Safety evaluation and reliability analysis of nuclear automation

Presentation of the SARANA project in SAFIR2014 Interim Seminar, March 21–22, 2013

Presented by Keijo Heljanko (keijo.heljanko@aalto.fi)

Project group

VTT: Janne Valkonen, Kim Björkman, Jan-Erik Holmberg, Jussi Lahtinen, Antti Pakonen, Tero Tyrväinen

Aalto University: Keijo Heljanko, Tuomas Kuismin, Siert Wieringa

Aalto University

Contents

1. Starting point, objectives
2. Model checking
3. Digital systems reliability analysis
4. Future challenges

Starting point

- Digitalization of nuclear Instrumentation&Control (I&C) systems
- Challenges in Verification&Validation (V&V)
- Relies heavily on subjective evaluation

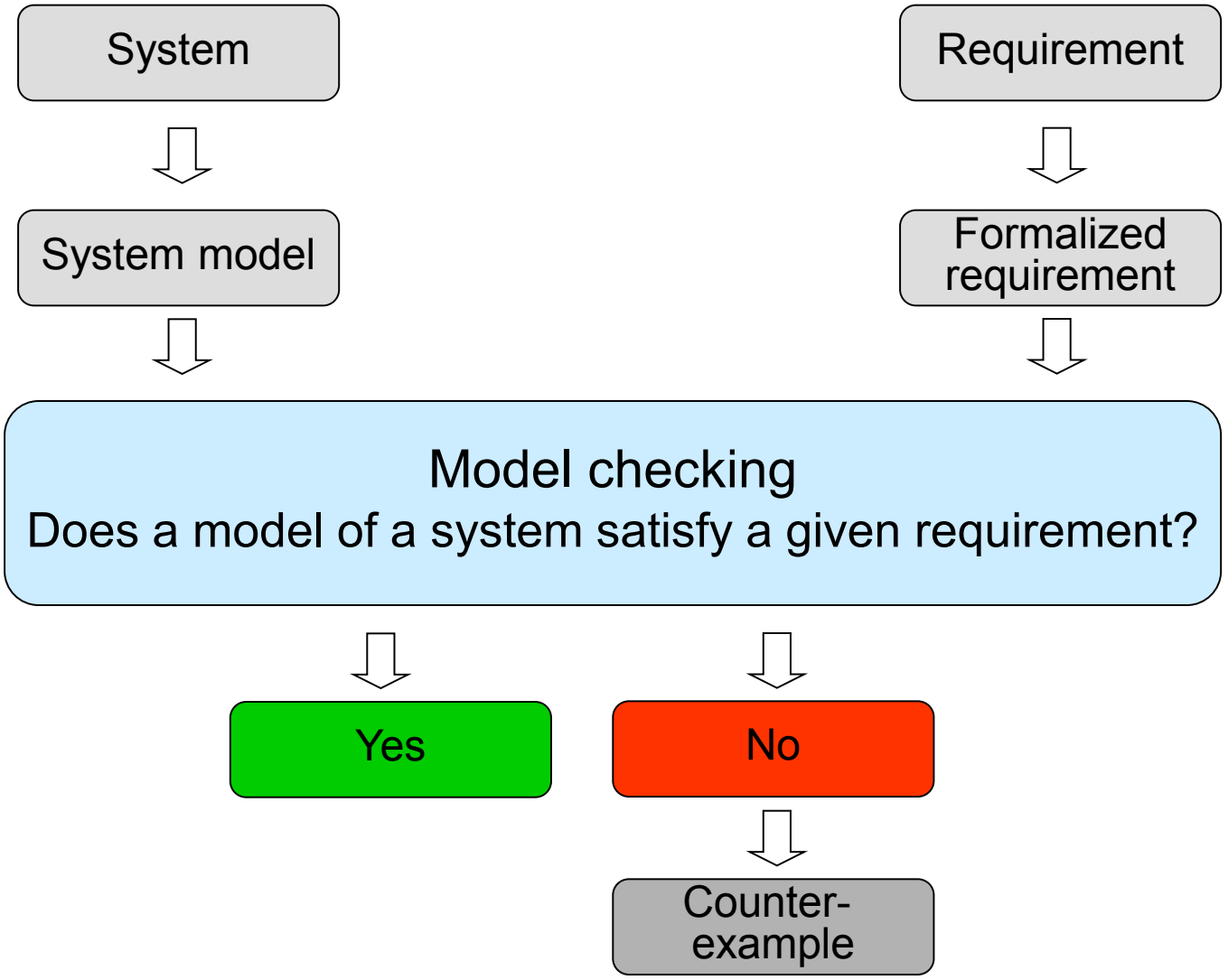
- Traditional methods such as testing and simulation:
  - Used late in the development cycle
  - Cover only a limited part of the possible system behaviour
  - Defining test scenarios and implementing them is challenging

