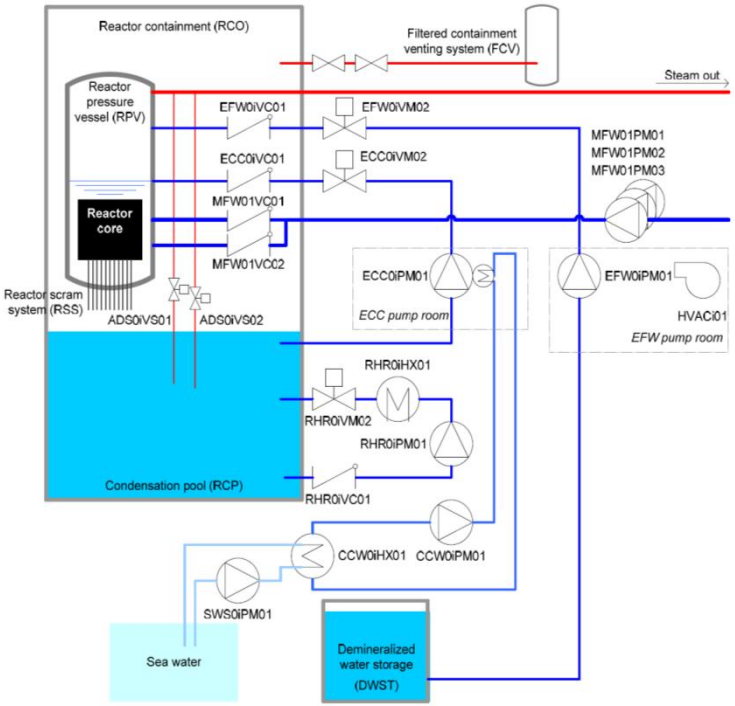
1. A taxonomy for failure modes of digital I&C systems was developed
2. A fictive digital I&C PRA model was developed for the demonstration and testing of modelling approaches
3. A method for the quantification of software reliability in the context of PRA was developed.



Aalto University
School of Science

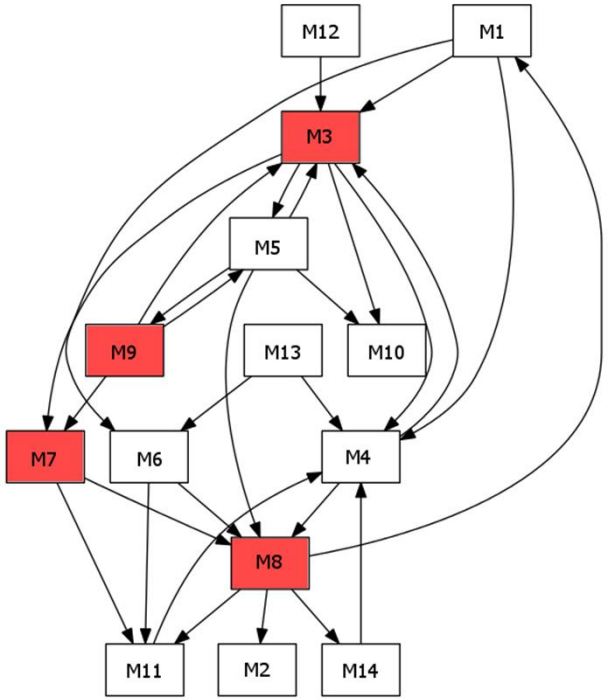
Verification of fault-tolerance using model checking

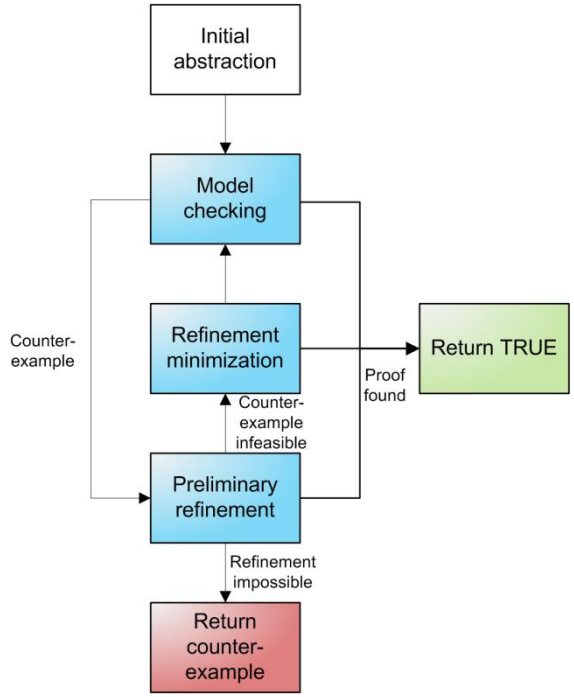
- Developed methodology for modelling hardware failures.
  - Closely follows PRA methodology for failures
  - Takes into account the detailed logic design of the systems
  - Enables the verification of **fault tolerance of the plant** using model checking
  - Spotting scenarios that are a combination of a hardware failure and a software error



