Raidelogiikoiden formaali verifiointi

Antti Pakonen
antti.pakonen@vtt.fi
ASAF Teemapäivä
Pasila 8.11.2022

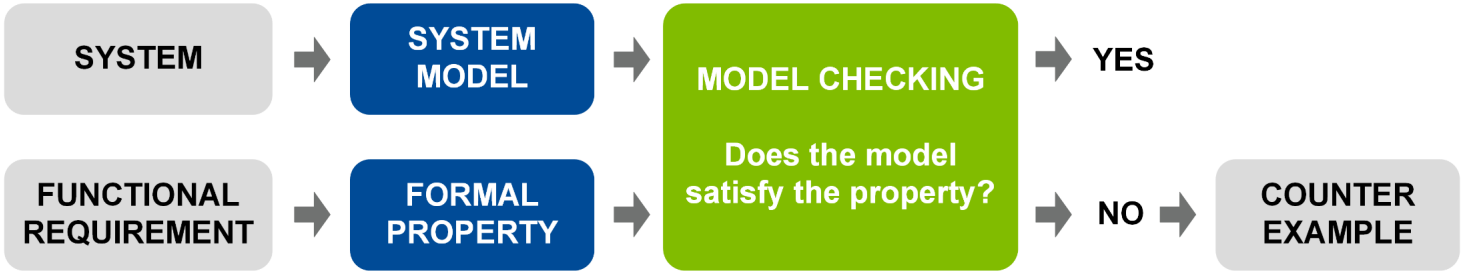
Proving the negative?

“The signaling device shall not give incorrect information.”

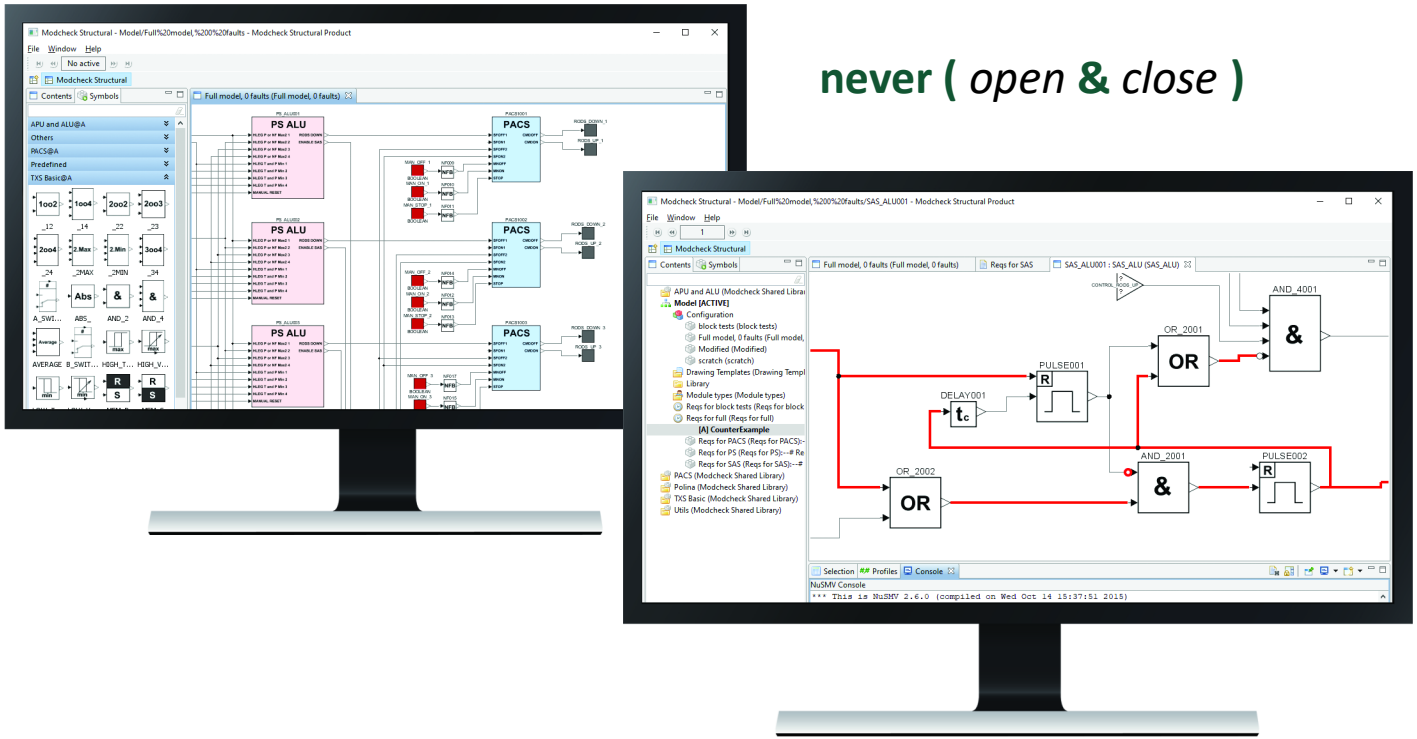
"The switch shall not direct train to a reserved track section.”

