Model checking of I&C software in the Loviisa NPP automation renewal project

Antti Pakonen, Janne Valkonen
VTT Technical Research Centre of Finland Ltd, P.O. Box 1000, FI-02044 VTT, Finland
Tel: +358 20 722 6783, E-mail: antti.pakonen@vtt.fi, janne.valkonen@vtt.fi, http://www.vtt.fi/

Sami Matinaho, Markus Hartikainen
Fortum Power and Heat, P.O. Box 1, FI-00048 FORTUM, Finland
Tel: +358 10 4511, E-mail: sami.matinaho@fortum.com, markus.hartikainen@fortum.com,
http://www.fortum.com

KEY WORDS model checking, verification and validation, digital I&C, nuclear power

ABSTRACT

Model checking is a formal method for verifying hardware and software designs. A software tool called a model checker is used to exhaustively verify that a system model fulfils stated properties. The exhaustiveness means that design errors can be found in systems that have already undergone V&V based on more traditional methods like testing and simulation.

In this paper, we discuss the application of model checking in the verification of instrumentation and control (I&C) application software. As a practical example, we look at the third party verification service VTT has provided for Fortum in the Loviisa nuclear power plant automation renewal project. We also introduce the tools developed by VTT and Fortum for the model checking of I&C software based on function block diagrams.

The experience of VTT (and others) has shown that the method is very powerful in the evaluation of function block based control software, particularly in safety-critical applications. Indeed, in Finland, model checking is already a well-established part of nuclear industry practices, as VTT has been evaluating the I&C systems of the Olkiluoto 3 plant for STUK, as well as supporting Fortum in the licensing of renewed systems for Loviisa.

Fortum has also cooperated with VTT on the development of model checking tools. A graphical toolset based on the open source modelling and simulation platform Simantics has already been put to use in VTT projects. A long term objective is the commercialisation of the tools as part of the Apros product family, as well as integration into different engineering and modelling tools.

1 INTRODUCTION

A modern digital I&C system is a complex entity. Verification of design solutions can be quite challenging, as reviews, testing, and simulation – proven and valuable methods as they are – cannot provide a 100% guarantee that the systems are error-free. Given the complexity of typical I&C functions, the traditional wisdom is that no such guarantees can be granted.

In selected domains, however, formal methods have made a breakthrough in verification. After decades of work on the algorithms behind techniques such as model checking, as well as the exponential growth of available processing power, microprocessors are being designed and exhaustively verified, with less emphasis on testing. Control system software is usually more complex, but similar methods can still be applied.

2 MODEL CHECKING OF I&C APPLICATION SOFTWARE

Model checking /1/ is a formal, computer-assisted verification method that can exhaustively prove that a certain type of model of a (software or hardware) system fulfils stated properties. A model checker is a software tool that is used to verify that no model state or execution violates a property. Properties can take the form of liveness ("a good thing always happens") or safety properties ("a bad thing never happens"). If a model execution contrary to a stated property is found, it is returned as a counterexample (error trace), the analysis of which can then reveal a design error. What sets model checking apart from more conventional methods is the exhaustive analysis (all possible scenarios are taken into account), and particularly the ability to evaluate safety properties, both of which are practically impossible if verification is only based on testing, for example.

Model checkers, such as the open source tool NuSMV (http://nusmv.fbk.eu/), take as input the system model (typically expressed as a type of finite state model), and formalised properties (stated using temporal logic languages such as Linear Temporal Logic (LTL), Computation Tree Logic (LTL), or Property Specification Language (PSL)). The computational power is based on the relative simplicity of the modelling language, and symbolic verification, where large numbers of states are processed at a single step /1/.

Hardware model checking has been commonplace since the 1990s, and is nowadays an integral part of the commercial microprocessor manufacturers' design process. Software model checking has gained ground in the 2000s, also in the I&C domain. In Finland, VTT has been studying the use of model checking in the nuclear domain with Aalto University /3/. After early success in industrial pilot cases, the method has been put to practical use. Currently, for example, VTT uses model checking to evaluate the design of I&C functions of the Olkiluoto 3 nuclear power plant, on commission from STUK.