➔ Testing and simulation alone are inadequate to produce sufficient evidence of correct functioning of safety critical systems in all possible scenarios

Objectives

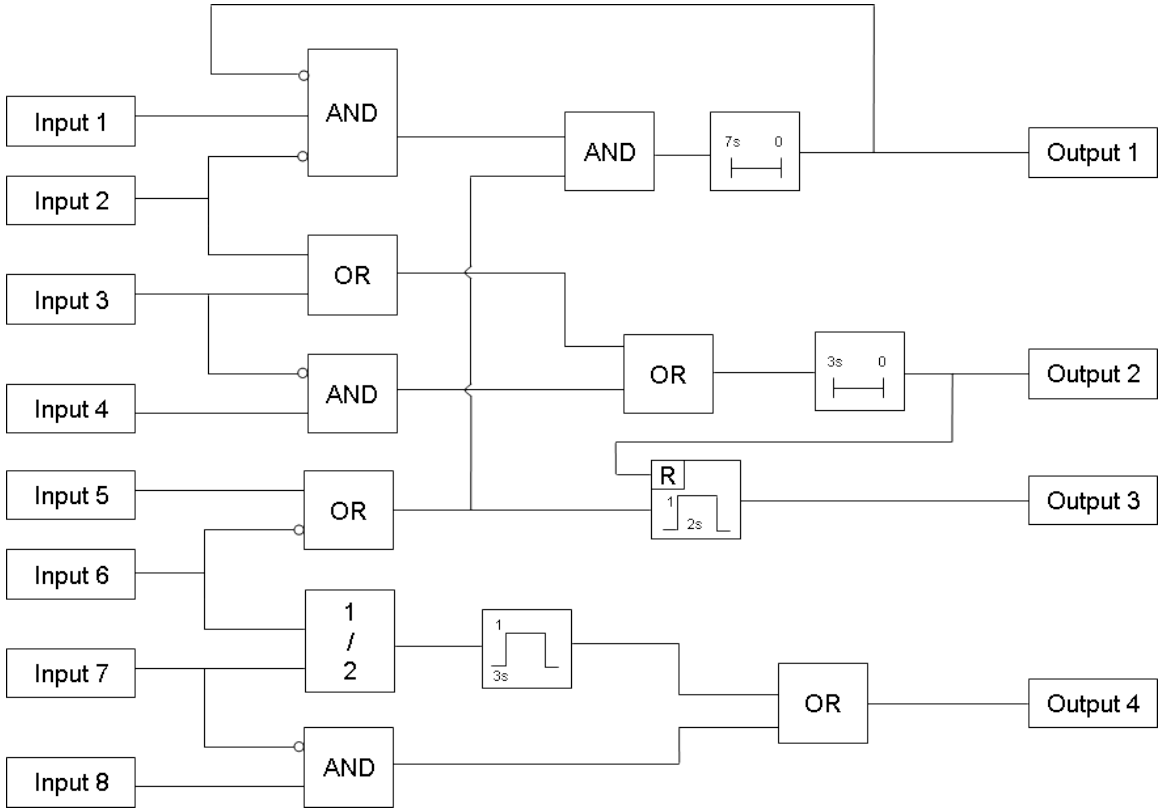
- Develop methods and procedures for model-based safety evaluation and reliability assessment of NPP automation.
- Apply the methods in selected case studies
- Evaluate the suitability of the methods for critical NPP automation analysis
- Practical utilization

What is model checking?