"The level crossing barrier shall never be raised when a train is at the level crossing or approaching within a certain distance.”

Model checking

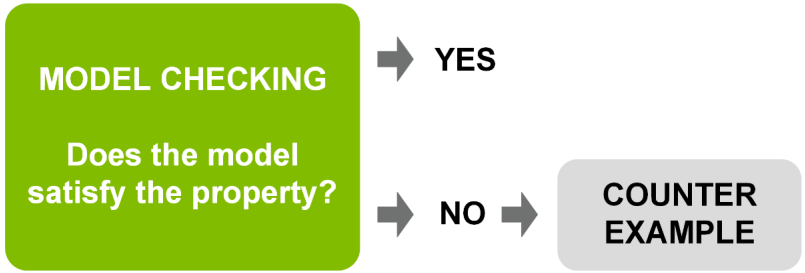


- 100% exhaustive verification
- **Mathematical proof of correctness**

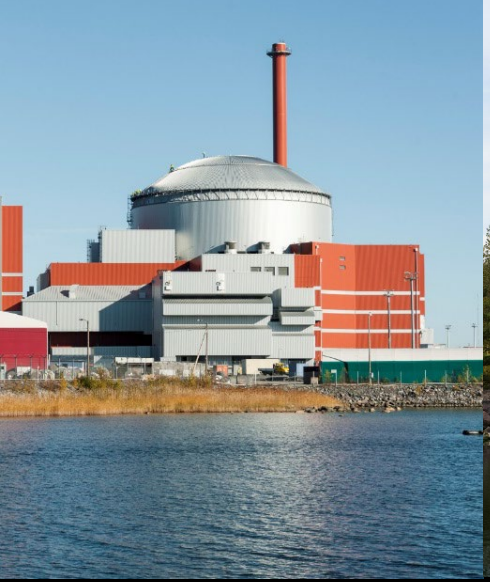


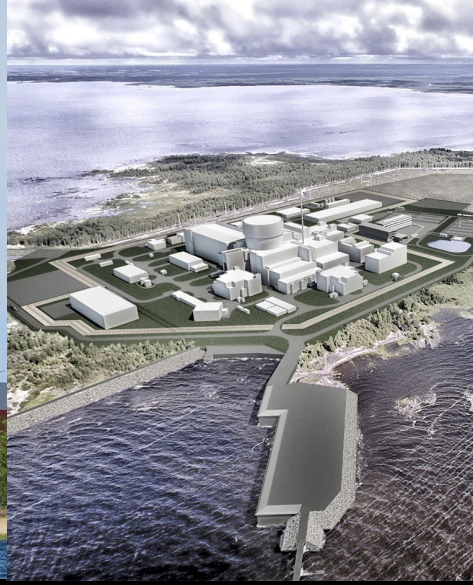
never (*open* & *close*)

Mistakes?