Due to the simplicity of the modelling languages, model checking can only be effectively applied to systems that can easily be expressed in discrete terms. For I&C software expressed as function block diagrams, this means that arithmetically complex control loops (e.g., PID) cannot be evaluated. Still, the method scales very well in the context of binary circuits, and aspects such as simple math, discretisation of analogue values, and complex timing can also be handled /4,5/.

3 MODEL CHECKING IN THE LOVIISA AUTOMATION RENEWAL PROJECT

3.1 LARA project background

The Loviisa nuclear power plant, operated by Fortum, includes two pressurised water reactors of the type VVER-440, with a joint capacity of 976 MW. The old I&C systems are based on Russian and German technology from the 1970s. Despite aging of systems had not yet caused any significant problems, Fortum decided in the early 2000s to start preparing the automation renewal project (LARA), due to concerns over the future availability of spare parts and maintenance. In LARA, the new systems were to be delivered by a consortium of AREVA and Siemens, with safety I&C based on TELEPERM XS technology.

The Finnish Regulatory Guides on nuclear safety (YVL guides) state that "with systems […] of considerable safety significance, a safety assessment shall be carried out by an independent third-party organisation" /5/. In part to address such requirements, VTT was commissioned by Fortum to provide a third-party verification service of safety-classified I&C systems in LARA, based on model checking.

3.2 Model checking in LARA

Verification covered selected I&C functions of several LARA subsystems, including reactor protection, preventive protection, and emergency generator functions /5/. The task was parallel with module level system software tests carried out by the system vendor. The work process consisted of a series of work phases, some of which included Fortum's input (Figure 1).

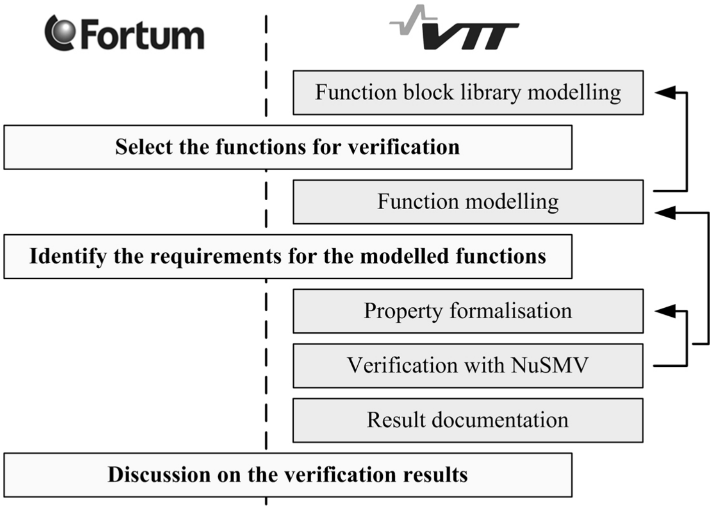
Fortum
VTT
Function block library modelling
Select the functions for verification
Function modelling
Identify the requirements for the modelled functions
Property formalisation
Verification with NuSMV
Result documentation
Discussion on the verification results

Figure 1. The work process in the LARA project called for the expertise of both VTT and Fortum.

A library of model components representing the set of elementary function blocks was first constructed by VTT. The model checker could also be used to verify that the function block models (based on functional block descriptions, as the source codes were not available) were correct. It was then up to Fortum to select the functions for verification, based primarily on their safety relevance, complexity, and applicability for model checking. VTT experts provided comments and recommendations related to the applicability, in particular. The modelling of the functions was then performed by VTT by connecting elementary function block components to reproduce the original diagrams /4/.

The next phase was identifying requirements for the modelled functions. The starting point could be a textual requirement specification document, or other kind of functional description. Since model checking calls for very strict formalisation, there was sometimes a need to further elaborate the requirements, which meant that Fortum's participation was crucial. One of the aspects specific to a renewal project is that it is often the licensee (plant operator) – not the system vendor – that has the best knowledge of the plant-specific requirements. The properties were then formalised by VTT experts, using languages such as LTL, CTL and PSL.