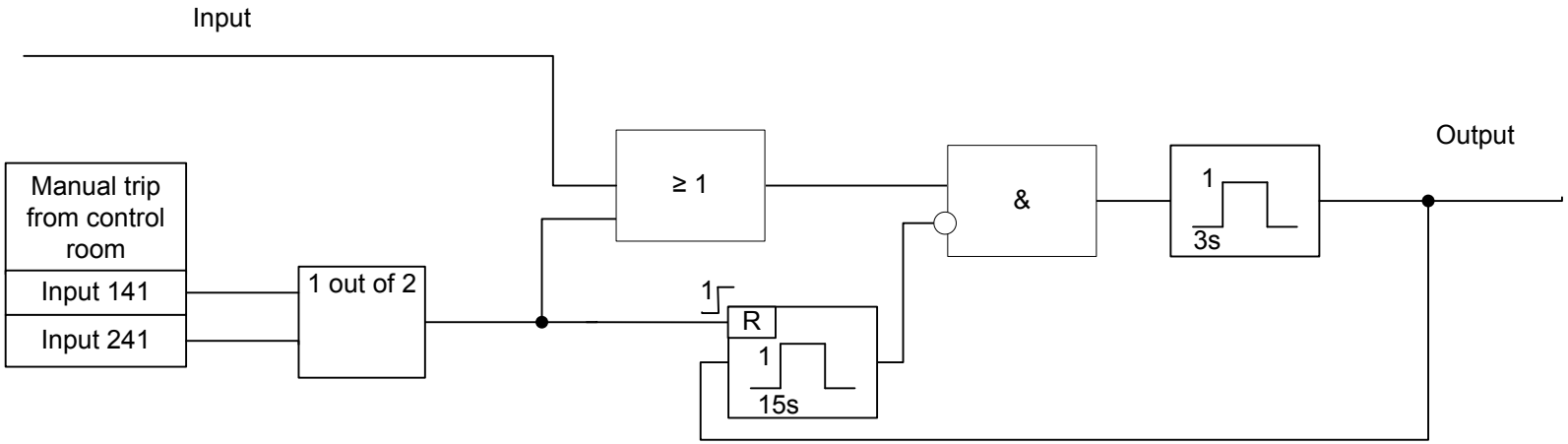
Large state spaces

- Typical logical circuits of safety critical automation systems contain delays, feedback loops and timers
- State spaces grow easily beyond 10^{10} even in designs that look rather simple



➔ Extensive verification manually or by testing and simulation becomes practically impossible

Formulation of properties



Test scenarios (are these sufficient ?):

- *Input = 1, but changes to 0 after 20 seconds*
- *Input = 1 and operator trips manually when the 15 second pulse has been running **6** seconds*
- *Input = 1 and operator trips manually when the 15 second pulse has been running **2** seconds*

Scenario for model checking

- *"In all possible cases when the Input = 1, Output finally gets value 1"*

Aalto University

Typical types of design errors

- Normal mode of operation is usually well tested and working
- Errors are usually found in corner cases: Scenarios that are difficult to take into account in test planning
  - Errors after subsystem re-initializations
  - Timing scenarios where multiple events happen simultaneously
  - Several improbable events occur simultaneously
  - Unexpected operator or maintenance actions

Model Checking Achievements in SARANA

- Exhaustive analysis of system models containing large state spaces, over 10^{20} states
- Improving automated tools that check timing-related behaviors
- Using two independent model checker tool chains to get more confidence in the results from both
- Developing automated, compositional model checking methodology for analysing large designs
- A success in technology transfer in SAFIR: From a research project to practical utilization

Reliability analysis of digital systems

- General objective is to provide guidelines to analyse and model digital systems in Probabilistic Risk Analysis (PRA) context
- Finalization of the digital Instrumentation&Control (I&C) failure modes taxonomy (OECD/NEA WGRISK's task DIGREL), VTT is task leader
- Suitable level of detail for an I&C architecture model will be investigated
- Modelling and quantification of software faults