- always (*criteria* -> *trip*) NO
- always {(*criteria*) *[*5]* |-> { *trip* }! NO
- always {(*criteria* & ! *reset*) *[*5]* |-> { *trip* }! NO
- always {! *trip* ; (*criteria* & ! *reset*) *[*5]* |-> { *trip* }! YES



stuk

fortum

tvo

FENNOVOIMA

”…a **very effective method**…”

”…found issues which would **otherwise have been left undetected**…”

”…**truly beneficial**...”

”The results are **remarkable**.”

75 confirmed design issues!

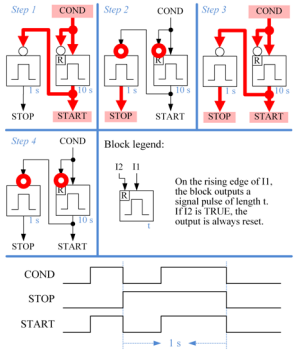
- Spurious actuation of safety function **may lead to leak of radionuclides**
- Spurious actuation of safety functions **reduces options for controlling accident**
- **System remains in non-safe state** after initiating event
- **Safety function lost** due to exceptional state of delay processing in I&C logic
- Component protection failure may lead to **loss of safety function** later
- …

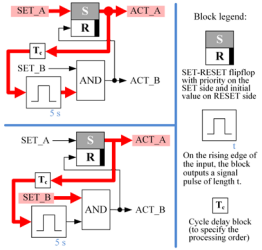
- Periodic test fails, no effect on plant operation
- Plant remains in safe state, exceptional state of I&C logic due to maintenance action
- Testing logic of preventive functions fails
- Short equipment transient due to test, plant remains in safe state
- 2-out-of-4 voting reduced to 2-out-of-3 vote
- Inaccuracy in specification
- …

NOTE: Analysis performed by VTT experts. See disclaimers in:
A. Helminen, A. Pakonen: Potential applications of model checking in probabilistic risk assessments, VTT Research Report VTT-R-00017-20

Statistics & examples

- A. Pakonen: "**Oops! Examples of I&C design issues detected with model checking**"
- *International Symposium on Future I&C for Nuclear Power Plants (ISOFIC 2021), Okayama, Japan, 15.-17.11.2021*





"What is "Oops!" in the title of the paper? Is it the name of the method or procedure the author proposes? If there is no meaning, it is desirable to avoid to use the word for the title of technical papers."

- Reviewer 1

Railway projects

MIPRO

- Pilot 6/2020
- **Point control logic** 12/2020-1/2021
- **Route locking logic** 7/2021-2/2022
  - Point
  - Main signal
  - Shunting signal
  - Track
  - Diamond crossing

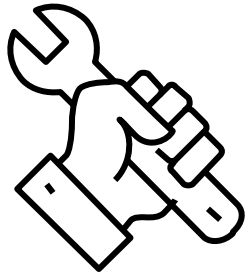
Detected issues

- **Several logic design issues**
  - Issues valid for (sub)functions of the overall signalling device logic, not necessarily valid for the system as a whole
  - Improvements & fixes ➔ **logics re-verified**
- **Inaccuracy / errors in requirement specifications**
  - Improvements & fixes ➔ **properties re-verified**
- **Unnecessary complexity in design**

Fast & easy solution iteration

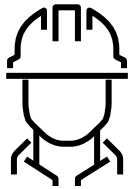
Mipro views on model checking

- ”The **benefit of model checking** over other methods is that manual review of complex functions is challenging, and testing cannot cover every possible scenario.”
- ”A challenge is to specify the requirements so that they support formal verification. The focus needs to be on the same level of hierarchy (system / function / sub-function).”



“We have utilised VTT's model checking as one method at Mipro to ensure the safety of the interlocking device. **The method is well suited for locating design errors and has helped us to improve railway safety**.”

Kari Haapala, Chief Technology Officer, Mipro



Safety & reliability

- Less (hidden) flaws in logic
- Increased product reliability

Higher performance for R&D and projects

- Fast and easy solution iteration
- Better time-management & on-time delivery
- Streamlined regulator approval
- Faster customer acceptance

VTT

beyond
the obvious

Antti Pakonen
antti.pakonen@vtt.fi
+358 40 129 2785

@VTTFinland

www.vtt.fi