Verification was then performed using the NuSMV model checker. In the case that a counterexample generated by NuSMV turned out to be a symptom of an error in the function block model, the function model, or a formalised property, earlier work phases were revisited to fix any errors. Potential design issues were reported in sufficient detail for Fortum experts to reproduce the counterexample scenario, and estimate the safety relevance.

Finally, VTT was to prepare a verification report – identifying the method and tools, the target system, the list of documents used in constructing the model and identifying the requirements, and the list of verified requirements – that Fortum could have then submitted to the regulator (STUK) as part of subsystem licencing. However, due to delays in project implementation, Fortum decided to discontinue the LARA project in May 2014.

3.3 Results and future work

According to Fortum, model checking is a rigorous method for verifying complex I&C designs. The key benefit is naturally exhaustive verification, covering all possible signal sequences. As an example, events occurring within very small time windows can be evaluated, which is particularly challenging with more traditional methods. The mere act of constructing the model – using the precision that is required – can sometimes reveal errors and inconsistencies in the design documentation that are easily missed upon manual review.

Upon deciding to discontinue the LARA project, Fortum signed an agreement with Rolls-Royce regarding the modernisation of the Loviisa plant. Fortum plans to continue using model checking in the new project (ELSA), as well.

4 SIMANTICS BASED TOOLS FOR MODEL CHECKING OF I&C SOFTWARE

A major challenge in model checking of I&C software is the lack of dedicated tools. Research on the domain has focused on automatic model translations, but practically every such approach is based assuming that an open standard like IEC 61131-3 is being used, or that the function block source codes are at least available /4/. In reality, many major PLC system vendors use vendor-specific languages, and are unwilling to disclose actual implementation algorithms. Even if the source codes were available, languages such as Java or C cannot usually be translated into the input language of tools such as NuSMV. Therefore, a functional description of the elementary block types if often the only starting point, which means that manual specification is a necessity /4/.

However, VTT’s experience has shown that model checking can still be made quite efficient, despite having to manually construct the elementary function block library. Accordingly, VTT and Fortum have been developing graphical tools for the model checking of function block diagrams. The tools are based on the open source modelling and simulation platform Simantics /2/ (https://www.simantics.org/).

One of the tools (for now called MODCHK) enables the user to construct the system models in a 2D graphical view by adding function block objects in a drag-and-drop fashion, and wiring them together (Figure 2). The resulting diagrams can also be encapsulated within reusable, composite function block types. When formalising the requirements, references to exact model signals can be copied from the diagram. The model can then be transformed into the input language of NuSMV.