Dynamic flowgraph methodology

- DFM is an approach for reliability assessment of systems with time dependencies and feedback loops
- YADRAT tool developed at VTT for analysing DFM models
- YADRAT models can be translated into models for the NuSMV model checker
- Improved algorithms to solve DFM models
- Computing importance measures and modeling common cause failures

Remaining challenges

- Minimizing human effort in modelling and interpreting analysis results
- Scalability of the methods to larger real world systems
- Methodology for expressing requirements formally but still in a light weight fashion
- Software reliability analysis is still a challenge
- Integration of the methods with e.g., traditional testing and simulation based approaches

Aalto University

Publications

1. Launiainen, T., Heljanko, K., and Junttila, T.: Efficient Model Checking of PSL Safety Properties. IET Computers & Digital Techniques 5(6):479-492, 2011. (doi: 10.1049/iet-cdt.2010.0154).
2. Dubrovin, J., Junttila, T., and Heljanko, K.: Exploiting Step Semantics for Efficient Bounded Model Checking of Asynchronous Systems. Science of Computer Programming, article in press. (doi: 10.1016/j.scico.2011.07.005).
3. Stefan Authén, Jan-Erik Holmberg, Failure modes taxonomy for digital I&C systems — common framework for PSA and I&C experts, in Proc. of Nordic PSA Conference – Castle Meeting 2011, 5–6 September 2011, Johannesberg Castle, Sweden
4. Kim Björkman, Ilkka Karanta, A dynamic flowgraph methodology approach based on binary decision diagrams, in Proc. of 2011 International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA 2011), Wilmington, NC, USA 13 - 17 March 2011
5. Gan, X., Dubrovin, J. and Heljanko, K.: A Symbolic Model Checking Approach to Verifying Satellite Onboard Software. In Proceedings of the 11th International Workshop on Automated Verification of Critical Systems (AVoCS 2011), Newcastle, UK, September 2011, accepted for publication.
6. Jussi Lahtinen, Tuomas Launiainen, Keijo Heljanko, Jonatan Ropponen, Model Checking Methodology for Large Systems, Faults and Asynchronous Behaviour,
7. Yvonne Adolfsson, Jan Erik Holmberg, Göran Hultqvist, Pavel Kudinov, Ilkka Männistö, DPSA - Deterministic/Probabilistic Safety Analysis workshop proceedings, October 3-5, 2011, Espoo
8. Janne Valkonen, Kim Björkman, Antti Pakonen, Applicability of safety and reliability analysis methods for critical I&C systems in nuclear power plants, SARANA work report 2011
9. Guidelines for reliability analysis of digital systems in PRA context, interim report to be published in NKS series (Stefan Authén, Johan Gustafsson, Jan-Erik Holmberg)
10. Proceedings of the NKS/WGRISK DIGREL seminar, "Development of best practice guidelines on failure modes taxonomy for reliability assessment of digital I&C systems for PSA", October 25, 2011
11. Use of IEC 61508 in Nuclear Applications Regarding Software Reliability — Pre-study, VTT-R-09293-11 (Kim Björkman, Ola Bäckström, Jan-Erik Holmberg)
12. Janne Kauttio, Keijo Heljanko, State-of-the-art report on probabilistic model checking and its applicability to critical I&C systems analysis, SARANA work report 2011
13. Tero Tyrväinen, Master's Thesis: Risk Importance Measures and Common Cause Failures in Dynamic Flowgraph Methodology
14. Barnat, J. and Heljanko, K. (eds.): Proceedings 10th International Workshop on Parallel and Distributed Methods in verifiCation. Electronic Proceedings in Theoretical Computer Science 72, Electronic Proceedings in Theoretical Computer Science, 2011. (doi: 10.4204/EPTCS.72)
15. Authén, Stefan; Holmberg, Jan-Erik. 2012. Reliability analysis of digital systems in a probabilistic risk analysis for nuclear power plants. Nuclear Engineering and Technology, vol. 44, 5, ss. 471 – 482, doi:10.5516/NET.03.2012.707 http://article.nuclear.or.kr/jknsfile/v44/JK0440471.pdf
16. Dubrovin, Jori; Junttila, Tommi; Heljanko, Keijo: Exploiting Step Semantics for Efficient Bounded Model Checking of Asynchronous Systems. Science of Computer Programming 77(10-11):1095-1121, 2012. http://dx.doi.org/10.1016/j.scico.2011.07.005
17. Lahtinen, Jussi; Valkonen, Janne; Björkman, Kim; Frits, J.; Niemelä, I.; Heljanko, K.. 2012. Model checking of safety-critical software in the nuclear engineering domain. Reliability Engineering and System Safety. Elsevier, vol. 105, Special Issue ESREL 2010, ss. 104 – 113. doi:10.1016/j.ress.2012.03.021
18. Kim Björkman, Solving dynamic flowgraph methodology models using binary decision diagrams, Reliability Engineering & System Safety, Volume 111, March 2013, Pages 206-216. http://dx.doi.org/10.1016/j.ress.2012.11.009
19. Piljugin, Ewgenij; Authén, Stefan; Holmberg, Jan-Erik. 2012. Proposal for the taxonomy of failure modes of digital system hardware for PSA. 11th International Probabilistic Safety Assessment and Management Conference & The Annual EuropeanSafety and Reliability Conference. International Association for Probabilistic Safety Assessment and Management (IAPSAM); European Safety and Reliability Association (ESRA), ss. 10-TH4-3. PSAM11/ESREL2012, Helsinki, 25 – 29.6.2012. http://www.vtt.fi/inf/julkaisut/muut/2012/10-Th4-3.pdf