Model checking large models

- The system can not be model checked as a whole
- An iterative algorithm for verifying system properties
  - A single property may be verified using only a small part of the whole model
  - The model is divided into modules
  - Look for a subset of the modules that is sufficient for proving the property
  - Outperforms traditional model checking techniques





Aalto University
School of Science

Improving Confidence in Model Checking

- Model checker can be buggy in two ways:
  - Incorrect counter-examples can be removed by simulation
  - Incorrectly missing a counter-example is dangerous!

- Improving confidence in model checking
  - Multiple tool chains with no common source code
    - Different model checking approaches a plus for added confidence
  - Efficient proof generating model checkers[1]

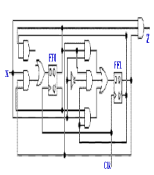
[1] Kuismin, T. and Heljanko, K.: Increasing Confidence in Liveness Model Checking Results with Proofs. In Proceedings of the 9th Haifa Verification Conference (HVC 2013), pages 32-43, Lecture Notes in Computer Science 8244, 2013.

Conclusions

Model checking timeline

Verification of digital I&C systems rely on testing and subjective “pen&paper” reviews

- 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | Now

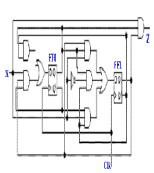


Model checking timeline

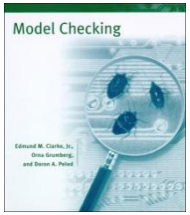
Verification of digital I&C systems rely on testing and subjective “pen&paper” reviews

SAFIR2010 / MODSAFE

- 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | Now



Methodology for model checking individual I&C systems

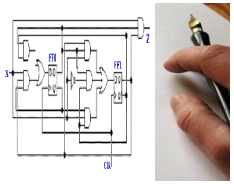


Model checking timeline

Verification of digital I&C systems rely on testing and subjective “pen&paper” reviews

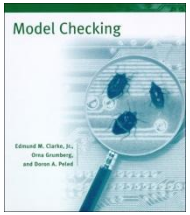
SAFIR2010 / MODSAFE

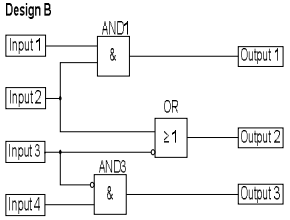
- 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | Now



Methodology for model checking individual I&C systems

Error-finding capabilities demonstrated in many case studies.





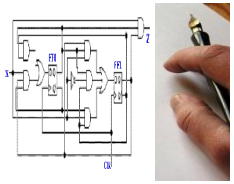
Model checking timeline

Verification of digital I&C systems rely on testing and subjective “pen&paper” reviews

Feasibility and benefits of model checking demonstrated.

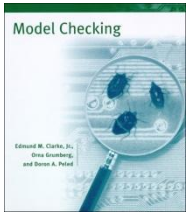
SAFIR2010 / MODSAFE

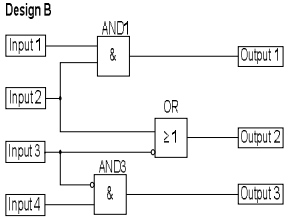
- 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | Now



Methodology for model checking individual I&C systems

Error-finding capabilities demonstrated in many case studies.





Aalto University
School of Science

Model checking timeline

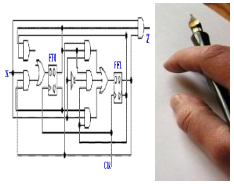
Verification of digital I&C systems rely on testing and subjective “pen&paper” reviews

Feasibility and benefits of model checking demonstrated.

SAFIR2010 / MODSAFE

SAFIR2014 / SARANA

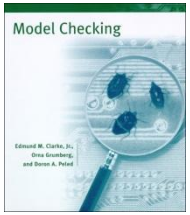
- 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | Now

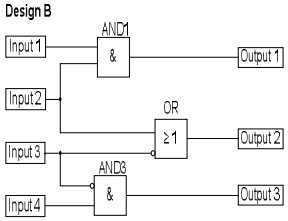


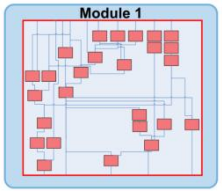
Methodology for model checking individual I&C systems

Error-finding capabilities demonstrated in many case studies.