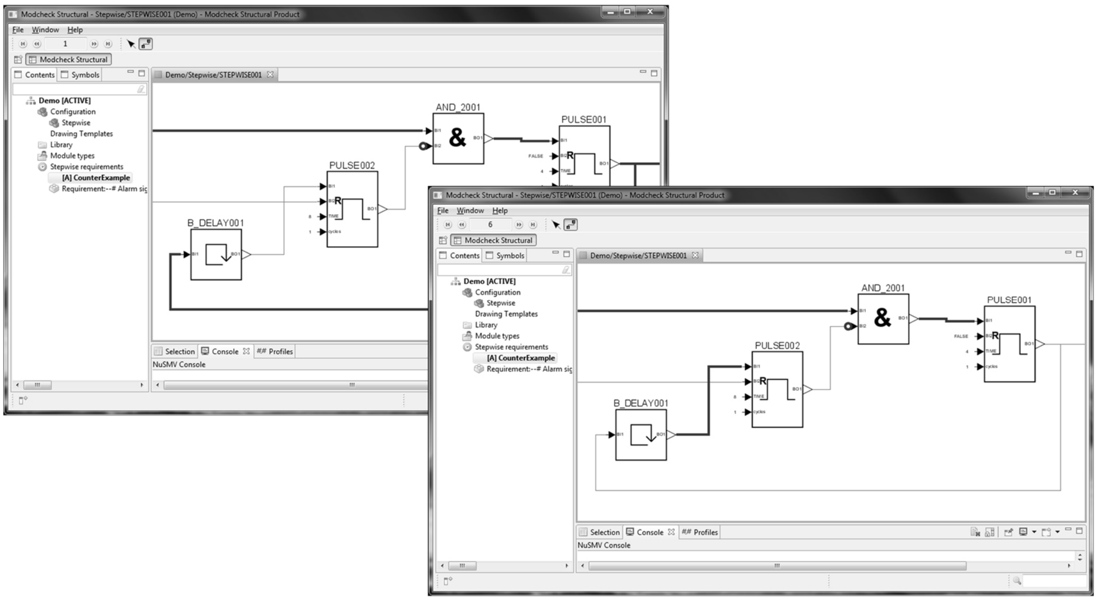

Figure 2. In the Simantics based modelling tool, animation is used to visualise counterexamples

A major advantage of MODCHK is that the counterexamples are visualised using a “living” function block diagram, an animation that can freely be played back and forth. Changes in binary signal values are shown by alternating the colour, thickness and style (dashed for invalid data) of block connection wires, while other signal values are shown using monitors attached to block gates. This intuitive presentation is often clearly superior to, e.g., trend graphs in helping the modeller find the root of the cause.

MODCHK is already used by VTT experts in practical verification work. A long term goal is to release the tool as a commercial product, most likely as part of the Apros product family (http://www.apros.fi/). Another future objective is to support automatic import from different legacy development and modelling tools. There already exists a prototype of a tool (MC-APROS) that translates the model for MODCHK directly from an Apros automation system model.

5 CONCLUSIONS

Despite obvious benefits, model checking is not yet widely used in Finnish process industry, other than in the nuclear domain. One reason is that the method is simply not generally known. Even if it were, the use of formal methods always calls for expertise, which means that there is a cost involved that many might deem too high. Still, safety is not the only motivation for strict verification, as problems with I&C systems can easily become a cost-critical issue. Hidden errors in I&C design can just as well lead to project implementation delays, or production losses, even if human health or lives were not on the line.

Model checking also calls for detailed requirement specification, which is often a challenge. Still, the properties to be verified can just as well be derived from different functional descriptions – for example user manuals. Property formalisation calls for such meticulous attention, that even an exemplar requirement specification document might not provide all the necessary details. In the work VTT has done for Fortum, participation of Fortum's experts on requirement elicitation and elaboration has been a key factor in successful application.

VTT and Fortum are developing tools that we hope will eventually bring model checking closer to the design phase of I&C systems, eventually integrated to the development tools. The earlier design issues can be identified, the better for all stakeholders.

6 REFERENCES

1. Clarke E.M. Jr., Grumberg O., Peled A.: Model Checking, The MIT Press, 1999, 314 p.

2. Karhela T., Villberg A., Niemistö H.: Open ontology based integration platform for modeling and simulation in engineering, International Journal of Modeling, Simulation, and Scientific Computing (IJMSSC), 3(2012).

3. Lahtinen J., Valkonen J., Björkman K., Frits J., Niemelä I., Heljanko K.: Model checking of safety critical software in the nuclear engineering domain, Reliability Engineering and System Safety, 105(2012), 104-113.

4. Pakonen A., Mätäsniemi T., Lahtinen J., Karhela T.: A Toolset for Model Checking of PLC Software, Proceedings of the 18th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2013), Cagliari, Italy, Sep. 10-13, 2013.

5. Pakonen A., Valkonen J., Matinaho S., Hartikainen M.: Model Checking for Licensing Support in the Finnish Nuclear Industry, International Symposium on Future I&C for Nuclear Power Plants (ISOFIC 2014), Jeju Island, Repulic of Korea, August 24-28, 2014.

6. STUK: Guide YVL B.1, Safety Design of a NPP, draft L5, 31.5.2013, STUK 2013.