Publications

20. Holmberg, Jan-Erik; Authén, Stefan; Amri, Abdallah. 2012. Development of best practice guidelines on failure modes taxonomy for reliability assessment of digital I&C systems for PSA. 11th International Probabilistic Safety Assessment andManagement Conference & The Annual European Safety and Reliability Conference. International Association for Probabilistic Safety Assessment and Management (IAPSAM); European Safety and Reliability Association (ESRA), ss. 10-TH4-1. PSAM11/ESREL2012,Helsinki, 25 – 29.6.2012. http://www.vtt.fi/inf/julkaisut/muut/2012/10-Th4-1.pdf
21. Holmberg, Jan-Erik; Authen, S.; Amri, A.; Sedlak, J.; Thuy, N.. 2012. Best practice guidelines on failure modes taxonomy for reliability assessment of digital I&C systems for PRA. 8th International Topical Meeting on Nuclear PlantInstrumentation, Control and Human Machine Interface Technologies, NPIC & HMIT 2012, 22 - 26 July 2012, San Diego, CA. American Nuclear Society, ss. 724 – 732
22. Bäckström, Ola; Holmberg, Jan-Erik. 2012. Use of IEC 61508 in nuclear applications regarding software reliability. 11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and ReliabilityConference. International Association for Probabilistic Safety Assessment and Management (IAPSAM); European Safety and Reliability Association (ESRA), ss. 10-TH2-4. PSAM11/ESREL2012, Helsinki, 25 – 29.6.2012. http://www.vtt.fi/inf/julkaisut/muut/2012/10-Th2-4.pdf
23. Pakonen, Antti; Mätäsniemi, Teemu; Valkonen, Janne. 2012. Model checking reveals hidden errors in safety-critical I&C software. 8th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine InterfaceTechnologies (NPIC & HMIT 2012), San Diego, California, USA, 22 - 26 July 2012. American Nuclear Society, ss. 1823 – 1834 http://www.vtt.fi/inf/julkaisut/muut/2012/NPIC-HMIT_2012_Pakonen_et_al.pdf
24. Lahtinen, Jussi; Björkman, Kim; Valkonen, Janne; Niemelä, I.. 2012. Emergency diesel generator control system verification by model checking and compositional minimization. Proceedings, ss. 49 - 60. 8th Doctoral Workshop on Mathematicaland Engineering Methods in Computer Science (MEMICS 2012), Znojmo, Czech Republic, 25 - 28 October 2012.
25. Gan, Xiang; Dubrovin, Jori; Heljanko, Keijo: A Symbolic Model Checking Approach to Verifying Satellite Onboard Software. In Proceedings of the 11th International Workshop on Automated Verification of Critical Systems, Newcastle, UK. Electronic Communications of the EASST 46, pages 1-15, 2012.