Focus on verification of larger system models







Aalto University
School of Science

Model checking timeline

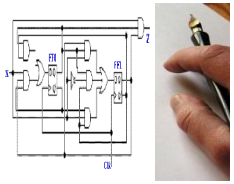
Verification of digital I&C systems rely on testing and subjective “pen&paper” reviews

Feasibility and benefits of model checking demonstrated.

SAFIR2010 / MODSAFE

SAFIR2014 / SARANA

- 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | Now

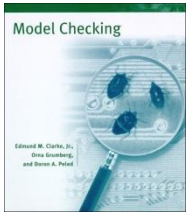


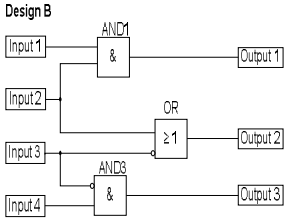
Methodology for model checking individual I&C systems

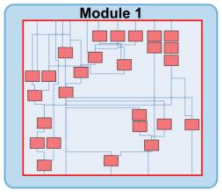
Error-finding capabilities demonstrated in many case studies.

Focus on verification of larger system models

Improving confidence in model checking







Model checking timeline

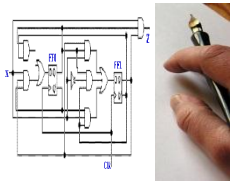
Verification of digital I&C systems rely on testing and subjective “pen&paper” reviews

Feasibility and benefits of model checking demonstrated.

SAFIR2010 / MODSAFE

SAFIR2014 / SARANA

- 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | Now



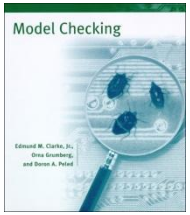
Methodology for model checking individual I&C systems

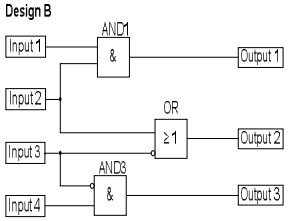
Error-finding capabilities demonstrated in many case studies.

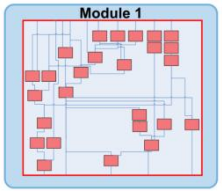
Focus on verification of larger system models

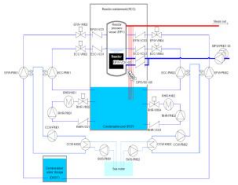
Improving confidence in model checking

Utilising PRA data sheets for model checking









Aalto University
School of Science

Model checking timeline

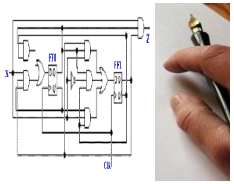
Verification of digital I&C systems rely on testing and subjective “pen&paper” reviews

Feasibility and benefits of model checking demonstrated.

Extended scalability and scope of applicability of model checking

SAFIR2010 / MODSAFE | SAFIR2014 / SARANA | SAFIR2018 / SAUNA

- 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | Now



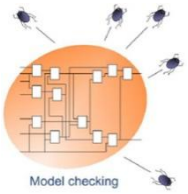
Methodology for model checking individual I&C systems

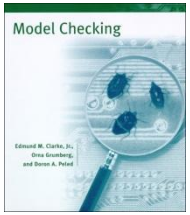
Error-finding capabilities demonstrated in many case studies.

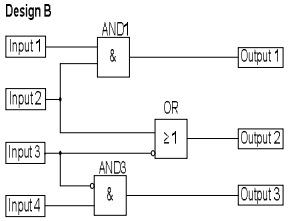
Focus on verification of larger system models

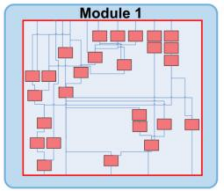
Improving confidence in model checking

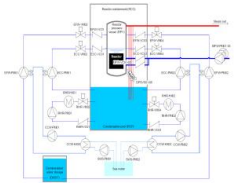
Utilising PRA data sheets for model checking











Aalto University
School of Science

Impact of research

- Model checking has become a well-established and integral part of the software verification processes used in the Finnish nuclear industry

- Fortum LARA project:
  - Model checking was used to verify the correct functionality of application I&C software in LARA subsystems

- Olkiluoto 3 project:
  - Evaluation of I&C system functions commissioned by STUK